eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
ZIENTZIA ETA TEKNOLOGIA FAKULTATEA
FACULTAD DE CIENCIA Y TECNOLOGÍA

Trabajo Fin de Grado
Grado en Física

Entrelazamiento como recurso para tareas de información

Resumen

En una carta datada en 1947 Albert Einstein definió el entrelazamiento como "acción fantasmal a distancia". A lo largo de los años esta propiedad insólita y aterradora para algunos, se ha convertido en una gran oportunidad para otros. Gracias al carácter del entrelazamiento, el paradigma de los procesos de tratamiento de información puede llegar a cambiar de forma radical, llegando incluso a producir una revolución en la información y la comunicación. El presente trabajo pretende identificar algunas de las propiedades que describe el entrelazamiento y su posible uso como recurso en tareas de información.

Autora:
Tamara Zarantón Nieto

Director:
Íñigo Luís Egusquiza Egusquiza
(*Departamento de Física Teórica, UPV-EHU)*

Leioa, 26 de junio de 2017

Índice

1 Introducción y objetivos

El entrelazamiento cuántico ha sido objeto de estudio desde la definición de la teoría de la mecánica cuántica hasta hoy día. Si bien su popularidad en sus comienzos se debió al formalismo cuántico, en los últimos años es visto como un recurso muy poderoso en el área de la comunicación, computación y criptografía cuántica.

El estudio de la comunicación cuántica trata de establecer tareas de procesado de información mediante el uso de sistemas mecánico-cuánticos. Aun cuando esta definición sea básica, y pueda ser comprendida por muchos, no implica que sea una labor sencilla. Sin embargo, el entrelazamiento ofrece un sinfín de ventajas que pueden llegar a producir grandes cambios en los métodos de comunicación utilizados en la actualidad.

"Las unidades de información son lo que crea la realidad, no las unidades de materia ni de energía."

Vlatko Vedral, 2011 [1].

Otra razón por la que el entrelazamiento resulta ser de gran atractivo es porque juega un papel crucial en computación cuántica. Aquí el entrelazamiento ofrece capacidades extraordinarias a los sistemas computacionales haciendo que puedan llegar a ser mucho más rápidos que lo implementado hasta ahora. De esta forma se pueden resolver velozmente problemas muy complejos.

Por otro lado, es inevitable hablar de la criptografía cuántica, una sistemática que usa el entrelazamiento como recurso para la codificación de información sensible. El uso del entrelazamiento para la encriptación es ya una realidad. Algunos organismos ya se han beneficiado de las ventajas que esta herramienta es capaz de proporcionar. Cabe destacar que el entrelazamiento permite que la encriptación de la información alcance niveles de seguridad máximos que no serían posibles de conseguir por otros medios.

El objetivo de este trabajo es identificar y clasificar el entrelazamiento como un potente recurso en tareas de información. La idea principal es identificar, en la medida de lo que el trabajo permita, lo que el entrelazamiento supone, siempre fijando la mira hacia la utilidad y el recurso potencial que alberga, para su aplicabilidad futura en procesos reales.

Para ello, primero realizaremos un resumen de algunos conceptos fundamentales de la mecánica cuántica. En este apartado identificaremos las herramientas principales de las que vamos a hacer uso a lo largo del trabajo.

Después definiremos el entrelazamiento partiendo del concepto de estado separable en oposición a este. Este concepto solo surge en sistemas compuestos, por dos o más subsistemas.

Una vez definido el entrelazamiento, y por tanto los estados entrelazados, veremos una selección de tareas que pueden darse solo con sistemas en estados entrelazados.

Sin embargo, estudiaremos como no todos los estados entrelazados pueden realizar todas las tareas. Debido a este hecho será necesario clasificar los estados en función a las tareas que pueden realizar. Las operaciones locales son las que nos van a determinar las distintas clasificaciones y equivalencias de estados.

Por último, se explicarán cuatro formas para calcular el grado de entrelazamiento de un estado. Las cuatro cantidades no tienen porque coincidir y dependerán del estado y su configuración.

2 Estado del arte

En 1932 Einstein, Podolsky y Rosen (EPR) reconocieron una característica subyacente de la mecánica cuántica no experimentada hasta el momento. Esta característica implica la existencia de sistemas cuánticos compuestos no factorizables, o separables, en los distintos subsistemas que los componen. A este hecho se le conoce con el nombre de entrelazamiento.

La paradoja EPR describía la mecánica cuántica como una teoría incompleta debido su carácter probabilístico. En 1964, Bell partió de la paradoja EPR y del supuesto de un mundo determinista clásico donde hubiera variables locales ocultas[1]. De esta forma Bell llegó a una desigualdad lógica bajo estas hipótesis, usando álgebra de conjuntos.

El supuesto indica que los resultados de las mediciones están determinados por las propiedades que presentan las propias partículas, independientemente de la acción de la medida. Bell asumió la localidad y la realidad: i) la localidad indica que los efectos físicos tienen una velocidad de propagación finita y ii) la realidad indica que los estados físicos existen incluso antes de ser medidos. Según estas hipótesis los resultados obtenidos en un lugar son independientes de cualquier acción realizada en un lugar causalmente disjunto. Es decir circunstancias no locales no interfieren en la medición.

Las expresiones a las que llegó Bell se denominan desigualdades de Bell. Bell demostró que estas desigualdades son violadas de manera sistemática por ciertos tipos de sistemas cuánticos, los sistemas cuánticos entrelazados.

Este hecho trajo consigo una serie de preguntas acerca de si las desigualdades de Bell estaban realmente basadas en una lógica clásica bien construida, o si en realidad lo que ocurre es que existe una teoría de variables ocultas no local, o por el contrario que tal vez los objetos físicos solo son reales cuando pueden ser medidos.

[1] La variable local oculta representa aquellas propiedades implícitas en la naturaleza que se desconocen y no son accesibles directamente, pero que dan lugar a correlaciones medibles.

Es por todo esto que el entrelazamiento es la característica del formalismo cuántico que hace imposible simular las correlaciones cuánticas, que son aquellas que dependen del proceso de observación. En el mundo clásico los objetos tiene propiedades definidas independientemente de si se los observa o no, mientras que en el mundo cuántico las propiedades se definen debido al proceso de medición y no antes [2].

En el caso partícular de los sistemas entrelazados podemos decir que los subsistemas que lo componen no podemos tratarlos como si estuviesen aislados, ya que de alguna manera están correlacionados en la acción de la observación y ejercen una especie de influencia entre ellos. En palabras del propio Schrödinger:

"Así se dispone provisionalmente, hasta que el entrelazamiento se resuelva mediante la observación real de sólo una descripción común de los dos en ese espacio de mayor dimensión. Esta es la razón por la que el conocimiento de los sistemas individuales puede disminuir hasta el más escaso, incluso a cero, mientras que el del sistema combinado permanece siempre máximo. El mejor conocimiento posible de un todo no incluye el mejor conocimiento posible de sus partes, y esto es lo que sigue regresando para atormentarnos."

Erwin Schrödinger, 1935 [2].

La teoría actual del entrelazamiento tiene sus raíces en algunos descubrimientos claves: la criptografía cuántica, la codificación cuántica y el teletransporte cuántico. Todos estos procesos, y más, se basan en el entrelazamiento y han sido demostrados experimentalmente. El entrelazamiento es por tanto un nuevo recurso cuántico para tareas que no pueden realizarse por medios clásicos.

Sorprendentemente, el entrelazamiento es un recurso que puede ayudar, o incluso a veces ser imprescindible, en tareas tales como la reducción de la complejidad clásica de la comunicación, la orientación asistida por el entrelazamiento en el espacio, la estimación cuántica de una constante de amortiguación, mejora de las normas de frecuencia... El entrelazamiento juega un papel fundamental en la comunicación cuántica entre partes separadas por distancias macroscópicas.

Todavía no se sabe si se producirá una aceleración de los procesos en computación cuántica frente a los de computación clásica. Sin embargo, sí se sabe que en cualquier caso la computación cuántica requiere del recurso del entrelazamientos para poder darse, como en los esquemas basados en la medición, la computación cuántica unidireccional... El entrelazamiento también ha dado nuevas perspectivas para comprender muchos fenómenos físicos como la superconductividad, los sistemas desordenados y la aparición de la clasicidad. En particular, la comprensión del papel del entrelazamiento en los métodos existentes de simulación de sistemas de espín cuántico permitió una mejora significativa de los métodos, así como la comprensión de sus limitaciones.

3 El entrelazamiento

En los últimos años el entrelazamiento ha llegado a ser un tema recurrente y muy estudiado, ya que resulta ser un recurso de gran potencial que puede llegar a cambiar el proceso de comunicación tal y como se conoce en la actualidad.

"Yo no la llamaría una propiedad, sino más bien el rasgo característico de la mecánica cuántica, esa que hace que te desvíes del pensamiento clásico."

Erwin Schrödinger, 1925 [2].

3.1 Fundamentos de la mecánica cuántica

Para poder interpretar correctamente el entrelazamiento como un recurso y sus múltiples aplicaciones debemos primero asentar las bases de la mecánica cuántica que lo sustenta.

La mecánica cuántica es una rama matemática que establece una serie de reglas de construcción para las teorías físicas. Estas normas son simples pero se consideran contraintuitivas respecto al mundo clásico con el que nos relacionamos comúnmente [3].

El espacio vectorial lineal que se usa en mecánica cuántica es conocido como el espacio de Hilbert. En este espacio se proyecta todo el aparato matemático de la mecánica cuántica sobre una base rigurosamente formal. Además, la mecánica cuántica requiere de espacios de Hilbert complejos. El espacio de Hilbert es un espacio completo de vectores. Los vectores son conocidos con el nombre de ket y la notación comúnmente usada es $|x\rangle$. Esta notación fue introducida por Dirac.

El espacio dual de los kets es conocido como el espacio bra. Este espacio, en vez de estar compuesto por kets, está compuesto por vectores conocidos como bras. Un bra se denota de la siguiente forma $\langle y|$.

Cualquier espacio vectorial precisa de la definición de su producto interno. En el caso del espacio de Hilbert el producto interno definido se denota como $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ y su definición es

$$\langle x|y\rangle = \sum_{i=1}^{n} x_i^* y_i = (x_1^*, x_2^*, ..., x_n^*) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \tag{3.1}$$

donde $\langle x|y\rangle$ será interpretado como la amplitud de transición de un estado. El módulo al cuadrado de esta amplitud, $|\langle x|y\rangle|^2$, es un número real y representa la probabilidad de transición. La probabilidad de transición es el valor que recupera el significado físico del problema que se está tratando [2, 3].

La dimensión del espacio de Hilbert viene definida por el tamaño máximo del con-

junto de kets linealmente independientes que contiene el espacio. En el ejemplo anterior vemos que el sumatorio va de 1 a n, siendo entonces n el número de dimensiones del espacio con el que estamos tratando. Además, x^* hace referencia al complejo conjugado de $x \in \mathbb{C}$.

Por tanto, el espacio lineal complejo $\mathbb{C}^n$ pasa a ser un espacio de Hilbert haciendo uso del producto interno. Existen dos postulados fundamentales que todo producto interno debe cumplir:

$$\langle x|y\rangle = \langle y|x\rangle^* \tag{3.2}$$

y

$$\langle x|x\rangle \geq 0, \text{ siendo } \langle x|x\rangle = 0 \text{ si y solo si } |x\rangle = 0. \tag{3.3}$$

Con el espacio de Hilbert debidamente construido podemos definir más operadores lineales o funciones que actúen sobre los vectores. Un ejemplo de operador lineal es el proyector[2], $|x\rangle\langle y|$, que actúa de la siguiente forma

$$|x\rangle\langle y||z\rangle \equiv |x\rangle\langle y|z\rangle = \langle y|z\rangle|x\rangle, \tag{3.4}$$

donde

$$|x\rangle\langle y| = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} (y_1^*, y_2^*, ..., y_n^*). \tag{3.5}$$

Una clasificación utilizada para definir sistemas cuánticos se basa en función a la pureza de los mismos. Es decir, un sistema cuántico puede estar compuesto por un único estado o ket, o por el contrario contener más de un estado.

Cualquier sistema descrito por un único estado, $|\psi\rangle$, es un estado puro. Sin embargo, en un sistema cuántico realista el estado no es del todo conocido. Cuando esto ocurre diremos que el estado es un estado mezcla.

Imaginemos que tenemos n máquinas capaces de preparar distintos estados puros que no tienen porque ser ortogonales entre si. Además, cada estado tiene una cierta probabilidad de preparación. Al finalizar la preparación se obtiene un estado final. La forma que tenemos para describir este estado final es a través del operador densidad, ρ. El operador densidad se define como,

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{3.6}$$

donde p_i es la probabilidad de preparación de un estado puro.

