UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS FÍSICAS
Departamento de Física Teórica I

ÓRDENES TOPOLÓGICOS EN INFORMACIÓN Y COMPUTACIÓN CUÁNTICAS

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Héctor Bombín Palomo

Bajo la dirección del doctor
Miguel Ángel Martín-Delgado Alcántara

Madrid, 2008

- **ISBN: 978-84-692-2772-5**

Ordenes Topológicos en Información y Computación Cuánticas

Héctor Bombín Palomo

Director de tesis: Miguel Angel Martín-Delgado Alcántara

Universidad Complutense de Madrid
2008

Agradecimientos

Me gustaría comenzar dando las gracias a mi director de tesis, no sólo por la libertad que me ha otorgado a la hora de abordar temas de investigación, sino también por su paciencia a la hora de iniciarme en las muy diversas vicisitudes de la vida investigadora. Agradezco también a familiares, amigos y compañeros el apoyo que me han prestado a lo largo de estos cuatro años. He de agradecer al Departamento de Física Teórica I de la Universidad Complutense de Madrid el espacio y material de oficina que me han cedido. Esta tesis nunca habría sido posible sin el apoyo económico del Gobierno Vasco a traves de su sistema de ayudas para la formación de investigadores, y tampoco habría sido posible realizar los viajes a congresos o las compras de libros y material informático sin la ayuda proveniente de los proyectos del Programa Nacional de Física y de la Comunidad de Madrid - Universidad Complutense.

yuku aki no
ware ni kami nashi
hotoke nashi

Shiki

Publicaciones:

- H. Bombin, M.A. Martin-Delgado, *Entanglement Distillation Protocols and Number Theory*, Phys. Rev. **A 72**, 032313 (2005), quant-ph/0503013
- H. Bombin, M.A. Martin-Delgado, *Homological Error Correction: Classical and Quantum Codes*, J. Math. Phys. **48**, 052105 (2007); quant-ph/0605094.
- H. Bombin, M.A. Martin-Delgado, *Topological Quantum Error Correction with Optimal Encoding Rate*, Phys. Rev. A **73**, 062303 (2006); quant-ph/0602063.
- H. Bombin, M. A. Martin-Delgado, *Topological Quantum Distillation*, Phys. Rev. Lett. **97**, 180501 (2006); quant-ph/0605138.
- H. Bombin, M.A. Martin-Delgado, *Topological Computation without Braiding*, Phys. Rev. Lett. **98**, 160502 (2007); quant-ph/0610024.
- H. Bombin, M.A. Martin-Delgado, *Optimal Resources for Topological 2D Stabilizer Codes: Comparative Study*, Phys. Rev. A **76**, 012305 (2007); quant-ph/0703272.
- H. Bombin, M.A. Martin-Delgado, *Quantum Measurements and Gates by Code Deformation*, arXiv: 0704.2540v1 [quant-ph].
- H. Bombin, M.A. Martin-Delgado, *Statistical Mechanical Models and Topological Color Codes*, Phys. Rev. A **77**, 042322 (2008), arXiv: 0711.0468v1 [quant-ph].
- H. Bombin, M.A. Martin-Delgado *Exact Topological Quantum Order in D=3 and Beyond: Branyons and Brane-Net Condensates*; Phys. Rev. B **75**, 075103 (2007); cond-mat/0607736.
- H. Bombin, M.A. Martin-Delgado, *An Interferometry-Free Protocol for Demonstrating Topological Order*, arXiv: 0705.0007v1 [cond-mat.str-el].
- H. Bombin, M.A. Martin-Delgado, *A Family of Non-Abelian Kitaev Models on a Lattice: Topological Confinement and Condensation*, arXiv: 0712.0190v2 [cond-mat.str-el], aceptado en Phys. Rev. B.
- H. Bombin, M.A. Martin-Delgado, *Nested Topological Order*, arXiv: 0803.4299v1 [cond-mat.str-el].

Participación en congresos como ponente presencial:

- H. Bombin, M.A. Martin-Delgado, *Quantum Distillation Protocols and Number Theory*, póster y artículo, NATO-ASI on Quantum Computation and Quantum Information Theory. Publicación: *Quantum Information Processing: From Theory to Experiment*, D.G. Angelakis, M. Christandl, A. Ekert, A. Kay and S. Kulik (editors), IOS Press, NATO Science Series: Computer and Systems Sciences, vol. 199, Mayo 2006 (pags. 34-40), Chania, Grecia, 2005.
- H. Bombin, M.A. Martin-Delgado, *Topological Clifford Group and Topological Order*, ponente invitado, Symposium on Quantum Technologies, The Cambridge-MIT Institute, Cambridge, Reino Unido, 2006.
- H. Bombin, M.A. Martin-Delgado, *D-Colexes: Topological Computation and Brane-Net Condensates*, póster y artículo, 8th Internacional Conference on Quantum Communication, Measurements and Computing, Tsukuba, Japón, 2006.
- H. Bombin, M.A. Martin-Delgado, *D-Colexes: Topological Computation and Brane-Net Condensates*, ponente, APS March Meeting, Denver, Estados Unidos, 2007.
- H. Bombin, M.A. Martin-Delgado, *Topological Color Codes*, ponente invitado, 2nd Mini Symposium on Topological Quantum Computation, Maynooth, Irlanda, 2007.
- H. Bombin, M.A. Martin-Delgado, *D-Colexes and Topological Color Codes*, póster, Informal Quantum Information Gathering, Innsbruck, Austria, 2007.
- H. Bombin, M.A. Martin-Delgado, *Quantum Measurements and Gates by Code Deformation*, ponente invitado, 3rd Mini-Symposium on Topological Phases and Quantum Computation, Innsbruck, Austria, 2007.
- H. Bombin, M.A. Martin-Delgado, *Quantum Measurements and Gates by Code Deformation*, secretario científico y ponente, Quantum Computation and Topological Orders (Cursos de Verano de El Escorial), El Escorial, España, 2007.
- H. Bombin, M.A. Martin-Delgado, *D-Colexes: Topological Computation and Brane-Net Condensates*, póster, Topological Quantum Computation 2007, Dublin, Irlanda, 2007.

- H. Bombin, M.A. Martin-Delgado, *Quantum Measurements and Gates by Code Deformation*, ponente, MPQ-MPIPKS, Garching, Alemania, 2007.
- H. Bombin, M.A. Martin-Delgado, *A family of non-Abelian Kitaev models on the lattice*, ponente invitado, 4th Mini-Symposium on Topological Quantum Computation, Castillo de Ringberg, Alemania, 2007.
- H. Bombin, M.A. Martin-Delgado, *Topological Color Codes*, ponente invitado, 1st International Conference on Quantum Error Correction, Los Angeles, Estado Unidos, 2007.
- H. Bombin, M.A. Martin-Delgado, *Topological Color Codes and Statistical Mechanical Models*, ponente invitado, Quantum Information and Graph Theory: Emerging Connections, Perimeter Institute, Waterloo, Canada, 2008.

Visitas a centros de investigación:

- Visita de dos semanas al Max-Planck-Institut Für Quantenoptik por invitación del profesor Ignacio Cirac, Septiembre de 2007, Garching, Alemania.
- Estancia de investigación bajo la tutela del profesor Xiao-Gang Wen durante los meses de Marzo a Mayo de 2008 en el Massachusetts Institute of Technology, Cambridge, Estados Unidos.

Organización de congresos:

- Secretario científico del Curso de Verano *Quantum Computation and Topological Orders*, El Escorial, España, 2007.

Indice

Introducción

1. Información y computación cuánticas

La información y computación cuánticas [1-3] comprenden el estudio de las tareas de procesamiento de información que pueden llevarse a cabo utilizando dispositivos cuánticos. El desarrollo de las tecnologías necesarias para construir dispositivos que permitan la transmisión, procesado y almacenamiento de información cuántica no es en absoluto trivial. A día de hoy, las técnicas experimentales disponibles sólo permiten realizar unas docenas de operaciones en sistemas cuánticos con unos pocos qubits, el análogo cuántico de los bits clásicos. Los trabajos que componen esta tesis [4-15] giran en torno al problema de la descoherencia, el gran obstáculo por vencer antes de que puedan concebirse sistemas de procesado de información cuántica escalables, es decir, basados en tecnologías que permitan ampliarlos a tamaños arbitrarios.

Por su naturaleza, los sistemas cuánticos están expuestos a la interacción con el entorno. Esta interacción da lugar a ruido, lo que deteriora la información cuántica almacenada en un sistema de forma inexorable. Para hacer frente a esta dificultad se ha desarrollado toda una serie de técnicas que, al menos en teoría, demuestran la viabilidad del procesado de información cuántica en presencia de un ruido moderado [16-22]. Hay dos problemas importantes sin embargo. El primero es la diferencia de varios ordenes de magnitud existente entre los niveles de ruido que presentan los dispositivos experimentales disponibles y los que se requerirían para llevar a la práctica las propuestas teóricas más sólidas. El segundo es que las cantidades de qubits que requieren estas propuestas son enormes.

Así pues, se hace evidente que no es suficiente con confiar en que los avances experimentales vayan a reducir paulatinamente el ruido y aumentar el número de qubits disponibles. Es esencial desarrollar propuestas teóricas que reduzcan todo lo posible los requerimientos para su implementación. Es con ese propósito que en esta tesis planteamos nuevas arquitecturas para la corrección de errores en las que se hace especial énfasis en aspectos tales como la localidad.

Sin embargo, un punto de vista más radical podría ser necesario. En vez de intentar corregir los errores de forma activa, una alternativa interesante es la de construir sistemas físicos en los que la información cuántica esté naturalmente protegida. En esta tesis perseguimos también esta dirección, en el ámbito de la llamada computación cuántica topológica [23, 24]. Esta forma de computación se realiza sobre sistemas que presentan lo que se conoce como orden topológico [25, 27], una forma exótica de orden en la materia que no es explicable en términos de la teoría de Landau de ruptura espontánea de la simetría [28, 29].

2. Protocolos de destilación de entrelazamiento cuántico

En el ámbito de la información cuántica, el entrelazamiento cuántico es un recurso fundamental. Es útil, por ejemplo, para mantener comunicaciones incondicionalmente seguras [30] o para teleportar información cuántica [31]. Un escenario habitual es aquel en el que existen dos sistemas separados, digamos Alice y Bob, que comparten un canal cuántico ruidoso y desean disponer de este recurso. Para ello Alice puede crear un sistema bipartito en un estado de Bell, que tiene el máximo entrelazamiento posible, y enviar una de las partes a Bob. Por desgracia, cuando Bob recibe su parte el entrelazamiento se ha degradado debido al ruido del canal.

¿Qué pueden hacer Alice y Bob para superar esta dificultad? Una alternativa son los protocolos cuánticos de destilación. En estos se considera el siguiente escenario: Alice y Bob comparten una serie de sistemas bipartitos parcialmente enredados, de un canal clásico para comunicarse y de la posibilidad de realizar cualquier manipulación local de sus respectivos subsistemas. Existen diversas estrategias que permiten a Alice y Bob obtener pares con un entrelazamiento mayor [32], [33], con la necesaria contrapartida de que su número ha de ser menor al inicial.

En el primer trabajo que constituye esta tesis [4] se estudia la destilación de sistemas bipartitos en los cuales cada constituyente es un qudit, es decir, un sistema cuántico de dimensión D, donde D es un cierto número entero. Tales sistemas habían sido poco estudiados en comparación al caso particular de los qubits, $D = 2$. Aunque resulta más complicado manejar sistemas con múltiples niveles, éstos presentan ventajas frente a los qubits. Son más resistentes al ruido, más seguros en criptografía y violan más fuertemente la localidad real.

2.1. El grupo de permutaciones locales

A cada qudit le podemos asociar una base de estados ortonormales $|k\rangle$ etiquetados con los elementos de $\mathbf{Z}_D := \mathbf{Z}/D\mathbf{Z}$, $k = 0, \ldots, D-1$. Dado un par de qudits compartidos por Alice y Bob, se denomina base computacional a aquella que tiene por elementos

$$|k\ j\rangle := |k\rangle_A \otimes |j\rangle_B, \qquad k, j \in \mathbf{Z}_D. \tag{2.1}$$

Tales estados se denominan separables y carecen de entrelazamiento cuántico alguno. Justamente al contrario, los elementos de la base de Bell tienen entrelazamiento máximo:

$$|k\ j\rangle_{\mathcal{B}} := D^{-1/2} \sum_{l \in \mathbf{Z}_D} e^{2\pi i k l/D} |l\ l-j\rangle, \qquad k, j \in \mathbf{Z}_D, \tag{2.2}$$

donde la substracción se realiza módulo D. Cuando Alice y Bob comparten n qudits, utilizamos la notación

$$|\mathbf{x}\rangle := |\mathbf{k}\,\mathbf{j}\rangle := \bigotimes_{l=1}^{n} |k_l\ j_l\rangle, \qquad |\mathbf{x}\rangle_{\mathcal{B}} := |\mathbf{k}\,\mathbf{j}\rangle_{\mathcal{B}} := \bigotimes_{l=1}^{n} |k_l\ j_l\rangle_{\mathcal{B}}, \tag{2.3}$$

donde $\mathbf{k}, \mathbf{j} \in \mathbf{Z}_D^n$ y $\mathbf{x} = (\mathbf{k}\,\mathbf{j}) \in \mathbf{Z}_D^{2n}$.

De entre todos los operadores unitarios que actúan sobre los n pares de qudits, Alice y Bob sólo pueden aplicar aquellos que pertenecen al grupo de operadores locales $\mathcal{U}_{\text{loc}}$, es decir, de la forma $U = U_{\text{A}} \otimes U_{\text{B}}$. En los protocolos de destilación de entrelazamiento cuántico resulta natural prestar especial atención a los estados diagonales en la base de Bell. Esto motiva el estudio del subgrupo $\mathcal{U}_{\text{B loc}} \subset \mathcal{U}_{\text{loc}}$ de operadores locales, unitarios y cerrado sobre el espacio de tales estados. Como demostramos en [4], la acción de cualquier $U \in \mathcal{U}_{\text{B loc}}$ produce una permutación de los estados de Bell de la forma

$$U\,|\mathbf{x}\rangle_{\mathcal{B}}\langle\mathbf{x}|\,U^\dagger = |\pi(\mathbf{x})\rangle_{\mathcal{B}}\langle\pi(\mathbf{x})|, \qquad \pi(\mathbf{x}) = M\mathbf{x} + \mathbf{a}, \tag{2.4}$$

donde $\mathbf{a} \in \mathbf{Z}_D^{2n}$ y M es una matriz con elementos en $\mathbf{Z}_D$ y simpléctica:

$$M^t\,\Omega\,M = \Omega\,, \qquad \Omega := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{2.5}$$

Denominamos grupo de permutaciones locales al grupo simpléctico afín de permutaciones (2.4). Esta caracterización de una amplia familia de operadores locales permite estudiar sistemáticamente posibles protocolos de destilación, como veremos en la siguiente sección.

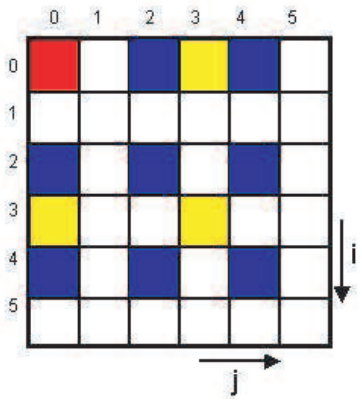


Figura 1: Representación de un estado heterotrópico genérico en el caso $D = 6$, para un solo par de qudits. Cada celda representa la probabilidad asociada al estado de Bell con índices i, j. Las celdas con el mismo color comparten probabilidad. Cada color se asocia a un divisor del seis: el uno al blanco, el dos al azul, el tres al amarillo y el seis al rojo.

Resulta útil considerar operaciones de despolarización, también conocidas como 'twirling'. En nuestro caso, estas consisten en la aplicación aleatoria de operadores unitarios locales del grupo $\mathcal{U}_{\mathrm{B\,loc}}$. Los estados resultantes, que denominamos heterotrópicos [4], sólo dependen de un número de parámetros igual al numero de divisores de D. Cuando D es primo, sólo hay dos tales números y se recuperan los comúnmente denominados estados isotrópicos [34]. La forma de tales estados aparece representada en la Fig. 1

Sumario de resultados

- Describimos el grupo de transformaciones locales que dejan invariante la base de estados de Bell. Encontramos que los elementos de este grupo producen permutaciones de los elementos de la base. Estas permutaciones forman un grupo simpléctico afín.

- Caracterizamos los estados invariantes bajo la acción de este grupo. Estos estados, que llamamos heterotrópicos, son relevantes pues son el resultado de las operaciones de despolarización.

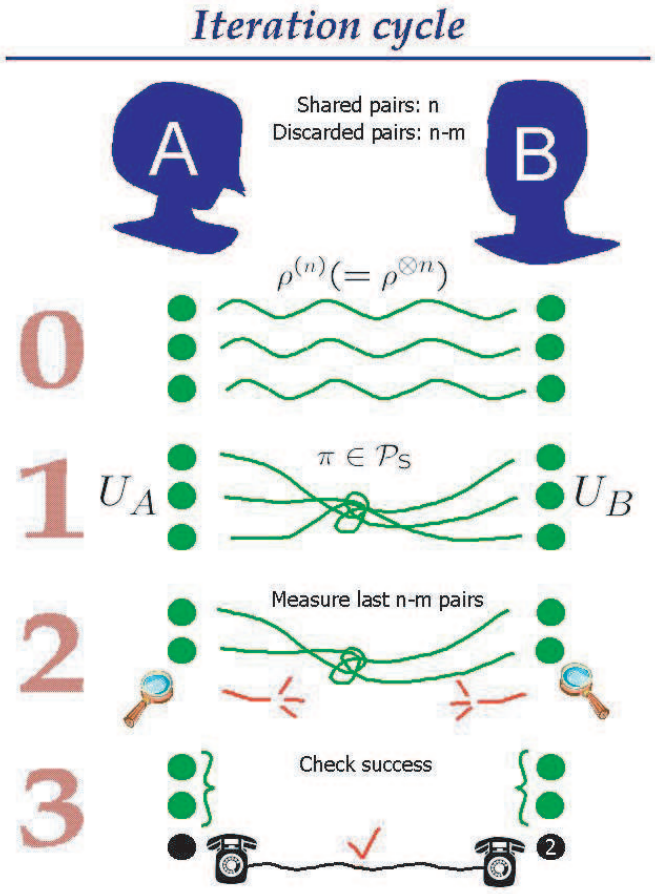


Figura 2: Representación gráfica de una iteración en los protocolos de destilación considerados.

2.2. Protocolos basados en permutaciones

En los protocolos considerados, que son iterativos, cada paso de la iteración discurre del siguiente modo, véase la Fig. 2:

1. Inicialmente, Alice y Bob comparten n pares de qudits con cierta fidelidad (probabilidad correspondiente al estado de Bell que se desea destilar).

2. Alice y Bob manipulan localmente sus sistema con objeto de obtener una de las permutaciones de los elementos de la base de Bell descritas en (2.4).

3. A continuación, miden $n-m$ pares de qudits en la base computacional (2.1).

4. Finalmente, utilizando comunicaciones clásicas comprueban si los resultados de las medidas coinciden. Si es así, se quedan con los m pares restantes, que ahora tienen una fidelidad mayor. En otro caso, los descartan.

Las relaciones recursivas asociadas a estos protocolos de destilación se pueden calcular analíticamente y resultan no depender de los elementos no diagonales. Un primer resultado que se extrae de estas relaciones es que los protocolos con $m > 1$ son inútiles para bajas fidelidades. Por otro lado, para fidelidades altas pueden mejorar mucho el rendimiento. También se observa que existen una serie de puntos fijos comunes a todos los protocolos, correspondientes a ciertas formas especialmente simples de estados heterotrópicos. Entre estos puntos fijos, de los que existe uno por cada divisor de D, se encuentra el estado puro de Bell que se desea obtener y el estado completamente ruidoso. En la práctica se observa que estos puntos fijos son además atractores. Así, cuantos mas divisores tiene D, más obstáculos se encuentran para la destilación de un estado.

Es posible efectuar una despolarización de los estados antes de cada paso, tal y como se explica en la anterior sección. Los estados despolarizados están descritos por unos pocos parámetros. De hecho, para D primo es suficiente un único parámetro, la fidelidad. Por tanto, cuando se introduce la despolarización en los protocolos estos se simplifican, permitiendo realizar un mayor número de cálculos explícitos en relación a la destilación y su optimización. Por otro lado, el rendimiento de la destilación con despolarización resulta ser muy inferior.

El estudio de los protocolos con despolarización puede verse como una generalización para qudits del protocolo de destilación original para qubits [32].

Eliminar la despolarización complica el análisis enormemente, pero permite rendimientos muchos más altos. Además, estados que no son destilables con despolarización resultan serlo cuando esta se elimina. Por ejemplo, existen estados con fidelidad inferior a $1/D$ que sólo son destilables si se suprime la despolarización. Por otro lado, y esta fue la motivación original para este estudio, en ausencia de despolarización puede generalizarse el algoritmo de amplificación de privacidad cuántico para qubits introducido en [33]. La generalización que presentamos en [4] requiere combinar dos permutaciones distintas, cuya aplicación ha de alternarse en iteraciones sucesivas del protocolo.

Finalmente, también estudiamos el problema de la destilabilidad. Para ello, dado un estado que se quiere testar, se procede a intentar destilarlo buscando a cada paso de la iteración la permutación que más incrementa la fidelidad. Para D primo, todos los estados que se sabe que son destilables, es decir, aquellos con fidelidad mayor que $\frac{1}{D}$, son destilables con este protocolo. No ocurre así en el caso de D no primo, en el cual el protocolo se comporta mucho peor.

Sumario de resultados

- Estudiamos una amplia familia de protocolos de destilación de entrelazamiento cuántico basados en el grupo de permutaciones locales.

- Consideramos protocolos de destilación con y sin despolarización.

- Para investigar los protocolos, empleamos métodos tanto analíticos como computacionales.

- Encontramos que los protocolos en los que se obtiene más de una pareja de qudits en cada iteración resultan ventajosos para fidelidades altas pero inútiles para fidelidades bajas.

- Describimos una familia de puntos fijos comunes a todos los protocolos considerados.

- Generalizamos el algoritmo de amplificación de privacidad cuántico a qudits.

- Estudiamos el problema de la destilabilidad, encontrando que con los protocolos considerados los qudits con dimensión no prima se comportan peor que los de dimensión prima.

3. Códigos cuánticos de corrección de errores

En la sección anterior hemos visto como la descoherencia en un canal puede ser combatida por medio de la destilación. Un punto débil importante de los protocolos de destilación es que presuponen que aunque el canal es ruidoso, las operaciones de destilación se pueden realizar sin errores de ningún tipo. Abandonar esta premisa es una condición indispensable si se quieren diseñar algoritmos cuánticos capaces de funcionar en dispositivos reales. Hasta la fecha no se ha construido ningún sistema cuántico en el cual la descoherencia sea un problema que se pueda obviar.

En última instancia la pregunta que se plantea es, ¿es posible realizar computaciones cuánticas de exactitud arbitraria partiendo de unos medios ruidosos? Durante mucho tiempo se creyó que la respuesta a esta cuestión era negativa. Se aducía, por ejemplo, que los errores en el medio cuántico tienen un carácter continuo que impide su corrección de forma exacta. No sin cierta sorpresa, el desarrollo de los códigos cuánticos de corrección de errores [17], [18] abrió el camino hacia la superación de esta dificultad, demostrando que la redundancia en la codificación es tan efectiva como en el caso clásico a la hora de preservar la información que atraviesa un canal ruidoso. Aún quedaban algunos escollos por superar, pues a la hora de realizar una computación cuántica ha de tenerse en cuenta que los errores están presentes en todo momento. Finalmente, con el desarrollo de la computación cuántica tolerante a fallos [19], [20], [21], [22], se puso punto final a la cuestión, por medio del conocido como teorema del umbral. Este teorema establece que, en principio, la computación cuántica es posible siempre y cuando el nivel de ruido este por debajo de un cierto umbral.

Y decimos en principio pues, por desgracia, los requisitos en términos del número de qubits necesarios y del pequeñísimo umbral de ruido que se requiere colocan los resultados del teorema demasiado lejos de la realidad experimental. Esta es la motivación que subyace en el resto de los trabajos que componen esta tesis. Sólo si los avances teóricos flexibilizan los requisitos para la computación cuántica podemos tener la esperanza de que estos serán satisfechos por algún dispositivo experimental en un futuro relativamente próximo.

Aquí daremos sólo una somera introducción a la corrección cuántica de errores, pero en [5] damos una extenso repaso a los códigos de corrección de errores tanto clásico como cuánticos. En el caso cuántico, se desarrolla en especial el tema de los denominados códigos simplécticos o estabilizadores para qudits. Cabe mencionar que la denominación de los códigos simplécticos hace referencia al papel que juega en su definición el grupo simpléctico (2.5).

3.1. Corrección cuántica de errores

Consideremos un sistema cuántico S que interacciona con un entorno incontrolable E produciéndose el consiguiente ruido. Supondremos que inicialmente E y S no están enredados cuánticamente, situación que cambia progresivamente debido a la interacción. El proceso de interacción puede describirse del siguiente modo [16]:

$$|e\rangle|s\rangle \rightarrow \sum_k |e_k\rangle M_k|s\rangle \tag{3.1}$$

donde $|e\rangle$ y $|s\rangle$ representan respectivamente los estados iniciales de entorno y sistema, los estados finales del entorno $|e_k\rangle$ no son necesariamente ortogonales ni están normalizados y los operadores M_k son unitarios. Podemos eliminar el entrelazamiento entre entorno y sistema aumentando este último con un sistema auxiliar A siempre que exista un operador unitario R sobre $S' = A \otimes S$ tal que

$$R(|a\rangle M_k|s\rangle) = |a_k\rangle|s\rangle \tag{3.2}$$

donde $|a\rangle$ representa el estado inicial del sistema auxiliar. En tal caso tenemos

$$\sum_k |e_k\rangle R(|a\rangle M_k|s\rangle) = \left(\sum_k |e_k\rangle|a_k\rangle\right)|s\rangle, \tag{3.3}$$

y los errores desaparecen. Si queremos que la estrategia funcione para un cierto subespacio $\mathcal{C}$ de S, es esencial que R funcione por igual para cualquier $|s\rangle \in \mathcal{C}$. Entonces podemos usar el subespacio $\mathcal{C}$ para almacenar información sin errores, y decimos que $\mathcal{C}$ es un código cuántico de corrección de errores.

Al igual que ocurre en el caso clásico, no podemos pretender corregir cualquier error. Debemos circunscribirnos a aquellos errores M_k que aparecen con mayor probabilidad. Introducimos por tanto un conjunto $\mathcal{E}$ de operadores sobre S, el conjunto de errores corregibles, que es un espacio lineal. La condición para que $\mathcal{C}$ corrija $\mathcal{E}$, conocida como teorema de Knill-Laflamme [16], es la siguiente. Para cualesquiera $M, N \in \mathcal{E}$ y $|\xi\rangle, |\eta\rangle \in \mathcal{C}$ tales que $\langle\xi|\eta\rangle = 0$,

$$\langle\xi|N^\dagger M|\eta\rangle = 0. \tag{3.4}$$

Puesto en palabras, la condición establece que los errores no han de mezclar estados ortogonales del código.

Los códigos normalmente se construyen como subespacios de sistemas con un cierto número n de qudits, diciéndose entonces que tienen longitud n. También suele asumirse que los errores más probables son aquellos con soporte en un número menor de estos qudits. Una noción importante es

entonces la de distancia del código. Decimos que $\mathcal{C}$ detecta un error N si para cualquier $|\xi\rangle, |\eta\rangle \in \mathcal{C}$ tenemos

$$\langle \xi | N | \eta \rangle = c(N) \, \langle \xi | \eta \rangle \tag{3.5}$$

para algún $c(N) \in \mathbf{C}$. Si un código detecta cualquier error con soporte en como mucho d qudits, decimos que tiene distancia d. Un código de distancia $d = 2t+1$ puede corregir errores con soporte en hasta t qudits. Se suele usar la notación $[[n, k, d]]$ para indicar que un código tiene longitud n, dimensión D^k y distancia d. Aquí D hace referencia a la dimensión de los qudits empleados, y se dice que el código codifica k qudits.

3.2. Códigos estabilizadores

Una familia de códigos cuánticos particularmente exitosa es la de los códigos estabilizadores [35], [36], que pasamos a describir ahora en el caso particular en que se emplean qubits. Puede encontrarse una descripción más detallada y que incluye el caso más general de los qudits en [5].

La construcción de los códigos estabilizadores gira en torno al denominado grupo de operadores de Pauli, $\mathcal{P}$. Fijado un número de qubits n, éste es el grupo generado por los operadores de Pauli X y Z que actúan en un sólo qubit

$$X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{3.6}$$

Un código estabilizador de longitud n se describe como aquel subespacio $\mathcal{C}$ estabilizado por un subgrupo abeliano $\mathcal{S} \subset \mathcal{P}$ que no ha de contener como elemento a -1. Si $\mathcal{S}$ tiene $n-k$ generadores independientes S_i, $\mathcal{C}$ codifica k qubits. Los estados codificados $|\psi\rangle \in \mathcal{C}$ se caracterizan mediante las condiciones

$$S_i |\psi\rangle = |\psi\rangle, \qquad i = 1, \ldots, n-k. \tag{3.7}$$

A la hora de corregir los errores que se han producido en un código estabilizador, lo que se hace es medir estos generadores. Esto tiene una doble función. Por un lado, de este modo se proyecta el estado a un cierto subespacio, lo que limita los errores a corregir a un cierto subconjunto de operadores de Pauli. En segundo lugar, los resultados de las medidas, que se conocen como síndromes, son suficientes para determinar el error que se ha producido y proceder a cancelarlo.

Una noción importante a la hora de analizar los códigos estabilizadores es la del normalizador $\mathcal{N}$ de $\mathcal{S}$. Este es el subgrupo $\mathcal{N} \subset \mathcal{P}$ que contiene aquellos elementos que conmutan con todos los estabilizadores en $\mathcal{S}$. La distancia de un código estabilizador corresponde al menor soporte de entre todos los

elementos de $\mathcal{N} - \mathcal{S}$. Siempre pueden elegirse operadores $X_i, Z_i \in \mathcal{N}$, $i = 1, \ldots, k$ tales que

$$[X_i, X_j] = 0, \qquad [Z_i, Z_j] = 0, \qquad X_i Z_j = (-1)^{\delta_{i,j}} X_j Z_i. \tag{3.8}$$

Estos generan el grupo de operadores de Pauli codificados, esto es, los operadores de Pauli para los qubits codificados, también conocidos como qubits lógicos.

3.3. Puertas transversales

Para poder realizar computaciones con qubits codificados, necesitamos saber cómo aplicar puertas lógicas a éstos. Esto naturalmente siempre es posible, pero si pretendemos tener éxito en la batalla contra los errores, se hace indispensable que las puertas se puedan aplicar de manera rápida y, en la medida de lo posible, de tal forma que los errores no se dispersen de unos qubits a otros. Con estas consideraciones en mente, la posibilidad de aplicar puertas de forma transversal resulta de enorme interés.

Por una puerta transversal entendemos un operador unitario que es un producto tensorial de operadores de un solo qubit. Esto al menos en el caso de que se aplique a un sólo código. Generalmente cada código codifica un solo qubit, con lo que la puerta transversal descrita es unaria, es decir, actúa sobre un sólo qubit codificado. Con mayor generalidad, también es posible aplicar transversalmente puertas n-arias. En ese caso, la puerta transversal será un producto tensorial de operadores unitarios actuando sobre n qubits, cada uno en posiciones equivalentes de n códigos iguales.

4. Códigos topológicos

A la hora de valorar la bondad de un código de corrección de errores, pueden considerarse aspectos tales como que la longitud sea pequeña y la distancia y el número de qubits codificados sean grandes. Pero existen otros aspectos a tener en cuenta, por ejemplo la simplicidad de los generadores del grupo estabilizador. Cuanto más complicados son estos, más lo son también las operaciones necesarias para medirlos. Este problema se vuelve muy relevante cuando tomamos en cuenta el hecho de que el proceso de medición es en si mismo susceptible a tener fallos, y por ello queremos mantenerlo lo más rápido y sencillo posible para que sea verdaderamente efectivo.

En este sentido, un aspecto muy interesante de los códigos es su localidad. De entre los dispositivos cuánticos que se proponen como aspirantes a formar parte de un futuro ordenador cuántico, muchos están limitados precisamente por el hecho de que sus componentes sólo pueden interactuar localmente.

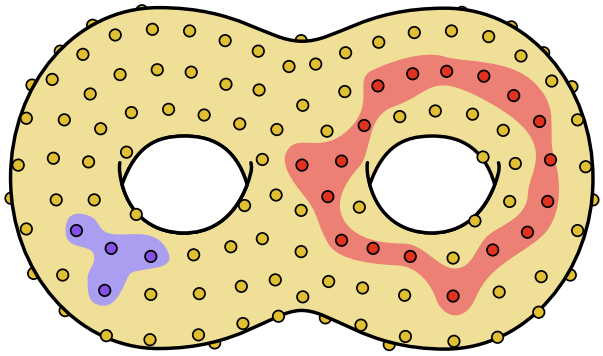


Figura 3: En los códigos topológicos, los qubits (representados aquí como pequeños círculos) se sitúan en una variedad dada, en este caso una superficie de genus 2. Su principal característica es el contraste entre el carácter local de los generadores del estabilizador (azul) y el global de los errores no detectables (rojo).

Aquí juega también un papel importante la dimensionalidad, pues cuando las interacciones son locales no es lo mismo que el sistema tenga una, dos o tres dimensiones.

Los códigos topológicos [37] que describimos en esta sección y que estudiamos en [5], [6], [7], [8], [9] y [11] destacan precisamente por lo localizado de los generadores del estabilizador. Los qubits se distribuyen en una superficie o algún espacio de dimensión mayor. Independiente del tamaño total del código, localmente éste siempre tiene el mismo aspecto. Así, por ejemplo, las medidas necesarias para corregir el código siempre tienen la misma dificultad, pues involucran el mismo número de qubits. Como veremos, los operadores indetectables han de tener un soporte topológicamente no trivial, es decir, tienen siempre un carácter global. De este modo, la distancia de los códigos topológicos crece con el tamaño geométrico de estos. Así, pueden tener una distancia arbitrariamente grande mientras que los generadores actúan sobre un cierto número limitado de qubits. Estas ideas están representadas en la Fig. 3.

4.1. Códigos homológicos

En [5] y [6] investigamos diversos aspectos de los códigos homológicos, también conocidos como códigos de superficie o códigos tóricos. Estos códigos fueron introducidos originalmente por Kitaev en [37], y los aspectos de su corrección de errores profusamente estudiados en [38].

Un código homológico se construye a partir de una red embutida en una

cierta superficie. A cada arista de la red se la identifica con un qubit, siendo por tanto la longitud n de un código homológico igual al número de aristas de la red. Los generadores del estabilizador están asociados a caras y vértices. A cada cara f se le asocia un operador X_f, y a cada vértice un operador Z_v. La forma de estos operadores, en los ejemplos de la Fig. 4 es

$$X_f = X_1 X_2 X_3 X_4, \qquad Z_v = Z_5 Z_6 Z_7. \tag{4.1}$$

La estructura de los estados del código es fácil de entender en términos de la homología de curvas en una superficie, que repasamos de forma autocontenida en [5]. Cada elemento de la base computacional $|x_1 x_2 \cdots x_n\rangle$ puede asociarse a un conjunto γ de aristas, aquellas aristas i para las que $x_i = 1$. Denotamos pues los elementos de la base computacional como $|\gamma\rangle$. Observamos entonces que $Z_v|\gamma\rangle = |\gamma\rangle$ se satisface si y sólo si γ tiene un número par de aristas incidentes en v. Si γ satisface esta condición para todo v, forma lo que en términos homológicos se denomina un 1-ciclo, es decir, una colección de curvas cerradas. Tomando en consideración también las condiciones impuestas por los generadores X_f se encuentra que una base para el código puede formarse con elementos de la forma

$$|\Gamma\rangle = \sum_{\gamma \in \Gamma} |\gamma\rangle, \tag{4.2}$$

donde Γ es el conjunto de todos los 1-ciclos homológicamente equivalentes a uno dado. Dos colecciones de curvas cerradas son homológicamente equivalentes cuando puede obtenerse una de la otra a través de transformaciones locales, lo que incluye deformaciones y la adición o substracción de curvas que formen la frontera de un área dada.

Como consecuencia de lo expuesto, el número de qubits k codificados por el código depende sólo de la topología de la superficie. En particular toma la forma $k = 2 - \chi$, siendo χ la característica de Euler de la superficie

$$\chi = V - E + F, \tag{4.3}$$

donde V, E y F son respectivamente el número de vértices, aristas y caras de la superficie. Los operadores de Pauli codificados (3.8) tienen también una interpretación geométrica. En particular, pueden asociarse a los 1-ciclos y 1-cociclos de la superficie. Estos 1-cociclos son 1-ciclos en la red dual.

En [6] probamos la existencia de códigos homológicos que saturan la máxima tasa k/n obtenible. Utilizando construcciones de la teoría de grafos, se presentan realizaciones explicitas de estos códigos en superficies de genus arbitrario. Encontramos también una clase óptima de códigos regulares en

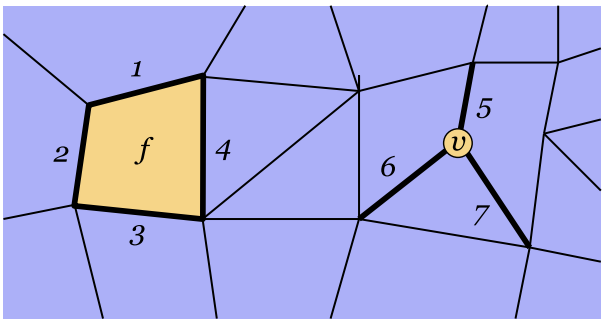


Figura 4: Los códigos homológicos se construyen a partir de una red en una superficie. Cada arista corresponde a un qubit, y los generadores del estabilizador están asociados a caras y vértices.

el toro. Se introducen además códigos en el plano, más aptos para realizaciones experimentales, donde la topología no trivial se obtiene mediante la introducción de fronteras abiertas y cerradas.

En [5] generalizamos los códigos homológicos al caso de los qudits, encontrando que tal generalización sólo es posible para superficies orientables. Consideramos también códigos homológicos en objetos más generales que las superficies, lo que permite dar una perspectiva geométrica a códigos previamente conocidos. Finalmente, introducimos la contrapartida clásica de los códigos homológicos, encontrando una familia que satura el conocido como límite de Hamming.

Sumario de resultados

- Introducimos versiones clásicas de los códigos homológicos que saturan el límite de Hamming.
- Generalizamos los códigos homológicos a complejos bidimensionales y al caso de los qudits.
- Encontramos que las superficies han de ser orientables para qudits de dimensión mayor a dos.
- Damos una perspectiva geométrica a códigos previamente conocidos.
- Construimos una familia de códigos homológicos que satura la tasa máxima k/n.
- Encontramos una clase óptima de códigos regulares en el toro.

- Introducimos códigos homológicos planos utilizando el concepto de homología relativa.

4.2. Códigos de color

Como se mencionó en la sección 3.3, las propiedades de transversalidad de los códigos son fundamentales a la hora de evaluar su utilidad con vistas a desarrollar computaciones cuánticas tolerantes a fallos. En este sentido los códigos homológicos resultan un tanto insuficientes, pues sólo permiten la implementación transversal de las puertas X, Z y la conocida como CNot (negación controlada), que es una puerta lógica de dos qubits que en la base computacional toma la forma

$$\Lambda = \begin{bmatrix} 1 & 0 \\ 0 & X \end{bmatrix}, \tag{4.4}$$

donde cada elemento de la matriz es una caja 2×2. Es con el ánimo de vencer esta dificultad que en [7] introducimos una nueva clase de códigos topológicos que llamamos códigos de color. Estos permiten la implementación transversal de otras dos puertas lógicas unarias, denominadas Hadamard y $\pi/4$, que en la base computacional toman la forma

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad K = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \tag{4.5}$$

Ocurre que los operadores (4.4, 4.5) generan el denominado grupo de Clifford. Este grupo puede definirse como aquel compuesto por los operadores que dejan invariante bajo conjugación el grupo de Pauli. Tiene una gran importancia en el ámbito de la información cuántica, pues es suficiente para realizar protocolos tales como los de teleportación o destilación. Así, vemos que utilizando los códigos de color, que ahora pasamos a describir, pueden realizarse de forma tolerante a fallos muchas tareas importantes. Resulta especialmente interesante la posibilidad de destilar, pues gracias a esto es posible realizar computaciones universales [39].

Los códigos de color se construyen también a partir de una red embutida en una cierta superficie pero, a diferencia de los códigos homológicos, esta red ha de verificar ciertas propiedades. En particular, la red debe ser trivalente y sus caras 3-coloreables. Es decir, deben incidir exactamente tres aristas en cada vértice y ha de ser posible colorear sus caras con tres colores de tal modo que caras adyacentes no compartan color. Un ejemplo puede verse en la Fig. 5. La segunda diferencia es que ahora hemos de asociar los qubits que componen el código no a las aristas, sino a los vértices de la red. Finalmente,

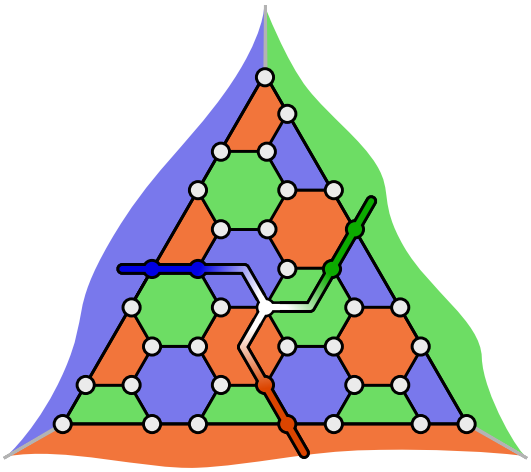


Figura 5: Un código de color triangular [[37,1,7]]. Los qubits se sitúan en los vértices de la red. Las tres cuerdas coloreadas que confluyen en el centro representan el soporte de un error no detectable o, alternativamente, de un operador de Pauli codificado. Cada uno de los bordes del triangulo esta coloreado de forma diferente. Este color es el que correspondería a una gran cara que ocupara su lugar en la red.

los generadores del grupo estabilizador están asociados a las caras, habiendo dos, Z_f y X_f, por cada cara f. Estos son, respectivamente, productos de los operadores Z y X correspondientes a los vértices de f. Como resultado de estás definiciones, puede verificarse [7] que los códigos de color codifican el doble de qubits en una superficie dada:

$$k = 4 - 2\chi. \tag{4.6}$$

Una característica que hace cualitativamente distintos a los códigos de color de los de superficie es la realización geométrica de los operadores de Pauli codificados. Ya hemos mencionado que en el caso de los códigos de superficie estos toman la forma de cuerdas cerradas sobre la superficie. El nuevo elemento que aparece en los códigos de color es que estas cuerdas pueden tener ramificaciones. En particular, pueden definirse cuerdas de tres tipos, una por cada color, de tal modo que tres cuerdas de diferentes colores pueden confluir, como indica la Fig. 5.

En cierto sentido, los códigos de color son también homológicos, dado que pueden ser descritos en términos de una cierta homología. Esta homología no es, sin embargo, una habitual. Hemos visto que en el caso de los códigos de Kitaev la homología relevante es la de las curvas en una superficie. Esta homología se obtiene a partir de un par de operadores borde ∂, que trans-

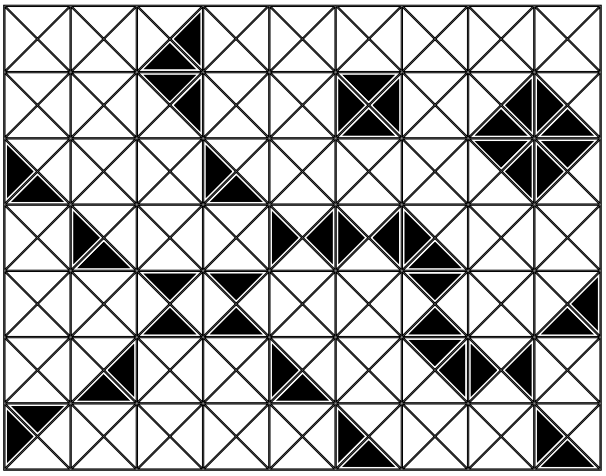


Figura 6: Se muestra la red dual de un cierto código de color junto con un ejemplo de ciclo de triángulos, es decir, de conjunto de triángulos tal que su borde es nulo. Ha de entenderse que la red continúa más allá de la figura. Los dos conjuntos de triángulos arriba a la derecha son ejemplos de bordes, pues cada uno de ellos se obtiene como el borde del vértice en su centro.

forman las caras en sus aristas y las aristas en sus extremos. En el caso de los códigos de color los operadores borde relevantes se visualizan mejor en la red dual, compuesta enteramente por caras triangulares. En particular, ∂ transforma los vértices en sus triángulos adyacentes y los triángulos en sus vértices. Un ejemplo de ciclo de triángulos se muestra en la Fig. 6. Los grupos de homología de triángulos obtenidos de este modo resultan contener dos copias del grupo de homología para las curvas en una superficie. De ahí que los códigos de color codifiquen el doble de qubits.

En [9] realizamos una comparativa de los códigos de superficie y los de color, tanto en términos de su construcción como en términos de su rendimiento. Además de discutir las diferencias ya mencionadas, definimos y comparamos la tasa topológica de corrección de errores $C := n/d^2$ para códigos de superficie C_s y códigos de color C_c en varios casos. En particular, encontramos que en el toro valores típicos son $C_s = 2$ y $C_c = 3/2$, valores que pueden optimizarse para dar $C_s = 1$ y $C_c = 9/8$. Para códigos en el plano el valor típico es $C = 2$, valor que puede optimizarse para dar $C_s = 1$ y $C_c = 3/4$. Vemos que a pesar de que los códigos de color codifican más qubits, necesitan menos qubits para hacerlo.

Sumario de resultados

- Introducimos una nueva clase de códigos topológicos bidimensionales, los códigos de color.
- Los códigos de color se fundamentan en cierta homología de triángulos que no forma parte de las habitualmente estudiadas.
- Los códigos de color tienen propiedades de transversalidad superiores a las de los códigos de superficie, permitiendo la implementación transversal del grupo de Clifford. Este grupo de operadores es fundamental en información cuántica. En particular, puede utilizarse para destilar.
- Dada una cierta topología, los códigos de color codifican el doble de qubits que los códigos de superficie.
- Describimos clases optimas de códigos de color regulares, mostrando que los códigos de color requieren un menor número de qubits físicos.

4.3. Computación universal

En la sección precedente hemos expuesto que los códigos de color pueden implementar un conjunto no universal de puertas transversalmente, lo que debido a sus buenas propiedades permite hacer destilaciones y a través de éstas realizar computaciones genéricas. Sin embargo, la destilación resulta muy desventajosa en términos de recursos, y exige umbrales de ruido más bajos que los que son naturales al código en cuestión. Idealmente, querríamos disponer de un código que, además de tener buenas propiedades de localidad, permitiera la implementación transversal de un conjunto universal de puertas lógicas, es decir, un conjunto que permita aproximar con precisión arbitraria cualquier operación unitaria en los qubits codificados. Por ejemplo, el conjunto $\{H, K^{1/2}, \Lambda\}$ es un conjunto universal [40]. Desafortunadamente, no existen códigos estabilizadores en los que sea posible implementar transversalmente un conjunto universal de puertas, ni topológicos ni de ningún otro tipo, como ha sido probado recientemente [41].

Sin embargo, las cosas no son tan malas, pues lo que sí es posible es construir códigos en los que las puertas $K^{1/2}$ y Λ y las mediciones en las bases X, Y, Z son transversales. La prueba de que este conjunto de operaciones es universal puede encontrarse en [42], donde se ofrecen unos códigos, denominados códigos de Reed-Muller cuánticos, que las implementan transversalmente. Códigos semejantes son, sin embargo, extremadamente raros, con lo que podría pensarse que no existen entre ellos códigos con buenas propiedades locales.

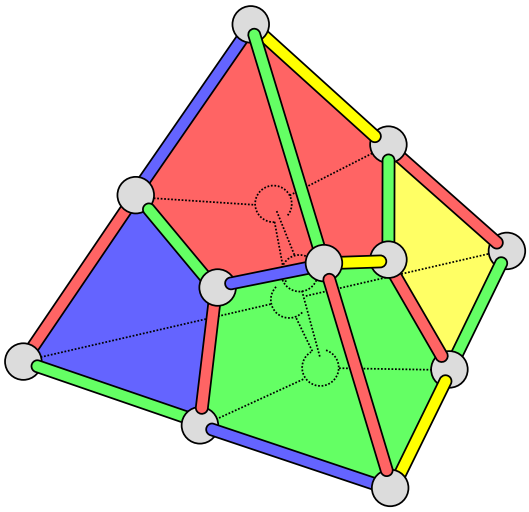


Figura 7: El código tetraédrico de color más pequeño que existe, [[15,1,3]]. Los qubits se sitúan en los vértices de la red, en la cual las celdas son de cuatro colores. Cada una de las cuatro caras del tetraedro lleva asociado un color, correspondiente a la celda que iría en ese lugar si la red no terminara ahí.

Sorprendentemente, como mostramos en [8], sí existen códigos topológicos con las buenas propiedades transversales de los códigos Reed-Muller. En particular, tales códigos resultan de la generalización de los códigos de color a tres dimensiones. Estos se construyen a partir de una red tridimensional tetravalente en la que las celdas han de ser 4-coloreables, véase un ejemplo en la Fig. 7. De nuevo los qubits se sitúan en los vértices de la red, pero ahora los generadores del estabilizador van asociados a dos tipos de objetos; a cada cara f se le asocia un operador X_f, y a cada celda c un operador Z_c. En los códigos de color bidimensionales los operadores de Pauli codificados estaban asociados a redes de cuerdas. Esto sigue siendo cierto en tres dimensiones para los que se forman como productos de operadores X, pero los que se forman con operadores Z van asociados ahora a redes de membranas. Tanto las cuerdas como las membranas pueden aparecer en distintos colores o combinaciones de colores, siendo estas etiquetas las que rigen los puntos o curvas de ramificación que pueden existir, véase la Fig. 8.

Sumario de resultados

- Generalizamos los códigos de color a tres dimensiones.
- Encontramos que las propiedades de transversalidad de los códigos de

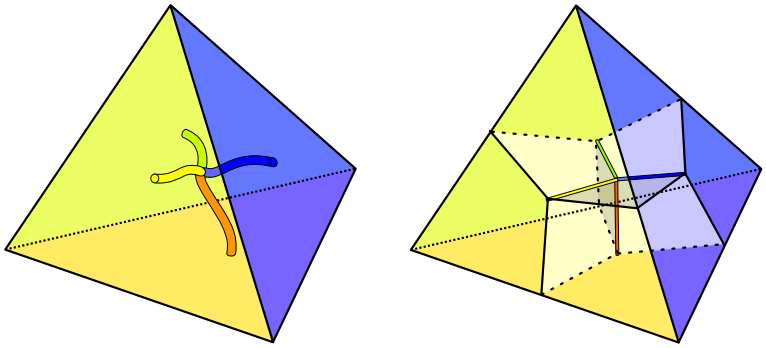


Figura 8: En los códigos de color tridimensionales los operadores de Pauli codificados están relacionados a dos tipos de objetos geométricos, cuerdas y membranas. Las cuerdas pueden presentar puntos de ramificación, y lo mismo es cierto para las membranas que pueden ramificarse a lo largo de curvas. En estas figuras se representa el aspecto geométrico de los operadores de Pauli codificados en un código tetrahédrico.

color tridimensionales son las mismas que las de los códigos de Reed-Muller cuánticos. Es decir, permiten la implementación transversal de ciertas puertas lógicas y medidas que son suficientes para la computación universal.

4.4. Puertas lógicas y mediciones vía deformaciones

En las secciones precedentes hemos expuesto diversos códigos topológicos y discutido sus propiedades de transversalidad. Aunque las puertas transversales son enormemente ventajosas, existen razones para buscar alternativas que flexibilicen el uso de un código dado. En [10] introducimos la deformación de códigos que, cuando se aplica a los códigos topológicos, tiene la facultad de reducir en una las dimensiones del sistema que se requiere para la implementación física. Esto es especialmente relevante en el caso de los códigos de color tridimensionales, donde se requieren cuatro dimensiones para realizar localmente la puerta CNot transversal.

La motivación para el trabajo mencionado se encuentra en [38], donde se propone una arquitectura para un ordenador cuántico basado en una red tridimensional dividida en capas horizontales. Cada una de las capas corresponde a un código homológico que codifica un único qubit, de tal modo que se pueden realizar CNots transversales localmente entre capas contiguas. Aunque esta arquitectura adolece de algunas serias dificultades debido a las malas propiedades de transversalidad de los código homológicos, no nos ocuparemos aquí de esto, máxime cuando tales problemas desaparecen al considerar

códigos de color. Lo que nos interesa es entender cómo es posible construir una variante de esta arquitectura que utilice una sola capa bidimensional.

La cuestión de codificar múltiples qubits en una sola capa de código homológico no plantea dificultades. De hecho, puede hacerse de múltiples formas, ya que para complicar la topología del plano podemos introducir tanto bordes cerrados como abiertos, estos pueden aparecer como agujeros o como modificaciones al borde exterior, etc. La verdadera dificultad radica en cómo recuperar la puerta CNot, que ya no puede ser de ningún modo transversal puesto que en la arquitectura tridimensional ésta se fundamenta en la disposición contigua de diferentes capas.

Como exponemos en [10], la solución radica en aplicar deformaciones al código para recuperar la CNot. Originalmente las deformaciones fueron introducidas en [38] como una manera para hacer crecer el número de qubits físicos en un código dado. Pero la potencialidad de las deformaciones es mucho más grande, pues como se muestra en [10] pueden utilizarse para aplicar puertas lógicas, inicializar qubits codificados y realizar mediciones no destructivas, todo permaneciendo en todo momento bajo la protección topológica que ofrece el código.

El efecto de las deformaciones puede entenderse de una forma completamente geométrica. Consideremos para fijar ideas que trabajamos con códigos de superficie. Empezamos por analizar las deformaciones continúas, en las que la topología de la superficie no cambia. Recordemos que los operadores de Pauli codificados están asociados a objetos geométricos, en particular a cuerdas. Estas cuerdas se deforman junto con la superficie, como mostramos en la Fig. 9. Si la deformación es tal que al final deja el código con la misma forma que tenía en un principio, entonces da lugar a una aplicación continúa de la superficie sobre si misma. Esta aplicación nos dice como han evolucionado las cuerdas con la deformación. Ahora bien, la evolución de los operadores de Pauli codificados es suficiente para determinar, excepto por una fase global, la evolución unitaria de los qubits codificados. Vemos pues que la geometría de la deformación determina la puerta lógica aplicada. En [10] mostramos en detalle como es posible aplicar CNots a los qubits codificados en códigos de superficie mediante deformaciones.

También es posible aplicar deformaciones discontinuas. Tales deformaciones alteran la topología del código, y por tanto el número de qubits codificados. Como analizamos en [10], las deformaciones discontinuas llevan emparejadas inicializaciones y mediciones de qubits codificados. En particular, en el caso de los códigos de superficie, cortar a lo largo de una cuerda equivale a medir su operador asociado, y pegar dos bordes inicializa con autovalor uno el operador asociado a la cuerda que corre a lo largo de la línea de unión.

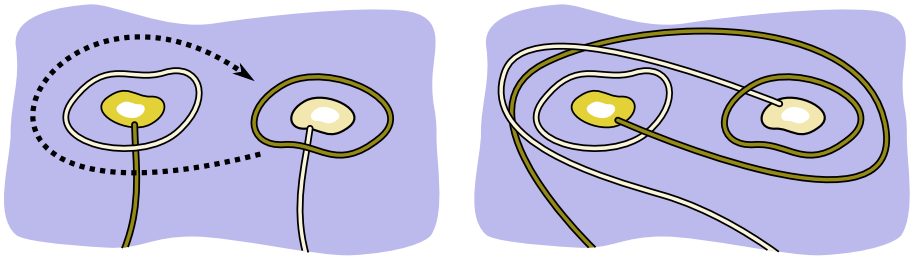


Figura 9: Ilustración del efecto de las deformaciones en un código de superficie. El código de superficie corresponde al área azul, en la que se han practicado agujeros que aparecen coloreados en dos tonos. Estos tonos distinguen entre dos tipos de borde, que en términos homológicos corresponden a fronteras abiertas y cerradas. Las cuerdas corresponden a operadores de Pauli codificados. A la izquierda se muestra el estado inicial, y a la derecha el estado final después de arrastrar uno de los agujeros en torno al otro. El efecto total equivale a una puerta CNot [10].

Sumario de resultados

- Introducimos las deformaciones en códigos estabilizadores como una alternativa a las operaciones transversales. Esto es especialmente natural en los códigos topológicos, pues las deformaciones tienen una interpretación puramente geométrica.

- Mostramos cómo por medio de las deformaciones es posible inicializar, transformar y medir los qubits codificados en un código.

- Consideramos en detalle los códigos de superficie, donde vemos que las puertas CNot se pueden implementar mediante deformaciones. Esto permite trasladar arquitecturas que previamente requerían tres dimensiones a una sola capa bidimensional de código.

4.5. Conexiones con la mecánica estadística

En [43], [44] se establece una conexión entre los códigos de superficie y los modelos clásicos de Ising bidimensionales. El interés de tales conexiones estriba en la posibilidad de establecer nuevos resultados y desarrollar nuevas herramientas a través de ellas. En [11] derivamos una conexión análoga entre los códigos de color y ciertos modelos clásicos de Ising bidimensionales a tres cuerpos. Dado un código de color, que supondremos que no codifica ningún qubit, el modelo asociado se construye en la red dual a la del código, véase la Fig. 10. En cada vértice i de esta red se situa un spin clásico $\sigma_i = \pm 1$. El

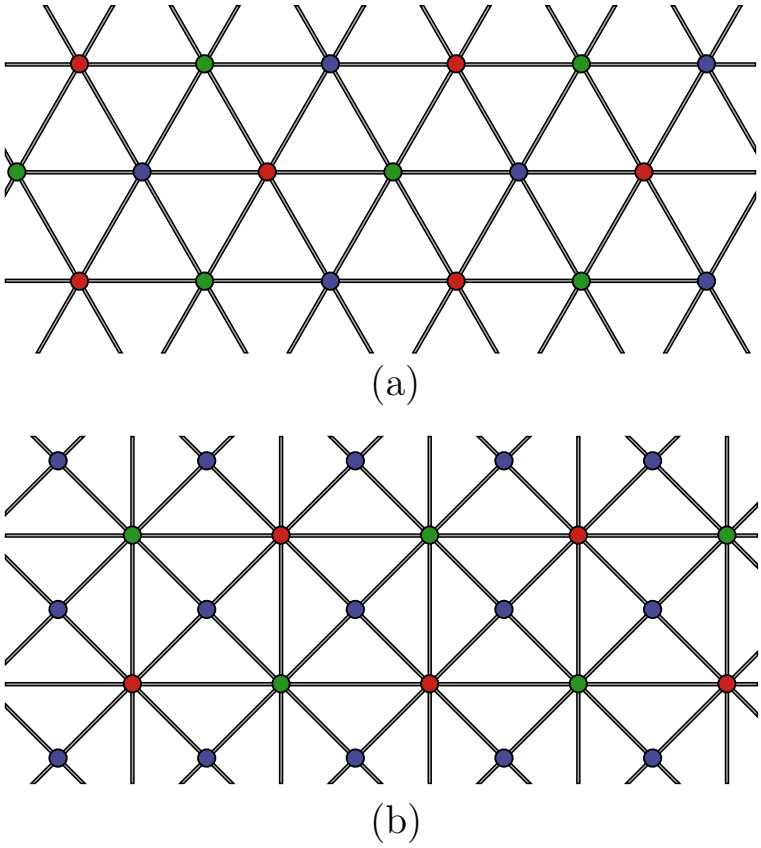


Figura 10: (Color online) Dos instancias de redes duales a la red de un código de color, que tienen por tanto triángulos por caras y vértices 3-coloreables. La red triangular (a) es dual a la red hexagonal. La red Union Jack (b) es dual a la red cuadrado-octogonal o 4-8.

Hamiltoniano clásico del modelo es

$$\mathcal{H} := -\sum_{\langle i,j,k\rangle} J_{ijk}\sigma_i\sigma_j\sigma_k, \tag{4.7}$$

donde la suma se extiende sobre los triángulos de la red y $\mathbf{J}$ es el conjunto de los acoplos a tres cuerpos J_{ijk} en los triángulos. La conexión mencionada relaciona la función de partición de este sistema con el siguiente producto escalar

$$\mathcal{Z}(\beta,\mathbf{J}) := \sum_{\{\sigma\}} \mathrm{e}^{-\beta\mathcal{H}} = C\,\langle\Psi_{\mathrm{c}}|\Phi(\beta,\mathbf{J})\rangle, \tag{4.8}$$

donde $|\Psi_c\rangle$ es el código de color, C es una constante y $|\Phi(\beta, \mathbf{J})\rangle$ es el estado producto:

$$|\Phi(\beta, \mathbf{J})\rangle := \bigotimes_{\langle i,j,k\rangle} [\cosh(\beta J_{ijk}|0\rangle + \sinh(\beta J_{ijk}|1\rangle]. \tag{4.9}$$

Entre las observaciones que se derivan de (4.9) cabe citar la siguiente. Para acoplos uniformes estos modelos a tres cuerpos pueden resolverse tanto en la red triangular como en la Union Jack, ambas representadas en la Fig. 10, resultando que las soluciones pertenecen a distintas clases de universalidad. Al mismo tiempo, los códigos de color correspondientes tienen propiedades de transversalidad diferentes. Esto sugiere algún tipo de conexión entre ambos hechos, por ejemplo la existencia de alguna simetría oculta.

Es posible generalizar (4.9) al caso con campo magnético externo aplicado

$$\mathcal{H} := -\sum_{\langle i,j,k\rangle} J_{ijk}\sigma_i\sigma_j\sigma_k - \sum_i h_i\sigma_i. \tag{4.10}$$

Para ello ya no es suficiente con los códigos de color. En su lugar se requiere lo que se denomina un estado de racimo ('cluster') [45], en particular uno del que se puede recuperar el código de color mediante la medición en la base Z de algunos de sus qubits. En realidad la descripción de este estado es en si mismo uno de los resultados interesantes de [11], pues los estados de racimo se pueden generar mediante interacciones tipo Ising y eso abre la vía a una implementación experimental de los códigos de color.

Sumario de resultados

- Derivamos una conexión entre los códigos de color y ciertos modelos estadísticos bidimensionales clásicos de Ising a tres cuerpos.

- Los resultados sugieren algún tipo de relación entre la aparición de clases de universalidad diferentes en distintas redes en el modelo clásico, y las distintas capacidades transversales de los códigos de color correspondientes.

- Explicamos como puede obtenerse un código de color a partir de ciertos estados de racimo.

- Al aplicar la conexión con modelos estadísticos, estos estados de racimo se relacionan con modelos de Ising a tres cuerpos que incluyen un campo magnético externo.

5. Orden topológico

Aunque hemos introducido ya ampliamente la idea de código topológico y descrito varios ejemplos, hasta ahora hemos obviado intencionadamente un punto importante: la motivación original que condujo a Kitaev a la introducción de los códigos tóricos [37]. Como hemos visto, la plausibilidad de la computación cuántica depende en buena medida del desarrollo de métodos de corrección de errores lo suficientemente efectivos. Asimismo, en los albores de la computación clásica se desarrollaron también semejantes discusiones en relación a la posibilidad de realizar computaciones en presencia de ruido. Sin embargo, si estudiamos el diseño de un microprocesador moderno no encontraremos ni rastro de sistemas para hacer frente a posibles errores. La razón de esta ausencia ha de buscarse en el hecho de que es posible construirlos de tal manera que los errores son virtualmente inexistentes. ¿Por qué? Porque los dispositivos físicos en los que se basan son intrínsecamente robustos frente al ruido del entorno.

Motivado por el escenario clásico, Kitaev buscaba una memoria cuántica que fuera intrínsicamente robusta, un análogo cuántico de los discos duros. Es con esa idea en mente que introduce los códigos tóricos o de superficie que ya hemos discutido. No hemos mencionado sin embargo el siguiente Hamiltoniano cuántico, propuesto por él,

$$\mathcal{H} = -\sum_{v} Z_v - \sum_{f} X_f, \tag{5.1}$$

donde el sistema cuántico es el de un determinado código de superficie, con la correspondiente red y los qubits en sus aristas, y las sumas se extienden sobre todos los vértices y caras del sistema, correspondiendo los términos del Hamiltoniano con los generadores locales del estabilizador discutidos en la sección 4.1. Este Hamiltoniano es exactamente soluble. El estado fundamental se corresponde con el código de superficie, lo que significa que la degeneración de éste tiene un origen topológico. A las excitaciones, que están localizadas en vértices y caras y poseen un 'gap' finito, se les puede asociar una carga topológica. Esta propiedad es una carga porque, dada una cierta región del sistema, no es posible variar su carga sin intercambiarla con el exterior, y es topológica porque tal es la naturaleza de la interacción que se produce entre las excitaciones. Por ejemplo, si llevamos una excitación de vértice alrededor de una excitación de cara el sistema recoge una fase global -1, siendo esto independiente del camino concreto que tracemos. Finalmente, debido al origen topológico de la degeneración del estado fundamental y al gap finito, un sistema con el Hamiltoniano (5.2) es robusto frente a perturbaciones locales [37], que era la propiedad buscada.

En realidad, (5.2) no es sino un ejemplo de lo que se conoce como orden topológico, un nuevo tipo de orden que se da en sistemas cuánticos fuertemente correlacionados y que no tiene cabida en la teoria de Landau [25], [27]. Aunque aún no se dispone de una definición completa del concepto de orden topológico, si podemos decir que características típicas de éste son la degeneración de origen topológico del estado fundamental, la presencia de un gap finito y la aparición de excitaciones localizadas con estadísticas anómalas, ni fermiónicas ni bosónicas, que son por ello conocidas como anyones. Hasta la fecha el único ejemplo experimental de orden topológico ha de buscarse en el efecto Hall cuántico fraccionario [46], pero existen razones para creer que nuevos ejemplos podrían construirse en los laboratorios próximamente [47]. Desde un punto de vista teórico, posibles mecanismos para la obtención de órdenes topológicos son los condensados de redes de cuerdas [26] o, como estudiamos en uno de los trabajos de esta tesis, los condensados de redes de branas [12].

El modelo (5.2) es un ejemplo de lo que se conoce como orden topológico abeliano, que se caracteriza por el hecho de que la carga total de una región esta completamente determinada si se conoce ésta en un conjunto de subregiones. Existen ejemplos de orden topológico no abeliano, en los cuales esto ya no es cierto. En particular, se tiene entonces que la fusión de dos excitaciones puede dar lugar a una excitación con diferentes valores de carga topológica. En ese caso, en presencia de una serie de excitaciones en un sistema surge una degeneración asociada a los posible canales de fusión. Si las excitaciones están lo suficientemente separadas entre sí, esta degeneración estará protegida del mismo modo que la del estado fundamental. Además, es posible transformar los estados de este espacio protegido moviendo las excitaciones unas en torno a otras de forma adecuada. Esta serie de consideraciones dan lugar a lo que se conoce como computación cuántica topológica [37], [23], [24]. En los trabajos [13], [14], [15] estudiamos la posibilidad de ampliar este concepto recuperando la idea de utilizar el estado fundamental para codificar la información cuántica, que sería manipulada entonces cambiando progresivamente la topología del sistema. Esto tiene por ejemplo la ventaja de que no se requiere la manipulación de excitaciones.

5.1. Anyones y branyones

En general, dado un código topológico con generadores del estabilizador S_i podemos construir un sistema con orden topológico introduciendo el Hamiltoniano

$$\mathcal{H} = -\sum_i S_i. \tag{5.2}$$

Cuando aplicamos esta receta a los códigos de color bidimensionales [12] obtenemos un sistema con anyones abelianos y que puede interpretarse como un condensado de redes de cuerdas. Esto último significa que podemos interpretar los estados del sistema en términos de configuraciones de unas ciertas cuerdas, y que el estado fundamental es tal que sólo contiene cierto tipo de configuraciones particulares, sometidas a intensas fluctuaciones cuánticas locales. Las cuerdas se organizan en redes, y las configuraciones permitidas son aquellas en las que estas redes no contienen 'cabos sueltos' y en las cuales los puntos de ramificación de la red obedecen ciertas reglas, diferentes en cada sistema, véase la Fig. 11.

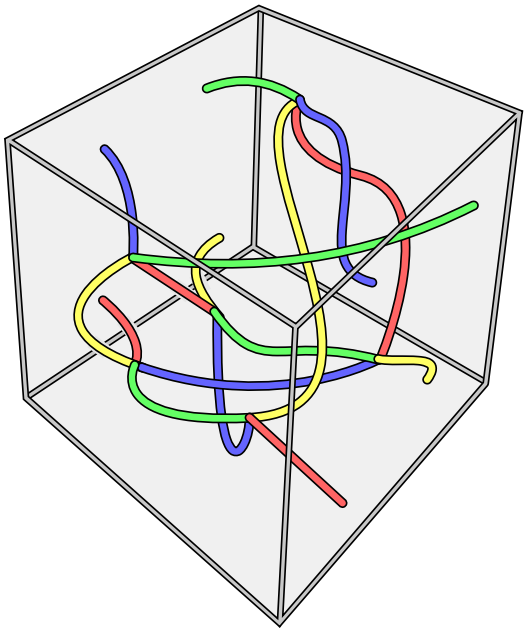


Figura 11: Los sistemas con orden topológico obtenidos a partir de los códigos de color 3D admiten una interpretación en términos de condensado de redes de cuerdas. Existen cuatro tipos de cuerdas, y se admiten puntos de ramificación donde confluyan una de cada tipo. En este ejemplo el sistema adopta la topología de un 3-toro, por lo que las caras opuestas del cubo han de identificarse.

En el caso de los códigos de color tridimensionales de nuevo puede hablarse de condensado de redes de cuerdas, pero una interpretación en términos de condensado de redes de membranas es igualmente posible [12]. Las membranas forman redes en las cuales no puede haber bordes de membrana sin emparejar y las membranas se bifurcan a lo largo de líneas. Las excitaciones en este sistema son de dos tipos, quasipartículas y flujos. Estos últimos

son excitaciones unidimensionales. La razón para denominarlos flujos es que pueden etiquetarse de tal modo que el valor de esta etiqueta se conserva a lo largo de longitud de la excitación. Los flujos pueden bifurcarse y tienen un carácter abeliano, en el sentido de que dados dos flujos con cierta etiqueta, la etiqueta para el flujo total sólo puede ser una. Respecto al carácter topológico de las excitaciones, encontramos que el movimiento de las quasipartículas en torno a los flujos conlleva la aparición de fases globales en el sistema, en analogía con el caso bidimensional.

Es posible generalizar los ejemplos citados a dimensiones superiores [12]. Para ello, el primer requisito es encontrar las redes coloreadas adecuadas, que nosotros denominamos D-colexes (por el inglés 'color complex') donde D es la dimensión de la variedad asociada a la red. Los colexes resultan tener una rica estructura, y pueden ser descritos puramente a partir de un grafo coloreado, de tal modo que este contiene toda la estructura topológica de la variedad. Así, por ejemplo, la orientabilidad de la variedad depende de si el grafo es bipartito o no. O también, la suma conexa de variedades tiene una contrapartida muy simple en términos de los grafos correspondientes, etc.

Cuando $D \geq 4$, pueden construirse distintos ordenes topológicos a partir del D-colex. En particular, ha de fijarse un parámetro entero k con $1 \leq k \leq D/2$. El sistema resultante puede interpretarse como un condensado de k-branas o de $(D-k)$-branas, y las excitaciones, que llamamos branyones, son objetos extensos de $k-1$ y $D-k-1$ dimensiones. Al existir distintos ordenes topológicos en una misma red, se plantea la posibilidad de estudiar transiciones de fase topológicas, pero ésta es una dirección en la que no hemos ahondado.

Sumario de resultados

- Estudiamos los sistemas con orden topológico asociados a los códigos de color en dimensión D.
- Para ello desarrollamos el concepto de D-colex, un tipo de redes D-dimensionales con ciertas propiedades de colorabilidad.
- Los modelos obtenidos son condensados de redes de branas.
- Las excitaciones de estos modelos son branyones, objetos extensos que interactáan de forma puramente topológica.
- En dimensión D, pueden construirse condensados de redes de d-branas con $d = 1, \ldots, D-1$. Un condensado de redes de d-branas es a su vez un condensado de redes de $(D-d)$-branas.

- Al existir distintos ordenes topológicos con el mismo sistema cuántico subyacente para $D \geq 4$, se plantea la posibilidad de estudiar transiciones de fase topológicas.

5.2. Bordes y orden topológico

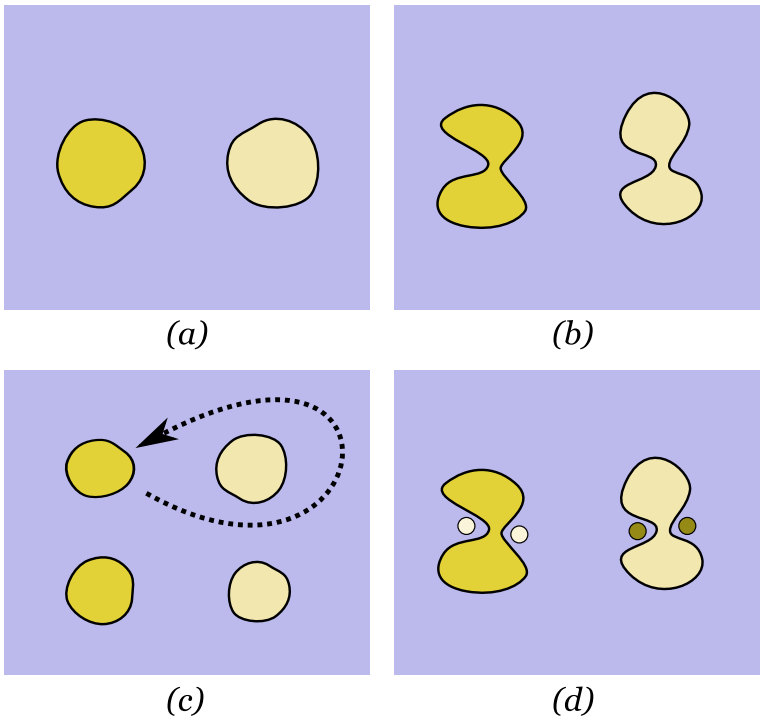


Figura 12: Esquema para testar el orden topológico en los códigos de superficie. Las zonas con el Hamiltoniano (5.2) aparecen en azul, y los agujeros corresponden a los lugares en los que dominan los términos de Zeeman, Z en un caso y X en el otro. Primero se crea un agujero de cada tipo (a), luego se dividen en dos (b) y uno de los cuatro se mueve en torno a uno del otro tipo (c). Finalmente (d), al juntar los agujeros del mismo tipo pueden surgir cargas topológicas en el punto de unión con un 50 % de posibilidades. Este es un efecto topológico, pues ocurrirá sólo si hemos movido un número impar de veces un agujero en torno del otro, independientemente de la trayectoria.

Cuando discutimos los códigos de superficie vimos la importancia de poder introducir bordes, tanto abiertos como cerrados, pues esta es la única manera de conseguir topologías no triviales en códigos planos. Además, también se discutió como la posibilidad de deformar estos bordes permite inicializar, medir y transformar los qubits codificados.

Supongamos ahora que queremos hacer lo mismo en el contexto de un sistema con el Hamiltoniano (5.2). Si quisiéramos introducir bordes de la misma manera en que lo hacemos en el código, deberemos de ser capaces de manipular el Hamiltoniano qubit a qubit. Esto será en general muy poco realista. Piénsese por ejemplo en la propuesta para realizar (5.2) a partir de moléculas dipolares en redes ópticas.

Claramente se necesita una alternativa, y esta es una de las motivaciones para el trabajo [13], donde investigamos como se pueden introducir bordes que no requieren cambios abruptos en el Hamiltoniano. En esencia, todo se reduce a introducir términos de Zeeman al Hamiltoniano original, de tipo Z o X, dependiendo de si se trata de un borde abierto o cerrado. Fuera del código dominan los nuevos términos, y el borde es una zona difusa donde se interpola entre ambos Hamiltonianos.

Una vez que disponemos de la posibilidad de crear bordes, podemos cambiarlos dinámicamente para realizar transformaciones en el espacio protegido que forman los estados fundamentales. En [13] exponemos como esto puede utilizarse para testar el orden topológico del sistema, véase una explicación del método en la Fig. 12. Anteriormente se habían presentado tests de este tipo, pero siempre basados en interferometría con excitaciones [48], lo que presenta problemas de descoherencia al requerirse superposiciones de estados con distintas cargas topológicas. Además, se hace necesario encontrar un método para mover las excitaciones con la suficiente precisión, pues sino la interferencia sería destruida por las fases dinámicas. Todos estos problemas desaparecen al trabajar en el estado fundamental, algo que sólo es posible si disponemos de bordes que podamos deformar a voluntad.

Sumario de resultados

- Describimos un Hamiltoniano cuántico que permite introducir bordes en los modelos topológicos asociados a los códigos de superficie.

- Los bordes se consiguen mediante la introducción de términos Zeeman que destruyen el orden topológico.

- Introducimos un test para el orden topológico no basado en la interferencia con excitaciones topológicas. En vez de eso, utilizamos la posibilidad de cambiar dinámicamente la topología del sistema moviendo los bordes.

5.3. Modelos topológicos no abelianos: condensación y confinamiento de cargas topológicas

Un aspecto que no hemos comentado aún es la similitud del Hamiltoniano (5.2) con el correspondiente a una teoría gauge $\mathbf{Z}_2$ en la red. La diferencia radica en que en (5.2) no se impone la simetría gauge, si bien el estado fundamental pertenece al sector que sí la posee. Resulta entonces natural considerar generalizaciones a grupos gauge discretos no abelianos, en las que los qudits tienen dimensión igual al orden del grupo. Estas generalizaciones las considera Kitaev en [37] con el ánimo de esbozar la computación cuántica topológica que hemos comentado más arriba. Eligiendo grupos no abelianos, el orden topológico resulta ser no abeliano también, viniendo las cargas topológicas descritas por las representaciones irreducibles del doble cuántico del grupo [37].

En [14] tratamos en cierta profundidad estas generalizaciones a grupos gauge discretos, completando e intentando iluminar el mencionado trabajo de Kitaev [37]. En particular, hacemos un énfasis mayor en ciertos operadores asociados a objetos geométricos con forma de cinta. Estos operadores cinta, que pueden interpretarse como procesos en los que un par de excitaciones se crea en uno de los extremos de la cinta y una de ellas se propaga hasta el otro extremo, fueron ya introducidos en [37]. Sin embargo, en [14] los caracterizamos por sus propiedades, introducimos las cintas cerradas y estudiamos una serie de algebras asociadas a las cintas de las que se extraen inmediatamente las cargas topológicas del sistema.

Una vez desarrollada esta maquinaria, y con la idea de generalizar el concepto de borde que encontrábamos en el caso $\mathbf{Z}_2$ en la sección anterior, estudiamos una amplia familia de variaciones de los modelos de Kitaev para grupos discretos arbitrarios. Estos modelos modificados incluyen nuevos términos a un solo cuerpo que generalizan los términos de Zeeman del caso $\mathbf{Z}_2$. Gracias a que los modelos son exactos, nos es posible extraer unan gran cantidad de información sobre los modelos. En particular, encontramos que los nuevos sistemas pueden interpretarse en términos de la condensación de algunas de las cargas del sistema original, junto con el confinamiento de otras. Utilizando los operadores cinta, encontramos que las paredes de dominio que surgen del confinamiento pueden etiquetarse. Clasificamos entonces los tipos de excitaciones en términos de su carga topológica y su etiqueta de confinamiento.

Como ya se ha dicho, la motivación original para estudiar esta familia de modelos modificados radicaba en el deseo de generalizar la noción de borde a sistemas con un grupo gauge discreto arbitrario. Este objetivo lo materializamos en [15], introduciendo el concepto de orden topológico anidado.

Recordemos que en el caso $\mathbf{Z}_2$ podíamos practicar dos tipos de agujeros, asociados a términos Zeeman X y Z. En ambos casos, el orden topológico en los agujeros queda completamente destruido. La novedad que surge al considerar grupos más grandes es que es posible introducir agujeros en los que el orden topológico es destruido sólo parcialmente, existiendo una gran variedad de tipos de agujeros. Esta es la razón por que hablamos de orden topológico anidado.

Utilizando una vez más los operadores cinta, en [15] mostramos como la introducción de estos agujeros, que ahora preferimos denominar islas, modifica el estado fundamental del sistema aumentando su degeneración topológica. Al igual que hacíamos en el caso $\mathbf{Z}_2$, las islas pueden crearse, dividirse, moverse y fusionarse, lo que da lugar a una generalización de la computación cuántica topológica usual basada en excitaciones.

Sumario de resultados

- Generalizamos el concepto de operador cinta en los modelos topológicos con grupo gauge no abeliano desarrollados por Kitaev. Esto nos permite caracterizar la carga topológica en términos de un algebra de proyectores asociada a operadores cinta cerrados.
- Introducimos nuevos términos en los Hamiltonianos de estos modelos, lo que da lugar a una familia de modelos exactamente solubles.
- En los nuevos modelos parte o la totalidad del orden topológico son destruidos, y por tanto la simetría gauge se reduce o desaparece.
- El mecanismo que produce esta reducción de la simetría es el confinamiento de parte de las cargas topológicas de los modelos originales.
- Asimismo, encontramos que algunas de las cargas topológicas aparecen condensadas.
- Caracterizamos las cargas topológicas y las paredes de dominio de los nuevos modelos utilizando álgebras de proyectores asociadas a operadores cinta tanto abiertos como cerrados.
- Consideramos la posibilidad de introducir el mecanismo de reducción de orden topológico sólo en ciertas áreas del sistema. Esto da lugar al concepto de orden topológico anidado.
- La introducción de islas con una simetría gauge reducida da lugar a una degeneración de origen topológico en el estado fundamental del sistema.

- Las islas pueden dividirse, moverse y fusionarse, lo que da lugar a una generalización de la computación cuántica topológica usual.

6. Resultados y conclusiones

En esta tesis se presentan trabajos encaminados a resolver el problema del ruido en los sistemas cuánticos. En el ámbito de la información cuántica, se estudia de forma sistemática una familia de protocolos de destilación cuántica para qudits:

- Describimos el grupo de transformaciones locales que dejan invariante la base de estados de Bell. Encontramos que los elementos de este grupo producen permutaciones de los elementos de la base. Estas permutaciones forman un grupo simpléctico afín.

- Caracterizamos los estados invariantes bajo la acción de este grupo. Estos estados, que llamamos heterotrópicos, son relevantes pues son el resultado de las operaciones de despolarización.

- Estudiamos una amplia familia de protocolos de destilación de entrelazamiento cuántico basados en el grupo de permutaciones locales.

- Consideramos protocolos de destilación con y sin despolarización.

- Para investigar los protocolos, empleamos métodos tanto analíticos como computacionales.

- Encontramos que los protocolos en los que se obtiene más de una pareja de qudits en cada iteración resultan ventajosos para fidelidades altas pero inútiles para fidelidades bajas.

- Describimos una familia de puntos fijos comunes a todos los protocolos considerados.

- Generalizamos el algoritmo de amplificación de privacidad cuántico a qudits.

- Estudiamos el problema de la destilabilidad, encontrando que con los protocolos considerados los qudits con dimensión no prima se comportan peor que los de dimensión prima.

En lo tocante a la corrección cuántica de errores, se introducen nuevos códigos de carácter topológico y técnicas especificas para su manipulación:

- Introducimos versiones clásicas de los códigos homológicos que saturan el límite de Hamming.
- Generalizamos los códigos homológicos a complejos bidimensionales y al caso de los qudits.
- Encontramos que las superficies han de ser orientables para qudits de dimensión mayor a dos.
- Damos una perspectiva geométrica a códigos previamente conocidos.
- Construimos una familia de códigos homológicos que satura la tasa máxima k/n.
- Encontramos una clase óptima de códigos regulares en el toro.
- Introducimos códigos homológicos planos utilizando el concepto de homología relativa.
- Introducimos una nueva clase de códigos topológicos bidimensionales, los códigos de color.
- Los códigos de color se fundamentan en cierta homología de triángulos que no forma parte de las habitualmente estudiadas.
- Los códigos de color tienen propiedades de transversalidad superiores a las de los códigos de superficie, permitiendo la implementación transversal del grupo de Clifford. Este grupo de operadores es fundamental en información cuántica. En particular, puede utilizarse para destilar.
- Dada una cierta topología, los códigos de color codifican el doble de qubits que los códigos de superficie.
- Describimos clases optimas de códigos de color regulares, mostrando que los códigos de color requieren un menor número de qubits físicos.
- Generalizamos los códigos de color a tres dimensiones.
- Encontramos que las propiedades de transversalidad de los códigos de color tridimensionales son las mismas que las de los códigos de Reed-Muller cuánticos. Es decir, permiten la implementación transversal de ciertas puertas lógicas y medidas que son suficientes para la computación universal.

- Introducimos las deformaciones en códigos estabilizadores como una alternativa a las operaciones transversales. Esto es especialmente natural en los códigos topológicos, pues las deformaciones tienen una interpretación puramente geométrica.
- Mostramos cómo por medio de las deformaciones es posible inicializar, transformar y medir los qubits codificados en un código.
- Consideramos en detalle los códigos de superficie, donde vemos que las puertas CNot se pueden implementar mediante deformaciones. Esto permite trasladar arquitecturas que previamente requerían tres dimensiones a una sola capa bidimensional de código.
- Derivamos una conexión entre los códigos de color y ciertos modelos estadísticos bidimensionales clásicos de Ising a tres cuerpos.
- Los resultados sugieren algún tipo de relación entre la aparición de clases de universalidad diferentes en distintas redes en el modelo clásico, y las distintas capacidades transversales de los códigos de color correspondientes.
- Explicamos como puede obtenerse un código de color a partir de ciertos estados de racimo.
- Al aplicar la conexión con modelos estadísticos, estos estados de racimo se relacionan con modelos de Ising a tres cuerpos que incluyen un campo magnético externo.

Finalmente, se exploran nuevas formas de orden topológico y nuevos mecanismos para explotarlo de cara a realizar computaciones cuánticas:

- Estudiamos los sistemas con orden topológico asociados a los códigos de color en dimensión D.
- Para ello desarrollamos el concepto de D-colex, un tipo de redes D-dimensionales con ciertas propiedades de colorabilidad.
- Los modelos obtenidos son condensados de redes de branas.
- Las excitaciones de estos modelos son branyones, objetos extensos que interactáan de forma puramente topológica.
- En dimensión D, pueden construirse condensados de redes de d-branas con $d = 1, \ldots, D-1$. Un condensado de redes de d-branas es a su vez un condensado de redes de $(D-d)$-branas.

- Al existir distintos ordenes topológicos con el mismo sistema cuántico subyacente para $D \geq 4$, se plantea la posibilidad de estudiar transiciones de fase topológicas.

- Describimos un Hamiltoniano cuántico que permite introducir bordes en los modelos topológicos asociados a los códigos de superficie.

- Los bordes se consiguen mediante la introducción de términos Zeeman que destruyen el orden topológico.

- Introducimos un test para el orden topológico no basado en la interferencia con excitaciones topológicas. En vez de eso, utilizamos la posibilidad de cambiar dinámicamente la topología del sistema moviendo los bordes.

- Generalizamos el concepto de operador cinta en los modelos topológicos con grupo gauge no abeliano desarrollados por Kitaev. Esto nos permite caracterizar la carga topológica en términos de un algebra de proyectores asociada a operadores cinta cerrados.

- Introducimos nuevos términos en los Hamiltonianos de estos modelos, lo que da lugar a una familia de modelos exactamente solubles.

- En los nuevos modelos parte o la totalidad del orden topológico son destruidos, y por tanto la simetría gauge se reduce o desaparece.

- El mecanismo que produce esta reducción de la simetría es el confinamiento de parte de las cargas topológicas de los modelos originales.

- Asimismo, encontramos que algunas de las cargas topológicas aparecen condensadas.

- Caracterizamos las cargas topológicas y las paredes de dominio de los nuevos modelos utilizando álgebras de proyectores asociadas a operadores cinta tanto abiertos como cerrados.

- Consideramos la posibilidad de introducir el mecanismo de reducción de orden topológico sólo en ciertas áreas del sistema. Esto da lugar al concepto de orden topológico anidado.

- La introducción de islas con una simetría gauge reducida da lugar a una degeneración de origen topológico en el estado fundamental del sistema.

- Las islas pueden dividirse, moverse y fusionarse, lo que da lugar a una generalización de la computación cuántica topológica usual.

De los estudios presentados en esta tesis se desprende claramente que el estudio de las propiedades topológicas en información y computación cuánticas, así como en sistemas fuertemente correlacionados en materia condensada, es un tema de investigación con numerosas preguntas abiertas que en la actualidad son objeto de intensa actividad investigadora.

Bibliografía

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, England, 2000.

[2] D. Bouwmeester, A. K. Ekert, A. Zeilinger (Eds.), *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, Springer-Verlag Berlin, Heidelberg, New York, 2000.

[3] A. Galindo, M. A. Martin-Delgado, *Information and Computation: Classical and Quantum Aspects*, Rev. Mod. Phys. **74**, 347 (2002).

[4] H. Bombin, M.A. Martin-Delgado, *Entanglement Distillation Protocols and Number Theory*, Phys. Rev. A **72**, 032313 (2005), quant-ph/0503013.

[5] H. Bombin and M.A. Martin-Delgado, *Homological Error Correction: Classical and Quantum Codes*, J. Math. Phys. **48**, 052105 (2007), quant-ph/0605094.

[6] H. Bombin and M.A. Martin-Delgado, *Topological Quantum Error Correction with Optimal Encoding Rate*, Phys. Rev. A **73**, 062303 (2006), quant-ph/0602063.

[7] H. Bombin and M. A. Martin-Delgado, *Topological Quantum Distillation*, Phys. Rev. Lett. **97**, 180501 (2006), quant-ph/0605138.

[8] H. Bombin and M.A. Martin-Delgado, *Topological Computation without Braiding*, Phys. Rev. Lett. **98**, 160502 (2007), quant-ph/0610024.

[9] H. Bombin and M.A. Martin-Delgado, *Optimal Resources for Topological 2D Stabilizer Codes: Comparative Study*, Phys. Rev. A **76**, 012305 (2007), quant-ph/0703272.

[10] H. Bombin, M.A. Martin-Delgado, *Quantum Measurements and Gates by Code Deformation*, arXiv:0704.2540v1 [quant-ph].

[11] H. Bombin and M.A. Martin-Delgado, *Statistical Mechanical Models and Topological Color Codes*, Phys. Rev. A **77**, 042322 (2008), arXiv:0711.0468v1 [quant-ph].

[12] H. Bombin and M.A. Martin-Delgado *Exact Topological Quantum Order in D=3 and Beyond: Branyons and Brane-Net Condensates*; Phys. Rev. B **75**, 075103 (2007); cond-mat/0607736.

[13] H. Bombin, M.A. Martin-Delgado, *An Interferometry-Free Protocol for Demonstrating Topological Order*, arXiv:0705.0007v1 [cond-mat.str-el].

[14] H. Bombin, M.A. Martin-Delgado, *A Family of Non-Abelian Kitaev Models on a Lattice: Topological Confinement and Condensation*, aceptado en Phys. Rev. B, arXiv:0712.0190v2 [cond-mat.str-el].

[15] H. Bombin, M.A. Martin-Delgado, *Nested Topological Order*, arXiv:0803.4299v1 [cond-mat.str-el].

[16] E. Knill, R. Laflamme, *A theory of quantum error-correcting codes*, Phys. Rev. A **55**, 900 (1997).

[17] P.W. Shor, *Scheme for Reducing Decoherence in Quantum Computer Memory*, Phys. Rev. A **52**, R2493 (1996).

[18] A.M. Steane, *Error Correcting Codes in Quantum Theory*, Phys. Rev. Lett. **77**, 793 (1996).

[19] P.W. Shor, *Fault Tolerant Quantum Computation*, in FOCS'37, 56-65, (1996), quant-ph/9605011.

[20] E. Knill, R. Laflamme, W. Zurek, *Threshold Accuracy for Quantum Computation*, quant-ph/9610011.

[21] A.Yu. Kitaev, *Quantum computations: algorithms and error correction*, Russian Math. Surveys **52**, 1191 (1997).

[22] D. Aharonov, M. Ben-Or, *Fault Tolerant Quantum Computation with Constant Error Rate*, quant-ph/9906129.

[23] Michael H. Freedman, Alexei Kitaev, Michael J. Larsen, Zhenghan Wang, *Topological Quantum Computation*, Bull. Am. Math. Soc. **40**, 31 (2002), quant-ph/0101025.

[24] J. Preskill, online lecture notes on Quantum Error Correction and Fault-Tolerance Quantum Computation: http://www.theory.caltech.edu/people/preskill/ph229/index.html

[25] X.-G. Wen, *Topological Orders in Rigid States* Int. J. Mod. Phys. B **4**, 239 (1990).

[26] X.-G. Wen, *Topological Orders and Edge Excitations in FQH States*, Int. J. Mod. Phys. B **6**, 1711 (1992).

[27] X.-G. Wen. *Quantum Field Theory of Many-body Systems*, Oxford University Press, (2004).

[28] L. D. Landau, *Theory of phase transformations*, Phys. Z. Sowjetunion **11**, 26 (1937).

[29] V. L. Ginzburg, L. D. Landau, *On the theory of superconductivity*, Zh. Ekaper. Teoret. Fiz. **20**, 1064 (1950).

[30] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolini, *Experimental Quantum Cryptography*, J. Cryptology **5**, 3-28 (1992).

[31] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. Wootters, *Teleporting an Unknown Quantum State via Dual Classical and EPR Channels*, Phys. Rev. Lett. **70**, 1895-1899 (1993).

[32] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters, *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, Phys. Rev. Lett. **76**, 722-725 (1996).

[33] D. Deutsch, A.Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, *Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels*, Phys. Rev. Lett. **77**, 2818-2821 (1996).

[34] R.F. Werner, *Quantum States with EPR Correlations Admitting a Hidden-Variable Model*, Phys. Rev. A **40**, 4277-4281.

[35] D. Gottesman, *Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound*Phys. Rev. A **54**, (1996) 1862.

[36] A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, *Quantum Error Correction and Orthogonal Geometry*, Phys. Rev. Lett. **78**, (1997) 405.

[37] A.Yu. Kitaev, *Fault-Tolerant Quantum Computation by Anyons*, Annals Phys. **303**, 2 (2003), quant-ph/9707021.

[38] E. Dennis, A. Kitaev, A. Landahl, J. Preskill, *Topological Quantum Memory*, J. Math. Phys. **43**, 4452-4505 (2002), quant-ph/0110143.

[39] S. Bravyi, A. Kitaev, *Universal Quantum Computation with Ideal Clifford Gates and Noisy Ancillas*, Phys. Rev. A **71**, 022316 (2005).

[40] P.O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, F. Vatan, *On Universal and Fault-Tolerant Quantum Computing*, Information Processing Letters **75**, 101 (2000), quant-ph/9906054.

[41] Bei Zeng, Andrew Cross, Isaac L. Chuang, *Transversality versus Universality for Additive Quantum Codes*, arXiv:0706.1382v3 [quant-ph]

[42] E. Knill, R. Laflamme, W. Zurek, *Threshold Accuracy for Quantum Computation*, quant-ph/9610011.

[43] M. Van den Nest, W. D}ur, and H. J. Briegel, *Classical Spin Models and the Quantum-Stabilizer Formalism*, Phys. Rev. Lett. **98**, 117207 (2007); arXiv:quant-ph/0610157.

[44] S. Bravyi and R. Raussendorf, *Measurement-Based Quantum Computation with the Toric Code States*; Phys. Rev. A **76**, 022304 (2007); arXiv:quant-ph/0610162.

[45] R. Raussendorf and H.-J. Briegel, *A One-Way Quantum Computer*, Phys. Rev. Lett. **86**, 5188 (2001).

[46] X.-G. Wen and Q. Niu, *Ground State Degeneracy of the FQH States in Presence of Random Potential and on High Genus Riemann Surfaces*, Phys. Rev. B **41**, 9377 (1990).

[47] A. Micheli, G.K. Brennen, P. Zoller, *A Toolbox for Lattice Spin Models with Polar Molecules*, quant-ph/0512222.

[48] S.S. Bullock, G.K. Brennen, *Qudit Surface Codes and Gauge Theory with Finite Cyclic Groups*, J. Phys. A **40**, 3481-3505 (2007).

La presente bibliografía no pretende ser exhaustiva, sino adaptada a las necesidades de esta introducción.

Destilación de Entrelazamiento Cuántico

Entanglement distillation protocols and number theory

H. Bombin and M. A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain
(Received 1 March 2005; published 13 September 2005)

We show that the analysis of entanglement distillation protocols for qudits of arbitrary dimension D benefits from applying basic concepts from number theory, since the set $\mathbf{Z}_D^n$ associated with Bell diagonal states is a module rather than a vector space. We find that a partition of $\mathbf{Z}_D^n$ into divisor classes characterizes the invariant properties of mixed Bell diagonal states under local permutations. We construct a very general class of recursion protocols by means of unitary operations implementing these local permutations. We study these distillation protocols depending on whether we use twirling operations in the intermediate steps or not, and we study them both analytically and numerically with Monte Carlo methods. In the absence of twirling operations, we construct extensions of the quantum privacy algorithms valid for secure communications with qudits of any dimension D. When D is a prime number, we show that distillation protocols are optimal both qualitatively and quantitatively.

DOI: 10.1103/PhysRevA.72.032313 PACS number(s): 03.67.Lx

I. INTRODUCTION

Quantum information theory (QIT) revolves around the concept of entanglement [1–4]. It is the product of combining the superposition principle of quantum mechanics with multipartite systems—described by the tensor product of Hilbert spaces. Entanglement is central to transmitting information in a quantum communication protocol or processing information in a quantum computation. There are two basic open problems in the study of entanglement: separability and distillability. Separability is concerned with two questions, namely whether a quantum state is factorizable, and if not, how much entanglement it contains. These questions are of great importance even in practice since entanglement amounts to interaction between two or more parties, and thus it demands more resources to establish an entangled state than a factorized one.

Likewise, distillability [5–11] is concerned with two questions: whether a quantum state is distillable, and if it is, how to devise an explicit protocol to extract entanglement out of the initial low entangled state. The main focus of our paper is on the construction of distillation protocols, rather than a direct analysis of the distillability issue.

The study of distillation protocols for qudits is justified since it is known that for mixed states of dimension higher than $2\times 2, 2\times 3$, neither a complete criterion for separability nor for distillability is known [9].

Separability and distillability are interconnected. Entanglement of a mixed state is a necessary condition for being distillable. However, it was quite a surprise to find that there exist states that, though they are entangled, cannot be distilled. They are the bound entangled states that are characterized by being positive partial transposition (PPT) entangled states [12–14]. This situation soon raised the question of whether non-PPT states were all distillable. Although there is not a conclusive answer, there is strong evidence that this is not the case since Werner states which are finite-n undistillable have been found [15,16].

In this paper, we study entanglement distillation protocols for qudits using the recursion method [5,6]. The mixed states to be distilled are diagonal Bell states of qudits, i.e., maximally entangled states, but they do not need to be tensor product of pairs of Bell states. Moreover, we can also distill nondiagonal states.

We make significant progress in the understanding of these protocols and find new efficient variants of them by using number theory. This number theory enters in the properties of the module $\mathbf{Z}_D^n$ that appears in the labeling of the Bell diagonal states of qudits. Local permutations acting on these states by means of unitary operations serve to construct generalized distillation protocols [10]. As a byproduct, we also introduce heterotropic states (38) as the invariant states under the group of local permutations.

As a result of this study, we find that qudit states with dimension D a prime number are qualitatively and quantitatively the best choices for quantum distillation protocols based on the recursion method. Qualitatively, these states are best since we show that for D not a prime number there appear disturbing attractor points in the space of fidelity parameters that deviate the distillation process from the desired fixed point that represents the maximally entangled state. This phenomenon is absent when D is a prime number and $\mathbf{Z}_D^n$ becomes a vector space [11]. Quantitatively, these states are best since we propose distillation protocols that when D is a prime number, they distill all states with fidelity bigger than $1/D$ without resorting to twirling operations.

We hereby summarize briefly some of our main results.

(i) We prove that the group of local permutations for qudits of arbitrary dimension D is the semidirect product of the group of translations and simplectic transformations. This structure plays an important role in the distillation protocols for qudits.

(ii) We simplify the problem of finding the best distillation protocol to that of finding the best set of coefficients of a certain polynomial constrained to the existence of a suitable vector space.

(iii) We introduce the concept of *joint performance parameter* η (65) that allows us the comparison of distillation protocols with different values of fidelity, probability of success, and number of Bell pairs used altogether. It is a figure

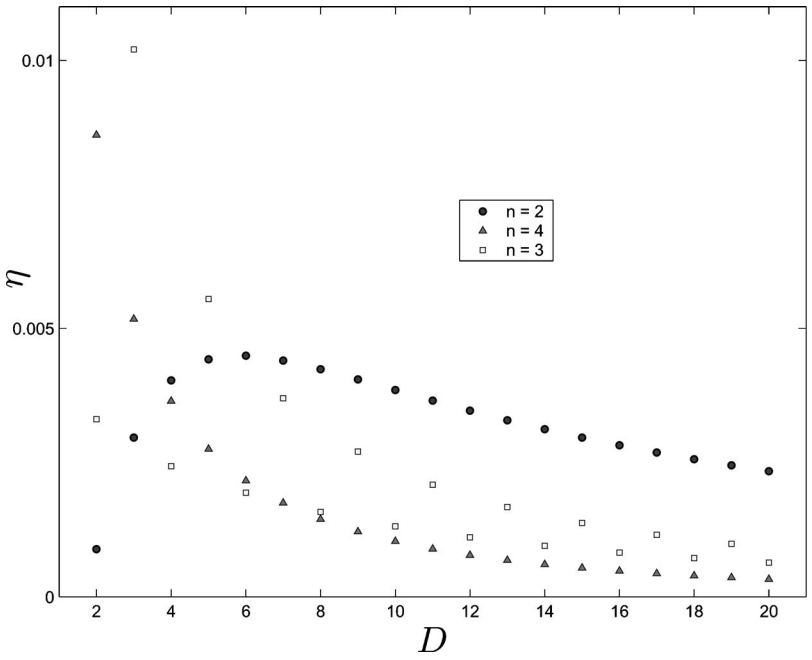


FIG. 1. Values of the coefficient η for the considered twirled-assisted protocols with $n=2,3,4$. Initial fidelity is close to $1/D$.

of merit for low fidelity states above the distillation threshold where the recursion method is specially suited for distillation, prior to switching a hashing or breeding method.

(iv) We analyze several distillation protocols assisted with twirling operations as the dimension D of qudits vary. We find that the best performance according to η is not achieved for qubits ($D=2$), but for qutrits ($D=3$) and $n=3$ input pairs of Bell states as shown in Fig. 1 and Fig. 2. We also find that it is not possible to improve η by indefinitely increasing the number of input pairs n.

(v) We propose a distillation protocol without resorting to twirling operations for $n=4$ input Bell states and $m=2$ output Bell states that is iterative and its yield is greatly improved: about four orders of magnitude with respect to the protocols based on twirling, even for states quite near the fixed point. This is shown in Fig. 5.

(vi) We propose and study an extension of the quantum privacy amplification protocols [7] that work for arbitrary dimension D.

(vii) We find indications of the existence of nondistillable NPPT states by studying the distillation capacities of protocols for several values of D, as shown in Fig. 7. By all means, the fact that some states are not distillable with a set of protocols does not necessarily mean that they are nondistillable.

This paper is organized as follows. In order to facilitate the reading and exposition of our results, we present the proofs of our theorems and technicalities of the numerical methods in independent Appendixes. Section II deals with the basic properties of diagonal Bell states for qudits and introduces a partition of the module $\mathbf{Z}_D^n$. Section III treats the group of local permutations acting on qudits in diagonal Bell

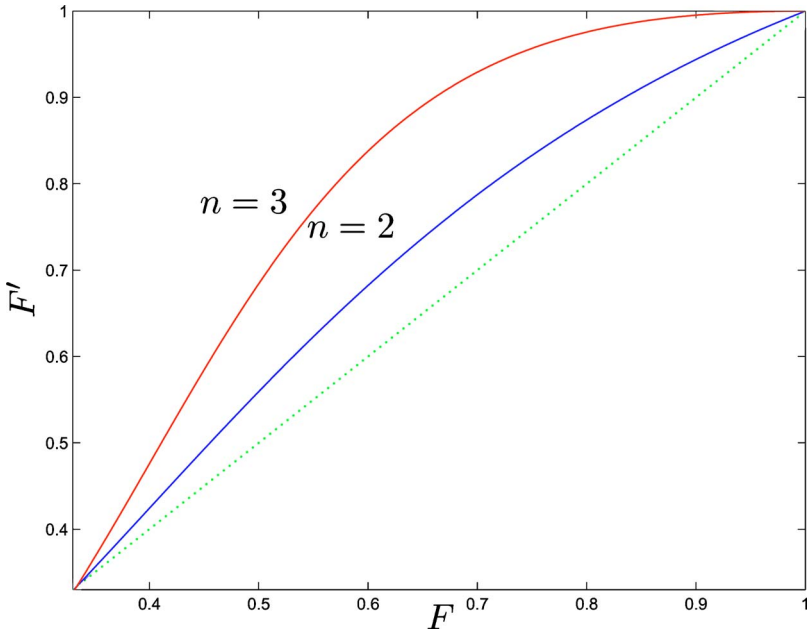


FIG. 2. (Color online) Evolution of the fidelity for the distillation protocols assisted by twirling when $n=2$, 3 for qudits with $D=3$.

states. Section IV describes the group of local permutations and the twirling operations associated with it. We characterize states that are invariant under these operations as heterotropic states. In Section V, we present all our distillation protocols based on local permutations of qudits in diagonal Bell states, both with and without resorting to twirling operations. To this end, we make extensive use of the theoretical results found in previous sections and devise numerical methods to analyze efficiently the properties of the proposed distillation protocols as different parameters such as D, F, n,m, etc. vary. Section VI is devoted to conclusions and future prospects.

II. BASIC PROPERTIES OF DIAGONAL BELL STATES FOR QUDITS

A. Bell states basic notation

The quantum systems we are going to consider are *qudits*, which are described by a Hilbert space of dimension $D \geqslant 2$, and finite. The elements of a given orthogonal basis can be denoted $|x\rangle$ with $x=0,\ldots,D-1$. This set of numbers is naturally identified with the elements of the set modulus,

$$\mathbf{Z}_D := \mathbf{Z}/D\mathbf{Z}, \tag{1}$$

and we shall informally use them as if they belonged to $\mathbf{Z}_D$. In general, whenever an element of $\mathbf{Z}_D$ appears in an expression, any integer in that expression must be understood to be mapped to $\mathbf{Z}_D$.

We consider two separate parties, Alice and Bob, each of them owning one of these systems. The entire Hilbert space is then $\mathcal{H}=\mathcal{H}_A \otimes \mathcal{H}_B$. A mixed state of the whole system is called *separable* when it can be expressed as a convex sum of *product states* [17],

$$\rho = \sum_i p_i |e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i|, \quad |e_i\rangle \in \mathcal{H}_A,\ |f_i\rangle \in \mathcal{H}_B; \tag{2}$$

a state which is not separable is said to be *entangled*.

Elements of the *computational basis* of a pair of qudits shared by Alice and Bob are denoted as

$$|ij\rangle := |i\rangle \otimes |j\rangle, \quad i,j \in \mathbf{Z}_D. \tag{3}$$

To shorthen the notation, it is convenient to introduce the symbols

$$\underset{k}{\boldsymbol{\mathcal{S}}} := \frac{1}{\sqrt{D}} \sum_{k \in \mathbf{Z}_D}, \quad \delta(k) := \sqrt{D}\delta_{k,0}, \quad \varphi(k) := \mathrm{e}^{(2\pi \mathrm{i}/D)k}, \tag{4}$$

chosen so that $\mathcal{S}_k \varphi(ik) = \delta(i)$ and $\mathcal{S}_k \delta(i-k) f(k) = f(i)(i \in \mathbf{Z}_D), \forall f$. *Bell states* are defined as [18–21]

$$|ij\rangle_{\mathcal{B}} := \underset{k}{\boldsymbol{\mathcal{S}}} \varphi(ki) |k\ k-j\rangle, \quad i,j \in \mathbf{Z}_D. \tag{5}$$

Bell states are an example of maximally entangled states. In fact, any maximally entangled state can be identified with the $|00\rangle_{\mathcal{B}}$ state by suitably choosing the computational basis of each of the qudits, due to the Schmidt decomposition.

The *fidelity* of a mixed state ρ is defined as

$$F := \max_{\Psi} \langle \Psi | \rho | \Psi \rangle, \tag{6}$$

where the maximum is taken over the set of maximally entangled states. The aim of distillation protocols is to get maximally entangled pairs (fidelity 1) by means of local operations and classical communication (LOCC), starting with entangled states of fidelity lower than 1. Because of the previous comment, we will always suppose, without loss of generality, that the initial fidelity of the states to be distilled is equal to ${}_{\mathcal{B}}\langle 00|\rho|00\rangle_{\mathcal{B}}$, and the aim of our protocols will be to obtain distilled states as close as possible to this Bell state.

Of special interest are the mixtures of perfectly entangled states and white noise, known as *isotropic states*,

$$\rho_{\mathrm{iso}} := F|0\ 0\rangle_{\mathcal{B}}\langle 0\ 0| + \frac{1-F}{D^2-1}(1 - |0\ 0\rangle_{\mathcal{B}}\langle 0\ 0|), \tag{7}$$

where F is the fidelity of the state. These states are known to be entangled and distillable iff $F > 1/D$ [9].

