Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional

Departamento de Computación

# Simulación de protocolos de comunicación eficientes basados en estados entrelazados

Tesis que presenta

**William de la Cruz de los Santos**

para obtener el grado de

**Maestro en Ciencias en**
**la Especialidad de Ingeniería Eléctrica**

Director de Tesis

**Dr. Guillermo Morales Luna**

México, D.F. Agosto 2007

# Agradecimientos

Al Consejo Nacional de Ciencia y Tecnología por la beca otorgada para poder realizar los estudios de maestría. Al Centro de Investigación y de Estudios Avanzados del IPN, por la calidad de las instalaciones y ambiente estudiantil. A la Biblioteca de Ingeniería Eléctrica por haber proporcionado sus materiales de consulta durante el transcurso de la maestría.

A mi asesor el Dr. Guillermo Morales-Luna, por su valiosa asesoría y enseñanza que desde los primeros cursos en la maestría impartió, y también por su peculiar manera de explicar, traduciendo problemas complicados en cosas cotidianas.

A los Drs. Francisco Rodríguez Henríquez y Debrup Chakraborty, por sus valiosos comentarios durante la revisión del documento de tesis.

En especial a mis padres que siempre me apoyaron en mis estudios, que sin sus esfuerzos no hubiera sido posible estar aquí. Y sin olvidarlo a mi hermano Fredy que me ayudo de una u otra forma con mis trámites.

También a todos los amigos que tuve la fortuna de conocer y que hicieron más amena la estadía de estudios. En especial a mi hermano Fredy que me ayudo de una u otra forma con mis trámites.

# Resumen

Los estados cuánticos *entrelazados* constituyen una fuente de varios esquemas de procesamiento y de comunicación, cuya formalización resulta en vectores en espacios de Hilbert. Un problema de decisión fundamental es saber si dado un vector en un espacio de Hilbert se puede representar como producto tensorial de vectores con dimensión más pequeña. A estos estados se les llama *separables*, y a los que no lo sean, *estados entrelazados*. La no-separabilidad es origen y a la vez consecuencia de la correlación que guardan las componentes de los vectores entrelazados con respecto a la toma de mediciones, es decir, al efecto de no-localidad que puede manifestar el proceso de medición en estados entrelazados, donde sistemas que interactuaron en un inicio siguen haciéndolo aún después de ser distanciados físicamente. Esta propiedad ha sido ampliamente usada en comunicación cuántica como los protocolos de distribución de llaves secretas, y en comunicación directa segura, entre otras aplicaciones. En algunos protocolos sólo intervienen dos partes en la comunicación tal como en el protocolo de *códigos superdensos*, y ha sido de importancia considerar su generalización a más de dos partes. Otro problema de interés es la *simulación del entrelazamiento*, haciendo uso de canales de comunicación convencionales para el envío de mensajes, de manera que reproduzca el mismo escenario de medición cuántico. Estos son los principales problemas que se consideran en esta tesis.

# Abstract

The *entangled quantum states* are in the origin of several processing and communication schemes. They are formalized as vectors in Hilbert spaces. A basic decision problem is to recognize whether a given vector in a Hilbert space can be separated (or factored) as the tensor product of any vectors with lower dimensionality. Opposite to the so called *separable states* are the entangled states which do not allow any separation. Non-separability is cause and consequence of the correlation shown by the components in entangled vectors under measurements. Indeed the measurements of components in entangled states posses a notion of non-locality: originally interacting systems maintain their interaction even if the components are physically located far from each other. This property has been widely used in quantum communication protocols as Quantum Key Distribution (QKD), Quantum Secure Direct Communication (QSDC), Quantum Secret Sharing (QSS), etc. In some of these protocols only two parts in the communication process take place, as in the Quantum Dense Coding protocol, thus it is rather important to consider their generalizations for more than two parts. Another important problem is the simulation of entanglement using conventional communications channels for message transmission, in such a way that exactly the same quantum measurements scenario is reproduced. These problems are the main topics considered in this thesis.

# Índice general

# Índice de figuras

# Índice de tablas

# Capítulo 1

# Introducción

## 1.1. Planteamiento del problema

En la teoría de la computación ha habido cambios importantes en cuanto a sus fundamentos, uno de los principales fue la contribución de Alan Turing en los años 50's, con el modelo de computación de la *máquina de Turing* (MT) y la definición de los conceptos de algoritmo. Esta formalización concluyó con la tesis Church-Turing que dice: *es Turing-computable aquello computable por una máquina de Turing*. Posteriormente Feynman en 1982, notó que la simulación de un sistema mecánico cuántico sobre una computadora ordinaria es exponencialmente lento, por lo que sugiere un nuevo modelo de computación conocido como la *Máquina de Turing Cuántica* (MTC), cuya ejecución sigue las leyes de la física cuántica. Este modelo fue formulado por Deutsch en 1985 y después mejorado por Bernstein y Vazirani en 1993, aunque este último es muy parecido al modelo de la *Máquina de Turing Probabilística* (MTP).

Antes de la formulación de la MTC se había probado la existencia de problemas que no se pueden resolver en tiempo polinomial sobre un modelo clásico de la MT o la MTP. Sin embargo, tienen una solución eficiente y elegante empleando el modelo de la MTC, que demuestra Peter Shor en 1995 [1], resolviendo el problema de factorización de enteros en tiempo polinomial empleando un modelo de computación cuántico. Otros ejemplos son el algoritmo cuántico propuesto por Lov Grover en 1996 [2], para la búsqueda en una secuencia no ordenada de datos con $N$ componentes en tiempo lineal y anteriormente el algoritmo propuesto por David Deutsch y Richard Jozsa en 1992, para decidir si una función booleana es constante o balanceada en un sólo paso de computación.

Desde la aparición de la computación cuántica se han desarrollado esquemas de computación, tal como las compuertas y circuitos cuánticos, como una forma análoga a las computadoras clásicas. En un algoritmo cuántico la unidad de procesamiento es el qubit o bit cuántico que forma parte de un registro cuántico. Con mucha frecuencia se presenta el problema de factorización o separación de registros. Este problema es llamado separación de registros cuánticos, y es de fundamental importancia en el tratamiento de la información en un algoritmo cuántico, en particular en la toma de

mediciones. A diferencia de una computadora clásica, la información en una computadora cuántica no puede ser medida sin alterar sus estados, ya que al llevar a cabo una medición los estados colapsan a estados determinados, destruyendo el cómputo realizado.

Dentro de los estados cuánticos existen los *estados entrelazados*. Son aquellos estados que exhiben propiedades de medición no locales, es decir, que la medición de uno de sus elementos afecta a los otros. Este fenómeno es empleado en la implementación de protocolos de comunicación, en la distribución de llaves secretas y en esquemas de seguridad. Existen protocolos de comunicación cuánticos que superan en complejidad a los esquemas clásicos, como el propuesto por Bennett y Wiesner en 1992 [3], se trata de un protocolo de dos partes, una parte que envía y otra que decodifica, donde se logra codificar dos bits por bit cuántico.

Estos son los problemas que se abordan en este trabajo de tesis, por un lado la factorización de registros cuánticos y por otro la exploración de algunos esquemas de comunicación cuánticos. También el problema de la toma de mediciones de registros cuánticos empleando la factorización y por último una pequeña exploración de la simulación de algoritmos cuánticos y su complejidad.

## 1.2. Marco teórico

El área en la que se centra el presente trabajo de tesis es el tratamiento de los sistemas cuánticos y de su aplicación en el cómputo y esquemas de comunicación. El cómputo cuántico es parte de la mécanica cuántica que describe modelos matemáticos para llevar a cabo el procesamiento de las entidades cuánticas. En particular el problema de separación de registros cuánticos abarca el tratamiento y representación de espacios vectoriales, así como su uso en la toma de mediciones, una de las operaciones fundamentales en un sistema cuántico.

En cuanto a los protocolos de comunicación cuánticos, se relaciona muy fuertemente con la teoría de complejidad de las comunicaciones y la teoría de la información. Y actualmente al área llamada Complejidad en la comunicación cuántica, introducida por Andrew Yao en 1979, cuyas primeras contribuciones aparecieron en [4], demostrando que la comunicación cuántica puede ser más eficiente que la comunicación clásica. También en [5] se prueba que la comunicación cúantica puede ser exponencialmente mejor que la clásica, en un modelo libre de errores.

### 1.2.1. Breve introducción a la computación cuántica

Cuando se habla de un sistema cuántico es natural relacionarlos con espacios vectoriales de Hilbert [6]. Un espacio de Hilbert, se define sobre el campo de los complejos, que tiene definido un producto interior y es completo bajo la norma (un espacio vectorial es completo si cualquier secuencia de Cauchy converge). Nos interesan espacios con dimensión finita $\mathbb{C}^d$, acompañados con un producto interior.

Dado un vector $v \in \mathbb{C}^d$ que describe el estado de un sistema físico. Este vector se suele representar en la notación de Dirac. Cuando se hable de un vector columna $v \in \mathbb{C}^d$ se escribirá $|v\rangle$ llamado un "ket". El conjugado transpuesto complejo de $v$ es un vector renglón $(v_0^*, \ldots, v_d^*)$, denotado por $\langle v|$, llamado un "bra". El producto interior de $v$ y $w$ representado por $(|v\rangle, |w\rangle)$ que es igual al producto $\langle v| \cdot |w\rangle$ (renglón por columna), se le denota como $\langle v|w\rangle$ llamado un "brackets".

**Definición 1.2.1** *Un* qubit *o bit cuántico se define sobre un espacio de Hilbert de dimensión dos* $\mathbb{C}^2$*, donde la base ortonormal* $\{|0\rangle, |1\rangle\}$*, representa los estados clásicos del sistema. El estado de un qubit es una "superposición" de estos dos estados clásicos,* $\psi = \alpha|0\rangle + \beta|1\rangle$*, donde* $\alpha, \beta$ *son complejos y* $|\alpha|^2 + |\beta|^2 = 1$*.*

Cuando se combinan dos sistemas cuánticos, vistos como elementos en espacios de Hilbert $A$ y $B$, el espacio de Hilbert que describe el nuevo sistema es el *producto tensorial* de $A$ y $B$. Si $V$ y $U$ son dos espacios de Hilbert de dimensión $n$ y $m$, respectivamente, se cumple que:

**Definición 1.2.2** *El producto tensorial* $W = V \otimes U$*, es un espacio de Hilbert de dimensión* $nm$*, que asocia pares de vectores al espacio* $W$*. Si* $v \in V$ *y* $u \in U$*, la transformación se define como* $v, u :\mapsto v \otimes u \in W$*. Donde* $\otimes$ *requiere ser lineal y asociativa.*

**Definición 1.2.3** *Un* $k$*-quregistro es un vector* $\psi \in \mathbb{H}_k = \mathbb{C}^{2^k}$*, representado como* $\psi = \sum_{j=0}^{2^k-1} \alpha_j |(j)_2\rangle$*, donde* $\alpha_0, \ldots, \alpha_{2^k-1} \in \mathbb{C}$*,* $\sum_{j=0}^{2^k-1} |\alpha_j|^2 = 1$ *y* $(j)_2$ *es la representación del índice* $j$ *en base 2. Al parámetro* $k$*, lo llamamos logitud del quregistro y* $2^k$ *es la dimensión del quregistro. Así pués, todo* $k$*-quregistro es longitud* $k$ *y de dimensión* $2^k$*.*

Dados dos espacios de Hilbert $V = \mathbb{H}_{k_1}$ y $U = \mathbb{H}_{k_2}$ con bases ortonormales $\{|i\rangle\}_{i=0}^{2^{k_1}-1}$ y $\{|j\rangle\}_{j=0}^{2^{k_2}-1}$, respectivamente. Entonces los estados $\{|i\rangle \otimes |j\rangle\} = \{|i, j\rangle\}$ forman una base ortonormal para $W = V \otimes U$. Dado dos vectores $\phi = \sum_{i=0}^{2^{k_1}-1} \alpha_i |i\rangle \in V$ y $\psi = \sum_{j=0}^{2^{k_2}-1} \beta_j |j\rangle \in U$, su producto tensorial por linealidad es tal que $\varphi = \phi \otimes \psi = \sum_{i=0}^{2^{k_1}-1} \sum_{j=0}^{2^{k_2}-1} \alpha_i \beta_j |i, j\rangle \in W$.

Se dice que $\varphi$ se factoriza o se descompone en el producto de $\phi$ y $\psi$. De aquí en adelante se empleará el término separable por factorización. Un sistema cuántico se encuentra en un *estado puro* si es un vector unitario en un espacio de Hilbert, como $|\alpha\rangle$. En general un estado puro, es una superposición de los estados base. Y por lo común un sistema cuántico no es un estado puro, esto se atribuye al hecho de que se tiene un conocimiento parcial acerca del sistema. Se dice que el sistema se encuentra en un *estado mixto* cuando se relaciona con el sistema una distribución de probabilidad, denotada por $\{\alpha\} = \{p_k|\alpha_k\}$. Esto significa que el sistema se encuentra en el estado puro $|\alpha_k\rangle$ con una probabilidad $p_k$. De aquí en adelante cuando se hable de separación de registros cuánticos, nos referimos a estados puros.