Si la probabilidad de que el sistema se encuentre en el estado final de preparación i es $p_i = 1$ y la probabilidad de que se encuentre en otros estados es $p_j = 0 \ \ \forall\ j \neq i$ entonces, diremos que el estado final es un estado puro. En caso contrario el estado final

[2]Los proyectores son operadores cuánticos idempotentes, $P^2 = P$, y hermíticos, $P = P^\dagger$.

es un estado mezcla ($p_j \geq 0$).

Independientemente de si estamos tratando con un estado puro o mezcla siempre se debe cumplir la siguiente propiedad de normalización, donde

$$\sum_i p_i = 1. \tag{3.7}$$

Este operador tiene dos interesantes propiedades. La primera es que el operador densidad es hermítico, lo que significa que es igual a su adjunto $\rho = \rho^\dagger$. Debido a esta propiedad podemos asegurar que los autovalores son reales. La segunda propiedad es que satisface la condición de normalización

$$\mathrm{Tr}(\rho) = 1. \tag{3.8}$$

El operador densidad correspondiente a un sistema puro es

$$\rho = |\psi_i\rangle\langle\psi_i|, \tag{3.9}$$

por lo que cláramente el operador densidad para un sistema puro es idempotente,

$$\rho^2 = \rho, \tag{3.10}$$

y por esto para un sistema puro siempre se cumple que

$$\mathrm{Tr}(\rho^2) = 1. \tag{3.11}$$

Sin embargo, para sistemas mezcla la traza del cuadrado del operador densidad será un número positivo pero inferior a 1,

$$0 \leq \mathrm{Tr}(\rho^2) < 1. \tag{3.12}$$

El operador densidad contiene toda la información física del sistema y resulta esencial a la hora de realizar mediciones.

En la teoría de información cuántica una medición se asocia con una colección de operadores u observables que satisfacen la condición de completitud [4],

$$\sum_i M_i = \mathbb{1}, \tag{3.13}$$

donde M_i es un operador que forma parte del conjunto que puede realizar mediciones sobre el sistema y $\mathbb{1}$ es la matriz identidad.

Para cada índice, i, se le asigna un operador, M_i. Las medidas realizadas con estos operadores siempre van a ser positivas. Esto se conoce como POVM o, en inglés, Positive Operator Valued Measure. Los operadores POVM no tienen porque ser ortogonales entre sí.

Si ρ resulta ser el operador densidad del sistema cuántico, la probabilidad de que se produzca el resultado i-ésimo será

$$p_i = \mathrm{Tr}(M_i\rho). \tag{3.14}$$

Un posible esquema del funcionamiento de un POVM puede ser el siguiente:

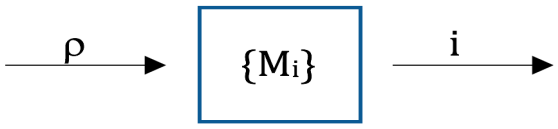

Figura 1: Esquema POVM.

Según el esquema anterior la entrada es el estado ρ y la salida que obtenemos es el resultado de la medida.

También nos puede interesar conocer el estado a la salida. Para ello necesitamos realizar una medida filtrante. Se denomina así porque al realizar la medida sobre el estado ρ, se obtiene el estado filtrado ρ_i, además del resultado de la medida.

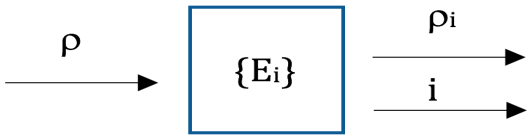

Figura 2: Esquema medida filtrante.

Sabemos que inmediatamente después de la medida el estado del sistema se describe como

$$\rho_i = \frac{1}{p_i}(E_i \rho E_i^\dagger), \tag{3.15}$$

donde E_i es un operador conocido como efecto y su definición es $M_i = E_i^\dagger E_i$.

3.2 Diferencias entre estados clásicos y cuánticos

3.2.1 BIT

La unidad fundamental de la rama de la información es el bit. Esto es así para el tratamiento de comunicación y computación clásica. El bit, si lo tratamos como un mero objeto matemático abstracto, resulta ser un sistema que solo puede tener dos estados o valores posibles, “0” y “1”, y bajo ninguna circunstancia el bit puede ser una superposición de ambos. Este sistema también es conocido como CBIT o bit clásico.

Podemos imaginarnos el bit como un interruptor que tiene solo dos posiciones posibles. También, podemos asemejar el bit como un sistema con dos estados posibles totalmente distinguibles, discretos y estables, y que además, entre ellos existe una barrera de energía lo suficientemente grande como para evitar las transiciones espontáneas de un estado a otro.

3.2.2 CÚBIT

En computación y comunicación cuántica la unidad fundamental es el cúbit o bit cuántico (en inglés qubit). Al igual que con el bit clásico, el cúbit puede tratarse como un objeto matemático abstracto con una serie de propiedades, aun cuando sabemos que en ambos casos (bit y cúbit) también resultan corresponder a sistemas físicos reales.

La decisión de caracterizar al cúbit como un objeto matemático abstracto es debido a que permite construir una teoría de computación y comunicación cuántica, dejando a un lado la correlación con sistemas físicos reales que pudiera tener.

La diferencia que se encuentra entre un bit clásico y un cúbit es que los cúbits pueden encontrarse en estados que son una combinación lineal o superposición de los estados base, $|0\rangle$ y $|1\rangle$. Un ejemplo de superposicion de estado es

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3.16}$$

donde el estado cuántico $|\psi\rangle$ del sistema cúbit resulta ser una combinación lineal que cumple la siguiente igualdad, $|\alpha|^2+|\beta|^2= 1$. Además, en general α y β son números complejos. La interpretación geométrica de esta propiedad puede visualizarse como si los estados se encontrasen normalizados a 1. Por esto, el estado de un cúbit podemos asemejarlo a un vector unitario de dos dimensiones en el espacio complejo $\mathbb{C}^2$(ver Figura 4).

Es importante destacar el hecho de que los vectores $|0\rangle$ y $|1\rangle$ forman una base ortogonal en el espacio de Hilbert con las siguientes propiedades:

$$\langle 0|0\rangle = \langle 1|1\rangle = 1 \qquad y \qquad \langle 0|1\rangle = \langle 0|1\rangle = 0. \tag{3.17}$$

Si se observa la ecuación 3.16 se puede determinar que la probabilidad de que del sistema $|\psi\rangle$ se obtenga el valor $|0\rangle$ en la medida es $p_0 = |\alpha|^2$, y de que se obtenga $|1\rangle$ es $p_1 = |\beta|^2$.

Más aún, una vez se ha realizada la medida filtrante el estado del sistema será $|0\rangle$ o $|1\rangle$ en función a lo que se halla obtenido en la medición (ver figura 2).

El principio de correspondencia establece que en el límite asintótico se debe recuperar la física clásica. Esto nos permite poder construir un hamiltoniano cuántico a partir de hacer corresponder las variables clásicas con operadores. El paso directo de un sistema cuántico, de la concepción matemática abstracta, a los sistemas físicos reales es tremendamente dificultoso.

Sin embargo, sabemos que los cúbits son objetos reales cuya existencia y comportamiento se han verificado a través de muchos experimentos. Ejemplos de la existencia de estos estados pueden ser: dos estados de polarización de un fotón, la alineación de un espín nuclear ante la presencia de un campo magnético, dos estados de un electrón orbitando alrededor de un átomo... En la figura 3 podemos ver la representación de este último ejemplo, donde los estados $|0\rangle$ y $|1\rangle$ son el estado fundamental y el primer estado

excitado, respectivamente.

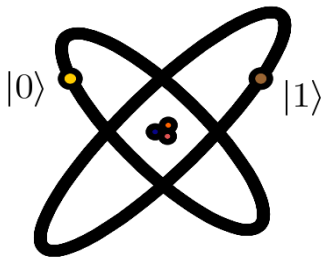

Figura 3: Representación de un cúbit por dos niveles electrónicos de un átomo. *(Creds.: M.A. Nielsen [2])*

La búsqueda de nuevos sistemas con esta configuración es un trabajo constante. Otros ejemplos de ello son: cúbits en circuitos superconductores, centros NV (nitrógeno-vacante) en diamantes, puntos cuánticos...y se trabaja activamente en buscar más. En la teoría de información cuántica esto se conoce como plataformas cuánticas.

Sin embargo, una cuestión subyacente de todo esto es la propiedad de indeterminismo que surge de forma inherente en los sistemas cuánticos. Para intentar visualizar los estados cuánticos, se propone la siguiente representación geométrica, la esfera de Bloch.

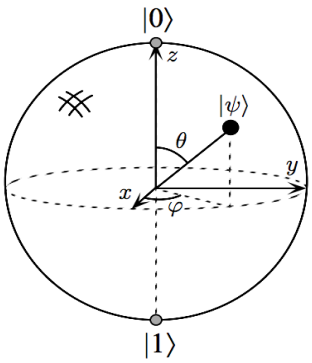

Figura 4: Representación de un cúbit en la esfera de Bloch. *(Creds.: M.A. Nielsen [2])*

Debido a que $|\alpha|^2 + |\beta|^2 = 1$, el radio de la esfera de Bloch es 1. Gracias a esta representación podemos construir el estado $|\psi\rangle$ como:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{3.18}$$

Las variables θ y φ son las coordenadas que nos indican la posición de estado en la esfera. La esfera de Bloch es una construcción que nos ayuda a entender de forma visual la composición de los cúbits, sin embargo tiene una limitación muy grande. No es válida para sistemas donde intervenga más de un cúbit. Existen construcciones análogas para sistemas compuestos pero no tienen una descripción geométrica fácilmente visualizable.

En cuanto a las medidas, es importante saber que, en el momento en el que medimos el estado cuántico de un cúbit, los posibles valores a obtener son $|0\rangle$ o $|1\rangle$. De lo que tenemos que ser conscientes es de que solo obtenemos un único valor. Entonces, ¿por qué resulta tan interesante la aplicación de una teoría de la información cuántica sobre sistemas computacionales?. Si la investigación de las propiedades de los estados cuánticos se frenase en este punto no se observaría ninguna ventaja del cúbit frente al bit clásico, con el inconveniente de que el cúbit es más difícil de tratar y controlar. Es justamente en este punto donde la peculiaridad del entrelazamiento de los sistemas cúbit se convierte en la clave esencial, que permitirá que los sistemas cuánticos se vuelvan más populares y sean unos de los objetos de estudio más seguidos en la actualidad.

3.3 Estados entrelazados

La superposición de estados hace posible la existencia de sistemas cuánticos en estados entrelazados. Una cuestión importante de la teoría de estados entrelazados es saber distinguir cuando un sistema se encuentra en un estado entrelazado y cuando no. El hecho de tener sistemas de dos o más cúbits no significa que el estado total que estén formando sea un estado entrelazado. Más aún, esta pregunta se responde fácilmente en muy pocos casos. El caso más simple es cuando tenemos un sistema cuántico en estado puro [2, 3, 4].

Para ello se expondrá el ejemplo más sencillo. Suponemos que el sistema cuántico está formado por dos cúbits. El estado total del sistema cuántico se expresaría como el producto tensorial $\otimes$,

$$|\Psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle, \tag{3.19}$$

donde los estados definidos como $|\psi_A\rangle$ y $|\psi_B\rangle$ corresponden a los estados de cada cúbit en el espacio de Hilbert $\mathcal{H}_A$ y $\mathcal{H}_B$. Entonces el estado del sistema total $|\Psi\rangle \in \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ y, teniendo en cuenta que estamos trabajando con cúbits de espín $\frac{1}{2}$, la dimensión de $|\Psi\rangle$ es de 2×2.

Además cada subsistema está definido de la siguiente manera

$$|\psi_A\rangle = \alpha_A|0\rangle + \beta_A|1\rangle \tag{3.20}$$

y

$$|\psi_B\rangle = \alpha_B|0\rangle + \beta_B|1\rangle. \tag{3.21}$$

Los estados que se pueden describir según la ecuación 3.19 son estados factorizables. Estos estados se pueden separar y distinguir en función a los dos subsistemas que lo componen. Por definición de entrelazamiento los estados no factorizables son estados entrelazados.

Un ejemplo de superposición de estado no factorizable o entrelazado es

$$|\Phi\rangle = \gamma(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \tag{3.22}$$

y de estado factorizable

$$|\Omega\rangle = \delta(|0\rangle_A \otimes |0\rangle_B + |0\rangle_A \otimes |1\rangle_B) = \delta|0\rangle_A \otimes (|0\rangle_B + |1\rangle_B). \tag{3.23}$$

Un sistema cuántico, compuesto por una combinación lineal de n subsistemas, se dirá que se encuentra entrelazado si no puede escribirse como una combinación del producto tensorial de los n estados según la ecuación

$$\rho_{sep} = \sum_i p_i |\psi_A^i\rangle\langle\psi_A^i| \otimes |\psi_B^i\rangle\langle\psi_B^i|. \tag{3.24}$$

La separabilidad define de forma directa el entrelazamiento por oposición.