The main interest of these states comes not only from their physical meaning, but also from the possibility of transforming any state in an isotropic one through a *twirling* operation. In general, the twirling consists in a random application of the elements of a certain group of unitary operations, say $\mathcal{U}$, to each of the systems in an ensemble. Namely, its action is

$$T_{\mathcal{U}}(\rho) := \int_{\mathcal{U}} dU U \rho U^{\dagger}. \tag{8}$$

The result of such an operator must be a sum over the states invariant under the action of the group. In the case of isotropic states, a suitable election is the set of transformations of the form $U \otimes U^*$.

When managing multiple shared pairs, vector notation is necessary; $\mathbf{k} \in \mathbf{Z}_D^n$ stands for $\mathbf{k}=(k_1,\ldots,k_n), k_i \in \mathbf{Z}_D$. A scalar product will be employed with its usual meaning. The generalization of the previous expressions is straightforward,

$$\underset{\mathbf{k}}{\boldsymbol{\mathcal{S}}} := \underset{k_1}{\boldsymbol{\mathcal{S}}} \cdots \underset{k_n}{\boldsymbol{\mathcal{S}}}, \quad \delta(\mathbf{k}) := \delta(k_1)\cdots\delta(k_n). \tag{9}$$

Again, $\mathcal{S}_{\mathbf{k}} \varphi(\mathbf{i}\cdot\mathbf{k}) = \delta(\mathbf{i})$ for any $\mathbf{i} \in \mathbf{Z}_D^n$. The computational basis and the Bell basis are

$$|\mathbf{i}\ \mathbf{j}\rangle := \bigotimes_{k=1}^{n} |i_k\ j_k\rangle,$$

$$|\mathbf{i}\ \mathbf{j}\rangle_{\mathcal{B}} := \bigotimes_{k=1}^{n} |i_k\ j_k\rangle_{\mathcal{B}} = \underset{\mathbf{k}}{\boldsymbol{\mathcal{S}}} \varphi(\mathbf{i}\cdot\mathbf{k}) |\mathbf{k}\ \mathbf{k}-\mathbf{j}\rangle, \tag{10}$$

with $\mathbf{i},\mathbf{j} \in \mathbf{Z}_D^n$. In order to simplify the notation, sometimes we will work with vectors over $\mathbf{Z}_D^{2n}$ and write states as $|\mathbf{x}\rangle$ in the place of $|\mathbf{i}j\rangle$, with

$$\mathbf{x} := (i_1,\ldots,i_n,j_1,\ldots,j_n). \tag{11}$$

B. A Partition of $\mathbf{Z}_D^n$ with divisor classes

In general, $\mathbf{Z}_D$ is not a field and thus $\mathbf{Z}_D^n$ is not a vector space but a module. We can still make use of some properties

associated with vector spaces and so we will abuse a bit of the term vector. For a detailed exposition, see Appendix A, but it is enough to know the following. The usual definition of linear independence makes sense, as one can demonstrate that any linearly independent set of vectors can be extended to a complete basis and also that a square matrix composed by such a set is invertible. A subspace is defined to be the set of linear combinations of a linearly independent set, and its dimension is the cardinality of these generators. Orthogonality poses no problem, since the set orthogonal to a subspace is a subspace, and it has the expected dimension.

Working with this pseudovector space $\mathbf{Z}_D^n$ requires care. Some vectors can be taken to the null vector by multiplying them by a nonzero number. For example, for $D=4$ we have $2\times(0,2)=(0,0)$. In order to classify this anomalous vectors, consider the set of divisors of D,

$$\mathrm{div}(D) \coloneqq \{d \in \mathbf{N}: d|D\}. \tag{12}$$

This set inherits the ordering of $\mathbf{N}$, and we shall use this property to introduce a suitable gcd function in $\mathbf{Z}_D$:

Definition II.1. For every $S \subset \mathbf{Z}_D$ we define the greatest common divisor of S, or $\gcd(S)$, to be the greatest $d \in \mathrm{div}(D)$ such that $(D/d)s=0$, $\forall s \in S$.

The nomenclature was chosen because for any $d \in \mathrm{div}(D)$ and $x \in \mathbf{Z}$ we have

$$d|x \Leftrightarrow D|\frac{D}{d}x \Leftrightarrow \frac{D}{d}x = 0 \pmod{D}, \tag{13}$$

and then for any set of integers X

$$\gcd(\bar{X}) = \max\{d \in \mathrm{div}(D): d|x \ \forall\, x \in X\}, \tag{14}$$

where $\bar{X}$ is the corresponding set in $\mathbf{Z}_D$.

Vectors over $\mathbf{Z}_D$ are n-tuples of elements in $\mathbf{Z}_D$, and so we extend the gcd function to act over $\mathbf{Z}_D^n$ in the natural way, that is, if $\mathbf{v}=(v_1,\ldots,v_n)$, $\gcd(\mathbf{v}) \coloneqq \gcd(\{v_1,\ldots,v_n\})$. Now we can consider an equivalence relation in $\mathbf{Z}_D^n$ governed by the equality under the gcd function. The corresponding partition consists in the sets

$$C_d(D,n) \coloneqq \{\mathbf{v} \in \mathbf{Z}_D^n : \gcd(\mathbf{v}) = d\},\ d \in \mathrm{div}(D). \tag{15}$$

The most important of these sets is $C_1(D,n)$, since it contains those vectors $\mathbf{v}$ for which $\{\mathbf{v}\}$ is linearly independent. Later we will need its cardinality when considering properties of local unitary operators acting on diagonal Bell states. Thus, it is useful to define

$$\phi_n(D) \coloneqq \begin{cases} 1 & \text{if } D = 1 \\ \mathcal{N}C_1(D,n) & \text{if } D > 1. \end{cases} \tag{16}$$

For the particular case of $n=1$, $\phi_1(x)$ corresponds to Euler's totient ϕ function [22]. Euler's ϕ function appears naturally in number theory since it gives for a natural number n, the cardinality of the set $\{m=1,\ldots,n-1:\gcd(m,n)=1\}$. That is, $\phi_1(n)$ is the total number of coprime integers (or totatives) below or equal to n. For example, there are eight totatives of 24, namely, $\{1,5,7,11,13,17,19,23\}$, thus $\phi_1(24)=8$. For $n \neq 1$, we have therefore introduced a generalization of Euler's totient function for elements in $\mathbf{Z}_D^n$. The following lemma tells us how to compute the cardinalities of the sets $C_d(D,n)$, which shall naturally arise in our analysis of distillation protocols.

TABLE I. Values of the generalized Euler's totient function $\phi_n(D)$ for several qudit dimensions D.

D	2	3	4	5	6
$\phi_1(D)$	1	2	2	4	2
$\phi_2(D)$	3	8	12	24	24
$\phi_3(D)$	7	26	56	124	182

Lemma II.2. For every $n \in \mathbf{N}$, $D \in \mathbf{N}-\{1\}$ and $d \in \mathrm{div}(D)$,

$$\text{(i)}\ \phi_n(D) = D^n \prod_{\substack{p|D \\ p \text{ prime}}} \frac{p^n-1}{p^n}, \tag{17}$$

$$\text{(ii)}\ \mathcal{N}C_d(D,n) = \phi_n\left(\frac{D}{d}\right), \tag{18}$$

$$\text{(iii)}\ \sum_{d' \in \mathrm{div}(D)} \phi_n(d') = D^n. \tag{19}$$

The proof of this lemma can be found in Appendix B. As an illustration, we list several values of $\phi_n(D)$ in Table I.

III. THE GROUP OF LOCAL PERMUTATIONS

The main constraint Alice and Bob have to face when they intend to distill qudits is that they can perform only local operations. If we consider only unitary operations, we are led to the group $\mathcal{U}_{\mathrm{loc}}$ of local unitary operations. Its elements are all of the form

$$U = U_{\mathrm{A}} \otimes U_{\mathrm{B}}. \tag{20}$$

In this section, we shall study the subgroup, $\mathcal{U}_{\mathrm{B\ loc}}$ defined as the group of local unitary operations which are closed over the space of Bell diagonal states, that is, states of the form

$$\rho^{(n)} = \sum_{\mathbf{x} \in \mathbf{Z}_D^{2n}} p_{\mathbf{x}}^{(n)} |\mathbf{x}\rangle_{\mathcal{B}}\langle\mathbf{x}|, \tag{21}$$

where the label (n) is a reminder that we are considering states of n pairs of qudits. The aim is to use the acquired knowledge to devise distillation protocols specially suited for these states.

More specifically, we analyze the group $\mathcal{U}_{\mathrm{B\ loc}}(D,n)$ of local unitary operators over the space spanned by the tensor product of n pairs of qudits of dimension D for which the image of a Bell diagonal state is another Bell diagonal state. The first we notice is that the result of applying such an operator over a pure Bell state is another Bell state (it cannot be the convex sum of several Bell states because it must remain pure). Since the mapping of Bell states must be one-to-one, the action of any $U \in \mathcal{U}_{\mathrm{B\ loc}}(D,n)$ involves a permutation of the Bell states,

TABLE II. Values of the number of elements of the group $\mathcal{P}_S(D,n)$ for several qudit dimensions D.

D	2	3	4	5	6
$\mathcal{NP}_S(D,1)$	6	24	48	120	144
$\mathcal{NP}_S(D,2)$	720	51840	737280	9.36×10^6	$\sim3.7\times10^7$
$\mathcal{NP}_S(D,3)$	1451520	$\sim9.2\times10^9$	$\sim3.0\times10^{12}$	$\sim9.1\times10^{13}$	$\sim1.3\times10^{16}$

$$U\rho U^\dagger = \sum_{\mathbf{x}\in\mathbf{Z}_D^{2n}} p_{\mathbf{x}}^{(n)} |\pi(\mathbf{x})\rangle_{\mathcal{B}}\langle\pi(\mathbf{x})|, \tag{22}$$

where $\pi:\mathbf{Z}_D^{2n}\to\mathbf{Z}_D^{2n}$ is a permutation. So we introduce $\mathcal{P}_{\text{loc}}(D,n)$, the *group of local permutations*, as the set of permutations over $\mathbf{Z}_D^{2n}$ implementable over Bell states by local (unitary) means.

Before stating the main result of this section, we shall define several groups. Consider the family of unitary operators $u_{\mathbf{x}}(\mathbf{x}\in\mathbf{Z}_D^{2n})$ over Bob's part of the system such that by definition

$$1\otimes u_{\mathbf{x}}^*|\mathbf{0}\rangle_{\mathcal{B}} := ||\mathbf{x}\rangle_{\mathcal{B}}, \tag{23}$$

where conjugation is taken with respect to the computational basis. With these operators at hand, we construct the group $\mathcal{U}_{\text{B inv}}(D,n)$ with the elements $U_{\mathbf{x}} := u_{\mathbf{x}}\otimes u_{\mathbf{x}}^*$. We claim that it is a subgroup of $\mathcal{U}_{\text{B loc}}(D,n)$. An explicit calculation shows that the action of its elements is

$$U_{\mathbf{x}}|\mathbf{y}\rangle_{\mathcal{B}} = \varphi(\mathbf{x}^t\Omega\mathbf{y})|\mathbf{y}\rangle_{\mathcal{B}}, \tag{24}$$

where $\Omega\in\mathbf{M}_{2n\times2n}(\mathbf{Z}_D)$ is

$$\Omega := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{25}$$

So the special feature of $\mathcal{U}_{\text{B inv}}$ is that for $\rho^{(n)}$ Bell diagonal $U_{\mathbf{x}}\rho^{(n)}U_{\mathbf{x}}^\dagger=\rho^{(n)}$, which means that its elements implement the identity permutation.

We also define two subgroups of the group of permutations over $\mathbf{Z}_D^{2n}$. The *translation group* $\mathcal{P}_T(D,n)$ contains the permutations of the form

$$\pi_{\mathbf{a}}(\mathbf{x}) = \mathbf{x}+\mathbf{a}, \tag{26}$$

with $\mathbf{a}\in\mathbf{Z}_D^{2n}$, and the *symplectic group* $\mathcal{P}_S(D,n)$ contains in turn those whose action is

$$\pi_M(\mathbf{x}) = M\mathbf{x}, \tag{27}$$

where $M\in\mathbf{M}_{2n\times2n}(\mathbf{Z}_D)$ is such that

$$M^t\Omega M = \Omega. \tag{28}$$

$\mathcal{P}_S(D,n)$ is a finite nonsimple group. A suitable generator set for this group is presented in Appendix C. Now, we are in a position to establish the following theorem that plays an important role in the distillation protocols for qudits to be devised later on.

Theorem III.1.

1. $\mathcal{P}_{\text{loc}}$ is the semidirect product of $\mathcal{P}_S$ and $\mathcal{P}_T$,

$$\mathcal{P}_{\text{loc}}(D,n) = \mathcal{P}_T(D,n)\ltimes\mathcal{P}_S(D,n). \tag{29}$$

2. Let h be the natural homomorphism from $\mathcal{U}_{\text{B loc}}$ onto $\mathcal{P}_{\text{loc}}$; then its kernel is

$$\ker h = \mathcal{U}_{\text{B inv}}(D,n)\otimes U(1), \tag{30}$$

where $U(1)$ denotes the global phase.

We prove this theorem in Appendix D. For qubits ($D=2$), part 1 of this theorem was proved in [10] using a mapping between Bell states and Pauli matrices. Our proof does not rely on this mapping, and being completely different, it becomes general enough so as to treat all qudits of dimension D on an equal footing.

$\mathcal{P}_S$ is specially well suited to construct distillation protocols, and so it is worth a closer study of its properties. There is another interesting way of writing (28); if we call $\mathbf{u}_i$ the first n rows (columns) of M and $\mathbf{v}_i$ the last n rows (columns), the condition can be rewritten in a canonical symplectic form,

$$\mathbf{u}_i^t\Omega\mathbf{u}_j = 0,$$

$$\mathbf{v}_i^t\Omega\mathbf{v}_j = 0,$$

$$\mathbf{u}_i^t\Omega\mathbf{v}_j = \delta_{ij}. \tag{31}$$

This point of view is especially useful when systematically constructing the elements of $\mathcal{P}_S$, thanks to the following result.

Theorem III.2.

1. Consider a linearly independent set of vectors $\{\mathbf{u}_1,\ldots,\mathbf{u}_r,\mathbf{v}_1,\ldots,\mathbf{v}_s,\mathbf{v}_{r+1},\ldots,\mathbf{v}_{r+t}\}\subset\mathbf{Z}_D^{2n}$ with $(s\leqslant r\leqslant n, s+t\leqslant n)$. If this set satisfies conditions (31), it is always possible to complete it while preserving them.

2. The cardinality of $\mathcal{P}_S$ is

$$\mathcal{NP}_S(D,n) = D^{n^2}\prod_{k=1}^{n}\phi_{2k}(D). \tag{32}$$

We prove this theorem in Appendix E. As an illustration, we list several values of $\mathcal{NP}_S(D,n)$ in Table II. Clearly numbers grow fast, which makes unfeasible any numerical investigation which requires going over the elements of the whole group even for not very large values of n. In any case, it can be helpful to have an algorithm which allows this task without the expense of storing the elements. Consider any suitable ordering over $\mathbf{Z}_D^{2n}$. Given an element of $\mathcal{P}_S(D,n)$, we can increase its last row according to this order until another element is reached. If this fails, the same can be done for the previous row, and so on and so forth. However, this is not very efficient, and we can do it better combining part one of theorem III.2 with lemma C.1. For example, for any of the

last n rows, we could substitute the search with the application of a suitable generator from lemma C.1. Then the additional information contained in the proof of theorem III.2 would guarantee that we were not forgetting any element of the group. Moreover, as we shall later see, typically we are only interested in some of the rows of the matrix, and then part 1 of the theorem is crucial since it allows us to ignore unimportant rows.

IV. TWIRLING WITH $\mathcal{U}_{\mathrm{B\ inv}}$ AND $\mathcal{P}_{\mathrm{loc}}$

We now explore the possibility of using the groups of the previous section with the twirling operator (8), which for finite groups is

$$T_{\mathcal{U}}(\rho) \coloneqq \frac{1}{\mathcal{N}\mathcal{U}} \sum_{U\in\mathcal{U}} U\rho U^{\dagger}. \tag{33}$$

Consider now the group $\mathcal{U}_{\mathrm{B\ inv}}(D,n)$. From (24), it follows that

$$\boldsymbol{\mathcal{S}}_{\mathbf{z}} U_{\mathbf{z}}|\mathbf{x}\rangle_{\mathcal{B}}\langle\mathbf{y}|U_{\mathbf{z}}^{\dagger} = \delta(\mathbf{x}-\mathbf{y})|\mathbf{x}\rangle_{\mathcal{B}}\langle\mathbf{x}|, \tag{34}$$

which means that the action of $T_{\mathcal{U}_{\mathrm{B\ inv}}}$ over a state leaves Bell diagonal elements invariant, whereas the off-diagonal components are sent to zero.

The group $\mathcal{P}_{\mathrm{S}}$ can also be successfully used in twirling operations. This asseveration, however, has no meaning by itself since $\mathcal{P}_{\mathrm{S}}$ is not a group of transformations over the n pairs of qudits. We have to choose any mapping $U:\mathcal{P}_{\mathrm{S}} \rightarrow \mathcal{U}_{\mathrm{B\ loc}}$ such that

$$U(\pi)|\mathbf{x}\rangle_{\mathcal{B}}\langle\mathbf{x}|U^{\dagger}(\pi) = |\pi(\mathbf{x})\rangle_{\mathcal{B}}\langle\pi(\mathbf{x})|. \tag{35}$$

There are many possible realizations for this mapping, and at least in general the image of the mapping is not a subgroup of $\mathcal{U}_{\mathrm{B\ loc}}$. However, it *is* a group when considered as a set of transformations over Bell diagonal states. Thus, for ρ Bell diagonal the following makes sense:

$$T_{\mathcal{P}_{\mathrm{S}}}(\rho) \coloneqq \frac{1}{\mathcal{N}\mathcal{P}_{\mathrm{S}}} \sum_{\pi\in\mathcal{P}_{\mathrm{S}}} U(\pi)\rho U(\pi)^{\dagger}. \tag{36}$$

To perform the sum, we need to know which are the states invariant under the action of the group.

Theorem IV.1. For every $\mathbf{x},\mathbf{y}\in\mathbf{Z}_D^{2n}$, $\gcd(\mathbf{x})=\gcd(\mathbf{y})$ if and only if there exists a permutation in $\mathcal{P}_{\mathrm{S}}(D,n)$ with associated matrix M such that $\mathbf{x}=M\mathbf{y}$.

Proof. The if direction follows from M being invertible, since then $dM\mathbf{i}=Md\mathbf{i}=0$ iff $d\mathbf{i}=0$. We now prove only the if direction. Let $d=\gcd(\mathbf{x})$ and consider any $\mathbf{u}\in\mathbf{Z}_D^{2n}$ such that $d\mathbf{u}=\mathbf{x}$ [note that $\gcd(\mathbf{u})=1$]. $\{\mathbf{u}\}$ is linearly independent, and so there exists a matrix M associated to a permutation in $\mathcal{P}_{\mathrm{S}}(D,n)$ having $\mathbf{u}$ as its first column (see theorem III.2). Then, if $\mathbf{v}=(d,0,\ldots,0)$ we have $\mathbf{x}=M_1\mathbf{v}$. The same reasoning is true for $\mathbf{y}$, giving $\mathbf{y}=M_2\mathbf{v}$ and thus $M=M_1M_2^{-1}$. □

Now, let us recall the partition in $\mathbf{Z}_D^{2n}$ associated to the function gcd [see (15)]. We define the related states

$$\rho_d \coloneqq \frac{1}{\mathcal{N}C_d} \sum_{\mathbf{x}\in C_d} |\mathbf{x}\rangle_{\mathcal{B}}\langle\mathbf{x}|. \tag{37}$$

These are the invariant states we were searching for. Thus, if ρ is Bell diagonal,

$$T_{\mathcal{P}_{\mathrm{S}}}(\rho) = \sum_{d\in\mathrm{div}(D)} \frac{\mathrm{Tr}(\rho_d\rho)}{\mathrm{Tr}(\rho_d\rho_d)}\rho_d. \tag{38}$$

Note that we have not taken into account the number of pairs involved, since it is unimportant. However, usually twirling operations are interesting for $n=1$. In this case, in analogy with isotropic states, we shall call heterotropic states those states invariant under (38). If ρ is not Bell diagonal, we can still obtain the same result with the operator

$$T_{\mathcal{U}_{\mathrm{B\ loc}}\times\mathcal{P}_{\mathrm{S}}}(\rho) \coloneqq \frac{1}{\mathcal{N}\mathcal{U}_{\mathrm{B\ inv}}}\frac{1}{\mathcal{N}\mathcal{P}_{\mathrm{S}}} \sum_{\pi\in\mathcal{P}_{\mathrm{S}}}\sum_{U\in\mathcal{U}_{\mathrm{B\ inv}}} U(\pi)U\rho U^{\dagger}U(\pi)^{\dagger}. \tag{39}$$

As a corollary, if D is prime there are just two Bell diagonal invariant states,

$$\rho_1 = \frac{1}{D^{2n}-1}(1-|0\rangle_{\mathcal{B}}\langle 0|), \tag{40}$$

$$\rho_D = |0\rangle_{\mathcal{B}}\langle 0|, \tag{41}$$

and thus the result of the twirling operation is an isotropic state, which is the simplest example of a heterotropic state.

V. PERMUTATION ASSISTED DISTILLATION

In the distillation protocols we consider, which are iterative, each iteration cycle can be decomposed in the following steps.

1. At start, Alice and Bob share n qudit pairs of dimension D and state matrix $\rho^{(n)}$.
2. They apply by local means one of the permutations $\pi_M\in\mathcal{P}_{\mathrm{S}}(D,n)$ in (27).
3. They measure the last n-m qudit pairs, both of them in their computational basis.
4. If the results of the measurement agree for each of the measured pairs, they keep the first m pairs (in the state $\rho^{(m)}$). Otherwise, they discard them.

In most situations, the initial n pairs are independent and have equal state matrices ρ. In these cases

$$\rho^{(n)} = \rho^{\otimes n}. \tag{42}$$

In general (for $m>1$) this does not guarantee that $\rho^{(m)}$ will be a product state, however, and thus it is preferable to consider the most general case.

The process can be performed several times in order to improve the entanglement progressively, but it is worth taking into account that a scheme of this kind with s steps and, say, $n=2$ and $m=1$, is equivalent to a single-step one with $n'=2^s$ and $m'=1$. It is enough to perform initially all the

permutations and afterward all the measurements *at the same time*. Although convergence properties are the same, the equivalence is not complete since from a practical point of view the step-by-step method will give a better yield. This is so because an undesired result in the measurement is more harmful in the second case, as more pairs must be discarded at once. An example clarifies this issue. Let us take a step-by-step case with $n=2$ and $m=1$, with a probability of success at the first step of P_1, and P_2 similarly for the second step. Then the yield in this case is $P_1P_2/2^2$. However, in the single-step protocol ($n'=2^2$, $m'=1$), there is a single probability of success given by $P_1^2P_2$, thus the corresponding yield is $P_1^2P_2/2^2$. Therefore, we see that in the single-step protocol there is an extra factor of $P_1<1$ that reduces its yield with respect to the step-by-step protocol, and this reduction gets amplified when considering a higher number of steps in the distillation.

In Appendix F, we derive an expression for the state of the remaining pairs of qudits after a successful measurement. It appears that the protocol is blind to nondiagonal states (in the Bell basis). So let us define

$$p_{\mathbf{x}}^{(n)} := {}_{\mathcal{B}}\langle \mathbf{x}|\rho^{(n)}|\mathbf{x}\rangle_{\mathcal{B}}, \quad \mathbf{x} \in \mathbf{Z}_D^{2n};$$

$$p_{\mathbf{x}}^{(m)} := {}_{\mathcal{B}}\langle \mathbf{x}|\rho^{(m)}|\mathbf{x}\rangle_{\mathcal{B}}, \quad \mathbf{x} \in \mathbf{Z}_D^{2m}.$$

If we call V_M the space generated by the last $n-m$ rows of M (the matrix associated to π_M), the probability of obtaining the desired measure is

$$P = \sum_{\mathbf{x}\in V_M^{\perp}} p_{\mathbf{x}}^{(n)}, \tag{43}$$

and the recurrence relation for the probabilities is

$$p_{\mathbf{x}}^{(m)} = \frac{1}{P}\sum_{\mathbf{y}\in V_M} p_{\Omega\mathbf{y}+M^{-1}\bar{\mathbf{x}}}^{(n)}, \tag{44}$$

where $\mathbf{x}\in\mathbf{Z}_D^{2m}$ and $\bar{\mathbf{x}}\in\mathbf{Z}_D^{2n}$ is

$$\bar{\mathbf{x}} := (x_1, \ldots, x_m, \underbrace{0, \ldots, 0}_{n-m}, x_{n+1}, \ldots, x_{n+m}, \underbrace{0, \ldots, 0}_{n-m}). \tag{45}$$

Note that since $M^{-1}=\Omega^t M^t \Omega$, rows $m+1$ to n (of M) do not take part in the expression, and therefore the protocol does not depend on them.

Consider the following family of heterotropic states:

$$\rho_d^{\mathrm{fix}} := \sum_{\mathbf{x}\in\mathbf{Z}_D^2} \frac{1}{Dd^2}\delta(d\mathbf{x})|\mathbf{x}\rangle_{\mathcal{B}}\langle\mathbf{x}|, \quad d\in \mathrm{div}(D). \tag{46}$$

From theorem IV.1, we know that

$$\delta(dM\mathbf{x}) = \delta(d\mathbf{x}). \tag{47}$$

Using this fact and Eq. (F4), one can readily check that for $\rho^{(n)}=\rho_d^{\mathrm{fix}\otimes n}$, Eq. (44) gives $\rho^{(m)}=\rho_d^{\mathrm{fix}\otimes m}$. Therefore, these heterotropic states are always fixed points of the protocol and candidates for attractors.

In the case of single-step protocols, we are only interested in the final joint fidelity (the probability of the state being $|\mathbf{0}\rangle_{\mathcal{B}}\langle\mathbf{0}|$),

$$F^{(m)} = \frac{1}{P}\sum_{\mathbf{x}\in V_M} p_{\Omega\mathbf{x}}^{(n)}, \tag{48}$$

where the label (m) reminds us that this is the joint probability of the m pairs being in the desired state. In general, the fidelity of each pair will be greater. If $m=1$, this distinction vanishes, and we will simply write F' instead of $F^{(1)}$. Equations (48) and (43) show how the effect of the entire process relies only on the set V_M, thereby reducing the search for efficient protocols according to part one of theorem III.2.

We now consider the Fourier transform of the probabilities,

$$p_{\tilde{\mathbf{x}}}^{(n)} := \sum_{\mathbf{x}\in\mathbf{Z}_D^{2n}} \varphi(\tilde{\mathbf{x}}\cdot\mathbf{x})p_{\mathbf{x}}^{(n)}, \quad \tilde{\mathbf{x}}\in\mathbf{Z}_D^{2n} \tag{49}$$

to obtain

$$P = D^{m-n}\sum_{\tilde{\mathbf{x}}\in V_M} p_{\tilde{\mathbf{x}}}^{(n)}, \tag{50}$$

where we have used

$$\sum_{\mathbf{v}\in V}\varphi(\mathbf{v}\cdot\mathbf{u}) := \begin{cases} 0 & \text{if } \mathbf{u}\notin V^{\perp} \\ \mathcal{N}V & \text{if } \mathbf{u}\in V^{\perp}, \end{cases} \tag{51}$$

with V being a subspace of $\mathbf{Z}_D^n$ and $\mathbf{u}\in\mathbf{Z}_D^n$. Gathering these results, we have

$$F^{(m)} = D^{n-m}\frac{\sum_{\mathbf{x}\in V_M} p_{\Omega\mathbf{x}}^{(n)}}{\sum_{\mathbf{x}\in V_M} p_{\tilde{\mathbf{x}}}^{(n)}}, \tag{52}$$

an expression for the final (joint) fidelity which can lighten its direct computation when (42) holds, since for this case we can define for $a, b\in\mathbf{Z}_D$

$$p_{ab} := {}_{\mathcal{B}}\langle ab|\rho|ab\rangle_{\mathcal{B}}, \quad p_{\tilde{a}\tilde{b}} := \sum_{a,b\in\mathbf{Z}_D}\varphi(\tilde{a}a+\tilde{b}b)p_{ab}, \tag{53}$$

and then

$$p_{\mathbf{x}}^{(n)} = \prod_{i=1}^{n} p_{x_i,x_{n+i}}, \quad p_{\tilde{\mathbf{x}}}^{(n)} = \prod_{i=1}^{n} p_{\tilde{x}_i,\tilde{x}_{n+i}}. \tag{54}$$

A. Twirling-assisted protocols

In order to understand better Eq. (44), we will adopt a useful simplification which generates by itself a whole family of distillation protocols. We consider only initial states for which the pairs are mutually independent and equal as in (42). Moreover, before each iteration we introduce any twirling operation which leads to an isotropic state while preserving the fidelity, as in (7). This way, the evolution of the state through the distillation protocol is described entirely by a single parameter, the fidelity F.

We would like to evaluate (54). We need

$$p_{ab} = F\delta_{ab} + \frac{1-F}{D^2-1}(1-\delta_{ab}), \tag{55}$$

$$p_{\bar{a}\bar{b}} = \delta_{\bar{a}\bar{b}} + \frac{D^2F - 1}{D^2 - 1}(1 - \delta_{\bar{a}\bar{b}}). \tag{56}$$

Defining $c_1(F) := (1-F)/[F(D^2-1)]$ and $c_2(F) := (D^2F - 1)/(D^2-1)$, this implies that for any $\mathbf{x}$ we have $p_{\mathbf{x}}^{(n)} = F^n c_1(F)^s$ and $p_{\bar{\mathbf{x}}}^{(n)} = c_2(F)^s$, where $n-s$ is the number of occurrences of p_{00} in the product (that is, $\mathcal{N}\{r=1,\ldots,n : x_r = x_{n+r}=0\}$). Since $p_{\Omega\mathbf{x}}^{(n)} = p_{\mathbf{x}}^{(n)}$, we can write

$$F^{(m)} = D^{n-m}F^n \frac{\chi[c_1(F)]}{\chi[c_2(F)]} \tag{57}$$

and

$$P = D^{m-n}\chi[c_2(F)], \tag{58}$$

where $\chi(x) = \sum_{s=0}^{n} \lambda_s x^s$ is a polynomial with coefficients defined by

$$\lambda_s := \mathcal{N}\{\mathbf{x} \in V_m : n - s = \mathcal{N}\{r = 1, \ldots, n : x_r = x_{n+r} = 0\}\}. \tag{59}$$

This definition is not very useful when trying to construct a suitable V_M for a given χ, but we can do better. Let V_r be the set of linear combinations of columns r and $n+r$ of the matrix formed by the last $n-m$ rows of M [or any other matrix of size $(n-m)\times 2n$ such that its rows span V_M]. If V_r is a subspace of $\mathbf{Z}_D^{n-m}$ for every r, which indeed is always the case for D prime, we can rewrite (59) as

$$\lambda_s = \mathcal{N}\{\mathbf{v} \in \mathbf{Z}_D^{n-m} : n - s = \mathcal{N}\{r = 1, \ldots, n : \mathbf{v} \in V_r^{\perp}\}\}. \tag{60}$$

We remark that χ depends only on V_M, which is a subspace of $\mathbf{Z}_D^{2n}$ of dimension $n-m$ constrained only by

$$\mathbf{u}^t \Omega \mathbf{v} = 0 \quad \forall\, \mathbf{u}, \mathbf{v} \in V_M. \tag{61}$$

It is apparent that $\chi(1) = D^{n-m}$ and $\chi(0) = 1$. For $m=1$, (57) becomes the recurrence relation $F' = F'(F)$, and then among the fixed points are $F=1$ (perfect entanglement), $F = 1/D$ (maximum fidelity for separable states) and $F = 1/D^2$ (pure noise).

Therefore, we have reduced the problem of finding the best protocol to that of finding the best coefficients for the polynomial, constrained to the existence of a suitable vector space. In the next subsection, we survey this issue for several values of n, but previously a small consideration is worthwhile. For the identity permutation (which of course is completely useless), the coefficients of the polynomial are $\lambda_s = \binom{n-m}{s}(D-1)^s$ and therefore

$$P = \left(\frac{1 + (D-1)F}{D}\right)^{n-m}. \tag{62}$$

One expects the probability of a useful protocol to be less than this, but then the decay is at least exponential with respect to an increase in $n-m$. This is an early advisory that considering progressively larger values of n need not be better.

1. Low fidelity states

Now we will concentrate on low fidelity states near $F = 1/D$. Since hashing and breeding protocols are available for high fidelities [6,11], one reason for studying this range is that it is the natural testing ground for the class of protocols we are analyzing. It is interesting also because we can develop a method to compare in a simple manner protocols with different n.

We start by discarding protocols with $m>1$. In order to see why this is reasonable, let us consider the individual fidelities of each of the resulting m pairs, say F_i, $i = 1, \ldots, m$. For isotropic states, $F \leqslant 1/D$ is equivalent to separability, and thus $F_i(1/D) \leqslant 1/D$. Since $F^{(m)}(1/D) = 1/D^m$, for uncorrelated pairs we have $F_i = 1/D$. However, for correlated pairs in general (although not necessarily) the individual fidelities will be less than $1/D$, making the algorithm useless near the point of interest. We will see later how protocols with $m>1$ can be fruitfully used.

A problem arising when comparing different protocols is that several factors take part at the same time, making it difficult to balance them in a simple manner. In our case, we have to take into account the probability of obtaining the right measure P, the number of pairs used n, and the output fidelity F'. We will now see, however, that restricting our attention to low fidelity states allows us to introduce a single coefficient, which makes possible the comparison. We shall call this coefficient the *joint performance* η of a distillation protocol and it is constructed as follows.

Let us consider an isotropic state of fidelity $(1/D)+\epsilon$. After q steps of the protocol, at the lowest order in ϵ, the state will have a fidelity $(1/D)+F_1^q\epsilon$ and the yield will be $(P_0/n)^q$, with

$$F_1 := \left.\frac{dF'}{dF}\right|_{F=1/D} = n - \frac{2D}{D^2-1}\left[\frac{d}{dx}\log[\chi(x)]\right]_{x=1/(D+1)}, \tag{63}$$

$$P_0 := \left. P \right|_{F=1/D} = D^{1-n}\chi\left(\frac{1}{D+1}\right). \tag{64}$$

We will assume $F_1 > 1$, since the protocol must be meaningful. The yield after amplifying ϵ by a factor t is $\eta^{\log(t)}$, and thus it is justified to introduce the coefficient

$$\eta := \exp\left(\frac{\log(P_0) - \log(n)}{\log(F_1)}\right). \tag{65}$$

As $F_1 < n$ and $P_0 \leqslant 1$, then $\eta < e^{-1}$.

We are ready to compare several protocols, which we shall do progressively increasing the number of discarded pairs.

(i) $n=2$. When Eq. (60) applies, there are just two possibilities. One corresponds to the identity permutation and the other is

$$\chi(x) = 1 + (D-1)x^2. \tag{66}$$

This corresponds to the original distillation protocol discussed in [6], as we expected. If D is not prime, there are other possibilities, but η is not greater for them.

(ii) $n=3$. We must distinguish two cases. If D is odd, the best value of η is attained with

$$\chi(x) = 1 + (D^2 - 1)x^3. \tag{67}$$

If D is even, however, the best option is

$$\chi(x) = 1 + (D - 1)x^2 + (D^2 - D)x^3. \tag{68}$$

The difference is due to the impossibility of constructing a suitable V_M in the second case, as we now show. Let $\{\mathbf{u},\mathbf{v}\}$ be a basis of V_M. Then, condition (61) is equivalent to

$$\sum_{i=1}^{3} \begin{vmatrix} u_i & u_{3+i} \\ v_i & v_{3+i} \end{vmatrix} = 0. \tag{69}$$

In order to obtain Eq. (67), the determinants appearing in the sum should have an invertible value [see Eq. (60)], but then they cannot sum up 0 if D is even.

(iii) $n=4$. In this case, we have found that the best polynomial is

$$\chi(x) = 1 + 4(D - 1)x^3 + (D^3 - 4D + 3)x^4. \tag{70}$$

As an example of realizing this case, set $V_M=\mathrm{Lin}\{\mathbf{u},\mathbf{v},\mathbf{w}\}$ with

$$\mathbf{u} = (1,0,0,1,0,1,0,0), \tag{71}$$

$$\mathbf{v} = (0,1,0,0,1,0,1,0), \tag{72}$$

$$\mathbf{w} = (1,1,-1,0,0,0,0,1). \tag{73}$$

Figure 1 displays the values of η for these protocols and several dimensions. Note the bad performance of the case $n=2$ for qubits, which is in fact the most important of all. On the other hand, qutrits ($D=3$) obtain the best yield among the proposed protocols, thanks to the advantage of odd dimensionality (for $n=3$). In connection with this, see also Fig. 2.

One could ask whether further improvement on η is possible by means of increasing n. Figure 1 suggests that this is not the case, at least for $D>2$. Exploration shows that nothing is gained in the case of qubits either. This result is an indication of the futility of increasing n with the aim of improving performance within the context of the current protocol. In [10] it is claimed that protocols with higher n should improve the yield, but apparently they do not take into account the (strong) reduction in the probability as n increases. This idea clarifies Fig. 1, since from Eq. (62) we expect $P_0 < 2^{n-1}(D+1)^{1-n}$ and then the reduction of the probability with n is more dramatic as D increases, whereas the performance gain from F_1 is at most linear ($F_1<n$).

2. Protocols with $m>1$

When considering states of higher fidelity, an important advantage of the proposed protocol for $n=3$ and D odd is that the derivative of $F'(F)$ vanishes for $F=1$, a qualitative difference with the $n=2$ case (see Fig. 2). This is important for states close to the Bell state, since a fidelity $1-\epsilon$ is mapped to $1-O(\epsilon^2)$. We now show how the ratio $n/m=2$ can be preserved while this desirable characteristic is added.

Using the definitions in lemma C.1, consider the permutation

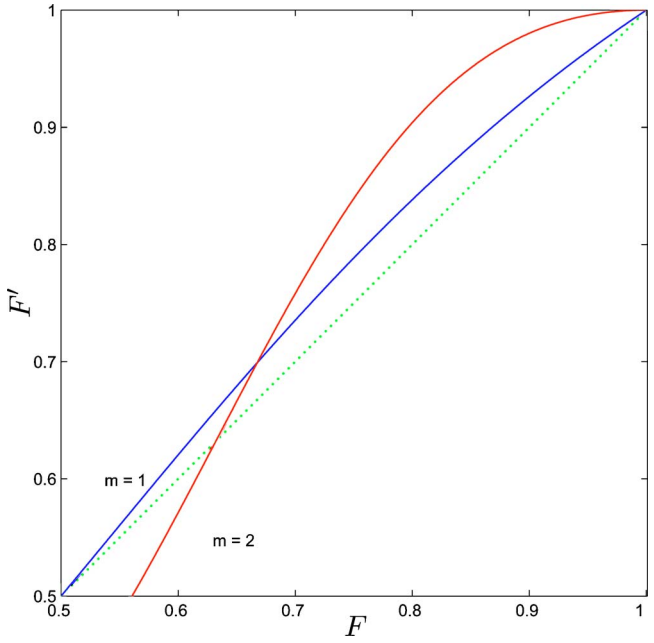


FIG. 3. (Color online) Evolution of fidelity through the proposed $n=2m$ twirled-assisted protocols for $D=2$.

$$\pi_{++}^{kl} := (\pi_{+}^{kl} \circ \pi_{+}^{l} \circ \pi_{+}^{k})^{-1} \circ \pi_{+}^{k} \circ \pi_{+}^{kl}. \tag{74}$$

The action of π_{++}^{12} is

$$\mu(\mathbf{i},\mathbf{j}) = \mathbf{i}, \tag{75}$$

$$\nu(\mathbf{i},\mathbf{j}) = (j_1 + i_2, j_2 + i_1, j_3, \ldots, j_n). \tag{76}$$

We propose for $n=4$ and $m=2$ a protocol in which the permutation π_M of step 2 is

$$\pi_{+}^{13} \circ \pi_{+}^{24} \circ \pi_{++}^{14} \circ \pi_{++}^{23}. \tag{77}$$

This permutation yields

$$\chi(x) = 1 + (D^2 - 1)x^4. \tag{78}$$

The resulting two pairs of qudits will be correlated, thereby providing us with a good scenario for hashing, and one could consider an iterative protocol in which the basic units were pairs of pairs of qudits (instead of pairs). We shall keep things simple by choosing $D=2$ and considering the partial traces of each of the pairs (which are equal due to symmetry of the permutation) in order to obtain the individual fidelity,

$$F' = \frac{F^4}{P}[1 + 4c_2(F)^2 + 4c_2(F)^3 + 7c_2(F)^4]. \tag{79}$$

The results for $D=2$ are displayed in Figs. 3 and 4. The yield Υ of Fig. 4 is calculated step by step through the following recursion relation:

$$\Upsilon_k = P_k \frac{m}{n} \Upsilon_{k-1}, \quad \Upsilon_0 = 1. \tag{80}$$

Regarding the $n=2$ case, the yield is greatly increased (four orders of magnitude) even for states quite near to the fixed point. The drawback is the impossibility of distillation for

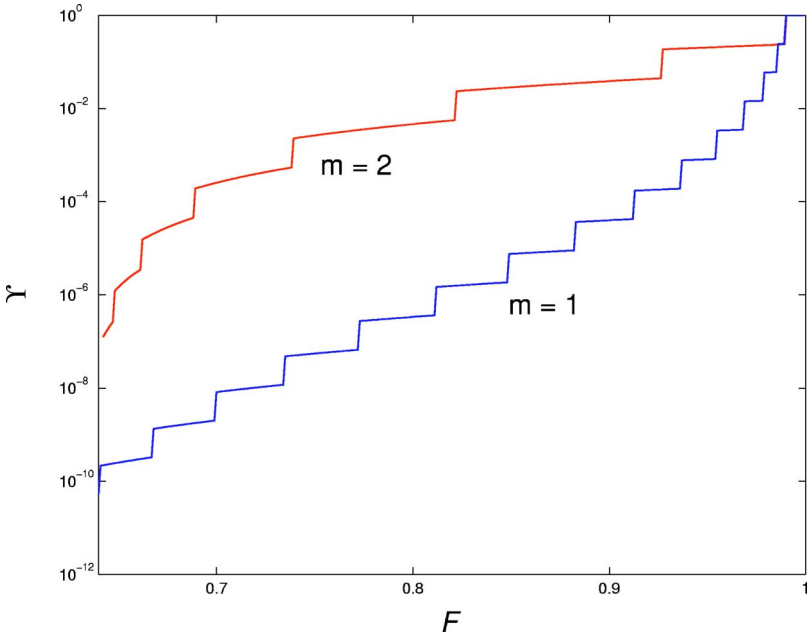


FIG. 4. (Color online) Yield Υ (80) after reaching a fidelity at least 0.99 through the proposed $n=2m$ twirled-assisted protocols for $D=2$. F is the initial fidelity.

$F \lesssim 0.64$, but let us recall that this is below the lowest fidelity distillable with a hashing method, $F \approx 0.81$ [6]. The conclusion then is that one should consider this kind of protocol in the latest steps prior to hashing.

B. Protocols without twirling

The use of twirling involves losing entanglement, and thus the protocols we have considered so far are a good starting point toward more sophisticated ones in which a careful selection of the permutations avoids the use of twirling techniques and allows for the distillation of states with fidelity less than $1/D$, if $D>2$.

1. Quantum privacy amplification

This idea was first explored (for qubits) in [7], where a quantum privacy amplification scenario was considered. In this situation, the state to be distilled is the average over an ensemble, not necessarily known, and so the permutations must work well in general. We shall now generalize this algorithm to qudits, guided by the main role the vector space V_M plays, as introduced in the beginning of Sec. V. The proposed generalization is an iteration with $n=2$ and $m=1$ as in the original case. It consists of an alternated application of two permutations,

$$\pi_+^{12} \circ \pi_+^1 \circ \pi_+^2,$$

$$\pi_+^{12} \circ (\pi_+^1 \circ \pi_+^2)^{-1}. \tag{81}$$

The (relative) simplicity of these operations is a first interesting point of the algorithm. The choice follows from the intention to preserve the form of V_M with respect to the known case $D=2$, as the number of iterations grows. For s iterations, M in this case is the $2^{s+1} \times 2^{s+1}$ matrix which would follow by considering the process as a single iteration, with a unique permutation and a unique measurement.

Although the two permutations alternate, it is possible to give a single recursion relation for every iteration cycle. To this end, let us introduce the elements of an alternative Bell basis as

$$|\mathbf{i}\ \mathbf{j}\rangle_{\mathcal{B}'} := |\mathbf{i}-\mathbf{j}\rangle_{\mathcal{B}}. \tag{82}$$

Then, in order to achieve this, it is enough to change the Bell basis to (82) after the first cycle, switch to the original Bell basis after the second, change again to (82) after the third one, and so on. with this little trick, we get the following recursion relation:

$$p'_{ij} = \frac{1}{P} \sum_{k \in \mathbf{Z}_D} p_{i+k,-i-j-k} p_{k,j-k}, \tag{83}$$

$$P = \frac{1}{D} \sum_{\tilde{k} \in \mathbf{Z}_D} p_{\tilde{k}\tilde{k}}^2. \tag{84}$$

It is interesting to note that the permutation that can switch between the two bases is not achievable by local means. If this were so, we could avoid the use of two different permutations and still get the same recursion relation, but unfortunately it is not the case.

Figure 5 shows the yield of this protocol compared to the equivalent protocol of the previous Sec. V A. The improvement is clear. As D increases, the results are less spectacular, however. An important detail is that now the distillable states are not simply those for which fidelity is greater than $1/D$. As one can check in Fig. 6, some states over this point are not distilled whereas other states beneath it are. Qubits are the only ones behaving as expected: the total volume of Bell states with $F>\frac{1}{2}$ is distilled, while those below it are undistilled. In any case, the normalized volume of states showing bad behavior, i.e., those with $F>1/D$ which are not distilled, is small if D is prime. This is not so for nonprime D's because, as discussed in Sec. V, new fixed states emerge for

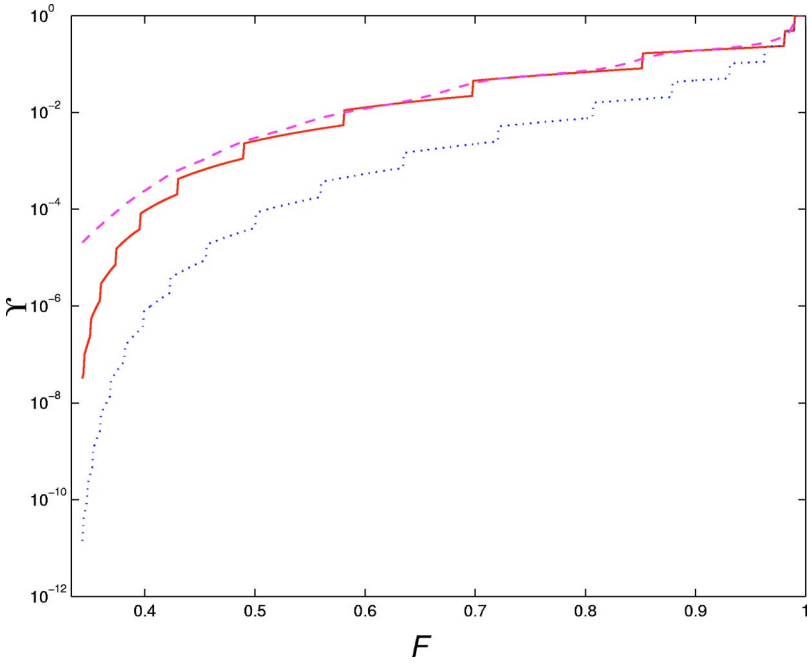


FIG. 5. (Color online) Yield Υ (80) after reaching a fidelity of at least 0.99 through the protocol proposed in the text: for isotropic states (solid line) and as a mean over Bell diagonal states (dashed line) compared to the same yield using the twirling protocol for $n=2$ (dotted line). The case under study is qutrits ($D=3$) and the mean refers to the measure discussed in Appendix G with Monte Carlo. F is the initial fidelity.

composite numbers creating undesirable attractors. We find that these attractors are especially harmful for states near to heterotropic states. As a corollary, we show that the permutational approach to distillation is more suited to prime D's.

2. Distillability

When the initial state is known, we can make use of this information to improve the distillation by selecting at each step the most convenient permutation. Then the question is whether the protocols we are managing are able to distill any distillable state. As we lack a working algorithm to decide whether a given state is distillable, we will compare the normalized volume of distilled states to that of NPPT states (states with a nonpositive partial transpose), since belonging to this set is a necessary condition for distillability.

We have chosen the following protocol with $n=2$ and $m=1$: At each step, one of the elements of $\mathcal{P}_S(D,1)$ is applied to both pairs of qudits before the permutation p_+^{12}. The element is chosen so as to give the best fidelity after the (correct) measurement. This does not necessarily lead to an optimal strategy.

Figure 7 shows the distillation capacities for $D=3$. In general, for D prime the behavior is good since all states known to be distillable, i.e., those for which the fidelity is more than $1/D$, happen to be distillable with our protocol. More precisely, we have not found computationally any counterexample of this fact. Not all the NPPT states are distilled. This is perhaps another indication of the existence of nondistillable

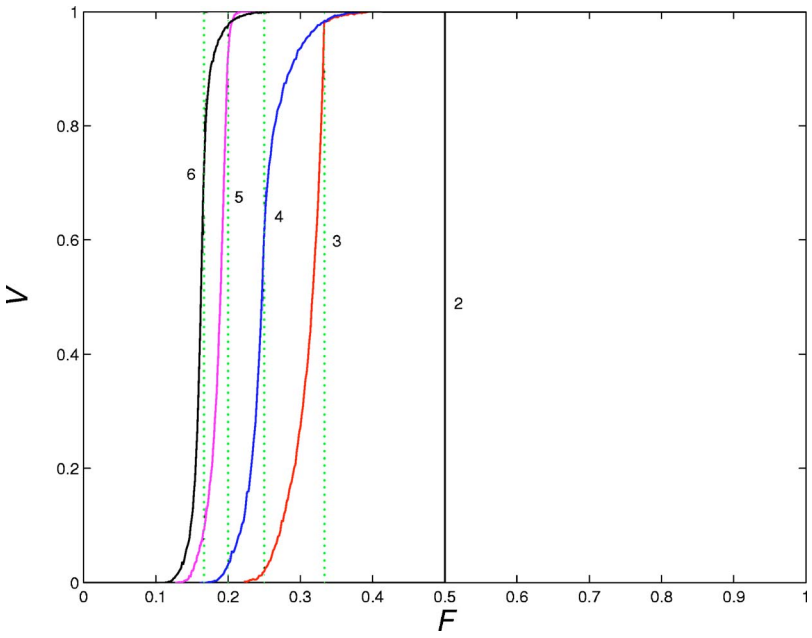


FIG. 6. (Color online) Normalized volume V of distilled Bell diagonal states for the protocol under study, given by permutations (81) with $D=2,3,4,5,6$. The measure is described in Appendix G and uses Monte Carlo. F is the initial fidelity.

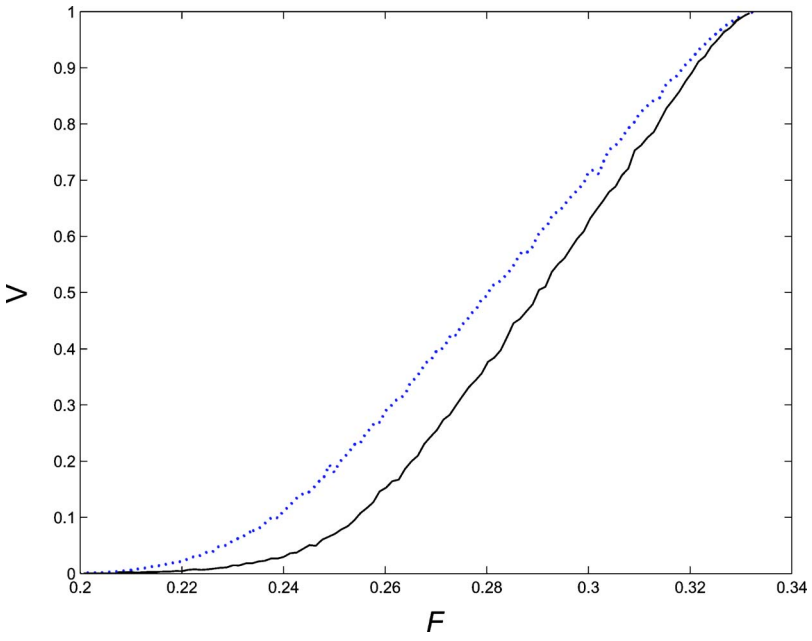


FIG. 7. (Color online) Normalized volume V of distilled Bell diagonal states compared to that of NPPT states for $D=3$. The metric and the measuring algorithm are discussed in Appendix G and uses Monte Carlo. F is the state fidelity.

NPPT states. In the case of composite numbers, the algorithm performs much worse.

VI. CONCLUSIONS AND PROSPECTS

We have shown that the study of entanglement distillation protocols based on the recursion method [5] benefits greatly from the application of basic number theory concepts when the set $\mathbf{Z}_D^n$ associated to qudits of arbitrary dimensions D is a module and not a vector space. In particular, we have found that a partition of $\mathbf{Z}_D^n$ into divisor classes is very useful to characterize the invariant properties of mixed Bell diagonal states under unitary groups that implement local permutations. These permutations, in turn, are used in very general distillation protocols based on the recursion method.

We have proposed and study a variety of distillation protocols that fall into two classes depending on whether we use twirling operations or not at intermediate steps of the protocols. When the twirling operations are absent, our distillation protocols amount to extensions of the quantum privacy amplification protocols [7] valid for arbitrary qudit dimensions D. This is very interesting and relevant for quantum communications with arbitrary large alphabets since they remain secure and operative even in the presence of quantum noisy channels.

These properties obtained from number theory are not only useful in the analytical understanding of the protocols, but also facilitate the construction of numerical methods for their study using Monte Carlo. In particular, we have characterized how the distillation protocols based on the recursion method and local permutations are qualitatively and quantitatively optimal when the dimension of the qudit states D is a prime number. We leave open the problem of how to construct better distillation protocols when D is not a prime number, and in this regard the use of the heterotropic states introduced here is a promising tool.

ACKNOWLEDGMENTS

We acknowledge financial support from the EJ-GV (H.B.) and DGS grant under Contract No. BFM 2003-05316-C02-01 (M.A.M-D.).

APPENDIX A: PROPERTIES OF THE MODULE $\mathbf{Z}_D^n$

In this appendix, we show how many ideas from genuine vector spaces can be adapted to the module $\mathbf{Z}_D^n$. First of all, we say that an element of $s \in \mathbf{Z}_D$ is *invertible* if there exists $s' \in \mathbf{Z}_D$ such that $ss'=1$. If $x \in \mathbf{N}$ is a representant of s, this is equivalent to $\gcd(x,D)=1$. When D is not prime, noninvertible elements other than zero exist (they are multiples of proper divisors of D) and we need to introduce a work around in the *Gaussian elimination* method, as we shall explain now.

Suppose we are given an element of $\mathbf{Z}_D^2$, say (x,y), and we are asked to get $x=0$ using two elementary transformations,

$$(x,y) \xrightarrow{\mathcal{O}_1} (x,x+y), \quad (x,y) \xrightarrow{\mathcal{O}_2} (x+y,y). \tag{A1}$$

The algorithm turns out to be quite simple. Consider for a moment the arbitrary ordering in $\mathbf{Z}_D$, $0<1<\cdots<D-1$. At each step, if $x \leqslant y$, use $\mathcal{O}_1$ to get $0 \leqslant y < x$; proceed inversely on the contrary. Clearly, $x=0$ or $y=0$ is reached in a finite number of steps. If $y=0$, just apply $\mathcal{O}_1$ once and $\mathcal{O}_2$ $D-1$ times.

We shall use Gaussian elimination, with the aid of the above trick, to convert any matrix M of size $p \times q$ into a very simple one. Suppose $p \leqslant q$; the converse case is similar. Summing one row to another amounts to taking the product (from the left) with a $p \times p$ invertible matrix. The same is true for columns (from the right, $q \times q$). Using these elementary operations, we can obtain

$$C = AMB, \quad C = [D\ 0], \tag{A2}$$

where A and B are invertible and D is a diagonal matrix.

With this tool at hand, we are ready to start with our analysis. We adopt the usual definition of linear independence for a finite subset of $\mathbf{Z}_D^n$, but the following is more surprising.

Definition A.1. Consider any $M \in \mathbf{M}_{p\times q}(\mathbf{Z}_D)$ and let S_r be the set of all $r\times r$ minors of M, $r \in R := \{1,\ldots,\min(p,q)\}$. The rank of M is defined as

$$\mathrm{rank}(M) := \max\{0\} \cup \{r \in R : \gcd(S_r) = 1\}. \tag{A3}$$

The rank of a matrix does not vary when we apply the elementary operations discussed above [see (14) and take into account that $d|x$ and $d|y$ iff $d|x$ and $d|x+y$]. As expected, a square matrix is invertible iff its rank is maximal. The following statement clarifies this strange definition.

Proposition A.2. The rows of a matrix $M \in \mathbf{M}_{p\times n}(\mathbf{Z}_D)$ form a linear independent (LI) set iff rank $(M)=p$.

Proof. Recall decomposition (A2) for M (we will use directly the notation there) and consider any $\mathbf{v} \in \mathbf{Z}_D^p$,

$$\mathbf{v}^t M = 0 \Leftrightarrow \mathbf{v}^t A^{-1} C B^{-1} = 0 \Leftrightarrow \mathbf{v}'^t C = 0,$$

where $\mathbf{v}=A^t\mathbf{v}'$. This shows that the rows of M form a LI set iff the rows of C do. On the other hand, $\mathrm{rank}(C)=\mathrm{rank}(M)$, and for the matrix C the statement is trivial. □

Given a set $S=\{\mathbf{v}_1,\ldots,\mathbf{v}_k\} \subset \mathbf{Z}_D^n$, we will denote by Lin S the subset of $\mathbf{Z}_D^n$ spanned by the elements of S, that is, the set of linear combinations of the vectors in S. Clearly, if S is LI, $\mathcal{N}\mathrm{Lin}\ S=D^k$, and so $k\leqslant n$. Not surprisingly, any LI set which spans $\mathbf{Z}_D$ will be called a basis of $\mathbf{Z}_D^n$. The usual definition of subspace does not work, however, and we introduce in its place the following.

Definition A.3. A set $V \subset \mathbf{Z}_D^n$ is said to be a subspace of $\mathbf{Z}_D^n$ if $V=\{0\}$ or if there exists a set $S=\{\mathbf{v}_1,\ldots,\mathbf{v}_k\} \subset \mathbf{Z}_D^n$ such that it is LI and Lin $S=V$. Such a set is called a basis of V, and its cardinality is the dimension of V (dim V).

Dimension is well defined since $\mathcal{N}V=D^{\sharp S}$ forbids the possibility of two bases of different cardinality.

Proposition A.4. Given a set $S=\{\mathbf{v}_1,\ldots,\mathbf{v}_k\} \subset \mathbf{Z}_D^n$ which is linearly independent, there exists a set $S'=\{\mathbf{v}_{k+1},\ldots,\mathbf{v}_n\}$ such that $S \cup S'$ is a basis of $\mathbf{Z}_D$.

Proof. Let M be a $k\times n$ matrix such that its rows are the elements of S. We recall (A2) but rewrite it in terms of $n \times n$ square matrices,

$$\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} M \\ 0 \end{bmatrix} B. \tag{A4}$$

Now consider the following:

$$\begin{bmatrix} M \\ M' \end{bmatrix} = \begin{bmatrix} A^{-1} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & 1 \end{bmatrix} B^{-1}. \tag{A5}$$

It is enough to construct S' with the rows of M'. □

Corollary A.5. Given a subspace V of dimension d and a set $S=\{\mathbf{v}_1,\ldots,\mathbf{v}_k\} \subset V$ which is linearly independent, there exists a set $S'=\{\mathbf{v}_{k+1},\ldots,\mathbf{v}_d\}$ such that $S \cup S'$ is a basis of V.

Proof. Select any basis of V and consider the components of vectors with respect to that basis as elements of $\mathbf{Z}_D^d$. □

We adopt the usual definition and notations for the scalar product and orthogonality.

Proposition A.6. The subset of $\mathbf{Z}_D^n$ orthogonal to a subspace V (that is, $V^\perp$) is a subspace. Moreover, $\dim V + \dim V^\perp = n$.

Proof. Let $d=\dim V$ and let M be a $d\times n$ matrix such that its rows form a basis of V. We use decomposition (A2) (again). For any $\mathbf{v} \in \mathbf{Z}_D^n$,

$$M\mathbf{v} = 0 \Leftrightarrow A^{-1} C B^{-1} \mathbf{v} = 0 \Leftrightarrow C(\mathbf{v}') = 0, \tag{A6}$$

with $\mathbf{v}=B\mathbf{v}'$. The set of the $\mathbf{v}'$'s verifying the equation is clearly a subspace of the expected dimension. □

APPENDIX B: CARDINALITY OF $C_d(D,n)$: GENERALIZED EULER'S TOTIENT FUNCTION

This appendix is devoted to the proof of Lemma II.2. We start with part 2, which can be rewritten as

$$\mathcal{N}C_1(D,n) = \mathcal{N}C_d(dD,n) \quad \forall\, D \geqslant 2, n \geqslant 1, d \geqslant 1. \tag{B1}$$

This is equivalent to the existence of a one-to-one mapping from $C_1(D,n)$ onto $C_d(dD,n)$. Consider the mapping

$$\mu : \mathbf{Z}^n \to \mathbf{Z}^n, \tag{B2}$$

$$\mathbf{v} \to d\mathbf{v}. \tag{B3}$$

μ induces a mapping $\bar{\mu}: \mathbf{Z}_D^n \to \mathbf{Z}_{dD}^n$, which is well defined and one-to-one because $x=y \pmod D \Leftrightarrow dx=dy \pmod{dD}$. From (14) we learn that $\forall \mathbf{v} \in \mathbf{Z}^n$,

$$d | \gcd(\dot{\bar{\mu}}(\bar{\mathbf{v}})),$$

where $\bar{\mathbf{v}}$ is the result of mapping $\mathbf{v}$ in $\mathbf{Z}_D^n$. Since for any $x \in \mathbf{Z}$ and $d' \in \mathrm{div}(D)$ we have $d'|x \Leftrightarrow d'd|dx$, it follows that

$$d\ \gcd(\bar{\mathbf{v}}) = \gcd(\bar{\mu}(\bar{\mathbf{v}})), \tag{B4}$$

which implies that $C_1(D,n)$ is mapped into $C_d(dD,n)$. Since for any element of $C_d(dD,n)$ there exists a suitable $\mathbf{v}$, the mapping is onto ■.

Now proving part 1 of the lemma is easy. Start with

$$\begin{aligned} \phi_n(D) &= D^n - \sum_{d \in \mathrm{div}(D)-\{1\}} \mathcal{N}C_d(D,n) \\ &= D^n - \sum_{d \in \mathrm{div}(D)-\{1\}} \phi_n\left(\frac{D}{d}\right). \end{aligned} \tag{B5}$$

Changing the index, we get a beautiful recursive relation,

$$\phi_n(D) = D^n - \sum_{d \in \mathrm{div}(D)-\{D\}} \phi_n(d). \tag{B6}$$

With some algebra on this expression it is possible to show that $\phi_n(D)$ is a multiplicative function: A function $f: \mathbf{N} \to \mathbf{N}$ is said to be multiplicative if $f(nm)=f(n)f(m)\ \forall n,m \in \mathbf{N}$ such that $\gcd(m,n)=1$. Thus, we only have to solve the recursion for $D=p^q$, p prime, but this poses no difficulty,

$$\phi_n(p^q) = p^{nq} - p^{(n-1)q}, \tag{B7}$$

from which (17) follows.

Part 3 of the lemma is merely the recursion relation just constructed.

APPENDIX C: GENERATORS OF $\mathcal{P}_S$

In order to study $\mathcal{P}_S$, it is preferable to consider its elements as permutations over $\mathbf{Z}_D^n \times \mathbf{Z}_D^n$, and so we change the notation

$$\mathbf{x} \to \pi(\mathbf{x}), \quad \mathbf{x} \in \mathbf{Z}_D^{2n} \tag{C1}$$

for

$$(\mathbf{i},\mathbf{j}) \to (\mu(\mathbf{i},\mathbf{j}), \nu(\mathbf{i},\mathbf{j})), \quad \mathbf{i},\mathbf{j} \in \mathbf{Z}_D^n, \tag{C2}$$

where the correspondence is the same as in (11).

Lemma C.1. $\mathcal{P}_S$ is generated by its following elements:

$$\pi_+^1, \quad \text{with } \mu(\mathbf{i},\mathbf{j}) = \mathbf{i},$$

$$\nu(\mathbf{i},\mathbf{j}) = (i_1 + j_1, j_2, \ldots, j_n);$$

$$\pi_{\text{xch}}^1, \quad \text{with } \mu(\mathbf{i},\mathbf{j}) = (j_1, i_2, \ldots, i_n),$$

$$\nu(\mathbf{i},\mathbf{j}) = (-i_1, j_2, \ldots, j_n);$$

$$\pi_+^{12}, \quad \text{with } \mu(\mathbf{i},\mathbf{j}) = (i_1 + i_2, i_2, \ldots, i_n),$$

$$\nu(\mathbf{i},\mathbf{j}) = (j_1, j_2 - j_1, \ldots, j_n);$$

$$\pi_{\text{swap}}^{lm}, \quad \text{with } \mu(\mathbf{i},\mathbf{j}) = (\ldots, i_{l-1}, i_m, i_{l+1}, \ldots, i_{m-1}, i_l, i_{m+1}, \ldots),$$

$$\nu(\mathbf{i},\mathbf{j}) = (\ldots, j_{l-1}, j_m, j_{l+1}, \ldots, j_{m-1}, j_l, j_{m+1}, \ldots), \quad l,m = 1, \ldots, n.$$

Proof. In order to prove this, first let us define

$$\pi_+^i := \pi_{\text{swap}}^{1i} \circ \pi_+^1 \circ \pi_{\text{swap}}^{1i}, \tag{C3}$$

$$\pi_{\text{xch}}^i := \pi_{\text{swap}}^{1i} \circ \pi_{\text{xch}}^1 \circ \pi_{\text{swap}}^{1i}, \tag{C4}$$

$$\pi_+^{ij} := \pi_{\text{swap}}^{1i} \circ \pi_{\text{swap}}^{2j} \circ \pi_+^{12} \circ \pi_{\text{swap}}^{1i} \circ \pi_{\text{swap}}^{2j}, \tag{C5}$$

with $i,j = 1, \ldots, n$. Consider any $p \in \mathcal{P}_S$; our goal is to act from the left and from the right with these permutations until we get the identity which is equivalent to the statement of the lemma. We shall use the matrix representation of the permutations, and the process is a suitable Gaussian elimination similar to the one used in Appendix A. The difference is that now we cannot perform freely any sum of lines or columns, but only those which have associated a permutation in the above set.

To work around this problem, in place of (A1) we consider

$$(x,y) \xrightarrow{\mathcal{O}_1} (x, x+y), \quad (x,y) \xrightarrow{\mathcal{O}_3(e)} (ey, x), \quad e = \pm 1. \tag{C6}$$

Since $\mathcal{O}_2$ can be constructed suitably combining $\mathcal{O}_1$ and $\mathcal{O}_3(-1)$, only the case $e=1$ is really different, but adapting the algorithm is straightforward. The point is that π_+^i and π_+^{ij} can be attached to $\mathcal{O}_1$, π_{xch}^i to $\mathcal{O}_3(-1)$, and π_{swap}^{ij} to $\mathcal{O}_3(1)$, with care in the case of π_+^{ij} and π_{swap}^{ij} for their additional effects.

To perform the elimination in an element of $\mathcal{P}_S$ with associated matrix M, start working over the first column (permutations act thereby from the left). Using p_+^i and p_{ex}^i, make zero the elements $M_{n+1,1}$ to $M_{2n,1}$, and then use p_+^{1i} and p_{swap}^{1i} until just M_{11} is nonzero in the first column. The process must be repeated for the first row (this time permutations act from the right). Now let us deal with the second column, first making zero the elements $M_{n+2,2}$ to $M_{2n,2}$, and afterward the elements $M_{3,2}$ to $M_{n,2}$. Do the same for the second row. The process must be carried out for the first n rows and columns, until we get something of the form

$$\begin{bmatrix} D & T_1 \\ T_2 & M \end{bmatrix}, \tag{C7}$$

with D diagonal, T_1 lower triangular, and T_2 upper triangular. But in fact applying the condition (28) forces $T_1 = T_2 = 0$ and $M = D^{-1}$. Now we note that

$$\begin{bmatrix} D & 0 \\ 0 & D^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -D & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ D-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \tag{C8}$$

Since the matrices in the right side are trivially constructed with the given set of generators, this ends the proof. □

APPENDIX D: PROOF OF THEOREM III.1

(This proof uses the notation and results of Appendix C.)

(1) Since $\mathcal{P}_T$ is invariant in the product group trivially, we prove both sides of the inclusion, starting with $\mathcal{P}_{\text{loc}} \subset \mathcal{P}_T \ltimes \mathcal{P}_S$.

Later we define local unitary operators implementing $\mathcal{P}_T$ [see (D7)], and so we just bother about those $U \in \mathcal{U}_{B\ \text{loc}}(D,n)$ that leave $|0\ 0\rangle_{\mathcal{B}}\langle 0\ 0|$ invariant. Moreover, as the global phase is unimportant, we select for the analysis those operators for which $U|0\ 0\rangle_{\mathcal{B}} = |0\ 0\rangle_{\mathcal{B}}$. But U is local, and then these constraints are equivalent to $U = U_A \otimes U_A^*$ (conjugation with respect to the computational basis). We can thus write

$$U|\mathbf{ij}\rangle = \sum_{\mathbf{kl}} \mathcal{S} A_{\mathbf{ki}} A_{\mathbf{lj}}^* |\mathbf{kl}\rangle, \quad \sum_{\mathbf{k}} \mathcal{S} A_{\mathbf{ik}} A_{\mathbf{jk}}^* = \delta(\mathbf{i}-\mathbf{j}) \tag{D1}$$

with A a unitary matrix on a single party (Alice or Bob). Using (5), we get

$$U|\mathbf{ij}\rangle_{\mathcal{B}} = \sum_{\mathbf{klmn}} \mathcal{S}\, \varphi(\mathbf{k}\cdot\mathbf{i} - \mathbf{m}\cdot\mathbf{l}) A_{\mathbf{lk}} A_{\mathbf{l-n,k-j}}^* |\mathbf{mn}\rangle_{\mathcal{B}}. \tag{D2}$$

On the other hand, the action of U involves a permutation over Bell states,

$$U|\mathbf{ij}\rangle_{\mathcal{B}} = \phi(\mathbf{i},\mathbf{j}) |\mu(\mathbf{i},\mathbf{j})\, \nu(\mathbf{i},\mathbf{j})\rangle_{\mathcal{B}}. \tag{D3}$$

Identifying both expressions (Bell states are orthogonal),

$$\phi(\mathbf{i},\mathbf{j})\,\delta(\mathbf{m}-\mu(\mathbf{i},\mathbf{j}))\,\delta(\mathbf{n}-\nu(\mathbf{i},\mathbf{j})) = \sum_{\mathbf{kl}} \mathcal{S}\varphi(\mathbf{k}\cdot\mathbf{i}-\mathbf{l}\cdot\mathbf{m})A_{\mathbf{lk}}A^{*}_{\mathbf{l-n,k-j}}. \quad \text{(D4)}$$

Act on both sides of this equation with the operator $\mathcal{S}_{\mathbf{mn}}\varphi(\mathbf{r}\cdot\mathbf{m})A_{\mathbf{r-n,s-j}}$ to obtain

$$A_{\mathbf{r}-\nu(\mathbf{i},\mathbf{j}),\mathbf{s-j}} = \varphi(\mathbf{s}\cdot\mathbf{i}-\mathbf{r}\cdot\mu(\mathbf{i},\mathbf{j}))\,\phi(\mathbf{i},\mathbf{j})^{*}A_{\mathbf{r,s}}. \quad \text{(D5)}$$

Choose any $\mathbf{r},\mathbf{s}$ such that $A_{\mathbf{rs}}\neq 0$, interpret this equation as a recurrence relation, and consider the commutative diagram

$$\begin{array}{ccc} A_{\mathbf{rs}} & \rightarrow & A_{\mathbf{r}-\nu(\mathbf{i},\mathbf{j}),\mathbf{s-j}} \\ \downarrow & & \downarrow \\ A_{\mathbf{r}-\nu(\mathbf{i}',\mathbf{j}'),\mathbf{s-j}'} & \rightarrow & A_{\mathbf{r}-\nu(\mathbf{i},\mathbf{j})-\nu(\mathbf{i}',\mathbf{j}'),\mathbf{s-j-j}'}. \end{array}$$

Switching again to the $\mathbf{Z}_D^{2n}$ notation, the commutation condition is

$$\mathbf{x}^t\Omega\mathbf{x}' = \pi(\mathbf{x})^t\Omega\,\pi(\mathbf{x}') \quad \text{(D6)}$$

for any $\mathbf{x},\mathbf{x}'\in\mathbf{Z}_D^{2n}$. Thus, $\pi\in\mathcal{P}_{\mathrm{S}}$.

We now show that $\mathcal{P}_{\mathrm{T}}\ltimes\mathcal{P}_{\mathrm{S}}\subset\mathcal{P}_{\mathrm{loc}}$. Thanks to lemma C.1, it is enough to construct a few permutations by means of unitary local operators. We start with translations. Choosing

$$U_{\mathrm{A}}|\mathbf{i}\rangle = \varphi(\mathbf{i}\cdot\mathbf{a})|\mathbf{i}\rangle, \quad U_{\mathrm{B}}|\mathbf{i}\rangle = |\mathbf{i}-\mathbf{b}\rangle, \quad \text{(D7)}$$

with $\mathbf{a},\mathbf{b}\in\mathbf{Z}_D^n$, the effect is

$$\mu(\mathbf{i},\mathbf{j}) = \mathbf{i}+\mathbf{a}, \quad \nu(\mathbf{i},\mathbf{j}) = \mathbf{j}+\mathbf{b}.$$

This is not the only subgroup easily generated. We have also that

$$U_{\mathrm{A}}|\mathbf{i}\rangle = |S\mathbf{i}\rangle, \quad U_{\mathrm{B}}|\mathbf{i}\rangle = |S\mathbf{i}\rangle, \quad \text{(D8)}$$

with $S\in\mathbf{Z}_D^n\times\mathbf{Z}_D^n$ and invertible give

$$\mu(\mathbf{i},\mathbf{j}) = (S^t)^{-1}\mathbf{i}, \quad \nu(\mathbf{i},\mathbf{j}) = S\mathbf{j}.$$

Both of these results can be checked with a few manipulations in (10). Since π_{swap}^{lm} is physically trivial and π_{+}^{lm} is contained in the last construction, the only permutations we have not still covered are π_{+}^{1} and π_{xch}^{1}, but as these involve only the first pair of qudits we can fix $n=1$ in (D5) and try the ansatz $A_{ij}=\varphi(\eta(i,j))$. Working modulo D, this results in

$$\eta(r-\nu(i,j),s-j) = \eta(r,s)+si-r\mu(i,j)-\tilde{\phi}(i,j), \quad \text{(D9)}$$

where $\varphi(\tilde{\phi}(i,j)) := \phi(i,j)$. Solutions to this equation require η to be a second-order polynomial, limiting the permutation to

$$\mu(i,j) = aj+b\nu(i,j), \quad \nu(i,j) = -a^{-1}(i+cj), \quad \text{(D10)}$$

where $a,b,c\in\mathbf{Z}_D$, a invertible. A compatible choice for η is

$$\eta(i,j) = aij+\frac{b}{2}i^2+\frac{c}{2}j^2. \quad \text{(D11)}$$

The permutations we were searching for belong to the set of (D10).

(2) In order to prove the second part of the theorem, it is enough to analyze which are the realizations of the identity permutation. Going back to (D5) and fixing $\mu(\mathbf{i},\mathbf{j})=\mathbf{i}$ and $\nu(\mathbf{i},\mathbf{j})=\mathbf{j}$, we find the equation

$$A_{\mathbf{r-j,s-j}} = \varphi(\mathbf{s}\cdot\mathbf{i}-\mathbf{r}\cdot\mathbf{i})\,\phi(\mathbf{i},\mathbf{j})^{*}A_{\mathbf{r,s}}. \quad \text{(D12)}$$

Modulo a global phase (30), the solutions are exactly of the form

$$\phi(\mathbf{i},\mathbf{j}) = \varphi(\mathbf{a}\cdot\mathbf{i}+\mathbf{b}\cdot\mathbf{j}), \quad \text{(D13)}$$

$$A_{\mathbf{rs}} = \varphi(\mathbf{b}\cdot\mathbf{s})\,\delta(\mathbf{s}-\mathbf{r}-\mathbf{a}), \quad \text{(D14)}$$

where $\mathbf{a},\mathbf{b}\in\mathbf{Z}_D^n$. But this is $U_{\mathbf{x}}$ in (30) with

$$\mathbf{x} = (b_1,\ldots,b_n,-a_1,\ldots,-a_n). \quad \text{(D15)}$$

APPENDIX E: ORDER OF $\mathcal{P}_{\mathrm{S}}$

In this Appendix, we offer a proof of Theorem III.2.

We first note that, except for a sign, $\mathbf{u}_i$ and $\mathbf{v}_i$ play interchangeable roles. Thus it is enough to consider a case with $t=0$ (if $t\geqslant 1$, suitable exchanges between $\mathbf{u}$'s and $\mathbf{v}$'s and sign adjustments will be enough). We shall consider two cases separately, depending on whether $r<n$. In both cases the target is to find out in how many ways a new vector can be included in the set. Such a vector must fulfill (31) and be linearly independent with respect to the initial set.

Suppose $r<n$. We would like to know how many vectors can take the role of $\mathbf{u}_{r+1}$. Let $S=\{\mathbf{u}_1,\ldots,\mathbf{u}_r,\mathbf{v}_1,\ldots,\mathbf{v}_s\}$ and $V=\mathrm{Lin}\{\Omega\mathbf{v}:\mathbf{v}\in S\}$. From (31) we have $\mathbf{u}_{r+1}\in V^{\perp}$ (and no further conditions), so let $S'=\{\mathbf{u}_{s+1},\ldots,\mathbf{u}_r,\mathbf{w}_1,\ldots,\mathbf{w}_{2(n-r)}\}$ be a basis of $V^{\perp}$. We claim that $S\cup S'$ is LI, that is, the equation

$$\sum_{i=1}^{r-s} a_i\mathbf{u}_{s+j}+\sum_{i=1}^{2(n-r)} b_i\mathbf{w}_i+\sum_{i=1}^{s}(c_i\mathbf{u}_i+d_i\mathbf{v}_i) = 0$$

holds only if all the scalars are zero. This is so because taking the scalar product with $\Omega\mathbf{u}_k(k\leqslant s)$ we get $d_k=0$; using $\Omega\mathbf{v}_k$, $c_k=0$. The rest of the scalars must be zero because S' is LI. Therefore, there are $D^{r-s}\phi_{2(n-r)}(D)$ suitable vectors, since we can choose any combination of the form

$$\mathbf{u}_{r+1} = \sum_{i=1}^{r-s} a_i\mathbf{u}_{s+j}+\sum_{i=1}^{2(n-r)} b_i\mathbf{w}_i$$

for which $\gcd(\{b_1,\ldots,b_{2(n-r)}\})=1$ [this is why the factor $\phi_{2(n-r)}(D)$ appears, see (16)].

Now suppose $r=n$, $s<n$. We pursue $\mathbf{v}_{s+1}$. Let $S=\{\mathbf{u}_1,\ldots,\mathbf{u}_s,\mathbf{u}_{s+2},\ldots,\mathbf{u}_n,\mathbf{v}_1,\ldots,\mathbf{v}_s\}$ and $V=\mathrm{Lin}\{\Omega\mathbf{v}:\mathbf{v}\in S\}$. From (31) we have $\mathbf{v}_{s+1}\in V^{\perp}$ and $\mathbf{u}_{s+1}^t\Omega\mathbf{v}_{s+1}=1$. Let $S'=\{\mathbf{u}_{s+1},\ldots,\mathbf{u}_n,\mathbf{w}\}$ be a base of $V^{\perp}$ and let $s:=\mathbf{u}_{s+1}^t\Omega\mathbf{w}$. We first show that s is invertible. Let $V'=\mathrm{Lin}\{\Omega\mathbf{u}_1,\ldots,\Omega\mathbf{u}_n,\Omega\mathbf{v}_1,\ldots,\Omega\mathbf{v}_s\}$. If s is noninvertible, choose any $k\neq 0$ such that $ks=0$. Then $k\mathbf{u}_{s+1}^t\Omega\mathbf{w}=0$ implies $k\mathbf{w}\in V'^{\perp}=\mathrm{Lin}\{\mathbf{u}_{s+1},\ldots,\mathbf{u}_n\}$, but this is not possible because S' is linearly independent. We now show that $S\cup\{\mathbf{u}_{s+1},\mathbf{w}\}$ is LI. If it is not, then $\mathbf{w}\in\mathrm{Lin}(S\cup\{\mathbf{u}_{s+1}\})$, but this in turn implies $\mathbf{u}_{s+1}^t\Omega\mathbf{w}=0$, which again is false. Therefore, there are

D^{n-s} suitable vectors, since we can choose any of the following combinations:

$$\mathbf{v}_{s+1} = s^{-1}\mathbf{w} + \sum_{i=1}^{n-s} c_i \mathbf{u}_{s+i}.$$

With this, part 1 of the theorem is proved. For part 2, it only remains to count. There are $\phi_{2n}(D)$ possible values for $\mathbf{u}_1$. If $\mathbf{u}_1$ is fixed, there are $D\phi_{2(n-1)}(D)$ possible elections for $\mathbf{u}_2$. Continuing this way, one gets the desired result.

APPENDIX F: RECURSION RELATIONS FOR DISTILLATION PROTOCOLS

In this appendix, we derive an expression for the final state of the remaining pairs of qudits when the procedure of Sec. V has been successfully performed. We will use the same notation found there.

So let us define for $\mathbf{x},\mathbf{y} \in \mathbf{Z}_D^{2n}$

$$\rho_{\mathbf{xy}}^{(n)} := {}_{\mathcal{B}}\langle \mathbf{x}|\rho^{(n)}|\mathbf{y}\rangle_{\mathcal{B}}, \tag{F1}$$

from which $p_{\mathbf{x}} = \rho_{\mathbf{xx}}^{(n)}$. After the permutation with associated matrix M and phase function ϕ, the state is

$$\rho^{(n)\prime} := \sum_{\mathbf{x},\mathbf{y}\in\mathbf{Z}_D^{2n}} \phi(\mathbf{x})\phi^*(\mathbf{y})\rho_{\mathbf{xy}}^{(n)} |M\mathbf{x}\rangle_{\mathcal{B}}\langle M\mathbf{y}|. \tag{F2}$$

The measurement is performed in the computational basis (for the last $n-m$ pairs), and the rest of the pairs are kept only if this measurement coincides for each of the measured pairs (if Alice measures $|3\rangle$, so does Bob for the corresponding qudit). Going back to (5), this means that j is zero for each of the pairs. Therefore, after the measurement and taking the partial trace over the measured pairs, the state of the first m pairs is

$$\rho^{(m)} = \frac{1}{P} \sum_{\mathbf{k}\in\mathbf{Z}_D^{n-m}} {}_{\mathcal{B}}\langle \mathbf{k0}|\rho^{(n)\prime}|\mathbf{k0}\rangle_{\mathcal{B}}, \tag{F3}$$

where the Bell states must be understood to belong to the space of the last $n-m$ pairs and P is the probability of having obtained the suitable measurement. Calculating it amounts to taking the total trace,

$$P = \sum_{\mathbf{x}\in\mathbf{Z}_D^{2m}} \sum_{\mathbf{k}\in\mathbf{Z}_D^{n-m}} ({}_{\mathcal{B}}\langle \mathbf{x}| \otimes {}_{\mathcal{B}}\langle \mathbf{k0}|)\rho^{(n)\prime}(|\mathbf{x}\rangle_{\mathcal{B}} \otimes |\mathbf{k0}\rangle_{\mathcal{B}}).$$

Inserting definition (F2), we get (43).

The state of the system before the measurement can also be expressed,

$$\rho^{(n)\prime} = \sum_{\mathbf{x},\mathbf{y}\in\mathbf{Z}_D^{2n}} \phi(M^{-1}\mathbf{x})\phi^*(M^{-1}\mathbf{y})\rho^{(n)}_{M^{-1}\mathbf{x},M^{-1}\mathbf{y}} |\mathbf{x}\rangle_{\mathcal{B}}\langle \mathbf{y}|.$$

Inserting this expression in (F3),

$${}_{\mathcal{B}}\langle \mathbf{x}|\rho^{(m)}|\mathbf{y}\rangle_{\mathcal{B}} = \frac{1}{P} \sum_{\mathbf{k}\in\mathbf{Z}_D^{n-m}} \phi(M^{-1}(\hat{\mathbf{k}}+\bar{\mathbf{x}}))\phi^*(M^{-1}(\hat{\mathbf{k}}+\bar{\mathbf{y}}))\rho^{(n)}_{M^{-1}(\hat{\mathbf{k}}+\bar{\mathbf{x}}),M^{-1}(\hat{\mathbf{k}}+\bar{\mathbf{y}})}, \tag{F4}$$

where $\mathbf{x},\mathbf{y}\in\mathbf{Z}_D^{2m}$, $\bar{\mathbf{x}}$ and $\bar{\mathbf{y}}$ are defined as in (45), and

$$\hat{\mathbf{k}} := (\underbrace{0,\ldots,0}_{m},k_1,\ldots,k_{n-m},\underbrace{0,\ldots,0}_{n}).$$

With the definition for V_M given in Sec. V, we have

$${}_{\mathcal{B}}\langle \mathbf{x}|\rho^{(m)}|\mathbf{y}\rangle_{\mathcal{B}} = \frac{1}{P} \sum_{\mathbf{z}\in V_M} \phi(\Omega\mathbf{z}+M^{-1}\bar{\mathbf{x}})\phi^*(\Omega\mathbf{z}+M^{-1}\bar{\mathbf{y}})\rho^{(n)}_{\Omega\mathbf{z}+M^{-1}\bar{\mathbf{x}},\Omega\mathbf{z}+M^{-1}\bar{\mathbf{y}}}.$$

Equation (44) follows setting $\mathbf{x}=\mathbf{y}$.

APPENDIX G: MONTE CARLO MEASURING

We introduce a suitable metric in the space of Bell diagonal states in order to perform several measures. For simplicity, we have chosen the metric induced by mapping physical states into Euclidean space taking the eigenvalues as coordinates.

We have chosen a Monte Carlo approach to perform the measurements. This approach consists in randomly generating points of the space according to the measure on that space, and counting how many of them are inside the measured set.

In our case, numerically implementing such a measure is not difficult if fidelity is not low. Consider a Bell diagonal state of fidelity F. There are D^2-1 free coordinates (eigenvalues) λ_i subject to the constraints

$$0 \leqslant \lambda_i \leqslant F, \quad \sum_i \lambda_i = 1 - F. \tag{G1}$$

The random generation is achieved as follows. We take for each point D^2-2 real random variables x_i uniformly distributed in $[0,1]$ $(i=1,\ldots,D^2-2)$. Defining $x_0 := 0$ and $x_{D^2-1} := 1$, we set $\lambda_i = (1-F)(x_{i+1}-x_i)$. If $\lambda_i > F$ for any i, we simply discard the point. Otherwise, it belongs to the space of interest. Then it is checked whether it belongs to the measured set by running the proper algorithm. For example, if we are checking distillability through a given protocol, this is the moment were the protocol is numerically simulated until the point converges.

[1] M. Lewenstein, D. Bruss, J. I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, and R. Tarrach, J. Mod. Opt. **47**, 2841 (2000).

[2] D. Bruss, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, J. Mod. Opt. **49**, 1399 (2002).

[3] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[4] A. Galindo and M. A. Martin-Delgado, Rev. Mod. Phys. **74**, 347 (2002).
[5] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[6] Ch. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[7] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[8] C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
[9] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
[10] J. Dehaene, M. Van den Nest, B. de Moor, and F. Verstraete, Phys. Rev. A **67**, 022310 (2003).
[11] K. G. H. Vollbrecht and M. M. Wolf, Phys. Rev. A **67**, 012303 (2003).
[12] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[13] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[14] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1056 (1999).
[15] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruss, Phys. Rev. A **61**, 062313 (2000).
[16] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
[17] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[18] G. Alber, A. Delgado, N. Gisin, and I. Jex, e-print quant-ph/000802.
[19] G. Alber, A. Delgado, N. Gisin, and I. Jex, J. Phys. A **34**, 8821 (2001).
[20] M. A. Martin-Delgado and M. Navascues, Eur. Phys. J. D **27**, 169 (2003).
[21] M. A. Martin-Delgado and M. Navascues, Phys. Rev. A **68**, 012322 (2003).
[22] J. H. Conway and R. K. Guy, Euler's Totient Numbers, in *The Book of Numbers* (Springer-Verlag, New York, 1996), pp. 154–156.

Códigos Topológicos

JOURNAL OF MATHEMATICAL PHYSICS **48**, 052105 (2007)

Homological error correction: Classical and quantum codes

H. Bombin and M. A. Martin-Delgado[a)]
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain

(Received 13 February 2007; accepted 27 March 2007; published online 21 May 2007)

We prove several theorems characterizing the existence of homological error correction codes both classically and quantumly. Not every classical code is homological, but we find a family of classical homological codes saturating the Hamming bound. In the quantum case, we show that for nonorientable surfaces it is impossible to construct homological codes based on qudits of dimension $D>2$, while for orientable surfaces with boundaries it is possible to construct them for arbitrary dimension D. We give a method to obtain planar homological codes based on the construction of quantum codes on compact surfaces without boundaries. We show how the original Shor's 9-qubit code can be visualized as a homological quantum code. We study the problem of constructing quantum codes with optimal encoding rate. In the particular case of toric codes we construct an optimal family and give an explicit proof of its optimality. For homological quantum codes on surfaces of arbitrary genus we also construct a family of codes asymptotically attaining the maximum possible encoding rate. We provide the tools of homology group theory for graphs embedded on surfaces in a self-contained manner. © *2007 American Institute of Physics.* [DOI: 10.1063/1.2731356]

I. INTRODUCTION

Quantum error correction (QEC) is an important breakthrough in the theory of quantum information and computation. Without this technique, quantum communication over noisy channels would be doom to failure and quantum computation would remain in the realm of sheer ideal theoretical constructs: powerful in principle, but without any chance of being implemented in practice.

It was Landauer[1–3] who soon prompted the quantum information community to look seriously at the problem of quantum errors since they are more harmful than classical errors and Unruh pointed out the severe negative effects of decoherence.[4] In fact, quantum errors may show up from different sources: (i) decoherence due to undesired coupling of the quantum data with the surrounding environment; and (ii) imperfections in quantum logic gates during the execution of an algorithm.

The problem of correcting quantum errors seemed likely impossible in the beginning, since the classical error correcting techniques based on redundancy or repetition codes seemed to contradict the quantum no-cloning theorem. Moreover, besides bit-flip errors, there are phase errors with no classical counterpart and thus no previous theory to compare with.

Fortunately, all these doubts were dispelled by the first QEC code proposed by Shor[5] and independently by Steane[6] who showed how to get around these difficulties explicitly. Soon, more general quantum codes were constructed known as CSS codes[7,8] based on classical correcting codes. These codes are very easy to deal with since the correction of bit-flip errors is factorized out from the correction of phase-flip errors. CSS codes have found very important applications in the security proof of quantum cryptography protocols without resorting to quantum computers.[9]

[a)]Electronic mail: mardel@miranda.fis.ucm-es

A more general class of codes, encompassing the CSS codes, are the stabilizer codes introduced by Gottesman.[10] In the stabilizer formalism, the construction of quantum codes can be thought of as a task in finite group theory for finding Abelian subgroups of the Pauli group, leaving invariant a certain subspace which used to encode quantum words. An alternative and independent realization was provided by Calderbank *et al.*[11] using the theory of binary vector spaces.

Despite having a general theory of QEC, explicit realization of quantum codes is also important in practical implementations. In this regard, the number of encoded qubits k, or logical qubits, with respect to the number of physical qubits $n>k$ plays an important role. The first codes discovered by Shor and Steane have a ratio of 1:9 and 1:7, respectively. It is possible to show that the best possible ratio for correcting one single error is 1:5.[12,13]

The quantum codes mentioned thus far are linear, also called additive, codes since the underlying structure is that of Abelian stabilizer codes. There are also a series of interesting extensions to nonstabilizer codes[14,15] with the aim of increasing the coding capabilities of quantum codes. For instance, a type of nonadditive codes encodes six states in five qubits and can correct the erasure of any single qubit.[16] A particularly interesting proposal for non-Abelian quantum codes is due to Ruskai[17] based on correcting (2-qubit) Pauli exchange errors besides all single qubit errors. This technique can be generalized to non-Abelian stabilizer groups based on the permutation group S_n.[18]

An alternative approach to QEC was introduced by Kitaev[19] known as topological quantum codes. The notion of topological quantum computation was also addressed independently by Freedman.[20] This technique allows us to devise topological quantum memories which are robust against local errors and capable of protecting stored quantum data.[21,22]

To understand the notion of a topological code, we first notice that a basic strategy in standard QEC is to protect logical qubits by spreading them out in a larger set of physical qubits ($n>k$). This is the reminiscent of redundancy in classical codes. In topological quantum codes, we go even farther and encode quantum words in the nonlocal degrees of freedom of topologically ordered physical systems, such as certain lattice gauge theories,[19,23–25] or condensed matter systems.[26–31] Detecting topologial order is an important issue in this regard.[32,33]

Due to this nonlocal encoding, these quantum code words are intrinsically resistant to the debilitating effects of noise, as long as it remains local. This construction is rather appealing since it relies on an intrinsic physical mechanism for the topological system to self-correcting local errors. It means that in a topological code, we do not have to check and fix quantum errors from outside the system whenever they appear like in standard (nontopological) quantum codes. It is the physical properties of the system which provide the intrinsic mechanism from protecting the encoded quantum states. This mechanism is controlled by the interactions described by Hamiltonians on certain lattices embedded in surfaces with nontrivial topology. The ground states of those Hamiltonians exhibit topological order, a type of degeneracy that is robust against local perturbations since it is protected by a gap from the rest of the spectrum and, moreover, the degeneracy depends on the topology of the lattice Hamiltonian. Due to this topological order, these states exhibit remarkable entanglement properties.[34,35]

In addition to being self-correcting, topological quantum codes exhibit more interesting properties: (i) they belong to the class of stabilizer codes, and (ii) the interaction terms in the Hamiltonian realizing these codes are local, i.e., nearest-neighbor interactions. The locality of property (ii) is very important since it facilitates the potential physical implementation of these lattice systems. In contrast, the stabilizer operators in nontopological codes are generically nonlocal.

There is another method for QEC known as decoherence free subspaces (DFSs).[36–38] In this method, quantum information is protected by using symmetry. The symmetry that protects quantum information exists naturally in the interaction of the quantum information processing system with its environment. There is a unified view of QEC strategies in which both DFSs and topological codes are instances of the algebraic notion of noiseless subsystem.[39] Kribs *et al.*[40] provided a further unification of quantum error methods by introducing the notion of operator QEC. This scheme relies on a generalized notion of noiseless subsystems that is not restricted to the commutant of the interaction algebra. Therefore, these considerations make topological quantum codes

rather interesting to study since they belong to the class of stabilizer codes and share the basic properties of quantum noiseless subsystems such as DFSs, while giving us the opportunity to have a more robust decoherence protection based on the topological properties of certain quantum systems.

Practical implementations of topological quantum codes have been proposed using optical lattices[41–43] simulating spin interactions in honeycomb lattices.[26] In this paper we shall consider only two-dimensional realizations of topological codes, but it is possible to make extensions to lattices in $3+1$ dimensions.[21,44,45]

The issue of topological quantum computation,[19,46–49] as an instance of fault-tolerance quantum computing[50–56] is closely related to quantum codes. However, this work concentrates only on topological quantum codes.

In this work we use the terminology of homological codes, both classically and quantumly, to highlight the fact that they are constructed solely on the information about the graph encoded in its homology groups, either as simple graphs or as graphs embedded on surfaces.

The paper is intended to be self-contained and is organized as follows: in Sec. II, we introduce the basic notions and definitions of classical codes and homology groups over $\mathbf{Z}_2$ for graphs. With these tools, we then proof Theorem 2 that allows us to construct classical homological codes. Not every classical code is homological, but there exists optimal families of homological codes that saturate the classical Hamming bound. In Sec. III we start recalling the definitions and characterizations of quantum codes, then we construct symplectic codes for qudits, i.e., quantum states of arbitrary dimension D. The idea is to apply the symplectic group $ESp_D(n)$ to a trivial code $\mathcal{C}_T(n,k)$ of distance 1. Symplectic codes are equivalent to stabilizer codes. We also introduce homology of 2-complexes, which are two dimensional generalizations of a graph or 1-complex. With these tools we go on to prove Theorem 4 for constructing qudit symplectic codes based on the homology and cohomology groups of graphs embedded in surfaces. Technically, these graph embeddings are called surface 2-complexes that are also introduced earlier. In particular, the celebrated Shor's original 9-qubit code can be thought of as a homological quantum code belonging to a family of codes $[[d^2,1,d]]$, with $d=3$ (see Fig. 20). Another topological realization exists for the Shor code on the projective plane.[58] In general, homological quantum codes can be degenerate codes. Next we prove a number of important results: as follows.

(i) The subgroup $\mathbf{Z}_2$ appearing in the first homology group of nonorientable surfaces is called the torsion subgroup. It plays an important role in the construction of homological quantum error correcting codes for qudits of dimension greater than 2. We show that it is impossible to construct these codes with $D>2$ on nonorientable surfaces, while it is possible to do so for codes based on qubits. For orientable surfaces with boundaries, it is possible to have homological codes of arbitrary dimension D.

(ii) We introduce the notion of topological subadditivity which is very helpful to find bounds on the efficiency (coding rates) of homological quantum codes.

(iii) For homological quantum codes on the torus, we find a family of optimal codes that outperform the original toric codes introduced in Ref. 19 and in addition, our optimal codes are extended for qudits.

(iv) We construct an explicit family of quantum homological codes for which we can show that the rate k/n of logical qubits to physical qubits approaches unity using topological graphs embedded on surfaces of arbitrary genus.

(v) It is possible to transform homological codes on compact surfaces of arbitrary genus, such as the g-torus, into homological codes embedded into planar surfaces with boundaries; this is interesting for practical purposes since constructing real torus of higher genus does not seem to be feasible.

The results concerning the quantum encoding rate were advanced without proof[57] in the particular case of qubits ($D=2$).

Section. IV is devoted to conclusions. In Appendix A we construct the generators of the sympletic group $Sp_D(n)$ for the general case of qudits, in Appendix B we give a detailed explicit

proof of the subadditivity property of quantum topological codes, and in Appendix C we prove that our homological quantum codes for qudits on the torus are optimal as far as the coding rate k/n is concern.

II. HOMOLOGICAL CODES FOR CLASSICAL ERROR CORRECTION

A. Classical error correcting codes

Classical error correction deals with the problem of transmitting messages through noisy channels.[59,60] Usually messages are composed with bits, which can take on the values 0 or 1. Such strings of bits, or *words*, can be regarded as vectors over the field $\mathbf{Z}_2$. The same idea holds for the errors introduced in a Communication, for if u and v are, respectively, the input and output words, we say that the channel has produced the error

$$e := v - u. \tag{1}$$

An important channel is the *(binary) symmetric channel*. This channel acts on each bit individually, flipping its value with certain probability $1-p$, $p>\frac{1}{2}$. Due to the symmetry between 0 and 1, it is possible to assign a probability to any given error e, since it does not depend on the input u. We introduce the *weight* of a vector $u \in \mathbf{Z}_2$, written $\mathrm{wt}(u)$, as the number of nonzero components of u. With this definition, for the symmetric channel we have that the probability for a given error e to occur is $(1-p)^{\mathrm{wt}(e)}$. Thus, errors with small weight are more probable, which is important since there is no chance to correct an arbitrary error. For words u of increasing length n, we expect $\mathrm{wt}(e) \simeq np$. If we were able to correct up to np errors, we would have a successful communication with a good probability.

Given a set of errors S, we say that two words u and v are *distinguishable* with respect to S if and only if (iff)

$$\forall e,e' \in Su + e \neq v + e'. \tag{2}$$

An *error correcting code* of length n is a subset C of $\mathbf{Z}_2^n$. Its elements are called *code words*. If $|C|=2^k$, we say that C encodes k bits. C corrects S if every pair of code words in C is distinguishable with respect to S. Let $S(t)$ consist of errors with $\mathrm{wt}(e) \leqslant t$. If C corrects $S(t)$ but not $S(t+1)$, we say that C is a *t-error correcting code*. In order to characterize this property, let us introduce the *distance* between the words u and v as $d(u,v) := \mathrm{wt}(u-v)$. Since $u+e=v+e'$ implies $d(u-v)=d(e'-e)>d(e')+d(e')$, we have that two vectors with distance d are distinguishable with respect to $S(t)$ iff $d>2t$. The distance of a code is the minimum distance between any of its code words, and C is a t-error correcting code iff $d>2t$. A code of length n, distance d, and encoding k bits is usually denoted by $[n,k,d]$.

Clearly, the values of n, k, and d cannot be arbitrary for an $[n,k,d]$ code to exist. In fact, consider a t-error correcting code C of length n and $|C|=m$. Let $S_n(t)$ contain the elements of $S(t)$ of length n. Since $|S_n(t)|=\Sigma_{i=0}^{t}\binom{n}{i}$ and $u+S_n(t) \cap v+S_n(t)=\emptyset$ for any pair of code words, we have the (upper) *Hamming bound*

$$m\sum_{i=0}^{t}\binom{n}{i} \leqslant 2^n. \tag{3}$$

Setting $m=2^k$ and taking the limit of large n, k, t,

$$\frac{k}{n} < \left(1 - H\left(\frac{t}{n}\right)\right)(1-\eta), \tag{4}$$

where $\eta \to 0$ as $n \to \infty$ and $H(x)$ is the entropy function

$$H(x) := -x\log_2 x - (1-x)\log_2(1-x). \tag{5}$$

k/n is called the *rate* of the code. A question that naturally arises here is whether this bound can

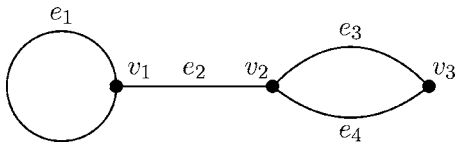


FIG. 1. A nonsimplicial graph with a self-loop e_1 and double edges e_3 and e_4.

be reached. A theorem by Shannon[61] states that this is asymptotically true, but the codes involved in the proof need not be of any practical use. For linear codes, a class of codes which we shall introduce below, there is also a lower bound known as the Gilbert-Varshamov bound: there exists a linear $[n,k,d]$ code provided

$$2^k \sum_{i=0}^{d-2} \binom{n-1}{i} < 2^n. \tag{6}$$

Again, in the limit of large numbers this becomes

$$\frac{k}{n} > \left(1 - H\left(\frac{2t}{n}\right)\right)(1-\eta), \tag{7}$$

where $\eta \to 0$ as $n \to \infty$.

We now focus on *linear codes*, which have certain properties that make them more convenient to use. A linear $[n,k,d]$ code is a subspace C of $\mathbf{Z}_2^n$ of dimension k for which $\min_{u \in C-\{0\}} \mathrm{wt}(u) = d$. The value for the distance follows from the fact that C is closed under substraction. A *generator matrix* G of C is any matrix with rows giving a basis for C. A *parity check matrix* H for C is any matrix with rows giving a basis for $C^\perp$, the subspace of vectors orthogonal to any vector in C. From this point on, vectors are column vectors. To understand why H is useful, first note that $Hu=0 \Leftrightarrow u \in C$. Thus, for any error e and code words u, v we have $H(u+e)=H(v+e)=He$, that is, H measures the error independently of the code word. He is called the error syndrome, and it gives enough information to distinguish among correctable errors. If this were not true, then we would have a pair of correctable errors such that $H(e-e')=0 \Rightarrow e-e' \in C$, a contradiction since $\mathrm{wt}(e-e') < \mathrm{wt}(e)+\mathrm{wt}(e') \leqslant 2t < d$. The real usefulness of linear codes comes from the fact that many codes can be constructed in such a way that the deduction of the error from the syndrome is a fast operation. As an easy example (due to Hamming), consider the following check matrix for a [7,4,3] code

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{8}$$

Notice that columns are the binary representation of numbers from one to seven, and thus in this case the error syndrome gives the position of the (single) error.

B. Homology of graphs

A *graph*, intuitively, is a collection of *vertices* and *edges*. Each edge connects two (non-necessarily distinct) vertices. Figure 1 shows how a graph can be depicted as a collection of points or nodes (vertices) linked by curves (edges). In such a representation, any intersection of edges at points which are not vertices is meaningless. The idea of a graph can be formalized in several ways. We take here a combinatorial approach, rather than topological, and we do not introduce any orientation for the edges.

A (finite) graph $\Gamma=(V,E,I)$ [or, if needed, $(V_\Gamma, E_\Gamma, I_\Gamma)$] consists of a finite set E of edges, a finite set V of vertices, and an incidence function $I: E \to \mathcal{P}(V)$ such that

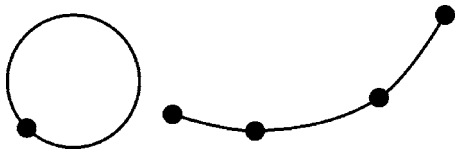


FIG. 2. The cycle C_1 and the path P_4.

$$1 \leqslant |I(e)| \leqslant 2, \quad \forall\, e \in E. \tag{9}$$

As usual, $\mathcal{P}(V)$ denotes the power set of V, that is, the set of subsets of V. The condition over I reflects the fact that an edge can only have one or two end points (in the former case, it is a *self-loop*). It is possible to arrange the information conveyed by I in a so-called *incidence matrix*. To this end, denote $V \coloneqq \{v_i\}_{i=1}^{|V|}$ and $E \coloneqq \{e_j\}_{j=1}^{|E|}$. The incidence matrix has $|V|$ rows and $|E|$ columns. The entry in row i and column j is 0 if $v_i \notin I(e_j)$, and $3-|I(e_j)|$ if $v_i \in I(e_j)$. The incidence matrix for the graph in Fig. 1 has incidence matrix

$$\begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}. \tag{10}$$

Whenever I is not injective we say that Γ has *multiple edges*. For example, edges e_3 and e_4 in Fig. 1 are multiple. A graph is called *simplicial* if it has no self-loops nor multiple edges. Note that this is the same as saying that the entries of the incidence matrix are 0 or 1 and there are no identical columns.

Two important families of graphs are the n-paths P_n and the n-cycles C_n ($n \in \mathbf{N}$). Formally, P_n can be defined by setting $V=1,\ldots,n$, $E=1,\ldots,n-1$, and $I(x)=\{x,x+1\}$. For C_n, set $V=E=\mathbf{Z}_n$ with the same description for I. In plain words, n paths are the combinatorial analog of a closed line segment, while n cycles are the counterpart of a circle. Pictorically, examples are shown in Fig. 2.

Let γ and Γ be graphs. γ is called a *subgraph* of Γ, denoted $\gamma \subseteq \Gamma$, if V_γ, E_γ, and I_γ are subsets, respectively, of V_Γ, E_Γ, and I_Γ. We say that two graphs Γ and Γ' are *isomorphic*, denoted $\Gamma \simeq \Gamma'$ if there exist two functions $\mu: V_\Gamma \to V_{\Gamma'}$ and $\nu: E_\Gamma \to E_{\Gamma'}$ which are one to one and onto and such that

$$I_{\Gamma'}(\nu(e)) = \{\mu(v) | v \in I_\Gamma(e)\}. \tag{11}$$

Figure 3 shows some examples of subgraphs.

A graph isomorphic to some P_n is a path, and a graph isomorphic to some C_n is a cycle. The *valence* of a vertex is the sum of the entries in its row in the incidence matrix. A path P has one or two distinguished vertices with valence distinct of 2. We shall call them the *end points* of P. Two vertices u and v of a graph Γ are said to be *connected* if there exists a path $P \subseteq \Gamma$ such that the end points of P are u and v. This defines an equivalence relation in V. The equivalence classes are called the *components* of Γ. A graph with a single component is said to be a connected graph.

A *tree* is a connected graph with no (sub)cycles. That is, a tree is a graph such that for any two vertices there exists exactly one path connecting them. Every tree which is not a point contains at

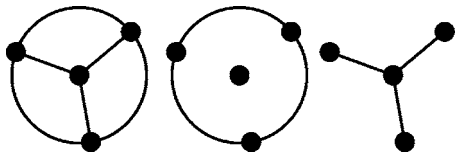


FIG. 3. The complete graph K_4 and 2 subgraphs, the second one a maximal subtree.

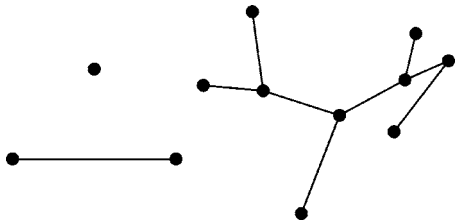


FIG. 4. Three trees with one, two, and nine vertices.

least two vertices of valence 1. Some examples of trees are shown in Fig. 4. A *maximal subtree* of a connected graph Γ is any tree $T \subseteq \Gamma$ such that $V_T = V_\Gamma$. Equivalently, a maximal subtree of Γ is any tree T such that $T \subset \Gamma' \subseteq \Gamma$ implies that Γ' is not a tree. Thus, there exists a maximal subtree for every connected graph. Moreover, given a tree $T \subseteq \Gamma$, there exists a maximal tree T' such that $T \subseteq T' \subseteq \Gamma$.

