UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

TESIS DOCTORAL

Entrelazamiento y Simetría en Sistemas Cuánticos de Muchos Cuerpos

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Carlos Eduardo González Guillén

Director

David Pérez García

Madrid, 2014

© Carlos Eduardo González Guillén, 2014

Entrelazamiento y Simetría en Sistemas Cuánticos de Muchos Cuerpos

Carlos Eduardo González Guillén

Memoria presentada para optar al grado de
Doctor en Ciencias Matemáticas
con mención de *Doctorado Europeo*

2014

Dirigida por el Profesor

David Pérez García

Agradecimientos

Ha llegado el mejor momento de un trabajo, el de agradecer a todas las personas que de alguna manera lo han hecho posible.

En primer lugar quiero agradecer a mi director David Pérez García, cuya guía ha hecho posible esta tesis. Su conocimiento, dedicación y pasión por la ciencia me han inspirado en todo momento. Desde el primer día he sentido su apoyo incondicional y siempre he encontrado en él las palabras de aliento necesarias.

También es mérito de David y de Nacho Villanueva el ambiente que se respira en el grupo de investigación. Me siento muy afortunado de pertenecer a dicho grupo. A la formación de esta familia científica han colaborado todos sus miembros presentes y pasados.

Durante este tiempo en la facultad he dado con muchas y muy buenas personas, con las que he tenido la suerte de compartir despacho: Pedro, Carlos, Pablo, Bea, Estíbalitz, Luis, Jerónimo, Oscar, ... o comidas, cafés, conversaciones y aficiones varias: Carlos, Grego, María(s), Marco, Nacho, Raquel, Ángel, Jose, Álvaro, Luis, ... Todos ellos han añadido un poquito de alegría al trabajo diario compartiendo conmigo muy buenos momentos dentro y fuera de la facultad.

Quería agradecer a todos los miembros del departamento de Análisis Matemático de la UCM por su ayuda durante este tiempo y a los miembros del departamento de Matemática Aplicada de ETSI Industriales de la UPM por hacerme sentir como uno más desde mi llegada y prestarme todo su apoyo.

I would like to thank Prof. Barbara Kraus for her hospitality in Innsbruck and all the helpful discussions that increased my knowledge of entanglement theory. Every one in the group of Prof. Briegel made me feel at home.

I would also like to thank Prof. Serge Fehr for allowing me to enjoy and discover the secrecy of Maths for three months in Amsterdam. I had such a great time there with the people in the Cryptology group of Prof. Cramer.

I am very happy to thank my other collaborators N. Bouman, I. Cirac, B. Collins, O. Gúhne, R. Hübener, M. Kleinmann, M. Sanz, C. Schaffner, T.C. Wei and M.M. Wolf in alphabetical order.

I am also very grateful to Sofyan Iblisdir, Juanjo Garcia Ripoll and Ion Nechita for enlightening conversations and helpful comments during the realisation of this thesis.

Para mi ha sido muy grato compartir tantos y tan buenos momentos con un gran

número de profesores volcados con la docencia y el estímulo de los más jóvenes: Merche, María, Joaquín, ...

Finalmente quiero agradecerle a mi familia y amigos por su amor, comprensión y apoyo. A mis hermanos. A “el mayor” por su bondad y su preocupación permanente. A “la chica” por esa fuerza y valentía que me contagia cada vez que veo sus hoyuelos. A “el del medio” por sus largas conversaciones de pocas palabras y esos gestos que me copia antes de que yo los haga. A “el que no es nadie” o como yo lo llamo “mi hermano pequeño” que ya ocupaba “mi” habitación antes de que yo llegara, por ese gran corazón que tiene. A ti, cielo, por aguantarme con todo lo que eso conlleva, pero sobre todo por quererme incondicionalmente.

A mis padres por crear una verdadera familia, darme una infancia muy feliz y una educación excelente, cuyas figuras veo en mi en cada momento. Pocas cosas me hacen tan feliz como acordarme de ellos cuando hago algo, creo que se sentirían orgullosos.

Resumen: Entrelazamiento y simetría en sistemas cuánticos de muchos cuerpos

La Teoría de Información Cuántica se basa en la idea de que los sistemas cuánticos pueden ser usados como "transportadores" de información. Por tanto, para ser usados de este modo, se necesitan usar las leyes de la Mecánica Cuántica que describe el comportamiento de los sistemas físicos en la escala atómica. Este comportamiento incrementa las posibilidades de procesamiento de la información y tareas de comunicación conllevando a diferentes aplicaciones, tales como factorización de números en tiempo polinómico [159], mejores protocolos para comunicación o criptografía más segura [9, 10].

Además, la ley de Moore predice que el número de transistores por circuito integrado se dobla cada dos años o, equivalentemente, el tamaño de los transistores se divide por dos cada dos años. Si este ritmo de mejora continúa, el tamaño de los transistores pronto llegará a la escala atómica, en la que empezarán a aparecer efectos cuánticos no controlados. Estos efectos ya no permitirán un tratamiento clásico de la información.

Uno de los fenómenos clave de la mecánica cuántica es el *entrelazamiento*. El entrelazamiento es el tipo de correlación entre dos o más sistemas físicos que no puede ser explicada por la física clásica (no cuántica). Informalmente, es la propiedad que permite a varios sistemas cuánticos estar correlados de tal forma que realizar una operación en uno de ellos puede cambiar *instantáneamente* el estado de los otros. Además de su interés teórico en las áreas de fundamentos de la mecánica cuántica y teoría de complejidad, muchos de los resultados mas sorprendentes en información cuántica se han beneficiado del entrelazamiento de una u otra manera [84]. Por ejemplo, la acción instantánea a distancia de los pares entrelazados de Einstein, Podolski y Rosen [43] es la base del protocolo de teleportación cuántica [10]. Este protocolo hace posible comunicar la información contenida en un sistema cuántico sin transmitir o incluso sin conocer dicha información. El entrelazamiento también ha jugado un papel relevante en la propuesta y el análisis de la seguridad de protocolos de distribución de clave cuántica [44, 96, 145].

En el caso más sencillo de dos sistemas físicos aislados, el entrelazamiento está totalmente caracterizado [174]. Esta simple caracterización contrasta con la complejidad a la hora de caracterizar el entrelazamiento multipartito. De hecho, el entrelazamiento multipartito ha sido uno de los retos más desafiantes en el campo durante las últimas dos décadas.

Para poder usar los sistemas cuánticos para transportar información se necesita codificar, almacenar, procesar y extraer la información en estos sistemas. Cuanto mayor sea la información con la que se quiere trabajar, mayor será el número de sistemas que se

necesitan considerar. Por tanto, en muchas situaciones, se necesitará trabajar con muchos sistemas cuánticos, tales como los registros cuánticos de una memoria u ordenador cuántico, las partes en un protocolo multipartito, etc.

Durante los últimos 30 años se ha producido un gran avance en la captura y control de los sistemas cuánticos de muchos cuerpos, hasta el punto de que Haroche y Wineland recibieron el premio Nobel de Física 2012 por su trabajo con fotones e iones atrapados respectivamente. Aunque se ha trabajado mucho en esta dirección, todavía hay un largo camino por delante hasta que el ordenador cuántico pueda ser construido. Además, entender totalmente los sistemas cuánticos de muchos cuerpos es todavía un reto para la comunidad física. Un área entera dentro de la física, la física de matería condensada, se dedica al estudio de los estados de la materia y sus propiedades, los cuales pueden ser categorizadas en *fases*.

Las propiedades de las diferentes fases dependen del modo en el que los átomos están organizados u ordenados en los materiales. Así, diferentes simetrías en la organización de un material dan lugar a difenteres fases y, por tanto, diferentes propiedades del material. Si un material cambia de una fase a otra entonces el orden en el material cambia. A este proceso se le llama transición de fase y normalmente[1] están caracterizadas por una simetría que deja de estar presente en la nueva fase (o al revés). Este fenómeno se conoce como ruptura de simetría. Por ejemplo, los líquidos tienen una invarianza translacional continua mientras que los átomos en un cristal tienen cierta estructura y en una transición de fase de líquido a cristal la simetría continua se rompe quedando sólo un simetría discreta.

La simetría también juega un papel importante en los protocolos de criptografía cuántica. Un ejemplo paradigmático es el uso de la simetría permutacional combinada con teoremas de tipo de Finetti para dar pruebas de seguridad en criptografía cuántica [145].

En esta tesis nos centraremos en cuatro objetivos concretos asociados a cuatro problemas diferentes en información cuántica y sistemas cuánticos de muchos cuerpos donde el entrelazamiento y la simetría aparecen de una manera natural.

Sistemas cuánticos de muchos cuerpos.

Un sistema cuántico de muchos cuerpos compuesto de N subsistemas de dimensión d se modeliza matemáticamente por su vector de *estado multipartito*, un vector unitario de $(\mathbb{C}^d)^{\otimes N}$ (el n-ésimo producto tensorial de $\mathbb{C}^d$), que describe las propiedades físicas del

[1] Algunas transiciones de fase no pueden ser explicadas de este modo. En estos casos, las transiciones de fase han sido explicadas por la aparición de algún orden topológico [187]

sistema. Es decir, se puede escribir como

$$|\psi\rangle = \sum_{i_1,\ldots,i_N=1}^{d} C_{i_1,\ldots,i_N} |i_1\rangle \otimes \cdots \otimes |i_N\rangle,$$

donde $\{|i_r\rangle\}_{i=1}^{d}$ es una base ortonormal de $\mathbb{C}^d$ que puede ser distinta para los distintos subsistemas $r = 1, ..., N$ y $C_{i_1,\ldots,i_N}$ son d^N coeficientes complejos. El espacio de Hilbert subyacente crece exponencialmente con el numero de subsistemas N y por tanto también el número de coeficientes necesarios para describir el estado del sistema en una base local. Por lo tanto, sin ninguna consideración adicional, estos sistemas son de una gran complejidad. Además, si se considera una estado cogido al azar de entre todo el espacio de Hilbert, entonces, con alta probabilidad, el entrelazamiento (medido en términos de la entropía de entrelazamiento) entre los subsistemas de una región y el resto es casi máximo. Esto es, la entropía de entrelazamiento del estado de menos de la mitad de los subsistemas es casi máxima y crece en función del número de subsistemas considerados [55, 75, 139].

Afortunadamente, las interacciones físicas son (o tienden a ser) locales, es decir, los subsistemas solo interactúan con un número finito de los subsistemas más cercanos, donde la noción de cercanía viene dada por la estructura del retículo. Más específicamente, las interacciones en un sistema cuántico de muchos cuerpos están codificadas en un Hamiltoniano, donde la intuición física de que las partículas solo interactúan con aquellas que están cercanas está formalmente impuesta por una estructura local en el Hamiltoniano. La localidad de las interacciones se refleja en el hecho de que las correlaciones también son locales. Es decir, el entrelazamiento entre subsistemas de dos regiones diferentes del retículo decae con la distancia entre las regiones. Más importante, los estados fundamentales (autoestados de mínima energía) de un Hamiltoniano local con un *gap*[2] espectral[3] obedecen la llamada *ley de área* para la entropía de entrelazamiento [17, 103, 135, 160, 177, 195]. Esto es, la correlación (medida en términos de la entropía de entrelazamiento) entre una región del retículo y el resto del sistema típicamente escala con el tamaño del área de la frontera de la región, en contraste con lo que pasa en los estados aleatorios. Por tanto, el conjunto de estados relevantes es una esquina diminuta, un conjunto exponencialmente pequeño, del espacio de Hilbert total (véase Fig. 1).

De hecho, el espacio de Hilbert total es realmente grande. Si uno considera los estados de un sistema cuántico de muchos cuerpos que pueden ser alcanzados a partir de la evolución de un estado inicial en un tiempo $O(Poly(N))$ con un Hamiltoniano local, este conjunto es también una variedad exponencialmente pequeña del espacio de Hilbert.

[2]Está muy extendido el uso de la palabra *gap* para indicar la distancia entre los dos autovalores menores de un operador autoadjunto.

[3]Casi todos los Hamiltonianos locales tienen un gap espectral. Esta condición garantiza que el sistema no es crítico, lo que se puede interpretar como el hecho de que las propiedades de los estados funadamentales son estables bajo pequeñas perturbaciones de las interacciones [115]. Para Hamiltonianos sin gap puede haber correcciones multiplicativas de la ley de área, véase e.g. Ref. [191].

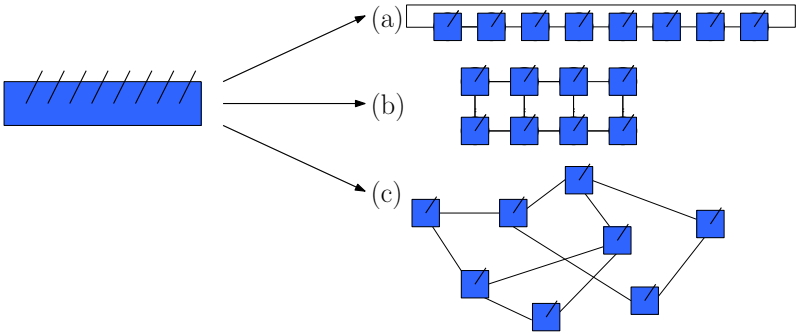

Figura 2: La descomposición del tensor C de coeficientes en términos de (a) un MPS con condiciones de frontera periódicas, (b) un PEPS con condiciones de frontera abiertas, and (c) un TNS arbitrario. Los tensores se representan por cajas, los índices se representan por líneas que salen de los tensores, los índices físicos salen fuera del papel y los índices virtuales se contraen por pares.

poniendo la misma estructura en el red de tensores. En 1D, estos estados cuánticos de muchos cuerpos son los así llamados *estados como producto de matrices* (MPS). En 2D o dimensiones mayores son los *estados como proyecciones de pares entrelazados* (PEPS) los cuales son una generalización de los MPS. Hay otros muchos conjuntos interesantes de TNS que no serán tratados aquí, como el ansatz de renormalización multi escala (MERA), que considera una red regular de tensores con una dimensión más que la red de interacciones.

Simetría en los MPS y los PEPS.

Los MPS y los PEPS heredan las buenas propiedades de los TNS como la descripción local del sistema y su entrelazamiento, o el hecho de que muchas propiedades del estado se pueden computar analíticamente. Su importancia viene del hecho de que los MPS son buenas aproximaciones de los sistemas de 1D que cumplen una ley de área [69, 157, 169] y por tanto describen eficientemente los autoestados de Hamiltonianos locales de 1D [68, 69, 70]. Además, los MPS son la clase de TNS detrás del método DMRG. Para sistemas de 2D esta buena aproximación no ha sido probada todavía. Sin embargo, existe un creciente número de resultados, ambos numéricos y analíticos, apoyando el hecho de que los estados fundamentales de los Hamiltonianos locales con gap se pueden aproximar bien por PEPS (véase, e.g., [45, 26, 27, 65, 69, 70, 170, 173, 176]).

Un MPS, como su nombre indica, es un estado cuyos coeficientes pueden ser escritos como un producto de matrices. Esto es,

$$|\psi\rangle = \sum_{i_1,\ldots,i_N} \mathrm{tr}\left[A_{i_N}\cdots A_{i_1}\right]|i_1\cdots i_N\rangle$$

donde podemos ver las matrices $\{A_{i_j}\}$ como un único tensor de tres índices, uno para cada uno de los índices de la matrices y otro para el valor de i_j. Este es el índice físico ya que representa que el sistema j está en el estado de la base $|i\rangle$. Por tanto, el estado viene definido por un único tensor local. Este tensor da lugar a un estado cuántico de tamaño cada vez mayor cuando se contrae consigo mismo en una línea (para una representación diagramática véase la Fig. 3.a).

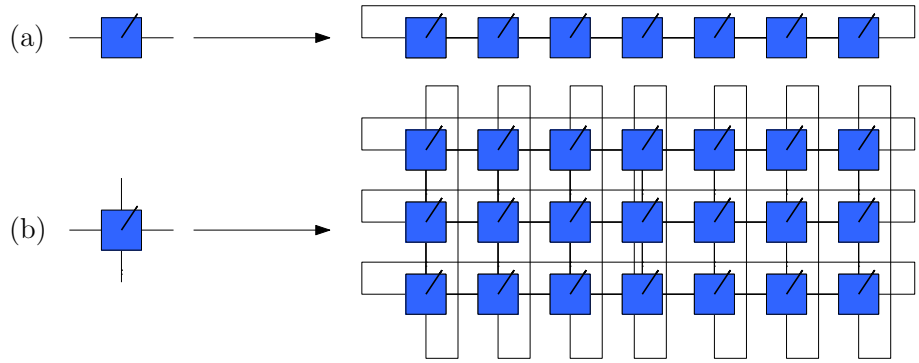

Figura 3: Tensor que genera (a) un MPS con condiciones de frontera periódicas, (b) un PEPS de 2D en un retículo rectangular con condiciones de frontera periódicas.

Una generalización inmediata a retículos regulares de dimensión mayor viene dada por los PEPS. El tensor local que define el PEPS tendrá un índice físico y un número de índices virtuales dependiendo de la dimensión y de la estructura del retículo (véase Fig. 3.b).

En el caso más general, en el que no se asume homogeneidad en el espacio, los tensores pueden depender de la posición. Sin embargo, casi siempre nos restringiremos al caso homogéneo.

Entonces parece claro que las propiedades globales del estado se deben poder caracterizar localmente, esto es, en el tensor local que define el estado. Para tener un idea intuitiva, el tensor local juega el papel del ADN del estado. Codifica toda la información. Por tanto, trabajar con los PEPS se puede entender como descodificar el genoma de los sistemas cuánticos con interacciones locales. Ahora, la 'genética', o caracterización local del genoma global del estado por supuesto es un hecho no trivial. Pero cuando uno la consigue, tiene acceso inmediato para entender el mecanismo detrás de esta propiedad.

Esto se puede ver, e.g., con el concepto de simetría global. Se ha demostrado [134] que la presencia de una simetría global en los llamados MPS inyectivos se puede caracterizar en el tensor local como en la Fig. 4. Esta caracterización de las simetrías fue el punto de partida de la caracterización completas de las fases en un sistema cuántico de 1D dada en [20, 49, 137, 155, 167].

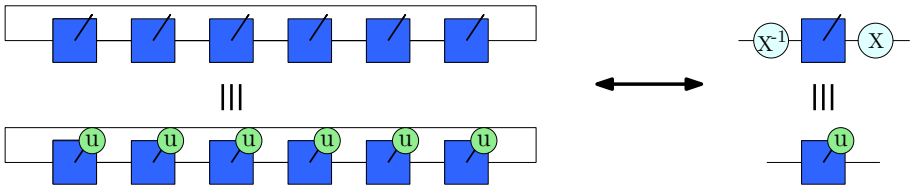

Figura 4: Caracterización de la existencia de una simetría $u^{\otimes n}$ en un MPS en función de su tensor local.

¿Qué ocurre en los sistemas de mayores dimensiones? ¿Es posible caracterizar sus simetrías en función de su tensor local? Este es el primer objetivo de la tesis.

Objetivo 1: Dar una caracterización de las simetrías globales de un PEPS en función del tensor local que lo define.

Nos ocuparemos de este problema en el Capítulo IV. En la Sección IV.4 daremos una caracterización de la existencia de simetrías espaciales y físicas globales para PEPS como un consecuencia directa de la libertad en la representación de un PEPS inyectivo (Teorema IV.3.1 en la Sección IV.3), el cual esencialmente dice que dos PEPS inyectivos que describen el mismo estado están relacionados por matrices invertibles (Fig. 5). Este hecho es una generalización de la llamada forma canónica de los MPS [131, 175]. Merece la pena destacar que nuestra demostración es por inducción en la dimensión y para ello necesitamos dar una versión mejorada del resultado en 1D (Teorema IV.2.1 de la Sección IV.2).

Esta simple caracterización ilumina las restricciones que las simetrías imponen en los sistemas cuánticos. En la Sección IV.5 damos ejemplos de las posibles aplicaciones de esta caracterización. Recuperamos una versión generalizada del teorema Lieb-Shultz-Mattis (Teorema IV.5.2). Además, podemos también entender por qué y cómo tres de los principales indicadores de orden topológico, como son la degeneración del espacio fundamental, la existencia de ciclos de Wilson y la corrección de la ley de área, están relacionados a través de la condición de inyectividad (Teorema IV.5.3).

En cuanto a la caracterización de las fases cuánticas, los mismos argumentos que en la clasificación de 1D, esto es, la caracterización de simetrías que presentamos aquí, han sido ya explotados en [155]. En él se ha comenzado una clasificación de las fases en sistemas de 2D con un único estado fundamental, espacio fundamental degenerado con un parámetro de orden local y sistemas con orden topológico. Véase también, e.g., [19].

Además, se ha probado en [134] que la existencia de simetrías en tamaños crecientes del sistema da la definición apropiada de orden de 'cadena' en 2D. La importancia del orden de 'cadena' en el estudio de las transiciones de fase cuánticas puede vaticinar interesantes aplicaciones futuras en esta dirección.

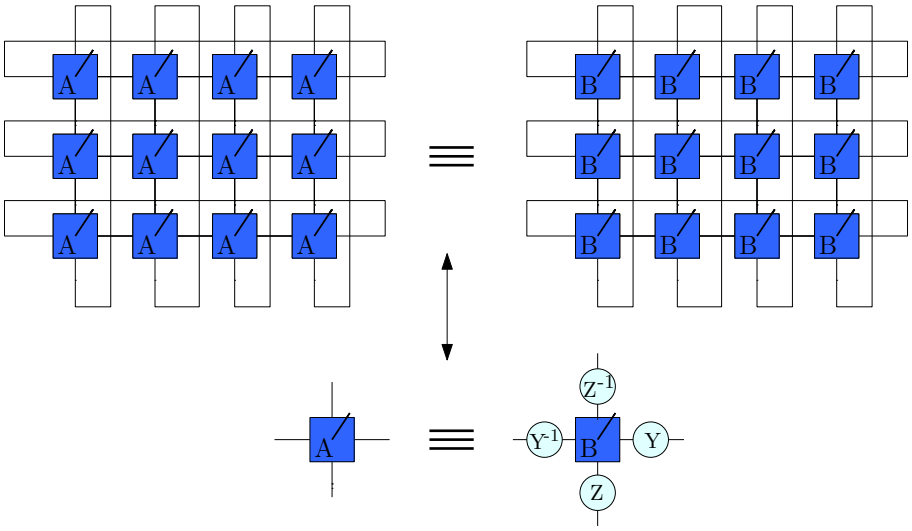

Figura 5: Esta es la libertad en la representación de los PEPS, i.e., la relación que se cumple entre dos tensores diferentes A y B que definen los PEPS cuando representan el mismo estado.

Entrelazamiento en los MPS.

En lugar de estudiar las propiedades de simetría de un estado cuántico de muchos cuerpos determinado, nos podemos preguntar cuales son las propiedades de los estados cuánticos de muchos cuerpos en el caso genérico. Ya hemos mencionado que, para casi todos los sistemas cuánticos compuestos por N subsistemas, el entrelazamiento entre un conjunto de subsistemas y el resto es casi máximo. De forma más precisa, si tomamos un estado aleatorio formado por N subsistemas (muestreado con respecto a la medida de Haar en la esfera unidad de $(\mathbb{C}^d)^{\otimes N}$) la probabilidad de que un conjunto de subsistemas dado (de menos de la mitad de los sistemas) no tenga entropía de entrelazamiento máxima es exponencialmente pequeña en N [75].

Este resultado tiene importantes consecuencias. Esencialmente dice que la matriz de densidad reducida de un conjunto de subsistemas de cualquier estado está tan cerca de del estado mixto, que son casi indistinguibles. El estado mixto es un estado clásico y por tanto se puede interpretar el resultado de la siguiente forma: para casi todos los estados cuánticos si solo tenemos acceso a menos de la mitad de los subsistemas, entonces no podemos observar ningún fenómeno cuántico en estos subsistemas. Como en la naturaleza no hay sistemas cuánticos aislados, este resultado formaliza la intuición de que usualmente no se observan fenómenos cuánticos fuera del laboratorio.

Además, el estado mixto es la mezcla uniforme de todos los posibles estados del sistema y tiene entropía máxima y por tanto también se puede interpretar el resultado como un

principio de máxima entropía. De entre todos los posibles estados compatibles con nuestra información a priori, la mejor elección es aquella que maximiza la entropía de Shannon[4]. Esto ha sido formalizado también cuando los subsistemas son parte de un sistema gobernado por un hamiltoniano concreto, en este caso el estado de densidad reducido del subsistema es indistinguible del estado termal [55, 139].

Aunque de gran interés teórico, estas dos ideas intuitivas consideran los estados de todo el espacio de Hilbert. ¿Qué ocurre en el conjunto de los estados físicamente relevantes? O más concretamente, ¿y si consideramos un sistema físico de 1D donde las interacciones son locales y homogéneas y trabajamos a temperatura cero, pero no hacemos ninguna hipótesis en las interacciones concretas del sistema? En ese caso estaríamos tratando con el conjunto de MPS homogéneos. Este es el segundo objetivo de la tesis.

Objetivo 2: Estudiar la validez del principio de máxima entropía en MPS.

Este estudio lo llevamos a cabo en el Capítulo V. Motivados por el tipo de sistemas que uno puede construir en el laboratorio, consideramos en la Sección V.1 el conjunto de MPS asociado a una cadena homogénea de sistemas y algunos efectos de frontera incontrolados que ocurren en regiones exponencialmente pequeñas de los dos extremos de la cadena, donde sólo tenemos acceso experimental a una región central exponencialmente pequeña (véase Fig. 1). El conjunto de MPS homogéneos con dimensión del vínculo D se puede (sobre)parametrizar de una manera natural por el grupo unitario $U(dD)$ en el cual el tensor local que define el MPS esta definido vía la aplicación $U \mapsto A_i = \langle i|U|0\rangle$ [131]. Por lo tanto, uno puede usar una asignación de distribución a priori basada en la simetría para muestrear con la medida de Haar y considerar la distribución de MPS aleatorios inducida por esta.

En esta configuración, probamos en la Sección V.3 que, típicamente, el estado reducido de los l subsistemas centrales tiene entropía máxima (Teorema V.0.1) y por consiguiente es esencialmente indistinguible del estado mixto. Alternativamente, se puede entender ver este resultado como que los l subsistemas están máximamente entrelazados con el resto del sistema para el escalamiento de parámetros considerado. Nótese que estos estados cumplen una ley de área si uno incrementa el número de sistemas accesibles sin incrementar la dimensión de vínculo. En un MPS, la entropía de entrelazamiento entre una región conectada y el resto esta acotada superiormente por dos veces la dimensión de vínculo [131].

La demostración del resultado se basa en el fenómeno de concentración de la medida el cual se introduce en la Sección V.2.1. También nos apoyaremos en avances recientes de la teoría de matrices aleatorias, en particular, en el cálculo gráfico de Weingarten

[4]La información a priori sería que el sistema es parte de un sistema como poco dos veces mas grande y el estado mixto es el que maximiza la entropía de Shannon.

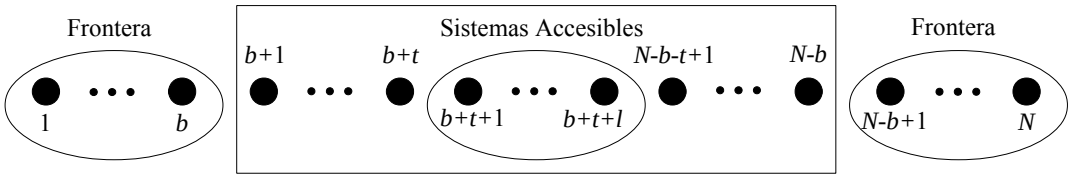

Figure 1: Consideramos una cadena de N sistemas, con interacciones homogéneas en el grueso de la cadena y efectos de frontera en regiones exponencialmente pequeñas de tamaño b en los extremos. Asumimos que la región experimentalmente accesible (y por tanto en la que estamos interesados) es un una región exponencialmente pequeña de tamaño l en el centro de la cadena.

introducido en [24] y descrito en la Sección V.2.2, y en una novedosa estimación de la función de Weingarten (Teorema V.2.10).

Nos hemos centrado en caracterizar las simetrías de un sistema cuántico de muchos cuerpos concreto y en las propiedades de entrelazamiento de pequeñas regiones de estos sistemas. Ahora, nos centraremos en el estudio del entrelazamiento en sistemas multipartitos en presencia de simetría permutacional.

Entrelazamiento y simetría en sistemas multipartitos.

El entrelazamiento se considera habitualmente como un recurso para la realización de diferentes tareas, tanto en el escenario bipartito (criptografía cuántica [44], teleportación [10], ...) como en el multipartito (algoritmos cuánticos [121], estados universales para computación cuántica [143], ...). Por lo tanto, para todas estas tareas, es fundamental entender, cuantificar y usar el entrelazamiento.

Mientras en el caso bipartito el entrelazamiento está totalmente caracterizado [174], existen muchas medidas de entrelazamiento multipartitas diferentes que se usan dependiendo de la tarea a realizar [84, 136]. Esta variedad de medidas de entrelazamiento multipartito proviene del hecho de que no existe un "estado máximamente entrelazado" en el escenario multipartito. Por lo tanto, los estados que tienen la cantidad de entrelazamiento máximo con respecto a la medida geométrica (la cual mide la distancia al conjunto de estados no entrelazados), no tienen que ser los que tengan entrelazamiento localizable máximo (el cual mide la cantidad de entrelazamiento que se puede localizar entre dos sistemas determinados haciendo operaciones locales en los otros).

Además, todas las medidas de entrelazamiento multipartitas tiene un grave inconve-

niente: son muy difíciles de computar ya que sus definiciones contienen optimizaciones sobre ciertos estados o protocolos de información cuánticos. Dichas optimizaciones sólo se pueden realizar de una manera exitosa para casos especiales, por ejemplo, si la matriz de densidad que estudiamos tiene un alta simetría o pertenece a una familia especial, e.g., con rango pequeño [108, 150, 164, 182].

La naturaleza de ciertas tareas nos puede permitir restringir el conjunto de posibles estados útiles. La invarianza permutacional de los sistemas (o partes) es una propiedad deseada en muchas situaciones. Considérese, por ejemplo, los protocolos en los que hay una autoridad A y un conjunto de N participantes que quieren ser tratados igual en el protocolo. Esta es la situación deseada en un amplia variedad de protocolos multipartitos, como compartición de secretos o votación, y nos lleva a

Suposición 1. Trabajaremos con estados de $N+1$ partes que tengan simetría permutacional con respecto a N de las partes (participantes).

Suposición 2. Por sencillez, el espacio de Hilbert de los participantes es 2, mientras que el de la autoridad es $N+1$, que es la dimensión más pequeña posible para poder purificar cualquier estado mixto de los participantes.

La simetría permutacional del estado es un recurso cuántico, sin análogo clásico, que permite asegurar que todos los participantes son tratados igualmente y son indistinguibles desde el punto de vista de la autoridad. Este tipo de requisitos están ganando mucha importancia hoy en día ya que la *privacidad* se esta convirtiendo en una importante cuestión en la nueva sociedad electrónica.

Podría perfectamente darse el caso de que cuando nos restringimos a un conjunto de estados particular, exista un estado máximamente entrelazado o que una determinada medida de entrelazamiento se pueda computar eficientemente. Por lo tanto, tiene completo sentido

Objetivo 3: Estudiar el entrelazamiento multipartito en la presencia de simetría permutacional.

En el Capítulo III, abordaremos este problema desde dos puntos de vista diferentes. Por una parte, estudiaremos la medida de entrelazamiento geométrico [185] para estados permutacionalmente simétricos en la Sección III.1. Por otra parte, estudiaremos el conjunto de estados que cumple las Suposiciones 1 y 2 en la Sección III.2.

La medida de entrelazamiento geométrica es una medida de entrelazamiento genuinamente multipartita y ampliamente usada que tiene muchas interpretaciones operacionales. Cuantifica la distinguibilidad por operaciones locales de los estados multipartitos [72], o la aditividad y la 'pureza de salida' de los canales cuánticos [188]. Ha sido usada para estudiar las transiciones de fase cuánticas en los modelos de espines [119, 124, 126, 183, 184]

y la utilidad de los estados como recursos para hacer computación cuántica basada en mediciones [14, 60]. Viene dada por $E_G(|\psi\rangle) = 1 - G(\psi)^2$, donde

$$G(\psi) = \max_{|\phi\rangle=|a\rangle|b\rangle|c\rangle\cdots} |\langle\psi|\phi\rangle|. \tag{1}$$

La pregunta que surge de manera natural es si para un estado simétrico $|\psi\rangle$ el estado producto más cercano se puede elegir simétrico, i. e., el estado que maximiza la Ec. 1 $|\phi\rangle = |a\rangle|a\rangle|a\rangle\cdots$ ya que simplifica drásticamente los cálculos. Daremos una respuesta afirmativa basada en la teoría de polinomios N-homogéneos sobre espacios de Banach (Corolario III.1.2). Sin embargo, este resultado no nos permite concluir que sólo existan soluciones simétricas. Damos una prueba alternativa para mostrar que el estado óptimo que maximiza $G(\psi)$ es *necesariamente* simétrico para estados de tres o más partes (Lemma III.1.3). También discutimos y clarificamos algunas conjeturas similares para estados traslacionalmente invariantes y operadores de densidad "simétricos".

De entre los estados que cumplen las Suposiciones 1 y 2, veremos que existe un "estado máximamente entrelazado" y un protocolo, que puede ser implementado usando solo operaciones locales y comunicación clásica, que transforma el estado máximamente entrelazado en cualquier otro estado con la misma simetría (Teorema III.2.1). Además, demostraremos como todos los pasos del protocolo, incluido la construcción del estado, se pueden realizar eficientemente y discutimos asuntos relativos a la seguridad de posibles aplicaciones en protocolos criptográficos. En la Sección III.2.1, como consecuencia sencilla recuperamos el resultado principal en [38] desde un punto de vista más general. La técnicas de la demostración son una mezcla de herramientas básicas de diferentes áreas: teoría de representaciones, análisis convexo, estados como producto de matrices y canales cuánticos.

Incertidumbre cuántica.

El principio de incertidumbre de Heisenberg [78] es, junto con el entrelazamiento, uno de los fenómenos fundamentales de la mecánica cuántica. Después de la aparición de la teoría de información clásica [158], la caracterización inicial del principio de incertidumbre en términos de la desviación estándar de observables fue enunciada como una relación de incertidumbre entrópica [7, 80, 109]. Estas no son más que caracterizaciones cuantitativas de la incertidumbre en términos de una medida de entropía. Además de contribuir al entendimiento de la mecánica cuántica, las relaciones de incertidumbre entrópicas tienen interesantes aplicaciones al 'asegurado de información con llave' [41], al problema de la separabilidad [62] y, mas importante, son un ingrediente fundamental en las prueba de seguridad de muchos protocolos criptográficos [34, 96, 98, 145, 179].

Las diferentes relaciones de incertidumbre usualmente vienen dadas en términos de las entropías de Rényi H_α [147] y sólo dan cotas inferiores en la entropía del resultado de la

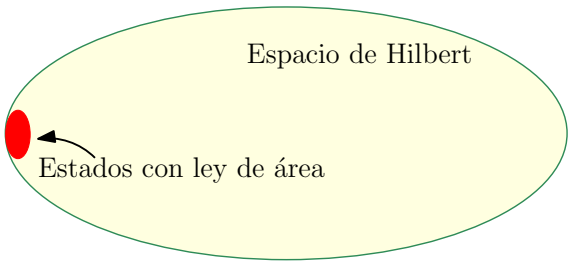

Figura 1: La esquina de los estados físicamente relevantes es exponencialmente pequeña comparada con todo el espacio de Hilbert del sistema cuántico de muchos cuerpos.

Esto quiere decir que si tenemos un sistema cuántico de muchos cuerpos inicializado en un estado (que probablemente será de la esquina de estados relevantes), entonces el conjunto de estados que se pueden alcanzar en un tiempo *razonable* es exponencialmente pequeño. Esta es la razón por la que a veces se dice que el espacio de Hilbert de un sistema cuántico de muchos cuerpos es una ilusión conveniente [141].

Para estudiar y trabajar con el conjunto de estados físicamente relevantes, uno debería encontrar una manera de describirlos. Esto es exactamente lo que hacen los estados de redes tensoriales (TNS) [125]. Los TNS han sido una herramienta muy exitosa para simular sistemas fuertemente correlados. Están detrás de muchos métodos numéricos como el famoso grupo de renormalización de matrices de densidad (DMRG) introducido por White [189, 190] para simular sistemas 1D fuertemente correlados. También han sido muy útiles para entender analíticamente y clasificar las fases cuánticas de la materia [20, 155].

Los TNS son aquellos estados cuyo tensor de coeficientes $C_{i_1,\ldots,i_N}$ está descrito por un conjunto de tensores más pequeños cuyos índices se contraen de acuerdo con alguna red de tensores interconectados. Intuitivamente, la forma en la que escribimos estos estados es describiendo el tensor general de coeficientes, el cual es un tensor de N índices de dimension d representando cada uno un subsistema físico, en términos de un conjunto de tensores locales con un número menor de índices. Estos tensores más pequeños tienen dos tipos diferentes de índices, aquellos que se identifican con los subsistemas físicos, y los nuevos índices virtuales que se contraen por parejas (véase Fig. 2). Podemos pensar en estas contracciones en la estructura de la red como las que llevan la estructura de las interacciones entre los subsistemas, esto es, como una descripción local del entrelazamiento de los sistemas. Por tanto, el entrelazamiento depende de la máxima dimensión de los sistemas virtuales (dimensión del vínculo) y la estructura de las contracciones. Por ello, para describir el estado eficientemente, uno puede elegir una estructura de red tensorial adecuada dependiendo del patrón de interacciones del sistema.

Especialmente interesantes son los TNS cuya estructura de la red es regular ya que intentan describir los estados que vienen de interacciones regulares en un retículo im-

medición X *en media* sobre una elección aleatoria de la medición. Esto es, sea ρ un estado cuántico del sistema arbitrario, denotemos por X el resultado de la medición cuando ρ se mide en una base elegida de un conjunto $\{\mathcal{B}_j\}$ y denotamos por $H_\alpha(X|J=j)$ la entropía α de Rényi del resultado de la medición cuando ρ se mide en la base $\mathcal{B}_j$ entonces las relaciones de incertidumbre suelen ser de la forma

$$\frac{1}{|J|}\sum_j H_\alpha(X|J=j) \geq h\,.$$

Una relación de incertidumbre de esta forma solo garantiza que hay incertidumbre en X para *algunas* mediciones, pero no especifica para cuantas. Las relaciones de incertidumbre mas conservadoras vienen dadas por la entropía 'min'. A dichas relaciones de incertidumbre también se les llama relaciones de incertidumbre de *orden alto*[5]. Además, la necesidad de una cota inferior de la entropía 'min' para tener amplificación de privacidad [145], hace que estas relaciones de incertidumbre sean especialmente útiles para argumentar seguridad en protocolos criptográficos. En este contexto, las relaciones de incertidumbre son usadas para acotar la información que una parte tramposa tiene sobre algún dato codificado en las posibles diferentes bases, donde la elección de la bases es desconocida por él.

Por tanto, en una relación de incertidumbre son deseables (aunque no necesarias) las siguientes propiedades:

1. Usa la *entropía 'min'* como medida de entropía (más fuerte que la entropía de Shannon).
2. Da una cota inferior de la incertidumbre del resultado de medir en *todas menos una* de las posibles mediciones (más fuerte que las relaciones de incertidumbre que acotan la incertidumbre en media sobre una elección aleatoria de la medición).
3. Se puede aplicar a conjuntos de mediciones generales. En particular, si las mediciones pueden ser tomadas como producto de mediciones sobre bits cuánticos (qubits) entonces podría ser aplicable a protocolos que se pueden implementar con la tecnología actual.

Hasta donde nosotros sabemos, ninguna relación de incertidumbre entrópica previa cumple (1) y (2) a la vez y mucho menos en combinación con (3). De hecho, como se señala en un trabajo retrospectivo reciente [180], se sabe muy poco sobre relaciones de incertidumbre entrópicas para más de dos resultados de las mediciones, e incluso menos cuando adicionalmente se considera la entropía 'min'. Las relaciones de incertidumbre previas para la entropía 'min' o no consideran muchas mediciones [34], o la cota inferior

[5] Esto es porque la entropía 'min' coincide con la entropía de Rényi H_α de mayor orden $\alpha = \infty$. En comparación, la entropía de Shannon coincide con la entropía de Rényi de orden (relativamente) bajo $\alpha = 1$.

no es para *todas menos una* de las mediciones [33, 47]. De este modo, dedicamos el Capítulo VI al

Objetivo 4: Dar una relación de incertidumbre entrópica de orden alto para todas las mediciones menos una.

Primero, en la Sección VI.1 recordamos algunos conceptos de teoría de probabilidad y resultados conocidos sobre la entropía 'min' tales como amplificación de privacidad (Teorema VI.1.8). Depués, proponemos y probamos una nueva relación de incertidumbre entrópica que cumple las tres propiedades (Teorema VI.2.4). En la demostración intervienen principalmente algebra lineal básico y argumentos bastante técnicos de teoría de probabilidad. Como aplicación de nuestra relación de incertidumbre entrópica, en la Sección VI.3, proponemos un nuevo *protocolo cuántico de identificación* que es una ligera modificación del protocolo de identificación dado por Damgård *et al.* [35]

El objetivo de la identificación por contraseña es el siguiente. Dado un usuario y un servidor que comparten una contraseña w acordada previamente, el usuario quiere convencer al servidor de que realmente conoce la contraseña w, de tal forma que revele tan poca información de w como sea posible en el caso de que se este interactuando con un servidor fraudulento.

Sin ninguna restricción en (alguno de) los participantes fraudulentos se sabe que la identificación segura es imposible (incluso en un escenario cuántico) [35, 107]. Por lo tanto, lo mejor que uno puede esperar de un protocolo que sea seguro contra un usuario fraudulento es que, para romper la seguridad, un servidor fraudulento *necesite* almacenamiento cuántico ilimitado y poder computacional cuántico ilimitado.

Nuestro protocolo de identificación tiene las siguientes propiedades de seguridad: es incondicionalmente seguro frente a un usuario fraudulento (Sección VI.4), seguro frente a un servidor fraudulento en el modelo de almacenamiento cuántico limitado (Sección VI.5), y seguro frente a un servidor fraudulento en el modelo de operaciones sobre un solo qubit, donde se asume que el adversario no puede hacer operaciones en varios qubits de forma conjunta (Sección VI.6).

El beneficio de esta última propiedad es que todavía queda algo de seguridad en el caso en que un servidor fraudulento pueda almacenar todos los qubits usados. Este servidor fraudulento además debería realizar operaciones cuánticas no triviales para romper la seguridad, en contraposición con lo que ocurre en el protocolo de identificación de Damgård *et al.* [35]

Organización y Resultados.

La tesis está organizada de la siguiente forma. El Capítulo II está dedicado a introducir las herramientas que se utilizarán en el resto de la tesis. Primero, se fija la notación de teoría de espacios de Hilbert. Posteriormente, se introduce el formalismo cuántico que abarca los postulados de la mecánica cuántica desde el punto de vista de teoría de la información y sus primeras consecuencias y algunos hechos básicos de canales cuánticos y teoría de entrelazamiento. Por último, se da una breve revisión de los estados como producto de matrices.

El resto de los capítulos tienen una estructura similar. Primero se da una introducción al problema tratado y se presentan los resultados comparándolos con trabajos anteriores. Acto seguido, si es necesario, se incluye una sección introduciendo las herramientas usadas para abordar los problemas que no sean necesarias para los otros capítulos. Añadimos tantas secciones como sean necesarias para resolver los problemas y tratar sus aplicaciones. Finalmente, en la última sección, discutimos los resultados obtenidos, posibles aplicaciones y problemas abiertos.

Los resultados del Capítulo III (Objetivo 3) han sido recogidos en los trabajos [85] and [57].

Los resultados principales del Capítulo IV (Objetivo 1) han dado lugar a la publicación [130]

Los resultados del Capítulo V (Objetivo 2) han sido recogidos en el artículo [23].

Los resultados presentados en el Capítulo VI (Objetivo 4) han dado lugar a la publicaión [11].

Index

Resumen **v**

I. Introduction **1**

I.1. Quantum Many Body Systems 2

I.2. Symmetry in MPS and PEPS 5

Objetive 1: Give a characterization of global symmetries in a PEPS 7

I.3. Entanglement in MPS 8

Objetive 2: Principle of maximum entropy in MPS 9

I.4. Entanglement and Symmetry in Multipartite Systems 10

Objetive 3: Study multipartite entanglement in the presence of permutational symmetry. 11

I.5. Quantum uncertainty 12

Objetive 4: Give an *all but one* min-entropy uncertainty relation 13

I.6. Organization and Results 14

II. Preliminaries **15**

II.1. The Quantum Formalism. 16

II.1.1. Systems and States 16

II.1.2. Quantum Transformations: Evolution and Measurement 18

II.1.3. Uncertainty 20

II.1.4. Quantum Channels 22

II.1.5. Entanglement 23

II.2. Matrix Product States 24

II.2.1. Representations 25

II.2.2. Translation invariant MPS 27

III. Multipartite Entanglement and Symmetry **31**

III.1. The geometric measure for symmetric states . . . 34

III.1.1. Physical interpretation of the proof . . . 39

III.1.2. Translationally invariant states . . . 39

III.1.3. Operators of higher rank . . . 40

III.2. Multipartite maximally entangled states in symmetric scenarios . . . 42

III.2.1. Properties of the state . . . 48

III.2.2. Checking symmetry. . . . 50

III.3. Discussion . . . 51

IV. MPS and Symmetry **53**

IV.1. Projected Entangled Pair States . . . 54

IV.2. The canonical form for MPS. . . . 56

IV.3. The canonical form for PEPSs . . . 59

IV.4. Symmetries . . . 68

IV.5. Applications . . . 71

IV.5.1. Lieb-Schultz-Mattis Theorem . . . 72

IV.5.2. Wilson loops . . . 74

IV.6. Discussion . . . 75

V. Many body systems and the principle of maximum entropy **77**

V.1. Random Matrix Product States . . . 80

V.2. Mathematical tools . . . 81

V.2.1. Concentration of Measure Phenomenon . . . 81

V.2.2. Integration over the unitary group. Weingarten function. . . . 83

V.3. Proof of Theorem V.0.1 . . . 86

V.4. Discussion . . . 94

VI. An entropic uncertainty inequality with application to quantum identification **97**

VI.1. Preliminaries . . . 101

VI.1.1. Probability Theory and Hybrid Systems 101
VI.1.2. Min-Entropy and Privacy Amplification 103
VI.2. The All-But-One Entropic Uncertainty Relation 106
VI.2.1. Constructing Good Families of Bases 112
VI.3. A New Quantum Identification Protocol 113
VI.4. (Unconditional) Server Security 116
VI.5. User Security in the Bounded-Quantum-Storage Model 117
VI.6. User Security in the Single-Qubit-Operations Model 119
VI.6.1. No Privacy Amplification 120
VI.6.2. Single-Qubit Measurements 121
VI.6.3. User Security of `Q-ID` 124
VI.6.4. Attack against `Q-ID` with Operations on Pairs of Qubits 129
VI.7. Discussion 130

Bibliography **133**

Chapter I

Introduction. Entanglement and Symmetry in Quantum Many Body Systems.

Quantum Information Theory is based on the idea that quantum systems (photons, atoms,...) can be used as information carriers. Therefore, to be used in such a way, one needs to use the laws of Quantum Mechanics that describe the behaviour of the physical systems at the atomic scale. This behaviour increases the possibilities in information processing and communication tasks leading to different applications, such as factorization of numbers in polynomial time [159], better protocols for communication or more secure cryptography [9, 10].

Moreover, Moore's law states that the number of transistors per integrated circuit doubles every two years or, equivalently, that the size of transistors divides by two every two years. Continuing this improvement will soon lead the size of transistors to an atomic scale, where uncontrolled quantum effects will occur. These effects will no longer make a classical treatment of information possible.

One of the key phenomena of quantum mechanics is *entanglement*. Entanglement is the kind of correlation between two or more physical systems that can not be explained by classical (non-quantum) physics. Informally, it is the property that allows several quantum systems to be correlated in such a way that performing some operation in one of them can *instantaneously* change the state of the others. Besides its theoretical interest in the areas of foundations of quantum mechanics and complexity theory, many of the most striking results in quantum information have benefit from entanglement in one way or another [84]. For example, Einstein Podolski and Rosen instantaneous action at a distance of entangled pairs [43] is the base of the Quantum Teleportation protocol [10]. This protocol makes it possible to communicate the information in a quantum system without sending or even knowing the information itself. Entanglement has also been present in the proposal and security analysis of quantum key distribution [44, 96, 145].

In the simplest case, two isolated physical systems, the entanglement is fully characterized [174]. This simple characterization contrasts with the complexity in characterizing multipartite entanglement. In fact, multipartite entanglement has been one of the most challenging issues in the field during the last two decades.

In order to use quantum systems to carry information one needs to encode, store, process and extract the information in these systems. The more information one wants to

work with the more systems one needs to consider. Thus, in many cases, one will need to work with many quantum systems, such as quantum registers of a quantum computer or a quantum memory, parties in multipartite protocols, etc.

During the last 30 years a great progress has been made in capturing and controlling quantum many body systems, up to the point that Haroche and Wineland were awarded the Nobel Prize in Physics 2012 for their work with trapped photons and ions respectively. Although a lot of work has been made in this direction, there is still a long way to go until a quantum computer can be constructed. Moreover, the fully understanding of quantum many body systems is still a challenge for the physics community. There is a whole branch of physics, condensed matter physics, dedicated to the study of the states of matter and their properties which can be categorized in *phases*.

The properties of the different phases depend on the way in which the atoms are organized or ordered in the materials. Thus, different symmetries in the organization of the atoms in a material gives different phases and, therefore, different properties of the material. If a material changes from one phase to another then the order in the material changes. This process is called phase transition and it is usually[1] characterized by a symmetry that is no longer present in the new phase (or the other way round). This phenomenon is known as symmetry breaking. As an example, liquids have continuous translational invariance whereas in a crystal the atoms obey some structure and in the phase transition from liquid to crystal the continuous symmetry is broken remaining only a discrete translational invariance.

Symmetry also plays an important role in quantum cryptographic protocols. A paradigmatic example is the use of permutational symmetry combined with de Finetti type theorems to give security proofs in quantum cryptography[145].

In this thesis we will focus on four concrete objetives associated to four different problems in quantum information theory and quantum many body systems where entanglement and symmetry appear in a natural way.

I.1 Quantum Many Body Systems

A quantum many body system composed of N subsystems of dimension d is modelled mathematically by its *multipartite state* vector, a unit vector of $(\mathbb{C}^d)^{\otimes N}$ (the N-fold tensor product of $\mathbb{C}^d$), that describes the physical properties of the system. That is, it can be written as

$$|\psi\rangle = \sum_{i_1,\ldots,i_N=1}^{d} C_{i_1,\ldots,i_N} |i_1\rangle \otimes \cdots \otimes |i_N\rangle,$$

[1] Some phase transitions cannot be explained in this way. In these cases, phase transitions have been explained by the emergence of some topological order [187]

where $\{|i_r\rangle\}_{i=1}^{d}$ is an orthonormal basis of $\mathbb{C}^d$ which can be different for different subsystems $r = 1, ..., N$ and $C_{i_1,...,i_N}$ are d^N complex coefficients. The underlying Hilbert space grows exponentially with the number of subsystems N and so does the number of coefficients needed to describe the state of the system in a local basis. Thus, without any further consideration, these systems are of a great complexity. Moreover, consider a state picked at random from the whole Hilbert space, then, with high probability, the entanglement (measured in terms of the entanglement entropy) between the subsystems of a region and the rest is almost maximal. That is, the entanglement entropy of the state of less than half of the subsystems is almost maximal and grows with the number of subsystems considered [55, 75, 139].

Fourtunately, physical interactions are (or tend to be) local, that is, subsystems only interact with a finite number of closer ones, where the notion of closeness is given by some lattice structure. More specifically, interactions in a quantum many body system are encoded in a Hamiltonian, where the physical intuition that particles can only interact with those that are closeby is formally imposed as a local structure in the Hamiltonian. Locality of interactions reflects on the fact that correlations are also local. That is, the entanglement between subsystems of two different regions of the lattice decays with the distance between those regions. More importantly, low energy eigenstates of local Hamiltonians with an spectral gap[2] obey the so called area law for the entanglement entropy [17, 103, 135, 160, 177, 195]. That is, the correlation (measured in terms of the entanglement entropy) between a region of the lattice and the rest of the system typically scales with the size of the boundary area of the region, in contrast to random states. Thus, this set of relevant states is a tiny corner, an exponentially small subset, of the total Hilbert space (see Fig. I.1).

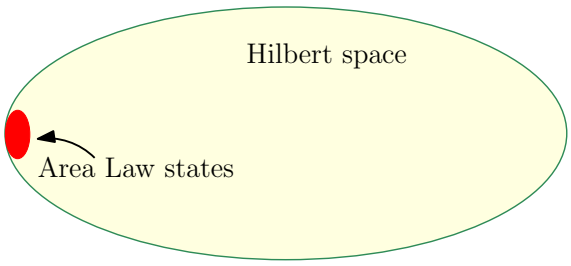

Figure I.1: The corner of physically relevant states is exponentially small compared to the whole Hilbert space of a quantum many body system.

In fact, the total Hilbert space is really big. If one considers the states of a quantum many body system that can be reached evolving an initial state a time $O(Poly(N))$ with

[2] Almost all local Hamiltonians have an spectral gap. This condition guarantees that the system is not critical, which one can interpret as the fact that the properties of the lowest energy eigenstates are stable under small perturbations of the interactions [115]. For gapless Hamiltonians there may be multiplicative corrections to the area law, see e.g. Ref. [191]

a local Hamiltonian, this set is also an exponentially small manifold of the Hilbert space. This means that if we have a quantum many body system initialised in a state (that will probably be in the corner of relevant states), then the set of states that are reachable in a *reasonable* time is exponentially small. This is the reason why the Hilbert space of a quantum many body system is sometimes referred to as a convenient illusion [141].

In order to study and work with this set of physical relevant states, one should find a way to describe them. This is exactly what Tensor Network States (TNS) do [125]. TNS have been a very successful tool to simulate strongly correlated systems. They are behind many numerical methods such as the so famous Density Matrix Renormalization Group (DMRG) introduced by White [189, 190] to simulate 1D strongly correlated systems. They have also been useful to analytically understand and classify quantum phases of matter [20, 155].