### 1.2.2. Mediciones

Las mediciones sobre un sistema mecánico cuántico son diferentes a las que se hacen en sistemas mecánicos clásicos. Se le llama un *observable* a una propiedad medible de un sistema. Formalmente, una medición se define como una matriz hermitiana ($O$ es hermitiana si $O = O^\dagger = (O^T)^*$). Una matriz hermitiana puede ser diagonizable por un conjunto ortonormal de eigenvalores con valores reales. Esto significa que existe una base $\{v_0, \ldots, v_{n-1}\} \subseteq V$ de dimensión $n$ tal que $O|v_i\rangle = v_i|v_i\rangle$ siendo $v_i$ el eigenvalor asociado a $|v_i\rangle$. Supóngase que un sistema se encuentra en el estado $\psi$ y $\sum_{i=0}^{n-1} \alpha_i|v_i\rangle = \psi$, entonces el resultado de una medición del observable $O$ puede ser sólo $v_1, \ldots, v_n$. El resultado de la medición será probabilístico y la probabilidad de obtener $v_i$ es $|\alpha_i|^2$.

Dada una colección $\{M_m\}$ de operadores de medición (matrices hermitianas), donde el índice $m$ se refiere a los posibles resultados de una medición. Si $\psi$ es el estado cuántico de un sistema, la probabilidad de que ocurra $m$ es

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{1.1}$$

y el estado del sistema después de la medición es

$$\frac{M_m\psi}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \tag{1.2}$$

también se cumple que las probabilidades suman uno,

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = 1 \tag{1.3}$$

### 1.2.3. Estados de Bell

El fenómeno del entrelazamiento cuántico es quizás el descubrimiento más importante del formalismo de la teoría cuántica (en [7] se comentan sus implicaciones). Los primeros en notar sus propiedades fueron Einstein, Podolsky y Rosen en su celebre artículo EPR [8]. Una de sus propiedades más importantes es su no-localidad con respecto a las mediciones. Propiedad que tiempo después explica Bell [9], dando una cota superior en la cual un sistema que interactuó en un principio puede seguir haciéndolo después de ser separados físicamente. Los estados entrelazados más básicos se dan en $\mathbb{H}_2$, son aquellos vectores que no se pueden representar como producto tensorial de dos factores en $\mathbb{H}_1$. Los estados son los siguientes:

$$\begin{aligned}
\mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
\mathbf{b}_{01} &= \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\
\mathbf{b}_{10} &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
\mathbf{b}_{11} &= \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)
\end{aligned} \tag{1.4}$$

Si se lleva a cabo una medición sobre el primer qubit de $\mathbf{b}_{11}$ se obtiene 0 ó 1 con igual probabilidad. Ya sea que el resultado sea 0 ó 1, el resultado de una medición sobre el segundo qubit queda determinado por el primero. En particular los estados en (1.4) forman una base ortonormal $\mathcal{B}_{Bell}$ en $\mathbb{H}_2$, llamada *de Bell*. Los estados de Bell han sido ampliamente usados en protocolos de comunicación cuántica. Uno de ellos es el propuesto por Bennett y Wiesner [3], llamado *de Códigos superdensos* (*Quantum dense coding*). En el protocolo se prepara un estado de Bell, digamos $\mathbf{b}_{00}$ donde Alicia se queda con el primer qubit y Beto el segundo. Beto aplica transformaciones unitarias dadas por las matrices de Pauli siguientes:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1.5)$$

La aplicación de las transformaciones producen los estados siguientes:

$$\begin{aligned} (\sigma_0 \otimes \sigma_0)\mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \sim \mathbf{b}_{00} \\ (\sigma_0 \otimes \sigma_x)\mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \sim \mathbf{b}_{01} \\ (\sigma_0 \otimes \sigma_y)\mathbf{b}_{00} &= \frac{i}{\sqrt{2}}(|01\rangle - |10\rangle) \sim \mathbf{b}_{11} \\ (\sigma_0 \otimes \sigma_z)\mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \sim \mathbf{b}_{10} \end{aligned} \quad (1.6)$$

donde la relación de equivalencia "$\sim$" es tal que, dado dos vectores como $e^{i\theta}\psi$ y $\psi$, si $e^{i\theta}\psi \sim \psi$ entonces los vectores son iguales para efectos de mediciones, es decir se ignora el factor global de fase. Para ver esto, suponga que $M_m$ es un operador de medición, entonces se puede ver que las probabilidades de éxito del estado $m$ son $\langle\psi|M_m^\dagger M_m|\psi\rangle$ y $\langle\psi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\psi\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Para una discusión más detallada sobre el factor de fase se puede ver [10].

Ya que los estados en (1.4) forman una base ortonormal $\mathcal{B}_{Bell}$ en $\mathbb{H}_2$, el estado después de aplicar las transformaciones es otro elemento en la misma base. Entonces Beto envía de regreso su qubit a Alicia quien lleva a cabo una medición en la base de Bell, distinguiendo sin ambigüedad el estado resultante. Ya que Alicia conoce el estado inicial y el nuevo estado, puede conocer qué transformación aplicó Beto, recuperando 2 bits de información.

Este protocolo ha sido demostrado experimentalmente por Mattle *et al* [11] en un sistema óptico y por Fang *et al* [12] empleando técnicas NMR (*Nuclear Magnetic Resonance*). Una buena referencia sobre estados de Bell y en general de computación cuántica son [6, 10].

### 1.2.4. Simulación de estados entrelazados

La complejidad de la simulación de estados entrelazados significa la cantidad de información que se tiene que transmitir por medio de un canal de comunicación

clásico [13, 14, 15]. El propósito de la simulación del entrelazamiento es reproducir el efecto a distancia que teóricamente se predice, empleando comunicación clásica. Un esquema que se emplea para la simulación es el de *variables locales ocultas* (VLO), éstas son una fuente infinita de bits aleatorios correlacionados que especifican parámetros de valores reales. Este esquema fue propuesto en la Mecánica Cuántica para explicar el efecto de una supuesta comunicación a distancia que exhiben las mediciones en estados de Bell.

Uno de los protocolos de simulación del entrelazamiento es el propuesto por Steiner en [16], que emplea el esquema de VLO para simular el entrelazamiento, donde se necesitan 1.485 bits en promedio de comunicación clásica. También se muestra que sin el esquema de VLO se necesitan 22 bits de comunicación. Otro protocolo es el propuesto por Brassard en [13], él considera las mediciones en estados entrelazados como eventos probabilísticos conjuntos, para simular el efecto de las mediciones; donde la complejidad de la simulación es de 4 bits de comunicación clásica. Recientemente se ha propuesto que la simulación de estados entrelazados se puede hacer sin comunicación alguna [17].

## 1.3. Organización de la tesis

El documento de tesis está organizado de la forma siguiente: en el capítulo 2 se aborda el problema de separabilidad en estados puros, en el capítulo 3 se explora la simulación de protocolos cuánticos, en el capítulo 4 se detalla la extensión a varias partes del protocolo de códigos superdensos, el capítulo 5 trata los esquemas de simulación de protocolos cuánticos, y finalmente en el capítulo 6 se presentan las conclusiones y trabajo futuro.

# Capítulo 2

# Separabilidad en registros cuánticos

En este capítulo se aborda el problema de separabilidad en estados puros en un enfoque de partición. Se describe una solución algorítmica que busca recursivamente una partición hasta obtener la separación completa de un registro cuántico. Se calcula su complejidad y se estudia su comportamiento estadístico para varios tamaños de un quregistro como instancia, variando el número de factores. También se muestran tiempos de ejecución del algoritmo y finalmente se compara con otros métodos para decidir separabilidad de quregistro.

## 2.1. Separabilidad y su complejidad

Sobre el problema de separabilidad en registros cuánticos existen estudios realizados para decidir si un registro es separable [18, 19, 20, 21]; como el uso de los operadores o matrices de densidad $\rho$, que asocian una probabilidad a cada estado que puede tomar el sistema. En términos de este operador que describe al sistema, es posible saber si un estado es separable. Por ejemplo, un sistema que consiste de dos subsistemas es separable si su matriz de densidad se puede escribir como $\rho = \Sigma_A w_A \rho_A^{'} \otimes \rho_A^{''}$ donde $\rho_A^{'}$ y $\rho_A^{''}$ son matrices de densidad de los dos subsistemas. Donde el operador de densidad cumple con: (i) $\rho$ es auto-adjunto $\rho = \rho^{\dagger}$ (llamada hermitiana conjugada, $\rho^{\dagger} = (\rho^T)^*$), (ii) $\rho$ es positivo y (iii) con traza igual a uno, $tr(\rho) = 1$.

Uno de los resultados más importantes son las desigualdades de Bell. Un sistema separable siempre satisface las desigualdades de Bell, pero lo contrario no es necesariamente cierto. En el famoso artículo EPR publicado en 1935 [8] se discute el fenómeno del entrelazamiento en estados cuánticos, argumentando que la descripción de la mecánica cuántica no es una teoría completa, en términos de lo que ellos definieron como los *elementos de la realidad física*. El artículo publicado en 1964 por John S. Bell titulado *On the Einstein Podolsky Rosen paradox* [9], contrario a los argumentos del artículo EPR, es considerado como uno de los descubrimientos más profundos en la ciencia. Bell no trata acerca de la mecánica cuántica, si no que es una

prueba general aplicable a cualquier teoría física; el demuestra que existe una cota superior para la cual un sistema que interactuó en un inicio puede seguir haciéndolo.

Recientemente en [22] se propone un nuevo criterio de separabilidad en términos de la matriz de densidad, el resultado se deriva de una manipulación algebraica. Si un sistema es separable se puede representar como $\rho = \Sigma_A w_A \rho_A^{'} \otimes \rho_A^{''}$ con eigenvalores no negativos, entonces resulta que en la matriz de densidad $\sigma = \Sigma_A w_A (\rho_A^{'})^T \otimes \rho_A^{''}$, ninguno de sus eigenvalores son negativos, lo cual resulta en un criterio más fuerte que las desigualdades de Bell.

### 2.1.1. Complejidad de la separación

De los trabajos relacionados sobre separación de estados puros y mixtos se pueden mencionar los trabajos publicados por Leonid Gurvits [23, 24, 25, 26]. Trata los temas sobre complejidad y separabilidad en estados cuánticos. En particular el problema de correlación bipartita perfecta, relacionado con el problema introducido por Edmond en 1967 (ahora conocido como el problema de Edmond). Se quiere saber si un subespacio lineal $M(N)$ contiene una matriz no singular, donde $M(N)$ es un espacio lineal de matrices complejas de tamaño $N \times N$.

El problema de Edmond se reformula en términos de matrices con entradas no negativas, cuya generalización resulta en la noción de operadores positivos o equivalentemente, en términos de matrices de densidad separables, que es de gran importancia en teoría cuántica. Resulta entonces que uno de los casos más importantes en el problema de Edmond se puede resolver en tiempo polinomial, el cual corresponde a matrices de densidad separables. También se muestra un algoritmo de complejidad polinomial para resolver el problema de Edmond. Finalmente se concluye que el problema de separabilidad en matrices de densidad es un problema NP-difícil [24].

## 2.2. Algoritmo de separación

La identificación de bloques entrelazados mínimos es un problema de gran interés en la toma de mediciones sobre estados cuánticos. El problema de separación en estados puros se plantea como sigue: dado $z \in \mathbb{H}_k$ decidir si existen $x \in \mathbb{H}_{k_1}$ y $y \in \mathbb{H}_{k_2}$ con $k = k_1 + k_2$, tales que $z = x \otimes y$ y en tal caso encontrarlos. Por ejemplo, supóngase que $k \geq 2$ y que $k_1 + k_2 = k$ con $1 \leq k_1, k_2 \leq k$, donde $x$ es un $k_1$-quregistro de longitud $k_1$ y dimensión $2^{k_1}$, $y$ es un $k_2$-quregistro de longitud $k_2$ y dimensión $2^{k_2}$, representados como sigue:

$$x = \sum_{j=0}^{2^{k_1}-1} x_j |(j)_{2,k_1}\rangle, \quad y = \sum_{j=0}^{2^{k_2}-1} y_j |(j)_{2,k_2}\rangle, \tag{2.1}$$

donde $|(j)_{2,k_1}\rangle$ es la representación binaria del índice $j$ de longitud $k_1$, y del mismo

modo para $|(j)_{2,k_2}\rangle$. Entonces el problema de separación es el siguiente:

$$\begin{aligned} z = x \otimes y &= \sum_{i=0}^{2^{k_1}-1} \sum_{j=0}^{2^{k_2}-1} x_i y_j |(i)_{2,k_1}\rangle \otimes |(j)_{2,k_2}\rangle \\ &= \sum_{i=0}^{2^{k_1}-1} \sum_{j=0}^{2^{k_2}-1} x_i y_j |(i \cdot j)_{2,k_1+k_2}\rangle, \end{aligned} \tag{2.2}$$

donde la operación $(\cdot)$ es concatenación y resulta que $z$ es un $(k_1 + k_2)$-quregistro. El mismo problema se puede ver en términos de la longitud de los factores cuya declaración es como sigue:

Dado un $k$-quregistro $z \in \mathbb{H}_k$, decidir si existen $x \in \mathbb{H}_{k_1}$, de forma que $x$ es un $k_1$-quregistro de longitud $k_1$ y dimensión $2^{k_1}$ con $1 \leq k_1 \leq k$, y $y \in \mathbb{H}_{k-k_1}$ un $(k-k_1)$-quregistro de longitud $k - k_1$ y dimensión $2^{k-k_1}$, tales que $z = x \otimes y$.