Los sistemas cuánticos pueden identificarse en función a sus correlaciones no clásicas. En sistemas puros si tenemos correlaciones no clásicas pueden estar, o no, entrelazados.

Veamos ahora un ejemplo concreto de dos cúbist pertenecientes a dos subsistemas A y B correspondiendo cada uno al espacio de Hilbert $\mathbb{C}^2$ donde,

$$|\psi_A\rangle = \sum_i p_i |\psi_A^i\rangle \tag{3.25}$$

y

$$|\psi_B\rangle = \sum_j q_j |\psi_B^j\rangle. \tag{3.26}$$

Entonces, el estado total $|\Psi\rangle$ se construye como la combinación tensorial de ambos subestados

$$|\Psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = \sum_{i,j} c_{ij} |\psi_A^i\rangle \otimes |\psi_B^j\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2, \tag{3.27}$$

cuya dimensión es 2×2.

Genéricamente el estado $|\Psi\rangle$ pueden ser combinaciones lineales de productos tensoriales [2, 5]. Haciendo uso de esta construcción, para el caso de dos cúbits de dimensión 2, aparecen los 4 "Estados Entrelazados de Bell" o "Estados EPR":

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B), \tag{3.28}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B), \tag{3.29}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) \tag{3.30}$$

y

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B). \tag{3.31}$$

Los cuatro estados que se acaban de definir tienen una serie de propiedades a destacar muy interesantes:

- La probabilidad de que un subsistema se encuentre en el estado $|0\rangle$ o en el estado $|1\rangle$ es la misma en todos ellos.
- Según esta configuración de estados, el sistema no ofrece una información concisa sobre los subsistemas de los que se compone.

- Los estados del sistema bipartito son puros, por lo que tendremos un conocimiento máximo del sistema.
- A través de una transformación unitaria local, U, podemos pasar de uno de los estados a cualquiera de los otros tres. Por lo que los cuatro estados están relacionados por operadores locales unitarios. Esto dará como resultado que los cuatro estados son equivalentes (ver apartado 5.1).
- Los estados EPR violan al máximo las desigualdades del Bell debido a su máximo entrelazamiento.

Los estados entrelazados de Bell son un caso especial de entrelazamiento máximo de dos cúdits en el espacio de Hilbert $\mathbb{C}^d \otimes \mathbb{C}^d$, dados por

$$|\Psi\rangle = U_A \otimes U_B |\phi_d^+\rangle_{AB}, \tag{3.32}$$

siendo $U_A \otimes U_B$ operadores unitarios de ambos subsistemas. Además, el estado canónico máximo entrelazado para dos cúdits se define como

$$|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle. \tag{3.33}$$

El estado entrelazado máximo EPR también es conocido como estado singlete, en el caso de dos cúbits.

Una vez identificado el sistema cuántico como estado entrelazado o estado separable, nos interesa saber si el estado que tenemos entre manos sigue entrelazado después de realizar ciertas tareas con él.

Además, es importante poder medir y determinar el grado de entrelazamiento de un sistema cuántico. Responder a esto resulta ser algo no trivial.

4 Usos del entrelazamiento

Hasta los años noventa, el entrelazamiento cuántico se consideraba una curiosidad física, una característica exótica sin uso práctico. Esta consideración comenzó a cambiar en 1991, cuando A. Ekert presentó una tarea realizada por la teoría de la información cuántica basada en la propiedad del entrelazamiento. En su trabajo A. Ekert demostró que si dos sistemas, A y B, comparten una gran cantidad de estados singlete entrelazados, el proceso de comunicación entre ambos es completamente seguro. Esta tarea se conoce como criptografía cuántica o distribución de clave cuántica [6].

Este resultado debe compararse con la criptografía clásica tal como la usamos hoy en día. La seguridad de la criptografía clásica se basa principalmente en la conjetura de que un número muy grande es difícil de factorizar, mientras que el protocolo de criptografía cuántica presentado por Ekert es totalmente seguro, debido al uso de los estados entrelazados. Esto hace que la criptografía cuántica sea 100 % segura desde este punto de vista.

La propuesta de A. Ekert incentivó a proponer más tareas que implicasen la característica de entrelazamiento. En 1992 C.H. Bennett y S.J. Wiesner demostraron que dos sistemas entrelazados pueden comunicar dos bits clásicos enviando un único cúbit, es decir, un sistema cuántico en un espacio de Hilbert bidimensional. Esta tarea también se conoce como codificación cuántica densa, ya que dos bits clásicos se pueden codificar en un bit cuántico o cúbit [7].

Otra aplicación del entrelazamiento resulta ser la comunicación de un estado cuántico desconocido entre dos partes. Un estado cuántico desconocido no puede comunicarse por medios clásicos (LOCC), debido al principio de no clonación (ver apartado 4.2). Sin embargo, si las dos partes comparten un sistema en el estado de singlete entrelazado, cualquier cúbit desconocido puede ser enviado. A este proceso se le llama teletransporte cuántico [2, 8].

Por tanto, los tres primeros usos reconocidos gracias a la propiedad de entrelazamiento son:

- Criptografía cuántica.
- Codificación densa.
- Teletransportación.

En este trabajo se va a exponer con mayor detalle el proceso de *Distribución cuántica de claves, Teletransporte y el Algoritmo computacional de Shor*.

4.1 Distribución cuántica de claves basadas en el entrelazamiento

Comenzaremos con la distribución cuántica de claves debido a que fue el primer uso en el que se pensó para aprovechar las características de los sistemas cuánticos entrelazados. Esta utilidad fue propuesta por A.K. Ekert [6, 9] en 1991 utilizando la base de estados de Bell indicada en la ecuación 3.28.

La criptografía es un método que se usa desde hace siglos. Su objetivo es cifrar mediante métodos matemáticos y algoritmos computacionales la información para transmitirla de una forma ininteligible desde un emisor a un receptor. El proceso de criptografía dispone de una clave de codificación y decodificación, la cual contiene las *instrucciones* para codificar y decodificar la información.

Se han desarrollado muchas mejoras para conseguir que no se comprometa la seguridad de las claves. La mayoría están orientadas a que las claves estén compuestas por más datos o unidades de bits. De esta forma es más complejo descifrar la clave pero no imposible. La diferencia reside en el tiempo que emplea un algoritmo computacional en descifrar la clave. A mayor número de bits más tiempo.

Aquí es donde entra la figura del entrelazamiento, ya que gracias a sus propiedades si se usan los estados singletes de Bell encontramos dos ventajas frente al sistema

clásico. En primer lugar estamos tratando con estados puros máximamente entrelazados y en segundo lugar, si hubiese un fallo de seguridad en la transmisión del mensaje, el sistema automáticamente perdería sus propiedades y la información sería irreproducible.

La metodología que propuso Ekert fue la siguiente. Los sistemas Alice y Bob reciben pares de estados entrelazados producidos por una fuente EPR, generadora de pares entrelazados en el estado EPR de forma aleatoria [9]. Estos pares máximamente entrelazados, en este contexto, resultan ser la clave para codificar y decodificar la información que se quieran transmitir Alice y Bob en un entorno totalmente privado y seguro [2, 5, 8]. Si durante el proceso de transmisión de los pares hubiese un intento de medición estos perderían su estado cuántico entrelazado debido a la decoherencia. Es decir, es cómo si la clave al medirla se autodestruyera sin posibilidad de ser reconstruida y, además, tanto Alice como Bob serían conscientes de la intrusión acaecida.

Suponemos que el sistema Charlie está intentando acceder a la clave que está siendo enviada a Alice y Bob desde la fuente EPR. Sabemos que Charlie no puede acceder a la clave sin perturbar el estado. Debido al principio de no-clonación, demostrado en el apartado 4.2, Charlie no puede clonar el estado entrelazado que está siendo enviado y, además, si intenta distinguir aunque sea entre dos estados cuánticos no ortogonales, se introducirá automáticamente en el estado una señal perturbativa [2, 5, 9].

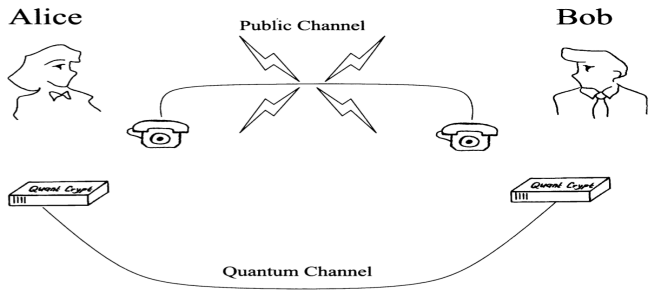

Figura 5: Distribución cuántica de claves. *(Creds.: D. Bouwmeester [5])*

La demostración de la introducción de la señal perturbativa es la siguiente. Suponemos dos estados cuánticos no ortogonales $|\psi\rangle$ y $|\phi\rangle$. Estos estados son los que está tratando de identificar Charlie. Asumiremos que el proceso de interacción, con el cual Charlie está trabajando para intentar determinar los estados, es mediante el uso de un estado unitario estandar aplicado sobre $|\psi\rangle$ o $|\phi\rangle$. Podemos representarlo como

$$|\psi\rangle|u\rangle \rightarrow |\psi\rangle|v\rangle \tag{4.1}$$

o

$$|\phi\rangle|u\rangle \rightarrow |\phi\rangle|w\rangle, \tag{4.2}$$

suponiendo que esta acción no perturba el estado $|\psi\rangle$ o $|\phi\rangle$.

El interés de Charlie reside en conocer las diferencias entre los dos estados obtenidos, $|v\rangle$ y $|w\rangle$. Sin embargo, sabemos que el producto interno es invariante bajo transformaciones unitarias. Por tanto

$$\langle v|w\rangle\langle\psi|\phi\rangle = \langle u|u\rangle\langle\psi|\phi\rangle, \tag{4.3}$$

donde se obtiene que

$$\langle v|w\rangle = \langle u|u\rangle = 1. \tag{4.4}$$

Finalmente el resultado anterior implica que

$$|v\rangle = |w\rangle, \tag{4.5}$$

por lo que ambos estados resultan ser equivalentes y no pueden ser distinguidos.

En definitiva, cada vez que Charlie pretenda averiguar la clave que se les distribuye a Alice y Bob el estado se verá perturbado y ya no servirá. Además, otra propiedad muy interesante es que, tal y como se ha mencionado antes, Alice y Bob pueden darse cuenta de que Charlie está intentado acceder a su clave. Por tanto, el entrelazamiento es una herramienta extremadamente segura en la distribución de claves criptográficas, mientras que, el mensaje cifrado puede ser transmitido por los canales clásicos de comunicación.

4.2 Teletransporte

Debido a que una de las características más controvertidas del entrelazamiento era el procesado de la información, mucho más rápido que lo conocido mediante procesos de comunicación clásica, se sugirió la posibilidad de copiar masivamente estados cuánticos para después transportarlos de un modo más eficiente. Pero al estudiar el proceso de copia de estos estados cuánticos se obtuvo un resultado inesperado: la mecánica cuántica prohíbe la copia de sistemas. A este descubrimiento se le llamó *Principio de no-clonación* siendo uno de los primeros hechos a destacar después del alumbramiento de la mecánica cuántica [2].

La demostración del Principio es muy sencilla. Se parte del siguiente escenario: tenemos un estado $|\psi\rangle$ perteneciente al sistema A y lo queremos copiar en el estado $|e\rangle$ del sistema B. Para ello definimos un operador U unitario que será el encargado de realizar la copia. Entonces, si aplicamos el operador

$$\mathrm{U}|\psi\rangle_A \otimes |e\rangle_B = |\psi\rangle_A \otimes |\psi\rangle_B \tag{4.6}$$

y utilizamos dos estados pertenecientes al sistema A para copiarlos en el sistema B de la siguiente forma

$$\begin{aligned} \langle\phi|\psi\rangle\langle e|e\rangle &= \langle\phi|_A\langle e|_B|\psi\rangle_A|e\rangle_B = \langle\phi|_A\langle e|_B\mathrm{U}^\dagger\mathrm{U}|\psi\rangle_A|e\rangle_B = \langle\phi|_A\langle\phi|_B|\psi\rangle_A|\psi\rangle_B \\ \langle\phi|\psi\rangle\langle e|e\rangle &= |\langle\phi|\psi\rangle|^2 \quad \text{donde,} \\ \langle e|e\rangle &= 1 \ \text{ por ser ortonormal, obtenemos que } \langle\phi|\psi\rangle = |\langle\phi|\psi\rangle|^2. \end{aligned} \tag{4.7}$$

Para que se cumpla la última igualdad será necesario que $|\langle\phi|\psi\rangle| = 1$ o $|\langle\phi|\psi\rangle| = 0$. En el primer caso implicaría que ambos estados son iguales, pero descartamos esta solución debido a que por hipótesis solicitamos que sean distintos. Por otro lado, que la solución sea nula implica que los estados son ortogonales, pero de nuevo por hipótesis especificamos que no lo sean ya que ambos estados son arbitrarios. Como no son válidas ninguna de las dos soluciones se determina que la clonación no es posible en sistemas

regidos por una física de naturaleza cuántica [2].