TNS are those states whose tensor of coefficients $C_{i_1,\ldots,i_N}$ is described by a set of smaller tensors whose indices are contracted according to some network of interconnected tensors. Intuitively, the way we write such states is by describing the general tensor of coefficients, which is a tensor of N indices of dimension d each one representing a physical subsystem, in terms of a set of local tensors with a lower number of indices. These smaller tensors have two different types of indices, those that are identified with the physical subsystems, and new virtual indices that are contracted in pairs (see Fig. I.2). One can think of these contractions in the network structure as the ones that carry the structure of the interactions between the subsystems, that is, as a local description of the entanglement of the system. Thus, the entanglement depends on both the maximum dimension of the virtual indices (bond dimension) and the structure of its contractions. Therefore, in order to describe the state efficiently, one could choose a suitable TN structure depending on the interaction pattern of the system.

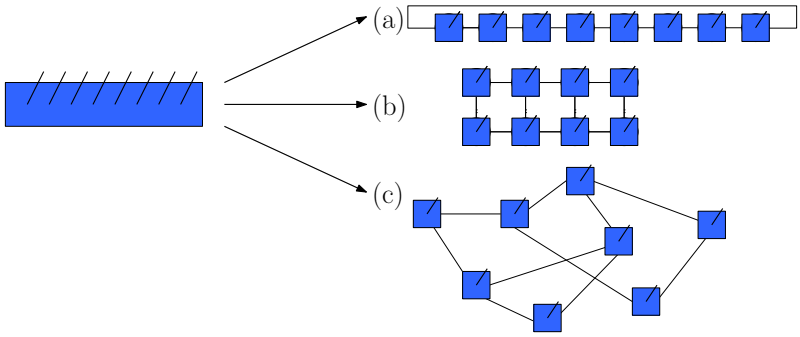

Figure I.2: Decomposition of coefficient tensor C in terms of (a) an MPS with periodic boundary conditions, (b) a PEPS with open boundary condition, and (c) an arbitrary tensor network. Tensors are represented by boxes, indices are represented by lines out of a tensor, physical indices go out of the paper and virtual indices are contracted in pairs.

TNS whose structure is a regular lattice are of special interest as they try to describe the states arising from regular interactions in a lattice imposing the same structure in the tensor lattice. In 1D, these quantum many body systems are the so called Matrix Product States (MPS). In 2D or higher dimensions these are the Projected Entangled Pair States (PEPS) which are a generalization of the MPSs. There are many other interesting sets of TNS that will not be treated here, such as the multi-scale entanglement renormalization ansatz (MERA), that considers a regular network of tensors with one dimension more than the network of interactions.

I.2 Symmetry in MPS and PEPS

MPS and PEPS inherit the nice properties of TNS such as the local description of the system and its entanglement, or the fact that many properties of the state can be computed analytically. Their importance comes from the fact that MPS are good approximations of 1D systems fulfilling an area law [69, 157, 169] and thus they describe low energy eigenstates of 1D local Hamiltonians efficiently [68, 69, 70]. Moreover, MPS is the class of TNS that is behind the DMRG method. For 2D system such a good approximation has not been proven. Nevertheless, there exists an increasing number of results, both numerical and analytical, supporting the fact that ground states of gapped local Hamiltonians are well approximated by PEPS (see for instance [45, 26, 27, 65, 69, 70, 170, 173, 176]).

A MPS, as its name says, is a state whose coefficients can be written as a product of matrices. That is,

$$|\psi\rangle = \sum_{i_1,\ldots,i_N} \operatorname{tr}\left[A_{i_N}\cdots A_{i_1}\right]|i_1\cdots i_N\rangle$$

where we can see the matrices $\{A_{i_j}\}$ as a single tensor of three indices, one for each of the matrices indices and another for the value of i_j. This one is the physical index as it represents the system j to be in the basis state $|i\rangle$. Thus, the state is defined by a single tensor. This tensor gives rise to a quantum state on larger and larger sizes by contracting it through a line (see Fig. I.3.a for a diagrammatic representation).

A straightforward generalization to regular lattices of higher dimension of this tensor structure gives a PEPS. The single tensor that defines the PEPS will have one physical index and a number of virtual indices depending on the dimension and the structure of the lattice (see Fig. I.3.b).

In the most general case, in which one does not assume homogeneity in space, the tensors may depend on the position, but we will almost always restrict to the homogeneous case.

It appears then clearly that all global properties of the state must be possible to characterize locally, that is, in the single tensor defining the state. To have an intuitive

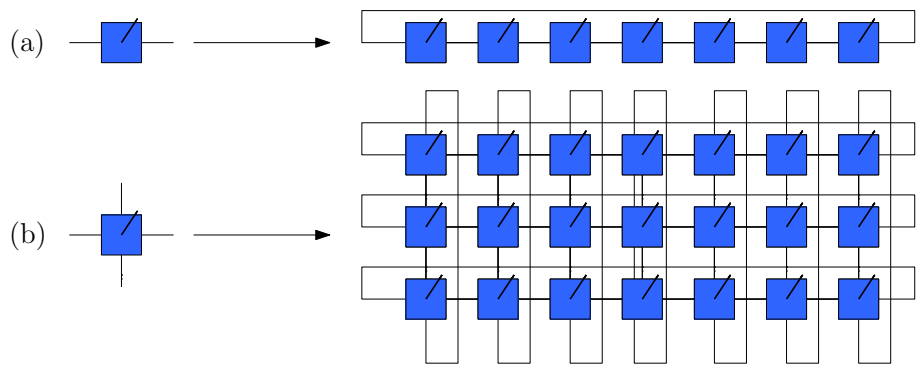

Figure I.3: Single tensor that generates (a) an MPS with periodic boundary conditions, (b) a 2D PEPS with periodic boundary conditions.

view, the single tensor plays the role of the DNA of the state. It encodes all the information. Therefore, working with PEPS can be understood as decoding the genome of locally interacting quantum systems. Now, the 'genetic', or local characterization of the global genome of a state is of course a non trivial fact. But whenever one gets it, one has immediate access to understanding the mechanisms behind this property.

This can be exemplified with the concept of a global symmetry. It has been shown [134] that the presence of a global symmetry in a so called injective MPS can be characterized locally in the single tensor as in Fig. I.4. This characterization of symmetries was the starting point to the full characterization of phases in 1D quantum systems given in [20, 49, 137, 155, 167].

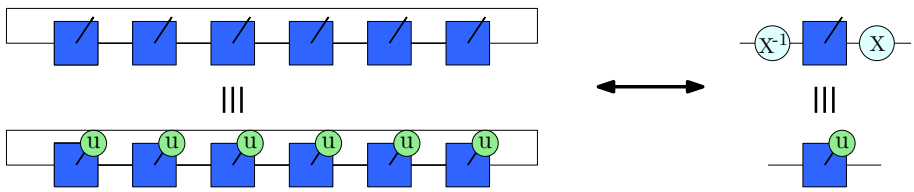

Figure I.4: Characterization of the existence of a $u^{\otimes n}$-symmetry in a MPS in terms of its local tensor.

What about higher dimensional systems? Is it possible to characterize their symmetries in terms of the local tensor? This is the first objetive of this thesis.

Objetive 1: Give a characterization of the global symmetries in a PEPS in terms of the local tensor defining the PEPS.

We will deal with this problem in Chapter IV. In Section IV.4 we give a characterization of the existence of global physical and spatial symmetries for PEPS as an straightforward consequence of the freedom in the representation of an 'injective' PEPS (Theorem IV.3.1 in Section IV.3), which essentially says that two injective PEPSs describing the same state in a lattice are related by invertible matrices (Fig. I.5). This is a generalization of the so called canonical form of MPS [131, 175]. It is worth noting that our proof is by induction on the dimension and for that we need to give an improve version of the 1D result (Theorem IV.2.1 in Section IV.2).

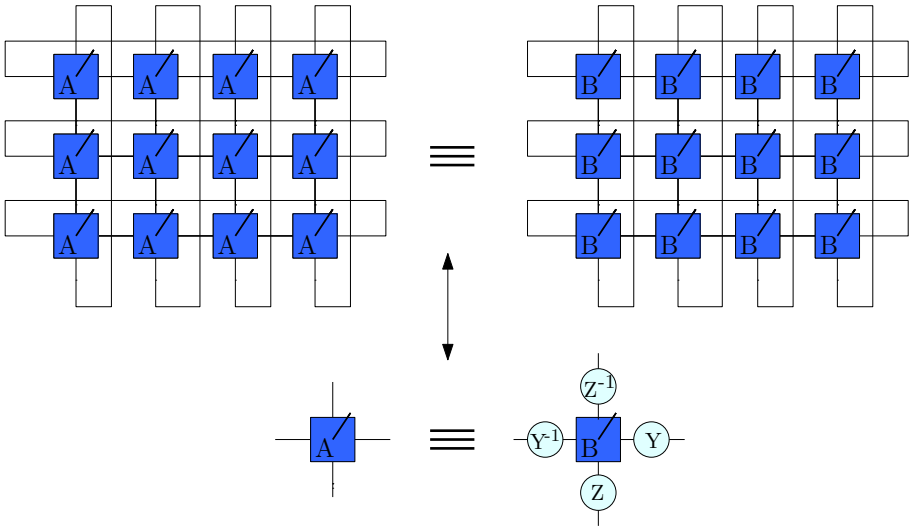

Figure I.5: This is the freedom in the representation of PEPSs, i.e., the relation that holds between two different tensors A and B which define the PEPSs when they represent the same state.

This simple characterization illuminates the restrictions that symmetries impose on quantum systems. In Section IV.5 we give examples of possible applications of this characterization. We recover a generalized version of the Lieb-Shultz-Mattis theorem (Theorem IV.5.2). Moreover, we can also understand why and how three of the main indicators of topological order, namely degeneracy of the ground state, existence of Wilson loops and correction to the area law, are related through the injectivity condition (Theorem IV.5.3).

Regarding the characterization of quantum phases, the same arguments as in the classification in 1D, that is, the characterization of symmetries that we present here, have already been exploited in [155]. There, a classification for 2D phases in systems with

unique ground state, degenerate ground state with a local order parameter, and systems with topological order has been started. See also, e.g.,[19].

Moreover, it has been proven in [134] that the existence of symmetries in increasing sizes of the system gives the appropriate definition of string order in 2D. The importance of string orders in the study of quantum phase transitions may vaticinate interesting applications in the future along this direction.

I.3 Entanglement in MPS

Instead of looking at the symmetry properties of a particular many body quantum state, one can also wonder which are the properties of many body quantum states in the generic case. We have already mentioned that, for almost every quantum system composed of N subsystems, the entanglement between a set of subsystems and the rest is almost maximal. More precisely, if we take a random N-partite state (with respect to the Haar measure in the unit sphere of $(\mathbb{C}^d)^{\otimes N}$) the probability that a given set of subsystems (of less than half of the systems) has not maximal entanglement entropy is exponentially small in N [75].

This result has strong consequences. It essentially says that the reduced density matrix of a set of subsystems of any state is so close to the mixed state, that they are almost indistinguishable. The mixed state is a classical state and thus one can physically interpret the result in the following way: for almost all multipartite state if we have access only to less than half of the subsystems, then we cannot observe any quantum phenomenon in these subsystems. As there is not isolated quantum systems in nature, this result formalizes the intuition that no quantum effects are usually observed outside the lab.

Moreover, the mixed state is the uniform mixture of all possible states of the system and has maximum entropy and thus one can also interpret the result as a principle of maximum entropy. Among all possible states compatible with our prior information, the best choice is the one which maximizes the Shannon entropy[3]. This was also formalized in the case that the subsystems are part of a system governed by a particular hamiltonian, in which the reduced density state of the subsystem is indistinguishable to the thermal state [55, 139].

Although of great theoretical interest, this two intuitive ideas consider the states of the whole Hilbert space. What happens to the set of physical relevant states? Or more concrete, what if we consider a physical 1D system where the interactions are local and homogeneous and we work at zero temperature, but we do not make any assumption on

[3]The prior information would be that the system is part of a system at least twice as big and the mixed state is the one that maximizes the Shannon entropy.

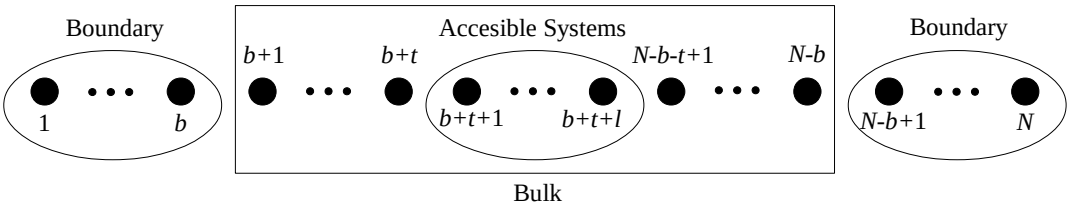

Figure I.6: We consider a chain of N sites, with homogeneous interactions in the bulk and boundary effects in exponentially small regions of size b at the borders. We assume that the experimentally accesible region (and hence the region we are interested in) is an exponentially small region of size l in the center of the chain.

the particular interactions in the system itself? In that case we would be dealing with the set of homogeneous MPS. This is objetive 2 of this thesis.

Objetive 2: Study the validity of the principle of maximum entropy in MPS.

We do so in Chapter V. Motivated by the kind of systems that one can construct in the lab, we consider in Section V.1 the set of MPS associated to a homogeneous chain of systems and some uncontrolled boundary effects in exponentially small regions at both ends of the chain, where we only have experimental access to an exponentially small central region (see Fig. I.6). The set of homogeneous MPS with bond dimension D has a natural (over)parametrization by the unitary group $U(dD)$ in which the local tensor defining MPS is given via the map $U \mapsto A_i = \langle i|U|0\rangle$ [131]. Thus, one can use a symmetry-based assignment of prior distributions to sample from the Haar measure and consider the distribution of random MPS given from it.

In this set up, we prove in Section V.3 that, typically, the reduced state of the l centered subsystems has maximum entropy (Theorem V.0.1) and therefore it is essentially indistinguishable from the mixed state. Alternatively, one can understand this result as the l subsystems being maximally entangled with the rest of the system for the given scaling of parameters. Note that these states fulfil an area law if one increases the number of accesible systems without increasing the bond dimension. In a 1D MPS, the entanglement entropy between a connected region and the rest is upper bounded by twice the bond dimension [131].

The proof of the result is based on the concentration of measure phenomenon which is introduced in Section V.2.1. We will also rely on recent developments of random matrix theory, in particular, on the graphical Weingarten calculus provided in [24] and described in Section V.2.2, and on a novel estimate of the Weingarten function (Theorem V.2.10).

We have already focused in characterizing the symmetries of a particular homogeneous quantum many body system and in the entanglement properties of small regions of these systems. Now, we focus in studying the entanglement properties of multipartite systems in the presence of permutational symmetry.

I.4 Entanglement and Symmetry in Multipartite Systems

Entanglement is usually seen as a resource for the realization of different tasks, both in the bipartite scenario (quantum cryptography [44], teleportation [10], ...) and in the multipartite one (quantum algorithms [121], universal states for quantum computation [143], ...). Thus, for all these tasks the understanding, quantification and use of entanglement is crucial.

Whereas in the pure bipartite case entanglement is fully characterised [174], there are many different inequivalent multipartite entanglement measures that are used depending on the task to be done [84, 136]. This variety of multipartite entanglement measures comes from the fact that there is not a "maximally entangled state" in the multipartite setting. Thus, for instance the states that have the maximum amount of entaglement with respect to the geometric measure, (which measures the distance to the set of non entangled states), do not have to be the ones with the maximal localizable entanglement (which measures the amount of entanglement that can be localized between two particular systems by applying local operations in the others).

Moreover, all multipartite entanglement measures suffer a serious drawback: they are very difficult to compute as their definitions contain optimizations over certain states or quantum information protocols. Such optimizations can be performed successfully for special cases only, for instance, if the density matrix under investigation possesses a high symmetry or belongs to a special family, e.g., with low rank [108, 150, 164, 182].

The nature of certain tasks may allow us to restrict the set of possible useful states. The permutational invariance of the parties is a desired property in many situations. Consider, for example, protocols in which there is an authority A, and a set of N participants which want to have the same treatment in the protocol. This is the desired situation in a wide variety of multipartite protocols, like secret sharing or voting, and leads to

Assumption 1. We will work with $(N+1)$-partite states which are permutational-symmetric with respect to N of the parties (participants).

Assumption 2. For simplicity, the Hilbert space dimension of the participants is 2, while that of the authority is $N+1$, which is the smallest possible dimension to purify any mixed state among the participants.

The permutational symmetry of the state is the quantum resource, with no classical analogue, which ensures that all participants are treated equally and are indistinguishable

from the authority's point of view. These kinds of requirements are gaining importance nowadays as *privacy* is becoming a serious issue in the new e-society.

It could well be that whenever we restrict to a particular set of states, there exists a maximally entangled state or that a particular multipartite entanglement measure could be computed efficiently. Thus, it has full sense to

Objetive 3: Study multipartite entanglement in the presence of permutational symmetry.

In Chapter III, we will tackle this problem from two different points of view. On the one hand, we will study the geometric measure of entanglement [185] for permutational symmetric states in Section III.1. On the other hand, we will study the set of states that fulfils Assumptions 1 and 2 in Section III.2.

The geometric measure of entanglement is a genuine multipartite and widely used entanglement measure that has many operational interpretations. It quantifies the distinguishability of multipartite states by local means [72], or the additivity and output purity of quantum channels [188]. It has also been used to study quantum phase transitions in spin models [119, 124, 126, 183, 184] and the usefulness of states as resources for measurement based quantum computation [14, 60]. It is given by $E_G(|\psi\rangle) = 1 - G(\psi)^2$, where

$$G(\psi) = \max_{|\phi\rangle = |a\rangle|b\rangle|c\rangle\cdots} |\langle\psi|\phi\rangle|. \tag{I.1}$$

The natural question that arises is whether for a symmetric state $|\psi\rangle$ the closest product state can be chosen symmetric, i.e., the state maximizing Eq. I.1 can be taken of the form $|\phi\rangle = |a\rangle|a\rangle|a\rangle\cdots$, as it drastically simplifies the calculation. We will give an affirmative answer based on the theory of N-homogeneous polynomials over Banach spaces (Corollary III.1.2). However, this result does not allow us to conclude that only symmetric solutions exist. We give an alternative proof to show that the optimal state maximizing $G(\psi)$ is *necessarily* symmetric for three or more parties (Lemma III.1.3). We also discuss and clarify some similar conjectures for translational invariant states and "symmetric" density operators.

Within the set of states fulfilling assumptions 1 and 2, we will show that there is a "maximally entangled state" and a protocol, that can be implemented only with Local Operations and Classical Communication (LOCC), which transforms the "maximally entangled state" into any other state with the same symmetry (Theorem III.2.1). In addition, we will show how all the elements of the protocol, including the construction of the state, can be performed efficiently and discuss some security issues concerning possible applications to cryptographic protocols. In Section III.2.1, as an easy consequence we recover the main result in [38] from a more general point of view. The proof techniques

are a mixture of basic tools from several areas: representation theory, convex analysis, matrix product states, and quantum channels.

I.5 Quantum uncertainty

Heisenberg's Uncertainty Principle [78] is, together with entanglement, one of the fundamental phenomena in quantum mechanics. After the emerging of information theory [158], the initial characterization of the uncertainty principle in terms of the standard deviation of observables was restated as an entropic uncertainty relation [7, 80, 109]. These are just quantitative characterizations of uncertainty in terms of an entropy measure. Besides contributing to the understanding of quantum mechanics, entropic uncertainty relations have interesting applications to information locking [41], the question of separability [62] and, more importantly, they are a key ingredient in the security proof of many cryptographic protocols [34, 96, 98, 145, 179].

The different uncertainty relations are usually given in terms of one of the Rényi entropies H_α [147] and they only give a lower bound on the entropy of the measurement outcome X *on average* over the random choice of the measurement. That is, let ρ be an arbitrary quantum state of the system, and let X denote the measurement outcome when ρ is measured in one of a possible set of bases $\{\mathcal{B}_j\}$ and $H_\alpha(X|J=j)$ denotes the α-Rényi entropy of the measurement outcome when ρ is measured in basis $\mathcal{B}_j$ then uncertainty relations usually are of the form

$$\frac{1}{|J|}\sum_j H_\alpha(X|J=j) \geq h\,.$$

An uncertainty relation of this form only guarantees that there is uncertainty in X for *some* measurements, but does not specify precisely for how many. The most conservative uncertainty relations in this form are given by the min-entropy. In addition, the need of a lower bound in the min-entropy por privacy amplification [145], makes these uncertainty relations specially useful for arguing security in cryptographic protocolos. In this context, uncertainty relations are used to bound the information that a cheating party has about some data encoded into several possible bases, where the choice of basis is initially unknown to him.

Thus, the following, although not necessary, are desirable properties for an uncertainty relation:

1. *Min-entropy* is used as entropy measure (stronger than Shannon entropy).
2. It lower bounds the uncertainty in the measurement outcome for *all but one* measurements (stronger than uncertainty relations that lower bound the uncertainty *on average* over the choice of the measurement).

3. It applies to general sets of measurements. In particular, if the measurements can be chosen to be qubit-wise measurements then it could be applicable to protocols that can be implemented using today's technology.

To the best of our knowledge no previous uncertainty relation fulfils (1) and (2) at the same time. Moreover, as pointed out in a recent overview article [180], little is known about entropic uncertainty relations for more than two measurement outcomes, and even less when additionally considering min-entropy. Previous uncertainty relations for the min-entropy or do not consider many measurements [34], or the lower bound is not for *all but one* measurements [33, 47]. Thus, we dedicate Chapter VI to

Objetive 4: Give an 'all but one' high order entropic uncertainty relation

First, in Section VI.1 we recall some concepts of probability theory and known results involving the min-entropy such as privacy amplification (Theorem VI.1.8). We then propose and prove a new entropic uncertainty relation satisfying the three properties in Section VI.2. The proof mainly involves basic linear algebra and quite technical arguments from probability theory. As an application of our entropic uncertainty relation, in Section VI.3, we propose a new *quantum identification protocol* that is an slight modification of the identification protocol by Damgård *et al.* [35]

The goal of password-based identification is as follows. Given a user and a server that hold a pre-agreed password w, the user wants to convince the server that he indeed knows w, in such a way that he gives away as little information on w as possible in case he is actually interacting with a dishonest server.

It is known that *without* any restriction on (one of) the dishonest participants, secure identification is impossible (even in the quantum setting) [35, 107]. Thus, the best one can hope for a protocol that is secure against a dishonest user is that, in order to break it, unbounded quantum storage *and* unbounded quantum-computing power is *necessary* for the dishonest server.

We prove that our identification protocol has the following security properties: it is unconditionally secure against a dishonest user (Section VI.4), secure against a dishonest server in the bounded quantum storage model (Section VI.5), and secure against a dishonest server in the single qubit operations model (SQOM), where it is assumed that the adversary cannot operate on multiple qubits coherently (Section VI.6).

The benefit of the latter property is that there is still some security left in case a dishonest server is able to store all qubits used in the protocol: this dishonest server must in addition perform a non-trivial quantum operation to break the scheme, in contrast to what happens in the identification protocol by Damgård *et al.* [35]

I.6 Organization and Results

The rest of the thesis is organized as follows. Chapter II is dedicated to introduce the tools that will be used in the rest of the thesis. We first fix the notation of Hilbert space theory. Afterwards, we introduce the quantum formalism that covers the postulates of quantum mechanics from the point of view of information theory and its very first consequences and some basic facts about quantum channels and entanglement theory. We finally give a short review of matrix product states.

The rest of the chapters follow a similar structure. We first give an introduction to the problem we are working on and present the results comparing them with previous work. Then, if needed, we add a section including the tools used to attack the problems that are not necessary for the other chapters. We add as many sections as necessary to solve the problems and give their applications. Finally, in the last section, we discus the results obtained, comment on further applications and open problems.

The results of Chapter III (Objective I.4) have been collected in the works [85] and [57].

The main results in Chapter IV (Objective I.2) have given rise to the publication [130].

The results in Chapter V (Objective I.3) have been collected in the article [23].

The results presented in Chapter VI (Objective I.5) have given rise to the publication [11].

Chapter II

Preliminaries

In this chapter we give a short description of the basic ingredients that will be used in the rest of this thesis. First, we fix the notation. Then, in Section II.1 we present a short introduction to the mathematical formalism of quantum mechanics. Finally, we give a description of the basic facts of matrix product states that will be used later on (Section II.2).

Throughout this thesis we will be working with complex separable Hilbert spaces, we assume the reader is familiar with the basic knowledge and we just introduce the notation and terminology we are going to use.

- $\langle\varphi|$ is the dual vector of $|\varphi\rangle$ (conjugate transposed). Also known as bra.
- $\langle\varphi|\psi\rangle$ is the scalar product between $|\varphi\rangle$ and $|\psi\rangle$.
- $|\varphi\rangle|\psi\rangle$ or $|\varphi\rangle \otimes |\psi\rangle$ is the tensor product of $|\varphi\rangle$ and $|\psi\rangle$.
- $A^\dagger$ is the conjugate transposed or adjoint operator of A.
- $\langle\varphi|A|\psi\rangle$ is the scalar product between $|\varphi\rangle$ and $A|\psi\rangle$ or, equivalently, the scalar product between $A^\dagger|\varphi\rangle$ and $|\psi\rangle$.
- $|\varphi\rangle\langle\psi|$ is the outer product between $|\varphi\rangle$ and $|\psi\rangle$.

Given a pair of Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ we will denote as $\mathcal{B}(\mathcal{H}_1, \mathcal{H}_2)$ the set of bounded linear operators from $\mathcal{H}_1$ to $\mathcal{H}_2$. We will write $\mathcal{B}(\mathcal{H}) := \mathcal{B}(\mathcal{H}, \mathcal{H})$.

Let $\rho \in \mathcal{B}(\mathcal{H})$ and $p \in [1, \infty)$, we denote as $\|\rho\|_p := \sqrt[p]{\sum_i \sigma_i^p}$ the **Schatten p-norm** of ρ, where σ_i are the singular values of ρ. Thus $\|\rho\|_1 = \operatorname{tr}\sqrt{\rho^\dagger\rho}$ is the trace norm of ρ, $\|\cdot\|_2$ is the Hilbert-Schmidt norm and $\|\rho\|_\infty := \max \sigma_i$ is the operator norm. The **trace distance** between two operators $\rho, \sigma \in \mathcal{B}(\mathcal{H})$ is given by $\Delta(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1$.

Definition II.0.1. *A density operator (or density matrix) $\rho \in \mathcal{B}(\mathcal{H})$ is a nonnegative self adjoint operator with unit trace, that is, $\rho \geq 0$ and $\operatorname{tr}\rho = 1$. A density operator ρ of rank one is called pure state. Otherwise, we say that ρ is a mixed state. We denote by $D_1(\mathcal{H})$ the set of density operators of a Hilbert space $\mathcal{H}$.*

The condition $\operatorname{tr}\rho = 1$ is known as the normalization condition. We will identify a positive operator with an unnormalized density operator. For pure states we can write $\rho = |\varphi\rangle\langle\varphi|$ where the normalization translates in $|\varphi\rangle$ being a unit vector of $\mathcal{H}$. In this case we will identify ρ and $|\varphi\rangle$ and we will refer to both representations as pure states. The vector $|\varphi\rangle$ is unique up to multiplication by a phase (a complex number of modulus one) $e^{i\theta}$. Thus, any two pure states that differs in a phase have the same density matrix and hence represent the same state vector. Equality of vectors representing pure states should be understood in this sense. Nevertheless, whenever we want to highlight this fact, we will write $|\varphi\rangle \equiv |\psi\rangle$ if $|\varphi\rangle$ and $|\psi\rangle$ represent the same state. That is, they differ in a phase or, if they are not normalized, they are equal up to a complex number.

Mixed states can also be diagonalised $\rho = \sum_i p_i|\varphi_i\rangle\langle\varphi_i|$, where $\sum_i p_i = 1$ and $|\varphi_i\rangle$ is a unit vector of $\mathcal{H}$ for all i. In this case, one usually refer to ρ as an (statistical) *ensemble* of pure states $\{p_i, |\varphi_i\rangle\}$[1].

Positive maps between operators of Hilbert spaces take positive operators to positive operators. Moreover, a map $T : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H}')$ is **completely positive** if the map $T \otimes \mathbb{1}_n : \mathcal{B}(\mathcal{H}) \otimes \mathcal{M}_n \longrightarrow \mathcal{B}(\mathcal{H}') \otimes \mathcal{M}_n$ is positive for all n, where $\mathcal{M}_n$ is the set of $n \times n$ complex matrices.

II.1 The Quantum Formalism

In this section we will describe the mathematical formalism of quantum mechanics from an information theoretic point of view. For that, we will enunciate the postulates of quantum mechanics giving some immediate consequences of them and introducing also the key concepts of uncertainty, quantum channels and entanglement. For a full review see, for example, [121, 142].

II.1.1 Systems and States

Postulate 1: Associated to every physical system there is a complex Hilbert space $\mathcal{H}$, that is known as the state space of the system. The system is described by its state, which is a density operator of the state space.

We denote physical system by capital letters A, B and C or numbers if there is an implicit order. Their Hilbert space is denoted by $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$ respectively and their density operator is denoted by greek letters ρ_A, σ_B and τ_C where the subindices will be removed if the system is clear from the context. The dimension of the physical system is given by the dimension of the Hilbert space associated to it.

[1] This representation is not unique as it was for pure states (up to normalization).

The easiest quantum system one could think of is a two dimensional system, whose state space is $\mathbb{C}^2$. Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis of $\mathbb{C}^2$, an arbitrary pure state can be written as $|\psi\rangle = a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$. The physical system can be in the state $|0\rangle$ and in the state $|1\rangle$, but also in a superposition of both $|\psi\rangle$. Despite its simplicity, this system is of extremely importance as it is the unit of information in quantum systems. Such a system is called quantum bit or **qubit** in analogy to the fundamental unit of classical information called bit. A d-dimensional quantum system or **qudit** will be represented in $\mathbb{C}^d$ and its pure states will be described in terms of an orthonormal basis of d elements $|1\rangle$, $|2\rangle$, ..., $|d\rangle$.

Postulate 2: The state space of a composite physical system $\mathcal{H}$ is the tensor product of the state spaces $\{\mathcal{H}_i\}$ of the component physical systems. Moreover, if we have systems labeled from 1 to n and system i is prepared in the state ρ_i, then the state of the total system is $\rho_1 \otimes ... \otimes \rho_n$.

We write ρ_{AB} for the density operator of a composite system $\mathcal{H}_A \otimes \mathcal{H}_B$ to stress that is a composite system of subsystems A and B. The state of system A when considered alone is given by its **reduced density operator** $\rho_A := \mathrm{tr}_B\, \rho_{AB}$, where the partial trace operator $\mathrm{tr}_B : \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ is defined as the unique linear operator such that

$$\mathrm{tr}_B\,(R \otimes S) = (\mathbb{1} \otimes \mathrm{tr})(R \otimes S) = R\,\mathrm{tr}\,(S),\ \forall R \in \mathcal{B}(\mathcal{H}_A),\ \forall S \in \mathcal{B}(\mathcal{H}_B).$$

One can also define the reduced density operator of system B, ρ_B, interchanging the roles of systems A and B. Moreover, if we have a composite system of several subsystems the reduced state of a set of them $\mathcal{X}$ is given by considering the partial trace over the others. That is, $\rho_{\mathcal{X}} = \mathrm{tr}_{All\setminus\mathcal{X}}\, \rho$.

We say that a pure state $|\varphi\rangle_{1,\dots,n}$ of a composite system $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ is in a **product state** if it can be written as a tensor product of elementary tensors in each of the systems, that is, $|\varphi\rangle_{1,\dots,n} = |\varphi_1\rangle \cdots |\varphi_n\rangle$, where $|\varphi_i\rangle \in \mathcal{H}_i$ for all i. This concept generalizes to mixed states as separable states. We say that a mixed state is **separable** if it can be written as a convex combination of tensor product of density operators. That is, a density operator $\rho_{1,\dots,n}$ acting on $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ is separable if there exist $p_k \geq 0$ with $\sum_k p_k = 1$ and density operators $\{\rho_i^k\}_{i,k}$ acting on $\mathcal{H}_i$ respectively such that

$$\rho_{1,\dots,n} = \sum_k p_k \rho_1^k \otimes \cdots \otimes \rho_n^k.$$

If a density operator is not separable we say that it is **entangled**. Examples of entangled pure states of two qubits are the so called *Bell states* or *Einstein-Podolski-Rosen* **(EPR) pairs**

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}},\ \frac{|01\rangle + |10\rangle}{\sqrt{2}},\ \frac{|00\rangle - |11\rangle}{\sqrt{2}} \text{ and } \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{II.1}$$

We will use the following conventions for qubits. The **computational basis** $\{|0\rangle, |1\rangle\}$ is given by $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$ and the **Hadamard basis** by $\{H|0\rangle, H|1\rangle\}$, where H denotes the 2-dimensional **Hadamard matrix** $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. We also call the computational basis the **plus** basis and associate it with the '+'-symbol, and we call the Hadamard basis the **times** basis and associate it with the '×'-symbol. For bit vectors $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ and $v = (v_1, \ldots, v_n) \in \{+, \times\}^n$ we then write $|x\rangle_v = |x_1\rangle_{v_i} \otimes \cdots \otimes |x_n\rangle_{v_n}$, where $|x_i\rangle_+ := |x_i\rangle$ and $|x_i\rangle_\times := H|x_i\rangle$.

A convenient basis for operators on $\mathbb{C}^2$ is given by the set of Hermitian matrices formed by the identity matrix and the 3 **Pauli matrices**.

$$\sigma_0 = \mathbb{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{II.2}$$

The following proposition gives a way to write systems of two subsystems.

Proposition II.1.1 (Schmidt decomposition)**.** *Let $|\psi\rangle_{AB} \in \mathbb{C}^d \otimes \mathbb{C}^n$ with $n \geq d$. There exist orthonormal bases $\{|u_1\rangle, ..., |u_d\rangle\} \subset \mathbb{C}^d$ and $\{|v_1\rangle, ..., |v_n\rangle\} \subset \mathbb{C}^n$ such that $|\psi\rangle = \sum_{i=1}^k \lambda_i |u_i\rangle \otimes |v_i\rangle$ where $\lambda_i \geq 0$ for all i, $\sum_{i=1}^k \lambda_i^2 = 1$ and $k \leq d$. Such a way of writing the state is called Schmidt decomposition, $\lambda_1, ..., \lambda_k$ are the Schmidt coefficients and the number of summands in such a decomposition is called the Schmidt rank of $|\psi\rangle$.*

This proposition is a straightforward consequence of the singular value decomposition (SVD) of a matrix and thus the Schmidt rank and coefficients are unique and the freedom in the basis is given by the freedom in the SVD. It is clear that the reduced density matrices of the state $|\psi\rangle_{AB}$ will be $\rho_A = \sum_{i=1}^n \lambda_i^2 |u_i\rangle\langle u_i|$ and $\rho_B = \sum_{i=1}^n \lambda_i^2 |v_i\rangle\langle v_i|$.

Given a density matrix $\rho_A \in \mathcal{B}(\mathbb{C}^d)$ of a system A, it can be diagonalized and written as $\rho_A = \sum_{i=1}^d \lambda_i |i\rangle\langle i|$ for some orthonormal basis $\{|i\rangle\}$. Consider another system B of the same dimension, then $\rho_A = \operatorname{tr}_B |\psi\rangle_{AB}$ where $|\psi\rangle_{AB} = \sum_{i=1}^d \sqrt{\lambda_i} |i\rangle_A |i\rangle_B$. We say that $|\psi\rangle_{AB}$ is a **purification** of the state ρ_A.

II.1.2 Quantum Transformations: Evolution and Measurement

Postulate 3: The time evolution of a closed quantum system is described by the Schrödinger equation,

$$i\frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where H is a hermitian operator known as the **Hamiltonian** of the system[2]. This postulate extends to density operators by linearity.

[2]We consider Planck's constant inside H.

The Hamiltonian has a spectral decomposition $H = \sum_i E_i |\psi_i\rangle\langle\psi_i|$ with eigenvalues E_i and associated eigenstates $|\psi_i\rangle$. States $|\psi_i\rangle$ are called *stationary states* with energy E_i and the eigenstates of lowest energy are known as the **ground states** of the system. The solution to the Schrödinger equation for a certain time is given by

$$|\psi(t_2)\rangle = e^{-iH(t_2-t_1)}|\psi(t_1)\rangle,$$

and thus stationary states are invariant in time up to a phase. Moreover, the states $\rho(t_1)$ and $\rho(t_2)$ of the system in times t_1 and t_2 respectively, are related by

$$\rho(t_2) = U(t_1, t_2)\rho(t_1)U^\dagger(t_1, t_2),$$

where $U(t_1, t_2) = e^{-iH(t_2-t_1)}$ is a unitary operator of the state space $\mathcal{H}$, which only depends on times t_1 and t_2. Thus, whenever we want to describe the evolution between two fixed times we will just work with a unitary operator.

Postulate 3 describes the evolution of closed quantum systems. However, we also need to describe the change of a system when one tries to observe it to gain some information about it. In this case, the system is no longer closed as the apparatus or the observer himself are interacting in some way with the system. This process of measurement is described by the following postulate.

Postulate 4: The measurement of a system is described by a collection of measurement operators $\{M_m\}$ that act in the state space of the system H. The index m refers to the possible outcomes of the measurement. If the state of a quantum system is ρ immediately before the measurement then the result of the measurement is m with probability $p(m) = \mathrm{tr}\,(M_m^\dagger M_m \rho)$. The state of the system after the measurement have outcome m is

$$\rho_m = \frac{M_m \rho M_m^\dagger}{p(m)} \ .$$

The measurement operators satisfy the completeness equation, $\sum_m M_m^\dagger M_m = \mathbb{1}$, which translates in probabilities of the results summing 1.

A measurement is a map that takes as input a state ρ and returns the state ρ_i with probability p_i, that is, it returns the ensemble of states $\{p_i, \rho_i\}$, where ρ_i can be mixed or pure states. Note that, $\rho = \sum_i p_i \rho_i$ by the completeness equation. Thus, it has full meaning to consider the state ρ as an statistical ensemble of the states ρ_i with probability p_i. Mixed states have attached the idea of some ignorance about the system beyond that of the probability distribution. A discrete probability distribution $\{p_i\}_i$ can be represented as $\rho = \sum_i p_i |i\rangle\langle i|$ where $\{|i\rangle\}$ is an orthonormal basis of the Hilbert space. If we measure the state ρ in that basis, that is, with measurement operators $\{|i\rangle\langle i|\}_i$, we will obtain the result i with probability p_i. We say that the state ρ models a classical system or

simply that it is classical. In this way, one can see classical probability distributions inside quantum states.

We say that a measurement is a von Neumann measurement if the measurement operators are orthogonal projections. Restrict to von Neumann measurements is not formally a restriction as one can represent a general measurement as a von Neumann measurement in a larger system via Naimark's dilation theorem [129].

In certain cases in which one is not interested in the result of the measurement it will be convenient to use the so called POVM (positive operator-valued measurement) formalism in which the measurement is described by an observable. An **observable** O is a linear functional acting on $D_1(\mathcal{H})$ given by a set of positive operators E_m, with $\sum_m E_m = \mathbb{1}$, such that $O = \sum_m mE_m$. In this case the probability of the result m to occur is $p(m) = \mathrm{tr}(E_m\rho)$ and the expected value of the measurement is given by the observable $\langle O\rangle = O(\rho) = \mathrm{tr}(O\rho) = \sum_m mp_m$.

II.1.3 Uncertainty

One of the immediate consequences of the measurement postulate is Heisenberg's uncertainty principle. In its more general form, it states that the outcome of two non-commuting observables cannot be simultaneously determined with arbitrary precision. That is, one or both of the outcomes are somehow uncertain. Although originally stated in terms of the standard deviation, in information theory it is frequently enunciated in terms of the entropy.

The entropy is a measure of the uncertainty of a random variable[3] and thus it does not depend on the possible outcomes of the random variable but in its probability distribution. Given a discrete random variable X with discrete probability distribution $P : \mathcal{X} \longrightarrow [0, 1]$ such that $\sum_{x\in\mathcal{X}} P(x) = 1$, the **Shannon entropy** [158] is given by

$$H(X) := H(P) := -\sum_{x\in\mathcal{X}} P(x)\log P(x), \tag{II.3}$$

where log denotes the binary logarithm from now on.

The Shannon entropy has other interpretations. It represents how much information one gains on average when learning the value of X. It also quantifies the average information contained in a message and thus the expected number of bits needed to encode it.

For simplicity, we state the easiest uncertainty relation for two dimensional systems. Let $\mathcal{B}_1 = \{|b_1\rangle, |b_2\rangle\}$ and $\mathcal{B}_2 = \{|v_1\rangle, |v_2\rangle\}$ be bases of $\mathbb{C}^2$, let ρ be an arbitrary quantum state of $\mathbb{C}^2$, and let X denote the measurement outcome when ρ is measured in

[3] In a broader context the term entropy usually refers to a measure of disorder.

one of the basis $\mathcal{B}_1$ or $\mathcal{B}_2$, that is, with measurement operators $\{|b_1\rangle\langle b_1|, |b_2\rangle\langle b_2|\}$ or $\{|v_1\rangle\langle v_1|, |v_2\rangle\langle v_2|\}$. Denote $H(X|\mathcal{B}_i)$ the Shannon entropy of the measurement outcome when ρ is measured in basis $\mathcal{B}_i$. Then, Maassen and Uffink's uncertainty relation [109] states that

$$H(X|\mathcal{B}_1) + H(X|\mathcal{B}_2) \geq -\log(c^2),$$

where $c := \max\{|\langle b_i|v_j\rangle| : |b_i\rangle \in \mathcal{B}_1, |v_j\rangle \in \mathcal{B}_2\}$ is the maximum overlap between the bases.

Consider the state $\rho = |0\rangle\langle 0|$ and the computational and Hadamard bases. The result of measuring ρ in the computational bases is always 0 and therefore there is no uncertainty. Then, as the maximum overlap is $c = 1/\sqrt{2}$, the uncertainty of the outcome (measure in terms of the Shannon entropy) when one measures ρ in the Hadamard bases should be at least 1. Indeed, the result of the measure would be both outcomes with equal probability and the Shannon entropy of this probability distribution is 1.

There are many other uncertainty relations, considering different setups (for example composite systems) or different entropic measures. Many of these uncertainty relations are given in terms of the following generalization of the Shannon entropy.

Definition II.1.2 ([147])**.** *For $\alpha \geq 0$ and $\alpha \neq 1$, the Rényi entropy of order α of a random variable X is defined as $H_\alpha(X) = H_\alpha(P) := \frac{1}{1-\alpha}\log\sum_{x\in\mathcal{X}} P(x)^\alpha$.*

Note that taking the limit $\alpha \to 1$ we recover the Shannon entropy and taking $\alpha \to \infty$ we have the min-entropy

$$H_{min}(X) = H_\infty(X) := \lim_{\alpha\to\infty} H_\alpha(X) = -\log\max_{x\in\mathcal{X}} P(x).$$

A generalization of the Shannon entropy to quantum states is given by the von Neumann entropy which quantifies the amount of uncertainty contained in a quantum ensemble.

Definition II.1.3 ([158])**.** *Let $\rho \in \mathcal{B}(\mathcal{H})$ be a density matrix, the von Neumann entropy is defined as*

$$S(\rho) := -tr(\rho\log\rho). \tag{II.4}$$

Let λ_i be the eigenvalues of ρ, then $S(\rho) = -\sum_i(\lambda_i\log\lambda_i) = H(\{\lambda_i\})$. In this sense, the von Neumann entropy can be seen as a measure of 'mixedness' of quantum states. The state with maximum von Neumann entropy is the identity, the uniform mixture of the possible quantum states. This allows us to call the identity the **maximally mixed** state. It is also worth to note that, as in the classical case, the von Neumann entropy represents the average quantum information contained in a 'quantum message' and thus the expected number of qubits needed to encode it.

II.1.4 Quantum Channels

In general, the description of the dynamics of an open quantum system will be given by a linear map T that takes density operators to density operators. In order to do that it is clear that the map has to be positive and trace preserving. Moreover, whenever one consider the system as part of a bigger system the map $T \otimes \mathbb{1}$, which leaves the rest of the system unchanged, also has to take density operators to density operators. Thus, the evolution of an open quantum system is given by a quantum channel from $\mathcal{B}(\mathcal{H})$ to itself.

Definition II.1.4. *A quantum channel $T : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H}')$ is a linear completely positive trace preserving (CPTP) map.*

If we restrict to finite dimensional Hilbert spaces we have the following representation theorem for quantum channels (see [192] for a proof).

Theorem II.1.5. *Given a map $T : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H}')$ the following are equivalent:*

1. *T is a quantum channel.*
2. *(Kraus representation) There exist a family of operators $\{E_k\} : \mathcal{H} \longrightarrow \mathcal{H}'$ such that $\sum_k E_k^\dagger E_k = \mathbb{1}_{\mathcal{B}(\mathcal{H})}$ and $T(\rho) = \sum_k E_k \rho E_k^\dagger$ for all $\rho \in D_1(\mathcal{H})$. These operators are called Kraus operators of T.*
3. *(Open-system representation) There exists a unitary $U \in \mathcal{B}(\mathcal{H} \otimes \mathcal{H}' \otimes \mathcal{H}')$ and a unit vector $|\varphi\rangle \in \mathcal{H}' \otimes \mathcal{H}'$ such that $T(\rho) = \mathrm{tr}_E(U(\rho \otimes |\varphi\rangle\langle\varphi|)U^\dagger)$ for all $\rho \in D_1(\mathcal{H})$, where tr_E denotes the partial trace over the first two Hilbert spaces $\mathcal{H} \otimes \mathcal{H}'$.*

While Kraus Representation gives an easy way to deal with quantum channels, the other makes it possible to consider the dynamics of an open quantum system as a unitary evolution of a bigger closed one. In addition, one could think of a measurement as a quantum channel $T : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathbb{C}^k \otimes \mathcal{H})$ such that $T(\rho) = \sum_{i=1}^k p_i |i\rangle\langle i| \otimes \rho_i$. Here, the first register is classical and contains the result of the measurement whereas the second contains the information of the state of the system after the measurement.

An important set of quantum transformations over composite systems is the set of local operations and classical communication (**LOCC**). In order to understand them and to see their practical importance consider the following situation. There are two distant laboratories each one having a subsystem of a given shared state. Without any additional resource (other shared states or communication of any kind) the operations that they can implement on the whole system are local operations (LO), that is, a local operation is just a composition of measurements and evolutions in each of the systems independently. Moreover, if we allow classical communication (CC) between the two laboratories, then the kind of operations that they can implement constitute a much bigger set. Consider for

example adaptive strategies, that is, any of the laboratories can apply a local operation depending on the result of a previous operation in the other laboratory. A consequence of these adaptive LO is that there is no known simple way to characterize LOCC [21].

II.1.5 Entanglement

Entanglement is nowadays understood as the quantum correlations that can occur in a composite system, where **quantum correlations** here should be understood as those correlations that are not of a classical nature. A possible way to define **classical correlations** is as those that can be generated by LOCC. On the contrary, entanglement is the sort of correlations that can not be generated by LOCC.

Suppose we have a composite system with no correlation at all between the constituent systems, that is, its state is a product state. It is easy to see that the set of states that one can generate from it under LOCC is the set of separable states. Thus, entangled states are those that have some non classical correlation.

Entanglement has proven to be a very useful resource with no classical analogue. It has been used to guarantee the security of protocols (quantum key distribution), to reduce the amount of time to perform certain tasks (Grover's algorithm), or the amount of communication (teleportation, superdense coding). Thus, quantifying entanglement has been one of the main problems in quantum information theory. This is the purpose of entanglement measures (see [136] for a review).

Definition II.1.6. *An entanglement (monotone) measure over the set of states of a composite system $D_1(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n)$ is a nonnegative real valued function $E : D_1(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n) \to \mathbb{R}^+$ which is zero for separable states and cannnot increase under LOCC.*

For bipartite states the Schmidt coefficients characterize completely the entanglement of the state. Thus, any entanglement measure is a function of these coefficients. Moreover, the following majorization theorem gives a preorder in the set of bipartite states.

Theorem II.1.7 ([122])**.** *Let $|\psi\rangle$, $|\varphi\rangle \in S_1(\mathbb{C}^d \otimes \mathbb{C}^d)$, there exists a LOOC protocol that transform $|\psi\rangle$ into $|\varphi\rangle$ if and only if $\sum_{i=1}^k \alpha_i \leq \sum_{i=1}^k \beta_i$ for all $k \in \{1, ..., d\}$. Where α_i and β_i are the ordered decreasingly Schmidt coefficients of $|\psi\rangle$ and $|\varphi\rangle$ respectively.*

This theorem makes it possible to define the concept of **maximally entangled state** of dimension d. Consider the pure state $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle_A |i\rangle_B$, where $|i\rangle_A$ and $|i\rangle_B$ are orthonormal bases of $\mathbb{C}^d$. Theorem II.1.7 says that it can be converted by LOCC into any other pure state in $S_1(\mathbb{C}^d \otimes \mathbb{C}^d)$. Thus, as the set of LOCC does not generate entanglement, the state $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle_A |i\rangle_B$ is maximally entangled among those of dimension d. Thus, the EPR pairs introduced in Section II.1.1 are maximally entangled states of two qubits.

The most often used measure of entanglement in pure bipartite systems is the **entropy of entanglement**, which for a given state $|\varphi\rangle_{AB} = \sum_{i=1}^{d} \lambda_i |i\rangle_A |i\rangle_B$, where $\{|i\rangle_A\}_i$ and $\{|i\rangle_B\}_i$ are local bases, is defined as

$$E(|\varphi\rangle\langle\varphi|) := S(\rho_A) = S(\mathrm{tr}_B(|\varphi\rangle\langle\varphi|)) = H(\lambda_i) = -\sum_{i=1}^{d} \lambda_i \log \lambda_i \,. \tag{II.5}$$

Where S and H are the von Neumann and Shannon entropy, respectively, introduced in Section II.1.3. It is then clear that the more entanglement a bipartite systems has, the more mixed its reduced density matrix is.

Theorem II.1.7 does not hold for multipartite systems. In fact, the result is already false for systems of three qubits as the states $W = 1/\sqrt{3}\,(|001\rangle + |010\rangle + |100\rangle)$ and $GHZ = 1/\sqrt{2}(|000\rangle + |111\rangle)$ cannot be converted into each other by means of LOCC [42]. Thus, the concept of maximally entangled state in multipartite systems has only sense referring to maximizing a particular entanglement measure.

For multipartite systems there are many entanglement measures already defined [136]. These are usually define from an operational point of view, which considers some task and quantify how well can we realize that task with a particular state. Examples of this are the localizable entanglement and entanglement of assistance. Other entanglement measures are distance-like measures that quantifies the entanglement as the distance to a particular set of states.

II.2 Matrix Product States

The set of MPS was already present in the ground state of the AKLT model [1] which triggered an intensive study on translationally invariant (TI) MPS or as they were first called finitely correlated states [46]. Since then this set of states has been repeatedly used to get both analytical results [20, 49, 134, 137, 155] and numerical methods [65, 170, 171, 176]. The importance of MPSs comes from the fact that they can be described efficiently (in the number of spins N) by a set of matrices $\{A_i\}_{i=1}^{N}$ and, at the same time, they approximate the lowest eigenstates of gapped local hamiltonians in spin chains[69, 70]. In fact, MPS describe the states over which numerical methods like DMRG optimize [46, 154, 189], which gives theoretical evidence why these methods, widely used in condensed matter, work so well. Thus, although the set of MPSs is *small* with respect to the whole Hilbert space, it exhibits and captures the phenomena appearing in quantum spin chains. In addition, the set of MPSs describes exactly the states that can be created by sequential generation [131]. Moreover, the properties of the state can be studied in terms of the local properties of the matrices.

In this section we introduce the mathematical formalism of MPSs. In what follows we consider a pure quantum state $|\varphi\rangle \in (\mathbb{C}^d)^{\otimes N}$ whose system is composed of N subsystems,

each one laying in the d-dimensional Hilbert space. Thus, the number of coefficients that determine the state of the system is d^N. This exponential growth in the number of subsystems, in principle, makes impossible to deal with arbitrary large systems.

A MPS is a state where the coefficients are given by a product of matrices in the following way

$$|\varphi\rangle = \sum_{i_1,\ldots,i_N} \operatorname{tr}\left[A^{[N]}_{i_N}\cdots A^{[1]}_{i_1}\right]|i_1\cdots i_N\rangle$$

where $A^{[k]}_i$ are $D_{k+1}\times D_k$ matrices with $D_1 = D_{N+1}$. If the MPS have $D_1 = D_{N+1} = 1$ the trace is no longer necessary and it receives the name of 'open boundary condition' (OBC-)MPS. It was shown in [175] by subsequent singular value decomposition that one can always find a *canonical* OBC-MPS of a state with $D_k \leq d^{N/2}$ sufficiently large, that is,

$$|\varphi\rangle = \sum_{i_1,\ldots,i_N} A^{[N]}_{i_N}\cdots A^{[1]}_{i_1}|i_1\cdots i_N\rangle.$$

This *canonical* OBC-MPS form of a state [131, 175] is characterized by the following conditions:

1. $\sum_i A^{[m]}_i A^{[m]\dagger}_i = \mathbb{1}$ for all $1 \leq m \leq N$.
2. $\sum_i A^{[m]\dagger}_i \Lambda^{[m-1]} A^{[m]}_i = \Lambda^{[m]}$, for all $1 \leq m \leq N$,
3. $\Lambda^{[0]} = \Lambda^{[N]} = 1$ and each $\Lambda^{[m]}$ is diagonal, positive, full rank and $\operatorname{tr}\Lambda^{[m]} = 1$.

Thus MPSs are a representation of states and not a proper subset of them. Nevertheless we will informally refer to the state being an MPS if it has an MPS representation with small *bond dimension* $D = \max_k D_k$, which, in the case of a sequence of states, it does not grow exponentially with N. This way, the number of coefficients that are needed in order to write a MPS is upper bounded by dND^2 whose asymptotic behavior is much better than d^N, the number of coefficients needed to describe a general state.

II.2.1 Representations

The MPS have a simple diagrammatic representation (Fig. II.1) that will be substantially used in Chapters IV and V. Each square represents a tensor, lines going out of the squares (legs) represent open indices and lines between squares represent contraction rules between the tensors associated to the corresponding legs.