En (2.2) la expresión para $z$ representa un sistema de ecuaciones cuadráticas que consta de $2^{k_1+k_2}$ ecuaciones y $2^{k_1} + 2^{k_2}$ variables complejas. Por ejemplo, considérese a $x_0$ un 3-quregistro y $x_1$ un 2-quregistro dados por:

$$\begin{aligned} x_0 = x_{0,0}|000\rangle + x_{0,1}|001\rangle + x_{0,2}|010\rangle + x_{0,3}|011+\rangle \\ x_{0,4}|100\rangle + x_{0,5}|101\rangle + x_{0,6}|110\rangle + x_{0,7}|111\rangle, \end{aligned} \tag{2.3}$$

$$x_1 = x_{1,0}|00\rangle + x_{1,1}|01\rangle + x_{1,2}|10\rangle + x_{1,3}|11\rangle, \tag{2.4}$$

y su producto tensorial es:

$$\begin{aligned} x_0 \otimes x_1 = x_{1,0}x_{0,0}|00000\rangle + x_{1,0}x_{0,1}|00001\rangle + \cdots + x_{1,0}x_{0,7}|00111\rangle + \\ x_{1,1}x_{0,0}|01000\rangle + x_{1,1}x_{0,1}|01001\rangle + \cdots + x_{1,1}x_{0,7}|01111\rangle + \\ \vdots \\ x_{1,3}x_{0,0}|11000\rangle + x_{1,3}x_{0,1}|11001\rangle + \cdots + x_{1,3}x_{0,7}|11111\rangle. \end{aligned} \tag{2.5}$$

En representación matricial se escribe como sigue:

$$\begin{pmatrix} x_{1,0}x_{0,0} & x_{1,0}x_{0,1} & \cdots & x_{1,0}x_{0,7} \\ x_{1,1}x_{0,0} & x_{1,1}x_{0,1} & \cdots & x_{1,1}x_{0,7} \\ \vdots & & \ddots & \vdots \\ x_{1,3}x_{0,0} & x_{1,3}x_{0,1} & \cdots & x_{1,3}x_{0,7} \end{pmatrix} = \begin{pmatrix} z_0 & z_1 & \cdots & z_7 \\ z_8 & z_9 & \cdots & z_{15} \\ \vdots & & \ddots & \vdots \\ z_{24} & z_{25} & \cdots & z_{31} \end{pmatrix} = Z, \tag{2.6}$$

cada ecuación es de la forma $x_{1i}x_{0j} = z_{ij}$ para $0 \leq i < 2^2$, $0 \leq j < 2^3$. De hecho cada entrada en la matriz $Z$ dada en (2.6) se obtiene por la relación $\phi_{k_1k_2}(i,j) = z_{i \cdot 2^{k_2}+j}$ y $x_{1i}x_{0j} = z_{\phi_{k_1k_2}(i,j)}$ donde $k_2$ es el número de columnas. Un vector $z \in \mathbb{H}_n$ es entrelazado si para ningún $n_0$, con $0 < n_0 < n$, $z$ es $(n - n_0, n_0)$-separable, es decir que

existan los factores $x$ un $(n-n_0)$-quregistro, $y$ un $n_0$-quregistro, tales que $z = x \otimes y$. O en forma negativa, $z \in \mathbb{H}_n$ es separable si existe $n_0$, con $0 < n_0 < n$, tal que $z$ es $(n-n_0, n_0)$-separable. En resumen son dos problemas que se quieren resolver, el problema de decisión y la recuperación de los factores:

**Problema de Decisión. Instancia:** Un vector $z \in \mathbb{H}_n$.
**Solución:** Una respuesta, $z$ es o no separable.

**Problema de separación. Instancia:** Un vector $z \in \mathbb{H}_n$ y un entero $n_0$ tal que $0 < n_0 < n$.
**Solución:** $x_1 \in \mathbb{H}_{n-n_0}$, $x_0 \in \mathbb{H}_{n_0}$ tal que $z = x_1 \otimes x_0$, si $z$ es $(n-n_0, n_0)$-separable.

### 2.2.1. Primer enfoque

Para saber si un vector $z \in \mathbb{H}_n$ es separable, se debe de decidir si el sistema de ecuaciones cuadráticas en (2.6) tiene solución sobre $\mathbb{C}$. Dado $n_0$ con $0 < n_0 < n$, el sistema de ecuaciones es el siguiente:

$$X = Z \quad \text{donde} \quad \begin{aligned} X &= \left(x_{1i}x_{0j}\right)_{0\le i<2^{n-n_0}}^{0\le j<2^{n_0}}, \\ Z &= \left(z_{\phi_{nn_0}(i,j)}\right)_{0\le i<2^{n-n_0}}^{0\le j<2^{n_0}}. \end{aligned} \tag{2.7}$$

De aquí en adelante se usará la siguiente notación: si $M$ es una matriz de complejos, $m_{ij}$ denota la $(i,j)$-ésima entrada de $M$, $M_i$ su $i$-ésimo renglón y $M^j$ su $j$-ésima columna. Para $i < j$, $[\![i,j]\!]$ denotará el conjunto de enteros $\{i, i+1, \ldots, j-1, j\}$. Ahora, supóngase que $X$ es una solución de (2.7) para alguna $Z$ y $n_0 \in [\![1, n-1]\!]$. Las siguientes observaciones son evidentes:

1. Para cualquier entrada $z_{ij}$ en $Z$, si $z_{ij} = 0$ entonces, ya sea que $X_i = 0$ ó $X^j = 0$.

2. Para cualquier $i \in [\![0, 2^{n-n_0} - 1]\!]$, el $i$-ésimo renglón de $X$ es de la forma $X_i = x_{1i}[x_{0j}]^{0\le j<2^{n_0}} = x_{1i}x_0^T$. Consecuentemente, el rango por renglones de $X$ es 1.

3. Para cualquier $j \in [\![0, 2^{n_0} - 1]\!]$, la $j$-ésima columna de $X$ es de la forma $X^j = [x_{1i}]_{0\le i<2^{n-n_0}} x_{0j} = x_1 x_{0j}$. Consecuentemente, el rango por columnas de $X$ es 1.

De las observaciones anteriores se proponen los siguientes criterios para decidir si un vector dado es separable:

**Criterio 1**: Si existe un par de índices $(i,j)$, tal que $Z_{ij} = 0$ y $Z_i \neq 0$ y $Z^j \neq 0$ entonces $Z$ no es $(n-n_0, n_0)$-separable.

De la forma de la matriz $Z$ en (2.6) se puede ver que cada columna se trata del vector $x_1$ multiplicado por $x_{0j}$ y de igual forma cada renglón es el vector $x_0$ multiplicado por $x_{1i}$. Por lo que el rango de la matriz (el número de columnas o renglones linealmente independientes) no puede ser mayor a 1. De esta observación se propone un segundo criterio:

**Criterio 2**: Si *rango* $Z > 1$ entonces $Z$ no es $(n - n_0, n_0)$-separable.

A partir de estos dos criterios se puede decidir si el quregistro es separable o no. Para recuperar los vectores factores observamos que cada renglón en $Z$ es el vector $x_0$ y cada columna el vector $x_1$ multiplicados por un complejo. Por ejemplo, si se toma el primer renglón $Z_0 = (z_0, z_1, \ldots, z_7)$ en (2.6) y se toma su norma al cuadrado:

$$\begin{aligned} \|Z_0\|^2 &= |z_0|^2 + |z_1|^2 + \cdots + |z_7|^2 \\ &= x_{1,0}^2 x_{0,0}^2 + x_{1,0}^2 x_{0,1}^2 + \cdots + x_{1,0}^2 x_{0,7}^2 \\ &= x_{1,0}^2 (x_{0,0}^2 + x_{0,1}^2 + \cdots + x_{0,7}^2) \\ &= x_{1,0}^2 \|x_0\|, \end{aligned} \tag{2.8}$$

por lo que $\|Z_0\| = |x_{1,0}|\|x_0\|$. Al normalizar se obtiene

$$\begin{aligned} \frac{1}{\|Z_0\|} Z_0 &= \frac{1}{|x_{1,0}|\|x_0\|}(z_0, z_1, \ldots, z_7) \\ &= \frac{1}{|x_{1,0}|\|x_0\|}(x_{1,0}x_{0,0}, x_{1,0}x_{0,1}, \ldots, x_{1,0}x_{0,7}), \end{aligned} \tag{2.9}$$

ya que $\frac{1}{\|x_0\|} = 1$, por el hecho de que $|x_{0,0}|^2 + |x_{0,1}|^2 + \cdots + |x_{0,7}|^2 = 1$, como lo requiere un quregistro válido. Entonces

$$\frac{1}{\|Z_0\|} Z_0 = \left( \frac{x_{1,0}}{|x_{1,0}|} \right) x_0. \tag{2.10}$$

Cada renglón $Z_i/\|Z_i\|$ es el vector $x_0$ multiplicado por el complejo con norma igual a uno, $x_{1j}/|x_{1j}|$. Del mismo modo se puede ver que para cada columna $Z^j$, $Z^j/\|Z^j\|$ es el vector $x_1$ multiplicado por $x_{0i}/|x_{0i}|$. Los nuevos vectores $x_0'$, $x_1'$ tienen norma igual a 1. Se tratan de los vectores $x_0$, $x_1$ desfasados pero que conservan la propiedad de que la suma de las probabilidades suman uno. En la tabla 2.1 se propone un algoritmo para decidir si un vector es separable siguiendo los criterios propuestos. El algoritmo es como sigue:

En el paso 1. del algoritmo se cambia a representación matricial el vector $z$, el paso 2. verifica que se cumpla el criterio 1, eliminando los renglones y columnas ceros, el paso 3. calcula el rango de la matriz $Z$, la cual es una matriz sin entradas ceros. El paso 4. verifica si los espacios generados por columnas y por renglones de $Z$ son 1-dimensional. Esto se puede llevar a cabo tomando en cuenta las siguientes observaciones:

**Entrada.** $n \in \mathbb{N}$, $n_0 \in [\![1, n-1]\!]$, $z \in \mathbb{H}_n$
**Salida.** $x_1 \in \mathbb{H}_{n-n_0}$, $x_0 \in \mathbb{H}_{n_0}$: $z = x_1 \otimes x_0$ si $z$ es $(n-n_0, n_0)$-separable.
**Procedimiento.** DescomParcial
(1) Sea $Z = \left(z_{\phi_{nn_0}(i,j)}\right)_{0\leq i\leq 2^{n-n_0}-1}^{0\leq j\leq 2^{n_0}-1}$ ;
(2) Para cada $(i,j)$ tal que $z_{ij} = 0$ hacer
Si $Z_i = 0$ entonces
$x_{1i} := 0$ ; suprimir el $i$-ésimo renglón en $Z$;
En otro caso Si $Z^j = 0$ entonces
$x_{0j} := 0$ ; suprimir la $j$-ésima columna en $Z$;
En otro caso $z$ no es $(n-n_0, n_0)$-separable;
(3) $k := rango(Z)$ ;
(4) Si $k > 1$ entonces $z$ no es $(n-n_0, n_0)$-separable
En otro caso
Sea $z_0 \in \mathbb{C}^{2^{n_0}}$ la expansión unitaria del vector $\mathcal{L}(Z_i)_{0\leq i\leq 2^{n-n_0}-1}$ ;
Sea $z^0 \in \mathbb{C}^{2^{n-n_0}}$ la expansión unitaria del vector $\mathcal{L}(Z^j)_{0\leq j\leq 2^{n_0}-1}$ ;
salida $x_0 = \texttt{Unir}(x_0, z_0)$ y $x_1 = \texttt{Unir}(x_1, z^0)$.

Tabla 2.1: Algoritmo de separación.