Si bien acabamos de demostrar que la clonación exacta no es una posibilidad, sigue siendo de gran interés tener la capacidad de transmitir una información de un sitio a otro. Por este motivo se propuso el proceso de *Teletransporte*.

Para que Alice y Bob puedan enviarse entre ellos los estados que quieran primero necesitan juntarse y generar un estado EPR. Elegimos para realizar el ejemplo el estado de Bell $|\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|01\rangle_{23} - |10\rangle_{23})$. Después cada cual deberá llevarse la mitad del par consigo. Una vez que Alice y Bob tienen sus pares entrelazados suponemos que Alice quiere enviar a Bob un estado $|\chi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$ cualquiera, el cual es totalmente desconocido. Entonces Alice hace interactuar el estado $|\chi\rangle_1$ con $|\psi^-\rangle_{23}$ y realiza un par de operaciones ayudada de dos puertas lógicas, CNOT y HADAMARD.

$$\begin{aligned} CNOT_{ct}|0\rangle_c|1\rangle_t &= |0\rangle_c|1\rangle_t, \qquad CNOT_{ct}|0\rangle_c|0\rangle_t = |0\rangle_c|0\rangle_t, \\ CNOT_{ct}|1\rangle_c|1\rangle_t &= |1\rangle_c|0\rangle_t, \qquad CNOT_{ct}|1\rangle_c|0\rangle_t = |1\rangle_c|1\rangle_t, \\ H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{y} \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

Los subíndices c y t corresponden al estado control y estado transmisión. En el caso de la puerta CNOT se cambia el estado a transmitir si el estado control es $|1\rangle$, en caso contrario se deja tal y como está. La puerta lógica HADAMARD actúa en cada estado $|0\rangle$ o $|1\rangle$ según lo indicado.

Entonces el estado que resulta de combinar $|\chi\rangle_1$ y $|\psi^-\rangle_{23}$ es

$$|\xi\rangle_{123} = |\chi\rangle_1 \otimes |\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}\alpha|0\rangle_1(|01\rangle_{23} - |10\rangle_{23}) + \frac{1}{\sqrt{2}}\beta|1\rangle_1(|01\rangle_{23} - |10\rangle_{23}). \tag{4.8}$$

Aplicando la puerta CNOT sobre el estado $|\xi\rangle_{123}$ tendremos que

$$\widetilde{|\xi\rangle}_{123} = CNOT_{12}|\xi\rangle_{123} = \frac{1}{\sqrt{2}}\alpha|0\rangle_1(|01\rangle_{23} - |10\rangle_{23}) + \frac{1}{\sqrt{2}}\beta|1\rangle_1(|11\rangle_{23} - |00\rangle_{23}). \tag{4.9}$$

Y aplicando ahora la puerta HADAMARD de nuevo sobre el estado $\widetilde{|\xi\rangle}_{123}$

$$\begin{aligned} |\Xi\rangle_{123} = H_3\widetilde{|\xi\rangle}_{123} &= \frac{1}{2}\alpha(|0\rangle_1 + |1\rangle_1)(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3) + \frac{1}{2}\beta(|0\rangle_1 - |1\rangle_1)(|1\rangle_2|1\rangle_3 - |0\rangle_2|0\rangle_3) \\ &= \frac{1}{2}[|00\rangle_{12}(\alpha|1\rangle_3 - \beta|0\rangle_3) + |01\rangle_{12}(-\alpha|0\rangle_3 + \beta|1\rangle_3) + |10\rangle_{12}(\alpha|1\rangle_3 + \beta|0\rangle_3) \\ &+ |11\rangle_{12}(-\alpha|0\rangle_3 - \beta|1\rangle_3)]. \end{aligned} \tag{4.10}$$

A continuación, Alice realiza sobre el estado $|\Xi\rangle_{123}$ una medición pudiendo obtener como resultados $|00\rangle_{12}$, $|01\rangle_{12}$, $|10\rangle_{12}$ o $|11\rangle_{12}$. En función del resultado de la medida el estado en el que se encuentra la partícula de Bob será el que está relacionado directamente con la medida. Si por ejemplo suponemos que la medida da como resultado el estado $|00\rangle_{12}$ entonces el estado que tiene Bob es $(\alpha|1\rangle_3 - \beta|0\rangle_3)$. A partir de este momento lo único que tiene que hacer Alice es comunicarle a Bob, mediante un canal clásico, el

resultado de su medida y de esta forma Bob puede realizar la operación unitaria correspondiente sobre su partícula para obtener el estado $|\chi\rangle_1$, completando así el proceso de teletransporte (ver figura 6) [2, 5, 8].

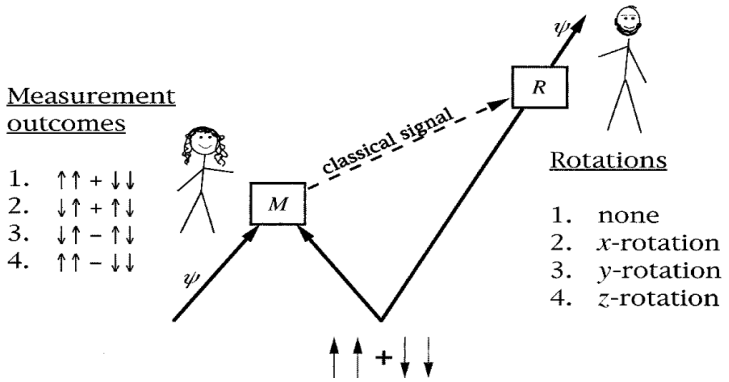

Figura 6: Teletransporte. *(Creds.: W.K. Wootters [8])*

Se debe destacar el hecho de que cuando Alice realiza la medida sobre la interacción de ambos estados el estado cuántico del par EPR desaparece. Por otro lado también resulta conveniente especificar que en el proceso de teletransporte el estado no viaja más rápido que la luz. Se debe hacer notar que Bob no obtiene el estado $|\chi\rangle_1$ hasta que Alice le informa del resultado de la medición a través de canales de comunicación clásicos. En parte es un alivio que esto sea así, ya que de lo contrario se estaría violando la Teoría de la Relatividad infringiendo el hecho de que nada puede viajar más rápido que la luz, ni siquiera la información.

El teletransporte puede ser utilizado en muchos procesos como por ejemplo en la construcción de puertas lógicas en computación cuántica. Esta utilidad se debe a que el teletransporte tiene una alta resistencia al ruido que puedan albergar los sistemas [2, 5].

4.3 Algoritmo de Shor

Una de las cuestiones más relevantes para apostar por la computación cuántica es que los sistemas pueden ser mucho más rápidos de los conocidos en la actualidad por la computación clásica. Para un ordenador clásico el proceso de factorización de N dígitos enteros precisa de un número finito de pasos que crece de forma sub-exponencial en función a N, aun no está excluido que exista un algoritmo polinómico clásico.

El problema se centra en el hecho de que cada vez resulta ser más necesario el proceso de factorización para el tratamiento masivo de datos con unos valores de N muy grandes, tanto que el tiempo de ejecución en un ordenador clásico podría llegar a suponer el mismo tiempo de vida del universo [5].

Estos tiempos de ejecución son inadmisibles y se requiere de otros métodos de computación que reduzcan este valor a tiempos razonables. La computación cuántica

podría ser la solución definitiva a este tipo de impedimentos.

En computación cuántica el proceso de factorización de N dígitos tiene una escala de tiempo polinómica, y no exponencial, haciendo que los tiempos de ejecución de tareas se reduzcan a tiempos que entran dentro del rango de lo razonable. El algoritmo de Shor resulta ser el algoritmo más eficiente ideado hasta el momento, por P. Shor en 1994, el cual puede dar solución a dos de las tareas más arduas con las que se encuentra la computación clásica a día de hoy, la factorización de N dígitos en tiempos razonables y la discretización de logaritmos [10].

En este apartado nos centraremos en el algoritmo para la factorización de N dígitos en sus factores primos, por lo que nuestro interés resulta ser la obtención de un número k distinto de 1 o N que divide de forma exacta N. En el caso clásico si pretendemos factorizar N, el tiempo de ejecución es sub-exponencial, $\exp[c(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}]$, donde c es una constante.

El algoritmo de Shor consiste en establecer una serie de pasos iterativos para la factorización de un número N, $O((\log\ N)^2\ (\log\log N)(\log\log\log N))$, en un ordenador cuántico con un tiempo de pos-procesamiento del orden del $\text{poly}(\log N)$ en un ordenador clásico. Para ello se hace uso de la Teoría de Números que nos permite reducir sustancialmente estos pasos encontrando la periodicidad de una función f.

El procedimiento es el siguiente. Se elige aleatoriamente un número x tal que $x < N$. Usando el Algoritmo de Euclides podemos calcular el máximo factor común primo de x y N. Si este factor es mayor que 1 hemos dado con la solución. Sin embargo, si esto no es así x y N son números coprimos, es decir, dos números enteros que no tienen ningún factor primo en común. El Teorema de los Números Primos dice que la probabilidad de que esto ocurra es mayor que $\frac{1}{\log N}$ cuando N es un número grande y dependiendo del valor aleatorio de x escogido [5].

Si se da el caso de que x y N son coprimos el Teorema de Euler garantiza que existe una potencia de x, la cual deja de resto la unidad al dividirlo entre N.

El proceso es el siguiente:

$$\text{si } x^r \equiv 1 \bmod N \text{ donde } r \text{ es la potencia mínima entonces,} \tag{4.11}$$

$$\text{para } r \text{ impar} \rightarrow x^r - 1 \equiv 0 \bmod N, \text{ se escoge otro valor de } x. \tag{4.12}$$

$$\text{para } r \text{ par} \rightarrow (x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) \equiv 0 \bmod N, \text{ entonces } \alpha\beta \equiv 0 \bmod N \tag{4.13}$$

$$\text{siendo } \alpha = (x^{\frac{r}{2}} - 1) \text{ y } \beta = (x^{\frac{r}{2}} + 1). \tag{4.14}$$

Hemos dado con un producto de dos números el cual divide de forma exacta a N, α y β. Teniendo en cuenta que ni α ni β son múltiplos de N, entonces N debe dividirse independientemente por α y β obteniéndose factores no triviales de N. Este procedimiento falla cuando r resulta ser un número impar que da lugar a un factor trivial. La probabilidad de que se encuentre un valor no trivial usando este procedimiento para un valor N es $\left(1 - \frac{1}{2^{(n-1)}}\right)$, siendo n el número de factores primos impares que existen para N [10].

Hasta ahora hemos conseguido reducir el problema de factorización de N en números primos a la búsqueda de un orden r. Dado un número aleatorio x y un número N, para encontrar el orden de x que verifique la ecuación 4.11 se propone lo siguiente. Primero se postula un número q,

$$q = 2^l, \tag{4.15}$$

que pertenece al intervalo de valores $N^2 \leq q \leq 2N^2$ [10].

Se comienza entonces inicializando los estados del sistema a una superposición uniforme, representando números del tipo a mod q, dejando la máquina en el estado superpuesto para el primer registro

$$|\psi\rangle = \frac{1}{q^{1/2}} \sum_{a=0}^{q-1} |a\rangle|0\rangle, \tag{4.16}$$

donde el estado $|a\rangle$ y el estado $|0\rangle$ son un números binarios compuestos de ceros y unos con un longitud de$l$ bits cada uno. El estado $|a\rangle$ se conoce como primer registro y el estado $|0\rangle$ como el segundo registro.

Si visualizásemos el estado del sistema inicializado con un valor de $l = 2$ veríamos que

$$|\psi\rangle = \frac{1}{2}(|00\rangle|00\rangle + |01\rangle|00\rangle + |10\rangle|00\rangle + |11\rangle|00\rangle). \tag{4.17}$$

Después se fija un valor x aleatorio, entre 1 y N, y se calculan los valores de la función periódica $f(a) = x^a$ mod N, donde $f(a) = f(a + r)$ por ser periódica. r es el valor de periodicidad mínimo, todavía desconocido y por determinar. Los valores de la función se almacenan en el segundo registro

$$|\psi\rangle = \frac{1}{q^{1/2}} \sum_{a=0}^{q-1} |a\rangle|x^a \text{ mod } N\rangle = \frac{1}{q^{1/2}} \sum_{a=0}^{q-1} |a\rangle|k\rangle, \tag{4.18}$$

donde se ha definido por comodidad $k = x^a$ mod N.

A continuación se realiza una medida sobre el estado $|\psi\rangle$, en concreto sobre el segundo registro, de forma que se proyecte sobre el subespacio de q dimensiones, que cubre todos los estados de la base $|a\rangle|k\rangle$ para el valor k fijado por la medida.