An alternative but equivalent view of an MPS is the valence bond construction (see Fig. II.2): consider a pair of D dimensional ancillary/virtual Hilbert spaces associated to each site and connect every pair of neighboring virtual Hilbert spaces by maximally entangled

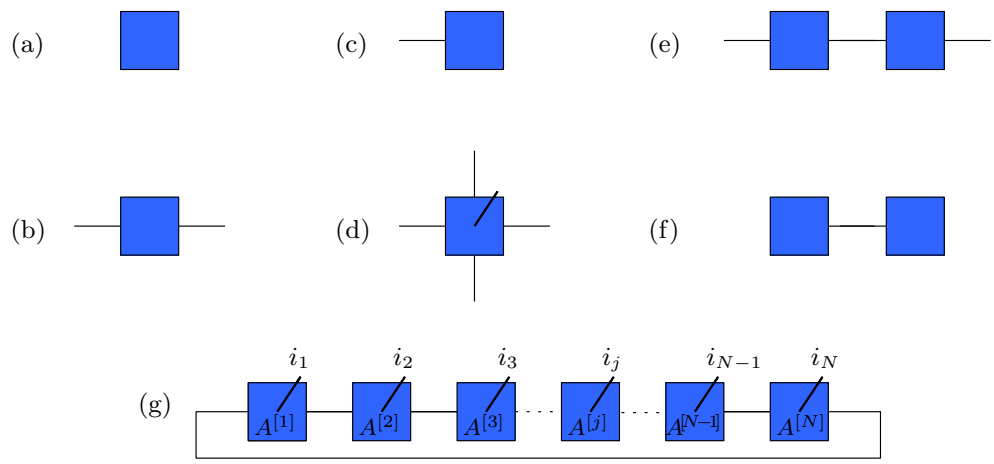

Figure II.1: Diagrammatic representation of (a) scalar, (b) matrix, (c) vector, (d) tensor with five indices, (e) matrix multiplication, (f) scalar product and (g) MPS.

states (usually called entangled *bonds*). The MPS is then the result of *projecting* the virtual Hilbert spaces into the real/physical one by the map $\mathcal{P}^{[k]} = \sum_{i_k\,\alpha_k\,\beta_k} A^{[k]}_{i_k,\alpha_k\beta_k} |i_k\rangle\langle\alpha_k\beta_k|$. With this equivalent representation of the MPS one can easily see that the entropy of entanglement of l consecutive sites is bounded by $2\log D$. Indeed, the entropy of entanglement between the virtual Hilbert spaces of these l physical systems and the rest of virtual systems is given by the entangled bonds in the boundary. This entropy of entanglement is exactly $2\log D$ and the local projections $\mathcal{P}^{[k]}$ cannot increase entanglement.

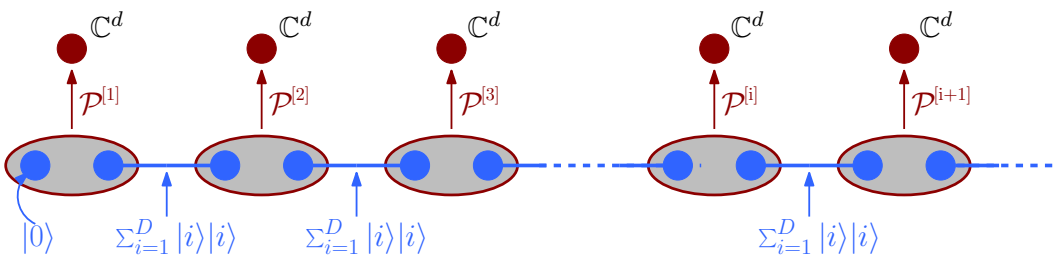

Figure II.2: Valence bond construction of an OBC-MPS. Entangled bonds in blue and projections into the physical systems in red.

One of the nice properties of MPS is that they are the set of states that can be created efficiently in the following sequential manner (see Fig. II.3):

$$|\varphi\rangle|0\rangle_a = V_{[N]}\cdots V_{[1]}|0\cdots 0\rangle_{N,\ldots,1}|0\rangle_a, \tag{II.6}$$

where a is an ancillary system of dimension $D = \max_k D_k$ and $V_{[j]}$ is the unitary gate,

involving only system j and the ancilla a, given by

$$V_{[j]}|0\rangle_j|r\rangle_a = \sum_{s,i_j} \langle s|A^{[j]}_{i_j}|r\rangle|i_j\rangle_j|s\rangle_a$$

The condition $\sum_{i_j} A^{[j]\dagger}_{i_j} A^{[j]}_{i_j} = \mathbb{1}$ makes $V_{[j]}$ unitary.

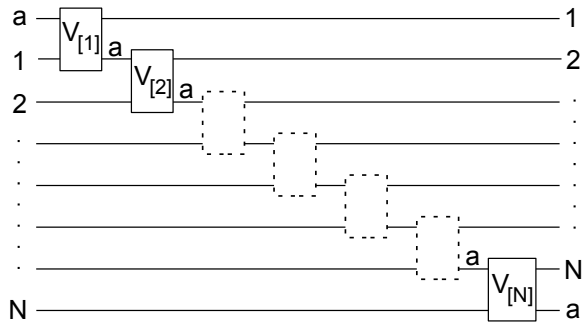

Figure II.3: Circuit for creating an MPS in a sequential way, where each box implements a unitary $V_{[i]}$ between the ancilla a and system i together with a swap operation between them.

II.2.2 Translation invariant MPS

In principle, the matrices appearing in the MPS representation of a state $A^{[j]}_{i_j}$ are dependent on the site j, hence the label $[j]$. The lack of this dependency means that the system is TI. Moreover, the reciprocal also holds, systems that are TI have a TI-MPS representation in which the matrices are independent of the sites [131], that is,

$$|\Phi\rangle = \sum_{i_1,\ldots,i_N} \operatorname{tr}\left[A_{i_N}\cdots A_{i_1}\right]|i_1\cdots i_N\rangle.$$

There is a close relation between a TI-MPS and the completely positive map $\mathcal{F}$ acting on the space of $D\times D$ matrices

$$\mathcal{F}(X) = \sum_i A_i X A_i^\dagger.$$

One can deduce many properties of the TI-MPS from the properties of the CP-map associated. In fact, one can consider a slight modification of $\mathcal{F}$ and define the associated CP-map $\mathcal{E}$ as $\mathcal{E}(X) : \mathcal{B}(H_A) \to \mathcal{B}(H_A \otimes H_B)$ with

$$\mathcal{E}(X) = \sum_{i,j} A_i X A_j^\dagger \otimes |i\rangle\langle j|. \tag{II.7}$$

Then, $\mathcal{E}$ can be understood as acting on ancillary system A of dimension $\dim(H_A) = D$ and *creating* a system B of dimension $\dim(H_B) = d$. The reduced density matrix of l systems can be expressed in terms of this map

$$\rho_l = tr_A[\mathcal{E}^l(\mathbb{1}_D)],$$

where the systems B are being *created* in order from 1 to l.

A key property within MPS theory is called *injectivity* [46, 131] and it essentially means that different boundary conditions give rise to different states.

Definition II.2.1. *Formally, an MPS $|\phi_A\rangle$ is injective in a region R (whose minimal length we denote by L_0) if the map $\Gamma_R(X) = \sum_{i_1,\ldots,i_{L_0}} \mathrm{tr}(XA_{i_1}\cdots A_{i_{L_0}})|i_1\cdots i_{L_0}\rangle$ which associates boundary conditions of R to states in R is injective. An MPS is said to be injective if it is injective for some region R.*

A simple characterization of injectivity that we will use repeatedly is given by the following lemma.

Lemma II.2.2. *A MPS is injective in a region R if and only if, for any tensor $X \in \Gamma_R$, there exists $|a_X\rangle \in \mathcal{H}^R$ defined in the Hilbert space of the physical indices such that $X = \langle a_X|\sum_{i_1,\ldots,i_{L_0}} A_{i_1}\cdots A_{i_{L_0}}|i_1\cdots i_{L_0}\rangle$.*

Injectivity is a generic condition, that is, almost all TI-MPS are injective. Moreover, if a TI-MPS is injective then there is a unique 'canonical' TI-MPS representation up to an isometry (see Fig. II.4). That is,

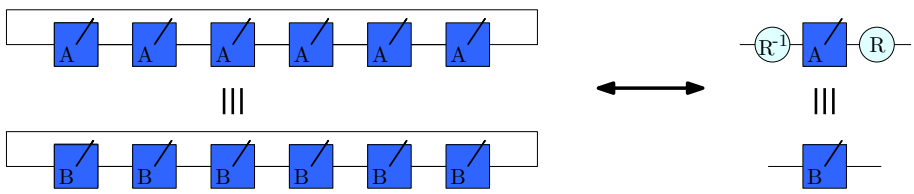

Figure II.4: Diagrammatic representation of the uniqueness of the MPS representation given by Theorem II.2.3.

Theorem II.2.3 ([131, Theorem 6])**.** *Let*

$$|\psi_A\rangle = \sum_{i_1,\ldots,i_N=1}^{d} \mathrm{tr}(A_{i_1}\cdots A_{i_N})|i_1\cdots i_N\rangle$$

be a translational invariant MPS representation with bond dimension D which is injective for regions of size L_0 and $N \geq 2L_0 + D^4$. Then

1. $\sum_i A_i A_i^\dagger = \mathbb{1}$ *for all* $1 \leq m \leq N$.
2. $\sum_i A_i^\dagger \Lambda A_i = \Lambda$, *for some positive, diagonal and full rank matrix* Λ.
3. $\mathbb{1}$ *is the only fixed point of* $\mathcal{F}(X) = \sum_i A_i X A_i^\dagger$.

Moreover, if we have another MPS representation of the same state with the same bond dimension,

$$|\psi_B\rangle = \sum_{i_1,\ldots,i_N=1}^{d} \mathrm{tr}(B_{i_1} \cdots B_{i_N}) |i_1 \cdots i_N\rangle,$$

with $|\psi_A\rangle = e^{i\theta}|\psi_B\rangle$, *then there exists an invertible matrix* R *and a phase* $\varphi \equiv \theta \pmod{2\pi}$ *such that* $A_i = e^{i\varphi/N} R B_i R^{-1}$, *for all* i.

Chapter III

Multipartite Entanglement and Symmetry

Entanglement is a key phenomenon in quantum mechanics and its understanding, classification, quantification and use is vital for the field of quantum information theory. In the simplest case, the pure bipartite case, entanglement is fully characterized by the coefficients appearing in the Schmidt decomposition [174]. This simple characterization contrasts with the lack of a criterion for separability in the mixed bipartite case and the complexity in characterizing multipartite entanglement.

Even in the tripartite case, strange phenomena start to occur, like the non-equivalence of W and GHZ states [42], the possibility of distributing entanglement with separable states [31], or the existence of unbounded violations for some correlation Bell inequalitites [15, 133]. Going into the N-partite situation only increases the number of interesting phenomena: universal states for quantum computation [143], topological entanglement [92], relations with complexity theory [66], and so on.

In order to quantify entanglement, many entanglement measures have been proposed for the two-particle as well as for the multiparticle case [64, 84, 136]. These different measures have been defined, focusing on the different aspects of entanglement, associated with the different points of view in the theory of multipartite entanglement: the topological entropy [93] measures the amount of topological entanglement in a state and is hence appropriate in the context of topological quantum computation and error correction; the localizable entanglement [140] measures the amount of bipartite entanglement that can be created between two sites in a collaborative scenario and is hence appropriate in the context of quantum networks and quantum repeaters; there are also measures which intend to be more general, and usually measure the distance (in some sense) to the set of separable states, like the relative entropy of entanglement, the global robustness of entanglement or the geometric measure of entanglement [185].

The variety of multipartite entanglement measures has its roots in the impossibility of defining the concept of a "maximally entangled state" in the multipartite setting, as is pointed out repeatedly in the literature [84, 136]. Moreover, all of the proposed entanglement measures suffer a serious drawback: They are very difficult to compute as their definition contains optimizations over certain states or quantum information protocols.[1] Such optimizations can be performed successfully for special cases only, for instance, if

[1] A well-known exception is the entanglement of formation (or the concurrence) for two qubits, see [193]

the density matrix under investigation possesses a high symmetry or belongs to a special family, e.g., with low rank [108, 150, 164, 182].

An often-used entanglement measure for multiparticle systems is the geometric measure of entanglement [185]. For a given multiparticle state $|\psi\rangle$, one first considers the closest fully separable state $|\phi\rangle = |a\rangle|b\rangle|c\rangle\cdots$ in terms of the overlap

$$G(\psi) = \max_{|\phi\rangle=|a\rangle|b\rangle|c\rangle\cdots} |\langle\psi|\phi\rangle|, \tag{III.1}$$

and then defines the geometric measure of the pure state as

$$E_G(|\psi\rangle) = 1 - G(\psi)^2.$$

Sometimes, the geometric measure for pure states is also taken as $\varepsilon_G(|\psi\rangle) = -2\log_2 G(\psi)$. Based on this definition, the geometric measure is extended to mixed states via the convex roof construction: For a given density matrix ϱ one minimizes over all possible decompositions of ϱ into pure states $\varrho = \sum_k p_k|\phi_k\rangle\langle\phi_k|$, where the p_k form a probability distribution,

$$E_G(\varrho) = \min_{p_k,|\phi_k\rangle} \sum_k p_k E_G(|\phi_k\rangle).$$

Clearly, also this optimization is not straightforward to compute.

The geometric measure has become one of the widely used entanglement measures for the multiparticle case. It fulfills all the desired properties of an entanglement monotone in Definition II.1.6 (see Ref. [185]). Moreover, it has a physical interpretation of quantifying the difficulty in distinguishing multiparticle quantum states by local means [72]. It has also been used to study quantum phase transitions in spin models [119, 124, 126, 183, 184] and the usefulness of states as resources for measurement based quantum computation [60].

In this chapter we will study how imposing symmetry restrictions on the state can simplify things in both, the optimization problem in Eq. (III.1) and the problem of defining a "maximally entangled state" in the multipartite setting.

For the optimization problem in Eq. (III.1), the natural question that arises is whether for a symmetric state $|\psi\rangle$ the closest product state can be chosen symmetric, i.e., $|\phi\rangle = |a\rangle|a\rangle|a\rangle\cdots$. If this is true, it drastically simplifies the calculation of the geometric measure for pure symmetric states, as the number of parameters in this optimization then does not depend on the number of particles anymore.

In Section III.1 we will give an affirmative answer to this conjecture based on the theory of N-homogeneous polynomials over Banach spaces. However, this result does not allow us to conclude that only symmetric solutions exist. We then go on to show that the optimal state maximizing $G(\psi)$ is *necessarily* symmetric for three or more particles. Finally, we will discuss consequences and generalizations of our results, concerning, among others, the maximization of the expectation value of symmetric positive operators.

For the latter problem, we will concentrate in protocols in which there is an authority A, and a set of participants $p_1, \ldots, p_N$ which *have to play the same role in the protocol.* This is the desired situation in a wide variety of multipartite protocols, like secret sharing or voting, and leads to

Assumption 1. We will work with $(N+1)$-partite states which are permutational-symmetric with respect to N of the parties.

Assumption 2. To make things simpler we will assume that the Hilbert space dimension of the participants is 2, while that of the authority is $N+1$, which is the smallest possible dimension to purify any mixed state among the participants.

The permutational symmetry of the state is the quantum resource, with no classical analogue, which ensures that all participants are treated equally and are indistinguishable from the authority's point of view. These kinds of requirements are gaining importance nowadays as *privacy* is becoming a serious issue in the new e-society. In fact, permutational symmetry also appears as a natural condition in quantum de Finetti theorems [97]. Within assumptions 1 and 2, we will show in Section III.2 that there is a "maximally entangled state" $|\Phi\rangle$ and a LOCC protocol that transforms this to any other state with the same symmetry.

Moreover, we will show how all the elements of the protocol, including the construction of the state, can be performed efficiently and discuss some security issues concerning possible applications to cryptographic protocols. Along the way we will recover the main result in [38] from a more general point of view. We will mix basic tools from several areas: representation theory, convex analysis, matrix product states, and quantum channels.

Relations to prior work. The value of E_G has been computed for many pure states [73, 112, 162, 163], and the convex roof for some important cases has been calculated in Refs. [63, 185]. The problem of whether for a symmetric state $|\psi\rangle$, the closest product state can be chosen symmetric, has recently drawn considerable attention in quantum information theory. Some effort has been made to prove it. For example, it has been used as a conjecture in Ref. [185]. In Ref. [73] it has been proved for two particles that there is always a symmetric state which gives the maximum value (but it can happen that also non-symmetric states yield the same value) and a first attempt for the N-particle case was given. Quite recently, special cases of this conjecture have been verified [74, 186], and related conjectures, that we study here, have been formulated [54].

As far as maximally entangled states is concerned, in the multipartite setting, the concept is well defined with respect to a particular entanglement measure or to a particular quantum information protocol. Nevertheless, there is not a maximally entangled state with respect to all of them at the same time [136, 84], as it is already clear from the non-equivalence of W and GHZ states [42]. Very recently the notion of the maximally

entangled set has been introduced [36]. This is the minimal set of states such that any state can be obtained by LOCC from one of the states within the set. Also, the set of states that are maximally entangled for any bipartition has been studied in [79]. For an even number of parties these states can be used to teleport from half of the parties to the other half in a collaborative way. Moreover, these states are in one to one correspondence with quantum secret sharing schemes. Thus, they exhibit genuine multipartite entanglement, and seem to be highly entangled in a multipartite way.

Other interesting subsets of multipartite states with different applications have also been considered. For example, graph or stabilizer states have been fruitful tools in the development of quantum error correction and models for quantum computing [77]. Likewise, the set of locally maximally entangleable states (defined as those states where all quantum information can be maximally washed out by coupling each particle to a local auxiliary qubit) is equivalent to the set of states that can be used for optimal local encoding of classical information [99].

Note that the sets of states in both problems are closely related. One could see the systems fulfilling assumptions 1 and 2 as a purification of a mixture of symmetric states where one have N systems of dimension 2. Although this link is clear, the analysis and results of the two problems will be given independently. Thus, we devote Sections III.1 and III.2 to each of the problems and we gather the conclusions and open problems in Section III.3.

III.1 The geometric measure for symmetric states

Let us fix our notation. The state of the system $|\psi\rangle \in S((\mathbb{C}^d)^{\otimes N})$ is composed of N d-dimensional subsystems. We write the overlap $|\psi\rangle$ with a product state $|\alpha_1, \ldots, \alpha_N\rangle$, where the vectors α_i are normalized elements of $\mathbb{C}^d$, as an evaluation of a corresponding N-linear form ψ, i.e.,

$$\langle\psi|\alpha_1, \alpha_2, \ldots, \alpha_N\rangle =: \psi(\alpha_1, \alpha_2, \ldots, \alpha_N),$$

where we will not use the braket notation inside the functions. If the state $|\psi\rangle$ is symmetric then it corresponds to a symmetric N-linear form ψ.

For any symmetric N-linear form there exists an associated N-homogeneous polynomial $\hat{\psi}$ (and vice versa), that is a polynomial such that $P(\lambda x) = \lambda^N P(x)$ for all $\lambda \in \mathbb{C}$, by virtue of the mapping

$$\begin{aligned} \hat{\psi}\colon \mathbb{C}^d &\longrightarrow \mathbb{R} \\ \alpha &\longmapsto \psi(\alpha, \ldots, \alpha). \end{aligned}$$

The norm of this polynomial is defined by

$$\|\hat{\psi}\| = \max_{\alpha \in \mathbb{S}(\mathbb{C}^d)} |\hat{\psi}(\alpha)|.$$

The relation between the norms $\|\hat{\psi}\|$ and $\|\psi\|$ is studied in the theory of polynomials over Banach spaces, cf. Ref. [40]. For a Banach space $\mathcal{E}$ the *N-th polarization constant* $c(N, \mathcal{E})$ is the smallest positive number K such that

$$\|\psi\| \leq K\|\hat{\psi}\|$$

holds for every symmetric N-linear form ψ over $\mathcal{E}$. We then have the following polarization constants:

Theorem III.1.1. *(i) Let H be a finite dimensional Hilbert space over a field $\mathbb{K}$ and N a positive integer then*

$$c(N, H) = 1$$

(ii) Let N, d be positive integers such that $N \leq d$ then

$$c(N, \mathfrak{H}_1^d) = \frac{N^N}{N!},$$

where $\mathfrak{H}_1^d$ is the real Banach space of d dimensional hermitian matrices equipped with the trace norm.

(i) is a classical result, cf. Ref. [5, 82, 91]. An exhaustive discussion can be found in Ref. [40]. The proof of (ii) follows from the facts that $c(N, \mathcal{E}) \leq N^N/N!$ for any Banach space $\mathcal{E}$ and l_1^d (i.e., $\mathbb{R}^d$ with the norm $\|\cdot\|_1$) can be embedded isometrically into $\mathfrak{H}_1^d$, thus $c(N, l_1^d) \leq c(N, \mathfrak{H}_1^d)$, and the N-th polarization constant of l_1^d is $c(N, l_1^d) = N^N/N!$, see [40].

In our particular case, where $H = \mathbb{C}^d$ we have the following Corollary.

Corollary III.1.2. *Let $|\psi\rangle \in S((\mathbb{C}^d)^{\otimes N})$, then there exists $|\alpha\rangle \in S(\mathbb{C}^d)$ such that*

$$G(\psi) = |\psi(\alpha, \alpha, \ldots, \alpha)| = |\hat{\psi}(\alpha)|,$$

that is, symmetric product states maximize the overlap with any symmetric state.

This corollary leaves open if also non-symmetric states may attain the maximal value. This is in fact never the case for $N \geq 3$, as we summarize in

Lemma III.1.3. *Let $\psi \neq 0$ be a symmetric N-linear form over $\mathbb{C}^d$ with $N \geq 3$ and let the vectors $\alpha_1, \ldots, \alpha_N$ maximize $|\psi|$, i.e.,*

$$G(\psi) = |\psi(\alpha_1, \alpha_2, \ldots, \alpha_N)|.$$

Then the vectors α_i are equal up to a phase, in other words, the span of $\alpha_1, \ldots, \alpha_N$ is one-dimensional.

In order to prove Lemma III.1.3, we will first consider the situation where $N = 2$. The following Lemma and its proof were already given Ref. [73], however, the proof provides some observations that are essential in order to establish our main result.

Lemma III.1.4 ([73])**.** *For any symmetric two-linear form ψ over $\mathbb{C}^d$ we can find a vector α such that*

$$G(\psi) = |\psi(\alpha, \alpha)|.$$

Rephrasing the statement of the Lemma, when maximizing $|\psi|$ for two particles, the maximum can be reached by a symmetric choice of vectors, although a solution maximizing $|\psi|$ is not necessarily symmetric.

Proof of Lemma III.1.4. In a fixed orthonormal basis $\{b_i\}$ the symmetric quadratic form ψ is represented by a symmetric matrix $\Psi_{ij} := \psi(b_i, b_j)$. Then we have $\psi(\alpha, \beta) = \alpha^T \Psi \beta$, where on the right-hand side α and β are column vectors with coefficients in the basis $\{b_i\}$. For a complex symmetric matrix $\Psi = \Psi^T$ Takagi's factorization theorem [161] states that Ψ can be written as

$$\Psi = U^T D U,$$

with a unitary matrix U and a diagonal matrix $D = \mathrm{diag}(r_1, \ldots, r_k)$ where the non-negative values r_i are in decreasing order, $r_1 \geq r_2 \geq \cdots \geq r_k \geq 0$. In this form, a symmetric choice of α and β maximizing $|\psi|$ becomes evident, namely $\alpha \equiv \beta \equiv U^\dagger e_1$ where $e_1 = (1, 0, \ldots, 0)^T$. Hence $G(\psi) = r_1$. □

Let us make some remarks on the remaining freedom in the choice of α and β. First, we note that if $r_1 > r_2$ the only choice to reach the maximum r_1 is the one given in the proof above. Hence for this case the maximizing solution is unique (up to a phase) and symmetric.

Otherwise, consider the case $r_1 = r_2 = \cdots = r_d$. We then say ψ is degenerate and define $R_1 := \mathrm{span}_{\mathbb{C}}(\{e_1, \ldots, e_d\})$. If $G(\psi) = |\psi(\alpha, \beta)|$, we can always write $\alpha \equiv U^\dagger e^*$ and $\beta \equiv U^\dagger e$ with some $e \in R_1$, where the vector $e^* \in R_1$ denotes the vector obtained from e by complex conjugation in the given basis. The case that $e \equiv e^*$ then corresponds to the symmetric solutions.

The symmetric maximizing solutions therefore correspond via U to real vectors in R_1 (up to a phase), and having a non-symmetric solution $\alpha \not\equiv \beta$ of the maximization

implies degeneracy. Moreover, in case of degeneracy we find a continuum of inequivalent asymmetric as well as symmetric solutions. The following observation will be needed in the main proof and expresses this fact.

Observation III.1.5. *Given a symmetric two-linear form ψ with*

$$G(\psi) = |\psi(\alpha, \beta)|,$$

where $\beta \not\equiv \alpha$, we can always find two orthonormal vectors δ_1 and δ_2 such that:

(i) δ_1 and δ_2 span the same space as α and β, in particular $\alpha, \beta \in \mathrm{span}_{\mathbb{C}}(\{\delta_1, \delta_2\})$.

(ii) We have $G(\psi) = |\psi(\delta_1, \delta_1)| = |\psi(\delta_2, \delta_2)| = |\psi(\eta, \eta)| = |\psi(\mu, \mu')|$, where

$$\begin{aligned} \eta &:= (\delta_1 + \delta_2)/\sqrt{2}, \\ \mu &:= (\delta_1 + i\delta_2)/\sqrt{2}, \\ \mu' &:= (\delta_1 - i\delta_2)/\sqrt{2}. \end{aligned}$$

(iii) The vectors $\delta_1, \delta_2, \eta, \mu'$ do not equal α, even modulo a phase.

Proof. Consider $G(\psi) = |\psi(\alpha, \beta)| = |\psi(U^\dagger e^*, U^\dagger e)|$ with the unitary matrix U from Takagi's factorization of Ψ, where $e \not\equiv e^*$ as $\beta \not\equiv \alpha$ by assumption. We can choose two real orthonormal vectors f_1, f_2 such that $\mathrm{span}_{\mathbb{C}}(\{f_1, f_2\}) = \mathrm{span}_{\mathbb{C}}(\{e, e^*\})$. They can be obtained from the real and imaginary parts of e and e^*.[2] Hence

$$\delta_1 = U^\dagger f_1 \text{ and } \delta_2 = U^\dagger f_2$$

is a valid choice of orthonormal vectors fulfilling (i), each providing a symmetric maximization of $|\psi|$. The vectors δ_1, δ_2 as well as the vectors η, μ, μ' derived from δ_1, δ_2 fulfill (ii) by construction, according to the observations above and because $\eta = U^\dagger(f_1 + f_2)/\sqrt{2}$, where $(f_1 + f_2)/\sqrt{2} \in R_1$ (likewise for μ, μ'). Finally, we have enough freedom to choose f_1, f_2 to satisfy (iii). □

After these preliminaries, we are ready to prove Lemma III.1.3:

Proof of Lemma III.1.3. The proof consists of two parts. In Part I we prove the case $N = 3$. In Part II we extend the result to arbitrary $N > 3$.

Part I. Assume a maximizing set of vectors $\{\alpha, \beta, \gamma\}$ has been found,

$$G(\psi) = |\psi(\alpha, \beta, \gamma)|.$$

[2] Note that e and e^* are vectors with complex conjugated elements, i.e., $e = e_r + ie_i$ and $e^* = e_r - ie_i$ where $e_r, e_i \in \mathbb{R}^d$. Hence e_r, e_i is an example for a real basis, being linearly independent since $e \not\equiv e^*$. In fact, any real orthonormal basis of $\mathrm{span}_{\mathbb{C}}(\{e_r, e_i\})$ can be used as f_1, f_2, as long as they fulfill (iii).

We show that the assumption $\dim[\mathrm{span}_{\mathbb{C}}(\{\alpha,\beta,\gamma\})] \neq 1$ leads to $\psi = 0$.

Without losing generality, we hence assume that $\gamma \not\equiv \beta$. Then we have a degenerate quadratic form $\psi(\alpha,\cdot,\cdot\cdot)$. Using Lemma III.1.4 we obtain a symmetric maximizing solution $\sigma \not\equiv \alpha$ (due to $\gamma \not\equiv \beta$, σ is not unique). Hence we have $G(\psi) = |\psi(\alpha,\sigma,\sigma)|$. From Observation III.1.5, applied to the quadratic form $\psi(\cdot,\cdot\cdot,\sigma)$, we take the vectors $\delta_1,\delta_2,\eta,\mu,\mu'$ with the properties as stated. With these vectors we define the 2×2-matrices A,B,N,M via

$$\begin{aligned} A_{kl} &:= \psi(\delta_1,\delta_k,\delta_l),\\ B_{kl} &:= \psi(\delta_2,\delta_k,\delta_l),\\ N_{kl} &:= \psi(\eta,\delta_k,\delta_l) = (A_{kl}+B_{kl})/\sqrt{2},\\ M_{kl} &:= \psi(\mu,\delta_k,\delta_l) = (A_{kl}+iB_{kl})/\sqrt{2}. \end{aligned} \tag{III.2}$$

As $\sigma,\delta_1,\delta_2,\eta$, and μ' are in $\mathrm{span}_{\mathbb{C}}(\{\delta_1,\delta_2\})$ the matrices A,B,N,M correspond to two-forms which assume the maximum $r_1 = G(\psi)$ on this span. Since $\delta_1,\delta_2,\eta,\mu' \not\equiv \sigma$, the quadratic forms A,B,N,M are degenerate with the value r_1. In terms of the Takagi factorization, we can write $A = U_A^T D U_A$ and $B = U_B^T D U_B$, etc. with $D = \mathrm{diag}(r_1,r_1)$. It follows that $A^\dagger A = B^\dagger B = N^\dagger N = M^\dagger M = D^2$, which implies $A^\dagger B + B^\dagger A = i(A^\dagger B - B^\dagger A) = 0$. Hence $B^\dagger A = 0$, which is only possible for $\psi = 0$.

Part II. The extension to $N > 3$ is proved as follows. If $G(\psi) = |\psi(\alpha_1,\alpha_2,\ldots,\alpha_N)|$ we define a symmetric 3-linear form by

$$\psi_{\hat{k}} := \psi(\hat{\alpha}_1,\hat{\alpha}_2,\ldots,\hat{\alpha}_k,\ldots,\alpha_N)$$

where $\hat{\alpha}_i$ denotes omission, i.e., $\alpha_1,\alpha_2,\alpha_k$ are omitted. As in Part 1, we have $G(\psi) = |\psi_{\hat{k}}(\alpha_1,\alpha_2,\alpha_k)|$ and thus $\alpha_1 \equiv \alpha_2 \equiv \alpha_k$ for all k. Hence all vectors $\alpha_1,\ldots,\alpha_N$ must be the same up to a phase. □

Lemma III.1.3 is stated for N-linear forms over a complex vector space. If $|\psi\rangle$ is real, one can also consider the maximization over real product vectors. In general this will yield a different result than the complex case. An example of a four-qubit state where the maximizations over real and complex product vectors differ is $|\psi\rangle = [|0000\rangle + |0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle - 2(|1110\rangle + |1101\rangle + |1011\rangle + |0111\rangle)]/\sqrt{21}$. Since the polarization constant is 1 also in the real case, one can find a symmetric state among the real product states which attains the maximum. In contrast to the complex case, the maximizing state is, however, not necessarily symmetric for three particles. A counterexample is $|\psi\rangle = (|001\rangle + |010\rangle + |100\rangle - |111\rangle)/2$ where the maximum of $1/2$ is also attained by $|\phi\rangle = |001\rangle$.

III.1.1 Physical interpretation of the proof

An interpretation of the proof of Lemma III.1.3 in physical terms is the following. The matrices A, B, N and M in Eq. (III.2) are representations of the state $|\psi\rangle$, after one site has been measured out and the remaining state has been projected onto a two-dimensional subspace. The values r_i correspond to Schmidt coefficients of this remaining state and, as they are equal, the state corresponds to a Bell state. The proof of Lemma III.1.3 shows that for qubits it is impossible to create a state of three particles that is both symmetric and always results in a Bell-pair like state after an arbitrary measurement on one site.

III.1.2 Translationally invariant states

It is interesting to ask whether also for translationally invariant states the maximum is attained in a symmetric state, as such states occur naturally in the analysis of spin models. This has sometimes been assumed when investigating the geometric measure in condensed matter systems.

First, a counterexample for this conjecture is the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle)$$

for which the closest separable states are the non-symmetric states $|0101\rangle$ and $|1010\rangle$. In fact, one can find translationally invariant states which are orthogonal to any symmetric product state, e.g., $|\psi\rangle \sim (|0101\rangle - |0011\rangle +$ all translations).

This situation gets worse as the number of particles increases. Let $\mathcal{T}$ denote the subspace of translationally invariant states for N qudits and let $\mathcal{S} \subset \mathcal{T}$ be the permutationally symmetric subspace. Then any state in $\mathcal{X} = \mathcal{T} \cap \mathcal{S}^{\perp}$ – the orthocomplement of $\mathcal{S}$ in $\mathcal{T}$ – has a vanishing overlap with any symmetric product state, hence the closest product state is not symmetric. The dimension of $\mathcal{T}$ is given by [138]

$$\dim(\mathcal{T}) = \frac{1}{N} \sum_{j|N} \varphi(j)\, d^{N/j},$$

where φ denotes Euler's totient function and the summation is over all divisors j of N. For $\mathcal{S}$ we have

$$\dim(\mathcal{S}) = \binom{N+d-1}{d-1}.$$

Therefore, if $N \gg d$ then the dimension of the subspace $\mathcal{X}$ is roughly given by $(d^N - N^d)/N$ and the fraction of states where the conjecture holds shrinks rapidly as the number of particles increases.

Concerning the analysis of entanglement in spin models, this shows that the assumption that the closest separable state to the ground state is symmetric, has to be handled with care. For some models, it seems to be true [181, 183], for other models (like the Majumdar-Ghosh model [111]) one can directly check that it is wrong.

III.1.3 Operators of higher rank

We now consider generalizations of our results. Let $\Pi_{\mathcal{S}}$ be the projector onto the symmetric subspace $\mathcal{S}$. An operator A is *permutationally symmetric* if it acts on the symmetric subspace only, i.e., it fulfills $A = \Pi_{\mathcal{S}} A \Pi_{\mathcal{S}}$. A is called *permutationally invariant* if it is invariant under permutation of the particles (the latter is a weaker condition than the former [165]). We hence define for an observable X

$$\begin{aligned}\hat{G}(X) &:= \max_{|\varphi\rangle = |a\rangle|b\rangle|c\rangle\cdots} |\langle\varphi|X|\varphi\rangle| \\ \hat{G}_{\mathcal{S}}(X) &:= \max_{|\varphi\rangle = |a\rangle\cdots|a\rangle} |\langle\varphi|X|\varphi\rangle|\end{aligned}$$

Such optimizations occur naturally in the construction of entanglement witnesses or in the estimation of entanglement measures via Legendre transforms [64].

To study the relation of these quantities, we can write $\langle\varphi|X|\varphi\rangle = \operatorname{tr}[X\,|\varphi\rangle\langle\varphi|]$ as an evaluation of a corresponding N-linear form ξ over $\mathfrak{H}_1^d$ due to

$$\xi(A_1, \ldots, A_N) = \operatorname{tr}[X A_1 \otimes \cdots \otimes A_N].$$

Then any permutationally invariant operator X corresponds to a symmetric N-linear form ξ and a N-homogeneous polynomial $\hat{\xi}$ by virtue of the mapping

$$\begin{aligned}\hat{\xi}\colon \mathfrak{H}_1^d &\longrightarrow \mathbb{R} \\ A &\longmapsto \xi(A, \ldots, A).\end{aligned}$$

This gives, using that pure states are the extremal points of $\mathfrak{H}_1^d$, that

$$\begin{aligned}\hat{G}(X) &= \max_{A_i = |a_i\rangle\langle a_i|} |\xi(A_1, ..., A_N)| = \max_{A_i \in \mathfrak{H}_1^d, \operatorname{tr}(|A_i|) \leq 1} |\xi(A_1, ..., A_N)| =: \|\xi\| \\ \hat{G}_S(X) &= \max_{A = |a\rangle\langle a|} |\hat{\xi}(A)| = \max_{A \in \mathfrak{H}_1^d, \operatorname{tr}(|A|) \leq 1} |\hat{\xi}(A)| =: \|\hat{\xi}\|\end{aligned}$$

As the N-th polarization constant is (Theorem III.1.1)

$$c(N, \mathfrak{H}_1^d) = N^N/N! \quad \text{for} \quad N \leq d,$$

the quotient $\hat{G}(X)/\hat{G}_{\mathcal{S}}(X)$ can get arbitrarily large as N and d increase.

We will provide a further explicit example and other counterexamples of different conjectures. Let us first discuss some cases where symmetry assumptions do hold:

Corollary III.1.6. *(i) If X is a positive permutationally symmetric observable then $\hat{G}(X)$ can be attained by a symmetric state.*
(ii) If X is a permutationally invariant N-qubit observable that contains only full correlation terms, then $\hat{G}(X)$ can be attained by a symmetric state.

Proof. (i) We note that

$$\hat{G}(X) \leq \max_{|\psi\rangle=|b_1\rangle\cdots|b_N\rangle} \max_{|\varphi\rangle=|a_1\rangle\cdots|a_N\rangle} |\langle\varphi|X|\psi\rangle|.$$

Fixing $|\psi\rangle$, the (unnormalized) state $X|\psi\rangle = \Pi_{\mathcal{S}} X \Pi_{\mathcal{S}}|\psi\rangle$ is symmetric and by virtue of Lemma III.1.3 the maximum is reached by a symmetric state $|a,\ldots,a\rangle$. Repeating the reasoning with the fixed state $|\varphi\rangle = |a,\ldots,a\rangle$, we get $\hat{G}(X) \leq \max_{|b\rangle} \max_{|a\rangle} |\langle a,\ldots,a|X|b,\ldots,b\rangle|$. The fact that for positive operators

$$2|\langle\alpha|P|\beta\rangle| \leq \langle\alpha|P|\alpha\rangle + \langle\beta|P|\beta\rangle \leq 2\max\{\langle\alpha|P|\alpha\rangle, \langle\beta|P|\beta\rangle\}$$

holds for arbitrary $|\alpha\rangle$ and $|\beta\rangle$ proves that $\hat{G}(X) \leq \hat{G}_{\mathcal{S}}(X)$, hence $\hat{G}(X) = \hat{G}_{\mathcal{S}}(X)$.

(ii) We say that an N-qubit operator X contains only full correlation terms if $X = \sum_{i,j,\ldots\in\{x,y,z\}} \lambda_{ij\ldots}\sigma_i \otimes \sigma_j \otimes \cdots$. Note that here $\sigma_0 = \mathbb{1}$ does not occur; a physically relevant and well known example for such an operator X is the Mermin inequality. As X is permutationally invariant, λ is equivalent to a symmetric N-linear form over $\mathbb{R}^3$. The Bloch representation for qubits implies that here the maximization is equivalent to finding $\max_{r_i\in\mathbb{R}^3} |\lambda(r_1, r_2, \ldots, r_N)|$ where the vectors r_i are the corresponding Bloch vectors. Since the polarization constant for real Hilbert spaces is 1 [40, 82, 91], the assertion follows. □

Putting together Lemma III.1.3 and the relation between the geometric measure of a state and its purification given in [90, Theorem 1], Corollary III.1.6 (i) can be improved to the following theorem.

Theorem III.1.7 ([196])**.** *The closest product state to any N-partite (pure or mixed) symmetric state is necessarily symmetric if $N \geq 3$.*

Now we give some examples where symmetry assumptions do not hold. If X is symmetric but not positive, then the maximum $\hat{G}(X)$ is, in general, not attained by a symmetric state. A counterexample for two qubits is $X = 6|\psi^+\rangle\langle\psi^+| - |00\rangle\langle 00| - 2|11\rangle\langle 11|$ with $|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$. Then $\hat{G}(X) = 3$ (we can take $|\phi_0\rangle = |01\rangle$) while the maximum for symmetric product states is 34/15. Also, if X is permutationally invariant (and even positive) then the maximum $\hat{G}(X)$ is, in general, not attained by a symmetric state. A

counterexample is the singlet state, $X = |\psi^-\rangle\langle\psi^-|$ with $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. This operator is invariant under permutation of the particles, but it does not act on the symmetric space. It has $\hat{G}(X) = 1/2$, but restriction to the symmetric $|\phi\rangle$ would yield again $\hat{G}(X) = 0$. This clarifies some questions raised in Ref. [54].

Finally we would like to note that for a fixed number of parties finding the closest symmetric product state is in the same complexity class as finding the closest product state. This problem, even for tripartite states, is known to be NP-hard [76], and it is connected to a wide range of different complexity problems [6, 66]. Thus, although our result is a simplification of the computations for symmetric states, there is no asymptotical gain over general states. The reduction from one problem to the other follows from the following chain of equalities.

Given a tripartite pure state $|\psi\rangle \in \mathbb{S}(\mathbb{C}^d)$ we express its closest product state as the norm of its associated trilinear form ψ over $\mathbb{C}^d$ then

$$\begin{aligned} G(\psi) &= \max\{\psi(\alpha,\beta,\gamma) : \alpha,\beta,\gamma \in \mathbb{S}(\mathbb{C}^d)\} \\ &= 3\sqrt{3}\max\{a\cdot b\cdot c\cdot\psi(\alpha,\beta,\gamma) : a^2+b^2+c^2 = 1, \alpha,\beta,\gamma \in \mathbb{S}(\mathbb{C}^d)\} \\ &= 3\sqrt{3}\max\{\psi(\alpha,\beta,\gamma) : a^2+b^2+c^2 = 1, \alpha \in a\cdot\mathbb{S}(\mathbb{C}^d), \beta \in b\cdot\mathbb{S}(\mathbb{C}^d), \gamma \in c\cdot\mathbb{S}(\mathbb{C}^d)\} \\ &= 3\sqrt{3}\max\{\psi(\alpha,\beta,\gamma) : (\alpha,\beta,\gamma) \in \mathbb{S}(\mathbb{C}^{3d})\}, \end{aligned}$$

where now ψ can be seen as a cubic homogeneous polynomial over $\mathbb{C}^{3d}$. Associated to it there is a symmetric trilinear form $\hat{\psi}$ over $\mathbb{C}^{3d}$. Now, this form can be seen as a tripartite symmetric pure state $|\hat{\psi}\rangle \in (\mathbb{C}^{3d})^{\otimes 3}$ (probably not normalized). Thus,

$$G(\psi) = 3\sqrt{3}G(\hat{\psi}).$$

The closest product states for both $|\psi\rangle$ and $|\hat{\psi}\rangle$ not only are in one to one correspondence, but each one can be recovered efficiently from the other.

III.2 Multipartite maximally entangled states in symmetric scenarios

In this section we present a state that trivially fulfills Assumptions 1 and 2 and can be transformed into any other state fulfilling them. This property justifies that we call it "multipartite maximally entangled state". Moreover, we show that it can be used for teleportation. We also discuss further properties of the state in Section III.2.1 and show, in Section III.2.2, how the participants can impose the symmetry on their state, that is, they can be sure that their state fulfills Assumption 1.

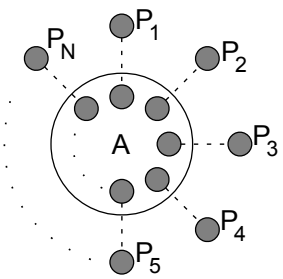

Figure III.1: Valence-bond representation of the maximally entangled state Φ. Solid circles connected with dotted lines denote virtual Einstein-Podolski-Rosen pairs; the big circle represents the projection in the Hilbert space $\mathcal{H}_{\text{sym}}$ of the authority.

The unnormalized state can be described in a valence bond picture in the following way (see Fig. III.1). Assume that we have singlets shared between any participant and the authority. Then we project the virtual space of the authority in the permutationally symmetric subspace, which is $N+1$ dimensional. That is, we project onto the space of total spin $N/2$. This can be seen as a star-shaped version of the famous AKLT state [1]. Expressed as a formula, our unnormalized state will be:

$$|\Psi\rangle = (P_{\text{sym}} \otimes \mathbb{1}_P)(|01\rangle - |10\rangle)^{\otimes N}.$$

Since we can transform the singlet to any other maximally entangled state using a local unitary in any participant qubit, we can assume the same construction starting with $|00\rangle + |11\rangle$, and we will call the resulting state $|\Phi\rangle$. In most parts of the rest of this chapter we will use the latter state. In this particular case, by considering the usual basis in the space of the authority, that is, $|\alpha\rangle = \sum_{\substack{i_1,\ldots,i_N \\ i_1+\ldots+i_N=\alpha}} \frac{1}{\sqrt{\binom{N}{\alpha}}} |i_1, \ldots, i_N\rangle$, we get the following explicit formula for $|\Phi\rangle$:

$$|\Phi\rangle = \sum_{\alpha=0}^{N} \sum_{\substack{i_1,\ldots,i_N \\ i_1+\ldots+i_N=\alpha}} \frac{1}{\sqrt{(N+1)\binom{N}{\alpha}}} |\alpha\rangle_A |i_1, \ldots, i_N\rangle_P. \tag{III.3}$$

Of course, this implies that $|\Phi\rangle = \frac{1}{\sqrt{N+1}} \sum_\alpha |\alpha\rangle_A |\alpha\rangle_P$ and therefore $|\Phi\rangle$ is the maximally entangled state along the bipartite cut AP. The problem now is that the set of participants P is delocalized and therefore one cannot use general quantum operations $\mathbb{E}$ in P, but only those that are of the form $\mathbb{E}_1 \otimes \cdots \otimes \mathbb{E}_N$. However, in many situations, since $V \mapsto V^{\otimes N}|_{H_{\text{sym}}}$ is an irrep of $\mathcal{SU}(2)$, Schur's lemma enables us to reduce to this situation. As we will see below, the price is the need for general POVMs, since von Neumann measurements are no longer sufficient. In any case, the state $|\Phi\rangle$ is also maximally entangled

in this more restrictive scenario, since one can construct from it any state with the same symmetry using only LOCC. This is the content of the following theorem.

Theorem III.2.1. *There is a LOCC protocol, given below, with one way communication that allows the authority to transform $|\Phi\rangle$ to any known pure state $|\varphi\rangle$ that is permutationally symmetric in the Hilbert space of the participants.*

Transformation protocol.

1. Let the Schmidt decomposition of the state $|\varphi\rangle = \sum_{i=0}^{N} \lambda_i |i\rangle_A |\varphi_i\rangle_P$. The authority A measures with measurement operators $\{F_U = \sqrt{N+1}\pi(U) \sum_{i=0}^{N} \lambda_i |\varphi_i^*\rangle\langle\varphi_i^*|\pi(U^\dagger)\}$ its part of the system (where $*$ means complex conjugation), the U's are distributed with respect to the Haar measure in $\mathcal{SU}(2)$, and π is the (unique) irrep of $\mathcal{SU}(2)$ in an $(N+1)$-dimensional space given by $V \mapsto V^{\otimes N}|_{\mathcal{H}_{\text{sym}}}$.
2. A broadcasts the result of the measure U_0.
3. Each participant applies to its system the unitary $YU_0^\dagger Y$ to obtain the state $|\varphi\rangle$.

This theorem shows also that our state could be of use in situations (like secret sharing or key distribution) in which one authority is assumed to distribute some quantum state among the set of participants. One advantage now is that only permutationally symmetric states can be constructed and all the participants are then sure that they are treated on an equal footing.

Proof of Theorem III.2.1. The result relies essentially on Schur's lemma, which guarantees that the measure in step 1 of the protocol is indeed a measure since

$$\frac{1}{N+1}\mathbb{1}_{H_A} = \int_{\mathcal{U}(2)} \pi(U)\rho^*\pi(U^\dagger)dU \ , \tag{III.4}$$

where $\rho^* = \sum_{i=0}^{N} \lambda_i^2 |\varphi_i^*\rangle\langle\varphi_i^*|$.

It only remains to show that the state after the protocol is the one we want, which is a routine calculation. Suppose the result of the measure is α; then the state after the measure reads

$$\left(\pi(U_\alpha)\sum_{i=0}^{N} \lambda_i |\varphi_i^*\rangle\langle\varphi_i^*|\pi(U_\alpha^\dagger) \otimes \mathbb{1}_P\right)|\Phi\rangle. \tag{III.5}$$

Now, by the definition of π and the fact that $|00\rangle + |11\rangle$ is $U \otimes YUY$ invariant for any $U \in \mathcal{U}(2)$, we get that $\pi(U) \otimes (YUY)^{\otimes N}|\Phi\rangle = |\Phi\rangle$ for every U. Using (III.3) it is now

trivial to conclude that (III.5) is indeed equal to

$$[\pi(U_\alpha) \otimes (YU_\alpha Y)^{\otimes N}] \sum_{i=0}^{N} \lambda_i |\varphi_i^*\rangle_A |\varphi_i\rangle_P. \tag{III.6}$$

Therefore, once the result α is known, each participant can apply $YU_\alpha^\dagger Y$ to its system to obtain the joint state $|\varphi\rangle$ and A can apply the unitary that takes $\pi(U_\alpha)|\varphi_i^*\rangle$ to $|i\rangle$. □

Considering $|\varphi\rangle$ to be a product state between the authority and the participants we have the following corollary.

Corollary III.2.2 (State-transfer). *Given $|\Phi\rangle$, there is a LOCC protocol, given below, with one-way communication that allows the authority to create in the Hilbert space of the participants any permutationally symmetric pure state $|\varphi\rangle$.*

The first thing to notice here is that the measurement required in step 1 of the state-transfer protocol has an infinite number of outcomes, which in turns implies that one needs an infinite-dimensional ancilla in order to implement it with orthogonal projectors. The way around this problem is by considering a set of unitaries $\{U_i\}_{i=1}^k \subset \mathcal{U}(2)$ and a set of scalars $\omega_i \geq 0$ such that $\sum_i \omega_i = 1$ and

$$\sum_{i=1}^{k} \omega_i \pi(U_i) \rho^* \pi(U_i^\dagger) = \int_{\mathcal{SU}(2)} \pi(U) \rho^* \pi(U^\dagger). \tag{III.7}$$

This allows one to replace the measurement in step 1 of the protocol by the one with operators $\{F_i = \sqrt{\omega_i(N+1)}\pi(U_i) \sum_{j=0}^{N} \lambda_j |\varphi_j^*\rangle\langle\varphi_j^*|\pi(U_i^\dagger)\}$. Using Caratheodory's theorem it is not difficult to show that, in this case, k can indeed be taken $\leq (N+1)^2 + 1$ and hence polynomial in N.

Theorem III.2.3 (Caratheodory's theorem [18])**.** *Let $\mathcal{H} \subset \mathbb{R}^d$ and $x \in co(\mathcal{H})$, there exists a set $\mathcal{A} \subset \mathcal{H}$ of at most $d+1$ elements such that $x \in co(\mathcal{A})$*

Lemma III.2.4. *Given a density matrix $\rho \in Herm(\mathcal{H}_{\text{sym}})$ there exists a set of unitaries $\{U_i\}_{i=0}^{(N+1)^2} \subset \mathcal{U}(2)$ and a set of scalars $\omega_i \geq 0$ such that $\sum_i \omega_i = 1$ and*

$$\sum_{i=0}^{(N+1)^2} \omega_i \pi(U_i) \rho \pi(U_i^\dagger) = \int_{\mathcal{SU}(2)} \pi(U) \rho \pi(U^\dagger)$$

Proof. Let $T : \mathcal{U}(2) \to \text{Herm}(\mathcal{H}_{\text{sym}})$ be defined by $U \to T_U$ where $T_U = U^{\otimes N} \rho U^{\otimes N\dagger}$. Let $S \in \text{Herm}(\mathcal{H}_{\text{sym}})$ be the result of applying the twirling operator to ρ, that is, $S :=$

$\int_{U\in\mathcal{U}(2)} U^{\otimes N}\rho U^{\otimes N\dagger}dU$. We have shown in (III.4) that $S = \frac{1}{N+1}\mathbb{1}_{\mathcal{H}_{\text{sym}}}$. Let h be a linear functional of $\text{Herm}(\mathcal{H}_{\text{sym}})$ whose positive closed half space contains $\text{Im}(T)$; then

$$h(S) = \int_{U\in\mathcal{U}(2)} h(T_U)dU \geq 0,$$

so $h(S) \in \overline{co}[\text{Im}(T)]$. Moreover, if $\text{Im}(T) \nsubseteq ker(h)$ then there is an $\epsilon > 0$ such that $\text{Im}(T)$ meets $h^{-1}[(\epsilon,\infty)]$. So the set $V = (h\circ T)^{-1}((\epsilon,\infty))$ of $\mathcal{U}(2)$ is nonvoid and, by the continuity of T, open. Therefore $h(S) > \epsilon\mu(V) > 0$. Hence

$$S \in \text{ri}(co[\text{Im}(T)]) \subseteq co[\text{Im}(T)],$$

where $\text{ri}(\mathcal{A}) = \{a \in \mathcal{A} : \exists\epsilon > 0, B(x,\epsilon)\cap \text{aff}(\mathcal{A}) \subseteq \mathcal{A}\}$ is the relative interior of $\mathcal{A}$, that is, the interior within the affine hull of $\mathcal{A}$. Then, applying Caratheodory's theorem III.2.3, there exist unitaries $U_0, U_1, ..., U_{(N+1)^2} \in \mathcal{U}(2)$ such that $S \in co\{T_{U_0}, T_{U_1}, ..., T_{U_{(N+1)^2}}\}$. That is, there exist $\omega_i \geq 0$, $U_i \in \mathcal{U}(2)$ for $i = 0, ..., (N+1)^2$ such that $\sum_i \omega_i = 1$ and

$$\frac{tr(A)}{N+1}\mathbb{1}_{\mathcal{H}_{\text{sym}}} = \sum_{i=0}^{(N+1)^2} \omega_i U_i^{\otimes N}\rho U_i^{\otimes N\dagger}.$$

□

Since in step 2, the authority will broadcast the outcome of the measurement, it is interesting to note that, from (III.6), the probability of obtaining the output i is ω_i and hence independent of the state $|\varphi\rangle$ being transferred. This is crucial in cryptographic applications, like secret sharing, in which the public communication should give no information at all. The main problem with this state-transfer protocol is that the measurement in A, although it is local, depends on the state to transfer, and therefore it does not work in situations in which the authority wants to transfer an unknown state. However, thanks to Schur's lemma, it is possible to design a teleportation-like protocol that also works under our assumptions and allows A to teleport with LOCC any permutationally symmetric unknown state to P. The procedure is a particular case of the situation described in [13] and can be summed up in the following protocol.