- Dos columnas $j_0, j_1$ son paralelas si las razones $\frac{z_{ij_0}}{z_{ij_1}}$ tienen un valor constante (independientemente de $i$), y

- el espacio generado por columnas es 1-dimensional si cada columna es paralela a la primera columna.

y de igual manera para los renglones. Por último, la operación `Unir` en el paso 4. agrega los ceros eliminados en el paso 2. del algoritmo. Así, si la matriz $Z$ satisface los criterios propuestos, se obtienen los factores $x_1$ y $x_0$, tales que satisfacen la siguiente condición:

$$\|x_1\| = 1 \ \& \ \|x_0\| = 1 \implies \|x_1 \otimes x_0\| = 1, \tag{2.11}$$

es decir, son vectores unitarios, con norma igual a uno. Aunque no se recuperan los factores originales, los vectores recuperados satisfacen las mismas propiedades en las amplitudes o probabilidades, y la suma de ellas es igual a uno. Para efecto de mediciones, si las amplitudes no son modificadas, el resultado de las mediciones reproducen las mismas estadísticas que los factores originales.

### 2.2.2. Segundo enfoque

Supóngase que para cada $z \in \mathbb{H}_n$, la matriz $X$ es una solución de (2.7), para $n_0 \in [\![1, n-1]\!]$. Sea $J_0 = \{j \in [\![0, 2^n - 1]\!] \mid x_{0j} \neq 0\}$ el conjunto de índices con valores $x_{0j}$ no cero, y

de igual forma, sea $I_1 = \{i \in [\![0, 2^{n-n_0} - 1]\!] |\ x_{1i} \neq 0\}$. Se define:

$$\forall j_0 \in J_0\ \forall j_1 \in [\![0, 2^n - 1]\!] \ \ : \ \ \xi_{0j_0j_1} = \frac{x_{0j_1}}{x_{0j_0}}, \tag{2.12}$$

$$\forall i_0 \in I_1\ \forall i_1 \in [\![0, 2^{n-n_0} - 1]\!] \ \ : \ \ \xi_{1i_0i_1} = \frac{x_{1i_1}}{x_{1i_0}}. \tag{2.13}$$

Primero, se observa que, para cada $j_0 \in J_0$:

$$\|x_0\|^2 = \sum_{j_1=0}^{2^{n_0}-1} |x_{0j_1}|^2 = \sum_{j_1 \in J_0} |x_{0j_1}|^2 = |x_{0j_0}|^2 \sum_{j_1 \in J_0} |\xi_{0j_0j_1}|^2, \tag{2.14}$$

es decir, es la suma de los valores no cero en $x_0$, así

$$|x_{0j_0}|^2 = \left[\sum_{j_1 \in J_0} |\xi_{0j_0j_1}|^2\right]^{-1} \|x_0\|^2 = \left[\sum_{j_1 \in J_0} |\xi_{0j_0j_1}|^2\right]^{-1}. \tag{2.15}$$

De igual forma, para cada $i_0 \in I_1$:

$$|x_{1i_0}|^2 = \left[\sum_{i_1 \in I_1} |\xi_{1i_0i_1}|^2\right]^{-1} \|x_1\|^2 = \left[\sum_{i_1 \in I_1} |\xi_{1i_0i_1}|^2\right]^{-1}. \tag{2.16}$$

Ahora, ya que $X$ es una solución de (2.7), y de (2.12) se tiene que $\forall i \in I_1$:

$$\xi_{0j_0j_1} = \frac{x_{0j_1}}{x_{0j_0}} = \frac{\frac{z_{\phi_{nn_0}(i,j_1)}}{x_{1i}}}{\frac{z_{\phi_{nn_0}(i,j_0)}}{x_{1i}}} = \frac{z_{\phi_{nn_0}(i,j_1)}}{z_{\phi_{nn_0}(i,j_0)}}, \tag{2.17}$$

o, en resumen:

$$j_0, j_1 \in J_0\ ,\ i \in I_1 \implies \xi_{0j_0j_1} = \frac{z_{\phi_{nn_0}(i,j_1)}}{z_{\phi_{nn_0}(i,j_0)}}, \tag{2.18}$$

y de igual forma,

$$i_0, i_1 \in I_1\ ,\ j \in J_0 \implies \xi_{1i_0i_1} = \frac{z_{\phi_{nn_0}(i_1,j)}}{z_{\phi_{nn_0}(i_0,j)}}. \tag{2.19}$$

Consecuentemente, las razones del lado derecho de la condición (2.18) tienen un valor constante para todo $i \in I_1$ y las razones al lado derecho de la condición (2.19) tienen un valor constante para todo $j \in J_0$. Si cualquiera de estas condiciones no se cumple, entonces $z$ no es $(n - n_0, n_0)$-separable. De otra forma, de (2.18) y (2.19) se pueden calcular las razones $\xi_{0j_0j_1}$ y $\xi_{1i_0i_1}$ respectivamente, y de (2.16) y (2.17) los valores absolutos de las entradas de $x_0$ y $x_1$, aseguran que todos los vectores involucrados son unitarios.

| | |
|---|---|
| **Procedimiento.** DescomParcial | |
| **Entrada.** $z$: $n$-quregistro, | |
| $n_0 : 0 < n_0 < n$ | |
| **Salida.** $x_1$: $(n - n_0)$-quregistro, | |
| $x_0$: $n_0$-quregistro | |
| con $z = x_1 \otimes x_0$ | Si existen $x_0$ y $x_1$ |
| Irreducible | En otro caso |

Tabla 2.2: Algoritmo para decidir separabilidad de registros cuánticos.

## 2.3. Complejidad algorítmica y análisis estadístico

Para ver el desempeño del algoritmo propuesto, se considera su estudio de complejidad y los tiempos de ejecución del mismo. Así como un pequeño análisis estadístico en la forma en que procede el algoritmo de la tabla 2.1. El tamaño de un $k$-quregistros crece de forma exponencial, por ejemplo para un 10-quregistro, su vector de estados es de dimensión $2^{10} = 1024$, es decir se necesitan almacenar 1024 complejos.

### 2.3.1. Complejidad del algoritmo

Dado el algoritmo de separación DescomParcial de la tabla 2.2 con las entradas $z \in \mathbb{H}_n$, y $0 < n_0 < n$. Se quiere decidir si $z$ es separable. El algoritmo se muestra en la tabla 2.1. Sean $P(n, n_0)$, $C(n, n_0)$ la cantidad de productos y de comparaciones de números complejos respectivamente. Las etapas que sigue el algoritmo son:

**(1)** Convierte un vector a matriz, esto se puede hacer directamente en un lenguaje de programación como ANSI C. Así que, si la dimensión del vector $z$ es de $2^n$, entonces se obtiene una matriz con entradas complejas de tamaño $2^{n-n_0} \times 2^{n_0}$.

**(2)** Revisa las entradas con ceros, para hacerlo se tiene que recorrer por completo la matriz y requiere $C_1(n, n_0) = 2^{n_0} \cdot 2^{n-n_0} = 2^n$ comparaciones.

**(3)** Busca columnas paralelas, dos columnas son paralelas si la razón $\frac{z_{ij_0}}{z_{ij_1}}$ se mantiene constante para dos columnas $j_0, j_1$, esto equivale a hacer la multiplicación $(z_{ij_1}^{-1})z_{ij_0}$. Si $j_0 = 0$, $0 < j_1 < 2^{n-n_0}$ y $0 \leq i < 2^{n_0}$, entonces el número de multiplicaciones es $P_1(n, n_0) = (2^{n-n_0} - 1)2^{n_0} = 2^n - 2^{n_0}$. Esto equivale a verificar si cada columna es paralela a la primera excepto ella misma. Y también el número de comparaciones es $C_2(n, n_0) = 2^n - 2^{n_0}$.

**(4)** Normaliza los factores como se muestra en la ecuación (2.10). Se necesita tomar una columna y un renglón, y normalizarlos. Entonces el número de multiplicaciones en la normalización es $f_{norm} = 2^{n_0} + 2^{n-n_0}$.

Por lo tanto el número total de comparaciones es:

$$\begin{aligned} C(n, n_0) &= C_1 + C_2 \\ &= 2^n + 2^n - 2^{n_0} \\ &= 2^{n+1} - 2^{n_0}, \end{aligned} \tag{2.20}$$

y el orden es $C(n, n_0) = O(2^{n+1} - 2^{n_0})$. El número total de multiplicaciones es

$$\begin{aligned} P(n, n_0) &= P_1 + f_{norm} \\ &= 2^n - 2^{n_0} + 2^{n_0} + 2^{n-n_0} \\ &= 2^n + 2^{n-n_0}, \end{aligned} \tag{2.21}$$

y consecuentemente el orden es $P(n, n_0) = O(2^n + 2^{n-n_0})$. El costo total si fuese reducible es

$$P_T = \sum_{n_0=1}^{n-1} P(n, n_0) = \sum_{n_0=1}^{n-1} O(2^n + 2^{n-n_0}), \tag{2.22}$$

$$C_T = \sum_{n_0=1}^{n-1} C(n, n_0) = \sum_{n_0=1}^{n-1} O(2^{n+1} - 2^{n_0}). \tag{2.23}$$

Las complejidades dadas en (2.22) y (2.23) son cotas superiores, ya que se pueden optimizar. Por ejemplo en el paso **(3)** al verificar las columnas paralelas. Si se considera el número promedio de iteraciones necesarias para encontrar un $n_0$ tal que un vector $z \in \mathbb{H}_n$ es $(n - n_0, n_0)$-separable. Entonces el costo total es el siguiente:

$$P_m = \sum_{n_0=1}^{T(n)} P(n, \pi(n_0)) = \sum_{n_0=1}^{T(n)} O(2^n + 2^{n-\pi(n_0)}), \tag{2.24}$$

$$C_m = \sum_{n_0=1}^{T(n)} C(n, \pi(n_0)) = \sum_{n_0=1}^{T(n)} O(2^{n+1} - 2^{\pi(n_0)}). \tag{2.25}$$

donde $T(n)$ es el número promedio de iteraciones necesarias para encontrar una separación y $\pi(\cdot)$ es una permutación tal que si $n_0 = \pi(i)$, entonces $z$ es $(n - n_0, n_0)$-separable. La forma más directa de obtener una separación completa de un quregistro es aplicar el algoritmo de la tabla 2.1 para $n_0 = 1, \ldots, n-1$ y obtener los factores $x_1, x_0$ y llamar nuevamente el algoritmo con los factores $x_1, x_0$ y volver aplicar el algoritmo sucesivamente. Un enfoque diferente a la versión exhaustiva es considerando el algoritmo que se muestra en la tabla 2.3.

En el algoritmo de la tabla 2.3 los resultados devueltos $\{band,\ x_a,\ x_b\}$ son: *band*=`Falso` si $z$ es separable, `Verdadero` de otro modo. Si *band*=`Falso` devuelve los factores $x_a, x_b$. La función `Insert` inserta en orden los factores en una lista ligada.

Para $n$ grande, aplicar el algoritmo de la tabla 2.1 requiere de mucho tiempo de cómputo. Si el número de factores es grande resulta mejor escoger los valores para

**Entrada.** $z$: $n$-quregistro,
$n_0^* = \pi(i = 1)$
**Salida.** $x_0, x_1, \ldots, x_k$: quregistros,
tales que $z = x_0 \otimes x_1 \otimes \cdots \otimes x_k$
**Procedimiento.** Reduce
$\{band,\ x_a,\ x_b\}$ = DescomParcial$(z, n_0^*)$
Si (**no** *band*) entonces
{
$r_1$ = Reduce$(x_a, \pi(i+1))$
Si (**no** $r_1$) entonces `Inserta`$(x_a)$
$r_2$ = Reduce$(x_b, \pi(i+1))$
Si (**no** $r_2$) entonces `Inserta`$(x_b)$
}
salida(**no** *band*)

Tabla 2.3: Algoritmo de separación completa.

$n_0$ aleatoriamente (uniformemente). Si se encuentra un $n_0$ tal que $z$ es $(n - n_0, n_0)$-separable, con $n_0$ cerca de $n/2$, que es lo que pasaría en el promedio para muchos intentos. Entonces el tamaño del problema en las llamadas siguientes al algoritmo de la tabla 2.1 se reduce a la mitad.

### 2.3.2. Pruebas y análisis estadístico

La figura 2.1 muestra los tiempos de ejecución para separar completamente un 21-quregistro variando el número de factores, para la versión exhaustiva y escogiendo aleatoriamente el valor de $n_0$. De la figura 2.1 se observa que para pocos factores la estrategia exhaustiva tiene mejor desempeño que la aleatoria, pero cuando el número de factores alcanza cerca de la mitad del tamaño del quregistro la estrategia aleatoria mejora a la exhaustiva. Las ejecuciones se llevaron a cabo en una computadora personal con un procesador Celeron a 1.7 GHz con 256 MB de RAM, bajo el sistema operativo Red Hat 9.0. El lenguaje de programación empleado fue C++ con el compilador g++ versión 4.1.