The *Euler characteristic* of a graph Γ, denoted $\chi(\Gamma)$, is defined by the formula

$$\chi(\Gamma) := |V_\Gamma| - |E_\Gamma|. \tag{12}$$

For any tree T, $\chi(T)=1$ (this can be proved by induction on $|V_T|$). Thus, if T is any maximal subtree of Γ, then $(|E_\Gamma - E_T|) = 1 - \chi(\Gamma)$. For each $e \in E_\Gamma - E_T$ we define $C_\Gamma(T,e)$ as the unique cycle of the graph $T+e$ (with the natural definition) $T+e := (V_T, E_T \cup \{e\}, I_T \cup \{(e, I_\Gamma(e))\})$. The interest of these cycles is that they form a maximal set of independent cycles, in a sense that will be made clear below. Meanwhile, Fig. 5 shows an example.

We now introduce the concept of the first homology group of a graph Γ. To this end, we start by defining 0-chains and 1-chains. Given a graph $\Gamma = (V,E,I)$, a 0-chain is a formal sum of vertices with coefficients in $\mathbf{Z}_2$,

$$\sum_{v \in V} \lambda_v v, \quad \lambda_v \in \mathbf{Z}_2. \tag{13}$$

The sum of two chains is defined in a term by term fashion

$$\sum_{v \in V} \lambda_v v + \sum_{v \in V} \lambda'_v v = \sum_{v \in V} (\lambda_v + \lambda'_v) v. \tag{14}$$

We adopt the convention that terms with zero coefficient are not written. The special element with all the coefficients equal to zero is denoted 0. Let $C_0(\Gamma)$ be de set of 0-chains of Γ; then $(C_0(\Gamma), +, 0)$ is an Abelian group isomorphic to $\mathbf{Z}_2^{|V|}$. Note that there is a natural inclusion of V in C_0 giving a basis. The definition of the space of 1-chains $C_1(\Gamma)$ runs along similar lines: just substitute V with E.

Next, we introduce a homomorphism, the boundary operator $\partial: C_1(\Gamma) \to C_0(\Gamma)$. It is enough to define its value over a set of generators,

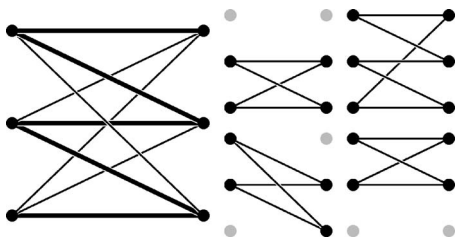


FIG. 5. The complete bipartite graph $K_{3,3}$ with a maximal subtree (thick line), and the corresponding generating set of cycles.

$$\partial(e) = \begin{cases} v_1 + v_2 & \text{if } I(e) = \{v_1, v_2\} \\ 0 & \text{if } I(e) = \{v_1\}. \end{cases} \tag{15}$$

It is possible to map naturally subgraphs onto chains; let $c_\gamma := \Sigma_{e \in E_\gamma} e$, where $\gamma \subseteq \Gamma$. Under this identification, the boundary of a path with more than one vertex are its end points, and the boundary of any cycle is 0.

The first homology group of a graph Γ is

$$H_1(\Gamma) := \ker \partial. \tag{16}$$

Its elements are always called cycles, but they do not necessarily correspond to cycles in the previous sense. To avoid confusion, we call the graphs isomorphic to some C_n simple cycles. We need a description of H_1.

Proposition 1: *Let Γ be a connected graph. Then $H_1(\Gamma) \simeq \mathbf{Z}_2^{1-\chi(\Gamma)}$. If T is a maximal subtree of Γ then the set $\{c_{C_\Gamma(T,e)} | e \in E_\Gamma - E_T\}$ forms a basis for $H_1(\Gamma)$. Moreover, if $c_1 \in H_1(\Gamma)$ has coefficients λ_e on this set of edges, then*

$$c_1 = \sum_{e \in E_\Gamma - E_T} \lambda_e c_{C_\Gamma(T,e)}. \tag{17}$$

If Γ is composed of several components Γ_i we have

$$H_1(\Gamma) \simeq \oplus_i H_1(\Gamma_i). \tag{18}$$

Let $C^0(\Gamma)$ denote the dual space of $C_0(\Gamma)$, that is, the space of homomorphisms taking $C_0(\Gamma)$ into $\mathbf{Z}_2$,

$$C^0(\Gamma) := \hom(C_0(\Gamma), \mathbf{Z}_2). \tag{19}$$

The elements of this space are called 0-cochains. It can be regarded as the additive group of functions $f: V_\Gamma \to \mathbf{Z}_2$, because a homomorphism is completely defined by giving its values on a generating set. Given $v \in V$, we define $v^* \in C^0(\Gamma)$ by

$$v^*(u) = \delta_{uv}, \tag{20}$$

where $u \in V$ and δ is the Kronecker symbol. The set $\{v^* | v \in V_\Gamma\}$ forms a basis of $C^0(\Gamma)$. For $c^0 \in C^0(\Gamma)$, $c_0 \in C_0(\Gamma)$, we define $(c^0, c_0) := c^0(c_0)$. Similarly, $C^1(\Gamma)$ denotes the dual space of $C_1(\Gamma)$ and its elements are called 1-cochains. The same comments as for C^0 are valid substituting V with E, and we use the notation e^* and (c^1, c_1) in the same way.

We define $\delta: C^0(\Gamma) \to C^1(\Gamma)$ to be the dual homomorphism of ∂, that is, for every $c^0 \in C^0(\Gamma)$ and $c_1 \in C_1(\Gamma)$ we have $(\delta c^0, c_1) := (c^0, \partial c_1)$. If we think of c^0 as a function over V, then δc^0 can be thought of as a derivative or gradient. What will be important for us is the fact that

$$\forall v \in V (\delta v^*, c_1) = 0 \Leftrightarrow c_1 \in H_1(\Gamma). \tag{21}$$

If we denote by $\text{star}(v)$ the set of edges incident *once* in v, we have

$$\delta v^* = \sum_{e \in \text{star}(v)} e^*. \tag{22}$$

Although we have maintained our discussion in the realm of combinatorics, it is interesting to comment briefly how the topological representation of a graph $\Gamma = (V, E, I)$ is constructed. One starts by giving to V the discrete topology. The points of V are called 0-cells. We also need a set $\{D_e | e \in E\}$ of closed segments or 1-cells. The boundary of each of these segments, denoted ∂D_e, consists of two points. The information contained in I is codified in functions $\phi_e: \partial D_e \to I(e) \subset V$ with the unique requirement that they must be onto. The topological space of the graph is then

constructed as the quotient space of the disjoint union $V \cup_e D_e$ under the identifications $x \sim \phi_e(x)$ for $x \in \partial D_e$. Properties such as connectedness or the first homology group are completely topological.

C. Classical homological codes

With all the machinery laid down, we are ready to introduce classical homological error correcting codes. We say that a simple cycle isomorphic to C_n has length n. Let $\mathrm{Cy}(\Gamma)$ be the set of simple subcycles of Γ. We introduce the distance of a graph Γ, denoted $\mathrm{d}(\Gamma)$, as the minimal length among the elements of $\mathrm{Cy}(\Gamma)$.

Given a graph Γ, let $E=\{e_i\}_{i=1}^{|E|}$. Consider the isomorphisms $\mathbf{h}_1: C_1(\Gamma) \to \mathbf{Z}_D^{|E|}$ and $\mathbf{h}_2: C^1(\Gamma) \to \mathbf{Z}_D^{|E|}$ defined by

$$\mathbf{h}_1\left(\sum_{i=1}^{|E|} \lambda_i e_i\right) := (\lambda_0, \lambda_1, \ldots, \lambda_{|E|}), \tag{23}$$

$$\mathbf{h}_2\left(\sum_{i=1}^{|E|} \lambda_i e_i^*\right) := (\lambda_0, \lambda_1, \ldots, \lambda_{|E|}). \tag{24}$$

Then

$$\mathbf{h}_2(c^1) \cdot \mathbf{h}_1(c_1) = (c^1, c_1). \tag{25}$$

Theorem 2: *Let Γ be a connected simplicial graph, not a tree. Construct a parity check matrix H by selecting a set of linearly independent rows of the incidence matrix of Γ. This gives an $[n,k,d]$ linear code C with $n=|E|$, $k=1-\chi$ and $d=\mathrm{d}(\Gamma)$.*

Proof: We claim that $\mathbf{h}_1[H_1(\Gamma)]$ is the code under consideration. Let F be the subspace generated by the elements of $B := \{\delta v^* | v \in V\}$. From Eq. (21) and (25) it follows that $\mathbf{h}_1[H_1(\Gamma)] = \mathbf{h}_2[F]^\perp$. On the other hand, since Γ is simplicial, Eq. (22) now reads

$$\delta v^* = \sum_{\{e \in E | v \in I(e)\}} e^*. \tag{26}$$

Thereby the set of vectors $\mathbf{h}_2[B]$ generates the same space as the rows of the parity check matrix H, which proofs the claim.

Since the length is clearly $|E|$ and $k = \dim \mathbf{h}_1[H_1(\Gamma)] = 1-\chi$, we only have to check the distance of the code. The weight function over $\mathbf{Z}_2$ can be pulled back to $C_1(\Gamma)$. For general 1-chains it gives the number of nonzero coefficients in the formal sum. Its restriction to $\mathrm{Cy}(\Gamma)$ gives the length function. Now, let $c_1 \in H_1(\Gamma)$, $c_1 \neq 0$. There exists a subgraph $\gamma \subset \Gamma$ such that $c_\gamma = c_1$. γ must contain a simple subcycle, for if not, then it is a collection of trees, and so it contains a vertex v of valence 1. But then Eq. (22) implies $(\delta v^*, \gamma) = 1$, a contradiction in view of Eq. (21). So let c be such a simple subcycle. Clearly, $\mathrm{wt}(\mathbf{h}_1(c_1)) \geqslant \mathrm{wt}(\mathbf{h}_1(c)) \geqslant \mathrm{d}(\Gamma)$, and the equality is obtained by taking γ a simple subcycle of minimal length. □

We do not let Γ be a tree just to prevent a code encoding 0 bits of information. Connectedness avoids having a code which can be decomposed into two more simple ones, but of course there is no problem at all in considering unconnected graphs. However, it is completely unnecessary to consider a set of disconnected graphs Γ_i since the wedge product of them, $\vee_i \Gamma_i$, will do the work equally well. The wedge product can be obtained by choosing one vertex from each graph and identifying them all; it does not change the first homology group. Finally, if the graph were not simplicial then the distance would be 1 or 2, something useless since $d = 2t+1$, $t \geqslant 1$.

Let us define $\nu(k,d)$ as the minimum value of n among all the possible $[n,k,d]$ homological codes. Clearly $\nu(k,d) < \nu(k+1,d)$. In addition, we note that $\nu(k+k',d) \leqslant \nu(k,d) + \nu(k',d)$, because the wedge product of two graphs leading, respectively, to $[n,k,d]$ and $[n',k,d']$ codes gives a graph associated with a $[n+n',k+k',d]$ code. The simplest example of a graph with a code

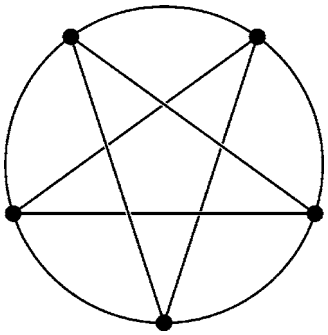


FIG. 6. The complete graph K_5.

associated is C_3. The corresponding code is the repetition code $\{(000), (111)\}$. This example can be extended to a family of codes in two ways. The easy one is the family C_d of $[d,1,d]$ repetition codes. They are clearly optimal, and thus, $\nu(1,d)=d$. More interesting is to regard C_3 as K_3. In general, the complete graph K_s is defined as a simplicial graph with s vertices and all the possible edges. As an example, K_5 is displayed in Fig. 6. The graph K_s yields an $\left[\binom{s}{2},\binom{s}{2}-s+1,3\right]$ code. These codes are clearly optimal among homological ones with $d=3$. Then we can use the family K_s to calculate the asymptotical value of $\nu(k,3)$. Clearly $\nu(k,3)>k$. Let $K(s)=\binom{s}{2}-s+1$. For $k<K(s)$, $\nu(k,3)<\binom{s}{2}=K(s)+O(\sqrt{K(s)})$. Thus

$$\lim_{k\to\infty}\frac{k}{n}=\lim_{k\to\infty}\frac{k}{\nu(k,3)}=1 \tag{27}$$

and asymptotically the point $k/n\sim 1$, $t/n\sim 0$ in the Hamming bound is reached. See Fig. 7 for a graphical representation of the rates.

A question that naturally arises is whether every linear code is homological. As we shall see, the answer is not. Note that the elements of any row of an incidence matrix always sum up to two, in $\mathbf{Z}$. So it might be the case that a subspace does not have a set of generators $\mathbf{u}_i=(u_{i1},\ldots,u_{in})$, $1\leqslant i\leqslant m$ fulfilling the condition $\Sigma_{i=1}^{m}u_{ij}=2$ (where the sum must be performed in $\mathbf{Z}$, not in $\mathbf{Z}_2$). The space generated by the rows of the H matrix in Eq. (8) is an example of this possibility. To verify this, simply check that summing one row to another one is equivalent to perform certain column permutation.

The function $\nu(k,d)$ behaves well for fixed $k=1$ and for fixed $d=3$. Is this true for other values of the parameters? We do not have a conclusive answer, but a partial one may be given. Consider the case $k=2$, the (topologically) most simple one apart from $k=1$. There are only two interesting topologies for a graph giving this value of k, see Fig. 8. For case A the inequalities $a+b\geqslant d$, $a+c\geqslant d$, and $b+c\geqslant d$ must hold. Summing up we get $2n\geqslant 3d$. The same procedure applied to case B easily yields $n\geqslant 2d$. We want n as small as possible, and so in principle the first case is the best one. This is confirmed by the (optimal) assignment $a=b=t+1$, $c=t$, where $d=2t+1$. For high

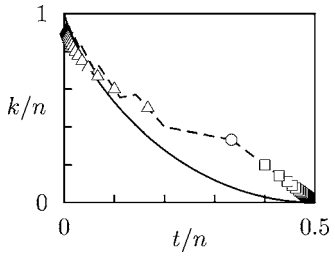


FIG. 7. The rate k/n vs t/n for the codes generated by the families C_d (□) and K_s (△), with the corresponding Hamming bound (dashed line). ○ is $C_3=K_3$. The asymptotic Hamming bound is displayed as a reference (continuous line).

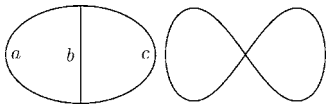


FIG. 8. The two (connected) topologies for the case $k=2$. Each curve represents a path, and the labels indicate the number of edges composing it. Other topologies are also possible, but they could be transformed in one of these by eliminating one by one any vertex of valence 1 (an operation which does not alter the homology nor the distance).

values of t, $t/n \simeq 1/3$, and there is no way to get a better result. Note how topologies with the same first homology group can somehow be classified according to their optimality for code composition. If a similar calculation is performed for $k=3$, K_4 is among the optimal ones (perhaps as expected) and gives $t/n \simeq 1/4$ for high values of t. Moreover, due to the high symmetry of K_s it is possible to construct a bound for its topology for any s. One has to consider all the C_3 cycles in K_s and proceed as above to get

$$(s-2)n \geqslant \binom{s}{3} d. \tag{28}$$

This is quite a disappointing result, since for high values of s one gets $t/n \sim 0$, even for low values of n. However, it is not conclusive as long as we do not know whether the topology of K_s is the optimal one for $k=K(s)$.

If one does not care about homology and only wants a way to visualize codes, then of course it is possible to allow "links" connecting an arbitrary number of "nodes." One can still consider chains of links, and the nodes impose the conditions of the H matrix as vertices did in the homological point of view. In such a scheme, the code (8) would look as Fig. 9. It is not clear, however, whether this could be of any use.

III. HOMOLOGICAL CODES FOR QUANTUM ERROR CORRECTION

A. Quantum error correcting codes

QEC is the quantum analog of its classical counterpart. As it usually happens, the quantum domain gives rise to difficulties not present in the classical case; the extension of techniques such as linear coding is far from being straightforward. In fact, in the early times of quantum information it was believed that QEC was impossible. As it happens quite often, the dangerous word "impossible" was soon substituted by the more encouraging "difficult."

Here we shall only consider error correction under the transmission through quantum noisy channels, which includes information storage. This means that we will suppose that the error correction stage can be performed without errors. In general this is not a realistic scenario, and the more general framework of fault-tolerant quantum computation is necessary.

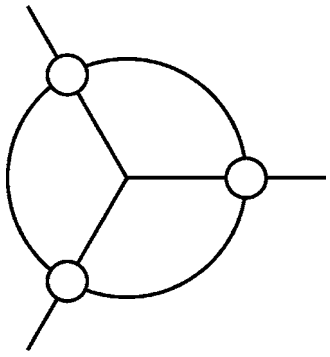


FIG. 9. A nonhomological visualization for the Hamming code [7, 4, 3]. There is one link connecting three nodes, something impossible with edges.

In the classical case we have been interested exclusively in bits. In the quantum case it would seem natural to consider only *qubits*, their quantum analog. Any quantum system with only two states can be regarded as a qubit. Its representation is a complex Hilbert space of dimension 2. We shall, however, consider higher-dimensional quantum systems, or *qudits*. Although classical computation is now far more interested in bits than in dits, it was not the case in its early times. In the quantum case it seems to be rather interesting to consider qudits,[62] and thus we will discuss them on equal footing throughout this section.

First a bit of notation. A qudit is described by a Hilbert space of dimension $D \geqslant 2$, and finite. This space will be denoted $\mathcal{D}$. The elements of a given orthogonal basis can be denoted $|x\rangle$ with $x=0,\ldots,D-1$. This set of numbers is naturally identified with the elements of the set modulus

$$\mathbf{Z}_D := \mathbf{Z}/D\mathbf{Z}. \tag{29}$$

In general, whenever an element of $\mathbf{Z}_D$ appears in an expression, any integer in that expression must be understood to be mapped to $\mathbf{Z}_D$. Messages are strings of qudits. Such a string of length n corresponds to the space $\mathcal{D}^{\otimes n}$. When expressing elements of this space, vector notation is useful. As usual, $\mathbf{v} \in \mathbf{Z}_D^n$ stands for $\mathbf{v}=(v_1,\ldots,v_n), v_i \in \mathbf{Z}_D$. With this notation, we define

$$|\mathbf{v}\rangle := \bigotimes_{i=1}^{n} |v_i\rangle. \tag{30}$$

The usual scalar product $\mathbf{u}\cdot\mathbf{v}$ will be employed. It is worth noting that, whenever D is not prime, $\mathbf{Z}_D$ is not a field and $\mathbf{Z}_D^n$ is not a vector space. This is not seriously dangerous and we will use the word vector in this wider sense.[62] For fixed dimension D, we also introduce the symbol

$$\varphi(k) := \mathrm{e}^{(2\pi \mathrm{i}/D)k}, \tag{31}$$

where $k \in \mathbf{Z}_D$.

The essence of QEC is what follows. We consider a system S and its environment E. The environment cannot be controlled, and it interacts with the system producing *noise*. The system is not initially entangled with the environment, but entanglement grows with the unavoidable interaction between E and S. Omitting the tensor product symbol, this interaction can be described as follows:[65]

$$|e\rangle|s\rangle \to \sum_k |e_k\rangle M_k |s\rangle, \tag{32}$$

where $|e\rangle$ and $|s\rangle$ are, respectively, the initial state of the environment and the system; the final states of the environment $|e_k\rangle$ are not necessarily orthogonal or normalized and the operators M_k acting on the system are unitary. In order to perform error correction we need to disentangle system and environment. This can be achieved by enlarging the system S with an ancilla system A and whenever it is possible to perform a unitary operation R over $S' = A \otimes S$ such that

$$R(|a\rangle M_k |s\rangle) = |a_k\rangle|s\rangle, \tag{33}$$

where $|a\rangle$ is the initial state of the ancilla. If this is the case, then we have

$$\sum_k |e_k\rangle R(|a\rangle M_k |s\rangle) = \left(\sum_k |e_k\rangle|a_k\rangle\right)|s\rangle, \tag{34}$$

and the errors are gone. Of course, the state $|s\rangle$ is unknown. This means that our strategy should work (with the same R) for certain subspace of S. Then we could use this subspace for information transmission or storage without errors. In general, however, we will not be able to correct every error and thus we will have to consider only errors M_k that happen with high probability, just as in the classical case.

Let us explain under which conditions there exists a recovery operation R as in Eq. (33). A *quantum error correcting code of length n* is a subspace $\mathcal{C}$ of $\mathcal{D}^{\otimes n}$ such that recovery is possible

after noise consisting of any combination of error operators from some set $\mathcal{E}$ of operators over $\mathcal{D}^{\otimes n}$. The set $\mathcal{E}$ is the set of *correctable errors*, and we say that $\mathcal{C}$ *corrects* $\mathcal{E}$. Note that any linear combination of correctable errors is also correctable. A requirement for correction to be possible that looks pretty intuitive is the following. For every $|\xi\rangle, |\eta\rangle \in \mathcal{C}$ such that $\langle\xi|\eta\rangle = 0$ and for every $M, N \in \mathcal{E}$

$$\langle\xi|N^\dagger M|\eta\rangle = 0. \tag{35}$$

This only says that errors do not mix up orthogonal states of the code. In what follows we show that, in fact, this condition is enough and sufficient for Eq. (33) to be possible.

Condition (35) can be rewritten in an equivalent form: For every $|\xi\rangle, |\eta\rangle \in \mathcal{C}$ and for every $N, M \in \mathcal{E}$

$$\langle\xi|N^\dagger M|\eta\rangle = c(N^\dagger M)\langle\xi|\eta\rangle, \tag{36}$$

where $c(N^\dagger M) \in \mathbf{C}$. Clearly this implies Eq. (35). For the converse, note that for every $|\xi\rangle, |\eta\rangle \in \mathcal{C}$ such that $\langle\xi|\eta\rangle = 0$ condition (35) implies

$$0 = \langle\xi - \eta|N^\dagger M|\xi + \eta\rangle = \langle\xi|N^\dagger M|\xi\rangle - \langle\eta|N^\dagger M|\eta\rangle, \tag{37}$$

from which Eq. (36) follows by considering any orthogonal basis of $\mathcal{C}$ and evaluating $N^\dagger M$ on it.

We now observe that the existence of an ancilla system A and a recovery operation R as in Eq. (33) implies Eq. (36). This is because

$$\langle\xi|M_i^\dagger M_j|\eta\rangle = \langle\xi|M_i^\dagger\langle a|R^\dagger R|a\rangle M_j|\eta\rangle = \langle\xi|\eta\rangle\langle a_i|a_j\rangle. \tag{38}$$

The converse is also true; it is enough to take $\mathcal{D}^{\otimes n}$ as the ancilla system and set

$$R(|a\rangle M|\xi\rangle) = M|a\rangle|\xi\rangle \tag{39}$$

for every $\xi \in \mathcal{C}$ and $M \in \mathcal{E}$ and for some $|a\rangle \in \mathcal{C}$ chosen as the initial state of the ancilla system. This does not define R completely, but it is enough to check that it can be extended to a unitary operator over $\mathcal{D}^{\otimes n} \otimes \mathcal{D}^{\otimes n}$. This in turn holds true if

$$\langle\eta|N^\dagger M|\xi\rangle\langle a|a\rangle = \langle a|N^\dagger M|a\rangle\langle\eta|\xi\rangle, \tag{40}$$

but this follows from Eq. (36).

Our next goal is to introduce a notion of code *distance*, just as in the classical case. A quantum code $\mathcal{C}$ is said to *detect* an error N if for every $|\xi\rangle, |\eta\rangle \in \mathcal{C}$

$$\langle\xi|N|\eta\rangle = c(N)\langle\xi|\eta\rangle \tag{41}$$

for some $c(N) \in \mathbf{C}$. From the above discussion follows that a code $\mathcal{C}$ corrects error from $\mathcal{E}$ iff it detects errors from the space

$$\mathcal{E}^\dagger\mathcal{E} := \left\{ \sum_l N_l^\dagger M_l | M_l, N_l \in \mathcal{E} \right\}. \tag{42}$$

For codes of length n, let $\mathcal{E}(n,k)$ be the set of operators acting on at most k qudits. We define the distance of the code $\mathcal{C}$, denoted $d(\mathcal{C})$, as the smallest number d for which the code does not detect $\mathcal{E}(n,d)$. Since $\mathcal{E}(n,t)^\dagger\mathcal{E}(n,t) = \mathcal{E}(n,2t)$, a code $\mathcal{C}$ corrects $\mathcal{E}(n,t)$ iff $d(\mathcal{C}) > 2k$. In this case we say that $\mathcal{C}$ corrects t errors. As in the classical case, we can talk about $[[n,k,d]]$ codes when referring to codes of length n, dimension D^k, and distance d. Such a code is said to encode k qudits. We use double brackets to distinguishing them from classical codes.

As an example, let us introduce the trivial code of length n encoding k qudits,

$$\mathcal{C}_T(n,k) := \{|\mathbf{0}\rangle \otimes |\xi\rangle | \xi \in \mathcal{D}^{\otimes k}\}, \tag{43}$$

where $|\mathbf{0}\rangle = |0\rangle^{\otimes n-k}$. Since it has distance 1, the trivial code is quite useless. However, its structure can give rise to a rich family of codes. To this end, let $U: \mathcal{D}^{\otimes n} \to \mathcal{D}^{\otimes n}$ be any unitary operator. Clearly

$$U\mathcal{C}_T(n,k) := \{U|c\rangle | c \in \mathcal{C}_T(n,k)\} \tag{44}$$

is also an error correcting code. In fact, it is clear that for any $[[n,k,d]]$ quantum error correcting code $\mathcal{C}$ for which k is an integer there exists a unitary operator U such that $U\mathcal{C}_T(n,k) = \mathcal{C}$. These kinds of codes are the most usual ones. Since

$$\langle \xi | N | \eta \rangle = \langle \xi | U^\dagger U N U^\dagger U | \eta \rangle, \tag{45}$$

the errors detected by $\mathcal{C}_T$ and $U\mathcal{C}_T$ are in a one to one correspondence through conjugation $U \cdot U^\dagger$. Exploiting this idea we could try to find a family of U operators for which the calculation of the distance of the code $U\mathcal{C}_T(n,k)$ is easy. This is the subject of the next section.

B. Symplectic codes

As a generalization of the usual X and Z Pauli matrices for qubits, we define for qudits of fixed dimension D the operators (31)

$$X := \sum_{k \in \mathbf{Z}_D} |k+1\rangle\langle k|, \tag{46}$$

$$Z := \sum_{k \in \mathbf{Z}_D} \varphi(k) |k\rangle\langle k|. \tag{47}$$

Note that $X^D = Z^D = 1$ and $XZ = \varphi(1) ZX$. With these operators a basis for the linear operators over $\mathcal{D}$ can be defined,

$$\sigma_{xz} := f(xz) X^x Z^z, \tag{48}$$

where $x, z \in \mathbf{Z}_D$ and $f: \mathbf{Z}_D \to \mathbf{C}$ is there to guarantee $\sigma_{xz}^D = 1$. Thus we have to define f by demanding $f(x)^D = \varphi(x)^{D(D-1)/2} = (-1)^{x(D+1)}$, and then we take

$$f(x) := \begin{cases} e^{\pi i/D} & \text{if } D \text{ is even and } x \text{ is odd} \\ 1 & \text{if } D \text{ is odd or } x \text{ is even.} \end{cases} \tag{49}$$

The set of σ operators is a basis because

$$|k\rangle\langle l| = \frac{1}{D} \sum_{m \in \mathbf{Z}_D} \varphi(-lm) X^{k-l} Z^m. \tag{50}$$

As an example, note that for qubits we recover the usual Pauli matrices: $\sigma_{00} = I$, $\sigma_{10} = X$, $\sigma_{01} = Z$, and $\sigma_{11} = Y$.

We consider strings of qudits. For $\mathbf{v} \in \mathbf{Z}_D^{2n}$ and $\mathbf{x}, \mathbf{z} \in \mathbf{Z}_D^n$ let us introduce the notation $\mathbf{v} = (\mathbf{xz})$ meaning

$$\mathbf{v} = (x_1, \ldots, x_n, z_1, \ldots, z_n). \tag{51}$$

We can extend our family of operators to act on $\mathcal{D}^{\otimes n}$,

$$\sigma_{\mathbf{v}} := \sigma_{\mathbf{xz}} := \bigotimes_{i=1}^{n} \sigma_{x_i z_i}, \tag{52}$$

where $\mathbf{v} = (\mathbf{xz})$. We have

$$\sigma_{\mathbf{x}0}|\mathbf{v}\rangle := |\mathbf{v}+\mathbf{x}\rangle, \tag{53}$$

$$\sigma_{0\mathbf{z}}|\mathbf{v}\rangle := \varphi(\mathbf{z}\cdot\mathbf{v})|\mathbf{v}\rangle. \tag{54}$$

An important commutation relation is[62]

$$\sigma_{\mathbf{u}}\sigma_{\mathbf{v}} = \varphi(\mathbf{u}^t\Omega\mathbf{v})\sigma_{\mathbf{v}}\sigma_{\mathbf{u}}, \tag{55}$$

where

$$\Omega := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{56}$$

is a $2n\times 2n$ matrix over $\mathbf{Z}_D$. The group of all the operators generated by the set of σ operators is the Pauli group $\mathbf{P}_D(n)$. Note that there is a natural homomorphism from this group onto $\mathbf{Z}_D^{2n}$ since $\sigma_{\mathbf{u}}\sigma_{\mathbf{v}} \propto \sigma_{\mathbf{u}+\mathbf{v}}$.

Let us now consider operators $U\cdot U^\dagger$ with U unitary such that they are closed over $\mathbf{P}_D(n)$, that is,

$$U\sigma_{\mathbf{v}}U^\dagger = \psi(\mathbf{v})\sigma_{\omega(\mathbf{v})}, \tag{57}$$

where $\psi:\mathbf{Z}_D^{2n}\to\mathbf{C}$ and $\omega:\mathbf{Z}_D^{2n}\to\mathbf{Z}_D^{2n}$ are functions depending on U. We call this group the extended symplectic group $ESp_D(n)$. It might look that this condition is not enough to guarantee that $U\cdot U^\dagger$ is closed over $\mathbf{P}_D(n)$, but since it implies $\psi(\mathbf{v})^D=1$, we have $\psi(\mathbf{v})=\varphi(g(\mathbf{v}))$ for some $g:\mathbf{Z}_D^{2n}\to\mathbf{Z}_D$. Thus, there is no problem at all. It is can be easily derived that

$$\sigma_{\omega(\mathbf{u}+\mathbf{v})} \propto \sigma_{\omega(\mathbf{u})}\sigma_{\omega(\mathbf{v})} \propto \sigma_{\omega(\mathbf{u})+\omega(\mathbf{v})}. \tag{58}$$

From it this follows that $\omega(\mathbf{u})=M\mathbf{u}$ where M is a $2n\times 2n$ matrix over $\mathbf{Z}_D$. From Eq. (55) we obtain the following condition on M:

$$M^t\Omega M = \Omega. \tag{59}$$

The matrix group described by this condition is the symplectic group $Sp_D(n)$. There is thus a natural group homomorphism

$$h:ESp_D(n)\to Sp_D(n). \tag{60}$$

But h is onto, see Appendix A, and so it induces the isomorphism

$$ESp_D(n)/\ker h \cong Sp_D(n). \tag{61}$$

It is interesting to study the kernel of h. For any of its elements we have

$$U\sigma_{\mathbf{v}}U^\dagger = \varphi(g(\mathbf{v}))\sigma_{\mathbf{v}}. \tag{62}$$

But this easily implies that $g(\mathbf{v})=\mathbf{w}\cdot\mathbf{v}$ for some $\mathbf{w}\in\mathbf{Z}_D^{2n}$. On the other hand,

$$\sigma_{\mathbf{u}}\sigma_{\mathbf{v}}\sigma_{\mathbf{u}}^\dagger = \varphi(\mathbf{u}^t\Omega\mathbf{v})\sigma_{\mathbf{v}}. \tag{63}$$

As a result, $\ker h\cong\mathbf{Z}_D^{2n}$.

Now that we have characterized $ESp_D(n)$, it is time to return to our initial purpose of constructing quantum error correcting codes. The idea is to apply the symplectic group $ESp_D(n)$ to $\mathcal{C}_T(n,k)$ and obtain the codes which are called symplectic. A first result is that $\ker h$ does not help a lot; it only generates codes of the form

$$\{|\mathbf{u}\rangle \otimes |\xi\rangle | \xi \in \mathcal{D}^{\otimes k}\}, \tag{64}$$

where $\mathbf{u} \in \mathbf{Z}_D^{n-k}$. This is an example of conjugated codes. More generally, for each symplectic $[[n,k,d]]$ code $\mathcal{C}$ there exists a family of D^{n-k} conjugated $[[n,k,d]]$ codes obtained from $\mathcal{C}$ by application of σ operators. This will become clear shortly. As a result, we only have to focus on $Sp_D(n)$ when looking for better codes.

For any subspace $V \subset \mathbf{Z}_D^{2n}$ we define the subspace

$$\hat{V} := \{\mathbf{u} \in \mathbf{Z}_D^{2n} | \forall\, \mathbf{v} \in V \mathbf{u}^t \Omega \mathbf{v} = 0\}. \tag{65}$$

If V has a basis which is a linearly independent set and $V \subset \hat{V}$ we say that V is *isotropic*. Now let $V_{\mathcal{C}_T} \subset \mathbf{Z}_D^{2n}$ be the isotropic subspace containing the elements of the form $(\mathbf{0z})$, where $\mathbf{z} \in \mathbf{Z}_D^n$ must have its last k elements equal to zero. It is not difficult to verify that $\mathcal{C}_T(n,k)$ detects $\sigma_\mathbf{v}$ iff

$$\mathbf{v} \notin \hat{V}_{\mathcal{C}_T} - V_{\mathcal{C}_T}. \tag{66}$$

Consider any symplectic code $\mathcal{C} = U\mathcal{C}_T(n,k)$ with $h(U) = M$. We can define $V_\mathcal{C} := MV_{\mathcal{C}_T}$, giving $\hat{V}_\mathcal{C} = \widehat{MV}_{\mathcal{C}_T} = M\hat{V}_{\mathcal{C}_T}$. Then $\mathcal{C}$ detects $\sigma_\mathbf{v}$ iff $\mathbf{v} \notin \hat{V}_\mathcal{C} - V_\mathcal{C}$. In analogy with the weight function for classical codes, for any $\mathbf{v} = (\mathbf{xz}) \in \mathbf{Z}_D^{2n}$, let

$$|\mathbf{v}| := |\{i = 1, \ldots, n | x_i \neq 0 \text{ or } z_i \neq 0\}|. \tag{67}$$

Recall that σ operators over one qudit form a basis. This, the fact that the space of operators detected by a code is a linear subspace, and the previous discussion imply altogether

$$d(\mathcal{C}) = \min_{\mathbf{v} \in \hat{V}_\mathcal{C} - V_\mathcal{C}} |\mathbf{v}|. \tag{68}$$

This equation shows that the distance of the code depends only upon $V_\mathcal{C}$. On the other hand, given two isotropic subspaces $V_1, V_2 \subset \mathbf{Z}_D^{2n}$ of the same dimension it is possible to find a matrix $M \in Sp_D(n)$ such that $MV_1 = V_2$.[62] Therefore, for any isotropic subspace of dimension $n-k$ such that $V \subset \hat{V}$ there exists an $[[n,k,d]]$ symplectic code $\mathcal{C}$ with $V_\mathcal{C} = V$. This way, the problem of finding good codes is reduced to the problem of finding good isotropic subspaces $V \subset \mathbf{Z}_D^{2n}$. This is analogous to the classical situation with linear codes.

It is worth revisiting the trivial code on a new light. Consider the following Abelian subgroup of $\mathbf{P}_D(n)$:

$$\mathcal{S}_T(n,k) := \{\sigma_\mathbf{v} | \mathbf{v} \in V_{\mathcal{C}_T}\}. \tag{69}$$

The trivial code can be defined just in terms of this group,

$$\mathcal{C}_T(n,k) = \{|\xi\rangle \in \mathcal{D}^{\otimes n} | \forall\, \sigma \in \mathcal{S}_T(n,k) \sigma |\xi\rangle = |\xi\rangle\}. \tag{70}$$

$\mathcal{S}_T(n,k)$ is called the *stabilizer* of $\mathcal{C}_T(n,k)$. The stabilizer of any code $\mathcal{C} = U\mathcal{C}_T(n,k)$ is the Abelian group $\mathcal{S}_\mathcal{C} := U\mathcal{S}_T(n,k)U^\dagger$, and $\mathcal{C}$ can be defined by its stabilizer just as we did for $\mathcal{C}_T(n,k)$. It is because of this point of view that symplectic codes are also called stabilizer codes. A question that naturally arises here is under which conditions an Abelian subgroup $\mathcal{S} \subset \mathbf{P}_D(n)$ is the stabilizer of a symplectic code. Clearly $\mathcal{S}$ must fulfill the condition

$$\forall\, \sigma_1, \sigma_2 \in \mathcal{S}, \quad \sigma_1 \propto \sigma_2 \Rightarrow \sigma_1 = \sigma_2. \tag{71}$$

For D prime this is the end of the story, but in other case a bit of care is necessary, as we shall show now. Because of condition (71), $\mathcal{S}$ is isomorphically mapped to a subgroup $V_\mathcal{S} \subset \mathbf{Z}_D^{2n}$. We claim that $\mathcal{S}$ is the stabilizer of a symplectic code iff $V_\mathcal{S}$ is a subspace of $\mathbf{Z}_D^{2n}$ with a basis that is a linearly independent set. We only have to check the if direction. First, the elements of $\mathcal{S}$ can be labeled with the elements of $V_\mathcal{S}$. We denote them $\sigma_\mathcal{S}(\mathbf{v})$, $\mathbf{v} \in V_\mathcal{S}$. $V_\mathcal{S}$ is isotropic, and so we can find

a symplectic code $\mathcal{C}$ such that $V_{\mathcal{C}}=V_{\mathcal{S}}$. Let us denote the elements of its stabilizer $\sigma_{\mathcal{C}}(\mathbf{v})$, but in such a way that

$$\sigma_{\mathcal{C}}(\mathbf{v}) = \varphi(g(\mathbf{v}))\sigma_{\mathcal{S}}(\mathbf{v}), \tag{72}$$

where $g:\mathbf{Z}_D^{2n}\to\mathbf{C}$ and $\mathbf{v}\in V_{\mathcal{C}}=V_{\mathcal{S}}$. This is always possible since $\sigma_{\mathcal{S}}(\mathbf{v})^D=\sigma_{\mathcal{C}}(\mathbf{v})^D=1$. It is easily verified that g is linear, but then $g(\mathbf{v})=\mathbf{w}\cdot\mathbf{v}$ for some $\mathbf{w}\in\mathbf{Z}_D^{2n}$. Due to Eq. (63), there is a conjugate code of $\mathcal{C}$ such that $\mathcal{S}$ is its stabilizer.

Although condition (35) guarantees that recovery is possible, it is worth giving a more concrete recipe for symplectic codes. So let $\mathcal{C}$ be a code of distance d, $\{\mathbf{v}_i\}$ a basis of $V_{\mathcal{C}}$, and $G:=\{\varphi(f_i)\sigma_{\mathbf{v}_i}\}$ a generating set for its stabilizer, where $f_i\in\mathbf{Z}_D$. Suppose that an encoded state $|\xi\rangle$ has been subject to correctable noise as in Eq. (32),

$$|e\rangle|\xi\rangle \to \sum_k |e_k\rangle\sigma_{\mathbf{u}_k}|\xi\rangle, \tag{73}$$

where $\mathbf{u}_k\in\mathbf{Z}_D^{2n}$ and $|\mathbf{u}_k|<d/2$. We first measure the *syndrome* of the error. This amounts to project the system to any of the eigenstates of each operator in G. For each of the eigenstates there is a corresponding eigenvalue $\varphi(g_i)$, $g_i\in\mathbf{Z}_D$. The final state then is proportional to

$$\sum_{k:\forall i v_i^t\Omega u_k=g_i} |e_k\rangle\sigma_{\mathbf{u}_k}|\xi\rangle. \tag{74}$$

Let $\sigma_{\mathbf{u}}$ and $\sigma_{\mathbf{u}'}$ be any of the error operators in this sum. Note that $\mathbf{u}-\mathbf{u}'\in\hat{V}_{\mathcal{C}}$. Also, $\sigma_{\mathbf{u}'}^\dagger\sigma_{\mathbf{u}}\propto\sigma_{\mathbf{u}-\mathbf{u}'}$ is detectable, and so, in fact, $\mathbf{u}-\mathbf{u}'\in V_{\mathcal{C}}$. With the information from the error syndrome, we can choose any $\mathbf{w}$ such that $\mathbf{u}_i'\Omega\mathbf{w}=g_i$ and $\sigma_{\mathbf{w}}$ is correctable. Then any of the error operators in the sum is of the form $\sigma_{\mathbf{u}_k}\propto\sigma_{\mathbf{w}}\sigma_{\mathbf{u}_k'}$ with $\mathbf{u}_k'\in V_{\mathcal{C}}$. In other words, Eq. (74) can be rewritten as

$$\left(\sum_{k:\forall i v_i^t\Omega u_k=g_i} |e_k'\rangle\right)\sigma_{\mathbf{w}}|\xi\rangle, \tag{75}$$

where $|e_k'\rangle\propto|e_k\rangle$. This means that the measurement by itself is enough to disentangle system and environment, and we only have to perform $\sigma_{\mathbf{w}}^\dagger$ to recover the original encoded state.

Due to the essential role of $V_{\mathcal{C}}$, symplectic codes are usually given in the form of a $2n\times(n-k)$ matrix whose rows form a basis for it. As an example, there is a [[5,1,3]] symplectic code[12,13] of the form

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{76}$$

An important class of codes is that of the so-called CSS codes. Initially, CSS codes were introduced as a tool to obtain quantum codes from classical ones.[7,8] Given a classical $[n,k,d]$ code $\mathcal{C}$ with $\mathcal{C}\subset\mathcal{C}^\perp$ and check matrix H, the quantum code with check matrix

$$\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}$$

is a $[[n,2k-n,d]]$ code. More generally, any code for which the matrix can be put in the form

$$\begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix},$$

in such a way that X and Z operators are not mixed up, is called CSS. Following Steane[63] and Preskill,[64] we adopt here this terminology to designate CSS codes in general, A good example of

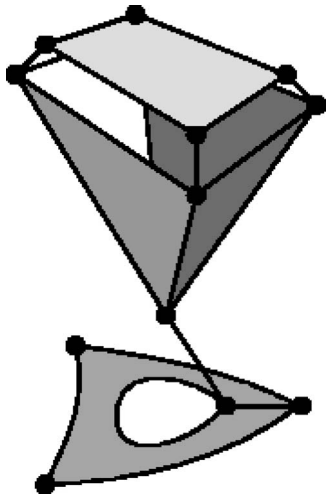


FIG. 10. A 2-complex composed of 9 vertices, 21 edges, and 4 faces.

these generalized CSS codes are the homological quantum codes, as we will see.

Returning to general codes, it is possible to derive a quantum analog of the Hamming bound for certain quantum codes. Let

$$\mathcal{E}_\sigma(n,t) := \{\sigma_{\mathbf{v}} || \mathbf{v}| \leqslant t\}. \tag{77}$$

It is clear that a code that corrects $\mathcal{E}_\sigma(n,t)$ corrects t errors. Let $\mathcal{C}$ be a code of length n and dimension m that corrects t errors and satisfies the condition that for every normalized $|\xi\rangle \in \mathcal{C}$ and for every $\mathbf{u},\mathbf{v} \in \mathbf{Z}_D^{2n}$ such that $|\mathbf{u}|, |\mathbf{v}| \leqslant t$

$$\langle \xi | \sigma_{\mathbf{u}}^\dagger \sigma_{\mathbf{v}} | \xi \rangle = \delta_{\mathbf{uv}}. \tag{78}$$

Such codes are called orthogonal or nondegenerate. Notice that for $\mathcal{D}^{\otimes n}$ there are $(D^2-1)^t\binom{n}{t}\sigma$ operators of weight t. This and condition (78) give the quantum Hamming bound[66]

$$m\sum_{i=0}^{t}(D^2-1)^i\binom{n}{i} \leqslant D^n. \tag{79}$$

C. Homology of 2-complexes

A 2-complex is the two-dimensional generalization of a graph or 1-complex. In general one can speak of cell complexes of arbitrary dimension, but we will keep things simple and restrict our attention to these low-dimensional cases. Recall that graphs were obtained by attaching 1-cells (arcs) to a set of 0-cells (points). We can continue the process by attaching 2-cells (disks) to the graph. Here attaching means "identify points in the boundary through continuous maps;" recall the end of Sec. II B. Indeed, we will not consider such general 2-complexes. We are interested in the combinatorial point of view, and our definition will reflect this fact. Figure 10 shows an example of the kind of objects we shall consider. The goal is to study the first homology group H_1 of these objects. Although our study of graphs only included $\mathbf{Z}_2$ homology, now we will discuss $\mathbf{Z}$ homology. In fact, when we talk about qudits we will be interested in $\mathbf{Z}_D$ homology, but this is constructed substituting $\mathbf{Z}$ for $\mathbf{Z}_D$ in the definitions.

Moving from $\mathbf{Z}_2$ homology to $\mathbf{Z}$ homology requires the introduction of orientation. An *oriented finite graph* $\Gamma=(V,E,I_s,I_t)$ consists of a finite set V of vertices, a finite set E of edges, and two incidence functions $I_s,I_t: E \to V$. The subindices stand for "source" and "target." We say that an edge $e \in E$ goes or points from $I_s(e)$ to $I_t(e)$. Let us introduce the set of inverse edges E^{-1}

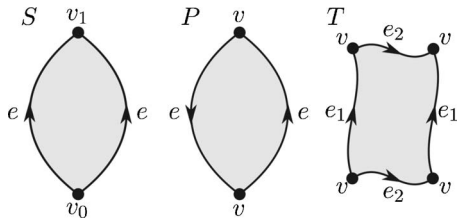


FIG. 11. Planar representations of several 2-complexes. They have the topology of the sphere S, the projective plane P, and the torus T. The identifiers for vertices and edges are the same as in the text.

$:=\{e^{-1}\,|\,e\in E\}$, where e^{-1} is just a symbol and we set $(e^{-1})^{-1}:=e$. We will use the notation $\bar{E}:=E\cup E^{-1}$. The incidence functions can be extended to $\bar{E}$ setting $I_s(e)=I_t(e^{-1})$ for any $e\in\bar{E}$.

In order to give a combinatorial meaning to the attachment of disks to graphs described above, we introduce the idea of walks on graphs. Given an n-tuple $(a,b,c,\ldots)$, let $[a,b,c,\ldots]$ denote the class of n-tuples equal to it up to cyclic permutations. We call such objects cyclic n-tuples, and its elements are naturally indexed by $\mathbf{Z}_n$. A *closed walk of length n* on a graph Γ is a cyclic n-tuple of oriented edges

$$w=[e_0,\ldots,e_{n-1}],\quad e_i\in\bar{E}, \tag{80}$$

such that $I_t(e_i)=I_s(e_{i+1})$ for every $i\in\mathbf{Z}_n$. The idea is that, given a graph, we can attach to it n-gons along closed walks. Note that the attachment can have two orientations, since given a closed walk w one could take the inverse walk $w^{-1}:=[e_{n-1}^{-1},\ldots,e_1^{-1}]$ to describe the same attachment. Our definition of walks excludes the possibility of attaching the boundary of a disk along a walk consisting of a single vertex, something very useful in other contexts but not for our purposes.

Let W_Γ denote the set of closed walks on the oriented graph Γ. An *oriented 2-complex* $\Sigma=(V,E,F,I_s,I_t,B)$ has the structure of a graph $\Gamma=(V,E,I_s,I_t)$ plus a finite set F of faces and a boundary function $B:F\to W_\Gamma$. Just as we did for edges, we can consider the set F^{-1} of inverse faces setting $B(f^{-1})=B(f)^{-1}$. We also set $\bar{F}:=F\cup F^{-1}$. The discussion above explains how a topological space M is related to this combinatorial structure Σ, and we will say that Σ represents M and use them almost indistinguishably. In any case, our application to quantum error correcting codes only depends on the combinatorial point of view. Some examples will illustrate the concept of 2-complex (see Figs. 11 and 12).

- The sphere S. Take two vertices v_0 and v_1, an edge e pointing from v_0 to v_1, and a face f with the boundary $[e,e^{-1}]$.
- The projective plane P. Only a single vertex v, a single edge e, and a single face f with boundary $[e,e]$ are needed.
- The torus T. This can be constructed with a vertex v, two edges e_1 and e_2, and a face f with boundary $[e_1,e_2,e_1^{-1},e_2^{-1}]$.

For any 2-complex Σ the Euler characteristic is

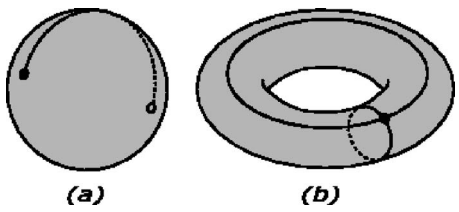


FIG. 12. A pair of 2-complexes embedded in $\mathbf{R}^3$. They represent (a) the sphere S and (b) the torus T.

$$\chi(\Sigma) := |V| - |E| + |F|. \tag{81}$$

Σ is said to be connected if its graph Γ is connected. $\Sigma' = (V', E', F', I'_s, I'_t, B')$ is said to be a subcomplex of Σ if $V' \subset V$, $E' \subset E$, $F' \subset F$, $I'_s \subset I_s$, $I'_t \subset I_t$ and $B' \subset B$. As usual, we call components the maximal connected subcomplexes of Σ. Although we have defined χ and connectedness in terms of Σ, they only depend upon the underlying topology. The same is true for H_1; its definition is our next goal.

Consider a 2-complex Σ. For the sake of simplicity, let us introduce the notation $\Delta_0 := V$, $\Delta_1 := E$, $\Delta_2 := F$. Let also the sets of 0-, 1-, and 2-chains be denoted $C_i(\Sigma)$ with $i = 0, 1, 2$. They contain formal sums of elements of Δ_i with integer coefficients. We adopt the same conventions as for 0- and 1-chains for graphs. As in that case, $C_i(\Sigma) \simeq \mathbf{Z}^{|\Delta_i|}$ and Δ_i is a natural basis of $C_i(\Sigma)$.

We introduce the boundary homomorphisms $\partial_i : \Delta_i \to \Delta_{i-1}$ for $i = 1, 2$. It is enough to give their value on a set of generators. We have

$$\forall e \in E, \quad \partial_1(e) = I_t(e) - I_s(e); \tag{82}$$

$$\forall f \in F, \quad \partial_2(f) = c_{B(f)}; \tag{83}$$

where for any $w = [e_1^{\sigma_1}, \ldots, e_n^{\sigma_n}] \in W_\Gamma$, $e_i \in E$, $\sigma_i = \pm 1$, we define

$$c_w := \sum_{i=1}^{n} \sigma_i e_i. \tag{84}$$

Whenever the index i in ∂_i can be inferred from the context, we will omit it. A simple but fundamental property is

$$\partial^2 = 0. \tag{85}$$

Let $Z_1(\Sigma) := \ker \partial_1$, $B_1(\Sigma) := \operatorname{ran} \partial_2$. The elements of Z_1 are called cycles and the elements of B_1 boundaries. We already encountered cycles in our study of the homology of a graph. Note that $B_1 \subset Z_1$. Thus we can define

$$H_1(\Sigma) := Z_1(\Sigma)/B_1(\Sigma). \tag{86}$$

Two cycles which represent the same element of the homology group are said to be homologous. Boundaries are homologous to zero. If Σ consists of several components Σ_i, we have

$$H_1(\Sigma) \simeq \oplus_i H_1(\Sigma_i). \tag{87}$$

Our next goal is the definition of the first cohomology group $H^1(\Sigma)$. For $i = 0, 1, 2$, let $C^i(\Sigma)$ denote the dual space of $C_i(\Sigma)$, that is,

$$C^i(\Sigma) := \hom(C_i(\Sigma), \mathbf{Z}). \tag{88}$$

The elements of these spaces are called i-cochains. They can be regarded as the additive group of functions $f : \Delta_i \to \mathbf{Z}$. Given $\sigma \in \Delta_i$, we define $\sigma^* \in C^i(\Sigma)$ by

$$\sigma^*(\sigma') = \delta_{\sigma\sigma'}, \tag{89}$$

where $\sigma' \in \Delta_i$. The set $\{\sigma^* \,|\, \sigma \in \Delta_i\}$ is a basis of $C^i(\Sigma)$. For $c^i \in C^i(\Sigma)$, $c_i \in C_i(\Sigma)$, we let $(c^i, c_i) := c^i(c_i)$.

For $i = 1, 2$, we define the coboundary maps $\delta_i : C^{i-1}(\Sigma) \to C^i(\Sigma)$ to be the dual homomorphism of ∂_i, that is, for every $c^{i-1} \in C^{i-1}(\Sigma)$ and $c_i \in C_i(\Sigma)$ we have $(\delta c^{i-1}, c_i) := (c^{i-1}, \partial c_i)$. Clearly, again omitting indices,

$$\delta^2 = 0. \tag{90}$$

The set of cocycles and coboundaries are, respectively, $Z^1(\Sigma) := \ker \delta_2$ and $B^1(\Sigma) := \mathrm{ran}\, \delta_1$. The first cohomology group is

$$H^1(\Sigma) := Z^1(\Sigma)/B^1(\Sigma). \tag{91}$$

Since they will be of interest when studying homological quantum error correcting codes, we collect here the following dual pair of properties. For any $c_1 \in C_1$ and $c^1 \in C^1$,

$$\forall v \in V(\delta v^*, c_1) = 0 \Leftrightarrow c_1 \in Z_1, \tag{92}$$

$$\forall f \in F(c^1, \partial f) = 0 \Leftrightarrow c^1 \in Z^1. \tag{93}$$

Also

$$\forall v \in V, \forall f \in F \quad (\delta v^*, \partial f) = 0. \tag{94}$$

We say that $(\delta v^*, \cdot)$ is a *star operator* and that $(\cdot, \partial f)$ is a *boundary operator*, reflecting their geometrical nature. The name of the boundary operator is clear enough, but perhaps the star operator deserves some explanation. Let the star of a vertex v be the set

$$\mathrm{star}(v) := \{(e,\sigma) \in E \times \{1,-1\} | I_i(e^\sigma) = v\}. \tag{95}$$

Then we have

$$\delta v^* = \sum_{(e,\sigma) \in \mathrm{star}(v)} \sigma e^*. \tag{96}$$

D. Surfaces

For a *surface* we understand a compact connected two-dimensional manifold. We already encountered several examples of surfaces constructed with 2-complexes, namely, S, T, and P. It is a fundamental result of surface topology that every other surface can be obtained by combination of these three; let us explain what is meant here by combination.

Consider two surfaces, M_1 and M_2. Let D_i, $i=1,2$, be a subset of M_i homeomorphic to a closed disk and let its boundary be ∂D_i. Let $h: \partial D_1 \to \partial D_2$ be a homeomorphism. The *connected sum* of M_1 and M_2, denoted $M_1 \sharp M_2$, is defined as the quotient space of the disjoint union $(M_1 - \mathring{D}_1) \cup (M_2 - \mathring{D}_2)$ under the identifications $x \sim h(x)$ for $x \in \partial D_1$. Here $\mathring{D}_i$ denotes the interior of D_i. $M_1 \sharp M_2$ is a surface, and its homeomorphism class depends only upon the homeomorphism classes of M_1 and M_2. To gain intuition, Fig. 13 shows a connected sum of two tori to give a 2-torus.

Let the Moëbius band B be the topological space obtained as the quotient space of $[0,1] \times [0,1]$ under the identifications $[0,x] \sim [1,1-x]$. For a picture, see Fig. 14. A surface is said to be *orientable* if it does not contain a subset homeomorphic to B. A surface is embeddable without self-intersections in $\mathbf{R}^3$ iff it is orientable. S and T are orientable, but P is not. Define recursively $gP := (g-1)P \sharp P$ for $g > 1$ and $1P := P$. Let also $gT := (g-1)T \sharp T$ for $g > 0$ and $0T := S$. No two of them are homeomorphic. gP is the sphere with n crosscaps and gT is the sphere with g handles or g-torus. gT and gP are said to have *genus* g.

Proposition 3. *Any orientable surface is homeomorphic to* gT *for some integer* $n \geqslant 0$. *Any nonorientable surface is homeomorphic to* gP *for some integer* $n \geqslant 1$.

See, for example, Ref. 67 for a proof. We already presented above the standard 2-complexes representing P and T. gP can be represented by the 2-complex consisting of a vertex v, n edges $\{a_1, \ldots, a_n\}$, and a face f with $B(f) = [a_1, a_1, \ldots, a_n, a_n]$. gT can be constructed with a vertex v, $2n$ edges $\{a_1, b_1, \ldots, a_n, b_n\}$, and a face f with $B(f) = [a_1, b_1, a_1^{-1}, b_1^{-1}, \ldots, a_n, b_n, a_n^{-1}, b_n^{-1}]$. Note that $\chi(gT) = 2(1-g)$ and $\chi(gP) = 2-g$. The corresponding homology and cohomology groups are

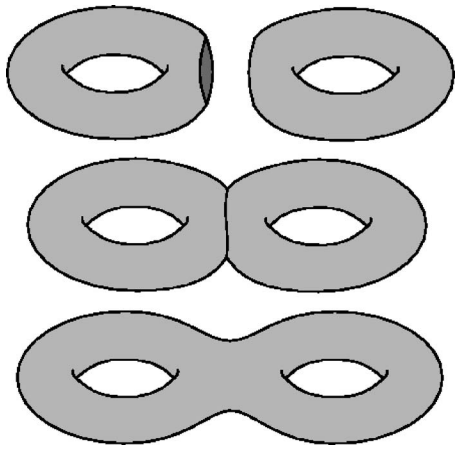


FIG. 13. The connected sum of two tori to give a 2-torus in three steps: cutting, gluing, and smoothing out.

$H_1(gT) \simeq H^1(gT) \simeq \mathbf{Z}^{2g}$ and $H_1(gP) \simeq H^1(gP) \simeq \mathbf{Z}^{g-1} \oplus \mathbf{Z}_2$. The subgroup $\mathbf{Z}_2$ appearing in the first homology group of nonorientable surfaces is called the torsion subgroup. It will play an important role when homological quantum error correcting codes for qudits of dimension greater than 2 are considered.

Consider a topological graph Γ embedded in a surface M, that is, a homeomorphism between Γ and a subset of M. When $M-\Gamma$ is a union of disks, we say that the embedding is a cell embedding. Clearly, such an embedding leads to a 2-complex whose faces are the mentioned disks. This raises the question of how to characterize combinatorially whether a 2-complex Σ represents a surface or not. It is enough to give a condition such that for each vertex the corresponding point for the represented topological space has a neighborhood isomorphic to a disk. Let us first define the index of face $f \in F$ on the "corner" described by the ordered pair (e,e'), where $e,e' \in \bar{E}$ and $I_t(e)=I_s(e')$. In plain words, the index counts the number of times that the walk $B(f)$ goes across the corner (e_1,e_2). Formally, let $B(f)=[e_0,\ldots,e_{k-1}]$ and

$$s_{e,e'} := |\{i \in \mathbf{Z}_k | e = e_i \text{ and } e' = e_{i+1}\}|; \tag{97}$$

(98)

then the index of f in (e,e') is

$$\text{index}(f,e,e') = \begin{cases} s_{e,e'} + s_{e'^{-1},e^{-1}} & \text{if } e^{-1} \neq e' \\ s_{e,e'} & \text{if } e^{-1} = e'. \end{cases} \tag{99}$$

So let $v \in V$ be a vertex and let $k := |\text{star}(v)|$. We say that v is a surface vertex if there exists a cyclic k-tuple $S(v)=[e_0^{\sigma_0},\ldots,e_{k-1}^{\sigma_{k-1}}]$ such that $\text{star}(v)=\{(e_i,\sigma_i)\}_{i=0}^{k-1}$ and

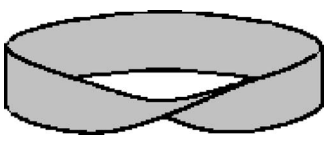


FIG. 14. The Moëbius band.

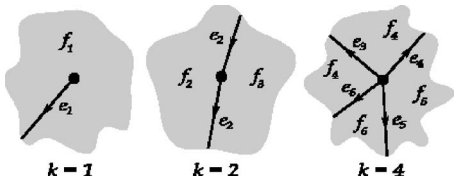


FIG. 15. An illustration of the definition of surface vertex and the expressions (99) and (100). We have, for example, $\mathrm{index}(f_1,e_1,e_1^{-1})=1$, $\mathrm{index}(f_2,e_2,e_2)=1$, and $\mathrm{index}(f_4,e_3^{-1},e_4)=1$.

$$\sum_{f\in F}\mathrm{index}(f,e_i^{\sigma_i},e_j^{-\sigma_j})=\begin{cases}1 & \text{if } k=1\\ 2 & \text{if } k=2, j-i\equiv 1\\ 1 & \text{if } k>2, j-i\equiv \pm 1\\ 0 & \text{in other case,}\end{cases} \tag{100}$$

where $\equiv$ is equality modulo k. Figure 15 illustrates the concept. Then, as a definition, a surface 2-complex is a connected 2-complex such that all its vertices are surface vertices. We also need a way to distinguish orientability. We say that a surface 2-complex is oriented if

$$\sum_{f\in F}\partial f=0. \tag{101}$$

A surface 2-complex for which there is a suitable sign selection for faces so that it is oriented is said to be orientable. Figure 16 clarifies this definition.

An interesting notion that emerges when considering the cell embedding of a graph in a surface is that of duality. The germ of this idea can be traced back to the five regular platonic solids. Each of these polyhedra has a dual polyhedron whose vertices are the center points of the given one. For example, the tetrahedron is self-dual and the cube and the octahedron are dual of each other. The idea can be generalized. Given a cell embedding of a graph Γ in the surface M, the dual embedded graph Γ^* is constructed as follows. For each face f a point f^* is chosen to serve as a vertex for the new graph. For each edge e lying on the boundary of the faces f_1 and f_2, the edge e^* connects f_1^* and f_2^* crossing e once but no other edge or dual edge. Figure 17 shows a pair of examples.

We now work out duality in the context of surface 2-complexes. Consider an oriented surface 2-complex $\Sigma=(V,E,F,I_s,I_t,B)$. We construct the dual 2-complex $\Sigma^*=(V'=F^*,E'=E^*,F'=V^*,I_s',I_t',B')$ where $V^*:=\{v^*|v\in V\}$ and so on. There is a unique $f\in F$ such that $(e^*,\partial f)=1$ (respectively -1) and we set $I_s'(e)=f^*$ [respectively $I_t'(e)=f^*$]. For each $v\in V$, let $S(v)=[e_0^{\sigma_0},\ldots,e_{k-1}^{\sigma_{k-1}}]$ be the cyclic k-tuple from the definition of surface 2-complexes. Then $B'(v^*)=[e_0^{*\sigma_0},\ldots,e_{k-1}^{*\sigma_{k-1}}]$. Now let the operator d take v to v^*, e to e^*, and f to f^*. Extend d linearly to act on any chain. Now, if we denote ∂^* and δ^* the ∂ and δ operators for Σ^*, we have

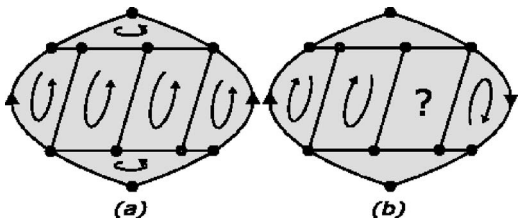


FIG. 16. Two planar representations of 2-complexes for (a) the sphere S and (b) the projective plane P. The identified vertices and edges are the same as in Fig. 11. S is shown with its faces oriented. On the other hand, P is not orientable. The picture shows an attempt to give a coherent orientation and the failure. Note that the impossibility comes from the presence of a Moëbius band. It consists of the faces already oriented and the one with the interrogation sign.

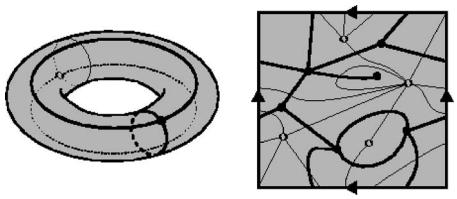


FIG. 17. (a) The standard cell embedding in the torus. The thin lines represent the dual graph. Notice self-duality. (b) A more complicated graph embedded in the torus and its dual. The torus is recovered from the plane model by identification of opposite edges.

$$\delta^* d = d\partial, \quad d\partial^* = \delta d, \tag{102}$$

where the domains must be defined in the apparent way so that the composed function is well defined. Finally, we observe that Σ^* is oriented and $\Sigma^{**} \simeq \Sigma$. If one wants to extend the notion of duality to nonorientable surface 2-complexes, $\mathbf{Z}_2$ homology must be considered in order to eliminate orientation-related problems. We shall not dwell upon this here, however.

Let us enlarge a bit the concept of surface. Take a surface M and a finite collection of disjoint sets $\{D_i\}$ such that each of them is homeomorphic to a disk. We say that $M - \cup_i \mathring{D}_i$ is a *surface with boundary*. We already encountered an important example of such an object, namely, the Moëbius band B. If one attaches to B a disk identifying homeomorphically its boundary with the rim of B, the projective plane P is obtained. We again need a combinatorial definition. Let Σ be a surface 2-complex and $F' \subset F$ a collection of faces with no edge or vertex in common along the boundary walk. We say that $\Sigma' := (V, E, F - F', I_s, I_t, B)$ is a surface with boundary 2-complex. It is quite tempting to atempt an extension of duality to this broader class of 2-complexes. As the dual of a face is a vertex, it is apparent that the dual of a surface with boundary would be a "surface with missing points." Such an object is not a 2-complex, however. To overcome this difficulty, relative homology can be considered. The relative homology of a complex with respect to certain subcomplex is a topic in which we shall not enter, but it is worth mentioning that it would be perfectly suited to the error correcting code construction. Another possibility is to construct the dual of a surface with boundary by identifying the correspondending vertices instead of deleting them. This construction leads us to what is called a pseudosurface, a "surface" which fails to be such a thing only in a finite set of points. From a homological point of view, the result is equivalent. See Fig. 18.

For us the most important example of surface with boundary will be the h-holed disk D_h, $h \geqslant 1$. As a 2-complex, D_h can be constructed with $h+1$ vertices, $2h+1$ edges, and 1 face. Instead of giving explicitly the construction, we prefer to illustrate it with an example in Fig. 19. We have $H_1(D_h) \simeq H^1(D_h) \simeq \mathbf{Z}^h$ and $\chi(D_h) = 1 - h$. The point of these perforated disks is that they have a nontrivial homology while still being a subset of the plane, something that we will find useful when physics come into play.

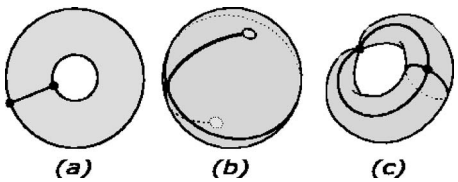


FIG. 18. (a) A 2-complex representing the disk with a hole, D_1. (b) The dual of D_1 in the form of a sphere with two vertices missing. (c) Another possibility for the dual of D_1, obtained by identifying the missing vertices of the previous sphere.

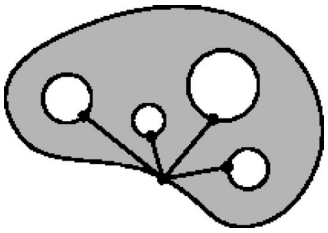


FIG. 19. A 2-complex representing the disk with four holes.

E. Quantum homological codes

From this point on we will be working with qudits of fixed dimension D. Unless otherwise stated, the homology considered will be always homology with coefficients in $\mathbf{Z}_D$.

Before introducing homological quantum error correcting codes we still need a pair of definitions. Given a 2-complex Σ, let $E=\{e_i\}_{i=1}^{|E|}$. Consider the isomorphisms $\mathbf{h}_1: C_1(\Sigma)\to\mathbf{Z}_D^{|E|}$ and $\mathbf{h}_2: C^1(\Sigma)\to\mathbf{Z}_D^{|E|}$ defined by

$$\mathbf{h}_1\left(\sum_{i=1}^{|E|}\lambda_i e_i\right) := (\lambda_0,\lambda_1,\ldots,\lambda_{|E|}), \tag{103}$$

$$\mathbf{h}_2\left(\sum_{i=1}^{|E|}\lambda_i e_i^*\right) := (\lambda_0,\lambda_1,\ldots,\lambda_{|E|}). \tag{104}$$

Let $\mathbf{h}: C_1(\Sigma)\cup C^1(\Sigma)\to\mathbf{Z}_D^{2|E|}$ be

$$\forall c_1 \in C_1(\Sigma), \quad \mathbf{h}(c_1) := (\mathbf{0}\mathbf{h}_1(c_1)), \tag{105}$$

$$\forall c^1 \in C^1(\Sigma), \quad \mathbf{h}(c^1) := (\mathbf{h}_2(c^1)\mathbf{0}). \tag{106}$$

Then

$$\mathbf{h}_2(c^1)\cdot\mathbf{h}_1(c_1) = \mathbf{h}(c^1)^t\Omega\mathbf{h}(c_1) = (c^1,c_1). \tag{107}$$

It is natural to use the notation $\sigma_{c_1} := \sigma_{\mathbf{h}(c_1)}$ and $\sigma_{c^1} := \sigma_{\mathbf{h}(c^1)}$ so that

$$\sigma_{c^1}\sigma_{c_1} = \varphi((c^1,c_1))\sigma_{c_1}\sigma_{c^1}. \tag{108}$$

As we did for graphs, we can pull back the weight function through $\mathbf{h}_1$ and $\mathbf{h}_2$. Then we let the distance $d(\Sigma)$ be the minimal weight among the representatives of nontrivial elements of H_1 and H^1.

Theorem 4: *Let Σ be a connected 2-complex. If*

$$V := \mathbf{h}[B^1(\Sigma)]\oplus\mathbf{h}[B_1(\Sigma)] \tag{109}$$

is generated by a linearly independent set, then setting $V_C=V$ a symplectic $[[n,k,d]]$ quantum error correcting code $\mathcal{C}$ is obtained with $n=|E|$, $H_1(\Sigma)\simeq H^1(\Sigma)\simeq\mathbf{Z}_D^k$, and $d=\mathrm{d}(\Sigma)$.

Proof: The isotropy of V_C follows from Eqs. (94) and (107). Also, from Eq. (92) we get $\mathbf{h}_1[Z_1(\Sigma)]=\mathbf{h}_2[B^1(\Sigma)]^\perp$ and $\mathbf{h}_2[Z^1(\Sigma)]=\mathbf{h}_1[B_1(\Sigma)]^\perp$, that is,

$$\hat{V}_C = \mathbf{h}[Z^1(\Sigma)]\oplus\mathbf{h}[Z_1(\Sigma)]. \tag{110}$$

But $\dim\hat{V}_C-\dim V_C=2k$, and since $\dim\mathbf{h}_1[Z_1(\Sigma)]+\dim\mathbf{h}_2[B^1(\Sigma)]=\dim\mathbf{h}_1[B_1(\Sigma)]+\dim\mathbf{h}_2[Z^1(\Sigma)]$ we get as desired $H_1(\Sigma)\simeq H^1(\Sigma)\simeq\mathbf{Z}_D^k$. As for the distance, we recall the expres-

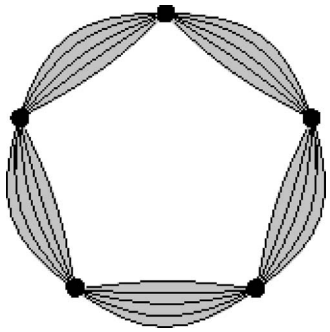


FIG. 20. A 2-complex giving rise to a [[25,1,5]] code.

sion for the code distance given in Eq. (68) and observe that a vector in $\hat{V}_C$ and not in V_C is of the form $\mathbf{h}(c_1)+\mathbf{h}(c^1)$ with c_1 or c^1 homologically nontrivial.

□

The condition that Σ be connected is just to avoid having a code which can be decomposed into two more simple ones. As for graphs, there is no point at all in considering disconnected 2-complexes; given such a disconnected 2-complex with components Σ_i one can consider the wedge product of them, $\vee_i\Sigma_i$, giving raise to the same code. The wedge product is obtained by choosing one vertex from each component and identifying them all.

Because of the condition stating that the subspace (109) must be a linear subspace with a basis which is a linearly independent set in $\mathbf{Z}_D^{2n}$, not every 2-complex can be used to produce codes for general qudits. For example, consider the case $D=4$ in P, the projective plane. In this case $H_1 \simeq \mathbf{Z}_2$ and thus a code cannot be constructed. The origin of the problem is in the torsion subgroup appearing in nonorientable surfaces. However, we can get rid of it if we only consider the case $D=2$ in this surfaces, as we shall do. Under this assumption and restricting attention to surface 2-complexes, we can give a more geometrical definition for the distance. Let Σ be a surface 2-complex, and let Γ be its graph. Let also $\mathrm{Cy}'(\Gamma)$ be the set of simple subcycles of Γ not homologous to a point, and $\mathrm{d}'(\Sigma)$ the minimal length among the elements of $\mathrm{Cy}'(\Gamma)$. Then

$$d(\Sigma) = \min\{d'(\Sigma), d'(\Sigma^*)\}. \tag{111}$$

To gain intuition on the construction of the codes, consider the special case of a graph as a 2-complex. In this case we obtain a pseudoclassical code, capable of correcting errors of the form $\sigma_{\mathbf{x}0}$ whenever $\mathbf{x}$ is correctable in the corresponding classical code.

It is possible to construct homological quantum codes inspired by classical ones. Consider for example, the graphs C_d, related to $[d,1,d]$ classical linear codes. Joining d copies of C_d along vertices and attaching $d(d-1)$ faces, as shown in Fig. 20, gives a $[[d^2,1,d]]$ code. In particular, for $d=3$ we get Shor's original [[9, 1, 3]] code. Unfortunately, $\lim_{d\to\infty} d/n=0$, which is very different to the classical case. This first example already shows that the length of quantum homological codes does not seem to behave very well when the distance grows. However, below we show that this is not the case when k grows.

In general, homological quantum codes can be degenerate. It is enough to have a vertex lying in less than $d/2$ edges or a boundary with less than $d/2$ edges to have degeneracy. Such examples of degenerate codes will show up in the next section.

F. Surface codes

In this section we study homological quantum codes derived from 2-complexes representing surfaces. Such 2-complexes are usually regarded as cell embeddings of graphs on surfaces, and so we will tend to use the language of topological graph theory. Note that the genus is directly related to the number of encoded qudits; codes derived from gT encode $k=2g$ qudits, and codes derived

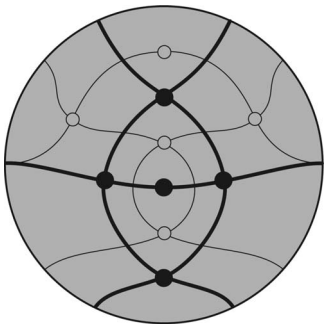


FIG. 21. A self-dual cell embedding in P. The projective plane is recovered by identifying opposite edges of the circumference. This embedding leads to a [[9,1,3]] code for qubits.

from gP encode $k=g$ *qubits*. This can be put altogether using the Euler characteristic; cell embeddings of graphs on a surface M will give codes with

$$k = 2 - \chi(M). \tag{112}$$

As a first example of a surface code, Fig. 21 shows a self-dual embedding on P giving a [[9, 1, 3]] code.

The whole problem of constructing good codes related to a certain surface relies on finding embeddings of graphs in such a way that both the embedded graph *and* its dual have a big distance whereas the number of edges keeps as small as possible. But let us be more accurate.

Definition 5: *Given a surface M and a positive integer d we let the quantity $\mu(M,d)$ be the minimum number of edges among the embeddings of graphs in M giving a code of distance d.*

Since we do not know how to calculate the value of the function μ, we shall investigate some properties of this function. The problem of locality suggests also the introduction of a refinement of μ; the quantity $\mu_l(M,d)$ is defined as $\mu(M,d)$ but with the restriction that the graphs can have faces with at most l edges and vertices lying on at most l edges. Locality here means that we want that the vertex $\sigma_{\delta v}$ and face $\sigma_{\partial f}$ operators act on at most l qudits. Having operators as local as possible simplifies the error correction stage. We shall return on this issue below.

We stress that in the case of nonorientable surfaces we *only* consider $\mathbf{Z}_2$ homology. Keeping this in mind, we can state the following.

Theorem 6: *The function $\mu(M,d)$ is subadditive in its first argument, in the sense that given two surfaces M_1 and M_2*

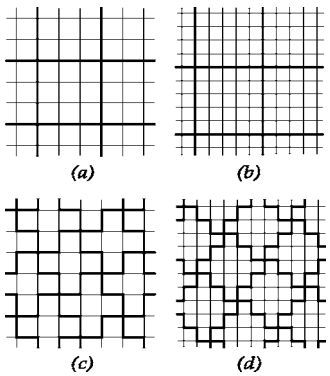


FIG. 22. A graphical comparison between the original toric codes and their optimized versions. The thick lines are the border of tesserae and the torus is recovered as a quotient of the plane and its tessellation. [(a) and (b)] The toric codes introduced in Ref. 19, for $d=3$ and $d=5$. [(c) and (d)] The optimal regular toric codes for $d=3$ and $d=5$.

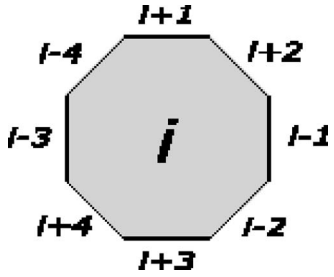


FIG. 23. The self-dual embedding of K_9 in the 10-torus can be described using addition in $\mathbf{Z}_9$. It is enough to label the eight-sided faces with $i=0,\ldots,8$ and glue them altogether as the picture indicates.

$$\mu(M_1 \sharp M_2, d) \leqslant \mu(M_1, d) + \mu(M_2, d). \tag{113}$$

The proof is given in Appendix B.

The most simple orientable surface with nontrivial first homology group is the torus. In Ref. 19, a family of so-called toric codes was presented, in the form of self-dual regular lattices on the torus. An investigation on other regular lattices on the torus led us to another system of lattices that demand half the number of qudits whereas it keeps the same good properties as the the first one; in particular, vertex and face operators act on four qudits. In fact, in Ref. 19 only qubits were considered. Examples of both systems of lattices are depicted in Fig. 22, where the torus is represented as a quotient of the plane through a tessellation. In Appendix C we show the optimality of our system. The original toric codes lead to a family of $[[2d^2, 2, d]]$ codes. Our lattices give $[[d^2+1, 2, d]]$ codes. This already shows that

$$\mu(T, d) \leqslant \mu_4(T, d) \leqslant d^2 + 1. \tag{114}$$

Invoking subadditivity, we learn that $\mu(gT, d)$ is $O(x^2)$ in its second argument, that is, it grows at most cuadratically with d.

A closer examination of Fig. 22 reveals that the lattice giving a [10,2,3] code is a self-dual embedding of K_5. This suggests considering self-dual embeddings of K_s, since such an embedding would give a $\left[\left[\binom{s}{2}, \binom{s}{2} - 2(s-1), 3\right]\right]$ code, see Fig. 23. In fact, these embeddings are possible in orientable surfaces with the suitable genus as long as $s \equiv 1 (\mathrm{mod}\ 4)$,[68] and this family of codes with self-dual embeddings of complete graphs is enough to show that the coding rate k/n behaves as

$$\lim_{k\to\infty} \frac{k}{n} = \lim_{g\to\infty} \frac{2g}{\mu(gT, 3)} = 1. \tag{115}$$

In order to verify this, note first that $\mu(gT, d) \geqslant \mu(gT, 1) = 2g$. Let $K(s) = \binom{s}{2} - 2(s-1)$. Due to subadditivity, for $K(s)/2 \leqslant g < K(s+1)/2$ we have $\mu(gT, 3) \leqslant \mu((K(s)/2)T, 3) + (g - (K(s)/2))\mu(T, 3) = \binom{s}{2} + O(s)$.

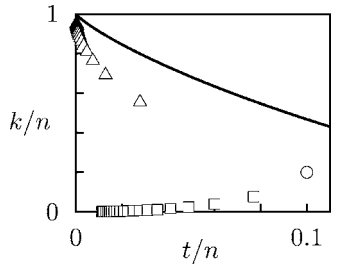


FIG. 24. The rate k/n vs t/n for the codes derived from self-dual embeddings of the complete graphs K_{4l+1} (△) and for the optimized toric codes (□); ○ corresponds to the embedding of K_5 in the torus. The quantum Hamming bound is displayed as a reference (solid line).

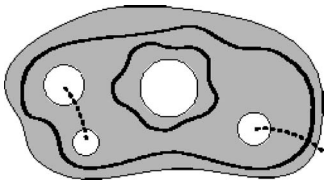


FIG. 25. Examples of noncorrectable errors in D_4. For clarity, the embedded graph is not shown. The thick lines represent typical elements of H_1, that is, cycles in the direct graph not homologous to zero. The dashed lines are elements of H^1, in the form of cycles in the dual graph.

The limit (115) shows that the ratio k/n is asymptotically 1, and thus good codes can be constructed using surfaces. Figure 24 displays the rates for this family of codes and also for the optimized toric codes. The differences with Fig. 7 are apparent.

G. Planar codes

We now focus on homological quantum codes derived from 2-complexes representing surfaces with boundary. The situation is similar to the previous section and again we talk about cell embeddings of graphs. Note that for such a cell embedding of a graph on a surface with boundary, the boundaries are a subset of the graph.

Surfaces with boundary offer more possible topologies to encode the same amount of qudits. If we remove from a g-torus l nonadjacent faces, H_1 is enlarged with $l-1$ dimensions; removing a single face is useless since its boundary is a linear combination of the boundaries of the remaining faces. The nonorientable case is similar, because we only consider $\mathbf{Z}_2$ homology. The results can again be collected using the Euler characteristic; given a surface with boundary M, not a surface, cell embeddings of graphs on it will give codes with

$$k = 1 - \chi(M). \tag{116}$$

It is time to return on the issue of locality. Although topological codes are local, one has to face the problem of constructing a physical system with the shape of the surface on which the code lyes. At this point, the problem of nonplanarity arises; surfaces with nontrivial first homology group are not a subset of the plane, and so are difficult to realize experimentally. Among surfaces with boundary, however, there *is* such a planar family: the disks with h holes, D_h, which encode h qudits. Figure 25 displays the shape of noncorrectable errors in D_h.

An interesting point is that cell embeddings in gT giving codes of distance d can be transformed to obtain cell embeddings in D_{2g-1}. The idea is to cut each of the handles of the torus, as shown in Fig. 26. The cut must be performed along a simple cycle of the graph, and so the edges of the cycle are duplicated in the process. This means that each cut introduces at least d new edges in the graph. On the other hand, the whole procedure produces the lost of a single encoded qudit. A fundamental drawback of this method is that cocycles of length less than d could appear, thus diminishing the distance of the code. In such a case some additional edges could be added. However, it is also very possible that some edges become unnecessary after the cut: Fig. 27 shows an example.

FIG. 26. How to cut a torus of genus 2 to obtain a surface with boundary homeomorphic to a disk with three holes.

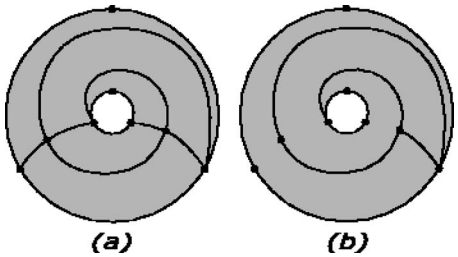


FIG. 27. (a) The result of cutting the self-dual embedding of K_5 in T. (b) Some of the edges of the previous embedding can be deleted and still obtain a code of distance 3.

Another possible drawback of the cutting procedure is that the resulting embedding could be quite odd shaped, and thus perhaps not very useful when true locality is necessary. In any case, one can always switch to more regular embeddings if the number of edges is unimportant. Figure 28 displays such an embedding.

It is possible to remove the condition that all faces must be homeomorphic to disks. In that case we are not dealing anymore with homology, but errors can still be visualized in a similar fashion. For example, Shor's [9,1,3] is displayed in Fig. 29.

IV. CONCLUSIONS

Quantum topology holds the promise of providing a mechanism for self-correcting errors without having to resort to constantly monitoring a quantum memory for error syndrome and error fixing. In this fashion, the functioning of a quantum memory would very much resemble the robustness of its classical counterpart. This is the main reason why it is very important to study quantum error correcting codes from a quantum topological point of view. In this paper we have acomplished this task by developing theorems characterizing homological quantum codes for qudits of arbitrary dimension D based on graphs embedded in surfaces of arbitrary topology, either with or without boundaries, orientable or nonorientable. Orientability becomes an issue when trying to construct homological quantum codes using qudits of dimension $D \geqslant 3$, due to the existence of a nontrivial torsion subgroup in the homology group.

In doing so, we have realized that homological codes can also be well defined in the classical case. This is interesting since not every classical code is of homological type. Nevertheless, we find that there exists a family of classical homological codes saturating the classical Hamming bound.

As a result of our work, we have found that the problem of constructing good quantum homological codes on arbitrary surfaces relies on finding embeddings of graphs in such a way that both the embedded graph and its dual graph have a big distance whereas the number of edges

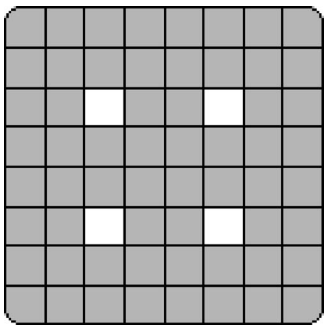


FIG. 28. An example of an embedding in D_4. The corresponding code has distance 3 and encodes four qudits. It is not difficult to generalize this embedding for general d and k; asymptotically the resulting code has $n \propto kd^2$. As usual, the growth is quadratic in d and linear in k.

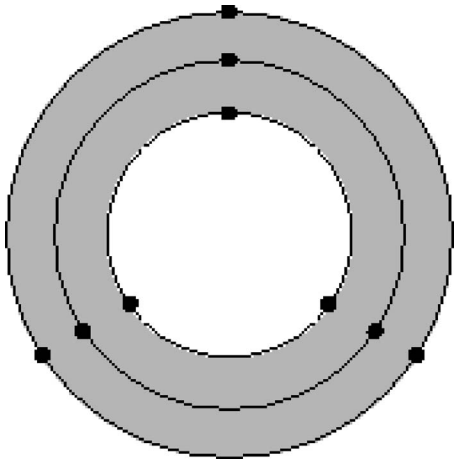


FIG. 29. A visualization of Shor's[9,1,3] code. It can also be considered as an embedding in the torus, since one face can be added for free.

keeps as small as possible. This provides a connection between the theory of quantum topological codes and topological graph theory.[68] More specifically, the problem of finding topological quantum codes is an instance of extremal graph theory which deals with the problem of finding maxima/minima of certain quantities defined on graphs. In our case, it is the distance of a quantum code which has to be maximal on both the embedded graph and its dual. We have given an asymptotically optimal family of codes for the case of distance $d=3$. We leave open the challenge of giving such optimal constructions for higher d.

Finally, we want to point out that our results on quantum homological error correction have further consequences in other areas of quantum information such as quantum channel capacities. In particular, our optimality results may have implications for finding bounds on those capacities. This application is possible, thanks to the result that it is possible to send a nonvanishing amount of quantum data undisturbed through a noisy quantum channel, provided the errors produced by this channel are small enough.[69]

ACKNOWLEDGEMENTS

We acknowledge financial support from a PFI fellowship of the EJ-GV [to one of the authors (H.B.)], DGS grant under Contract No. BFM 2003-05316-C02-01 [to the other author (M.A.M.D.)] and CAM-UCM grant under Ref. No. 910758.

APPENDIX A: GENERATORS OF $Sp_D(n)$

In order to proof that the homomorphism h introduced in Eq. (60) is onto, it is enough to exhibit a subset $S \subset ESp_D(n)$ such that $h[S]$ generates $Sp_D(n)$. We consider the following.

- The Fourier operator on one qudit

$$\mathcal{F} := \sum_{k,l \in \mathbf{Z}_D} \varphi(kl)|k\rangle\langle l|, \tag{A1}$$

$$\mathcal{F}X\mathcal{F}^{\dagger} = Z, \quad \mathcal{F}Z\mathcal{F}^{\dagger} = X^{-1}. \tag{A2}$$

- The operator on one qudit

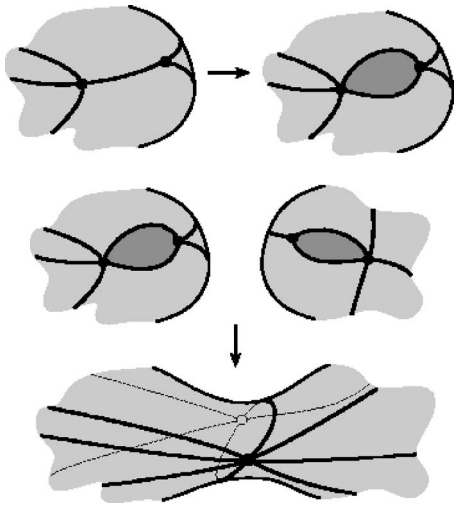


FIG. 30. The construction used to proof the subadditivity of μ. The first step is to perform a cut along a selected edge in each of the embeddings to be added. Then the resulting boundaries must be identified.

$$K := \sum_{k \in \mathbf{Z}_D} f(1)^k \varphi\left(\frac{k(k+1)}{2}\right) |k\rangle\langle k|, \tag{A3}$$

where the argument of φ must be evaluated in $\mathbf{Z}$;

$$KXK^\dagger = f(1)XZ, \quad KZK^\dagger = Z. \tag{A4}$$

- The controlled NOT operator on two qudits

$$U_{\mathrm{CNot}} := \sum_{k,l \in \mathbf{Z}_D} |k,l\rangle\langle k,k+l|; \tag{A5}$$

$$U_{\mathrm{CNot}} X^i \otimes X^j U_{\mathrm{CNot}}^\dagger = X^i \otimes X^{i+j}, \tag{A6}$$

$$U_{\mathrm{CNot}} Z^i \otimes Z^j U_{\mathrm{CNot}}^\dagger = Z^{i-j} \otimes Z^j. \tag{A7}$$

The images under h of these operator on the first qudit(s) plus any qudit permutation generate $Sp_D(n)$.[62]

APPENDIX B: TOPOLOGICAL SUBADDITIVITY OF μ

We proof Theorem 6. The assertion is quite trivial in the case $d=1$. In order to proof it for $d \geqslant 2$, it is enough to construct an embedding of distance d in $M_1 \sharp M_2$ starting with two embeddings of distance d in M_1 and M_2 in such a way that the number of edges does not increase; see Fig. 30. So let Σ_1 and Σ_2 be 2-complexes of distance d representing, respectively, M_1 and M_2. We can suppose that neither of them is a sphere. Since $d \geqslant 2$, there exists an edge e_1 in E_{Σ_1} which is not a self-loop. Let f_1 be a face such that $B_{\Sigma_1}(f) = [\sigma e_1, a, b, \ldots]$, $\sigma \in \{1, -1\}$. We construct a new 2-complex Σ_1' introducing in Σ_1 a new edge e_1' with the same source and target as e_1 and changing the boundary of f_1 so that $B_{\Sigma_1'}(f_1) = [\sigma e_1', a, b, \ldots]$. We proceed in the same manner with Σ_2. Up to this point, we have performed the cutting step of Fig. 13 and constructed two surfaces with boundary, Σ_1' and Σ_2'. Then we construct Σ as a union of Σ_1' and Σ_2' but identifying e_1 and e_2 in a single edge e, and similarly for their primed versions. Of course, the end points of e_1 and e_2 must be properly identified also, but the construction is clear enough so as to be self-explanatory. The resulting 2-complex is a surface, and that it represents the expected one follows from the two

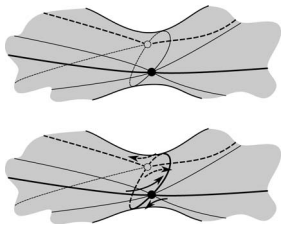


FIG. 31. A simple cycle over the connected sum is divided into two, with each new simple cycle in one of the initial surfaces.

facts: it is orientable iff both Σ_1 and Σ_2 are orientable and $\chi(\Sigma)=\chi(\Sigma_1)+\chi(\Sigma_2)-2$. We still have to check that its distance is d. The key observation is that $e-e'$ is a boundary, in particular, the boundary of the sum of all the faces in Σ_1', properly oriented in the orientable case. Consider, for example, a simple cycle not homologous to zero that contains edges both from $E_{\Sigma_1'}-\{e,e'\}$ and $E_{\Sigma_1'}-\{e,e'\}$; see Fig. 31. It must pass through each end point $\{v_1,v_2\}$ of e exactly once. Then we can construct two simple cycles γ_1 and γ_2 contained, respectively, in Γ_1' and Γ_2'. To this end we "cut" γ in v_1 and v_2 and glue again one of the pieces with e and the other with e'. At least one of the new simple cycles, say γ_1, is not homologous to zero in Σ, and thus in Σ_1'. Then its length is at least d, and the same is then true for the length of γ. Other possible simple cycles, including those in the dual graph, can be similarly worked out.

APPENDIX C: OPTIMAL SELF-DUAL REGULAR TORIC CODES

Let a cell embedding of a simplicial graph on a surface be a (v,f) regular cell embedding if the star of any vertex comprises v edges and the boundary of any face consists of f edges. On the torus, only the combinations (4,4), (3,6), and (6,3) are possible, since Euler's characteristic must be zero. We shall investigate here the self-dual case, (4,4). In particular, given a distance $d=2t+1$, we want to know which is the minimum number of edges in a (4,4) regular cell embedding on the torus such that its distance is d.

We shall answer the question using homotopy. We say that an n-tuple $w=(e_1,\ldots,e_n)$, $e_i\in\bar{E}$, is a walk of length n if $I_t(e_i)=I_s(e_{i+1})$, $i=1,\ldots,n-1$. Its inverse is $w^{-1}=(e_n^{-1},\ldots e_1^{-1})$. The empty walk is also a walk. If $w=(\ldots,e_n)$ and $w'=(e_1',\ldots)$ are such that $I_t(e_n)=I_s(e_1)$, then the composed walk is $w+w'=(\ldots,e_n,e_1',\ldots)$. If a walk is of the form $w=w_1+w_2+w_3$, and the boundary of a face (or its inverse) can be expressed as a walk as $b=w_2+w_4$, then we say that w and $w'=w_1+w_4^{-1}$

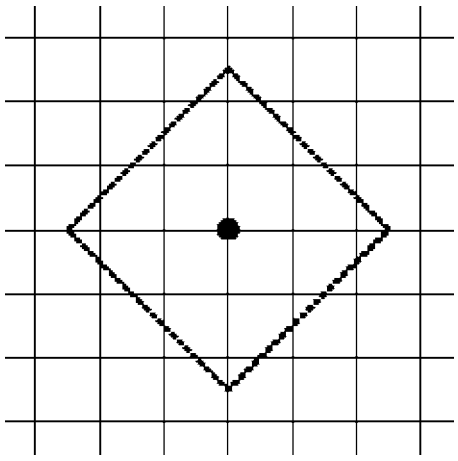


FIG. 32. An infinite square lattice on the plane. The vertices inside the dashed square are at most at distance 2 from the distinguished one.

$+w_3$ are homotopic and write $w \sim w'$. On a given embedding of a graph, we can choose any vertex v as a base point and consider the walks starting at v under the equivalence just stated. The resulting equivalence classes are the vertices of a new graph, naturally embedded in the universal cover of the surface under consideration.

In the case of (4,4) regular cell embeddings in the torus, the resulting graph is an infinite square lattice on the plane, as in Fig. 32. Let Γ be the original graph on the torus and Γ' the obtained graph on the plane. There is a natural projector $p:\Gamma' \to \Gamma$ taking vertices to vertices and edges to edges. Let v be the distinguished vertex in Γ' representing the class of walks homotopic to a point. As in Fig. 32, we can consider the set of vertices at a distance at most t from v. If two of them have equal projections, say $p(v_1)=p(v_2)$, then there exists a walk going from v_1 to v_2 of length less or equal to $2t$ such that its projection in Γ is not homotopic to a point. On a torus, this also means that it is not homologous to zero. Therefore, if Γ has distance $d=2t+1$, no such two vertices can exist. This means that Γ must have at least $(d^2+1)/2$ vertices, and thus at least d^2+1 edges. As this minimal size is attained by the embeddings of Sec. III F, we have the desired result.

[1] R. Landauer, Philos. Trans. R. Soc. London, Ser. A **353**, 367 (1995).
[2] R. Landauer, Phys. Lett. A **217**, 188 (1996).
[3] R. Landauer, in *Proceedings of Drexel-4 Symposium on Quantum Nonintegrability-Quantum-Classical Correspondence, Philadelphia, PA, 8 September 1994*, edited by D. H. Feng and B.-L. Hu (International Press, Boston, MA, 1997).
[4] W. G. Unruh, Phys. Rev. A **51**, 992 (1995).
[5] P. Shor, Phys. Rev. A **52**, 2493 (1995).
[6] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[7] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[8] A. M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[9] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[10] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[11] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[12] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Phys. Rev. A **54**, 3824 (1996).
[13] R. Laflamme, C. Miquel, J. P. Paz, and W. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[14] E. Knill, e-print arXiv:quant-ph/9608049.
[15] A. Klappenecker and M. Roetteler, e-print arXiv:quant-ph/0010082.
[16] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **79**, 953 (1997).
[17] M. B. Ruskai, Phys. Rev. Lett. **85**, 194 (2000).
[18] H. Pollatsek and M. B. Ruskai, Linear Algebr. Appl. **392**, 255 (2004).
[19] A. Yu. Kitaev, Ann. Phys. **303**, 2 (2003); e-print arXiv:quant-ph/9707021.
[20] M. H. Freedman, Proc. Natl. Acad. Sci. U.S.A. **95**, 98 (1998).
[21] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).
[22] S. B. Bravyi and A. Yu. Kitaev, e-print arXiv:quant-ph/9811052.
[23] M. Levin and X.-G. Wen, Phys. Rev. B **71**, 045110 (2005).
[24] M. Freedman, C. Nayak, and K. Shtengel, Phys. Rev. Lett. **94**, 147205 (2005).
[25] P. Fendley and E. Fradkin, Phys. Rev. B **72**, 024412 (2005).
[26] A. Kitaev, Ann. Phys. **321**, 2–111 (2003).
[27] M. Freedman, C. Nayak, and K. Shtengel, Phys. Rev. Lett. **94**, 066401 (2005).
[28] S. H. Simon, N. E. Bonesteel, M. H. Freedman, N. Petrovic, and L. Hormozi, Phys. Rev. Lett. **96**, 070503 (2006).
[29] X.-G. Wen and Q. Niu, Phys. Rev. B **41**, 9377 (1990).
[30] M. Freedman, C. Nayak, and K. Walker, Phys. Rev. B **73**, 245307 (2006).
[31] S. Das Sarma, M. Freedman, and C. Nayak, Phys. Rev. Lett. **94**, 166802 (2005).
[32] A. Kitaev and J. Preskill, Phys. Rev. Lett. **96**, 110404 (2006).
[33] M. Levin and X.-G. Wen, Phys. Rev. Lett. **96**, 110405 (2006).
[34] F. Verstraete, M. A. Martin-Delgado, and J. I. Cirac, Phys. Rev. Lett. **92**, 087201 (2004).
[35] J. J. Garcia-Ripoll, M. A. Martin-Delgado, and J. I. Cirac, Phys. Rev. Lett. **93**, 250405 (2004).
[36] L. M. Duan and G. C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).
[37] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[38] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[39] P. Zanardi and S. Lloyd, Phys. Rev. Lett. **90**, 067902 (2003).
[40] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).
[41] L.-M. Duan, E. Demler, and M. D. Lukin, Phys. Rev. Lett. **91**, 090402 (2003); e-print arXiv:cond-mat/0210564.
[42] A. Micheli, G. K. Brennen, and P. Zoller, Nat. Phys. **2**, 341–347 (2007).
[43] J. K. Pachos, e-print arXiv:quant-ph/0511273.
[44] C. Wang, J. Harrington, and J. Preskill, Ann. Phys. (N.Y.) **303**, 31 (2003).
[45] K. Takeda and H. Nishimori, Nucl. Phys. B **686**, 377 (2004).
[46] R. W. Ogburn and J. Preskill, Lect. Notes Comput. Sci. **1509**, 341 (1999).

[47] M. H. Freedman, A. Kitaev, and Z. Wang, Commun. Math. Phys. **227**, 587 (2002).
[48] M. Freedman, M. Larsen, and Z. Wang, Commun. Math. Phys. **227**, 605 (2002).
[49] M. H. Freedman, A. Kitaev, M. J. Larsen, and Z. Wang, Bull. Am. Math. Soc. **40**, 31 (2003); e-print arXiv:quant-ph/0101025.
[50] P. W. Shor, IEEE Symposium on Foundations of Computer Science, 1996 (unpublished).
[51] E. Knill, R. Laflamme, and W. Zurek, e-print arXiv:quant-ph/9610011.
[52] D. Gottesman, Phys. Rev. A **57**, 127 (1998).
[53] D. Aharonov and M. Ben-Or, in Proceedings of the 29th Annual ACM Symposium on Theory of Computing, El Paso, TX, May 1997 (unpublished), pp. 176–188.
[54] C. Zalka, e-print arXiv:quant-ph/9612028.
[55] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 385 (1998).
[56] P. Aliferis, D. Gottesman, and J. Preskill, Quantum Inf. Comput. **6**, 97 (2006).
[57] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **73**, 062303 (2006).
[58] M. H. Freedman and D. A. Meyer, e-print arXiv:quant-ph/9810055.
[59] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, New York, 1977).
[60] D. Welsh, *Codes and Cryptography* (Oxford University Press, Oxford, 1988).
[61] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[62] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **72**, 032313 (2005).
[63] A. Steane, in *Introduction to Quantum Computation and Information*, edited by H.-K. Lo, T. Spiller, and S. Popescu (World Scientific, Singapore, 1998).
[64] J. Preskill, *Lecture Notes on Quantum Computation*; http://www.theory.caltech.edu/people/preskill/ph229/notes/chap7.ps
[65] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[66] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
[67] P. J. Giblin, *Graphs, Surfaces, and Homology: An Introduction to Algebraic Topology* (Chapman and Hall, London, 1981).
[68] J. L. Gross and T. W. Tucker, *Topological Graph Theory* (Wiley, New York, 1987).
[69] M. Keyl and R. F. Werner, Lect. Notes Phys. **611**, 263 (2002) and references therein.

Topological quantum error correction with optimal encoding rate

H. Bombin and M. A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain
(Received 10 February 2006; published 6 June 2006)

We prove the existence of topological quantum error correcting codes with encoding rates k/n asymptotically approaching the maximum possible value. Explicit constructions of these topological codes are presented using surfaces of arbitrary genus. We find a class of regular toric codes that are optimal. For physical implementations, we present planar topological codes.

DOI: 10.1103/PhysRevA.73.062303 PACS number(s): 03.67.Lx

I. INTRODUCTION

Quantum computation has overcome major difficulties and has become a field of solid research. On the theoretical side, several models of quantum computation are already proposed, such as the quantum network model using a set of universal logic gates. Quantum error correction and fault tolerant quantum computation have been proved to be well established theoretically. On the experimental side, test-ground experiments have been conducted with a small number of quantum logic gates based on several proposals for realizing qubits. These constitute proof-of-principle experimental realizations showing that theory meets experiment.

Yet, it still faces a major challenge in order to build a real quantum computer: for a scalable quantum computer to ever be built, we have to battle decoherence and systematic errors in an efficient way [1,2]. In fact, the network model corrects errors combinatorially and this requires a very low initial error rate, known as the threshold, in order to stabilize a quantum computation [3–6].

There exists a very clever proposal of fault-tolerant quantum computation based on quantum topological ideas [7,8]. The idea is to design the quantum operations so as to have a physically built-in mechanism for error correction, without resorting to external corrections every time an error occurs [9]. The key point here is that quantum topology is a global resource that is robust against local errors, thereby providing a natural setup for fault tolerance [10].

II. TOPOLOGICAL CODES ON ARBITRARY SURFACES

A prerequisite for a topological quantum code (TQC) is a TQC for error detection and correction. It serves also as a quantum memory. In addition, quantum error correction codes are useful for quantum communication channels while sharing the feature of being quantumly robust.

A Hamiltonian can be constructed such that its ground state coincides with the code space. The nice thing about TQCs is that the generators are local and this makes feasible the experimental implementation of these codes, although other obstacles have to be overcome, as we shall explain.

In this paper we shall provide explicit constructions of TQCs with encoding rates beating those that can be achieved with current toric codes [7] [see Fig. 1 and Eq. (10)].

A *quantum error correcting code of length n* is a subspace $\mathcal{C}$ of $\mathcal{H}_2^{\otimes n}$, with $\mathcal{H}_2$ the Hilbert space of one qubit, such that recovery is possible after noise consisting of any combination of error operators from some set $\mathcal{E}$ of operators on $\mathcal{H}_2^{\otimes n}$. The set $\mathcal{E}$ is the set of *correctable errors*, and we say that $\mathcal{C}$ *corrects* $\mathcal{E}$. For codes of length n, let $\mathcal{E}(n,k)$ be the set of operators acting on at most k qubits. We define the *distance* of the code $\mathcal{C}$, denoted $d(\mathcal{C})$, as the smallest number d for which the code does not detect $\mathcal{E}(n,d)$. A code $\mathcal{C}$ corrects $\mathcal{E}(n,t)$ if and only if $d(\mathcal{C})>2t$. In this case we say that $\mathcal{C}$ corrects t errors. We talk about $[[n,k,d]]$ codes when referring to quantum codes of length n, dimension 2^k, and distance d. Such a code is said to encode k qubits. The *encoding rate* is k/n.

We consider the following family of operators acting on a string of qubits of length n:

$$\sigma_{\mathbf{v}} := \sigma_{\mathbf{xz}} := \bigotimes_{j=1}^{n} i^{x_j z_j} X^{x_j} Z^{z_j}, \tag{1}$$

where $\mathbf{x},\mathbf{z}\in\mathbf{Z}_2^n$, $\mathbf{v}=(\mathbf{xz}):=(x_1,\ldots,x_n,z_1,\ldots,z_n)$ and X,Z are the standard Pauli matrices. They commute as follows:

$$\sigma_{\mathbf{u}}\sigma_{\mathbf{v}} = \varphi(\mathbf{u}^t\Omega\mathbf{v})\sigma_{\mathbf{v}}\sigma_{\mathbf{u}}, \tag{2}$$

where

$$\Omega := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \tag{3}$$

is a $2n\times 2n$ matrix over $\mathbf{Z}_2$ and $\varphi(k):=e^{\pi i k}$, $k\in\mathbf{Z}_2$. We keep the minus sign in Ω because it appears for higher dimensionality or qudits [11]. The group of all the operators generated by the set of σ operators is the Pauli group $\mathbf{P}_D(n)$.

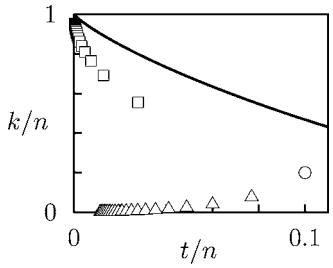


FIG. 1. The rate k/n vs t/n for the optimized toric codes (△) and for the codes derived from self-dual embeddings of graphs K_{4l+1} (□); ○ corresponds to the embedding of K_5 in the torus. The quantum Hamming bound is displayed as a reference (solid line).

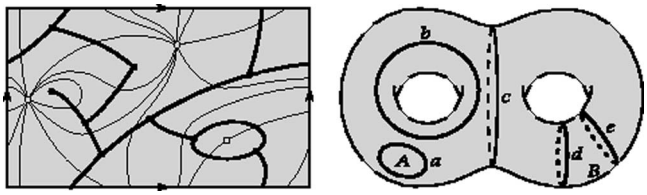


FIG. 2. Left: A graph (thick lines) in the torus and its dual (weak lines). Right: Several cycles in the two-torus. a is the boundary of A, and c is also homologous to zero because it encloses half of the surface. b, d, and e are not homologous to zero. d and e are homologous because they enclose the area B.

There exists a nice construction using the Pauli group to construct the symplectic or stabilizer codes [12,13]. For any subspace $V \subset \mathbf{Z}_2^{2n}$, we define the subspace $\hat{V} := \{\mathbf{u} \in \mathbf{Z}_2^{2n} | \forall \mathbf{v} \in V \mathbf{v}^t \Omega \mathbf{u} = 0\}$. Let $V_{\mathcal{C}} \subset \mathbf{Z}_2^{2n}$ be any *isotropic* subspace, that is, one verifying $V_{\mathcal{C}} \subset \hat{V}_{\mathcal{C}}$ [11]. Let B be one of its basis and set $\mathcal{S} = \{\boldsymbol{\sigma}_{\mathbf{v}} | \mathbf{v} \in B\}$. The code

$$\mathcal{C} := \{|\xi\rangle \in \mathcal{H}_2^{\otimes n} | \forall\, \sigma \in \mathcal{S} \sigma |\xi\rangle = |\xi\rangle\}, \tag{4}$$

detects the error $\sigma_{\mathbf{u}}$ if and only if $\mathbf{u} \in \hat{V}_{\mathcal{C}} - V_{\mathcal{C}}$ and thus its distance is

$$d(\mathcal{C}) = \min_{\mathbf{u} \in \hat{V}_{\mathcal{C}} - V_{\mathcal{C}}} |\mathbf{u}|, \tag{5}$$

where the norm is just the number of qubits on which $\sigma_{\mathbf{u}}$ acts nontrivially. The set $\mathcal{S}$ is the stabilizer of the code. This way, the problem of finding good codes is reduced to the problem of finding good isotropic subspaces $V_{\mathcal{C}}$.