Teleportation-like protocol

1. The initial joint system is $|\varphi\rangle_{A_1} \otimes |\Phi\rangle_{A_2P}$, where $|\varphi\rangle$ is the state to be teleported.
2. The authority A measures with measurement operators $\{F_U = (N+1)(\pi(U)_{A_1} \otimes \mathbb{1}_{A_2})|\Phi\rangle\langle\Phi|(\pi(U^\dagger)_{A_1} \otimes \mathbb{1}_{A_2})\}$ its part of the system, where the U's are distributed with respect to the Haar measure in $\mathcal{U}(2)$.
3. A broadcasts the result of the measure U_0.
4. Each participant applies to its system the unitary U_0 to obtain the state $|\varphi\rangle$.

Exactly as before, one can use a discrete set of unitaries to avoid the continuous parameter. In this case Eq. (III.7) should hold for any matrix $\rho \in \mathcal{M}_{N+1}$. By a similar reasoning one can show that the number of unitaries needed is upper bounded by $4(N+1)^4 + 1$. Nevertheless, weighted N-designs in $\mathcal{U}(2)$ already solve this problem and such a design exists with $\leq \binom{2N+3}{3}$ unitaries [149]. Likewise, not only is the output of the measurement completely independent of the state to be teleported, but also the set of unitaries itself. Finally, it is trivial to see that the same protocol allows one to teleport arbitrary unknown mixed states supported on the symmetric subspace.

In light of this result, it seems that if we restrict ourselves to our Assumptions 1 and 2 everything works essentially as in the bipartite case, in which we start with the maximally entangled state $|\Phi\rangle = \sum_\alpha |\alpha\rangle_A|\alpha\rangle_P$. As we commented above, there is at least one important difference. In the protocols presented here we use POVMs instead of von Neumann measurements. It is interesting to note that it is indeed *impossible* to reduce the protocol to von Neumann measurements, as is shown in the following theorem.

Theorem III.2.5. *It is not possible to implement the teleportation-like protocol using von Neumann measurements.*

Proof. Let us assume that it is possible to teleport from A to P the unknown permutationally symmetric state $|\varphi\rangle$ with von Neumann measurements. It implies that there must exist a decomposition of the form

$$|\varphi\rangle_{A_1}|\Phi\rangle_{A_2P} = \sum_{r\in R} \sqrt{p_r}|r\rangle_A \otimes \pi(U_r)|\varphi\rangle,$$

where $|r\rangle$ is an orthonormal set in the joint system $A = A_1A_2$. On one hand, if we trace out system A we get $\mathbb{1}_{H_{\text{sym}}} = \sum_r p_r \pi(U_r)|\varphi\rangle\langle\varphi|\pi(U_r)^\dagger$, which implies that $|R| \geq N+1$. On the other hand, suppose we trace out system P, we get $|\varphi\rangle\langle\varphi| \otimes \mathbb{1}_{\mathcal{H}_{\text{sym}}} =$

$\sum_{r,s\in R}\sqrt{p_r p_s}\langle\varphi|\pi(U_s^\dagger U_r)|\varphi\rangle|r\rangle\langle s|$, which implies that

$$\mathbb{1}_{\mathcal{H}_{\rm sym}\otimes\mathcal{H}_{\rm sym}} = \sum_{r,s}\sqrt{p_r p_s}\,\mathrm{tr}(U_s^\dagger U_r)^N|r\rangle\langle s|$$

and hence $\mathrm{tr}(U_s^\dagger U_r)=\delta_{rs}$. But this is not possible since $U_r, U_s \in \mathcal{U}(2)$. □

III.2.1 Properties of the state

Characterization by symmetries.

Just as the state $|00\rangle+|11\rangle$ can be characterized as the unique pure two-qubit state that is invariant under the action of $U\otimes U$ for any unitary U, one can show that our state $|\Phi\rangle$ is the unique pure state, within assumptions 1 and 2, that is invariant under the action of $U^{\otimes N}\otimes\pi(YUY)$ for any unitary $U\in\mathcal{U}(2)$, where π is the (unique) unitary irrep of $\mathcal{SU}(2)$ in an $(N+1)$-dimensional space given by $V\mapsto V^{\otimes N}|_{\mathcal{H}_{\rm sym}}$.

Creation of the state.

Is there an efficient way, that is, polynomial in the parameters, to construct the maximally entangled state $|\Phi\rangle$? The answer is yes and comes from the following OBC-MPS representation:

$$|\Phi\rangle = \sum_{\alpha_0,i_1,\ldots,i_N} A^{[0]}_{\alpha_0}A^{[1]}_{i_1}\cdots A^{[N]}_{i_N}|\alpha_0 i_1\cdots i_N\rangle,$$

where

$$A^{[0]}_{\alpha_0} = (0,\ldots,0,\underset{\alpha_0}{1},0,\ldots,0),$$
$$A^{[j]}_{i_j} = \sum_{\alpha_j=0}^{N-j}\frac{\sqrt{(N-j+1)\binom{N-j}{\alpha_j}}}{\sqrt{(N-j+2)\binom{N-j+1}{\alpha_j+i_j}}}|\alpha_j+i_j\rangle\langle\alpha_j|,\ j=1,\ldots,N.$$

Using the efficient sequential generation of a OBC-MPS II.6. Thus,

$$|\Phi\rangle_{AP}|0\rangle_a = V_{[0]}\cdots V_{[N]}|0\cdots 0\rangle_{AP}|0\rangle_a,$$

where a is an ancillary system of dimension $N+1$ and $V_{[j]}$ is the unitary gate of II.6, involving only participant j (0 being the authority) and the ancilla a (see Fig. II.3). Of course, one may take the authority system as the ancilla and then obtain the state $|\Phi\rangle$ after one round of two-body interactions between the authority and each participant.

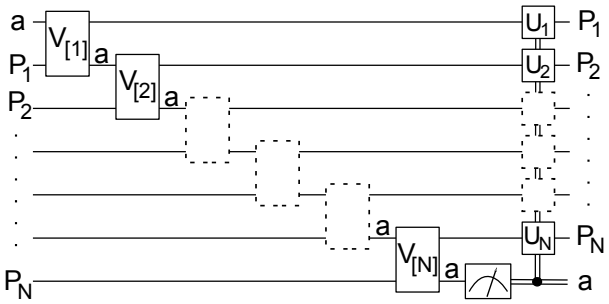

Figure III.2: Sequential circuit implementing cloning. First, the maximally entangled state is created sequentially between the ancilla and the participants. Second, the ancilla is measured. Finally, depending on the result of the measurement, local unitary corrections are applied to the participants.

Sequential cloning.

The fundamental no-cloning theorem [194] states that it is impossible to clone unknown quantum states. However, as one can infer from the excellent review [152], there are many situations in cryptography in which the optimal approximate cloning is important. In [38] (see [100] for a refinement), the authors use MPS theory to design a protocol which implements the $1 \to N$ symmetric universal quantum cloning in the following sequential manner (see Fig. IV.6):

Sequntial cloning protocol.

1. An ancilla of dimension $O(N)$ interacts sequentially with each qubit.
2. A final measurement is implemented in the ancilla.
3. A local unitary correction is made in the qubits depending on the output of the measurement.

Since in the symmetric universal cloning the final state is supported in the symmetric subspace, one can use step 1 to create our maximally entangled state and steps 2 and 3 to teleport the cloned state to all the qubits with our teleportation-like protocol. Of course, the same can be done for *any* protocol in which the final state lies in the symmetric subspace.

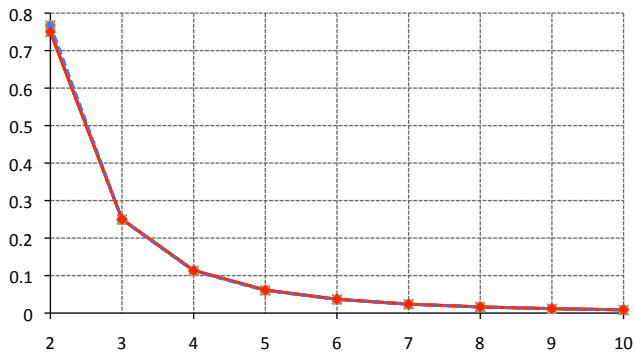

Figure III.3: Distance between the first and second eigenvalues of the channel T as a function of the number of participants (green line) compared with the values of its regression function when considering a power regression model (red dashed line). The exponent of the function is -2.77.

III.2.2 Checking symmetry.

Since the participants want to keep their privacy, they must have a way to be sure that the state they receive from the authority is permutationally symmetric or, even more, is supported in the symmetric subspace. The latter is indeed equivalent to implementing the measure of the total spin in N spin-$\frac{1}{2}$ particles. A simple way to do so is the following protocol which requires very little computational power in the participants: a one-qubit channel from participant i to participant $i+1$ and the ability to implement two-qubit measurements. The protocol aims to (i) do nothing if the original state was supported on the symmetric subspace, and (ii) end up with a state supported on the symmetric subspace.

The protocol consists of repeating the following round R times. With probability $1/N$, participant i sends its qubit to participant $i+1$, which checks if the $(i, i+1)$ qubits are supported in the symmetric or the antisymmetric subspace. If it is the latter, participant $i+1$ constructs the mixed state over the symmetric subspace and sends the i-th qubit back to participant i.

The quantum channel implemented is $T = 1/N \sum_{i=1}^{N} T_{i,i+1} \otimes \mathbb{1}_{All \setminus i,i+1}$ where $T_{i,i+1}(\rho) = P_{\text{sym}} \rho_{i,i+1} P_{\text{sym}} + 1/4 \langle \Psi_- | \rho_{i,i+1} | \Psi_- \rangle \mathbb{1}$. It is clear that this channel verifies (i). (ii) is a consequence of the fact that all fixed points of Φ are supported in the symmetric subspace. To see this we rely on [172], in which the fixed points are characterized as those matrices ρ that are fixed points of $T_{i,i+1}$ for any $i = 1, ..., N$; these are density matrices that are supported in the symmetric subspace of any pair of consecutive participants.

The efficiency of the protocol, that is, how it approaches a fixed point with the number

of iterations is governed by the modulus of the second largest eigenvalue of T. Numerically (see Fig. IV.7) the second eigenvalue of the protocol after $O(N^3)$ rounds seems to behave as $(1 - cN^{-2.77})^{O(N^3)}$, where c is a constant, which is exponentially small in N.

Alternatively one can use the general procedures concerning secure multipartite quantum computation in [8, 30].

III.3 Discussion

We have studied entanglement in the set of permutation symmetric N-partite states both from a quantitative and a qualitative point of view.

From the quantitative point of view, we have discussed a widely used conjecture concerning the geometric measure of entanglement. Our results not only simplify the calculation of the geometric measure for symmetric states (numerical computations of N-qubits states with highest geometric entanglement has been done in [3, 113]), but they also have applications to subjects in condensed matter physics.

Furthermore, from a mathematical perspective, the quantity G, as defined in Eq. III.1, is known as the injective tensor norm [37]. On the one hand, this norm is of central importance in tensor analysis [61]. On the other hand, this norm has also occurred in the discussion of the maximal output purity of quantum channels [188].

Moreover, these quantities have been recently connected with other problems. The geometric entanglement has been the first multipartite entanglement measure to be related with topological order of 2D systems [127]. The injective tensor norm has been related to problems in complexity theory, such as the quantum version of the NP class [66] and with the unique game conjecture, about the complexity of approximating the value of certain games, widely studied in the area [6].

We have also discussed generalizations of our result to operators of higher rank. For this operators the maximum separation between the value $\hat{G}(X)$ and its symmetric counterpart $\hat{G}_S(X)$ is given by the N-th polarization constant of $\mathfrak{H}_1^d$. A simple argument allow us to compute this constant for $N \leq d$. Nevertheless, we pose the question of how big this quantity can be for $d > N$. Up to our knowledge, this mathematical quantity was of no previous interest.

From the qualitative point of view, we have considered the set of symmetric multipartite states shared between the participants and whose state is purified by the authority. Among this set we find a maximally entangled state which, thanks to Schur's lemma, can be transformed into any other and makes it possible to make teleportation from the authority to the participants. Nevertheless, POVMs are needed for both applications. We have shown how to create this maximally entangled state sequentially in an efficient way thanks to its Matrix Product State representation. Putting together the sequential gen-

eration and the teleportation result, we recover an alternative proof of the fact that any protocol in which the final state lives in the symmetric subspace can be done sequentially in an efficient way. This is illustrated with the $1 \to N$ symmetric universal quantum cloning. Moreover, we have argued that the result of the measures in the protocols does not reveal information and that the participants can make sure that their state lives in the symmetric subspace. Although we have described many interesting good properties of the maximally entangled state and it can be used in several protocols, we would like to find different cryptographic applications of it.

Chapter IV

MPS and Symmetry

It has already been justified in Section II.2 that ground states of gapped local 1D Hamiltonians are exactly represented by the set of MPSs with *polynomial* bond dimension. For 2D MPSs, the so called PEPSs [1, 110, 123, 168, 170], the same result seems to hold [169] and has been formally proven under an assumption on the density of Hamiltonians's eigenstates [70]. This representation for ground states of 2D local Hamiltonians turns the problem of understanding 2D quantum many body systems into the question: How can one characterize the different phases of matter in terms of the tensors defining a PEPS?

Though there are known examples of PEPSs with topological order [16, 173], power law decay of correlations [173], $SU(2)$-symmetry [1, 148], or universal power for measurement based quantum computation [58, 59, 173], characterizing these phases has turned out to be a daunting task. In this chapter we provide a simple characterization of the existence of symmetries (both local and spatial) as a trivial consequence of the fact, which we call canonical form, that two injective PEPSs describing the same translational invariant state in a square lattice are related by invertible matrices in the virtual spins, as in Fig. IV.1.

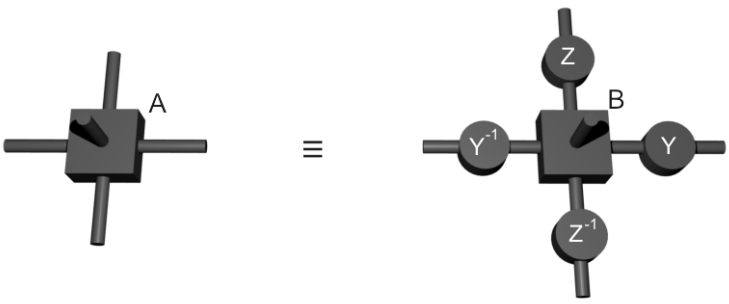

Figure IV.1: This is the Canonical Form for PEPSs, i.e., the relation that holds between the tensors which define the PEPSs when they represent the same state.

This simple characterization illuminates the restrictions that symmetries impose on quantum systems. For instance one can in this context understand the validity of the Lieb-Shultz-Mattis theorem in arbitrary dimensions [67, 104, 118], as well as its $U(1)$ generalization due to Oshikawa, Yamanaka and Affleck [128] (originally only in the 1D case). We can also understand why and how three of the main indicators of topological order, namely degeneracy of the ground state, existence of Wilson loops and correction to the area law, are related. Moreover, it has been proven in [134] that the existence of symmetries in increasing sizes of the system gives the appropriate definition of string order in 2D, overcoming the drawbacks sketched in [2]. The importance of string orders in the study of quantum phase transitions, may vaticinate interesting applications in the future along this direction.

Relations to prior work. The results in this chapter generalize to higher dimensions, and in particular to PEPSs, the following results for MPSs. In [131, 175] a canonical form for MPS was derived (Theorem II.2.3). This was used in [134] to prove that the existence of a string order is equivalent to the existence of a local symmetry for TI injective MPSs. Moreover, the authors proved that the symmetry properties of a TI injective MPS are determined by the symmetry properties of the tensor defining the MPS. This result was generalized to non injective TI-MPSs in [151] and used to recover a version of the Lieb-Shultz-Mattis theorem, which states that MPSs with an $\mathcal{SU}(2)$ symmetry and even physical dimension d cannot be injective.

The rest of the chapter is organized as follows. First, we introduce PEPSs, the generalization of MPS to 2D (Section IV.1). Then, in order to prove the canonical form for PEPSs, (Section IV.3), we need to have independence of the bond dimension in the statement of the canonical form for MPSs (Theorem II.2.3). We prove this theorem in Section IV.2. The immediate consequences of this canonical form for PEPSs will be given in Section IV.4, we will see how to characterize the local and spatial symmetries of a PEPS in terms of the symmetries of the tensor defining it. As first applications of this characterization, in Section IV.5, we recover a generalized Lieb-Shultz-Mattis theorem and prove a necessary condition for the existence of Wilson loops. We finally conclude with a discussion of the results in Section IV.6.

IV.1 Projected Entangled Pair States

PEPSs are the natural extension of the MPS beyond the 1D case, where the *projection* is performed from a larger number of virtual Hilbert spaces depending on the co-ordination number of the lattice (the square lattice, for instance, has four virtual Hilbert spaces). Therefore, the local *building blocks* are tensors instead of matrices which implies that most calculations become much harder [156].

Let us consider an $L \times N$ square lattice of spins of dimension d. A PEPS consists on

a tensor A^i_{ldru} with 5 indices: i corresponding to the physical spin of dimension d and l, d, r, u (left, down, right, up) corresponding to four virtual spaces of dimensions (*bonds*) D_1 and D_2, as we did for MPS. The connections between two sites are again performed by means of maximally entangled states $|\Omega\rangle = \sum_\alpha |\alpha\alpha\rangle$. Then, the shape of these states is

$$|\phi_A\rangle = \sum_{i_1,\ldots,i_{NL}} \mathcal{C}(A^i_{ldru})|i_1 \ldots i_{NL}\rangle$$

where $\mathcal{C}$ means the contraction of all tensors A^i_{ldru} along the square lattice.

Associated to any PEPS $|\phi_A\rangle$ we can define a parent Hamiltonian H_A [132], which is locally defined by the projector onto range$(\Gamma_R)^\perp$, where $\Gamma_R : X \longrightarrow \mathcal{C}(XA^R)$ takes a boundary condition X to the state defined by contracting the indices in the boundary condition with the open virtual indices in region R. It is clear that $|\phi_A\rangle$ is a ground state for H_A and that it minimizes the energy locally, that is, H_A is frustration free. In the case of 1D it is proven in [46, 131] that a MPS is injective if and only if $|\phi_A\rangle$ is the unique ground state of H_A.

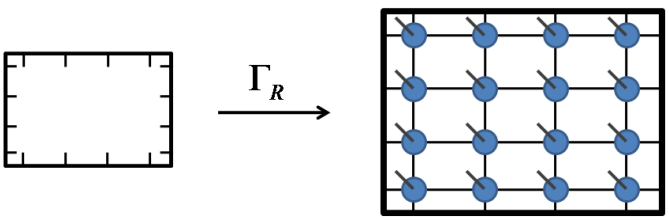

Figure IV.2: A PEPS is injective in a region R if Γ_R is injective, that is, if different boundary conditions give rise to different states in R.

We can define the injectivity property for PEPSs in the same way that we have done for MPS in Definition II.2.1 (see Fig. IV.2). That is, the PEPS $|\phi_A\rangle$ is injective in a region R if the map Γ_R is injective. As in the 1D case (Lemma II.2.2) one could look at injectivity as the possibility of producing any tensor X on the boundary by contracting with a particular state $\langle a_X|$ in the physical indices (see Fig. IV.3). This argument will be repeatedly used throughout Sections IV.3 and IV.4. It is also clear that injectivity is a generic condition.

In the applications we will give below (Lieb-Shultz-Mattis, Wilson loops), the conclusion will often be that a given PEPS is not injective. What does this mean? As we list below, injectivity is closely related to uniqueness of the ground state of the parent Hamiltonian and to the saturation of the area law for the 0-Rényi entropy.

Figure IV.3: A PEPS is injective in a region R if any tensor X of the systems in the boundary can be attained by contracting with a state in the physical indices.

1. If a PEPS is injective, it is the unique ground state of its parent Hamiltonian [132].
2. If a PEPS is not-injective for any cylinder-shape region, any local frustration free Hamiltonian for which the given PEPS is a ground state has a degenerate ground space, as long as we grow one of the directions exponentially faster than the other. This is a trivial consequence of the 1D case [131].
3. The 0-Rényi entropy of the reduced density matrix ρ_R of a region R of a PEPS with bond dimension D is $\leq |\partial R| \log D$. It is easy to see that if $S_0(\rho_R) = |\partial R| \log D$, then the PEPS is injective. That is, if a PEPS is not injective, there is a *correction* to the area law for the 0-Rényi entropy.

In the rest of this chapter we will be using the following notation. If R is a region of the considered lattice underlying the PEPS, we denote by A^R the joint tensor obtained after contracting all the tensors inside region R.

IV.2 The canonical form for MPS

Theorem II.2.3 shows that two injective representations of the same MPS must be related by an invertible matrix R and a phase θ as $A_i = e^{i\theta} R B_i R^{-1}$. This holds if the number of sites satisfies $N \geq 2L_0 + D^4$, where L_0 is the size from which on one has injectivity and D is the bond dimension of the MPS. Since we are interested (see the argument in Theorem IV.3.1 below) to apply this to a "column" of a PEPS, the exponential dependence on D would be critical. So in this section, we modify the proof of Theorem II.2.3 given in [131, Theorem 6] to make N depend on L_0 only. In particular, we obtain that the result holds when $N \geq 4L_0 + 1$.

Theorem IV.2.1. *Let*

$$|\psi_A\rangle = \sum_{i_1,\dots,i_N=1}^{d} \mathrm{tr}(A_{i_1}\cdots A_{i_N})|i_1\cdots i_N\rangle$$

and

$$|\psi_B\rangle = \sum_{i_1,\dots,i_N=1}^{d} \mathrm{tr}(B_{i_1}\cdots B_{i_N})|i_1\cdots i_N\rangle$$

be translational invariant MPS representations with bond dimension D which are injective for regions of size L_0. Then, if $|\psi_A\rangle = \lambda|\psi_B\rangle$ with $\lambda \in \mathbb{C}$ and $N \geq 4L_0 + 1$, there exists an invertible matrix R and $\mu \in \mathbb{C}$ such that $A_i = \mu R B_i R^{-1}$, for all i and $\mu^N = \lambda$.

Proof. We can obtain an OBC representation by noticing that

$$|\psi_A\rangle = \sum_{i_1,\dots,i_N=1}^{d} a_{i_1}^{[1]}(A_{i_2}\otimes \mathbb{1})\cdots(A_{i_{N-1}}\otimes \mathbb{1})a_{i_N}^{[N]}|i_1\cdots i_N\rangle$$

where $a_i^{[1]}$ is the $1\times D^D$-dimensional vector that contains all the rows of A_i, $a_i^{[N]}$ is the $D^D\times 1$-dimensional vector that contains all the columns in A_i, and $\mathbb{1}$ is the identity matrix of dimension $D\times D$. Doing the same with the B's

$$|\psi_A\rangle = \lambda|\psi_B\rangle = \sum_{i_1,\dots,i_N=1}^{d} \lambda b_{i_1}^{[1]}(B_{i_2}\otimes \mathbb{1})\cdots(B_{i_{N-1}}\otimes \mathbb{1})b_{i_N}^{[N]}|i_1\cdots i_N\rangle$$

Getting from them an OBC canonical representation (with matrices C's for the A's and matrices D's for B's) as in [131, Theorem 2] we obtain Y_j^1, Z_j^1, Y_j^2 and Z_j^2 with $Y_j^1 Z_j^1 = \mathbb{1}$, $Y_j^2 Z_j^2 = \mathbb{1}$ such that

$$\begin{gathered}
C_i^{[1]} = a_i^{[1]} Z_1^1, C_i^{[N]} = Y_{N-1}^1 a_i^{[N]} \\
C_i^{[m]} = Y_{m-1}^1 (A_i\otimes \mathbb{1}) Z_m^1 \text{ for } 1 < m < N \\
D_i^{[1]} = \lambda b_i^{[1]} Z_1^2, D_i^{[N]} = Y_{N-1}^2 b_i^{[N]} \\
D_i^{[m]} = Y_{m-1}^2 (B_i\otimes \mathbb{1}) Z_m^2 \text{ for } 1 < m < N
\end{gathered}$$

Using theorem 3.1.1' in [83], we get that any two OBC canonical representations are related by unitaries, that is, there exists $V_1, ..., V_{N-1}$ such that

$$C_i^{[1]}V_1 = D_i^{[1]}, V_{N-1}^\dagger C_i^{[N]} = D_i^{[N]}$$
$$V_{j-1}^\dagger C_i^{[j]} V_j = D_i^{[j]} \text{ for } 1 < j < N$$

Now, by using injectivity as in [131, Theorem 6], we know that Z_s^r, Y_s^r are invertible for $r = 1, 2$ and $L_0 \leq s \leq N - L_0$ and so are the $D^2 \times D^2$ matrices W_k defined as

$$W_k = Z_{L_0+k}^2 V_{L_0+k} Y_{L_0+k}^1 \;\; k = 0, ..., 2L_0 + 1.$$

It is easy to verify that for all i,

$$W_k(A_i \otimes \mathbb{1})W_{k+1}^{-1} = (B_i \otimes \mathbb{1}) \text{ for } 0 \leq k \leq 2L_0. \tag{IV.1}$$

In fact, using the multi-index $I_l = (i_1, ..., i_l)$, grouping the matrices, and denoting $A_{I_l} = A_{i_1} \cdots A_{i_l}$, we have

$$W_m(A_{I_{n-m}} \otimes \mathbb{1})W_n^{-1} = B_{I_{n-m}} \otimes \mathbb{1} \tag{IV.2}$$

for every $0 \leq m < n \leq 2L_0 + 1$ and every multi-index I_{n-m}. Then for suitable values of m and n, we obtain

$$W_{k+1}^{-1} W_k (A_{I_{2L_0-k}} \otimes \mathbb{1}) W_{2L_0}^{-1} W_{2L_0+1} = A_{I_{2L_0-k}} \otimes \mathbb{1}$$

for every $0 \leq k \leq L_0$.

As we are in an injective region for every k, the matrix could be taken as the identity and then we get that

$$T := W_{k+1}^{-1} W_k = W_{2L_0+1}^{-1} W_{2L_0} \tag{IV.3}$$

for every $0 \leq k \leq L_0$.

Therefore, $T(X \otimes \mathbb{1})T^{-1} = (X \otimes \mathbb{1})$ for every X. Let us make use of the following lemma, which is a consequence of [83, Theorem 4.4.14]:

Lemma IV.2.2. *If B, C are squares matrices of the same size $n \times n$, the space of solutions of the matrix equation*

$$W(C \otimes \mathbb{1}) = (B \otimes \mathbb{1})W$$

is $S \otimes M_n$ where S is the space of solutions of the equation $XC = BX$.

With this at hand it is easy to deduce that there exists a phase φ such that $T = (e^{i\varphi}\mathbb{1}) \otimes Z$ with $Z_{11} \in \mathbb{R}$ so that

$$W_{L_0}^{-1} W_0 = W_{L_0}^{-1} W_{L_0-1} W_{L_0-1}^{-1} \cdots W_0 = (e^{i\varphi}\mathbb{1} \otimes Z)^{L_0}$$

from where we obtain

$$W_{L_0}^{-1} = (e^{iL_0\varphi}\mathbb{1} \otimes Z^{L_0})W_0^{-1}$$

and in the same way

$$W_{L_0+1}^{-1} = (e^{i(L_0+1)\varphi}\mathbb{1} \otimes Z^{L_0+1})W_0^{-1} \ .$$

Replacing in Eq. (IV.2)

$$\begin{aligned}(B_{I_{L_0}} \otimes \mathbb{1}) &= W_0(A_{I_{L_0}} \otimes \mathbb{1})W_{L_0}^{-1} \\ &= e^{iL_0\varphi}W_0(A_{I_{L_0}} \otimes Z^{L_0})W_0^{-1} \\ (B_{I_{L_0+1}} \otimes \mathbb{1}) &= W_0(A_{I_{L_0+1}} \otimes \mathbb{1})W_{L_0+1}^{-1} \\ &= e^{i(L_0+1)\varphi}W_0(A_{I_{L_0+1}} \otimes Z^{L_0+1})W_0^{-1}\end{aligned}$$

By using injectivity of $B_{I_{L_0}}$ and $B_{I_{L_0+1}}$, we can sum with appropriate coefficients to obtain $\mathbb{1}$ on the LHS. Then, we get that $Z^{L_0} \equiv \mathbb{1} \equiv Z^{L_0+1}$, which gives $Z \equiv \mathbb{1}$. Hence $Z = x\mathbb{1}$ with $x \in \mathbb{R}$ as $Z_{11} \in \mathbb{R}$ and $W_0 = xe^{i\varphi}W_1$ from Eq. (IV.3). Substituting in Eq. (IV.1) we have

$$B_i \otimes \mathbb{1} = \frac{1}{x}e^{-i\varphi}W_0(A_i \otimes \mathbb{1})W_0^{-1} \text{ for every } i.$$

Now, by means of Lemma IV.2.2, we know that there exist matrices R and S such that $W_0 = R \otimes S$ and

$$RA_i = xe^{i\varphi}B_iR \text{ for every } i. \tag{IV.4}$$

Moreover R is invertible as so is W_0. Finally, substituting Eq. (IV.4) in $|\psi_A\rangle = \lambda|\psi_B\rangle$ we get that $x^Ne^{iN\varphi} = \lambda$ as desired. □

IV.3 The canonical form for PEPSs

In this section, we show that Theorem IV.2.1 holds in any spatial dimension: two injective representations of the same PEPS are related by the trivial gauge freedom in the bonds (Fig. IV.1).

We prove the result in 2D by using the result in 1D, and the argument can be generalized to larger spatial dimensions by induction. We will initially consider a square lattice, but we show at the end of the section how to extend the result to the honeycomb lattice.

Theorem IV.3.1. *Let $|\psi_A\rangle$ and $|\psi_B\rangle$ be two PEPSs in a $L \times N$ square lattice given by tensors $A = \sum_{i;ldru} A^i_{ldru}|i\rangle\langle ldru|$, $B = \sum_{i;ldru} B^i_{ldru}|i\rangle\langle ldru|$ with the property that for a region of size smaller than $L/5 \times N/5$ both PEPSs are injective. Then $|\psi_A\rangle = \lambda|\psi_B\rangle$ if and only if there exist invertible matrices Y, Z and $\mu \in \mathbb{C}$ such that $A^i = \mu B^i(Y^{-1} \otimes Z^{-1} \otimes Y \otimes Z)$ for all i and $\mu^{LN} = \lambda$ (Fig. IV.1). Moreover Y and Z are unique up to proportionality and μ is unique.*

The uniqueness part is a simple consequence of injectivity. Suppose there exist two sets (μ_1, Y_1, Z_1) and (μ_2, Y_2, Z_2) fulfilling the equation in Fig. IV.1, then $\mu_1 B^i(Y_1^{-1} \otimes Z_1^{-1} \otimes Y_1 \otimes Z_1) = \mu_2 B^i(Y_2^{-1} \otimes Z_2^{-1} \otimes Y_2 \otimes Z_2)$. Then, grouping to have an injective R-S region, we get that

$$\begin{aligned} \mu_1^{RS} X(Y_1^{\otimes R} \otimes Z_1^{\otimes S} \otimes Y_1^{-1\otimes R} \otimes Z_1^{-1\otimes S}) = \\ = \mu_2^{RS} X(Y_2^{\otimes R} \otimes Z_2^{\otimes S} \otimes (Y_2^{-1})^{\otimes R} \otimes (Z_2^{-1})^{\otimes S}), \end{aligned} \tag{IV.5}$$

for any matrix X. Taking $X = \mathbb{1}$, we get that $\mu_1^{RS} = \mu_2^{RS}$. In particular, taking the four cases with $R = \{L/5, L/5+1\}$ and $S = \{N/5, N/5+1\}$, summing and simplifying to get rid of the $L/5$ and $N/5$ terms, we get $\mu_1 = \mu_2$. Now, grouping tensors in Eq. IV.5 we get that $Y_1 Y_2^{-1} \otimes Z_1 Z_2^{-1}$ commutes with every matrix. Thus $Y_1 = \alpha Y_2$ and $Z_1 = \beta Z_2$ with α, $\beta \in \mathbb{C}$.

For the existence part, let us split the proof into a sequence of lemma, in order to make it clearer.

We can reduce the 2D case to the 1D case by grouping all the tensors in a column. The 1D case (Theorem IV.2.1) ensures that there is a global invertible matrix Y which verifies the equality in Fig. IV.4. Now

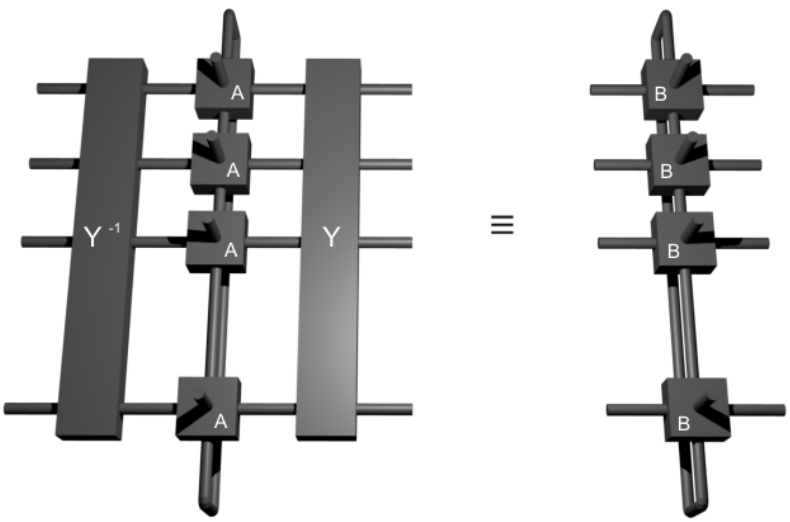

Figure IV.4: Translational invariance and injectivity allow us to reduce the 2D case to the 1D case.

Lemma IV.3.2. *Y maps product vectors into product vectors.*

We will show that Y maps any product vector to a vector with the property:

(*) *It is a product in any bipartition R-S, for regions R and S of consecutive spins and size* $\geq L/5$.

Since any vector with property (*) is trivially a product vector, this would finish the proof. So let us take a product $\otimes_i |x_i\rangle$ and assume that this product is mapped by Y into a vector that can be written in some orthonormal basis as $Y(\otimes_i |x_i\rangle) = \sum_{r=1,2,...} \beta_r |v_r w_r\rangle$ in a partition R-S for regions of consecutive spins and size $\geq L/5$. For the same bipartition, we may write $\otimes_i \langle x_i| Y^{-1} = \sum_{r=1,2,...} \alpha_r \langle v'_r w'_r|$, which could be a product. We group $N/5$ columns, sandwich with $\otimes_i |x_i\rangle$ in Fig. IV.4 and analyze the Schmidt rank between the two physical $R \times N/5$ and $S \times N/5$ systems in both the right and left part of Fig. IV.4. It clearly gives $D^{2N/5}$ in the RHS by using injectivity. By performing the changes of bases $|r\rangle \mapsto |v_r\rangle$ and $|r\rangle \mapsto |w_r\rangle$ (and the same for the primes) to the tensors $A^{R\times N/5}$ and $A^{S\times N/5}$ in the LHS, it gives new tensors A' and A'' for which we get

$$\sum_{abcd} \alpha_a \beta_c [\sum_i A'^i_{abcd} |i\rangle][\sum_j A''^j_{adcb} |j\rangle]$$

By means of injectivity, we know that the set $\{\sum_i A'^i_{abcd} |i\rangle\}_{abcd}$ is linearly independent (and the same for A''). This means that the Schmidt rank of the LHS is at least $2D^{2N/5}$, which is the desired contradiction.

The following three lemmas specify the form of Y:

Lemma IV.3.3. *If Y is invertible and takes products to products it is of the form $P_\pi(Y_1 \otimes \cdots \otimes Y_L)$ where P_π implements a permutation π of the Hilbert spaces.*

Proof. We reason for simplicity in the bipartite case—the argument generalizes straightforwardly to the general case by induction. Let $Y : \mathbb{C}^d \otimes \mathbb{C}^d \longrightarrow \mathbb{C}^d \otimes \mathbb{C}^d$ be invertible which takes products to products and denote $\{|i,j\rangle\}_{i,j=1,...,d}$ the product basis. Let $Y(|i,1\rangle) = |\alpha_i, \beta_i\rangle$. Take $i_0 \neq i_1 \in \{1,...,d\}$, then $Y(|i_0,1\rangle + |i_1,1\rangle) = |\alpha_{i_0}, \beta_{i_0}\rangle + |\alpha_{i_1}, \beta_{i_1}\rangle$ is a product and, as Y is invertible, then either I) $\alpha_{i_0} \propto \alpha_{i_1}$ & $\beta_{i_0} \not\propto \beta_{i_1}$ or II) $\alpha_{i_0} \not\propto \alpha_{i_1}$ & $\beta_{i_0} \propto \beta_{i_1}$, where $\propto$ means proportional to. In fact, we are always in the same case: if $d = 2$ there is only one case, otherwise take three distinct $i_0, i_1, i_2 \in \{1,...,d\}$ such that $\alpha_{i_0} \not\propto \alpha_{i_1}$ and $\beta_{i_1} \not\propto \beta_{i_2}$ then we get a contradiction from the fact that $Y(|i_0,1\rangle + |i_2,1\rangle)$ is a product.

The same argumentation can be carried out for the second tensor. We can therefore assume w.l.o.g. that

$$Y(|i,1\rangle) = |\alpha_i, \beta_1\rangle$$

and

$$Y(|1,j\rangle) = |\alpha_1, \beta_j\rangle$$

In the other case, we just permute the indices by means of the swap operator P_π.

Let us consider $Y(|i,j\rangle) = |a_{i,j}, b_{i,j}\rangle$. Now, since

$$Y(|i,j\rangle + |i,1\rangle) = |\alpha_i, \beta_1\rangle + |a_{i,j}, b_{i,j}\rangle$$

is a product, we obtain that $\alpha_i \propto a_{i,j}$ or $\beta_1 \propto b_{i,j}$. However, the second case is only possible if $j = 1$ because of the invertibility of Y, and then $a_{i,j} \propto \alpha_i$. A similar argumentation over the second tensor gives $Y(|i,j\rangle) = c_{i,j}|\alpha_i, \beta_j\rangle$. Now making $Y(\sum_{i,j=1}^d |ij\rangle) = \sum_{i,j=1}^d c_{i,j}|\alpha_i, \beta_j\rangle$ and knowing that the Schmidt rank of the resulting vector must be one, we conclude that the matrix $(c_{i,j})_{i,j}$ has rank one and therefore is of the form $c_{i,j} = r_i s_j$ giving $Y(|i,j\rangle) = |r_i\alpha_i, s_j\beta_j\rangle$, the desired result. □

Let us now show that P_π is the trivial permutation:

Lemma IV.3.4. $P_\pi = \mathbb{1}$

Proof. Assume that P_π is not the identity. Take a $R - S$ bipartition (with sizes $\geq L/5$) such that P_π maps one Hilbert space of R into one of S. We block again $N/5$ columns to get two injective $R \times N/5$ and $S \times N/5$ regions. Denoting by R_1 and S_1 the parts of the regions that stay within the regions and by R_2, S_2 the ones that are mapped to the other side, we can decompose Y as in Fig. IV.5.

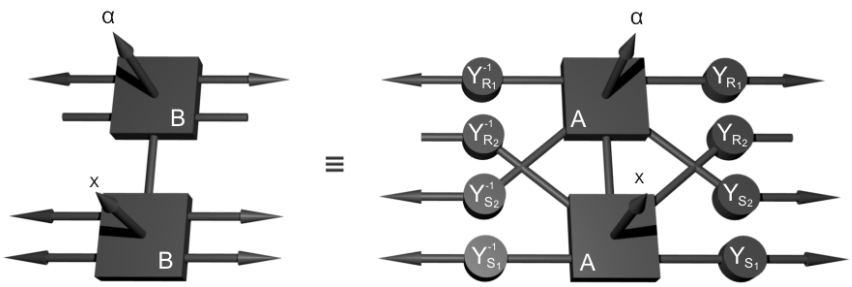

Figure IV.5: The cones represent vectors multiplying the legs of the tensor. In the virtual space, these vectors are $|0\rangle$, while the vectors in the leg corresponding to the real space are $|x\rangle$ and $|\alpha\rangle$ respectively.

Consider now Fig. IV.5. We contract all virtual indices but the pair in the second row with $|0\rangle$ and the physical indices with $|\alpha\rangle$ and $|x\rangle$ where the latter is chosen such that

$A|x\rangle = |0\rangle|0\rangle|0\rangle|0\rangle$. Let V be the span in the remaining two virtual indices under the variation of $|\alpha\rangle$. It is clear that in the LHS of Fig. IV.5, $\dim V = \dim(\text{support}(Y_{R_2}))$, whereas in the RHS $\dim V = 1$, which leads to a contradiction unless R_2 and S_2 are empty. □

By using both, injectivity and translational invariance of the RHS in Fig. IV.4, we observe that

Lemma IV.3.5. *$Y_i = Y$ for all i.*

We redefine now A^i as $\sum_{ldru} A^i_{ldru}(Y^{-1}\otimes\mathbb{1})|ld\rangle\langle ru|(Y\otimes\mathbb{1})$, block $N/5$ columns together and sandwich with $|nn\cdots n\rangle$ and $\langle mm\cdots m|$ in Fig. IV.4. Defining $\tilde{A}^{i;nm}$ as

$$\sum_{bd} \tilde{A}^{i;nm}_{bd}|b\rangle\langle d| = \sum_{bd}\langle m|A^{1\times N/5}|n\rangle|b\rangle\langle d|$$

and the analogue for $\tilde{B}^{i;nm}$, we have two injective representations of the same MPS with $|\tilde{\psi}_B\rangle = \lambda'|\tilde{\psi}_A\rangle$. By means of the 1D case (Theorem IV.2.1), we obtain invertible matrices Z_{nm} and $\mu_{nm} \in \mathbb{C}$ such that $\mu^L_{nm} = \lambda'$ and

$$\mu_{nm} Z^{-1}_{nm}\tilde{A}^{i;nm} Z_{nm} \equiv \tilde{B}^{i;nm}. \tag{IV.6}$$

The next step is to show that Z_{nm} does not depend on n and m. We sandwich in Fig. IV.4 with $\langle m'|^{\otimes L/2}\langle m|^{\otimes L/2}$ and $|n'\rangle^{\otimes L/2}|n\rangle^{\otimes L/2}$ and, using Eq. (IV.6), we get Fig. IV.6 for the corresponding $\tilde{A}^i$ tensors. By summing with appropriate coefficients in order to obtain "deltas", we obtain that $\mu^{L/2}_{nm}\mu^{L/2}_{n'm'}\langle l|Z_{nm}Z^{-1}_{n'm'}|k\rangle\langle r|Z^{-1}_{nm}Z_{n'm'}|s\rangle = \lambda'\delta_{kl}\delta_{rs}$, so $Z_{nm} \equiv Z$ is indeed independent of n and m (up to a constant that can be embeded in Z_{nm} itself). Considering the bipartition $(L/2+1)$-$(L/2-1)$ and repeating the argument we get that $\mu^{L/2+1}_{nm}\mu^{L/2-1}_{n'm'} = \lambda'$ and then $\mu_{nm} = \mu$ is also independent of n and m. By reasoning as above in the other direction, one can prove that $Z = Z'^{\otimes N/5}$.

Up to now, we have proven the following lemma.

Lemma IV.3.6. *For any length H for which one gets injectivity in the orthogonal direction, we have the structure shown in Fig. IV.7. The case where vertical is interchanged by horizontal is equivalent.*

In order to have the same result for a single tensor (a region of size 1x1) we will use that rectangular regions are injective from a size on.

Lemma IV.3.7. *If a region of size $H \times K$ of a translational invariant PEPS is injective, the same happens for a region of size $(H+1)\times K$ (and $H \times (K+1)$)*

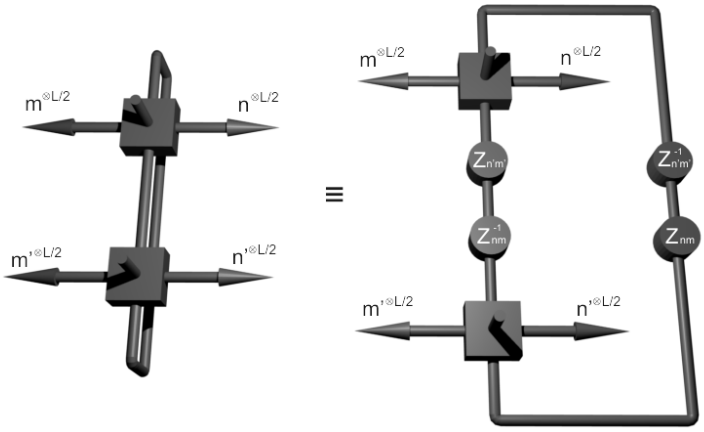

Figure IV.6: This is a representation of the resulting tensor after blocking $\frac{L}{2} \times \frac{N}{2}$ sites. The vectors in the virtual space correspond to tensor products of $\frac{L}{2} \times \frac{N}{5}$ local vectors.

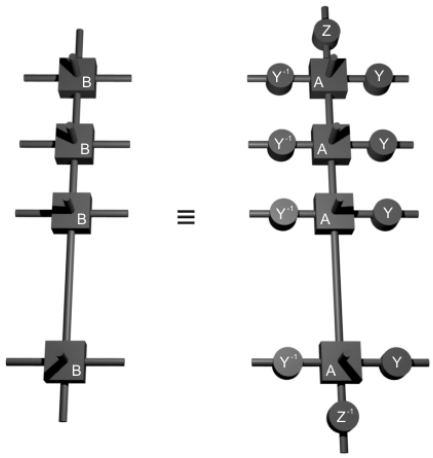

Figure IV.7: A subsystem of H spins has two equivalent injective TI-PEPS representations iff they are connected by invertible matrices.

Proof. Note that the region of size $1 \times K$ is injective when the upper and the physical system are considered as inputs (left picture of Fig. IV.8). To see this, take an injective region S of dimension $H \times K$ and split it into two subregions, as in the right picture of Fig. IV.8 with $T = H - 1$. For simplicity in the rest of the proof we gather the indices u^1, u^2, u^3 and d^1, d^2, d^3 and call them u and d respectively.

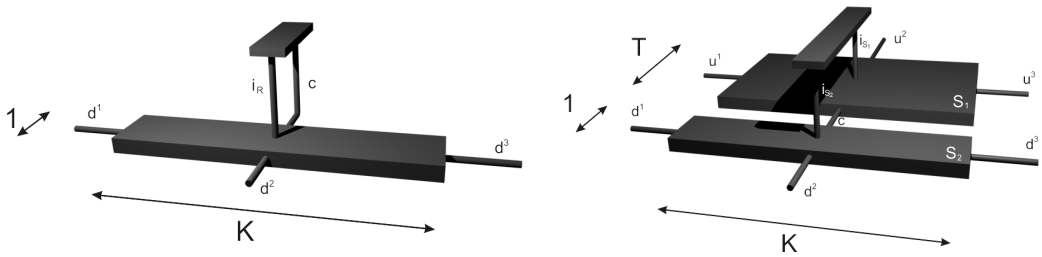

Figure IV.8: This figure represents the argument used to prove Lemma IV.3.7.

Using injectivity of the region S, there exists $\{\alpha^{u_0,d_0}_{i_{S_1},j_{S_2}}\}_{i_{S_1},j_{S_2}}$ for any u_0, d_0 such that

$$\sum_{c,i_{S_1},j_{S_2}} \alpha^{u_0,d_0}_{i_{S_1},j_{S_2}} A^{u,c}_{i_{S_1}} A^{c,d}_{j_{S_2}} = \delta_{u,u_0}\delta_{d,d_0}$$

Taking $u = u_0$ we get

$$\sum_{c,i_{S_1},j_{S_2}} \alpha^{u_0,d_0}_{i_{S_1},j_{S_2}} A^{u_0,c}_{i_{S_1}} A^{c,d}_{j_{S_2}} = \delta_{d,d_0}$$

Now, if we take a region S of size $(H+1)\times K$ and divide it as in Fig. IV.8 with $T = H$, there exists $\{\beta^{d_0}_{c,j_{S_2}}\}_{c,j_{S_2}}$ for any d_0 such that

$$\sum_{c,j_{S_2}} \beta^{d_0}_{c,j_{S_2}} A^{c,d}_{j_{S_2}} = \delta_{d,d_0}$$

By using injectivity of a region of dimension $H \times K$, there exists $\{\alpha^{u_0,c_0,d_0}_{i_{S_1},j_{S_2}}\}_{i_{S_1}}$ such that

$$\sum_{i_{S_1}} \alpha^{u_0,c_0,d_0}_{i_{S_1},j_{S_2}} A^{u,c}_{i_{S_1}} = \beta^{d_0}_{c_0,j_{S_2}} \delta_{u,u_0}\delta_{c,c_0}$$

By putting both equalities together, we find

$$\begin{aligned}
&\sum_{c,c_0,i_{S_1},j_{S_2}} \alpha^{u_0,c_0,d_0}_{i_{S_1},j_{S_2}} A^{u,c}_{i_{S_1}} A^{c,d}_{j_{S_2}} = \\
&= \sum_{c,c_0 j_{S_2}} \beta^{d_0}_{c_0,j_{S_2}} \delta_{u,u_0}\delta_{c,c_0} A^{c,d}_{j_{S_2}} = \\
&= \sum_{c_0 j_{S_2}} \beta^{d_0}_{c_0,j_{S_2}} \delta_{u,u_0} A^{c_0,d}_{j_{S_2}} = \delta_{u,u_0}\delta_{d,d_0}
\end{aligned}$$

and so S is an injective region. □

We want to prove now Theorem IV.3.1. Let us consider a $H \times K$ injective region, for instance $H = L/5$, $K = N/5$. From Lemma IV.3.7, the larger regions in Fig. IV.9 are also injective. If we replace Fig. IV.7 first in each subregion (not the center), and then in the whole region, we get $A^i = \mu B^i(Y^{-1} \otimes Z^{-1} \otimes Y \otimes Z)$ with $\mu \in \mathbb{C}$. As in the 1D case the condition $\mu^{LN} = \lambda$ can be recovered considering the equations between the two PEPSs representations and substituting the relation between the tensors given in Fig. IV.1.

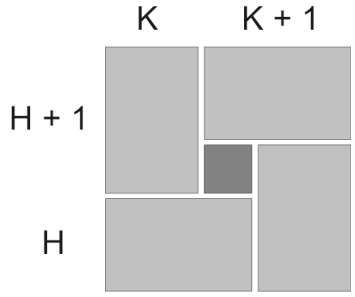

Figure IV.9: Representation of the regions of injectivity for the proof of Theorem IV.3.1.

As we said in the introduction of this section, we can generalize Theorem IV.3.1 to the honeycomb lattice. The construction of the state in the honeycomb lattice is the same as in the square lattice. The state is described by two tensors A^i_{lud} and $B^i_{d'u'l'}$ with 4 indices each: i corresponding to the physical spin of dimension d and the others corresponding to three virtual spaces of dimensions (*bonds*) D_1, D_2 and D_3 as we did for PEPSs. The connections between two sites are again performed by means of maximally entangled states $|\Omega\rangle = \sum_\alpha |\alpha\alpha\rangle$. Then, the state is now given by the contractions of these tensors according to the honeycomb lattice (see Fig. IV.10).

Figure IV.10: Tensors defining a state in a honeycomb lattice. In order to define the state indices l, u and r of A tensors are contracted with indices l', u' and r' respectively of different B tensors.

As we said in the introduction of this section, we can generalize Theorem IV.3.1 to the honeycomb lattice. We need to prove first the following

Lemma IV.3.8. *Let $A, C \in \mathcal{M}_{d_1,d_2}$ and $B, D \in \mathcal{M}_{d_2,d_3}$. Then, if $AB = CD$ and* $\mathrm{rank}(A) = \mathrm{rank}(B) = d_2$ *there exists an invertible matrix W such that $A = CW$ and $B = W^{-1}D$.*

Proof. Since B is full-rank, there exists a matrix that we can call B^{-1} such that $BB^{-1} = \mathbb{1}_{d_2}$. Therefore, $A = C(DB^{-1})$ and we can denote $W = DB^{-1}$. Similarly $B = A^{-1}CD$ and we can denote $U = A^{-1}C$. Since $UW = A^{-1}CDB^{-1} = BB^{-1} = \mathbb{1}_{d_2}$, we get that $U = W^{-1}$ and hence $B = W^{-1}D$. □

We can now prove the theorem for the honeycomb lattice. Let us remark that the unit cell of this lattice contains two sites and that the lattice associated to the unit cells is a square lattice. The translational invariance is not site by site, but unit cell by unit cell.

Theorem IV.3.9 (The honeycomb lattice)**.** *Let $|\Psi\rangle$ and $|\Psi'\rangle$ be two PEPSs defined in a honeycomb lattice and such that the square lattice constituted by the unit cells fulfils the conditions of Theorem IV.3.1. Then, $|\Psi\rangle \equiv |\Psi'\rangle$ iff the conditions shown in Fig. IV.11 hold.*

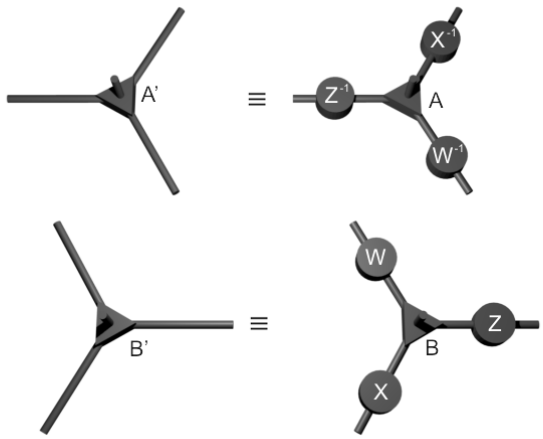

Figure IV.11: These are the relations which the tensors defining two TI-PEPSs on a honeycomb lattice must fulfill in order to represent the same state.

Proof. Let us apply Theorem IV.3.1 to the square lattice which the unit cell constitutes. Then, we obtain the equality shown in Fig. IV.12 and Lemma IV.3.8 completes the proof of the theorem. □

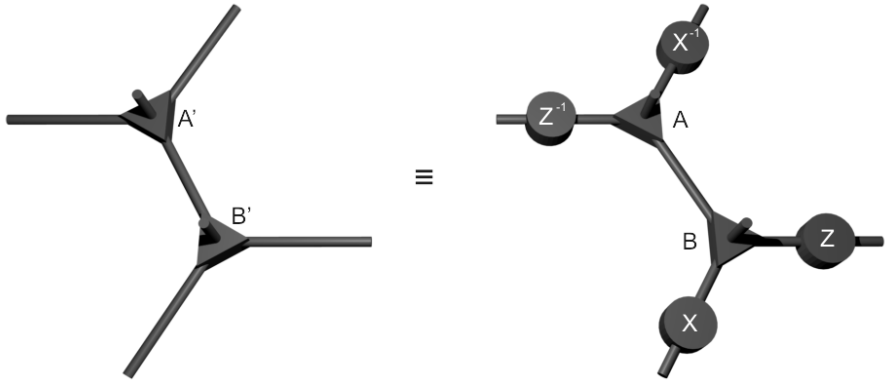

Figure IV.12: The possibility of transforming the honeycomb lattice into a square lattice by blocking tensors enables us to apply the result on equivalent TI-PEPSs representations for the square lattice.