El nuevo estado que resulta de la medición es

$$|\psi\rangle_k = \frac{1}{M^{1/2}} \sum_{a \in A} |a\rangle|k\rangle, \tag{4.19}$$

donde A es el conjunto formado por aquellos $a < q$, tales que para un $k = x^a$ mod N fijo. Además, definimos $M = |A|$. Lo que significa que

$$A = \{a_0, a_0 + r, a_0 + 2r, ..., a_0 + (M-1)r\} \tag{4.20}$$

donde,

$$M \approx \frac{q}{r} \gg 1. \tag{4.21}$$

De esta forma el estado se puede escribir como

$$|\psi\rangle_k = \frac{1}{M^{1/2}} \sum_{d=0}^{M-1} |a_0 + dr\rangle |k\rangle. \tag{4.22}$$

A partir de aquí se realiza una transformación de Fourier cuántica sobre el primer registro [10]

$$|a_0 + dr\rangle = \frac{1}{q^{1/2}} \sum_{c=0}^{q-1} \exp(2\pi i c(a_0 + dr)/q) |c\rangle \tag{4.23}$$

e introducimos en el estado la transformada en la ecuación 4.22 de la forma

$$\begin{aligned} |\psi\rangle_k &= \frac{1}{\sqrt{qM}} \sum_{c=0}^{q-1} \sum_{d=0}^{M-1} \exp\left(2\pi i \frac{c(a_0 + dr)}{q}\right) |c\rangle |k\rangle & (4.24)\\ &= \sum_{c=0}^{q-1} \frac{e^{\frac{2\pi i c a_0}{q}}}{\sqrt{qM}} \sum_{d=0}^{M-1} \exp\left(2\pi i \frac{cdr}{q}\right) |c\rangle |k\rangle & (4.25)\\ &= \sum_{c=0}^{q-1} \frac{e^{\frac{2\pi i c a_0}{q}}}{\sqrt{qM}} \left(\sum_{d=0}^{M-1} \zeta^d \right) |c\rangle |k\rangle, & (4.26) \end{aligned}$$

donde

$$\zeta = \exp\left(2\pi i \frac{cr}{q}\right). \tag{4.27}$$

A continuación se miden los valores del primer registro $|c\rangle$ donde la probabilidad de que el estado se encuentre en un estado en particular es

$$p(c) = \frac{1}{qM} \left| \sum_{d=0}^{M-1} \zeta^d \right|^2. \tag{4.28}$$

Si la cantidad $\frac{cr}{q}$ no es cercana a un número entero entonces las potencias de ζ, que son $d = 2\pi i \frac{cr}{q}$, tienden a un valor muy pequeño, por lo que los correspondientes valores de $c$son poco probables, $p(c) \to 0$. Teniendo en cuenta que

$$\sum_{d=0}^{M-1} \zeta^d = \frac{1 - \zeta^M}{1 - \zeta}, \tag{4.29}$$

y, por otro lado, que la cantidad $\frac{cr}{q} \approx d$, donde d es un entero, entonces $\zeta \approx 1$ y la probabilidad es

$$p(c) \approx \frac{M}{qM} = \frac{1}{q}, \tag{4.30}$$

resulta que la probabilidad de observar el estado $|c\rangle$ bajo estas condiciones es mucho mayor que en el anterior caso, con un valor alrededor de $\frac{c}{q} \approx \frac{d}{r}$, siendo d un número entero.

Para el valor observado de $|c\rangle$ se utiliza un ordenador clásico que busque valores de $\frac{d}{r}$ cercanos a $\frac{c}{q}$ con la intención de obtener finalmente el orden r donde se verifique $x^r = 1 \bmod N$.

El ordenador realizará un método de fracciones continuadas para encontrar un posible valor de r, de manera que:

$$\frac{c}{q} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots}}}, \tag{4.31}$$

registrando aquellos valores que estén cercanos a $\frac{c}{q}$ y comprobando que se cumple la igualdad $x^r = 1 \bmod N$, con $r < N$. Esta búsqueda de valores se repetirá todas las veces que sean necesarias hasta encontrar un valor de r fiable.

Supongamos que el valor de $\frac{c}{q}$ obtenido es $\frac{4915}{8192}$. El proceso de fracciones continuadas nos daría como resultado que

$$\frac{c}{q} = \frac{4915}{8192} = \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1638}}}}. \tag{4.32}$$

Entonces tenemos que

$$\frac{1}{1} = 1 \tag{4.33}$$

$$\frac{1}{1 + \frac{1}{1}} = \frac{1}{2} \tag{4.34}$$

$$\frac{1}{1 + \frac{1}{1 + \frac{1}{2}}} = \frac{3}{5} \tag{4.35}$$

$$\frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1638}}}} = \frac{4915}{8192}. \tag{4.36}$$

Por lo que el valor de r_1 será el denominador máximo que cumpla que $r_1 < N$. En este caso en concreto será $r_1 = 5$, suponiendo que $8192 > N$. Entonces el valor de r será un múltiplo de r_1 que cumpla la condición $x^r = 1 \bmod N$. Con el valor de r se calcularán entonces los valores de α y β.

De esta forma se ha implementado un algoritmo cuántico capaz de factorizar un número N en un tiempo de ejecución imposible de cumplir por algoritmos clásicos hasta la fecha.

4.4 Utilidad de los distintos estados entrelazados

Los sistemas cuánticos que se encuentran en estados entrelazados son capaces de realizar tareas que son impensables dentro del paradigma de la física clásica. Sin embargo, es de esperar que no todos los estados obren por igual ante una misma tarea, es decir, en función al objetivo final que persigue cada tarea se deberá elegir un estado u otro para que la lleve a cabo.

Los distintos usos del entrelazamiento, expuestos en los subapartados anteriores, hacen referencia a las tres ramas de la física cuántica que ven, de forma directa, el recurso

del entrelazamiento como un gran potencial. Estas tres ramas son la criptografía cuántica (distribución de claves), la comunicación cuántica (teletransporte) y la computación cuántica (algoritmo de factorización de Shor).

Cada tarea tiene un objetivo raíz bien diferenciado. En el caso de la criptografía cuántica el valor añadido sobre las herramientas clásicas actuales es la promesa de un sistema de encriptado con una seguridad inviolable. Es por esto que el estado cuántico que se use en estos casos deberá ser sensible a las intrusiones o perturbaciones que interfieran en él. De manera que pierda la información de encriptado por completo y sea de esta forma irrecuperable.

Para las tareas de comunicación cuántica el interés reside en la fiabilidad del mensaje, tanto emitido como recibido. Lo que queremos es que la información se codifique, se envíe y se reciba tal y como lo hemos determinado. En caso contrario será un proceso totalmente inútil.

Por último, para las tareas necesarias en el ámbito de la computación cuántica el objeto reside en la velocidad en la realización de la tarea misma. Es decir, lo más importante es cuán de rápido se puede realizar una instrucción cuántica mediante un estado cuántico entrelazado. Consiguiendo de esta manera que los algoritmos cuánticos sean muchísimo más eficientes que los algoritmos clásicos actuales.

5 Operaciones

Acabamos de ver cómo dependiendo de las tareas que pretendamos realizar los estados entrelazados a usar se deben elegir en función a distintas finalidades. Sin embargo, un mismo estado entrelazado puede usarse como recurso en múltiples tareas. En esta sección nos interesa saber qué estados resultan ser equivalentes ante una misma tarea, es decir, qué estados pueden utilizarse de manera que lleguen al mismo resultado en la acción. Si podemos determinar y establecer una clasificación de distintos estados que sean capaces de realizar por igual las mismas tareas diremos que estos estados resultan ser equivalentes. Por tanto, para determinar la equivalencia de estados deberemos someterlos a distintas operaciones en función a su naturaleza, Así, operaciones locales unitarias (LU), operaciones locales y comunicación clásica (LOCC) u operaciones locales estocásticas y comunicación clásica (SLOCC) [11].

El estudio de las relaciones de equivalencia resulta ser un enfoque tremendamente exitoso a la hora de caracterizar estados puros bipartitos y multipartitos [12].

Suponemos que partimos de un estado $|\psi\rangle$. A este estado le aplicamos un operador, θ, que corresponde a una operación Θ. La aplicación del operador reduce el estado $|\psi\rangle$ al estado $|\phi\rangle$,

$$\theta|\psi\rangle \rightarrow|\phi\rangle. \tag{5.1}$$

Entonces diremos que el estado $|\psi\rangle$ es reducible al estado $|\phi\rangle$ a través de esta operación.

Sin embargo, para que dos estados sean equivalentes deben ser reducibles entre si. En general se puede decir que si tenemos una operación, $\Theta \in \{\text{LU}, \text{LOCC}, \text{SLOCC}\}$, dos estados, $|\psi\rangle$ y $|\phi\rangle$, serán equivalentes Θ si existen operadores θ_i tales que [13]

$$|\psi\rangle \to \theta_1|\phi\rangle \text{ y } |\phi\rangle \to \theta_2|\psi\rangle, \tag{5.2}$$

donde θ_1 y $\theta_2 \in \Theta$.

Por tanto, para determinar la equivalencia entre dos estados necesitamos que el estado $|\psi\rangle$ sea reducible, a través de cierta operación, al estado $|\phi\rangle$ y que a su vez el estado $|\phi\rangle$ sea reducible, a través de otra operación de la misma familia, al estado $|\psi\rangle$.

En los siguientes apartados damos cuenta de distintas operaciones que nos establezcan unas relaciones de equivalencia entre los diferentes tipos de estados entrelazados.

5.1 Operaciones LU

Las operaciones locales unitarias o LU (Local Unitary Operations) son aquellas operaciones que transforman un estado en otro conservando el producto interno. Aquellas operaciones que solo actúan sobre un subsistema son locales. Además, el producto de operaciones locales también es local:

$$A \otimes B = (A \otimes \mathbb{1})(\mathbb{1} \otimes B). \tag{5.3}$$

Las operaciones locales LU actúan sobre los estados de forma que se preserva la probabilidad. En consecuencia, para bipartitos mantienen los valores de sus respectivos coeficientes de Schmidt [13].

Por ejemplo, escribamos un estado bipartito puro entrelazado como su descomposición de Schmidt,

$$|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i^{\psi}}|i\rangle|i\rangle, \tag{5.4}$$

donde d es la dimensión del estado y λ_i son los coeficientes de Schmidt. La transformación del estado $|\psi\rangle$ a un estado $|\phi\rangle$ mediante una LU mantendrá invariantes los valores de λ_i de la siguiente forma,

$$(\lambda_i^{\psi})_{i=1}^{d} = (\lambda_j^{\phi})_{j=1}^{d}. \tag{5.5}$$

Si esto ocurre diremos que los estados son equivalentes LU [13]

$$|\psi\rangle \rightleftharpoons_{LU} |\phi\rangle. \tag{5.6}$$

Un ejemplo de este tipo de transformación se dá cuando pasamos de un estado EPR a otro, los cuales se encuentran en el estado de máximo entrelazamiento con $\lambda_i = \frac{1}{2}$ (ver estados EPR, ecuación 3.28). Por este motivo se dice que los estados EPR son equivalentes entre sí bajo transformaciones LU [14].

Uno de los resultados más importantes fue cuando se comprobó que un sistema bipartito en un estado puro, como el que estamos estudiando, tiene como estados asintóticos los estados EPR [15, 16]. Los estados asintóticos son el número mínimo de estados entrelazados que se necesitan para poder formar el estado bipartito que deseamos (ver apartado 6.1). Gracias a este hecho cualquier estado bipartito creado puede compararse con su estado asintótico. De hecho la entropía de entrelazamiento para este tipo de sistemas se conserva [15, 16]. Lo que significa que el entrelazamiento de un estado puro bipartito $|\psi_{AB}\rangle$ es asintóticamente equivalente, bajo operaciones locales, a un estado EPR [11].

5.2 Operaciones LOCC

En este apartado estudiaremos las operaciones locales y comunicaciones clásicas (LOCC). Las operaciones LOCC que tienen como objetivo transformar unos estados en otros para poder realizar distintas tareas y establecer así una clasificación de estados equivalentes LOCC [17]. Imaginemos un estado $|\phi\rangle$ que sabemos puede realizar la tarea X de forma eficaz. Pero nosotros solo tenemos la capacidad de crear estados $|\psi\rangle$. A través de una operación tipo LOCC, implementada por un operador θ, podemos reducir el estado $|\psi\rangle$ al estado $|\phi\rangle$,

$$\theta|\psi\rangle \rightarrow|\phi\rangle. \tag{5.7}$$

Por tanto, hemos conseguido transformar el estado $|\psi\rangle$ en el estado $|\phi\rangle$ y así poder llevar a cabo la tarea X.