Thus far we have dealt with the purely algebraic structure of codes. Now, we turn to the connection with topology. For a *surface* we understand a compact connected two-dimensional manifold. Well known examples of surfaces are the sphere S, the torus T, and the projective plane P. More generally one can consider the g-torus or sphere with g handles gT, and the sphere with g crosscaps gP. gT and gP are said to have *genus* g. In fact, it is a well known result of surface topology that the previous list of surfaces is complete.

We shall not be restricted to codes based on regular lattices on a torus, or toric codes [7], but we shall use general graphs embedded in surfaces of arbitrary genus in order to explore optimal values of the encoding rate k/n. A *graph* Γ is a collection of *vertices* V and *edges* E. Each edge joins two vertices. A graph is usually visualized flattened on the plane. Now consider a graph Γ embedded in a surface M (see Fig. 2). When M-Γ is a disjoint collection of disks, we say that the embedding is a *cell embedding*. Let us gather these disks into a set of *faces* F.

We now introduce the notion of a *dual graph*, which is crucial for the construction of quantum topological codes. Given a cell embedding Γ_M of a graph Γ in a surface M, the dual embedding Γ_M^* is constructed as follows. For each face f a point f^* is chosen to serve as a vertex for the new graph Γ^*. For each edge e lying in the boundary of the faces f_1 and f_2, the edge e^* connects f_1^* and f_2^* and crosses e. Each vertex v corresponds to a face v^*. The idea is illustrated in Fig. 2.

Let us enlarge a bit the concept of surface. Take a surface M and delete the interiors of a finite collection of nonoverlapping disks. We say that the resulting space is a *surface with boundary*. Note that for any cell embedding in such a surface, the boundary is a subset of the embedded graph. One could argue that no dual graph can be defined for this surface, but in fact this is not a major difficulty. It is enough to think that some of the vertices in the dual graph are "erased." For us the most important example of a surface with boundary will be the h-holed disk D_h, $h \geq 1$.

Consider a cell embedding Γ_M on a surface, with or without a boundary. In order to construct the physical system realizing the topological code $\mathcal{C}$, we attach a qubit to each edge of the graph Γ. The study of the stabilizer and correctable errors of the code gets a benefit by using the Z_2 homology theory, which we shall now introduce. Consider a Z-type operator $\sigma_{\mathbf{0\lambda}}$. A chain is a formal sum of edges $c_1 = \Sigma_j \lambda_j e_j$. We relate chains and Z-type operators setting $\sigma_{c_1} := \sigma_{\mathbf{0\lambda}}$. Similarly, given a cochain or formal sum of dual edges $c^1 = \Sigma_j \lambda'_j e_j^*$, we relate it to an X-type operator setting $\sigma_{c^1} := \sigma_{\mathbf{\lambda' 0}}$. There is a natural product between chains and cochains, namely $(c^1, c_1) := \boldsymbol{\lambda} \cdot \boldsymbol{\lambda}'$. The point is that

$$\sigma_{c^1} \sigma_{c_1} = \varphi((c^1, c_1)) \sigma_{c_1} \sigma_{c^1}. \tag{6}$$

This expression already shows that the commutation relations of operators are determined by the topology of the cell embedding Γ_M. Compare with Eq. (2).

Note that a chain is nothing but a collection of edges, those with a coefficient equal to one, and thus can be easily visualized as lines drawn on the surface. If a chain has an even number of edges at every vertex, we call it a *cycle*. When a cycle encloses an area of the surface, we say that it is a *boundary*. If two cycles enclose an area altogether, they are said to be *homologous*. Boundaries are homologous to zero. Figure 2 illustrates these concepts. *Cocycles* are defined analogously but in the dual graph. *Coboundaries* are a bit different, however, at least in the case of surface with boundary. If cutting the surface along a cocycle divides it into two pieces, then it is a coboundary. Given a face f, we shall denote its boundary by ∂_f. Similarly, given a dual face v^* we denote its coboundary by δv^* (see Fig. 5).

Before stating the main result about general constructions of topological quantum codes for arbitrary graphs embedded in surfaces, we need a pair of ingredients. Given a surface M there always exists some cell embedding on it. The *Euler characteristic* of M is defined by

$$\chi(M) := |V| - |E| + |F|, \tag{7}$$

and it does not depend upon the embedded graph. Now, let Γ_M be a cell embedding of a graph Γ in a surface M. We define the distance $d(\Gamma_M)$ as the minimal length (edge amount) among those cycles which are not homologous to zero. For surfaces with boundary, $d(\Gamma_M^*)$ should be understood as a symbol denoting the minimal length among cocycles.

Theorem 1. Topological codes. Let Γ_M be a cell embed-

ding of a graph in a surface. The symplectic code $\mathcal{C}$ of length $n=|E|$ with stabilizer $\mathcal{S}=\{\sigma_{\delta v^*}|v\in V\}\cup\{\sigma_{\partial f}|f\in F\}$ has distance $d=\min\{d(\Gamma_M),d(\Gamma_M^*)\}$ and encodes $k=2-\chi(M)$ qubits if M does not have any boundary or $k=1-\chi(M)$ qubits if it does.

Proof. This proof involves homology theory. Following standard notation, we denote the first homology group by $H_1=Z_1/B_1$ and the first cohomology group by $H^1=Z^1/B^1$. Now, since $(\delta v^*,\partial f)=0$, the space $V_{\mathcal{C}}$ is isotropic. Note that $V_{\mathcal{C}}\simeq B^1\oplus B_1$. A key observation is that $(\delta v^*,c_1)=0$ if and only if $c_1\in Z_1$, and similarly for ∂f and Z^1. In other words, $\hat{V}_{\mathcal{C}}\simeq Z^1\oplus Z_1$, and the distance [Eq. (5)] is the one stated. As $\dim\hat{V}_{\mathcal{C}}-\dim V_{\mathcal{C}}=2k$, where k is the number of encoded qubits, it only remains to know the dimension of the homology and cohomology group. But we have $H_1\simeq H^1\simeq\mathbf{Z}_2^{2-\chi}$ for surfaces without boundary and $H_1\simeq H^1\simeq\mathbf{Z}_2^{1-\chi}$ for surfaces with boundary. □

Since $\chi(gT)=2-2g$, the g-torus yields codes with $k=2g$ logical qubits. $\chi(gP)=2-g$, and thus codes from gP encode $k=g$ qubits. For the h-holed disk D_h, $\chi(D_h)=1-h$ and $k=h$. The parity check matrix H of a topological code has the diagonal form $\mathrm{diag}(H_1,H_2)$ where the matrices H_1 and H_2 are in essence the incidence matrices of Γ and Γ^*. Thus, topological codes are an example of generalized CSS codes [14,15].

Note that uncorrectable errors are related to cycles which are not homologous to zero. This is exemplified as part of Fig. 5. Therefore, the whole problem of constructing good topological codes related to a certain surface relies on finding embeddings of graphs in such a way that both the embedded graph *and* its dual have a big distance whereas the number of edges keeps as small as possible. Thus, we find that this quantum problem can be mapped onto a problem of what is called *extremal topological graph theory*, a branch devoted to graph embeddings on surfaces [16] and the computation of the maxima and/or minima of certain graph properties. To this end, we find it very useful to introduce the following concept.

Definition 2. Given a surface M and a positive integer d, we let the quantity $\mu(M,d)$ be the minimum number of edges among the embeddings of graphs in M giving a code of distance d.

Since calculating the value of the function μ is a hard problem, we shall investigate some of its properties. The issue of connectivity between sites suggests also the introduction of a refinement of μ. The quantity $\mu_c(M,d)$ is defined as $\mu(M,d)$ but with the restriction that the graphs can have faces with at most c edges and vertices lying in at most c edges. By connectivity here we mean that vertex $\sigma_{\delta v^*}$ and face $\sigma_{\partial f}$ operators should act over at most c qubits. A loosely connected system simplifies the error correction stage.

III. OPTIMAL ENCODING RATES

There is an interesting result in surface topology stating that every surface can be obtained by a combination of S, P, and T. To perform this connection over two surfaces, say M_1 and M_2, one chooses two disks, $D_i\subset M_i$. The *connected sum* of M_1 and M_2, denoted $M_1\sharp M_2$, is constructed by deleting the interiors of D_1 and D_2 and identifying its boundaries. Connecting $g\geqslant 0$ tori to a sphere one gets gT, and connecting $g\geqslant 1$ projective planes one gets gP. The point is that given embeddings of distance d in M_1 and M_2, a new embedding can be constructed in $M_1\sharp M_2$ in such a way that the number of edges does not increase and the distance is preserved. The procedure is displayed in Fig. 3. This implies the following result, which we shall use to proof asymtoptic properties about minimal sizes of topological codes.

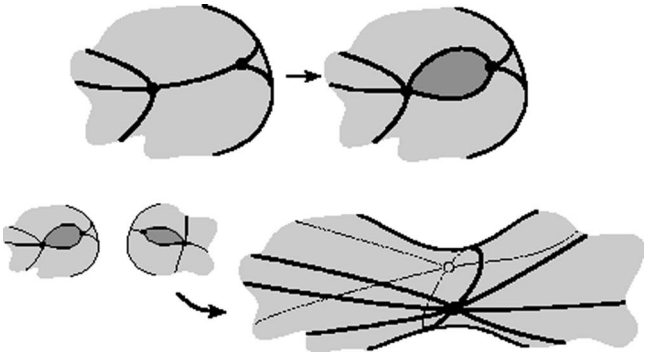


FIG. 3. The construction that proves the topological subadditivity of μ. The first step is to perform a cut along a selected edge in each of the embeddings to be connected. Then the resulting boundaries must be identified.

Proposition 3. Topological subadditivity. Given two surfaces M_1 and M_2

$$\mu(M_1\#M_2,d)\leqslant\mu(M_1,d)+\mu(M_2,d). \tag{8}$$

Let us apply these tools starting with the torus T, the simplest orientable surface with nontrivial first homology group. In Ref. [7], a family of toric codes was presented, in the form of self-dual regular lattices on the torus. This is a very simple instance of topological graph theory. One can consider other self-dual regular lattices embedded on the torus. All of them share the property that vertex $\sigma_{\delta v^*}$ and face $\sigma_{\partial f}$ operators act on $c=4$ qubits. Among them, we have found an optimal family of lattices that demand half the number of qubits. Examples of both systems of lattices are depicted in Fig. 4, where the torus is represented as a quotient of the plane through a tessellation. The original toric codes lead to a family of $[[2d^2,2,d]]$ codes [7]. Our lattices give $[[d^2+1,2,d]]$ codes. This already shows that

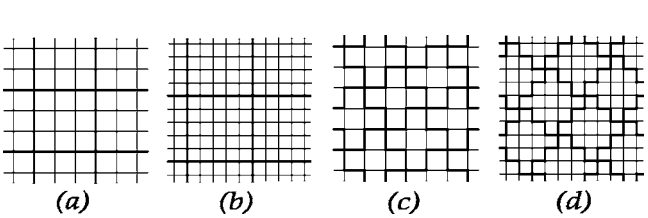


FIG. 4. Four self-dual lattices on the torus. Here the torus is represented as a quotient of the plane and a tessellation of it. Thick lines are the border of tesserae. (a) and (b) The toric codes introduced in Ref. [7], for $d=3$ and $d=5$. (c) and (d) The optimal regular toric codes for $d=3$ and $d=5$.

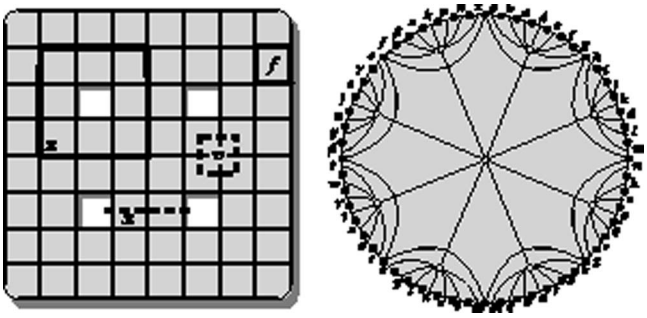


FIG. 5. Left: A graph embedding in the surface D_4 yielding a code of distance 3. We display a boundary ∂f, a coboundary δv^* and two uncorrectable errors of Z- and X-type: The cycle z is not a boundary, and the cocycle x is not a coboundary. Right: The self-dual embedding of K_9 in the ten-torus. Thick lines represent the graph, thin lines represent its dual.

$$\mu(T,d) \leqslant \mu_4(T,d) \leqslant d^2+1. \tag{9}$$

Invoking topological subadditivity, we learn that $\mu(nT,d)$ is $O(d^2)$, that is, it grows at most quadratically with d.

This analysis shows that our toric lattices yield a better encoding rate $k/n \sim 2/d^2$ than the original ones with $k/n \sim 1/d^2$. However, despite being optimal, these toric lattices produce encoding rates vanishing in the limit of large n qubits (see Fig. 1). Then, a major challenge arises: is it possible to find topological quantum codes with nonvanishing encoding rates? And what about approaching the maximum value of 1? The answer is positive in both cases and we hereby show the construction.

To this end, let us introduce the complete graph K_s as the graph consisting of s vertices and all the possible edges among them. A closer examination of Fig. 4 reveals that the lattice giving a [[10,2,3]] code is a self-dual embedding of K_5. This suggests considering self-dual embeddings of K_s, since such an embedding would give a $\left[\left[\binom{s}{2},\binom{s}{2}-2(s-1),3\right]\right]$ code. In fact, these embeddings are possible in orientable surfaces with the suitable genus as long as $s=1 \pmod 4$ [16]. In Fig. 2 we show the constructions of such an embedding. Due to topological subadditivity and the fact that $\mu(gT,d) \geqslant \mu(gT,1)=2g$, the family of codes given by self-dual embeddings of complete graphs K_s is enough to show that for $d=3$

$$\lim_{n\to\infty} \frac{k}{n} = \lim_{g\to\infty} \frac{2g}{\mu(gT,3)} = 1, \tag{10}$$

that is, the ratio k/n is asymptotically one, and thus good topological codes can be constructed, at least in the case of codes correcting a single error. Figure 1 displays the rates for this family of codes and also for the optimized toric codes. Now we can appreciate the very different behavior between toric codes and topological codes embedded in higher genus surfaces, the latter ones allowing us to increase the encoding rate up to its maximal value.

So far we have not touched upon the question of physical implementations. Consider the system of qubits arranged according to a given graph embedding, as explained above. The Hamiltonian

$$H = -\sum_{f\in F} \sigma_{\partial f} - \sum_{v\in V} \sigma_{\delta v^*}, \tag{11}$$

has a degenerate ground state whose elements are the protected codewords. This system is naturally protected against errors [7]. A major drawback is the requirement that the physical disposition of the qubits must give rise to a nontrivial topology. It is difficult to imagine an experimentalist constructing a system living in a torus, for example.

However, the formalism that we have presented allows us to use surfaces with boundary. In particular, the h-holed disk D_h gives rise to codes encoding $k=h$ qubits but has the advantage of being a subset of the plane. Figure 5 shows an example of a very regular embedding in D_4. It is apparent how to generalize this example to a higher number of encoded qubits k and distances d. As in the case of surfaces without boundaries, the length of the code will scale as $O(kd^2)$.

IV. CONCLUSIONS

Finally, we want to emphasize that the locality of topological codes is a very important issue for their implementation in physical systems, now more feasible after the introduction of planar topological codes. The embeddings of complete graphs provide encoding rates that overcome the barrier established so far by toric codes. Moreover, we have introduced a measure of μ that establishes an interplay between quantum information and extremal topological graph theory.

ACKNOWLEDGMENTS

We acknowledge financial support from the EJ-GV (H.B.), DGS grant under Contract No. BFM 2003-05316-C02-01 (M.A.M-D.) and a CAM-UCM grant under Ref. No. 910758.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1996).
[2] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[3] P. W. Shor, in FOCS'37, 56–65 (1996).
[4] E. Knill, R. Laflamme, and W. Zurek, e-print quant-ph/9610011.
[5] A. Yu. Kitaev, Russ. Math. Surveys **52**, 1191 (1997).
[6] D. Aharonov and M. Ben-Or, e-print quant-ph/9611025; e-print quant-ph/9906129.
[7] A. Yu. Kitaev, Ann. Phys. **303**, 2 (2003).
[8] M. H. Freedman *et al.*, Bull., New Ser., Am. Math. Soc. **40**, 31 (2002); e-print quant-ph/0101025.
[9] E. Dennis, A. Kitaev, and A. Landahl, J. Math. Phys. **43**, 4452

(2002)
[10] J. Preskill, http://www.theory.caltech.edu/people/preskill/ph229/index.html
[11] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **72**, 032313 (2005).
[12] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[13] A. R. Calderbank, E. M. Rains, D. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[14] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[15] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[16] J. L. Gross and T. W. Tucker, *Topological Graph Theory* (Wiley, New York, 1987).

Topological Quantum Distillation

H. Bombin and M. A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain
(Received 22 May 2006; published 30 October 2006)

We construct a class of topological quantum codes to perform quantum entanglement distillation. These codes implement the whole Clifford group of unitary operations in a fully topological manner and without selective addressing of qubits. This allows us to extend their application also to quantum teleportation, dense coding, and computation with magic states.

DOI: 10.1103/PhysRevLett.97.180501 PACS numbers: 03.67.Mn, 03.67.Lx

One of the main motivations for introducing topological error-correction codes [1–4] in quantum-information theory is to realize a naturally protected quantum system: one that is protected from local errors in such a way that there is no need to explicitly perform an error syndrome measurement and a fixing procedure. Physically, this is achieved by realizing the code space in a topologically ordered quantum system. In such a system, we have a gap to system excitations and topological degeneracy, which cannot be lifted by any local perturbations to the Hamiltonian. Only topologically nontrivial errors are capable of mapping degenerate ground states onto one another. Thus, a natural question is how to implement quantum-information protocols in a topological manner, thereby getting the benefits provided by quantum topology.

Quantum distillation of entanglement is one of those very important protocols in quantum information [5]. It allows us to purify initially mixed states with a low degree of entanglement towards maximally entangled states, which are needed in many quantum-information tasks. The most general description of entanglement distillation protocols [5–7] relies on the implementation of unitary operations from the Clifford group. This is the group of unitary operators acting on a system of n qubits that map the group of Pauli operators onto itself under conjugation.

In this Letter, we have been able to construct quantum-topological codes that allow us to implement the Clifford group in a fully topological manner. The Clifford group also underlies other quantum protocols besides distillation. Thus, as a bonus, we obtain complete topological implementations of quantum teleportation and superdense coding. We call these topological codes triangular codes. In addition, they have two virtues: (i) There is no need for selective addressing, and (ii) there is no need for braiding quasiparticles. The first property means that we do not have to address any particular qubit or set of qubits in order to implement a gate. The second one means that all we use are ground state operators, not quasiparticle excitations.

In order to achieve these goals, we shall proceed in several stages. First, we introduce a new class of topological quantum error-correcting codes that we call color codes. Unlike the original topological codes in Ref. [1], these are not based in a homology-cohomology setting. Instead, there is an interplay between homology and a property that we call color for visualization purposes. This color is not a degree of freedom but a property emerging from the geometry of the codes. After color codes have been presented for closed surfaces, we show how colored borders can be introduced by doing holes in a surface. In particular, we define triangular codes, so called because they consist of a planar layer with three borders, one of each color. These codes completely remove the need for selective addressing. If the lattice of a triangular code is suitably chosen, we show that the whole Clifford group can be performed on it. Finally, we give the Hamiltonian that implements the desired self-correcting capabilities. It is an exactly solvable local Hamiltonian defined on spin-$1/2$ systems placed at the sites of a two-dimensional lattice.

A quantum error-correcting code of length n is a subspace $\mathcal{C}$ of $\mathcal{H}_2^{\otimes n}$, with $\mathcal{H}_2$ the Hilbert space of one qubit. Let the length of an operator on $\mathcal{H}_2^{\otimes n}$ be the number of qubits on which it acts nontrivially. We say that the code $\mathcal{C}$ corrects t errors when it is possible to recover any of its (unknown) states after any (unknown) error of length at most t has occurred. Let $\Pi_{\mathcal{C}}$ be the projector onto $\mathcal{C}$. We say that $\mathcal{C}$ detects an operator $\mathcal{O}$ if $\Pi_{\mathcal{C}}\mathcal{O}\Pi_{\mathcal{C}} \propto \Pi_{\mathcal{C}}$. The distance of a code is the smallest length of a nondetectable error. A code of distance $2t + 1$ corrects t errors. We talk about $[[n, k, d]]$ codes when referring to quantum codes of length n, dimension 2^k, and distance d. Such a code is said to encode k logical qubits in n physical qubits.

Now let X, Y, and Z denote the usual Pauli matrices. A Pauli operator is any tensor product of the form $\bigotimes_{i=1}^{n} \sigma_i$, with $\sigma_i \in \{1, X, Y, Z\}$. The closure of such operators as a group is the Pauli group $\mathbf{P}_n$. Given an Abelian subgroup $\mathcal{S} \subset \mathbf{P}_n$ not containing $-I$, a stabilizer code of length n is the subspace $\mathcal{C} \subset \mathcal{H}_2^{\otimes n}$ formed by those vectors with eigenvalue 1 for any element of $\mathcal{S}$ [8,9]. If its length is n and $\mathcal{S}$ has s generators, it will encode $k = n - s$ qubits. Let $\mathcal{Z}$ be the centralizer of $\mathcal{S}$ in $\mathbf{P}_n$, i.e., the set of operators in $\mathbf{P}_n$ that commute with the elements of $\mathcal{S}$. The distance of the code $\mathcal{C}$ is the minimal length among the elements of $\mathcal{Z}$ not contained in $\mathcal{S}$ up to a sign.

Suppose that we have a two-dimensional lattice embedded in a torus of arbitrary genus such that three links meet at each site and plaquettes can be three-colored; see

Fig. 1 for an example in a torus of genus one. We will take red, green, and blue as colors (RGB). Notice that we can attach a color to the links in the lattice according to the plaquettes they connect: A link that connects two red plaquettes is red, and so on. With such an embedding at hand, we can obtain a color code by choosing as generators for $\mathcal{S}$ suitable plaquette operators. For each plaquette p, there is a pair of operators: B_p^X and B_p^Z. Let I be an index set for the qubits in p's border, then

$$B_p^\sigma := \bigotimes_{i\in I} \sigma_i, \qquad \sigma = X, Z. \tag{1}$$

Color codes are local because [1] each generator acts on a limited number of qubits and each qubit appears in a limited number of generators, whereas there is no limit in the code distance, as we shall see.

We will find it very useful to introduce the notion of shrunk lattices, one for each color. The red shrunk lattice, for example, is obtained by placing a site at each red plaquette and connecting them through red links; see Fig. 1. Note that each link of a shrunk lattice corresponds to two sites in the colored one. Note also that green and blue plaquettes correspond to the plaquettes of the red shrunk lattice.

We classify the plaquettes according to their color into three sets R, G, and B. Observe that for $\sigma = X, Z$

$$\prod_{p\in R} B_p^\sigma = \prod_{p\in G} B_p^\sigma = \prod_{p\in B} B_p^\sigma \tag{2}$$

hold because these products equal $\hat{\sigma} := \sigma^{\otimes n}$. We shall be using this hat notation for operators acting bitwise on the physical qubits of the code. Equation (2) implies that four of the generators are superfluous. We can now calculate the number of encoded qubits using the Euler characteristic of a surface $\chi = f + v - e$. Here f, v, and e are the number of plaquettes, sites, and links of any lattice on the surface.

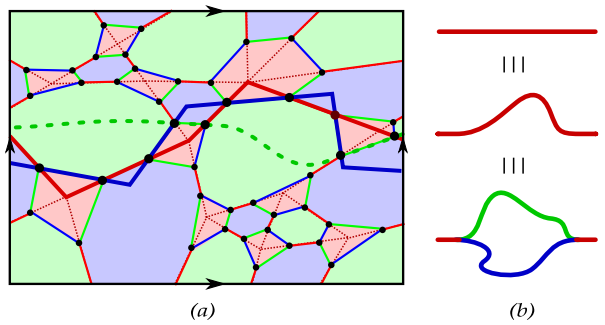


FIG. 1 (color online). (a) A color code in a torus. Each site is a qubit and each plaquette a generator of the stabilizer $\mathcal{S}$. The dashed red line corresponds to the shrunk red lattice. The thick red and blue lines are string operators. They act on the sites lying on their links. The dotted green line is the string operator that results from the product of the red and the blue one. (b) There are two ways in which we can change the shape of a red string operator. We can either consider homologous strings only or also use the operator equivalence (5).

Applying the definition to a shrunk lattice, we get

$$k = 4 - 2\chi. \tag{3}$$

Observe that the number of encoded qubits depends only upon the surface, not the lattice. When the code is rephrased in terms of a ground state in a quantum system (11), this will be an indication of the existence of topological quantum order [10].

So far, we have described the Hilbert space of the logical qubits in terms of the stabilizer. Now we want to specify the action of logical operators on those qubits. To this end, we introduce an equivalence relation among the operators in $\mathcal{Z}$, which we shall use repeatedly. We say that $A \sim B$ if A and B represent the same quotient in $\mathcal{Z}/\mathcal{S}$. Notice that two equivalent operators will have the same effect in $\mathcal{C}$. Now we introduce the key idea of string operators. They can be red, green, or blue, depending on the shrunk lattice we are considering. Let P be any closed path in a shrunk lattice. We attach to it two operators: If P is a path and the qubits it contains are indexed by I, we define

$$S_P^\sigma := \bigotimes_{i\in I} \sigma_i, \qquad \sigma = X, Z. \tag{4}$$

The point is that string operators commute with the generators of the stabilizer. Also observe that, let us say, a red plaquette operator can be identified both with a green string or with a blue string; see Fig. 2. In both cases, the paths are boundaries, but in the first case it is a boundary for the green shrunk lattice and in the second for the blue one.

We can now relate $\mathbf{Z}_2$ homology theory [11] and string operators. We recall that a closed path is a boundary iff it is a combination of boundaries of plaquettes. For the, say, red shrunk lattice, green and blue plaquettes make up the set of its plaquettes. Thus, two string operators of the same color are equivalent iff their corresponding paths are homologous, that is, if they differ by a boundary. Then it makes sense to label the string operators as $S_\mu^{C\sigma}$, where C is a

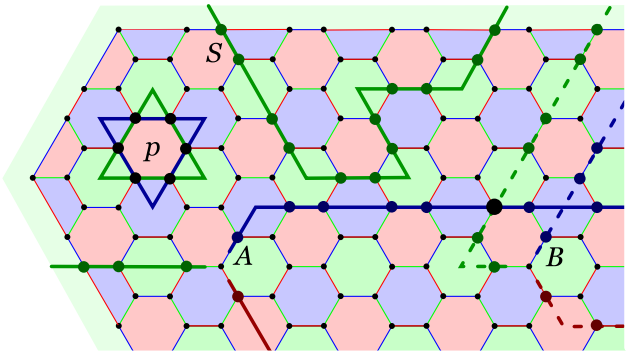


FIG. 2 (color online). A honeycomb lattice with a green border. Notice the two possible points of view for the operators of the plaquette p as boundary paths. The green string S is homologous to part of the border and, thus, is equivalent to the identity. There is also a pair of equivalent three-string operators A and B.

color, σ is a Pauli matrix, and μ is a label related to the homology class. But what about the equivalence of strings of different colors? Figure 1 shows how the product of a pair of homologous red and blue strings related to the same Pauli matrix produces a green string. Note that at those qubits in which both strings cross they cancel each other. In general, we have

$$S_\mu^{R\sigma} S_\mu^{G\sigma} S_\mu^{B\sigma} \sim 1. \tag{5}$$

This property gives the interplay between homology and color, as we will see later.

The commutation properties of strings are essential to their study as operators on $\mathcal{C}$. It turns out that:

$$[S_\mu^{C\sigma}, S_\nu^{C'\sigma}] = [S_\mu^{C\sigma}, S_\mu^{C'\sigma'}] = [S_\mu^{C\sigma}, S_\nu^{C\sigma'}] = 0. \tag{6}$$

The first commutator is trivially null; for the second, note that two homologous strings must cross an even number of times; the third is zero because two strings of the same color always share an even number of qubits. Other commutators will depend on the homology; they will be nonzero iff the labels of the strings are completely different and closed paths in the respective homology classes cross an odd number of times. For example, consider the torus with the labels 1 and 2 for its two fundamental cycles. If we make the identifications

$$Z_1 \leftrightarrow S_1^{RZ}, \quad Z_2 \leftrightarrow S_1^{GZ}, \quad Z_3 \leftrightarrow S_2^{RZ}, \quad Z_4 \leftrightarrow S_2^{GZ}, \tag{7}$$

$$X_1 \leftrightarrow S_2^{GX}, \quad X_2 \leftrightarrow S_2^{RX}, \quad X_3 \leftrightarrow S_1^{GX}, \quad X_4 \leftrightarrow S_1^{RX}, \tag{8}$$

then we recover the usual commutation relations for Pauli operators in $\mathcal{H}_2^4$.

We now determine the distance of color codes. Recall that in order to calculate the distance we must find the smallest length among those operators in $\mathcal{Z}$ which act nontrivially on $\mathcal{C}$. Let the support of an operator in $\mathcal{Z}$ be the set of qubits in which it acts nontrivially. We can identify this support with a set of sites in the lattice. The point is that any operator in $\mathcal{Z}$ such that its support does not contain a closed path which is not a boundary must be in $\mathcal{S}$. The idea behind this assertion is illustrated in Fig. 3. For such an operator O, we can construct a set of string operators with two properties: Their support does not intersect the support of O, and any operator in $\mathcal{S}$ commuting with all of them must be trivial. The distance thus is the minimal length among paths with nontrivial homology.

Strings are all we need to handle tori of arbitrary genus. Things get more interesting if we consider oriented surfaces with a border, which can be obtained by opening holes in a closed surface. In particular, we will introduce holes by removing plaquettes. If we remove, for example, a green plaquette, green strings can have an end point on it, but not blue or red ones. Then borders have a color, and only a green string can end at a green border; see Fig. 2.

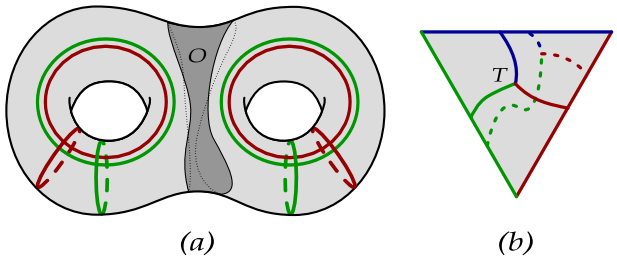


FIG. 3 (color online). (a) The gray area is the support of an operator O in $\mathcal{Z}$. It must be trivial since it commutes with the colored string operators shown, which are enough to construct all X and Z operators for logical qubits. (b) The color structure of a planar triangular code. A three-string operator T and a deformation of it are displayed, showing why $\{T^X, T^Z\} = 0$.

The most important case of such bordered codes are triangular codes. They are constructed starting with a color code in a sphere from which a site and its neighboring three links and three plaquettes are removed. From constraints (2), we observe that two generators of the stabilizer are removed in the process. Since a color code in the sphere encodes zero qubits, a triangular code will encode a single qubit. Examples of triangular codes are displayed in Fig. 4.

So let us show why new features are introduced through triangular codes. Observe that Eq. (5) suggests the construction displayed in Fig. 2: Three strings, one of each color, can be combined at a point and obtain an operator that commutes with plaquette operators. Figure 3(b) shows the color structure of the borders in a triangular code. Let T^σ, $\sigma \in \{X, Z\}$, be the three-string operators depicted in the figure. By deforming T a little, it becomes clear that $\{T^X, T^Z\} = 0$, because T and its deformation cross each other once at strings of different colors. Such an anticommutation property is impossible with strings because of (6).

Although three-string operators can be used to construct an operator basis for the encoded qubit in a triangular code, this can equivalently be done with the operators $\hat{X}$ and $\hat{Z}$. They commute with the stabilizer operators, and $\{\hat{X}, \hat{Z}\} = 0$ because the total number of qubits is odd. The generators

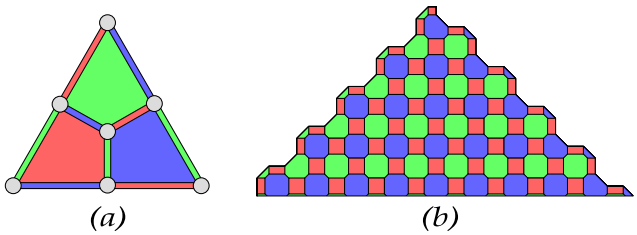


FIG. 4 (color online). (a) The simplest example of a triangular code. The original lattice in the sphere can be recovered by adding a site and linking it to the sites at the vertices of the triangle. (b) Triangular codes of any size can be constructed with the special property that any plaquette has $v = 4m$ sites, with m an integer. This extra requirement is needed in order to implement the phase-shift gate K.

of the Clifford group are the Hadamard gate H and the phase-shift gate K applied to any qubit and the controlled-not gate $\Lambda(X)$ applied to any pair of qubits:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad \Lambda(X) = \begin{pmatrix} I_2 & 0 \\ 0 & X \end{pmatrix}. \tag{9}$$

The action of these gates is completely determined up to a global phase by their action on the operators X and Z of individual qubits, for example,

$$H^\dagger X H = Z, \qquad H^\dagger Z H = X. \tag{10}$$

Now consider $\hat{H}$, $\hat{K}$, and $\hat{\Lambda}(X)$. Of course, $\hat{\Lambda}(X)$ acts pairwise on two code layers that must be placed one on top of the other so that the operation is locally performed. The fact is that in the triangular codes both $\hat{H}$ and $\hat{\Lambda}(X)$ act as the local ones at the logical level, for example:

$$\hat{H}^\dagger \hat{X} \hat{H} = \hat{Z}, \qquad \hat{H}^\dagger \hat{Z} \hat{H} = \hat{X}. \tag{11}$$

Unfortunately, $\hat{K}$ is more tricky because, in general, it does not take ground states to ground states. This is so because $\hat{K} B_p^X \hat{K}^\dagger = (-1)^{v/2} B_p^X B_p^Z$ if the plaquette p has v sites. However, this difficulty can be overcome by choosing a suitable lattice, as shown in Fig. 4. For such a suitable code, if the number of sites is congruent with 3mod4, then $\hat{K}$ acts like $K^\dagger$, but this is a minor detail. As a result, any operation in the Clifford group can be performed on certain triangular codes in a fault-tolerant way and without selective addressing. As for the distance of triangular codes, it can be arbitrarily large: Notice that an operator in $\mathcal{Z}$ acting nontrivially on $\mathcal{C}$ must have a support connecting the red, green, and blue borders.

We can give an expression for the states of the logical qubit $\{|\bar{0}\rangle, |\bar{1}\rangle\}$:

$$|\bar{0}\rangle := 2^{(1-n)/2} \prod_b (1 + B_b^X) \prod_p (1 + B_p^X) |0\rangle^{\otimes n} \tag{12}$$

and $|\bar{1}\rangle := \hat{X}|\bar{0}\rangle$, so that $\hat{Z}|\bar{l}\rangle = (-1)^l |\bar{l}\rangle$, $l = 0, 1$. Observe that, if we have a state in $\mathcal{C}$ and we measure each physical qubit in the Z basis, we are also performing a destructive measurement in the $\hat{Z}$ basis. This is so because the two sets of outputs do not have common elements. In fact, the classical distance between any output of $|\bar{0}\rangle$ and any of $|\bar{1}\rangle$ is at least $2t + 1$. Moreover, we can admit faulty measurements, since the faulty measurement of a qubit is equivalent to an X error previous to it. In this sense, the measuring process is as robust as the code itself.

Now let us return to the general case of an arbitrary color code in a surface with a border. We can give a Hamiltonian such that its ground state is $\mathcal{C}$:

$$H = -\sum_p B_p^X - \sum_p B_p^Z. \tag{13}$$

Observe that color plays no role in the Hamiltonian; rather, it is just a tool we introduce to analyze it. Any eigenstate $|\psi\rangle$ of H for which any of the conditions $B_p^\sigma |\psi\rangle = |\psi\rangle$ is not fulfilled will be an excited state. Then we can say, for example, that a state $|\psi\rangle$ for which $B_p^X |\psi\rangle = -|\psi\rangle$ has an X-type excitation or quasiparticle at plaquette p. These excitations have the color of the plaquette where they live. In a quantum system with this Hamiltonian and the geometry of the corresponding surface, any local error will either leave the ground state untouched or produce some quasiparticles that will decay. This family of quantum systems shows topological quantum order: They become naturally protected from local errors by the gap [12,13].

As a final remark, we want to point out that the ability to perform fault tolerantly any operation in the Clifford group is enough for universal quantum computation as long as a reservoir of certain states is available [14]. These states need not be pure, and so they could be obtained, for example, by faulty methods, perhaps semitopological ones. Namely, one can distill these imperfect states until certain magic states are obtained [14]. These magic states are enough to perform universal quantum computation with the Clifford group, which is different from topological computation based on braiding quasiparticles [1,15,16].

H. B. acknowledges useful discussions with L. Tarruell. We acknowledge financial support from a PFI grant of the EJ-GV (H. B.), a DGS grant under Contract No. BFM 2003-05316-C02-01 (M. A. M.-D.), and CAM-UCM Grant No. 910758.

[1] A. Yu. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (2003).
[2] E. Dennis *et al.*, J. Math. Phys. (N.Y.) **43**, 4452 (2002).
[3] S. B. Bravyi and A. Yu. Kitaev, quant-ph/9811052.
[4] A. Kitaev, cond-mat/0506438.
[5] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
[6] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996).
[7] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **72**, 032313 (2005).
[8] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[9] A. R. Calderbank *et al.*, Phys. Rev. Lett. **78**, 405 (1997).
[10] X.-G. Wen, *Quantum Field Theory of Many-Body Systems* (Oxford University, New York, 2004).
[11] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **73**, 062303 (2006).
[12] A. Kitaev and J. Preskill, Phys. Rev. Lett. **96**, 110404 (2006).
[13] M. Levin and X.-G. Wen, Phys. Rev. Lett. **96**, 110405 (2006).
[14] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[15] M. H. Freedman, A. Kitaev, M. J. Larsen, and Z. Wang, Bull. Am. Math. Soc. **40**, 31 (2003).
[16] J. Preskill, Lecture Notes on Topological Quantum Computation, http://www.theory.caltech.edu/preskill/ph219/topological.ps.

Optimal resources for topological two-dimensional stabilizer codes: Comparative study

H. Bombin and M. A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain
(Received 4 April 2007; published 6 July 2007)

We study the resources needed to construct topological two-dimensional stabilizer codes as a way to estimate in part their efficiency, and this leads us to perform a comparative study of surface codes and color codes. This study clarifies the similarities and differences between these two types of stabilizer code. We compute the topological error-correcting rate $C:=n/d^2$ for surface codes C_s and color codes C_c in several instances. On the torus, typical values are $C_s=2$ and $C_c=3/2$, but we find that the optimal values are $C_s=1$ and $C_c=9/8$. For planar codes, a typical value is $C_s=2$, while we find that the optimal values are $C_s=1$ and $C_c=3/4$. In general, a color code encodes twice as many logical qubits as does a surface code.

DOI: 10.1103/PhysRevA.76.012305 PACS number(s): 03.67.Lx, 03.67.Pp

I. INTRODUCTION

Decoherence of quantum states is one of the main reasons why we have not achieved so far many of the impressive results predicted by quantum-information theory. Battling decoherence has become a very important issue in this field. Devising new strategies to deal with decoherence effects is equally important. One of these strategies, "the topological way," relies on quantum states endowed with a robustness arising when they are embedded into certain Hilbert spaces that exhibit topological protection [1].

Quantum error correction has provided us with definite techniques to do error correction on quantum states belonging to quantum codes [2,3]. A suitable formalism to study quantum error-correction codes is the stabilizer formalism [4]. In fact, a topological quantum code is a special type of stabilizer code [1], as will be discussed in Sec. II. It is a reservoir of states that are intrinsically robust against decoherence due to the encoding of information in the topology of the system.

From the point of view of quantum computation, a quantum error-correcting code is a quantum memory [5–7]. Thus, a topological code amounts to a quantum memory with topological protection, and it can be endowed with extra computational capabilities under certain circumstances [8–10]. Moreover, one remarkable property of topological codes is the fact that their generators are local in the physical qubits of the quantum system. This means that each code generator involves only near-neighbor qubits. This locality property proves to be very useful for performing quantum error-correcting tasks with ancilla qubits, and it becomes an advantage with respect to standard codes, which are nontopological.

The physical mechanism that underlies a topological quantum code is called a topological order [11–13]. This is a new type of quantum phase for matter. In a topological order, there exists ground-state degeneracy without breaking any symmetry, in sharp contrast with more standard phases based on the spontaneous symmetry-breaking mechanism. This degeneracy has a topological origin. Thus, topological orders deviate significantly from more standard orders treated within the Landau symmetry-breaking theory [14–17].

Topological protection is very appealing and has many virtues, but there are also difficulties to implement it in practice. This is currently an active and broad area. We shall not be concerned with experimental realizations of topological codes here.

Our main interest is to analyze the resources needed for their construction and the optimality of those resources. In doing so, we shall perform a very illustrative comparative study of the similarities and differences between the main examples of topological stabilizer codes, namely, surface codes [1] and color codes [18].

This paper is organized as follows. In Sec. II, we introduce the surface codes in a slightly different manner than the usual one [1], but otherwise equivalent. We do so because their comparison with color codes [18] is more transparent in this way. Color codes are constructed with certain two-dimensional complexes, two-colexes, introduced in [15]. We point out the shortcoming of the surface codes with respect to color codes for implementation of a variety of important transverse quantum logic gates belonging to the Clifford group. Another advantage of color codes is that they encode twice the number of logical qubits as do surface codes. In Sec. III, we introduce the notion of topological error-correcting rate C for topological codes. It gives information about how good a code is for error correction when the number of physical qubits, n, is increased. We compute this scaling for both surface codes and color codes with the topology of a torus and a plane, which are the most important examples of topologies in two-dimensional (2D) for practical reasons. Moreover, we compute the optimal values of this figure of merit C for those topological 2D stabilizer codes. Section IV is devoted to conclusions.

II. TOPOLOGICAL 2D STABILIZER CODES

We start by introducing the notion of a stabilizer quantum error-correcting code [4]. Let X, Y, and Z denote the usual Pauli matrices, which act on the space $\mathcal{H}_2$ of a single qubit. A Pauli operator p_n of length n is any tensor product of the form

$$p_n := \bigotimes_{i=1}^{n} \sigma_i, \quad \sigma_i \in \{I,X,Y,Z\}. \tag{1}$$

The closure of such operators as a group is the Pauli group $\mathbf{P}_n$. Given an Abelian subgroup $\mathcal{S} \subset \mathbf{P}_n$ not containing

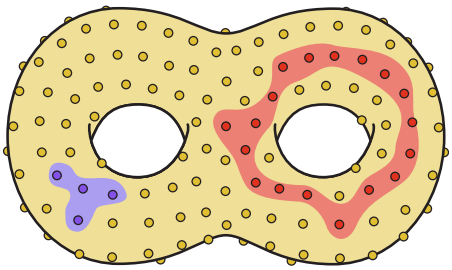


FIG. 1. (Color online) A two-torus is an example of a topological space in which a topological stabilizer code can be constructed. Here the dots represent the qubits pinned down onto the surface. The small blue (darker gray) area on the left is the support of a local generator of the stabilizer $\mathcal{S}$ (2). The big red (darker gray) area on the right, which cannot be deformed to a point, is the support of an undetectable error (in $\mathcal{Z}-\mathcal{S}$).

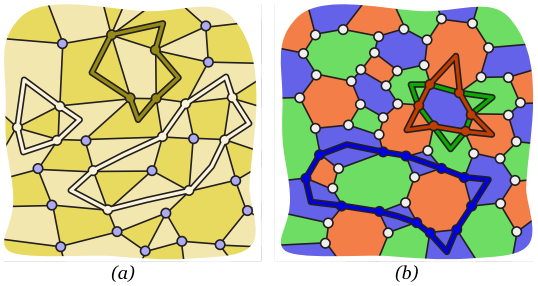
I, a stabilizer code of length n is the subspace $\mathcal{C}\subset\mathcal{H}_2^{\otimes n}$ formed by those vectors $|\phi\rangle$ with eigenvalue 1 for any element $s\subset\mathcal{S}$,

$$s|\phi\rangle = |\phi\rangle. \tag{2}$$

Let $\mathcal{Z}$ be the centralizer of S in $\mathbf{P}_n$, i.e., the set of operators in $\mathbf{P}_n$ that commute with the elements of $\mathcal{S}$. A Pauli operator $z\in\mathcal{Z}$ not contained in S up to a phase leaves $\mathcal{C}$ invariant and acts nontrivially in $\mathcal{C}$. Such operators, when regarded as errors, are clearly undetectable. Let the weight of an operator be the number of qubits in which it acts nontrivially. Then the minimal length among the operators in $\mathcal{Z}-\mathcal{S}$ is called the distance of the code. Indeed, the code is capable of correcting a set of Pauli errors $\mathcal{E}$ as long as for any $M,N\in\mathcal{E}$ the operator $M^\dagger N$ is not an undetectable error. Therefore, a code of distance $d=2t+1$ can correct all the errors of length less than or equal to t. Given $z\in\mathcal{Z}$ and $s\in\mathcal{S}$, z and zs act equally in $\mathcal{C}$. Then, choosing suitably among the equivalence classes of $\mathcal{Z}/\mathcal{S}$, we can find a Pauli operator basis for the encoded qubits.

Topological stabilizer codes can be roughly defined as stabilizer codes in which the generators of $\mathcal{S}$ can be chosen to be local and undetectable errors have a support that is topologically nontrivial, as shown in Fig. 1. We are assuming that the physical qubits that make up the stabilizer code are placed in a certain topological space. In particular, we will only consider codes placed onto two-dimensional surfaces. One of the ideas behind topological stabilizer codes is that the locality of the generators is something very advantageous in order to perform error correction. Another important idea is that of self-protected quantum memories, something that we will touch upon later.

The first example of topological stabilizer codes were the toric codes [1], in which the qubits are placed in a torus. More generally, other surfaces and arbitrary lattices on them can be considered, and the resulting codes were termed, in general, surface codes [19,5]. We will introduce here surface codes in a way that differs slightly from the original one but is absolutely equivalent. Consider any tetravalent lattice [20] with bicolorable plaquettes, such as the one shown in Fig. 2(a). The plaquettes are split into two sets, which we label as



(a) (b)

FIG. 2. (Color online) Typical lattices for both kinds of 2D topological stabilizer codes. In both cases, qubits are represented as circles placed at sites. (a) A piece of a surface code [1]. Dark plaquettes have B_p^X stabilizers attached, while light plaquettes have B_p^Z stabilizers attached. In both cases, these operators correspond to closed strings. For example, an X-string operator which is the product of three dark plaquette operators is shown. (b) A piece of a color code [18]. All plaquettes have B_p^X and B_p^Z stabilizers attached, which can be both visualized as two strings of different colors. In the case of a blue (darkest gray) plaquette, its operators can be considered either as green (softest gray) or as red strings. For example, a blue string operator which is the product of two red and one green plaquette operators is shown.

dark and light sets of plaquettes. A surface code can be obtained from such a lattice by placing a qubit at each of its sites and choosing suitable plaquette operators. In general, given a plaquette p, we define the plaquette operators

$$B_p^\sigma := \bigotimes_i \sigma^{s_p(i)}, \quad \sigma = X,Z, \tag{3}$$

where the product is over all the sites and $s_p(i)$ equals 1 for sites belonging to p and zero otherwise. In the case of surface codes, the generators of $\mathcal{S}$ are B_p^X for dark plaquettes and B_p^Z for light plaquettes. Note how all these operators commute, thus generating an Abelian subgroup. The encoded states $|\phi\rangle$ satisfy the conditions

$$B_p^X|\phi\rangle = |\phi\rangle, \quad \forall \quad p\in P_D, \tag{4}$$

$$B_p^Z|\phi\rangle = |\phi\rangle, \quad \forall \quad p\in P_L, \tag{5}$$

where P_D and P_L are, respectively, the sets of dark and light plaquettes.

Let a Z operator (X operator) be any tensor product of Z's (X's) and I's. Then any Z operator (X operator) can be visualized as a string that connects dark (light) plaquettes and acts nontrivially on those qubits it goes through [see Fig. 2(a)]. Any light (dark) plaquette operator is a Z-string (X-string) operator. Then the product of several plaquette operators of the same kind is a string operator lying on the boundary of certain area containing precisely the plaquettes [see Fig. 2(a)]. Any Pauli operator is, up to a phase, the product of an X string and a Z string. In this sense, the strings belonging to $\mathcal{S}$ are all boundaries. More generally, any operator in $\mathcal{Z}$ is a product of closed string operators. Closed strings are strings without end points, and their importance is now clear since those closed strings which are not boundaries make up precisely the set of undetectable errors. From these undetectable errors we can choose a Pauli operator ba-

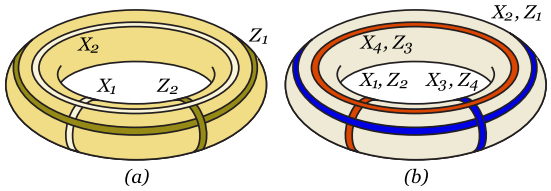


FIG. 3. (Color online) Pauli operator bases in the torus. The encoded operators correspond to certain strings operators. (a) For surface codes [1], the number of encoded qubits is 2. (b) For color codes [18], the number of encoded qubits is 4. Note that each string has two operators attached, one of each type.

sis for the encoded qubits, that is, we can choose the encoded Z and X operators, acting on the logical qubits. It is customary to denote these encoded operators as $\bar{Z}$ and $\bar{X}$ to distinguish them from the standard operators acting on the physical qubits instead. To this end, we note two properties. (i) String operators of the same kind that differ only by a boundary, that is, which are equal up to a deformation, have the same action on encoded states. (ii) A light and a dark string operator commute if they cross an even number of times and anticommute otherwise. Observe that this crossing parity is preserved by the string deformations just mentioned.

Taking this into account, one can obtain the desired Pauli operator basis and find out that the number of encoded qubits is $2g$ for a g torus, that is, a sphere with g "handles," [see Fig. 3(a)].

The topological nature of surface codes makes them very attractive. In particular, the measurements required for quantum error correction can be locally performed and involve the few qubits lying on each plaquette. On the other hand, they are not so nice if one intends to perform transversal operations with codes. In fact, only the controlled-NOT (CNOT) gate can be performed transversally in surface codes. It was precisely with the aim to overcome this difficulty that color codes [18] were devised, which are also 2D topological stabilizer codes but allow the transverse implementation of any operation in the Clifford group. This set of operations is especially suited for quantum-information tasks, such as quantum teleportation or entanglement distillation.

In the case of color codes [18], the starting point is a trivalent lattice with tricolorable plaquettes [see Fig. 2(b)]. We label the plaquettes as green, red, or blue. Again, qubits must be placed at sites, but now for each plaquette p we have both operators B_p^X and B_p^Z as generators of the stabilizer $\mathcal{S}$. The encoded states $|\phi\rangle$ satisfy the conditions

$$B_p^X|\phi\rangle = |\phi\rangle, \quad \forall \quad p, \tag{6}$$

$$B_p^Z|\phi\rangle = |\phi\rangle, \quad \forall \quad p. \tag{7}$$

As in the case of surface codes, string operators are essential for the analysis of color codes. However, now the same geometrical string can be attached to two different operators, the corresponding X and Z strings. An extra labeling turns out to be extremely useful, and so we speak of red, green, and blue strings. Blue strings connect blue plaquettes, and so on, just as X strings connect dark plaquettes in surface codes. Observe how any blue plaquette operator, for example, can be considered both a green and a blue string operator. Also, the product of, say, several green and red plaquette operators is a blue string operator lying in the boundary of certain area containing precisely the plaquettes [see Fig. 2(b)]. As in surface codes, the strings appearing in $\mathcal{S}$ are all boundaries, and the strings appearing in $\mathcal{Z}$ are closed strings. Also, those closed strings that are not boundaries comprise undetectable errors, and from these undetectable errors we can choose the encoded $\bar{Z}$'s and $\bar{X}$'s. Again, we have two guiding properties. (i) String operators of the same type (X or Z) and color that are equal up to a deformation have the same action on encoded states. (ii) String operators commute with one another, unless they cross an odd number of times and have different color and type.

Taking this into account one can obtain a Pauli operator basis and find that the number of encoded qubits is $4g$ for a g torus, that is, two times the number of encoded qubits in surface codes [see Fig. 3(b)]. It is customary to denote a quantum error correcting code made with n physical qubits, encoding k logical qubits and with distance d as $[[n,k,d]]$. With this notation we have that for a fixed surface topology

$$k_c = 2k_s, \tag{8}$$

where the subscript c stands for color codes and s for surface codes. Thus, we see that color codes are more efficient than surface codes as far as the number of encoded qubits is concerned. However, we may wonder whether this doubling of logical qubits has been achieved at the expense of introducing a bigger number of physical qubits n, or whether it affects the correcting capabilities d of the code.

III. EFFICIENCY OF TOPOLOGICAL CODES

To answer those questions, we need to study how efficient 2D topological stabilizer codes are in terms of the number of qubits required with respect to the distance of the code. In fact, regular lattices in which all plaquettes have the same number of qubits are especially relevant. More specifically, it is instructive to consider surface and color codes obtained from regular lattices on the torus. In this case, the plaquettes must be squares for surface codes, and hexagons for color codes (see Fig. 4). Let us consider first the family of surface codes corresponding to Fig. 4(a), which was in fact the first family of topological stabilizer codes [1]. The code in the figure has distance $d=4$, the number of physical qubits is $n=32$, and the number of encoded qubits is $k=2$. More generally, this particular example can easily be generalized to a family of codes in which clearly

$$C_s := \frac{n_s}{d_s^2} = 2. \tag{9}$$

Here, we have defined the notion of error-correcting rate C_s for surface codes, a figure of merit which allows us to compare 2D topological stabilizer codes. It is a measure of how the error-correction capabilities of the code scales when the number of physical qubits is increased. The fact that the number of required qubits scales quadratically with distance

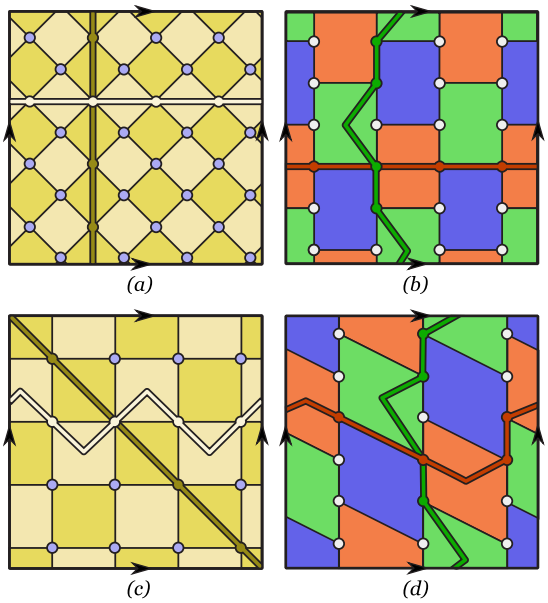


FIG. 4. (Color online) Examples of regular codes in the torus with distance $d=4$. Some nontrivial strings of minimal length are displayed. (a) In the surface code [1], plaquettes are squares and the number of physical qubits is $n=32$. (b) For the color code [18], plaquettes are hexagons and $n=24$. (c) An optimal regular surface code reduces the number of qubits to $n=16$. (d) An optimal regular color code with $n=18$.

is not surprising and is a common feature of all 2D topological stabilizer codes. However, the asymptotic value of C for a quantum error-correction code may vary, and the value 2 is not a particularly good one, as we shall see. Let us consider now the color code in Fig. 4(b). It encodes $k=4$ qubits, is made up of $n=24$ qubits, and its distance is $d=4$. Then we have that the error-correcting rate for this color code is

$$C_c := \frac{n_c}{d_c^2} = \frac{3}{2}. \tag{10}$$

Moreover, this is just an example of an infinite family in which this ratio is preserved, so that apparently color codes not only encode more qubits (8), but also require fewer physical qubits for a given distance.

However, as was noted in [6], the surface codes just considered are not optimal in terms of the number of physical qubits n. In fact, if the optimal codes are chosen, only half of them are really needed, as Fig. 4(c) illustrates. Thus, for optimal regular surface codes in a torus we have

$$C_s^{\mathrm{op}} = 1. \tag{11}$$

Can a similar optimization be obtained for regular color codes? The answer is yes, and the corresponding lattice is illustrated in Fig. 4(d). For this code we have

$$C_c^{\mathrm{op}} = \frac{9}{8}, \tag{12}$$

very close to the value for surface codes. Again, attaching l^2 copies of this lattice together gives a family of codes of distance $4l$ with the same ratio n/d^2. Therefore, we conclude

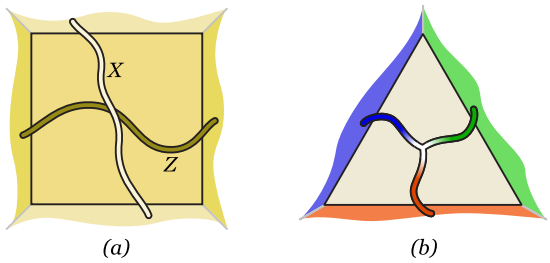


FIG. 5. (Color online) Geometry of planar codes encoding a single qubit. The colors in the borders represent the class of the missing face. Only suitable strings can have end points at each border. The string operators corresponding to encoded operators are shown. (a) A planar surface code. (b) The triangular (color) code, in which encoded operators are related to a string net.

that, in a torus, color codes encode twice as many qubits but surface codes require slightly fewer physical qubits for optimal regular lattices.

Is this true also for other surfaces, or is it something particular to the torus? Instead of trying to answer this question in general, we consider probably the most important example of topological stabilizer codes in practice. By this, we mean planar codes, that is, topological codes that can be placed in a piece of planar surface. More particularly, we want to compare surface and color codes encoding a single qubit, which are the most interesting not only as quantum memories but also for quantum computation [5,8].

The trick to obtain planar codes from lattices related to surfaces without borders is the same for surface and color codes. In particular, it is enough to remove plaquettes from the original lattice until the resulting surface can be unfolded onto a plane. The new lattice has borders, and we have to explain which are the strings that now play the role that closed strings played before in the case of a compact surface like the torus. First, consider what happens when a dark plaquette, that is, the corresponding plaquette operator, is removed from a surface code. Take any Z string that has an end point in the removed plaquette. Since this Z-string operator does not commute with the plaquette operator from the removed plaquette, prior to the removal it was not in $\mathcal{Z}$, but after the removal it could be, at least as far as this end point is concerned. Therefore, the removal of a dark (light) plaquette creates a dark (light) border at which only Z strings (X strings) can end. Additionally, some string operators winding around the removed plaquette are no longer boundaries, but these considerations do not have relevance in the geometries that we are considering. As for color codes, the situation is similar. When a blue plaquette is removed, a blue border is created in which only blue strings can end, and so on and so forth.

With these ideas in mind, it is not difficult to understand the code geometries shown in Fig. 5, which solves the question we have raised before.

For surface codes there are two borders of each type, so that the nontrivial X strings (Z strings) connect light (dark) borders [see Fig. 5(a)]. In the case of color codes, there are three borders, one of each color, and the nature of the encoded operators shows a feature of color codes that we have

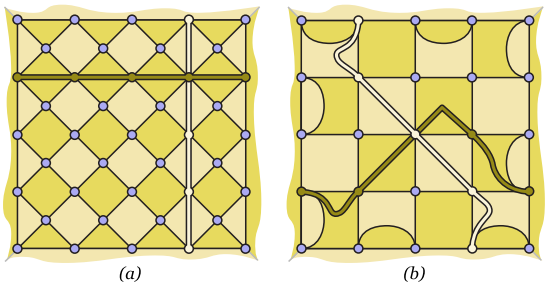


FIG. 6. (Color online) Surface codes encoding a single qubit and with distance $d=5$. (a) A nonoptimal version with $n=41$. (b) An optimized version with $n=25$.

not discussed yet. The point is that in color codes string nets are allowed. In particular, branching points at which three different colored strings of the same type meet are allowed. This means that such a configuration does not violate any of the plaquette conditions. Then, for these triangular codes, the encoded $\bar{X}$ and $\bar{Z}$ operators are constructed with such a string net, as Fig. 5(b) shows.

We want to consider the efficiency of these families of planar codes, which encode a single qubit. In Fig. 6, two different versions of the surface code with distance $d=5$ are shown. The version of Fig. 6(a) belongs to the original family of single-qubit surface codes, for which the asymptotic value of the ratio is

$$C_s \sim 2. \tag{13}$$

This is not the best that can be done, as the code of Fig. 6(b) shows with approximately half the number of qubits and equal distance. In fact, the optimized value for planar surface codes is

$$C_s^{\mathrm{op}} = 1. \tag{14}$$

As for triangular codes, examples for distances $d=3,5,7$ are shown in Fig. 7. It is straightforward to continue this family for arbitrarily large distances. For these color codes, the asymptotic value yields the following optimized value:

$$C_c^{\mathrm{op}} \sim \frac{3}{4}. \tag{15}$$

Therefore, triangular codes are not only particularly interesting for quantum computation [8], but also more efficient in terms of the number of physical qubits required.

Finally, we would like to touch upon how topological stabilizer codes give rise to the idea of self-protected quantum memories. To this end, one must consider a physical system in which qubits are placed according to the geometry of the topological code, and introduce certain Hamiltonian dictated by the generators of the stabilizer. In the case of surface codes, the Hamiltonian is

$$H := -\sum_{p\in P_D} B_p^X - \sum_{p\in P_L} B_p^Z, \tag{16}$$

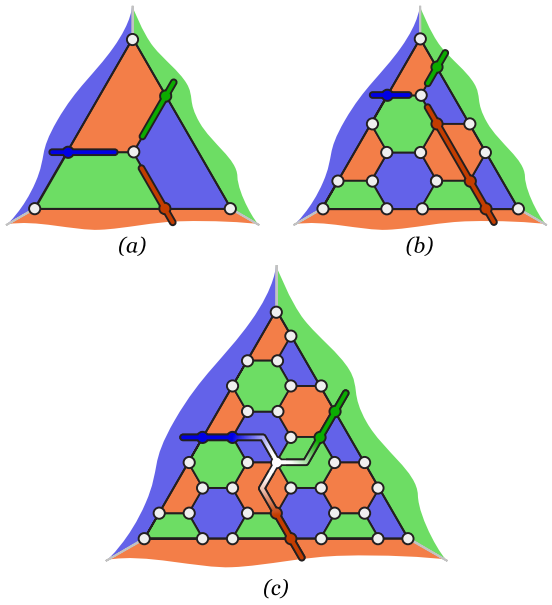


FIG. 7. (Color online) Color codes encoding a single qubit. (a) Triangular code with distance $d=3$ and number of qubits $n=7$. (b) Triangular code with $d=5$ and $n=19$. (c) Triangular code with $d=7$ and $n=37$.

while for color codes it is

$$H := -\sum_{p} (B_p^X + B_p^Z). \tag{17}$$

One of the main differences between these Hamiltonians is that for color codes all plaquettes play the same role, whereas in the case of surface codes we have to distinguish between light and dark plaquettes. In any case, in both cases the ground states correspond to encoded states, and there exists a gap that separates them from excited states. Moreover, no local operator can connect ground states. Only those operators with a topologically nontrivial support are able to distinguish among these protected states, something which makes this quantum memories remarkably robust against perturbations with a local nature.

IV. CONCLUSIONS

In this paper, we have made a presentation of surface codes [1] and color codes [18] on equal footing. This allows us to make a comparative study of their properties in more detail, such as the possible set of gates that they can implement transversally and the number k of encoded qubits (logical qubits).

We have also introduced the notion of the error-correcting rate $C := n/d^2$ as a means to evaluate the performance of topological 2D codes as far as the error-correction capability is concerned. We have computed this figure of merit for surface codes and color codes in the most representative and important topologies: the torus and the plane. In the torus, we find that the optimal value for surface codes is $C_s=1$, while for color codes we find $C_c=\frac{9}{8}$, which is are very close. For practical applications, planar codes are the most valuable

topologies. For them we find that the optimized values for surface codes are again $C_s=1$, but this time color codes yield a better value, $C_c=\frac{3}{4}$. Having in mind that the number of encoded logical qubits for color codes is always, i.e., in any topology, twice as much as for surface codes (8), this means that color codes demand a lower number of physical qubits for their construction.

Finally, we want to point out that it would be very interesting to perform additional comparative studies between Kitaev's codes and color codes regarding other performance properties like the percolation threshold, for instance.

ACKNOWLEDGMENTS

We acknowledge financial support from the EJ-GV (H.B.), a DGS grant under Contract No. BFM 2003-05316-C02-01 (M.A.M.D.), and a CAM-UCM Grant No. 910758.

[1] A. Yu. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (2003).
[2] P. Shor, Phys. Rev. A **52**, R2493 (1995).
[3] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[4] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[5] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).
[6] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **73**, 062303 (2006).
[7] H. Bombin and M. A. Martin-Delgado, J. Math. Phys. **48**, 052105 (2007).
[8] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **98**, 160502 (2007).
[9] R. Raussendorf, J. Harrington, and K. Goyal, e-print arXiv:quant-ph/0703143.
[10] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).
[11] X.-G. Wen and Q. Niu, Phys. Rev. B **41**, 9377 (1990).
[12] X.-G. Wen, Int. J. Mod. Phys. B **4**, 239 (1990).
[13] X.-G. Wen, *Quantum Field Theory of Many-body Systems* (Oxford University Press, Oxford, 2004).
[14] M. A. Levin and X.-G. Wen, Phys. Rev. B **71**, 045110 (2005).
[15] H. Bombin and M. A. Martin-Delgado, Phys. Rev. B **75**, 075103 (2007).
[16] X.-Y. Feng, G.-M. Zhang, and T. Xiang, Phys. Rev. Lett. **98**, 087204 (2007).
[17] A. Hamma and D. A. Lidar, e-print arXiv:quant-ph/0607145.
[18] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **97**, 180501 (2006).
[19] S. B. Bravyi and A. Yu. Kitaev, arXiv:quant-ph/9811052.
[20] A tetravalent lattice is a lattice with coordination number 4, i.e., each site has four nearest-neighbor sites.

Topological Computation without Braiding

H. Bombin and M. A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain
(Received 13 September 2006; published 19 April 2007)

We show that universal quantum computation can be performed within the ground state of a topologically ordered quantum system, which is a naturally protected quantum memory. In particular, we show how this can be achieved using brane-net condensates in 3-colexes. The universal set of gates is implemented without selective addressing of physical qubits and, being fully topologically protected, it does not rely on quasiparticle excitations or their braiding.

DOI: 10.1103/PhysRevLett.98.160502 PACS numbers: 03.67.Lx, 02.40.−k

Topological quantum computation offers the possibility of implementing a fault-tolerant quantum computer avoiding the extremely low threshold error rates found with the standard quantum circuit model [1–4]. Physical systems exhibiting a topological quantum ordered state [5,6] can be used as naturally protected quantum memories [1,7,8]. Characteristic properties of topologically ordered systems are the energy gap between ground state and excited states, topology-dependent ground state degeneracies, braiding statistics of quasiparticles, edge states, etc. [6]. The idea is then to place the information in the topologically degenerate ground state of such a system, so that the protection of the encoded information comes from the gap and the fact that local perturbations cannot couple ground states. In fact, the probability of tunneling between orthogonal ground states is exponentially suppressed by the system size and vanishes in the thermodynamic limit.

A stabilizer code [9,10] can be topological. The best known example are Kitaev's surface codes [1,7]. In general a code is topological if its stabilizer has local generators and nondetectable errors are topologically nontrivial (in the particular space where the qubits are to be placed). Given such a code, one can always construct a local Hamiltonian such that the resulting system is topologically ordered and the error correcting code corresponds to the ground state. An explicit example of this Hamiltonian construction is given later in Eq. (3). Errors in the code amount to excitations.

Although the storage of quantum information is interesting by itself, one would like to perform computations on it. A natural approach in this context is that of considering a topological stabilizer code in which certain operators can be implemented transversally, which avoids error propagation within codes. In terms of the corresponding topologically ordered system, this means that operations are implemented without selective addressing of the physical subsystems that make up each memory. This is important for physical applications.

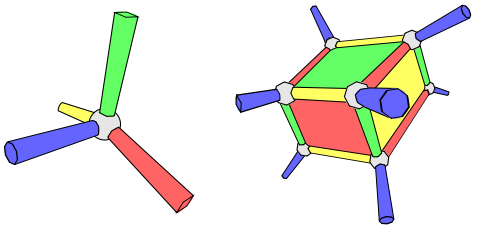
Unfortunately, surface codes only allow the transversal implementation of the CNOT gate. Then the problem arises of whether there exists a topological stabilizer code in which a universal set of gates can be performed transversally. In fact, even at the level of general codes it is a difficult task to find such codes [11]. For most codes, additional tricks such as the generation of large cat states are unavoidable. However, quantum Reed-Muller codes [12] have the very special property of allowing the transversal implementation of the gates:

$$K^{1/2} = \begin{pmatrix} 1 & 0 \\ 0 & i^{1/2} \end{pmatrix}, \qquad \Lambda = \begin{pmatrix} I_2 & 0 \\ 0 & X \end{pmatrix}, \tag{1}$$

where X is the usual σ_1 Pauli matrix. Complemented with the ability to initialize eigenstates of X and Z and to measure these operators, these gates are enough to perform arbitrary computations. In particular, the Hadamard gate can be reconstructed and the set of gates $\{H, K^{1/2}, \Lambda\}$ is known to be universal [13].

In this Letter we will construct a 3-dimensional system showing topological quantum order in which the gates (1) can be implemented. The ground state of the system is a topological stabilizer code. No other topological code of any dimension is known such that the transversal implementation of a universal set of gates is possible. In fact, a key ingredient in our approach is the appearance of membranes [14]. Our system is a 3-dimensional lattice with qubits located at the sites, and the operations on the ground state are implemented without any selective addressing of these physical qubits. This is in contrast with the current approach to topological computation which relies on the topological properties of quasiparticle excitations instead of ground states properties and needs a selective braiding of quasiparticles to produce quantum gates. In fact our system is Abelian, in the sense that monodromy operations on excitations can give rise only to global phases. In contrast, in the context of quasiparticle braiding Abelian systems can never give universal computation. Therefore, our results enlarge the range of applicability of the topological approach to quantum computation [15].

To achieve this goal, we start with a brief description of the topologically ordered 3-dimensional condensed matter systems [16] that we need for our construction. Consider a lattice with coordination number 4 in which links are colored with four colors as in Fig. 1(a). Color is introduced as a bookkeeping tool to keep track of the different sites,



(a) (b)

FIG. 1 (color online). (clockwise and lightest to darkest: yellow, green, red, blue) (a) A generic site in a 3-colex. (b) The neighborhood of a particular b cell: faces are colored according to the color of their visible side (they are br, bg, and by faces).

links, faces, and cells in the 3D lattice. We will use red, green, blue, and yellow labels (r, g, b, y) as colors. Assume that the cells can also be colored, in such a way that, for example, the boundary links of a red cell is a net with coordination number 3 formed by green, blue, and yellow links, as in Fig. 1(b). We call those 3D lattices with this set of properties 3-colexes. For any color q, q links connect q cells. A face lying between an r and a y cell has a boundary link made up of g and b links. We call such a face an ry face.

At each site of the lattice we place a qubit. We will be considering operators of the form

$$B_S^\sigma := \bigotimes_{i=1}^{n} \sigma^{f_i}, \qquad \sigma = X, Z, \qquad f_i = \begin{cases} 0 & i \notin S, \\ 1 & i \in S, \end{cases} \tag{2}$$

where S is a given set of qubits in the system, n the total number of qubits. The Hamiltonian proposed in [16] is

$$H = -\sum_{c \in C} B_c^X - \sum_{f \in F} B_f^Z, \tag{3}$$

where C and F are the cells and faces of the lattice, respectively. It gives rise to topological order. In particular, the degeneracy of the ground state is 2^k with $k = 3h_1$, where h_1 is the number of independent cycles of the 3-manifold in which the lattice is built. In particular, in a 3-sphere $h_1 = 0$ and there is no degeneracy at all, whereas in a 3-torus $h_1 = 3$. In topology, h_1 is known as a Betti number [17].

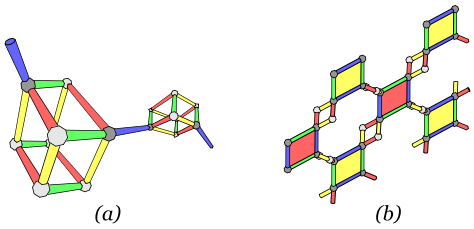
The ground states $|\psi\rangle$ of (3) are characterized by the conditions

$$\forall\ c \in C \qquad B_c^X|\psi\rangle = |\psi\rangle, \tag{4}$$

$$\forall\ f \in F \qquad B_f^Z|\psi\rangle = |\psi\rangle. \tag{5}$$

In fact, cell and face operators commute, and the ground state is a stabilizer quantum error correcting code [1,9,18]. Those eigenstates $|\psi'\rangle$ for which any of the conditions (4) and (5) are violated are excited states or, in code terms, erroneous states.

Both excitations and degeneracy are best understood introducing string and membrane operators. A q string, for some color $q \in \{\text{r, g, b, y}\}$, is a collection of q links, as in Fig. 2(a). Strings can have end points, which are always



(a) (b)

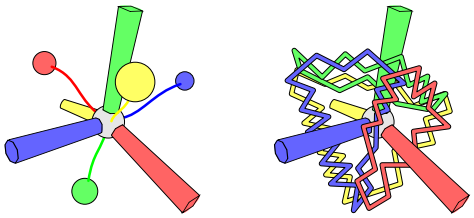
FIG. 2 (color online). (a) A b string consists of several b links that connect b cells. (b) An ry membrane is made up of ry faces linked by bg faces. bg faces are not shown here, only their links.

located at q cells. Along with every q string s we introduce the string operator B_s^Z. If $|\psi\rangle$ is a ground state, then $B_s^Z|\psi\rangle$ is, in general, an excited state, with excitations or quasiparticles at those q cells that are end points of s. If s is closed, that is, if it has no end points, B_s^Z commutes with the Hamiltonian (3).

Similarly, a collection of pq faces, for any colors p and q, is a pq membrane, as in Fig. 2(b). For any pq membrane m the corresponding membrane operator is B_m^X. If $|\psi\rangle$ is a ground state and m an rg membrane, for example, then $B_m^X|\psi\rangle$ is in general an excited state, with excitations at those by faces that form the border of m. These excitations are closed fluxes crossing the excited faces. As an example, consider an ry membrane such as the one in Fig. 2(b). Its border will create an ry flux, which will cross those bg faces at the border of the membrane. If m is closed, that is if it has no borders, then B_m^X commutes with the Hamiltonian (3).

As long as we consider closed manifolds in 3D, closed strings and membranes are enough to form a basis from which any operator that leaves the ground state invariant can be constructed. There are three key points here. First, any two string or membrane operators which are equal up to a deformation have the same action on the ground state, which is in itself a uniform superposition generated by all the possible local deformations. Second, a q-string operator B_s^Z and a pq-membrane operator B_m^X anticommute if and only if s crosses m an odd number of times. Otherwise, they commute and the same is true if they do not share any color. Third, not all colors are independent. For example, the combination of an r, a g, and a b string gives a y string. In fact , there are exactly 3 independent colors for strings and 3 independent color combinations for membranes. Therefore, all that matters about strings and membranes is their color and topology, and the appearance of the number 3 in the degeneracy is directly related to the number of independent colors.

On the other hand, strings and membranes with a single color are not enough to describe excitations. In general, strings can form a net with branch points at which four strings meet, one for each color [see Figs. 3(a) and 4(b)] Likewise, membranes can form nets in which, for example, a gb, a br, and an rg membrane meet along a line [see Fig. 4(c)]. In order to study the exact properties of general excitations, one can consider the elementary excitations

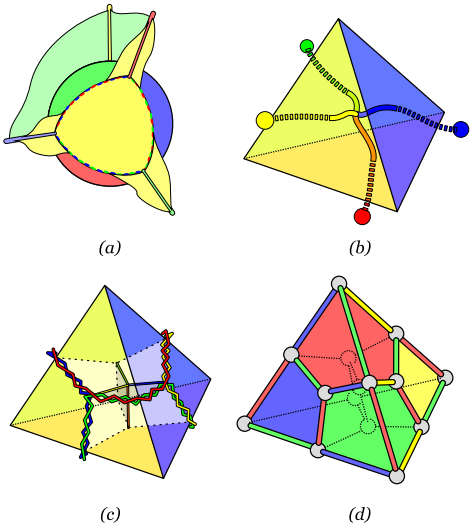


(a) (b)

FIG. 3 (color online). (a) The Z operator of a site creates one quasiparticle at each of the cells that meet at the site. (b) The X operator of a site creates the flux structure shown, which corresponds to a flux excitation at each of the faces meeting at the site.

attached to the operators X and Z at any particular site i of the lattice. Let $|\psi\rangle$ be a ground state. Then the state $Z_i|\psi\rangle$ is an excited state with four quasiparticles; see Fig. 3(a). The state $X_i|\psi\rangle$ is an excited state with six elementary fluxes which can be arranged in four single color closed fluxes, as in Fig. 3(b). From this class of elementary excitations one can build any general excitation.

If we restrict ourselves to closed manifolds, there is no way in which we can have a ground state with twofold degeneracy, or equivalently, that encodes a single qubit. However, we will now explain how one can obtain such a system by puncturing a 3-manifold. In particular, consider any 3-colex in a 3-sphere. The ground state in this case is nondegenerate. Now we choose any site in the lattice and remove it. Moreover, we also remove the four links, six faces, and four cells that meet at the site. As a result, we obtain a lattice with the topology of a solid 2-sphere; see Fig. 4(a). In order to calculate the degeneracy of the new system, we note that we have removed one physical qubit and two independent generators [16] of the stabilizer. This is so because (i) although we remove 4 cells, three of the cell operators can be obtained from the remaining one and the rest of cell operators (see [16]), and (ii) although we remove 6 faces, 5 of the face operators can be obtained from the remaining one and the rest of face operators in the corresponding cells. Then, from the theory of stabilizer codes it readily follows that the new code encodes one qubit. This can also be understood using strings and membranes. The surface of the system is divided into four faces, each of them being the boundary with one of the removed cells. Thus, we can color these areas with each color of the faces from the removed cells, as in Fig. 4(a). It is natural to deform this sphere into a tetrahedron, and we will do so. Then each of its faces can be the end point of a string of the same color, and thus there is a single independent nontrivial configuration for a string-net, as depicted in Fig. 4(b). This configuration, of course, corresponds to a string-net operator that creates one quasiparticle excitation at each missing cell. In a similar fashion, one can consider a net of membranes that creates the flux configuration shown in Fig. 4(c). This net consists of six membranes, meeting in groups of three at four lines that



(a) (b) (c) (d)

FIG. 4 (color online). (a) Here we represent the 3-sphere as $\mathbf{R}^3$ plus the point at infinity where we place the site to be removed. The faces and links perpendicular to the colored sphere are partially displayed but they continue to infinity. These faces and links must be removed as well. After their removal, we get a solid 2-sphere with a surface divided in four triangular areas. This colored sphere represents the remaining 3-colex itself. Then it can be reshaped to get a tetrahedron. (b) A nontrivial string-net in the tetrahedron. Its end points lie on the missing cells. (c) A nontrivial membrane-net configuration in the tetrahedron. Its borders create fluxes that cross the missing faces. Branching lines have been suitably colored. (d) The simplest tetrahedral lattice. Here colors have been given both to links and to cells. In the language of error correction, it is a $[[15, 1, 5]]$ code, that is, it encodes a qubit in 15 physical qubits, whereas its distance is 5 and so corrects up to 2 errors.

meet at a central point. Observe that these excitations are in exact correspondence with those in Fig. 3, when we see them from the point of view of the removed site.

Although these string-net and membrane-net operators just discussed can be used to introduce an operator basis for the encoded qubit, this can be done in an alternative way that is more convenient for practical implementations. Given any operator O that acts on a single qubit, we will use the notation $\hat{O} := O^{\otimes n}$ for the operator that applies O to each of the n physical qubits in the 3D lattice. Then, in any tetrahedral lattice we have $\{\hat{X}, \hat{Z}\} = 0$, because the total number of sites is odd: every 3-colex has an even number of sites and we have removed one [see Fig. 4(d) for $n = 15$]. Since both $\hat{X}$ and $\hat{Z}$ commute with the Hamiltonian (4), they can be considered the X and Z Pauli operators on the protected qubit. As usual, let $|0\rangle$ and $|1\rangle$ be a positive and a negative eigenvector of Z, respectively, so that they form an orthogonal basis for the qubit state space. Let also $|\mathbf{v}\rangle := |v_1\rangle \otimes \cdots \otimes |v_n\rangle$ be a vector state for any binary vector $\mathbf{v} \in \mathbf{Z}_2^n$, $\mathbf{Z}_2 = \{0, 1\}$. These binary vectors are usually introduced in error correcting codes [10]. A basis for the protected qubit can be constructed as follows:

$$|\hat{0}\rangle := \prod_c (1 + B_c^X)|\mathbf{0}\rangle = \sum_{\mathbf{v}\in V} |\mathbf{v}\rangle, \tag{6}$$

$$|\hat{1}\rangle := \prod_c (1 + B_c^X)|\mathbf{1}\rangle = \hat{X}|\hat{0}\rangle = \sum_{\mathbf{v}\in V} |\bar{\mathbf{v}}\rangle, \tag{7}$$

where $\mathbf{0} := (0 \cdots 0)$, $\mathbf{1} := (1 \cdots 1)$, $\bar{\mathbf{v}} := \mathbf{1} + \mathbf{v}$, c runs over all cells in the lattice, and V is the subspace spanned by vectors $\mathbf{v}_c$ such that $|\mathbf{v}_c\rangle = B_c^X|\mathbf{0}\rangle$. In order to be able to apply the $K^{1/2}$ gate to the protected qubit in the tetrahedral lattice, we must introduce a new requirement. We impose that faces (cells) must have a number of sites which is a multiple of four (eight). The simplest example of such a tetrahedral lattice is displayed in Fig. 4(d). As we will show below, it follows from these conditions that

$$\forall\ \mathbf{v} \in V \quad \mathrm{wt}(\mathbf{v}) \equiv 0 \mod 8, \tag{8}$$

where the weight of a vector $\mathrm{wt}(\mathbf{v})$ is the number of 1's it contains. But then we have

$$\hat{K}^{1/2}|\hat{0}\rangle = |\hat{0}\rangle, \qquad \hat{K}^{1/2}|\hat{1}\rangle = i^{l/2}|\hat{1}\rangle, \tag{9}$$

where $l \equiv n \mod 8$, $l \in \{1, 3, 5, 7\}$. This means that the global $\hat{K}^{1/2}$ operator can be used to implement $K^{1/2}$ on the encoded qubit, by repeated application in the case that $l \neq 1$.

We still have to prove (8). Let the weight of a Pauli operator be the number of sites on which it acts nontrivially, and let us work modulo 8. Then (8) says that for any product $\pi = B_{c_1}^X \cdots B_{c_m}^X$, $\mathrm{wt}(\pi) \equiv 0$. This follows by induction on m. The case $m = 0$ is trivial. For the induction step, we first observe that if $\mathrm{wt}(\pi) \equiv 0$, then $\mathrm{wt}(\pi B_c^X) \equiv 0$ if and only if π and B_c^X share s sites with $s \equiv 0, 4$. But if $f_1, \ldots, f_j$ are those faces of c shared with some cell of π, then $s = \mathrm{wt}(B_{f_1}^Z \cdots B_{f_j}^Z)$. These faces are part of the 2D color lattice that forms the boundary of the cell c, from which it follows that $s \equiv 0, 4$ [19].

The Λ gate (1), known as the CNOT gate, is more straightforward. Imagine that we take two identical tetrahedral lattices and superpose them so that corresponding sites get very near. Then we apply $\hat{\Lambda}$, that is, we apply Λ pairwise. This can be achieved through single qubit operations and Ising interactions. As a result, it is easily checked that we get a Λ gate between the protected qubits.

As for measurements, the situation is the same as in any CSS code [20,21]. If we measure each physical qubit in the Z basis, then we are also performing a destructive measurement in the $\hat{Z}$ basis. Then nondestructive measurements of $\hat{Z}$ can be carried out performing a CNOT gate with the qubit to be measured as source and a $|\hat{0}\rangle$ state as target, and measuring the target destructively. Similarly, if we measure each physical qubit in the X basis we are performing a measurement in the $\hat{X}$ basis. We can admit faulty measurements, since the faulty measurement of a qubit is equivalent to an error prior to it. Thus the measuring process is as robust as the code itself and is topologically protected [7]. The results of the measurements must be classically processed to remove errors and recover the most probable code word.

Initialization is always a subtle issue in quantum computation, whether topological or not, and it certainly depends upon the physical implementation. In any case, even if perfectly pure $|\hat{0}\rangle$ or $|\hat{+}\rangle$ states cannot be provided, one can still purify them as much as necessary if their fidelity is above $\frac{1}{2}$. To do this, only the CNOT gate $\hat{\Lambda}$ and measurements in the $\hat{Z}$ and $\hat{X}$ bases are necessary.

As a concluding remark, we observe that the lattice that we have described so far unifies the strategies used in fault-tolerant computation, such as transversal operations, with the concept of a topologically protected quantum memory. Note that this approach is very different from the usual one in topological quantum computation, based on the braiding of non-Abelian anyons in a two-dimensional system. In fact, the topological order of the 3-dimensional system that we have described is Abelian.

We acknowledge support from EJ-GV (H. B.), DGS grant under Contract No. BFM 2003-05316-C02-01 and EU Project INSTANS (M. A. M-D.), and CAM-UCM Grant under reference 910758.

[1] A. Yu. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (2003).
[2] M. H. Freedman, Proc. Natl. Acad. Sci. U.S.A. **95**, 98 (1998).
[3] M. H. Freedman, A. Kitaev, M. J. Larsen, and Z. Wang, Bull. Am. Math. Soc. **40**, 31 (2003).
[4] J. Preskill, http://www.theory.caltech.edu/~preskill/ph219/topological.ps.
[5] X.-G. Wen and Q. Niu, Phys. Rev. B **41**, 9377 (1990).
[6] X.-G. Wen, *Quantum Field Theory of Many-Body Systems* (Oxford University, New York, 2004).
[7] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. (N.Y.) **43**, 4452 (2002).
[8] S. B. Bravyi and A. Yu. Kitaev, quant-ph/9811052.
[9] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[10] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405, (1997).
[11] E. Knill, R. Laflamme, and W. Zurek, quant-ph/9610011.
[12] E. Knill, R. Laflamme, and W. Zurek, quant-ph/9610011.
[13] P. O. Boykin *et al.*, Inf. Proc. Lett. **75**, 101 (2000); quant-ph/9906054.
[14] A. Hamma, P. Zanardi, and X.-G. Wen, Phys. Rev. B **72**, 035307 (2005).
[15] M. Freedman, M. Larsen, and Z. Wang, Commun. Math. Phys. **227**, 605 (2002).
[16] H. Bombin and M. A. Martin-Delgado, Phys. Rev. B **75**, 075103 (2007).
[17] M. Nakahara, *Geometry, Topology and Physics* (IOP, London, 2003).
[18] A. R. Calderbank *et al.*, Phys. Rev. Lett. **78**, 405 (1997).
[19] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **97**, 180501 (2006).
[20] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[21] A. M. Steane, Proc. R. Soc. A **452**, 2551 (1996).

Quantum Measurements and Gates by Code Deformation

H. Bombin and M.A. Martin-Delgado

Departamento de Física Teórica I, Universidad Complutense, 28040. Madrid, Spain.

The usual scenario in fault tolerant quantum computation involves certain amount of qubits encoded in each code block, transversal operations between them and destructive measurements of ancillary code blocks. We propose to complement this techniques with code deformation, in which a given code is progressively changed in such a way that encoded qubits can be created, manipulated and non-destructively measured. We apply this approach to surface codes, where the computation is performed in a single code layer which is deformed using 'cut and paste' operations. All the interactions between qubits remain purely local in a two-dimensional setting.

I. INTRODUCTION

Quantum computing is the art of controlling quantum coherence at will. It is no surprise then that the main obstacle towards this enormous achievement is the decoherence that any real-life quantum system will suffer unavoidably. The quest to overcome this difficulty, first believed to be insurmountable, led to the creation of quantum error correcting codes [1], [2]. These codes revolve around the idea of storing a small amount of quantum information in a large number of quantum degrees of freedom, so that the redundancy makes the information more resilient to errors. Among the most fruitful ones are stabilizer quantum error correcting codes [3], [4], which are particularly easy to analyze. Some of them even allow to implement interesting sets of gates transversally, that is, in such a way that localized errors do not spread uncontrolledly over the code block.

Transversal gates have proved themselves very useful, but sometimes they are not enough. In this paper we consider the concept of code deformation, which enlarges the amount of fault tolerant gates naturally implementable in a given code. The idea is that a quantum error correcting code can be slightly changed to give a new one, and that such changes can be applied one after the other to produce quantum gates on encoded qubits. The amount of encoded qubits can change due to deformations, giving rise to initialization and measurement operations. As we will see such ideas are natural in the context of topological codes, but they could be applied in other kinds of quantum error correcting codes.

An important practical problem regarding many theoretical proposals involving quantum error correction and fault tolerant computation is the non-locality of the elementary gates between the physical qubits that make up the codes. In some practical devices, elementary gates have a local nature, a severe restriction when errors are to be taken into account. Here dimensionality is another important issue, since it is not the same thing to have local gates in a 1D, 2D or 3D system.

Surface codes, introduced by Kitaev [5], are stabilizer codes with the interesting feature of being local in a 2D setup. In particular, the qubits can be arranged in a 2D lattice in such a way that the necessary measurements to control the errors only involve as few as four neighboring qubits. Then one can envision a quantum computer as a stack of layers. Each layer is a surface code encoding a single qubit, and CNot gates are performed transversally in pairs of layers. The problem with surface codes is that no other gate can be transversally

implemented. To overcome this difficulty color codes were developed [6], which are also local in 2D, but allow the transversal implementation of the whole Clifford group, which is enough for quantum distillation and many other quantum information tasks, such as quantum teleportation. Extensions of color codes to 3D with nice transversal properties for universal quantum computation are also possible [7].

However, working with a 2D setup is a rather typical scenario in technological applications such as lithographic techniques and the like. In that case, the above setting with several stacks of planar codes becomes useless. Then one can wonder wether it is possible to implement non-trivial gates by means of some different scheme. In this paper we answer this question in the positive. In particular, we show how non-destructive measurements and CNot gates can be obtained by deforming a single-layered surface code. This is in sharp contrast with the standard approach to surface codes.

The idea of inserting and removing physical qubits from a surface code was introduced in [8] as a way to correct transversal Hadamard gates. This insertion an removal gives rise to a progressive reshaping of the lattice or, what is the same, a deformation of the code. We want to stress that indeed there is a fixed underlying lattice of qubits. When we say that a site is added to or removed from the surface code, we do not mean a change in the underlying physical system but just on the stabilizers that define our code. In a sense, what we are reshaping is a 'software' lattice, whereas the underlying 'hardware' lattice remains intact.

Similar ideas have already been discussed in the context of cluster states [9]. Our approach differs in several aspects. First, our discussion is based solely on the properties of 2D topological codes with no additional structure, which makes it clearer. It is natural for us to consider not only surfaces with holes, but really any kind of topologies, including those in which two types of boundaries appear next to each other. The way in which we propose to perform deformations fits naturally in the error correction scheme discussed in [8], and we show how the gates discussed in that work can be applied in our context. Moreover, we discuss code deformation in such a way that it can be inmediately applied to other codes, for example those in [6], [7].

II. CODE DEFORMATION

An error correcting code is a subspace of the space of states of a given quantum system. The error correcting capabilities are related to the fact that certain operators or errors, those that the code can detect, do not connect orthogonal encoded states. We want to consider small changes that progressively deform one stabilizer code into another. The motivation is that such deformations can be used to initialize, transform and measure encoded qubits.

A. Stabilizer codes

Given a certain number of qubits, its group of Pauli operators $\mathcal{P}$ is defined as that generated by tensor products of the usual X and Z single-qubit Pauli operators. For example, if we have five qubits, a generator would be $X \otimes 1 \otimes Y \otimes Z \otimes X$. A stabilizer code [3], [4] of length n is a subspace of the quantum system of n qubits. It is described as the subspace $\mathcal{C}$ stabilized by an Abelian subgroup $\mathcal{S} \subset \mathcal{P}$. The stabilizer group $\mathcal{S}$ must not contain -1 as an element, and if it has $n-k$ independent generators S_i, the encoded subspace $\mathcal{C}$ has dimension 2^k and thus we say that it encodes k qubits. The encoded states $|\psi\rangle \in \mathcal{C}$ are characterized by the conditions $S_i|\psi\rangle = |\psi\rangle$, $i = 1, \ldots, n-k$.

An important tool in the understanding of stabilizer codes is the normalizer $\mathcal{N}$ of $\mathcal{S}$. This is the subgroup of Pauli operators that commute with all the elements of $\mathcal{S}$. Define the weight of a Pauli operator as the number of non-trivial terms in its tensor product expression. Then, the minimum of the weights of the elements of $\mathcal{N} - \mathcal{S}$ gives the so called distance of the code. This is the minimun number of qubits that we have to manipulate in order to change one encoded state into another. Thus, the bigger this distance, the bigger the noise resilience of the code. From the normalizer one can always choose elements X_i, Z_i, $i = 1, \ldots, k$ such that

$$[X_i, X_j] = 0, \qquad [Z_i, Z_j] = 0, \qquad X_i Z_j = (-1)^{\delta_{i,j}} X_j Z_i. \tag{1}$$

These generate the group of encoded Pauli operators, that is, the Pauli operators of the encoded qubits.

B. Code transformations

Consider two codes $\mathcal{C}$, $\mathcal{C}'$ with stabilizers $\mathcal{S}$, $\mathcal{S}'$, both with the same number of physical qubits n and encoded qubits k. Let us denote the generators of the stabilizers as S_i, S'_i, and the elements of the basis of encoded Pauli operators as X_i, Z_i and X'_i, Z'_i, respectively. The Clifford group [10] consists of those unitary operators U in our system of n qubits such that for any element $T \in \mathcal{P}$ we have $U^\dagger T U \in \mathcal{P}$. Consider the subset of Clifford operators U with $U^\dagger \mathcal{S} U = \mathcal{S}'$, that is, those that transform $\mathcal{C}$ into $\mathcal{C}'$. Such operators are very general. For example, they include transversal operations [11], [3], in which $\mathcal{C}' = \mathcal{C}$ and $\mathcal{U} = u^{\otimes n}$ with u some unitary single-qubit operator. Transversal operations have a great importance in fault-tolerant quantum computation [12], [13], but it is interesting to look for alternatives that can widen the applicability of fault-tolerant codes. Here we explore the idea of code deformations, in which only some of the generators of the stabilizer change. Then, if r of them change we can write $S'_i = U^\dagger S_i U = S_i$ for $i = r+1, \ldots, n-k$. If this r is somehow small, it makes sense to talk about code deformations. We will see how in surface codes deformations have indeed a geometrical meaning, because they take the form of localized changes in the shape of a given surface. Because these changes do not alter the topology of the surfaces, we call them smooth deformations.

When $\mathcal{C} = \mathcal{C}'$, we have

$$U^\dagger X_i U \sim_{\mathcal{S}} \prod_j X_j^{a_{ij}} Z_j^{b_{ij}}, \qquad U^\dagger Z_i U \sim_{\mathcal{S}} \prod_j X_j^{c_{ij}} Z_j^{d_{ij}}, \tag{2}$$

where $a_{ij}, b_{ij}, c_{ij}, d_{ij} \in \mathbf{Z}_2$ and $A \sim_{\mathcal{S}} B$ if $A = BS$ for some $S \in \mathcal{S}$. The evolution of the encoded Pauli operators (2) determines, up to a phase, the unitary evolution of the encoded qubits under U. In the case of code deformations, which change the code only partially, we can successively apply several operators U_i so that $U = U_t \ldots U_1$ takes the code into itself. Thus, we can use deformations to perform Clifford gates, as we will see in particular in surface codes.

We have said that both codes, the initial and the final, have the same number of physical qubits. However, it should be noted that we can use the previous description also in a case in which the numbers differ. This is so because we can always enlarge any code with additional qubits. We simply add one stabilizer generator per new qubit, each one, for example, a Z on the corresponding qubit. This way, extra qubits are in a fixed state for encoded states

and thus do not affect the code.

Indeed, it was the need to enlarge an existing code qubit by qubit which motivated the introduction of code deformations in [8] for surface codes. In the mentioned work the operator U, which amounts to several local CNot gates, is applied explicitly to the code in order to deform it. Alternatively, one can perform the deformation by measuring the new stabilizers S_i', $i = 1, \ldots, r$. Some of the measurements can give an undesired value, so that the obtained code has stabilizers $m_i S_i$ with $m_i = \pm 1$. This could then be corrected applying a suitable Pauli operator, as we will see in specific examples. In practice, however, this correction is unnecessary, at least when error correction reduces to monitor errors in the system, as in [8]. In that case, one performs round after round of measurements. In each round, all the generators S_i are measured. These measurements are used to calculate with high confidence which errors occurred. When some measurement is done on encoded qubits, it must be interpreted taking these errors into account, which are never really corrected in any other way. Performing deformations by measuring the stabilizers fits nicely in this error correction scheme, because we can change the stabilizers to be measured from one round to another in order to get the desired deformations. However, for this deformation procedure to work it must be possible to correct errors successfully with high probability. In other case, one has to apply directly a suitable unitary operator. In the case of surface codes, deformations can be done through measurements as long as we keep them local when compared to the support of encoded Pauli operators, except for encoded operators which are being initialized or measured, as we discuss in the next section.

C. Initialization and measurement

The code transformations discussed in the previous section cannot change the number of encoded qubits. They can be done without introducing stabilizer violations, simply by implementing U suitably. But we can consider more general Clifford operators U, in particular such that the initial code $\mathcal{C}$ and the final code $\mathcal{C}'$ have a different number of encoded qubits. The condition $U^\dagger \mathcal{S} U = \mathcal{S}'$ can no longer be imposed. In the case of deformations in surface codes, as will see, these correspond to changes in the topology of the surface, and thus we call them non-smooth deformations.

Suppose first that $\mathcal{C}$ encodes k qubits and $\mathcal{C}'$ encodes $k+1$ qubits. Then $\mathcal{C}'$ has one

stabilizer generator less. We consider those Clifford operators U with $\mathcal{S}' \subsetneq U^\dagger \mathcal{S} U$, that is, those which transform encoded states into encoded states. Then $U^\dagger \mathcal{S} U$ is a subset of $\mathcal{N}'$ generated by $\{S_i\}_{i=1}^{n-k} \cup \{T\}$ where T is a nontrivial encoded Pauli operator, $T \in \mathcal{N}' - \mathcal{S}'$. This T has eigenvalue one after U has been applied. Thus, U not only adds one qubit but also initializes it in a definite way. We can consider in a similar way the introduction of several new qubits and their initialization. In the particular case of surface code deformations, such operators U will introduce changes in the topology which increase the number of nontrivial cycles.

Now consider the reverse case, so that $\mathcal{C}$ encodes k qubits and $\mathcal{C}'$ encodes $k-1$ qubits. Then $\mathcal{C}'$ has one stabilizer generator more. We consider those Clifford operators U with $U^\dagger \mathcal{S} U \subsetneq \mathcal{S}'$, that is, those which are inverses of the transformations just considered. Then $U \mathcal{S}' U^\dagger$ is a subset of $\mathcal{N}$ generated by $\{S_i\}_{i=1}^{n-k} \cup \{T\}$ where T is a nontrivial encoded Pauli operator, $T \in \mathcal{N} - \mathcal{S}$. This T is mapped onto an element of $\mathcal{S}'$ through U, and in this sense gets measured. Thus, U removes one qubit and the corresponding degrees of freedom map onto possible violations of the stabilizer in the new code. Again, we can consider the removal and measurement of several qubits at the same time. For surface codes, such operators U will introduce changes in the topology which decrease the number of nontrivial cycles.

III. SURFACE CODES

In order to construct surface codes one starts considering any two-dimensional lattice in which four links meet at each site and plaquettes can be two-colored. For our purposes and to fix ideas, a 'chessboard' lattice in the plane will mostly suffice, see Fig. 1. This lattice will have borders, which can be best understood as big missing faces. Since there are two kinds of plaquettes, dark and light, borders have also this labeling. In the interface between a dark and a light border there are missing edges that would separate the missing plaquettes.

To construct the quantum error correcting code from the lattice, a physical qubit must be placed at each site. The stabilizer $\mathcal{S}$ is generated by plaquette operators. Given a plaquette p we define the plaquette operator X_p (Z_p) as the tensor product of X (Z) Pauli operators acting on those qubits lying on the plaquette. Then we attach X_p operators to dark plaquettes and Z_p operators to light plaquettes. All these operators commute due to the properties of the lattice, and thus the stabilizer is well defined.

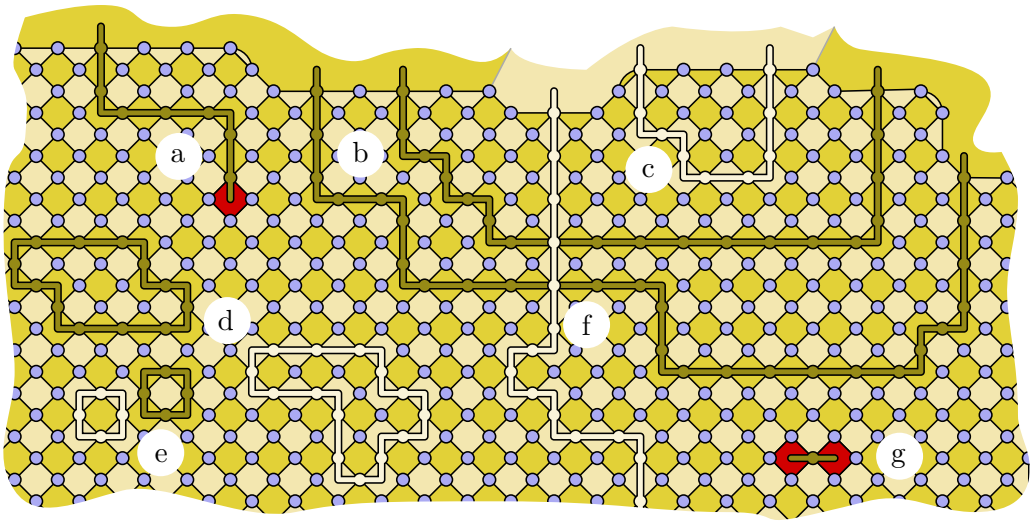


FIG. 1: A piece of a surface code with an irregular dark-light-dark border on the top part. There is a qubit at each site of the lattice. Dark (light) strings represent products of Z (X) operators. (e) Plaquette operators as strings. (c, d) Products of plaquette operators are boundary strings. (a, g) If a string operator has an endpoint at a plaquette, it will not commute with the plaquette operator. (b) If two strings operators are equal up to deformation, their action on encoded states is the same. (f) Crossing X and Z string operators anticommute.

Any operator which is just a tensor product of Z (X) operators acting on certain qubits can be visualized as a string that goes through the corresponding sites and lives on dark (light) plaquettes, see Fig. 1. So given a dark (light) strings s, i.e. a geometric object, we attach to it the operator Z_s (X_s). If a light (dark) plaquette p is considered as a small closed dark (light) string, this definition agrees with the previous one, see Fig. 1 (e). For a closed string we mean a string with no endpoints. Given a dark (light) string operator s and a dark (light) plaquette p, $[Z_s, X_p] = 0$ ($[X_s, Z_p] = 0$) iff p is not an endpoint of s, see Fig. 1(a,g). Thus, if s is dark (light) closed string then $Z_s \in \mathcal{N}$ ($X_s \in \mathcal{N}$). As borders are indeed missing plaquettes, a dark (light) string s with its endpoints at dark (light) borders should be considered a closed string because $Z_s \in \mathcal{N}$ ($X_s \in \mathcal{N}$). In terms of homology, the homology of dark (light) strings is a homology relative to dark (light) borders [14], [15].

The previous observations imply that closed string operators generate the normalizer $\mathcal{N}$ of the stabilizer $\mathcal{S}$. Moreover, $\mathcal{S}$ is generated by boundary string operators. A dark (light) boundary string is a string which encloses some portion of the surface, which can include

dark (light) borders but not light (dark) ones. Then the elements of $\mathcal{N}-\mathcal{S}$ take the form $X_s Z_{s'}$, with s, s' closed and at least one of them not a boundary. The elements of the basis of encoded Pauli operators, $X_i, Z_i \in \mathcal{N}-\mathcal{S}$, can be chosen graphically. To this end, two points must be taken into account. First, when two dark (light) strings s, s' of the same type differ only by a boundary, see Fig. 1(b), the corresponding operators are equivalent up to products with stabilizer elements, $Z_s \sim_{\mathcal{S}} Z_{s'}$ ($X_s \sim_{\mathcal{S}} X_{s'}$). When we say that s and s' differ only by a boundary we mean that they can be deformed one into the other or, more exactly, that they are equivalent up to $\mathbf{Z}_2$ homology, $s \sim_H s'$. Secondly, if s is a dark string and s' a light string, $\{X_s, Z_s\} = 0$ iff s and s' have an odd number of sites in common or, what is the same, they cross an odd number of times, see Fig. 1(f).

All this is best illustrated with an example. Consider the surface code depicted in Fig. 2(a). It encodes a single qubit. Let s be the dark string and s' the light one. These strings are closed but not boundaries, and any other homologycally non-trivial string is equivalent to one of them. The Pauli operator basis is given by $Z_1 = Z_s$ and $X_1 = X_{s'}$. The bigger the width and height of the rectangular surface are (in terms of qubits), the more resilient the code will be to Z and X errors, respectively.

IV. SURFACE CODE DEFORMATION

We are now in position to discuss deformations in surface codes. As we have already mentioned, these take the form of geometrical changes in the shape of the surface. As qubits enter and exit the code, the dark and light borders of the surface change. We can move the borders, glue them together or create new ones cutting the surface. Although we talk about introducing and removing qubits from the surface, there is a fixed underlying square lattice of physical qubits. We change the stabilizers that define the code, not the physical system.

The basic mechanism is exemplified in Fig. 2(b), where a qubit in a light border is erased, causing the removal of a light plaquette operator and the change of two dark plaquette operators. To perform the deformation of the code, the new two-sited plaquette operators must be measured. In the absence of errors, their eigenvalues must agree. If they are negative, we can apply Z operators on those qubits marked in red. In practice, errors may appear and we just perform the measurements, which will then be interpreted at the error correction stage [8]. If the inverse deformation of that of Fig. 2(b) is performed, corrections

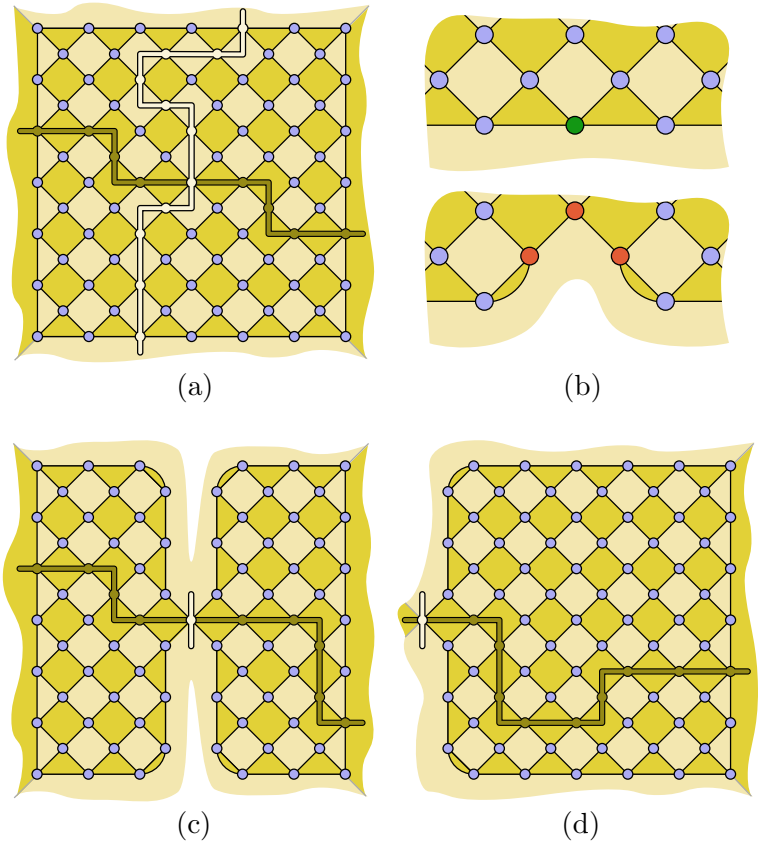
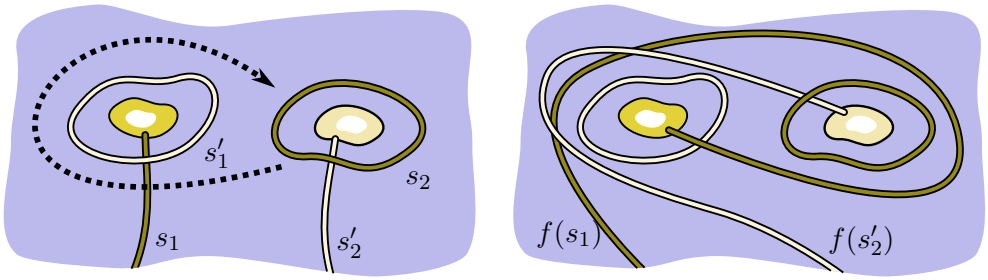


FIG. 2: (a) A surface code with a dark-light-dark-light border structure. It encodes a single qubit. Nontrivial strings that correspond to the encoded X and Z operators are displayed. (b) An elementary deformation. In case that after the removal of the green qubit the new two-sited plaquette operators have negative eigenvalue, Z operators are applied at red qubits. (c) The previous code after being deformed so that the encoded X becomes exposed to local measurements. (d) A dark border was reduced to expose the encoded X.

have to be made on the qubit marked in green.