IV.4 Symmetries

Order parameters measure the degree of order in a system and thus are fundamental in the description of the different phases of matter. Nevertheless there are certain phases that cannot be characterized by these parameters. In such cases, string order parameters have been proven to be a very useful tool in the detection and understanding of quantum phase transitions. However, as pointed out in [2], their application could not go beyond the 1D case. In [134], with the aid of MPS, it was shown that the existence of a string order parameter is intimately related to the existence of a symmetry, which allows us to design an appropriate 2D definition: the existence of a local symmetry when we consider increasing sizes of the system. A trivial sufficient condition for this to hold in PEPSs is proposed there (see Fig. IV.13). The aim of this section is to prove that, for injective PEPSs, the condition is also necessary. The 1D version is proven in [134] with the assumption of injectivity and in [151] for the general 1D case.

Theorem IV.4.1 (Local symmetry)**.** *If a TI-PEPS defined on an $L \times N$ lattice has a symmetry u, i.e. $u^{\otimes NL}|\psi_A\rangle = e^{i\theta'}|\psi_A\rangle$, and is injective in regions of size $L/5 \times N/5$, then the tensors defining it satisfy the relation in Fig. IV.13 with $e^{i\theta NL} = e^{i\theta'}$. Moreover, if u_g is a representation of a continuous group G, then Y_g and Z_g are projective representations and $e^{i\theta_g}$ is a representations as well.*

Proof. Notice that when acting with u on the tensor A which defines the PEPS (see Fig.

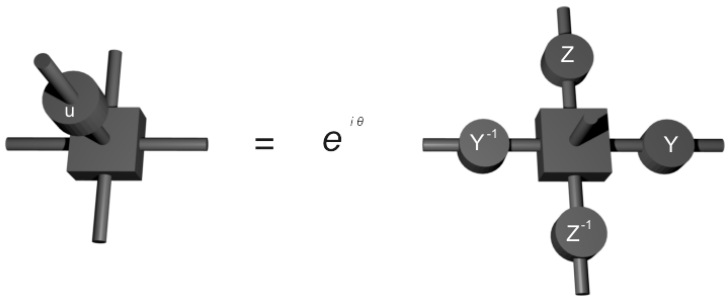

Figure IV.13: This is a graphical representation of the equation that a PEPS fulfills if it is invariant under a representation u^g of a group G. Then, the symmetry is inherited into a couple of representations of G, called Y_g and Z_g, up to a phase $e^{i\theta_g}$.

IV.13), we get a new tensor B that is also injective in regions of size $L/5 \times N/5$ and such that $|\psi_A\rangle = e^{i\theta'}|\psi_B\rangle$. Theorem IV.3.1 then gives the result.

In order to prove that the invertible matrices Y_g and Z_g are representations of G, we adapt the arguments used in [151, Theorem 7]. Consider the representation $g \longrightarrow u^g$ of the group G. For a particular u^g, Fig. IV.13 reads

$$\sum_j u^g_{ij} A^j = e^{i\theta_g} A^i (Y_g \otimes Z_g \otimes Y_g^{-1} \otimes Z_g^{-1}).$$

Then, given $g_1, g_2 \in G$, we have

$$\begin{aligned} e^{i\theta_{g_2 g_1}} A^i (Y_{g_2 g_1} \otimes Z_{g_2 g_1} \otimes Y_{g_2 g_1}^{-1} \otimes Z_{g_2 g_1}^{-1}) &= \sum_j u^{g_2 g_1}_{ij} A^j = \\ &= \sum_j u^{g_2}_{ik} u^{g_1}_{kj} A^j = e^{i(\theta_{g_1}+\theta_{g_2})} A^i (Y_{g_1} Y_{g_2} \otimes Z_{g_1} Z_{g_2} \otimes Y_{g_1}^{-1} Y_{g_2}^{-1} \otimes Z_{g_1}^{-1} Z_{g_2}^{-1}). \end{aligned}$$

Now, grouping to have an injective R-S region, we get that

$$\begin{aligned} &e^{iRS\theta_{g_2 g_1}} X (Y_{g_2 g_1}^{\otimes R} \otimes Z_{g_2 g_1}^{\otimes S} \otimes Y_{g_2 g_1}^{-1 \otimes R} \otimes Z_{g_2 g_1}^{-1 \otimes S}) = \\ &= e^{iRS(\theta_{g_1}+\theta_{g_2})} X ((Y_{g_1} Y_{g_2})^{\otimes R} \otimes (Z_{g_1} Z_{g_2})^{\otimes S} \otimes (Y_{g_1}^{-1} Y_{g_2}^{-1})^{\otimes R} \otimes (Z_{g_1}^{-1} Z_{g_2}^{-1})^{\otimes S}), \end{aligned} \tag{IV.7}$$

for any matrix X. Taking $X = \mathbb{1}$, we get that $RS\theta_{g_2 g_1} = RS(\theta_{g_2}+\theta_{g_1}) + 2k\pi$. In particular, taking the four cases with $R = \{L/5, L/5+1\}$ and $S = \{N/5, N/5+1\}$, summing and

simplifying to get rid of the $L/5$ and $N/5$ terms, we get that $\theta_{g_2 g_1} = \theta_{g_2} + \theta_{g_1} + 2k_0\pi$. Thus the map $g \longrightarrow e^{i\theta_g}$ is a representation of G.

Finally, to show that the maps $g \longrightarrow Y_g$ and $g \longrightarrow Z_g$ are representations of G it is enough to note that grouping tensors in Eq. IV.7 we get that $Y_{g_2 g_1} Y_{g_2}^{-1} Y_{g_1}^{-1} \otimes Z_{g_2 g_1} Z_{g_2}^{-1} Z_{g_1}^{-1}$ commutes with every matrix. Thus $Y_{g_2 g_1} = \lambda Y_{g_1} Y_{g_2}$ and $Z_{g_2 g_1} = \mu Z_{g_1} Z_{g_2}$ with λ, $\mu \in \mathbb{C}$. This fact together with the freedom in the matrices Y and Z shows that Y_g and Z_g are projective representations of G. □

With exactly the same reasoning, we can characterize the spatial symmetries: reflection, $\pi/2$-rotations and π-rotations:

Theorem IV.4.2 (Reflection symmetry)**.** *Let us consider an $L \times N$ TI-PEPS with the property that for a region of size smaller than $L/5 \times N/5$ it is injective. If this PEPS is invariant under a reflection with respect to a vertical axis, then there exist invertible matrices Y, Z such that the tensors defining the PEPS verify Fig. IV.14, that is, $\sum_{ldru} A^i_{ldru} \langle ldru| = e^{i\theta} (\sum_{ldru} A^i_{ldru} \langle rdlu|) Y \otimes Z \otimes Y^{-1} \otimes Z^{-1}$ for all i.*

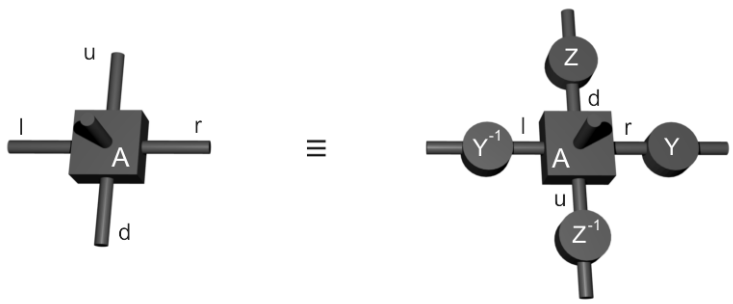

Figure IV.14: This figure represents the condition which must be fulfilled by a TI-PEPS in order to generate a state invariant under reflections (in this case with respect to the horizontal plane).

Moreover, it is easy to see that Y, Z must satisfy $Y^T = Y$, $Z^2 = \mathbb{1}$. The characterization of the reflection with respect to the horizontal axis follows straightforwardly by changing the roles of the horizontal/vertical directions.

Theorem IV.4.3 (spatial $\pi/2$-rotation symmetry)**.** *If an $L \times L$ TI-PEPS with the property that for a region of size smaller than $L/5 \times L/5$ it is injective has a spatial $\pi/2$-rotation*

invariance, then there exist invertible matrices Y, Z such that the tensors A^i defining the PEPS verify Fig. IV.15, that is, $\sum_{ldru} A^i_{ldru}\langle ldru| = e^{i\theta}(\sum_{ldru} A^i_{ldru}\langle uldr|)Y \otimes Z \otimes Y^{-1} \otimes Z^{-1}$ *for all i.*

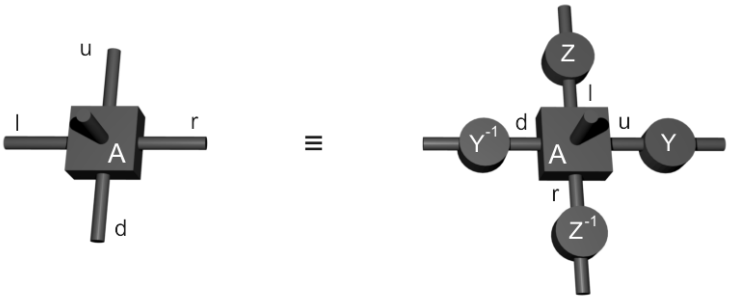

Figure IV.15: This figure represents the condition which must be fulfilled by a TI-PEPS in order to generate a state invariant under $\frac{\pi}{2}$-rotations (in this case a clockwise rotation).

In this case, one can see that Y, Z must satisfy the additional constraints $(YZ)^T = YZ$, $(ZY)^T = ZY$.

Finally, we characterize the PEPSs which are symmetric respect to a π-rotation.

Theorem IV.4.4 (spatial π-rotation symmetry)**.** *Let us consider an $L \times N$ TI-PEPS with the property that for a region of size smaller than $L/5 \times N/5$ it is injective and that it is invariant under a π-rotation, then there exist invertible matrices Y, Z such that the tensors defining the PEPS verify Fig. IV.16, that is,* $\sum_{ldru} A^i_{ldru}\langle ldru| = e^{i\theta}(\sum_{ldru} A^i_{ldru}\langle ruld|)Y \otimes Z \otimes Y^{-1} \otimes Z^{-1}$ *for all i.*

Now the constraints are $Z^T = Z$, $Y^T = Y$.

IV.5 Applications

It is clear that a symmetry must impose restrictions on the possible behaviors and properties of a quantum system. Understanding these restrictions is a hard problem that has led the research in Quantum Many Body Physics in the last decades. For PEPSs, which seem to provide a reasonably complete description of quantum states, we have

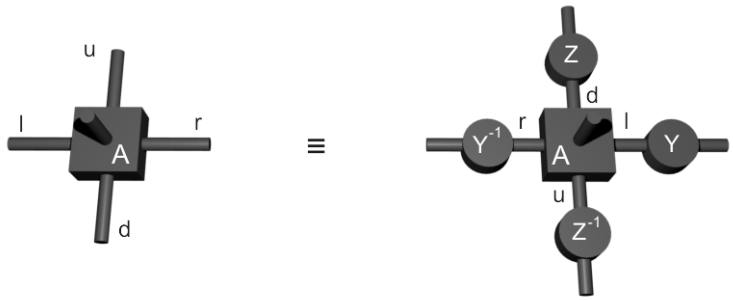

Figure IV.16: This figure represents the condition which must be fulfilled by a TI-PEPS in order to generate a state invariant under π-rotations (in this case a clockwise rotation).

proven a simple characterization of the existence of symmetries, which immediately leads to a number of consequences. In the lines below we list some of them.

IV.5.1 Lieb-Schultz-Mattis Theorem

The Lieb-Schultz-Mattis theorem states that, for semi-integer spin, a $SU(2)$-invariant 1D *Hamiltonian* cannot have a uniform (independent of the size of the system) energy gap. This theorem has been generalized in a number of ways. Still in the 1D case but relaxing the symmetry to a $U(1)$ symmetry, Oshikawa, Yamanaka and Affleck showed in [128] that the same conclusion holds if $J - m$ is not an integer, where J is the spin and m the magnetization per particle. For the $SU(2)$ case in 2D, Hastings and Nachtergaele-Sims proved that the same results holds [67, 118]. In [151], it has been shown how the orginial Lieb-Schultz-Mattis Theorem can be understood on the level of states. More precisely, it was shown that any $SU(2)$ invariant MPS with semi-integer spin cannot be injective. In this section we will give a 2D version of the Oshikawa-Yamanaka-Affleck theorem, by showing that a $U(1)$ symmetric PEPSs for which $J - m$ is not an integer cannot be injective.

Let us start with a PEPS $|\psi_A\rangle$ of spin J particles with a $U(1)$ symmetry in the z direction, that is

$$u_g^{\otimes N}|\psi_A\rangle = e^{i\theta_g}|\psi_A\rangle$$

where $u_g = e^{igS_z}$ and S_z is the usual generator of spin J. Since $g \mapsto e^{i\theta_g}$ is clearly a representation, there exists θ such that $\theta_g = Ng\theta$. We will show that

Lemma IV.5.1. *θ coincides with the magnetization per particle m.*

The magnetization per particle m is given by the total magnetization M along the direction of an axis (conventionally the z-axis is taken), divided by the number of particles N. That is,

$$M = Nm = \langle\psi_A| \sum_j S_j^z |\psi_A\rangle,$$

where S_j^z is the usual generator of spin J along the z-axis acting on the j-th particle.

To see Lemma IV.5.1 it is enough to expand both sides of the expression $u_g^{\otimes N}|\psi_A\rangle = e^{iNg\theta}|\psi_A\rangle$ around the identity: from the LHS we get $u_g^{\otimes N}|\psi_A\rangle \simeq (\mathbb{1} + ig\sum_j S_j^z)|\psi_A\rangle$, while the RHS gives $(1 + iNg\theta)|\psi_A\rangle$. By simplifying both results, we get $N\theta = \langle\psi_A|\sum_j S_j^z|\psi_A\rangle$, the desired result.

Now we can prove the announced generalized Lieb-Schulz-Mattis theorem for PEPSs.

Theorem IV.5.2. *Let us consider a PEPS $|\psi_A\rangle$ in a square $L \times N$ lattice that is injective in regions of size $L/5 \times N/5$. If $|\psi_A\rangle$ is invariant under a representation of $U(1)$ with the usual generator of spin J given by S_z, then the magnetization per particle m fulfils that $(J - m)$ is an integer.*

If the state has full $SU(2)$ symmetry, then $m = 0$ and we get the "Lieb-Schultz-Mattis theorem" for PEPSs.

Proof. We will choose $R \geq L/5$, $S \geq N/5$ and consider the PEPS (with periodic boundary conditions) associated to the region $R \times S$, $|\psi_A^{R\times S}\rangle$. By injectivity it is clear that $|\psi_A^{R\times S}\rangle \neq 0$. Applying e^{igS_z} to all spins and using Theorem IV.4.1 we get that there must exist a choice of indices $k_1, \dots k_{RS} \in \{-J, -J+1, \dots, J-1, J\}$ such that $k_1 + \cdots + k_{RS} = SR\theta$. We do the same for regions of size $R \times (S+1), (R+1) \times S, (R+1) \times (S+1)$, getting indices k', k'' and k''' respectively. Now

$$\theta = (R+1)(S+1)\theta - (R+1)S\theta - R(S+1)\theta + RS\theta =$$

$$= \sum_{r=1}^{RS} k_r + \sum_{r=1}^{(R+1)S} k'_r + \sum_{r=1}^{R(S+1)} k''_r + \sum_{r=1}^{(R+1)(S+1)} k'''_r \ .$$

The RHS has the same character as J, that is, it is integer if J is and semi-integer if J is. Therefore $\theta - J \in \mathbb{Z}$. Since, by Lemma IV.5.1, θ is the magnetization per particle, we are done. $\square$

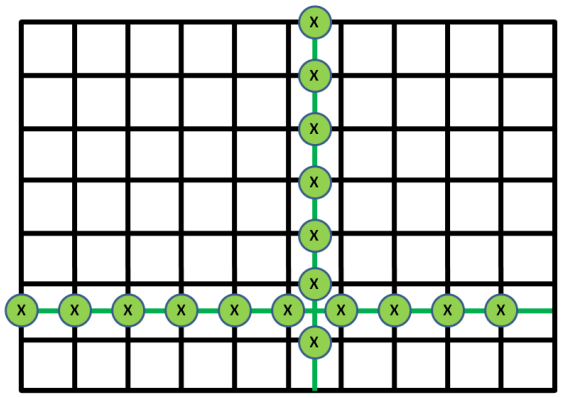

Figure IV.17: "Wilson loops" that keep invariant the PEPS associated to the toric code.

IV.5.2 Wilson loops

It has been observed in [173] that the equal superposition of the four logical states of the toric code $|\psi\rangle$ has a PEPS representation with bond dimension 2. Since the logical σ_X in the first (resp. second) logical qubit is implemented by a non-contractible cut of σ_X operators along the vertical (resp. horizontal) direction [94], $|\psi\rangle$ remains invariant under these two "Wilson loops" (see Fig. IV.17).

We will see in this section how the existence of this kind of Wilson loops imply again that the PEPS cannot be injective.

Theorem IV.5.3. *Let $|\psi_A\rangle$ be PEPS in a $L \times N$ square lattice with local Hilbert space dimension d such that there exists a $u \in U(d)$ with the properties:*

(i) $u^{\otimes L} \otimes \mathbb{1}_{rest}|\psi_A\rangle = |\psi_A\rangle$ *for a loop in the vertical direction.*

(ii) $u^{\otimes N} \otimes \mathbb{1}_{rest}|\psi_A\rangle = |\psi_A\rangle$ *for a loop in the horizontal direction.*

(iii) $u \otimes \mathbb{1}_{rest}|\psi_A\rangle \neq |\psi_A\rangle$ *for u acting on a single site.*

Then $|\psi_A\rangle$ cannot be injective for any region of size $\leq L/5 \times N/5$.

Proof. We assume injectivity for a region of size $L/5 \times N/5$, (i) and (ii) and will show that (iii) does not hold. By applying (i) to all columns and Theorem IV.4.1, we get that there exist unique Y and Z such that Fig. IV.13 holds. Applying now (i) to $N/5$ columns and

injectivity we get that $Y = \mathbb{1}$ and applying (ii) to $L/5$ rows and injectivity we get that $Z = \mathbb{1}$. So $u \otimes \mathbb{1}_{\text{rest}}|\psi_A\rangle = |\psi_A\rangle$ for u acting on a single site. □

IV.6 Discussion

In this chapter we have provided a simple characterization of the existence of symmetries in PEPSs. The result is based on the proven existence of a "canonical form". Since PEPSs seem to give a fairly complete characterization of the low energy sector of local Hamiltonians, the result paves the way for a better understanding of the restrictions that symmetries impose on quantum systems. As a first example of the kind of results that one can obtain from this characterization, we have shown a 2D version of the Oshikawa-Yamanaka-Affleck extension for $U(1)$ of the Lieb-Schultz-Mattis theorem. We have also outlined, via the injectivity property, how three of the main indicators of topological order (degeneracy of the ground state, existence of Wilson loops and corrections to the area law) are related.

Moreover, the characterization of the existence of symmetries for MPS has given rise to a full classification of the phases of matter in 1D systems [20, 49, 137, 155, 167]. For higher dimensional systems the same arguments has also been exploited in [155], where a classification for 2D phases in systems with unique ground state, degenerate ground state with a local order parameter, and systems with topological order has been started.

Chapter V

Many body systems and the principle of maximum entropy

The principle of maximum entropy, which briefly states that, among all possible probability distributions compatible with our prior information, the best choice is the one which maximizes the Shannon entropy, gives a pretty satisfactory solution to the old problem of dealing with prior information in probability theory, generalizing the old *principle of indifference* of Bernoulli and Laplace. Although it was formalized by Jaynes [87, 88], thanks to the development of Information Theory by Shannon, the essential content of the principle of maximum entropy was already present in the foundations of statistical mechanics as it can be inferred from Boltzman's *method of the most probable distribution* and Gibbs *canonical ensemble* [89, 101].

Apart from its important applications on decision theory, from its origin the principle of maximum entropy has succeeded in giving a very useful information-theoretical view of statistical mechanics, both classical [87] and quantum [88]–where the function to maximize is the von Neumann entropy. As an easy illustration, given the average energy of a quantum system as prior information, the density matrix which maximizes entropy is exactly the thermal state associated to that particular energy. This spirit has been recently recovered with great success in [139] and further developed in a number of ways in [12, 28, 105, 106, 114, 178].

To which extent the principle of maximum entropy can be extended to more and more general situations has been a very active and controversary field in the last half-century. For instance, very recently a series of theoretical and experimental works [29, 50, 166] seem to validate the principle in relaxation processes of quantum systems when focusing on a particular small subsystem –which, as argued in Fig. V.1, is the most relevant situation.

Another, even older, principle to assign prior probabilities in physical problems relies on the symmetries of the problem (see [86] for a discussion). For instance, if one wants to incorporate in the problem some invariance, i.e. independence of the reference frame, this already reduces the class of prior probability distributions available. Indeed, if one has enough symmetries –they form a compact group– there is indeed a unique way of defining a prior distribution compatible with the symmetries –the Haar measure– and the problem is solved.

But what if one wants to incorporate to the problem some less *standard* knowledge?

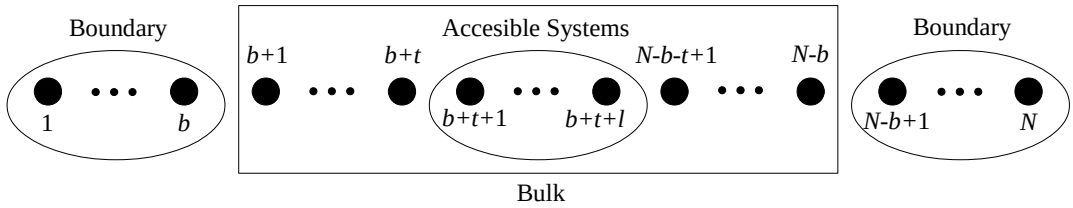

Figure V.1: We consider a chain of N sites, with homogeneous interactions in the bulk and boundary effects in exponentially small regions of size b at the borders. We assume that the experimentally accesible region (and hence the region we are interested in) is an exponentially small region of size l in the center of the chain.

For instance, that the interactions in our model are local and homogeneous and that we work at zero temperature, but not any assumption on the particular interactions in the model itself. Note the difference with Jaynes' approach where the particular Hamiltonian of the model is known. Is there any way of incorporating this information to the problem? Which is then the right prior probability? Is it related to maximizing some entropy? Since this type of assumptions are natural and widely accepted, solving these questions could be of utmost importance in quantum condensed-matter problems. In this chapter we attack (and to some extent solve) them in the particular case of 1D spin systems.

To do that we will take advantage of the recent developments in the understanding of quantum spin chains. It has already been justified in Section II.2 that their ground states are exactly represented by the set of Matrix Product States (MPSs) with *polynomial* bond dimension. We will concentrate in the situation of a chain with boundary effects in exponentially small regions of size b at both ends, homogeneity in the bulk and experimental access to an exponentially small central region of size l (see Fig. V.1). Tracing out the boundary terms leads to a bulk state given by

$$\rho = \sum_{i_{b+1},\dots i_{N-b},j_{b+1},\dots j_{N-b}=1}^{d} \operatorname{tr}(LA_{i_{b+1}}\cdots A_{i_{N-b}}RA^{\dagger}_{j_{N-b}}\cdots A^{\dagger}_{j_{b+1}})|i_{b+1}\dots i_{N-b}\rangle\langle j_{b+1}\dots j_{N-b}|, \tag{V.1}$$

where all A_i, $L \geq 0$ and $R \geq 0$ are $D \times D$ matrices with $D = \operatorname{poly}(N)$. This will be our starting point, that is, the prior information can be understood as restricting the bulk-states of our system to have the form (V.1).

Now, it is also known from the general theory of MPS [131] that this set has a natural (over)parametrization by the group $U(dD)$, via the map $U \mapsto A_i = \langle i|U|0\rangle$. Since $U(dD)$ is the unitary group, one can use the symmetry-based assignment of prior distributions to sample from the Haar measure. Similarly, the fact that the map $X \mapsto \sum_i A_i X A_i^{\dagger}$ is trace-preserving leads to consider $\operatorname{tr}(R) = 1$, $\|L\|_{\infty} \leq 1$, giving us natural ways of sampling

also the boundary conditions (see below). One can therefore ask about which is then the generic reduced density matrix ρ_l of $l \ll N$ sites. Note that, by the above comments, this is nothing but asking about generic observations of 1D quantum systems. The aim of this chapter is to show that ρ_l has generically maximum entropy:

Theorem V.0.1. *Let ρ_l be taken at random from the ensemble introduced with $D \geq N^5$. Then $S(\rho_l/\operatorname{tr}\rho_l) \geq \log d^l - d^l O(D^{-1/5})$ except with probability exponentially small in D.*

Note that, since the accessible region l is exponentially smaller than the system size, the bound can be made arbitrary close to $\log d^l$ while keeping the size of the matrices D polynomial in the system size.

To prove the theorem, we will rely on recent developments of random matrix theory, in particular on the graphical Weingarten calculus provided in [24], and on a novel estimate of the Weingarten function.

Relations to prior work. The ensemble of MPSs was already considered in [52, 53] as a set of relevant physical states. There, the authors show how concentration arises for the reduced density matrix through concentration of the expected value of local observables around its average. Moreover, for non-homogeneous MPSs, they show that the average reduced density matrix is the identity, and thus a reduced density matrix has typically maximum entropy. Nevertheless, they do not compute the average of the reduced density matrix in the homogeneous case which is more mathematically involved. This is exactly what we prove here.

The research in [52, 53] was inspired by previous similar results [55, 139, 144] where the randomization takes place over the ensemble of general quantum states. All these randomization results together with ours can be seen as static versions of thermalization in the sense that, for most states of any of the different ensembles, the reduced density matrix of a small subsystem is close to the canonical state (Corollary V.3.7). The problem of thermalization has recently got a renewed interest, see [28, 56] and references therein. In particular, randomization has already been considered in dynamical approaches to thermalization [12, 28, 105, 106, 114, 178], where the randomization is over the set of hamiltonians with a given energy spectrum. The MPS formalism has also been used to study thermalization numerically in the case of an infinite 1D system under the effect of a homogeneous local interaction hamiltonian [4], where different degrees of thermalization appear.

The rest of the chapter is organized as follows. First we describe the ensemble of Matrix Product States. In Section V.2 we introduce the mathematical tools that we will use for the proof of Theorem V.0.1. These tools are both concentration of measure phenomenon and integration over the unitary group. Moreover, we introduce the Weingarten function, that arises naturally in the computation of such integrals, and gives a novel asymptotic

bound of the Weingarten function. This bound will be essential in Section V.3 devoted to the proof of Theorem V.0.1. We finally conclude with a discussion of the results in Section V.4.

V.1 Random Matrix Product States

In this section we just fix the ensemble of MPS. In the rest of this chapter we will be interested in the reduced state of the l consecutive central sites of the chain, where $l << n = 2t + l$, that, up to trace normalization, will be described as

$$\rho_l = tr_{A,B_1\dots B_t,B_{t+l+1}\dots B_n}[L\mathcal{E}^n(R)].$$

where the map $\mathcal{E}$ is the CP-map associated to the MPS II.7 and the general boundary conditions L and R come from tracing out the boundary sites as described in Figure V.1. MPS theory leads to consider them belonging respectively to the sets $\mathcal{L} = \{L \geq 0 : \|L\|_\infty \leq 1, L \in M_D\}$ and $\mathcal{R} = \{R \geq 0 : \mathrm{tr}(R) = 1, R \in M_D\}$, where $\|\cdot\|_\infty$ means the usual operator norm. Diagonalizing $L = V\Lambda V^\dagger$ and $R = W\Omega W^\dagger$ we can parametrize $\mathcal{L}$ by $[0,1]^D \times U(D)$ and $\mathcal{R}$ by $\mathbb{S}_1([0,1]^D) \times U(D)$, being $\mathbb{S}_1([0,1]^D)$ the set of D-event probability distributions. Again by symmetry considerations, this leads to sample L using the Lebesgue measure on $[0,1]^D$ and the Haar measure on $U(D)$ and to sample R using any permutational invariant measure on $\mathbb{S}_1([0,1]^D)$ and the Haar measure on $U(D)$. We finally recall from the introduction that the matrices A_i in Eq. (V.1) will be sampled from the Haar measure on $U(Dd)$ via the parametrization $U \mapsto A_i = \langle i|U|0\rangle$.

Summarizing, we consider the ensemble of MPSs defined by the tuple $(U, L, R) = (U, V, W, \Lambda, \Omega)$ where U, V and W are distributed with respect to the Haar measure in the respective unitary group, Λ is distributed according to the Lebesgue measure in $[0,1]^D$ and Ω according to any permutation invariant probability measure in $\mathbb{S}_1([0,1]^D)$.

Now our problem can be rephrased as:

Given (U, L, R) randomly chosen find the behavior of the normalized state corresponding to

$$\rho_l(U, L, R) = \mathrm{tr}_{A,B_1\dots B_t,B_{t+l+1}\dots B_n}(LU_{A,B_1}\cdots U_{A,B_n}(R \otimes (|0\rangle\langle 0|)^{\otimes n})U^\dagger_{A,B_n}\cdots U^\dagger_{A,B_1}).$$

where the systems of the sites B_i are labeled from left to right and the unitary matrices are acting in the site indicated and the ancillary system A from right to left living the other sites invariant.

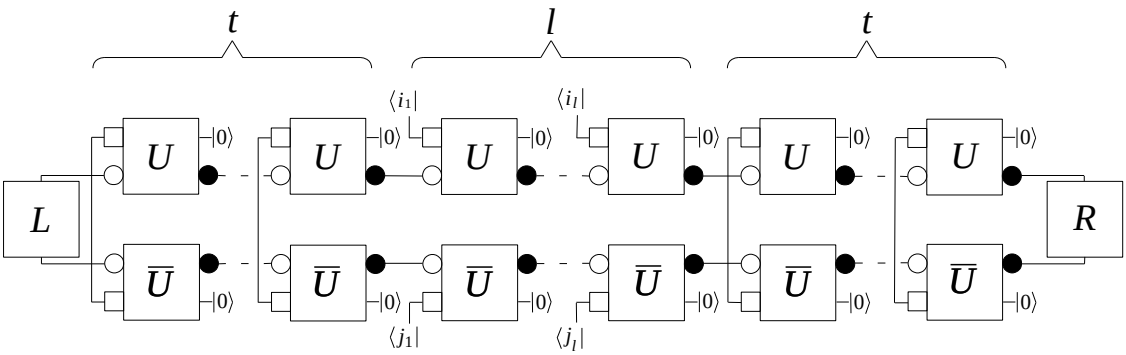

Figure V.2: Graphical representation of ρ_l, where big squares represent matrices seen as tensors of 4 inedexes (smaller tensors), each tensor is labelled by small objects attached to them. Dark objects correspond to "ket" tensors, white objects correspond to "bra" tensors, squares are used for dimension d and circles for dimension D. Wires represent contraction rules between tensors.

This state is represented in the diagrammatic description of Section II.2.1 in Figure V.2.

V.2 Mathematical tools

In this section we describe the mathematical tools we are going to use in the proof of Theorem V.0.1. These are the concentration of measure phenomenon where we just review some basic material and the integration over the unitary group. In this part we also describe the main ingredients of the Weingarten function and calculus that appear in the computation of such integrals. Moreover, we give a novel asymptotic bound of the Weingarten function that, besides being a key point in the proof of Theorem V.0.1, it is interesting in its own.

V.2.1 Concentration of Measure Phenomenon

This section contains some basic material on the concentration of measure phenomenon that we are going to use; for a detailed exposition see for example [116, 102].

Definition V.2.1. *Let (X, d) be a metric space with probability measure μ, its concentration function $\alpha_{(X,d,\mu)}$ is defined as*

$$\alpha_{(X,d,\mu)}(r) = \sup\{1 - \mu(A_r); A \subset X, \mu(A) \geq \frac{1}{2}\},\ r > 0$$

where $A_r = \{x \in X; d(x, A) < r\}$ is the open r-neighbourhood of A (with respect to d).

This definition allows us to prove directly that almost all the images of a Lipschitz function concentrate around the median, where the concentration factor is given by the concentration function. Nevertheless, we are interested in the concentration around the mean which is a consequence of the other, as one can bound the distance between the median and the mean depending on the concentration function.

Theorem V.2.2 (Concentration of measure phenomenon)**.** *Let F be a Lipschitz function on (X, d), and μ a probability measure on (X, d), then*

$$\mu(\{F > \mathbb{E}_\mu(F) + r\}) \leq 2\alpha_\mu(r/\|F\|_{Lip}),$$

$$\mu(\{F < \mathbb{E}_\mu(F) - r\}) \leq 2\alpha_\mu(r/\|F\|_{Lip}),$$

where $\mathbb{E}_\mu(F)$ is the mean of F with respect to μ and $\|F\|_{Lip}$ is the Lipschitz constant of F.

When one is interested in the concentration properties of a family of spaces, what matters is the scaling of the concentration function depending on the parameter defining the family . Thus looking at the definition of concentration function one can prove that the concentration properties of two spaces behave at least as well as the worst one of the two.

Proposition V.2.3. *Let μ, ν two probability measures on metric spaces (X, d) and (Y, δ) respectively. Then, if $\mu \times \nu$ is the product measure in $X \times Y$ equipped with the l^1-metric, $\alpha_{(X\times Y, d+\delta, \mu\times\nu)} \leq \alpha_{(X,d,\mu)} + \alpha_{(Y,\delta,\nu)}$*

If we apply this proposition to the spaces we are interested in we have the following lemma.

Lemma V.2.4. *Let μ be the Haar measure in $(U(D), d_2)$, the unitary group with the Hilbert-Schmidt distance. Let ν be the Lebesgue measure in $([0, 1]^D, d_\infty)$, the hypercube with the maximum distance. Then, for any $k \in \mathbb{N}$, the product space (X, d_1), where $X = U(kD) \times U(D) \times U(D) \times [0, 1]^D$ and d_1 is the l_1 distance of the product space, with the product probability measure $\eta = \mu \times \mu \times \mu \times \nu$ has concentration function*

$$\alpha_{(X,d_1,\eta)}(r) \leq ce^{-CDr^2},$$

where c and C are universal constants.

Remark V.2.5. *Note that in this lemma, that will be used to prove the concentration in Theorem V.3.6, we do not consider the space $\mathbb{S}_1([0, 1]^D)$, as in all the theorems below the result holds independently of $\Omega \in \mathbb{S}_1([0, 1]^D)$.*

V.2.2 Integration over the unitary group. Weingarten function.

Here we describe the main ingredients of the Weingarten function and calculus that we are going to use to compute averages over the unitary group, for a complete description of this function we refer to [22]. We first describe the standard notation of representation theory of symmetric groups, see [51].

Let $\sigma \in S_p$, we denote by $|\sigma|$ the minimum number k such that σ can be written as a product of k transpositions, $\#\sigma$ is the number of cycles in σ and both quantities are related by the formula $|\sigma| = p - \#\sigma$.

We denote by $\lambda \vdash p$ that $\lambda = (\lambda_1, ..., \lambda_r)$ is a partition of p, that is, a non-increasing sequence of positive integers λ_i with $|\lambda| = \sum_{i=1}^r \lambda_i = p$, where $r = l(\lambda)$ is the length. Irreducible representations (irreps) of the symmetric group are labelled by partitions. The conjugacy class of a permutation is labelled by the cycle type of the permutation, that is, the orders of the cycles in the permutation in non-increasing order.

For a partition $\lambda \vdash p$ with $l(\lambda) = r$ define the polynomial $q_\lambda = q_{\lambda_1} \cdots q_{\lambda_r}$ with $q_k = \sum_{i=1}^n x_i^k$ and the Schur polynomial $s_\lambda(x_1, ..., x_r) := \frac{\det (x_i^{\lambda_j+k-j})_{i,j=1}^k}{\det (x_i^{k-j})_{i,j=1}^k}$, which is a homogeneous polynomial over r variables of degree p. The polynomials q_ρ form a orthogonal basis of the symmetric functions and the Schur polynomials form a orthonormal basis of the symmetric functions. The character χ^λ of S_p associated to the representation λ is given by $\chi^\lambda_{\rho(\sigma)} = \chi^\lambda(\sigma) = \langle q_{\rho(\sigma)}, s_\lambda \rangle$, where $\rho(\sigma)$ is the cycle type (partition) associated to the conjugacy class of σ. That is, the characters are given by the change of basis from $q_\rho(\sigma)$ to s_λ and thus they fulfill the two orthogonality relations

$$\sum_{\lambda \vdash p} \chi^\lambda(\sigma)\chi^\lambda(\sigma') = z_{\rho(\sigma)}\delta_{\rho(\sigma)\rho(\sigma')}$$

$$\frac{1}{n!} \sum_{\sigma \in S_p} \chi^\lambda(\sigma)\chi^{\lambda'}(\sigma) = \delta_{\lambda\lambda'},$$

where $z_{\rho(\sigma)}$ is the order of the centralizer of σ.

The space $(\mathbb{C}^n)^{\otimes p}$ is a representation space for the group S_p via the action of permuting the tensors. It is also a representation space for $U(n)$ via the action of multiplying by the p-fold tensor product of an element of $U(n)$. These two representations are related by Schur-Weyl duality

Theorem V.2.6 (Schur-Weyl duality)**.** *As a representation of $U(n) \times S_p$,*

$$(\mathbb{C}^n)^{\otimes p} = \bigoplus_{\lambda \vdash p} V^\lambda_{U(n)} \otimes V^\lambda_{S_p}$$

where $V^{\lambda}_{U(n)}$ and $V^{\lambda}_{S_p}$ are the irreducible components of the irreps of $U(n)$ and S_p respectively and the sum is over partitions with $l(\lambda) \leq n$.

A direct consequence of this theorem is that any operator in $(\mathbb{C}^n)^{\otimes p}$ which commutes with the action of $U(n)$ is a linear combination of permutation matrices $D_n(\sigma) = \sum_{i_1,\ldots,i_p=1}^{n} |i_{\sigma(1)}\rangle \cdots |i_{\sigma(p)}\rangle\langle i_1| \cdots \langle i_p|$. In particular, we have the following theorem for integrals over the unitary group with respect to the Haar measure.

Theorem V.2.7. *Let M be a matrix over $(\mathbb{C}^n)^{\otimes p}$, then*

$$I(M) = \int_{\mathcal{U}(n)} U^{\otimes p} M U^{\dagger \otimes p} dU = \sum_{\sigma \in S_p} \alpha_\sigma D_n(\sigma)$$

where $D_n(\sigma)$ is the representation of $\sigma \in S_p$ which acts on $(\mathbb{C}^n)^{\otimes p}$ by permutting the tensors.

The coefficients α_σ are determined by the equation

$$\operatorname{tr} I(M) D_n(\pi) = \sum_{\sigma \in S_p} \alpha_\sigma d^{\#(\sigma\pi)} = d^k \sum_{\sigma \in S_p} A_{\sigma^{-1}\pi} \alpha_\sigma \tag{V.2}$$

where $A_{\sigma\pi} = d^{\#(\sigma^{-1}\pi)-p}$, with $\pi, \sigma \in S_p$. Thus, in order to compute the coefficients α_σ it is enough to give the inverse of the matrix A.

Definition V.2.8. *The Weingarten function $Wg(n, \sigma)$ is a function taking as inputs a dimension parameter n and a permutation σ in the symmetric group S_p such that the inverse of A in Eq. (V.2) is given by $A^{-1}_{\sigma\pi} = d^k Wg(n, \pi^{-1}\sigma)$. Then it is given by*

$$Wg(n, \sigma) = \frac{1}{p!^2} \sum_{\lambda \vdash p} \frac{(\chi^\lambda(1))^2 \chi^\lambda(\sigma)}{s_{\lambda,n}(1)} \tag{V.3}$$

Putting all together we have the following theorem from [22], which states that the average of a monomial over the unitary group can be computed in terms of sums of Weingarten functions.

Theorem V.2.9. *Let n be a positive integer and $i = (i_1, ..., i_p)$, $i' = (i'_1, ..., i'_p)$, $j = (j_1, ..., j_p)$ and $j' = (j'_1, ..., j'_p)$ be p-tuples of positive integers from $1, 2, ..., n$. Then*

$$\int_{\mathcal{U}(n)} U_{i_1 j_1} ... U_{i_p j_p} \overline{U_{i'_1 j'_1}} ... \overline{U_{i'_p j'_p}} dU = \sum_{\sigma, \tau \in S_p} \delta_{i_1 i'_{\sigma(1)}} ... \delta_{i_p i'_{\sigma(p)}} \delta_{j_1 j'_{\tau(1)}} ... \delta_{j_p j'_{\tau(p)}} Wg(n, \tau\sigma^{-1}).$$

In [24] the authors introduce a graphical paradigm in order to simplify the computation of the average of polynomials over the unitary group. Consider a homogeneous polynomial $P(U)$ of degree p in U and $\overline{U}$ then

$$\mathbb{E}_U(P(U)) = \sum_{\sigma,\tau\in S_p} C_{(\sigma,\tau)} Wg(n, \tau\sigma^{-1}), \tag{V.4}$$

where the coefficients $C_{(\sigma,\tau)}$ can be computed by the following procedure in Figures V.2, V.3 and V.4. One has to enumerate the matrices U and $\overline{U}$ respectively from 1 to p and for any two permutations $\sigma, \tau \in S_p$ we delete the U and $\overline{U}$ boxes and we connect the white square and circle in U_i with the white square and circle respectively in $\overline{U_{\sigma(i)}}$, and analogously with the black objects and the τ permutation. Now, loops represent traces over the matrices involved in it. If there is no matrix involved in a loop then it represents the trace of the identity of the system. Finally, if there are paths that are not loops they translate into the contraction with the boundary conditions that appear in it. The number $C_{(\sigma,\tau)}$ is just the product of the values of all the contractions.

In this chapter we will be interested in computing the average of a polynomial over the unitary group as a function of its degree p and the dimension of the unitary group $U(n)$ when both quantities are growing at a given ratio. For that, we need to give a novel asymptotic bound of the Weingarten function.

Theorem V.2.10. *Let p, n and k be nonnegative integers such that $p^k \leq n$. Then there exists a constant K depending only on k such that for any $\sigma \in S_p$,*

$$|Wg(n, \sigma)| \leq K n^{-p-|\sigma|(1-2/k)}.$$

Proof. We recall, see [51], that for any partition $\lambda \vdash p$ of the integer p,

$$s_{\lambda,n}(1) = \frac{\chi^\lambda(1)}{p!} \prod_{i=1}^{p} (n - \lambda_i)$$

where λ_i is an integer in $\{-p+1, ..., p-1\}$. Equivalently, the Weingarten function becomes

$$Wg(n, \sigma) = \frac{1}{n^p p!} \sum_{\lambda\vdash p} \frac{\chi^\lambda(1)\chi^\lambda(\sigma)}{\prod_{i=1}^{p}(1 - \lambda_i/n)}. \tag{V.5}$$

Consider the function

$$f_\lambda : z \to (\prod_{i=1}^{p}(1 - z\lambda_i))^{-1}$$

This function is holomorphic in a neighborhood of zero. Moreover $2 \leq k$, since $p^2 \leq n$, we have, for any $|z| \leq p^{-2}$,

$$|f_\lambda(z)| \leq \frac{1}{(1 - p^{-2}(p-1))^p} \leq e$$

As a consequence, writing $f_\lambda(z) = \sum_{i\geq 0} a_{i,\lambda} z^i$, we obtain the Cauchy estimate

$$|a_{i,\lambda}| \leq ep^{2i}.$$

But Eq. (V.5) implies that

$$Wg(n,\sigma) = \frac{1}{n^p p!} \sum_{\lambda \vdash p} \chi^\lambda(1)\chi^\lambda(\sigma)(1 + \sum_{i\geq 1} a_{i,\lambda} n^{-i}).$$

Taking absolute value, using the fact that $|\chi^\lambda(\sigma)| \leq \chi^\lambda(1)$ and considering the orthogonality relations for irreducible characters we have

$$|Wg(n,\sigma)| \leq \frac{1}{n^p p!} \sum_{\lambda \vdash p} \chi^\lambda(1)|\chi^\lambda(\sigma)|(1 + \sum_{i\geq 1} |a_{i,\lambda}| n^{-i}) \leq n^{-p}(1 + \sum_{i\geq 1} ep^{2i} n^{-i}). \tag{V.6}$$

Therefore the coefficient in n^{-p-i} has absolute value smaller than ep^{2i}. But all coefficients are zero until $i = |\sigma|$ [22], therefore

$$|Wg(n,\sigma)| \leq n^{-p-|\sigma|} e(1 + \frac{p^2}{n} + (\frac{p^2}{n})^2 + ...)p^{2|\sigma|}.$$

For $n \geq 2$, and since $p^k \leq n$, this implies $p^{2|\sigma|} \leq n^{2|\sigma|/k}$. Furthermore $(1 + \frac{p^2}{n} + (\frac{p^2}{n})^2 + ...)$ can be bounded by a universal constant (5, for example). The result follows. □

Note, that an asymptotic bound of the Weingarten function, which states

$$Wg(n,\sigma) = n^{-p-|\sigma|}(Moeb(\sigma) + O(n^{-2})),$$

where $Moeb(\sigma)$ is a function that can be upper bounded by the (p-1)-th Catalan number, was already proven in [25]. Unfortunately, this is not useful in this case as the term $O(n^{-2})$ hides an undetermined dependence on p. Also, the very recent work [117] gives a bound of the Weingarten function with explicit dependence on p. Nevertheless, this bound does not seem to be sufficient for our purpose.

V.3 Proof of Theorem V.0.1

Recall that we are considering the ensemble of MPSs defined by the tuple $(U, L, R) = (U, V, W, \Lambda, \Omega)$ where U, V and W are distributed with respect to the Haar measure in the respective unitary group, Λ is distributed according to the Lebesgue measure in $[0,1]^D$ and Ω according to any permutation invariant probability measure in $\mathbb{S}_1([0,1]^D)$. To prove Theorem V.0.1 we need to compute the mean of the trace normalized version of $f(\rho) = \mathrm{tr}(\rho_l^2(U, L, R))$ over the introduced ensemble and its Lipschitz constant. The

difficulty of this calculus comes from computing the mean of the function. To simplify our computations we will first compute the mean and the Lipschitz constant for both function $f(\rho)$ and its normalization function $g(\rho) = (\operatorname{tr} \rho_l(U, L, R))^2$ and then argue about the concentration of $\operatorname{tr}(\rho_{Norm}^2) = f(\rho)/g(\rho)$.

To organize the computations and the reasoning used in the bound of the mean of $f(\rho)$ we prove the following two lemmas.

Lemma V.3.1. *Let $\alpha, \beta, \gamma \in S_p$,*

a) the quantity $|\gamma^{-1}\alpha\gamma\alpha^{-1}\beta| + |\beta|$ is an even number.

b) If $\gamma^{-1}\alpha\gamma\alpha^{-1}\beta = c$ and $\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta = c$, then $\alpha'^{-1}\alpha$ commutes with γ.

c) If $p = 2n+4$ and $\gamma = (2n+1, 1, 2, ..., n, 2n+3)(2n+2, n+1, n+2, ..., 2n, 2n+4)$ and $\alpha(2n+i) = 2n+i$ for $i = 1, ..., 4$. Then the function that takes (α, β) to (g, h) with $g = \gamma^{-1}\alpha\gamma\alpha^{-1}$ and $h = \beta\alpha^{-1}$ is one to one.

Proof. a) The result follows from the fact that the parity of $|\alpha\beta|$ is the same as the parity of $|\alpha| + |\beta|$.

b) If $\gamma^{-1}\alpha\gamma\alpha^{-1}\beta = c$ and $\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta = c$, then $\alpha\gamma\alpha^{-1} = \alpha'\gamma\alpha'^{-1}$. Multiplying by the inverse of the right hand side we have $\gamma^{-1}\alpha'^{-1}\alpha\gamma\alpha^{-1}\alpha' = \mathbb{1}$ which happens if and only if $\alpha'^{-1}\alpha$ commutes with γ.

c) If α is fixed, the change $h = \beta\alpha^{-1}$ is clearly one to one. Now, by b), the change $g = \gamma^{-1}\alpha\gamma\alpha^{-1}$ is one to one if and only if $\gamma^{-1}\alpha\gamma\alpha^{-1} = \mathbb{1}$ has only the trivial solution $\alpha = \mathbb{1}$, which can be easily checked to be the case by the definition of γ and the constraints in α. □

Lemma V.3.2. *Let $L \in \mathcal{L}$ and $R \in \mathcal{R}$ be given at random with respect to the measures introduced in Section V.1. For any $\Omega \in \mathbb{S}_1([0,1]^D)$, we have $\mathbb{E}[\operatorname{tr}(L)] = D/2$, $\mathbb{E}[\operatorname{tr}(L^2)] = D/3$, $\mathbb{E}[\operatorname{tr}(R)] = 1$, $\mathbb{E}[\operatorname{tr}(R^2)] \leq 1$, $\mathbb{E}[\operatorname{tr}(LR)] = 1/2$, $\mathbb{E}[\operatorname{tr}(LRR)] \leq 1/2$, $\mathbb{E}[\operatorname{tr}(LLR)] = 1/3$, $\mathbb{E}[\operatorname{tr}(LLRR)] \leq 1/3$ and $\mathbb{E}[\operatorname{tr}(LRLR)] \leq 1/4 + 1/12D$.*

Proof. These averages are not difficult to compute directly, but they can also be computed using the graphical calculus described in Section V.2 as a warming up for the forthcoming computations. We compute the last one as an example.

$$\mathbb{E}[\operatorname{tr}(LRLR)] = \mathbb{E}[\operatorname{tr}(V\Lambda V^\dagger W\Omega W^\dagger V\Lambda V^\dagger W\Omega W^\dagger)] = \mathbb{E}[\operatorname{tr}(U\Lambda U^\dagger\Omega U\Lambda U^\dagger\Omega)],$$

where $\Lambda \in [0,1]^D$, $\Omega \in \mathbb{S}_1([0,1]^D)$ and $U, V, W \in U(D)$ and the second equation follows by the invariance of the Haar measure. Using that $\mathbb{E}_\Lambda[\operatorname{tr}\Lambda] = D/2$, $\mathbb{E}_\Lambda[\operatorname{tr}(\Lambda^2)] = D/3$,

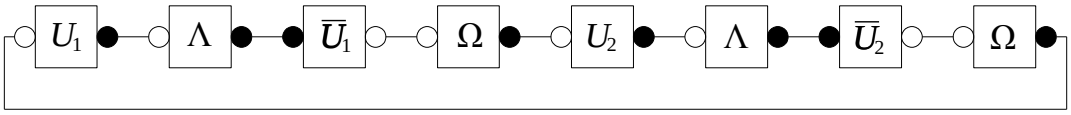

Figure V.3: Computation of $\mathbb{E}_{L,R}[\mathrm{tr}(LRLR)]$ using Weingarten graphical calculus: for any two permutations $\alpha, \beta \in S_2$ delete the U and $\overline{U}$ matrices, join the white circle of U_i with the white circle of $U_{\alpha(i)}$, join the black circle of U_i with the black circle of $U_{\beta(i)}$. The number $C_{(\alpha,\beta)}$ is the product of the traces involved in the new picture.

$\mathrm{tr}(\Omega^2) \leq 1$ and $(\mathrm{tr}\,\Omega)^2 = 1$ together with the graphical calculus in Figure V.3 we get

$$\begin{aligned}
\mathbb{E}_{L,R}[\mathrm{tr}(LRLR)] &= \mathbb{E}_{\Lambda,\Omega}[\sum_{\alpha,\beta\in S_2} C_{(\alpha,\beta)} Wg(D, \alpha\beta^{-1})] = \\
&= \mathbb{E}_{\Lambda,\Omega}[((\mathrm{tr}\,\Lambda)^2\,\mathrm{tr}(\Omega^2) + \mathrm{tr}(\Lambda^2)(\mathrm{tr}\,\Omega)^2) Wg(D,(1)(2)) + \\
&\qquad - ((\mathrm{tr}\,\Lambda)^2(\mathrm{tr}\,\Omega)^2 + \mathrm{tr}(\Lambda^2)\,\mathrm{tr}(\Omega^2)) Wg(D,(12))] \leq \\
&\leq (\frac{D^2}{4} + \frac{D}{3})(Wg(D,(1)(2)) + Wg(D,(12))) = \\
&= (\frac{D^2}{4} + \frac{D}{3})(\frac{1}{D^2-1} + \frac{-1}{D(D^2-1)}) \leq \frac{1}{4} + \frac{1}{12D},
\end{aligned} \tag{V.7}$$

where the values of the Weingarten function are computed by Eq. (V.3). □

Now, we have all the ingredients in order to compute the averages of $f(\rho)$ and $g(\rho)$.