Elegimos como ejemplo de nuevo dos estados puros bipartitos que podemos expresar en función a su descomposición de Schmidt como

$$|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i^{\psi}}|i\rangle|i\rangle, \tag{5.8}$$

y

$$|\phi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i^{\phi}}|i\rangle|i\rangle. \tag{5.9}$$

La transformación LOCC podrá darse si sus respectivos coeficientes de Schmidt cumplen la siguiente condición [18, 19],

$$\sum_{j=1}^{k} \lambda_j^{\psi\downarrow} \leq \sum_{j=1}^{k} \lambda_j^{\phi\downarrow}. \tag{5.10}$$

Este teorema fue demostrado por Nielsen en 1999 y es conocido como la condición de mayorización [20]. Entonces diremos que el estado $|\psi\rangle$ es reducible al estado $|\phi\rangle$ mediante una operación LOCC con una probabilidad de éxito igual a uno. Esta transformación se conoce como reducción exacta [19].

La flecha hacia abajo en el superíndice de ambos coeficientes de Schmidt indica que los coeficientes están ordenados en función a su valor en orden descendente.

En general las transformaciones LOCC son de carácter irreversible a no ser que los coeficientes sean iguales, uno a uno, como ocurre en el apartado 5.1 [11]. Si tenemos dos sistemas bipartitos que se encuentran en un estado puro cada uno, diremos que ambos estados son equivalentes LOCC,

$$|\psi\rangle \rightleftharpoons_{LOCC} |\phi\rangle, \tag{5.11}$$

si se cumple que la condición de mayorización, ecuación 5.10, se convierte en una igualdad. En este caso, ambos estados pertenecen a la misma clase o familia de entrelazamiento. Debido a esto, dos estados serán equivalentes LOCC si y solo si son equivalentes LU, ya que la condición de equivalencia es la misma en ambos casos para sistemas puros bipartitos [19].

$$|\psi\rangle \rightleftharpoons_{LOCC} |\phi\rangle \Leftrightarrow |\psi\rangle \rightleftharpoons_{LU} |\phi\rangle. \tag{5.12}$$

Sin embargo, cuando el sistema es tripartito aparecen estados entrelazados que son totalmente inequivalentes bajo transformaciones LOCC. En el caso concreto del sistema tripartito aparecen dos estados inequivalentes conocidos como $|GHZ\rangle$ y $|W\rangle$. Evidentemente cuando pasamos a sistemas multipartitos el número de clases de estados inequivalentes aumenta de forma incontrolada.

5.3 Operaciones SLOCC

Cuando una operación LOCC tiene cierta probabilidad de éxito de reducir un estado en otro esta operación se conoce como SLOCC o, en inglés, Stochastic Local Operations and Classical Communication.

Debemos tener en cuenta que los estados equivalentes bajo transformaciones LOCC también lo son bajo transformaciones SLOCC, ya que las operaciones LOCC están contenidas dentro de las SLOCC [11, 17, 21]. Y por este motivo los estados equivalentes bajo transformaciones LU también son equivalentes SLOCC.

Una operacion SLOCC puede transformar cualquier estado $|\psi\rangle$ en un estado $|\phi\rangle$ con una cierta probabilidad de éxito, finita y distinta de cero, si

$$|\phi\rangle = A \otimes B|\psi\rangle, \tag{5.13}$$

donde A y B son dos operadores que actúan sobre el subsistema A y B de ψ respectivamente. Estos operadores no tienen porque ser unitarios ni estar normalizados. Además también podemos tener una operación SLOCC invertible de forma que,

$$|\psi\rangle = A^{-1} \otimes B^{-1}|\phi\rangle. \tag{5.14}$$

Veamos qué ocurre con los sistemas bipartitos aprovechando que son bien conocidos. Apoyándonos en el hecho de que las operaciones LU están contenidas por las operaciones SLOCC definimos entonces el estado $|\psi_1\rangle$ en función a su descomposción de Schmidt para estados puros. Si tenemos un sistema $\psi \in \mathbb{C}^n \otimes \mathbb{C}^m$ con $n \leq m$ definimos un correspondiente estado bipartito como

$$|\psi_1\rangle = \sum_{i=1}^{n_\psi} \sqrt{\lambda_i^\psi}|i\rangle|i\rangle = \mathrm{U}_A \otimes \mathrm{U}_B|\psi\rangle, \tag{5.15}$$

donde U_A y U_B son dos operadores unitarios. Se cumple que

$$\lambda_i^{\downarrow} > 0 \quad y \quad n_\psi \leq n,$$

donde $\lambda_i^{\downarrow}$ son los coeficientes de Schmidt ordenados por sus valores decrecientes y n_ψ es el número de Schmidt, que resulta ser el número de coeficientes distintos de cero.

A continuación se aplica una operación local inversa (ILO),

$$\frac{1}{\sqrt{n_\psi}}\left(\sum_{i=1}^{n_\psi}\frac{1}{\sqrt{\lambda_i}}|i\rangle\langle i| + \sum_{i=n_\psi+1}^{n}|i\rangle\langle i|\right)\otimes \mathbb{1}_B, \tag{5.16}$$

que no tiene porque ser unitaria, sobre la ecuación 5.15. Lo que se consigue es un estado máximamente entrelazado [11],

$$|ME\rangle_{n_\psi} = \frac{1}{\sqrt{n_\psi}}\sum_{i=1}^{n_\psi}|i\rangle|i\rangle, \tag{5.17}$$

que depende únicamente del número de Schmidt, n_ψ.

Hemos obtenido que para cualquier estado bipartito puro, $|\psi\rangle$, existe una operación local invertible que conecta con el estado máximamente entrelazado para un n_ψ dado. Más aún, si tenemos dos estados bipartitos conectados por un operador invertible serán equivalentes SLOCC si tienen el mismo número de Schmidt. De manera que [11]

$$|\psi\rangle \rightleftharpoons_{SLOCC} |\phi\rangle \text{ cuando } n_\psi = n_\phi. \tag{5.18}$$

Como la dependencia de estados equivalentes reside en el número de Schmidt se puede deducir que tendremos n clases de estados entrelazados. Donde el rango de n va de 1 a n_ψ. En el caso en el que $n_\psi = 1$ es evidente que el estado no está entrelazado, solo tenemos un término en el sumatorio y claramente resulta ser separable.

Cuando dos estados no están conectados por una operación invertible podremos transformarlos, uno en otro, dependiendo del número de Schmidt. Si tenemos dos estados con distinto número de Schmidt el estado $|\psi\rangle$ es reducible por operaciones SLOCC al estado $|\phi\rangle$, con una probabilidad finita, si $n_\psi \geq n_\phi$. Pero en este supuesto los estados no son equivalentes SLOCC.

5.4 3-cúbits y sistemas múltiples

En el caso de tener un sistema compuesto por 3-cúbits se obtienen seis clases inequivalentes, jerarquizadas en tres niveles de potencia de entrelazamiento (ver figura 7). Dos de estas clases no son reducibles, de una a otra, mediante operaciones SLOCC. Estas clases inequivalentes son conocidas como $|GHZ\rangle$ (Greenberger-Horne-Zeilinger) y $|W\rangle$, y se representan por los siguientes estados:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{5.19}$$

y

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle). \tag{5.20}$$

Que los estados $|GHZ\rangle$ y $|W\rangle$ correspondan a clases distintas implica que no pueden ser convertibles bajo transformaciones SLOCC. En la figura 7 podemos ver como los estados superiores pueden transformase bajo operaciones de tipo SLOCC en los estados inferiores. El estado más inferior, $|A - B - C\rangle$, es un estado completamente separable producto de los tres sistemas. Los estados que se encuentran en medio son estados con un entrelazamiento de acuerdo a una bipartición $2 \otimes (2 \otimes 2)$ [22].

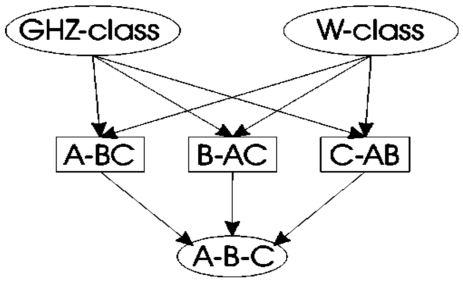

Figura 7: Estados que aparecen en un sistema de 3-cúbits. *(Creds.: EPTCS 52, 2011 [11])*

Los estados que se encuentran a la misma altura representan una jerarquía de potencia de entrelazamiento pero no son equivalentes entre si.

Debido a la existencia de estos dos estados superiores podemos determinar que, si el estado $|\psi\rangle$ podemos convertirlo en el estado $|GHZ\rangle$ y el estado $|\phi\rangle$ podemos transformarlo en $|W\rangle$, entonces la probabilidad de transformar $|\psi\rangle$ en $|\phi\rangle$ es muy pequeña [11].

Una característica reseñable del estado $|GHZ\rangle$ (estado entrelazado y puro) es que es el estado de 3-cúbits que posee el grado máximo de entrelazamiento. Sin embargo, si por cualquier perturbación perdemos la información de uno de los 3-cúbits, el estado resultante es totalmente separable y ya no nos quedaría un estado entrelazado. Podemos ver esto con el siguiente ejemplo. Si realizamos la traza sobre el cúbit etiquetado con el número 3 tenemos que,

$$\rho_{12} = \mathrm{Tr}_3(|GHZ\rangle\langle GHZ|) = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) \tag{5.21}$$

y si realizamos otra traza sobre otro cúbit se obtiene que,

$$\rho_1 = \rho_2 = \rho_3 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|). \tag{5.22}$$

El estado $|GHZ\rangle$ pasa de ser un estado puro entrelazado a un estado mezcla y separable. Por este motivo el estado $|GHZ\rangle$ se considera un estado frágil.

Por otro lado, el estado $|W\rangle$ es un estado más robusto ya que se mantiene entrelazado aun cuando se pierda la información de un cúbit. Cuando realizamos la traza parcial

sobre un cúbit se obtiene que,

$$\rho_{12} = \mathrm{Tr}_3(|W\rangle\langle W|) = \frac{1}{3}(|00\rangle\langle 00|+|01\rangle\langle 01|+|01\rangle\langle 10|+|10\rangle\langle 01|+|10\rangle\langle 10|) \tag{5.23}$$

donde el estado se mantiene entrelazado. Si realizamos otra traza sobre otro cúbit obtenemos que,

$$\rho_1 = \rho_2 = \rho_3 = \frac{1}{3}(2|0\rangle\langle 0|+|1\rangle\langle 1|) \tag{5.24}$$

donde aparece un estado mezcla separable.

En el caso de 4-cúbits no nos sorprende que la clasificación sea más compleja. En concreto, las infinitas clases no equivalentes que aparecen forman una familia de estados continua que a su vez pueden dividirse en nueve subfamilias cualitativamente diferentes.

Finalmente para el caso general de n-cúbits aparecerán infinitas clases no equivalentes, con sus respectivas familias, subfamilias, etc...

6 Medidas del entrelazamiento

La utilidad que ofrece un estado cuántico, como un recurso eficiente para realizar determinadas tareas, está definida de forma cuantitativa en función al grado de entrelazamiento que presenta el estado en cuestión. Hasta ahora hemos visto como clasificar los distintos estados en base a su equivalencia por el entrelazamiento pero no hemos cuantificado el entrelazamiento de estos estados.

Además, resulta razonable pensar que la mayoría de los estados cuánticos, en particular los entrelazados, van a estar en situaciones de estados mezcla en vez de puros, ya que en la naturaleza los estados son mezcla. Por lo que nace la necesidad de poder cuantificar el entrelazamiento que presentan ambas tipologías de sistemas, puros y mezcla. Dependiendo del estado en el que se encuentre nuestro sistema cuántico el grado de entrelazamiento se medirá con distintos métodos.

6.1 Entropía de entrelazamiento

Una de las herramientas de medición más extendidas para sistemas en estado puro es el cálculo de la entropía de von Neumann. Se hace razonable asumir que la medida del grado de entrelazamiento de un sistema no resulta ser trivial, sin embargo, se pueden generalizar tres propiedades que todo sistema entrelazado debe cumplir:

1. El entrelazamiento, E, se conserva cuando se realizan operaciones de tipo LU [23].
2. El entrelazamiento, E, no aumenta con las operaciones LOCC [23]. En general el entrelazamiento, E, disminuirá.
3. El entrelazamiento, E, desaparece en los estados separables o factorizables. Es decir, la cantidad de entrelazamiento es cero $(E = 0)$. Esta propiedad es razonable dado que estamos definiendo entrelazamiento como no separabilidad.

Además, sabemos que también existen los estados con un grado de máximo entrelazamiento. Es interesante saber si para asegurar el correcto funcionamiento de los procesos que utilizan el recurso del entrelazamiento, como teletransporte, criptografía cuántica, codificación densa..., los estados deben ir siempre de forma que el entrelazamiento sea máximo, o por el contrario, pueden ser sustituidos por estados de entrelazamiento parcial y, de esta forma, conocer la relación que existe entre ambos tipos.