A. Smooth deformations

First we want to consider smooth deformations, in which the topology of the surface is not altered. Such transformations cannot change the number of encoded qubits, but can perform unitary gates on them. So suppose that we deform a surface in an arbitrary way, taking it finally back to its original form. The total deformation gives a continuous mapping f of the original surface onto itself. In particular, this mapping takes strings s to $f(s)$.



(a) (b)

FIG. 3: A deformation that takes a light hole around a dark one gives rise to a CNot gate. (a) A piece of a surface code with a dark and a light hole and the nontrivial closed strings of interest. (b) After the deformation, two of the strings are mapped to different ones.

Recall that encoded Pauli operators can be chosen to be string operators. Moreover, we can find light strings s_i and dark strings s_i' so that $X_i := X_{s_i}$ and $Z_i := Z_{s_i'}$ satisfy (1). Then, if U is the Clifford operator that performs the desired deformation on the surface code, we have

$$U^\dagger X_i U = X_{f(s_i)} \sim_{\mathcal{S}} \prod_j X_j^{a_{ij}}, \qquad U^\dagger Z_i U = Z_{f(s_i')} \sim_{\mathcal{S}} \prod_j Z_j^{d_{ij}}, \tag{3}$$

where $a_{ij}, d_{ij} \in \mathbf{Z}_2$ and $f(s_i) \sim_H \sum a_{ij} s_j$, $f(s_i') \sim_H \sum d_{ij} s_j'$.The equations (3) give the evolution of encoded Pauli operators under U in terms of the continuous map f produced by the deformation related to U. It should be noted that (3) is very restrictive when compared to the general (2), so that many Clifford operations cannot be implemented using deformations. In particular, Hadamard gates H are out of reach because $H^\dagger X H = Z$ and deformations do not mix X and Z operators.

An example is displayed in Fig. 3, where the effect of moving a light hole around a dark one is analized. There are two encoded qubits involved in this operation. The deformation maps the strings s_1', s_2 to themselves and changes the strings s_1, s_2' giving $f(s_1) \sim_H s_1 + s_2$ and $f(s_2') \sim_H s_1' + s_2'$. Taking $X_i := X_{s_i}$ and $Z_i := Z_{s_i'}$, $i = 1, 2$, as the relevant encoded operators, the result of the deformation is

$$U^\dagger X_1 U \sim_{\mathcal{S}} X_1, \qquad U^\dagger Z_1 U \sim_{\mathcal{S}} Z_1 Z_2, \qquad U^\dagger X_2 U \sim_{\mathcal{S}} X_1 X_2, \qquad U^\dagger Z_2 U \sim_{\mathcal{S}} Z_2, \tag{4}$$

which corresponds to a CNot gate with the first qubit as source.

B. Non-smooth deformations

What happens when a surface code is drastically deformed? Let us return to the example code of Fig. 2(a) and deform it till there exists a nontrivial string of length one, see Fig. 2(c). Observe that at this point our code is absolutely exposed to X errors, but not to Z errors. The point then is that not only the environment can measure the encoded X_1, but *we also can*. Since Z errors are still unlikely, the measurement is protected by the code. Although the measurement seems local, in practice we have to take error correction into account. For now, we will just concentrate on the effects of deformations in the absence of errors, and leave the discussion of their correction for later. The deformation can be undone, with the net result that the encoded state has been projected. Thus, we have succeeded in performing a non-destructive quantum measurement by code deformation. Visually, the measurement amounts to temporarily shrink one of the dimensions of the surface. We could have also employed a similar procedure to measure in the border, as shown in Fig. 2(d). In this case one of the dark borders is contracted.

The procedures that we have just described involve only smooth deformations, because we did not change the topology of the surface. However, in Fig. 2(c,d) the removal of a single qubit would have changed the topology. Because of the topological nature of the codes and their error correction procedures, it is more natural to consider non-smooth deformations. For example, let $\mathcal{C}$ be the surface code of Fig. 2(c) and let q be the qubit that maintains both pieces of the surface connected. Suppose that we remove q to obtain a new surface code $\mathcal{C}'$. The dark square plaquettes that contained q in $\mathcal{C}$ are triangular after its removal. We call these new plaquettes p, p'. Because we want C' to include q, we need also an extra stabilizer to fix it. We choose X_q, the X Pauli operator on q. Removing q amounts to cut the surface, and $\mathcal{C}'$ encodes no qubits, so that we know that the deformation maps some encoded Pauli operator of the original code to a stabilizer of the new one. In fact, we can take $U = 1$ as the deformation operator. Let $|\psi\rangle \in \mathcal{C}$. Then, if $X_1|\psi\rangle = X_q|\psi\rangle = |\psi\rangle$, we have $|\psi\rangle \in \mathcal{C}'$. On the contrary, if $X_1|\psi\rangle = X_q|\psi\rangle = -|\psi\rangle$ then $|\psi\rangle \notin \mathcal{C}'$. In particular, $|\psi\rangle$ violates the stabilizer conditions for the generators X_q, X_p and $X_{p'}$. In this sense, in going from $\mathcal{C}$ to $\mathcal{C}'$ we are measuring X_1.

More generally, cutting a surface along a light string s that connects two different light borders amounts to measuring X_s. For cutting the surface along s we mean removing all

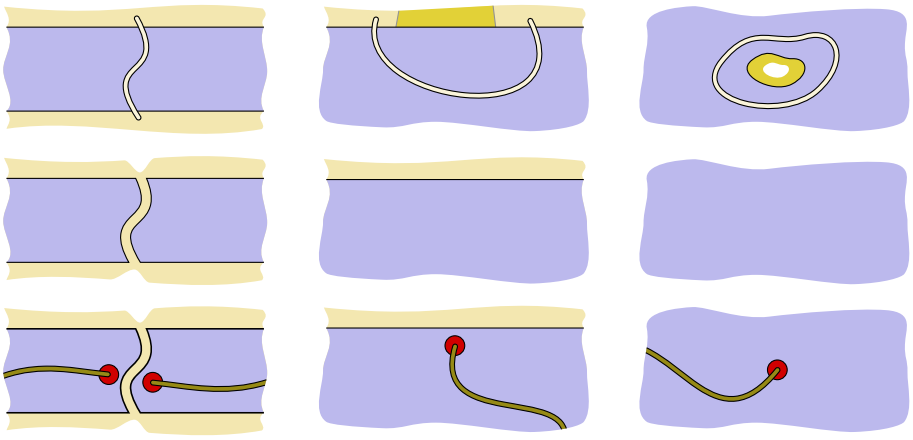


FIG. 4: The effect of non-smooth deformations. The pictures at the top part represent the initial situation. The X string operator to be measured is displayed as a light string. The two pictures below represent the situation afterwards, depending on the measurement outcome. The figures in the bottom correspond to the situation in which $X = -1$. The stabilizer violations appearing in this case correspond to nonlocal Z-strings, as displayed. These discontinuous deformations can be read off bottom-up, but in this case $X = 1$ necessarily. (a) A cut from border to border. (b) The contraction of a border. (c) The contraction of a hole.

the qubits along it, and we suppose that the operator U that performs the cut acts locally, in a neighborhood of the string. To check the previous statement, consider a light string s_d which is a slight deformation of s lying out of the support of U. Then $U^\dagger X_{s_d} U = X_{s_d}$ and $X_s \sim_{\mathcal{S}} X_{s_d}$. In addition, $X_{s_d} \in \mathcal{C}'$ because s_d is a boundary in the new surface. Moreover, if $|\psi\rangle$ is an eigenstate of the stabilizers of $\mathcal{S}'$, then $X_{s_d}|\psi\rangle = -|\psi\rangle$ iff the number of violations in dark plaquettes in an area with boundary s_d is odd. Thus, the cut maps the eigenvalue of X_s to the parity of the number of violations that appear at each side of the cut. In the case of cuts along dark strings s, the measured operator is of course Z_s. We can consider also inverse processes, using similar arguments: If we paste two borders of the lattice together, the new string operator that runs along the junction is left with definite eigenvalue 1. Other non-smooth deformations such as puncturing and border removal are summarized in Fig. 4.

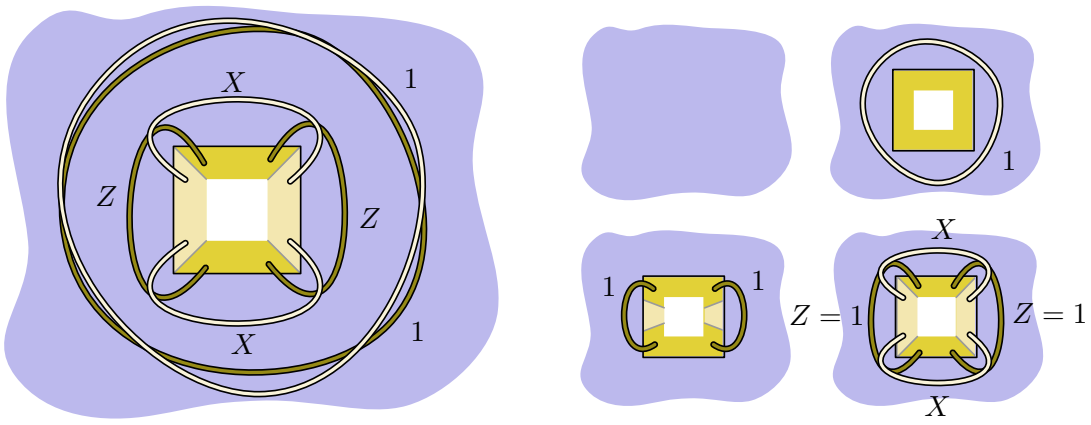
C. Error correction

Error correction in surface codes was analyzed in great detail in [8]. Thus, here we only intend to show how code deformation can be integrated into the picture given there, which we summarize now. First, error correction amounts really to keep track of errors as they show up. To this end, the local generators of the stabilizer are measured time after time. The results of each round of measurements gives a time slice, or indeed two, one for violations of X-type generators and one for violations of Z-type generators. For each type, the slices are arranged in a (2+1)-D fashion, where the extra dimension is time. Then, if violations at a given time are considered as particles, in the (2+1)-D picture we have their wordlines. In fact, from the measurements we do not get the actual wordlines. Rather, they have to be inferred, which can be done correctly with high probability using certain algorithm[8] as long as errors are below a threshold. For the procedure to succeed, the actual wordlines and the inferred ones must be homologically equivalent.

When deformations enter the picture, the error correction procedure that we have just described is left basically unchanged. When deformations involve a measurement, that is, the lost of an encoded qubit, the value of the measurement must be recovered taking into account the corrections. That is, the relevant stabilizer violations must be checked after errors have been canceled out. This is consistent with the fact that only the homology of the wordlines is relevant.

D. A particular implementation

There are many ways to encode qubits and to manipulate them through deformations in a surface code. Here we have chosen an implementation that is closely connected to the one in [8]. However, many other implementations could be given. For example, a disk with a dark external border and n dark holes encodes n qubits: X_i operators correspond to strings that enclose the holes and Z_i operators correspond to strings that connect holes to the external border.



(a) (b)

FIG. 5: (a) Each qubit is associated to a hole with a dark-light-dark-light border structure. Non-trivial operators are labeled with their value. (b) The deformation procedure to initialize a qubit in the state $|1\rangle$, as explained in the text.

1. Encoded qubits and initialization

Our starting point is a surface code with an arbitrary shape. As long as cut and paste operations are performed far enough from the borders, they are unimportant. The encoded qubits are holes in this surface, with the particular dark-light-dark-light border structure depicted in Fig. 5(a). We impose the condition that any string operator that surrounds such a hole must have eigenvalue 1, something that will be preserved by the gates proposed below. The encoded Z and X operators can be measured by shortening a suitable border. As for the initialization procedure for these encoded qubits in $|1\rangle$ ($|+\rangle$) states, it comprises two steps. First a dark (light) hole is created by puncturing the code. Then a pair of light (dark) borders are grown along the border of the hole. See Fig. 5(b) for a picture. The non-smooth operations involved in the procedure are the inverses of the ones shown in Fig. 4(b,c).

2. CNot gate

The deformation procedure to obtain a CNot gate is explained in Fig. 6. It has three steps. First the shape of the source and target qubits must be altered pasting respectively their dark and light borders, see Fig. 6(b). This operation introduces two new encoded

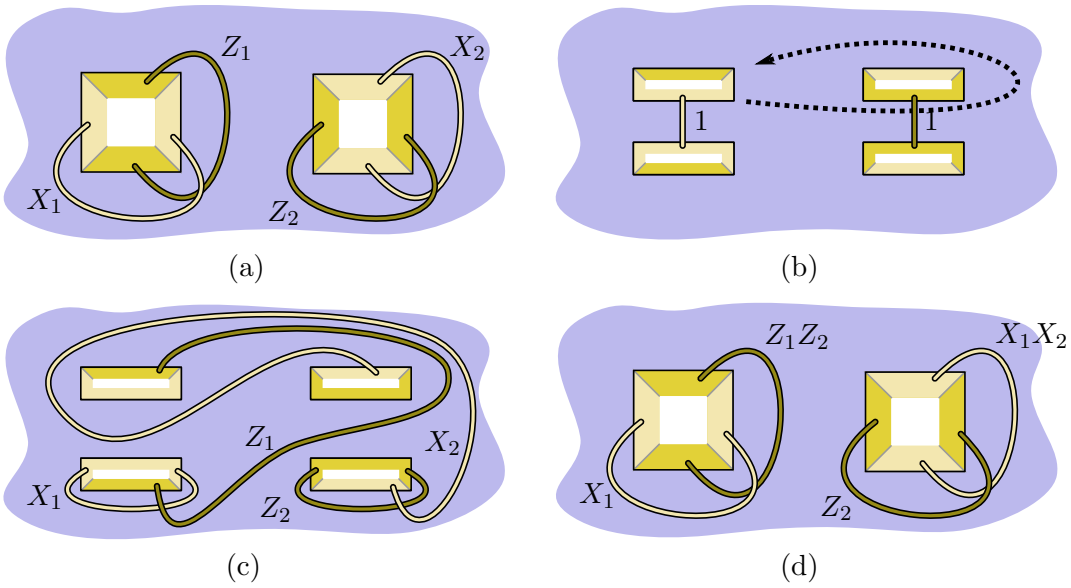
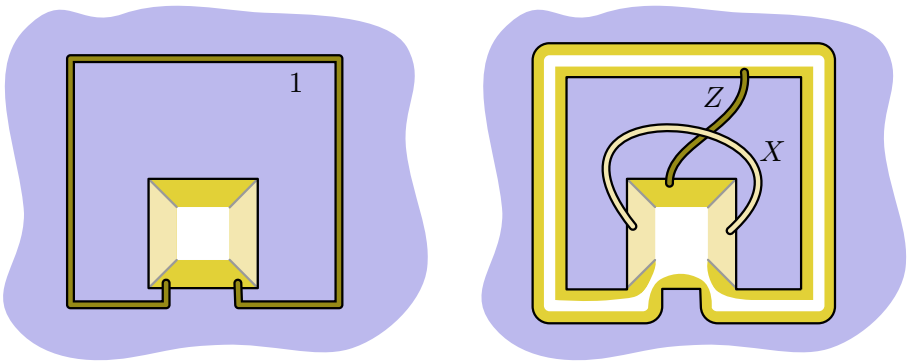


FIG. 6: The code deformation procedure to obtain a CNot gate. To improve readability, only some of the nontrivial strings are shown. (a) The qubits prior to the gate: the left one is the source qubit while the right one is the target. (b) A pair of paste operations are performed to obtain two-holed qubits. The hole movement which is about to be performed is displayed dashed. (c) The hole on the top of the first qubit winds around one of the holes of the second qubit and the string operators deform accordingly. (d) Finally a pair of cut operations are performed to recover the initial configuration. Encoded operators have evolved according to the intended CNot.

qubits because now new nontrivial strings exist. Next, one of the holes on the source qubit winds around one of the holes of the target qubit, as shown in Figs. 6(b,c). This step is where the CNot gate really takes place. Finally, both qubits must recover their original shape. This step involves cutting along strings, so that the two qubits that where created in the first step are measured. Comparing Fig. 6(a) and Fig. 6(d) we see that encoded operators evolve as in (4), so that a CNOT is obtained.

3. Qubit disconnection and reconnection

It is useful to disconnect a qubit from the rest of the surface code. This can be done in several ways, but we choose the one shown in Fig. 7. Observe that the isolated qubit lives in a lattice equivalent, up to smooth deformations, to the one in Fig. 2. These were precisely the qubits considered in [8], and thus we can apply all the single layer processes



(a) (b)

FIG. 7: The code deformation procedure to disconnect a qubit from the rest of the surface code. It can be inverted to reconnect a qubit. (a) The string operator along which the cut is done has eigenvalue 1. (b) After the cut is done, the resulting isolated qubit lives in the inner lattice, which is identical up to deformations to the one in Fig. 2(a).

considered there, such as transversal initialization of $|0\rangle$ and $|+\rangle$ states, X and Z destructive measurements and encoded Hadamard gates.

V. CONCLUSIONS

We have introduced code deformation as a tool to perform gates, initializations and measurements in stabilizer codes. The approach has been demonstrated in surface codes, where in conjunction with the techniques discussed in [8] allows to perform initialization in $|+\rangle$ or $|1\rangle$ states, measurements in Z or X basis, CNot gates and Hadamard gates without exposing any encoded qubit to errors. It is possible to use these operations to distill noisy states obtained through progressive 'growth' [8]. In particular, magic states [16] can be distilled in order to perform universal quantum computation.

Acknowledgements We acknowledge financial support from a PFI fellowship of the EJ-GV (H.B.), DGS grant under contract BFM 2003-05316-C02-01 (M.A.MD.), and CAM-UCM grant under ref. 910758.

[1] P. Shor, 1995 Phys. Rev. A **52**, 2493, 1995.

[2] A. M. Steane, Phys. Rev. Lett. **77** 793, 1996.

[3] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[4] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Phys. Rev. Lett. **78**, 405, (1997).

[5] A. Yu. Kitaev, Annals of Physics **303** no. 1, 2–30 (2003), `quant-ph/9707021`.

[6] H. Bombin, M.A. Martin-Delgado; Phys. Rev. Lett. **97**, 180501 (2006); quant-ph/0605138.

[7] H. Bombin, M.A. Martin-Delgado; Phys. Rev. Lett. 98, 160502 (2007); quant-ph/0610024.

[8] E. Dennis, A. Kitaev, A. Landahl, J. Preskill; J. Math. Phys. **43**, 4452-4505 (2002).

[9] R. Raussendorf, J. Harrington, K. Goyal; New J. Phys. 9 199 (2007); arXiv:quant-ph/0703143.

[10] M. A. Nielsen and I. L. Chuang. "Quantum Computation and Quantum Information", Cambridge University Press, Cambridge, United Kingdom, 2000.

[11] P.W. Shor in Proc. Symp. on the Found. Comp. Sci. (IEEE press, Los Alamitos, California), 56-65, (1996).

[12] E. Knill, R. Laflamme, and W. H. Zurek, Philos. Trans. R. Soc. London, Ser. A 454, 365 (1998); arXiv:quant-ph/9702058.

[13] B. Zeng, A. Cross, I. L. Chuang; arXiv:0706.1382.

[14] S. B. Bravyi, A. Yu. Kitaev; arXiv:quant-ph/9811052.

[15] H. Bombin, M.A. Martin-Delgado, J. Math. Phys. 48, 052105 (2007); arXiv:quant-ph/0605094.

[16] S. Bravyi, A. Kitaev. Phys. Rev. A **71**, 022316 (2005)

Statistical mechanical models and topological color codes

H. Bombin and M. A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain
(Received 16 November 2007; published 24 April 2008)

We find that the overlap of a topological quantum color-code state, representing a quantum memory, with a factorized state of qubits can be written as the partition function of a three-body classical Ising model on triangular or Union Jack lattices. This mapping allows us to test that different computational capabilities of color codes correspond to qualitatively different universality classes of their associated classical spin models. By generalizing these statistical mechanical models for arbitrary inhomogeneous and complex couplings, it is possible to study a measurement-based quantum computation with a color-code state and we find that their classical simulability remains an open problem. We complement the measurement-based computation with the construction of a cluster state that yields the topological color code and this also gives the possibility to represent statistical models with external magnetic fields.

DOI: 10.1103/PhysRevA.77.042322 PACS number(s): 03.67.Lx, 75.10.Hk, 05.50.+q

I. INTRODUCTION

Recently, a very fruitful relationship has been established between partition functions of classical spin models and a certain class of quantum stabilizer states with topological protection [1,2]. The topological quantum code states considered so far in these studies correspond to the toric code states introduced by Kitaev [3–5]. The classical spin model that emerges when a planar toric code is projected onto a product state of single qubits with very specific coefficients is the standard classical Ising model in two dimensions with homogeneous real couplings and zero magnetic field.

Single-qubit measurements also appear naturally in a measurement-based quantum computation (MQC) scheme [6,7]. Thus, these connections between classical spin models and topological quantum states are also useful to test whether those topological states can be classically simulated with MQC efficiently. It has been shown that MQC with a planar Kitaev code state as input can be efficiently simulated in a classical computer if at each step of the computation, the sets of measured qubits form simply connected subsets of the two-dimensional lattice [2]. The connection of classical spin models with measurement-based quantum computation has been shown to be useful to prove the completeness of the classical two-dimensional (2D) Ising model with suitably tuned complex nearest-neighbor couplings in order to represent the partition function of the classical Ising model on arbitrary lattices, with inhomogeneous pairwise interactions and local magnetic fields [8].

Topological color codes (TCC) were introduced to implement the set of quantum unitary gates of the whole Clifford group by means of a topological stabilizer code in a two-dimensional lattice [9], and then generalized to three-dimensional (3D) lattices in order to achieve a universal set of topological quantum gates [10]. These 2D and 3D realizations of TCC are instances of general D-dimensional realizations. We call those lattices related to these codes as D-colexes (for color complexes), and they are D-dimensional lattices with coordination number $D+1$ and certain colorability properties. Moreover, this code can also appear as the ground state of suitable Hamiltonians, and the corresponding quantum systems are brane-net condensates [11].

Given these nice properties exhibited by the topological color codes, it is natural to ask what type of classical spin models can be constructed out of them and see whether they belong or not to the same universality class of the classical Ising model arising in the Kitaev model. In this work we address this issue and find that the overlapping of a TCC state with a product state of single qubits with appropriate coefficients is mapped onto the partition function of the three-body classical Ising model on the dual lattice of the original lattice where the color code is defined. For concreteness, we consider the triangular and the Union Jack lattice for these classical many-body spin systems. This represents a sharp difference with the result obtained with the topological states in the Kitaev code. In fact, the universality classes of the three-body classical Ising model in several lattices are quite different from the corresponding universality class of the standard two-body Ising model.

Moreover, we also study the topological color-code states in a MQC scenario to test their classical simulability. We find that the current state of knowledge in statistical mechanical models with three-body interactions, arbitrary inhomogeneous complex couplings, and lattice shapes is much less developed than the two-body Ising model which is relevant for the case of the toric code states. Thus, we conclude that the classical simulability of TCC states with MQC remains an open problem.

In a MQC, the usual initial many-particle entangled state is a cluster state [6,7] instead of a topological code. Then, we also show how to construct a color-code state from a certain cluster state. Interestingly enough, this construction turns out to be useful for the description of statistical mechanical systems with three-body interactions in the presence of an external field.

This paper is organized as follows: In Sec. II we give an introduction to the topological color-code states needed to present in Sec. III the mapping onto the classical three-body Ising model in the triangular and Union Jack lattices. In Sec. IV we study the measurement-based quantum computation with topological color-code states by generalizing the results of the preceding section. In Sec. V we show how to prepare a topological color code from a cluster state as those introduced in MQC. This is also useful for studying partition

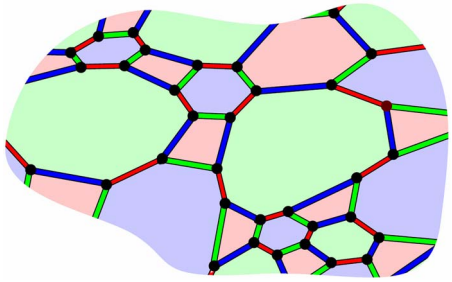


FIG. 1. (Color online) An example of 2-colex. Both edges and faces are three-colorable and they are colored in such a way that green edges connect green faces (light gray) and so on and so forth for red (medium gray) and blue (dark gray) edges and faces.

functions of statistical mechanical models with three-body interactions and external magnetic fields. Section VI is devoted to conclusions.

II. TOPOLOGICAL COLOR CODES

A. Construction

Let us start by recalling the notion of a topological color code in order to see what type of classical spin models we obtain from them with appropriate projections onto factorized quantum states and specific lattices.

A TCC, denoted by $\mathcal{C}$, is a quantum stabilizer error correction code constructed with a certain class of two-dimensional lattices called 2-colexes. The word "colex" is a contraction that stands for color complex, where complex is the mathematical terminology for a rather general lattice. A 2-colex, denoted by $\mathfrak{C}_2$, is a 2D trivalent lattice which has three-colorable faces and is embedded in a compact surface of arbitrary topology such as a torus of genus g. A trivalent lattice is one for which three edges meet at every vertex. The property of being three-colorable means that the faces (or plaquettes) of the lattice can be colored with these colors in such a way that neighboring faces never have the same color. We select as colors red (r), green (g), and blue (b). An example of a 2-colex construction is shown in Fig. 1.

Edges can be colored according to the coloring of the faces. In particular, we attach red color to the edges that connect red faces, and so on and so forth for the blue and green edges and faces. When studying higher dimensional colexes, it turns out that the coloring of the edges is the key property of D-colexes: all the information about a D-colex is encoded in its 1-skeleton, i.e., the set of edges with its coloring [11].

Given a 2-colex ($\mathfrak{C}_2$), a TCC ($\mathcal{C}$) is constructed by placing one qubit at each vertex of the colored lattice. Let us denote by $\mathfrak{V}$, $\mathfrak{E}$, and $\mathfrak{F}$ the sets of vertices $\mathfrak{v}$, edges $\mathfrak{e}$, and faces $\mathfrak{f}$, respectively, of the given 2-colex. Then, the generators of the stabilizer group, denoted by $\mathcal{S}$, are given by face operators only. For each face $\mathfrak{f}$, they come into two types depending on whether they are constructed with Pauli operators of X or Z type,

$$X_{\mathfrak{f}} := \bigotimes_{\mathfrak{v}\in\mathfrak{f}} X_{\mathfrak{v}},$$

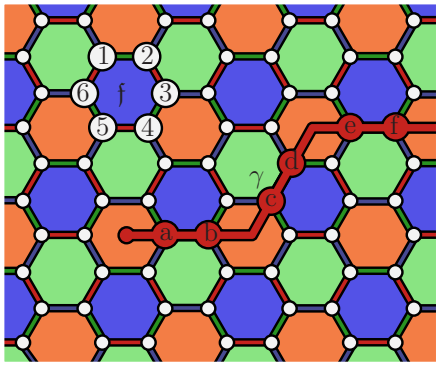


FIG. 2. (Color online) A hexagonal lattice is an instance of 2-colex. Numbered vertices belong to the face $\mathfrak{f}$. Vertices labeled with letters correspond to the red string γ displayed. γ is an open string, because it has an end point in a red face.

$$Z_{\mathfrak{f}} := \bigotimes_{\mathfrak{v}\in\mathfrak{f}} Z_{\mathfrak{v}}, \tag{1}$$

and there are no generators associated to lattice vertices. For example, a hexagonal lattice is an instance of a 2-colex, see Fig. 2. The operators for the face $\mathfrak{f}$ displayed in the figure take the form $X_{\mathfrak{f}}=X_1X_2X_3X_4X_5X_6$, $Z_{\mathfrak{f}}=Z_1Z_2Z_3Z_4Z_5Z_6$.

We notice that for the purpose of this paper, we are dealing only with lattices of trivial topology, such as the plane or the sphere. In these cases, it suffices to require the lattice to have the following properties: (i) Each vertex has coordination number 3; (ii) each face has even number of edges (vertices). These conditions guarantee that the stabilizers X_f and Z_f pairwise commute and the TCC state is unique for the trivial topology. Nevertheless, we have kept the general definition of a 2-colex in terms of three-colorability since we are referring to previous works where nontrivial topologies are considered.

A given state $|\Psi_c\rangle\in\mathcal{C}$ is left trivially invariant under the action of the face operators,

$$X_{\mathfrak{f}}|\Psi_c\rangle = |\Psi_c\rangle, \quad Z_{\mathfrak{f}}|\Psi_c\rangle = |\Psi_c\rangle, \quad \forall\, \mathfrak{f}\in\mathfrak{F}. \tag{2}$$

An erroneous state $|\Psi\rangle_e$ is one that violates conditions (2) for some set of face operators of either type. As the generator operators $X_{\mathfrak{f}}, Z_{\mathfrak{f}}\in\mathcal{S}$ satisfy that they square to the identity operator, $(X_{\mathfrak{f}})^2=\mathbb{1}=(Z_{\mathfrak{f}})^2$, $\forall\mathfrak{f}\in\mathfrak{F}$, then an erroneous state is detected by having a negative eigenvalue with respect to some set of stabilizer generators: $X_{\mathfrak{f}}|\Psi\rangle_e=-|\Psi\rangle_e$ and/or $Z_{\mathfrak{f}}|\Psi\rangle_e=-|\Psi\rangle_e$.

Interestingly enough, it is possible to construct a quantum lattice Hamiltonian H_c such that its ground state is degenerate and corresponds to the TCC ($\mathcal{C}$), while the erroneous states are given by the spectrum of excitations of the Hamiltonian [9]. Such Hamiltonian is constructed out of the generators of the topological stabilizer group $\mathcal{S}$,

$$H_c = -\sum_{\mathfrak{f}\in\mathfrak{F}} (X_{\mathfrak{f}} + Z_{\mathfrak{f}}). \tag{3}$$

The ground state of this Hamiltonian exhibits what is called a topological order [12], as opposed to a more standard order based on a spontaneous symmetry breaking mechanism. One of the signatures of that topological order is precisely the

topological origin of the ground-state degeneracy: The number of degenerate ground states depends on topological invariants such as Betti numbers [11]. In two-dimensional lattices, the relevant Betti number corresponds to the Euler characteristic χ of the surface where the 2-colex is embedded.

B. String-net operators

In order to better understand both the ground state and excitations of this Hamiltonian and their topological properties, it is rather convenient to introduce the set of string operators that can be defined on a 2-colex ($\mathfrak{C}_2$). String operators are generalizations of face operators (1) that can be either open or closed, i.e., with or without end points. These strings are topological and as in the Kitaev model, the homology is defined on $\mathbf{Z}_2$ since we work with two-level quantum systems located at the sites of the lattice. However, in a TCC we have an additional ingredient to play around: Color. Let us split the sets of edges and faces into colored subsets denoted by $\mathfrak{E}:=\mathfrak{E}_r\cup\mathfrak{E}_g\cup\mathfrak{E}_b$ and $\mathfrak{F}:=\mathfrak{F}_r\cup\mathfrak{F}_g\cup\mathfrak{F}_b$, where $\mathfrak{E}_r$ is the subset of red edges, and similarly for the rest of subsets.

A colored string γ is a collection of edges of a given color. Thus, a blue string γ takes the form $\gamma=\{e_i\}$ with $e_i\in\mathfrak{E}_b$. The definition of colored string operators is completely analogous to that of face operators,

$$X_\gamma := \bigotimes_{\mathfrak{e}\in\gamma} X_\mathfrak{e}, \quad Z_\gamma := \bigotimes_{\mathfrak{e}\in\gamma} Z_\mathfrak{e}, \tag{4}$$

where, in turn, $X_\mathfrak{e}=X_{\mathfrak{v}_1}\otimes X_{\mathfrak{v}_2}$ if $\mathfrak{v}_1$ and $\mathfrak{v}_2$ are the sites at the ends of the edge $\mathfrak{e}$, and similarly for $Z_\mathfrak{e}=Z_{\mathfrak{v}_1}\otimes Z_{\mathfrak{v}_2}$. For instance, consider the red string operator in Fig. 2, where we have $X_\gamma=X_aX_bX_cX_dX_eX_f\cdots$, $Z_\gamma=Z_aZ_bZ_cZ_dZ_eZ_f\cdots$.

Colored strings are open if they have end points. These end points are localized at faces which share color with the string. In particular, a face $\mathfrak{f}$ is an end point of γ if the number of edges of γ meeting at $\mathfrak{f}$ is odd, see Fig. 2. In terms of string operators, a face $\mathfrak{f}$ is an end point of γ if $\{X_\gamma,Z_\mathfrak{f}\}=0$ or, equivalently, if $\{Z_\gamma,X_\mathfrak{f}\}=0$. Thus, open string operators do not commute with those face operators in their ends. In other words, a string operator that commutes with all the face operators must correspond to a closed string, that is, a string without end points. In terms of the Hamiltonian (3), string operators produce quasiparticle excitations at their ends when applied to the ground state. These quasiparticle excitations are Abelian anyons.

Closed strings are mainly of two types. They can be homologically trivial, meaning that they are the boundary of certain area of the surface, or homologically nontrivial. In terms of operators, a string is a boundary if and only if its string operators belong to the stabilizer group $\mathcal{S}$ of the color code $\mathcal{C}$. Such boundary string operators are thus products of face operators. In fact, face operators themselves are the basic boundary string operators.

Although we have introduced colored strings and the corresponding operators for illustrative purposes, in fact in a TCC we must deal with more general objects, namely string nets. A string net is a collection of strings meeting at certain branching or ramification points. An example of these types of configurations are shown in Fig. 3.

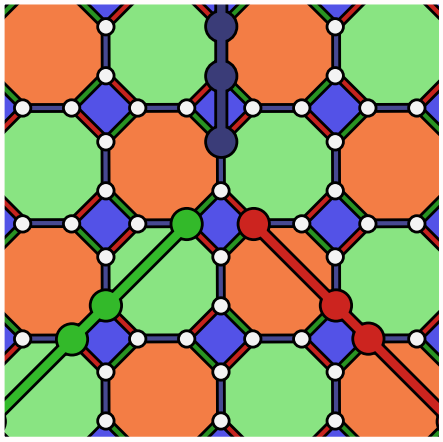


FIG. 3. (Color online) A 4–8 lattice is an instance of 2-colex. A closed string net is displayed, composed of three strings of different colors meeting at a branching point. The string net is closed because at each face we find an even number of its vertices.

A string-net γ is a collection of vertices $\gamma\subset\mathfrak{V}$. Equivalently, γ is a formal sum of lattice vertices $\mathfrak{v}\in\mathfrak{V}$ with coefficients $\gamma_\mathfrak{v}\in\mathbf{Z}_2$, i.e.,

$$\gamma=\sum_{\mathfrak{v}\in\mathfrak{V}}\gamma_\mathfrak{v}\mathfrak{v}, \tag{5}$$

where $\gamma_\mathfrak{v}=1$ if $\mathfrak{v}\in\gamma$ and $\gamma_\mathfrak{v}=0$ otherwise. Given a string-net γ, we define the string-net operators

$$X_\gamma := \bigotimes_\mathfrak{v} X^{\gamma_\mathfrak{v}}, \quad Z_\gamma := \bigotimes_\mathfrak{v} Z^{\gamma_\mathfrak{v}}. \tag{6}$$

Just as in the case of colored strings, we can talk about open and closed string nets, and about trivial and nontrivial closed string nets. In terms of operators, the situation is exactly the same as with strings. That is, a string-net γ has an end point at a face $\mathfrak{f}$ if $\{X_\gamma,Z_\mathfrak{f}\}=0$, it is closed if its string-net operators commute with all the face operators, and it is a boundary if it is a product of face operators. In order to translate these ideas into purely geometric terms, we can define the boundary operator

$$\partial_c\gamma := \sum_\mathfrak{f} x_\mathfrak{f}\mathfrak{f}, \quad x_\mathfrak{f}=\begin{cases}0, & |\gamma\cap\mathfrak{f}| \text{ is even},\\ 1, & |\gamma\cap\mathfrak{f}| \text{ is odd},\end{cases} \tag{7}$$

where $|\gamma\cap\mathfrak{f}|$ is the number of vertices that γ and $\mathfrak{f}$ share. Thus $\partial_c\gamma$ is the formal sum of the end points of γ. It is also natural to define an operator ∂_c for faces

$$\partial_c\mathfrak{f} := \sum_\mathfrak{v} x_\mathfrak{v}\mathfrak{v}, \quad x_\mathfrak{v}=\begin{cases}0, & \mathfrak{v}\notin\mathfrak{f},\\ 1, & \mathfrak{v}\in\mathfrak{f},\end{cases} \tag{8}$$

so that $\partial_c\mathfrak{f}$ is the string net composed of the vertices of $\mathfrak{f}$. With this definition, γ is closed if and only if

$$\partial_c\gamma=0, \tag{9}$$

and it is a boundary if and only if there exist a collection of faces $S=\Sigma_\mathfrak{f}S_\mathfrak{f}\mathfrak{f}$ such that

$$\gamma=\partial_c S. \tag{10}$$

It is possible to give explicit expressions for the states of the TCC or, equivalently, for the ground states of the Hamiltonian (3). The states are superposition's of all possible closed string nets, a typical feature of the ground states of systems with topological order [12,13]. The following is an unnormalized ground state for any given 2-colex [9,11]:

$$|\Psi_c\rangle := \prod_{\mathfrak{f}} (1 + X_{\mathfrak{f}})|0\rangle^{\otimes|\mathfrak{V}|} = \sum_{\gamma\in\Gamma_0} X_\gamma|0\rangle^{\otimes|\mathfrak{V}|} =: \sum_{\gamma\in\Gamma_0} |\gamma\rangle, \tag{11}$$

where $|\mathfrak{V}|$ is the number of vertices in the 2-colex $\mathfrak{C}_2$, Γ_0 denotes the set of boundary string nets, and $|0\rangle$ is the eigenstate $Z|0\rangle=|0\rangle$.

The degeneracy of the ground state or, equivalently, the number of logical states encoded in the color code, depends on the topology of the lattice. For a general 2-colex $\mathfrak{C}_2$ with Euler characteristic $\chi(\mathfrak{C}_2) := |\mathfrak{V}|-|\mathfrak{E}|+|\mathfrak{F}|$, the number k of encoded qubits is given by $k=4-2\chi(\mathfrak{C}_2) := 2h_1$ [9], where h_1 is the first Betti number of the surface where the 2-colex is embedded [11]. These additional ground states can be obtained from the one given by (11) by the action of the encoded logical operators $\bar{X}_i, \bar{Z}_i$ with $i=1,\ldots,k$. These, in turn, take the form of string-net operators of nontrivial closed string nets [9].

For the purpose of this work, we shall be interested only in a representative ground state as in (11). Thus, we will have to consider suitable surface topologies such that the corresponding TCC is unique. We will return to this issue later when we consider particular lattices.

III. CONNECTION WITH CLASSICAL SPIN SYSTEMS

A. Overlap and partition function

Now, we come to the issue of what type of classical spin models may arise from the color-code state (11) when we project it onto a product state of a number of qubits given by $|\mathfrak{V}|$. In this section we shall not consider the most general factorized state, but one specifically adapted for the purpose of this connection in its most simple form, namely,

$$|\Phi_P\rangle := \bigotimes_{\mathfrak{v}\in\mathfrak{V}} |\phi\rangle_{\mathfrak{v}}, \quad |\phi\rangle_{\mathfrak{v}} := \cosh(\beta J)|0\rangle_{\mathfrak{v}} + \sinh(\beta J)|1\rangle_{\mathfrak{v}}, \tag{12}$$

with $\beta := 1/k_B T$ the inverse temperature parameter.

The classical spin model arises when computing the overlapping between the ground state of the color-code Hamiltonian (11) and this factorized state (12),

$$O(\beta J) := \langle\Psi_c|\Phi_P\rangle. \tag{13}$$

Using (11) and (12) we obtain the following expression for this overlapping:

$$O(\beta J) = \sum_{\gamma\in\Gamma_0} \langle\gamma| \bigotimes_{\mathfrak{v}\in\mathfrak{V}} |\phi\rangle_{\mathfrak{v}} = [\cosh(\beta J)]^{|\mathfrak{V}|} \sum_{\gamma\in\Gamma_0} u^{|\gamma|}, \tag{14}$$

$u := \tanh(\beta J)$, and $|\gamma|$ is the number of vertices of γ.

We want to relate (14) to the partition function of a classical spin system. So let $\mathfrak{C}_2$ be an arbitrary 2-colex. Consider the dual lattice Λ. The vertices of Λ correspond to the faces of $\mathfrak{C}_2$, and the faces of Λ are vertices in $\mathfrak{C}_2$. In particular, Λ is a lattice in which all faces are triangular and vertices are three-colorable. Moreover, for any such lattice Λ there exist a suitable dual 2-colex $\mathfrak{C}_2$.

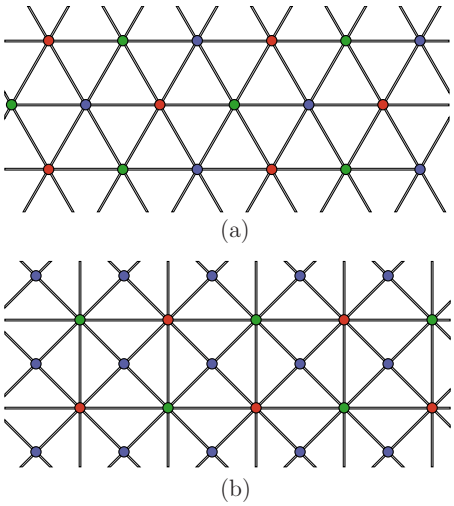


FIG. 4. (Color online) Two instances of dual lattices of a 2-colex, which have triangles as faces and have three-colorable sites. The triangular lattice (a) is dual to the hexagonal one. The Union Jack lattice (b) is dual to the square-octagonal or 4–8 lattice.

So let us associate a classical system to Λ by attaching classical spin variables $\sigma_i = \pm 1$ to each of its sites i (equivalently, to each face $\mathfrak{f}$ of $\mathfrak{C}_2$). The classical Hamiltonian is

$$\mathcal{H} := -J \sum_{\langle i,j,k\rangle} \sigma_i\sigma_j\sigma_k, \tag{15}$$

where J is a coupling constant and the sum $\Sigma_{\langle i,j,k\rangle}$ is over all triangles with spins $\sigma_i\sigma_j\sigma_k$ at their vertices. Thus, we have a classical Ising model with three-body interactions. The case $J>0$ corresponds to a ferromagnetic model with an even parity to be discussed below, and similarly $J<0$ to an antiferromagnetic model with odd parity. The partition function of the model is

$$\mathcal{Z}(\beta J) := \sum_{\{\sigma\}} e^{\beta J \Sigma_{\langle i,j,k\rangle}\sigma_i\sigma_j\sigma_k}, \tag{16}$$

where the sum $\Sigma_{\{\sigma\}}$ is over all possible configurations of spins. The point then is that we have

$$\mathcal{Z}(\beta J) = 2^N O(\beta J), \tag{17}$$

where N is the number of sites.

Before we show why this identity holds, let us give a pair of representative examples of dual lattices $\mathfrak{C}_2$ and Λ. First, if the 2-colex is an hexagonal lattice then the dual lattice Λ is a triangular lattice, Fig. 4(a). Second, if the 2-colex is a square-octagonal lattice (also denoted by 4–8 lattice), then its dual is a Union Jack lattice, see Fig. 4(b). The relevance of these examples is twofold. On the one hand, the hexagonal lattice is the simplest lattice for a 2-colex and the 4–8 lattice is the simplest one when we want to obtain TCC with certain transversal properties for quantum computation (see below). On

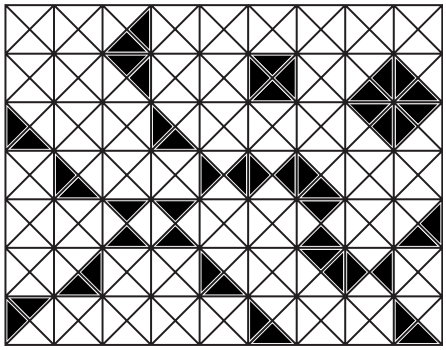


FIG. 5. A typical chain of triangles $\delta \in \Delta_0$ in a triangular lattice. It is understood that only part of the lattice is displayed. Black triangles represent the elements of δ. The fact that $\delta \in \Delta_0$ means that at each vertex it always meets an even number of triangles.

the other hand, three-body classical Ising models on both lattices have been studied in statistical mechanics to some extent.

To prove (17), let us start expanding the partition function $\mathcal{Z}(\beta J)$ (16) using the following identity:

$$e^{\beta J \sigma_i \sigma_j \sigma_k} = \cosh(\beta J) + \sigma_i \sigma_j \sigma_k \sinh(\beta J). \tag{18}$$

Inserting it into (16), we may expand the partition function as

$$\mathcal{Z}(\beta J) = [\cosh(\beta J)]^N \sum_{\{\sigma\}} \prod_{\langle i,j,k \rangle} (1 + u \sigma_i \sigma_j \sigma_k). \tag{19}$$

Let us rewrite (19) in the form

$$\mathcal{Z}(\beta J) = [\cosh(\beta J)]^N \sum_{\delta} u^{|\delta|} \sum_{\{\sigma\}} \prod_{\langle i,j,k \rangle} (\sigma_i \sigma_j \sigma_k)^{\delta_{ijk}}, \tag{20}$$

where $\delta = \Sigma_{\langle i,j,k \rangle} \delta_{ijk} \Delta_{ijk}$ is a chain of triangles, that is, a formal sum over triangles with binary coefficients, and $|\delta|$ is the number of triangles in δ. Using the identities

$$\sum_{\sigma = \pm 1} \sigma^{n_o} = 0, \quad \sum_{\sigma = \pm 1} \sigma^{n_e} = 2, \tag{21}$$

where n_o and n_e are odd and even numbers, respectively, we obtain

$$\mathcal{Z}(\beta J) = [2 \cosh(\beta J)]^N \sum_{\delta \in \Delta_0} u^{|\delta|}, \tag{22}$$

where Δ_0 contains those chains of triangles such that at any given site i an even number of triangles meet, as shown in Fig. 5. In fact, this type of expansion is called a high-temperature expansion of the partition function of a statistical mechanical model [14–16].

In order to compare (40) and (52), we simply observe that triangles Δ_{ijk} in Λ correspond to vertices of the 2-colex $\mathfrak{v} \in \mathfrak{V}$. This correspondence relates in an obvious way a string-net γ with a triangle chain δ, in such a way that Δ_0 is identified with Γ_0. Therefore, we have the desired relationship between the overlapping and the partition function (17).

Although the previous derivation was performed for a model with uniform couplings, it is possible to obtain a completely analogous result for triangle-dependent couplings J_{ijk}. For simplicity we have preferred to do the exposition with uniform couplings because, in fact, the case of nonuniform couplings is contained in the more general case of nonuniform couplings with nonuniform external field, to be considered in Sec. V.

B. Consequences

We hereby draw a series of very important consequences from these results, that will continue in the next section.

(i) *Interactions*. We see that there is a clear qualitative difference between topological color-code states and Kitaev's toric code states since they yield quite different type of spin interactions: A TCC state yields a three-body interaction as in (16), while a Kitaev's code produces the standard two-body classical Ising model, namely,

$$\mathcal{Z}_{\text{Ising}}(\beta J) := \sum_{\{\sigma\}} e^{\beta J \Sigma_{\langle i,j \rangle} \sigma_i \sigma_j}. \tag{23}$$

(ii) *Symmetry*. A distinctive feature of our result (16) is that the classical spin model associated to the TCC state does not possess the up-down $\mathbf{Z}_2$ spin-reversal symmetry. However, the partition function (16) exhibits a $\mathbf{Z}_2 \times \mathbf{Z}_2$ symmetry. Recall that the lattice Λ is three-colorable at sites, so that we can redundantly label our classical spin variables as σ_i^c with $c = r, g, b$ the color at site i. Then the change of variables

$$\sigma_i^c \to s(c) \sigma_i^c, \quad s(r)s(g)s(b) = 1, \quad s(c) = \pm 1, \tag{24}$$

gives a global symmetry, which has symmetry group $\mathbf{Z}_2 \times \mathbf{Z}_2$ because $s(b) = s(r)s(g)$. The ground states must display this symmetry, in fact. Consider states in which the values of the spin variables only depend on the color, that is, for which $\sigma_i^c = f_c$ with $f_c = \pm 1$. Such states can be labeled with the tag (f_r, f_g, f_b). Then it is easy to check that for the ferromagnetic case, $J > 0$, the ground states are labeled with the positive parity tags $(+,+,+)$, $(+,-,-)$, $(-,+,-)$, and $(-,-,+)$, whereas in the antiferromagnetic case, $J < 0$, they are labeled with the negative parity tags $(-,-,-)$, $(-,+,+)$, $(+,-,+)$, and $(+,+,-)$. Thus, each parity sector, or classical ground state of (15) is fourfold degenerate. Notice that the three-body Ising model in such three-colorable lattices of triangles shows no frustration, as opposed to the standard Ising model (23) in such lattices which is indeed frustrated.

Remarkably, the gauge group underlying the topological order related to Hamiltonian (3) is also $\mathbf{Z}_2 \times \mathbf{Z}_2$. The situation is the same also with toric codes, where the global symmetry of the classical system is $\mathbf{Z}_2$ and the gauge group for the toric code topological order is $\mathbf{Z}_2$. This is certainly not a matter of chance, since one can relate the types of domain walls in the classical system to the types of condensed strings in the quantum system.

(iii) *Self-duality*. The models in the triangular and Union Jack lattices turn out to be self-dual as in the usual two-body Ising model, with a critical temperature β_c given by the same condition,

$$\sinh 2K_c = 1, \quad K_c := \beta_c J_c = 0.4407. \tag{25}$$

Duality is a property between high-temperature and low-temperature expansions of a statistical mechanical model as

in (16) or (23). A high-temperature expansion is a polynomial in the variable $u=\tanh(\beta J)$ that is small when $T\to\infty$, while a low-temperature expansion is another polynomial in the variable $u^*:=e^{-2\beta J^*}$ that is small in the limit $T\to 0$. Then, a self-duality is a relationship between the high-temperature expansion of one classical spin model in a given lattice Λ and the low-temperature expansion of the same lattice. This is precisely the case of the three-body Ising model (16) on both the triangular and Union Jack lattices [17,18] and the standard Ising model (23) [19]. Self-duality for more general 3-valent lattices is also satisfied [18].

(iv) *Universality classes*. Interestingly enough, the three-body Ising model on the triangular lattice [20,21] and the Union Jack lattice [22] are exactly solvable models under certain circumstances and this fact allows us to check their criticality properties when compared with those of the standard Ising model solution.

The critical exponent for the specific heat in the three-body Ising model on the triangular lattice is $\alpha=\frac{2}{3}$. This represents a power law behavior which is in sharp contrast with the well-known logarithmic divergence ($\alpha=0$) of the specific heat in the standard Ising model (23). Other representative exponents are also different: The correlation length exponent is $\nu=\frac{2}{3}$ (vs $\nu=1$), the magnetization exponent is $\beta=\frac{1}{12}$ (vs $\beta=\frac{1}{8}$), while they share the same two-point correlation function exponent at the critical point $\eta=\frac{1}{4}$.

For the three-body Ising model on the Union Jack lattice, the specific heat critical exponent is also remarkably different $\alpha=\frac{1}{2}$. In fact, if the coupling constant J is allowed to be anisotropic, then even the critical exponent α may take on a set of continuous values in $(0,\frac{1}{2})$ depending on a parameter related to the coupling constants [22].

The computational capabilities of a topological color code depends on the 2-colex lattices where it is defined. For a TCC on a square-octagonal lattice it is possible to implement the whole Clifford group of unitary gates generated by the set of gates $\{H,K^{1/2},\Lambda_2\}$, where H is the Hadamard gate, $K^{1/2}$ the $\pi/8$ gate, and Λ_2 the controlled-NOT (CNOT) gate [9]. However, for a 2-colex such as the hexagonal lattice the set of available gates is more reduced since the $\pi/8$ gate cannot be implemented topologically [9]. Thus we point out a remarkable connection between different computational capabilities of color codes that correspond to qualitatively different universality classes of their associated classical spin models, despite the fact that both color codes have the same topological order.

C. Borders

If we want to consider classical systems of spins with a finite number of sites, then we must introduce either borders or a nontrivial topology. Since in TCCs the nontrivial topology gives rise to degeneracy, it is preferable to have borders. Also, borders play a role for the ideas to be explained in the next section.

In TCCs, borders can be of several types. For example, in [9] it was shown how to build borders of a given color. Here our guide to construct the border must be the dual lattice Λ, which now has a border, along with the properties of the classical system. Then, as shown in Fig. 6, in order to construct the stabilizer for a TCC with border in such a way that (17) remains true is to start with an infinite 2-colex $\mathfrak{C}_2$ and then keep only part of it following certain criteria. (i) Keep those vertices $\mathfrak{v}$ of $\mathfrak{C}_2$ which correspond to triangles in Λ. (ii) For those faces $\mathfrak{f}$ of $\mathfrak{C}_2$ which keep all their vertices, we keep the face operators $X_\mathfrak{f}$ and $Z_\mathfrak{f}$. (iii) For those faces $\mathfrak{f}$ which only keep a subset $\mathfrak{f}'$ of their vertices, we introduce a face operator $Z_{\mathfrak{f}'}$ acting on those qubits. Condition (i) ensures the correspondence between triangle chains in Λ and string nets in $\mathfrak{C}_2$. Conditions (ii) and (iii) ensure the correspondence between Γ_0 and Δ_0.

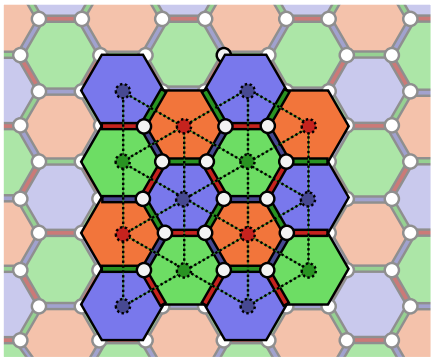


FIG. 6. (Color online) Here both an hexagonal 2-colex $\mathfrak{C}_2$ and its dual triangular lattice Λ (dashed) are displayed to illustrate how borders are introduced in the 2-colex if Λ has borders. All vertices of the 2-colex which are not triangles in Λ have been removed, and also all the faces which keep no vertices. The faces that only keep part of their vertices remain, but only their Z face operators are kept in the stabilizer.

IV. MEASUREMENT-BASED QUANTUM COMPUTATION WITH COLOR CODES

In a measurement-based quantum computer (MQC) [6], information processing is carried out via a sequence of one-qubit measurements on an initialized entangled quantum register. This is an alternative to the standard gate-based quantum computation that can simulate quantum networks efficiently.

An interesting problem is to study the performance of the MQC when the initial entangled multiparticle state is a topological toric code, such as in Kitaev's model [2]. In particular, under which general circumstances the MQC based on the planar Kitaev code can be efficiently simulated by a classical computer. The answer to this question is that the planar code state can be efficiently simulated on a classical computer if at each step of MQC, the sets of measured and unmeasured qubits correspond to simply connected subsets of the lattice [2].

Likewise, another very interesting problem is whether a topological color-code state can be classically simulated in a scenario of measurement-based quantum computation. By extending the results of Sec. III, it is possible to address this problem here. Our aim is to see what conclusions can we learn from the statistical mechanical models in order to test

the classical simulability by MQC of the topological code states.

The results of Sec. III can be interpreted as a complete projective measurement of the planar topological color-code state (11) onto a very specific product of single-qubit states (12). This type of global measurement is not enough for performing a MQC based on the color-code state. Instead, we need to allow for more general one-qubit measurements and to perform them in an adaptive fashion as the computation proceeds from the starting point until the end.

To be more specific, let us consider a generic qubit state with complex coefficients

$$|\varphi\rangle_{\mathfrak{v}} := c_{\mathfrak{v}}^0|0\rangle_{\mathfrak{v}} + c_{\mathfrak{v}}^1|1\rangle_{\mathfrak{v}}, \quad c_{\mathfrak{v}}^0, c_{\mathfrak{v}}^1 \in \mathbf{C}. \tag{26}$$

Then, a MQC starts with a planar color code (11) and we apply a series of projective measurements $M_{\mathfrak{v}}$, as specified by a unity decomposition $I=|\psi^0\rangle_{\mathfrak{v}}\langle\psi^0|+|\psi^1\rangle_{\mathfrak{v}}\langle\psi^1|$ with ψ^i arbitrary orthonormal one-qubit states, from the first qubit $\mathfrak{v}=1$ in the code until the last one $\mathfrak{v}=|\mathfrak{V}|$. The order in which this sequence of measurements is carried out through the 2-colex lattice is arbitrary. After each measurement, the corresponding qubit at the vertex $\mathfrak{v}$ gets projected onto one of the states in (26) and the result is a value for the outcome denoted by $m_{\mathfrak{v}}=0,1$.

The result of a run of a MQC is a set of outputs $m_1,\ldots,m_{\mathfrak{v}},\ldots,m_{|\mathfrak{V}|}$ with a certain probability distribution $P(m_1,\ldots,m_{|\mathfrak{V}|})$. We adopt the definition [2] that a MQC can be classically simulated in an efficient way if there exists a classical randomized algorithm that allows one to sample the outputs $m_1,\ldots,m_{|\mathfrak{V}|}$ from the probability distribution $P(m_1,\ldots,m_{|\mathfrak{V}|})$ in a time poly$(|\mathfrak{V}|)$.

Then, after a complete run of a MQC with (11) we obtain the following generalized overlapping:

$$O_{\mathrm{MQC}} := \langle\Psi_{\mathrm{c}}| \bigotimes_{\mathfrak{v}\in\mathfrak{V}} |\varphi\rangle_{\mathfrak{v}}. \tag{27}$$

Using the same type of computations that led to (14), we arrive at the following expression:

$$O_{\mathrm{MQC}} = \sum_{\gamma\in\Gamma_0} \langle\gamma| \bigotimes_{\mathfrak{v}\in\mathfrak{V}} |\varphi\rangle_{\mathfrak{v}} = \prod_{\mathfrak{v}\in\mathfrak{V}} c_{\mathfrak{v}}^0 \sum_{\gamma\in\Gamma_0} \prod_{\mathfrak{v}\in\mathfrak{V}:x_{\mathfrak{v}}=1} \left(\frac{c_{\mathfrak{v}}^1}{c_{\mathfrak{v}}^0}\right). \tag{28}$$

This result can also be turned into the partition function of a statistical model with three-body Ising interactions (16) but with complex and inhomogeneous Boltzmann weights

$$w_{ijk} = e^{\beta J_{ijk}} \in \mathbf{C}, \tag{29}$$

depending on each triangular plaquette $\langle i,j,k\rangle$. The generalized overlapping (28) is proportional to a generalized partition function of a three-body Ising model with inhomogeneous and complex coupling constants

$$\mathcal{Z}(\beta,\{J_{ijk}\}) := \sum_{\{\sigma\}} e^{\beta\Sigma_{\langle i,j,k\rangle\in\Lambda} J_{ijk}\sigma_i\sigma_j\sigma_k}, \tag{30}$$

where the lattice Λ can be the complete triangular or the complete Union Jack lattice.

At an intermediate stage of a run of a MQC with the color-code state, the 2-colex will split into two subsets $\mathfrak{C}_2$: $=\mathfrak{M}\cup\overline{\mathfrak{M}}$, with $\mathfrak{M}$ the set of measured qubits and $\overline{\mathfrak{M}}$ the set of unmeasured qubits [2]. Thus, during the running of the MQC starting with the color-code state, we shall find generalized partition functions of the type (30) but for a lattice that is the dual of the subset of measured qubits, $\Lambda=\mathfrak{M}^*$.

Therefore, we arrive at the situation that in order to classically simulate a topological color-code state in a MQC we need to simulate the conditional probabilities $P(m_{\mathfrak{v}+1}|m_1,\ldots,m_{|\mathfrak{v}|})$ (at step $\mathfrak{v}+1$ knowing the probabilities of previous steps) and for these we need to be able to compute efficiently in a time poly(L) on the size L of the intermediate lattice at step $\mathfrak{v}+1$.

At this point there is a sharp difference between the classical simulation with MQC of the Kitaev states and the color-code states. Kitaev states can be classically simulated under very general conditions: The subsets $\mathfrak{M}$ and $\overline{\mathfrak{M}}$ must be simply connected. The basic ingredient to achieve this result in the two-body Ising model is that even though a generalized standard Ising model (with arbitrary complex and inhomogeneous couplings) may not be translationally invariant, nevertheless there always exist a technique allowing it to be mapped onto a dimer covering problem (DCP) which in turn can be solved efficiently through the Paffian method in polynomial time [2,23,24].

However, the dimer problem technique is applicable to two-body interactions but not for the three-body interactions that arise in the generalized statistical mechanical models from color codes. In the case of the three-body Ising model with uniform and real couplings $J_{ijk}=J\in\mathbf{R}$ in a triangular lattice, it can be exactly solved by mapping it onto the generating function of a suitable site-coloring problem (SCP) on a hexagonal lattice [20,21], which can be solved by the Bethe ansatz. In order for this site-coloring mapping to work, certain restrictive conditions on the triangular lattice must be fulfilled. In particular, the partition function (16) must be defined on a periodic triangular lattice with L rows in the horizontal direction and N columns in the vertical direction. Let us denote it as $Z_{LN}^{(3)}$. Let us also denote by Z_{MN}^{SCP} the generating function of a site-coloring problem on a hexagonal lattice with $M=\frac{2}{3}L$ and N columns. Then, the aforementioned mapping works in the limit $N\to\infty$ as

$$Z_{LN}^{(3)} = Z_{MN}^{\mathrm{SCP}}, \quad N \gg 1. \tag{31}$$

Furthermore, the SCP is solved by Bethe ansatz technique. This technique also poses another fundamental problem in this situation since it is used to compute the eigenvalues of the associated transfer matrix of the SCP, and then the issue about the completeness of that spectrum in terms of Bethe ansatz eigenfunctions arises. This issue is always a difficult question and, strictly speaking, it is a conjecture. Quite on the contrary, these difficulties are absent in the standard Ising model case since the DCP is more versatile.

The situation becomes even more difficult if we consider the generalized partition function (30) in the framework of an intermediate step in the MQC. Then, it is not known how to solve it efficiently with a mapping to a SCP in an hexagonal lattice without restrictions.

This site-coloring mapping plays a similar role as the dimer covering mapping in the standard two-body Ising

model. However, the known solutions to this site-coloring problem demand more restrictive conditions on the type of lattices and they are less powerful than the dimer mapping technique.

As for the topological color code on a 2-colex such as the Union Jack lattice, similar conclusions apply: In the case of real couplings $J_{ijk}=J\in\mathbf{R}$, it is exactly solvable since it can be mapped onto a 8-vertex model [22], which in turn must be solved by the Bethe ansatz.

The fact that the three-body classical Ising model is exactly solvable in the triangular and Union Jack lattices for real and isotropic couplings, is not enough so as to conclude that the corresponding topological color-code states can be classically simulated in a MQC scenario. Therefore, the classical simulability of topological color codes with MQC remains an open problem.

V. CLUSTER STATES AND MODELS WITH AN EXTERNAL FIELD

In a MQC scheme of quantum computation, the input state is called a cluster state [6] which is a rather general entangled state associated to a great variety of graph states, i.e., states constructed from qubit states located at the vertices of a lattice specified by the incidence matrix of a graph. A very important property of these cluster states is that they can be created efficiently in any system with a quantum Ising-type interaction between two-state particles in the specified lattice configuration. In Sec. IV we have assumed that the input state for the MQC was a TCC state, without caring about how it could be prepared. Here we show how such a topological color-code state can be obtained from a appropriate cluster state. As a by-product, this construction will turn out to be useful for obtaining classical Ising models in an external magnetic field being associated to color-code states.

A. Cluster state formulation of TCC

Instead of giving a general definition of cluster states, we will consider only bipartite cluster states. So let $\mathfrak{G}$ be a finite bipartite graph, that is, a graph such that its set of vertices $\mathfrak{U}$ is the disjoint union of two sets $\mathfrak{U}=\mathfrak{U}_1\cup\mathfrak{U}_2$ in such a way that neighboring vertices never belong to the same $\mathfrak{U}_i$. Consider the quantum system obtained by attaching a qubit to each of the vertices $\mathfrak{u}$. For each such vertex, we denote by $N(\mathfrak{u})$ the set containing both $\mathfrak{u}$ and its neighbors. The cluster state $|\kappa\rangle$ for the graph $\mathfrak{G}$ is then completely characterized by the conditions

$$\forall \mathfrak{u}\in\mathfrak{U}_1,\quad X_{N(\mathfrak{u})}|\kappa\rangle=|\kappa\rangle,$$

$$\forall \mathfrak{u}\in\mathfrak{U}_2,\quad Z_{N(\mathfrak{u})}|\kappa\rangle=|\kappa\rangle. \tag{32}$$

In order to relate the TCC $\mathcal{C}$ of a 2-colex $\mathfrak{C}_2$ to a cluster state, we construct a bipartite graph $\mathfrak{G}$ by setting $\mathfrak{U}_1=\mathfrak{V}$ and $\mathfrak{U}_2=\mathfrak{F}$. Then, the edges are defined so that $\mathfrak{u}_1=\mathfrak{v}\in\mathfrak{U}_1$ is a neighbor of $\mathfrak{u}_2=\mathfrak{f}\in\mathfrak{U}_2$ if $\mathfrak{v}$ is a vertex of $\mathfrak{f}$ in $\mathfrak{C}_2$, see Fig. 7. Observe that the corresponding cluster state $|\kappa\rangle$ satisfies

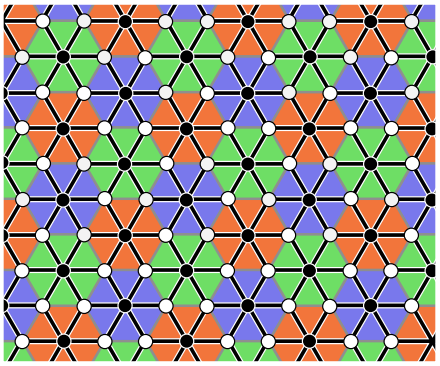


FIG. 7. (Color online) The graph needed to obtain a color-code state from a cluster state. The graph is bipartite, and the vertices are divided in black and white. Black vertices correspond to the faces of the 2-colex. White vertices correspond to the vertices of the 2-colex. Black thick lines represent the edges of the graph, and gray lines correspond to the edges of the 2-colex.

$$\forall \mathfrak{f}\in\mathfrak{F},\quad X_{\mathfrak{f}}|\kappa\rangle=|\kappa\rangle, \tag{33}$$

because $X_{\mathfrak{f}}=\otimes_{\mathfrak{v}\in\mathfrak{f}}X_{N(\mathfrak{v})}$. In fact, if γ is a string net with $\partial_c\gamma=0$, then $X_\gamma|\kappa\rangle=|\kappa\rangle$. However, to keep things as simple as possible, let us just consider 2-colexes in which all closed string nets are boundaries. If we measure in the Z basis all the qubits corresponding to vertices $\mathfrak{u}\in\mathfrak{U}_2$ we will obtain a series of binary values $x_{\mathfrak{u}}=x_{\mathfrak{f}}$. The remaining qubits are then in a state characterized by the conditions

$$\forall \mathfrak{f}\in\mathfrak{F},\quad X_{\mathfrak{f}}|\kappa\rangle=|\Psi_c(\mathbf{x})\rangle,$$

$$\forall \mathfrak{f}\in\mathfrak{F},\quad Z_{\mathfrak{f}}|\kappa\rangle=x_{\mathfrak{f}}|\Psi_c(\mathbf{x})\rangle. \tag{34}$$

Thus, if $x_{\mathfrak{f}}=0$ for all the faces $\mathfrak{f}$, the result is the TCC state $|\Psi_c\rangle$ (11). In the other cases the result is essentially a TCC, in particular the state is

$$|\Psi_c(\mathbf{x})\rangle:=\sum_{\gamma\in\Gamma_{\mathbf{x}}}|\gamma\rangle, \tag{35}$$

where $\mathbf{x}$ denotes the binary vector of the measurement results and $\Gamma_{\mathbf{x}}$ is the set of string-nets γ with $\partial_c\gamma=\Sigma_{\mathfrak{f}}x_{\mathfrak{f}}\mathfrak{f}$.

In fact, the original cluster state can be written as follows:

$$|\kappa\rangle=\sum_{\mathbf{x}}\left(|\mathbf{x}\rangle\otimes\sum_{\gamma\in\Gamma_{\mathbf{x}}}|\gamma\rangle\right), \tag{36}$$

where $|\mathbf{x}\rangle=\otimes_{\mathfrak{u}\in\mathfrak{U}_2}|x_{\mathfrak{u}}\rangle_{\mathfrak{u}}$ is an element of the computational basis of the subsystem of qubits in $\mathfrak{U}_2$. To check that this is indeed the correct expression for the cluster state, it is enough to note that it satisfies (32).

B. Models with an external field

Thus far, we have only considered statistical mechanical models with zero external magnetic field. Here we go beyond that situation, considering the formulation of models with three-body Ising interactions and arbitrary magnetic fields from the projection of topological color codes onto appropriate product states.

Let us define the product state

$$|\Phi_P(\mathbf{J},\mathbf{h})\rangle := \bigotimes_{\mathfrak{v}\in\mathfrak{U}_1} |\phi(J_\mathfrak{v})\rangle_\mathfrak{v} \otimes \bigotimes_{\mathfrak{f}\in\mathfrak{U}_2} |\phi(h_\mathfrak{f})\rangle_\mathfrak{f}, \tag{37}$$

where $\mathbf{J}=(J_\mathfrak{v})\in\mathbf{R}^{|\mathfrak{V}|}$, $\mathbf{h}=(h_\mathfrak{f})\in\mathbf{R}^{|\mathfrak{F}|}$, and

$$|\phi(s)\rangle := \cosh s|0\rangle + \sinh s|1\rangle, \quad s\in\mathbf{R}. \tag{38}$$

Consider the overlapping

$$O(\beta,\mathbf{J},\mathbf{h}) := \langle\Psi_c|\Phi_p(\beta\mathbf{J},\beta\mathbf{h})\rangle. \tag{39}$$

Its value is

$$\sum_{\mathbf{x}} \langle\mathbf{x}| \bigotimes_{\mathfrak{f}\in\mathfrak{U}_2} |\phi(h_\mathfrak{f})\rangle_\mathfrak{f} \sum_{\gamma\in\Gamma_\mathbf{x}} \langle\gamma| \bigotimes_{\mathfrak{v}\in\mathfrak{U}_1} |\phi(J_\mathfrak{v})\rangle_\mathfrak{v} = \prod_\mathfrak{f} \cosh(\beta h_\mathfrak{f}) \prod_\mathfrak{v} \cosh(\beta J_\mathfrak{v}) \sum_{\mathbf{x}} \sum_{\gamma\in\Gamma_\mathbf{x}} \prod_\mathfrak{f} u_\mathfrak{f}^{x_\mathfrak{f}} \prod_\mathfrak{v} u_\mathfrak{v}^{\gamma_\mathfrak{v}}, \tag{40}$$

where

$$u_\mathfrak{f} := \tanh(\beta h_\mathfrak{f}), \quad u_\mathfrak{v} := \tanh(\beta J_\mathfrak{v}). \tag{41}$$

We want to relate (39) to the partition function of a classical spin system. As in Sec. III, we consider the lattice Λ dual to the 2-colex $\mathfrak{C}_2$ and we associate a classical system to Λ by attaching classical spin variables $\sigma_i=\pm 1$ to each of its sites i. This time however we include triangle-dependent couplings J_{ijk} in triangles and a site-dependent external field h_i. Thus, we want to derive the high-temperature expansion for the partition function

$$\mathcal{Z}(\beta,\mathbf{J},\mathbf{h}) := \sum_{\{\sigma\}} e^{-\beta\mathcal{H}(\mathbf{J},\mathbf{h})}, \tag{42}$$

where the classical Hamiltonian is

$$\mathcal{H}(\mathbf{J},\mathbf{h}) := -\sum_i h_i\sigma_i - \sum_{\langle i,j,k\rangle} J_{ijk}\sigma_i\sigma_j\sigma_k. \tag{43}$$

We start using the identities

$$e^{\beta h_i\sigma_i} = \cosh(\beta h_i) + \sigma_i \sinh(\beta h_i),$$

$$e^{\beta J_{ijk}\sigma_i\sigma_j\sigma_k} = \cosh(\beta J_{ijk}) + \sigma_i\sigma_j\sigma_k \sinh(\beta J_{ijk}), \tag{44}$$

so that,

$$\mathcal{Z}(\beta,\mathbf{J},\mathbf{h}) = C\sum_{\{\sigma\}} \prod_i (1+u_i\sigma_i) \prod_{\langle i,j,k\rangle} (1+u_{ijk}\sigma_i\sigma_j\sigma_k), \tag{45}$$

where

$$C := \prod_i \cosh(\beta h_i) \prod_{\langle i,j,k\rangle} \cosh(\beta J_{ijk}), \tag{46}$$

$$u_i := \tanh(\beta h_i), \quad u_{ijk} := \tanh(\beta J_{ijk}). \tag{47}$$

Let us rewrite (45) in the form

$$\mathcal{Z}(\beta,\mathbf{J},\mathbf{h}) = C\sum_{\mathbf{x}} \sum_{\delta} \sum_{\{\sigma\}} \prod_i (u_i\sigma_i)^{x_i} \prod_{\langle i,j,k\rangle} (u_{ijk}\sigma_i\sigma_j\sigma_k)^{\delta_{ijk}}, \tag{48}$$

where $\mathbf{x}=(x_i)$ is a binary vector and $\delta=\Sigma_{\langle i,j,k\rangle}\delta_{ijk}\Delta_{ijk}$ is a chain of triangles, that is, a formal sum over triangles with binary coefficients. Reordering the expression we obtain

$$\mathcal{Z}(\beta,\mathbf{J},\mathbf{h}) = C\sum_{\mathbf{x}} \sum_{\delta} \epsilon(\mathbf{x},\delta) \prod_i u_i^{x_i} \prod_{\langle i,j,k\rangle} u_{ijk}^{\delta_{ijk}}, \tag{49}$$

where

$$\epsilon(\mathbf{x},\delta) := \sum_{\{\sigma\}} \prod_i \sigma_i^{x_i} \prod_{\langle i,j,k\rangle} (\sigma_i\sigma_j\sigma_k)^{\delta_{ijk}}. \tag{50}$$

From (21) it follows that

$$\epsilon(\mathbf{x},\delta) = \begin{cases} 2^N & \text{if } \forall\, i \prod_{\langle j,k\rangle_i} = x_i, \\ 0 & \text{in other case,} \end{cases} \tag{51}$$

where $\langle j,k\rangle_i$ denotes the pairs (j,k) which form a triangle with i, and N is the number of sites. Finally we can give the desired high-temperature expansion of the partition function,

$$\mathcal{Z}(\beta,\mathbf{J},\mathbf{h}) = 2^N C\sum_{\mathbf{x}} \sum_{\delta\in\Delta_\mathbf{x}} \prod_i u_i^{x_i} \prod_{\langle i,j,k\rangle} u_{ijk}^{\delta_{ijk}}, \tag{52}$$

where $\Delta_\mathbf{x}$ contains those chains of triangles such that at any given site i an even (odd) number of triangles meet if $x_i=0$ $(x_i=1)$.

In order to compare (40) and (52), we first observe that sites i correspond to faces of the 2-colex $\mathfrak{f}\in\mathfrak{F}=\mathfrak{U}_2$ and triangles Δ_{ijk} correspond to vertices of the 2-colex $\mathfrak{v}\in\mathfrak{V}=\mathfrak{U}_1$. This correspondence relates in an obvious way x_i with $x_\mathfrak{v}$, h_i, with $h_\mathfrak{v}$ and so on and so forth. Also, there is an exact correspondence between chains of triangle δ and string-nets γ. In particular, this correspondence identifies $\Delta_\mathbf{x}$ with $\Gamma_\mathbf{x}$, so that we obtain the desired relationship between the overlapping and the partition function

$$\mathcal{Z}(\beta,\mathbf{J},\mathbf{h}) = 2^N O(\beta,\mathbf{J},\mathbf{h}). \tag{53}$$

VI. CONCLUSIONS

We have shown that the classical spin models associated to quantum topological color-code states in the two-dimensional lattices called 2-colexes are Ising models with three-body interactions. We have studied this mapping in the triangular and the Union Jack lattices, which are the duals of the two very representative 2-colexes, namely, the hexagonal and the square-octagonal lattices, respectively. This is a genuine difference with respect to the case with toric code states which yield the partition function of the standard Ising model with two-body interactions. Ising models with different n-body interactions have very different properties in general. Remarkably, different computational capabilities of the topological color codes depending on the chosen 2-colex correspond to different universality classes of the associated classical three-body Ising models.

The tools employed to relate classical spin models with topological color-code states can be extended to study the performance of such topological states when they are considered as input in a measurement-based quantum computation. Then, the classical three-body models that arise involve arbitrary complex couplings and lattice shapes. The problem of evaluating their corresponding generalized partition functions cannot be performed with the dimer covering technique that is so successful in the case of the classical two-body Ising model. The similar technique in the three-body case is a particular site-coloring problem that only in very specific instances has been solved by means of the Bethe ansatz. The completeness of the Bethe ansatz poses in turn more fundamental problems in this regard. Therefore, the fact that the three-body Ising model is exactly solvable in certain conditions is not enough to conclude so far that the parent quantum topological color states are efficiently classically simulated by MQC.

Another interesting result is the construction of a cluster state from which we can construct the topological color-code state. This turns out to be useful in order to obtain classical spin models in the presence of arbitrary external magnetic fields. Likewise, there are other two-dimensional multipartite states that arise in the study of quantum antiferromagnets that may lead to a variety of classical spin models [25].

ACKNOWLEDGMENTS

We acknowledge financial support from a PFI grant of the EJ-GV (H.B.), DGS grants under Contracts No. BFM 2003-05316-C02-01 and No. FIS2006-04885 (H.B.,M.A.M-D.), and the ESF Science Programme INSTANS 2005-2010 (M.A.M-D.).

[1] M. Van den Nest, W. Dür, and H. J. Briegel, Phys. Rev. Lett. **98**, 117207 (2007).
[2] S. Bravyi and R. Raussendorf, Phys. Rev. A **76**, 022304 (2007).
[3] A. Yu. Kitaev, Ann. Phys. **303**, 2 (2003).
[4] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).
[5] H. Bombin and M. A. Martin-Delgado, J. Math. Phys. **48**, 052105 (2007).
[6] R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[7] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[8] M. Van den Nest, W. Dür, and H. J. Briegel, Phys. Rev. Lett. **98**, 117207 (2007).
[9] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **97**, 180501 (2006).
[10] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **98**, 160502 (2007).
[11] H. Bombin and M. A. Martin-Delgado, Phys. Rev. B **75**, 075103 (2007).
[12] X.-G. Wen, *Quantum Field Theory of Many-body Systems* (Oxford University Press, Oxford, 2004).
[13] M. A. Levin and X.-G. Wen, Phys. Rev. B **71**, 045110 (2005).
[14] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **76**, 012305 (2007).
[15] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[16] G. F. Newell and E. W. Montroll, Rev. Mod. Phys. **25**, 353 (1953).
[17] D. W. Wood and H. P. Griffiths, J. Phys. C **5**, L253 (1972).
[18] D. Merlini and C. Gruber, J. Math. Phys. **13**, 1814 (1972).
[19] H. A. Krammers and G. H. Wannier, Phys. Rev. **60**, 252 (1941).
[20] R. J. Baxter and F. Y. Wu, Phys. Rev. Lett. **31**, 1294 (1973).
[21] R. J. Baxter and F. Y. Wu, Aust. J. Phys. **27**, 357 (1974).
[22] A. Hintermann and D. Merlini, Phys. Lett. A **41**, 208 (1972).
[23] F. Barahona, J. Phys. A **15**, 3241 (1982).
[24] P. Kasteleyn, Physica **27**, 1209 (1961).
[25] E. Rico and H. J. Briegel, e-print arXiv:0710.2349.

Orden Topológico

Exact topological quantum order in $D=3$ and beyond: Branyons and brane-net condensates

H. Bombin and M. A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain
(Received 4 August 2006; revised manuscript received 19 October 2006; published 7 February 2007)

We construct an exactly solvable Hamiltonian acting on a three-dimensional lattice of spin-$\frac{1}{2}$ systems that exhibits topological quantum order. The ground state is a string net and a membrane-net condensate. Excitations appear in the form of quasiparticles and fluxes, as the boundaries of strings and membranes, respectively. The degeneracy of the ground state depends on the homology of the 3-manifold. We generalize the system to $D \geqslant 4$, where different topological phases may occur. The whole construction is based on certain special complexes that we call colexes.

DOI: 10.1103/PhysRevB.75.075103 PACS number(s): 11.15.−q, 71.10.−w

I. INTRODUCTION

Deviations from a standard theory in a certain field of physics have always attracted attention in the search for new physics. In condensed matter, the standard model is the Landau theory of quantum liquids (Fermi liquid) supplemented with the spontaneous symmetry-breaking (SBB) mechanism and the renormalization group scheme.[1–3] The concept of local order parameter plays a central role in detecting quantum phases or orders within the Landau theory. Quite on the contrary, topological orders cannot be described by means of local order parameters or long-range interactions. Instead, a new set of quantum numbers is needed for this new type of phase, such as ground-state degeneracy, quasiparticle braiding statistics, edge states,[4–6] topological entropy,[7,8] etc.

A consequence of the SBB is the existence of a ground-state degeneracy. However, in a topological order, there exists a ground-state degeneracy with no breaking of any symmetry. This degeneracy has a topological origin. Thus, topological orders deviate significantly from more standard orders covered within the Landau symmetry-breaking theory. The existence of topological orders seems to indicate that nature is much richer than what the standard theory has predicted so far.

Emblematic examples of topological orders are fractional quantum Hall (FQH) liquids. FQH systems contain many different phases at $T=0$ which have the same symmetry. Thus those phases cannot be distinguished by symmetries and Landau's SBB does not apply.[4,9–11] Therefore we need to resort to other types of quantum numbers to characterize FQH liquids. For example, the ground-state degeneracy d_g depends on the genus g of the $D=2$ surface where the electron system is quantized; that is, $d_g=m^g$ with the filling factor being $\nu=\frac{1}{m}$.

There are several other examples of topological orders such as short-range resonating valence bond models,[12–15] quantum spin liquids,[5,16–23] etc. Due to this topological order, these states exhibit remarkable entanglement properties.[24,25] Besides these physical realizations, there have been other proposals for implementing topological orders with optical lattices,[26–28] with spin interactions in honeycomb lattices.[29] In this paper, we shall be concerned with topological models constructed with spins $S=\frac{1}{2}$ located at the sites of certain lattices with a coordination number, or valence, depending on the dimension D of the space and the color properties, which will be explained in Sec. II.

From the point of view of quantum information,[30] a topological order is a different type of entanglement: it exhibits nonlocal quantum correlations in quantum states. A topological phase transition is a change between quantum states with different topological orders. In dimensions $D \geqslant 4$, we construct exact examples of quantum lattice Hamiltonians exhibiting topological phase transitions in Sec. IV A. Here, we find an example of topology-changing transition as certain coupling constant is varied in $D=4$. This is rather remarkable since the most usual situation is to have an isolated topological point or phase surrounded by nontopological phases.[24,25]

In two dimensions, a large class of "doubled" topological phases has been described and classified mathematically using the theory of tensor categories.[47,48] The physical mechanism underlying this large class of topological orders is called string-net condensation. This mechanism is equivalent to particle condensation in the emergence of ordered phases in the Landau theory. A string net is a network of strings, and it is a concept more general than a collection of strings, either closed or open. In a string net, we may have a situation in which a set of strings meet at a branching point or node, something that is missing in ordinary strings which have two ends at most (see Fig. 14). More specifically, the ground state of these theories is described by superpositions of states representing string nets. The physical reason for this is the fact that local energy constraints can cause the local microscopic degrees of freedom present in the Hamiltonian to organize into effective extended objects such as string nets.

A different field of applications for topological orders has emerged with the theory of quantum information and computation.[31–34] Quantum computation, in a nutshell, is the art of mastering quantum phases to encode and process information. However, phases of quantum states are very fragile and decohere. A natural way to protect them from decoherence is to use topologically ordered quantum states which have a nonlocal kind of entanglement. The nonlocality means that the quantum entanglement is distributed among many different particles in such a way that it cannot be destroyed by local perturbations. This reduces decoherence significantly. Moreover, the quantum information encoded in the topological states can be manipulated by moving quasiparticle excitations around one another producing braiding effects that translate into universal quantum gates.[31,35–39]

Nevertheless, there are also alternative schemes to do lots of quantum information tasks by using only the entanglement properties of the ground state.[40–42]

The situation for topological orders in $D=3$ is less understood. This is due in part to the very intricate mathematical structure of topology in three dimensions. While the classification of all different topologies is well established in two dimensions, in $D=3$ the classification is much more difficult, and only recently does it appear to be settled with the proof of Thurston's geometrization conjecture,[43] a result that includes the Poincaré conjecture as a particular case.[44–46] Topological orders have been investigated in three dimensions with models that exhibit string-net condensation[47] using trivalent lattices that extend the case of trivalent lattices in two dimensions. However, a problem arises when one wishes to have an exactly solvable Hamiltonian describing this topological phase since this type of magnetic flux operators does not commute in three dimensions anymore. A solution to this problem can be found by imposing additional constraints to the mechanism found in $D=2$, but this somehow obscures the geometrical picture of the resulting exactly solvable model. Alternatively, it is possible to use a three-dimensional (3D) generalization of Kitaev's toric code to provide examples with a topological order based both on string condensation and on membrane condensation.[49] In the theory of topological quantum error correcting codes, there are also studies of toric codes in dimensions higher than $D=2$.[33,50,51]

In this paper, we introduce a solvable model in $D=3$ that exhibits a topological order. Here, we construct models in which local operators of several kinds commute among each other. This is achieved by requiring certain geometrical properties of the lattices, for which the models are defined. As a result, we can study the whole spectrum of the models and, in particular, their quantum topological properties. The ground state can be described as a string-net condensate or, alternatively, as a membrane-net condensate. A membrane-net condensate is a generalization of a collection of membranes, much like a string-net-condensate is a generalization of the notion of strings. Thus, in a membrane-net, membranes can meet at branching lines instead of at points. Excitations come in two classes: there are quasiparticles that appear as the end points of strings or certain type of fluxes that appear as the boundaries of membranes. These fluxes are extended objects. Interestingly enough, when a quasiparticle winds around a closed flux, the system picks up a nontrivial Abelian phase (see Fig. 17), very similar to when one anyon[52,53] winds around another anyon, acquiring an Abelian factor in the wave function of the system. We coin the name branyons to refer to this quasiparticles that are anyons with an extended structure. In fact, in our models they appear as Abelian branyons.

Our constructions can be nicely generalized to higher dimensions, where different classes of topological orders are possible. We can compute exactly the ground-state degeneracies in terms of the Betti numbers of the manifolds where the lattice models are defined. This allows us to discriminate between manifolds with different homological properties using quantum Hamiltonians. The generalized membranes are called branes, and we also find a brane-net mechanism.

We call the lattices that we introduce in this paper colexes. The motivation for their introduction is that they produce quantum Hamiltonians with a richer topology than others previously considered. For instance, in $D=2$ (see Ref. 40) we have constructed trivalent lattices on tori of genus g for which the ground-state degeneracy is 2^k, where k is given by $k=4-2\chi$, ($\chi=2-2g$ is the Euler characteristic), which is bigger by a factor of 2 than the degeneracy found in Kitaev's toric Hamiltonians. This factor of 2 is related to the appearance of two independent colors for the strings in the model.

In this paper, we have found a complete theory and properties of colexes of any dimension. In particular, we have found other instances of topological orders in $D=3$, where much little is known about the classification of topological orders as it is in $D=2$. The picture is even richer for $D\geqslant 4$ because different topological orders emerge from the same colex structure. We show how this is related to the fact that we can obtain several complexes from a single colex.

In order to summarize the main contributions that we present in this paper, we hereby advance a list of some of our most relevant results.

(i) We introduce a different class of exactly solvable models in $D=3$ and beyond based on a different type of lattices that we call D colexes (or colexes for short).

(ii) Our models present a different mechanism to generate topological orders in $D=3$ based on the concept of membrane-net condensation. Then, it is generalized to $D>3$ in terms of brane-net condensations.

(iii) In the excitation spectrum of these models, there are extended objects (not merely points) that exhibit nontrivial braiding properties. We call them branyons, which stands for brane anyons.

(iv) The ground-state degeneracy of our Hamiltonians has a topological origin, and it is different from those of other topological models. For instance, our models have higher degeneracy than Kitaev's toric codes.

(v) Colexes show a rich mathematical structure. The computation of topological invariants is reduced to a combinatorial problem. From a physical point of view, their structure gives rise to a remarkable property, namely, that the number of charges depends on the dimension of the space.

(vi) The topological structures exhibited by our models have natural applications in quantum information theory, where they can serve to construct topological quantum codes for error correction (see Ref. 40).

(vii) We have constructed families of Hamiltonians with topology-changing quantum phase transitions (see Sec. IV).

This paper is organized as follows. In Sec. II, we introduce the models defined in three-dimensional lattices placed on different manifolds. These lattices are constructed by means of color complexes that we call colexes of dimension 3, or 3-colexes. In Sec. III, the notion of colexes is generalized to arbitrary dimensions. In Sec. IV, we extend the topological quantum Hamiltonians beyond $D=3$ dimensions. In particular, we find instances of topology-changing phase transitions. Section V is devoted to conclusions. In a set of appendixes, we provide a full account of technical details pertaining to particular aspects of our models.

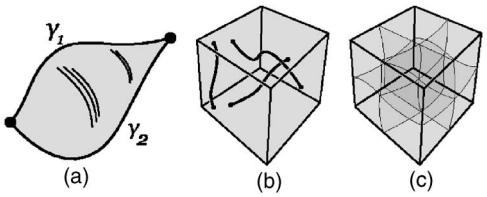


FIG. 1. In (a), the two curves are homologous because they form the boundary of a deformed disk. In (b) and (c), the 3-torus is represented as a cube in which opposite sides must be identified. In (b), a basis for 1-cycles is shown and in (c), a basis for 2-cycles.

II. THE MODEL IN 3-MANIFOLDS

A. Topological order and homology

The model that we are going to study belongs to the category of topologically ordered quantum systems. A system with topological quantum order is a gapped system that shows a dependency between the degeneracy of its ground state and the topology of the space where it exists. Certainly, such a dependency could manifest in many ways, typically as a function of certain topological invariants of the space.

In the case at hand, these topological invariants turn out to be the Betti numbers of the manifold. These in turn reflect the $\mathbf{Z}_2$ homology[42] of the manifold, and so we will now introduce several concepts and we will illustrate them using a well-known 3-manifold, the 3-torus.

Consider any 3-manifold $\mathcal{M}$. For a 1-cycle, we understand any closed nonoriented curve γ in it, or several such curves. In other words, it is a closed 1-manifold embedded in $\mathcal{M}$. Suppose that we can embed in $\mathcal{M}$ a 2-manifold in such a way that its boundary is γ. In that case, γ is called a 1-boundary and is said to be homologous to zero. More generally, consider two nonoriented curves γ_1 and γ_2 with common end points, as in Fig. 1(a). We can combine these two curves into a single 1-cycle, and then we say that they are homologous if the 1-cycle is a 1-boundary. In other words, $\gamma_1 \sim \gamma_2$ if and only if $\gamma_1+\gamma_2 \sim 0$. This kind of equivalence can also be applied to two 1-cycles, and thus two 1-cycles are homologous if and only if their combination is a 1-boundary. Then, the idea is that any 1-cycle can be constructed, up to homology equivalence, by a combination of certain basic 1-cycles. The number of 1-cycles needed to form such a basis is a topological invariant, the first Betti number h_1 of the manifold $\mathcal{M}$. For the 3-torus, $h_1=3$. A possible basis in this case is the one formed by the three 1-cycles that cross the torus in the three spatial directions, as in Fig. 1(b).

Similarly, we can think of 2-cycles as closed 2-manifolds embedded in $\mathcal{M}$. Then, when a 2-cycle is the boundary of some embedded 3-manifold, it is called a 2-boundary and is said to be homologous to zero. Two 2-manifolds with a common boundary can be sewn together to form a 2-cycle, and they are homologous if this 2-cycle is a 2-boundary. As in the case of 1-cycles, there exists a basis for 2-cycles up to homology. Again, these can be exemplified in the case of a 3-torus [see Fig. 1(c)]. The topological invariant that gives the cardinality of such a basis is the second Betti number h_2 and this equals h_1.

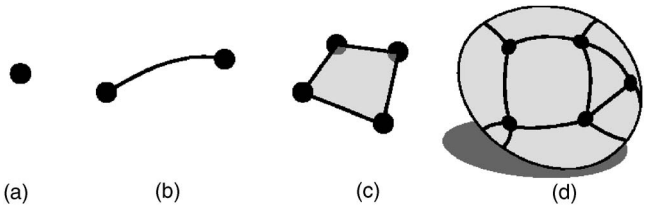


FIG. 2. (a) A vertex, (b) an edge, (c) a face, and (d) a polyhedral solid.

Throughout the text, we sometimes use a more suggestive language. Instead of curves, we talk about strings, closed or open with end points. Similarly, we refer to embedded 2-manifolds as membranes, either closed or with a boundary.

B. System and Hamiltonian

Usually, when we think of a lattice, say, a three-dimensional one, we first imagine or fix the space in which it exists. However, it is also natural to construct the space from the pieces that make up the lattice, say, its sites, links, and so on. Consider, for example, a football made up of hexagons and pentagons sewed together. In this case, the resulting topological space is a sphere made from several polyhedra that are attached, putting together vertices with vertices and sides with sides. Any closed 2-manifold can be constructed by sewing together polyhedra in this way. Such a construction is called a 2-complex, and its constituents are called general cells. Vertices are 0-cells, links are 1-cells, and the polyhedra or faces are 2-cells.

One can use these ideas for spaces of arbitrary dimension. In particular, we are now interested in three-dimensional spaces, which by analogy can be constructed by gluing together polyhedral solids. Let M be a closed connected manifold that has been constructed this way. Its polyhedral solids are balls whose boundary surface is a polyhedron, i.e., a sphere divided into faces, edges, and vertices (see Fig. 2). It is important that the gluing of polyhedral solids must be such that this structure is respected; that is, faces are glued to faces, edges to edges, and vertices to vertices. For brevity, we will call polyhedral solids simply cells. Thus, we have a 3-manifold divided into vertices V, edges E, faces F, and cells C. Such a structure in a 3-manifold is called a 3-complex.

In order to construct the topological quantum system that we propose, we consider a 3-complex such that (i) the neighborhood of every vertex is as the one in Fig. 3 and (ii) cells are four colored in such a way that adjacent cells have different colors. The colors we shall use are red, green, blue, and yellow (r,g,b,y). The main point of condition (i) is that the coordination of the lattice is 4, the minimum number to be able to construct interesting three-dimensional lattices. This first condition says more because it also states that six faces and four cells meet at each site in the most natural way. Thus, condition (i) states which is the local appearance of our lattice. As for condition (ii), its nature is global. Note that locally, at each site, it is immediately true. Moreover, we observe that at least four colors will be necessary to color any lattice satisfying (i) since at each site there are four dif-

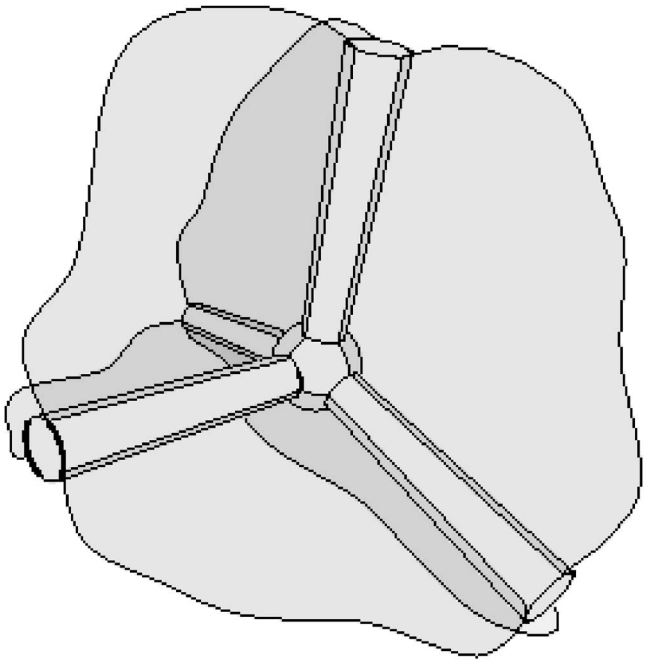


FIG. 3. The neighborhood of a vertex in a 3-colex. Four edges, six faces, and four cells meet at each vertex.

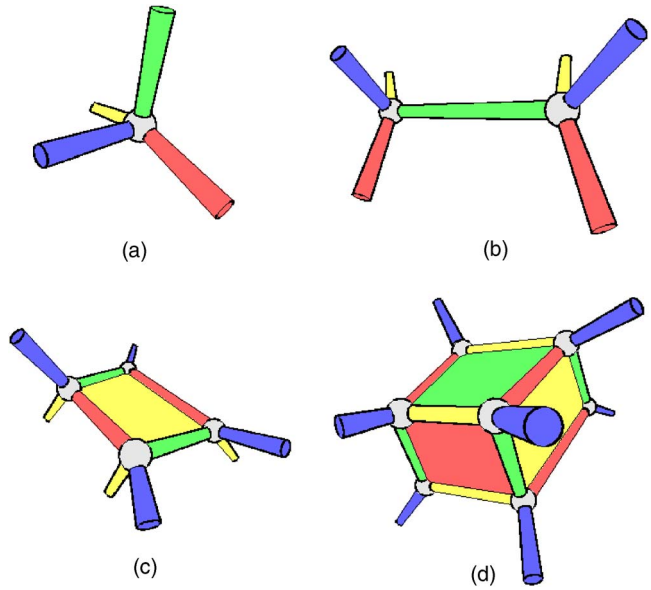


FIG. 4. (Color online) Neighborhoods in a 3-colex of (a) a vertex, (b) a g edge, (c) a by face, with the yellow side visible and the blue one hidden, and (d) a b cell. Faces are colored according to the color of the cell at their visible side.

ferent cells that meet. Condition (ii) is highly constraining, as we will show throughout this section. For example, the commutativity of the operators that sum up to give Hamiltonian (4) is contained in this condition.

We should stress that the name color does not imply that our lattices have to be colored with a new degree of freedom. The quantum degrees of freedom are always spin $\frac{1}{2}$ located at the sites of the colexes. In fact, we could have used another type of labeling in $D=3$ instead of using R,G,B,Y for $3+1$ colors. The important point here is the fact that color is introduced as a bookkeeping tool to keep track of the different sites, links, faces, and cells in the 3D lattice. We could have used another type of labeling, but we chose color because it is more appealing and facilitates the illustration of colexes in the figures.

From this point on, we will use assumptions (i) and (ii) to color edges and faces, and finally, we will see that the whole structure of the manifold is contained in the coloring of the edges.

With a glance at Fig. 3, we see that the four cells meeting at each vertex must have different colors. In the figure, we also see that each edge lies in three cells of different colors. Then each of the end points of the edge is in the corner of a cell of a fourth color, so that we can say that it connects two cells of the same color. We proceed to label edges with the color of the cells they connect [see Fig. 4(b)]. As a result, the four edges that meet at a vertex all have different colors [see Fig. 4(a)]. Also, the edges lying on a r cell are not r edges. However, much more is true. Consider r cell c and any vertex v in its boundary. The red edge that ends in v does not lie on cell c, so that the other three edges incident in v do. But then, any connected collection of g, b, and y edges corresponds exactly to the set of edges of some r-cells.

We label faces with two colors. If a face lies between a p cell and a q cell, we say that it is a pq face [see Fig. 4(c)]. Then consider, for example, a ry cell. Since neither r nor y edges can lie on its boundary, this must consist of a sequence of alternating b and g edges. Conversely, any such path is the boundary of some ry face. To check this, first note that exactly one such path traverses any given g edge e. But e must lie exactly on one ry face, the one that separates the r and the y cell it lies on.

As promised, we have shown that the entire structure of the manifold is contained in two combinatorial data: the graph and the colors of its edges. We call the resulting structure a 3-colex, for color complex in a 3-manifold. The simplest example of such a 3-colex with nontrivial homology is displayed in Fig. 5. It corresponds to the projective space P^3. In Appendix A, we will give a procedure to construct a colex of arbitrary dimension D, or D colex, starting with an arbitrary complex in a D manifold.

Although we shall be considering 3D manifolds with several different topologies in order to see the relationship between the ground-state degeneracy with the homology of the colex, we can also give now an example of a 3-colex in a more familiar closed manifold such as the 3D torus in condensed-matter systems. This is shown in Fig. 6. The virtue of this 3-colex is that it can fill the whole infinite space in case we want to take the thermodynamic limit along a family of lattices having the same topological properties. Thus far, we have only considered closed manifolds. Later, in Sec. II G, we shall also provide another example of a colex lattice with a boundary, so that our catalog of 3-colexes will be complete.

We now associate a physical system with the 3-colex. To this end, we place at each vertex (site) a spin-$\frac{1}{2}$ system. To each cell c, we attach the cell operator

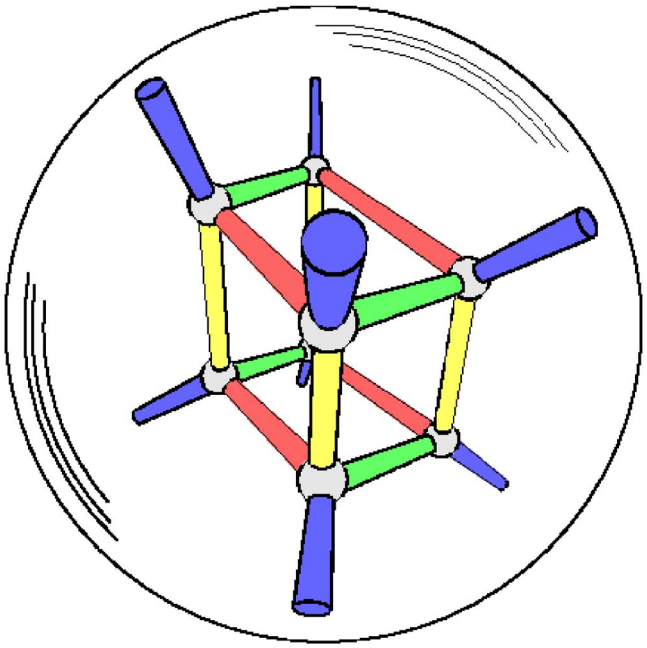


FIG. 5. (Color online) The projective space P^3 can be obtained starting with a solid sphere and identifying opposite points in its surface. Here, we use such a representation to show a 3-colex in P^3.

$$B_c^X := \bigotimes_{i \in I_c} X_i, \tag{1}$$

where X_i is the Pauli σ_1 matrix acting on site i and I_c is the set of sites lying on the cell. Similarly, to each face f we attach the face operator

$$B_f^Z := \bigotimes_{i \in I_f} Z_i, \tag{2}$$

where Z_i is the Pauli σ_3 matrix acting in site i and I_f is the set of sites lying on the face. We have

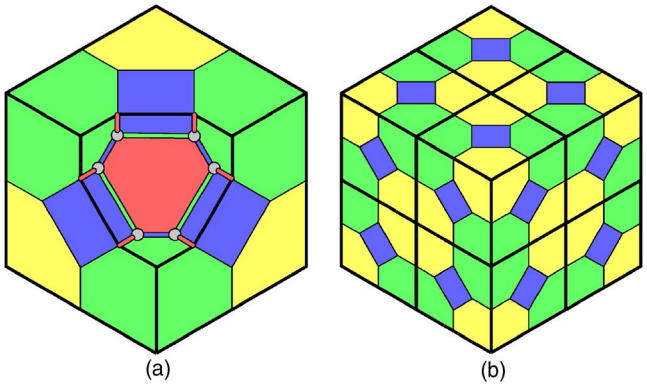


FIG. 6. (Color online) (a) The unit cell of a colex that can fill either the infinite space or a three-dimensional torus. Forgetting about colors, which are unphysical, its symmetries are those of the cube, with a single r cell at its core. Here, colors have been given both to cells and to links. A yellow cell was removed to show the interior of the unit cell. (b) Eight unit cells put together. Recall that color is not reflected in the Hamiltonian, so that all unit cells are equal although they look different due to the coloring.

$$\forall c \in C, f \in F, \quad [B_c^X, B_f^Z] = 0. \tag{3}$$

To show this, consider any cell c and face f. The edges of c come in three colors and the edges of f in two. Thus, they have at least a common color, say, q. Given any shared vertex, we consider its q-edge e. But e lies both on c and on f, and thus its other end point is also a shared vertex. Therefore, c and f share an even number of vertices and $[B_c^X, B_f^Z] = 0$.

The Hamiltonian that we propose is constructed by combining cell and face operators:

$$H = -\sum_{c \in C} B_c^X - \sum_{f \in F} B_f^Z. \tag{4}$$

Observe that color plays no role in the Hamiltonian; rather, it is just a tool we introduce to analyze it. In Appendix C, we calculate the degeneracy of the ground state. It is 2^k with

$$k = 3h_1, \tag{5}$$

and therefore depends only on the manifold, which is a sign of topological quantum order.

The ground states $|\psi\rangle$ are characterized by the conditions

$$\forall c \in C, \quad B_c^X |\psi\rangle = |\psi\rangle, \tag{6}$$

$$\forall f \in F, \quad B_f^Z |\psi\rangle = |\psi\rangle \tag{7}$$

for cell and face operators. Those eigenstates $|\psi'\rangle$ in which any of the conditions is violated are excited states. There are two kinds of excitations. If $B_c^X|\psi'\rangle = -|\psi'\rangle$, we say that there is an excitation at cell c. Similarly, if $B_f^Z|\psi'\rangle = -|\psi'\rangle$, then the face f is excited. Below, we will show that cell excitations are related to quasiparticles and face excitations to certain fluxes. For now, we are just interested in noting that excitations have a local nature and thus the Hamiltonian (4) is gapped. Then, since the ground-state degeneracy depends on the topology, we have a topological quantum order.

In order to look at our models with a broader perspective, let us briefly recall the notion of a lattice gauge theory (LGT) in the Hamiltonian formalism (space=discrete; time =continuous) to see if our lattice Hamiltonians given by Eq. (4) and higher-dimensional extensions [Eq. (27) in Sec. IV] do not fit directly into a standard LGT framework.

(a) In a LGT, the gauge degrees of freedom are located at the edges (links) of the lattice, while the gauge symmetry transformations are local operators defined at the sites (vertices) of the lattice. This is not the case for our lattices that we call D-colexes (or colexes for short) since our spin-1/2 degrees of freedom are located at the site of the colexes. Although this is not a big obstacle is defining a LGT in this setting, it is related to the major difference that we will point out next.

(b) The Hamiltonian in a LGT is constructed out of face operators (magnetic part) and site operators (electric part). This is not the case for our Hamiltonians. For example, the Hamiltonian in Eq. (4) has two contributions: one is made up of face operators B_f^Z, which fall into the class of LGT terms, and the other one is made up of cell operators B_c^X, which are not pure face operators. In fact, the X part of H cannot be written as a sum of single face or plaquette operators; in-

stead, it can be written as a sum of products of face operators, which is something different from a standard LGT.

For models in higher dimensions such as in Eq. (27), the difference is even more notorious since it may also apply to the Z part of our Hamiltonians.

It is true that our models have a certain degree of gauge symmetry since we can define local operators acting on faces (plaquettes) that commute with the Hamiltonian in Eq. (4). These operators would be analogous to the gauge transformations acting locally at the sites of a standard LGT. In our case, each face operator B_f^Z commutes with H. However, we see that our models go beyond the standard LGT.

In summary, in our models there are two main ingredients: one is the lattice structure we call colexes and the other one is the choice of X and Z terms in the Hamiltonian. Playing with these ingredients, we may find interesting physics in different dimensions D.

We would like to mention that knowing the gauge group in a LGT does not tell us everything about the physics of the model. In this regard, we look at our Hamiltonians not only as models in condensed-matter physics but also as models in quantum information.

The best way to show this is with one explicit example that we have introduced in Ref. 40. Here, we constructed two Hamiltonians, say, H_1 and H_2, in $D=2$. This time, both X- and Z-terms were face or plaquette terms for both Hamiltonians, as in a standard LGT. Also, both Hamiltonians were defined in 2-colexes with the same coordination number 3 (trivalent lattices). The difference was that for H_1 the 2-colex was a honeycomb lattice, while for H_2 the 2-colex was a mixed square-octagonal lattice.

The outcome of our study is that the quantum information capabilities of each Hamiltonian are different. The technical results can be found in Ref. 40. To be specific, H_1 does not allow us to implement the set of gates of the Clifford group, while H_2 does allow us to implement it. The benefit of this is enormous since with H_2 we can do a lot of interesting tasks altogether: quantum distillation, quantum teleportation, and quantum dense coding. In summary, the knowledge of the gauge group (when it applies) does not fix the full physical content of a given lattice Hamiltonian in certain aspects.

C. Strings and membranes

From this point on, we shall pursue a better understanding of both the ground-state degeneracy and the excitations by means of the introduction of string and membrane operators. In this direction, an essential notion will be that of a *shrunk complex*, both of the first and the second kind. The motivation after the construction of these complexes from the colexes is that only at the shrunk complex level is it possible to visualize neatly the strings and membranes that populate the model. These new shrunk complexes are not colexes, but their cells are associated with cells in the colex, and thus have color labels.

1. Shrunk complex of the first kind

The shrunk complex of the first kind is associated with a color, and it allows one to visualize strings of that particular color. Consider, for example, the b-shrunk complex. The idea is that we want to keep only the b edges, whereas the g, r, and y edges get shrunk and disappear. To this end, we start by placing a vertex at each b cell and by connecting them through edges, which are in one to one correspondence with the b edges. Then, we have to place the faces of the new complex, and they correspond to the rg, ry, and gy faces. In particular, consider a rg face. It has b and g edges, but after the g edges are shrunk, only the b edges remain. Finally, we need cells. They come from g, r and y cells. In particular, consider a g cell. It has r, y, and b edges, but only the b edges are retained. Similarly, it has gb, gr, and gy faces, but we keep only the gb faces [see Figs. 7(c) and 8 for examples].