Theorem V.3.3. *Let ρ_l be taken at random from the ensemble introduced. Then, for any $\Omega \in \mathbb{S}_1([0,1]^D)$ and $U \in U(dD)$, we have*

$$\mathbb{E}_{\Lambda,V,W}(\mathrm{tr}\,\rho_l(\Lambda,\Omega,U,V,W)) = 1/2$$

Proof.

$$\mathbb{E}_{\Lambda,V,W}(\mathrm{tr}\,\rho_l(\Lambda,\Omega,U,V,W)) = \mathbb{E}_{\Lambda}(\mathrm{tr}\,\mathbb{E}_{V,W}[V\Lambda V^\dagger \mathcal{E}^n(W\Omega W^\dagger)]) =$$

$$= \mathbb{E}_{\Lambda}(\mathrm{tr}_A\,\mathrm{tr}_{B_1,\ldots,B_n}[\mathrm{tr}(\Lambda)\frac{\mathbb{1}_A}{D}\mathcal{E}^n(\mathrm{tr}(\Omega)\frac{\mathbb{1}_A}{D})]) = \mathbb{E}_{\Lambda}(\mathrm{tr}_A\,\mathrm{tr}(\Lambda)\frac{\mathbb{1}_A}{D^2}) = \mathbb{E}_{\Lambda}(\mathrm{tr}(\Lambda)/D) = 1/2.$$

The first equality follows by linearity of the trace, the third because $\mathbb{1}_A$ is the fixed point of $tr_B(\mathcal{E})$, the second and fourth just by computing the averages themselves. □

Note that in this proof we are averaging over V and W, and our expression is a polynomial of degree one with respect to them. This, together with the fact that the

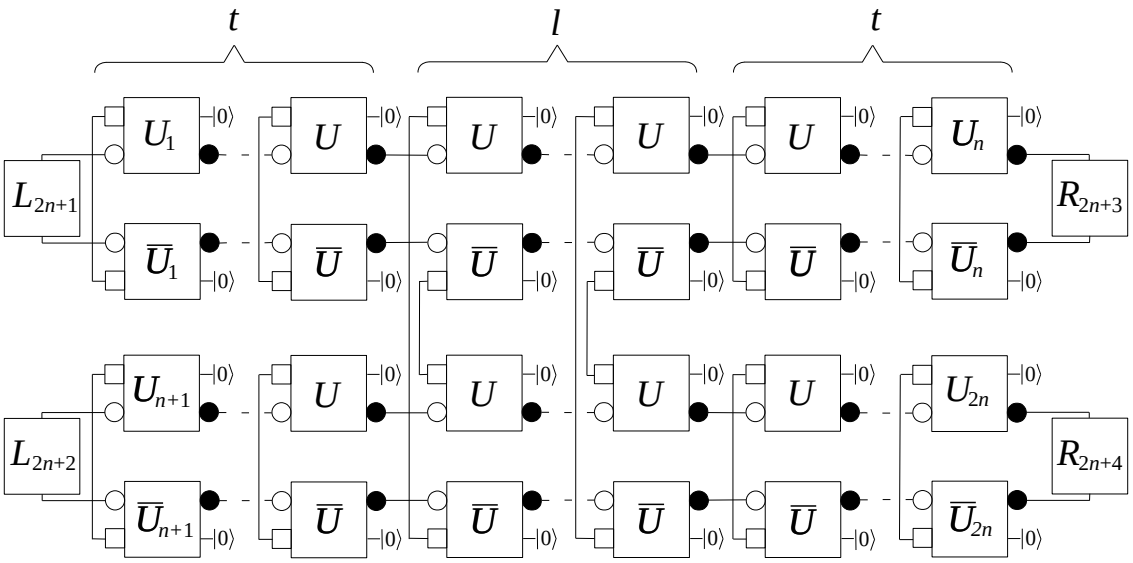

Figure V.4: Computation of $\mathbb{E}_U(\operatorname{tr}\rho_l^2(L,R,U))$ using Weingarten graphical calculus: for any two permutations $\alpha,\beta \in S_{2n}$ delete the U and $\overline{U}$ matrices, join the white circle of U_i with the white circle of $U_{\alpha(i)}$, join the black circle of U_i with the black circle of $U_{\beta(i)}$. The number $C_{(\alpha,\beta)}$ is the product of the traces involved in the new picture.

average is independent of U make it easy to compute the average. The bound of the other function is much more involved and makes use of the asymptotic bound of the Weingarten function (Theorem V.2.10) and Lemmas V.3.1 and V.3.2.

Theorem V.3.4. *Let ρ_l be taken at random from the ensemble introduced and $D \geq n^5$. For any $\Omega \in \mathbb{S}_1([0,1]^D)$, then*

$$\mathbb{E}(\operatorname{tr}\rho_l^2) \leq \frac{1}{4d^l} + O(D^{-1/5}).$$

Proof. We can take first the average in U and using Eq. (V.4) together with the bound of Theorem V.2.10 we have

$$\begin{aligned}\mathbb{E}_{L,R,U}[\operatorname{tr}\rho_l^2(L,R,U)] &= \sum_{\alpha,\beta\in S_l}\mathbb{E}_{L,R}[C_{(\alpha,\beta)}]Wg(Dd,\beta\alpha^{-1}) = \\ &= \mathbb{E}_{L,R}[C_{(\mathbb{1},\mathbb{1})}]Wg(Dd,\mathbb{1}) + \sum_{(\alpha,\beta)\neq(\mathbb{1},\mathbb{1})}\mathbb{E}_{L,R}[C_{(\alpha,\beta)}]Wg(Dd,\beta\alpha^{-1}) \leq \\ &\leq (Dd)^{-2n}(1+O(D^{-3/5}))\mathbb{E}_{L,R}[C_{(\mathbb{1},\mathbb{1})}] + K\sum_{(\alpha,\beta)\neq(\mathbb{1},\mathbb{1})}\mathbb{E}_{L,R}[C_{(\alpha,\beta)}](Dd)^{-2n-3/5|\beta\alpha^{-1}|},\end{aligned}$$

where we are separating the case where $\alpha = \beta = \mathbb{1}$. The reason to do so is that this term is the largest one in the sum (as it will become clear through the proof). In the last inequality we are also using the bound $Wg(Dd,\mathbb{1}) \leq (Dd)^{-2n}(1+O(D^{-3/5}))$ that can be deduced from Eq. (V.6) using that $n^5 \leq D$.

In order to compute the coefficients $C_{(\alpha,\beta)}$ we apply the graphical Weingarten Calculus to Figure V.4. That is, given a permutation α that links the white squares and circles of the $U's$ with the white squares and circles in $\overline{U}'s$ and a permutation β that links the black circles of the $U's$ with the black circles in $\overline{U}'s$. We numerate the U matrices from left to right and top to bottom and the same for the $\overline{U}$ matrices. Moreover, we enumerate the matrices L as $2n+1$ and $2n+2$ and the matrices R as $2n+3$ and $2n+4$.

Now the links (from left to right) between the circles of the matrices $U's$, L and R are given by the function $\gamma = \begin{pmatrix} 2n+1 & 1 & 2 & ... & n \\ 1 & 2 & 3 & ... & 2n+3 \end{pmatrix}\begin{pmatrix} 2n+2 & n+1 & n+2 & ... & 2n \\ n+1 & n+2 & n+3 & ... & 2n+4 \end{pmatrix}$. One can add two extra (non-existing) links $\gamma(2n+3) = 2n+1$ and $\gamma(2n+4) = 2n+2$; that way γ is a permutation. Analogously, we have the same permutation γ for the $\overline{U}$ matrices. The permutation relating the links of the squares of U and $\overline{U}$ is $\tau = (t+1, n+t+1)(t+2, n+t+2)...(t+l, n+t+l)$. Besides, define $\alpha' = \alpha(2n+1)(2n+2)(2n+3)(2n+4)$ and $\beta' = \beta(2n+1)(2n+2)(2n+3)(2n+4)$ as the permutation α, β but considering it as an element of S_{2n+4}.

The number of loops relating the circles in the computation of $C_{(\alpha,\beta)}$ is $\#\gamma^{-1}\alpha'\gamma\beta'^{-1} - 2 = 2n+2-|\gamma^{-1}\alpha'\gamma\beta'^{-1}|$ (see Section V.2). Note that we are subtracting 2 loops $(2n+1)(2n+2)$ that we have added when including the (non-existing) links of the permutation γ. The number of loops relating the squares is $\#\tau\alpha = 2n - |\tau\alpha|$. All the loops are trivial and thus they correspond to the dimension of the system, except those where L or R appear, in which we will take averages and use the bounds of Lemma V.3.2. Hence, we can write

$$\mathbb{E}_{L,R}[C_{(\alpha,\beta)}] = \mathbb{E}_{L,R}[M]D^{2n+2-|\gamma^{-1}\alpha'\gamma\beta'^{-1}|-m}d^{2n-|\tau\alpha|}, \tag{V.8}$$

where m is the number of loops in which the matrices L and R are involved and M is the product of the traces of these loops. For example, consider (α,β) such that $2n+1$ and $2n+2$ are in the same cycle of $\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta$ and $2n+3$ and $2n+4$ are in different cycles each, then $M = \operatorname{tr}(L^2)\operatorname{tr}(R)\operatorname{tr}(R)$ and $m = 3$.

For $\alpha = \beta = \mathbb{1}$, we have

$$\mathbb{E}_{L,R}[C_{(\mathbb{1},\mathbb{1})}] = \mathbb{E}_{L,R}[(\operatorname{tr} L)^2(\operatorname{tr} R)^2]D^{2n-2}d^{2n-l} = 1/4D^{2n}d^{2n-l}.$$

For $(\alpha, \beta) \neq (\mathbb{1}, \mathbb{1})$, in order to bound these coefficients, Eq. V.8 seems to indicate that one should consider all the possible combinations of L and R in different loops. Nevertheless, $\mathbb{E}_{L,R}[M]D^{-m}$ can be bounded adequately distinguishing the following two cases:

a) $(\alpha, \beta) \in \mathcal{A}_{2n}$, where $\mathcal{A}_{2n}$ is the set of tuples $(\alpha, \beta) \neq (\mathbb{1}, \mathbb{1})$ in which $2n+3$ and $2n+4$ are not in the same cycle of the permutation $\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta$, that is, the R matrices appear in different loops. In all the possible combinations of L and R in different loops included in this case we have $\mathbb{E}_{L,R}[M]D^{-m} \leq D^{-2}/3$. Therefore

$$\mathbb{E}_{L,R}[C_{(\alpha,\beta)}] \leq 1/3D^{2n-|\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta|}d^{2n-|\tau\alpha|} \leq D^{2n-|\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta|}d^{2n}.$$

Making the change of variables $h = \beta\alpha^{-1}$, $g = \gamma^{-1}\alpha'\gamma\alpha'^{-1}$ that is proven to be one to one in Lemma V.3.1, and denoting $h' = h(2n+1)(2n+2)(2n+3)(2n+4)$ we get that

$$\sum_{(\alpha,\beta)\in A_{2n}} \mathbb{E}_{L,R}[C_{(\alpha,\beta)}]Wg(Dd, \beta\alpha^{-1}) \leq K \sum_{(g,h)\in S_{2n+4}\times S_{2n}} D^{-|gh'^{-1}|-(3/5)|h|}d^{-(3/5)|h|} =$$

$$= K \sum_{g\neq\mathbb{1}\in S_{2n+4}} D^{-|g|} + K \sum_{h\neq\mathbb{1},g\in S_{2n+4}} D^{-|gh|-3/5|h|} \leq$$

$$\leq K\left(\sum_{|g|=1}^{2n+3}\left(\frac{(2n+4)(2n+3)}{2D}\right)^{|g|} + \sum_{|g|=0}^{2n+3}\left(\frac{(2n+4)(2n+3)}{2D}\right)^{|g|}\sum_{|h|=1}^{2n-1}\left(\frac{2n(2n-1)}{2D^{3/5}}\right)^{|h|}\right) \leq$$

$$\leq K\left(\frac{(2n+4)(2n+3)}{2D-(2n+4)(2n+3)} + \frac{2D}{2D-(2n+4)(2n+3)}\frac{2n(2n-1)}{2D^{3/5}-2n(2n-1)}\right).$$

In the second inequality we just bound the number of permutations with a given number of transpositions and the last inequality is just the sum of a geometric series. As $D \geq n^5$ we get further

$$\sum_{(\alpha,\beta)\in A_{2n}} \mathbb{E}_{L,R}[C_{(\alpha,\beta)}]Wg(Dd, \beta\alpha^{-1}) \leq O(D^{-1/5})$$

b) $(\alpha, \beta) \in \mathcal{B}_{2n}$, where $\mathcal{B}_{2n}$ is the set of tuples in which $2n+3$ and $2n+4$ are in the same cycle of the permutation $\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta$, that is, both R matrices appear in the same loop. In all the possible combinations of L and R included in this case we have $\mathbb{E}_{L,R}[M]D^{-m} \leq D^{-1}/3$. Therefore

$$\mathbb{E}_{L,R}[C_{(\alpha,\beta)}] \leq 1/3D^{2n+1-|\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta|}d^{2n-|\tau\alpha|} \leq D^{2n+1-|\gamma^{-1}\alpha'\gamma\alpha'^{-1}\beta|}d^{2n}.$$

Applying the same change of variables as in case a) and considering $\mathcal{B}'_{2n}$ the image of $\mathcal{B}_{2n}$ under the change of variables, we get

$$\sum_{(\alpha,\beta)\in\mathcal{B}_{2n}} \mathbb{E}_{L,R}[C_{(\alpha,\beta)}]Wg(Dd,\beta\alpha^{-1}) \leq K \sum_{(g,h)\in\mathcal{B}'_{2n}} D^{1-|gh'^{-1}|-(3/5)|h|}d^{-(3/5)|h|}.$$

In order to bound this sum one has to proceed more carefully. The proof follows by bounding independently over the different cases where: $h = \mathbb{1}$, $h = (2n+3, 2n+4)$, h is a different transposition, and the rest of terms. For all these cases one has to take into account the properties of the elements in $\mathcal{B}'_{2n}$, that is, $2n+3$ and $2n+4$ belongs to the same cycle of gh'^{-1} and the parity of $|gh'^{-1}| + |h|$ that is proven in Lemma V.3.1. Following this procedure one can prove that

$$\sum_{(\alpha,\beta)\in\mathcal{B}_{2n}} \mathbb{E}_{L,R}[C_{(\alpha,\beta)}]Wg(Dd,\beta\alpha^{-1}) \leq O(D^{-1/5})$$

The result follows joining the two cases and the case $\alpha = \beta = \mathbb{1}$

□

In order to apply the concentration of measure phenomenon we only need to compute the Lipschitz constant of the functions we are interested in.

Theorem V.3.5 (Lipschitz constants)**.** *For any* $\Omega \in \mathbb{S}_1([0,1]^D)$*, let* $f(U,V,W,\Lambda) = (\operatorname{tr}\rho_l(U,V,W,\Lambda,\Omega))^2$ *and* $g(U,V,W,\Lambda) = \operatorname{tr}\rho_l^2(U,V,W,\Lambda,\Omega)$ *where*

$$\rho_l(U,V,W,\Lambda,\Omega) = \operatorname{tr}_{A,B_{All\setminus l}}(V\Lambda V^\dagger U_{A,B_1}\cdots U_{A,B_n}(W\Omega W^\dagger \otimes (|0\rangle\langle 0|)^{\otimes n})U^\dagger_{A,B_n}\cdots U^\dagger_{A,B_1}).$$

Then the Lipschitz constants of both functions are upper bounded by $4n+10$*.*

Proof. We use the notation $\|\cdot\|_p$ for the Schatten p-norm. For the first function we have

$$\begin{aligned}
\|f\|_{Lip} &= \frac{|f(U,V,W,\Lambda,\Omega)-f(U',V',W',\Lambda',\Omega)|}{d((U,V,W,\Lambda),(U',V',W',\Lambda'))} \leq \frac{|(\operatorname{tr}\rho_l(U,V,W,\Lambda,\Omega))^2-(\operatorname{tr}\rho_l(U',V',W',\Lambda',\Omega))^2|}{d((U,V,W,\Lambda),(U',V',W',\Lambda'))} = \\
&= \frac{|(\operatorname{tr}\rho_l(U,V,W,\Lambda,\Omega)-\operatorname{tr}\rho_l(U',V',W',\Lambda',\Omega))(\operatorname{tr}\rho_l(U,V,W,\Lambda,\Omega)+\operatorname{tr}\rho_l(U',V',W',\Lambda',\Omega))|}{d((U,V,W,\Lambda),(U',V',W',\Lambda'))} \leq \\
&\leq \frac{2|\operatorname{tr}(\rho_l(U,V,W,\Lambda,\Omega)-\rho_l(U',V',W',\Lambda',\Omega))|}{d((U,V,W,\Lambda),(U',V',W',\Lambda'))} \leq \frac{2\operatorname{tr}|\rho_l(U,V,W,\Lambda,\Omega)-\rho_l(U',V',W',\Lambda',\Omega)|}{d((U,V,W,\Lambda),(U',V',W',\Lambda'))} \leq \\
&\leq \frac{2\|V\Lambda V^\dagger U^n(W\Omega W^\dagger \otimes (|0\rangle\langle 0|)^{\otimes n})(U^\dagger)^n - V'\Lambda' V'^\dagger U'^n(W'\Omega W'^\dagger \otimes (|0\rangle\langle 0|)^{\otimes n})(U'^\dagger)^n\|_1}{\|U-U'\|_2+\|V-V'\|_2+\|W-W'\|_2+\|\Lambda-\Lambda'\|_\infty},
\end{aligned}$$

where we are using standard inequalities and for the sake of simplicity we are denoting by the same U unitaries that are acting on different systems and with the same letter V a unitary and its tensor product with the identity. Adding and substracting terms and applying the triangular inequality we get 2n+5 terms of the following form

$$\frac{2\|V^*\Lambda^*V^{\dagger *}U^{*n}(W^*\Omega W^{*\dagger}\otimes(|0\rangle\langle 0|)^{\otimes n})(U^{*\dagger})^n\|_1}{\|U-U'\|_2+\|V-V'\|_2+\|W-W'\|_2+\|\Lambda-\Lambda'\|_\infty},$$

where any X^* stands for X, X' or $X-X'$ and in any term the latter only appears once. Then

$$\|f\|_{Lip}\leq\frac{(4n+10)\|V^*\Lambda^*V^{\dagger *}U^{*n}(W^*\Omega W^{*\dagger}\otimes(|0\rangle\langle 0|)^{\otimes n})(U^{*\dagger})^n\|_1}{\|U-U'\|_2+\|V-V'\|_2+\|W-W'\|_2+\|\Lambda-\Lambda'\|_\infty}.$$

Applying the inequality $\|XY\|_1\leq\|X\|_1\|Y\|_\infty$ we get

$$\|f\|_{Lip}\leq(4n+10)\frac{\|V^*\|_\infty\|\Lambda^*\|_\infty\|V^{\dagger *}\|_\infty\|U^{*n}\|_\infty\|W^*\|_\infty\|\Omega\|_1\|W^{*\dagger}\|_\infty\|(U^{*\dagger})^n\|_\infty}{\|U-U'\|_2+\|V-V'\|_2+\|W-W'\|_2+\|\Lambda-\Lambda'\|_\infty}.$$

Now, by the decomposition we have done, any term has only one norm in the numerator of the form of the ones in the denominator. The other norms in the numerator are trivially bounded by one. Thus we get

$$\|f\|_{Lip}\leq 4n+10$$

For the second function we have

$$\begin{aligned}\|g\|_{Lip}&=\frac{|g(U,V,W,\Lambda,\Omega)-g(U',V',W',\Lambda',\Omega)|}{d((U,V,W,\Lambda),(U',V',W',\Lambda'))}\leq\\&\leq\frac{|\operatorname{tr}(\rho_l^2(U,V,W,\Lambda,\Omega)-\rho_l^2(U',V',W',\Lambda',\Omega))|}{\|U-U'\|_2+\|V-V'\|_2+\|W-W'\|_2+\|\Lambda-\Lambda'\|_\infty}\leq 4n+10\end{aligned}$$

where the result follows using the same techniques.

□

Now we can show which is the behavior of the 2-Rényi entropy, or equivalently the purity of the normalized state $\rho_{Norm}=\rho_l/\operatorname{tr}(\rho_l)$.

Theorem V.3.6. *Let ρ_l be taken at random from the ensemble introduced with $D\geq n^5$. Then $\operatorname{tr}(\rho_{Norm}^2)=\operatorname{tr}\rho_l^2/(\operatorname{tr}\rho_l)^2\leq 1/d^l+O(D^{-1/5})$ except with probability exponentially small in D.*

Proof. Putting together the concentration of measure phenomenon V.2.2, the bounds on the Lipschitz constant V.3.5 and the union bound, we have for all $\Omega\in\mathbb{S}_1([0,1]^D)$ that except with probability $c_1e^{-c_2\epsilon^2D/n^2}$

$$\operatorname{tr}(\rho_l^2)\leq\mathbb{E}(\operatorname{tr}(\rho_l^2))+\epsilon\qquad\text{and}\qquad(\operatorname{tr}\rho_l)^2\geq\mathbb{E}((\operatorname{tr}\rho_l)^2)-\epsilon$$

both at the same time where c_1 and c_2 are universal constants. Thus, we can bound

$$\frac{\operatorname{tr}(\rho_l^2)}{(\operatorname{tr}\rho_l)^2} \leq \frac{\mathbb{E}(\operatorname{tr}(\rho_l^2)) + \epsilon}{\mathbb{E}((\operatorname{tr}\rho_l)^2) - \epsilon} \leq \frac{\mathbb{E}(\operatorname{tr}(\rho_l^2)) + \epsilon}{(\mathbb{E}(\operatorname{tr}\rho_l))^2 - \epsilon} \leq \frac{\frac{1}{4d^l} + O(D^{-1/5}) + \epsilon}{1/4 - \epsilon} = \frac{1}{d^l} + O(D^{-1/5}),$$

where the second inequality follows from Jensen's inequality, the third inequality follows from Theorem V.3.3 and V.3.4 and in the last equality we have used that we can take $\epsilon = O(D^{-1/5})$. The result follows. □

As a corollary we can bound the distance between the reduced density matrix of a generic random MPS and the completely mixed state.

Corollary V.3.7. *Let ρ_l be taken at random from the ensemble introduced with $D \geq N^5$. Then $\|\rho_l/\operatorname{tr}\rho_l - \mathbb{1}/d^l\|_\infty \leq O(D^{-1/10})$ except with probability exponentially small in D.*

Proof. $\rho_{Norm} = \rho_l/\operatorname{tr}\rho_l$ is trace normalized, that is, its eigenvalues sum up to one. Thus, in order to have an eigenvalue of ρ_{Norm} as far as possible from $1/d^l$ fulfilling that $\operatorname{tr}(\rho_{Norm}^2) \leq \frac{1}{d^l} + O(D^{-1/5})$, the distribution of eigenvalues optimizing this problem is the one that has one eigenvalue as small or big as possible and the rest all equal. In both cases the distance between this eigenvalue and $1/d^l$ is upper bounded by $O(D^{-1/10})$. □

Finally we can easily prove our main theorem, which states that the reduced density matrix of a random MPS has generically maximum entropy.

Proof of Theorem V.0.1.

A direct application of Jensen's inequality shows that $S(\rho) = -\operatorname{tr}(\rho\log\rho) \geq -\log\operatorname{tr}(\rho^2)$. Using Theorem V.3.6 and trivial inequalities we have

$$S(\rho_{Norm}) \geq -\log\frac{1 + d^l O(D^{-1/5})}{d^l} = \log(d^l) - \log(1 + d^l O(D^{-1/5})) \geq \log(d^l) - d^l O(D^{-1/5})$$

except with probability exponentially small in D. □

V.4 Discussion

We have shown how reduced density matrices of small subsystems of translational invariant random MPS have generically maximum entropy or alternatively the subsystem is maximally entangled with the rest of the system. This can be read as recovering Jayne's principle of maximum entropy in the situation where the prior information to incorporate in the sampling procedure is the locality and homogeneity of the interactions. For that we have relied on the (well justified) fact that MPSs are the right representation for ground

states of one dimensional local Hamiltonians and in the natural way of sampling MPSs based on the symmetry principle.

Alternatively one could consider two similar interesting models in which there are no boundaries, the infinite spin chain and the circular spin chain. Unfortunately the same argument used here does not apply to these models.

In the circular spin chain the Lipschitz constant of the functions under consideration is not good enough. For the infinite spin chain one does not even have the description of the functions in terms of polynomials over the unitary group. Nevertheless, in this case the reduced density matrix of l particles can be described as

$$\rho_l = \mathcal{E}^l(\Lambda_U),$$

where Λ_U is the fixed point of the channel $E : \mathbb{C}^D \longrightarrow \mathbb{C}^D$ given by $E(M) = \mathrm{tr}_B(\mathcal{E}(M))$. This description of the state makes us wonder whether it is possible to give a concentration result for the fixed point of a channel E or, alternatively, if one can give a concentration result for the behavior of the second largest eigenvalue of a channel E where the dimension of the ancillary system B is fixed and the concentration result comes as a function of the dimension of the system A where the channel is acting (see [71] for a positive answer in a restrictive family of random channels). Both questions have interest on there own and depending on their answer could lead to a concentration of the entropy in the infinite spin chain.

Chapter VI

An entropic uncertainty inequality with application to quantum identification

In this chapter, we propose and prove a new general entropic uncertainty relation. Uncertainty relations are quantitative characterizations of the uncertainty principle of quantum mechanics, which expresses that for certain pairs of measurements, there exists no state for which the measurement outcome is determined for *both* measurements: at least one of the outcomes must be somewhat uncertain. *Entropic* uncertainty relations express this uncertainty in at least one of the measurement outcomes by means of an entropy measure, usually the Shannon entropy. Our new entropic uncertainty relation distinguishes itself from previously known uncertainty relations by the following collection of features:

1. It uses the *min-entropy* as entropy measure, rather than the Shannon entropy. Such an uncertainty relation is sometimes also called a *high-order* entropic uncertainty relation.[1] Since privacy amplification needs a lower bound on the min-entropy, high-order entropic uncertainty relations are useful tools in quantum cryptography.

2. It lower bounds the uncertainty in the measurement outcome for *all but one* measurement, chosen from an *arbitrary* (and arbitrarily large) family of possible measurements. This is clearly *stronger* than typical entropic uncertainty relations that lower bound the uncertainty on *average* (over the choice of the measurement).

3. The measurements can be chosen to be qubit-wise measurements, in the computational or Hadamard basis, and thus the uncertainty relation is applicable to practical protocols (which can be implemented using current technology).

To the best of our knowledge, no previous entropic uncertainty relation satisfies (1) and (2) simultaneously, let alone in combination with (3). Indeed, as pointed out in a recent overview article by Wehner and Winter [180], little is known about entropic uncertainty relations for more than two measurement outcomes, and even less when additionally considering min-entropy.

[1] This is because the min-entropy coincides with the Rényi entropy H_α of high(est) order $\alpha = \infty$. In comparison, the Shannon entropy coincides with the Rényi entropy of (relatively) low order $\alpha = 1$.

To explain our new uncertainty relation, we find it helpful to first discuss a simpler variant, which does not satisfy (1), and which follows trivially from known results. Fix an arbitrary family $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of bases for a given quantum system (i.e., Hilbert space). The *maximum overlap* of such a family is defined as

$$c := \max\{|\langle\phi|\psi\rangle| : |\phi\rangle \in \mathcal{B}_j, |\psi\rangle \in \mathcal{B}_k, 1 \leq j < k \leq m\},$$

and let $d := -\log(c^2)$. Let ρ be an arbitrary quantum state of that system, and let X denote the measurement outcome when ρ is measured in one of the bases. We model the choice of the basis by a random variable J, so that $H(X|J=j)$ denotes the Shannon entropy of the measurement outcome when ρ is measured in basis $\mathcal{B}_j$. It follows immediately from Maassen and Uffink's uncertainty relation [109] that

$$H(X|J=j) + H(X|J=k) \geq -\log(c^2) = d \quad \forall j \neq k.$$

As a direct consequence, there exists a choice j' for the measurement so that $H(X|J=j) \geq \frac{d}{2}$ for all $j \in \{1, \ldots, m\}$ with $j \neq j'$. In other words, for any state ρ there exists j' so that unless the choice for the measurement coincides with j', which happens with probability at most $\max_j P_J(j)$, there is at least $d/2$ bits of entropy in the outcome X.

Our new high-order entropic uncertainty relation shows that this very statement essentially still holds when we replace Shannon by min-entropy, except that j' becomes randomized: for any ρ, there exists a *random variable* J', independent of J, such that[2]

$$H_{\min}(X|J=j, J'=j') \gtrsim \frac{d}{2} \quad \forall\, j \neq j' \in \{1, \ldots, m\}$$

no matter what the distribution of J is. Thus, unless the measurement J coincides with J', there is roughly $d/2$ bits of min-entropy in the outcome X. Furthermore, since J' is *independent* of J, the probability that J coincides with J' is at most $\max_j P_J(j)$, as is the case for a fixed J'.

Note that we have no control over (the distribution of) J'. We can merely guarantee that it exists and is independent of J. It may be insightful to interpret J' as a *virtual guess* for J, guessed by the party that prepares ρ, and whose goal is to have little uncertainty in the measurement outcome X. The reader may think of the following specific way of preparing ρ: sample j' according to some arbitrary distribution J', and then prepare the state as the, say, first basis vector of $\mathcal{B}_{j'}$. If the resulting mixture ρ is then measured in some basis $\mathcal{B}_j$, sampled according to an arbitrary (independent) distribution J, then unless $j = j'$ (i.e., our guess for j was correct), there is obviously lower bounded uncertainty in the measurement outcome X (assuming a non-trivial maximum overlap). Our uncertainty relation can be understood as saying that for *any* state ρ, no matter how it is prepared, there exists such a (virtual) guess J', which exhibits this very behavior: if it differs from

[2]The rigorous version of the approximate inequality $\gtrsim$ is stated in Theorem VI.2.4.

the actual choice for the measurement then there is lower bounded uncertainty in the measurement outcome X. As an immediate consequence, we can for instance say that X has min-entropy at least $d/2$, except with a probability that is given by the probability of guessing J, e.g., except with probability $1/m$ if the measurement is chosen uniformly at random from the family. This is clearly the best we can hope for.

We stress that because the min-entropy is more conservative than the Shannon entropy, our high-order entropic uncertainty relation does not follow from its simpler Shannon-entropy version. Neither can it be deduced in an analogous way; the main reason being that for fixed pairs $j \neq k$, there is no strong lower bound on $H_{\min}(X|J=j)+H_{\min}(X|J=k)$, in contrast to the case of Shannon entropy. More precisely and more generally, the *average* uncertainty $\frac{1}{|J|}\sum_j H_{\min}(X|J=j)$ does not allow a lower bound higher than $\log|J|$. To see this, consider the following example for $|J| = 2$ (the example can easily be extended to arbitrary $|J|$). Suppose that ρ is the uniform mixture of two pure states, one giving no uncertainty when measured in basis j, and the other giving no uncertainty when measured in basis k. Then, $\frac{1}{2}H_{\min}(X|J=j) + \frac{1}{2}H_{\min}(X|J=k) = 1$. Because of a similar reason, we cannot hope to get a good bound for all but a *fixed* choice of j'; the probabilistic nature of J' is necessary (in general). Hence, compared to bounding the average uncertainty, the all-but-one form of our uncertainty relation not only makes our uncertainty relation stronger in that uncertainty for all-but-one implies uncertainty on average (yet not vice versa), but it also allows for *more* uncertainty.

By using asymptotically good error-correcting codes, one can construct families of bases that have a large value of d, and thus for which our uncertainty relation guarantees a large amount of min-entropy (we discuss this in more detail in Section VI.2.1). These families consist of qubit-wise measurements in the computational or the Hadamard basis, hence these measurements can be performed with current technology.

The proof of our new uncertainty relation comprises a rather involved probability reasoning to prove the existence of the random variable J' and builds on earlier work presented in [153].

As an application of our entropic uncertainty relation, we propose a new *quantum identification protocol*. Informally, the goal of (password-based) identification is to prove knowledge of a possibly low-entropy password w, without giving away any information on w (beyond what is unavoidable). In [35], Damgård *et al.* showed the existence of such an identification protocol in the *bounded-quantum-storage model* (BQSM). This means that the proposed protocol involves the communication of qubits, and security is proven against any dishonest participant that can store only a limited number of these qubits (whereas legitimate participants need no quantum storage at all to honestly execute the protocol).

Our uncertainty relation gives us the right tool to prove security of the new quantum identification protocol in the BQSM. The distinguishing feature of our new protocol is that it also offers some security in case the assumption underlying the BQSM fails to

hold. Indeed, we additionally prove security of our new protocol against a dishonest server that has unbounded quantum-storage capabilities and can reliably store all the qubits communicated during an execution of the protocol, but is restricted to non-adaptive single-qubit operations and measurements.[3] This is in sharp contrast to protocol QID by Damgård *et al.*, which completely breaks down against a dishonest server that can store all the communicated qubits in a quantum memory and postpone the measurements until the user announces the correct measurement bases. On the downside, our protocol only offers security in case of a perfectly single-qubit (e.g. single-photon) source, because multi-qubit emissions reveal information about w. Hence, given the state of single-qubit-source technology, our protocol is currently mainly of theoretical interest.

The security of our protocol in this *single-qubit-operations model* (SQOM) relies on a certain minimum-distance property of random binary matrices and makes use of Diaconis and Shahshahani's XOR inequality (Theorem VI.1.1, see also [39]).

Relations to prior work. The study of *entropic* uncertainty relations, whose origin dates back to 1957 with the work of Hirschman [80], has received a lot of attention over the last decade due to their various applications in quantum information theory. We refer the reader to [180] for a recent overview on entropic uncertainty relations. Most of the known entropic uncertainty relations are of the form

$$\frac{1}{|J|}\sum_j H_\alpha(X|J=j) \geq h\,,$$

where H_α is the Rényi entropy. I.e., most uncertainty relations only give a lower bound on the entropy of the measurement outcome X *on average* over the (random) choice of the measurement. As argued in Section VI, the bound h on the *min*-entropy can be at most $\log|J|$, no matter the range of X. Furthermore, an uncertainty relation of this form only guarantees that there is uncertainty in X for *some* measurement(s), but does not specify precisely for how many, and certainly it does not guarantee uncertainty for *all but one* measurements. The same holds for the high-order entropic uncertainty relation from [33], which considers an exponential number of measurement settings and guarantees that except with negligible probability over the (random) choice of the measurement, there is lower-bounded min-entropy in the outcome. On the other hand, the high-order entropic uncertainty relation from [34] only considers *two* measurement settings and guarantees lower-bounded min-entropy with probability (close to) $\frac{1}{2}$.

The uncertainty relation we know of that comes closest to ours is Lemma 2.13 in [47]. Using our notation, it shows that X is ϵ-close to having roughly $d/2$ bits of min-entropy (i.e., the same bound we get), but only for all but an ϵ-fraction of all the m possible choices for the measurement j, where ϵ is about $\sqrt{2/m}$.

[3] It is known that *some* restriction is necessary (see [35]).

With respect to our application, backing up the security of the identification protocol by Damgård *et al.* [35] against an adversary that can overcome the quantum-memory bound assumed by the BQSM was also the goal of [32]. However, the solution proposed there relies on an unproven computational-hardness assumption, and as such, strictly speaking, can be broken by an adversary in the SQOM, i.e., by storing qubits and measuring them later qubit-wise and performing (possibly infeasible) classical computations. On the other hand, by *assuming* a lower bound on the hardness of the underlying computational problem against quantum machines, the security of the protocol in [32] holds against an adversary with much more quantum computing power than our protocol in the SQOM, which restricts the adversary to single-qubit operations.

VI.1 Preliminaries

Sets as well as families are written using a calligraphic font, e.g. $\mathcal{A}, \mathcal{X}$, and we write $|\mathcal{A}|$ etc. for the cardinality. We use $[n]$ as a shorthand for $\{1, \ldots, n\}$.

For an n-bit vector vector $v = (v_1, \ldots, v_n)$ in $\{0,1\}^n$, we write $|v|$ for its Hamming weight, and, for any subset $\mathcal{I} \subseteq [n]$, we write $v_{\mathcal{I}}$ for the restricted vector $(v_i)_{i \in \mathcal{I}} \in \{0,1\}^{|\mathcal{I}|}$. For two vectors $v, w \in \{0,1\}^n$, the *Schur product* is defined as the element-wise product $v \odot w := (v_1 w_1, v_2 w_2, \ldots, v_n w_n) \in \{0,1\}^n$, and the *inner product* between v and w is given by $v \cdot w := v_1 w_1 \oplus \cdots \oplus v_n w_n \in \{0,1\}$, where the addition is modulo 2. We write $\mathrm{span}(F)$ for the *row span* of a matrix F; the set of vectors obtained by making all possible linear combinations (modulo 2) of the rows of F, i.e. the set $\{sF : \forall s \in \{0,1\}^\ell\}$, where s should be interpreted as a row vector and sF denotes a vector-matrix product.

VI.1.1 Probability Theory and Hybrid Systems

We recall that a finite probability space is a non-empty finite set Ω together with a function $\Pr : \Omega \to \mathbb{R}$ such that $\Pr(\omega) \geq 0 \quad \forall \omega \in \Omega$ and $\sum_{\omega \in \Omega} \Pr(\omega) = 1$. An *event* is a subset of Ω. A *random variable* is a function $X : \Omega \to \mathcal{X}$ from a finite probability space $(\Omega, \Pr)$ to a finite set $\mathcal{X}$. We denote random variables as capital letters, for example X, Y, Z. The *distribution* of X, which we denote as P_X, is given by $P_X(x) = \Pr[X = x] = \Pr[\{\omega \in \Omega : X(\omega) = x\}]$. The joint distribution of two (or more) random variables X and Y is denoted by P_{XY}, i.e., $P_{XY}(x, y) = \Pr[X = x \wedge Y = y]$. Specifically, we write $U_{\mathcal{X}}$ for the uniform probability distribution over $\mathcal{X}$. Usually, we leave the probability space $(\Omega, \Pr)$ implicit, and understand random variables to be defined by their joint distribution, or by some "experiment" that uniquely determines their joint distribution.

Random variables X and Y are *independent* if $P_{XY} = P_X P_Y$ (which should be understood as $P_{XY}(x, y) = P_X(x) P_Y(y) \; \forall x \in \mathcal{X}, y \in \mathcal{Y}$). The random variables X, Y and Z form a (first-order) Markov chain, denoted by $X \leftrightarrow Y \leftrightarrow Z$, if $P_{XZ|Y} = P_{X|Y} P_{Z|Y}$. The

statistical distance (also knows as variational distance) between distributions P_X and P_Y is written as $\mathrm{SD}(P_X, P_Y) := \frac{1}{2}\|P_X - P_Y\|_1$.

The *bias* of a binary random variable X is defined as $\mathrm{bias}(X) := \big|P_X(0) - P_X(1)\big|$. This also naturally defines the bias of X conditioned on an event $\mathcal{E}$ as $\mathrm{bias}(X|\mathcal{E}) := \big|P_{X|\mathcal{E}}(0) - P_{X|\mathcal{E}}(1)\big|$. The bias thus ranges between 0 and 1 and can be understood as a degree of predictability of a bit: if the bias is small then the bit is close to random, and if the bias is large (i.e. approaches 1) then the bit has essentially no uncertainty. For a sum of two independent binary random variables X_1 and X_2, the bias of the sum is the product of the individual biases, i.e. $\mathrm{bias}(X_1 \oplus X_2) = \mathrm{bias}(X_1)\mathrm{bias}(X_2)$.

Theorem VI.1.1 (Diaconis and Shahshahani's Information-Theoretic XOR Lemma)**.** *Let X be a random variable over $\mathcal{X} := \{0,1\}^n$ with distribution P_X. Then, the following holds,*

$$\mathrm{SD}(P_X, U_{\mathcal{X}}) \leq \frac{1}{2}\Big[\sum_{f\in\{0,1\}^n\setminus\{0^n\}} \mathrm{bias}(f\cdot X)^2\Big]^{\frac{1}{2}}.$$

The original version of Theorem VI.1.1 appeared in [39], where it is expressed in the language of representation theory. The version above is due to [120].

Theorem VI.1.2 (Hoeffding's Inequality)**.** *Let $X_1, X_2, \ldots, X_n$ be independent binary random variables, each distributed according to the Bernoulli distribution with parameter μ, and let $\bar{X} := n^{-1}\sum_{i\in[n]} X_i$. Then for $0 < t < 1-\mu$*

$$\Pr[\bar{X} - \mu \geq t] \leq \exp(-2nt^2).$$

For a proof, the reader is referred to [81].

Subsystem X of a bipartite quantum system XE is called *classical*, if the state of XE is given by a density matrix of the form

$$\rho_{XE} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_E^x\,,$$

where $\mathcal{X}$ is a finite set of cardinality $|\mathcal{X}| = \dim(\mathcal{H}_X)$, $P_X : \mathcal{X} \to [0,1]$ is a probability distribution, $\{|x\rangle\}_{x\in\mathcal{X}}$ is some fixed orthonormal basis of $\mathcal{H}_X$, and ρ_E^x is a density matrix on $\mathcal{H}_E$ for every $x \in \mathcal{X}$. Such a state, called *hybrid* or *cq-* (for *c*lassical-*q*uantum) state, can equivalently be understood as consisting of a *random variable* X with distribution P_X, taking on values in $\mathcal{X}$, and a system E that is in state ρ_E^x exactly when X takes on the value x. This formalism naturally extends to two (or more) classical systems X, Y etc. For any event $\mathcal{E}$ (defined by $P_{\mathcal{E}|X}(x) = \Pr[\mathcal{E}|X = x]$ for all x), we may write

$$\rho_{XE|\mathcal{E}} := \sum_x P_{X|\mathcal{E}}|x\rangle\langle x| \otimes \rho_E^x.$$

If the state of XE satisfies $\rho_{XE} = \rho_X \otimes \rho_E$, where $\rho_X = \mathrm{tr}_E(\rho_{XE})$ and $\rho_E = \mathrm{tr}_X(\rho_{XE})$, then X is *independent* of E, and thus no information on X can be obtained from system E. Moreover, if $\rho_{XE} = \frac{1}{|\mathcal{X}|}\mathbb{I}_X \otimes \rho_E$, where $\mathbb{I}_X$ denotes the identity on $\mathcal{H}_X$, then X is *random-and-independent* of E. We also want to be able to express that a random variable X is (close) to being independent of a quantum system E *when given a random variable* Y. Formally, this is expressed by saying that ρ_{XYE} equals $\rho_{X\leftrightarrow Y\leftrightarrow E}$, where

$$\rho_{X\leftrightarrow Y\leftrightarrow E} := \sum_{x,y} P_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^y.$$

This notion, called *conditional independence*, for the quantum setting was introduced in [35].

If two states ρ and σ are ε-close in trace distance, i.e. $\frac{1}{2}\|\rho - \sigma\|_1 \leq \varepsilon$, we use $\rho \approx_\varepsilon \sigma$ as shorthand. In case of classical states, the trace distance coincides with the statistical distance. Moreover, the trace distance between two states cannot increase when applying the same quantum operation (i.e., CPTP map) to both states. As a consequence, if $\rho \approx_\varepsilon \sigma$ then the states cannot be distinguished with statistical advantage better than ε.

Definition VI.1.3. *For a density matrix $\rho_{XE} \in S(\mathcal{H}_X \otimes \mathcal{H}_E)$ with classical X, the* distance to uniform *of X given E is defined as*

$$d_{\mathrm{unif}}(X|E) := \tfrac{1}{2}\|\rho_{XE} - \rho_U \otimes \rho_E\|_1,$$

where $\rho_U := \frac{1}{\dim(\mathcal{H}_X)}\mathbb{I}_X$.

VI.1.2 Min-Entropy and Privacy Amplification

We make use of Renner's notion of the *conditional min-entropy* $H_{\min}(\rho_{AB}|B)$ of a system A conditioned on another system B [145]. If the state ρ_{AB} is clear from the context, we may write $H_{\min}(A|B)$ instead of $H_{\min}(\rho_{AB}|B)$. The formal definition is given by $H_{\min}(\rho_{AB}|B) := \sup_{\sigma_B} \max\{h \in \mathbb{R} : 2^{-h} \cdot \mathbb{I}_A \otimes \sigma_B - \rho_{AB} \geq 0\}$ where the supremum is over all density matrices σ_B on $\mathcal{H}_B$. If $\mathcal{H}_B$ is the trivial space $\mathbb{C}$, we obtain the min-entropy of ρ_A. Recall that $H_{\min}(\rho_A) = -\log \lambda_{\max}(\rho_A)$, where $\lambda_{\max}(\rho_A)$ is the largest eigenvalue of ρ_A.

We will need the following chain rule.

Lemma VI.1.4. *For any density matrix ρ on $\mathcal{H}_{XYE}$ with classical X and Y it holds that*

$$H_{\min}(X|YE) \geq H_{\min}(X|Y) - H_{\max}(E).$$

For the special case of a hybrid state $\rho_{XE} \in S(\mathcal{H}_X \otimes \mathcal{H}_E)$ with classical X, it is shown in [98] that the conditional min-entropy of a quantum state coincides with the negative

logarithm of the *guessing probability conditional on quantum side information*

$$\mathrm{Guess}(X|E) := \max_{\{M_x\}} \sum_x P_X(x)\ \mathrm{tr}(M_x \rho_E^x),$$

where the latter is the probability that the party holding $\mathcal{H}_E$ guesses X correctly using the POVM $\{M_x\}_x$ on $\mathcal{H}_E$ that maximizes Guess. Thus,

$$H_{\min}(X|E) = -\log \mathrm{Guess}(X|E). \tag{VI.1}$$

For random variables X and Y, we have that $\mathrm{Guess}(X|Y)$ simplifies to

$$\mathrm{Guess}(X|Y) = \sum_y P_Y(y)\mathrm{Guess}(X|Y=y) = \sum_y P_Y(y) \max_x P_{X|Y}(x|y).$$

To prove Lemma VI.1.4, we need to introduce some more tools.

The following proposition guarantees that the "averaging property" of the guessing probability (which holds by definition in the classical case) still holds when additionally conditioning on a quantum system.

Proposition VI.1.5. *For any state $\rho_{XYE} \in S(\mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_E)$ that is classical on X and Y it holds that*

$$\mathrm{Guess}(X|YE) = \sum_y P_Y(y)\, \mathrm{Guess}(X|E, Y=y).$$

Proof. First, note that for any matrix M_x acting on $\mathcal{H}_Y \otimes \mathcal{H}_E$, we can always write $M_x = \sum_{y,y'} |y\rangle\langle y'| \otimes M_x^{y,y'}$, where $M_x^{y,y'}$ acts on $\mathcal{H}_E$ for every x, y, y'. Now, we write

$$\begin{aligned}
\mathrm{Guess}(X|YE) &= \max_{\{M_x\}} \sum_x P_X(x)\, \mathrm{tr}(M_x \rho_{YE}^x) \\
&= \max_{\{M_x\}} \sum_x P_X(x)\, \mathrm{tr}(M_x \sum_y P_{Y|X}(y|x)\, |y\rangle\langle y| \otimes \rho_E^{x,y}) \\
&= \max_{\{M_x\}} \sum_{x,y} P_{XY}(x,y)\, \mathrm{tr}((\sum_{v,w} |v\rangle\langle w| \otimes M_x^{v,w})(|y\rangle\langle y| \otimes \rho_E^{x,y})) \\
&= \max_{\{M_x\}} \sum_{x,y} P_{XY}(x,y) \sum_v \langle v|y\rangle\, \mathrm{tr}(M_x^{v,y} \rho_E^{x,y}) \\
&= \max_{\{M_x\}} \sum_{x,y} P_{XY}(x,y)\, \mathrm{tr}(M_x^{y,y} \rho_E^{x,y}) \\
&= \sum_y P_Y(y) \max_{\{M_x^{y,y}\}} \sum_x P_{X|Y}(x|y)\, \mathrm{tr}(M_x^{y,y} \rho_E^{x,y}) \\
&= \sum_y P_Y(y)\, \mathrm{Guess}(X|E, Y=y).
\end{aligned}$$

□

The following proposition is known as the chain rule for min-entropy.

Proposition VI.1.6 ([145]). *The following holds for all $\rho_{ABC} \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$,*

$$H_{\min}(A|BC) \geq H_{\min}(AB|C) - H_{\max}(B).$$

Finally, we need the following lemma.

Lemma VI.1.7. *For any state $\rho_{XYE} \in S(\mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_E)$ that is classical on X and Y it holds that*

$$H_{\min}(XE|Y=y) \geq H_{\min}(X|Y=y) \tag{VI.2}$$

for every $y \in \mathcal{Y}$.

Proof. Note that it suffices to show that $\lambda_{\max}(\rho^y_{XE}) \leq \lambda_{\max}(\rho^y_X)$ holds for every $y \in \mathcal{Y}$. Because ρ^y_{XE} is classical on X, there exists a unitary U acting on $\mathcal{H}_X$ such that $\tilde{\rho}^y_{XE} := (U \otimes \mathbb{I}_E)\rho^y_{XE}(U^\dagger \otimes \mathbb{I}_E)$ is classical with respect to the computational basis $\{|x\rangle\}_{x\in\mathcal{X}}$ on $\mathcal{H}_X$ with $\mathcal{X} := [d]$. In particular, this means that $\tilde{\rho}^y_{XE}$ has block-diagonal structure:

$$\tilde{\rho}^y_{XE} = \sum_{x\in[d]} P_{X|Y}(x|y)|x\rangle\langle x| \otimes \rho^{x,y}_E = \begin{bmatrix} P_{X|Y}(1|y)\,\rho^{1,y}_E & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & P_{X|Y}(d|y)\,\rho^{d,y}_E \end{bmatrix}.$$

Note that because U is unitary, $\tilde{\rho}^y_{XE}$ has the same eigenvalues as ρ^y_{XE}, where these eigenvalues are given by the union of the eigenvalues of the blocks on the diagonal of $\tilde{\rho}^y_{XE}$. From this we see that the largest eigenvalue of $\tilde{\rho}^y_{XE}$ (and thus of ρ^y_{XE}) cannot be larger than the largest eigenvalue of $\tilde{\rho}^y_X := \mathrm{tr}_E(\tilde{\rho}^y_{XE})$ (and thus of ρ^y_X). □

Proof of Lemma VI.1.4 . By (VI.1) it is equivalent to show that

$$\mathrm{Guess}(X|YE) \leq \mathrm{Guess}(X|Y)\, 2^{H_{\max}(E)}.$$

Using Proposition VI.1.5, we write

$$\begin{aligned}
\mathrm{Guess}(X|EY) &= \sum_y P_Y(y)\,\mathrm{Guess}(X|E, Y=y) = \sum_y P_Y(y)\, 2^{-H_{\min}(X|E,Y=y)} \\
&\leq \sum_y P_Y(y)\, 2^{-(H_{\min}(XE|Y=y) - H_{\max}(E))} \\
&\leq 2^{H_{\max}(E)} \sum_y P_Y(y) 2^{-H_{\min}(X|Y=y)} = 2^{H_{\max}(E)}\,\mathrm{Guess}(X|Y),
\end{aligned}$$

where the first inequality is Proposition VI.1.6, and the second inequality follows by Lemma VI.1.7. Hence, the claim follows. □

Finally, we make use of Renner's privacy amplification theorem [145, 146], as given below. Recall that a function $g : \mathcal{R} \times \mathcal{X} \to \{0,1\}^\ell$ is called a *universal* (hash) function, if for the random variable R, uniformly distributed over $\mathcal{R}$, and for any distinct $x, y \in \mathcal{X}$: $\Pr[g(R,x) = g(R,y)] \leq 2^{-\ell}$.

Theorem VI.1.8 (Privacy amplification)**.** *Let ρ_{XE} be a hybrid state with classical X. Let $g : \mathcal{R} \times \mathcal{X} \to \{0,1\}^\ell$ be a universal hash function, and let R be uniformly distributed over $\mathcal{R}$, independent of X and E. Then $K = g(R,X)$ satisfies*

$$d_{\text{unif}}(K|RE) \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(H_{\min}(X|E)-\ell)} .$$

Informally, Theorem VI.1.8 states that if X contains sufficiently more than ℓ bits of entropy when given E, then ℓ nearly random-and-independent bits can be extracted from X.

VI.2 The All-But-One Entropic Uncertainty Relation

Throughout this section, $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ is an arbitrary but fixed family of bases for the state space $\mathcal{H}$ of a quantum system. For simplicity, we restrict our attention to an n-qubit system such that $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ for $n \in \mathbb{N}$, but our results immediately generalize to arbitrary quantum systems. We write the 2^n basis vectors of the j-th basis $\mathcal{B}_j$ as $\mathcal{B}_j = \{|x\rangle_j : x \in \{0,1\}^n\}$. Let c be the maximum overlap of $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$, i.e.,

$$c := \max\{|\langle x|_j |y\rangle_k| : x, y \in \{0,1\}^n, 1 \leq j < k \leq m\}.$$

In order to obtain our entropic uncertainty relation that lower bounds the min-entropy of the measurement outcome for all but one measurement, we first show an uncertainty relation that expresses uncertainty by means of the probability measure of given sets.

Theorem VI.2.1 (Theorem 4.18 in [153])**.** *Let ρ be an arbitrary state of n qubits. For $j \in [m]$, let $Q^j(\cdot)$ be the distribution of the outcome when ρ is measured in the $\mathcal{B}_j$-basis, i.e., $Q^j(x) = \langle x|_j \, \rho \, |x\rangle_j$ for any $x \in \{0,1\}^n$. Then, for any family $\{\mathcal{L}^j\}_{j\in[m]}$ of subsets $\mathcal{L}^j \subset \{0,1\}^n$, it holds that*

$$\sum_{j\in[m]} Q^j(\mathcal{L}^j) \leq 1 + c\,(m-1) \cdot \max_{j\neq k\in[m]} \sqrt{|\mathcal{L}^j||\mathcal{L}^k|}.$$

A special case of Theorem VI.2.1, obtained by restricting the family of bases to the specific choice $\{\mathcal{B}_+, \mathcal{B}_\times\}$ with $\mathcal{B}_+ = \{|x\rangle : x \in \{0,1\}^n\}$ and $\mathcal{B}_\times = \{H^{\otimes n}|x\rangle : x \in \{0,1\}^n\}$ (i.e. either the computational or Hadamard basis for all qubits), is an uncertainty relation that was proven and used in the original paper about the BQSM [34]. The proof of Theorem VI.2.1 goes along similar lines as the proof in the journal version of [34] for the special case outlined above. It is based on the following norm inequality.

Proposition VI.2.2. *For orthogonal (or self-adjoint) projectors $A_1, A_2, \ldots, A_m$, it holds that*

$$\left\|A_1 + \ldots + A_m\right\| \leq 1 + (m-1) \cdot \max_{1 \leq j < k \leq m} \left\|A_j A_k\right\|,$$

where the norm is the operator norm

The case $m = 2$ was proven in [34], adapting a technique by Kittaneh [95]. We extend the proof to an arbitrary m.

Proof. Defining

$$X := \begin{pmatrix} A_1 & A_2 & \cdots & A_m \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad Y := \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ A_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ A_m & 0 & \cdots & 0 \end{pmatrix}$$

yields

$$XY = \begin{pmatrix} A_1 + A_2 + \ldots + A_m & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad YX = \begin{pmatrix} A_1 & A_1 A_2 & \cdots & A_1 A_m \\ A_2 A_1 & A_2 & \cdots & A_2 A_m \\ \vdots & \vdots & \ddots & \vdots \\ A_m A_1 & A_m A_2 & \cdots & A_m \end{pmatrix}$$

The matrix YX can be additively decomposed into m matrices according to the following pattern

$$YX = \begin{pmatrix} * & & & & \\ & * & & & \\ & & \ddots & & \\ & & & * & \\ & & & & * \end{pmatrix} + \begin{pmatrix} 0 & * & & & \\ & 0 & & & \\ & & \ddots & \ddots & \\ & & & 0 & * \\ * & & & & 0 \end{pmatrix} + \ldots + \begin{pmatrix} 0 & & & & * \\ * & 0 & & & \\ & \ddots & \ddots & & \\ & & & 0 & \\ & & & * & 0 \end{pmatrix}$$

where the $*$ stand for entries of YX and for $i = 1, \ldots, m$ the ith star-pattern after the diagonal pattern is obtained by i cyclic shifts of the columns of the diagonal pattern.