Para ello, imaginemos que Alice y Bob se encuentran en dos localidades distanciadas. Ambos quieren compartir en un momento dado n pares de partículas entrelazadas en el estado $|\psi\rangle$. Ya sabemos que esto no puede realizarse mediante los sistemas de comunicación clásicos. Por lo que, o bien Alice o bien Bob deben preparar los n pares de cúbits entrelazados. Si Alice fuese quien los preparase después debería enviar un miembro de cada par a Bob. Esto supone que Alice debe enviar los n pares de partículas pero, ¿existe un modo más eficiente de conseguir lo mismo sin necesidad de tener que enviar los n pares?. La respuesta es sí. Una vez que Alice tiene los n pares, puede ver cómo comprimirlos para mandárselos a Bob de manera que cuando Bob los reciba este sea capaz de reconstruir los n pares que Alice quería mandarle al inicio [8].

A partir de aquí el objetivo es calcular el número mínimo de cúbits entrelazados en estado singlete que hay que enviar comprimidos para que al descomprimir la información vuelva a su estado original. El valor máximo de compresión de n pares de cúbits entrelazados se conoce como compresión asintótica. Para que este valor sea alcanzable es preciso que el número de pares entrelazados n sea muy grande. De esta forma se obtiene un rendimiento en el proceso con un valor de $nE - O(\log_2 n)$ [16]. Además, se necesita que n sea grande para asegurar que el estado enviado se puede reconstruir, así como todas sus propiedades. Una de estas propiedades es la entropía de entrelazamiento.

Para un estado cualquiera,

$$|\psi\rangle = a|00\rangle + b|11\rangle, \tag{6.1}$$

podemos calcular el factor de compresión mínimo haciendo uso de la definición de la entropía de von Neumann,[24]

$$S(\rho) = -\mathrm{Tr}(\rho \ \log_2 \ \rho) \text{ donde, } \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{6.2}$$

Si aplicamos la ecuación 6.2 sobre el estado $|\psi\rangle$ obtenemos [8]

$$S = -(|a|^2 \log_2 |a|^2 + |b|^2 \log_2 |b|^2), \text{ donde } S \leq 1, \tag{6.3}$$

siendo S el valor de la entropía de entrelazamiento, que nos indica el valor de compresión asintótico, para un sistema puro descrito por el estado $|\psi\rangle$. Esto es, para un n muy grande, basta con que Alice le envíe Sn cúbits a Bob.

Derivado de la entropía se define el grado de entrelazamiento de cualquier sistema bipartito en estado puro es el número mínimo asintótico de cúbits por par que se deben enviar, para poder reconstruir todos los pares en el estado deseado.

En el caso del estado $|\psi\rangle$ el grado de entrelazamiento y el valor de la entropía es el mismo, E=S. Generalizando, si tenemos un estado,

$$|\phi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \tag{6.4}$$

el grado de entrelazamiento viene descrito como

$$E = \mathrm{H}\left(\frac{1+\sqrt{1-\tau}}{2}\right) \text{ donde, } 0 \leq E \leq 1, \tag{6.5}$$

con

$$\mathrm{H}(x) = -(x\log_2 x + (1-x)\log_2(1-x)) \tag{6.6}$$

y

$$\tau = 4|ad - bc|^2. \tag{6.7}$$

Tanto el entrelazamiento, E, como el enlace (tangle), τ, son indicadores del grado del entrelazamiento. En el apartado 6.4 veremos con más detalle el enlace, τ. Lo que distingue el entrelazamiento, E, del enlace, τ, es que el entrelazamiento tiene un significado físico, mientras que el enlace es una función de las componentes del estado. Por otro lado, la función $\mathrm{H}(x)$ es la función de entropía binaria [8, 25].

El proceso por el cual se define el grado de compresión de pares con entrelazamiento máximo se conoce como "concentración del entrelazamiento". La dependencia viene determinada de forma que a mayor compresión mayor grado de entrelazamiento. Si la compresión adquiere su valor máximo entonces el grado de entrelazamiento también lo será. Es por este motivo que nos van a interesar estados entrelazados puros con máximo grado de entrelazamiento en los procesos de transmisión de información.

6.2 Entrelazamiento de formación

Ya se ha mencionado a lo largo del trabajo que los estados cuánticos con los que nos vamos a encontrar en la naturaleza van a ser estados mezcla. Bien porque provienen de la combinación de estados que no son en su totalidad mezcla, o bien porque existe algo más desconocido que también está entrelazado con el sistema.

Cuando tenemos un estado mezcla no existe una única forma de medir el grado de entrelazamiento del sistema. Cuantificar el estado de entrelazamiento de un sistema mezcla es sustancialmente más complicado que cuando tratamos con estados puros. La unidad fundamental que se va a usar son los estados singletes [25].

El entrelazamiento de formación para un estado mezcla, descrito por su matriz densidad ρ, es el número mínimo de estados singlete que se necesitan para generar ρ ensamblando sistemas que se encuentran en estados puros [25].

La cuestión que difiere respecto de los sistemas en estado puro es que el número de singletes puros que necesitamos para construir un estado total mezcla (entrelazamiento de formación) es distinto al número de singletes en estado puro que se pueden extraer

de un estado total mezcla (entrelazamiento destilable). En el caso de sistemas puros el entrelazamiento de formación y el entrelazamiento destilable son iguales.

En el caso del entrelazamiento de formación debemos tener en cuenta todas las posibilidades para construir, a través de estados puros, el estado total descrito por la matriz de densidad ρ. Por lo que, dado un sistema bipartito en el estado mezcla, ρ, se deberán considerar todas las posibilidades que tenemos para construir el estado ρ a través de estados singletes puros. Por ejemplo, si tenemos los estados $|\psi_i\rangle$ y les asignamos una probabilidad p_i a cada uno,

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|. \tag{6.8}$$

Tenemos infinitas formas de construir el estado mezcla pero elegiremos la que minimiza el número de estados singlete.

Por tanto, el entrelazamiento de formación, $E(\rho)$, se define como el valor mínimo de entrelazamiento sobre todas las descomposiciones posibles del estado mezcla en una combinación de estados puros,

$$E(\rho) = \min \sum_i p_i E(\psi_i), \tag{6.9}$$

siendo $E(\psi_i)$ el valor de entrelazamiento de cada estado puro $|\psi_i\rangle$ [23].

Al igual que en los estados puros, el entrelazamiento de formación deberá ser cero si el estado mezcla puede expresarse como una combinación de productos tensoriales de los estados que lo componen. Además, el entrelazamiento de formación para un estado bipartito puro es igual a la entropía de von Neumann, definida en la ecuación 6.2.

Es importante resaltar que el valor de E para muchos estados mezcla es desconocido, incluso para estados de dos cúbits. Además, no es nada intuitivo que se pueda expresar el grado de entrelazamiento como una función de la matriz densidad [25].

6.3 Entropía relativa del entrelazamiento

Desde el punto de vista de la inferencia estadística, la entropía cuántica relativa es un buen método de medición para distinguir entre dos estados cuánticos, incluso entre dos clases de estados [18, 26, 27].

La entropía cuántica relativa entre dos estados σ y ρ es por definición

$$S(\sigma||\rho) := \mathrm{Tr}(\sigma \ln \sigma - \sigma \ln \rho), \tag{6.10}$$

donde $S(\sigma||\rho)$ es una medida de la distinguibilidad entre el estado ρ y σ.

Suponemos que tenemos dos estados, σ y ρ, y queremos distinguirlos. Para ello usamos un conjunto de operadores de valores positivos (POVM, pag. 8), $\{M_i\}$.,

$$\sum_{i=1}^{m} M_i = \mathbb{1}, \tag{6.11}$$

que genere distintas distribuciones de probabilidad para cada estado,

$$p_i = \text{Tr } M_i\sigma \tag{6.12}$$

y

$$q_i = \text{Tr } M_i\rho. \tag{6.13}$$

Entonces, la entropía relativa de entrelazamiento es

$$S(p_i||q_i) = \sum_i \left(p_i \ln p_i - p_i \ln q_i\right). \tag{6.14}$$

La complejidad viene a la hora de determinar el operador que mejor distinga ambos estados. Se define la entropía relativa de entrelazamiento como

$$S_1(\sigma||\rho) := \sup\left[A\left(\sum_i \left(\text{Tr}(M_i\sigma)\ln(\text{Tr}(M_i\sigma)) - \text{Tr}(M_i\sigma)\ln(\text{Tr}(M_i\rho))\right)\right)\right], \tag{6.15}$$

donde el valor superior es elegido entre todos los resultados que se obtienen al aplicar el conjunto de los operadores $\{M_i\}$ y A es una constante. El resultado determina el POVM que más distingue en sus valores al aplicarse sobre el estado σ y ρ.

Si ahora tenemos N copias de los estados σ y ρ,

$$\sigma^N = \sigma\otimes\sigma\otimes\cdots\otimes\sigma \quad y \quad \rho^N = \rho\otimes\rho\otimes\cdots\otimes\rho, \tag{6.16}$$

aplicamos los operadores según la ecuación 6.11 sobre σ^N y ρ^N. La entropía relativa de entrelazamiento ahora es

$$S_N(\sigma||\rho) := \sup\left[A\left(\frac{1}{N}\sum_i \left(\text{Tr}(M_i\sigma^N)\ln(\text{Tr}(M_i\sigma^N)) - \text{Tr}(M_i\sigma^N)\ln(\text{Tr}(M_i\rho^N))\right)\right)\right]. \tag{6.17}$$

La siguiente desigualdad viene demostrada en el artículo de Hiai & Petz 1991 [28],

$$S(\sigma||\rho) \geq S_N \tag{6.18}$$

donde si $N\to\infty$ entonces la entropía cuántica relativa será

$$S(\sigma||\rho) = \lim_{N\to\infty} S_N. \tag{6.19}$$

La entropía cuántica relativa es una cantidad que nos va a indicar la "distancia" a la que se encuentran dos estados distintos de forma que podamos distinguirlos. Es una medida de distinguibilidad entre estados.

Para entender el resultado mejor ponemos el siguiente ejemplo. Tenemos dos estados, uno es un estado de Bell, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, y otro es un estado mezcla, $\rho = \frac{1}{2}(|00\rangle\langle 00|+|11\rangle\langle 11|)$. Elegimos realizar N proyecciones sobre el estado $|\phi^+\rangle$. Por lo que hemos elegido como operador el proyector $|\phi^+\rangle\langle\phi^+|$. Si el estado con el que estamos tratando es el estado de Bell siempre obtendremos el mismo resultado al proyectarlo. Sin embargo, si lo que tenemos es el estado mezcla ρ, en un 50 % de los casos tendremos como resultado el estado $|\phi^+\rangle$ y el otro 50 % el estado $|\phi^-\rangle$ [26, 27]. Hay que tener en cuenta que no conocemos el estado que estamos proyectando.

6.4 τ - tangle o enlace

Una de las propiedades descubiertas en el año 2000 por V. Coffman et al. fue que el entrelazamiento es monógamo [29]. Según esta característica si los sistemas Alice y Bob se encuentran entrelazados, Alice tiene una limitación a la hora de compartir información con el sistema Charlie. Más aún, si Alice y Bob están máximamente entrelazados, Alice no puede entrelazarse con Charlie. Esta propiedad resulta ser muy interesante sobre todo en procesos de criptografía cuántica.

Para entender la propiedad de monogamia necesitamos entonces poder estudiar los distintos enlaces que pueden surgir entre sistemas multipartitos. El enlace (tangle) de un sistema bipartito descrito por ρ_{AB} se denota como $\tau(\rho_{AB})$ [17, 18, 30] y su definición es

$$\tau(\rho_{AB}) = C^2(\rho_{AB}) \text{ donde, } \rho_{AB} = \sum_i p_i \rho_A \otimes \rho_B \tag{6.20}$$

y $C^2(\rho_{AB})$ es el cuadrado de la concurrencia.

El cálculo de la concurrencia podemos asimilarlo al siguiente proceso. Se prepara un estado y se le aplica una operación antiunitaria de inversión temporal. La concurrencia es la proyección de este estado modificado sobre un estado igual al preparado inicialmente, al que no se le ha aplicado ninguna operación.

En concreto, para estados puros bipartitos la concurrencia es

$$C(\psi) = 2|ad - cd| = |\langle\psi|\sigma_y \otimes \sigma_y|\psi^*\rangle| \tag{6.21}$$

donde,

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \tag{6.22}$$

y

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{6.23}$$

La concurrencia es un cálculo del entrelazamiento del estado, no una operación física. Podemos ver la relación entre el entrelazamiento y la concurrencia de la siguiente forma. El estado $|\psi\rangle$ es factorizable cuando $ad - bc = 0$ por lo que esta cantidad nos está dando una medida del entrelazamiento. Si se cumple que $ad = bc$ el entrelazamiento es cero y la concurrencia también (ver ecuación 6.21) [31].