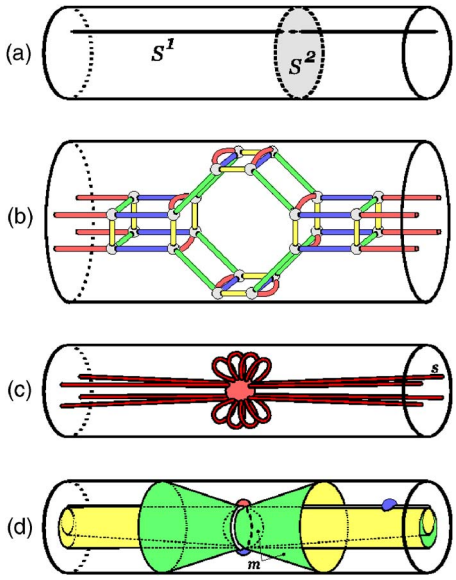


FIG. 7. (Color online) (a) A representation of the space $S^2\times S^1$. Each section of the solid tube is a sphere, and both ends of the tube are identified. (b) A 3-colex in $S^2\times S^1$. It consists of 24 vertices, twelve edges of each color, four br faces, eight by faces, six rg faces, four ry faces, four gy faces, two b cells, one r cell, three g cells, and two y cells. (c) The r-shrunk complex of the previous colex. The vertex corresponds to a r cell, and edges to r edges. An example of a closed string is the edge marked with an s. It has nontrivial homology. (d) The gy-shrunk complex of the previous colex. Vertices correspond to b and r cells, edges to rb faces, face to gy faces, and cells to g and y cells. An example of a closed membrane is a combination of the faces marked with an m. This membrane has nontrivial homology.

Now consider any path, closed or not, in the b-shrunk complex. We call such a path a b string. Recall that each edge of a shrunk complex corresponds to a b edge in the 3-colex. Thus, at the colex level, a b string is a collection of b edges that connect b cells [see Fig. 8(a)]. Each b edge contains two vertices. Then, to each b-string s, we can associate an operator $B_s^Z=\otimes_{i\in I_s}Z_i$, where I_s is the set of vertices lying in the string.

As shown in Fig. 8(b), the operator B_f^Z of a yr face corresponds to a closed b-string s. This string is the boundary of the corresponding face in the b-shrunk complex. As an operator, B_s^Z clearly commutes with the Hamiltonian and acts trivially on the ground state (6).

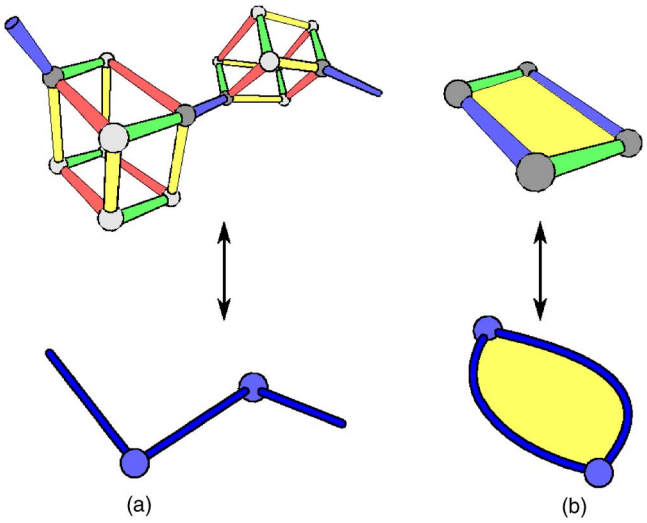


FIG. 8. (Color online) In this figure, the top represents part of a colex, and the bottom the corresponding portion of the b-shrunk complex. Vertices in the b-shrunk complex come from b-cells in the colex, edges from b-edges, faces from ry-, rg-, and gy-faces, and cells from r-, y-, and g-cells. (a) A b-string. In the colex, it is a collection of b-edges linking b-cells. In the b-shrunk complex, the path of edges can be clearly seen. (b) A ry-face corresponds to a face in the b-shrunk complex, and thus its boundary can be viewed as a b-string.

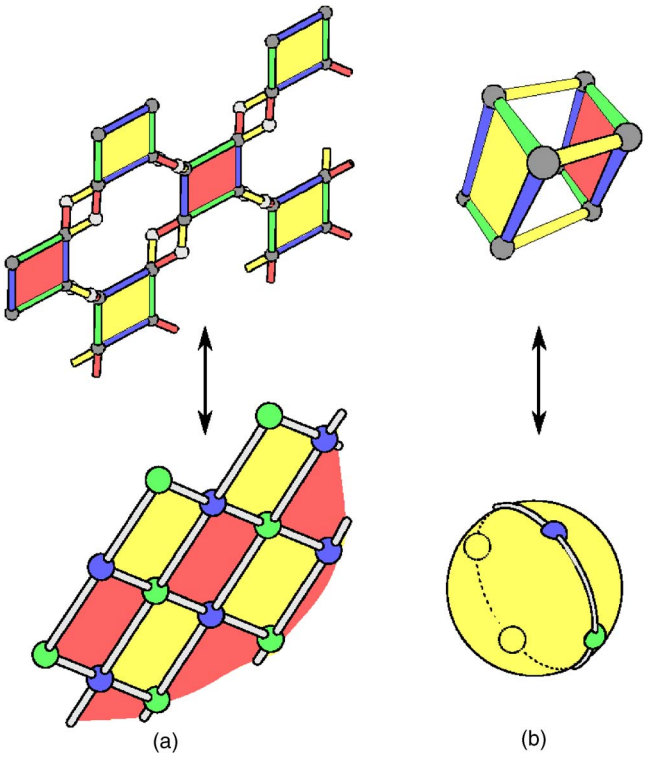


FIG. 9. (Color online) In this figure, the top represents part of a colex, and the bottom the corresponding portion of the ry-shrunk complex. Vertices in the ry-shrunk complex come from g and b cells in the colex, edges from gb faces, faces from ry faces, and cells from r and y cells. (a) An ry membrane. In the colex, it is a collection of ry faces linked by gb faces. In the ry-shrunk complex, the brane can be clearly seen. (b) An r cell corresponds to a cell in the ry-shrunk complex, and thus its boundary can be viewed as a ry membrane.

In fact, any closed string gives rise to a string operator that commutes with the Hamiltonian (4). If the string is homologous to zero, the corresponding string operator acts trivially on the ground state. In order to understand this, consider a closed red string homologous to zero. It must be a combination of boundaries of faces. Then, the string operator is the product of the operators of these faces. Similarly, the actions of two string operators derived from homologous strings of the same color are identical on the ground state. Therefore, it makes sense to label the string operators as S_μ^p, where p is a color and μ is a label denoting the homology of the string.

2. Shrunk complex of the second kind

The shrunk complex of the second kind is associated with two colors, and it allows the visualization of certain membranes, as we explain now. Let us consider, for example, the ry-shrunk complex. The idea is that we want to keep only the ry faces, whereas the rest of the faces get shrunk and disappear. This time, vertices correspond to b and g cells. Edges come from bg faces. A bg face lies between a g and a b cell, and the corresponding edge will connect the vertices coming from these cells. We have already mentioned that the faces of the ry-shrunk complex come from the ry faces in the colex, but we have to explain how they are attached. Observe that each ry face has a certain amount of adjacent gb faces. Here, for adjacent objects, we only mean that their intersection is not empty. In particular, there is a gb face at each of the vertices of the ry face. Then, the face in the complex has in its perimeter the edges coming from its adjacent gb faces. Finally, we have to consider cells, which come from r and y cells, and only keep their ry faces. So, in the boundary of a cell coming from a r cell, we see vertices from adjacent b and g cells, edges from adjacent bg faces, and faces from ry faces in the boundary of the r cell [see Figs. 7(d) and 9].

Now consider any membrane, that is, a connected collection of faces, closed or with a boundary, in the ry-shrunk complex. We call such a membrane m an ry membrane [see Figs. 7(d) and 9(a)]. We can associate an operator B_m^X with it. It is the product of the B_f^X operators of the corresponding ry faces in the colex.

As shown in Fig. 9(b), the operator B_c^X of an r-cell c corresponds to a closed ry-membrane m. This membrane is the boundary of the corresponding cell in the ry-shrunk complex. As an operator, B_m^X clearly commutes with the Hamiltonian and acts trivially on the ground state (7).

In complete analogy with strings, any closed membrane gives rise to a membrane operator that commutes with the Hamiltonian. If the membrane is homologous to zero, then the corresponding membrane operator acts trivially on the ground state. Similarly, the actions of two string operators derived from homologous membranes of the same color are identical on the ground state, and we label membrane operators as M_μ^{pq}, where p and q are colors and μ is a label denoting the homology of the membrane.

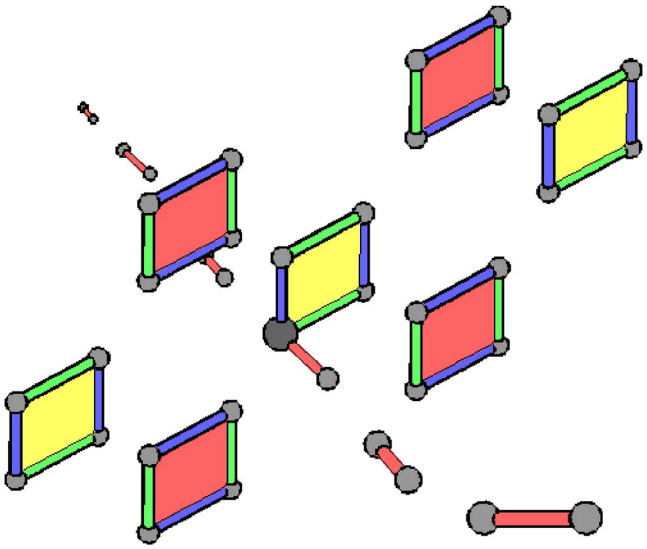


FIG. 10. (Color online) When an r string s crosses an ry membrane m, they meet at a vertex. In terms of string and membrane operators, this means that B_m^X and B_s^Z act in a common site.

3. Commutation rules

We will now consider the commutation rules between string and membrane operators. We first consider the case of a membrane and a string with no common color in their labels. As displayed in Fig. 9(a), a rg-membrane is made up of g and b edges. Then, for the same argument of Eq. (3), we have

$$\forall \mu, \nu, \quad [M_\mu^{rg}, S_\nu^b] = 0, \tag{8}$$

and analogously for any combination of three different colors. More interesting is the case in which there is a shared color. As displayed in Fig. 10, at each place where a p-string crosses a pq-membrane, they have a site in common. Thus, if the labels μ and ν are such that a ν string crosses a μ membrane an odd number of times, we have

$$\{M_\mu^{pq}, S_\nu^p\} = 0. \tag{9}$$

In another case, that is, if they cross an even number of times, the operators commute.

D. Ground state

We have discussed above how the action of string or membrane operators on the ground state depends only on their homology. It is in this sense that homologous strings or membranes give rise to equivalent operators. This equivalence, however, can be extended to take color into account, and we say that two membrane or string operators are equivalent if they are equal up to combinations with cell and face operators. Then, as we prove for general D in Appendix B, we have the following interplay between homology and color:

$$S_\mu^r S_\mu^g S_\mu^b S_\mu^y \sim 1, \tag{10}$$

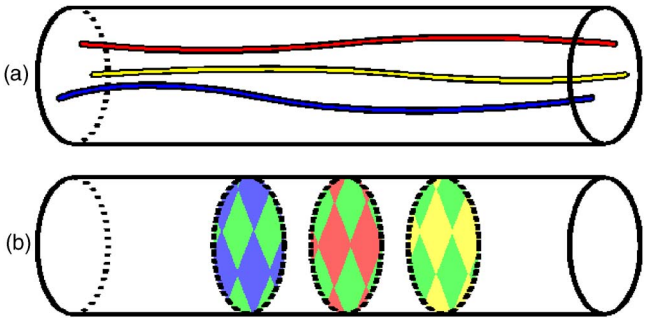


FIG. 11. (Color online) Here, we represent $S^2 \times S^1$ as in Fig. 7. In (a), a basis for nontrivial closed strings is shown. The other possible such string is green, but it is a combination of these ones (10). (b) A membrane basis in $S^2 \times S^1$. We have chosen a gb, a gr, and a gy membrane. There are three other nontrivial membranes, in particular, a br, a by and a yr membrane, but they are combinations of these ones (11).

$$M_\mu^{pq} M_\mu^{qo} M_\mu^{op} \sim 1, \tag{11}$$

where o, p, and q are distinct colors.

If we take all the r, g, and b strings for a given homology basis of 1-cycles, we obtain a complete set of compatible observables for the ground-state subspace: any other string operator is equivalent to a combination of these strings, and no membrane operator that acts nontrivially in the ground state can commute with all of them. This is, in fact, why number 3 appears in Eq. (5). As an example, a string basis in $S^2 \times S^1$ is displayed in Fig. 11(a).

Similarly, if we take all the ry, gy, and by membranes for a given homology basis of 2-cycles, we obtain a complete set of compatible observables for the ground-state subspace: any other membrane operator is equivalent to a combination of these membranes, and no string operator that acts nontrivially in the ground state can commute with all of them. A membrane basis in $S^2 \times S^1$ is displayed in Fig. 11(b).

Observe that only those string operators that have nontrivial homology, that is, which act in a global manner in the system, are capable of acting nontrivially in the ground state while living it invariant. This is the signature of a string condensate, as introduced in Ref. 49. Then, it would be tempting to let S_b be the set of all boundary strings and to try to write a ground state as

$$\sum_{s \in S_b} B_s^Z |\rightarrow\rangle^{\otimes |V|}, \tag{12}$$

where $|\rightarrow\rangle^{\otimes |V|}$ is the state with all spins pointing to the positive x direction. However, this fails. In fact, what we have is a *string-net condensate*[47] because, as indicated by Eq. (10), we can have branching points in which one string of each color meet. This means that the ground state is a superposition of all possible nets of strings, as depicted in Fig. 12. The correct way to write an example of a ground state is

$$\sum_{f \in F} (1 + B_f^Z) |\rightarrow\rangle^{\otimes |V|} =: \sum_{\text{string nets}} B_s^Z |\rightarrow\rangle^{\otimes |V|}. \tag{13}$$

We can state all of the above also in the case of membranes, and thus we should speak of a *membrane-net con-*

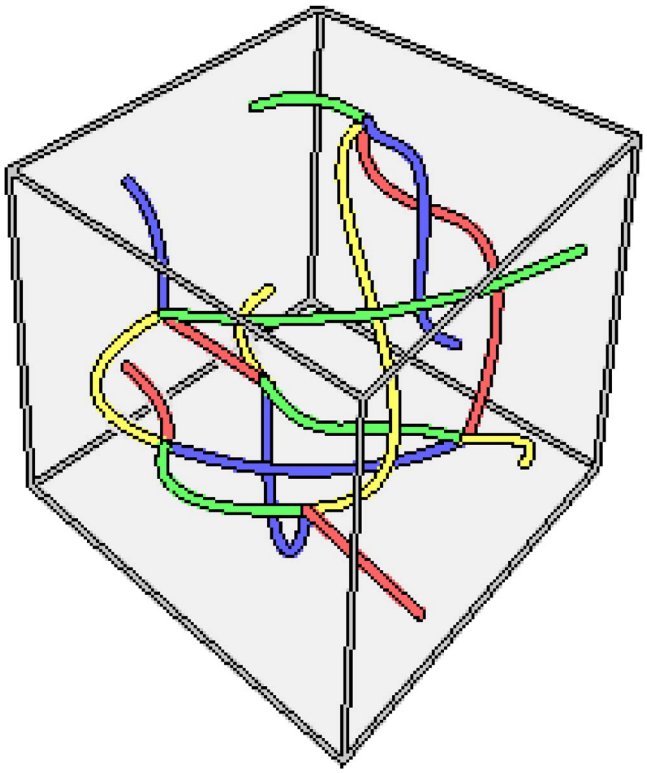


FIG. 12. (Color online) The ground state of the system is a string-net condensate. This picture represents in a 3-torus a typical element of the summation (13).

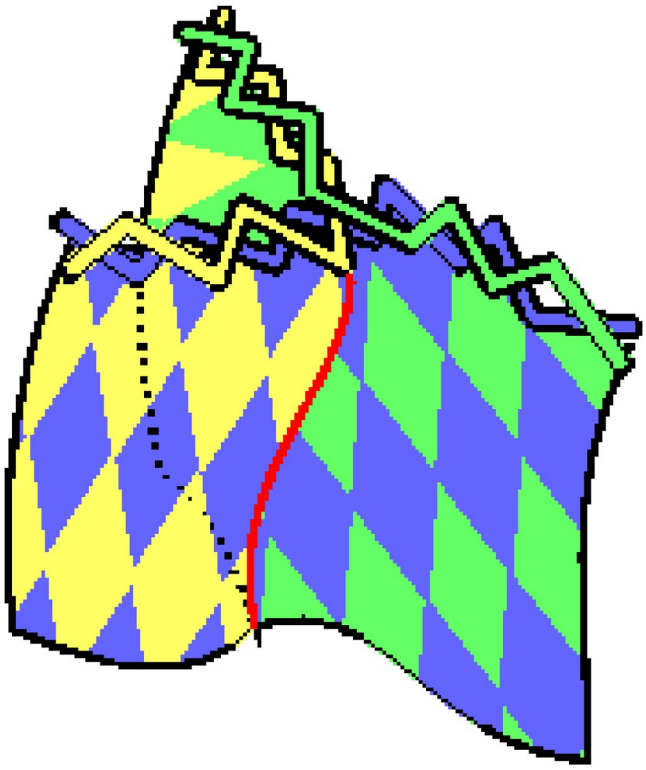


FIG. 13. (Color online) In a membrane net, different membranes can connect along common boundaries. This is related to the preservation of flux, as shown in this figure.

densate. An example of this is shown in Fig. 13. Interestingly enough, other topological orders in $D=3$ based on toric codes do not exhibit a condensation of membrane-nets.[49] It is a membrane condensate because only membranes with nontrivial homology can act nontrivially in the ground state. It is also a net because, for example, as indicated by Eq. (11), a *gr*, a *gb*, and a *br* membrane can combine along a curve. Then, if we let $|\uparrow\rangle^{\otimes|V|}$ denote the state with all spins up, the following is an example of a ground state:

$$\sum_{c\in C}(1+B_c^X)|\uparrow\rangle^{\otimes|V|} =: \sum_{\text{membrane nets}} B_m^X|\uparrow\rangle^{\otimes|V|}. \tag{14}$$

E. Excitations

We now focus on excitations from the point of view of string and membrane operators. We can have two kinds of excitations, depending on whether a cell or a face condition is violated. We start by considering excitations in r cells, for example. Let $|\psi\rangle$ be a ground state and S_{ij}^r an open string operator connecting the cells i and j. The state $S_{ij}^r|\psi\rangle$ is an excited state. The excitations live precisely at cells i and j, and we call them quasiparticles with an r-charge. Why should color be considered a charge? We have the following three constraints:

$$\prod_{c\in C_r} B_c^X = \prod_{c\in C_g} B_c^X = \prod_{c\in C_b} B_c^X = \prod_{c\in C_y} B_c^X, \tag{15}$$

where C_p is the set of p cells. They imply that the number of quasiparticles of each color must agree in their evenness or oddness. Therefore, if we want to create quasiparticles of a single color from the vacuum, we must create them in pairs, and so such a creation can be performed with an open string operator. Alternatively, four quasiparticles, one of each color, can also be created locally [see Fig. 14(b)]. For example, let $|\psi\rangle$ be a ground state and i any site. Then, the state $Z_i|\psi\rangle$ is a state with four quasiparticle excitations, one at each of the 3-cells that meet at site i. Observe that Eq. (15) is in agreement with Eq. (10).

Now let $|\psi\rangle$ be a ground state and M_b^{gy} a membrane operator which has a boundary ∂b. Recall that ∂b is a set of edges in the gy-shrunk complex that corresponds to a set of rb faces at the colex level. The state $M_b^{gy}|\psi\rangle$ is an excited state with excitations placed at the faces in ∂b. The excited segments, as viewed in the gy-shrunk complex, form a closed path. This introduces the idea of a gy flux in the boundary of the membrane, as illustrated in Fig. 15, for a

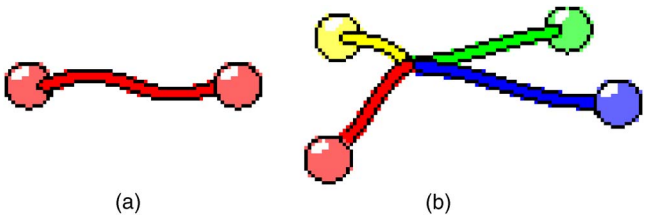


FIG. 14. (Color online) There are two ways in which quasiparticles can be created locally. We can create them either (a) by pairs of the same color forming a string or (b) in groups, one of each color forming a string net.

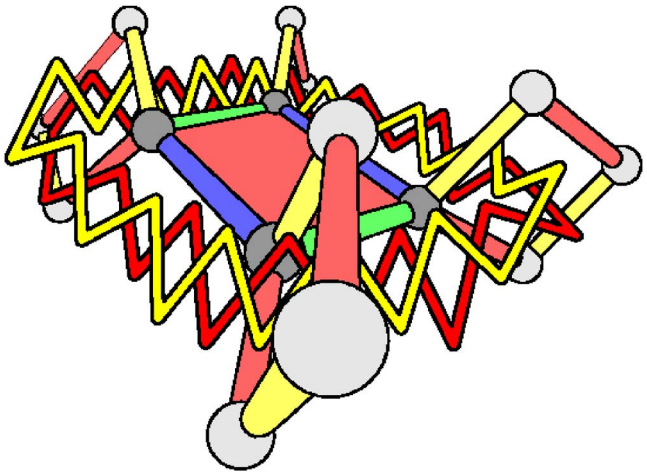


FIG. 15. (Color online) The flux excitation created with the membrane operator B_m^X of an ry membrane made up of a single ry face.

membrane with a single face. However, we have to check that this flux makes sense. Not only must it be conserved at any vertex in the gy-shrunk graph, but the existence of fluxes of other colors must also be considered. So take, for example, r-cell c. We have two constraints for the faces of c, analogous to those in Eq. (15) but in the subcolex that forms the boundary of c:

$$\prod_{f\in F_{rb}^c} B_f^Z = \prod_{f\in F_{rg}^c} B_f^Z = \prod_{f\in F_{rb}^c} B_f^Z, \tag{16}$$

where F_{pq}^c is the set of pq faces of cell c. These constraints guarantee that the gy flux is preserved at the corresponding vertex in the gy-shrunk complex. Additionally, Eq. (16) implies that a gy flux can split into a gb flux and a yb flux [see Fig. 16(b)]. This is, of course, in agreement with Eq. (11).

Fluxes can be analyzed from a different point of view. Let $|\psi\rangle$ be a ground state and i any site. Then the state $X_i|\psi\rangle$ is an excited state. We can visualize it as small p fluxes winding around the p edges incident at i, as shown in Fig. 16(c). Observe that the idea of a pq flux as something composed of a p flux and a q flux is also suggested by the flux splitting (16). Any flux configuration is a combination of these microfluxes at sites. In particular, the total flux through any closed surface must be null, and thus we cannot have, for example, an isolated rg flux in a loop which is not homologous to zero.

F. Winding quasiparticles around fluxes

In the theory of a topological order in two dimensions, it is known that quasiparticles show special statistics:[52,53] when a charge is carried around another one, sometimes the system gets a global phase, a behavior which bosons and fermions do not show. Which is the analogous situation in 3D? We can carry a charged particle along a closed path, which winds around a loop of flux, as in Fig. 17. If the system gets a global phase, then it makes sense to introduce the notion of branyons as the higher-dimensional generalization of the

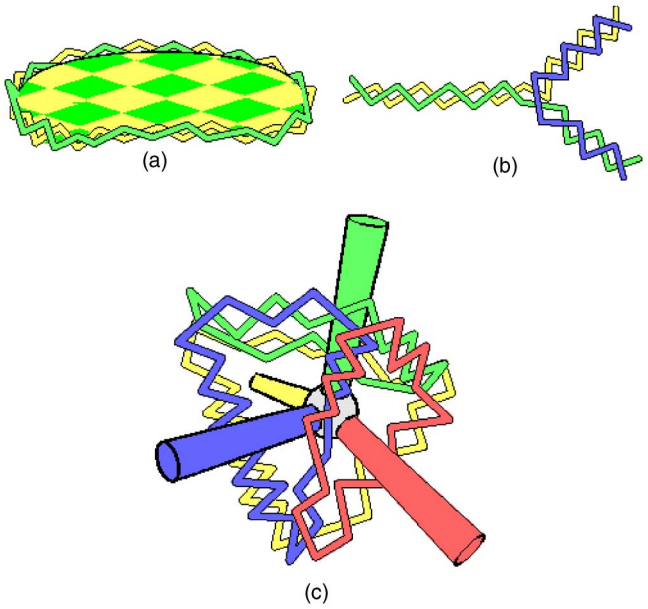


FIG. 16. (Color online) (a) The border of a gy membrane is a gy flux. (b) A gy flux can split into a gb flux and a by flux when it goes across an r cell (16). (c) The microfluxes at a given site, as explained in the text.

usual anyons. Thus, in the system at hand, we have 0-branyons (quasiparticles) and 1-branyons (fluxes). Higher-dimensional branyons will appear when we consider systems with $D \geqslant 4$.

In order to see the effect of winding a color charge around a color flux, we have to consider the closed string operator associated with the charge path and the membrane giving rise to the flux loop. If a p charge winds once around a pq flux, the system will get a global -1 phase because $\{M^{pq}, S^p\}=0$. Observe that this reinforces the idea of a pq flux as a composition of a p flux and a q flux. Other color combinations, i.e., those in which the string and the membrane do not share a color, give no phase.

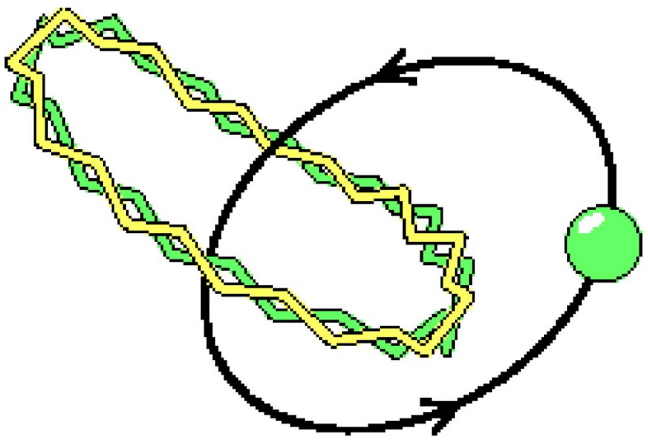


FIG. 17. (Color online) When a g charge winds around a loop of a gy flux, the system gets a global -1 phase. This is because the membrane operator giving rise to the flux and the string operator associated with the winding anticommute.

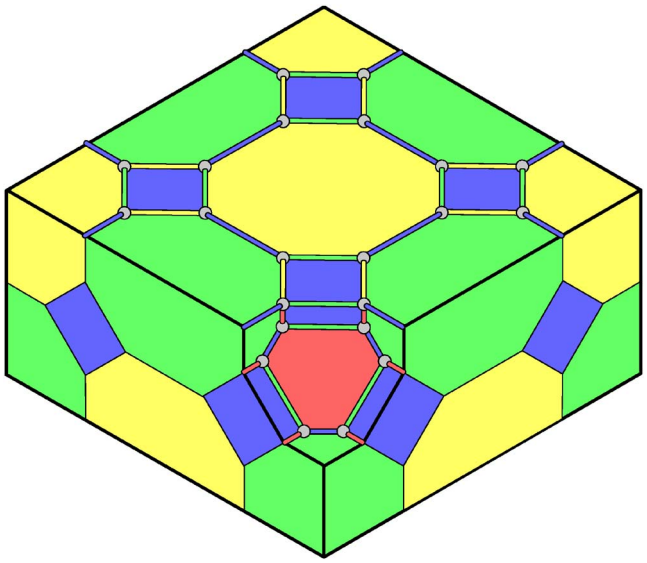


FIG. 18. (Color online) An example of a red surface, located at the boundary between the 3-colex and an erased big r cell. At a red surface, r strings can have end points without quasiparticles, and bg, gy, and by membranes can have borders without fluxes. These quasiparticles and fluxes would live precisely in the red cell that is missing. Note that a y cell was removed in the figure.

G. 3-manifolds with boundary

Up to this point, we have only considered systems contained in closed 3-manifolds. This is rather unphysical since such systems fill the whole space in which they exist, whereas any system that we can manipulate must be confined to a certain piece of space, and thus must have a boundary.

Fortunately, it is very easy to obtain manifolds with boundary from closed ones. In particular, it is enough to make holes. For example, by puncturing a 3-sphere, one obtains the usual three-dimensional Euclidean space. Of course, instead of erasing a single point, we can also remove open subsets. For example, by erasing an open ball from the 3-sphere, we get a closed ball.

How do we perform such erasures of open subsets in the case of 3-colexes? The most natural approach is to remove a certain number of cells and also all the vertices and edges that are not contained in any of the remaining cells. In doing so, we will certainly change the degeneracy of the ground state. For example, consider the 3-sphere, which gives no degeneracy. If we remove a pair of r cells, the resulting space is topologically equivalent to a thick spherical shell. In the new colex, r strings that connect both missing r cells will commute with the Hamiltonian, giving a twofold degeneracy. In general, after such a removal of cells, the new manifold will show several surfaces. We can attach a color to the surfaces, in particular, that of the cell that was removed to give that portion of the surface. Then, at a red surface, for example, r strings can have end points and bg, gy, and by membranes can have borders, whereas they still commute with the Hamiltonian. Figure 18 shows an example.

III. D COLEXES

In order to generalize the three-dimensional model to a higher dimension D, first we have to construct the underlying structure. That is, we want to define color complexes of arbitrary dimension. This section is devoted to the definition and basic properties of D colexes.

A. Definitions

First, we define color graphs or *c graphs*. A v-valent c graph is a graph Γ satisfying the conditions that (i) v edges meet at every vertex, (ii) edges are not loops, and (iii) edges are v colored. We mean by v colored that labels from a color set $Q=\{q_1,\ldots,q_v\}$ have been assigned to edges in such a way that two edges meeting at a vertex have different colors. This is a generalization of what we already saw in the $D=3$ case, as in Fig. 4. A c graph Γ' with color set Q' is a c subgraph of Γ if $\Gamma'\subset\Gamma$, $Q'\subset Q$, and the colorings coincide in common edges.

Now we introduce *complexes*. One can give to a D manifold a combinatorial structure by means of what is called a D complex. The idea is to divide the manifold in a hierarchy of objects of increasing dimension: points, edges, faces, solid spheres, etc. These objects are called n cells, $n=0,\ldots,D$. 0-cells are points, 1-cells are edges, and so on. The boundary of an n cell is an n sphere and is made up of cells of dimension $n'<n$. So, what we have is a D manifold constructed by gluing together the higher-dimensional analogs of the polyhedral solids that we considered in $D=3$ (recall Fig. 2).

A D colex is a complex in a D manifold which has $(D+1)$-colored edges in such a way that (i) its underlying lattice or graph is a $(D+1)$-valent c graph, (ii) the subgraph that lies on the boundary of any n cell for $n=2,\ldots,D$ is an n-valent c subgraph, and (iii) any connected c subgraph with valence $v=2,\ldots,D$ lies on the boundary of one unique v cell. Therefore, the point is that the c graph *completely* determines the cell structure and thus the whole topology of the manifold.

Some c graphs yield a colex, but not all of them. We define recursively this partially defined mapping from the space of $(D+1)$-valent c graphs to the space of closed D manifolds. First, any 2-valent c graph is a collection of loops. So, as a topological graph, it naturally yields a 1-manifold, namely, a collection of 1-spheres. Then, consider any 3-valent c graph. We construct a 2-complex starting with the corresponding topological graph or 1-complex. The idea is to list first all 2-valent c subgraphs, which are embeddings of S^1 in the 1-complex. Then, for each of these subgraphs, we attach a 2-cell, gluing its boundary to S^1. The resulting space is certainly a 2-manifold. It is enough to check a neighborhood of any vertex, but the one to one correspondence between cells and connected c subgraphs makes this straightforward. Then, we consider a 4-valent c graph. If not all of its 3-valent c subgraphs yield S^2, we discard it. Otherwise, we first proceed to attach 2-cells as we did for the 3-valent graph. Then, we list all 3-valent c subgraphs, which by now correspond to embeddings of S^2 in a 2-complex. At each of these spheres, we glue the surface of a solid sphere. The process can be continued in an obvious way, and thus in general a $(D+1)$-valent c graph yields a D colex if and only if all its D-valent c subgraphs yield S^D.

B. Examples

As a first example of a colex, consider the c graph composed of only two vertices, for any valence $v=D+1\geq 2$. An

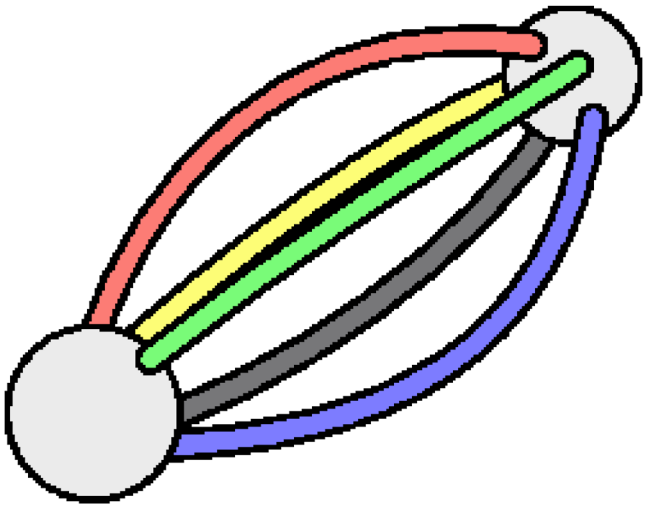


FIG. 19. (Color online) A c graph that yields a 4-sphere. It is the simplest possible 4-colex, with only two vertices.

example can be found in Fig. 19. This family of c graphs yields the spheres S^D. This can be visualized by viewing S^D as $\mathbf{R}^D$ plus the point at infinity. We can place one vertex at the origin and the other at infinity. Then, edges are straight lines that leave the origin in different directions.

The projective space P^D can also be described easily with a colex, though less economically in terms of vertices. Recall that P^D can be constructed by identifying opposite points of the boundary of a D-dimensional ball. The idea is to consider a D cube and to construct a D-valent c graph with its vertices and edges, coloring parallel edges with the same color. Then, we add 2^{n-1} extra edges to connect opposite vertices, and we give them a new color. The resulting c graph yields P^D. See Fig. 5 for an example of the case $D=3$.

In Appendix A, we give a procedure to construct colexes from arbitrary complexes. This guarantees that we can construct our topologically ordered physical system in any closed manifold with $D \geqslant 2$.

C. *R*-shrunk complex

This section is devoted to the construction of several new complexes from a given colex. These constructions will be essential to the understanding of the physical models to be built. In particular, as we learned in the $D=3$ case, only at the shrunk complex level will it be possible to visualize neatly the branes that populate the system. Shrunk complexes also provide us with several relations among the cardinalities of the sets C_n of n cells, which in turn will be essential in calculating the degeneracy of the ground state. These relations are based on the Euler characteristic of a manifold, a topological invariant defined in a D complex as

$$\chi := \sum_{n=0}^{D} (-1)^n |C_n|. \tag{17}$$

Before starting with the construction, it is useful to introduce the notion of the Poincaré dual of a complex $\mathcal{C}$ in a D manifold. The dual complex $\mathcal{C}^*$ is obtained by transforming the n cells of $\mathcal{C}$ in $(D-n)$ cells and by inverting the relation being-the-boundary-of. This means that if a certain $(n-1)$ cell c' is in the boundary of the n cell c in $\mathcal{C}$, then c^* is in the boundary of c'^* in $\mathcal{C}^*$.

We say that a cell is a R-cell if its c graph has as color set R. Note that this notation is different from the one we used in $D=3$, but it is more suitable for high D. What was before a gy membrane will now be a $\{r,b\}$ brane, or more simply a br brane, and so on.

Consider a D colex $\mathcal{C}$ with color set Q. We want to construct its R-shrunk complex $\mathcal{C}_R$, where R is a nonempty proper subset of Q, $\emptyset \subsetneq R \subsetneq Q$. What we seek is a new complex in which only R-cells remain, whereas the rest of the $|R|$-cells disappear. This construction is accomplished by a partial Poincaré dualization of cells. We already saw examples of this construction in $D=3$. Due to the different notation, what was called a gy-shrunk complex now will be called a rb-shrunk complex.

The R-shrunk complex has two main sets of cells. The first one corresponds to the cells in the set

$$S_1 := \bigcup_{R \subseteq S \subsetneq Q} C_S, \tag{18}$$

where C_S is the set of S cells. Cells in S_1 keep their dimension and the relation being-the-boundary-of among them. The second cell set is

$$S_2 := \bigcup_{\bar{R} \subseteq S \subsetneq Q} C_S, \tag{19}$$

where $\bar{R}$ is the complement of R in Q,

$$\bar{R} := Q - R. \tag{20}$$

Cells in S_2 get dualized. This means that an n cell in the colex will be a $(D-n)$ cell in the R-reduced complex. The relation being-the-boundary-of is inverted among the cells in S_2. So, S_2 provides us with cells of dimensions $0,\ldots,|R|-1$ and S_1 with cells of dimensions $|R|,\ldots,D$. Up to dimension $|R|-1$, the construction is clear, but we have to explain how to attach the cells in S_1. To this end, we observe that the intersection of an n-cell in S_1 and an R cell is either empty or a cell of dimension $n'=n-|\bar{R}|$. The n cell gives rise to a cell of dimension $D-n=|R|-1-n'$. Thus, the partial dualization is, in fact, a complete dualization, as seen on the boundary of any R cell, and the attachment of each R cell is then naturally described by this dualization process, as shown in Fig. 20. For the cells coming from S cells with $R \subsetneq S$, the attachment can be described recursively. The boundary of these cells is a $(|S|-1)$-colex, so we can obtain its R-shrunk complex and use it as the new boundary for the cell. In fact, what we are doing is a projection of the shrinking process in the boundary of the cell. Figure 21 displays examples of shrunk complexes for $D=2$.

The Euler characteristic for a R-shrunk complex is

$$\chi = \sum_{R \subseteq S \subsetneq Q} (-1)^{|S|} |C_S| + \sum_{\bar{R} \subseteq S \subsetneq Q} (-1)^{D-|S|} |C_S|. \tag{21}$$

If we sum up all such equations for all different color combinations but for a fixed cardinality $|R|=r$, we get

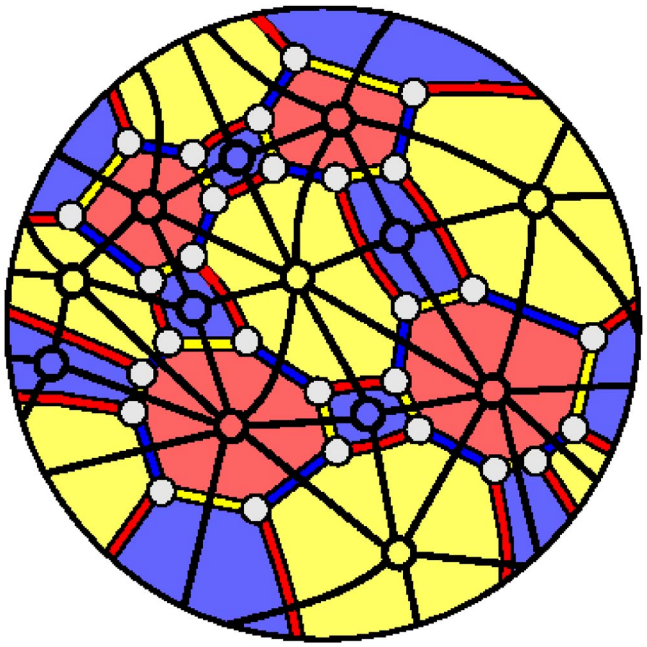


FIG. 20. (Color online) A *bry* cell belonging to some D colex with $D \geqslant 3$. We show superimposed in black thick line the structure of its dual boundary, which plays an important role when constructing the *bry*-shrunk complex.

$$\binom{D+1}{r}\chi = \sum_{n=r}^{D} (-1)^n \binom{n}{r} |C_n| + \sum_{n=0}^{r-1} (-1)^n \binom{D-n}{D-r+1} |C_{D-n}|. \tag{22}$$

The case $r=0$ is also included since it reduces to the definition of χ. The right-hand side (rhs) in the cases $r=s$ and $r=D-s+1$ are equal except for the sign, so that we get

$$\chi = (-1)^D \chi. \tag{23}$$

Of course, it is a well-known fact that χ vanishes in manifolds of odd dimension. In these cases in which $D=2k+1$, Eq. (22) for $r=k+1$ vanishes identically. So, in general, we have $\lceil D/2 \rceil$ independent relations. They tell us that the cardinalities $|C_0|, \ldots, |C_{\lfloor D/2 \rfloor}|$ depend on the cardinalities $|C_{\lfloor D/2+1 \rfloor}|, \ldots, |C_D|$, which shows quantitatively the fact that colexes are much more "rigid" than more general complexes.

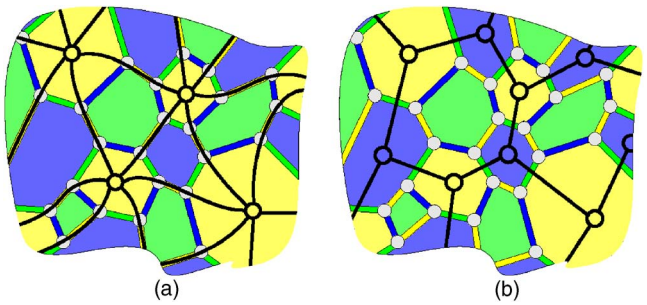


FIG. 21. (Color online) This figure shows the two possible kinds of shrunk complex in a 2-colex. The shrunk complexes appear superimposed in black thick line to the original colex. In (a), the *y*-shrunk complex is shown, and in (b) the *by*-shrunk complex.

IV. THE MODEL IN D-MANIFOLDS

A. System and Hamiltonian

We now associate a physical system with a D-colex structure in a D-manifold, $D \geqslant 2$. To this end, we place at each vertex (site) a spin-$\frac{1}{2}$ system. To each n-cell c, we can attach the cell operators

$$B_c^\sigma := \bigotimes_{i \in I_c} \sigma_i, \quad \sigma = X, Z, \tag{24}$$

where X_i and Z_i are the Pauli σ_1 and σ_3 matrices acting on the spin in the vertex i and I_c is the set of vertices lying on cell c. In order to generalize the Hamiltonian (4), we need sets of cells such that their X and Z operators commute. However, we have the following result. For every n-cell c_n and m-cell c_m with $n+m > D+1$,

$$[B_{c_n}^X, B_{c_m}^Z] = 0. \tag{25}$$

This is a consequence of the fact that c_n and c_m have colexes with at least one color in common because they have respectively $p+1$ and $(q+1)$ colors. Then, their intersection is a colex of valence of at least 1, and thus contains an even number of sites.

From this point on, we choose fixed integers $p, q \in \{1, \ldots, D-1\}$ with

$$p + q = D. \tag{26}$$

The Hamiltonians that we propose are

$$H_{p,q} = -\sum_{c \in C_{p+1}} B_c^Z - \sum_{c \in C_{q+1}} B_c^X. \tag{27}$$

Again, color plays no role in the Hamiltonian. It is an exactly solvable system, and the ground state corresponds to a quantum error correcting code with cell operators as stabilizers.[54] We give a detailed calculation of the degeneracy in Appendix C. The degeneracy is 2^k with

$$k = \binom{D}{p} h_p = \binom{D}{q} h_q, \tag{28}$$

where $h_p = h_q$ is the pth Betty number of the manifold. The ground states $|\psi\rangle$ are characterized by the conditions

$$\forall c \in C_{p+1}, \quad B_c^Z |\psi\rangle = |\psi\rangle, \tag{29}$$

$$\forall c \in C_{q+1}, \quad B_c^X |\psi\rangle = |\psi\rangle. \tag{30}$$

Those eigenstates $|\psi'\rangle$ for which some of these conditions are violated are excited states. As in the $D=3$ case, excitations have a local nature and we have a gapped system.

For $D \geqslant 4$, different combinations of the parameters (p, q) are possible. Each of these combinations gives rise to different topological orders, thus making transitions between them possible. For example, in $D=4$, the Hamiltonian

$$H = H_{1,3} + \lambda H_{2,2} \tag{31}$$

exhibits a topological phase transition as λ is varied.

The Hamiltonian in Eq. (31) is not exactly solvable, while $H(1,3)$ and $H(2,2)$ are exactly solvable separately, by construction. The reason is that the sets of face operators B_f^Z and cell operators B_c^X of type (1,3) do not commute with the corresponding sets of operators of type (2,2).

The Hamiltonian H does not have an exact topological order for arbitrary values of the coupling constant λ; only at the weak coupling $\lambda \ll 1$ or strong coupling $\lambda \gg 1$ does it show a topological order of a different type. As the coupling is varied, we connect two different topological phases, but the whole line in λ is not necessarily topological.

Now that we have seen this mechanism for producing topological quantum phase transitions with colexes in the simplest case, we can extend it to arbitrary dimensions $D \geqslant 4$ by introducing the following set of Hamiltonians:

$$H_D = \sum_{p,q:p+q=D} \lambda_{p,q} H_{p,q}, \tag{32}$$

where the Hamiltonians $H_{p,q}$ are given by Eq. (27). As the coupling constants $\lambda_{p,q}$ are varied and meet the topological points characterized by $\lambda_{p,q}=0$, $\forall p$, $q \neq p_t$, q_t, $\lambda_{p_t,q_t}=1$, we find again examples of topology-changing phase transitions.

B. Branes

In analogy with the string and membranes that appeared in the $D=3$ case, here we have to consider p branes. We mean by a p brane an embedded p manifold, closed or with a boundary. A p brane is homologous to zero when it is the boundary of a $p+1$ brane. Then, two p branes are homologous if the p brane obtained by their combination is homologous to zero.

Let Q be the set of colors of the D colex. Then, for any nonempty set $R \subsetneq Q$, a R brane is a collection of R cells. It can be truly visualized as a $|R|$-brane in the R-shrunk complex. There, we also see that its boundary corresponds to $\bar{R}$ cells. Let b be an R brane and C_b its set of R cells. Then, we can attach to b operators $B_b^\sigma := \Pi_{c \in C_b} B_c^\sigma$ for $\sigma = X, Z$. Suppose, in particular, that $|R|=p$ and let b be a closed R brane. Then, B_b^Z commutes with the Hamiltonian. If this were not the case, there would exist a $(q+1)$ cell, particularly an $\bar{R}$ cell c, such that $\{B_b^Z, B_c^X\}=0$. However, in that case, in the R-shrunk complex, the p brane would have a boundary at the cell coming from c. Similarly, closed q-brane X operators also commute with the Hamiltonian.

The operator B_c^Z of a $(p+1)$ cell c with color set $R \cup \{r\}$, $r \in Q-R$, is a closed R-brane. As the R-shrunk complex reveals, it corresponds to the boundary of c. B_c^Z acts trivially in ground states (29), and the same holds true for any closed p-brane homologous to zero since it is a combination of such operators B_c^Z. This is not the case for closed p branes, which are not homologous to zero, and thus they act nontrivially in the ground state.

1. Equivalent branes

It is natural to introduce an equivalence among those operators of the form $\otimes_{v \in V} Z_v^{i_v}$, where V is the set of vertices of the colex and $i_v \in \{0,1\}$. We say that two such operators O_1 and O_2 are equivalent, $O_1 \sim O_2$, if $O_1 O_2$ is a combination of $(p+1)$ cell operators B_c^Z. This induces an equivalence among p branes since they have such an operator attached. In fact, two R branes, b and b', with $|R|=p$, are equivalent if and only if they are homologous. Observe that two equivalent p brane Z operators produce the same result when applied to a ground state. This motivates the introduction of the notation P_μ^R, $|R|=p$, for any operator B_b^Z, with b a R brane with homology labeled by μ.

Likewise, we can introduce an equivalence among those operators of the form $\otimes_{v \in V} X_v^{i_v}$, just as we have done for Z operators. This induces an equivalence relation among q branes, and we use the notation Q_ν^R, $|R|=q$, for any q-brane operator B_b^X, with b an R brane with homology labeled by ν.

In Appendix B, we show that for any color set $R \subset Q$ with $|R|=p-1$,

$$\prod_{r \in Q-R} P_\mu^{rR} \sim 0, \tag{33}$$

where rR is a shorthand for $\{r\} \cup R$. Similarly, if $|R|=q-1$,

$$\prod_{r \in Q-R} Q_\mu^{rR} \sim 0. \tag{34}$$

These relations generalize Eqs. (10) and (11). They give the interplay between homology and color, and show that for each homology class only $\binom{D}{p}$ color combinations are independent, those which can be formed without using one of the $D+1$ colors. This is why a combinatorial number appears in the degeneracy of the ground state. The other factor, h_p, follows from the fact that a homology basis for p-branes has h_p elements. By using the theory of quantum stabilizer codes,[54] one can see that by selecting a basis for p-branes with labels $\mu=1,\ldots,h_p$ and a color r, we can form a complete set of observables $\{P_\mu^R\}_{\mu,R \ni r}$.

2. Commutation rules

In general, for suitable color sets R,S, we have

$$R \cap S \neq \emptyset \Rightarrow [P_\mu^R, Q_\nu^S] = 0. \tag{35}$$

This follows from the same reasoning used in Eq. (25). We now explore the situation when R and S have no color in common. Consider a basis $\{p_\mu\}$ for closed p-branes. Consider also a basis for q-branes $\{q_\nu\}$, chosen so that p_μ and q_ν cross once if $\mu=\nu$ and do not cross in other cases. Then,

$$R \cap S = \emptyset \Rightarrow P_\mu^R Q_\nu^S = (-1)^{\delta_{\mu,\nu}} Q_\mu^S P_\nu^R. \tag{36}$$

This can be reasoned without resorting to the geometrical picture. Suppose that $[P_\mu^R, Q_\mu^S]=0$ and let $R=R' \cup \{r\}$, $Q-R-S=\{q\}$. From Eq. (33), we have $[\Pi_{r'} P_\mu^{R'r'}, Q_\mu^S]=0$. Then, Eq. (35) implies $[P_\mu^{Rq}, Q_\mu^S]=0$, and thus we have a homologically nontrivial q-brane X operator that commutes with all the p-brane Z operators. This being impossible, the assumption is necessarily false.

C. Excitations

There are two kinds of excitations, depending on whether a $(p+1)$-cell or a $(q+1)$-cell condition is violated. We label

excitations with the color set of the cell they live in. Although we focus on the violation of $(q+1)$ cells, the situation is analogous for $(p+1)$ cells.

Let $|\psi\rangle$ be a ground state and b an R brane, $R\subset Q$, $|R|=p$. We first observe that b has a boundary in the R-shrunk complex at the cell corresponding to the $\bar{R}$ cell c if and only if

$$\{P_b^R, B_c^X\} = 0. \tag{37}$$

However, $B_b^Z|\psi\rangle$ has $\bar{R}$ excitation exactly at those cells fulfilling Eq. (37). This means that the excitation produced by the p brane b has the form of a $p-1$-brane, precisely the boundary of b, ∂b.

Consider the particular case $p=1$. The excitations living at D-cells are, as in the $D=3$ case, quasiparticles (anyons) with color charge. In a connected manifold, we have D constraints generalizing Eq. (15). They have the form

$$\prod_{c\in C_R} B_c^X = \prod_{c\in C_S} B_c^X, \tag{38}$$

where $|R|=|S|=D$ and C_R is the set of R cells. These relations imply that the number of particles of each color must agree in their parity. Therefore, from the vacuum, we can create pairs of particles of a single color or groups of $D+1$ particles, one of each color. This is completely analogous to $D=3$.

Now suppose that $p>1$. We have seen that excitations can be created as the boundary of a p brane. If, in particular, it is an R brane, then excitations live in $\bar{R}$ cells. It is natural to interpret these excitations as some kind of $(p-1)$-dimensional flux, an $\bar{R}$ branyon. Then, it must be conserved. In fact, for each $(q+2)$ cell c, we have the constraint

$$\prod_{c\in C_R^c} B_c^X = \prod_{c\in C_S^c} B_c^X, \tag{39}$$

where $|R|=|S|=q+1$ and C_R^c is the set of R cells lying on cell c. This is a generalization of Eq. (16) and is in agreement with Eq. (33).

Finally, as in the three-dimensional case, we can wind branyons around each other and sometimes get a global phase. Let $|R|=q+1$ and $|S|=p+1$. Then, when a R branyon winds around a S branyon, the system gets a global minus sign if and only if $|R\cap S|=1$, following the commutation rules (36).

V. CONCLUSIONS

In this paper, we have explored topological orders in $D=3$ by means of models for quantum lattice Hamiltonians constructed with spins $S=\frac{1}{2}$ located at lattice sites. These models are exactly solvable, and this is a feature that allows us to explore the quantum properties of the whole spectrum. The ground state is found to be in a string-net condensate or, alternatively, in a membrane-net condensate. This type of membrane-net condensation is an interesting feature of our models that does not appear in 3D toric codes. In dimensions higher than $D=3$, we have also extended the construction of our models and found brane-net condensation. As for excitations, they are either quasiparticles or a certain type of extended fluxes. These excitations show unusual braiding statistical properties similar to anyons in $D=2$, and we call them branyons since they involve extended objects associated with branes.

Another interesting result is the possibility of having a topology-changing transition between two topologically ordered phases that we find with our models in $D=4$. We may wonder whether it is possible to have a similar topology-changing process in dimension $D=3$ as in Eq. (31). One obvious way to achieve this is by using the construction in $D=4$ and flattening it into $D=3$, thereby reducing the dimensionality of the interaction but at the expense of losing the locality of the interaction.

A fully or completely topological order does not exist in $D=3$ dimensions, unlike in $D=2$. That is to say, a topological order that can discriminate among all the possible topologies in three-dimensional manifolds does not exist. We may introduce the notion of a topologically complete class of quantum Hamiltonians when they have the property that their ground-state degeneracy (and similarly for excitations) is different, depending on the topology of the manifold where the lattice is defined. From this perspective, we have found a class of topological orders based on the construction of certain lattices called colexes that can distinguish between 3D-manifolds with different homology properties. Homology is a topological invariant, but not enough to account for the whole set of topologically inequivalent manifolds in $D=3$. For instance, the famous Poincaré sphere is an example of a 3D-manifold that has the same homology as a 3-sphere. Poincaré was able to prove that the fundamental group (or first homotopy group) of this new sphere has the order 120. As the standard 3-sphere has a trivial fundamental group, it is different. Since then, many other examples of homology spheres that are different topological structures have been constructed. In this regard, we could envisage the possibility of finding a quantum lattice Hamiltonian, possibly with a non-Abelian lattice gauge theory, that could distinguish between any topology in three dimensions by means of its ground-state degeneracy. This would amount to solving the Poincaré conjecture with quantum mechanics.

From the viewpoint of quantum information, the topologically ordered ground states that we have constructed provide us with an example of topological quantum memory: a reservoir of states that are intrinsically robust against decoherence due to the encoding of information in the topology of the system.

ACKNOWLEDGMENTS

We acknowledge financial support from a PFI fellowship of the EJ-GV (H.B.), DGS grant under Contract No. BFM 2003-05316-C02-01 and INSTANS (M.A.MD.), and CAM-UCM grant under Ref. No. 910758.

APPENDIX A: HOW TO CONSTRUCT D COLEXES

We present a procedure to construct colexes in arbitrarily closed manifolds. The idea is to start with an arbitrary com-

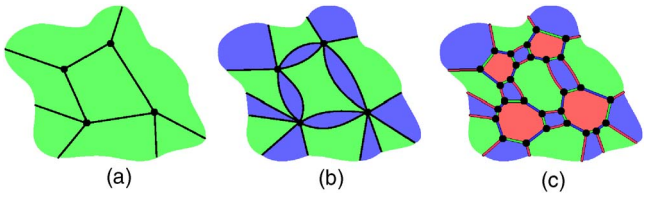


FIG. 22. (Color online) This figure explains a process that converts an arbitrary 2-complex on a surface into a 2-colex. In (a), green color is given to all the 2-cells of the 2-complex. In (b), 1-cells are inflated to give blue 2-cells. Finally, in (c), 0-cells are inflated to give red 2-cells, and 1-cells are accordingly colored.

plex and inflate its cells until a colex is obtained. We now explain the process in detail. It is illustrated in Fig. 22.

First, we have to state what we mean by inflating an n cell, $0 \leqslant n \leqslant D$. The idea is to keep the boundaries of the cell untouched but to inflate all other points in order to obtain a D-cell. For each $(n+l)$ cell that belongs to the boundary of the inflated cell, we must introduce an $(n+l-1)$ cell. The inflation of cells of the same dimension can be performed in any order, and all the cells must be inflated. Inflation starts with $(n-1)$ cells, then continues with $(n-2)$ cells, and so on, until 0-cells are inflated in the end.

We can prove that this procedure gives a D colex by an inductive argument. We will need some facts. First, we observe that the D cells of a D colex can be labeled with the unique color, which its subcolex does not contain. Conversely, if we can color the D cells of a D colex with $D+1$ colors in such a way that neighboring cells have different colors, then we can color edges according to the D cells they connect. Note also that for each cell in the original D complex, the inflated one has a D cell. This means that we can label inflated D cells with the dimension of the cell in the original complex.

Finally, we proceed with the proof. The case $D=1$ is trivial. We suppose that the procedure works for D manifolds, and we check it for $(D+1)$ manifolds. To this end, consider the boundary of any inflated $(D+1)$ cell which comes from the inflation of a 0-cell. Imagine all the inflation processes projected into this (fixed) D sphere. In the beginning, we can see a complex in this sphere. Its vertices correspond to edges that cross the surface, edges to faces that cross it, and so on. As the inflation proceeds in the original complex, the projected complex is also inflated. When 1-cells are inflated, the projected complex has become a D colex because of the induction hypothesis. Thus, it can be properly colored. Moreover, we can perform the coloring on its D cells using the labels attached to the corresponding $(D+1)$ cells in the inflated $(D+1)$ complex. From this coloring, we deduce a coloring for the edges of the D colex. In fact, all this is true for each of the subgraphs on the surfaces of $(D+1)$ cells obtained by inflation of 0-cells. Finally, we give a different color to the edges that are not contained in these surfaces. Checking that this coloring gives the desired properties that make the complex a colex is now easy.

APPENDIX B: BRANE COMBINATION

Consider a D colex with color set Q. Let b_R be a closed R brane, $\emptyset \subsetneq R \subsetneq Q$. It is the purpose of this section to show that for any $r \in R$, there exists a family of closed $|R|$ branes b_S homologous to B_R such that

$$B^{\sigma}_{b_R} = \prod_S B^{\sigma}_{b_S}. \tag{B1}$$

The sum extends over all $S \subset \bar{r} := Q - \{r\}$ with $|S| = |R|$.

We first consider the case $R=\{r\}$. Then, b_R is a string. It consists of r edges that link $\bar{R}$ cells. $B^{\sigma}_{b_R}$ acts nontrivially in an even number of vertices per $\bar{R}$ cell. Thus, we can gather them together in pairs and connect them through a path which only contains edges with colors in $Q-R$. Then, for each $s \in Q-R$, the set of all s edges we have used forms a string b_S, $S=s$. Then, certainly, Eq. (B1) holds true and each string b_S is closed because the rhs commutes with operators from $\bar{S}$ cells, and so does the left-hand side (lhs).

Now consider the case $|R|>1$. Let $\tilde{r} := R-\{r\}$. Consider the restriction of $B^{\sigma}_{b_R}$ to any $\bar{r}$-cell c, denoted as B^{σ}_{b}. This operator corresponds to a closed $\tilde{r}$ brane b in the $(D-1)$ colex that forms the boundary of c. Since this colex is a sphere, b is a boundary and thus B^{σ}_{b} is a combination of $|R|$ cells. As we did for strings, we can do this for every $\bar{r}$ cell, gather cells together by color and form the required closed $|R|$ branes.

APPENDIX C: DEGENERACY OF THE GROUND STATE

In the theory of quantum error correcting codes, the ground state of the Hamiltonian (27) is called a stabilizer code.[54] Thus, the theory of stabilizer codes naturally fits in the study of degeneracy, but we will avoid using its language although this makes the exposition less direct.

The ground state of the Hamiltonian (27) is the intersection of subspaces of eigenvalue 1 of $(p+1)$-cell and $(q+1)$-cell operators, as expressed in Eqs. (29) and (30). This subspace has an associated projector, which in turn will be the product of the projectors onto each of the subspaces of eigenvalue 1:

$$\prod_{c \in C_{p+1}} \frac{1}{2}(1 + B^{Z}_{c}) \prod_{c \in C_{q+1}} \frac{1}{2}(1 + B^{X}_{c}). \tag{C1}$$

Each of these projectors reduces the dimension of the space by half, but not all of them are independent because certain relations among cell operators exist. For $(p+1)$ cells, these relations have the form

$$\prod_{c \in C_{p+1}} (B^{Z}_{c})^{i_c} = 1, \tag{C2}$$

where $i_c = 0, 1$. Analogous relations exist for $(q+1)$ cells:

$$\prod_{c \in C_{q+1}} (B^{X}_{c})^{i_c} = 1. \tag{C3}$$

If the number of spins is n and the number of independent projectors is l, then the degeneracy of the ground state will be 2^k, with $k=n-l$. Suppose that the number of independent relations of type (C2) is l_1 and that for relations (C3) is l_2. Then, we have $l = |C_{p+1}| - l_1 + |C_{q+1}| - l_2$. Our starting point is then the equation

$$k = |C_0| - |C_{p+1}| - |C_{q+1}| + I(D,p+1) + I(D,q+1), \tag{C4}$$

where $n=|C_0|$ is the number of sites and $I(D,s)$ is the number of independent relations among s cells in a D colex.

$I(D,s)$ only depends on the cardinalities of cell sets $|C_i|$ and the Betty numbers of the manifold h_i, as we will show by calculating its value recursively. First, we note that

$$I(D,D) = dh_0 \tag{C5}$$

because the unique independent relations in this case are those in Eq. (38), for each connected component. For $s<D$, a relation between cells has the general form

$$\prod_{|S|=s} \prod_{c \in D_S} B_c^{\sigma} = 1, \tag{C6}$$

where $D_S \subset C_S$. Let $r \in Q$ be a color. If we only consider those relations that include color sets $R \subset \bar{r}$, we effectively reduce the problem by one dimension. By gathering together all such relations that appear in $\bar{r}$ cells, we get a total count of

$$I_{\bar{r}}(D,s) = I(D-1,s)\big|_{h_0=h_D=|C_{\bar{r}}|, h_{i\neq 0,D}=0}. \tag{C7}$$

Since the rhs of Eq. (C6) commutes with any cell operator, the relation has the form

$$\prod_{|S|=s} B_{b_S}^{\sigma} = 1, \tag{C8}$$

where b_S is a *closed* S-brane b_S. Then, consider any such relation in which a R-brane b_R appears with $r \in R$. If we have at hand all the relations of the form (B1), we can use them to eliminate the term b_R in Eq. (C8). This can be done for every such R, until a relation containing only colors in $\bar{r}$ is obtained. Therefore, our next task is to count how many of the relations (B1) are independent for each R.

Suppose then that we have a relation of the form (B1) that follows from other t relations of the same form (but not from a subset of them):

$$B_{b_{R,i}}^{\sigma} = \prod_{S} B_{b_{S,i}}^{\sigma}, \quad i = 1, \ldots, t. \tag{C9}$$

Then, for the lhs of the relations, the following is true:

$$B_{b_R} = \prod_{i=1}^{t} B_{b_{R,i}}. \tag{C10}$$

Since all the branes that appear in Eq. (B1) are R branes, the equation can be interpreted in terms of Z_2 chains of $|R|$ cells in the R-shrunk complex. It states that $b_R = b_{R,1} + \cdots + b_{R,t}$. The argument can be reversed; any such dependence between $|R|$ cycles in the R-shrunk complex corresponds to a dependence among relations of the form (B1).

Therefore, counting the number of independent relations of the form (B1) for a given R amounts to counting the number of independent $\mathbf{Z}_2$ chains of closed $|R|$ cycles in the R-shrunk complex. For $|R|=s$, this number is

$$S(D,s) = \sum_{i=0}^{n-s} (-1)^i h_{s+i} + \sum_{i=1}^{n-s} (-1)^i |C_{s+i}|. \tag{C11}$$

This follows by recursion. $S(D,D)=h_0$ and $S(D,s)=h_{D-s} + [|C_{s+1}| - S(D,s+1)]$.

We have to consider all the possible sets R in which r is contained:

$$I_r(D,s) = \sum_{\substack{R \ni r \\ |R|=s}} S(D,s)\big|_{R\text{-shrunk}}. \tag{C12}$$

Then,

$$I(D,s) = I_{\bar{r}}(D,s) + I_r(D,s), \tag{C13}$$

which can be solved and gives

$$I(D,s) = \binom{D}{s-1} \sum_{i=0}^{D-s} (-1)^i h_{s+i} + \sum_{i=0}^{D-s-1} \binom{s+i}{s-1} (-1)^i |C_{s+i+1}|. \tag{C14}$$

Now recall Eq. (22). We can sum up these equations for $r=0,\ldots,s$ with an alternating sign $(-1)^r$. Using the fact that

$$\sum_{i=0}^{a} \binom{b+1}{i} (-1)^i = (-1)^a \binom{b}{a}, \tag{C15}$$

we get

$$\binom{D}{s}\chi = (-1)^s C_0 + \sum_{i=0}^{s-1} \binom{D-i-1}{D-s} (-1)^i |C_{D-i}| + \sum_{i=r+1}^{D} \binom{i-1}{s} (-1)^i |C_i|. \tag{C16}$$

By gathering together Eqs. (C4), (C14), and (C16), we finally obtain Eq. (28).

[1] L. D. Landau, Phys. Z. Sowjetunion **11**, 26 (1937).

[2] V. L. Ginzburg and L. D. Landau, Zh. Eksp. Teor. Fiz. **20**, 1064 (1950).

[3] X.-G. Wen, *Quantum Field Theory of Many-body Systems* (Oxford University Press, 2004).

[4] X.-G. Wen and Q. Niu, Phys. Rev. B **41**, 9377 (1990).

[5] X.-G. Wen, Int. J. Mod. Phys. B **4**, 239 (1990).

[6] X.-G. Wen, Int. J. Mod. Phys. B **6**, 1711 (1992).

[7] A. Kitaev and J. Preskill, Phys. Rev. Lett. **96**, 110404 (2006).

[8] M. Levin and X.-G. Wen, Phys. Rev. Lett. **96**, 110405 (2006).

[9] B. Blok and X.-G. Wen, Phys. Rev. B **42**, 8145 (1990).
[10] N. Read, Phys. Rev. Lett. **65**, 1502 (1990).
[11] J. Froöhlich and T. Kerler, Nucl. Phys. B **354**, 369 (1991).
[12] D. S. Rokhsar and S. A. Kivelson, Phys. Rev. Lett. **61**, 2376 (1988).
[13] N. Read and B. Chakraborty, Phys. Rev. B **40**, 7133 (1989).
[14] R. Moessner and S. L. Sondhi, Phys. Rev. Lett. **86**, 1881 (2001).
[15] E. Ardonne, P. Fendley, and E. Fradkin, Ann. Phys. (N.Y.) **310**, 493 (2004).
[16] V. Kalmeyer and R. B. Laughlin, Phys. Rev. Lett. **59**, 2095 (1987).
[17] X. G. Wen, F. Wilczek, and A. Zee, Phys. Rev. B **39**, 11413 (1989).
[18] N. Read and S. Sachdev, Phys. Rev. Lett. **66**, 1773 (1991).
[19] X.-G. Wen, Phys. Rev. B **44**, 2664 (1991).
[20] T. Senthil and M. P. A. Fisher, Phys. Rev. Lett. **86**, 292 (2001).
[21] X.-G. Wen, Phys. Rev. B **65**, 165113 (2002).
[22] S. Sachdev and K. Park, Ann. Phys. (N.Y.) **298**, 58 (2002).
[23] L. Balents, M. P. A. Fisher, and S. M. Girvin, Phys. Rev. B **65**, 224412 (2002).
[24] F. Verstraete, M. A. Martin-Delgado, and J. I. Cirac, Phys. Rev. Lett. **92**, 087201 (2004).
[25] J. J. Garcia-Ripoll, M. A. Martin-Delgado, and J. I. Cirac, Phys. Rev. Lett. **93**, 250405 (2004).
[26] L.-M. Duan, E. Demler, and M. D. Lukin, Phys. Rev. Lett. **91**, 090402 (2003).
[27] A. Micheli, G. K. Brennen, and P. Zoller, Nat. Phys. **2**, 341 (2006).
[28] J. K. Pachos, quant-ph/0511273 (unpublished).
[29] A. Kitaev, cond-mat/0506438 (to be published).
[30] A. Galindo and M. A. Martin-Delgado, Rev. Mod. Phys. **74**, 347 (2002).
[31] A. Yu. Kitaev, Ann. Phys. (N.Y.) **303**, 2 (2003).
[32] M. H. Freedman, Proc. Natl. Acad. Sci. U.S.A. **95**, 98 (1998).
[33] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).
[34] S. B. Bravyi and A. Yu. Kitaev, quant-ph/9811052 (to be published).
[35] R. W. Ogburn and J. Preskill, Lect. Notes Comput. Sci. **1509**, 341 (1999).
[36] Michael H. Freedman, Alexei Kitaev, and Zhenghan Wang, Commun. Math. Phys. **227**, 587 (2002).
[37] M. Freedman, M. Larsen, and Z. Wang, Commun. Math. Phys. **227**, 605 (2002).
[38] M. H. Freedman, A. Kitaev, M. J. Larsen, and Z. Wang, Bull., New Ser., Am. Math. Soc. **40**, 31 (2003).
[39] J. Preskill, http://www.theory.caltech.edu/preskill/ph219/topological.ps
[40] H. Bombin and M. A. Martin-Delgado, Phys. Rev. Lett. **97**, 180501 (2006).
[41] H. Bombin and M. A. Martin-Delgado, quant-ph/0605094 (to be published).
[42] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **73**, 062303 (2006).
[43] W. Thurston, in *Three-dimensional Geometry and Topology*, edited by Silvio Levy, Princeton Mathematical Series Vol. 35 (Princeton University Press, Princeton, NJ, 1997), Vol. 1.
[44] G. Perelman, math.DG/0211159 (unpublished).
[45] G. Perelman, math.DG/0303109 (unpublished).
[46] G. Perelman, math.DG/0307245 (unpublished).
[47] M. A. Levin and X.-G. Wen, Phys. Rev. B **71**, 045110 (2005).
[48] M. Levin and X.-G. Wen, Rev. Mod. Phys. **77**, 871 (2005).
[49] A. Hamma, P. Zanardi, and X.-G. Wen, Phys. Rev. B **72**, 035307 (2005).
[50] C. Wang, J. Harrington, and J. Preskill, Ann. Phys. (N.Y.) **303**, 31 (2003).
[51] K. Takeda and H. Nishimori, Nucl. Phys. B **686**, 377 (2004).
[52] F. Wilczek, Phys. Rev. Lett. **49**, 957 (1982).
[53] J. M. Leinaas and J. Myrheim, Nuovo Cimento Soc. Ital. Fis., B **37**, 1 (1977).
[54] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

An Interferometry-Free Scheme for Demonstrating Topological Order

H. Bombin and M.A. Martin-Delgado

Departamento de Física Teórica I, Universidad Complutense, 28040. Madrid, Spain.

We propose a protocol to demonstrate the topological order of a spin-1/2 lattice model with four-body interactions. Unlike other proposals, it does not rely on the controlled movement of quasiparticles, thus eliminating the addressing, decoherence and dynamical phase problems related to them. Rather, the protocol profits from the degeneracy of the ground state. It involves the addition of Zeeman terms to the original Hamiltonian that are used to create holes and move them around in the system.

PACS numbers: 71.10.Pm, 71.10.-w, 73.43.Nq

I. INTRODUCTION

The notion of topological order (TO) has gradually become a new and relevant topic in condensed matter physics [1], [2]. It gives rise to a new paradigm of quantum phases of matter which are endowed with long range correlations that cannot be detected by local order parameters [3], [4]. This is a new feature not associated with the spontaneous breaking of a symmetry. Instead, the detection of these new phases involve non-local order parameters that reflect the global nature of these new highly strongly correlated systems. Similarly, TOs turn out to be of great interest in quantum information since they are considered as a resource of robustness against the decoherence that typically affects all quantum systems when we try to manipulate them with ease and control [5]. The possibilities range from quantum memories for storage of quantum states [6] to quantum computers capable of performing a set of universal quantum operations [7], [8], [9]. The underlying mechanism for this robustness arises in a typical scenario where the possible errors in the system are local, while quantum logical operations are non-local and thus potentially resilient to decoherence.

A practical way of describing a TO is as a strongly correlated system with a quantum lattice Hamiltonian with the following properties: i/ there is an energy gap between the ground state and the excitations; ii/ the ground state is degenerate; iii/ this degeneracy cannot be lifted by local perturbations. These features reflects the topological nature of the system. In addition, a signature of the TO is the dependence of that degeneracy on topological invariants of the lattice where the system is defined, like Betti numbers [10]. When the system is placed onto an infinite plane, which has trivial topology, then the TO manifests itself through the non trivial braiding properties of their quasiparticle excitations [11]: when two identical particles are exchanged on the plane, their common wave function picks up a nontrivial statistical phase. More generally, when one particle completely encircles another particle, the state of the system picks up a phase factor that is only trivial for bosons and fermions, otherwise they are Abelian [12], [13] or non-Abelian anyons [14]. Thus, braiding statistics is also a signature of TO that can be tried experimentally. Other signatures like the topological entanglement entropy has also been proposed recently [15], [16].

There has been a number of interesting experiments in order to detect braiding statistics [17], [18], [19] in fractional quantum Hall effect systems. This has turned out to be more elusive than detecting fractional charge [20]. Thus, a number of experimental proposals has

been introduced aiming at providing additional signatures of braiding statistics [21], [22], [23], [24], [25] in fractional quantum Hall systems, both Abelian and non-Abelian, which in turn would imply TO. For non-Abelian gauge theories, it is also possible to detect anomalous braiding statistics by interferometric means [26], [27]. There exist such intereferometric proposals for the surface code introduced by Kitaev [28], [29]. This is the system in which we are interested here.

In this paper we propose an alternative route to detect TO directly and without having to resort to interferometry of quasiparticles to probe their non-trivial braiding statistics. We use the fact that the ground state degeneracy is sensitive to the topology of the surface, which we can altere introducing Zeeman terms in certain areas of the system. In particular, our scheme for detecting TO relies on the notion of code deformations for surface codes [6], [30], [31].

II. A MODEL WITH STRING CONDENSATION

A. Hamiltonian and ground state

The topologically ordered system that we consider here was introduced by Kitaev [5]. It is a 2-dimensional array of spin-1/2 systems. Note that any subset C of the spins can be identified with a binary vector (e_i), where $e_i = 1$ if the i-th spin belongs to C and $e_i = 0$ otherwise. Then, for each such set C we introduce the operators

$$X^C := \bigotimes_i \sigma_X^{e_i}, \qquad Z^C := \bigotimes_i \sigma_Z^{e_i}. \tag{1}$$

Spins are located at the sites of a 'chessboard' lattice, see Fig. 1. The Hamiltonian is a sum of plaquette operators X^p, Z^p which depend on the coloring of the plaquette p, dark or light,

$$H = -\sum_{p\in\mathcal{P}_D} g_p X^p - \sum_{p\in\mathcal{P}_L} g_p Z^p, \tag{2}$$

where $g_p > 0$ is the coupling constant at plaquette p, $\mathcal{P}_D$ ($\mathcal{P}_L$) is the set of dark (light) plaquettes and we identify each plaquette with the set of spins in its corners. The spectrum of plaquette operators is $\{1, -1\}$ and they commute, so that the ground state is defined by the conditions

$$X^p|\psi\rangle = Z^{p'}|\psi\rangle = |\psi\rangle, \qquad p \in \mathcal{P}_D,\ p' \in \mathcal{P}_L, \tag{3}$$

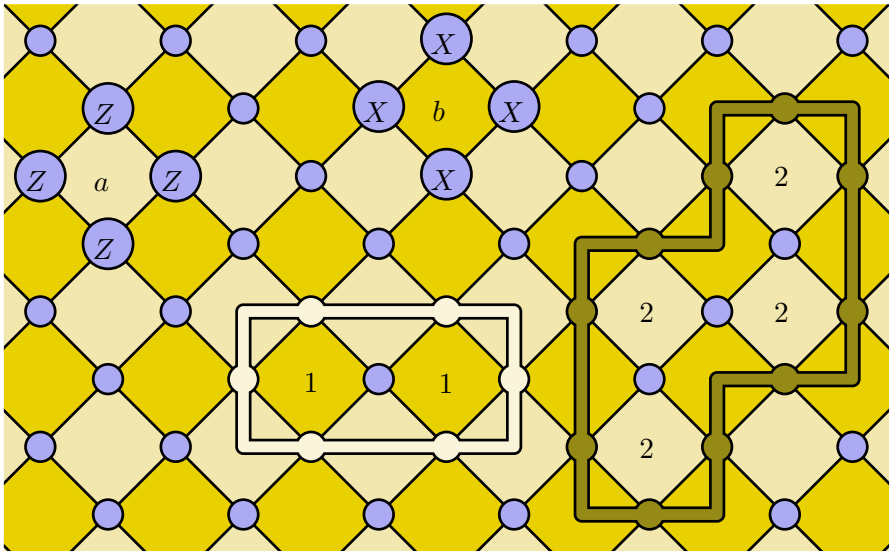


FIG. 1: Blue circles represent the spin-1/2 systems, lying on the sites of the lattice. Z^p (X^p) operators correspond to light (dark) plaquettes like a (b). The light (dark) string represents the product of the plaquette operators of those dark (light) plaquettes marked with a 1 (2).

which must hold for all the plaquettes. If we consider that the lattice extends to infinity or lyes on a sphere, there is no ground state degeneracy. In particular, the unnormalized ground state takes the form

$$|\mathrm{GS}\rangle = \prod_{p\in\mathcal{P}_D} (1 + X^p)|\psi_0\rangle, \tag{4}$$

where ψ_0 is the state with all spins up. However, if the topology of the surface is nontrivial the ground state is degenerate [5].

B. String operators

A useful notion is that of dark and light strings, see Fig. 1 for examples. Light (dark) strings connect light (dark) plaquettes, so that each string segment contains a spin. Let γ be a light string and γ' a dark one. Then we attach string operators to them, X^γ and $Z^{\gamma'}$, identifying strings with the sets of spins in their segments. An important property is that $\{X^\gamma, Z^{\gamma'}\} = 0$ if γ crosses γ' and odd number of times, $[X^\gamma, Z^{\gamma'}] = 0$ otherwise. Strings are either closed or have endpoints at plaquettes of their color. When γ and γ' are closed we have

$$[X^\gamma, H] = [Z^{\gamma'}, H] = 0. \tag{5}$$

Among closed strings we find boundary strings, which receive this name because they form the boundary of a portion of the surface. Ground states can be characterized by the fact that if γ and γ' are boundaries then

$$X^{\gamma}|\psi\rangle = Z^{\gamma'}|\psi\rangle = |\psi\rangle. \tag{6}$$

This is equivalent to (3), because plaquettes can be identified with small boundaries, and boundary string operators are products of plaquette operators. We can also rewrite (4) as

$$|\mathrm{GS}\rangle = \sum_{\gamma \in \mathcal{B}^L} X^{\gamma}|\psi_0\rangle, \tag{7}$$

where the elements of $\mathcal{B}_L$ are collections of boundary strings. If we identify each state $X^{\gamma}|\psi_0\rangle$ with a string configuration, that corresponding to γ, then the ground state is a coherent superposition of string states. This is why we say that the model is a string condensate [11].

C. Excitations and topological charge

The excitations of the system have a localized nature and are subject to an energy gap. In particular, these quasiparticles are related to plaquette operators, so that we say that the state $|\psi\rangle$ has an excitation at plaquette p if the corresponding condition (3) is violated. The energy of the quasiparticle is $\Delta = 2g_p$. Excited states can be obtained from the ground state by applying open string operators: they create quasiparticles at their endpoints.

Excitations have a topological charge, which can be understood in terms of string operators also. Suppose that we have several excitations in the shaded region of Fig. 2. Consider a light string γ and a dark string γ' that surround the region. We construct four orthogonal projectors that resolve the identity

$$P_{a,b} := \frac{1}{4}\left(1 + (-1)^a X^{\gamma}\right)\left(1 + (-1)^b Z^{\gamma'}\right), \qquad a, b = 0, 1. \tag{8}$$

Each of the sectors (a, b) projected by $P_{a,b}$ corresponds to a different topological charge inside the region. These charges are integrals of motion because of (5). In the ground state the charge is $(0, 0)$, so this is the trivial charge. Consider a dark string γ'' with an endpoint inside the region, as in Fig. 2. Then we have $Z^{\gamma''}P_{a,b} = P_{a+1,b}Z^{\gamma''}$, with addition modulo two. Since γ'' switches the excitations of the dark plaquettes in its endpoints, we see that excitations of dark plaquettes carry the charge $(1, 0)$. Similarly, an excitation of a light

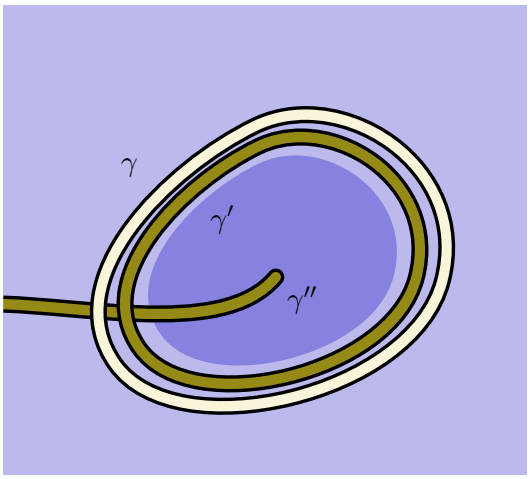


FIG. 2: The total topological charge in the shaded region can be measured using the string operators X^{γ} and $Z^{\gamma'}$. String operators from strings with endpoints in the region, such as γ', change the charge of the region as they create or destroy a quasiparticle inside it.

plaquette carries the charge $(0, 1)$. It is easy to check that if a region is divided on two subregions with charges (a_1, b_1), (a_2, b_2), then its total charge is $(a_1 + a_2, b_1 + b_2)$, again with addition modulo two. The topological nature of these charges relies in the fact that when a charge (a_1, b_1) is moved around a charge (a_2, b_2) the system will pick up a phase $(-1)^{a_1 b_2 + a_2 b_1}$ which does not depend on the particular trajectory [5].

III. BORDERS AND TOPOLOGICAL DEGENERACY

A. Borders in surface codes

The ground state subspace of the Hamiltonian (2) is a surface code, a kind of topological stabilizer code [5]. For our purposes here, a stabilizer code is a subspace defined by certain conditions, which for surface codes are (6). At first, surface codes were defined in closed surfaces, but this has a limited use since it is difficult to construct experimental setups with non-planar geometries. However, even in the plane a nontrivial topology is possible if we introduce borders [32], [33].

Two kind of borders can be considered in surface codes, dark or light. Borders change the concept of closed string. A dark (light) string is closed either if it has no endpoints or if its endpoints lye on dark (light) borders. Boundaries also change. A dark (light) string

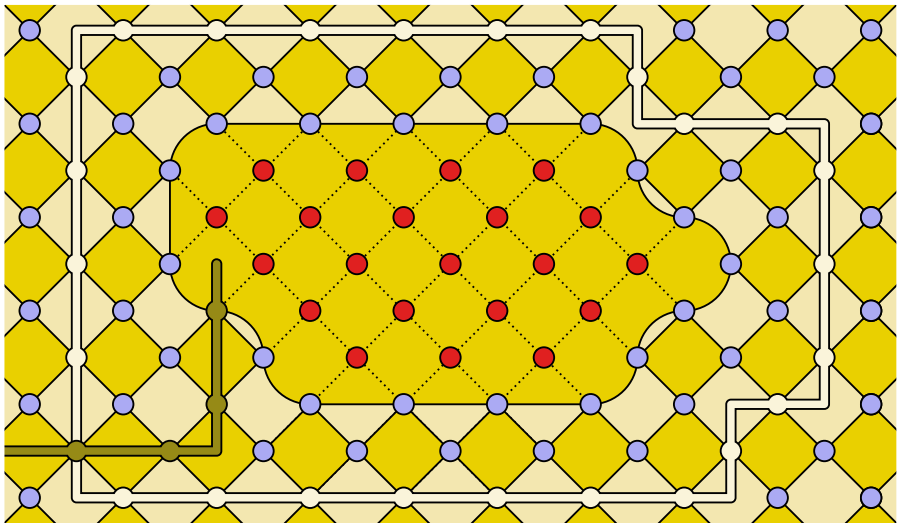


FIG. 3: This figure represents a dark hole in a surface code. Red sites correspond to spins that are not part of the lattice. Note that a dark hole is nothing but a missing big dark plaquette. The strings on display are closed but not boundaries.

is a boundary if it encloses a portion of surface which contains no light (dark) borders. In surface codes, borders can be introduced by changing the geometry of the lattice. In particular, a dark (light) border corresponds to a missing big dark (light) plaquette. Then the code can be described using the conditions (6) under the new notion of boundary string. As an example, Fig. 3 shows a dark hole in a lattice. It has been created by erasing several spins from the lattice, shown in red, and rearranging the plaquettes accordingly.

The introduction of borders in surface codes allows to have non-trivial topologies and thus a code subspace with dimension greater than one. For example, if the surface is a disc with h holes, with the borders of the same type, then the dimension of the code is 2^h[33]. However, there is more to borders than this. In particular, we can consider adding dynamics to the picture. By changing the borders with time we can initialize, transform and measure the states of the code [31]. This is a feature of surface codes that we would like to introduce in the quantum Hamiltonian model, a possibility that we explore next.

B. Borders in the string condensate

In principle, one could introduce borders in the quantum Hamiltonian model (2) simply by changing the geometry of the lattice, that is, as in the surface code of Fig. 3. However,

this would require the ability to engineer a Hamiltonian in which for example a 3-body plaquette term must exist next to a 4-body one and so on. Such a detailed engineering is not feasible in many situations. Thus, we propose a different setting, in which changes in the topology are produced by modifying the original Hamiltonian through the introduction of Zeeman terms and smooth spatial changes of the couplings.

We start by dividing the system surface in five regions, M, D, L, D_B and L_B. M is the main system, where we are going to keep the original Hamiltonian and thus the topological order remains untouched. In the areas D and L there will be no topological order. As for D_B and L_B, these are thick boundaries that separate D from M and L from M, respectively. D_B will play the role of a dark boundary, and L_B that of a light boundary. An example can be seen in Fig. 4, where the geometry is that of a disc with a hole, with both borders of light type.

We have to define the concepts of closed and boundary strings in our new geometry with the five regions. A dark (light) string is closed either if it has no endpoints or if they lye inside D (L). A dark (light) string is a boundary if it encloses a portion of surface not containing any piece of $L \cup L_B$ ($D \cup D_B$). With these definitions, we need a Hamiltonian that satisfies (5) for closed strings and such that its ground states satisfies (6) for boundary strings and there exists an energy gap to states not satisfying them. We will first show why these conditions are enough to get the desired properties, and afterwards give an example of a Hamiltonian that satisfies the constrains.

We will work with a particular geometry to fix ideas, the disc with a hole of Fig.(4). Considering a general case has no additional complications, but the discussion would be less transparent. Let V be the subspace defined by conditions (6), so that the ground state subspace is $V_{\rm GS} \subset V$. Consider the light string γ_1 and the dark string γ_1' of Fig.(4). They are closed but not boundaries, and since they cross we have $\{X^{\gamma_1}, Z^{\gamma_1'}\} = 0$. These operators are the X and Z operators of a qubit or two-level subsystem, both in V and in $V_{\rm GS}$. Let us show this in detail. Note that X^{γ_1}, $Z^{\gamma_1'}$ leave V invariant, as closed string operators always commute with boundary string operators. Then we can choose an orthonormal basis $\{|0;k\rangle\}_k$ for the subspace of V such that $Z^{\gamma'} = 1$, which can be completed in V with the elements $|1;k\rangle := X^{\gamma_1}|0;k\rangle$, which satisfy $Z^{\gamma_1'} = -1$. In other words, $V \simeq V' \otimes V_2$, with V_2 a two dimensional space. The same is true for $V_{\rm GS}$, as follows from (5). That is, $V_{\rm GS} \simeq V'_{\rm GS} \otimes V_2$ and $V' \simeq V'' \oplus V'_{\rm GS}$.

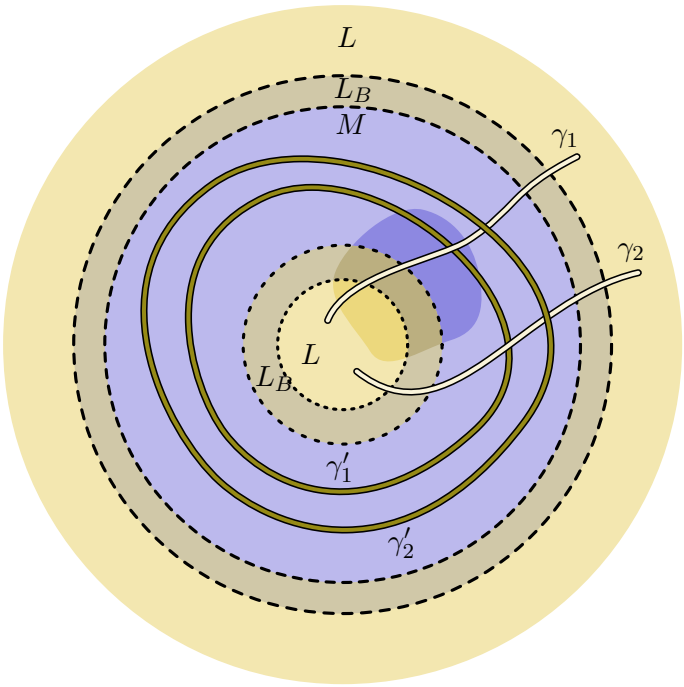


FIG. 4: An example of how light borders are introduced in terms of the regions L, L_B and M. In this case the main region M, in blue, has the topology of a disc with a hole, with both borders of light type. Examples of closed nontrivial strings are displayed. The γ_i are closed because they have no endpoints. The γ_i' are closed because their endpoints lye in L. The shaded area represents the support of a local operator, which neither encloses the interior L region nor connects both L regions.

The point is that the degeneracy of the ground state that comes from the qubit subsystem has a topological origin and cannot be lifted by a small local perturbation. This a consequence of the fact that there is an energy gap to states out of V and that if σ is any local operator then

$$\langle a;k|\sigma|b;k'\rangle = \delta_{a,b}\,\langle 0;k|\sigma|0;k'\rangle, \qquad a,b=0,1 \tag{9}$$

We shall prove this equation in the following. For a local operator we mean one with a support such as the shaded area in Fig.(4), which neither encloses the central L region nor connects the interior and exterior L regions. Then there exist a light string γ_2 and a dark string γ_2', as in the figure, with the following properties. First, they do not touch the support of σ, so that $[X^{\gamma_2},\sigma] = [Z^{\gamma_2'},\sigma] = 0$. Second, we have the equivalences up to homology $\gamma_1 \sim \gamma_2$, $\gamma_1' \sim \gamma_2'$, so that $X^{\gamma_1}X^{\gamma_2} = X^{\gamma_3}$ and $Z^{\gamma_1'}Z^{\gamma_2'} = Z^{\gamma_3'}$ with γ_3, γ_3' boundaries. From

these properties (9) follows immediately. This equation can also be interpreted in terms of quantum error correction theory. It states that we can correct information codified in the qubit subsystem that has suffered a family of errors $\{E_i\}$ as long as any $\sigma = E_i^\dagger E_j$ is local [34].

We now give an exactly solvable Hamiltonian that satisfies the desired constrains. It takes the form

$$H = -\sum_{p\in\mathcal{P}_D} g_p\, X^p - \sum_{p\in\mathcal{P}_L} g_p\, Z^p - \sum_i (\mu_i\, X^i + \nu_i\, Z^i), \tag{10}$$

where i runs over the sites of the lattice, $g_p, \mu_i, \nu_i \geq 0$ are coupling constants and we identify a site i with the set $\{i\}$. As long as $\nu_i = 0$ ($\mu_i = 0$) for all the sites i that lye on the corner of a dark (light) plaquette p with $g_p > 0$, the Hamiltonian is exactly solvable because all the non-vanishing terms are commuting projectors. Then, the ground state subspace is characterized by the conditions

$$X^p|\psi\rangle = Z^{p'}|\psi\rangle = Z^i|\psi\rangle = X^j|\psi\rangle = |\psi\rangle, \tag{11}$$

which must hold for all the dark plaquettes p with $g_p > 0$, light plaquettes p' with $g_{p'} > 0$, sites i with $\nu_i > 0$ and sites j with $\mu_j > 0$. It is possible to choose the couplings in such a way that the conditions (5,6) are satisfied. In particular, $\mu_i > 0$ ($\nu_i > 0$) must be fulfilled in L (D), whereas $\mu_i = 0$ ($\nu_i = 0$) in $M \cup D \cup D_B$ ($M \cup L \cup L_B$). Also, $g_p > 0$ must hold for dark (light) plaquettes in $M \cup L_B$ ($M \cup D_B$), whereas $g_p = 0$ in D (L). All this can be done in such a way that the couplings vary smoothly across the surface, due to the thickness of the boundary regions L_B and D_B.

As a result of the above construction, we will find in general a local degeneracy in the ground state, since there exist areas in L_B (D_B) where the only non-zero coupling is g_p in dark (light) plaquettes. This local degeneracy can be removed by letting the support of μ_i (ν_i) overlap with that of the g_p of light (dark) plaquettes. In doing so, the Hamiltonian is no longer exactly solvable, but it will fulfill the required conditions at least as long as the overlap is not too big. To see this, note that we can write the Hamiltonian as $H' = H + H_p$, where H_p contains those terms that do not commute with all the terms of H'. Then H is exactly solvable and has the required properties. Also, $[H_p, H] = 0$. Indeed, each of the terms of H_p commutes with each of the terms in H. Thus, an small H_p will not destroy the properties of H discussed above. Still, if the overlap is too big, a level crossing could occur taking the ground state out of the subspace V described by (6).

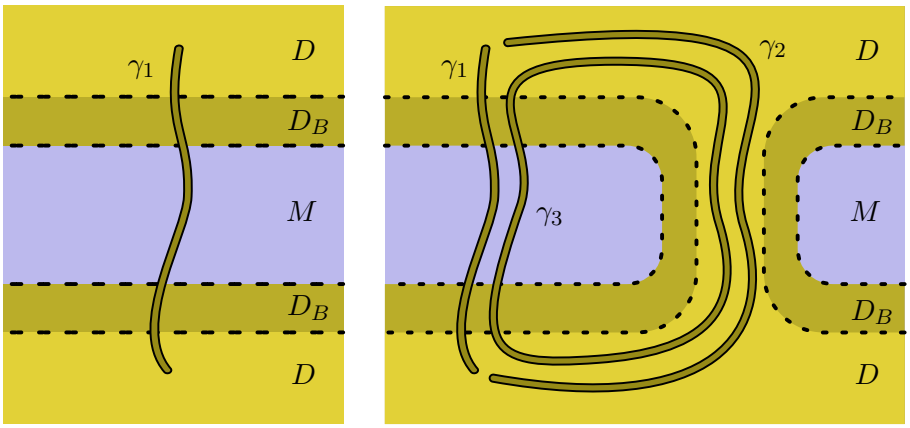


FIG. 5: A deformation in which two separated D regions are put together, which amounts to cut the main region M. To the left, the geometry before the cut is done. We suppose that γ_1 is a nontrivial closed string. To the right, the geometry after the cut. Now γ_1 is a boundary string, and so are γ_2 and γ_3. If $Z^{\gamma_2} = 1$, then $Z^{\gamma_1} = Z^{\gamma_3}$, that is, the cut maps the value of Z^{γ_1} to the light plaquete charge in the region surrounded by γ_3.

C. Surface deformation

Once one is able to engineer the Hamiltonian (10), the next step is to adiabatically modify the couplings so that the geometry of the surface changes slowly with time. Here we can distinguish too kind of such surface deformations. First, we can perform deformations in which only the geometry of the surface, not its topology, change with time. When the initial and the final state of the system are the same, these produce a continuous map of the surface onto itself, so that in particular strings get transformed. This gives a string operator mapping, which amounts to perform a definite operation on the encoded subsystem [31]. Second, deformations that change the topology can be considered, such as introducing or destroying holes and cutting or gluing pieces of the main surface M. These kind of processes change the topological degeneracy of the ground state. When it grows, the new degrees of freedom will be initialized in a definite way [31], due to topological considerations. When it decreases, the lost degrees of freedom get mapped to possible excitations in the final state.

This deserves a more detailed explanation. Consider for example the surface deformation illustrated in Fig. (5), where too separate pieces of region D get connected, producing a cut in M. Consider the dark string γ that connects both D areas. We want to show that the deformation amounts to a measurement of Z^{γ}. Before the deformation γ is closed — and

we assume that nontrivial — and after the deformation it is a boundary. Because of the local nature of the deformation, it cannot change the value of Z^{γ_1}, which lyes outside the area where the action occurs. But if $Z^{\gamma_1} = -1$, then the final state cannot fulfill conditions (6) and thus it is not a ground state. Which excitations should we find? To answer this, let us suppose that the coupling μ_i is big enough in D, so that in the final state we know that $Z^{\gamma_2} = 1$ is fulfilled for any dark string γ_2 lying inside D. Then for the dark boundary string γ_3 formed by composing γ_1 and γ_2, see Fig. 5, and for the final state $|\psi\rangle$ we have $Z^{\gamma_3}|\psi\rangle = Z^{\gamma_1}Z^{\gamma_2}|\psi\rangle = Z^{\gamma_1}|\psi\rangle$. Since the value $Z^{\gamma_3} = \pm 1$ is related to light plaquette charge inside γ_3 through (8). We see that the cutting process, as announced, amounts to a measurement of Z_2^{γ}, as its value is mapped to the possible appearance of charge at both sides of the cut.

For the previous analysis, the deformation needs not really be adiabatic. It is enough if we can guarantee that there are no excitations inside D. The particularity of the adiabatic case is that we expect to find a final state with a single light plaquette excitation at each side of the cut, since this is a state in a local energy minimum. We will see an application of these measurements through surface cutting — and indeed of all the mentioned kinds of surface deformations — in the scheme to demonstrate the topological character of the phase discussed below .

It is worth mentioning that these ideas can be used to adiabatically initialize the topologically ordered phase. In this regard, a question was raised in [35] about how to adiabatically initialize these systems so that the topological protection is present all along the way and not only after reaching the topological phase. The answer is that, instead of initializing the whole system at a time, one should progressively grew it from a small island till the desired surface is covered. In surfaces with non-trivial topology, this means that at some point two different borders of the system will fuse. At that point the degeneracy of the ground state will change, as new nontrivial string operators appear. The eigenvalues of the new string operators that run along such junctions are necessarily one [31], and thus the final particular ground state of the system is perfectly determined.

IV. A SCHEME FOR DEMONSTRATING TOPOLOGICAL ORDER

When trying to demonstrate TO, the usual approaches focus on interferometric experiments with quasiparticles in which topologically different paths are compared. An immediate problem of such approaches is that the required quasiparticle superposition of states are subject to decoherence due to their localized nature and the presence of a noisy environment. Also dynamical phases have to be taken into account and properly controlled. Here we adopt a different approach that eliminates both problems by focusing on the ground state degeneracy. The idea is to show that the outcome of certain processes depends only on topological properties, thus revealing the topological nature of the system.

The scheme is as follows. We start by making a pair of holes in our system, a dark one and a light one, see Fig. 6(a). Then we deform both of them as in Fig. 6(b), till they are separated into two pieces. Notice that since in figure Fig. 6(b) γ_1 and γ_1' are boundaries we have $X^{\gamma_1} = Z^{\gamma_1'} = 1$. After the hole breaks into two pieces they still must have the same value because it is a global property[31], so that we reach the situation in Fig. 6(c), where X^{γ_2} and $Z^{\gamma_2'}$ have completely undefined values since $\{X^{\gamma_1}, Z^{\gamma_2'}\} = \{X^{\gamma_2}, Z^{\gamma_1'}\} = 0$. We then proceed to move one of the dark holes along a closed path. Suppose for the moment that the path is as the one shown in Fig. 6(d), that is, that it encloses one of the light holes. The point is that, after this has been accomplished, the string operators have deformed accordingly. For example, γ_1' has changed and now its place is occupied by γ_3', see Fig. 6(e). If $|\psi\rangle$ is the state corresponding to that figure, we have $Z^{\gamma_3'}|\psi\rangle = Z^{\gamma_1'}Z^{\gamma_2'}|\psi\rangle = Z^{\gamma_2'}|\psi\rangle$. A similar analysis holds for a light string connecting the light holes. When we finally refuse the holes, as in Fig. 6(f), we are measuring these string operators that connect each pair of holes, which have a completely undefined value, so that there exists a 1/2 probability that we find charges at both sides of the fusion point, as follows from the explanation in section III C. The problem of how to detect this charge would depend on the particular experimental situation.

Now return to the path in Fig. 6(d) and consider any line l joining both light holes. We can imagine many other closed paths, some of them never crossing this line and others crossing it many times. The topological property in which we are interested is the number of times a path crosses l. If the number is odd, the situation is the one described above. If it is even, then it is equivalent to doing nothing and if we refuse the holes we will never find

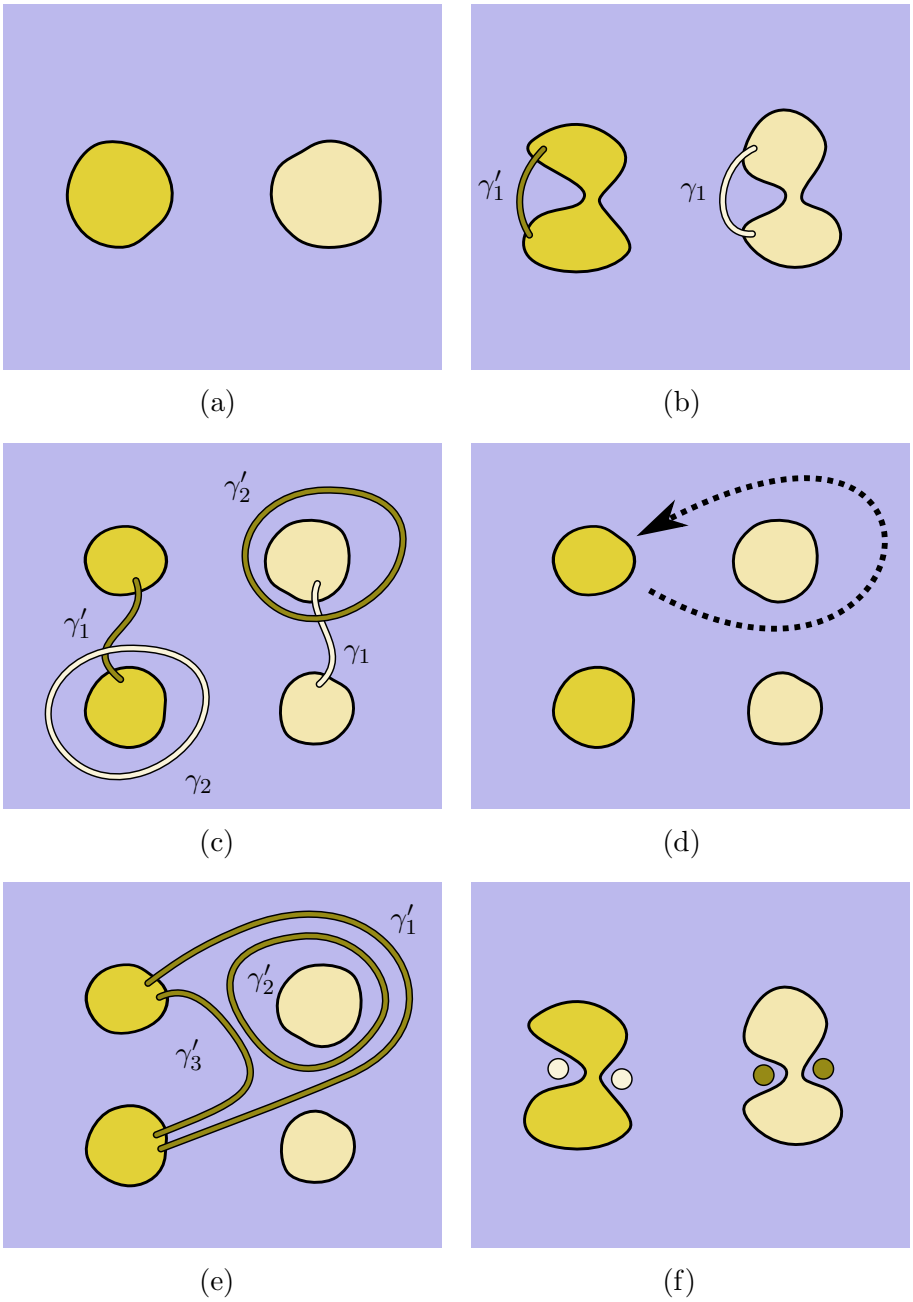


FIG. 6: A step-by-step representation of the proposed scheme, as explained in section IV.

charges [31]. Also, note that several quasiparticles could be created during the fusion of the holes if it is not adiabatic, but the evenness or oddness of the number of particles created at each side is topologically protected since it gives the total topological charge.

Thus the topological nature of the system manifests in the fact that the experiment is sensitive to the topology of the chosen path. Moreover, the underlying Z_2 nature of the system is revealed also: only the evenness or oddness of the linking number is important.

With this scheme we have introduced a new way to probe the existence of a TO. It does not involve the ability to manipulate individual quasiparticle excitations, but instead relies solely on the peculiar ground state properties of topologically ordered quantum systems.

V. FINAL REMARKS

Although we have restricted ourselves to the Kitaev Z_2 model, it is possible to consider generalizations to Z_D systems or even non-abelian models. In this regard, as noted above, the definition of holes in terms of open strings is a natural starting point and a much more richer family of 'holes' is expected in such systems, but the basic mechanism for topological detection without resorting to quasiparticle interferometry remains the same.

Acknowledgements We acknowledge financial support from a PFI fellowship of the EJ-GV (H.B.), DGS grant under contract BFM 2003-05316-C02-01 (M.A.MD.), and CAM-UCM grant under ref. 910758.

---

[1] X.-G. Wen. *Quantum Field Theory of Many-body Systems*, Oxford University Press, (2004).

[2] X.-G. Wen and Q. Niu, Phys. Rev. **B 41**, 9377 (1990).

[3] L. D. Landau, Phys. Z. Sowjetunion **11**, 26 (1937).

[4] V. L. Ginzburg, L. D. Landau, Zh. Ekaper. Teoret. Fiz. **20**, 1064 (1950).

[5] A. Yu. Kitaev, Annals of Physics **303** no. 1, 2–30 (2003), `quant-ph/9707021`.

[6] E. Dennis, A. Kitaev, A. Landahl, J. Preskill, J. Math. Phys. **43**, 4452-4505 (2002).

[7] M. H. Freedman, A. Kitaev, Z. Wang, Commun.Math.Phys. **227** 587-603, (2002).

[8] M. Freedman, M. Larsen, Z. Wang, Comm.Math. Phys. **227** 605–622, (2002).

[9] M. H. Freedman, A. Kitaev, M. J. Larsen, Z. Wang, Bull. Amer. Math. Soc. **40** 31-38, (2003); quant-ph/0101025.

[10] H. Bombin, M. A. Martin-Delgado, Phys. Rev. **B** 75, 075103 (2007).

[11] M. Levin, X.-G. Wen, Phys. Rev. **B 71**, 045110 (2005).

[12] J. M. Leinaas, J. Myrheim, Nuovo Cimento **37** B, 1 (1977).

[13] F. Wilczek, Phys. Rev. Lett. **48**, 1144 (1982); Phys. Rev. Lett. **49**, 957 (1982).

[14] G.Moore, N.Read, Nucl. Phys. **B** 360, 362 (1991).

[15] A. Kitaev, J. Preskill, Phys. Rev. Lett. **96**, 110404 (2006)

[16] M. Levin, X.-G. Wen, Phys. Rev. Lett. **96**, 110405 (2006).

[17] V.J.Goldman, J.Liu, and A.Zaslavsky, Phys. Rev. **B** 71, 153303 (2005).

[18] F.E.Camino, W.Zhou, V.J.Goldman, Phys. Rev. Lett. **95**, 246802 (2005).

[19] F.E.Camino, W.Zhou, V.J.Goldman, Phys. Rev. Lett. **98**, 076805 (2007).

[20] V. J. Goldman, B. Su, Science **267**, 1010 (1995).

[21] S. Das Sarma, M. Freedman, C. Nayak, C., Phys. Rev. Lett. **94**, 166802 (2005)

[22] A. Stern, B.I. Halperin, Phys. Rev. Lett. **96**, 016802 (2006)

[23] P. Bonderson, A. Kitaev, K. Shtengel, Phys. Rev. Lett. **96**, 016803 (2006).

[24] D.E. Feldman, A. Kitaev; Phys. Rev. Lett. **97**, 186803 (2006).

[25] K.T. Law, D.E. Feldman, Y. Gefen, Phys. Rev. **B** 74, 045319 (2006).

[26] F. A. Bais, Nucl. Phys. **B** 170, 32 (1980).

[27] R. W. Ogburn and J. Preskill, Lecture Notes in Computer Science **1509**, 341–356, (1999).

[28] S.S. Bullock, G.K. Brennen; J.Phys. **A**40, 3481-3505 (2007).