XY and YX are Hermitian and thus have the same eigenvalues and $\|XY\| = \|YX\|$. Then, by applying the triangle inequality, the unitary invariance of the operator norm and the facts that for all $j \neq k : \|A_j\| = 1$, $\|A_j A_k\| = \|A_k A_j\|$, we obtain the desired statement. □

Proof of Theorem VI.2.1. For $j \in [m]$, we define the orthogonal projectors $A^j := \sum_{x \in \mathcal{L}^j} |x\rangle_j \langle x|_j$. Using the spectral decomposition of $\rho = \sum_w \lambda_w |\varphi_w\rangle\langle\varphi_w|$ and the linearity of the trace, we

have

$$\sum_{j\in[m]} Q^j(\mathcal{L}^j) = \sum_{j\in[m]} \operatorname{tr}(A^j\rho) = \sum_{j\in[m]}\sum_w \lambda_w \operatorname{tr}(A^j|\varphi_w\rangle\langle\varphi_w|) = \sum_w \lambda_w \Big(\sum_{j\in[m]} \langle\varphi_w|A^j|\varphi_w\rangle\Big)$$
$$= \sum_w \lambda_w \langle\varphi_w|\Big(\sum_{j\in[m]} A^j\Big)|\varphi_w\rangle \leq \Big\|\sum_{j\in[m]} A^j\Big\| \leq 1 + (m-1)\cdot \max_{j\neq k\in[m]} \big\|A^jA^k\big\|,$$

where the last inequality is Proposition VI.2.2. To conclude, we show that $\|A^jA^k\| \leq c\sqrt{|\mathcal{L}^j||\mathcal{L}^k|}$. Let us fix $j \neq k \in [m]$. Note that by the restriction on the overlap of the family of bases $\{\mathcal{B}_j\}_{j\in[m]}$, we have that $|\langle x|_j|y\rangle_k| \leq c$ holds for all $x, y \in \{0,1\}^n$. Then, with the sums over x and y understood as over $x \in \mathcal{L}^j$ and $y \in \mathcal{L}^k$, respectively,

$$\Big\|A^jA^k|\psi\rangle\Big\|^2 = \Big\|\sum_x |x\rangle_j\langle x|_j \sum_y |y\rangle_k\langle y|_k|\psi\rangle\Big\|^2 = \Big\|\sum_x |x\rangle_j \sum_y \langle x|_j|y\rangle_k \langle y|_k|\psi\rangle\Big\|^2$$
$$= \sum_x \Big|\sum_y \langle x|_j|y\rangle_k \langle y|_k|\psi\rangle\Big|^2 \leq \sum_x \Big(\sum_y \big|\langle x|_j|y\rangle_k \langle y|_k|\psi\rangle\big|\Big)^2$$
$$\leq c^2 \sum_x \Big(\sum_y \big|\langle y|_k|\psi\rangle\big|\Big)^2 \leq c^2\big|\mathcal{L}^j\big|\big|\mathcal{L}^k\big|.$$

The third equality follows from Pythagoras, the first inequality holds by triangle inequality, the second inequality by the bound on $|\langle x|_j|y\rangle_k|$, and the last follows from Cauchy-Schwarz. This implies $\|A^jA^k\| \leq c\sqrt{|\mathcal{L}^j||\mathcal{L}^k|}$ and finishes the proof. □

In the same spirit as in (the journal version of) [34], we reformulate the uncertainty relation of Theorem VI.2.1 in terms of a "good event" $\mathcal{E}$, which occurs with reasonable probability, and if it occurs, the measurement outcomes have high min-entropy. The statement is obtained by choosing the sets $\mathcal{L}^j$ in Theorem VI.2.1 appropriately.

Because we now switch to entropy notation, it will be convenient to work with a measure of overlap between bases that is logarithmic in nature and *relative* to the number n of qubits. Hence, we define

$$\delta := -\frac{1}{n}\log c^2\,.$$

We will later see that for "good" choices of bases, δ stays constant for growing n.

Corollary VI.2.3. *Let ρ be an arbitrary n-qubit state, let J be a random variable over $[m]$ (with arbitrary distribution P_J), and let X be the outcome when measuring ρ in basis $\mathcal{B}_J$.*[4] *Then, for any $0 < \epsilon < \delta/4$, there exists an event $\mathcal{E}$ such that*

$$\sum_{j\in[m]} \Pr[\mathcal{E}|J{=}j] \geq (m-1) - (2m-1)\cdot 2^{-\epsilon n}$$

[4] I.e., $P_{X|J}(x|j) = Q^j(x)$, using the notation from Theorem VI.2.1.

and

$$H_{\min}(X|J=j,\mathcal{E}) \geq \left(\frac{\delta}{2} - 2\epsilon\right)n$$

for $j \in [m]$ *with* $P_{J|\mathcal{E}}(j) > 0$.

Proof. For $j \in [m]$ define

$$\mathcal{S}^j := \left\{x \in \{0,1\}^n : Q^j(x) \leq 2^{-(\delta/2-\epsilon)n}\right\}$$

to be the sets of strings with small probabilities and denote by $\mathcal{L}^j := \overline{\mathcal{S}}^j$ their complements[5]. Note that for all $x \in \mathcal{L}^j$, we have that $Q^j(x) > 2^{-(\delta/2-\epsilon)n}$ and therefore $|\mathcal{L}^j| < 2^{(\delta/2-\epsilon)n}$. It follows from Theorem VI.2.1 that

$$\sum_{j\in[m]} Q^j(\mathcal{S}^j) = \sum_{j\in[m]} (1 - Q^j(\mathcal{L}^j)) \geq m - (1 + (m-1)\cdot 2^{-\epsilon n}) = (m-1) - (m-1)2^{-\epsilon n}.$$

We define $\mathcal{E} := \{X \in \mathcal{S}^J \wedge Q^J(\mathcal{S}^J) \geq 2^{-\epsilon n}\}$ to be the event that $X \in \mathcal{S}^J$ and at the same time the probability that this happens is not too small. Then $\Pr[\mathcal{E}|J=j] = \Pr[X \in \mathcal{S}^j \wedge Q^j(\mathcal{S}^j) \geq 2^{-\epsilon n}|J=j]$ either vanishes (if $Q^j(\mathcal{S}^j) < 2^{-\epsilon n}$) or else equals $Q^j(\mathcal{S}^j)$. In either case, $\Pr[\mathcal{E}|J=j] \geq Q^j(\mathcal{S}^j) - 2^{-\epsilon n}$ holds and thus the first claim follows by summing over $j \in [m]$ and using the derivation above. Furthermore, let $p = \max_j P_J(j)$, then $\Pr[\bar{\mathcal{E}}] = \sum_{j\in[m]} P_J(j)\Pr[\bar{\mathcal{E}}|J=j] \leq p\sum_{j\in[m]} \Pr[\bar{\mathcal{E}}|J=j] \leq p(m-(\sum_{j\in[m]} Q^j(\mathcal{S}^j)-2^{-\epsilon n})) \leq p(1+(2m-1)\cdot 2^{-\epsilon n})$, and $\Pr[\mathcal{E}] \geq (1-p) - p(2m-1)\cdot 2^{-\epsilon n}$

Regarding the second claim, in case $J = j$, we have

$$\begin{aligned} H_{\min}(X|J=j,\mathcal{E}) &= -\log\left(\max_{x\in\mathcal{S}^j} \frac{Q^j(x)}{Q^j(\mathcal{S}^j)}\right) \\ &\geq -\log\left(\frac{2^{-(\delta/2-\epsilon)n}}{Q^j(\mathcal{S}^j)}\right) = (\delta/2-\epsilon)n + \log(Q^j(\mathcal{S}^j)). \end{aligned}$$

As $Q^j(\mathcal{S}^j) \geq 2^{-\epsilon n}$ by definition of $\mathcal{E}$, we have $H_{\min}(X|J=j,\mathcal{E}) \geq (\delta/2 - 2\epsilon)n$. □

We are now ready to state and prove our new all-but-one entropic uncertainty relation.

Theorem VI.2.4. *Let* ρ *be an arbitrary* n*-qubit state, let* J *be a random variable over* $[m]$ *(with arbitrary distribution* P_J*), and let* X *be the outcome when measuring* ρ *in basis* $\mathcal{B}_J$*. Then, for any* $0 < \epsilon < \delta/4$*, there exists a random variable* J' *with joint distribution* $P_{JJ'X}$ *such that (1)* J *and* J' *are independent and (2) there exists an event* Ψ *with* $\Pr[\Psi] \geq 1 - 2\cdot 2^{-\epsilon n}$ *such that*[6]

$$H_{\min}(X|J=j, J'=j', \Psi) \geq \left(\frac{\delta}{2} - 2\epsilon\right)n - 1$$

[5] Here's the mnemonic: $\mathcal{S}$ for the strings with *S*mall probabilities, $\mathcal{L}$ for *L*arge.

[6] Instead of introducing such an event Ψ, we could also express the min-entropy bound by means of the *smooth* min-entropy of X given $J = j$ and $J' = j'$.

for all $j, j' \in [m]$ *with* $j \neq j'$ *and* $P_{JJ'|\Psi}(j, j') > 0$.

Note that, as phrased, Theorem VI.2.4 requires that J is fixed and known, and only then the existence of J' can be guaranteed. This is actually not necessary. By looking at the proof, we see that J' can be defined simultaneously in all m probability spaces $P_{X|J=j}$ with $j \in [m]$, without having assigned a probability distribution to J yet, so that the resulting random variable J' we obtain by assigning an *arbitrary* probability distribution P_J to J, satisfies the claimed properties. This in particular implies that the (marginal) distribution of J' is fully determined by ρ.

The idea of the proof of Theorem VI.2.4 is to (try to) define the random variable J' in such a way that the event $J \neq J'$ coincides with the "good event" $\mathcal{E}$ from Corollary VI.2.3. It then follows immediately from Corollary VI.2.3 that $H_{\min}(X|J = j, J' \neq J) \geq (\delta/2 - 2\epsilon)n$, which is already close to the actual min-entropy bound we need to prove. This approach dictates that if the event $\mathcal{E}$ does not occur, then J' needs to *coincide* with J. Vice versa, if $\mathcal{E}$ does occur, then J' needs to be *different* to J. However, it is a priori unclear *how* to choose J' different to J in case $\mathcal{E}$ occurs. There is only one way to set J' to be equal to J, but there are many ways to set J' to be different to J (unless $m = 2$). It needs to be done in such a way that without conditioning on $\mathcal{E}$ or its complement, J and J' are independent.

Somewhat surprisingly, it turns out that the following does the job. To simplify this informal discussion, we assume that the sum of the m probabilities $\Pr[\mathcal{E}|J=j]$ from Corollary VI.2.3 equals $m - 1$ exactly. It then follows that the corresponding complementary probabilities, $\Pr[\bar{\mathcal{E}}|J = j]$ for the m different choices of $j \in [m]$, add up to 1 and thus form a probability distribution. J' is now chosen, in the above spirit depending on the event $\mathcal{E}$, so that its marginal distribution $P_{J'}$ coincides with this probability distribution: $P_{J'}(j') = \Pr[\bar{\mathcal{E}}|J = j']$ for all $j' \in [m]$. Thus, in case the event $\mathcal{E}$ occurs, J' is chosen according to this distribution but conditioned on being different to the value j, taken on by J. The technical details, and how to massage the argument in case the sum of the $\Pr[\mathcal{E}|J=j]$'s is not exactly $m - 1$, are worked out in the proof below.

Proof of Theorem VI.2.4. From Corollary VI.2.3 we know that for any $0 < \epsilon < \delta/4$, there exists an event $\mathcal{E}$ such that $\sum_{j\in[m]} \Pr[\mathcal{E}|J = j] = m - 1 - \alpha$, and thus $\sum_{j\in[m]} \Pr[\bar{\mathcal{E}}|J = j] = 1 + \alpha$, for $-1 \leq \alpha \leq (2m - 1)2^{-\epsilon n}$. We make a case distinction between $\alpha = 0$, $\alpha > 0$ and $\alpha < 0$; we start with the case $\alpha = 0$, we subsequently prove the other two cases by reducing them to the case $\alpha = 0$ by "inflating" and "deflating" the event $\mathcal{E}$ appropriately. The approach for the case $\alpha = 0$ is to define J' in such way that $\mathcal{E} \iff J \neq J'$, i.e., the event $J \neq J'$ coincides with the event $\mathcal{E}$. The min-entropy bound from Corollary VI.2.3 then immediately translates to $H_{\min}(X|J = j, J' \neq J) \geq (\delta/2-2\epsilon)n$, and to $H_{\min}(X|J = j, J' = j') \geq (\delta/2 - 2\epsilon)n$ for $j' \neq j$ with $P_{JJ'}(j, j') > 0$, as we will show. What is not obvious about the approach is how to define J' when it is supposed

to be different from J, i.e., when the event $\mathcal{E}$ occurs, so that in the end J and J' are independent.

Formally, we define J' by means of the following conditional probability distributions:

$$P_{J'|JX\bar{\mathcal{E}}}(j'|j,x) := \begin{cases} 1 & \text{if } j = j' \\ 0 & \text{if } j \neq j' \end{cases} \quad \text{and} \quad P_{J'|JX\mathcal{E}}(j'|j,x) := \begin{cases} 0 & \text{if } j = j' \\ \dfrac{\Pr[\bar{\mathcal{E}}|J=j']}{\Pr[\mathcal{E}|J=j]} & \text{if } j \neq j' \end{cases}$$

We assume for the moment that the denominator in the latter expression does not vanish for any j; we take care of the case where it does later. Trivially, $P_{J'|JX\bar{\mathcal{E}}}$ is a proper distribution, with non-negative probabilities that add up to 1, and the same holds for $P_{J'|JX\mathcal{E}}$:

$$\sum_{j'\in[m]} P_{J'|JX\bar{\mathcal{E}}} = \sum_{j'\in[m]\setminus\{j\}} P_{J'|JX\bar{\mathcal{E}}} = \sum_{j'\in[m]\setminus\{j\}} \frac{\Pr[\bar{\mathcal{E}}|J=j']}{\Pr[\mathcal{E}|J=j]} = 1$$

where we used that $\sum_{j\in[m]} \Pr[\bar{\mathcal{E}}|J=j] = 1$ (because $\alpha = 0$) in the last equality. Furthermore, it follows immediately from the definition of J' that $\bar{\mathcal{E}} \implies J = J'$ and $\mathcal{E} \implies J \neq J'$. Hence, $\mathcal{E} \iff J \neq J'$, and thus the bound from Corollary VI.2.3 translates to $H_{\min}(X|J=j, J' \neq J) \geq (\delta/2 - 2\epsilon)n$. It remains to argue that J' is independent of J, and that the bound also holds for $H_{\min}(X|J=j, J'=j')$ whenever $j \neq j'$.

The latter follows immediately from the fact that conditioned on $J \neq J'$ (which is equivalent to $\mathcal{E}$), X, J and J' form a Markov chain $X \leftrightarrow J \leftrightarrow J'$, and thus, given $J = j$, additionally conditioning on $J' = j'$ does not change the distribution of X. For the independence of J and J', consider the joint probability distribution of J and J', given by

$$\begin{aligned} P_{JJ'}(j,j') &= P_{J'J\mathcal{E}}(j',j) + P_{J'J\bar{\mathcal{E}}}(j',j) \\ &= P_J(j)\Pr[\mathcal{E}|J=j]P_{J'|J\mathcal{E}}(j'|j) + P_J(j)\Pr[\bar{\mathcal{E}}|J=j]P_{J'|J\bar{\mathcal{E}}}(j'|j) \\ &= P_J(j)\Pr[\bar{\mathcal{E}}|J=j'], \end{aligned}$$

where the last equality follows by separately analyzing the cases $j = j'$ and $j \neq j'$. It follows immediately that the marginal distribution of J' is $P_{J'}(j') = \sum_j P_{JJ'}(j,j') = \Pr[\bar{\mathcal{E}}|J=j']$, and thus $P_{JJ'} = P_J \cdot P_{J'}$.

What is left to do for the case $\alpha = 0$ is to deal with the case where there exists j^* with $\Pr[\mathcal{E}|J=j^*] = 0$. Since $\sum_{j\in[m]} \Pr[\bar{\mathcal{E}}|J=j] = 1$, it holds that $\Pr[\bar{\mathcal{E}}|J=j] = 0$ for $j \neq j^*$. This motivates to define J' as $J' := j^*$ with probability 1. Note that this definition directly implies that J' is independent from J. Furthermore, by the above observations: $\mathcal{E} \iff J \neq J'$. This concludes the case $\alpha = 0$.

Next, we consider the case $\alpha > 0$. The idea is to "inflate" the event $\mathcal{E}$ so that α becomes 0, i.e., to define an event $\mathcal{E}'$ that contains $\mathcal{E}$ (meaning that $\mathcal{E} \implies \mathcal{E}'$) so that

$\sum_{j\in[m]} \Pr[\mathcal{E}'|J=j] = m-1$, and to define J' as in the case $\alpha = 0$ (but now using $\mathcal{E}'$). Formally, we define $\mathcal{E}'$ as the disjoint union $\mathcal{E}' = \mathcal{E} \vee \mathcal{E}_\circ$ of $\mathcal{E}$ and an event $\mathcal{E}_\circ$. The event $\mathcal{E}_\circ$ is defined by means of $\Pr[\mathcal{E}_\circ|\mathcal{E}, J=j, X=x] = 0$, so that $\mathcal{E}$ and $\mathcal{E}_\circ$ are indeed disjoint, and $\Pr[\mathcal{E}_\circ|J=j, X=x] = \alpha/m$, so that indeed

$$\sum_{j\in[m]} \Pr[\mathcal{E}'|J=j] = \sum_{j\in[m]} (\Pr[\mathcal{E}|J=j] + \Pr[\mathcal{E}_\circ|J=j]) = (m-1-\alpha)+\alpha = m-1\,.$$

We can now apply the analysis of the case $\alpha = 0$ to conclude the existence of J', independent of J, such that $J \neq J' \iff \mathcal{E}'$ and thus $(J \neq J') \wedge \bar{\mathcal{E}}_\circ \iff \mathcal{E}' \wedge \bar{\mathcal{E}}_\circ \iff \mathcal{E}$. Setting $\Psi := \bar{\mathcal{E}}_\circ$, it follows that

$$H_{\min}(X|J=j, J\neq J', \Psi) = H_{\min}(X|J=j,\mathcal{E}) \geq (\delta/2 - 2\epsilon)n\,,$$

where $\Pr[\Psi] = 1 - \Pr[\mathcal{E}_\circ] = 1 - \alpha/m \geq 1 - (2m-1)2^{-\epsilon n}/m \geq 1 - 2\cdot 2^{-\epsilon n}$. Finally, using similar reasoning as in the case $\alpha = 0$, it follows that the same bound holds for $H_{\min}(X|J=j, J'=j', \Psi)$ whenever $j \neq j'$. This concludes the case $\alpha > 0$.

Finally, we consider the case $\alpha < 0$. The approach is the same as above, but now $\mathcal{E}'$ is obtained by "deflating" $\mathcal{E}$. Specifically, we define $\mathcal{E}'$ by means of $\Pr[\mathcal{E}'|\bar{\mathcal{E}}, J=j, X=x] = \Pr[\mathcal{E}'|\bar{\mathcal{E}}] = 0$, so that $\mathcal{E}'$ is contained in $\mathcal{E}$, and $\Pr[\mathcal{E}'|\mathcal{E}, J=j, X=x] = \Pr[\mathcal{E}'|\mathcal{E}] = \frac{m-1}{m-1-\alpha}$, so that

$$\sum_{j\in[m]} \Pr[\mathcal{E}'|J=j] = \sum_{j\in[m]} \Pr[\mathcal{E}'|\mathcal{E}]\cdot\Pr[\mathcal{E}|J=j] = m-1\,.$$

Again, from the $\alpha = 0$ case we obtain J', independent of J, such that the event $J \neq J'$ is equivalent to the event $\mathcal{E}'$.

It follows that

$$\begin{aligned} H_{\min}(X|J=j, J\neq J') &= H_{\min}(X|J=j,\mathcal{E}') = H_{\min}(X|J=j,\mathcal{E}',\mathcal{E}) \\ &\geq H_{\min}(X|J=j,\mathcal{E}) - \log(P[\mathcal{E}'|\mathcal{E}, J=j]) \geq (\delta/2-2\epsilon)n - 1\,, \end{aligned}$$

where the second equality holds because $\mathcal{E}' \implies \mathcal{E}$, the first inequality holds because additionally conditioning on $\mathcal{E}'$ increases the probabilities of X conditioned on $J=j$ and $\mathcal{E}$ by at most a factor $1/P[\mathcal{E}'|\mathcal{E}, J=j]$, and the last inequality holds by Corollary VI.2.3 and because $P[\mathcal{E}'|\mathcal{E}, J=j] = \frac{m-1}{m-1-\alpha} \geq \frac{1}{2}$, where the latter holds since $\alpha \geq -1$. Finally, using similar reasoning as in the previous cases, it follows that the same bound holds for $H_{\min}(X|J=j, J'=j')$ whenever $j \neq j'$. This concludes the proof. □

VI.2.1 Constructing Good Families of Bases

Here, we discuss some interesting choices for the family $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of bases. We say that such a family is "good" if $\delta = -\frac{1}{n}\log(c^2)$ converges to a strictly positive constant

as n tends to infinity. There are various ways to construct such families. For example, a family obtained through sampling according to the Haar measure will be good with overwhelming probability (a precise statement, in which "good" means $\delta = 0.9$, can be found at the very end of the proof of Theorem 2.5 of [47]). The best possible constant $\delta = 1$ is achieved for a family of *mutually unbiased bases*. However, for arbitrary quantum systems (i.e., not necessarily multi-qubit systems) it is not well understood how large such a family may be, beyond that its size cannot exceed the dimension plus 1.

In the upcoming section, we will use the following simple and well-known construction. For an arbitrary binary code $\mathcal{C} \subset \{0,1\}^n$ of size m, minimum distance d and encoding function $\mathfrak{c} : [m] \to \mathcal{C}$, we can construct a family $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of bases as follows. We identify the jth codeword, i.e. $\mathfrak{c}(j) = (c_1, \ldots, c_n)$ for $j \in [m]$, with the basis $\mathcal{B}_j = \{|x\rangle_{\mathfrak{c}(j)} : x \in \{0,1\}^n\} = \{(H^{c_1} \otimes \cdots \otimes H^{c_n})|x\rangle : x \in \{0,1\}^n\}$. In other words, $\mathcal{B}_j$ measures qubit-wise in the computational or the Hadamard basis, depending on the corresponding coordinate of $\mathfrak{c}(j)$.[7] It is easy to see that the maximum overlap c of the family obtained this way is directly related to the minimum distance of $\mathcal{C}$, namely $\delta = -\frac{1}{n}\log(c^2)$ coincides with the relative minimal distance d/n of $\mathcal{C}$. Hence, choosing an asymptotically good code immediately yields a good family of bases.

VI.3 A New Quantum Identification Protocol

Our application of the new uncertainty relation is in proving security of a new identification protocol in the quantum setting. The goal of (password-based) identification is to "prove" knowledge of a password w (or some other low-entropy key, like a PIN) without giving w away. More formally, given a user U and a server S that hold a pre-agreed password $w \in \mathcal{W}$, U wants to convince S that he indeed knows w, but in such a way that he gives away as little information on w as possible in case he is actually interacting with a dishonest server S^*.

In [35], Damgård *et al.* showed the existence of a secure identification protocol in the *bounded-quantum-storage* model. The protocol involves the communication of qubits, and is secure against an arbitrary dishonest server S that has limited quantum storage capabilities and can only store a certain fraction of the communicated qubits, whereas the security against a dishonest user U^* holds unconditionally.

On the negative side, it is known that *without* any restriction on (one of) the dishonest participants, secure identification is impossible (even in the quantum setting). Indeed, if a quantum protocol is unconditionally secure against a dishonest user, then unavoidably it can be broken by a dishonest server with unbounded quantum-storage and unbounded

[7] If $c_j = 0$, $\mathcal{B}_j$ measures qubit j in the computational basis $+ = \{|0\rangle, |1\rangle\}$. If $c_j = 1$, $\mathcal{B}_j$ measures qubit j in the *Hadamard basis* $\times = \{H|0\rangle, H|1\rangle\}$. Thus we identify $\{0,1\}^n$ with the set of product basis where each of them is taken to be the computational or the *Hadamard basis*.

quantum-computing power; this follows essentially from [107] (see also [35]). Thus, the best one can hope for (for a protocol that is unconditionally secure against a dishonest user) is that in order to break it, unbounded quantum storage *and* unbounded quantum-computing power is *necessary* for the dishonest server. This is not the case for the protocol of [35]: storing all the communicated qubits as they are, and measuring them qubit-wise in one or the other basis at the end, completely breaks the protocol. Thus, no quantum computing power at all is necessary to break the protocol, only sufficient quantum storage.

In this section, we propose a new identification protocol, which can be regarded as a first step towards closing the above gap. Like the protocol from [35], our new protocol is secure against an unbounded dishonest user and against a dishonest server with limited quantum storage capabilities. The new uncertainty relation forms the main ingredient in the user-security proof in the BQSM. Furthermore, and in contrast to [35], a minimal amount of quantum computation power is *necessary* to break the protocol, beyond sufficient quantum storage. Indeed, next to the security against a dishonest server with bounded quantum storage, we also prove—in Section VI.6—security against a dishonest server that can store all the communicated qubits, but is restricted to measure them qubit-wise (in arbitrary qubit bases) at the end of the protocol execution. Thus, beyond sufficient quantum storage, quantum computation that involves *pairs* of qubits is necessary (and in fact sufficient) to break the new protocol.

Restricting the dishonest server to qubit-wise measurements may look restrictive; however, we stress that in order to break the protocol, the dishonest server needs to store many qubits *and* perform quantum operations on them that go beyond single-qubit operations; this may indeed be considerably more challenging than storing many qubits and measuring them qubit-wise. Furthermore, it turns out that proving security against such a dishonest server that is restricted to qubit-wise measurements is already challenging; indeed, standard techniques do not seem applicable here. Therefore, handling a dishonest server that can, say, act on *blocks* of qubits, must be left to future research.

We first formalize the security properties we want to achieve. We borrow the definitions from [35], which are argued to be "the right ones" in [48].

Definition VI.3.1 (Correctness)**.** *An identification protocol is said to be* ε-correct *if, after an execution by honest* U *and honest* S*,* S *accepts with probability* $1-\varepsilon$*.*

Definition VI.3.2 (User security)**.** *An identification protocol for two parties* U*,* S *is* ε*-secure for the user* U *against (dishonest) server* S^* *if the following holds: If the initial state of* S^* *is independent of* W*, then its state* E *after execution of the protocol is such that there exists a random variable* W' *that is independent of* W *and such that*

$$\rho_{WW'E|W\neq W'} \approx_\varepsilon \rho_{W\leftrightarrow W'\leftrightarrow E|W\neq W'}.$$

Definition VI.3.3 (Server security)**.** *An identification protocol for two parties* U*,* S *is* ε*-secure for the server* S *against (dishonest) user* U^* *if the following holds: whenever the*

initial state of U^* *is independent of* W*, then there exists a random variable* W' *(possibly* $\perp$*) that is independent of* W *such that if* $W \neq W'$ *then* S *accepts with probability at most* ε*. Furthermore, the common state* ρ_{WE} *after execution of the protocol (including* S*'s announcement to accept or reject) satisfies*

$$\rho_{WW'E|W\neq W'} \approx_\varepsilon \rho_{W\leftrightarrow W'\leftrightarrow E|W\neq W'}.$$

We will prove the user-security of the protocol in two different models, in which different assumptions are made. Because these assumptions are in some sense "orthogonal", the hope is that if security would break down in one model to a failing assumption, the protocol is still secure by the other model.

Let $\mathcal{C} \subset \{0,1\}^n$ be a binary code with minimum distance d, and let $\mathfrak{c} : \mathcal{W} \to \mathcal{C}$ be its encoding function. Let $m := |\mathcal{W}|$, and typically, $m < 2^n$. Let $\mathcal{F}$ be the class of all linear functions from $\{0,1\}^n$ to $\{0,1\}^\ell$, where $\ell < n$, represented as $\ell \times n$ binary matrices. It is well-known that this class is two-universal. Furthermore, let $\mathcal{G}$ be a strongly two-universal class of hash functions from $\mathcal{W}$ to $\{0,1\}^\ell$. Protocol `Q-ID` is shown below.

Protocol `Q-ID`

1. U picks $x \in \{0,1\}^n$ independently and uniformly at random and sends $|x\rangle_{\mathfrak{c}(w)}$ to S.
2. S measures in basis $\mathfrak{c}(w)$. Let x' be the outcome.
3. U picks $f \in \mathcal{F}$ independently and uniformly at random and sends it to S
4. S picks $g \in \mathcal{G}$ independently and uniformly at random and sends it to U
5. U computes and sends $z := f(x) \oplus g(w)$ to S
6. S accepts if and only if $z = z'$ where $z' := f(x') \oplus g(w)$

Our protocol is quite similar to the protocol in [35]. The difference is that in our protocol, both parties, U and S, use $\mathfrak{c}(w)$ as basis for preparing/measuring the qubits in step (1) and (2), whereas in [35], only S uses $\mathfrak{c}(w)$ and U uses a *random* basis $\theta \in \{0,1\}^n$ instead, and then U communicates θ to S and all the positions where θ and $\mathfrak{c}(w)$ differ are dismissed. Thus, in some sense, our new protocol is more natural since why should U use a random basis when he knows the right basis (i.e., the one that S uses)? In [35], using a random basis (for U) was crucial for their proof technique, which is based on an entropic uncertainty relation of a certain form, which asks for a random basis. However, using a random basis, which then needs to be announced, renders the protocol insecure against a dishonest server S^* that is capable of storing all the communicated qubits and then measure them in the right basis once it has been announced. Our new uncertainty relation applies to the case where an n-qubit state is measured in a basis that is sampled from a code $\mathcal{C}$, and thus is applicable to the new protocol where U uses basis $\mathfrak{c}(w) \in \mathcal{C}$. Since this basis is common knowledge (to the honest participants), it does not have to be communicated, and as such a straightforward store-and-then-measure attack as above does not apply.

A downside of our protocol is that security only holds in case of a perfect quantum source, which emits exactly one qubit when triggered. Indeed, a multi-photon emission enables a dishonest server S^* to learn information on the basis used, and thus gives away information on the password w in our protocol.

It is straightforward to verify that (in the ideal setting with perfect sources, no noise, etc.) `Q-ID` satisfies the correctness property (Definition VI.3.1) perfectly, i.e. $\varepsilon = 0$. In the remaining sections, we prove (unconditional) security against a dishonest user, and we prove security against two kinds of restricted dishonest servers. First, against a dishonest server that has limited quantum storage capabilities, and then against a dishonest server that can store an unbounded number of qubits, but can only store and measure them qubit-wise.

VI.4 (Unconditional) Server Security

We claim security of `Q-ID` against an arbitrary dishonest user U^* (that is merely restricted by the laws of quantum mechanics).

Theorem VI.4.1. `Q-ID` *is ε-secure for the server with $\varepsilon = \binom{m}{2}2^{-\ell}$.*

Proof. Clearly, from the steps (1) to (5) in the protocol `Q-ID`, U^* learns no information on W at all. The only information he may learn is by observing whether S accepts or not in step (6). Therefore, in order to prove server security, it suffices to show the existence of a random variable W', independent of W, with the property that S rejects whenever $W' \neq W$ (except with probability $\frac{1}{2}m(m-1)2^{-\ell}$).

We may assume that $\mathcal{W} = \{1, \ldots, m\}$. Let $\rho_{WX'FGZE}$ be the state describing the password W, the variables X', F, G and Z occurring in the protocol from the server's point of view, and U^*'s quantum state E *before* observing S's decision to accept or reject. For any $w \in \mathcal{W}$, consider the state $\rho^w_{X'FGZE} := \rho_{X'FGZE|W=w}$. Note that the reduced state ρ^w_{FGZE} is the same for any $w \in \mathcal{W}$; this follows from the assumption that U^*'s initial state is independent of W and because F, G and Z are produced independently of W. We may thus write $\rho^w_{X'FGZE}$ as $\rho_{X'_wFGZE}$, and we can "glue together" the states $\rho_{X'_wFGZE}$ for all choices of w. This means, there exists a state $\rho_{X'_1\cdots X'_mFGZE_1\cdots E_m}$ that correctly reduces to $\rho_{X'_wFGZE_w} = \rho_{X'_wFGZE}$ for any $w \in \mathcal{W}$, and conditioned on FGZ, we have that X'_iE_i is independent of X'_jE_j for any $i \neq j \in \mathcal{W}$. It is easy to see that for any $i \neq j \in \mathcal{W}$, G is independent of X'_i, X'_j and F. Therefore, by the strong two-universality of G, for any $i \neq j$ it holds that $Z'_i \neq Z'_j$ except with probability $2^{-\ell}$, where $Z'_w = FX'_w + G(w)$ for any w. Therefore, by the union bound, $Z'_1, \ldots, Z'_m$ are pairwise distinct and thus Z can coincide with at most one of the Z'_w's, except with probability $\varepsilon = \frac{1}{2}m(m-1)2^{-\ell}$. Let W' be defined such that $Z = Z'_{W'}$; if there is no such Z'_w then we let $W' = \perp$, and if there are more than one then we let it be the first. Recall, the latter can happen

with probability at most ε. We now extend the state $\rho_{X_1'\cdots X_m' FGZW'E_1\cdots E_m}$ by W, chosen independently according to P_W. Clearly W' is independent of W. Furthermore, except with probability at most ε, if $W \neq W'$ then $Z \neq Z_W'$. Finally note that $\rho_{X_W' FGZW'WE_W}$ is such that $\rho_{X_W' FGZWE_W} = \sum_w P_W(w)\rho_{X_w' FGZE_w} \otimes |w\rangle\langle w| = \sum_w P_W(w)\rho^w_{X'FGZE} \otimes |w\rangle\langle w| = \rho_{X'FGZWE}$. Thus, also with respect to the state $\rho_{X'FGZWE}$ there exist W', independent of W, such that if $W' \neq W$ then $Z \neq Z'$ except with probability at most ε. This was to be shown. □

VI.5 User Security in the Bounded-Quantum-Storage Model

We consider a dishonest server S^*, and prove security of `Q-ID` in the *bounded-quantum-storage model*. In this model, as introduced in [34], it is assumed that the adversary (here S^*) cannot store more than a fixed number of qubits, say q. The security proof of `Q-ID` in the bounded-quantum-storage model is very similar to the corresponding proof in [35] for their protocol, except that we use the new uncertainty relation from Section VI.2. Furthermore, since our uncertainty relation (Theorem VI.2.4) already guarantees the existence of the random variable W' as required by the security property, no *entropy-splitting* as in [35] is needed.

In the following, let $\delta := d/n$, i.e. the relative minimum distance of $\mathcal{C}$.

Theorem VI.5.1. *Let S^* be a dishonest server whose quantum memory is at most q qubits at step 3 of* `Q-ID`*. Then, for any $0 < \kappa < \delta/4$,* `Q-ID` *is ε-secure for the user with*

$$\varepsilon = 2^{-\frac{1}{2}((\delta/2-2\kappa)n-1-q-\ell)} + 4 \cdot 2^{-\kappa n}.$$

Proof. We consider and analyze a purified version of `Q-ID` where in step (1) instead of sending $|X\rangle_c$ to S^* for a uniformly distributed X, U prepares a fully entangled state $2^{-n/2}\sum_x |x\rangle|x\rangle$ and sends the second register to S^* while keeping the first. Then, in step (3) when the memory bound has applied, U measures his register in the basis $\mathfrak{c}(W)$ in order to obtain X. Note that this procedure produces exactly the same common state as in the original (non-purified) version of `Q-ID`. Thus, we may just as well analyze this purified version.

The state of S^* consists of his initial state and his part of the EPR pairs, and may include an additional ancilla register. Before the memory bound applies, S^* may perform any unitary transformation on his composite system. When the memory bound is applied (just before step (3) is executed in `Q-ID`), S^* has to measure all but q qubits of his system. Let the classical outcome of this measurement be denoted by y, and let E' be the remaining quantum state of at most q qubits. The common state has collapsed to a $(n+q)$-qubit state and depends on y; the analysis below holds for any y. Next, U measures his n-qubit part of the common state in basis $\mathfrak{c}(W)$; let X denote the classical outcome of this measurement.

By our new uncertainty relation (Theorem VI.2.4) and subsequently applying the min-entropy chain rule that is given in Lemma VI.1.4 (to take the q stored qubits into account) it follows that there exists W', independent of W, and an event Ψ that occurs at least with probability $1 - 2 \cdot 2^{-\kappa n}$ such that

$$H_{\min}(X|E', W = w, W' = w', \Psi) \geq (\delta/2 - 2\kappa)n - 1 - q.$$

for any w, w' such that $w \neq w'$. Because U chooses F independently at random from a 2-universal family, privacy amplification guarantees that

$$d_{\text{unif}}(F(X)|E'F, W = w, W' = w') \leq \varepsilon' := \frac{1}{2} \cdot 2^{-\frac{1}{2}((\delta/2-2\kappa)n-1-q-\ell)} + 2 \cdot 2^{-\kappa n},$$

for any w, w' such that $w \neq w'$. Recall that $Z = F(X) \oplus G(W)$. By security of the one-time pad it follows that

$$d_{\text{unif}}(Z|E'FG, W = w, W' = w') \leq \varepsilon', \tag{VI.3}$$

for any w, w' such that $w \neq w'$. To prove the claim, we need to bound,

$$\begin{aligned}
&\delta(\rho_{WW'E|W\neq W'}, \rho_{W\leftrightarrow W'\leftrightarrow E|W\neq W'}) \\
&\quad = \tfrac{1}{2}\|\rho_{WW'E'FGZ|W\neq W'} - \rho_{W\leftrightarrow W'\leftrightarrow E'FGZ|W\neq W'}\|_1 \\
&\quad \leq \tfrac{1}{2}\|\rho_{WW'E'FGZ|W\neq W'} - \rho_{WW'E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I}\|_1 \\
&\qquad + \tfrac{1}{2}\|\rho_{WW'E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} - \rho_{W\leftrightarrow W'\leftrightarrow E'FGZ|W\neq W'}\|_1
\end{aligned} \tag{VI.4}$$

where the equality follows by definition of trace distance (Definition **??**) and the fact that the output state E is obtained by applying a unitary transformation to the set of registers (E', F, G, W', Z). The inequality is the triangle inequality; in the remainder of the proof, we will show that both terms in (VI.4) are upper bounded by ε'.

$$\begin{aligned}
&\tfrac{1}{2}\|\rho_{WW'E'FGZ|W\neq W'} - \rho_{WW'E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I}\|_1 \\
&\quad = \sum_{w\neq w'} P_{WW'|W\neq W'}(w, w')\, d_{\text{unif}}(Z|E'FG, W = w, W' = w') \leq \varepsilon',
\end{aligned}$$

where the latter inequality follows from (VI.3).For the other term, we reason as follows:

$$
\begin{aligned}
&\tfrac{1}{2}\|\rho_{WW'E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} - \rho_{W\leftrightarrow W'\leftrightarrow E'FGZ|W\neq W'}\|_1 \\
&= \tfrac{1}{2}\sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\,\|\rho^{w,w'}_{E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} - \rho^{w'}_{E'FGZ|W\neq W'}\|_1 \\
&= \tfrac{1}{2}\sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\,\|\rho^{w,w'}_{E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} \\
&\qquad - \sum_{\substack{w'' \\ \text{s.t. } w''\neq w'}} P_{W|W',W\neq W'}(w''|w')\rho^{w'',w'}_{E'FGZ|W\neq W'}\|_1 \\
&= \tfrac{1}{2}\sum_{w'} P_{W'|W\neq W'}(w')\,\|\sum_{\substack{w \\ \text{s.t. } w\neq w'}} P_{W|W',W\neq W'}(w|w')\rho^{w,w'}_{E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} \\
&\qquad - \sum_{\substack{w'' \\ \text{s.t. } w''\neq w'}} P_{W|W',W\neq W'}(w''|w')\rho^{w'',w'}_{E'FGZ|W\neq W'} \sum_{\substack{w \\ \text{s.t. } w\neq w'}} P_{W|W',W\neq W'}(w|w')\|_1 \\
&= \tfrac{1}{2}\sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\,\|\rho^{w,w'}_{E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} - \rho^{w,w'}_{E'FGZ|W\neq W'}\|_1 \\
&= \sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\, d_{\mathrm{unif}}(Z|E'FG, W=w, W'=w') \leq \varepsilon',
\end{aligned}
$$

where the first equality follows by definition of conditional independence and by a basic property of the trace distance; the third and fourth equality follow by linearity of the trace distance. The inequality on the last line follows from (VI.3). This proves the claim. □

VI.6 User Security in the Single-Qubit-Operations Model

We now consider a dishonest server S^* that can store an unbounded number of qubits. Clearly, against such a S^*, Theorem VI.5.1 provides no security guarantee anymore. We show here that there is still *some* level of security left. Specifically, we show that `Q-ID` is still secure against a dishonest server S^* that can reliably store all the communicated qubits and measure them qubit-wise and non-adaptively at the end of the protocol. This feature distinguishes our identification protocol from the protocol from [35], which completely breaks down against such an attack.

Formally, a dishonest server S^* in the SQOM is modeled as follows.

1. S^* may reliably store the n-qubit state $|x\rangle_{\mathfrak{c}(w)} = |x_1\rangle_{\mathfrak{c}(w)_1} \otimes \cdots \otimes |x_n\rangle_{\mathfrak{c}(w)_n}$ received in step (1) of `Q-ID`.

2. At the end of the protocol, in step (5), S^* chooses an arbitrary sequence $\theta = (\theta_1, \ldots, \theta_n)$, where each θ_i describes an arbitrary orthonormal basis of $\mathbb{C}^2$, and mea-

sures each qubit $|x_i\rangle_{\mathtt{c}(w)_i}$ in basis θ_i to observe $Y_i \in \{0,1\}$. Hence, we assume that S^* *measures all qubits at the end of the protocol.*

3. The choice of θ may depend on all the classical information gathered during the execution of the protocol, but we assume a *non-adaptive* setting where θ_i does not depend on Y_j for $i \neq j$, i.e., S^* has to choose θ entirely before performing any measurement.

Considering complete von Neumann measurements acting on individual qubits, rather than general single-qubit POVMs, may be considered a restriction of our model. Nonetheless, general POVM measurements can always be described by von Neumann measurements on a bigger system. In this sense, restricting to von Neumann measurements is consistent with the requirement of single-qubit operations. It seems non-trivial to extend our security proof to general single-qubit POVMs.

The restriction to non-adaptive measurements (item 3) is rather strong, even though the protocol from [35] already breaks down in this non-adaptive setting. The restriction was introduced as a stepping stone towards proving the adaptive case. Up to now, we have unfortunately not yet succeeded in doing so, hence we leave the adaptive case for future research.

We also leave for future research the case of a less restricted dishonest server S^* that can do measurements on blocks that are less stringently bounded in size. Whereas the adaptive versus non-adaptive issue appears to be a proof-technical problem (`Q-ID` looks secure also against an adaptive S^*), allowing measurements on larger blocks will require a new protocol, since `Q-ID` becomes insecure when S^* can do measurements on blocks of size 2, as we show in Section VI.6.4.

VI.6.1 No Privacy Amplification

One might expect that proving security of `Q-ID` in the SQOM, i.e., against a dishonest server S^* that is restricted to single-qubit operations should be straightforward, but actually the opposite is true, for the following reason. Even though it is not hard to show that after his measurements, S^* has lower bounded uncertainty in x (except if he was able to guess w), it is not clear how to conclude that $f(x)$ is close to random so that z does not reveal a significant amount of information about w. The reason is that standard privacy amplification fails to apply here. Indeed, the model allows S^* to postpone the measurement of all qubits to step (5) of the protocol. The hash function f, however, is chosen and sent already in step (3). This means that S^* can choose his measurements in step (5) depending on f. As a consequence, the distribution of x from the point of view of S^* may depend on the choice of the hash function f, in which case the privacy-amplification theorem does not give any guarantees.

VI.6.2 Single-Qubit Measurements

Consider an arbitrary sequence $\theta = (\theta_1, \ldots, \theta_n)$ where each θ_i describes an orthonormal basis of $\mathbb{C}^2$. Let $|\psi\rangle$ be an n-qubit system of the form

$$|\psi\rangle = |x\rangle_b = H^{b_1}|x_1\rangle \otimes \cdots \otimes H^{b_n}|x_n\rangle,$$

where x and b are arbitrary in $\{0,1\}^n$. Measuring $|\psi\rangle$ qubit-wise in basis θ results in a measurement outcome $Y = (Y_1, \ldots, Y_n) \in \{0,1\}^n$. Suppose that x, b and θ are in fact realizations of the random variables X, B and Θ respectively. It follows immediately from the product structure of the state $|\psi\rangle$ that

$$P_{Y|XB\Theta}(y|x,b,\theta) = \prod_{i=0}^{n} P_{Y_i|X_iB_i\Theta_i}(y_i|x_i,b_i,\theta_i),$$

i.e. the random variables Y_i are statistically independent conditioned on arbitrary fixed values for X_i, B_i and Θ_i but such that $P_{X_iB_i\Theta_i}(x_i,b_i,\theta_i) > 0$.

Lemma VI.6.1. *The distribution $P_{Y_i|X_iB_i\Theta_i}(y_i|x_i,b_i,\theta_i)$ exhibits the following symmetries:*

$$P_{Y_i|X_iB_i\Theta_i}(0|0,b_i,\theta_i) = P_{Y_i|X_iB_i\Theta_i}(1|1,b_i,\theta_i)$$

and

$$P_{Y_i|X_iB_i\Theta_i}(0|1,b_i,\theta_i) = P_{Y_i|X_iB_i\Theta_i}(1|0,b_i,\theta_i)$$

for all $i \in [n]$, for all b_i and θ_i with $P_{X_iB_i\Theta_i}(\xi,b_i,\theta_i) > 0$ for all $\xi \in \{0,1\}$.

Proof. Let $\alpha, \beta \in \mathbb{C}$ be such that $\theta_i := \{\alpha|0\rangle + \beta|1\rangle, \beta|0\rangle - \alpha|1\rangle\}$. (We can always find such α and β.) Writing out the measurement explicitly gives

$$\begin{aligned} P_{Y_i|X_iB_i\Theta_i}(0|x_i,b_i,\theta_i) &= |(\alpha\langle 0| + \beta\langle 1|)H^{b_i}|x_i\rangle|^2 \qquad \text{and} \\ P_{Y_i|X_iB_i\Theta_i}(1|x_i,b_i,\theta_i) &= |(\beta\langle 0| - \alpha\langle 1|)H^{b_i}|x_i\rangle|^2. \end{aligned}$$

Hence, it suffices to prove that

$$|(\alpha\langle 0| + \beta\langle 1|)H^{b_i}|x_i\rangle|^2 = |(\beta\langle 0| - \alpha\langle 1|)H^{b_i}|x_i \oplus 1\rangle|^2 \tag{VI.5}$$

for every $x_i, b_i \in \{0,1\}$.

We first show (VI.5) for $b_i = 0$. Using that σ_X is unitary and hermitian we have

$$\begin{aligned} |(\alpha\langle 0| + \beta\langle 1|)|x_i\rangle|^2 &= |(\alpha\langle 0| + \beta\langle 1|)\sigma_X\sigma_X|x_i\rangle|^2 = |(\alpha\langle 1| + \beta\langle 0|)|x_i \oplus 1\rangle|^2 \\ &= |(\beta\langle 0| - \alpha\langle 1|)|x_i \oplus 1\rangle|^2 \end{aligned}$$

The last equation follows because the expression equals either $|\alpha|^2$ or $|\beta|^2$ (depending on $x_i \in \{0,1\}$), hence we may freely change the sign of α. For $b_i = 1$, we have

$$|(\alpha\langle 0| + \beta\langle 1|)H|x_i\rangle|^2 = |(\alpha\langle 0| + \beta\langle 1|)(|0\rangle + (-1)^{x_i}|1\rangle)|^2 = |\alpha + (-1)^{x_i}\beta|^2$$

and

$$|(\beta\langle 0| - \alpha\langle 1|)H|x_i \oplus 1\rangle|^2 = |(\beta\langle 0| - \alpha\langle 1|)(|0\rangle - (-1)^{x_i}|1\rangle)|^2 = |\beta + (-1)^{x_i}\alpha|^2.$$

We see that those expressions are equal for every $x_i \in \{0,1\}$. □

The symmetry characterized in Lemma VI.6.1 coincides with that of the *binary symmetric channel*, i.e. we can view Y as a "noisy version" of X, where this noise—produced by the measurement—is independent of X.

Formally, we can write Y as

$$Y = X \oplus \Delta, \tag{VI.6}$$

where the random variable $\Delta = (\Delta_1, \ldots, \Delta_n) \in \{0,1\}^n$ thus represents the error between the random variable $X \in \{0,1\}^n$ that is "encoded" in the quantum state and the measurement outcome $Y \in \{0,1\}^n$. By substituting (VI.6) in Lemma VI.6.1, we get the following corollary.

Corollary VI.6.2 (Independence Between Δ and X)**.** *For every $i \in [n]$ it holds that*

$$P_{\Delta_i|X_iB_i\Theta_i}(\delta_i|x_i, b_i, \theta_i) = P_{\Delta_i|B_i\Theta_i}(\delta_i|b_i, \theta_i)$$

for all $\delta_i \in \{0,1\}$ and for all x_i, b_i and θ_i such that $P_{X_iB_i\Theta_i}(x_i, b_i, \theta_i) > 0$.

Furthermore, since the random variables Y_i are statistically independent conditioned on fixed values for X_i, B_i and Θ_i, it follows that the Δ_i are statistically independent conditioned on fixed values for B_i and Θ_i.

Definition VI.6.3 (Quantized Basis)**.** *For any orthonormal basis $\theta_i = \{|v_1\rangle, |v_2\rangle\}$ on $\mathbb{C}^2$, we define the* quantized basis *of θ_i as*

$$\hat{\theta}_i := j^* \in \{0,1\}, \quad \textit{where } j^* \in \operatorname*{arg\,max}_{j\in\{0,1\}} \max_{k\in\{1,2\}} |\langle v_k|H^j|0\rangle|.$$

If both $j \in \{0,1\}$ attain the maximum, then j^* is chosen arbitrarily. The quantized basis of the sequence $\theta = (\theta_1, \ldots, \theta_n)$ is naturally defined as the element-wise application of the above, resulting in $\hat{\theta} \in \{0,1\}^n$.

We will use the bias as a measure for the predictability of Δ_i.

Theorem VI.6.4. *When measuring the qubit $H^{b_i}|x_i\rangle$ for any $x_i, b_i \in \{0,1\}$ in any orthonormal basis θ_i on $\mathbb{C}^2$ for which the quantized basis $\hat{\theta}_i$ is the complement of b_i, i.e. $\hat{\theta}_i = b_i \oplus 1$, then the bias of $\Delta_i \in \{0,1\}$, where $\Delta_i = Y_i \oplus x_i$ and $Y_i \in \{0,1\}$ is the measurement outcome, is upper bounded by*

$$\mathrm{bias}(\Delta_i) \leq \frac{1}{\sqrt{2}}.$$

Since the theorem holds for any $x_i \in \{0,1\}$ and since Corollary VI.6.2 guarantees that Δ_i is independent from an arbitrary random variable X_i, the theorem also applies when we replace x_i by the random variable X_i.

In order to prove Theorem VI.6.4, we need the following lemma.

Lemma VI.6.5. *If, for any orthonormal basis θ_i on $\mathbb{C}^2$, there exists a bit $b_i \in \{0,1\}$ so that when measuring the qubit $H^{b_i}|x_i\rangle$ for any $x_i \in \{0,1\}$ in the basis θ_i to obtain $Z_i \in \{0,1\}$ it holds that*

$$\mathrm{bias}(Z_i) \geq 1/\sqrt{2},$$

then it holds that when measuring the qubit $H^{b_i \oplus 1}|x_i\rangle$ in the basis θ_i to obtain $Y_i \in \{0,1\}$,

$$\mathrm{bias}(Y_i) \leq 1/\sqrt{2}.$$

Proof. First note that for any $x_i, b_i \in \{0,1\}$ and any orthonormal basis θ_i on $\mathbb{C}^2$, measuring a state $H^{b_i}|x_i\rangle$ in $\theta_i = \{|v\rangle, |w\rangle\}$ where $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|w\rangle = \beta|0\rangle - \alpha|1\rangle$ gives the same outcome distribution (up to permutations) as when measuring one of the basis states of θ_i (when viewed as a quantum state), say $|w\rangle$, using the basis $\{H^{b_i}|x_i\rangle, H^{b_i}|x_i \oplus 1\rangle\}$. To see why this holds, note that it follows immediately that $|\langle w|H^{b_i}|x_i\rangle|^2 = |\langle x_i|H^{b_i}|w\rangle|^2$. Furthermore, we have already shown in the proof of Lemma VI.6.1 that

$$|\langle v|H^{b_i}|x_i\rangle|^2 = |\langle w|H^{b_i}|x_i \oplus 1\rangle|^2$$

holds.