En un estudio más detallado se puede considerar al número promedio de intentos para encontrar un primera separación en las primeras instancias del vector $z$. En la figura 2.2 se prueba experimentalmente el desempeño del algoritmo DescomParcial. Se muestra el número de intentos para encontrar una primera separación de un $n$-quregistro con $n = 30$, respecto al número de factores desde $n_0 = 2$ hasta $n - 1$. Cada punto en la gráfica representa el promedio de 300 instancias del problema. En la figura 2.3 se muestra el valor $n_0$ para el cual $z$ es $(n - n_0, n_0)$-separable, aunque no es ninguna sorpresa, la versión exhaustiva encuentra valores pequeños para $n_0$, mientras que la versión aleatoria tiende a partir el quregistro en dos factores de igual longitud. En la figura 2.4 se muestra experimentalmente la probabilidad para encontrar un $n_0$

para el cual $z$ es $(n - n_0, n_0)$-separable. Se observa que se necesitan al menos $n/2$ intentos para encontrar una primera separación.

Considérese una variable aleatoria $E$ valuada en $\{0, 1\}$, tal que para $n_0 \in [\![1, n-1]\!]$, $E(n, n_0) = 1$ si y sólo si, $n_0$ verifica que un $n$-quregistro es $(n - n_0, n_0)$-separable y sea $F(m)$ el número de éxitos cuando $E(n, n_0) = 1$, escogiendo $n_0$ aleatoriamente en el intervalo $[\![1, n-1]\!]$ llevando a cabo $m$ ensayos. A la variable aleatoria $E$ se le puede considerar como un experimento de Bernoulli con probabilidad de éxito $p \approx \frac{1}{n}$(número de factores en el quregistro) y como $F(m)$ es una suma de $m$ experimentos de Bernoulli, entonces tiene un distribución binomial, con función de densidad dada por $f_B(m, k) = \binom{m}{k} p^k (1-p)^{m-k}$, que aproxima a una distribución de Poisson con parámetro $\lambda \approx mp$, para cuando $m$ es grande y la probabilidad de éxito $p$ se vuelve lo suficientemente pequeña, con función de densidad dada por $f_P(k) = \frac{e^{-\lambda}\lambda^k}{k!}$. Nos interesa conocer el valor promedio $\overline{m}$ para cuando $F(m) = 1$, es decir, el número promedio de intentos para encontrar un $n_0$ tal que $z$ es $(n-n_0, n_0)$-separable. Usando la aproximación a la distribución de Poisson se puede calcular $f_B(m, k) \approx f_P(k)$ con $k = 1$ y $\lambda = mp$, entonces se puede igualar:

$$\frac{m\alpha}{n}\left(1 - \frac{\alpha}{n}\right)^{m-1} = e^{-\lambda}\lambda \tag{2.26}$$

y obtener $\overline{m}$, dada por:

$$\overline{m} = \left\lfloor \frac{\ln(1-p)}{\ln(1-p)+p} \right\rfloor \tag{2.27}$$

para $0 < p < 1$, si $p = 0$ significa $k = 0$ y el problema es trivial. La figura 2.5 muestra una comparación del número promedio de intentos para encontrar la primera separación dado por (2.27), con respecto a los casos con y sin reemplazo, al escoger el valor de $n_0$. Empleando la aproximación dada en (2.27) se puede proponer un algoritmo para obtener una separación completa de un quregistro, considerando $n_0 = \lfloor \frac{n}{\overline{\lambda}} \rfloor$ con $\overline{\lambda} = \overline{m}p$. Y así, obtener con probabilidad alta un $n_0$ para el cual $z$ es $(n - n_0, n_0)$-separable.

## 2.4. Comparación con otros métodos

La solución propuesta al problema de separación es de complejidad exponencial con respecto al tamaño del quregistro y aunque se muestran tiempos de ejecución para obtener los factores de un 21-quregistro, éstos son relativamente bajos. Actualmente la simulación de un algoritmo cuántico requiere de mucho tiempo de procesamiento, por lo que se han propuesto esquemas de ejecución en paralelo como una alternativa para mejorar el tiempo de ejecución de un algoritmo cuántico, como en [27, 28] que se proponen esquemas de simulación en paralelo, donde se logra simular algoritmos cuánticos por arriba de 30 qubits.

En la separación de quregistros el costo computacional es muy similar al de la simulación de un algoritmo cuántico. Por ejemplo un método para decidir si un quregistro

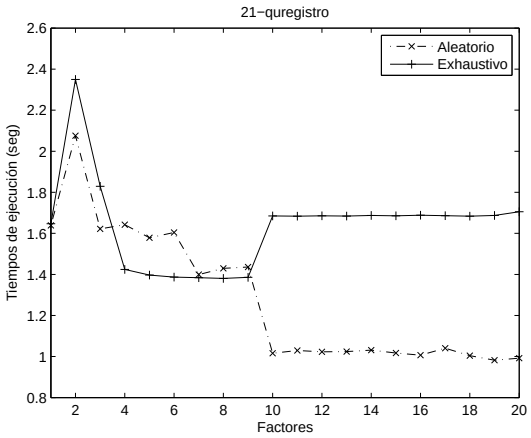


Figura 2.1: Tiempos de ejecución del algoritmo DescomParcial variando el número de factores.

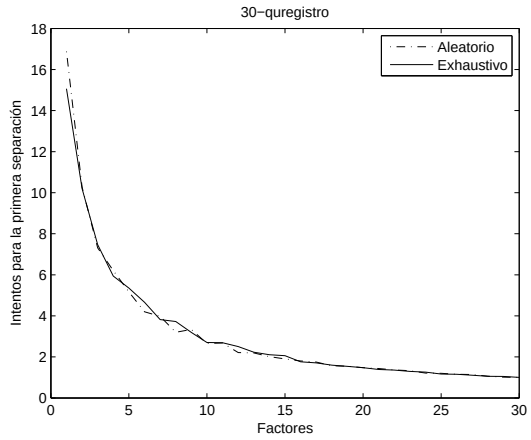


Figura 2.2: Se muestra el número de intentos para encontrar la primera separación en un 30-quregistro, variando el número de factores, para la versión aleatoria y exhaustiva. El experimento se realizó 300 veces y se promediaron la cantidad de intentos.

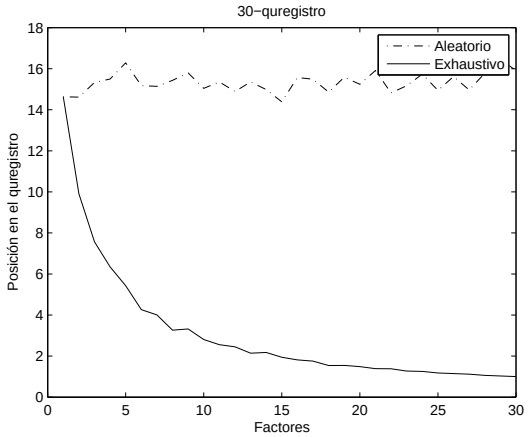


Figura 2.3: Se muestra la posición en el quregistro donde encuentra la primera separación en un 30-quregistro, variando el número de factores, para la versión aleatoria y exhaustiva. El experimento se realizó 300 veces y se promediaron las posiciones.

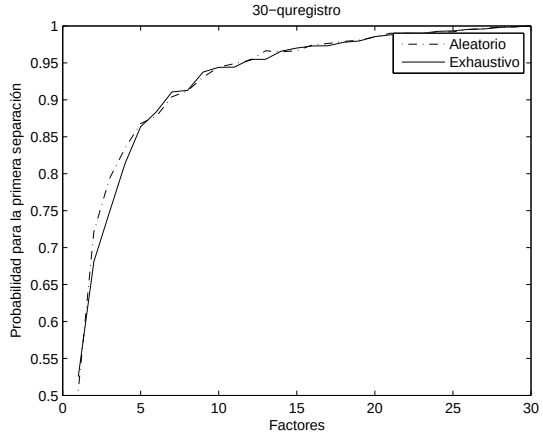


Figura 2.4: Distribución de probabilidades para encontrar la primera separación en un 30-quregistro, variando el número de factores, para la versión aleatoria y exhaustiva. El experimento se realizó 300 veces y se promediaron las probabilidades.

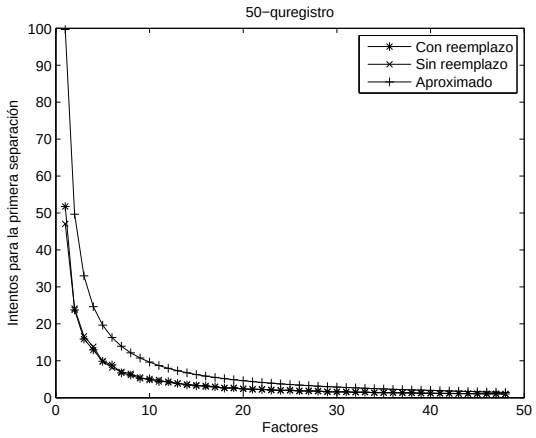


Figura 2.5: La curva superior muestra el número promedio de intentos para encontrar una primera separación dado por (2.27), las curvas inferiores muestras los resultados experimentales para los casos con y sin reemplazo, al escoger el valor de $n_0$.

es separable es el propuesto en [18], que también es de complejidad exponencial con respecto al tamaño del quregistro. El criterio empleado es el siguiente: se demuestra que dadas las bases ortonormales $\mathcal{B}_a^{(2^{d_a})} = \{|i\rangle_a : i = 0, 1, \ldots, 2^{d_a} - 1\}$ para los espacios factores $\mathbb{H}_a^{(d_a)}$. Por ejemplo, si $\mathbb{H}$ es separable como producto de dos factores, entonces existe una base para $\mathbb{H}$ dada por $\mathcal{B} = \{|i\rangle_1 \otimes |j\rangle_2 : i = 0, 1, \ldots, 2^{d_1} - 1, j = 0, 1, \ldots, 2^{d_2} - 1\}$, tal que para cualquier estado $\Psi \in \mathcal{H}$ se puede reescribir en la siguiente forma:

$$\Psi = \sum_{i=0}^{2^{d_1}-1} \sum_{j=0}^{2^{d_2}-1} C_{ij}|i\rangle_1 \otimes |j\rangle_2 \tag{2.28}$$

donde los coeficientes $C_{ij}$ son complejos y forman una matriz de $2^{d_1} \times 2^{d_2}$. Si la matriz de coeficientes satisface la condición de micro-singularidad

$$C_{ij}C_{ab} = C_{ib}C_{aj} \tag{2.29}$$

para todos los valores posibles de los índices, entonces el estado $\Psi$ es separable. Uno de los problemas al emplear este resultado es la prueba exhaustiva de la condición (2.29) de micro-singularidad, que para matrices grandes se hace impráctico en términos computacionales, ya que la dimensión del espacio de estados de un sistema cuántico crece exponencialmente con el número de qubits. Por ejemplo, empleando el criterio propuesto en [18] su costo computacional es $Ci(d_1, d_2) = O(2^{2(d_1+d_2)})$ sólo para decidir si un quregistro es separable y requiere de un cómputo extra para recuperar los factores.

# Capítulo 3

# Simulación eficiente de protocolos cuánticos basados en entrelazamiento

El propósito de la simulación del entrelazamiento es reproducir el efecto a distancia que teóricamente se predice, empleando comunicación clásica. Un esquema que se emplea para la simulación del entrelazamiento es el de *variables locales ocultas*, éstas son una fuente infinita de bits aleatorios correlacionados que especifican parámetros de valores reales. Dos protocolos que emplean este esquema son los propuestos por Steiner [16, 14, 15] y Brassard [13]. En este capítulo se explora el uso de éstos para la simulación de protocolos cuánticos.

## 3.1. Simulación del entrelazamiento

En lo que sigue se expone brevemente el protocolo de Steiner y se da una demostración alternativa del protocolo de Brassard. También se muestran dos esquemas de comunicación que emplean estados entrelazados.