[29] Y.-J. Han, R. Raussendorf, L.-M. Duan, Phys. Rev. Lett. **98**, 150404 (2007).

[30] R. Raussendorf, J. Harrington, K. Goyal; arXiv:quant-ph/0703143.

[31] H. Bombin, M.A. Martin-Delgado; arXiv:0704.2540.

[32] S. B. Bravyi, A. Yu. Kitaev; arXiv:quant-ph/9811052.

[33] H. Bombin, M.A. Martin-Delgado, J. Math. Phys. 48, 052105 (2007); arXiv:quant-ph/0605094.

[34] M. Nielsen, D. Poulin, quant-ph/0506069.

[35] A. Hamma, D.A. Lidar; arXiv:quant-ph/0607145.

A Family of Non-Abelian Kitaev Models on a Lattice: Topological Condensation and confinement

H. Bombin and M.A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040. Madrid, Spain.

We study a family of non-Abelian topological models in a lattice that arise by modifying the Kitaev model through the introduction of single-qudit terms. The effect of these terms amounts to a reduction of the discrete gauge symmetry with respect to the original systems, which corresponds to a generalized mechanism of explicit symmetry breaking. The topological order is either partially lost or completely destroyed throughout the various models. The new systems display condensation and confinement of the topological charges present in the standard non-Abelian Kitaev models, which we study in terms of ribbon operator algebras.

PACS numbers: 71.10.-w, 11.15.-q, 03.67.Pp, 71.27.+a

I. INTRODUCTION

The subject of topological orders poses new challenges in the understanding of new phases of matter due to novel effects in quantum many-body physics [1]. There is by now a good deal of examples in condensed matter, like in fractional Hall effect systems [2], [3], [4], [5], [6], short range RVB (Resonating Valence Bond) models [7], [8], [9], [10]. or in quantum spin liquids [11], [12], [13], [5], [14], [15], [16], [17]. There exists also exactly solvable models [18], [19], [20], [39], [40], that are paradigmatic examples for exhibiting topological properties that can be addressed in full detail since the whole spectrum of those models is known. Although topological orders typically arise in the quantum physics of two spatial dimensions, it is possible to construct exactly solvable models in three spatial dimensions and beyond [21]. There is yet another field in which topological orders appear naturally. It corresponds to discrete gauge theories that arise as a consequence of a spontaneous symmetry breaking mechanism from a continuous gauge group down to a discrete gauge group [22], [23], [24], [25], [26], [27], [28]. In these two-dimensional topological quantum field theories, the standard algebraic language to describe the residual gauge invariant properties of the excitations is that of quasitriangular Hopf algebras (quantum groups) [29].

At the same time, quantum systems with topological order provide new expectations for finding alternative ways of robust quantum computation [18], [30], [31]. In fact, there are several forms to set up schemes for topological quantum computation, some of them based on the braiding of quasiparticles [18], [32], [33], [34], [35], [36], [37], [38], some of them based solely on the topological entangled properties of the degenerate ground states, without selective addressing of the physical qubits and without resorting to braiding of excitations [39], [40], and others based on cluster states [41].

Topological orders can be thought of as new forms of long range entanglement and they are at the crossroads of condensed matter and quantum information [42], [43], [44], [45], [46], [47], [48], [49], [50]. Some forms of hidden topological orders in quantum spin chains can be detected with string order parameters, which in turn can be interpreted in the light of quantum information techniques, and their long-range entanglement detected with them [45] using matrix product states from condensed matter.

There are experimental proposals based on optical lattices [51], [52] to implement models with Abelian topological orders [53], and in particular, the study of the string order parameter mentioned above can also be proposed by means of these techniques [54]. There are also proposals for non-Abelian models based on Josephson junction arrays [55], [56], [57], in addition to the largely studied case of the fractional quantum Hall effect [38].

One of the emblematic examples of exactly solvable models to study topological orders on a lattice is the Kitaev model [18], both in its Abelian and non-Abelian versions. It captures the algebraic properties exhibited by the discrete gauge theories mentioned above. In addition, it provides us with an explicit realization of a Hamiltonian on a lattice, with the bonus that it allows for a model of topological quantum computation.

Comparatively, there are much less works on the non-Abelian Kitaev model than in the Abelian case (toric code). This is due, to some extent, to the additional mathematical technical difficulties presented by the non-Abelian case which is traditionally introduced with the language of quasi-triangular Hopf algebras and their representations [58], [59]. Here we have made an effort to explain its contents in full detail and clarity with simpler algebraic tools based on group theory and their representations. Our goal is twofold: to make the model more accessible to a broader audience with a previous knowledge on the Abelian toric code, and to use that simpler presentation as a starting point for considering more general models.

In this paper we introduce a family of non-Abelian topological models on a lattice, such that the standard Kitaev model corresponds to a particular case. More specifically, we study a two-parameter family labeled by a pair of subgroups $N \subset M \subset G$, N normal in G, where G is a discrete non-Abelian gauge group. The particular case $N = 1$, $M = G$ correspond to the original

Kitaev models. The Hamiltonians of the family, denoted $H_G^{N,M}$, are explicitly constructed in eq. (35). The standard vertex ('electric') operators are modified according to the subgroup M, while the face ('magnetic') operators change in accordance with N. In addition, there are new terms entering in the Hamiltonians which act on the edges of the lattice. Since there is a qudit attached to each edge these are single-qudit terms. Depending on the choice of the pair of subgroups (M, N) with respect to G, the non-Abelian discrete gauge group of the whole Hamiltonian $H_G^{N,M}$ may range from G down to the trivial group when $M = N$. This is so because the gauge group for these models turns out to be given by $G' = M/N$. Therefore, the new family of non-Abelian models provides us with a mechanism of explicit symmetry breaking of an original Hamiltonian with large discrete gauge symmetry group. In other words, this mechanism can also be seen as a symmetry-reduction mechanism, since we may have still a smaller gauge symmetry present in the Hamiltonian.

The new edge terms do not commute with the vertex and face terms of the original Hamiltonian, but this can be compensated by slightly changing these vertex and face terms. This change corresponds to studying the regimen in which the single-qudit terms have a higher coupling constant. Choosing the models this way, we can study their ground state and also the charge condensation phenomena. At least in some cases, single-qudit terms can be understood as a mechanism for introducing string tension, or more appropriately 'ribbon tension', to some of the quasiparticle excitations which thus get confined. In those cases, a complete characterization of the charge types and domain wall fluxes will be given.

In order to facilitate both the exposition of the results and the readability of the manuscript, throughout the main text we will be giving the main constructions and results omitting many auxiliary details or proofs. However, all these can be found in a well-ordered form in a complete set of appendices.

We hereby summarize briefly some of our main results:
i/ we introduce a family of Hamiltonians defined on two-dimensional spatial lattices of arbitrary topology which exhibit a variety of discrete non-Abelian gauge group symmetry and topological orders;
ii/ the ground state of the models can be exactly given and characterized in terms of open a boundary ribbon operators. In many interesting cases the spectrum of excitations can be characterized accordingly;
iii/ the new models show condensation and confinement of the charges in the original models with Hamiltonian H_G;
iv/ in order to facilitate and complement the study of the family of models, we have carried out a thorough clarification of the main properties of the standard non-Abelian Kitaev model. In particular:
iv.a/ The ribbon operator algebra is introduced in an intrinsic way, with the motivation to find operators that describe excitations.
iv.b/ We study in detail and generalize the concept of ribbon. In particular, closed ribbons and a related algebra are defined, and their transformation properties described.
iv.c/ The vertex and face operators that appear in the Hamiltonian are related to elementary closed ribbon operators, showing that everything in the models can be translated to the language of ribbons.
iv.d/ We give a detailed account of two-particle states, giving explicitly a basis for the states that clarifies the meaning of the labels for topological charge.
v/ A description of the ground state in terms of boundary ribbon operators is given.

This paper is organized as follows: in Sect.II we treat the standard non-abelian Kitaev model. We start explaining the terms appearing in the Hamiltonian and go on characterizing the ground state and quasiparticle excitations by means of closed ribbon operators. We also present an explicit characterization of the topological charges of the model and study when single-quasiparticle states are possible. In Sect.III we motivate the new family of non-Abelian model Hamiltonians and present their generic properties. Then, we show how these models exhibit topological condensation and confinement described by domain walls. To this end we make use of closed and open ribbon operator algebras. Sect.IV is devoted to conclusions.

Appendices deserve special attention since they contain the detailed and basic explanations of all the constructions used throughout the text. Specifically, Appendix A contains a brief summary of representation theory for group algebras, their centers and induced characters. In Appendix B we perform an extensive treatment of ribbon operators, which are necessary to describe the whole spectrum of the models. We define ribbons as geometrical objects and then construct and characterize a series of ribbon operator algebras. In Appendix C we study the relationship between certain ribbon transformations and the action of ribbon operator algebras on suitable subspaces, which is a key ingredient in describing the topological properties of the models. In Appendix D we give some details about the local degrees of freedom that appear in the Hilbert space of two-particle excitations. In Appendix E we explain why single-quasiparticle states exist in non-abelian models on surfaces of nontrivial topology. Finally, in Appendix F we show several results needed for condensation and ground state characterization.

II. NON-ABELIAN KITAEV MODEL

A. Hamiltonian

The data necessary for building up the model, as introduced by Kitaev[18], are any given finite group G and a lattice embedded in an orientable surface. The edges of the lattice must be oriented, as shown in Fig. 1.

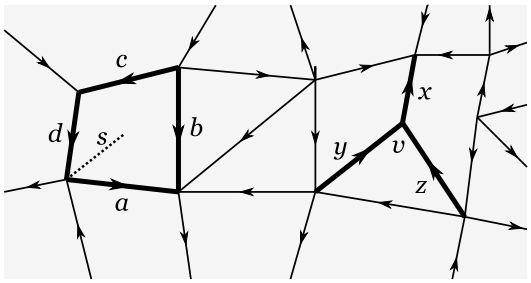


FIG. 1: The two dimensional lattice that we consider are arbitrary in shape and have oriented edges. Thick lines display the support of a face operator (left) and a vertex operator (right).

At every edge of the lattice we place a qudit, that is, a $|G|$-dimensional quantum system, with Hilbert space $\mathcal{H}'_G$ with orthonormal basis $\{\,|g\rangle\,|\,g\in G\,\}$. This way, we identify $\mathcal{H}'_G$ with the group algebra $\mathbf{C}[G]$. The Hilbert space for the whole system is then $\mathcal{H}_G := {\mathcal{H}'_G}^{\otimes n}$, with n the number of edges in the lattice. For notational convenience, we will denote the inverse of elements of G as $\bar{g}$ instead of the usual g^{-1}. For completeness, we give a recollection of some basic properties of the group algebra $\mathbf{C}[G]$ in Appendix A.

Usually, when we talk about sites in a lattice we mean its vertices. However, here we will say that a site s is a pair $s=(v,f)$ with f a face and v one of its vertices[18]. The need to consider sites will be clarified later, when we discuss the excitations of the model in terms of strips associated to ribbon operators. This is in contrast with the Abelian case where one only needs to consider strings both in the direct and dual lattices. As it happens, to obtain a non-Abelian generalization we need to consider vertices and faces (plaquettes) in an unified manner through the concepts of sites, and strings and dual strings in an unified manner through the concept of ribbons.

The Hamiltonian of interest, as introduced in [18], is

$$H_G = -\sum_v A_v - \sum_f B_f, \tag{1}$$

where the sums run over vertices v and faces f. The terms A_v and B_f are projectors, called respectively vertex and face operators, or electric and magnetic operators. They commute with each other(B37). In what follows, we give their explicit form.

First, we need a group of local operators at each vertex. We label its elements as A^g_v, $g\in G$, with $A^g_v A^{g'}_v = A^{gg'}_v$ so that they form a representation of G on $\mathcal{H}_G$. The operators A_v act only on those edges that meet at v, and this action depends on the orientation of the edge, inwards or outwards v. For example, for the vertex v of figure (1) we have

$$A^g_v|x,y,z,\cdots\rangle := |gx, y\bar{g}, z\bar{g},\cdots\rangle, \tag{2}$$

where the dots represent other qudits, which do not change. These are the "local gauge transformation"[18] operators. The vertex operators A_v that appear in the Hamiltonian are projectors onto the trivial sector of the representation of G at v, that is

$$A_v := \frac{1}{|G|}\sum_{h\in G} A^h_v. \tag{3}$$

Now let $s=(v,f)$ be a site and p_s denote the closed path with its endpoints in v and running once and counterclockwise through the border of f. That is, p_s is related to an elementary plaquette. We can then consider operators B^g_s, $g\in G$, that project onto those states with value g for the 'product along p_s'. For example, for the site s of figure (1) we have

$$B^g_s|a,b,c,d,\dots\rangle := \delta_{g,a\bar{b}cd}|a,b,c,d,\dots\rangle. \tag{4}$$

These are the "magnetic charge"[18] operators. Note that the orientation of the edges respect to the path is relevant. The face operators B_f that appear in the Hamiltonian are projectors onto the trivial flux, that is

$$B_f := B^1_s, \tag{5}$$

where s is any site with $s=(v,f)$ and 1 is the unit of G. The operator B_f can be labeled just with the face, not with the particular site, because if the flux is trivial for a site then it is so for any other in the same face.

Since the Hamiltonian is a sum of projector operators, the ground state subspace contains those states $|\xi\rangle$ which are left invariant by the action of the vertex and face operators, namely,

$$A_v|\xi\rangle = B_f|\xi\rangle = |\xi\rangle, \tag{6}$$

for every v and f. That is, the projector onto the ground state is

$$P_{\rm GS} = \prod_v A_v \prod_f B_f. \tag{7}$$

In the sphere or the plane, there is no ground state degeneracy[18]. In particular, the ground state can be obtained easily

$$|\psi_G\rangle = P_{\rm GS}\,|\mathbf{1}\rangle = \prod_v A_v\,|\mathbf{1}\rangle, \tag{8}$$

where $|\mathbf{1}\rangle$ is the state with all the qudits in the state $|1\rangle$.

If an eigenstate violates some of the conditions (6) it is an excited state. Note that there is an energy gap from the ground state to excited states and that excitations are localized. If $A_v|\xi\rangle = 0$, then we say that there is an electric quasiparticle at vertex v. If $B_f|\xi\rangle = 0$, then we say that there is a magnetic quasiparticle at face f. In general electric and magnetic charges are interrelated, as we will see, and one says that quasiparticles are dyons that live at sites.

The excitations of these models carry topological charge. Let us explain what this means. First, consider a configuration with several excitations, far apart

from each other. Each of these excitations has a type, a property that can be measured locally and does not change[18]. It is this type what we refer as a topological charge. The point is that there exist certain degrees of freedom with a global, topological nature. In particular, there exists a subsystem which depends on the value of the charges and such that no local measurement is able to distinguish its states[18]. This subsystem is thus protected and a good place to store quantum information. When two quasiparticles get close, some degrees of freedom of the protected subsystem become local. This operation, called fusion, allows to perform measurements. Finally, one can perform unitary operations on the protected subsystem by suitably 'braiding' the excitations.

We will not be concerned with the particular rules that govern the processes of fusion and braiding. Instead, we only want to be able to label the topological charges. But for this, as we shall see, it is enough to study certain ribbon operator algebras, which are introduced next.

B. Ribbon operators

This section is devoted to ribbon operators[18], which will be extensively employed throughout the paper. The main motivation is that ribbon operators describe quasiparticle excitations above the ground state in the Non-Abelian Kitaev model, much like string operators describe the corresponding excitations in the Abelian case. A full account of the properties and definitions for ribbon operators used in this section is presented in Appendix B, specially in B 8 where a basic characterization theorem for ribbon operators is proven.

The basic idea behind ribbon operators is the following. First, ribbons are certain 'paths' that connect sites (not vertices), as shown in Fig. 2. Suppose that for every pair of sites s and s' and for every ribbon ρ connecting them we have at our disposal certain family of operators $\{O^i_\rho\}_i$ with support in the ribbon ρ. In particular, suppose that any state $|\psi\rangle$ with no excitations along ρ except possibly at s and s' can be written as

$$|\psi\rangle = \sum_i O^i_\rho |\psi_i\rangle \tag{9}$$

in terms of certain states $|\psi_i\rangle$ which have no excitations along ρ except possibly at s', but *not* at s. Then, any state can be obtained from states with one excitation less by application of such ribbon operators. In the sphere, where as we will see there are no states with one excitation, this means that any configuration of excited sites can be obtained from the GS by application of ribbon operators connecting these sites. Thus, we are addressing a situation for quasiparticle excitations which clearly resembles that of the Abelian Kitaev model, where strings in the dual and direct lattice have operators attached to them that create excitations at their endpoints.

Before ribbons can be further considered, we need to give more structure to our lattice. In particular, we will

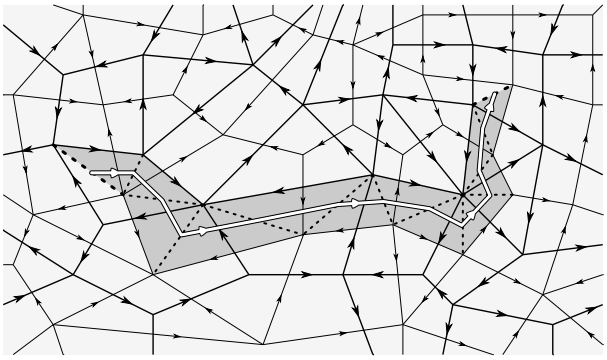


FIG. 2: Thick lines correspond to the lattice and thin lines to the dual lattice. Arrows show the orientation of edges and dual edges. Note that dual edges are oriented in agreement with edges (see explanation in main text). The shaded area is a ribbon. All the sites that form the ribbon are displayed as dashed lines, thicker in the case of the two sites in the ends. The arrowed thick white line shows the orientation of the ribbon.

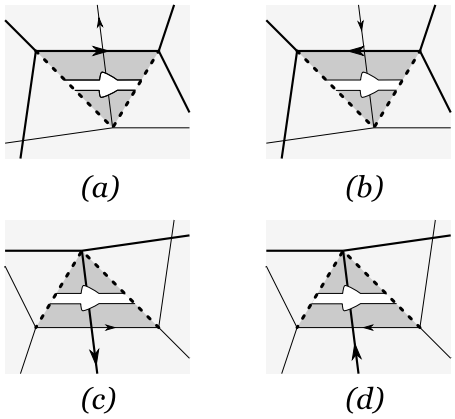


FIG. 3: Each figure represents a triangle τ (shaded area) that connects two sites (dashed lines): $\partial_0\tau$ to the left and $\partial_1\tau$ to the right. Thick lines correspond to the lattice and thin lines to the dual lattice. Arrows show the orientation of edges and dual edges. (a) A direct triangle with an edge which matches its direction. (b) A direct triangle with an edge which does not match its direction. (c) A dual triangle with a dual edge which matches its direction. (d) A dual triangle with a dual edge which does not match its direction.

have to deal with a 'merged' lattice in which the lattice and its dual play a simultaneous role. The reason to consider this merged lattice is that the excitations, as commented above, are related to sites, i.e., pairs $s = (v, f)$ of a vertex and a face. Since the dual of a face is a vertex in the dual lattice, we could equally well say that a site is a pair of a vertex v and a neighboring dual vertex $v' = f^*$. Thus, a site is best visualized as a line connecting these two vertices, as the dashed lines shown in Fig. 2.

In order to have an oriented merged lattice, we orient the edges of the dual lattice in such a way that a dual

edge e^* crosses the edge e 'from right to left', as in Fig. 2. This can be done because we are considering orientable surfaces only. Just as edges connect vertices in a normal lattice, we need something that connects sites in the merged lattice. These connectors turn out to be certain oriented triangles that come into two types: direct and dual triangles. A direct triangle τ is formed with two sites and an edge, as shown in Fig. 3(a,b). The idea is that τ points from a site $\partial_0\tau$ (dashed side to the left) to a site $\partial_1\tau$ (dashed side to the right) through an edge e_τ in the direct lattice. Note that the directions of τ and e_τ can either match or not, as the figure shows. A dual triangle τ' is formed with two sites and a dual edge, see Fig. 3(c,d). Again, it points from a site $\partial_0\tau'$ to a site $\partial_1\tau'$ through an edge $e^*_{\tau'}$, which now belongs to the dual lattice. Again, the directions of τ' and $e^*_{\tau'}$ can either match or not, as the figure shows.

Just as in a usual lattice a list of composable edges forms a path, in the merged lattice a list of composable triangles forms a triangle strip. So a strip is a sequence of triangles $\rho = (\tau_1, \ldots, \tau_n)$ with the end of a triangle being the beginning of the next one, $\partial_1\tau_i = \partial_0\tau_{i+1}$. The ends of a strip are $\partial_0\rho = \partial_0\tau_1$ and $\partial_1\rho = \partial_1\tau_n$. A triangle strip is called a ribbon when it does not self-overlap, except possibly on its ends. A generic example of ribbon is shown in Fig. 2. For a detailed description of triangles, strips and ribbons on a lattice, we refer to Appendix B 1.

Our next task is to attach to each triangle an algebra of operators which is enough to move quasiparticles between its two ends, in the sense of (9). With this aim in mind, we first define triangle operators, which are single qudit operators acting on the edge e_τ of a triangle τ. these operators depend on whether the triangle is direct or dual and on the relative orientation of e_τ. The four possibilities are depicted in Fig. 3. The corresponding operators are

$$\text{(a)}\ \ T^g_\tau|k\rangle = \delta_{g,k}|k\rangle, \qquad \text{(b)}\ \ T^g_\tau|k\rangle = \delta_{\bar{g},k}|k\rangle, \tag{10}$$

$$\text{(c)}\ \ L^g_\tau|k\rangle = |gk\rangle, \qquad \text{(d)}\ \ L^g_\tau|k\rangle = |k\bar{g}\rangle, \tag{11}$$

where $|k\rangle$ is the state of the qudit at the edge e_τ. Thus, the triangle operators T^g_τ of direct triangles are projectors, like the B^g_s, and the triangle operators L^g_τ of dual triangles form a representation of G, like the A^g_v.

We start considering a direct triangle τ. Since direct triangles connect sites with the same face but different vertices, triangle operators for direct triangles must be able to move electric, or vertex, excitations. Let v, v' be the two vertices of τ. Then, as a special case of (B46),

$$|G| \sum_{g\in G} T^g_\tau A_v T^g_\tau = 1. \tag{12}$$

Thus, any state $|\psi\rangle$ can be expressed as

$$|\psi\rangle = \sum_{g\in G} T^g_\tau |\psi_g\rangle \tag{13}$$

with $|\psi_g\rangle = |G| A_v T^g_\tau |\psi\rangle$ an state with no excitation at v because A_v projects out electric excitations. Moreover, T^g_τ commutes with all face operators and all vertex operators apart from those in the ends of τ, so that $|\psi_g\rangle$ has no excited spots which are not already in $|\psi\rangle$, except possibly at v'. These are the properties we were looking for and thus we define the algebra $\mathcal{A}_\tau$ as that with basis $\{T^g_\tau\}_{g\in G}$.

Next we consider a dual triangle τ. Since dual triangles connect sites with the same vertex but different face, triangle operators for dual triangles must be able to move magnetic, or face, excitations. Let f, f' be the two faces of τ. Then, as a special case of (B47),

$$\sum_{g\in G} L^{\bar{g}}_\tau B_f L^g_\tau = 1. \tag{14}$$

Thus, any state $|\psi\rangle$ can be expressed as

$$|\psi\rangle = \sum_{g\in G} L^{\bar{g}}_\tau |\psi_g\rangle \tag{15}$$

with $|\psi_g\rangle = B_f L^g_\tau |\psi\rangle$ an state with no excitation at f, because B_f projects out magnetic excitations. Moreover, L^g_τ commutes with all vertex operators apart from those in the only vertex of τ and all face operators except those from the two faces connected by τ, so that $|\psi_g\rangle$ has no excited sites which are not already in $|\psi\rangle$, except possibly at f'. These are the properties we were looking for and thus we define the algebra $\mathcal{A}_\tau$ as that with basis $\{L^g_\tau\}_{g\in G}$.

Now that we have triangle operators at our disposal, we can move quasiparticles at will, in the sense of (9). In particular, if we want to move an excitation from one end of a ribbon $\rho = (\tau_1, \ldots, \tau_n)$ to the other end, we just proceed triangle by triangle. In other words, we can introduce an algebra $\mathcal{A}_\rho := \bigotimes_i \mathcal{F}_{\tau_i}$ which contains a family of operators $\{O^i_\rho\}$ with the properties related to (9). $\mathcal{A}_\rho$ can be thought of as the algebra of all quasiparticle processes along ρ. Note that it is closed under the adjoint operator, $\mathcal{A}^\dagger_\rho = \mathcal{A}_\rho$.

However, if we are just interested in processes were no quasiparticles are created or destroyed but in the ends of ρ, as is the case for (9), then $\mathcal{A}_\rho$ is just too general. Instead, we consider the ribbon operator algebra $\mathcal{F}_\rho \subset \mathcal{A}_\rho$, which contains those operators that do not create or destroy excitations along ρ. In other words $F \in \mathcal{F}_\rho$ if $[F, A_v] = [F, B_f] = 0$ for any vertex v and face f which do not lie in the ends of ρ. Note that $\mathcal{F}_\rho$ is closed under the adjoint operator because $A_v = A^\dagger_v$, $B_f = B^\dagger_f$. These are the operators we were searching for in (9): a basis of $\mathcal{F}_\rho$ gives the desired operators O^i_ρ, see (B46, B47). $\mathcal{F}_\rho$ can be thought of as the algebra of processes in which a pair of quasiparticles is created in one end of the ribbon and then one of them is moved to the other end. In these terms, it is clear why excited states are expressible by means of ribbon operators acting on ground states.

A particularly meaningful basis for $\mathcal{F}_\rho$, explicitly given in (B66), consists of certain operators $F^{RC;\mathbf{uv}}_\rho$, labeled by C, a conjugacy class of the group G, R, an irreducible representation of certain group $\mathbf{N}_C$ defined below, and the indices $\mathbf{u} = (i, j)$, $\mathbf{v} = (i', j')$ with $i, i' = 1, \ldots, |C|$,

$j, j' = 1, \ldots, n_R$. Here $|C|$ is the cardinality of C and n_R is the degree of the representation R. The group $\mathbf{N}_C$ is defined as that with elements $g \in G$ with $gr_C = r_C g$ for some chosen representative $r_C \in C$. In order to construct the operators $F_\rho^{RC;\mathbf{uv}}$, one also has to choose a particular unitary matrix representation Γ_R for R and enumerate the elements of the conjugacy class as $C = \{c_i\}$, together with a suitable subset $\{q_i\}_{i=1}^{|C|} \subset G$ such that $c_i = q_i r_C \bar{q}_i$. Later we will relate the labels R, C to the topological charges of the model and show how the indices $\mathbf{u}, \mathbf{v}$ are related to local degrees of freedom at both ends of the ribbon. We will use the following notation to denote linear combinations of ribbon operators with the same topological charge label R, C

$$F_\rho^{RC}(\boldsymbol{\alpha}) := \sum_{\mathbf{u},\mathbf{v}} \alpha^{\mathbf{u},\mathbf{v}} F_\rho^{RC;\mathbf{uv}}, \tag{16}$$

where $\alpha^{\mathbf{uv}} \in \mathbf{C}$.

In the case of abelian groups there are no local degrees of freedom and the elements of the basis are $F_\rho^{RC} = F_\rho^{\chi,g}$ with $g \in G$ and χ an element of the character group of G. These operators are unitary and form a group:

$$F_\rho^{\chi,g} F_\rho^{\chi',g'} = F_\rho^{\chi\chi',gg'}, \qquad F_\rho^{\chi,g\,\dagger} = F_\rho^{\bar{\chi},\bar{g}}. \tag{17}$$

Indeed, $T_\rho^\chi := F_\rho^{\chi,1}$ are the string operators of abelian models, and $L_\rho^g := F_\rho^{e,g}$ the co-string operators, with e the identity character.

An essential property of ribbon operators, which reflects the topological nature of the model, is that in the absence of excitations the particular shape of the ribbon is unimportant: We can deform the ribbon while keeping the action of the ribbon operator invariant. More exactly, if the state $|\psi\rangle$ is such that the ribbon ρ can be deformed, with its ends fixed, to obtain another ribbon ρ' without crossing any excitation, then

$$F_\rho^{RC}(\boldsymbol{\alpha})|\psi\rangle = F_{\rho'}^{RC}(\boldsymbol{\alpha})|\psi\rangle. \tag{18}$$

This is illustrated in Fig. 4.

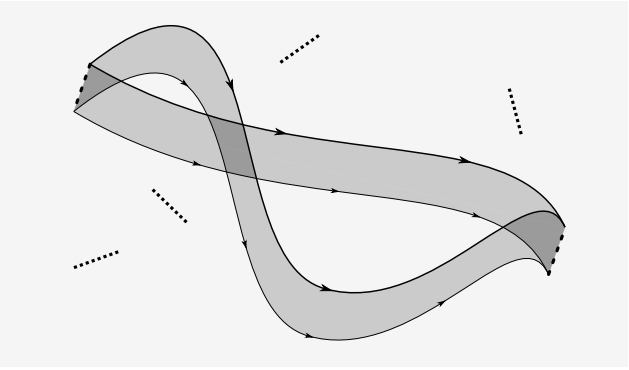


FIG. 4: An example of a deformation of a ribbon. The endpoints are fixed, and the area in between the two ribbons does not contain any excited site, which are represented with dotted lines.

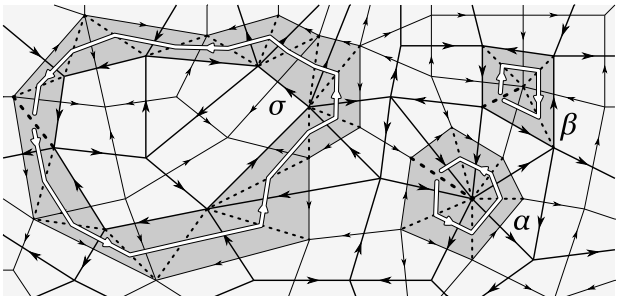


FIG. 5: Three examples of closed ribbons. σ is a proper closed ribbon, containing both dual and direct triangles. It is also a boundary ribbon, as it encloses an area with the topology of a disc. α is a dual closed ribbon and thus encloses a single vertex. β is a direct closed ribbon and thus encloses a single face.

C. Closed ribbons

For a closed ribbon σ we mean one for which both ends coincide, so that we can set $\partial\sigma := \partial_0\sigma = \partial_1\sigma$. In view of the definition of $\mathcal{F}_\rho$, in the case of closed ribbons it is natural to consider a subalgebra $\mathcal{K}_\sigma \subset \mathcal{A}_\sigma$ such that it forgets the single end $\partial\sigma$. With this goal in mind, we let $\mathcal{K}_\sigma \subset \mathcal{A}_\sigma$ contain those operators in $\mathcal{A}_\sigma$ that commute with all vertex and face operators A_v, B_f. In terms of quasiparticle processes, such closed ribbon operators are related to processes in which a pair of quasiparticles is created and one end of them is moved along the ribbon till they meet again to fuse into vacuum. Closed ribbon operators play a fundamental role in characterizing the ground state of the model in a similar fashion as how closed strings are the building blocks for the ground state in the Abelian case (toric code). A detailed analysis of closed ribbon operators is performed in Appendix B 9.

We first consider the smallest examples of closed ribbons, i.e., dual and direct closed ribbons. We say that a ribbon is direct (dual) if it consists only of direct (dual) triangles. A dual ribbon like α in Fig. 5 encloses a single vertex v, and $\mathcal{K}_\alpha$ has as basis the operators A_v^h, $h \in G$. A direct ribbon like β in Fig. 5 encloses a single face f, and $\mathcal{K}_\beta$ has as basis the operators B_f^C. These are labeled by the conjugacy classes C of G and take the form $B_s^C = \sum_{g\in C} B_s^g$ for any $s = (v, f)$. Thus, after defining ribbon operators by means of vertex and face operators, we now see that vertex and face operators are themselves ribbon operators.

As for the rest of closed ribbons σ, which we call proper closed ribbons, it turns out that $\mathcal{K}_\sigma$ has as basis certain orthogonal projectors K_σ^{RC} that form a resolution of the identity, as shown in proposition 9. The labels R, C of these projectors are the same appearing in the basis for $\mathcal{F}_\rho$. In fact, in the next section we will characterize exci-

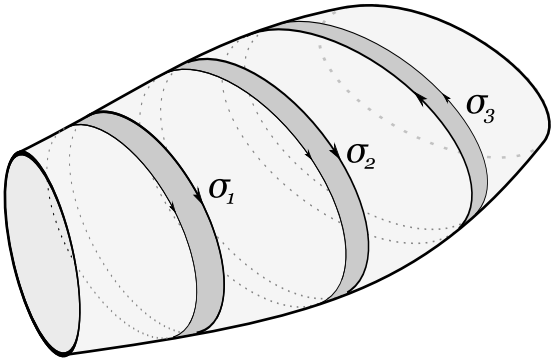


FIG. 6: Examples of closed ribbon transformations. A tubular piece of surface is displayed. The closed ribbon σ_1 is a deformation of σ_2 as long as there are no excitations between them. The ribbon σ_3 has an inverse orientation, and thus to obtain it from σ_2 we have to consider a deformation plus an inversion.

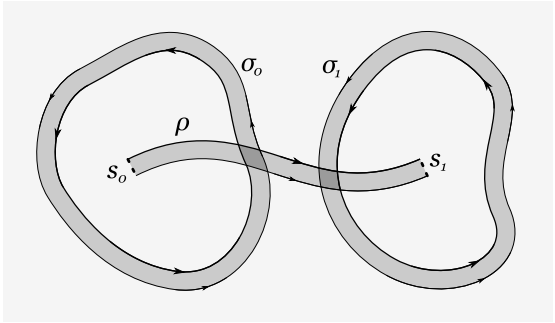


FIG. 7: An open ribbon ρ that connects two sites s_0 and s_1 and two closed ribbons σ_0 and σ_1 that surround counterclockwise s_0 and s_1, respectively. The ribbon operators $F_\rho^{h,g}$ of the open ribbon change the excitations at s_0, s_1. The ribbon operators $K_{\sigma_0}^{RC}$, $K_{\sigma_1}^{\bar{R}\bar{C}}$ of the closed ribbons project the system onto states with a given topological charge at s_0, s_1.

tations in terms of closed ribbon operators.

The algebra $\mathcal{K}_\sigma$ does not see the ends of σ. Because of this, unlike $\mathcal{F}_\sigma$, it can stand deformations in which the end $\partial\sigma$ is not fixed or, for that matter, rotations of the ribbon. More exactly, if the state $|\psi\rangle$ is such that the closed ribbon σ can be deformed to obtain another ribbon σ' without crossing any excitation then

$$K_\sigma^{RC}|\psi\rangle = K_{\sigma'}^{RC}|\psi\rangle, \tag{19}$$

see appendix C 2. This is illustrated in Fig. 6. Another kind of transformation is possible for closed ribbons. In particular, we can consider deformations plus inversions of the orientation of the ribbon, as shown in Fig. 6. When σ' is a transformation of σ which includes an inversion we have

$$K_\sigma^{\bar{R}^C\bar{C}}|\psi\rangle = K_{\sigma'}^{RC}|\psi\rangle. \tag{20}$$

where $\bar{C}$ is the inverse conjugacy class of C, $\bar{R}^C$ is the conjugate representation of R^C and R^C is an irreducible representation of $\mathbf{N}_{\bar{C}}$ defined by $R^C(\cdot) := R(g\cdot\bar{g})$ if $\bar{r}_C = g r_{\bar{C}} \bar{g}$ for some $g \in G$. In the next section we relate this to inversion of topological charge.

D. Topological charges

Let s_0,s_1 be two non-adjacent sites in a lattice embedded in the sphere. From the discussion on ribbon operators it follows that the states

$$|RC;\mathbf{uv}\rangle := F_\rho^{RC;\mathbf{uv}}|\psi_G\rangle \tag{21}$$

form a basis for the subspace with excitations only at s_0 and s_1. Here $|\psi_G\rangle$ is the ground state (8) and ρ is any ribbon with $\partial_i\rho = s_i$.

For each site $s = (v, f)$, we introduce the algebra $\mathcal{D}_s$ with basis $\{D_s^{hg} := A_v^h B_s^g\}_{h,g\in G}$. The reason to introduce it is that its action on an excitation at s gives all possible local action on the excitation [18]. In other words, $\mathcal{D}_s$ is useful to show why $\mathbf{u}, \mathbf{v}$ are just local degrees of freedom. The action of the algebras $\mathcal{D}_{s_i}$ on the states (21) is

$$\begin{aligned} D_{s_0}^{h,g}|RC;\mathbf{uv}\rangle &= \delta_{g,c_i}\sum_{s=1}^{n_R}\Gamma_R^{sj}(n(hq_i))\,|RC;\mathbf{u}(s)\mathbf{v}\rangle,\\ D_{s_1}^{h,g}|RC;\mathbf{uv}\rangle &= \delta_{g,\bar{c}_{i'}}\sum_{s=1}^{n_R}\bar{\Gamma}_R^{sj'}(n(hq_{i'}))\,|RC;\mathbf{uv}(s)\rangle, \end{aligned} \tag{22}$$

where $\mathbf{u} = (i, j)$, $\mathbf{v} = (i', j')$, $\mathbf{u}(s) = (i(hq_i), s)$, $\mathbf{v}(s) = (i(hq_{i'}), s)$ and we set for any $g \in G$ $g =: q_{i(g)}n(g)$ with $n(g) \in \mathbf{N}_C$. Equations (22) are a consequence of (B69, 6).

As shown in detail in appendix D, it is possible to find operators $d_{\mathbf{u}''}^{\mathbf{u}'} \in \mathcal{D}_{s_0}$ and $d_{\mathbf{v}''}^{\mathbf{v}'} \in \mathcal{D}_{s_1}$ with

$$d_{\mathbf{u}''}^{\mathbf{u}'}\, d_{\mathbf{v}''}^{\mathbf{v}'}\,|RC;\mathbf{uv}\rangle = \delta_{\mathbf{u},\mathbf{u}''}\delta_{\mathbf{v},\mathbf{v}''}|RC;\mathbf{u}'\mathbf{v}'\rangle. \tag{23}$$

Thus we see that a state with particular labels $\mathbf{u}$, $\mathbf{v}$ can be transformed with local operators into one with any other labels $\mathbf{u}'$, $\mathbf{v}'$. Roughly speaking, for local operators we mean operators which act on a neighborhood of the excitations. More exactly, local operators should have a support which does not connect excitations.

What about the degrees of freedom related to the labels R and C? They can certainly be measured locally, because there exists a set of projectors $D_{s_0}^{RC} \in \mathcal{D}_{s_0}$ with

$$D_{s_0}^{RC}\,|R'C';\mathbf{uv}\rangle = \delta_{R,R'}\delta_{C,C'}|RC;\mathbf{uv}\rangle. \tag{24}$$

However, R and C cannot be changed locally, in the sense that an operator with a support not connecting both sites and which creates no additional excitations will not change their values. To see this, consider two closed ribbons σ_0 and σ_1 that enclose respectively the sites s_0 and s_1 counterclockwise, as in Fig. 7. From the discussion in appendix C 3 it follows that

$$K_{\sigma_0}^{RC}\,|R'C';\mathbf{uv}\rangle = K_{\sigma_1}^{\bar{R}^C\bar{C}}\,|R'C';\mathbf{uv}\rangle = \delta_{R,R'}\delta_{C,C'}|RC;\mathbf{uv}\rangle. \tag{25}$$

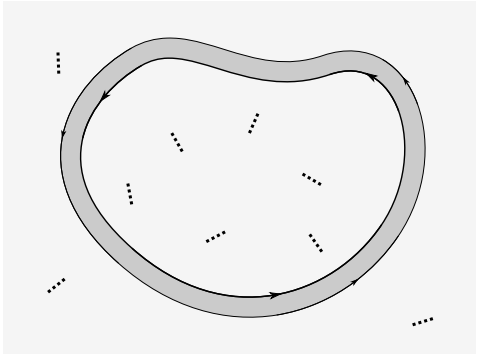


FIG. 8: A boundary ribbon σ that encloses several excitations counterclockwise. The corresponding operators K_σ^{RC} are projectors onto the sector with total topological charge (R, C) inside the ribbon.

Any operator with no common support with σ will commute with the projectors K_σ^{RC}, and thus cannot change the value of R and C. In particular, any operator which changes R and C must have a support that connects the sites s_0 and s_1.

Indeed, the preceding discussion shows that R and C are the labels of the topological charges of the model. Thus the charge of an excitation is the pair (R, C), with C a conjugacy class of G and R an irreducible representation of $\mathbf{N}_C$. If a closed ribbon σ encloses certain amount of excitations, as in Fig. 8, the projectors K_σ^{RC} correspond to sectors with different total topological charge in the region surrounded. If $|\xi\rangle$ is a state with no excitations in the area enclosed by σ, we have

$$K_\sigma^{e\,1}|\xi\rangle = |\xi\rangle, \tag{26}$$

with e the identity representation, see appendix F. Thus, $(e, 1)$ is the trivial charge. This offers a way to describe the ground state of (1) as the space of states for which (26) holds for any boundary ribbon, that is, any closed ribbon enclosing a disc or simply connected region.

In a region with no excitations, quasiparticles can only be locally created in pairs, so that the two excitations have opposite charges and the total charge in the region remains trivial. From (20) or (25) it follows that the opposite of the charge (R, C) is $(\bar{R}^C, \bar{C})$,

E. Single-quasiparticle states

In a sphere there do not exist states with a single excitation. The reason, as shown in Fig. 9, is that any closed ribbon σ divides the sphere in two regions, both of them simply connected. The ribbon σ surrounds one of this region counterclockwise, call it R_1, and the other one clockwise, call it R_2. Then the operator K_σ^{RC} is a projector onto the subspace with total charge (R, C) in R_1, but also a projector onto the subspace with total charge $(\bar{R}^C, \bar{C})$ in R_2. Thus, if there are no excitations in R_1, we have a total charge $(e, 1)$ in R_1 and also a total

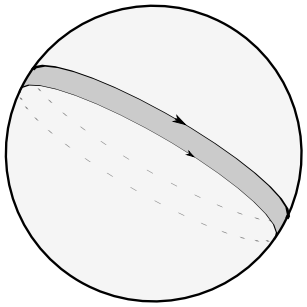


FIG. 9: A closed ribbon in a sphere. Its ribbon operators K_σ^{RC} project onto states with topological charge (R, C) in the upper side of the sphere and $(\bar{R}^C, \bar{C})$ in the lower side.

charge $(e, 1)$ in R_2. But a single excited site cannot have trivial charge, and thus R_2 contains either zero or more than one excitation

What about surfaces with non-trivial topology, such as a torus? In the case of Abelian groups, the situation is the same as in the sphere: there are no states with a single excitation. In the case of vertex excitations, that is, electric charges, this follows from the fact that

$$\prod_{v\in V} A_v^g = 1. \tag{27}$$

For face excitations, that is, magnetic charges, an analogous result holds. For any character χ of G, let $B_f^\chi := \sum_{g\in G} \chi(g) B_s^g$ for $s = (v, f)$. Then

$$\prod_{f\in F} B_f^\chi = 1. \tag{28}$$

For non-Abelian groups, the situation is very different. In fact, examples of single-quasiparticle states can be constructed, see appendix (E).

III. CONDENSATION AND CONFINEMENT

A. The models

We want to modify the Hamiltonian H_G by introducing single qudit terms. In particular, we propose to consider projectors of the form

$$L_\tau^N := \frac{1}{|N|} \sum_{n\in N} L_\tau^n, \qquad T_\tau^M := \sum_{m\in M} T_\tau^m, \tag{29}$$

where τ is a dual or direct triangle and N, M are subgroups of G. Thus L_τ^N projects out the trivial representation of N and T_τ^M selects those states within M. We want to have single qudit operators that do not depend on the orientation of the edge $e = e_\tau$. This is automatic for $T_e^M := T_\tau^M$, but in the case of dual triangles this is true if and only if N is normal, so that we can set $L_e^N := L_\tau^N$. That is, if $n \in N$ and $g \in G$, then $gn\bar{g} \in N$.

Moreover, we want these two kinds of single-qudit terms to commute

$$[L_e^N, T_e^M] = 0, \tag{30}$$

which is true if and only if $N \subset M$.

Now consider a Hamiltonian of the form

$$H = H_G - \mu \sum_e \left(L_e^N + T_e^M \right) \tag{31}$$

where μ is a positive coupling constant and the sum runs over edges e. The problem with this Hamiltonian is that the new terms do not commute with H_G. However, as we show now, we can still consider the limit of large μ. In this limit, the low energy sector is projected out by

$$P := \bigotimes_e T_e^M L_e^N. \tag{32}$$

Let us define the following vertex and face projectors

$$A_v^M := \frac{1}{|M|} \sum_{m \in M} A_v^m, \qquad B_f^N := B_s^N := \sum_{n \in N} B_s^n, \tag{33}$$

where $s = (v, f)$ is a site. Note that B_s^N only depends on f because N is normal. We now make the following observation

$$\begin{aligned} |M| P\, A_v^M\, P &= |G| P\, A_v\, P, \\ P\, B_f^N\, P &= |N|\, P\, B_f\, P. \end{aligned} \tag{34}$$

Thus, studying the low energy sector of (31) for large μ amounts to study the sector with no edge excitations of the Hamiltonian

$$H_G^{N,M} := -\sum_v A_v^M - \sum_f B_f^N - \sum_e \left(T_e^M + L_e^N \right). \tag{35}$$

The point of these Hamiltonians is that all its vertex, face and edge terms commute and thus the ground state of the system can be exactly given. It turns out that it is related to that of (1) but for the group $G' := M/N$, as we will see in the next section. Note that $H_G^{1,G}$ is just the original Hamiltonian (1), up to a constant. Although we have motivated the introduction of (35) through (31), our aim is to study the models H_G^{NM} in their own right, for arbitrary subgroups $N \subset M \subset G$ with N normal.

B. Ground state

The ground state of Hamiltonian (35) is described by the conditions

$$A_v^M |\psi\rangle = B_f^N |\psi\rangle = L_e^N |\psi\rangle = T_e^M |\psi\rangle = |\psi\rangle \tag{36}$$

where v is any vertex, f any face and e any edge. Violations of these conditions amount to vertex, face or edge excitations. Let V be the subspace of states with no edge excitations, which is projected out by the projector P of (32). V is a tensor product of single qudit subspaces $V := \bigotimes_e V_{M/N}$, with $V_{M/N} \subset \mathcal{H}'_G$ the subspace with orthonormal basis:

$$|\tilde{m}\rangle := |N|^{-\frac{1}{2}} \sum_{n \in N} |mn\rangle, \qquad \tilde{m} \in M/N. \tag{37}$$

Thus $V \simeq \mathcal{H}_{M/N}$, that is, within the subspace V we are effectively dealing with qudits of dimension $|M/N|$ which are naturally labeled through the group quotient. We denote the corresponding isomorphism by

$$p : \mathcal{H}_{M/N} \longrightarrow V. \tag{38}$$

Let us write

$$H'_{M/N} := p\; H_{M/N}\; p^{-1}, \tag{39}$$

that is, $H'_{M/N}$ is the Hamiltonian (1), for the group M/N, applied to the subspace $V_{M/N}$. We have

$$H'_{M/N} P = \left(H_G^{N,M} + 2|E| \right) P. \tag{40}$$

Thus, within the sector with no edge excitations we are effectively dealing with the Hamiltonian $H_{M/N}$ (1). Moreover, the ground state of $H_G^{N,M}$ in $\mathcal{H}_G$ is that of $H'_{M/N}$ in V. The projector onto the ground state is

$$P_{\rm GS}^{N,M} := P \prod_v A_v^M \prod_f B_f^N = P \prod_v A'_v \prod_f B'_f \tag{41}$$

where $A'_v := pA_vp^{-1}$, $B'_f := pB_fp^{-1}$ with A_v and B_f acting in $\mathcal{H}_{M/N}$. In the sphere, the normalized ground state is

$$|\psi_G^{N,M}\rangle \propto P_{\rm GS}^{N,M} |\mathbf{1}\rangle \propto \prod_v A'_v |\tilde{\mathbf{1}}\rangle. \tag{42}$$

Thus the new edge terms in the Hamiltonian, which can be thought of as a sort of generalized 'Zeeman terms'[60], have the role of selecting a particular sector of the Hilbert space in which a new non-Abelian discrete gauge symmetry appears, namely $G' = M/N$. Thus, edge terms amount to an explicit symmetry breaking mechanism, since in general the gauge symmetry is reduced, even to a trivial one if $M = N$. Alternatively, we can say that they provide a symmetry-reduction mechanism. Thus, the sector with no edge excitations is completely understood. In the remaining sections we study the meaning of edge excitations.

C. An example

Before we go on with the general case and its details, let us first give a flavor of what is going on by considering a family of examples. We take $N = 1$ and M normal in G, so that the new gauge group is $G' = M$. Note that

in this case we can forget about the L_e^N terms because $L_e^1 = 1$. Our aim is to study the result of applying quasiparticle creation operators (16) on a ground state of the Hamiltonian (35):

$$|\psi\rangle := F_\rho^{RC}(\boldsymbol{\alpha})|\psi_G^{NM}\rangle. \tag{43}$$

We first consider purely magnetic quasiparticle creation operators, fixing R as the identity representation. For simplicity we set $\alpha^{\mathbf{uv}} = c \in \mathbf{C}$. Then from (B69) it follows that $[A_v^M, F^{RC}(\boldsymbol{\alpha})] = 0$ for every vertex v and from (B50) it follows that $[T_e^M, F^{RC}(\boldsymbol{\alpha})] = 0$ for any edge e not in a dual triangle of ρ. Then due to (36) the state $|\psi\rangle$ can have, at most, face excitations on the ends of ρ and edge excitations on dual triangles of ρ. In particular, from (B69, B52,36) it follows that if f is an end face of ρ and e is *any* dual edge of ρ we have

$$B_f^1|\psi\rangle = u|\psi\rangle, \qquad T_e^M|\psi\rangle = u'|\psi\rangle, \tag{44}$$

with $u, u' = 0, 1$. As long as $C \neq 1$, we have $u = 0$ and thus $|\psi\rangle$ contains a pair of face excitations. On the other hand, $u' = 1$ iff $C \subset M$, which means that $|\psi\rangle$ contains a chain of edge excitations along ρ if we try to create magnetic charges which do not belong to the new gauge group G'. Therefore, we find out that some face excitations are confined, in particular those created with $C \not\subset M$. By this, we mean that the energy of $|\psi\rangle$ increases linearly with the length of ρ in terms of dual triangles.

Next, we consider purely electric quasiparticle creation operators, that is, we set $C = 1$. Reasoning in the same way as in the previous case, one finds out that the state $|\psi\rangle$ can have, at most, vertex excitations on the ends of ρ, but no face or edge excitations. In particular, if v is an end vertex of ρ we have

$$A_v^M|\psi\rangle = u|\psi\rangle, \tag{45}$$

with $u = 1$ if the restriction of R to M is an identity representation and $u = 0$ otherwise. That is, in some cases $|\psi\rangle$ is a ground state although R is not trivial. Since there is no local degeneracy in the ground state we know that $|\psi\rangle = c|\psi_G^{NM}\rangle$ for some $c \in \mathbf{C}$. Moreover, c can be nonzero, because, as we will see below, for $\alpha^{\mathbf{uv}} = \delta_{\mathbf{u},\mathbf{v}}$ and R trivial in M

$$\langle F_\rho^{R1}(\boldsymbol{\alpha})\rangle_{\psi_G^{NM}} = 1. \tag{46}$$

Moreover, if σ is any boundary ribbon we have for R trivial in M

$$\langle K_\sigma^{R1}\rangle_{\psi_G^{NM}} = \frac{n_R\,|M|}{|G|}. \tag{47}$$

Thus, those electric charges with trivial restriction of R to M are condensed: they are part of the ground state.

D. Condensation

Let σ be a boundary ribbon, that is, a ribbon that encloses some region r. Motivated by the previous example, we want to study the expectation value in the ground state of H_G^{NM} of the operators K_σ^{RC}. Recall that these operators project onto the space with total topological charge (R, C) in systems with Hamiltonian H_G. Then if for a particular charge type we have

$$\langle K_\sigma^{RC}\rangle := \langle\psi_G^{N,M}|K_\sigma^{RC}|\psi_G^{N,M}\rangle > 0 \tag{48}$$

we say that the charges (R, C) of the original Hamiltonian H_G get condensed in the system with Hamiltonian H_G^{NM}: if one measures the charge of the region r in the ground state of H_G^{NM} there exists some probability of finding the charge (R, C).

As we show in appendix F

$$\langle K_\sigma^{RC}\rangle = \frac{n_R\,|M|}{|G||N|}\,(\chi_R, \chi_{e_M\uparrow})_{\mathbf{N}_C}\,|C \cap N|, \tag{49}$$

where the product $(\cdot,\cdot)_M$ is defined in (A1) and $e_M\uparrow$ is the induced representation in G of the identity representation of M, see appendix A 2. Another way to write the product is

$$(\chi_R, \chi_{e_M\uparrow})_{\mathbf{N}_C} = \frac{1}{|\mathbf{N}_C||M|}\sum_{g\in G}|M_C^g|(\chi_R, 1)_{M_C^g}, \tag{50}$$

where $M_C^g := \mathbf{N}_C \cap \bar{g}Mg$. Note in particular that for M normal the sum has a single term, simplifying the form of (49). The result (49) not only shows that some of the charges are condensed, but also that the expectation value is independent of the shape or size of the ribbon, a feature that underlines the topological nature of the condensation. Such behavior for a perimeter expectation is called a zero law[61].

Let us consider several examples. First, under Kitaev's original Hamiltonian $H_G^{1,G}$ we have

$$\langle K_\sigma^{RC}\rangle = \delta_{C,1}, \delta_{R,e_G} \tag{51}$$

where e_G is the identity representation of G. Thus none of the nontrivial charges is condensed, as expected. In the case $N = M = G$ we have

$$\langle K_\sigma^{RC}\rangle = \frac{|C|}{|G|}\,\delta_{R,e_{\mathbf{N}_C}}, \tag{52}$$

which means that the purely magnetic charges are condensed. On the contrary, in the case $N = M = 1$ we have

$$\langle K_\sigma^{RC}\rangle = \frac{n_R^2}{|G|}\,\delta_{C,1} \tag{53}$$

which means that the purely electric charges are condensed. Another illustrative case is that of an Abelian group G. In that case we can label the projectors as $K_\sigma^{\chi,g}$

with $g \in G$ and χ is an element of the character group of G. Then

$$\langle K_\sigma^{\chi,g} \rangle = \frac{|M|}{|G|\,|N|}\ \delta_{gN,N}\ \delta_{\chi_M,e_M} \tag{54}$$

where χ_M is the restriction of χ to M.

It is possible to show which charges condense using another kind of expectation values, namely those for operators (16), which create a particle-antiparticle pair in the original model (1). From the discussion in appendix F it follows that if $|C \cap N| = \emptyset$ or $(\chi_R, 1)_{M_C^g} = 0$ for all g, we have

$$\langle F_\rho^{RC}(\boldsymbol{\alpha}) \rangle = 0. \tag{55}$$

In the case of M normal, for a charge (R, C) that is not condensed according to (49) the operator $F_\rho^{RC}(\boldsymbol{\alpha})$ always has expectation value zero. Even if M is not normal, if we trace out the local degrees of freedom and set $F_\rho^{RC} := F_\rho^{RC}(\boldsymbol{\alpha})$ with $\alpha^{\mathbf{uv}} = \delta_{\mathbf{u},\mathbf{v}}$ we get

$$\langle F_\rho^{RC} \rangle = \frac{1}{|C|}\,(\chi_R, \chi_{e_M\uparrow})_{\mathbf{N}_C}\,|C \cap N|. \tag{56}$$

Therefore, for that particular choice we get an expectation value which vanishes if an only if (49) does, showing that both approaches agree. Again topology makes its appearance in the fact that the length or shape of the ribbon ρ are not relevant. For Abelian groups (56) reads

$$\langle F_\rho^{\chi,g} \rangle = \delta_{gN,N}\delta_{\chi_M,e_M}. \tag{57}$$

E. Confinement

The example studied in (III C) suggests that the edge terms L_e^N and T_e^M could be interpreted as string tension terms, which in turn would confine some of the charges of the original model H_G. However, one has to be a bit cautious with such a viewpoint in general. Certainly, in those cases in which N is central in M and M is normal (from now on, case I) such a viewpoint makes sense. Only in those cases do certain properties hold, see appendix B 6. In case I we can write the relations, see (B52),

$$P_{e,e'}^{NM}\,F_\rho^{RC;\mathbf{uv}}\,P_{e,e'}^{NM} = d_{RC}^{NM}\,F_\rho^{RC;\mathbf{uv}}\,P_{e,e'}^{NM} \tag{58}$$

where d_{RC}^{NM} equals one (zero) if $C \subset M$ and the restriction of R to $N \subset N_C$ is trivial (in other case), $P_{e,e'}^{NM} = L_e^N T_{e'}^M$ and $e = e_\tau, e' = e_{\tau'}$ with τ, τ' direct and dual triangles in an open ribbon ρ, respectively. The relation (58) show that edge operators project out certain states among those which were created by applying a string operator to a ground state. Note that the projection only takes into account the quasiparticle labels R, C of the string operators. Moreover, it is not important which the particular edges are. Outside of case I such nice properties, reasonable for string tension terms, do not hold. As a consequence of (58), we now that a state of the form (43) will have a chain of edge excitations along ρ unless $C \subset M$ and R is trivial in N: all other charges get confined when moving from H_G to H_G^{NM}, which means that they exist at the end of chains of edge excitations. We shall refer to these chains of excitations as domain walls. They can be labeled just as we labeled topological charges in H_G, something that we will do in the next section.

Unfortunately, as soon as any of the mentioned conditions for case I fails many nice properties of the models are lost. Indeed, only for those systems that fall in that class will we be able to classify domain walls and confined charges in terms of open an closed ribbon operator algebras, in the fashion of what we already did for topological charges in H_G. On the other hand, in certain more general cases it is still possible to classify domain wall types. In particular, we will show that this can be done in all models with N abelian (from now on, the case II). Interestingly enough, the domain wall fluxes in case II are qualitatively richer than in case I. Such fluxes have in general a non-abelian character for case II systems, whereas for case I they have always an abelian nature.

F. Case I systems

This section is devoted to those models $H_G^{N,M}$ with N central in M and M normal in G. We will show that edge excitations appear in the form of domain walls that terminate in certain site excitations which are therefore confined. With this goal in mind, we start introducing the excitations which will turn out to be confined. Consider the projectors

$$A_v^N := \frac{1}{|N|}\sum_{n\in N} A_v^n, \qquad B_f^M := B_s^M = \sum_{m\in M} B_s^m. \tag{59}$$

They commute among each other and with the terms of Hamiltonian (35), so that we could choose the energy eigenstates to be eigenstates of the projectors (59). We say that the state $|\psi\rangle$ has a confined excitation at a site $s = (v, f)$ whenever $A_v^N B_f^M |\psi\rangle = 0$. That these are really excitations follows from

$$A_v^N B_f^M |\psi\rangle = 0 \quad \Longrightarrow \quad A_v^M B_f^N |\psi\rangle = 0, \tag{60}$$

where we have used $A_v^N A_v^M = A_v^M$ and $B_f^M B_f^N = B_f^N$. That they are really confined will be revealed later, but we can already give a clue: a state with a confined excitation at the site s must have an edge excitation at least at one of the edges e meeting at v or in the border of f. Thus, confined excitations cannot appear isolated: there must be edge excitations around them. Conversely, it is also true that a chain of edge excitations cannot terminate without a confined excitation in its end. However, this is not enough to demonstrate confinement, but we can do it better by introducing suitable ribbon operator algebras.

1. Open ribbon operators.

Domain walls have a type, and this type behaves as a flux in the absence of confined excitations. We thus need a family of projectors that distinguish between the domain wall fluxes that cross a particular line, analogous to the projectors K_σ^{RC} that distinguished the topological charge in a the area enclosed by σ. So we consider as our starting point the ribbon operator algebra $\mathcal{F}_\rho$ for an open ribbon ρ. Since the flux should be the same if we move the ends of our flux-measuring ribbon in an area with no edge excitations, we need a ribbon algebra which to some extent forgets the ends of the ribbon. In particular, we should choose ribbon operators that do not create or destroy excitations. Thus, we define $\mathcal{J}_\rho \subset \mathcal{F}_\rho$ as the subalgebra containing those operators $F \in \mathcal{F}_\rho$ which commute with all vertex operators A_v^M and face operators B_f^N. Such operators also commute with all edge terms L_e^N and T_e^M, see colollary 12.

As we show in proposition 11, $\mathcal{J}_\rho$ is linearly generated by certain orthogonal projectors $J_\rho^{\chi t}$ that form a resolution of the identity. The labels (χ, t) of these projectors are χ, an element of the character group of N, and t, an element of the quotient group G/M. If $|\psi\rangle$ has no edge excitations along ρ then

$$J_\rho^{e1}|\psi\rangle = |\psi\rangle, \tag{61}$$

where e and 1 are both identity elements, see (F4, B85).

The algebra $\mathcal{J}_\rho$ can stand deformations in which the ends of ρ are not fixed. More exactly, if the state $|\psi\rangle$ is such that the open ribbon ρ can be deformed, without fixing its ends, to obtain another ribbon ρ' in such a way that no confined excitations are crossed and the ends do not touch edge excitations, then

$$J_\rho^{\chi t}|\psi\rangle = J_{\rho'}^{\chi t}|\psi\rangle, \tag{62}$$

see appendix C 2. This is illustrated in Fig. 10. As in the case of closed ribbons in H_G, here we can consider inversions in the orientation of the ribbon, as shown in Fig. 10. When ρ' is a transformation of ρ which includes an inversion we have

$$J_\rho^{\chi t}|\psi\rangle = J_{\rho'}^{\bar{\chi}^t \bar{t}}|\psi\rangle, \tag{63}$$

where for any $n \in N$ we set $\chi^t(n) := \chi(tn\bar{t})$, see appendix C 2.

When a ribbon ρ_2 crosses two domain walls which are respectively crossed by two other ribbons ρ_3, ρ_4 with the same orientation as ρ, as in Fig. 12, we have

$$J_{\rho_2}^{\chi t} = \sum_\xi \sum_{k \in G/M} J_{\rho_3}^{\bar{\xi}^k \bar{k}} J_{\rho_4}^{\xi\chi\, kt}, \tag{64}$$

where ξ runs over the group of characters, see appendix B 10.

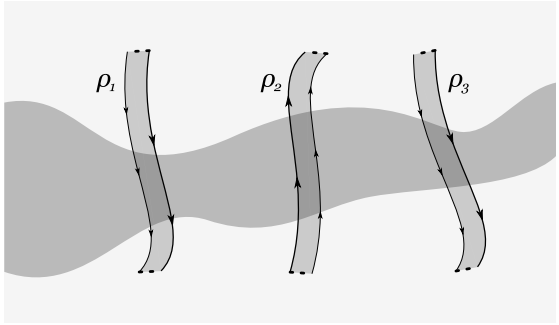


FIG. 10: Examples of open ribbon transformations for $\mathcal{J}_\rho$. Edge excitations are present only in the shaded area. No confined quasiparticle excitations are present. The ribbon ρ_1 is a deformation of ρ_3, and ρ_2 has an inverse orientation with respect to them.

2. Closed ribbon operators.

Before we can further analyze the consequences of the properties of $\mathcal{J}_\rho$, as we shall do in the next section, we have to introduce a family of projectors that distinguish the charges in our models. The situation is different to the one we found in the models H_G, because now some charges are confined, and thus the rules for deforming closed ribbons will change qualitatively to reflect this fact. Our starting point is the ribbon operator algebra $\mathcal{F}_\sigma$ for a closed ribbon σ, from which we want to select certain suitable operators, just as we did for other projector algebras. In the case of open ribbons just considered, we made this selection requiring that the operators commuted with all vertex and face terms. Here that will not be enough, because since σ is closed we would be considering operators that create a closed domain wall, with no ends and no confined excitations. Therefore, we define $\mathcal{K}'_\sigma \subset \mathcal{F}_\sigma$ as the subalgebra containing those operators $K \in \mathcal{F}_\sigma$ which commute with all vertex operators A_v^M, face operators B_f^N and edge operators L_e^N, T_e^M.

As we show in proposition 14, $\mathcal{K}'_\sigma$ is linearly generated by certain orthogonal projectors K_σ^{RC} that form a resolution of the identity. The labels (R, C) of these projectors are C, a set of the form $\{\, mg\bar{m} \,|\, m \in M \,\}$ for some g in G, and R, an irreducible representation of the group $\mathbf{N}'_C := \{\, m \in M \,|\, mr_C\bar{m}\bar{r}_C \in N \,\}$ for some fixed $r_C \in C$. If σ is a boundary ribbon surrounding an area with no vertex or face excitations in the state $|\psi\rangle$, then

$$K_\sigma^{e1}|\psi\rangle = |\psi\rangle, \tag{65}$$

where e and 1 are both identity elements, see (F6, B86, B75).

The algebra $\mathcal{K}'_\sigma$ can stand deformations in which the end $\partial\sigma$ is not fixed, as long as it crosses no domain walls. If the state $|\psi\rangle$ is such that the open ribbon σ can be deformed to obtain another ribbon σ' in such a way that no vertex or face excitations are crossed and the end of

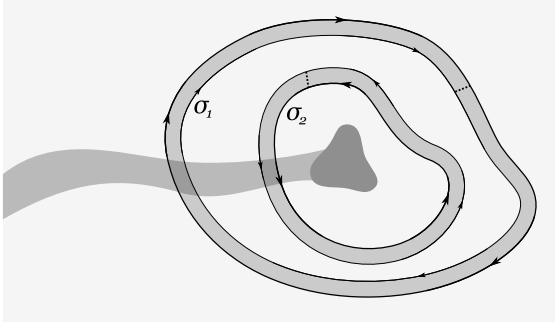


FIG. 11: Examples of closed ribbon transformations for $\mathcal{K}'_\rho$. The light shaded area represents edge or domain wall excitations, and the dark shaded area confined quasiparticle excitations. The ribbon σ_1 is a deformation of σ_2 which includes an inversion.

σ touches no edge excitations, then

$$K^{RC}_\sigma|\psi\rangle = K^{RC}_{\sigma'}|\psi\rangle, \tag{66}$$

see appendix C 2. This is illustrated in Fig. 11. As in the case of closed ribbons in H_G, here we can consider inversions in the orientation of the ribbon, as shown in Fig. 11. When σ' is a transformation of σ which includes an inversion we have

$$K^{RC}_\sigma|\psi\rangle = K^{\bar{R}^C\bar{C}}_{\sigma'}|\psi\rangle, \tag{67}$$

where R^C is an irreducible representation of $\mathbf{N}'_{\bar{C}}$ defined by $R^C(\cdot) := R(m\cdot\bar{m})$ if $\bar{r}_C = mr_{\bar{C}}\bar{m}$ for some $m \in M$, see appendix C 2.

3. *Domain walls and charges.*

The deformation properties of the projectors in $\mathcal{J}_\rho$ that we have introduced indicate that edge excitations appear in the form of domain walls to which a flux can be attached. Branching points are possible in these walls. Each value of the flux corresponds to a projector $J^{\chi t}_\rho$, and we know that it is preserved along a domain wall due to the deformation property (62). The trivial flux is given by (61) and the inverse flux by (63). Since deformations of $J^{\chi t}_\rho$ only require that no confined excitations are crossed, a domain wall can only end in the presence of confined excitations. Domain wall fluxes have an abelian nature: as indicated by (64), the addition of two given fluxes always produces the same combined flux. All these ideas are reflected in Fig. 12.

Regarding charge labeling, the properties of the projectors in $\mathcal{K}'_\sigma$ very much resemble those already found in the study of $\mathcal{K}_\sigma$ in systems with Hamiltonian H_G. The trivial charge is given by (65) and the inverse charge by (67). Indeed, the new element that appears is that now the deformation properties (66) take into account that the charge could be attached to a domain wall.

But if we want to neatly describe confinement, we have to establish the relationship between domain walls and charges. To this end, consider Fig. 12. We can deform each ribbon ρ_i, without changing the flux it measures, till ρ_i is equal to σ_i, the boundary ribbon enclosing the charge at the end of the domain wall. At that point we can compare both projector algebras, with the following result: there exists a function f onto the group character of N such that

$$J^{\chi t}_\sigma = \sum_{C\subset tM}\sum_R \delta_{\chi,f(R)}K^{RC}_\sigma, \tag{68}$$

where the sum on R runs over irreducible representations in $\mathbf{N}'_C$, see (B90). Equation (68) tells us at the end of which domain walls can each charge exist. In other words, the projectors in $\mathcal{J}_\sigma$ classify charge types from $\mathcal{K}'_\sigma$ in different compartments or sectors: each of these sectors gives a confined charge type. The different charge labels within a sector give us the topological part of the charge. In particular, for the trivial confined charge we recover the topological charge types for a system with Hamiltonian $H_{M/N}$, in accordance with the study of the ground state of section III B. Finally, all charges which do not belong to the trivial confined charge sector are indeed confined, because if we take any circle surrounding them we must always have a domain wall crossing it. When excitations are localized in a single site, it turns out that confined excitations are exactly described, as expected, by the projectors (59).

As we already did in the particular case of H_G models, the ground state can be described in terms of ribbon operators of arbitrary size. In this case, we have to impose that no region should contain a nontrivial charge *and* no line should be crossed by a nontrivial domain wall flux. That is, a state ξ is a ground state if and only if

$$K^{e1}_\sigma|\xi\rangle = |\xi\rangle, \qquad J^{e1}_\rho|\xi\rangle = |\xi\rangle, \tag{69}$$

for all boundary ribbons σ and proper ribbons ρ. This conditions generalize to arbitrary N and M, see appendix F.

G. Case II systems

This section is devoted to those models $H^{N,M}_G$ with N abelian. As we have already commented, in this case we will only be able to describe, using ribbon projector algebras, domain wall fluxes, but not charge types, except those in the sector with no edge excitations which are already classified through the mapping to $H_{M/N}$. Thus we proceed to describe the algebra $\mathcal{J}_\rho$, which is defined exactly as in case I. As discussed in appendix B 10, in this case the projectors are J^{RT}_ρ with T an element of the double coset $M\backslash G/M$ and R an induced representation in $\mathbf{N}_T$ of an irreducible representation in N, with $\mathbf{N}_T$ the group $\{\, m\in M \,|\, mr_TM = r_TM \,\}$ for some fixed $r_T \in T$. We recall that each element of the double coset takes the form $T = \{\, mr_Tm' \,|\, m, m' \in M \,\}$. From the double coset structure, we can obtain a subalgebra of the group

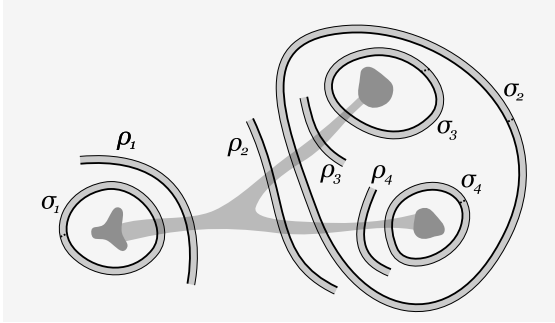


FIG. 12: An illustration of the relationship between domain wall fluxes and quasiparticle charges. The light shaded area represents edge or domain wall excitations, and the dark shaded area quasiparticle excitations. Each of the open ribbons ρ_i can be deformed to the boundary ribbon σ_i, so that the domain wall flux measured by ρ_i corresponds to the confined charge measured by σ_i. Since ρ_1 and ρ_2 are equivalent up to an inversion, the confined charges measured by σ_1 and σ_2 are inverses. The total flux in ρ_2 is the combination of that in ρ_3 and ρ_4, and thus the confined charge measured by σ_2 is the combination of that measured by σ_3 and σ_4.

algebra $\mathbf{C}(G)$. Indeed, for $T, T' \in M\backslash G/M$ we have

$$TT' = \sum_{T'' \in M\backslash G/M} C_{TT'}^{T''}\, T'', \tag{70}$$

where $C_{TT'}^{T''}$ are positive integers. The rules for deformations of J_ρ^{RT}, discussed in appendix C 2, state that the ribbon ρ can move across regions in which $B_f^N|\psi\rangle = |\psi\rangle$ and $A_v^N|\psi\rangle = |\psi\rangle$ are satisfied, and the ends can be displaced as long as they do not touch edge excitations, with the result that the flux measured by J_ρ^{RT} does not change. The inverse flux of (R,T) is $(\bar{R}^T, \bar{T})$, where $\bar{M}$ contains the inverses of the elements of M and R^T is defined by $R^T(\cdot) := R(r_T m \cdot \bar{m}\bar{r}_T)$ if $m \in M$ is such that $M = r_T m r_{\bar{T}} M$. Finally, there is no analog of (64), in the sense that the knowledge of two fluxes is not enough to determine the total combined flux. This can be seen for example in (70). When M is normal (case I), the sum is reduced to a single term, so that combining a flux (e,T) with a flux (e,T') will give certain determinate total flux (e,T''). This is no longer true when M is not normal (case II), giving a non-abelian nature to the domain wall fluxes, which disappears in case I.

IV. CONCLUSIONS

In this paper we have introduced a family of quantum lattice Hamiltonians with a discrete non-Abelian gauge symmetry such that the standard Kitaev model for topological quantum computation is a particular case of this class. The ground state of the models can be exactly given and, in many cases, quasiparticles or at least domain wall excitations can be classified. They can be characterized by operator algebras corresponding to closed and open ribbon operators. This is done in full generality for arbitrary topologies. The models can be understood in terms of topological charge condensation and confinement with respect to the standard Kitaev models.

We have given a detailed account of the quasiparticle excitations in the standard non-Abelian Kitaev model. In particular, we have seen that for orientable closed surfaces other than the sphere, like the torus, excitations may show up in the form of single quasiparticles.

One of the features exhibited by the family of non-Abelian models considered in this paper is the existence of a string tension for the motion of quasiparticle excitations. It would be interesting to study the role of such tensions when the action of external source of decoherence such as local external fields or thermal effects are studied [30], [62]. Another aspect that deserves further study is the properties of these models for topological quantum computation, since here we have only focused on their properties as far as topological order is concerned.

Acknowledgements We acknowledge financial support from a PFI grant of the EJ-GV (H.B.), DGS grants under contracts BFM 2003-05316-C02-01, FIS2006-04885 (H.B., M.A.M.D,), and the ESF Science Programme INSTANS 2005-2010 (M.A.M.D.).

APPENDIX A: GROUP ALGEBRAS

We present some basic properties of the algebras of finite groups. We will find them useful for establishing several results on ribbon operator algebras in the next section. In particular, we need them to label the charges and domain walls of our models.

1. Representations and classes

Given a finite group G, let $(G)_{\rm cj}$ be the set of conjugacy classes of G and $(G)_{\rm ir}$ be the set of irreducible representations of G, up to isomorphisms[63]. For $R \in (G)_{\rm ir}$, $g \in G$, we denote by R_g the image of g under R and by $\Gamma_R(g)$ the unitary matrix of R_g in a particular basis. The character of a representation R is $\chi_R(g) := \sum_i \Gamma_R^{ii}(g)$. Characters are examples of class functions $\phi, \psi : (G)_{\rm cj} \longrightarrow \mathbf{C}$, for which we introduce the product [63]

$$(\phi,\psi)_G := \frac{1}{|G|} \sum_{C \in (G)_{\rm cj}} |C|\, \phi(C)\, \bar{\psi}(C), \tag{A1}$$

where the bar denotes complex conjugation.

The following are the well-known orthogonality relations for irreducible representations, characters and con-

jugacy classes [63]

$$\sum_{g\in G}\Gamma_R^{ij}(g)\bar{\Gamma}_{R'}^{i'j'}(g)=\frac{|G|}{n_R}\delta_{R,R'}\delta_{i,i'}\delta_{j,j'},\qquad\text{(A2)}$$

$$\sum_{C\in(G)_{\rm cj}}|C|\,\chi_R(C)\,\bar{\chi}_{R'}(C)=|G|\,\delta_{R,R'},\qquad\text{(A3)}$$

$$\sum_{R\in(G)_{\rm ir}}\chi_R(C)\bar{\chi}_R(C')=\frac{|G|}{|C|}\,\delta_{C,C'},\qquad\text{(A4)}$$

where $R,R'\in(G)_{\rm ir}$, $C,C'\in(G)_{\rm cj}$ and $n_R=\chi_R(1)$ is the degree of R. (A3,A4) imply that $|(G)_{\rm cj}|=|(G)_{\rm ir}|$. The identities (A3), which are just a particular case of (A2), can be written more concisely as $(\chi_R,\chi_{R'})_G=\delta_{R,R'}$.

2. Induced representations

Given a finite group G and a normal subgroup $H\subset G$, let $(H,G)_{\rm cj}$ be the set of conjugacy classes of G contained in H and $(H,G)_{\rm ir}$ be the set of induced representations in G of irreducible representations in H, up to isomorphisms[63]. Recall that for each representation R of H there exists a representation $R_{\rm Ind}$, called the induced representation of R in G, such that for $g\in G$

$$\chi_{R_{\rm Ind}}(g):=\begin{cases}\sum_{r\in G/H}\chi_R(rg\bar{r}), & g\in H,\\ 0, & g\notin H.\end{cases}\qquad\text{(A5)}$$

The Frobenius reciprocity formula asserts that for $\phi:(G)_{\rm cj}\longrightarrow\mathbf{C}$ and $R\in(H)_{\rm ir}$

$$(\phi|_H,\chi_R)_H=(\phi,\chi_{R_{\rm Ind}})_G,\qquad\text{(A6)}$$

where $\phi|_H$ is the restriction of ϕ to H.

Let us introduce an equivalence relation in $(H)_{\rm cj}$. For $D,D'\in(H)_{\rm cj}$, we set $D\sim D'$ if $D'=gD\bar{g}$ for some $g\in G/H$. Each $C\in(H,G)_{\rm cj}$ is related to a unique equivalence class $\tilde{C}$ in the following way

$$C=\bigcup_{D\in\tilde{C}}D.\qquad\text{(A7)}$$

Given $S\in(H)_{\rm ir}$ and $r\in G/H$, define a representation $S^r\in(H)_{\rm ir}$ setting $S^r_h:=S_{rh\bar{r}}$. We introduce an equivalence relation in $(H)_{\rm ir}$. For $S,S'\in(H)_{\rm ir}$, we set $S\sim S'$ if $S=S^g$ for some $g\in G/H$. Each $R\in(H,G)_{\rm ir}$ is related to a unique equivalence class $\tilde{R}$ in the following way

$$\chi_R(g)=\begin{cases}\frac{|G|}{|H||\tilde{R}|}\sum_{S\in\tilde{R}}\chi_S(g), & g\in H,\\ 0, & g\notin H,\end{cases}\qquad\text{(A8)}$$

and $S\in\tilde{R}$ iff $S_{\rm Ind}=R$.

As a generalization of (A3,A4) we have the following orthogonality relations

$$\sum_{C\in(H,G)_{\rm cj}}|C|\,\chi_R(C)\,\bar{\chi}_{R'}(C)=\frac{|G|^2}{|H|\,|\tilde{R}|}\,\delta_{R,R'},\qquad\text{(A9)}$$

$$\sum_{R\in(H,G)_{\rm ir}}|\tilde{R}|\,\chi_R(C)\,\bar{\chi}_R(C')=\frac{|G|^2}{|H|\,|C|}\,\delta_{C,C'},\qquad\text{(A10)}$$

where $R,R'\in(H,G)_{\rm ir}$ and $C,C'\in(H,G)_{\rm cj}$. (A9,A10) imply that $|(H,G)_{\rm cj}|=|(H,G)_{\rm ir}|$. Note that (A9) can be rewritten in terms of the product $(\cdot,\cdot)_G$ and derived from (A6) as follows:

$$(\chi_R,\chi_{R'})_G=(\chi_{S_0},\chi_{R'})_H=\frac{|G|}{|H|\,|\tilde{R}|}\,\delta_{R,R'},\qquad\text{(A11)}$$

where $S_0\in\tilde{R}$. As for (A10), it follows from (A8, A4)

$$\begin{aligned}&\sum_{R\in(H,G)_{\rm ir}}|\tilde{R}|\,\chi_R(C)\,\bar{\chi}_R(C')=\\ &=\sum_{R\in(H,G)_{\rm ir}}\frac{|G|^2}{|H|^2|\tilde{R}|}\sum_{S,S'\in\tilde{R}}\chi_S(D_0)\,\bar{\chi}_{S'}(D_0')=\\ &=\sum_{g\in G/H}\sum_{R\in(H,G)_{\rm ir}}\frac{|G|}{|H|}\sum_{S\in\tilde{R}}\chi_S(D_0)\,\bar{\chi}_S(gD_0'\bar{g})=\\ &=\frac{|G|}{|D_0|}\sum_{g\in G/H}\delta_{D_0,gD_0'\bar{g}}=\frac{|G|^2}{|H|\,|C|}\,\delta_{C,C'},\end{aligned}\qquad\text{(A12)}$$

where $D_0\in\tilde{C}$, $D_0'\in\tilde{C}'$.

3. The group algebra $\mathbf{C}[G]$

Given a finite group G, the group algebra $\mathbf{C}[G]$ consists of formal sums $\sum_{g\in G}c_g g$, $c_g\in\mathbf{C}$. We are interested in certain representation $\mathcal{R}:\,G\times G\longrightarrow\mathbf{GL}(\mathbf{C}[G])$. Let us denote by $\mathcal{R}_{g_1,g_2}$ the image of $(g_1,g_2)\in G\times G$. Then $\mathcal{R}$ is defined by:

$$\mathcal{R}_{g_1,g_2}(g):=g_1g\bar{g}_2,\qquad g\in G,\qquad\text{(A13)}$$

where $\bar{g}$ denotes the inverse of g. It turns out that the following isomorphism holds, as we shall check below,

$$\mathbf{C}[G]\simeq\sum_{R\in(G)_{\rm ir}}V_R\otimes V_{\bar{R}}\qquad\text{(A14)}$$

where V_R is the representation space of R.

With the aim of checking (A14) explicitly, let us consider the following elements of $\mathbf{C}[G]$:

$$e_R^{ij}:=\frac{n_R}{|G|}\sum_{g\in G}\bar{\Gamma}_R^{ij}(g)\;g\qquad\text{(A15)}$$

where R is a representation of G and $i,j=1,\ldots,n_R$. For irreducible R, there are $|G|$ such elements, because $\sum_{R\in(G)_{\rm ir}}n_R^2=|G|$ due to (A14). In fact, they give a new basis for $\mathbf{C}[G]$:

$$g=\sum_{R\in(G)_{\rm ir}}\sum_{i,j=1}^{n_R}\Gamma_R^{ij}(g)\;e_R^{ij},\qquad\text{(A16)}$$

which can be checked using (A4). In this basis

$$\mathcal{R}_{g_1,g_2}\;e_R^{ij}=\sum_{k,l=1}^{n_R}\Gamma_R^{ki}(g_1)\bar{\Gamma}_R^{lj}(g_2)\;e_R^{kl},\qquad\text{(A17)}$$

which gives explicitly the isomorphism (A14), as desired. Let us define

$$\overline{\left(\sum_g c_g\, g\right)} := \sum_g \bar{c}_g\, \bar{g}. \tag{A18}$$

Then, we have

$$e^{ij}_R e^{i'j'}_{R'} = \delta_{R,R'}\delta_{j,i'}\; e^{ij'}_R, \qquad \bar{e}^{ij}_R = e^{ji}_R. \tag{A19}$$

which follow from (A2).

4. The algebra $\mathcal{Z}_G$

The center of a group algebra $\mathbf{C}[G]$, denoted $\mathcal{Z}_G$, is the subalgebra of elements that commute with all the elements of $\mathbf{C}[G]$. A basis for the center of $\mathbf{C}[G]$ is the following:

$$e_C := \sum_{g\in C} g \qquad\qquad C \in (G)_{\rm cj}. \tag{A20}$$

We have

$$e_C e_{C'} =: \sum_{C''\in(G)_{\rm cj}} N^{C''}_{C,C'} e_{C''}, \qquad \bar{e}_C = e_{\bar{C}}, \tag{A21}$$

where $\bar{C}$ denotes the inverse class of C and $N^{C''}_{C,C'} \geq 0$ are integers.

With the aim of finding an alternative basis for $\mathcal{Z}_G$, we define

$$e_R := \sum_i e^{ii}_R, \qquad R \in (G)_{\rm ir}, \tag{A22}$$

which are a nice set of projectors:

$$\begin{aligned} e_R e_{R'} &= \delta_{R,R'} e_R, \\ \bar{e}_R &= e_R, \\ \sum_{R\in(G)_{\rm ir}} e_R &= 1, \end{aligned} \tag{A23}$$

as follows from (A4). They provide us with a new basis for $\mathcal{Z}_G$ since

$$e_R = \frac{n_R}{|G|} \sum_{C\in(G)_{\rm cj}} \bar{\chi}_R(C)\; e_C, \tag{A24}$$

$$e_C = \sum_{R\in(G)_{\rm ir}} \frac{|C|}{n_R} \chi_R(C)\; e_R, \tag{A25}$$

as can be checked using (A4).

5. The algebra $\mathcal{Z}_{H,G}$

Let H be a normal subgroup of G. There is a natural inclusion $\mathbf{C}[H] \subset \mathbf{C}[G]$. We are interested in the intersection of their centers $\mathcal{Z}_{H,G} := \mathcal{Z}_H \cap \mathcal{Z}_G$. A basis for the algebra $\mathcal{Z}_{H,G}$ is

$$e^G_C := \sum_{g\in C} g \qquad\qquad C \in (H,G)_{\rm cj}. \tag{A26}$$

Its elements can be rewritten in terms of elements of $\mathcal{Z}_H$ as follows

$$e^G_C = \sum_{D\in\tilde{C}} e^H_D = \frac{|H|\,|\tilde{C}|}{|G|} \sum_{g\in G/H} g e^H_D \bar{g}, \tag{A27}$$

where we are using the notation of (A7).

We have the aim of finding a basis of projectors for $\mathcal{Z}_{H,G}$, analogous to (A23). Let

$$e'_R := \frac{|H|\,|\tilde{R}|}{|G|} e^G_R = \sum_{S\in\tilde{R}} e^H_S, \qquad R \in (H,G)_{\rm ir}, \tag{A28}$$

so that,

$$\begin{aligned} e'_R e'_{R'} &= \delta_{R,R'} e'_R, \\ {e'_R}^{\dagger} &= e'_R, \\ \sum_{R\in(H,G)_{\rm ir}} e'_R &= 1, \end{aligned} \tag{A29}$$

showing also that the e_R are linearly independent. Indeed, $\{\, e'_R \,|\, R \in (H,G)_{\rm ir} \,\}$ is the desired projector basis for $\mathcal{Z}_{H,G}$, because we have

$$e'_R = \frac{n_R\,|\tilde{R}|\,|H|}{|G|^2} \sum_{C\in(H,G)_{\rm cj}} \bar{\chi}_R(C)\, e^G_C, \tag{A30}$$

$$e^G_C = \sum_{R\in(H,G)_{\rm ir}} \frac{|C|}{n_R} \chi_R(C)\, e'_R, \tag{A31}$$

where $R \in (H,G)_{\rm ir}$ and $C \in (H,G)_{\rm cj}$. In order to check (A31), insert (A30) and apply (A10). Finally, not that if H belongs to the center of G we have $e'_R = e^H_R$.

APPENDIX B: RIBBON OPERATORS

In this appendix we discuss ribbon operator algebras. We will first introduce the geometric aspects of ribbons, then we will attach operators to ribbons, and we will finish describing and characterizing certain projector ribbon subalgebras. These projectors are directly related to the topological charges and domain wall fluxes in the models under study.

1. Sites, triangles and strips

Our starting point is a lattice embedded in an orientable two-dimensional manifold. Let V, E and F be the sets of its vertices, edges and faces respectively. The

edges of the direct and dual lattices must be oriented accordingly, as explained in the main text in sect.II and Fig.1. A direct edge e points from the vertex $\partial_0 e$ to the vertex $\partial_1 e$, and a dual edge e^* points from the dual vertex $\partial_0 e^*$ to the dual vertex $\partial_1 e^*$. The shape of the lattice is arbitrary, but with certain conditions. Namely *(i)* if e is an edge, then $\partial_0 e \neq \partial_1 e$ and *(ii)* a face with s edges must have s different vertices. The same conditions must hold for the dual lattice.

For each edge $e \in E$, we introduce an inverse edge $\bar{e}$ which is an edge with the direction reversed,i.e., with $\partial_0 \bar{e} = \partial_1 e$ and $\partial_1 \bar{e} = \partial_0 e$. We let $\bar{\bar{e}} = e$ and denote by $E_{\text{ext}} := E \cup \bar{E}$ the disjoint union of the original and inverse edges. For dual edges, we set $\overline{(e^*)} = (\bar{e})^*$ so that $E^*_{\text{ext}} = E^* \cup \bar{E}^*$.

A (direct) path p is a list $(v_0, e_1, v_1, \ldots, e_n, v_n)$ such that $v_i \in V$, $e_i \in E_{\text{ext}}$, $\partial_0 e_i = v_{i-1}$ and $\partial_1 e_i = v_i$. A dual path p^* is a list $(f_0^*, e_1^*, f_1^*, \ldots, f_r^*)$ such that $f_i \in F$, $e_i \in E_{\text{ext}}$, $\partial_0 e_i^* = f_{i-1}^*$ and $\partial_1 e_i^* = f_i^*$.

Sites. A site is a pair $s = (v, f)$ with f a face and v one of its vertex. We visualize sites as dashed lines connecting the vertex v and the dual vertex f^*, as shown in Fig.13, and use the notation $s =: (v_s, f_s)$.

Triangles. A direct triangle $\tau = (s_0, s_1, e)$ consists of two sites s_i and a direct edge $e \in E_{\text{ext}}$ such that (i) $f_{s_0} = f_{s_1}$ (ii) $\partial_i e = v_{s_i}$ and (iii) s_0, s_1 and e form a triangle with sides listed in *counterclockwise* order. We use the notation $\tau =: (\partial_0\tau, \partial_1\tau, e_\tau)$, and say that τ points from $\partial_0\tau$ to $\partial_1\tau$ through e_τ.

A dual triangle $\tau = (s_0, s_1, e^*)$ consists of two sites s_i and a dual edge $e^* \in E^*_{\text{ext}}$ such that (i) $v_{s_0} = v_{s_1}$ (ii) $\partial_i e^* = f^*_{s_i}$ and (iii) s_0, s_1 and e^* form a triangle with sides listed in *clockwise* order. We use the notation $\tau =: (\partial_0\tau, \partial_1\tau, e^*_\tau)$, and say that τ points from $\partial_0\tau$ to $\partial_1\tau$ through e^*_τ.

Each direct (dual) triangle τ has a complementary triangle $\bar{\tau}$, the unique direct (dual) triangle with $e_{\bar{\tau}} = \bar{e}_\tau$.

Two triangles overlap if they 'share part of their area'. Specifically, a dual triangle τ and a direct triangle τ' overlap if $\partial_i\tau = \partial_i\tau'$ either for $i = 0$ or $i = 1$, and two triangles of the same type overlap if they are the same triangle. Triangles and their properties are illustrated in Fig.13.

Strips. A (triangle) strip of length $n \geq 0$ is an alternating sequence of sites and triangles $\rho = (s_0, \tau_1, s_1, \tau_2, \ldots, s_{n-1}, \tau_n, s_n)$ with $\partial_0\tau_i = s_{i-1}$ and $\partial_1\tau_i = s_i$. We define $\partial_0\rho := s_0$ and $\partial_1\rho := s_n$. Strips can be given just as a list of sites $\rho = (s_0, s_1, \ldots, s_n)$ or, if they have non-zero length, as a list of triangles $\rho = (\tau_1, \ldots, \tau_n)$. They could also be given as a pair $\rho = (s, \mathbf{x})$, with $s = s_0$ the initial site and $\mathbf{x} \in 2^n$ a binary vector, because for any given site there exists exactly a dual and a direct triangle pointing from it. Examples of strips are given in Fig.13.

Let ρ be a strip with $s_i = \partial_i\rho$. We say that ρ is *(i)* trivial if it has length zero, *(ii)* direct (dual) if it consists only of direct (dual) triangles, *(iii)* proper if it is neither direct nor dual, *(iv)* open if $v_{s_0} \neq v_{s_1}$ and $f_{s_0} \neq f_{s_1}$ and

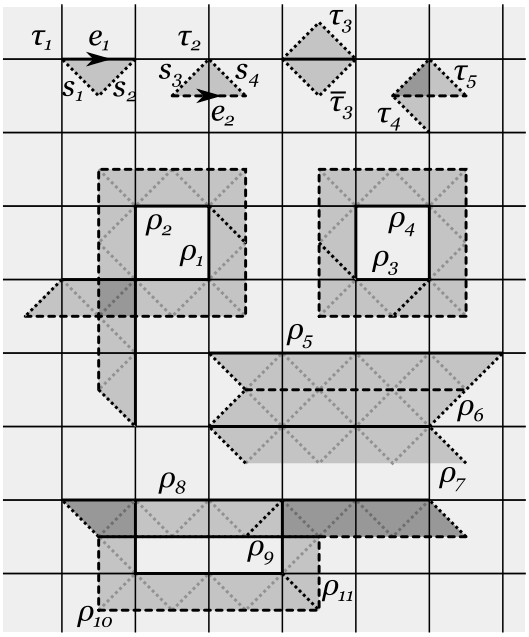


FIG. 13: Several examples of sites, triangles and strips. Sites are displayed as black dotted lines when they are an end of some ribbon. Triangles and strips are displayed as grey bands. The direct path of each strip is a thick black line, and the dual path a dashed line. The s_i are sites, the τ_i are triangles and the ρ_i strips (indeed ribbons). $\tau_1 = (s_1, s_2, e_1)$ is a direct triangle and $\tau_2 = (s_3, s_4, e_2^*)$ is a dual triangle. $\bar{\tau}_3$ is the complementary triangle of τ_3. τ_4 and τ_5 overlap. $\rho = \rho_1\rho_2$ is a strip but not a ribbon. $\sigma = \rho_3\rho_4$ and $\sigma' = \rho_4\rho_3$ are closed strips (indeed ribbons), with σ' a rotation of σ and $\sigma \triangleright \sigma' = \rho_3$. ρ_5 is a dual complementary ribbon or ρ_6, $(\rho_5, \rho_6)_\triangle$, and ρ_7 is direct complementary ribbon of ρ_6, $(\rho_6, \rho_7)_\triangledown$. The ribbons $\rho_8, \rho_9, \rho_{10}, \rho_{11}$ illustrate various types of joints, so that $(\rho_8, \rho_{10})_\prec$, $(\rho_9, \rho_{11})_\succ$ and $(\rho_8\rho_9, \rho_{10}\rho_{11})_{\prec\succ}$.

(v) closed if $s_0 = s_1$. When σ is a closed strip we write $\partial\sigma$ instead of $\partial_i\sigma$.

Two strips are composable if $\partial_1\rho_1 = \partial_0\rho_2$. In that case the composed strip is $\rho = \rho_1\rho_2 := (s_0, \ldots, s_m)$ with $\rho_1 = (s_0, \ldots, s_n)$ and $\rho_2 = (s_n, \ldots, s_m)$. This composition operation is clearly associative.

The cyclic nature of the list of triangles of a closed strip allows to rotate it, see Fig.13. We say that σ' is a rotation of σ, denoted $(\sigma, \sigma')_\circ$, if $\sigma \neq \sigma'$, $\sigma = \rho_1\rho_2$ and $\sigma' = \rho_2\rho_1$. In that case we set $\sigma \triangleright \sigma' := \rho_1$. Note that if $(\sigma, \sigma')_\circ$ then both σ and σ' are closed.

We can attach both a direct and a dual path to a strip ρ, see Fig.13. If $(\tau_1, \ldots, \tau_q)$ is the ordered list of direct triangles in ρ, we set $p_\rho = (v_{\partial_0\tau_1}, e_{\tau_1}, v_{\partial_1\tau_1}, \ldots, e_{\tau_q}, v_{\partial_1\tau_q})$. Similarly, if $(\tau'_1, \ldots, \tau'_r)$ is the ordered list of dual triangles in ρ, we set $p^*_\rho = (f^*_{\partial_0\tau'_1}, e^*_{\tau'_1}, f^*_{\partial_1\tau'_1}, \ldots, e^*_{\tau'_r}, f^*_{\partial_1\tau'_r})$.

Consider two strips ρ_1 and ρ_2. We say that ρ_1 and ρ_2 *(i)* do not overlap, denoted $(\rho_1, \rho_2)_\oslash$, if no triangle of ρ_1 overlaps with a triangle of ρ_2, *(ii)* form a left joint, denoted $(\rho_1, \rho_2)_\prec$, if $\rho_i = \rho\tau_i\rho'_i$ with τ_1 a dual triangle, τ_2 a direct triangle and $(\rho'_1, \rho'_2)_\oslash$, *(iii)* form a right joint,

denoted $(\rho_1,\rho_2)_\succ$, if $\rho_i=\rho_i'\tau_i\rho$ with τ_1 a dual triangle, τ_2 a direct triangle and $(\rho_1',\rho_2')_\oslash$, *(iv)* form a left-right joint, denoted $(\rho_1,\rho_2)_{\prec\succ}$, if $\rho_i=\rho\tau_i\rho_i'\tau_i'\rho'$ with τ_1,τ_1' dual triangles, τ_2,τ_2' direct triangles and $(\rho_1',\rho_2')_\oslash$, and *(v)* form a crossed joint, denoted $(\rho_1,\rho_2)_+$, if $\rho_i=\rho_i'\rho_i''$ with $(\rho_1',\rho_2')_\prec$, $(\rho_2'',\rho_1'')_\succ$, $(\rho_1',\rho_2'')_\oslash$ and $(\rho_1'',\rho_2')_\oslash$. Closed crossed joints are only possible in surfaces of nontrivial topology, see Fig. 15. Indeed, their name was chosen with those cases in which ρ_1, ρ_2 are closed in mind. The other joint types are illustrated in Fig.13.

We denote by V_ρ (F_ρ) the set of vertices (faces) in a strip ρ, by $E_\rho^\triangle$ ($E_\rho^\triangledown$) the set of edges $e\in E_{\rm ext}$ with $e=e_\tau$ for some dual (direct) triangle τ in ρ, and by $\bar E_\rho^\triangle$ ($\bar E_\rho^\triangledown$) the set of their inverses. If ρ and ρ' are non-direct (non-dual) closed strips with $E_\rho^\triangle=\bar E_{\rho'}^\triangle$ ($E_\rho^\triangledown=\bar E_{\rho'}^\triangledown$), we say that ρ' is a dual (direct) complementary ribbon of ρ, denoted $(\rho,\rho')_\triangle$ ($(\rho,\rho')_\triangledown$), see Fig.13.

2. Ribbons

Ribbons are strips such that its direct and dual path do not self-cross.

Definition 1 *Let ρ be a triangle strip, $p_\rho=(v_0,\dots,e_q,v_q)$ and $p_\rho^*=(f_0^*,\dots,e_r^*,f_r^*)$. We say that ρ is a ribbon if*

- *for any triangle τ in ρ, $\bar\tau$ is not in ρ,*
- *for $0\le i\ne j\le q$ with $i\ne 0$ or $j\ne q$, $v_i\ne v_j$ and*
- *for $0\le i\ne j\le r$ with $i\ne 0$ or $j\ne r$, $f_i\ne f_j$.*

A rotation of a ribbon is a ribbon. Two ribbons ρ_1 and ρ_2 are composable if they are composable as strips and $\rho=\rho_1\rho_2$ is a ribbon. If ρ is a ribbon and $\rho=\rho_1\rho_2$ as strips, then ρ_1 and ρ_2 are ribbons also, and $(\rho_1,\rho_2)_\oslash$. Complementary ribbons do not overlap.

Consider any two sites s and s'. If $v_s=v_{s'}$, we denote by $\alpha_{s,s'}$ the unique nontrivial dual ribbon ρ with $\partial_0\rho=s$ and $\partial_1\rho=s'$. If $f_s=f_{s'}$, we denote by $\beta_{s,s'}$ the unique nontrivial direct ribbon ρ with $\partial_0\rho=s$ and $\partial_1\rho=s'$. All nontrivial dual (direct) ribbons take the form $\alpha_{s,s'}$ ($\beta_{s,s'}$) for some s,s'. We also write $\alpha_s:=\alpha_{s,s}$ and $\beta_s:=\beta_{s,s}$. Then if $(\alpha_s,\alpha_{s'})_\circ$ we have $\alpha_s\triangleright\alpha_{s'}=\alpha_{s,s'}$, and if $(\beta_s,\beta_{s'})_\circ$ we have $\beta_s\triangleright\beta_{s'}=\beta_{s,s'}$.

3. Triangle operators

From this point on we are working with a fixed finite group G. To each edge $e\in E$ we attach a Hilbert space $\mathcal{H}_G'$ with orthonormal basis $\{|g\rangle\}_{g\in G}$. The total Hilbert space of our system is then $\mathcal{H}_G:=\mathcal{H}_G'^{\otimes|E|}$. If O is a single-qudit operator, O_e with $e\in E_{\rm ext}$ denotes that operator acting on the qudit attached to the edge e ($\bar e$) if $e\in E$ ($e\in\bar E$).

Before we can define operators for arbitrary ribbons we must consider their elementary components, triangles. To this end, let

$$L^h:=\sum_{g\in G}|hg\rangle\langle g|,\quad T^g:=|g\rangle\langle g|,\quad I:=\sum_{g\in G}|\bar g\rangle\langle g|. \tag{B1}$$

If τ is a dual triangle, we set

$$L_\tau^h:=I^xL_{e_\tau}^hI^x \tag{B2}$$

with $x=0$ ($x=1$) if $e_\tau\in E$ ($e_\tau\in\bar E$). If τ' is a direct triangle, we set

$$T_{\tau'}^g:=I^xT_{e_{\tau'}}^gI^x \tag{B3}$$

with $x=0$ ($x=1$) if $e_\tau\in E$ ($e_\tau\in\bar E$)). With these definitions we have

$$\begin{aligned} L_\tau^hL_\tau^{h'}&=L_\tau^{hh'},\qquad & T_{\tau'}^gT_{\tau'}^{g'}&=\delta_{g,g'}T_{\tau'}^g,\\ L_\tau^{h\,\dagger}&=L_\tau^{\bar h},\qquad & T_{\tau'}^{g\,\dagger}&=T_{\tau'}^g,\\ L_\tau^1&=1,\qquad & \sum_{g\in G}T_{\tau'}^g&=1. \end{aligned} \tag{B4}$$

As for the commutation rules, we have

$$L_\tau^hT_{\tau'}^g=\begin{cases}T_{\tau'}^{hg}L_\tau^h, & \text{if } \partial_0\tau=\partial_0\tau';\\ T_{\tau'}^{g\bar h}L_\tau^h & \text{if } \partial_1\tau=\partial_1\tau';\\ T_{\tau'}^gL_\tau^h, & \text{otherwise.}\end{cases} \tag{B5}$$

If $\tau_1\ne\tau_2$ are dual triangles and τ_1', τ_2' are direct triangles then

$$[L_{\tau_1}^h,L_{\tau_2}^{h'}]=[T_{\tau_1'}^g,T_{\tau_2'}^{g'}]=0. \tag{B6}$$

Thus, non-overlapping triangles have commuting triangle operators.

4. Ribbon operators

For each ribbon ρ we introduce a set of operators $\{F_\rho^{h,g}\}$ with $h,g\in G$. We call them ribbon operators. First, if ϵ is a trivial ribbon we define

$$F_\epsilon^{h,g}:=\delta_{1,g} \tag{B7}$$

If τ is a dual triangle and τ' a direct triangle we set [18]

$$F_\tau^{h,g}:=\delta_{1,g}L_\tau^h,\qquad F_{\tau'}^{h,g}:=T_{\tau'}^g. \tag{B8}$$

If ρ is an arbitrary ribbon of length $l>1$, we let $\rho=\rho_1\rho_2$ and recursively define a gluing or composition procedure by means of the folowing relations

$$F_\rho^{h,g}:=\sum_{k\in G}F_{\rho_1}^{h,k}F_{\rho_2}^{\bar khk,\bar kg}. \tag{B9}$$

We must of course ensure that this definition of $F_\rho^{h,g}$ is independent of the particular choice of ρ_1 and ρ_2. But this amounts to check that if $\rho = \rho_1\rho_2\rho_3$ then

$$\sum_{k\in G} F_{\rho_1}^{h,k} F_{\rho_2\rho_3}^{\bar{k}hk,\bar{k}g} = \sum_{k\in G} F_{\rho_1\rho_2}^{h,k} F_{\rho_3}^{\bar{k}hk,\bar{k}g} \tag{B10}$$

which follows by expanding $F_{\rho_2\rho_3}^{\bar{k}hk,\bar{k}g}$ and $F_{\rho_1\rho_2}^{h,k}$ with (B9). We also have to check that if $\rho = \epsilon\rho = \rho\epsilon'$ then

$$F_\rho^{h,g} \;=\; \sum_{k\in G} F_\epsilon^{h,k} F_\rho^{\bar{k}hk,\bar{k}g} \;=\; \sum_{k\in G} F_\rho^{h,k} F_{\epsilon'}^{\bar{k}hk,\bar{k}g}, \tag{B11}$$

which indeed holds true.

We will find useful the notation

$$T_\rho^g := F_\rho^{1,g}, \qquad L_\rho^h := \sum_{g\in G} F_\rho^{h,g}. \tag{B12}$$

conceived so that

$$F_\rho^{h,g} = L_\rho^h T_\rho^g = T_\rho^g L_\rho^h. \tag{B13}$$

Also, for any $S \subset G$, $g \in G$ we set

$$F^{S,g} := \frac{1}{|S|}\sum_{s\in S} F^{s,g}, \quad F^{g,S} := \sum_{s\in S} F^{g,s}. \tag{B14}$$

We now list several properties of ribbon operators. They follow from the properties of triangle operators and (B9). For any ribbon ρ

$$F_\rho^{h,g} F_\rho^{h',g'} = \delta_{g,g'} F_\rho^{hh',g}, \qquad F_\rho^{h,g\,\dagger} = F_\rho^{\bar{h},g}, \tag{B15}$$

$$L_\rho^1 = \sum_{g\in G} T_\rho^g = 1. \tag{B16}$$

Thus, for each ρ, ribbon operators linearly generate an algebra closed under Hermitian conjugation. If ρ is dual and ρ' direct then

$$F_\rho^{h,g} = \delta_{g,1} L_\rho^h, \qquad F_{\rho'}^{h,g} = T_{\rho'}^g. \tag{B17}$$

If $(\rho_1,\rho_2)_\prec$ then

$$F_{\rho_1}^{h,g} F_{\rho_2}^{k,l} = F_{\rho_2}^{hk\bar{h},hl} F_{\rho_1}^{h,g}. \tag{B18}$$

If $(\rho_1,\rho_2)_\succ$ then

$$F_{\rho_1}^{h,g} F_{\rho_2}^{k,l} = F_{\rho_2}^{k,l\bar{g}\bar{h}g} F_{\rho_1}^{h,g}. \tag{B19}$$

If $(\rho_1,\rho_2)_{\prec\succ}$ then

$$F_{\rho_1}^{h,g} F_{\rho_2}^{k,l} = F_{\rho_2}^{hk\bar{h},hl\bar{g}\bar{h}g} F_{\rho_1}^{h,g}. \tag{B20}$$

If $(\rho_1,\rho_2)_+$ then

$$F_{\rho_1}^{h,g} F_{\rho_2}^{k,l} = F_{\rho_2}^{hk\bar{h},hl} F_{\rho_1}^{h,g\bar{l}kl}. \tag{B21}$$

If $(\sigma_1,\sigma_2)_\circ$ then

$$F_{\sigma_1\triangleright\sigma_2}^{k,l} F_{\sigma_1}^{h,g} = F_{\sigma_1\triangleright\sigma_2}^{kh\bar{g}\bar{h}g,l} F_{\sigma_2}^{\bar{l}hl,\bar{l}gl}. \tag{B22}$$

If $(\rho_1,\rho_2)_\oslash$ then

$$[F_{\rho_1}^{h,g}, F_{\rho_2}^{k,l}] = 0. \tag{B23}$$

Proposition 2 *Let ρ be a ribbon, $h,g \in G$.*
(i) If ρ is dual

$$\mathrm{Tr}(L_\rho^h) = \delta_{h,1}\mathrm{Tr}(1). \tag{B24}$$

(ii) If ρ is direct

$$|G|\mathrm{Tr}(T_\rho^g) = \mathrm{Tr}(1). \tag{B25}$$

(iii) If ρ is proper

$$|G|\mathrm{Tr}(F_\rho^{h,g}) = \delta_{h,1}\mathrm{Tr}(1). \tag{B26}$$

Proof. If ρ is not dual, choose any direct triangle τ in ρ, so that $\rho = \rho_1\tau\rho_2$. Let $\rho' = \rho_1\tau'$ with τ' dual. Then $(\rho',\rho)_\prec$ and thus using (B18)

$$\mathrm{Tr}(F_\rho^{h,g}) = \mathrm{Tr}(L_{\rho'}^k F_\rho^{h,g} L_{\rho'}^{\bar{k}}) = \mathrm{Tr}(F_\rho^{kh\bar{k},kg} L_{\rho'}^k L_{\rho'}^{\bar{k}}) = \mathrm{Tr}(F_\rho^{kh\bar{k},kg}). \tag{B27}$$

If ρ is not direct, choose any dual triangle τ in ρ, so that $\rho = \rho_1\tau\rho_2$. Let $\rho' = \rho_1\tau'$ with τ' direct. Then $(\rho,\rho')_\prec$ and thus using (B18)

$$\mathrm{Tr}(F_\rho^{h,g}) = \sum_{k\in G}\mathrm{Tr}(T_{\rho'}^k F_\rho^{h,g} T_{\rho'}^k) = \sum_{k\in G}\mathrm{Tr}(F_\rho^{h,g} T_{\rho'}^{hk} T_{\rho'}^k) = \delta_{h,1}\mathrm{Tr}(F_\rho^{h,g}). \tag{B28}$$

Equations (B27, B28) together with (B16, B17) give the desired results. □

As a consequence of the previous proposition and (B15) we have the following orthogonality results.