Para estados mezcla, al igual que en el apartado 6.2 (entrelazamiento de formación), se define la concurrencia de un sistema bipartito en un estado mezcla ρ como el valor de la concurrencia que da como resultado de la elección del conjunto de estados puros mínimos que representan el estado ρ [31]. Entonces,

$$C(\rho) = \inf \sum_i p_i C(\psi_i) \text{ donde, } \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{6.24}$$

Usando el último resultado se define el enlace como

$$\tau(\rho) = \inf \sum_i p_i C^2(\psi_i). \tag{6.25}$$

En el caso de estados mezcla de dos cúbits se puede demostrar que la concurrencia es [32]

$$C(\rho) = \max\{0, \sqrt{r_1} - \sqrt{r_2} - \sqrt{r_3} - \sqrt{r_4}\}, \tag{6.26}$$

donde r_1, r_2, r_3 y r_4 [17, 32] son los autovalores de la matriz

$$R = \rho(\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y). \tag{6.27}$$

Imaginemos que tenemos un sistema tripartito con los subsistemas, A, B y C. Queremos calcular el valor de los enlaces de las biparticiones, $A : B$ y $A : C$, donde ignoramos el no mencionado en cada caso. Para después compararlos con el enlace de la bipartición que resulta de la agrupación BC, sin ignorar ninguno, $A : BC$. Se puede comprobar que aparece la siguiente desigualdad

$$\tau(A : B) + \tau(A : C) \leqslant \tau(A : BC), \tag{6.28}$$

conocida como la relación de monogamia [29].

Si el estado se define como,

$$\begin{aligned} |\Psi\rangle &= a_{000}|000\rangle + a_{001}|001\rangle + a_{010}|010\rangle + a_{011}|011\rangle \\ &+ a_{100}|100\rangle + a_{101}|101\rangle + a_{110}|110\rangle + a_{111}|111\rangle, \end{aligned} \tag{6.29}$$

entonces los enlaces de los sistemas bipartitos $A : B$ y $A : C$ se calculan con la ecuación 6.20. Pero el enlace del subsistema $A : BC$ se calcula según la siguiente ecuación,

$$\tau(A : BC) = 2\left|\sum a_{imn}\overline{a}_{jmn}a_{i'pq}\overline{a}_{j'pq} \times \epsilon_{ii'}\epsilon_{jj'}\right|, \tag{6.30}$$

donde las barras indican el complejo conjugado, la suma se realiza sobre todos los índices cuyos posibles valores son 0 o 1 y los objetos ϵ_{ij} son el tensor de Levi-Civita en dos dimensiones.

Podemos definir entonces una cantidad

$$\tau_{res} = \tau(A : BC) - \tau(A : B) - \tau(A : C), \tag{6.31}$$

conocida como enlace residual. Cuando se calcula τ_{res} se observa que puede darse una expresión cerrada a esta cantidad,

$$\tau_{res} \equiv \tau(ABC) = 2\left|\sum a_{ijk}a_{i'j'm}a_{npk'}a_{n'p'm'} \times \epsilon_{ii'}\epsilon_{jj'}\epsilon_{kk'}\epsilon_{mm'}\epsilon_{nn'}\epsilon_{pp'}\right|, \tag{6.32}$$

donde se está midiendo el enlace compartido por los tres subsistemas. Esta cantidad es simétrica bajo permutaciones en los índices.

Lo importante de la ecuación 6.31 es que la cantidad que establece la igualdad es un término que hace referencia, exclusivamente, al enlace del sistema tripartito. Además, debido a la desigualdad (ecuación 6.28) existe un valor límite para el enlace tripartito, τ_{ABC} [29, 30].

V. Coffman et al. propusieron que el enlace para sistemas multipartitos podría satisfacer la siguiente desigualdad [18, 29, 30]

$$\tau(A:B)+\tau(A:C)+\tau(A:D)+...\leqslant\tau(A:BCD...), \tag{6.33}$$

donde la suma de los enlaces de subsistemas bipartitos es menor que el enlace del subsistema A con el resto de subsistemas formando un colectivo. Este resultado fue demostrado por Osborne & Verstraete [30].

7 Conclusiones

El estudio realizado al entrelazamiento cuántico, a lo largo de todo el trabajo, ha puesto de manifiesto las numerosas características y propiedades que lo forman, dejando en evidencia el gran recurso que puede llegar a ser en procesos de comunicación, computación y criptografía cuántica. Este era el objetivo principal que se pretendía alcanzar desde el inicio.

La mecánica cuántica establece la base matemática necesaria para poder desplegar los sistemas cuánticos sobre un espacio adecuado. Hemos indicado como el espacio de Hilbert es el espacio vectorial lineal diseñado para que estos sistemas habiten. Además, se ha definido un cúbit como un sistema cuyo estado se puede representar según la esfera de Bloch. Los cúbits pueden estar en estados superpuestos a diferencia de los bits clásicos. Para sistemas multipartitos la capacidad de los sistemas cuánticos de superponer estados hace que surjan los estados entrelazados. Pero se debe recordar que no todo estado superpuesto está entrelazado. La principal forma de clasificar si un estado está entrelazado o no es mirando si puede factorizarse. Por tanto, un estado entrelazado es aquel que no puede factorizarse como un producto tensorial de estados. Sin embargo, comprobar si el estado está entrelazado, o no, no es una tarea sencilla.

En la mayoría de los apartados del trabajo se han estudiado las características y propiedades de los estados entrelazados de sistemas bipartitos, en particular de dos cúbits. Los estados entrelazados que surgen de este tipo de sistemas son conocidos como estados EPR.

Una vez definidos los estados entrelazados se han comentado tres usos del entrelazamiento: distribución cuántica de claves, teletransporte (demostración del Principio de no-clonación) y algoritmo de Shor. Los tres son un claro ejemplo de las grandes posibilidades que ofrece el entrelazamiento a la hora de establecer comunicaciones seguras u optimizar procesos. Se podían haber elegido otros ejemplos pero la intención era la de exponer uno por cada rama de estudio, criptografía, comunicación y computación cuántica.

Lo interesante resulta ser que no todos los estados entrelazados se comportan de igual forma ante una misma tarea o proceso. Es por esto que es necesario estudiar las distintas formas de poder determinar si dos estados entrelazados son o no equivalentes. De esta forma se pueden elegir distintos estados en función a las tareas a realizar. Decir que dos

estados son equivalentes es lo mismo que asegurar que esos dos estados van a ser capaces de realizar las mismas tareas. Para clasificar estas equivalencias entre estados se ha estudiado el uso de operaciones locales. En concreto se han identificado las operaciones LU, LOCC y SLOCC. Para sistemas de dos cúbits se obtiene una única clase de estados equivalentes (estados EPR). Para sistemas de tres cúbits se obtienen seis clases. A partir de cuatro cúbits en adelante surgen infinitas clases de estados equivalentes. Hoy en día la clasificación de familias y clases equivalentes es todo un reto en sistemas multipartitos.

Por último se han identificado cuatro medidas para cuantificar el grado de entrelazamiento de estados. En concreto, se ha estudiado la entropía de entrelazamiento (estados puros), el entrelazamiento de formación, entropía relativa de entrelazamiento y el enlace (tangle). La medida del entrelazamiento es una cantidad muy útil ya que define la eficiencia de un estado al realizar una tarea. Es de forma indirecta la medida de la capacidad del entrelazamiento como recurso.

Una propiedad del entrelazamiento muy interesante es la monogamia. Debido a esta propiedad existe una limitación a la hora de establecer enlaces entre los distintos subsistemas. Es decir, la cantidad de enlace entre los distintos subsistemas está acotado por un valor. También ha quedado en evidencia que el entrelazamiento, sobretodo en sistemas multipartitos mezcla, sigue siendo una incógnita en aspectos tan simples como la medición del grado de entrelazamiento o incluso a la hora de definir si los estados están entrelazados, o no.

Desde un punto de vista físico, el entrelazamiento puede proporcionarnos las herramientas necesarias, tanto en comunicación como en computación cuántica, para poder desentrañar cuestiones de la naturaleza para sistemas muy pequeños y muy complejos. A priori, sin estas herramientas no seríamos capaces de abordar tales escenarios.

No cabe la menor duda de que aún queda mucho por investigar y, a medida que se vayan esclareciendo y respondiendo a distintas cuestiones, más cerca estaremos de poder utilizar el entrelazamiento como un recurso que alcance su máximo potencial.

Referencias

[1] Punset, E. (Director). (2011). Redes - La incertidumbre del universo cuántico [programa de televisión]. Universidad de Oxford, Reino Unido: rtve.

[2] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Communication*, Cambridge University Press, Cambridge, 2000.

[3] J.J. Sakurai and J.J. Napolitano, *Modern Quantum Mechanics*, Pearson Education Inc., 2011.

[4] A. Streltsov, *Quantum Correlations Beyond Entanglement*, Springer, 2015.

[5] D. Bouwmeester, A.K. Ekert and A. Zeilinger, *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, Springer, New York, 2000.

[6] A.K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661, 1991.

[7] C.H. Bennett and S.J. Wiesner, *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Phys. Rev. Lett. **69**, 2881, 1992.

[8] W.K. Wootters, *Quantum entanglement as a quantificable resource*, Phil. Trans. R. Soc. Lond. A **356**, 1717, 1998.

[9] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Quantum Cryptography*, Rev. Mod. Phys. **74**, 145, 2002.

[10] P.W. Shor, *Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer*, Siam Review Vol. **41**, 303, 1999.

[11] W. Dür, G. Vidal and J.J. Cirac, *Three qubits can be entanglement in two inequivalent ways*, Phys. Rev. A **62**, 062314, 2000.

[12] W. Dür and J. I. Cirac, *Equivalence classes of non-local unitary operations*, Quant. Inf. Comput. **2**, 240, 2002.

[13] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van Den Nest and H.J. Briegel, *Entanglement in Graph States and its Applications*, Proceedings of the International School of Physics Enrico Fermi Vol. **162**, 115, 2006 DOI: 10.3254/978-1-61499-018-5-11.

[14] R. Horodecki, P. Horodecki, M., Horodecki and K. Horodecki, *Quantum entanglement*, Rev. Mod. Phys. Vol. **81**, 2009.

[15] G. Vidal, W. Dür, J.I. Cirac, *Reversible combination of inequivalent kinds of multipartite entanglement*, Phys. Rev. Lett. **85**, 658, 2000.

[16] C.H. Bennett, H.J. Bernstein, S. Popescu, B. Schumacher, *Concentrating Partial Entanglement by Local Operations*, Phys. Rev. A **53**, 2046, 1996.

[17] C. Eltschka and J. Siewert, *Quantifying entanglement resources*, J. Phys. A: Math. Theor. **47**, 424005, 2014.

[18] M.B. Plenio and S. Virmani, *An introduction to entanglement measures*, Quant. Inf. Comput. **7**, 1, 2007.

[19] C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin and A.V. Thapliyal, *Exact and asymptotic measures of multipartite pure-state entanglement*, Phys. Rev. A **63**, 012307, 2000.

[20] M.A. Nielsen, *Conditions for a Class of Entanglement Transformations*, Phys. Rev. Lett. **83**, 436, 1999.

[21] A. Miyake, *Multipartite Entanglement under Stochastic Local Operations and Classical Communication*, Int. J. Quant. Info. **2**, 65, 2004.

[22] B. Coecke and B. Edwards, *Three qubit entanglement within graphical Z/X-calculus*, EPTCS **52**, 22, 2011.

[23] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. A **54**, 3824, 1996.

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

[25] S. Hill and W.K.Wootters, *Entanglement of a Pair of Quantum Bits*, Phys. Rev. Lett. **78**, 5022, 1997.

[26] V. Vedral and M.B. Plenio, *Entanglement measures and purification procedures*, Phys. Rev. A **57**, 1619, 1998.

[27] V. Vedral, M.B. Plenio, K. Jacobs and P.L. Knight, *Statistical inference, distinguishability of quantum states and quantum entanglement*, Phys. Rev. A **56**, 4452, 1997.

[28] F. Hiai and D. Petz, *The proper formula for relative entropy and its asymptotics in quantum probability*, Commun. Math. Phys. **143**, 99, 1991.

[29] V. Coffman, J. Kundu and W.K. Wootters, *Distributed entanglement*, Phys. Rev. A **61**, 052306, 2000.

[30] T.J. Osborne and F. Verstraete, *General Monogamy Inequality for Bipartite Qubit Entanglement*, Phys. Rev. Lett. **96**, 220503, 2006.

[31] W.K. Wootters, *Entanglement of Formation and Concurrence*, Quant. Inf. Comput. **1**, 27, 2001.

[32] W.K. Wootters, *Entanglement of Formation of an Arbitrary State of Two Qubits*, Phys. Rev. Lett. **80**, 2245, 1998.