## 3.2. El protocolo de Steiner

Comúnmente en los esquemas de simulación llevan a cabo sus mediciones sobre los elementos de la base de Bell. Considérese el observable,

$$M_x = \begin{pmatrix} \cos x & \operatorname{sen} x \\ \operatorname{sen} x & -\cos x \end{pmatrix} \tag{3.1}$$

donde $x \in [0, 2\pi]$, la transformación lineal $M_x : \mathbb{H} \to \mathbb{H}$, con respecto a la base canónica, con eigenvalores $\lambda_0 = -1, \lambda_1 = +1$. Denotando a los vectores canónicos como $\mathbf{e}_0 = |0\rangle$ y $\mathbf{e}_1 = |1\rangle$, entonces los eigenvectores son los siguientes:

$$\mathbf{u}_{x0} = \operatorname{sen}\frac{x}{2}\mathbf{e}_0 - \cos\frac{x}{2}\mathbf{e}_1 \tag{3.2}$$

$$\mathbf{u}_{x1} = \cos\frac{x}{2}\mathbf{e}_0 + \operatorname{sen}\frac{x}{2}\mathbf{e}_1. \tag{3.3}$$

Para cualquier $\mathbf{y} \in \mathbb{H}$, el observable $M_x$ da como resultado el eigenvalor $\lambda_i$ con probabilidad $\langle \mathbf{y}|\mathbf{u}_{xi}\rangle$. Si $\mu_x(\mathbf{y})$ es el resultado de aplicar $M_x$ sobre $\mathbf{y}$, entonces $\mu_x$ es una medición. La probabilidad de que una medición sobre un vector canónico $\mathbf{e}_i$ sea $\lambda_j$ es:

$$\Pr(\mu_x(\mathbf{e}_i) = \lambda_j) = \langle \mathbf{e}_i|\mathbf{u}_{xj}\rangle^2 = \left(\operatorname{sen}^2\frac{x}{2}\right)\delta_{ij} + \left(\cos^2\frac{x}{2}\right)(1-\delta_{ij}) \tag{3.4}$$

donde $\delta_{ij}$ es la delta de Kronecker ($\delta_{ij} = 1$ si $i = j$, $\delta_{ij} = 0$ de otro modo). A las mediciones $(M_x)_{x\in[0,2\pi]}$ son llamadas de *von Neumann*. Si $\{\mathbf{e}_{00}, \mathbf{e}_{01}, \mathbf{e}_{10}, \mathbf{e}_{11}\}$ son los vectores canónicos en $\mathbb{H}_2$, la base de Bell se puede renombrar como:

$$\begin{aligned}
\mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(\mathbf{e}_{00} + \mathbf{e}_{11}) \\
\mathbf{b}_{01} &= \frac{1}{\sqrt{2}}(\mathbf{e}_{10} + \mathbf{e}_{01}) \\
\mathbf{b}_{10} &= \frac{1}{\sqrt{2}}(\mathbf{e}_{00} - \mathbf{e}_{11}) \\
\mathbf{b}_{11} &= \frac{1}{\sqrt{2}}(\mathbf{e}_{10} - \mathbf{e}_{01})
\end{aligned} \tag{3.5}$$

Supóngase que dos partes, Alicia y Beto, aplican mediciones de von Neumann $M_{x_0}$ y $M_{x_1}$ sobre el primer y el segundo qubit de un vector en la base de Bell $\mathbf{b}_{i_0 i_1}$, respectivamente. Cuyos resultados son $\mu_{x_k}(\mathbf{e}_{i_k})$, $k = 0, 1$. De acuerdo a (3.4), para cualquier $j_0, j_1 \in \{0, 1\}$, se tiene que:

$$\begin{aligned}
&\Pr((\mu_{x_0}(\mathbf{e}_{i_0}), \mu_{x_1}(\mathbf{e}_{i_1})) = (\lambda_{j_0}, \lambda_{j_1})) \\
= \;& \frac{1}{2}\begin{cases}
\left(\cos^2\frac{x_0-(-1)^{i_0}x_1}{2}\right)\delta_{j_0 j_1} + \left(\operatorname{sen}^2\frac{x_0-(-1)^{i_0}x_1}{2}\right)(1-\delta_{j_0 j_1}) & \text{si } i_0 = i_1 \\
\left(\operatorname{sen}^2\frac{x_0-(-1)^{i_0}x_1}{2}\right)\delta_{j_0 j_1} + \left(\cos^2\frac{x_0-(-1)^{i_0}x_1}{2}\right)(1-\delta_{j_0 j_1}) & \text{si } i_0 \neq i_1
\end{cases}
\end{aligned} \tag{3.6}$$

Ahora, supóngase que Alicia y Beto comparten una sucesión $(t_n)_n$ de números aleatorios distribuidos uniformemente en el intervalo real $[0, 1]$. Supóngase que Alicia conoce el número $y_0 \in [0, 1]$ y Beto conoce el número $y_1 \in [0, 1]$. Alicia genera otra sucesión $(s_n)_n$ de números aleatorios distribuidos uniformemente en $[0, 1]$. Entonces busca un $k_0 = \min(k|s_k \leq |\cos(2\pi(t_k - y_0))|)$ y lo envía a Beto. Y Alicia da como salida el valor $a_0 = \operatorname{Sgn}(\cos(2\pi(t_{k_0} - y_0)))$. Beto recibe $k_0$ y da como salida el valor $a_1 = \operatorname{Sgn}(\cos(2\pi(t_{k_0} - y_1)))$.

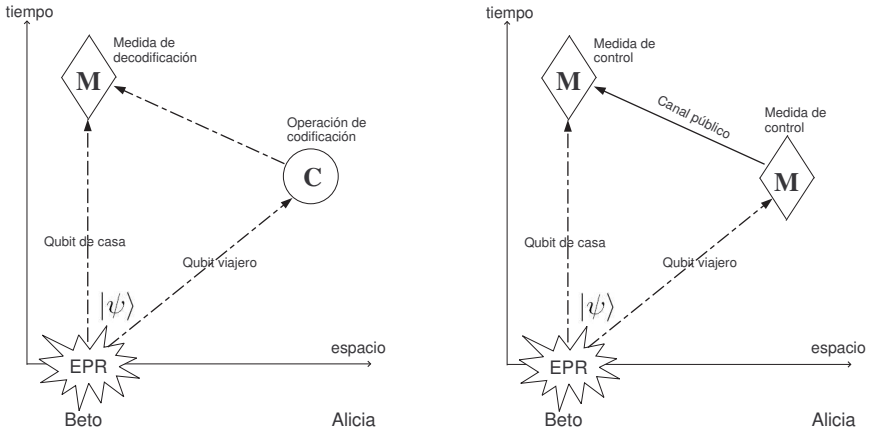


Figura 3.1: En el lado izquierdo se muestra el modo mensaje y del otro el modo control. Las flechas punteadas representan transferencia de qubits y las sólidas transferencia clásica.

Se tiene que $\Pr(a_0 = a_1) = \cos^2(2\pi(t_{k_0} - y_1))$. Así, siempre que $y_0 = y_1$, Alicia y Beto darán como salida el mismo valor. Este protocolo equivale a hacer mediciones sobre el estado $\mathbf{b}_{00}$, de acuerdo a (3.6).

A la sucesión $(t_n)_n$ se le considera como una variable local oculta.

## 3.3. Simulación empleando el protocolo de Steiner

Para simular un protocolo de comunicación cuántico se emplea el esquema de variables locales ocultas. La complejidad de la simulación de un protocolo cuántico se define como la cantidad de información clásica que se tiene que emplear para reproducir las estadísticas del mismo escenario cuántico.

Uno de los protocolos que emplean estados entrelazados es el presentado en [29, 30], llamado el protocolo *ping-pong*. Se basa en el protocolo de *códigos superdensos* (propuesto por Bennett y Wiesner en [3]). Emplea dos modos de operación, el *modo mensaje* y el *modo control*, en el primero se emplean códigos superdensos para comunicarse y en el segundo se hace una prueba de seguridad. La figura 3.1 muestra estos dos modos. Basándose en la figura 3.1 del lado derecho, un protocolo parecido es el siguiente:

Si se cuenta con una fuente de pares entrelazados creados a*priori* de los cuales Beto posee el primer qubit, y Alicia el segundo qubit. Entonces, si Alicia realiza una medición sobre su qubit y envía su resultado a Beto (a través de un canal clásico), y cuando Beto recibe el resultado de Alicia lleva a cabo una medición sobre su qubit y compara su resultado con el de Alicia, entonces si son diferentes decodifica un 1 y si son iguales decodifica un 0. Para cualquiera que pueda interferir el canal público, no puede ganar información del mensaje, por que no conoce el estado creado inicialmente por Alicia. A menos de que pueda interceptar ambos qubits.

En el protocolo de Steiner se tenía que la probabilidad de que el resultado de las

| | $\Pr[b=0]$ | $\Pr[b=1]$ |
|---|---|---|
| $\Pr[a=0]$ | $\frac{1}{2}\cos^2(\frac{x-y}{2})$ | $\frac{1}{2}\sin^2(\frac{x-y}{2})$ |
| $\Pr[a=1]$ | $\frac{1}{2}\sin^2(\frac{x-y}{2})$ | $\frac{1}{2}\cos^2(\frac{x-y}{2})$ |

Tabla 3.1: Distribución de probabilidad de los resultados $a, b$ dados por (3.1).

mediciones sean iguales es $\Pr(a_0 = a_1) = \cos^2(\pi(y_0 - y_1))$ y para $y_0 = y_1$ siempre se obtienen valores iguales para Alicia y Beto; esto equivale a simular mediciones sobre el estado de Bell $\mathbf{b}_{00}$. De igual forma, $\Pr(a_0 \neq a_1) = 1 - \Pr(a_0 = a_1) = \text{sen}^2(\pi(y_0 - y_1))$ y para $y_0 - y_1 = \pm\frac{(2k-1)}{2}$ con $k \in \mathbb{N}$, los valores de Alicia y Beto siempre serán diferentes, equivalente a realizar mediciones sobre el estado de Bell $\mathbf{b}_{01}$.

Así, para simular mediciones sobre el estado $\mathbf{b}_{00} = (1/\sqrt{2})(|00\rangle + |11\rangle)$ se emplean los parámetros $y_0 = 0, y_1 = 0$, para Alicia y Beto, respectivamente. Y para realizar mediciones sobre el estado de Bell $\mathbf{b}_{01} = (1/\sqrt{2})(|01\rangle + |10\rangle)$, se pueden emplear los parámetros $y_0 = 1/2, y_1 = 0$.

La complejidad de la simulación en el protocolo de Steiner requiere un número infinito de bits para enviar el valor correcto $t_k$ a Beto. Para evitar el esquema de variables locales ocultas se puede generar una variable aleatoria real $t = \sum_{k\geq 1} a_k 2^{-k}$ con función de densidad $p : t \mapsto \frac{\pi}{2}|\cos(2\pi(t-x))|$. En [16] se demuestra que sólo son necesarios una cierta cantidad de bits para enviar el valor de $t$ a Beto, y poder determinar el valor de $a_1 = \text{Sgn}(\cos(2\pi(t - y_1)))$. Se necesitan 5 bits de $t$ para determinar el valor de $a_1$ y para simular una medición arbitraria de von Neumann, con respecto al operador $M_x$ en (3.1) se requieren a lo más 22 bits.

## 3.4. El protocolo de Brassard

Se define un escenario de medición cuántico como una tercia de la forma $(\Psi_{AB}, M_A, M_B)$, donde $\Psi_{AB} \in \mathcal{B}_{Bell}$, $M_A$ y $M_B$ son conjuntos de medición sobre el primer y segundo componente, respectivamente. Las mediciones están dadas por el observable en (3.1) (de von Neumann). Sean $x, y \in [0, 2\pi]$ los parámetros de medición para el primer y segundo componente de $\Psi_{AB}$ y sean $a, b \in \{0, 1\}$ sus respectivos resultados. Entonces la distribución de probabilidad conjunta de sus resultados se muestra en la tabla 3.1.

Existe un esquema de variables locales ocultas que reproduce las estadísticas de esta distribución de probabilidad, que es como sigue.

A través de $x \mapsto e^{2i\pi x}$, el intervalo unitario $[0, 1]$ se identifica con el círculo unitario del plano complejo. La colección $V_{10} = \left(e^{i\frac{\pi}{5}j}\right)_{j\in[\![0,9]\!]}$ es el decágono regular del círculo unitario en $\mathbb{C}$. Para cada $j \in [\![0, 9]\!]$, sea $A_j = \{e^{2i\pi x} \in \mathbb{C} | \frac{j}{10} \leq x < \frac{j+1}{10}\}$ el arco que une al $j$-ésimo y al $(j + 1)$-ésimo vértice en el decágono regular. De igual forma, sea $t \in [0, \frac{3}{10}[$ y $j \in [\![0, 2]\!]$,

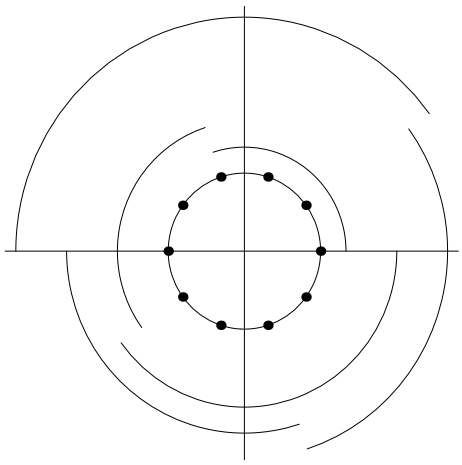

Figura 3.2: Conjuntos $B_{tj}$ y $C_{tj}$, para $t = 0$.

$$\begin{aligned} \beta_{tj} &= \frac{3}{10}j + t, \\ B_{tj} &= \left\{ e^{2i\pi x} \in \mathbb{C} |\, \beta_{tj} \leq x < \beta_{t,(j+1)\bmod 3} \right\}, \\ \gamma_{tj} &= \beta_{tj} + 1/2, \\ C_{tj} &= \left\{ e^{2i\pi x} \in \mathbb{C} |\, \gamma_{tj} \leq x < \gamma_{t,(j+1)\bmod 3} \right\}. \end{aligned} \tag{3.7}$$

En la figura 3.2, el círculo interno representa al círculo unitario, el conjunto $V_{10}$ se representa por puntos, y del radio más interno al externo, aparecen los conjuntos, cuyas proyecciones sobre el círculo unitario son $B_{t0}$, $B_{t1}$, $B_{t2}$, $C_{t0}$, $C_{t1}$, $C_{t2}$, para $t = 0$.