Hence, we can apply Theorem VI.2.1 with $\rho = |w\rangle\langle w|$ (this implies that $n = 1$), $m = 2$ and $\mathcal{B}_0$ and $\mathcal{B}_1$ are the computational and Hadamard basis respectively. The maximum overlap between those bases is $c = 1/\sqrt{2}$. Theorem VI.2.1 gives us that

$$p_{\max}^{\{|0\rangle,|1\rangle\}} + p_{\max}^{\{|+\rangle,|-\rangle\}} \leq 1 + \frac{1}{\sqrt{2}},$$

where $p_{\max}^{\{|0\rangle,|1\rangle\}}$ and $p_{\max}^{\{|+\rangle,|-\rangle\}}$ respectively denote the maximum probability in the distribution obtained by measuring in the computational and Hadamard basis. By simple

manipulations we can write this as a bound on the sum of the biases:

$$\begin{aligned}\frac{2}{\sqrt{2}} &\geq (2p_{\max}^{\{|0\rangle,|1\rangle\}} - 1) + (2p_{\max}^{\{|+\rangle,|-\rangle\}} - 1) \\ &= \mathrm{bias}(Y_i) + \mathrm{bias}(Z_i). \end{aligned} \tag{VI.7}$$

From this relation, the claim follows immediately. □

Following [153], we want to remark that both biases in (VI.7) are equal to $1/\sqrt{2}$ when θ_i is the *Breidbart basis*, which is the basis that is precisely "in between" the computational and the Hadamard basis:[8]

$$|v\rangle = \cos(\tfrac{\pi}{8})|0\rangle + \sin(\tfrac{\pi}{8})|1\rangle \qquad \text{and} \qquad |w\rangle = \sin(\tfrac{\pi}{8})|0\rangle - \cos(\tfrac{\pi}{8})|1\rangle.$$

Proof of Theorem VI.6.4 . Let $\theta_i = \{|v_0\rangle, |v_1\rangle\}$. We will make a case distinction based on the value of

$$\mu := \max_{k\in\{0,1\}} |\langle v_k|H^{\hat{\theta}_i}|0\rangle|. \tag{VI.8}$$

If $\mu \leq \cos(\pi/8)$, then we also have that $\max_{k\in\{0,1\}} |\langle v_k|H^{b_i}|x_i\rangle| \leq \cos(\pi/8)$ where $b_i = \hat{\theta}_i \oplus 1$, this holds by definition of the quantized basis (Definition VI.6.3). Then, the probability of obtaining outcome $Y_i = k^*$, where $k^* \in \{0,1\}$ achieves the maximum in (VI.8), is bounded by

$$P_{Y_i}(k^*) = |\langle v_{k^*}|H^{b_i}|x_i\rangle|^2 \leq \cos^2(\pi/8) = \tfrac{1}{2} + \tfrac{1}{2\sqrt{2}}.$$

Hence,

$$\mathrm{bias}(\Delta_i) = \mathrm{bias}(Y_i) = |P_{Y_i}(k^*) - (1 - P_{Y_i}(k^*))| = |2P_{Y_i}(k^*) - 1| \leq \tfrac{1}{\sqrt{2}}.$$

If $\mu > \cos(\pi/8)$, then when measuring the state $H^{\hat{\theta}_i}|x_i\rangle$ in θ_i to obtain $Z_i \in \{0,1\}$, we have that $\mathrm{bias}(Z_i) > 1/\sqrt{2}$ (this follows from similar computations as performed above). We now invoke Lemma VI.6.5 to conclude that when measuring the state $H^{b_i}|x_i\rangle$ in θ_i to obtain Y_i, $\mathrm{bias}(\Delta_i) = \mathrm{bias}(Y_i) < \frac{1}{\sqrt{2}}$. □

VI.6.3 User Security of `Q-ID`

We are now ready to state and prove the security of `Q-ID` against a dishonest user in the SQOM.

[8] In [153], the corresponding state is called the "Hadamard-invariant state."

Theorem VI.6.6 (User Security)**.** *Let* S^* *be a dishonest server with unbounded quantum storage that is restricted to non-adaptive single-qubit operations, as specified in Section VI.6. Then, for any* $0 < \beta < \frac{1}{4}$*, user security (as defined in Definition VI.3.2) holds with*

$$\varepsilon \leq \tfrac{1}{2} 2^{\frac{1}{2}\ell - \frac{1}{4}(\frac{1}{4}-\beta)d} + \tbinom{m}{2} 2^{2\ell} \exp(-2d\beta^2)$$

Note that d is typically linear in n whereas ℓ is chosen independently of n, hence the expression above is negligible in d.

To prove Theorem VI.6.6 we need the following technical lemma and corollary. Recall that $\mathcal{F}$ denotes the class of all linear functions from $\{0,1\}^n$ to $\{0,1\}^\ell$, where $\ell < n$, represented as binary $\ell \times n$ matrices.

Lemma VI.6.7. *Let* n*,* k *and* ℓ *be arbitrary positive integers, let* $0 < \beta < \frac{1}{4}$ *and let* $\mathcal{I} \subset [n]$ *such that* $|\mathcal{I}| \geq k$*, and let* F *be uniform over* $\mathcal{F} = \{0,1\}^{\ell \times n}$*. Then, it holds except with probability* $2^{2\ell} \exp(-2k\beta^2)$ *(the probability is over the random matrix* F*) that*

$$\big|(f \odot g)_{\mathcal{I}}\big| > (\tfrac{1}{4} - \beta)k \qquad \forall f, g \in \operatorname{span}(F) \setminus \{0^n\}$$

Proof. Without loss of generality, we will assume that $|\mathcal{I}| = k$. Now take arbitrary but non-zero vectors $r, s \in \{0,1\}^\ell$ and let $V := rF$ and $W := sF$. We will analyze the case $r \neq s$; the case $r = s$ is similar but simpler. Because each element of F is an independent random bit, and r and s are non-zero and $r \neq s$, V and W are independent and uniformly distributed n-bit vectors with expected relative Hamming weight $1/2$. Hence, on average $|(V \odot W)_{\mathcal{I}}|$ equals $k/4$. Furthermore, using Hoeffding's inequality (Theorem VI.1.2), we may conclude that

$$\Pr\left[\frac{k}{4} - |(V \odot W)_{\mathcal{I}}| > \beta k\right] = \Pr\left[|(V \odot W)_{\mathcal{I}}| < \big(\tfrac{1}{4} - \beta\big)k\right] \leq \exp(-2k\beta^2)\,.$$

Finally, the claim follows by applying the union bound over the choice of r and s (each 2^ℓ possibilities). □

Recall that $\mathcal{C}$ is a binary code with minimum distance d, $\mathfrak{c}(\cdot)$ its encoding function, and that $m := |\mathcal{W}|$.

Corollary VI.6.8. *Let* $0 < \beta < \frac{1}{4}$*, and let* F *be uniformly distributed over* $\mathcal{F}$*. Then,* F *has the following property except with probability* $\binom{m}{2} 2^{2\ell} \exp(-2d\beta^2)$*: for any string* $s \in \{0,1\}^n$ *(possibly depending on the choice of* F*), there exists at most one* $\tilde{c} \in \mathcal{C}$ *such that for any code word* $c \in \mathcal{C}$ *different from* $\tilde{c}$*, it holds that*

$$|f \odot (c \oplus s)| \geq \tfrac{1}{2}(\tfrac{1}{4} - \beta)d \qquad \forall f \in \operatorname{span}(F) \setminus \{0^n\}$$

We prove the statement by arguing for two $\tilde{c}$'s and showing that they must be identical. In the proof, we will make use of the two following propositions.

Proposition VI.6.9. *$|a| \geq |a \odot b|$ for all $a, b \in \{0,1\}^n$.*

Proof. Follows immediately. □

Proposition VI.6.10. *$|a \odot b| + |a \odot c| \geq |a \odot (b \oplus c)|$ for all $a, b, c \in \{0,1\}^n$.*

Proof. $|a \odot (b \oplus c)| = |a \odot b \oplus a \odot c| \leq |a \odot b| + |a \odot c|$, where the equality is the distributivity of the Schur product, and the inequality is the triangle inequality for the Hamming weight. □

Proof of Corollary VI.6.8. By Lemma VI.6.7 with $\mathcal{I} := \{i \in [n] : c_i \neq c'_i\}$ for $c, c' \in \mathcal{C}$, and by applying the union bound over all possible pairs (c, c'), we obtain that except with probability $\binom{m}{2} 2^{2\ell} \exp(-2d\beta^2)$ (over the choice of F), it holds that

$$|f \odot g \odot (c \oplus c')| > (\tfrac{1}{4} - \beta)d \tag{VI.9}$$

for all $f, g \in \operatorname{span}(F) \setminus \{0^n\}$ and all $c, c' \in \mathcal{C}$ with $c \neq c'$.

Now, for such an F, and for every choice of $s \in \{0,1\}^n$, consider $\tilde{c}_1, \tilde{c}_2 \in \mathcal{C}$ and $f_1, f_2 \in \operatorname{span}(F) \setminus \{0^n\}$ such that

$$|f_1 \odot (\tilde{c}_1 \oplus s)| < \tfrac{1}{2}(\tfrac{1}{4} - \beta)d \quad \text{and} \quad |f_2 \odot (\tilde{c}_2 \oplus s)| < \tfrac{1}{2}(\tfrac{1}{4} - \beta)d.$$

We will show that this implies $\tilde{c}_1 = \tilde{c}_2$, which proves the claim. Indeed, we can write

$$\begin{aligned}(\tfrac{1}{4} - \beta)d &> |f_1 \odot (\tilde{c}_1 \oplus s)| + |f_2 \odot (\tilde{c}_2 \oplus s)| \\ &\geq |f_1 \odot f_2 \odot (\tilde{c}_1 \oplus s)| + |f_1 \odot f_2 \odot (\tilde{c}_2 \oplus s)| \geq |f_1 \odot f_2 \odot (\tilde{c}_1 \oplus \tilde{c}_2)|\end{aligned}$$

where the second inequality is Proposition VI.6.9 applied twice and the third inequality is Proposition VI.6.10. This contradicts (VI.9) unless $\tilde{c}_1 = \tilde{c}_2$. □

Now we are ready to prove Theorem VI.6.6. In the proof, when $F \in \mathcal{F}$ acts on an n-bit vector $x \in \{0,1\}^n$, we prefer the notation $F(x)$ over matrix-product notation Fx.[9]

Proof of Theorem VI.6.6. Consider an execution of `Q-ID`, with a dishonest server S^* as described in Section VI.6. We let W, X and Z be the random variables that describe the values w, x and z occurring in the protocol.

From `Q-ID`'s description, we see that F is uniform over $\mathcal{F}$. Hence, by Corollary VI.6.8 it will be "good" (in the sense that the bound from Corollary VI.6.8 holds) except with probability $\binom{m}{2} 2^{2\ell} \exp(-2d\beta^2)$. From here, we consider a fixed choice for F and condition

[9] When using matrix-product notation ambiguities could arise, e.g. in subscripts of probability distributions like P_{FX}: then it is not clear whether this means the joint distribution of F and X or the distribution of F acting on X?

on the event that it is "good," we thus book-keep the probability that F is "bad" and take it into account at the end of the analysis. Although we have fixed F, we will keep using capital notation for it, to emphasize that F is a matrix. We also fix $G = g$ for an arbitrary g; the analysis below holds for any such choice.

Let Θ describe the qubit-wise measurement performed by S^* at the end of the execution, and Y the corresponding measurement outcome. By the non-adaptivity restriction and by the requirement in Definition VI.3.2 that S^* is initially independent of W, we may conclude that, once G and F are fixed, Θ is a function of Z. (Recall that $Z = F(X) \oplus g(W)$.)

We will define W' with the help of Corollary VI.6.8. Let $\hat{\Theta}$ be the quantized basis of Θ, as defined in Definition VI.6.3. Given a fixed value θ for Θ, and thus a fixed value $\hat{\theta}$ for $\hat{\Theta}$, we set s, which is a variable that occurs in Corollary VI.6.8, to $s = \hat{\theta}$. Corollary VI.6.8 now guarantees that there exists *at most one* $\tilde{c}$. If $\tilde{c}$ indeed exists, then we choose w' such that $\mathfrak{c}(w') = \tilde{c}$. Otherwise, we pick $w' \in \mathcal{W}$ arbitrarily (any choice will do). Note that this defines the random variable W', and furthermore note that $Z \to \Theta \to \hat{\Theta} \to W'$ forms a Markov chain. Moreover, by the choice of w' it immediately follows from Corollary VI.6.8 that for all $w \neq w'$ and for all $f \in \operatorname{span}(F) \setminus \{0^n\}$ it holds that

$$\left| f \odot (\mathfrak{c}(w) \oplus \hat{\theta}) \right| \geq \tfrac{1}{2}(\tfrac{1}{4} - \beta)d. \tag{VI.10}$$

We will make use of this bound later in the proof.

Since the model (Section VI.6) enforces the dishonest server to measure all qubits at the end of the protocol, the system $E = (Y, Z, \Theta)$ is classical and hence the trace-distance-based user-security definition (Definition VI.3.2) simplifies to a bound on the statistical distance between distributions. I.e., it is sufficient to prove that

$$\mathrm{SD}(P_{EW|W'=w',W'\neq W}, P_{W|W'=w',W\neq W'} P_{E|W'=w',W\neq W'}) \leq \varepsilon$$

holds for any w'. Consider the distribution that appears above as the first argument to the statistical distance, i.e. $P_{EW|W'=w',W'\neq W}$. By substituting $E = (Y, Z, \Theta)$, it factors as follows[10]

$$\begin{aligned} P_{YZ\Theta W|W',W\neq W'} &= P_{W|W',W\neq W'}\ P_{Z\Theta|WW',W\neq W'}\ P_{Y|Z\Theta WW',W\neq W'} \\ &= P_{W|W',W\neq W'}\ P_{Z\Theta|W',W\neq W'}\ P_{Y|F(X)\Theta WW',W\neq W'}, \end{aligned} \tag{VI.11}$$

where the equality $P_{Z\Theta|WW',W\neq W'} = P_{Z\Theta|W',W\neq W'}$ holds by the following argument: Z is independent of W (since $F(X)$ acts as one-time pad) and $Z \to \Theta \to W'$ is a Markov chain, and S^* (who computes Θ from Z) is initially independent of W by Definition VI.3.2, hence W is independent of Z, Θ and W', which implies the above equality. The equality

[10] Note that we shorten notation here by omitting the parentheses containing the function arguments. The quantification is over all inputs for which all involved conditional probabilities are well-defined.

$P_{Y|Z\Theta WW',W\neq W'} = P_{Y|F(X)\Theta WW',W\neq W'}$ holds by the observation that given W, Z is uniquely determined by $F(X)$ and vice versa.

In the remainder of this proof we will show that

$$d_{\text{unif}}(Y|F(X)=u,\Theta=v,W=w,W'=w') \leq \tfrac{1}{2}2^{\frac{\ell}{2}-\frac{1}{4}(\frac{1}{4}-\beta)d},$$

for all u,v,w such that $w \neq w'$, where w' is determined by v. This then implies that the rightmost factor in (VI.11) is essentially independent of W, and concludes the proof.

To simplify notation, we define $\mathcal{E}$ to be the event

$$\mathcal{E} := \{F(X)=u,\Theta=v,W=w,W'=w'\}$$

for fixed but arbitrary choices u, v and w such that $w \neq w'$, where w' is determined by v. We show closeness to the uniform distribution by using the XOR inequality from Diaconis *et al.* (Theorem VI.1.1), i.e., we use the inequality

$$d_{\text{unif}}(Y|\mathcal{E}) \leq \tfrac{1}{2}\Big[\sum_{\alpha} \text{bias}(\alpha\cdot Y|\mathcal{E})^2\Big]^{\frac{1}{2}},$$

where the sum is over all α in $\{0,1\}^n \setminus \{0^n\}$. We split this sum into two parts, one for $\alpha \in \text{span}(F)$ and one for α not in $\text{span}(F)$, and analyze the two parts separately.

Since X is uniformly distributed, it follows that for any $\alpha \notin \text{span}(F)$, it holds that $P_{\alpha\cdot X|F(X)}(\cdot|u) = \frac{1}{2}$ (for any u). We conclude that

$$\begin{aligned}\tfrac{1}{2} &= P_{\alpha\cdot X|F(X)} = P_{\alpha\cdot X|F(X)W} = P_{\alpha\cdot X|F(X)\Theta WW'}\\ &= P_{\alpha\cdot Y|F(X)\Theta WW'} = P_{\alpha\cdot Y|\mathcal{E}} \quad \forall\alpha\notin\text{span}(F).\end{aligned}$$

The second equality follows since W is independent of X. The third equality holds by the fact that Θ is computed from $F(X)\oplus g(W)$ and W' is determined by Θ. The fourth equality follows by the security of the one-time pad, i.e. recall that $Y = X\oplus\Delta$, where by Corollary VI.6.2 it holds that $\Delta\in\{0,1\}^n$ is independent of X when conditioned on fixed values for $B=\mathfrak{c}(W)$ and Θ. Hence, it follows that $\text{bias}(\alpha\cdot Y|\mathcal{E})=0$ for $\alpha\notin\text{span}(F)$.

For any non-zero $\alpha \in \operatorname{span}(F)$, we can write

$$\begin{aligned}
\operatorname{bias}(\alpha \cdot Y|\mathcal{E}) &= \operatorname{bias}(\alpha \cdot (X \oplus \Delta)|\mathcal{E}) \\
&= \operatorname{bias}(\alpha \cdot X \oplus \alpha \cdot \Delta|\mathcal{E}) && \text{(distributivity of dot product)} \\
&= \operatorname{bias}(\alpha \cdot X|\mathcal{E})\operatorname{bias}(\alpha \cdot \Delta|\mathcal{E}) && \text{(Corollary VI.6.2)} \\
&\leq \operatorname{bias}(\alpha \cdot \Delta|\mathcal{E}) && (\operatorname{bias}(\alpha \cdot X) \leq 1) \\
&= \prod_{i \in [n]} \operatorname{bias}(\alpha_i \cdot \Delta_i|\mathcal{E}) && (\Delta_i \text{ independent}) \\
&= \prod_{i \in [n]:\alpha_i = 1} \operatorname{bias}(\Delta_i|\mathcal{E}) \\
&\leq \prod_{\substack{i \in [n]:\alpha_i = 1 \\ \hat{\theta}_i = \mathfrak{c}(w)_i \oplus 1}} 2^{-\frac{1}{2}} && \text{(Theorem VI.6.4)} \\
&= 2^{-\frac{1}{2}|\alpha \odot (\mathfrak{c}(w) \oplus \hat{\theta})|} \leq 2^{-\frac{1}{4}(\frac{1}{4}-\beta)d} && \text{(by (VI.10))}
\end{aligned}$$

Combining the two parts, we get

$$\begin{aligned}
d_{\text{unif}}(Y|\mathcal{E}) &\leq \tfrac{1}{2}\Big[\sum_{\alpha} \operatorname{bias}(\alpha \cdot Y|\mathcal{E})^2\Big]^{\frac{1}{2}} \\
&= \tfrac{1}{2}\Big[\sum_{\alpha \in \operatorname{span}(F)\setminus\{0^n\}} \operatorname{bias}(\alpha \cdot Y|\mathcal{E})^2 + 0\Big]^{\frac{1}{2}} \leq \tfrac{1}{2} 2^{\frac{\ell}{2} - \frac{1}{4}(\frac{1}{4}-\beta)d}\,.
\end{aligned}$$

Incorporating the error probability of having a "bad" F completes the proof. □

VI.6.4 Attack against Q-ID with Operations on Pairs of Qubits

We present an attack with which the dishonest server S^* can discard two passwords in one execution of Q-ID using coherent operations on pairs of qubits.

Before discussing this attack, we first explain a straightforward strategy by which S^* can discard one password per execution: S^* chooses a candidate password $\hat{w}$ and measures the state $H^{\mathfrak{c}(W)}|X\rangle$ qubit-wise in the basis $\mathfrak{c}(\hat{w})$ to obtain Y. S^* then computes $F(Y) \oplus g(\hat{w})$ and compares this to $Z = F(X) \oplus g(W)$, which he received from the user. If indeed $Z = F(Y) \oplus g(\hat{w})$, then it is very likely that $W = \hat{w}$, i.e. that S^* guessed the password correctly.

Let us now explain the attack, which is obtained by modifying the above strategy. The attack is based on the following observation [34]: if S^* can perform Bell measurements on qubit pairs $|x_1\rangle_a|x_2\rangle_a$, for $a \in \{0,1\}$, then he can learn the parity of $x_1 \oplus x_2$ for both choices of a simultaneously. This strategy can also be adapted to determine both parities

of a pair in which the first qubit is encoded in a basis that is opposite to that of the second qubit, i.e. by appropriately applying a Hadamard gate prior to applying the Bell measurement.

Let the first bit of Z be equal to $f \cdot X \oplus g(W)_1$,[11] where $f \in \mathrm{span}(F) \setminus \{0^n\}$. Let $\hat{w}_1$ and $\hat{w}_2$ be two candidate passwords. With the trick from above, S^* can measure the positions in the set

$$\mathcal{P} := \{i \in [n] : f_i = 1, \mathfrak{c}(\hat{w}_1)_i = 1 \oplus \mathfrak{c}(\hat{w}_2)_i\}$$

pairwise (assuming $|\mathcal{P}|$ to be even) using Bell measurements, while measuring the positions where $\mathfrak{c}(\hat{w}_1)$ and $\mathfrak{c}(\hat{w}_2)$ coincide using ordinary single-qubit measurements. This allows him to compute both "check bits" corresponding to both passwords *simultaneously*, i.e. those check bits coincide with $f \cdot Y_1 \oplus g(\hat{w}_1)_1$ and $f \cdot Y_2 \oplus g(\hat{w}_2)_1$, where Y_1 and Y_2 are the outcomes that S^* would have obtained if he had measured all qubits qubit-wise in either $\mathfrak{c}(\hat{w}_1)$ or $\mathfrak{c}(\hat{w}_2)$, respectively. If both these check bits are different from the bit Z_1, then S^* can discard both w_1 and w_2.

We have seen that in the *worst case*, the attack is capable of discarding two passwords in one execution, and hence clearly violates the security definition. On *average*, however, the attack seems to discard just one password per execution, i.e. a candidate password cannot be discarded if its check bit is consistent with Z_1, which essentially happens with probability 1/2. This raises the question whether the security definition is unnecessarily strong, because it seems that not being able to discard more than one password on average would be sufficient. Apart from this, it might be possible to improve the attack, e.g. by selecting the positions where to measure pairwise in a more clever way, as to obtain multiple check bits (corresponding to multiple fs in the span of F) per candidate password, thereby increasing the probability of discarding a wrong candidate password.

VI.7 Discussion

In this chapter we have proven a sharp entropic uncertainty inequality that uses the min-entropy as entropy measure and gives uncertainty of the measurement outcome for all but one measurements, in contrast to average uncertainty of previous uncertainty inequalities on the min-entropy. As application, we propose a `Q-ID` protocol and our new uncertainty relation forms the core of the new protocols security proof in the BQSM. This protocol also offers some security in case the bounded quantum storage assumption fails to hold. Specifically, it remains secure in the SQOM, i.e., against an adversary that has unbounded storage capabilities but is restricted to nonadaptive single-qubit operations.

We view our work related to `Q-ID` as a first step in a promising line of research, aimed at achieving security in multiple models simultaneously. We want to stress that

[11] By $g(W)_1$ we mean the first bit of $g(W)$.

proving security of our protocol in the SQOM is non-trivial, as standard tools like privacy amplification are not applicable. The main open problem in the context of the SQOM is to reprove our results in a more general model in which the dishonest server S^* can choose his basis adaptively.

We hope that with future research on this topic, new quantum identification (or other cryptographic) protocols will be developed with security in the same spirit as our protocol, but with a more relaxed restriction on the adversary's quantum computation capabilities, for instance that he can only perform a limited number of quantum computation steps, and in every step he can only act on a limited number of qubits coherently.

Bibliography

[1] Affleck, I., Kennedy, T., Lieb, E. H., and Tasaki, H. Rigorous results on valence-bond ground states in antiferromagnets. *Phys. Rev. Lett. 59* (1987), 799–802.

[2] Anfuso, F., and Rosch, A. Fragility of string orders. *Physical Review B 76*, 8 (2007), 085124.

[3] Aulbach, M., Markham, D., and Murao, M. The maximally entangled symmetric state in terms of the geometric measure. *New Journal of Physics 12*, 7 (2010), 073025.

[4] Bañuls, M. C., Cirac, J. I., and Hastings, M. B. Strong and weak thermalization of infinite nonintegrable quantum systems. *Phys. Rev. Lett. 106* (2011), 050405.

[5] Banach, S. Über n-lineare symmetrische formen. *Ann. Polon. Math. 12*, 116 (1933).

[6] Barak, B., Brandao, F. G., Harrow, A. W., Kelner, J., Steurer, D., and Zhou, Y. Hypercontractivity, sum-of-squares proofs, and their applications. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (2012), IEEE, pp. 307–326.

[7] Beckner, W. Inequalities in Fourier analysis. *Ann. of Math. (2) 102*, 1 (1975), 159–182.

[8] Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., and Smith, A. Secure multiparty quantum computation with (only) a strict honest majority. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (2006), IEEE, pp. 249–260.

[9] Bennett, C. H., and Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the 16th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (1984), IEEE, pp. 175–179.

[10] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W. K. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett. 70* (1993), 1895–1899.

[11] Bouman, N., Fehr, S., González-Guillén, C., and Schaffner, C. An all-but-one entropic uncertainty relation, and application to password-based identification. In *Theory of Quantum Computation, Communication, and Cryptography* (2013), K. Iwama, Y. Kawano, and M. Murao, Eds., vol. 7582 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, pp. 29–44.

[12] Brandão, F. G. S. L., Ćwikliński, P., Horodecki, M., Horodecki, P., Korbicz, J. K., and Mozrzymas, M. Convergence to equilibrium under a random hamiltonian. *Phys. Rev. E 86* (2012), 031101.

[13] Braunstein, S. L., D'Ariano, G. M., Milburn, G. J., and Sacchi, M. F. Universal teleportation with a twist. *Phys. Rev. Lett. 84* (2000), 3486–3489.

[14] Bremner, M. J., Mora, C., and Winter, A. Are random pure states useful for quantum computation? *Physical Review Letters 102*, 19 (2009), 190502.

[15] Briët, J., and Vidick, T. Explicit lower and upper bounds on the entangled value of multiplayer xor games. *Communications in Mathematical Physics 321*, 1 (2013), 181–207.

[16] Buerschaper, O., Aguado, M., and Vidal, G. Explicit tensor network representation for the ground states of string-net models. *Physical Review B 79*, 8 (2009), 085119.

[17] Calabrese, P., and Cardy, J. Entanglement entropy and quantum field theory. *Journal of Statistical Mechanics: Theory and Experiment 2004*, 6 (2004), 06002.

[18] Carathéodory, C. Über den variabilitätsbereich der fourier'schen konstanten von positiven harmonischen funktionen. *Rendiconti del Circolo Matematico di Palermo 32* (1911), 193–217.

[19] Chen, X., Gu, Z.-C., Liu, Z.-X., and Wen, X.-G. Symmetry-protected topological orders in interacting bosonic systems. *Science 338*, 6114 (2012), 1604–1606.

[20] Chen, X., Gu, Z.-C., and Wen, X.-G. Classification of gapped symmetric phases in one-dimensional spin systems. *Phys. Rev. B 83* (Jan 2011), 035107.

[21] Chitambar, E., Leung, D., Manĉinska, L., Ozols, M., and Winter, A. Everything you always wanted to know about locc (but were afraid to ask). *Communications in Mathematical Physics* (2014), 1–24.

[22] Collins, B. Moments and cumulants of polynomial random variables on unitarygroups, the itzykson-zuber integral, and free probability. *International Mathematics Research Notices 2003*, 17 (2003), 953–982.

[23] Collins, B., González-Guillén, C. E., and Pérez-García, D. Matrix product states, random matrix theory and the principle of maximum entropy. *Communications in Mathematical Physics 320*, 3 (2013), 663–677.

[24] Collins, B., and Nechita, I. Random quantum channels i: Graphical calculus and the bell state phenomenon. *Communications in Mathematical Physics 297*, 2 (2010), 345–370.

[25] Collins, B., and Śniady, P. Integration with respect to the haar measure on unitary, orthogonal and symplectic group. *Communications in Mathematical Physics 264* (2006), 773–795.

[26] Corboz, P., Läuchli, A. M., Penc, K., Troyer, M., and Mila, F. Simultaneous dimerization and su(4) symmetry breaking of 4-color fermions on the square lattice. *Phys. Rev. Lett. 107* (2011), 215301.

[27] Corboz, P., White, S. R., Vidal, G., and Troyer, M. Stripes in the two-dimensional model with infinite projected entangled-pair states. *Phys. Rev. B 84* (2011), 041108.

[28] Cramer, M. Thermalization under randomized local hamiltonians. *New Journal of Physics 14*, 5 (2012), 053051.

[29] Cramer, M., Flesch, A., McCulloch, I. P., Schollwöck, U., and Eisert, J. Exploring local quantum many-body relaxation by atoms in optical superlattices. *Phys. Rev. Lett. 101* (2008), 063001.

[30] Crépeau, C., Gottesman, D., and Smith, A. Secure multi-party quantum computation. In *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (2002), IEEE, pp. 643–652.

[31] Cubitt, T. S., Verstraete, F., Dür, W., and Cirac, J. I. Separable states can be used to distribute entanglement. *Phys. Rev. Lett. 91* (2003), 037902.

[32] Damgård, I., Fehr, S., Lunemann, C., Salvail, L., and Schaffner, C. Improving the security of quantum protocols via commit-and-open. In *Advances in Cryptology - CRYPTO '09* (2009), vol. 2577 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 408–427.

[33] Damgård, I., Fehr, S., Renner, R., Salvail, L., and Schaffner, C. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology - CRYPTO '07* (2007), vol. 4622 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 360–378.

[34] Damgård, I., Fehr, S., Salvail, L., and Schaffner, C. Cryptography in the bounded quantum-storage model. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (2005), IEEE, pp. 449–458. Also in *SIAM Journal on Computing*, 37(6):1865-1890, 2008.

[35] Damgård, I., Fehr, S., Salvail, L., and Schaffner, C. Secure identification and QKD in the bounded-quantum-storage model. In *Advances in Cryptology - CRYPTO '07* (2007), vol. 4622 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 342–359.

[36] de Vicente, J. I., Spee, C., and Kraus, B. Maximally entangled set of multipartite quantum states. *Phys. Rev. Lett. 111* (2013), 110502.

[37] Defant, A., and Floret, K. *Tensor norms and operator ideals*, vol. 176 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam, 1993.

[38] Delgado, Y., Lamata, L., León, J., Salgado, D., and Solano, E. Sequential quantum cloning. *Phys. Rev. Lett. 98* (2007), 150502.

[39] Diaconis, P. *Group Representations in Probability and Statistics*, vol. 11 of *Lecture Notes — Monograph series*. Institute of Mathematical Statistics, Hayward, CA, 1988.

[40] Dineen, S. *Complex analysis on infinite-dimensional spaces*. Springer Monographs in Mathematics. Springer-Verlag London Ltd., London, 1999.

[41] DiVincenzo, D. P., Horodecki, M., Leung, D. W., Smolin, J. A., and Terhal, B. M. Locking classical correlations in quantum states. *Phys. Rev. Lett. 92* (2004), 067902.

[42] Dür, W., Vidal, G., and Cirac, J. I. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A 62* (2000), 062314.

[43] Einstein, A., Podolsky, B., and Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev. 47* (1935), 777–780.

[44] Ekert, A. K. Quantum cryptography based on bell's theorem. *Physical Review Letter 67*, 6 (1991), 661–663.

[45] Evenbly, G., and Vidal, G. Quantum criticality with the multi-scale entanglement renormalization ansatz. In *Strongly Correlated Systems, Numerical Methods*, A. Avella and F. Mancini, Eds., vol. 176 of *Springer Series in Solid-State Sciences*. Springer Berlin Heidelberg, 2013, pp. 99–130.

[46] Fannes, M., Nachtergaele, B., and Werner, R. F. Finitely correlated states on quantum spin chains. *Comm. Math. Phys. 144*, 3 (1992), 443–490.

[47] Fawzi, O., Hayden, P., and Sen, P. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. *J. ACM 60*, 6 (2013), 1–44.

[48] Fehr, S., and Schaffner, C. Composing quantum protocols in a classical environment. In *Theory of Cryptography Conference - TCC 09* (2009), vol. 5444 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 350–367.

[49] Fidkowski, L., and Kitaev, A. Topological phases of fermions in one dimension. *Phys. Rev. B 83* (2011), 075103.

[50] Flesch, A., Cramer, M., McCulloch, I. P., Schollwöck, U., and Eisert, J. Probing local relaxation of cold atoms in optical superlattices. *Phys. Rev. A 78* (2008), 033608.

[51] Fulton, W. *Young tableaux: With applications to representation theory and geometry*, vol. 35 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1997.

[52] Garnerone, S., de Oliveira, T. R., Haas, S., and Zanardi, P. Statistical properties of random matrix product states. *Physical Review A 82*, 5 (2010).

[53] Garnerone, S., de Oliveira, T. R., and Zanardi, P. Typicality in random matrix product states. *Physical Review A 81*, 3 (2010).

[54] Gawron, P., Puchala, Z., Miszczak, J. A., Skowronek, L., and Zyczkowski, K. Restricted numerical range: A versatile tool in the theory of quantum information. *Journal of Mathematical Physics 51*, 10 (2010), 102204.

[55] Goldstein, S., Lebowitz, J. L., Tumulka, R., and Zanghì, N. Canonical typicality. *Phys. Rev. Lett. 96* (2006), 050403.

[56] Goldstein, S., Lebowitz, J. L., Tumulka, R., and Zanghì, N. Long-time behavior of macroscopic quantum systems. *The European Physical Journal H 35* (2010), 173–200.

[57] González-Guillén, C. E. Multipartite maximally entangled states in symmetric scenarios. *Phys. Rev. A 86* (2012), 022304.

[58] Gross, D., and Eisert, J. Novel schemes for measurement-based quantum computation. *Physical Review Letters 98*, 22 (2007), 220503.

[59] Gross, D., Eisert, J., Schuch, N., and Perez-Garcia, D. Measurement-based quantum computation beyond the one-way model. *Physical Review A 76*, 5 (2007), 052315.

[60] Gross, D., Flammia, S. T., and Eisert, J. Most quantum states are too entangled to be useful as computational resources. *Physical Review Letters 102*, 19 (2009), 190501.

[61] Grothendieck, A. Résumé de la théorie métrique des produits tensoriels topologiques. *Bol. Soc. Mat. São Paulo 8* (1953), 1–79.

[62] Gühne, O. Characterizing entanglement via uncertainty relations. *Phys. Rev. Lett. 92* (Mar 2004), 117903.

[63] Gühne, O., Bodoky, F., and Blaauboer, M. Multiparticle entanglement under the influence of decoherence. *Physical Review A 78*, 6 (2008), 060301.

[64] Gühne, O., and Tóth, G. *Entanglement Detection.* Elsevier, 2009.

[65] Haegeman, J., Cirac, J. I., Osborne, T. J., Pižorn, I., Verschelde, H., and Verstraete, F. Time-dependent variational principle for quantum lattices. *Phys. Rev. Lett. 107* (2011), 070601.

[66] Harrow, A. W., and Montanaro, A. An efficient test for product states with applications to quantum merlin-arthur games. In *Proceedings of the 51st IEEE Annual Symposium on Foundations of Computer Science (FOCS)* (2010), IEEE, pp. 633–642.

[67] Hastings, M. B. Lieb-schultz-mattis in higher dimensions. *Physical Review B 69*, 10 (2004), 104431.

[68] Hastings, M. B. Solving gapped hamiltonians locally. *Phys. Rev. B 73* (2006), 085115.

[69] Hastings, M. B. An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment 2007*, 08 (2007), 08024.

[70] Hastings, M. B. Entropy and entanglement in quantum ground states. *Physical Review B 76*, 3 (2007).

[71] Hastings, M. B. Random unitaries give quantum expanders. *Phys. Rev. A 76* (2007), 032315.

[72] Hayashi, M., Markham, D., Murao, M., Owari, M., and Virmani, S. Bounds on multipartite entangled orthogonal state discrimination using local operations and classical communication. *Physical Review Letters 96*, 4 (2006), 040501.

[73] Hayashi, M., Markham, D., Murao, M., Owari, M., and Virmani, S. Entanglement of multiparty-stabilizer, symmetric, and antisymmetric states. *Physical Review A 77*, 1 (2008), 012104.

[74] Hayashi, M., Markham, D., Murao, M., Owari, M., and Virmani, S. The geometric measure of entanglement for a symmetric pure state with non-negative amplitudes. *Journal of Mathematical Physics 50*, 12 (2009), 122104.

[75] Hayden, P., Leung, D. W., and Winter, A. Aspects of generic entanglement. *Commun. Math. Phys. 265*, 1 (2006), 95–117.

[76] He, S., Li, Z., and Zhang, S. Approximation algorithms for homogeneous polynomial optimization with quadratic constraints. *Mathematical Programming 125*, 2 (2010), 353–383.

[77] Hein, M., Dür, W., Eisert, J., Raussendorf, R., Van den N est, M., and Briegel, H.-J. Entanglement in graph states and its applications. In *Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos"* (2006), pp. 115–218.

[78] Heisenberg, W. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik 43*, 3-4 (1927), 172–198.

[79] Helwig, W., Cui, W., Latorre, J. I., Riera, A., and Lo, H.-K. Absolute maximal entanglement and quantum secret sharing. *Phys. Rev. A 86* (2012), 052335.

[80] Hirschman, I. I., J. A note on entropy. *American Journal of Mathematics 79*, 1 (1957), 152–156.

[81] Hoeffding, W. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association 58*, 301 (1963), 13–30.

[82] Hörmander, L. On a theorem of grace. *Math. Scand. 2* (1954), 55–64.

[83] Horn, R. A., and Johnson, C. R. *Topics in matrix analysis.* Cambridge University Press, Cambridge, 1994. Corrected reprint of the 1991 original.

[84] Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K. Quantum entanglement. *Rev. Mod. Phys. 81* (2009), 865–942.

[85] Hübener, R., Kleinmann, M., Wei, T.-C., González-Guillén, C., and Gühne, O. Geometric measure of entanglement for symmetric states. *Phys. Rev. A 80* (2009), 032324.

[86] Jaynes, E. Prior probabilities. *IEEE Transactions on Systems Science and Cybernetics 4*, 3 (1968), 227 –241.

[87] Jaynes, E. T. Information theory and statistical mechanics. *Physical Review 106*, 4 (1957).

[88] Jaynes, E. T. Information theory and statistical mechanics ii. *Physical Review 108*, 2 (1957).

[89] Jaynes, E. T. Where do we stand on maximum entropy? In *Maximum entropy formalism (Conf., Mass. Inst. Tech., Cambridge, Mass., 1978).* MIT Press, Cambridge, Mass., 1979, pp. 15–118.

[90] Jung, E., Hwang, M.-R., Kim, H., Kim, M.-S., Park, D., Son, J.-W., and Tamaryan, S. Reduced state uniquely defines the groverian measure of the original pure state. *Phys. Rev. A 77* (2008), 062317.

[91] Kellogg, O. D. On bounded polynomials in several variables. *Math. Z. 27*, 55 (1928).

[92] Kitaev, A. Anyons in an exactly solved model and beyond. *Annals of Physics 321*, 1 (2006), 2 – 111.

[93] Kitaev, A., and Preskill, J. Topological entanglement entropy. *Phys. Rev. Lett. 96* (2006), 110404.

[94] Kitaev, A. Y. Fault-tolerant quantum computation by anyons. *Annals of Physics 303*, 1 (2003), 2–30.

[95] Kittaneh, F. Norm inequalities for certain operator sums. *Journal of Functional Analysis 143*, 2 (1997), 337 – 348.

[96] Koashi, M. Unconditional security of quantum key distribution and the uncertainty principle. *Journal of Physics: Conference Series 36*, 1 (2006), 98.

[97] Konig, R., and Renner, R. A de finetti representation for finite symmetric quantum states. *Journal of Mathematical Physics 46*, 12 (2005), 122108.

[98] Konig, R., Renner, R., and Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory 55*, 9 (2009), 4337–4347.

[99] Kruszynska, C., and Kraus, B. Local entanglability and multipartite entanglement. *Phys. Rev. A 79* (2009), 052304.

[100] Lamata, L., León, J., Pérez-García, D., Salgado, D., and Solano, E. Sequential implementation of global quantum operations. *Phys. Rev. Lett. 101* (2008), 180506.

[101] Landau, L. D., and Lifshitz, E. M. *Course of theoretical physics. Vol. 5: Statistical physics.* Translated from the Russian by J. B. Sykes and M. J. Kearsley. Second revised and enlarged edition. Pergamon Press, Oxford, 1968.

[102] Ledoux, M. *The concentration of measure phenomenon*, vol. 89 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2001.

[103] Legeza, O., and Sólyom, J. Quantum data compression, quantum information generation, and the density-matrix renormalization-group method. *Phys. Rev. B 70* (2004), 205118.

[104] Lieb, E., Schultz, T., and Mattis, D. Two soluble models of an antiferromagnetic chain. *Annals of Physics 16*, 3 (1961), 407–466.

[105] Linden, N., Popescu, S., Short, A. J., and Winter, A. Quantum mechanical evolution towards thermal equilibrium. *Phys. Rev. E 79* (2009), 061103.

[106] Linden, N., Popescu, S., Short, A. J., and Winter, A. On the speed of fluctuations around thermodynamic equilibrium. *New Journal of Physics 12*, 5 (2010), 055021.

[107] Lo, H.-K. Insecurity of quantum secure computations. *Phys. Rev. A 56* (1997), 1154–1162.

[108] Lohmayer, R., Osterloh, A., Siewert, J., and Uhlmann, A. Entangled three-qubit states without concurrence and three-tangle. *Physical Review Letters 97*, 26 (2006), 260502.

[109] Maassen, H., and Uffink, J. B. M. Generalized entropic uncertainty relations. *Physical Review Letters 60*, 12 (1988).

[110] Maeshima, N., Hieida, Y., Akutsu, Y., Nishino, T., and Okunishi, K. Vertical density matrix algorithm: A higher-dimensional numerical renormalization scheme based on the tensor product state ansatz. *Physical Review E 64*, 1 (2001), 016705–.

[111] Majumdar, C. K., and Ghosh, D. K. On next-nearest-neighbor interaction in linear chain. I, II. *J. Mathematical Phys. 10* (1969), 1399–1402.

[112] Markham, D., Miyake, A., and Virmani, S. Entanglement and local information access for graph states. *New Journal of Physics 9*, 6 (2007).

[113] Martin, J., Giraud, O., Braun, P. A., Braun, D., and Bastin, T. Multiqubit symmetric states with high geometric entanglement. *Phys. Rev. A 81* (2010), 062347.

[114] Masanes, L., Roncaglia, A. J., and Acín, A. Complexity of energy eigenstates as a mechanism for equilibration. *Phys. Rev. E 87* (2013), 032137.

[115] Michalakis, S., and Zwolak, J. Stability of frustration-free hamiltonians. *Communications in Mathematical Physics 322*, 2 (2013), 277–302.

[116] Milman, V., and Schechtman, G. *Asymptotic theory of finite dimensional normed spaces.* Lecture notes in mathematics. Springer, 1986.

[117] Montanaro, A. Weak multiplicativity for random quantum channels. *Communications in Mathematical Physics 319*, 2 (2013), 535–555.

[118] Nachtergaele, B., and Sims, R. A multi-dimensional lieb-schultz-mattis theorem. *Communications in Mathematical Physics 276* (2007), 437–472.

[119] Nakata, Y., Markham, D., and Murao, M. Thermal robustness of multipartite entanglement of the one-dimensional spin-1/2 xy model. *Physical Review A 79*, 4 (2009), 042313.

[120] Naor, J., and Naor, M. Small-bias probability spaces: Efficient constructions and applications. *SIAM J. Comput 22* (1993), 838–856.

[121] Nielsen, M., and Chuang, I. *Quantum Computation and Quantum Information.* Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

[122] Nielsen, M. A. Conditions for a class of entanglement transformations. *Phys. Rev. Lett. 83* (1999), 436–439.

[123] Nishino, Y., Maeshima, N., Gendiar, A., and Nishino, T. Tensor product variational formulation for quantum systems. `http://arXiv:cond-mat/0401115v1`, 2004.

[124] Orús, R. Universal geometric entanglement close to quantum phase transitions. *Physical Review Letters 100*, 13 (2008), 130502.

[125] Orus, R. A practical introduction to tensor networks: Matrix product states and projected entangled pair states. `arXiv:1306.2164v2`, 2013.

[126] Orús, R., Dusuel, S., and Vidal, J. Equivalence of critical scaling laws for many-body entanglement in the lipkin-meshkov-glick model. *Physical Review Letters 101*, 2 (2008), 025701.

[127] Orus, R., Wei, T.-C., Buerschaper, O., and Van den Nest, M. Topological Order from Geometric Entanglement. arxiv:1304.1339, 2013.

[128] Oshikawa, M., Yamanaka, M., and Affleck, I. Magnetization plateaus in spin chains: "haldane gap" for half-integer spins. *Physical Review Letters 78*, 10 (1997), 1984–1987.

[129] Paulsen, V. *Completely Bounded Maps and Operator Algebras.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2002.

[130] Pérez-García, D., Sanz, M., González-Guillén, C. E., Wolf, M. M., and Cirac, J. I. Characterizing symmetries in a projected entangled pair state. *New Journal of Physics 12*, 2 (2010), 025010.

[131] Pérez-García, D., Verstraete, F., Wolf, M. M., and Cirac, J. I. Matrix product state representations. *Quantum Information & Computation 7*, 5 (2007), 401–430.

[132] Pérez-García, D., Verstraete, F., Wolf, M. M., and Cirac, J. I. Peps as unique ground states of local hamiltonians. *Quantum Information & Computation 8*, 6 (2008), 650–663.

[133] Pérez-García, D., Wolf, M., Palazuelos, C., Villanueva, I., and Junge, M. Unbounded violation of tripartite bell inequalities. *Communications in Mathematical Physics 279* (2008), 455–486.

[134] Pérez-García, D., Wolf, M. M., Sanz, M., Verstraete, F., and Cirac, J. I. String order and symmetries in quantum spin lattices. *Physical Review Letters 100*, 16 (2008), 167202.

[135] Plenio, M. B., Eisert, J., Dreissig, J., and Cramer, M. Entropy, entanglement, and area: Analytical results for harmonic lattice systems. *Phys. Rev. Lett. 94* (Feb 2005), 060503.

[136] Plenio, M. B., and Virmani, S. An introduction to entanglement measures. *Quantum Info. Comput. 7* (2007), 1–51.

[137] Pollmann, F., Turner, A. M., Berg, E., and Oshikawa, M. Entanglement spectrum of a topological phase in one dimension. *Phys. Rev. B 81* (2010), 064439.

[138] Pólya, G. Kombinatorische anzahlbestimmungen für gruppen, graphen, und chemische verbindungen. *Acta Math. 68*, 145 (1937).

[139] Popescu, S., Short, A. J., and Winter, A. Entanglement and the foundations of statistical mechanics. *Nat Phys 2*, 11 (2006), 754–758.

[140] Popp, M., Verstraete, F., Martín-Delgado, M. A., and Cirac, J. I. Localizable entanglement. *Phys. Rev. A 71* (2005), 042306.

[141] Poulin, D., Qarry, A., Somma, R., and Verstraete, F. Quantum simulation of time-dependent hamiltonians and the convenient illusion of hilbert space. *Phys. Rev. Lett. 106* (2011), 170501.

[142] Preskill, J. Lecture notes for physics 229: Quantum information and computation. `www.theory.caltech.edu/people/preskill/ph229/notes/book.ps`, 1998.

[143] Raussendorf, R., and Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett. 86* (2001), 5188–5191.

[144] Reimann, P. Typicality for generalized microcanonical ensembles. *Phys. Rev. Lett. 99* (2007), 160404.

[145] Renner, R. *Security of Quantum Key Distribution.* PhD thesis, ETH Zürich (Switzerland), 2005. `http://arxiv.org/abs/quant-ph/0512258`.

[146] Renner, R., and König, R. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference (TCC)* (2005), vol. 3378 of *Lecture Notes in Computer Science*, Springer, pp. 407–425.

[147] Rényi, A. On measures of entropy and information. In *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability* (1961), vol. 1, pp. 547–561.

[148] Rico, E., and Briegel, H. J. 2d multipartite valence bond states in quantum antiferromagnets. *Annals of Physics 323*, 9 (2008), 2115–2131.

[149] Roy, A., and Scott, A. Unitary designs and codes. *Designs, Codes and Cryptography 53* (2009), 13–31.

[150] Rungta, P., and Caves, C. M. Concurrence-based entanglement measures for isotropic states. *Physical Review A 67*, 1 (2003), 012307.

[151] Sanz, M., Wolf, M. M., Pérez-García, D., and Cirac, J. I. Matrix product states: Symmetries and two-body hamiltonians. *Physical Review A 79*, 4 (2009), 042308–.

[152] Scarani, V., Iblisdir, S., Gisin, N., and Acín, A. Quantum cloning. *Rev. Mod. Phys. 77* (2005), 1225–1256.

[153] Schaffner, C. *Cryptography in the Bounded-Quantum Storage Model.* PhD thesis, University of Aarhus (Denmark), September 2007. `http://arxiv.org/abs/0709.0289`.

[154] Schollwöck, U. The density-matrix renormalization group. *Rev. Mod. Phys. 77* (2005), 259–315.

[155] Schuch, N., Pérez-García, D., and Cirac, I. Classifying quantum phases using matrix product states and projected entangled pair states. *Phys. Rev. B 84* (2011), 165139.

[156] Schuch, N., Wolf, M. M., Verstraete, F., and Cirac, J. I. Computational complexity of projected entangled pair states. *Physical Review Letters 98*, 14 (2007), 140506.

[157] Schuch, N., Wolf, M. M., Verstraete, F., and Cirac, J. I. Entropy scaling and simulability by matrix product states. *Phys. Rev. Lett. 100* (2008), 030504.

[158] Shannon, C. E. A mathematical theory of communication. *Bell System Technical Journal 27*, 3 (1948), 379–423.

[159] Shor, P. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS)* (1994), IEEE, pp. 124–134.

[160] Srednicki, M. Entropy and area. *Phys. Rev. Lett. 71* (1993), 666–669.

[161] Takagi, T. On an algebraic problem related to an analytical theorem of caratheodory and fejer and on an allied theorem of landau. *Jpn. J. Math. 1*, 83 (1927).

[162] Tamaryan, L., Park, D., and Tamaryan, S. Analytic expressions for geometric measure of three-qubit states. *Physical Review A 77*, 2 (2008), 022325–.

[163] Tamaryan, S., Wei, T.-C., and Park, D. Maximally entangled three-qubit states via geometric measure of entanglement. *Physical Review A 80*, 5 (2009), 052315.

[164] Terhal, B. M., and Vollbrecht, K. G. H. Entanglement of formation for isotropic states. *Physical Review Letters 85*, 12 (2000), 2625–2628.

[165] Tóth, G., and Gühne, O. Entanglement and permutational symmetry. *Phys. Rev. Lett. 102*, 17 (2009), 170503, 4.

[166] Trotzky, S., Chen, Y.-A., Flesch, A., McCulloch, I. P., Schollwock, U., Eisert, J., and Bloch, I. Probing the relaxation towards equilibrium in an isolated strongly correlated one-dimensional bose gas. *Nat Phys 8*, 4 (2012), 325–330.

[167] Turner, A. M., Pollmann, F., and Berg, E. Topological phases of one-dimensional fermions: An entanglement point of view. *Phys. Rev. B 83* (2011), 075102.

[168] Verstraete, F., and Cirac, J. I. Renormalization algorithms for quantum-many body systems in two and higher dimensions. `http://arXiv:cond-mat/0407066v1`, 2004.

[169] Verstraete, F., and Cirac, J. I. Matrix product states represent ground states faithfully. *Physical Review B 73*, 9 (2006), 094423.

[170] Verstraete, F., Murg, V., and Cirac, J. I. Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems. *Advances in Physics 57*, 2 (2008), 143–224.

[171] Verstraete, F., Porras, D., and Cirac, J. I. Density matrix renormalization group and periodic boundary conditions: A quantum information perspective. *Phys. Rev. Lett. 93* (2004), 227205.

[172] Verstraete, F., Wolf, M. M., and Ignacio Cirac, J. Quantum computation and quantum-state engineering driven by dissipation. *Nat Phys 5*, 9 (2009), 633–636.

[173] Verstraete, F., Wolf, M. M., Perez-Garcia, D., and Cirac, J. I. Criticality, the area law, and the computational power of projected entangled pair states. *Physical Review Letters 96*, 22 (2006), 220601.

[174] Vidal, G. Entanglement of pure states for a single copy. *Phys. Rev. Lett. 83* (1999), 1046–1049.

[175] Vidal, G. Efficient classical simulation of slightly entangled quantum computations. *Physical Review Letters 91*, 14 (2003), 147902.

[176] Vidal, G. Classical simulation of infinite-size quantum lattice systems in one spatial dimension. *Phys. Rev. Lett. 98* (2007), 070201.

[177] Vidal, G., Latorre, J. I., Rico, E., and Kitaev, A. Entanglement in quantum critical phenomena. *Phys. Rev. Lett. 90* (2003), 227902.

[178] Vinayak, and Žnidarič, M. Subsystem dynamics under random hamiltonian evolution. *Journal of Physics A: Mathematical and Theoretical 45*, 12 (2012), 125204.

[179] Wehner, S., Schaffner, C., and Terhal, B. M. Cryptography from noisy storage. *Phys. Rev. Lett. 100* (2008), 220502.

[180] Wehner, S., and Winter, A. Entropic uncertainty relations—a survey. *New Journal of Physics 12*, 2 (2010).

[181] Wei, T.-C. Phd-thesis. `http://arXiv:/0905.2467`, 2004.

[182] Wei, T.-C. Relative entropy of entanglement for multipartite mixed states: Permutation-invariant states and dür states. *Physical Review A 78*, 1 (2008), 012327.

[183] Wei, T.-C. Entanglement under the renormalization-group transformations on quantum states and in quantum phase transitions. *Phys. Rev. A 81* (2010), 062313.

[184] Wei, T.-C., Das, D., Mukhopadyay, S., Vishveshwara, S., and Goldbart, P. M. Global entanglement and quantum criticality in spin chains. *Physical Review A 71*, 6 (2005), 060305.

[185] Wei, T.-C., and Goldbart, P. M. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Phys. Rev. A 68* (2003), 042307.

[186] Wei, T.-C., and Severini, S. Matrix permanent and quantum entanglement of permutation invariant states. *Journal of Mathematical Physics 51*, 9 (2010), 092203.

[187] Wen, X. G. Topological orders in rigid states. *International Journal of Modern Physics B 04*, 02 (1990), 239–271.

[188] Werner, R. F., and Holevo, A. S. Counterexample to an additivity conjecture for output purity of quantum channels. *J. Math. Phys. 43*, 9 (2002), 4353–4357.

[189] White, S. R. Density matrix formulation for quantum renormalization groups. *Phys. Rev. Lett. 69* (1992), 2863–2866.

[190] White, S. R. Density-matrix algorithms for quantum renormalization groups. *Phys. Rev. B 48* (1993), 10345–10356.

[191] Wolf, M. M. Violation of the entropic area law for fermions. *Phys. Rev. Lett. 96* (2006), 010404.

[192] Wolf, M. M. Quantum channels and operators: A guided tour. Lecture notes available at `http://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf`, 2012.

[193] Wootters, W. K. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters 80*, 10 (1998), 2245–2248.

[194] Wootters, W. K., and Zurek, W. H. A single quantum cannot be cloned. *Nature 299*, 5886 (1982), 802–803.

[195] Xiang, T., Lou, J., and Su, Z. Two-dimensional algorithm of the density-matrix renormalization group. *Phys. Rev. B 64* (2001), 104414.

[196] Zhu, H., Chen, L., and Hayashi, M. Additivity and non-additivity of multipartite entanglement measures. *New Journal of Physics 12*, 8 (2010), 083002.