Corolary 3 *Let ρ be a ribbon, $h,g \in G$.*
(i) If ρ is dual

$$\mathrm{Tr}(L_\rho^{h\,\dagger} L_\rho^{h'}) = \delta_{h,h'}\mathrm{Tr}(1). \tag{B29}$$

(ii) If ρ is direct

$$|G|\mathrm{Tr}(T_\rho^{g\,\dagger} T_\rho^{g'}) = \delta_{g,g'}\mathrm{Tr}(1). \tag{B30}$$

(iii) If ρ is proper

$$|G|\mathrm{Tr}(F_\rho^{h,g\,\dagger} F_\rho^{h',g'}) = \delta_{h,h'}\delta_{g,g'}\mathrm{Tr}(1). \tag{B31}$$

Definition 4 Rotationally invariant ribbon operators *Given a closed ribbon σ, we say that an operator $F = \sum_{h,g\in G} c_{h,g} F_\sigma^{h,g}$, $c_{h,g} \in \mathbf{C}$, is rotationally invariant if for any σ' with $(\sigma,\sigma')_\circ$ we have $F = \sum_{h,g\in G} c_{h,g} F_{\sigma'}^{h,g}$.*

In this regard, results (B15, B16, B22) imply that if $(\sigma_1,\sigma_2)_\circ$ then

$$F_{\sigma_1}^{h,g} = \sum_{l\in G} F_{\sigma_1\triangleright\sigma_2}^{h\bar{g}\bar{h}g,l} F_{\sigma_2}^{\bar{l}hl,\bar{l}gl}. \tag{B32}$$

5. Vertex and face operators

We now define vertex and face operators in terms of ribbon operators. Let α_s (β_s) be the unique dual (direct) closed ribbon with $\partial\alpha_s = s$ ($\partial\beta_s = s$). For any site $s = (v, f)$ let

$$A_s^h := F_{\alpha_s}^{h,1} \qquad B_s^g := F_{\beta_s}^{1,\bar{g}}. \tag{B33}$$

Let s', s'' be sites with $(\alpha_s, \alpha_{s'})_\circ$, $(\beta_s, \beta_{s''})_\circ$. From (B17, B32) we get

$$A_s^h = A_{s'}^h, \qquad B_s^k = T_{\beta_{s,s''}}^g B_{s''}^{\bar{g}kg}. \tag{B34}$$

Thus, vertex operators are rotationally invariant and we can write $A_v^h := A_s^h$ for $v = v_s$. These definitions of A_v^h and B_s^g agree with those given in (2,4).

Let us list several useful properties. If $s \neq s'$ then

$$A_s^h A_s^{h'} = A_s^{hh'}, \quad A_s^1 = 1, \quad A_s^{h\dagger} = A_s^{\bar{h}}, \tag{B35}$$

$$B_s^g B_s^{g'} = \delta_{g,g'} B_s^g, \quad \sum_{g\in G} B_s^g = 1, \quad B_s^{g\dagger} = B_s^g. \tag{B36}$$

$$A_s^h B_s^g = B_s^{hg\bar{h}} A_s^h, \tag{B37}$$

$$[A_s^h, B_{s'}^g] = [A_s^g, A_{s'}^{g'}] = [B_s^h, B_{s'}^{h'}] = 0. \tag{B38}$$

All these properties follow from the properties of ribbon operators. Note in particular that the well-known[22] flux metamorphosis (B37) is a consequence of $(\alpha_s, \beta_s)_{\prec\succ}$.

For subgroups $H, H' \subset G$, H' normal, we define the operators

$$A_v^H := A_s^H := L_{\alpha_s}^H, \qquad B_f^{H'} := B_s^{H'} := T_{\beta_s}^{H'}, \tag{B39}$$

where $s = (v, f)$ is a site. We set $A_v := A_v^G$ and $B_f := B_f^1$. From (B37,B38) we have for arbitrary vertices v, v' and faces f, f'

$$[A_v^H, A_{v'}^H] = [A_v^H, B_f^{H'}] = [B_f^{H'}, B_{f'}^{H'}] = 0. \tag{B40}$$

Of particular interest are the commutation rules between ribbon operators and vertex and face operators at their ends. We first consider non-closed ribbons. Let $s_i = \partial_i\rho$. If $v_0 \neq v_1$ then $(\alpha_{s_0}, \rho)_\prec$, $(\alpha_{s_1}, \rho)_\succ$ and from (B18, B19) we get

$$\begin{aligned} A_{s_0}^k F_\rho^{h,g} &= F_\rho^{kh\bar{k},kg} A_{s_0}^k, \\ A_{s_1}^k F_\rho^{h,g} &= F_\rho^{h,g\bar{k}} A_{s_1}^k. \end{aligned} \tag{B41}$$

If $f_0 \neq f_1$ then $(\rho, \beta_{s_0})_\prec$, $(\rho, \beta_{s_1})_\succ$ and from (B18, B19) we get

$$\begin{aligned} B_{s_0}^k F_\rho^{h,g} &= F_\rho^{h,g} B_{s_0}^{kh}, \\ B_{s_1}^k F_\rho^{h,g} &= F_\rho^{h,g} B_{s_1}^{\bar{g}\bar{h}gk}. \end{aligned} \tag{B42}$$

If ρ is dual but not closed then $\alpha_{s_0} = \alpha_{s_0,s_1}\alpha_{s_1,s_0}$ and from (B9, B15, B23) we get

$$A_{s_i}^k F_\rho^{h,1} = F_\rho^{kh\bar{k},1} A_{s_i}^k, \tag{B43}$$

and if ρ is direct but not closed then $\beta_{s_0} = \beta_{s_0,s_1}\beta_{s_1,s_0}$ and from (B9, B15, B23) we get

$$[B_{s_i}^k, F_\rho^{1,g}] = 0. \tag{B44}$$

Now we consider closed ribbons. So let σ be a closed ribbon with $s = \partial\sigma$. If σ is a proper closed ribbon then $(\alpha_s, \sigma)_{\prec\succ}$ and $(\sigma, \beta_s)_{\prec\succ}$ so that from (B20) we get

$$\begin{aligned} A_s^k F_\sigma^{h,g} &= F_\sigma^{kh\bar{k},kg\bar{k}} A_s^k, \\ B_s^k F_\sigma^{h,g} &= F_\sigma^{h,g} B_s^{\bar{g}\bar{h}gkh}. \end{aligned} \tag{B45}$$

If σ is closed but not proper, then either $\sigma = \alpha_s$ or $\sigma = \beta_s$, but for that case we already have (B37).

Equations (12, 14) can be generalized. Let ρ be a ribbon with two ends $i = 0, 1$ and set $s_i = \partial_i\rho$, $v_i = v_{s_i}$, $f_i = f_{s_i}$. If $v_0 \neq v_1$ from (B41) we get

$$|G| \sum_{g\in G} T_\rho^g A_{v_i} T_\rho^g = 1 \tag{B46}$$

and if $f_0 \neq f_1$ from (B42) we get

$$\sum_{h\in G} L_\rho^{\bar{h}} B_{f_i} L_\rho^h = 1. \tag{B47}$$

As explained in the main text, section II B, these identities show how ribbon operators can be used to obtain arbitrary states with a number of excited spots from states with one excited spot less.

6. Edge operators

For subgroups $H \subset H' \subset G$, H normal in G, we define the operators

$$L_e^H := L_\tau^H, \qquad T_{e'}^{H'} := T_{\tau'}^{H'}, \tag{B48}$$

where $e = e_\tau$, $e' = e_{\tau'}$ with τ a dual triangle and τ' a direct one. Then from (B5,B6) we have for arbitrary edges e, e'

$$[L_e^H, L_{e'}^H] = [L_e^H, T_{e'}^{H'}] = [T_e^{H'}, T_{e'}^{H'}] = 0. \tag{B49}$$

In some particular cases, triangle operators and ribbons have nice commuting properties, but this is not always the case. If H, H', τ, τ' are as above, with τ and τ' either in ρ or with no overlap with it then from (B9, B15, B23) we have

$$[L_\tau^H, F_\rho^{h,g}] = [T_{\tau'}^{H'}, F_\rho^{h,g}] = 0. \tag{B50}$$

Other triangles are more complicated. Let $\rho = \rho_1\rho_2$, $(\tau_1, \rho_1)_\succ$, $(\tau_2, \rho_2)_\prec$, $(\rho_1, \tau_3)_\succ$, $(\rho_2, \tau_4)_\prec$, $h \in H$ and $k, l \in$

G with $ks\bar{k} = s$ for any $s \in H$. Then from (B9, B18, B19) we have

$$\begin{aligned} L^h_{\tau_1} F^{k,l}_\rho &= \sum_{g\in G} T^g_{\rho_1} F^{k,gh\bar{g}l}_\rho L^h_{\tau_1}, \\ L^h_{\tau_2} F^{k,l}_\rho &= \sum_{g\in G} T^g_{\rho_1} F^{k,g\bar{h}\bar{g}l}_\rho L^h_{\tau_2}, \\ T^h_{\tau_3} F^{k,l}_\rho &= \sum_{g\in G} T^g_{\rho_1} F^{k,l}_\rho T^{h\bar{g}kg}_{\tau_3}, \\ T^h_{\tau_4} F^{k,l}_\rho &= \sum_{g\in G} T^g_{\rho_1} F^{k,l}_\rho T^{\bar{g}\bar{k}gh}_{\tau_4}. \end{aligned} \tag{B51}$$

As a result, if $N \subset M \subset G$ with N, M normal and N central in M we have for any $h, g \in G$, $\tau = \tau_1$ (or τ_2) and $\tau' = \tau_3$ (or τ_4) with τ_i as above

$$L^N_\tau T^M_{\tau'} F^{h,g}_\rho L^N_\tau T^M_{\tau'} = \delta_{hM,M} \frac{1}{|N|} F^{h,Ng} L^N_\tau T^M_{\tau'}, \tag{B52}$$

which then gives (58).

7. The algebra $\mathcal{A}_\rho$

We want to define the ribbon operator algebra $\mathcal{F}_\rho$, but as an intermediate step we introduce the algebra $\mathcal{A}_\rho$. If ϵ is a trivial ribbon then $\mathcal{A}_\epsilon := \mathbf{C}$. If τ is a direct (dual) triangle then $\mathcal{A}_\tau := \mathrm{Lin}\{\, T^g_\tau \,|\, g \in G \,\}$ ($\mathcal{A}_\tau := \mathrm{Lin}\{\, L^h_\tau \,|\, h \in G \,\}$). Finally, if $\rho = (\tau_i)$ is an arbitrary ribbon $\mathcal{A}_\rho := \bigotimes_i \mathcal{A}_{\tau_i}$. That $\mathcal{A}_\tau$ is really an algebra follows from (B4).

We now proceed to show several results which are essential in order to characterize ribbon operator algebras in the next sections.

Lemma 5 *Let ρ be a ribbon, $O \in \mathcal{A}_\rho$ an operator, H a subgroup of G, and s a site*
(i) If ρ is not a rotation or a complement of α_s then

$$OA^H_s = 0 \quad \Longrightarrow \quad O = 0. \tag{B53}$$

(ii) If ρ is not a rotation or a complement of β_s then

$$OB^H_s = 0 \quad \Longrightarrow \quad O = 0. \tag{B54}$$

(iii) If τ is a dual triangle such that neither it nor its complement belong to ρ

$$OL^H_\tau = 0 \quad \Longrightarrow \quad O = 0. \tag{B55}$$

(iv) If τ is a direct triangle such that neither it nor its complement belong to ρ

$$OT^H_\tau = 0 \quad \Longrightarrow \quad O = 0. \tag{B56}$$

Proof. First, note that $A^H_s A^G_s = A^G_s$ implies $OA^H_s = 0 \Rightarrow OA^G_s = 0$, and similarly for L^H_τ, so that it suffices to consider $H = G$ in these cases. Also, $B^H_s B^1_s = B^1_s$ and similarly for T^H_τ, so that it suffices to consider $H = 1$ for them.
(i) There exists a direct triangle τ such that it overlaps with α_s but not with ρ, so that $[T^h_\tau, O] = 0$, and a site s' such that $(\alpha_{s'}, \alpha_s)_\circ$ and $(\tau, \alpha_{s'})_\prec$ or $(\tau, \alpha_{s'})_\succ$. In the first case $A^G_s = A^G_{s'}$ and from (B41) we have $0 = \sum_g T^g_\tau O A^G_{s'} T^g_\tau = |G|^{-1} \sum_{g,h} O A^h_{s'} T^{\bar{h}g}_\tau T^g_\tau = O A^1_{s'} T^G_\tau = O$ and the other case is similar.
(ii) There exists a dual triangle τ such that it overlaps with β_s but not with ρ, so that $[L^h_\tau, O] = 0$, and a site s' such that $(\beta_{s'}, \beta_s)_\circ$ and $(\beta_{s'}, \tau)_\prec$ or $(\beta_{s'}, \tau)_\succ$. In the first case $B^1_s = B^1_{s'}$ from (B42) we have $0 = \sum_h L^h_\tau O B_{s'} L^{\bar{h}}_\tau = \sum_h O B^{\bar{h}}_{s'} L^h_\tau L^{\bar{h}}_\tau = O B^G_{s'} L^1_\tau = O$ and the other case is similar.
(iii, iv) The proofs are analogous to (i,ii). □

Given a vertex v and a dual triangle τ we set for any $O \in \mathcal{A}_\rho$

$$O_k := A^k_v O A^{\bar{k}}_v, \qquad O'_k := L^k_\tau O L^{\bar{k}}_\tau. \tag{B57}$$

One can check that $O_k, O'_k \in \mathcal{A}_\rho$. Then if ρ satisfies the conditions of lemma 5

$$[O, A^H_v] = 0 \quad \Longleftrightarrow \quad |H| O = \sum_{k\in H} O_k, \tag{B58}$$

$$[O, L^H_\tau] = 0 \quad \Longleftrightarrow \quad |H| O = \sum_{k\in H} O'_k, \tag{B59}$$

because for $k \in H$ we have $O_k A^H_v = O_k A^k A^H_v = A^k_v O A^H_v = A^k A^H_v O = A^H_v O = O A_v$ giving $O_k = O$, and similarly for L^H_e. As a consequence, we also get under the same conditions and $k \in H$

$$[O, A^H_v] = 0 \quad \Longrightarrow \quad [O, A^k_v] = 0. \tag{B60}$$

Given a site s in ρ and a direct triangle τ , one can check that unless ρ is both a non-closed and non-direct ribbon with $f_{\partial_i \rho} = f_s$, for any $O \in \mathcal{A}_\rho$ there exist $O_{k,k'}, O'_{k,k'} \in \mathcal{A}_\rho$ such that $O = \sum_{k,k'\in G} O_{k,k'} = \sum_{k,k'\in G} O'_{k,k'}$ with

$$B^g_s O_{k,k'} = O_{k,k'} B^{\bar{k}gk'}_s, \quad T^g_\tau O_{k,k'} = O_{k,k'} T^{\bar{k}gk'}_\tau. \tag{B61}$$

Then if ρ satisfies the conditions of lemma 5 and H is normal in G

$$[O, B^H_f] = 0 \quad \Longleftrightarrow \quad O = \sum_{k,k'\in G \,|\, \bar{k}k'\in H} O_{k,k'}, \tag{B62}$$

$$[O, T^H_\tau] = 0 \quad \Longleftrightarrow \quad O = \sum_{k,k'\in G \,|\, \bar{k}k'\in H} O'_{k,k'} \tag{B63}$$

because $O B^H_f = O B^H_f B^H_f = B^H_f O B^H_f = \sum_{k,k'} B^H_s O^{k,k'} B^H_s = \sum_{k,k'} O^{k,k'} B^{\bar{k}Hk'}_s B^H_s = \sum_{\bar{k}k'\in H} O^{k,k'} B^H_f$ and similarly for T^H_τ. As a consequence, we also get under the same conditions and $C \in (G/H)_{\mathrm{cj}}$

$$[O, B^H_f] = 0 \quad \Longrightarrow \quad [O, B^C_f] = 0, \tag{B64}$$

where $B^C_f = \sum_{c\in C} \sum_{h\in H} B^{ch}_f$.

8. The algebra $\mathcal{F}_\rho$

In this section we characterize the ribbon operator algebra that has been introduced so far.

Definition 6 *Let ρ be a ribbon. The ribbon operator algebra $\mathcal{F}_\rho \subset \mathcal{A}_\rho$ consists of those operators $F \in \mathcal{A}_\rho$ such that $[F, A_v] = [F, B_f] = 0$ for any vertex $v \neq v_{\partial_i \rho}$ and any face $f \neq f_{\partial_i \rho}$, i=0,1.*

Proposition 7 *Let ρ be a ribbon. The $|G|^2$ ribbon operators $F_\rho^{h,g}$, $h, g \in G$, linearly generate $\mathcal{F}_\rho$. Moreover, ρ is proper if and only if they form a basis of $\mathcal{F}_\rho$.*

Proof. For ribbons ρ of length zero or one, $\mathcal{F}_\rho = \mathcal{A}_\rho$ because of (B23) and the first part of the statement follows since ribbon operators generate $\mathcal{A}_\rho$. For ribbons of length $l > 1$, we proceed inductively on l. So let ρ be such a ribbon and set $\rho =: \rho'\tau$, with τ a triangle. Observe that e_τ is not part of ρ' and that ρ' and τ share vertices or faces only at their ends, so that $\mathcal{F}_\rho \subset \mathcal{F}'_\rho := \mathcal{F}_{\rho'} \otimes \mathcal{F}_\tau = (\, F_{\rho'}^{h_1,g_1} F_\tau^{h_2,g_2} \,|\, h_i, g_i \in G\,)$, where $(\cdot)$ is the subspace linearly generated by the set $\cdot$. In view of (B9), what we want to show is that

$$\mathcal{F}''_\rho = (\, \sum_{k \in G} F_{\rho'}^{h,k} F_\tau^{\bar{k}hk,\bar{k}g} \,|\, h, g \in G\,) \tag{B65}$$

is indeed equal to $\mathcal{F}_\rho$. We set $s = \partial_0 \tau$, $v = v_s$, $f = f_s$ and distinguish two cases.

(a) τ is direct. In this case, $\mathcal{F}_\rho \subset \mathcal{F}'_\rho$ is the subalgebra of operators commuting with A_v. Then from(B58) and (B41) we get $\mathcal{F}_\rho = (\, \sum_{k \in G} F_{\rho'}^{h,k} F_\tau^{\bar{k}h'k,\bar{k}g} \,|\, h, h', g \in G\,)$. Applying $F_\tau^{h,g} = F_\tau^{h',g}$ here and in (B65) gives $\mathcal{F}_\rho = \mathcal{F}''_\rho$.

(b) τ is dual. In this case, $\mathcal{F}_\rho \subset \mathcal{F}'_\rho$ with $\mathcal{F}_\rho$ the subalgebra of operators commuting with B_f. Then from(B62) and (B42) we get $\mathcal{F}_\rho = (\, F_{\rho'}^{h,g} F_\tau^{\bar{g}hg,g'} \,|\, h, g, g' \in G\,)$. Applying $F_\tau^{h,g} = F_\tau^{h,1} \delta_{g,1}$ here and in (B65) gives $\mathcal{F}_\rho = \mathcal{F}''_\rho$.

This completes the inductive step. The second part of the statement follows from (B17) and corollary 3. □

We now construct an alternative basis for $\mathcal{F}_\rho$. For each conjugacy class $C \in (G)_{\rm cj}$ we choose an element r_C and denote by $\mathbf{N}_C \subset G$ the subgroup of elements commuting with r_C and by Q_C a set of representatives of $G/\mathbf{N}_C$. Then for each $C \in (G)_{\rm cj}$ we set $C = \{c_i\}_{i=1}^{|C|}$, and $Q_C = \{q_i\}_{i=1}^{|C|}$ so that $c_i = q_i r_C \bar{q}_i$. Any $g \in G$ can be written in a unique way as $g = q_i n$, with $n \in \mathbf{N}_C$. We introduce index functions as follows: $i(g) := i$ and $n(g) := n$. For each irreducible representation $R \in (\mathbf{N}_C)_{\rm ir}$, we choose a particular basis and denote by $\Gamma_R(k)$, $k \in G$, the corresponding unitary matrices of the representation. The desired new basis is the following:

$$F_\rho^{RC;\mathbf{uv}} := \frac{n_R}{|\mathbf{N}_C|} \sum_{n \in \mathbf{N}_C} \bar{\Gamma}_R^{jj'}(n)\, F_\rho^{\bar{c}_i, q_i n \bar{q}_{i'}}, \tag{B66}$$

where $\mathbf{u} = (i,j)$, $\mathbf{v} = (i',j')$ with $i, i' = 1, \dots, |C|$ and $j, j' = 1, \dots, n_R$. The inverse change is

$$F_\rho^{h,g} = \sum_{R \in (\mathbf{N}_C)_{\rm ir}} \sum_{j,j'=1}^{n_R} \Gamma_R^{jj'}(n_{h,g})\, F_\rho^{RC;\mathbf{uv}} \tag{B67}$$

where $\bar{h} \in C \in (G)_{\rm cj}$, $n_{h,g} = \bar{q}_{i(\bar{h})} g q_{i(\bar{g}\bar{h}g)}$, $\mathbf{u} = (i(\bar{h}), j)$ and $\mathbf{v} = (i(\bar{g}\bar{h}g), j')$ using the index functions for C. That (B66) is really a basis follows from

$$\begin{aligned} \mathrm{Tr}(F_\rho^{RC;\mathbf{uv}\,\dagger} F_\rho^{R'C';\mathbf{u'v'}}) = \\ = \frac{|n_R|}{|\mathbf{N}_C|\,|G|} \delta_{R,R'} \delta_{C,C'} \delta_{\mathbf{u},\mathbf{u}'} \delta_{\mathbf{v},\mathbf{v}'} \mathrm{Tr}(1). \end{aligned} \tag{B68}$$

Instead of (B41, B42) we can now write for $D_s^{h,g} := A_s^h B_s^g$, $s_i = \partial_i \rho$,

$$\begin{aligned} D_{s_0}^{h,g} F^{RC;\mathbf{uv}} &= \sum_{s=1}^{n_R} \Gamma_R^{sj}(n(hq_i))\, F^{RC;\mathbf{u}(s)\mathbf{v}} D_{s_0}^{h,g\bar{c}_i}, \\ D_{s_1}^{h,g} F^{RC;\mathbf{uv}} &= \sum_{s=1}^{n_R} \bar{\Gamma}_R^{sj'}(n(hq_{i'}))\, F^{RC;\mathbf{uv}(s)} D_{s_1}^{h,c_{i'}g}, \end{aligned} \tag{B69}$$

where $\mathbf{u} = (i,j)$, $\mathbf{v} = (i',j')$, $\mathbf{u}(s) = (i(hq_i), s)$, $\mathbf{v}(s) = (i(hq_{i'}), s)$.

9. The algebra $\mathcal{K}_\sigma$

Here we discuss the algebra of operators that gives the projectors onto states of different topological charge in systems with Hamiltonian H_G (1).

Definition 8 *Let σ be a closed ribbon. The closed ribbon operator algebra $\mathcal{K}_\sigma \subset \mathcal{A}_\sigma$ consists of those operators $K \in \mathcal{A}_\sigma$ such that $[K, A_v] = [K, B_f] = 0$ for every vertex v and face f.*

Note that $\mathcal{K}_\sigma \subset \mathcal{F}_\sigma$. It is not difficult to check that $\mathcal{K}_{\alpha_s}$ is linearly generated by the operators A_s^h, $h \in G$, and $\mathcal{K}_{\beta_s}$ is linearly generated by the operators B_s^C, with $C \in (G)_{\rm cj}$ and $B_s^C = \sum_{g \in C} B_s^g$. Note that these are exactly the rotationally invariant subalgebras of $\mathcal{F}_{\alpha_s}$ and $\mathcal{F}_{\beta_s}$.

For any closed ribbon σ we define the operators

$$K_\sigma^{DC} := \sum_{q \in Q_C} \sum_{d \in D} F_\sigma^{qd\bar{q}, qr_C\bar{q}}, \tag{B70}$$

where $C \in (G)_{\rm cj}$ and $D \in (\mathbf{N}_C)_{\rm cj}$. The point of these operators is that they are rotationally invariant:

$$(\sigma, \sigma')_\circ \quad \Longrightarrow \quad K_{\sigma'}^{DC} = K_\sigma^{DC}, \tag{B71}$$

as can be checked applying (B32). In fact, it can be shown that if σ is proper they form a basis of the subalgebra of rotationally invariant ribbon operators of $\mathcal{F}_\sigma$.

From (B15, B16) we get

$$K_\sigma^{DC} K_\sigma^{D'C'} = \delta_{C,C'} \sum_{D''} N_{DD'}^{D''} K_\sigma^{D''C},$$
$$K_\sigma^{DC\dagger} = K_\sigma^{\bar{D}C},$$
$$\sum_{C\in(G)_{\rm cj}} K_\sigma^{1C} = 1. \tag{B72}$$

where the sum runs over $D'' \in (\mathbf{N}_C)_{\rm cj}$, $DD' = \sum_{D''} N_{D,D'}^{D''} D''$ and $\bar{D}$ denotes the inverse class of D. The result (B26) implies for any proper σ

$$|G|{\rm Tr}(K_\sigma^{DC}) = |C|\delta_{D,1}{\rm Tr}(1), \tag{B73}$$

which together with (B72) and $N_{DD'}^1 = \delta_{\bar{D},D'}|D|$ gives

$${\rm Tr}(K_\sigma^{DC\dagger} K_\sigma^{D'C'}) = \frac{|D||C|}{|G|}\delta_{D,D'}\delta_{C,C'}{\rm Tr}(1). \tag{B74}$$

Proposition 9 *Let σ be a proper closed ribbon. The operators K_σ^{DC}, $C \in (G)_{\rm cj}$, $D \in (\mathbf{N}_C)_{\rm cj}$, form a basis of $\mathcal{K}_\sigma$.*

Proof. This is just a particular case of proposition 14. □

For any proper closed ribbons σ, consider the subalgebra $\mathcal{K}_\sigma^C \subset \mathcal{K}_\sigma$ with basis $\{\, K_\sigma^{DC} \,|\, D \in (\mathbf{N}_C)_{\rm cj} \,\}$. The point is that in view of (B72, A21) we have $\mathcal{K}_\sigma^C \simeq \mathcal{Z}_C$, where $\mathcal{Z}_C$ is the center of the group algebra $\mathbf{C}[\mathbf{N}_C]$. In particular the isomorphism identifies K^{DC} with $e_D := \sum_{h\in D} h$. Note that the isomorphism preserves adjoints as defined in (A18). This suggests the introduction of a different basis for $\mathcal{K}_\sigma$. We define in analogy with (A24)

$$K_\sigma^{RC} := \frac{n_R}{|\mathbf{N}_C|} \sum_{D\in(\mathbf{N}_C)_{\rm cj}} \bar{\chi}_R(D)\, K_\sigma^{DC}, \tag{B75}$$

where $R \in (\mathbf{N}_C)_{\rm ir}$. Due to (A25), the reverse change of basis is:

$$K_\sigma^{DC} = \sum_{R\in(\mathbf{N}_C)_{\rm ir}} \frac{|D|}{n_R}\chi_R(D)\, K_\sigma^{RC}. \tag{B76}$$

And due to (A23), the elements of the new basis are orthogonal projectors summing up to the identity:

$$K_\sigma^{RC\dagger} = K_\sigma^{RC},$$
$$K_\sigma^{RC} K_\sigma^{R'C'} = \delta_{R,R'}\delta_{C,C'} K_\sigma^{RC},$$
$$\sum_{R,C} K_\sigma^{RC} = 1. \tag{B77}$$

10. The algebra $\mathcal{J}_\rho$

We discuss now the algebra of operators that gives the projectors onto states with different domain wall types in systems with Hamiltonian H_G^{NM} (35), with $N \subset M \subset G$ subgroups, N normal in G.

Definition 10 *Let ρ be an open ribbon. The ribbon operator algebra $\mathcal{J}_\rho \subset \mathcal{F}_\rho$ consists of those operators $J \in \mathcal{F}_\rho$ such that $[J, A_v^M] = [J, B_f^N] = 0$ for every vertex v and face f.*

We denote by r_T an arbitrarily chosen representative of a class T of the double coset $M\backslash G/M$, by $\mathbf{N}_T \subset M$ the subgroup of elements m such that $mr_TM = r_TM$ and by Q_T a set of representatives of $M/\mathbf{N}_T$. For any open ribbon ρ we define the operators

$$J_\rho^{CT} := \sum_{q\in Q_T}\sum_{c\in C} F_\rho^{qc\bar{q},qr_TM}, \tag{B78}$$

where $C \in (N, \mathbf{N}_T)_{\rm cj}$ and $T \in M\backslash G/M$. From (B15) we get

$$J_\rho^{CT} J_\rho^{C'T'} = \delta_{T,T'} \sum_{C''} N_{CC'}^{C''} J_\rho^{C''T},$$
$$J_\rho^{CT\dagger} = J_\rho^{\bar{C}T},$$
$$\sum_{T\in M\backslash G/M} J_\rho^{1T} = 1, \tag{B79}$$

where the sum runs over $C'' \in (N, M)_{\rm cj}$, $CC' = \sum_{C''} N_{C,C'}^{C''} C''$ and $\bar{C}$ denotes the inverse class of C. From (B26) we get

$$|G|{\rm Tr}(J_\rho^{CT}) = |T|\delta_{C,1}{\rm Tr}(1), \tag{B80}$$

which together with (B79) and $N_{CC'}^1 = \delta_{\bar{C},C'}|C|$ gives

$$|G|{\rm Tr}(J_\rho^{CT\dagger} J_\rho^{C'T'}) = |C||T|\delta_{C,C'}\delta_{T,T'}{\rm Tr}(1) \tag{B81}$$

Proposition 11 *Let ρ be an open ribbon. The operators J_ρ^{CT}, $C \in (N, \mathbf{N}_T)_{\rm cj}$, $T \in M\backslash G/M$, form a basis of $\mathcal{J}_\rho$.*

Proof. Set $(v_i, f_i) = \partial_i\rho$ and let $\mathcal{F}'_\rho \subset \mathcal{F}_\rho$ be the subalgebra of operators commuting with $A_{v_i}^M$. From (B41) and (B58) we get $\mathcal{F}'_\rho = (\,\sum_{m\in M} F_\rho^{mh\bar{m},mgM} \,|\, h, g \in G\,)$. $\mathcal{J}_\rho \subset \mathcal{F}'_\rho$ is the subalgebra of operators commuting with $B_{f_i}^N$. From (B42, B62) we get $\mathcal{J}_\rho = (\,\sum_{m\in M} F_\rho^{mh\bar{m},mgM} \,|\, h \in N, g \in G\,)$. Finally, if $h \in C \in (N, \mathbf{N}_T)_{\rm cj}$ and $g \in T \in M\backslash G/M$ we have $\sum_{m,\in M} F_\rho^{mh\bar{m},mgM} = \frac{|\mathbf{N}_T|}{|C|} J_\rho^{CT}$. The result follows in view of (B81). □

From the previous proposition and (B9, B51, B52) we get the following result, which is no longer true if the condition of N being abelian is removed.

Corolary 12 *Let ρ be an open ribbon and e an edge. If N is abelian $[J, L_e^N] = [J, T_e^M] = 0$ for any $J \in \mathcal{J}_\rho$.*

For any open ribbon ρ and $T \in M\backslash G/M$, consider the subalgebra $\mathcal{J}_\rho^T \subset \mathcal{J}_\rho$ with basis $\{\, J_\rho^{CT} \,|\, C \in (N, \mathbf{N}_T)_{\rm cj} \,\}$. The point is that in view of (A21, B79) we have $\mathcal{J}_C \simeq \mathcal{Z}_{N,\mathbf{N}_T}$. In particular the isomorphism identifies J^{CT} with e_C^M. Note that the isomorphism preserves adjoints

as defined in (A18). This suggests the introduction of a different basis for $\mathcal{J}_\rho$. We define in analogy with (A30),

$$J_\rho^{RT} := \frac{n_R\,|\tilde{R}|\,|N|}{|\mathbf{N}_T|^2} \sum_{C\in(N,\mathbf{N}_T)_{\rm cj}} \bar{\chi}_R(C)\, J_\rho^{CT}, \qquad \text{(B82)}$$

where $R \in (N,\mathbf{N}_T)_{\rm ir}$. Due to (A31), the reverse change of basis is:

$$J_\rho^{CT} = \sum_{R\in(N,\mathbf{N}_T)_{\rm ir}} \frac{|C|}{n_R}\chi_R(C)\, J_\rho^{RT} \qquad \text{(B83)}$$

And due to (A29), the elements of the new basis are orthogonal projectors summing up to the identity:

$$\begin{aligned} J_\rho^{RT\dagger} &= J_\rho^{RT}, \\ J_\rho^{RT} J_\rho^{R'T'} &= \delta_{R,R'}\delta_{T,T'} J_\rho^{RT}, \\ \sum_{R,T} J_\rho^{RT} &= 1. \end{aligned} \qquad \text{(B84)}$$

Two comments should be made here. First, in the particular case of M normal in G, $M\backslash G/M = G/M$ and for $T \in G/M$ we have $\mathbf{N}_T = M$, so that the two labels for the basis of $\mathcal{J}_\rho$ are not related anymore. Secondly, although definition 10 only applies to open ribbons, the algebra $\mathcal{J}_\rho$ can be extended to any ρ taking proposition 11 as a definition. As long as ρ is proper, the properties (B79-B84) will still hold.

The special case of M normal and N central in M deserves special attention. Instead of (B78,B82) we can write

$$J_\rho^{n,t} := F^{n,tM}, \quad J_\rho^{\chi,t} := \frac{1}{|N|}\sum_{n\in N} \bar{\chi}(n)\, J_\rho^{n,t}, \qquad \text{(B85)}$$

where $n \in N$, $\tilde{t} \in G/M$ and $\chi \in (N)_{\rm ch}$, with $(N)_{\rm ch}$ the character group of N. Then, if $\rho = \rho_1\rho_2$ is an open ribbon from (B9) we get (64).

11. The algebra $\mathcal{K}'_\sigma$

Here we discuss the algebra of operators that gives the projectors onto states of different charge, confined and topological, in systems with Hamiltonian H_G^{NM} (35), where $N \subset M \subset G$ are normal subgroups in G with N central in M.

Definition 13 *Let σ be a closed ribbon. The closed ribbon operator algebra $\mathcal{K}'_\sigma \subset \mathcal{F}_\sigma$ consists of those operators $K \in \mathcal{F}_\sigma$ such that $[K, A_v^M] = [K, B_f^N] = [K, T_e^M] = [K, L_e^N] = 0$ for any vertex v, face f and edge e.*

Note that if $N = 1$ and $M = G$ then $\mathcal{K}'_\sigma = \mathcal{K}_\sigma$. We extend our previous notation and set $(A,B)_{\rm cj} := \{\, \{\, bab\bar{b} \,|\, b \in B \,\} \,|\, a \in A \,\}$ for two subgroups A, B of some other group. For each class $C \in (G/N, M/N)_{\rm cj}$, we choose a representative $r_C \in G$. Let $\mathbf{N}'_C := \{\, m \in M \,|\, mr_C\bar{m}\bar{r}_C \in N \,\}$ and choose a set $Q_C \subset M$ of representatives of $M/\mathbf{N}'_C$. For any closed ribbon σ we define the operators

$$K_\sigma^{DC} := \sum_{q\in Q_C}\sum_{d\in D}\sum_{n\in N} F_\sigma^{qd\bar{q},qr_C\bar{q}n}, \qquad \text{(B86)}$$

where $C \in (G/N, M/N)_{\rm cj}$ and $D \in (\mathbf{N}'_C)_{\rm cj}$. With this notation, the results (B72) remain true, and (B73, B88) only need a slight modification:

$$|G|{\rm Tr}(K_\sigma^{DC}) = |C||N|\delta_{D,1}{\rm Tr}(1), \qquad \text{(B87)}$$

$${\rm Tr}(K_\sigma^{DC\dagger} K_\sigma^{D'C'}) = \frac{|D||C||N|}{|G|}\delta_{D,D'}\delta_{C,C'}{\rm Tr}(1). \qquad \text{(B88)}$$

Proposition 14 *Let σ be a proper closed ribbon. The operators K_σ^{DC}, $C \in (G/N, M/N)_{\rm cj}$, $D \in (\mathbf{N}'_C)_{\rm cj}$, form a basis of $\mathcal{K}'_\sigma$.*

Proof. Set $(v,f) = \partial\sigma$ and let $\mathcal{F}'_\sigma \subset \mathcal{F}_\sigma$ be the subalgebra of operators commuting with A_v^M and B_f^N. From (B45, B58, B62) we get $\mathcal{F}'_\sigma = (\sum_{m\in M} F_\sigma^{\bar{m}hm,\bar{m}gm} \,|\, h,g \in G, hg\bar{h}\bar{g} \in N)$. $\mathcal{K}'_\sigma \subset \mathcal{F}'_\sigma$ is the subalgebra of operators commuting with L_e^N and T_e^M for every edge e. From (B50, B51, B59, B63) it follows that $\mathcal{K}_\sigma = (\sum_{m\in M}\sum_{n\in N} F_\sigma^{mh\bar{m},mg\bar{m}n} \,|\, h \in M, g \in G, hg\bar{h}\bar{g} \in N)$. But given such h and g there exists a class $C \in (G/N, M/N)_{\rm cj}$ and $q \in Q_C$ with $\bar{q}gq\bar{r}_C \in N$, and a class $D \in (\mathbf{N}'_C)_{\rm cj}$ with $\bar{q}hq \in D$, so that $\sum_{m\in M}\sum_{n\in N} F_\sigma^{mh\bar{m},mg\bar{m}n} = \frac{|\mathbf{N}'_C|}{|D|}K_\sigma^{DC} = \frac{|M|}{|C||D|}K_\sigma^{DC}$. The result follows in view of (B88). □

The change of basis (B75) that leads to the relations (B77) is possible for $\mathcal{K}'_\sigma$ just as it was for $\mathcal{K}_\sigma$, with the only difference that now the representations R belong to $(\mathbf{N}'_C)_{\rm ir}$.

For any proper closed ribbon we have $\mathcal{J}_\sigma \subset \mathcal{K}'_\sigma$. In fact

$$J_\sigma^{nt} = \sum_{C\subset tM} K_\sigma^{nC}, \qquad \text{(B89)}$$

where $n \in N$, $t \in G/M$, $C \in (G/N, M/N)_{\rm cj}$ and $K_\sigma^{nC} = K_\sigma^{DC}$ with $D = \{n\} \in (N, \mathbf{N}'_C)_{\rm cj} \subset (\mathbf{N}'_C)_{\rm cj}$. From (B76, B82, B89) we get the following relation between the corresponding projector bases

$$J_\sigma^{\chi t} = \sum_{C\subset tM}\sum_{R\in(\mathbf{N}'_C)_{\rm ir}} \frac{(\chi_R,\chi)_N}{n_R} K_\sigma^{RC}, \qquad \text{(B90)}$$

where $\chi \in (N)_{\rm ch}$, $t \in G/M$ and $C \in (G/N, M/N)_{\rm cj}$.

APPENDIX C: RIBBON TRANSFORMATIONS

In this appendix we discuss several transformations that can be applied to ribbons. These transformations are interesting because they leave invariant the action of

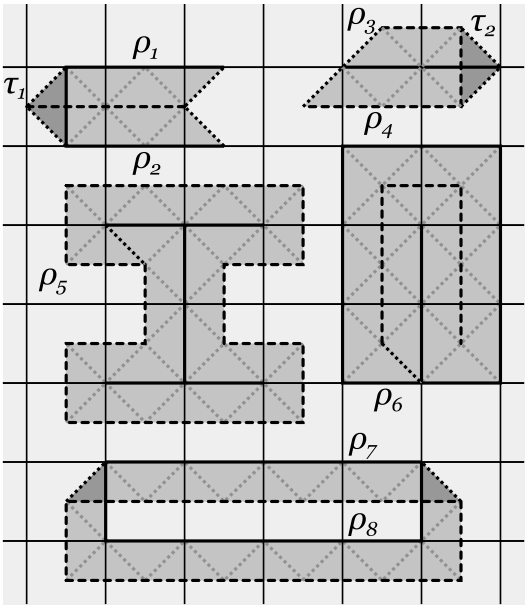


FIG. 14: Several constructions with nice strips and ribbons. All elements are displayed as in Fig. 13. The ρ_i are ribbons, except ρ_5 and ρ_6 which are just nice strips. We have $(\rho_1, \tau_1, \rho_2)_\triangleleft$ and $(\rho_3, \tau_2, \rho_4)_\triangleright$. ρ_5 is a dual block and ρ_6 is a direct block. ρ_7 and ρ_8 form a simple deformation, $(\rho_7, \rho_8)_=$.

certain ribbon operator algebras on suitable subspaces of $\mathcal{H}_G$. In order to proof the desired properties, we need some preliminary results. We will find useful the notation $\cdot =_\psi \cdot$ for $\cdot|\psi\rangle = \cdot|\psi\rangle$. Also, for strips ρ, ρ' and a triangle τ, we write $(\rho, \tau, \rho')_\triangleleft$ if τ is direct, $(\rho, \tau)_\prec$, $(\rho', \tau)_\succ$ and we write $(\rho, \tau, \rho')_\triangleright$ if τ is dual, $(\tau, \rho)_\prec$, $(\tau, \rho')_\succ$, see Fig. 14.

Lemma 15 *Let ρ, ρ' be ribbons, $|\psi\rangle \in \mathcal{H}_G$ and $H, H' \subset G$ normal subgroups with $hh' = h'h$ for any $h \in H$, $h' \in H'$.*
(i) If $(\rho, \rho')_\triangle$, there exist a direct triangle τ such that $(\rho, \tau, \rho')_\triangleleft$ and for any $f \in F_\rho - \{f_{\partial_0\rho}, f_{\partial_1\rho}\}$ we have $B_f^H =_\psi 1$ then for $h' \in H'$

$$L_\rho^{h'} =_\psi \sum_{k,l\in G} F_{\rho'}^{l\bar{k}\bar{h}'k\bar{l},l} T_\tau^k. \tag{C1}$$

(ii) If $(\rho, \rho')_\triangledown$ then for $g \in G$

$$T_\rho^g =_\psi T_{\rho'}^{\bar{g}} \tag{C2}$$

Proof. *(i)* Let $p_\rho^* = (f_0^*, \ldots, e_r^*, f_r^*)$ and set $s_i = (\partial_0 e_{i+1}, f_i)$ for $i = 1, \ldots, r-1$. Consider the states $|\psi^{g,\mathbf{h}}\rangle := L_{e_1}^{H'} T_\tau^g L_{e_2}^{H'} B_{s_1}^{h_1} \cdots L_{e_r}^{H'} B_{s_{r-1}}^{h_{r-1}} |\psi\rangle$, $g \in G$, $\mathbf{h} \in H^{r-1}$. Then $L_{e_i}^{H'} =_{\psi^{g,\mathbf{h}}} 1$ and thus $L_\rho^{H'} =_{\psi^{g,\mathbf{h}}} L_{\rho'}^{H'} =_{\psi^{g,\mathbf{h}}} 1$. But $|\psi\rangle = \sum_{g\in G} T_\tau^g \sum_{\mathbf{h}\in H^{r-1}} \prod_{i=1}^{r-1} B_{s_{i-1}}^{h_i} |\psi^{\mathbf{g}}\rangle$, and the result follows using (B51) and the fact that $[L_\rho^k, B_{s_i}^h] = [L_{\rho'}^k, B_{s_i}^h] = 0$ for $k \in H'$, $h \in H$.
(ii) The proof is dual to (i). Just note that one must use $\sum_{k\in G} L_\tau^{\bar{k}} T_{e_1}^1 L_\tau^k = 1$ instead of $\sum_{k\in G} T_\tau^k L_{e_1}^{H'} T_\tau^k = 1$ and $\sum_{k\in G} A_{v_{i-1}}^{\bar{k}} T_{e_i}^1 A_{v_{i-1}}^k = 1$ instead of $\sum_{k\in H} B_{f_{i-1}}^k L_{e_i}^{H'} B_{s_{i-1}}^k = B_{f_{i-1}}^H$. Alternatively, the result is trivial in terms of Wilson loops. □

When working with ribbon deformations, it is useful to consider triangle strips that are more general than ribbons but still allow to introduce operators. We say that a strip ρ is nice if no two of its triangles overlap or, equivalently, if $\rho = \rho_1 \cdots \rho_n$ with ρ_i ribbons such that$(\rho_i, \rho_j)_\oslash$ for $i \neq j$. Then ribbon operators can be generalized for nice strips using (B9). Although such nice strip operators still commute with all vertex operators A_v and face operators B_f except those in their ends, they can no longer be characterized by this property. A direct (dual) block ρ is a nice closed strip such that $(\rho, \rho)_\triangle$ ($(\rho, \rho)_\triangledown$), see Fig. 14.

Lemma 16 *Let ρ be a nice closed strip, $|\psi\rangle \in \mathcal{H}_G$ and $H \subset G$ a normal subgroup.*
(i) If ρ is a dual block and for any $v \in V_\rho$ we have $A_v^H =_\psi 1$ then

$$L_\rho^H =_\psi 1 \tag{C3}$$

(ii) If ρ is a direct block and for any $f \in F_\rho$ we have $B_f^H =_\psi 1$ then

$$T_\rho^H =_\psi 1 \tag{C4}$$

Proof. *(i)* We proceed recursively on $|V_\rho|$. For $|V_\rho| = 0, 1$ the result is trivial. So let $|V_\rho| > 1$. Note that if $(\rho, \rho')_\circ$ then $L_\rho^H = L_{\rho'}^H$ due to (B32). Also, the path $p_\rho = (v_0, \ldots, e_q', v_r)$ forms a tree. Thus, w.l.o.g. we can choose ρ such that $v_1 = v_{r-1}$ and there exists a dual triangle τ such that $\rho = \rho_1\rho_2$ with $\alpha := \alpha_{\partial_0\rho} = \rho_1\tau$ and $(\rho_2, \tau, \rho_2)_\triangleleft$. Set $\rho_2 = \tau'\rho_3\bar{\tau}'$, with τ' a direct triangle. Then $L_\rho^{h'} = L_{\rho_1}^{h'} L_{\rho_2}^{h'} = L_{\rho_1}^{h'} \sum_{k\in G} T_{\tau'}^k L_{\rho_3}^{\bar{k}h'k} =_\psi L_{\rho_1}^{h'} \sum_{k\in G} T_{\tau'}^k L_{\bar{\tau}}^{\bar{k}h'k} = L_{\rho_1}^{h'} L_\tau^{h'} = L_\alpha^{h'} =_\psi 1$, where we have used the fact that $\rho_3\bar{\tau}$ is a block and (C1) for $\tau, \bar{\tau}$.
(ii) Again the proof is dual to (i) or, alternatively, trivial in terms of Wilson loops. □

Corolary 17 *Let $\rho = \rho_1\rho_2$ be a nice strip. Under the same conditions of the previous lemma we have, respectively,*
(i) for $h \in H$

$$L_{\rho_1}^h =_\psi \sum_{g\in G} T_{\rho_1}^g L_{\rho_2}^{\bar{g}hg}, \tag{C5}$$

(ii) for $g \in G$

$$T_{\rho_1}^{gH} =_\psi T_{\rho_2}^{\bar{g}H}. \tag{C6}$$

Proof. Apply (B9, B15) to (i) (C3) and (ii) (C4). □

For a region R we will understand a collection of faces f. We also consider dual regions R^*, collections of dual faces v^*.

1. Transformation rules

a. Deformations

Before we define general ribbon deformations, such as the one in Fig. 4, we have to introduce certain simpler ones which are easier to manage in proofs, as the one depicted in Fig. 14. Then simple deformations can be combined together to give the general ones. We say that the ribbons ρ, ρ' form a simple deformation, denoted $(\rho,\rho')_{=}$, if *(i)* they are open, *(ii)* they share no triangles, *(iii)* $(\rho,\rho')_{\prec\succ}$ and *(iv)* for any $e\in E^{\triangle}_{\rho}$ we have $\partial_1 e\in V'_{\rho}$. The dual of *(iv)* is automatically true: for any $e\in E^{\triangledown}_{\rho'}$ we have $f\in F_\rho$ for $f^*=\partial_1 e^*$. We will use the notation $F_{\rho,\rho'}=F_\rho-\{f_{s_0},f_{s_1}\}$ and $V_{\rho,\rho'}=V_{\rho'}-\{v_{s_0},v_{s_1}\}$, where $s_i=\partial_i\rho=\partial_i\rho'$.

Let $R=(R_1,R_2^*)$ with R_1 a region and R_2^* a region of the dual lattice. We introduce the relation between ribbons $\simeq_R$ as the minimal equivalence relation such that $\rho'_1\simeq_R\rho'_1$ if the following conditions are all true: $\rho_1=\rho_2\rho\rho_3$, $\rho'_1=\rho_2\rho'\rho_3$, $(\rho,\rho')_{=}$, $F_{\rho,\rho'}\subset R_1$ and $V^*_{\rho,\rho'}\subset R_2^*$. Thus, two ribbons are equivalent in the sense of $\simeq_R$ if they can be transformed one into the other through simple deformations within R. Given a state $|\psi\rangle\in\mathcal{H}_G$ and subgroups $H,H'\subset G$, H normal, we define $R^{H.H'}_{\psi}=(R_1,R_2^*)$ with R_1 the region such that $f\in R_1$ iff $B^H_f=_\psi 1$ and R_2^* the dual region such that $v^*\in R_2^*$ iff $A^{H'}_v=_\psi 1$. Then we write $\simeq^{HH'}_{\psi}$ for $\simeq_{R^{HH'}_{\psi}}$.

Proposition 18 *Let $|\psi\rangle\in\mathcal{H}_G$ and $H,H'\subset G$ normal subgroups with $hh'=h'h$ for any $h\in H$, $h'\in H'$. If ρ, ρ' are ribbons with $\rho\simeq^{H,H'}_{\psi}\rho'$ then*

$$F^{h',S}_{\rho}=_\psi F^{h',S}_{\rho'}, \tag{C7}$$

where $h'\in H'$, $S\in G/H$.

Proof. Using (B9) for $\rho=\rho_1\rho_2\rho_3$ we can write

$$F^{h',gH}_{\rho}=\sum_{l,m\in G}F^{h',l}_{\rho_1}F^{\bar l h' l,\bar l g m H}_{\rho_2}F^{\bar m\bar g h' g m,\bar m}_{\rho_3}, \tag{C8}$$

and thus it is enough to consider simple deformations $(\rho,\rho')_{=}$. In that case, we can set $\rho=\tau_1\rho_1\tau'_1$ with τ_1,τ'_1 dual triangles and there exists a ribbon ρ_2 such that $\rho_1\rho_2$ is a block and the conditions of lemma 16 (ii) are satisfied, so that (C6) applies. But $(\rho_2,\rho')_{\triangledown}$, so that using (C2) we get $T^S_\rho=T^S_{\rho_1}=_\psi T^{\bar S}_{\rho_2}=T^S_{\rho'}$. We can write $\rho_2=\bar\tau'_2\rho'_2\bar\tau_2$ and $\rho'=\tau_2\rho_3\tau'_2$ with τ_2,τ'_2 direct triangles, and set $\rho''_2=\bar\tau_1\rho'_2\bar\tau'_1$. Then $(\rho,\rho''_2)_{\triangle}$ and (C1) applies. Also, $\rho''_2\rho_3$ is a block and the conditions of lemma 16 (i) are satisfied, so that (C5) applies (for H'). Putting everything together we get $L^{h'}_\rho=_\psi\sum_{k,l\in G}F^{l\bar k\bar h' k\bar l}_{\rho''_2}T^k_{\tau_2}=_\psi\sum_{k\in G}L^{\bar k h' k}_{\rho_2}T^k_{\tau_2}=_\psi L^{h'}_{\rho'}$, where we have used also (B9, B16). □

b. Extensions, contractions and rotations

We also want to consider deformations in which the ends of ribbons are not fixed. Let $Q=(Q_1,Q_2^*)$ with $Q_1,Q_2\subset E_{\rm ext}$. We introduce the relation between ribbons $\asymp_Q$ as the minimal equivalence relation such that $\rho\asymp_Q\rho'$ if $\rho=\rho_1\rho'\rho_2$, $E^{\triangledown}_{\rho_i}\subset Q_1$ and $E^{\triangle}_{\rho_i}\subset Q_2$. Thus, two ribbons are equivalent in the sense of $\asymp_Q$ if they can be transformed one into the other through extensions or contractions within Q. We also introduce an equivalence relation $\eqsim_Q$ for closed ribbons, the minimal such that $\sigma\eqsim_Q\sigma'$ if $(\sigma,\sigma')_\circ$, $E^{\triangledown}_{\sigma\triangleright\sigma'}\subset Q_1$ and $E^{\triangle}_{\sigma\triangleright\sigma'}\subset Q_2$. Thus, two closed ribbons are equivalent in the sense of $\eqsim_Q$ if they can be transformed one into the other through rotations within Q. Given a state $|\psi\rangle\in\mathcal{H}_G$ and subgroups $H,H'\subset G$, H' normal, we set $Q^{HH'}_{\psi}:=(Q_1,Q_2^*)$ with Q_1 the collection of edges e with $T^H_e|\psi\rangle=|\psi\rangle$ and Q_2 the collection of edges e' with $L^{H'}_{e'}|\psi\rangle=|\psi\rangle$. Then we write $\asymp^{H,H'}_{\psi}$ for $\asymp_{Q^{HH'}_{\psi}}$ and similarly for $\eqsim$.

Proposition 19 *Let $|\psi\rangle\in\mathcal{H}_G$ and $H,H'\subset G$ subgroups with H' normal.*
(i) If ρ, ρ' are ribbons with $\rho\asymp^{HH'}_{\psi}\rho'$ then

$$\sum_{k\in H}F^{kh'\bar k,kgH}_{\rho}=_\psi\sum_{k\in H}F^{kh'\bar k,kgH}_{\rho'}, \tag{C9}$$

where $h'\in H'$, $g\in G$.
(ii) If σ, σ' are closed ribbons with $\sigma\eqsim^{HH'}_{\psi}\sigma'$ then

$$\sum_{k\in H}F^{kh\bar k,kg\bar k}_{\sigma}=_\psi\sum_{k\in H}F^{kh\bar k,kg\bar k}_{\sigma'}. \tag{C10}$$

where $h,g\in G$, $hg\bar h\bar g\in H'$.

Proof. (i) It is enough to consider $\rho=\rho'\tau$ or $\rho=\tau\rho'$ with τ a triangle and then apply (B9).
(ii) It is enough to consider that $\sigma\triangleright\sigma'=\tau$ and then apply (B32). □

c. Inversions

We finally consider other kind of ribbon transformations in which basically ribbons are reversed. As in the other cases, we start introducing suitable relations. For open ribbons ρ, ρ' and $R=(R_1,R_2^*)$ as above, we write $\rho\doteqdot_R\rho'$ if $\partial_0\rho=\partial_1\rho'$, $\partial_1\rho=\partial_0\rho'$ and either *(i.a)* $(\rho,\rho')_{\triangledown}$ and $V^*_\rho\subset R_2^*$ or *(i.b)* $(\rho,\rho')_{\triangle}$ and $F_\rho\subset R_1$. For closed ribbons σ, σ' and a triangle τ, we write $\sigma\doteqdot_{R,\tau}\sigma'$ if either *(ii.a)* $(\sigma,\sigma')_{\triangledown}$, τ is dual, $(\sigma,\tau,\sigma')_{\triangleright}$ and $V^*_\rho\subset R_2^*$ or *(ii.b)* $(\sigma,\sigma')_{\triangle}$, τ is direct, $(\sigma,\tau,\sigma')_{\triangleleft}$ and $F_\rho\subset R_1$. For $|\psi\rangle\in\mathcal{H}_G$, we write $\doteqdot^{HH'}_{\psi}$ for $\doteqdot_{R^{HH'}_{\psi}}$ and also $\doteqdot^{HH'}_{\psi}$ for $\doteqdot_{R^{HH'}_{\psi},\tau}$ if either τ is dual and $L^H_\tau=_\psi 1$ or τ is direct and $T^{H'}_\tau=_\psi 1$.

Proposition 20 *Let $|\psi\rangle \in \mathcal{H}_G$ and $H, H' \subset G$ normal subgroups with $hh' = h'h$ for any $h \in H$, $h' \in H'$.*
(i) If ρ, ρ' are open ribbons with $\rho \doteq_\psi^{H,H'} \rho'$ then

$$F_\rho^{h',S} =_\psi F_{\rho'}^{\bar{s}\bar{h}'s,\bar{S}}, \tag{C11}$$

where $h' \in H'$, $s \in S \in G/H$.
(ii) If σ, σ' are closed ribbons with $\sigma \doteqdot_\psi^{HH'} \sigma'$ then

$$\sum_{k\in H'} F_\rho^{\bar{k}h'k,\bar{k}Sk} =_\psi \sum_{k\in H'} F_{\rho'}^{\bar{k}\bar{s}\bar{h}'sk,\bar{k}\bar{S}k}, \tag{C12}$$

where $h' \in H'$ and $s \in S \in G/H$ with $sg\bar{s}\bar{g} \in H$.

Proof. (i.a) This case follows from (C2,C5).
(i.b) There exists ribbons ρ_i and direct ribbons ρ_i', ρ_i'', $i = 1, 2$, such that $\rho = \rho_1'\rho_1\rho_1''$ and $\rho = \rho_2'\rho_2\rho_2''$. Then there exists a direct triangle τ so that (C1) applies to ρ_1, ρ_2. Moreover, for $s = \partial_0\rho_1$ we have $\beta_s = \tau\rho_2''\rho_1'$ and $B_s^H =_\psi 1$. Then using also (B9) we have $L_\rho^{h'} =_\psi \sum_{m\in G} T_{\rho_1'}^m L_{\rho_1}^{\bar{m}h'm} =_\psi \sum_{k,l\in G} F_{\rho_2}^{l\bar{k}\bar{h}'k\bar{l},l} T_{\rho_1'\tau}^k =_\psi \sum_{l\in G} F_{\rho_2\rho_2''}^{l\bar{h}'\bar{l},l} T_{\rho_1'\tau\rho_2''}^H =_\psi \sum_{l\in G} F_{\rho'}^{l\bar{h}'\bar{l},l}$. Together with (C5), this gives (C11).
(ii.a) From (C2) we have $T_\sigma^g =_\psi T_{\sigma'}^{\bar{g}}$. We can set $\sigma = \tau'\rho$, $\sigma' = \rho'\bar{\tau}'$ with τ' a direct triangle. The strip $\sigma_0 = \bar{\tau}\rho\tau\rho'$ is a nice closed strip, and indeed a block. Then (B9,C5) give $L_\sigma^{h'} =_\psi \sum_{k\in G} T_\sigma^k L_{\tau\rho'\bar{\tau}}^{\bar{k}\bar{h}'k} =_\psi \sum_{k,l\in G} T_\sigma^k L_\tau^{\bar{k}\bar{h}'k} F_{\rho'}^{\bar{k}\bar{h}'k,l} L_{\bar{\tau}}^{\bar{l}\bar{k}\bar{h}'kl}$. But (C1) implies $L_\tau^g = \sum_{k\in G} T_{\tau'}^k L_{\bar{\tau}}^{\bar{k}\bar{g}k}$ for any $g \in G$, and then $L_\sigma^{h'} =_\psi \sum_{k\in G} T_\sigma^k L_{\sigma'}^{\bar{k}\bar{h}'k}$. The result follows.
(ii.b) From (C1) we have $L_\rho^{h'} =_\psi \sum_{k,l\in G} F_{\rho'}^{l\bar{k}\bar{h}'k\bar{l},l} T_\tau^k$. We can set $\sigma = \tau'\rho$, $\sigma' = \rho'\bar{\tau}'$ with τ' a dual triangle. The strip $\sigma_0 = \bar{\tau}\rho\tau\rho'$ is a nice closed strip, and indeed a block. Then (B9,C6) give $T_\sigma^{gH} =_\psi T_\rho^{gH} =_\psi T_{\tau\rho'\bar{\tau}}^{\bar{g}H} =_\psi \sum_{k\in H'} T_\tau^k T_{\sigma'}^{\bar{k}\bar{g}kH}$. Using (B13) the result follows. □

2. Deformations in $\mathcal{F}_\rho$, $\mathcal{K}_\sigma$, $\mathcal{J}_\rho$ and $\mathcal{K}'_\sigma$.

We are now in position to discuss the transformation properties of the ribbon operator algebras introduced in appendix B. We distinguish three cases, which depend on the values of the subgroups N, M that label the Hamiltonian (35).

a. *The original Kitaev model: $N = 1$, $M = G$.*

In this case we are interested in the algebras $\mathcal{F}_\rho$ and $\mathcal{K}_\sigma$. As for the first, open ribbons can be deformed so that if $\rho \simeq_\psi^{1G} \rho'$ then $F_\rho^{h,g} =_\psi F_{\rho'}^{h,g}$. That is, the action of $\mathcal{F}_\rho$ is invariant as long as ribbons are deformed without crossing any excitation. They can also be reversed: if $\rho \doteq_\psi^{1G} \rho'$ then $F_\rho^{h,g} =_\psi F_{\rho'}^{\bar{g}\bar{h}g,\bar{g}}$. Regarding closed ribbons, the action of $\mathcal{K}_\sigma$ is invariant under deformations ($\simeq_\psi^{1G}$) or rotations ($\eqcirc_\psi^{G1}$). Closed ribbon inversions give charge inversion: if $\sigma \doteqdot_\psi^{1G} \sigma'$ then $K_\sigma^{RC} =_\psi K_{\sigma'}^{\bar{R}^C\bar{C}}$, where $R^C := R^g$ (as defined in section A 2) with $r_{\bar{C}} = \bar{g}\bar{r}_C g$ for some $g \in G$.

b. *String tension: N and M normal, N central in M.*

In this case we are interested in the algebras $\mathcal{J}_\rho$, which gives the domain wall fluxes, and $\mathcal{K}'_\sigma$, which gives the charges. The action of $\mathcal{J}_\rho$ is invariant under deformations which do not cross confined excitations ($\simeq_\psi^{MN}$), even if ends change as long as they do not cross a domain wall ($\asymp_\psi^{MN}$). Inversions ($\doteq_\psi^{MN}$) give domain flux inversion: (χ, t) goes to $(\bar{\chi}^t, \bar{t})$. The action of $\mathcal{K}'_\sigma$ is invariant under deformations ($\simeq_\psi^{NM}$) or rotations in which the end of σ does not cross domain walls ($\eqcirc_\psi^{MN}$). Charge inversion ($\doteqdot_\psi^{NM}$) is as follows: (R, C) goes to $(\bar{R}^C, \bar{C})$ where $R^C := R^m$ with $r_{\bar{C}} = \bar{m}\bar{r}_C m$ for some $m \in M$.

c. *Domain walls: N normal and abelian.*

In this case we are only interested in domain wall fluxes, that is, in $\mathcal{J}_\rho$. Its action is invariant under deformations (those allowed by $\simeq_\psi^{NN}$), even if ends change as long as they do not cross a domain wall ($\asymp_\psi^{MN}$). Domain wall flux inversion ($\doteq_\psi^{NN}$) is as follows: (R, T) goes to $(\bar{R}^T, \bar{T})$, where $R^T := R^{r_T m}$ with $r_{\bar{T}} M = \bar{m}\bar{r}_T M$ for some $m \in M$, so that $\mathbf{N}_{\bar{T}} = \bar{m}\bar{r}_T \mathbf{N}_T r_T m$.

3. Charge types

The previous results about closed ribbon transformations must be complemented with the following one, which relates proper closed ribbon operators with local vertex and face operators. Let $N, M \subset G$ be normal subgroups of G with N central in M, and define for $R \in (\mathbf{N}'_C)_{\rm ir}$ and $C \in (G/N)_{\rm cj}$

$$D_s^{RC} := \frac{n_R}{|\mathbf{N}'_C|} \sum_D \sum_{q\in Q_C} \sum_{d\in D} \bar{\chi}_R(d) A_s^{qd\bar{q}} B_s^{qr_C\bar{q}} \tag{C13}$$

where D runs over $(\mathbf{N}'_C)_{\rm cj}$.

Proposition 21 *Let s be a site, σ a closed ribbon and τ a dual triangle with $\beta_s \doteqdot_{V_\sigma,\tau} \sigma$. If $|\psi\rangle \in \mathcal{H}_G$ is such that $A_v^M =_\psi 1$ for any vertex $v \neq v_s$ in f_s and $L_\tau^N =_\psi 1$ then*

$$K_\sigma^{RC} = D_s^{RC}, \tag{C14}$$

where $R \in (\mathbf{N}'_C)_{\rm ir}$, $C \in (G/N)_{\rm cj}$.

Proof. Let s' be the second site of σ, so that $v_{s'} = v_s$ and e_τ does not belong to $f_{s'}$. The states $|\psi^g\rangle := A_v^M B_{s'}^g$, $g \in G$, are such that

$\beta_s \doteqdot_{\psi^g}^{NM} \sigma$. Then with the notation of (C12) we have $\sum_{k\in H'} F_\sigma^{\bar{k}h'k,\bar{k}Sk} B_{s'}^g = \sum_{k\in H'} B_{s'}^{\bar{k}h'kg\bar{k}h'k} F_\sigma^{\bar{k}h'k,\bar{k}Sk} =_{\psi^g} \sum_{k\in H'} B_{s'}^{\bar{k}h'kg\bar{k}h'k} B_s^{\bar{k}Sk} =_{\psi^g} \sum_{k\in H'} A_s^{\bar{k}h'k} B_s^{\bar{k}Sk} B_{s'}^g$. Since $|\psi\rangle = \sum_g B_{s'}^g |\psi^g\rangle$, the result follows. □

APPENDIX D: LOCAL DEGREES OF FREEDOM

In this appendix we give the details of the results indicated in section (II D). Choose any $C \in (G)_{\rm cj}$ and two indices i, i' and define

$$|n\rangle := |n; i, i'\rangle := F_\rho^{\bar{c}_i, \bar{q}_i n q_{i'}} |\psi_G\rangle, \tag{D1}$$

where $|\psi_G\rangle$ is a ground state of H_G (1). Let V be the space with basis $|n\rangle$, $n \in \mathbf{N}_C$. Then there exists an evident isomorphism $p : \mathbf{C}[\mathbf{N}_C] \longrightarrow V$. For $n, n' \in \mathbf{N}_C$ and $s = \partial_0\rho$, $s' = \partial_1\rho$, consider the operators

$$a_{n,n'} := A_s^{\bar{q}_i n q_i} A_{s'}^{\bar{q}_{i'} n' q_{i'}}. \tag{D2}$$

They give a representation $a : \mathbf{N}_C \times \mathbf{N}_C \longrightarrow \mathbf{GL}(V)$ because

$$a_{n_1,n_2}|n\rangle = |n_1 n \bar{n}_2\rangle \tag{D3}$$

so that if $\mathcal{R} : \mathbf{N}_C \times \mathbf{N}_C \longrightarrow \mathbf{GL}(\mathbf{C}[\mathbf{N}_C])$ is the representation of appendix A, we have $a_{n_1,n_2}\, p = p\, \mathcal{R}_{n_1,n_2}$. This has several consequences. First, if we define in accordance with (A15) a basis for V with elements

$$|R; jj'\rangle := \sum_{n\in\mathbf{N}_C} \bar{\Gamma}_R^{jj'}(n)|n\rangle \tag{D4}$$

then in the new basis

$$a_{n,n'}|R; jj'\rangle = \sum_{k,k'=1}^{n_R} \Gamma_R^{kj}(n)\bar{\Gamma}_R^{k'j'}(n')|R; kk'\rangle. \tag{D5}$$

In $\mathbf{C}[\mathbf{N}_C]$ from (A19) we get

$$e_R^{uv} e_{R'}^{jj'} e_R^{v'u'} = \delta_{R,R'}\delta_{v,j}\delta_{v',j'} e_R^{uu'}, \tag{D6}$$

$$e_R e_{R'}^{jj'} = e_{R'}^{jj'} e_R = \delta_{R,R'} e_R^{jj'} \tag{D7}$$

which through the isomorphism p give

$$a_R^{uv} a'^{\,u'v'}_{\bar{R}} |R'; jj'\rangle = \delta_{R,R'}\delta_{v,j}\delta_{v',j'}|R; uu'\rangle, \tag{D8}$$

$$a_R|R'; jj'\rangle = a'_{\bar{R}}|R'; jj'\rangle = \delta_{R,R'}|R; jj'\rangle, \tag{D9}$$

where

$$a_R^{uv} := \frac{n_R}{|\mathbf{N}_C|} \sum_{n\in\mathbf{N}_C} \bar{\Gamma}_R^{uv}(n)\, a_{n,1}, \tag{D10}$$

$$a'^{\,uv}_R := \frac{n_R}{|\mathbf{N}_C|} \sum_{n\in\mathbf{N}_C} \bar{\Gamma}_R^{uv}(n)\, a_{1,n} \tag{D11}$$

$$a_R = \sum_{u=1}^{n_R} a_R^{uu}, \qquad a'_R = \sum_{u=1}^{n_R} a'^{\,uu}_R. \tag{D12}$$

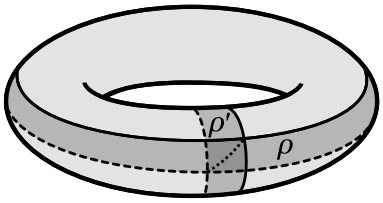


FIG. 15: In a torus we can find a pair of closed ribbons σ, σ' such that they form a crossed joint, $(\sigma, \sigma')_+$. This is not possible in a sphere.

Note that $a_R^{uv}, a_R \in \mathcal{D}_s$, $a'^{\,uv}_R, a'_R \in \mathcal{D}_{s'}$.

Finally, from (B42) we have

$$B_s^{c_k} B_{s'}^{\bar{c}_{k'}} |n; i, i'\rangle = \delta_{k,i}\delta_{k',i'}|n; i, i'\rangle \tag{D13}$$

and from (B41)

$$A_s^{\bar{q}_k q_i} A_{s'}^{\bar{q}_{k'} q_{i'}} |n; i, i'\rangle = |n; k, k'\rangle. \tag{D14}$$

Note that $|R; jj'\rangle$ is just a shorthand for (21). Finally, these results must be complemented with proposition 21.

APPENDIX E: SINGLE-QUASIPARTICLE STATES

Only in a surface of non-trivial topology can we find two closed ribbons σ, σ' such that $(\sigma, \sigma')_+$, see Fig. 15. When such ribbons exist, we can construct for any $h, g \in G$ the state

$$|\psi_{hg}\rangle := F_\sigma^{hg} L_{\sigma'}^{\bar{g}} \prod_v A_v |\mathbf{1}\rangle. \tag{E1}$$

The state $|\psi\rangle$ is not zero, because (B21,B45)

$$L_{\sigma'}^g L_\sigma^{\bar{h}} |\psi_{hg}\rangle = \prod_v A_v|\mathbf{1}\rangle. \tag{E2}$$

At most, it can have an excitation at $(v, f) = \partial\sigma = \partial\sigma'$. In fact (B45)

$$B_f|\psi_{hg}\rangle = \delta_{gh,hg}|\psi_{hg}\rangle, \tag{E3}$$

showing that for non-abelian groups single-quasiparticle excitations exist.

APPENDIX F: CONDENSATION

In this appendix we give the details of the calculations of certain expected values for ribbon operators $\langle F\rangle$ for a ground state of the Hamiltonian (35) for $N \subset M \subset G$ subgroups of G, N normal. Such ground states are characterized by the conditions (36). For $S \subset G$, $g \in G$ we introduce the notation

$$\delta_{g,S} := \delta_{gS,S}. \tag{F1}$$

Proposition 22 *Let $h, g \in G$, $n \in N$ and $|\psi\rangle, |\psi\rangle' \in \mathcal{H}_G$ satisfy* (36).
(i) For an arbitrary ribbon ρ

$$F_\rho^{h,g}|\psi\rangle = \delta_{g,M} F_\rho^{hn,g}|\psi\rangle, \tag{F2}$$

$$\langle\psi'|F_\rho^{h,g}|\psi\rangle = \delta_{h,M}\langle\psi'|F_\rho^{h,gn}|\psi\rangle. \tag{F3}$$

(ii) If ρ is an open ribbon

$$F_\rho^{NM}|\psi\rangle = |\psi\rangle, \tag{F4}$$

$$\langle\psi'|F_\rho^{h,g}|\psi\rangle = \delta_{h,N}\delta_{g,M}\frac{1}{|M|}\langle\psi'|\psi\rangle. \tag{F5}$$

(iii) If σ is a boundary ribbon

$$F_\sigma^{MN}|\psi\rangle = |\psi\rangle, \tag{F6}$$

$$\langle\psi'|F_\sigma^{h,g}|\psi\rangle = \delta_{h,M}\delta_{g,N}\frac{1}{|N|}\langle\psi'|\psi\rangle. \tag{F7}$$

Proof. (i) If ρ is a triangle this is a direct consequence of the identities $L_\tau^n L_\tau^N = L_\tau^N$, $T_\tau^g T_\tau^M = \delta_{g,M} T_\tau^g T_\tau^M$, $T_\tau^M L_\tau^h T_\tau^M = \delta_{h,M} T_\tau^M L_\tau^h T_\tau^M$ and $L_\tau^N T_\tau^g L_\tau^N = L_\tau^N T_\tau^{gn} L_\tau^N$. For general ribbons, just apply (B9).
(ii) From (i) we get $F_\sigma^{NM}|\psi\rangle = F_\sigma^{1G}|\psi\rangle = |\psi\rangle$ using (B16). Let $s_i = \partial_i\rho$ and set $\langle\cdot\rangle := \langle\psi'|\cdot|\psi\rangle$. Then from (B42, 36) we have $\langle F_\rho^{h,g}\rangle = \langle B_{s_0}^N F_\rho^{h,g}\rangle = \langle F_\rho^{h,gm} B_{s_0}^{Nh}\rangle = \delta_{h,N}\langle F_\rho^{h,gm}\rangle$ and for $m \in M$ from (B41, 36) we have $\langle F_\rho^{h,g}\rangle = \langle F_\rho^{h,g} A_{s_1}^m\rangle = \langle A_{s_1}^m F_\rho^{h,gm}\rangle = \langle F_\rho^{h,gm}\rangle$. Thus $\langle F_\sigma^{h,g}\rangle = \delta_{g,M}\delta_{h,N}\langle F_\sigma^{1,1}\rangle$ and the result follows since $\langle F_\rho^{1,M}\rangle = \langle F_\rho^{1,G}\rangle = \langle 1\rangle$.
(iii) Using the notation of appendix C, p_σ encloses a disc $R \subset R_\psi^N$ so that $F_\sigma^{MN}|\psi\rangle = |\psi\rangle$. Also, $L_\sigma^m|\psi\rangle = |\psi\rangle$ for any $m \in M$. To check this, suppose for example that the edges $E_\rho^\triangle$ lie outside R and choose for each vertex v in R a ribbon ρ_v with p_{ρ_v} a path inside R from $v_0 = v_{\partial_0\rho}$ to v. If we set $A_\rho^m = A_{v_0}^m \prod_{v\neq v_0}\sum_k T_{\rho_v}^k A_v^{\bar{k}mk}$, with the product running over all vertices in R, one can check that $|\psi\rangle = A^m|\psi\rangle = L_\sigma^m|\psi\rangle$. The other case is similar. Thus, for $m \in M$ we get $\langle F_\sigma^{h,g}\rangle = \delta_{g,N}\langle F_\sigma^{hm,g}\rangle$, so that $\langle F_\sigma^{h,g}\rangle = \delta_{g,N}\delta_{h,M}\langle F_\sigma^{1,1}\rangle$. The result follows since $\langle F_\rho^{1,N}\rangle = \langle F_\rho^{1,G}\rangle = \langle 1\rangle$. □

A state satisfying (F4,F6) for all open ribbons ρ and boundary ribbons σ cannot contain vertex, face or edge excitations. Therefore, these conditions characterize ground states.

We proceed to check (49), the derivation of (56) is similar. From (B70, F7) we get

$$\langle K_\sigma^{DC}\rangle = \frac{|C\cap N|}{|N||G|}\sum_{g\in G}|D\cap\bar{g}Mg|, \tag{F8}$$

where $D \in (\mathbf{N}_C)_{\rm cj}$, $C \in (G)_{\rm cj}$. This together with (B75) gives (49) because if $e_M\uparrow$ is the induced representation in G of the identity representation in M

$$\chi_{e_M\uparrow}(g) = \frac{1}{|M|}\sum_{k\in G}\delta_{g,\bar{k}Mk}. \tag{F9}$$

As for (55), from (F5) we have

$$|M|\langle\sum_{n\in\mathbf{N}_C}\Gamma_R^{jj'}(n)F_\rho^{\bar{c}_i,\bar{q}_i n q_i'}\rangle = \delta_{c_i,N}\sum_{n\in M_c^{i,i'}}\Gamma_R^{jj'}(n), \tag{F10}$$

where $M_c^{i,i'} := \mathbf{N}_C \cap q_i M \bar{q}_i'$. If $M_c^{i,i'}$ is empty, we are done. Else, $M_c^{i,i'} = M_c^{i,i}s$ for some $s \in \mathbf{N}_C$, so that $\sum_{n\in M_c^{i,i'}}\Gamma_R(n) = \sum_{n\in M_c^{i,i}}\Gamma_R(n)\Gamma_R(s)$. But[63] $\sum_{n\in M_c^{i,i}}\Gamma_R(n) = 0$ if $(\chi_R, 1)_{M_C^{i,i}} = 0$.

[1] X.-G. Wen. *Quantum Field Theory of Many-body Systems*, Oxford University Press, (2004).
[2] X.-G. Wen and Q. Niu, Phys. Rev. **B 41**, 9377 (1990).
[3] X.-G. Wen, Int. J. Mod. Phys. **B 4**, 239 (1990).
[4] X.-G. Wen, Int. J. Mod. Phys. **B 6**, 1711 (1992).
[5] X.-G. Wen, Phys. Rev. B **44**, 2664 (1991).
[6] J. Fröhlich and T. Kerler, Nucl. Phys. **B 354**, 369 (1991).
[7] D.S. Rokshar and S.A. Kivelson, Phys. Rev. Lett. **61**, 2376 (1988).
[8] N. Read and B. Chakraborty, Phys. Rev. **B 40**, 7133 (1989).
[9] R. Moessner and S.L. Sondhi, Phys. Rev. Lett. **86**, 1881 (2001).
[10] E. Ardonne, P. Fendley and E. Fradkin, Annals of Phys. **310**, 493 (2004).
[11] V. Kalmeyer and R.B. Laughlin, Phys. Rev. Lett. **59**, 2095 (1987).
[12] X. G. Wen, F. Wilczek, and A. Zee, Phys. Rev. B **39**, 11413 (1989).
[13] N. Read and S. Sachdev, Phys. Rev. Lett. **66**, 1773 (1991).
[14] T. Senthil and M.P. Fisher, Phys. Rev. Lett. **86**, 292 (2001).
[15] X.-G. Wen, Phys. Rev. B **65**, 165113 (2002).
[16] S. Sachdev and K. Park, Annals of Phys. **298**, 58 (2002).
[17] L. Balents, M. P. A. Fisher, and S. M. Girvin Phys. Rev. B **65**, 224412 (2002).
[18] A.Yu. Kitaev, Annals Phys. **303**, 2 (2003), `quant-ph/9707021`.
[19] M. Levin and X.-G. Wen, Phys. Rev. **B 67**, 245316 (2003).
[20] M. Levin and X.-G. Wen, Phys. Rev. **B 71**, 045110 (2005).
[21] H. Bombin and M.A. Martin-Delgado Phys. Rev. B **75**, 075103 (2007); cond-mat/0607736.
[22] F.A. Bais, Nucl. Phys. **B**170, 3 (1980).
[23] F.A. Bais, Phys. Lett. **B**98, 437 (1981).
[24] L.M. Krauss and F. Wilczek, Phys. Rev. Lett. **62**, 1221 (1989).
[25] J. Preskill and L.M. Krauss, Nucl. Phys. **B**341, 50 (1990).
[26] M. de Wild Propitius and F.A. Bais, in Particles and Fields, edited by G. Semenoff and L. Vinet, CRM Series

in Mathematical Physics (Springer-Verlag, New York, 1998), p. 353.
[27] F. A. Bais, B. J. Schroers, and J. K. Slingerland, Phys. Rev. Lett. **89**, 181601 (2002); arXiv:hep-th/0205117.
[28] F. A. Bais, B. J. Schroers, and J. K. Slingerland, JHEP 0305 (2003) 068; arXiv:hep-th/0205114.
[29] J. K. Slingerland and F. A. Bais, Nucl. Phys. **B**612, 229 (2001); cond-mat/0104035.
[30] E. Dennis, A. Kitaev, A. Landahl, J. Preskill, J. Math. Phys. **43**, 4452-4505 (2002).
[31] S. B. Bravyi, A. Yu. Kitaev, quant-ph/9811052.
[32] R. W. Ogburn and J. Preskill, Lecture Notes in Computer Science **1509**, 341–356, (1999).
[33] Michael H. Freedman, Alexei Kitaev, Zhenghan Wang, Commun.Math.Phys. **227** 587-603, (2002).
[34] M. Freedman, M. Larsen, Z. Wang, Comm.Math. Phys. **227** 605–622, (2002).
[35] M. H. Freedman, A. Kitaev, M. J. Larsen, Z. Wang, Bull. Amer. Math. Soc. **40** 31-38, (2003); quant-ph/0101025.
[36] C. Mochon, Phys. Rev. **A** 69, 032306 (2004); arXiv:quant-ph/0306063.
[37] L.S. Georgiev, arXiv:hep-th/0611340v2.
[38] S. Das Sarma, M. Freedman, C. Nayak, S.H. Simon, A. Stern arXiv:0707.1889.
[39] H. Bombin and M. A. Martin-Delgado; Phys. Rev. Lett. **97**, 180501 (2006); quant-ph/0605138.
[40] H. Bombin and M.A. Martin-Delgado; Phys. Rev. Lett. **98**, 160502 (2007); quant-ph/0610024.
[41] R. Raussendorf, J. Harrington1 and K. Goyal, New J. Phys. **9**, 199 (2007); arXiv:quant-ph/0703143v1.
[42] A. Galindo and M.A. Martin-Delgado, Rev.Mod.Phys. **74** 347 (2002); quant-ph/0112105.
[43] H. Bombin and M.A. Martin-Delgado; J. Math. Phys. **48**, 052105 (2007); quant-ph/0605094.
[44] H. Bombin and M.A. Martin-Delgado; Phys. Rev. A **76**, 012305 (2007); quant-ph/0703272.
[45] F. Verstraete, M.A. Martin-Delgado, J.I. Cirac, Phys. Rev. Lett. **92**, 087201 (2004).
[46] W. Dur, H.J. Briegel, Rep. Prog. Phys. **70**, 1381 (2007); arXiv:0705.4165.
[47] E. Rico and H.J. Briegel, arXiv:0710.2349.
[48] H. Katsura, T. Hirano, V.E. Korepin; arXiv:0711.3882.
[49] S. Yang, D.L. Zhou, C.P. Sun, arXiv:0708.0676, (2007).
[50] A. Hamma, D. A. Lidar; arXiv:quant-ph/0607145.
[51] L.-M. Duan, E. Demler, M. D. Lukin, Phys. Rev. Lett. **91**, 090402 (2003), `cond-mat/0210564`.
[52] A. Micheli, G.K. Brennen, P. Zoller, quant-ph/0512222.
[53] J. Du, J. Zhu, M. Shi, X. Peng, D. Suter, Phys. Rev. A 76, 042121 (2007); arXiv:0705.3566.
[54] J. J. Garcia-Ripoll, M. A. Martin-Delgado, J. I. Cirac, Phys. Rev. Lett. **93**, 250405 (2004).
[55] L.B. Ioffe, M.V. Feigel'man, A. Ioselevich, D. Ivanov, M. Troyer, and G. Blatter, Nature 415, 503 (2002).
[56] B. Doucot, L.B. Ioffe, J. Vidal, Phys.Rev. **B**69 214501 (2004); arXiv:cond-mat/0302104.
[57] A.F. Albuquerque, H.G. Katzgraber, M. Troyer, G. Blatter, arXiv:0708.0191.
[58] R. Dijkgraaf, V. Pasquier, and P. Roche, Nucl. Phys. (Proc. Suppl.) **B**18, 60 (1990).
[59] F.A. Bais, P. van Driel, and M. de Wild Propitius, Phys. Lett. **B** 280, 63 (1992).
[60] H. Bombin, M.A. Martin-Delgado, arXiv:0705.0007;
[61] M. B. Hastings, Xiao-Gang Wen, Phys.Rev. **B**72 (2005) 045141;
[62] R. Alicki, M. Fannes, M. Horodecki, J. Phys. A: Math. Theor. **40**, 6451 (2007); arXiv:quant-ph/0702102.
[63] J.-P. Serre, "Linear Representations of Finite Groups", Springer-Verlag, New York, 1977

Nested Topological Order

H. Bombin and M.A. Martin-Delgado
Departamento de Física Teórica I, Universidad Complutense, 28040. Madrid, Spain.

We introduce the concept of nested topological order in a class of exact quantum lattice Hamiltonian models with non-abelian discrete gauge symmetry. The topological order present in the models can be partially destroyed by introducing a gauge symmetry reduction mechanism. When symmetry is reduced in several islands only, this imposes boundary conditions to the rest of the system giving rise to topological ground state degeneracy. This degeneracy is related to the existence of topological fluxes in between islands or, alternatively, hidden charges at islands. Additionally, island deformations give rise to an extension of topological quantum computation beyond quasiparticles.

PACS numbers: 71.10.-w, 11.15.-q, 03.67.Pp, 71.27.+a

I. INTRODUCTION

The concept of topological orders [1] offers the possibility of finding new states of matter with a common picture of string-net condensation [2] and other variants thereof [3]. They correspond to examples of long range entanglement in quantum many-body systems where those correlations emerge in quantum states that are encoded in non-local degrees of freedom of topologically ordered systems. Their global properties are the source for yet another application as the suitable systems to implement topological quantum computation [4–7], a form of fault-tolerant quantum computation intrinsically resistant to the debilitating effects of local noise. Quantum field theories with an spontaneous symmetry breaking mechanism of a continuous gauge group down to a discrete group have been proposed as a scenario for realizing their physics [8–14].

In this paper we introduce the concept of nested topological order in a class of quantum lattice Hamiltonians. Our starting point are the family of Kitaev's models [4], which are labeled by a discrete gauge group. Such models can be modified [15] introducing an explicit symmetry breaking mechanism. Our aim is to study the effect of 'nesting' subsystems with a reduced symmetry inside systems with the complete gauge symmetry. We will consider a topologically ordered system divided in two regions, say A and C, and show that it is possible to partially destroy the topological order in region C in such a way that this imposes boundary conditions to the subsystem A. The system C can take the form of several islands, which is why we talk about 'nested' topological order. The boundary conditions induce a topological ground state degeneracy which is due to the possible values of certain fluxes in between islands. As we will see, the values of these fluxes correspond to the types of domain walls that exist in C. If we allow the region C to be deformed, then islands can be initialized, braided and fused, giving an interesting extension of the ideas of topological quantum computation beyond quasiparticles.

The models that we consider are string-net condensates in a 2D lattice [1], [2]. The configurations of the lattice are regarded as string-net states: a collection of labeled strings meeting at branching points. A string-net is closed if certain conditions hold at branching points and there are no loose ends. The ground state is a superposition of all possible deformations of such closed string-nets, and excited states correspond to configurations with loose ends: quasiparticle excitations appear at the ends of strings. Now, to such system Hamiltonians we can add string tension terms, which penalize with a higher energy those configurations with longer strings. As such terms get more important with respect to the original ones, longer strings become less relevant in the ground state and finally the topological order is destroyed as excitations get confined. Alternatively, we can add suitable terms so that only part of the topological order is destroyed. This is in fact the case for the Hamiltonians $H_G^{N,M}$ that we consider (1), which are labeled with a discrete group G and two subgroups $N \subset M \subset G$, with N abelian and normal in G. If $N = 1$ and $M = G$, we have the original topologically ordered models with gauge group G considered by Kitaev [4]. Otherwise, the gauge symmetry is reduced the quotient group $G' = M/N$. In particular, if $N = M$ the topological order is completely destroyed.

This paper is organized as follows: in Sect.II we introduce a model Hamiltonian which contains vertex, face and edge operators depending on a discrete gauge group G and two subgroups N and M. We describe some of its physical properties. In Sect.III we also introduce certain types of algebras for the so called ribbon operators which allow us to study in more detail the type of quasiparticle excitations present in the model Hamiltonian as well as a characterization of its ground state. In Sect.IV we study the appearence of nested phases associated to different choices of the groups G and N,M in different parts (islands) of the system. This gives rise to interesting physical phenomena like quasiparticle dilution, domain wall dilution and induced topological fluxes. In Sect.V we show how to prepare topologically protected subsystems based on the notion of nested topological order. These subsystems can be braided and fused in order to implement forms of topological quantum computation without quasiparticles. Sect.VI is devoted to conclusions.

II. TOPOLOGICAL PHASES

The systems of interest are constructed from a two-dimensional orientable lattice, of arbitrary shape. At every edge of the lattice we place a qudit, a $|G|$-dimensional quantum system with Hilbert space $\mathcal{H}'_G$ and a basis $|g\rangle$ labeled with the elements of G. The Hamiltonians read as follows[15]

$$H_G^{N,M} := -\sum_{v\in V} A_v^M - \sum_{f\in F} B_f^N - \sum_{e\in E} \left(T_e^M + L_e^N\right), \quad (1)$$

where the sums run over the set of vertices V, faces F and edges E. Explicit expressions for the terms in (1) will be given below, but before that, we will discuss their physical content. First, all the terms are projectors and commute with each other, so that the ground state is described by conditions of the form $P|\mathrm{GS}\rangle = |\mathrm{GS}\rangle$ with P either a vertex, face or edge operator. Excitations are gapped and localized; they correspond to violations of the previous conditions and so can be related to vertices, faces and edges; they are regarded respectively as electric, magnetic and domain wall excitations.

We first recall the case $H_G := H_G^{1,G}$[4]. For non-Abelian groups G, vertex and face excitations are interrelated and the excitation types, labeled as (R, C), are dyons: C, the magnetic part, is a conjugacy class of G and R, the electric part, is an irrep of $\mathbf{N}_C$, the group $\mathbf{N}_C := \{\, g \in G \,|\, gr_C = r_C g \,\}$, where r_C is some chosen element of C. These charges have a topological nature: if there are several excited spots in the system, far apart from each other, there exist certain global degrees of freedom which cannot be accessed through local operators.

In the general case $H_G^{N,M}$ there are two new phenomena, quasiparticle condensation and the appearance of domain wall excitations. The latter have an energy proportional to their length and can be labeled by pairs (R, T), with $T \in M\backslash G/M$ and R an induced representation in M of an irrep of the group $\mathbf{N}_T := \{\, m \in M \,|\, mr_T M = r_T M \,\}$, where r_T is some chosen element of T. Thus there exists a flux related to domain walls, with values (R, T); it is conserved in the absence of quasiparticle excitation, so that domain walls only can end at them. As for condensation, we will comment upon it below.

III. RIBBON OPERATORS

In order to motivate the introduction of ribbon operators, we first note that dyons, the excitations of our system, are located at vertex-face pairs, which are called sites. In Fig. 1 sites are represented as dotted lines connecting the vertex to the center of the face. The basic connectors between sites are triangles: just as an edge connects two vertices, triangles connects two sites. A direct (dual) triangle τ is composed by two sites and a direct (dual) edge e_τ, see Fig. 1. Triangles can be concatenated to form ribbons connecting distant sites. Ribbons are open if they connect disjoint sites and closed if their ends coincide. The point is that it is possible to attach to each ribbon ρ certain operators $F_\rho^{h,g}$, $h, g \in G$, which are very well suited to represent excited states. For example, any state with only two dyons is a linear combination of the states $F_\rho^{h,g}|\mathrm{GS}\rangle$, with ρ any ribbon connecting the sites where the dyons are located[4]. In fact, one can consider that ribbon operators represent a process in which a particle-antiparticle is created in one end of the ribbon and one of them is moved to the other end.

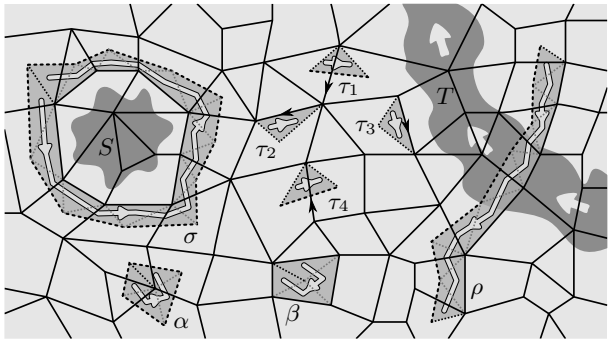


FIG. 1: Examples of lattice constructions. Although all the edges must be oriented, only the orientation of some of them is shown. The $\tau_i, i = 1, 2, 3, 4$ are triangles; the light thick arrow shows their orientation. τ_1 and τ_4 are dual, the others are direct. σ is a closed ribbon; the projectors $K_\sigma^{R,C}$ give the charge in the region S that σ encloses. ρ is an open ribbon; the projectors $J_\sigma^{R,T}$ give the domain wall flux in the region T in the direction of the arrows. α and β are minimal closed ribbons, enclosing respectively a single vertex and face.

In order to describe ribbon operators, we start with triangles, which are the smallest ribbons. Recall that a triangle is formed by two sites and one edge, direct or dual. Triangle operators act on the qudit attached to that edge, and the action depends on the orientation of the edge and the type of the triangle. The four possible cases are illustrated in Fig. 1. With the notation of that figure, we have $F_{\tau_1}^{h,g} = \delta_{g,1} \sum_k |hk\rangle\langle k|$, $F_{\tau_2}^{h,g} = |g^{-1}\rangle\langle g^{-1}|$, $F_{\tau_3}^{h,g} = |g\rangle\langle g|$ and $F_{\tau_4}^{h,g} = \delta_{g,1} \sum_k |kh^{-1}\rangle\langle k|$, where the sums run over G. Then if ρ is a ribbon formed by the concatenation of the ribbons ρ_1 and ρ_2, we set $F_\rho^{h,g} = \sum_k F_{\rho_1}^{h,k} F_{\rho_2}^{k^{-1}hk,k^{-1}g}$. The terms in the Hamiltonians (1) are built from ribbon operators. Let $F_\rho^{UV} := |U|^{-1} \sum_{u\in U} \sum_{v\in V} F_\rho^{u,v}$ for any subgroups $U, V \subset G$. Then $A_v^M := F_\alpha^{NG}$, $B_f^N := F_\beta^{1N}$, $T_e^M := F_\tau^{1M}$ and $L_e^N := F_{\tau'}^{NG}$, with α and β suitable minimal closed ribbons as in Fig. 1 and τ (τ') a direct (dual) triangle with $e = e_\tau$.

Ribbon operators commute with all the vertex operators A_v^G and face operators B_f^1, except with those at their ends. Moreover, they can be characterized by this

property[15]. This suggests considering, for closed ribbons σ, those ribbon operators which commute with all vertex and face operators, so that they 'forget' the single end of σ. It turns out that a linear basis for such operators is given by a family of projectors $K_\sigma^{R,C}$, labeled with the charge types (R, C) of the system H_G. In fact, if σ is a boundary ribbon, that is, a closed ribbon enclosing certain region S as in Fig. 1, then $K_\sigma^{R,C}$ projects out those states with total topological charge (R, C) in S. As a result, the ground state of H_G can be described by the conditions

$$F_\sigma^{G1}|\psi\rangle = |\psi\rangle, \tag{2}$$

which must hold for all boundary ribbon σ. This amounts to impose that all disc shaped regions must have trivial charge because $K_\sigma^{e1} = F_\sigma^{G,1}$, where e is the identity representation. In systems with Hamiltonian H_G^{NM} we can use the projectors K_σ^{RC} to describe condensation. Namely, for some charges [15] we have a ground state expectation value $\langle K_\sigma^{RC}\rangle > 0$ for any boundary ribbon σ, showing that there exist a non-zero probability of finding such charges in a given region.

Domain wall types can be obtained in a similar fashion in systems with Hamiltonian H_G^{NM}. For any open ribbons ρ, those ribbon operators that commute with all vertex operators A_v^M and face operators B_f^N are linear combinations of certain projectors $J_\rho^{R,T}$, with (R, T) a domain wall type. If ρ crosses an area with domain wall excitations then $J_\rho^{R,T}$ projects out those states with total domain wall flux (R, T) across ρ. For example, in Fig. 1 ρ will measure the flux of the excited region T in the direction of the white arrows.

The ground states of (1) can also be described in terms of conditions for ribbon operators, in particular by

$$F_\sigma^{MN}|\mathrm{GS}\rangle = |\mathrm{GS}\rangle, \quad F_\rho^{NM}|\mathrm{GS}\rangle = |\mathrm{GS}\rangle, \tag{3}$$

where σ and ρ are arbitrary boundary and open ribbons, respectively. The first condition is related to vertex and face excitations, and the second to edge excitations.

IV. NESTED PHASES

We are now in position to discuss a more complicated system. In particular, we want to consider a surface divided in two regions of arbitrary shape, A and C, plus a third region B which is just a thick boundary separating them, included so that the Hamiltonian does not have to change abruptly from A to C. The idea is to have a local Hamiltonian such that conditions (2) are satisfied in A, conditions (3) in C and the conditions

$$F_\sigma^{NN}|\mathrm{GS}\rangle = |\mathrm{GS}\rangle, \tag{4}$$

with σ an arbitrary boundary ribbon, in the whole system. The last condition is needed to ensure that domain wall flux is preserved through region B, a key ingredient of our construction as we will see. The ground state of the Hamiltonian $H_0 := -\sum_v A_v^N - \sum_f B_f^N$ is described precisely by (4). In addition, H_0 commutes with H_G, H_G^{NM}. Indeed, a Hamiltonian of the form $H' = H_G + \lambda H_0$, $\lambda \geq 0$, only differs from H_G in the gap for some excitations, and the same is true for H_G^{NM}. The Hamiltonian that we want to consider takes the form $H = H_0 + \lambda H_G + \mu H_G^{NM}$, where $\lambda, \mu \geq 0$ vary spatially so that $\lambda = 1$ and $\mu = 0$ in A and $\lambda = 0$ and $\mu = 1$ in C. If we take $\lambda\mu = 0$, the ground state has the desired properties but there exists some local degeneracy at B. This local degeneracy can be lifted if λ and μ are allowed to overlap, but on the other hand if the overlap is too big, it could produce a level crossing taking the ground state of H out of that of H_0, which spoils conditions (4).

Quasiparticle dilution. Our aim is to understand the effects of the nested region C on the topologically ordered region A. A first effect is the possibility to locally create or destroy single quasiparticle excitations in the vicinity of the A-C border, something prohibited in systems with Hamiltonian H_G due to charge conservation. In terms of ribbon operators, this is reflected in the fact that for any ρ_1 connecting C to A, as the one in Fig. 2(a), a state of the form $\sum_{m\in M} F_{\rho_1}^{mn\bar{m},mg}|\mathrm{GS}\rangle$, $n \in N$, contains no excitation at C. In terms of quasiparticle processes, this corresponds to create a particle-antiparticle pair in A and then move one of them into C, where it disappears because it is condensed.

Domain wall dilution. A second effect is related to the existence of domain walls in region C. Consider again a ribbon ρ_2 connecting C to A, see Fig. 2(a). Some of the states of the form $|\psi\rangle = \sum_{h,g} c_{h,g} F^{h,g}|\mathrm{GS}\rangle$, $c_{h,g} \in \mathbf{C}$, will contain edge excitations all along the portion of ρ_2 contained in C, for example those with $c_{h,g} \neq 0$ for some $g \in G, h \notin M$. These excitations form a domain wall, to which we can relate a type or flux given by the projector $J_{\rho_3}^{RC}$, where ρ_3 is a ribbon that lies in C and crosses the domain wall, see Fig. 2(a). Such a ribbon can be deformed without crossing any quasiparticle excitation onto another ribbon ρ_4 that only has its endpoints in C and thus avoids the domain wall, so that $J_{\rho_3}^{R,T}|\psi\rangle = J_{\rho_4}^{R,T}|\psi\rangle$ due to (4). Both ribbon operators are measuring the same domain wall flux. However, in the case of ρ_4 the flux is being measured in A, where the domain wall gets diluted as it turns into a condensed string. Note that $J_{RC}^{\rho_4}$ cannot detect changes in the interior of C. In this regard, if we restrict our attention to region A, domain wall flux projectors from ribbons like ρ_4, that is, which enclose a portion of the $A - C$ border, can be related to charges (R, T) that lie in that piece of the $A - C$ border.

Induced topological fluxes. Things get even more interesting if we consider that C consists of several disjoint parts. For example, consider a plane and choose as the region C two islands C_1 and C_2, see Fig. 2(b). Now instead of considering a domain wall flux coming out from a region of B (such as the one measured by ρ_4 in Fig. 2(a)), we consider the flux in between the two islands (as indicated by the arrows in Fig. 2(b)). This is the

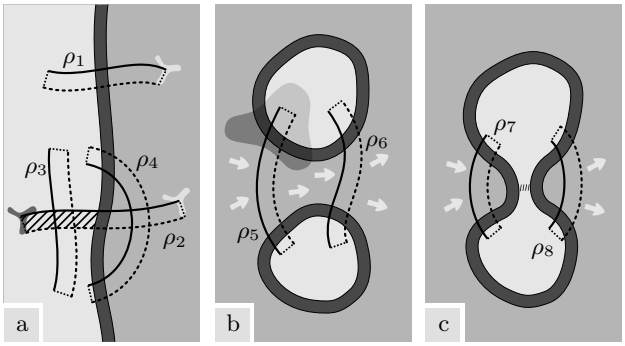


FIG. 2: In this figure regions A, B and C are shaded respectively with medium, dark and light gray. Ribbons $\rho_i, i = 1, \ldots, 8$ are displayed as pairs of solid and dashed parallel lines which correspond respectively to their direct and dual edges. Light spots at the end of ribbons represent excitations in A and the dark one an excitation in C. The striped areas are domain wall excitations. (a) Due to condensation, suitable ribbon operators attached to ρ_1 will create an excitation in A but no excitation in C. Ribbon operators attached to ρ_2 can create a domain wall excitation in C. The resulting state ψ is such that $J^{R,T}_{\rho_3}|\psi\rangle = J^{R,T}_{\rho_4}|\psi\rangle$. (b) Both ρ_5 and ρ_6 measure the flux in between the islands. If O is an operator with support in the shaded area an takes ground states to ground states, it cannot change the flux. (c) If the previous islands are deformed till they fuse, the flux measured by ρ_7, ρ_8 will remain the same as it was for ρ_5, ρ_6. If it is nontrivial, opposite border charges are present at the sides of the meeting point.

flux measured by the projectors $J^{R,T}_{\rho_5}$, where ρ_5 is any ribbon that connects the islands, as in Fig. 2(b). The point is that such a flux is a global (topological) property as long as the islands are distant. Indeed, measuring the flux requires an operator with a support connecting C_1 and C_2. And, if an operator changes the flux, its support must loop around C_1 (or C_2). Suppose to the contrary that O is an operator that leaves the ground state invariant and has a support not enclosing C_1, as the shaded region in Fig. 2(b). Let ρ_6 be another ribbon connecting the islands but lying outside the support of O. Due to (4) we have $J^{R,T}_{\rho_5}|\mathrm{GS}\rangle = J^{R,T}_{\rho_6}|\mathrm{GS}\rangle$, so that $[J^{R,T}_{\rho_5}, O]|\mathrm{GS}\rangle = [J^{R,T}_{\rho_6}, O]|\mathrm{GS}\rangle = 0$ and thus O does not change the flux. Those operators which do change the flux are related to processes in which a particle-antiparticle pair is created, one of them loops around C_1 and they meet again to fuse into a charge that disappears into C_1.

V. TOPOLOGICALLY PROTECTED SUBSYSTEMS

It follows that there exist a topological degeneracy in the ground state, related to the distinct values that the flux in between C_1 and C_2 can take. For example, if $N = M = 1$ the flux can take any value $g \in G$. In general, for a C composed of multiple disconnected regions, the degeneracy of the ground state depends on N, M and the topology of A. Tunneling between ground states corresponds to virtual processes in which topological charges move from island to island or around an island, and thus are exponentially suppressed as the corresponding distances grow.

Now, it is natural to ask how does this protected space compares with the one due to to the existence of several separated quasiparticles in A. In other words, do islands add something new? This can be positively answered through an example: two excitations give no protected subspace [4], but we have just seen the contrary for the case of two islands. Perhaps more dramatically, for abelian groups G the protected subsystem is always trivial whatever the amount of excitations, but this is not the case for islands. A source for the additional dimensionality of the protected subsystem lies in the fact that islands can hold different charge values, which admit coherent superpositions. This is not the case for quasiparticles, in the sense that local decoherence will destroy any superposition of different topological charges. An additional difference between a charged island and a charged excitation is that some of the local degrees of freedom of the excitation become global in the case of the island.

Braiding. The physics of the system so far has a static nature. If we want to consider the setting as an scenario for quantum computation, then the possibility of dynamically deforming the region C must be included in it. Such deformations need not be strictly adiabatic, but the state should be kept in the subspace defined by conditions (2-4) at all time. We can then braid islands to perform unitary operations, in complete analogy with quasiparticle braiding. An advantage of islands is that they do not require the selective addressing that quasiparticles do. It is also natural to enrich the physics by considering islands with different (N, M) labels, increasing the variety of protected subsystems.

Fusion. We must consider also the analogue of the quasiparticle fusion processes, which is the way in which measurements are carried out in topological quantum computation. There are two natural ways in which global degrees of freedom can be made local. The first is to decrease the size of an island till it disappears leaving a small charged region. The outcome of such a process is the charge, which can be measured but not changed locally. The second way is closer to the idea of fusion. Indeed, it is also a fusion, but of islands instead of quasiparticles. The idea is depicted in Fig. 2(c). As two islands of the same (N, M) type get closer, some of the ribbon operators connecting them become small and thus the flux between the islands is exposed to local measurements. If we continue the approach till the islands meet, the flux will take the form of a domain wall excitation at the meeting place, as in Fig. 2(c). Due to confinement the domain wall can decay to several smaller walls, but there is something that will not disappear, the two border charges in its ends on B. As explained in the caption

of Fig. 2(c), the appearance of this border charges can be seen directly in terms of ribbon operators. Regarding the initialization of the system, reverse processes can be used. That is, if an island is divided in two, the topological flux in between them will be trivial, and if an island is created from the vacuum, it will have trivial charge. In both cases the reason is that topological properties cannot be changed by local processes.

VI. CONCLUSIONS

In this work we have introduced the concept of nested topological order and explicit constructions which are relevant for the study of the relationship between topological orders in condensed matter systems and its application to novel ways of topological quantum computation. We summarize some of them:

i/ We have found new possibilities of having subsystems with different topological orders based on a newly introduced class of Hamiltonians, eq. (1) with non-abelian discrete symmetries.

Among these new possibilities, we can mention the phenomena of quasiparticle dilution, domain wall dilution, induced topological fluxes etc. which are of interest for the foundations of novel topological orders. In addition, these new phenomena serve as the basis for new ways of topological quantum computation as we explain below.

ii/ We pay special attention to those cases in which within a system with a given topological order, we introduce a series of islands with a reduced order. When the interfaces between the subsystems obey certain properties, we find that the ground state of the system is degenerate due to the appearance of certain topological fluxes in between the islands, which are labeled in the same way as domain walls inside the islands.

iii/If we add island deformations to our nested topological scheme, we get a generalization of the ideas of topological quantum computation beyond quasiparticles.

iv/ The advantages of this proposal for topological quantum computation is mainly two-fold: on one hand, the protected space is bigger. This is most evident in the abelian case, where there is no protected space at all whatever the number of quasiparticles. A reason for this increased protected space is that islands can hold different charges, which means that quantum superpositions of different charges can be constructed (these not being allowed for quasiparticles in the sense that local decoherence destroys them). On the other hand, another advantage is that manipulation of islands could be easier than that of quasiparticles, in the sense that the need for addressing excitations is eliminated.

Acknowledgements We acknowledge financial support from a PFI grant of the EJ-GV (H.B.), DGS grants under contracts BFM 2003-05316-C02-01, FIS2006-04885 (H.B., M.A.M.D,), and the ESF Science Programme INSTANS 2005-2010 (M.A.M.D.).

[1] X.-G. Wen. *Quantum Field Theory of Many-body Systems*, Oxford University Press, (2004).
[2] M.Levin and X.-G.Wen, Phys. Rev. **B71**, 045110 (2005).
[3] H. Bombin and M.A. Martin-Delgado ; Phys. Rev. B **75**, 075103 (2007); cond-mat/0607736.
[4] A.Yu. Kitaev, Annals Phys. **303**, 2 (2003)
[5] Michael H. Freedman, Alexei Kitaev, Zhenghan Wang, Commun.Math.Phys. **227** 587-603, (2002).
[6] M. Freedman, M. Larsen, Z. Wang, Comm. Math. Phys. **227** 605–622, (2002).
[7] S. Das Sarma, M. Freedman, C. Nayak, S.H. Simon, A. Stern arXiv:0707.1889.
[8] F.A. Bais, Nucl. Phys. **B**170, 3 (1980).
[9] F.A. Bais, Phys. Lett. **B**98, 437 (1981).
[10] L.M.Krauss and F.Wilczek, Phys. Rev. Lett. **62**, 1221 (1989).
[11] J. Preskill and L.M. Krauss, Nucl. Phys. **B**341, 50 (1990).
[12] F. A. Bais, B. J. Schroers, and J. K. Slingerland, Phys. Rev. Lett. **89**, 181601 (2002); arXiv:hep-th/0205117.
[13] F. A. Bais, B. J. Schroers, and J. K. Slingerland, JHEP 0305 (2003) 068; arXiv:hep-th/0205114.
[14] F.A. Bais, P. van Driel, and M. de Wild Propitius, Phys. Lett. **B** 280, 63 (1992).
[15] H. Bombin, M.A. Martin-Delgado, arXiv:0712.0190.