De la figura 3.2 se ve que aplicando una rotación de $2\pi t$ radianes, las siguientes ecuaciones se mantienen:

$$\begin{aligned} e^{2i\pi t} A_0 &= B_{t0} \cap C_{t1} \\ e^{2i\pi t} (A_1 \cup A_2) &= B_{t0} \cap C_{t2} \\ e^{2i\pi t} (A_3 \cup A_4) &= B_{t1} \cap C_{t2} \\ \\ e^{2i\pi t} A_5 &= C_{t0} \cap B_{t1} \\ e^{2i\pi t} (A_6 \cup A_7) &= C_{t0} \cap B_{t2} \\ e^{2i\pi t} (A_8 \cup A_9) &= C_{t1} \cap B_{t2} \end{aligned} \tag{3.8}$$

Sea $\mathcal{P}_t = (A_{j_a} \cap B_{tj_b} \cap C_{tj_c})_{(j_a,j_b,j_c) \in [\![0,9]\!] \times [\![0,2]\!]^2}$ la partición inducida sobre el círculo unitario. Si $t$ es un múltiplo de $\frac{1}{10}$ entonces $\mathcal{P}_t$ consiste de 10 arcos $A_j$, de otra forma consistiría de 16 arcos (cada 6 arcos $A_j$ es dividido en dos arcos). Obviamente, para cada $x \in [0, 1]$ el punto $e^{2i\pi x}$ está sobre el circulo unitario y existe una única tercia $(j_a, j_b, j_c)(x, t) \in [\![0, 9]\!] \times [\![0, 2]\!]^2$ tal que $e^{2i\pi x} \in A_{j_a(x,t)} \cap B_{tj_b(x,t)} \cap C_{tj_c(x,t)}$. Ya que $\mathcal{P}_t$ tiene a lo más 16 arcos, se necesitan 4 bits para determinar la tercia $(j_a, j_b, j_c)(x, t)$. Sea $\boldsymbol{\varepsilon}(x, t) \in \{0, 1\}^4$ la palabra de 4-bits.

El protocolo de simulación del entrelazamiento es el siguiente. Alicia y Beto comparten una variable local oculta $c \in \{0,1\}$, y acuerdan en un parámetro $t \in [0, \frac{3}{10}[$. Alicia conoce $x \in [0,1]$ y Beto conoce $y \in [0,1]$ (multiplicados por $2\pi$). Entonces siguen el procedimiento que se describe a continuación:

1. Alicia calcula $\boldsymbol{\delta} = \boldsymbol{\varepsilon}(x,t)$ y lo envía a Beto. Ella da como salida el bit $a = c$.

2. Beto calcula la tercia $(i_a, i_b, i_c)$ correspondiente a $\boldsymbol{\delta}$ y su propia tercia $(j_a, j_b, j_c) = (j_a, j_b, j_c)(y,t)$.

   *a*) Si $|i_a - j_a| > 2$ entonces $y = y + \frac{1}{2}$ y $c = 1 - c$ ;

   *b*) para cada $j \in [\![0,2]\!]$ sea $\alpha_j = \beta_{tj}$;

   *c*) Si $j_a \in \{7,8,9,0,1\}$ entonces para cada $j \in [\![0,2]\!]$ sea $\alpha_j = \gamma_{tj}$;

   *d*) Si $\exists j \in [\![0,2]\!]$: $\alpha_j \leq x, y \leq \alpha_{j+1}$ entonces se da de salida $b = c$
   En otro caso existe $j \in [\![0,2]\!]$ tal que $\alpha_j$ se encuentra entre $x$ y $y$; salida $b = c$ con probabilidad $1 - \frac{3\pi}{5}\sin(2\pi|y - \alpha_j|)$.

El procedimiento anterior reproduce las estadísticas dadas por la distribución de probabilidad de la tabla 3.1. Para verificar el comportamiento estocástico, se ve que después de aplicar la transformación hecha sobre $y$ se puede asumir que $|x - y| \leq \frac{3}{10}$. Así, $\Pr(i_b \neq j_b) = \frac{10}{3}|x - y|$ y en este caso la posición de $\alpha_j$ en el paso $(d)$ es uniforme entre $x$ y $y$, por lo tanto

$$\begin{aligned}
\Pr(a = b) &= \left(1 - \frac{10}{3}|x - y|\right) \\
&\quad + \frac{10}{3}\int_0^{|x-y|} \left(1 - \frac{3\pi}{5}\sin(2\pi u)\right) du \\
&= \frac{1}{2}\left(1 + \cos(2\pi|x - y|)\right) \\
&= \cos^2(\pi|x - y|)
\end{aligned}$$

como se requiere. Entonces para simular el entrelazamiento, con mediciones de von Neumann, se necesitan $4 = 2^2$ bits de comunicación clásica. En general para un $2^{n+1}$-quregistro, sea

$$\mathbf{b}_{0^{n+1}} = \frac{1}{2^{\frac{1}{2}}}\left(\mathbf{e}_{0^{n+1}} + \mathbf{e}_{1^{n+1}}\right), \tag{3.9}$$

la simulación requiere de $2^{n+1}$ bits de comunicación clásica. La derivación de este resultado sigue muy de cerca a la demostración dada en [13].

## 3.5. Simulación empleando el protocolo de Brassard

Si se emplea el esquema de variables locales ocultas con los parámetros $x \in \{0, \pi\}$ y $y = 0$, para Alicia y Beto, respectivamente. Producen las estadísticas siguientes: para $x = 0, y = 0$, la distribución de probabilidades es:

| | $\Pr[b=0]$ | $\Pr[b=1]$ |
|---|---|---|
| $\Pr[a=0]$ | 0.5 | 0.0 |
| $\Pr[a=1]$ | 0.0 | 0.5 |

equivalente a hacer mediciones sobre el estado $\mathbf{b}_{00} = (1/\sqrt{2})(|00\rangle + |11\rangle)$. Es decir, si $b = 0$ entonces $a = 0$ y si $b = 1, a = 1$. Para $x = \pi, y = 0$, su distribución es la siguiente:

| | $\Pr[b=0]$ | $\Pr[b=1]$ |
|---|---|---|
| $\Pr[a=0]$ | 0.0 | 0.5 |
| $\Pr[a=1]$ | 0.5 | 0.0 |

y ahora sobre el estado $\mathbf{b}_{01} = (1/\sqrt{2})(|01\rangle + |10\rangle)$. Es decir, si $b = 0$ entonces $a = 1$ y si $b = 1, a = 0$. De igual forma se puede emplear el protocolo de Steiner con parámetros similares.

La probabilidad de éxito en el protocolo es de 100 % por las características de las distribuciones. Es decir, con $x = 0, y = 0$ siempre que Alicia obtenga 0 ó 1, Beto medirá el mismo valor, y de manera similar para $x = \pi, y = 0$. Sin embargo, si se utilizan las distribuciones que producen los parámetros $x = \frac{3\pi}{8}$ y $y = \frac{\pi}{8}$, cuya distribución es la siguiente:

| | $\Pr[b=0]$ | $\Pr[b=1]$ |
|---|---|---|
| $\Pr[a=0]$ | 0.425 | 0.075 |
| $\Pr[a=1]$ | 0.075 | 0.425 |

y con los parámetros $x = \frac{11\pi}{8}, y = \frac{\pi}{8}$, su distribución de probabilidades es:

| | $\Pr[b=0]$ | $\Pr[b=1]$ |
|---|---|---|
| $\Pr[a=0]$ | 0.075 | 0.425 |
| $\Pr[a=1]$ | 0.425 | 0.075 |

Entonces la probabilidad de éxito es del 85 %. Por ejemplo, para $x = \frac{3\pi}{8}, y = \frac{\pi}{8}$; si Alicia obtiene un 1, habrá una probabilidad alta de que Beto mida un 1, pero también se puede dar el caso de que mida un 0 (con probabilidad de 7.5 %). Considérese la siguiente distribución,

| | $\Pr[b=0]$ | $\Pr[b=1]$ |
|---|---|---|
| $\Pr[a=0]$ | $p_0$ | $p_1$ |
| $\Pr[a=1]$ | $p_1$ | $p_0$ |

donde $0 \leq p_0, p_1 \leq \frac{1}{2}$ y se debe de cumplir que $2(p_0 + p_1) = 1$. Así, si Alicia obtiene un 0 ó 1, la probabilidad de que Beto mida el mismo valor es $p_0$ y de que mida diferente valor es $p_1$. Para transmitir un mensaje de $n$ bits de Alicia hacia Beto, tienen que emplear la siguiente codificación:

$$\text{Si } a = b \text{ entonces decodifica } 0$$
$$\text{Si } a \neq b \text{ entonces decodifica } 1$$

para codificar un cero se emplean las probabilidades $p_0, p_1$ y para codificar un uno se emplean $p_0^{'}, p_1^{'}$. Se tiene que la probabilidad de éxito en la codificación de los 0's es $2p_0$ y para la codificación de los 1's es $2p_1^{'}$. Resulta entonces que la probabilidad de que el mensaje se transmita correctamente es $p_m = p_0 + p_1^{'}$. Este tipo de escenario podría emplearse para aumentar la seguridad contra ataques. Si se introduce un factor de incertidumbre dado por las distribuciones de probabilidad, para cualquiera que pueda intervenir el protocolo, le sería más difícil recuperar el mensaje enviado.

# Capítulo 4

# Sistemas entrelazados y protocolos de comunicaciones

Actualmente se han propuesto esquemas de comunicación empleando estados entrelazados tales como la Distribución de llaves (QKD, *Quantum Key Distribution*) [31], comunicación cuántica segura (QSDC, *Quantum Secure Direct Communication*) [32], para compartir mensajes secretos (QSS, *Quantum Secret Sharing*) [31], entre otros. Uno de ellos es el protocolo de códigos superdensos (ver capítulo 1). Permite la transmisión de dos bits empleando un sólo qubit, aprovechando las propiedades de no-localidad del entrelazamiento, aplicando transformaciones de Pauli. En la versión original del protocolo involucra a dos partes, una que aplica una transformación unitaria sobre un estado de Bell para luego enviarlo a la parte receptora, quien lleva a cabo una medición en la base de Bell; y ya que los estados de Bell forman una base ortonormal, el nuevo estado puede ser distinguido sin ambigüedad.

En este capítulo se trata el problema de la generalización a varias partes del protocolo de códigos superdensos. Primero se propone el uso de estados cuánticos multidimensionales para implementar un protocolo de dos partes, para luego seguir con su generalización a varias partes. También se propone un protocolo de tres partes con el uso de transformaciones de Pauli y se considera su versión multipartes. A lo largo de este capítulo se detallan los protocolos propuestos así como los problemas que se presentan cuando se quiere generalizar a más de dos partes. Al final del capítulo se comentan las implicaciones de este tipo de protocolos.

## 4.1. Códigos superdensos de varias partes

En un espacio de dimensión mayor a dos se trabaja con una base de Bell generalizada y el esquema de comunicación cambia de muchos a uno (muchos codifican y uno decodifica). Dos trabajos relacionados con la generalización del protocolo son [33, 34], en ambos se propone un protocolo de $(N+1)$ partes (uno decodifica y N envían) que comparten un estado entrelazado de $(N+1)$-qubits. La parte receptora tiene el primer qubit y los restantes, las $N$ partes codificadoras que aplican una transformación uni-

Tabla 4.1: Cada entrada $T_{\boldsymbol{\varepsilon\delta}}$ es tal que $\mathbf{b}_{\boldsymbol{\varepsilon}} = T_{\boldsymbol{\varepsilon\delta}}\mathbf{b}_{\boldsymbol{\delta}}$.

| $\mathbf{b}_{\boldsymbol{\varepsilon}} \setminus \mathbf{b}_{\boldsymbol{\delta}}$ | $\mathbf{b}_{00}$ | $\mathbf{b}_{01}$ | $\mathbf{b}_{10}$ | $\mathbf{b}_{11}$ |
|---|---|---|---|---|
| $\mathbf{b}_{00}$ | $\tau_{00}$ | $\tau_{01}$ | $\tau_{10}$ | $-i\,\tau_{11}$ |
| $\mathbf{b}_{01}$ | $\tau_{01}$ | $\tau_{00}$ | $-i\,\tau_{11}$ | $\tau_{10}$ |
| $\mathbf{b}_{10}$ | $\tau_{10}$ | $-i\,\tau_{11}$ | $\tau_{00}$ | $\tau_{01}$ |
| $\mathbf{b}_{11}$ | $-i\,\tau_{11}$ | $\tau_{10}$ | $\tau_{01}$ | $\tau_{00}$ |

taria. Cuando el receptor recibe los qubits de las $N$ partes, lleva a cabo una medición en la base de Bell generalizada y puede distinguir de qué estado se trata. Debido a que el número de transformaciones unitarias es mayor al número de elementos en la base de Bell, es difícil para la parte receptora, saber qué transformaciónes aplicaron las $N$ partes. Por lo que se tiene que restringir el número de las mismas, a un subconjunto de ellas que sean fácilmente identificables. Reduciendo así, el número de bits que se pueden codificar por qubit, que es de dos bits en el protocolo de códigos superdensos. Si se numeran las matrices de Pauli,

$$\begin{aligned}\sigma_{00} &= \sigma_0,\\ \sigma_{01} &= \sigma_x,\\ \sigma_{10} &= \sigma_y,\\ \sigma_{11} &= \sigma_z,\end{aligned}$$

Entonces, haciendo $\tau_{ij} = (\sigma_{00} \otimes \sigma_{ij})$ cada vector en la base de Bell puede ser transformado en otro por múltiplos constantes de matrices $\tau_{ij}$. En la tabla 4.1 se muestra esta transformación, donde cada entrada de la matriz $T_{\boldsymbol{\varepsilon\delta}}$ es tal que $\mathbf{b}_{\boldsymbol{\varepsilon}} = T_{\boldsymbol{\varepsilon\delta}}\mathbf{b}_{\boldsymbol{\delta}}$. Esto permite un protocolo de códigos superdensos de dos partes, donde se logra codificar 2 bits por qubit. Empleando la tabla 4.1 es posible conocer el estado resultante después de aplicar una transformación $\sigma_{ij}$. En el protocolo original se emplean transformaciones de Pauli, en lo que sigue se considera el uso de transformaciones aplicadas a qubits de dimensión $k$.

Sea $k \geq 2$ un entero positivo y sea $\rho_k = e^{i\frac{2\pi}{k}}$ la *$k$-ésima raíz primitiva de la unidad.* Sea $\mathbb{H}_1^{(k)} = \mathbb{C}^k$ el espacio complejo de Hilbert de dimensión $k$ y sean $\mathbf{e}_0$, …, $\mathbf{e}_{k-1}$ los vectores en su base canónica. Para cualquier $m, n \in [\![0, k-1]\!]$ sea

$$\mathbf{b}_{mn} = \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \rho_k^{jm} \mathbf{e}_j \otimes \mathbf{e}_{(j+n) \bmod k}. \tag{4.1}$$

Entonces $B_{k2} = (\mathbf{b}_{mn})_{m,n\in[\![0,k-1]\!]}$ es una base ortonormal en $\mathbb{H}_2^{(k)} = \mathbb{H}_1^{(k)} \otimes \mathbb{H}_1^{(k)}$. Para cualquier $m, n \in [\![0, k-1]\!]$ sea $U_{mn} = [u_{mn\mu\nu}]_{\mu,\nu\in[\![0,k-1]\!]}$ la matriz con entradas en el círculo unitario de $\mathbb{C}$ tal que

$$u_{mn\mu\nu} = \rho_k^{m\nu} \delta_{\mu,(\nu+n) \bmod k}, \tag{4.2}$$

donde, $\delta_{ij}$ es la delta de Kronecker. Entonces,

$$U_{mn}\mathbf{e}_j = \sum_{\mu=0}^{k-1} \rho_k^{mj} \delta_{\mu,(j+n) \bmod k} \mathbf{e}_\mu = \rho_k^{mj} \mathbf{e}_{(j+n) \bmod k} \tag{4.3}$$

y, denotando por $\mathbf{1}_k$ a la matriz identidad de orden $k$, se tiene

$$\begin{aligned}
(\mathbf{1}_k \otimes U_{mn})\, \mathbf{b}_{00} &= (\mathbf{1}_k \otimes U_{mn}) \left( \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \mathbf{e}_j \otimes \mathbf{e}_j \right) \\
&= \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} (\mathbf{1}_k \otimes U_{mn}) (\mathbf{e}_j \otimes \mathbf{e}_j) \\
&= \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \mathbf{e}_j \otimes U_{mn}\mathbf{e}_j \\
&= \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \rho_k^{mj} \mathbf{e}_j \otimes \mathbf{e}_{(j+n) \bmod k} \\
&= \mathbf{b}_{mn}
\end{aligned} \tag{4.4}$$

Sea $C_k = \left[\delta_{\mu,(\nu+1) \bmod k}\right]_{\mu,\nu \in [\![0,k-1]\!]}$ la matriz que representa la transformación lineal dada como la "rotación" de la base canónica $\mathbf{e}_\nu \mapsto \mathbf{e}_{(\nu+1) \bmod k}$. Entonces, de la relación (4.2) se puede ver que

$$\begin{aligned}
\forall m,n: \quad U_{mn} &= C_k^n U_{m0} = C_k^n U_{10}^m \\
&= C_k^n \left( \operatorname{diag} \left[\rho_k^\nu\right]_{\nu \in [\![0,k-1]\!]} \right)^m .
\end{aligned} \tag{4.5}$$

Además,

$$U_{10} C_k = \rho_k C_k U_{10}. \tag{4.6}$$

Consecuentemente, $U_{10} C_k^p = \rho_k^p C_k^p U_{10}$ y $U_{10}^q C_k^p = \rho_k^q C_k^p U_{10}^q$, lo cual implica

$$\forall m,n,p,q: \quad U_{mn} U_{pq} = \rho_k^{nq} U_{(m+p) \bmod k,(n+q) \bmod k}. \tag{4.7}$$

Así,

$$\begin{aligned}
(\mathbf{1}_k \otimes U_{mn})\, \mathbf{b}_{pq} &= (\mathbf{1}_k \otimes U_{mn}) \circ (\mathbf{1}_k \otimes U_{pq})\, \mathbf{b}_{00} \\
&= (\mathbf{1}_k \otimes (U_{mn} U_{pq}))\, \mathbf{b}_{00} \\
&= \rho_k^{nq} \left( \mathbf{1}_k \otimes U_{(m+p) \bmod k,(n+q) \bmod k} \right) \mathbf{b}_{00} \\
&= \rho_k^{nq}\ \mathbf{b}_{(m+p) \bmod k,(n+q) \bmod k},
\end{aligned} \tag{4.8}$$

y

$$\forall m,n,p,q: \left[ \rho_k^{-(m-p)(n-q) \bmod k} \left( \mathbf{1}_k \otimes U_{(m-p) \bmod k,(n-q) \bmod k} \right) \right] \mathbf{b}_{pq} = \mathbf{b}_{mn}. \tag{4.9}$$

La ecuación (4.4) permite un protocolo de códigos superdensos de dos partes que trabaja con el estado $\mathbf{b}_{00}$. Pero las ecuaciones (4.8) y (4.9) permiten un protocolo más general que trabaja con cualquier elemento en la base de Bell:

1. Dos partes, Alicia y Beto, convienen en un estado entrelazado $\mathbf{b}_{pq}$.

2. Beto aplica una transformación $U_{uv}$ a su qubit para producir un desplazamiento de fase en $\mathbf{b}_{mn}$, de acuerdo a la ecuación (4.8), y envía su qubit a Alicia.

3. Conociendo ambos qubits, Alicia tiene en su posesión un desplazamiento de fase en $\mathbf{b}_{mn}$. Ella lleva a cabo una medición en la base de Bell $B_{k2}$, y puede reconocer $\mathbf{b}_{mn}$ y usando la ecuación (4.9) puede saber que transformación $U_{uv}$ aplicó Beto.

Con la transmisión de un qubit, Beto puede comunicar $\log_2 k^2$ bits clásicos a Alicia. Aunque el uso de cualquier elemento de la base de Bell no mejora la razón de bits transmitidos, se pueden seguir las ideas del protocolo de Códigos Superdensos Dobles (*Double Dense Coding*) propuesto en [30]. El protocolo funciona como el de códigos superdensos, pero cuando Alicia recupera el estado transformado, le envía a Beto el resultado de su medición (a través de un canal clásico). Entonces Beto puede calcular el estado inicial generado por Alicia al invertir la ecuación (4.9) dada por (4.10). Y así, recibir $\log_2 k^2$ bits de Alicia (ya que hay $k^2$ estados en la base de Bell). En este esquema se comparten $2\log_2 k^2$ bits entre Alicia y Beto.

$$\left[\left(\rho_k^{-(m-p)(n-q)\bmod k}\right)^{-1}\left(\mathbf{1}_k\otimes U_{(m-p)\bmod k,(n-q)\bmod k}\right)^{-1}\right]\mathbf{b}_{mn}=\mathbf{b}_{pq}. \tag{4.10}$$

### 4.1.1. Protocolo de varias partes

Sea $k\geq 2$ un entero positivo, y sea $\mathbb{H}_k^{(k)}=\left(\mathbb{H}_1^{(k)}\right)^{\otimes k}$ el producto tensorial de potencia $k$ de $\mathbb{H}_1^{(k)}=\mathbb{C}^k$. Para cualquier $n_0,n_1,\ldots,n_{k-1}\in[\![0,k-1]\!]$ sea

$$\mathbf{b}^{(k)}_{n_0n_1\cdots n_{k-1}}=\frac{1}{\sqrt{k}}\sum_{j=0}^{k-1}\rho_k^{jn_0}\mathbf{e}_j\otimes\bigotimes_{\ell=1}^{k-1}\mathbf{e}_{(j+n_\ell)\bmod k}. \tag{4.11}$$

Entonces $B_{kk}=\left(\mathbf{b}^{(k)}_{n_0n_1\cdots n_{k-1}}\right)_{n_0,n_1,\ldots,n_{k-1}\in[\![0,k-1]\!]}$ es una base ortonormal de $\mathbb{H}_k^{(k)}$. Como en la ecuación. (4.8), se tiene que

$$\left(\mathbf{1}_k\otimes\bigotimes_{\ell=1}^{k-1}U_{p_\ell q_\ell}\right)\mathbf{b}^{(k)}_{n_0n_1\cdots n_{k-1}}=\rho_k^{\sum_{\ell=1}^{k-1}q_\ell n_\ell}\,\mathbf{b}^{(k)}_{(n_0+\sum_{\ell=1}^{k-1}p_\ell)\bmod k,(q_1+n_1)\bmod k,\cdots,(q_{k-1}+n_{k-1})\bmod k} \tag{4.12}$$

la cual da una equivalencia de la forma (4.9), que transforma un registro en la base de Bell en otro registro en la misma base. La ecuación (4.12) permite realizar un protocolo de $k$ partes, un receptor y $k-1$ que envían. Sin embargo, en este caso existen $\left(k^2\right)^{k-1}=k^{2k-2}$ transformaciones de la forma $\left(\mathbf{1}_k\otimes\bigotimes_{\ell=1}^{k-1}U_{p_\ell q_\ell}\right)$ y hay $k^k$ estados en la base de Bell. Se puede ver que para cualquiera $\mathbf{b}^{(k)}_{n_0n_1\cdots n_{k-1}}$, $\mathbf{b}^{(k)}_{m_0m_1\cdots m_{k-1}}$ hay

exactamente $\frac{k^{2k-2}}{k^k} = k^{k-2}$ transformaciones que llevan del primer vector al segundo vector. Por lo que no existe una transformación única para un vector dado.

Escogiendo un subconjunto de las $k^{2k-2}$ transformaciones de tamaño $k^k$, de forma que lleven de un vector dado a un vector único en la base Bell. Se puede implementar un protocolo de varias partes, pero la cantidad de bits transmitidos por qubit se reduce. Sean los subconjuntos $U^r_{m_0 m_1 \cdots m_{k-1}} \subset \left(\mathbf{1}_k \otimes \bigotimes_{\ell=1}^{k-1} U_{p_\ell q_\ell}\right)$ para $r \in [\![0, k^{k-2}-1]\!]$, tal que

$$U^r_{m_0 m_1 \cdots m_{k-1}} \mathbf{b}^{(k)}_{n_0 n_1 \cdots n_{k-1}} = \mathbf{b}^{(k)}_{m_0 m_1 \cdots m_{k-1}}, \tag{4.13}$$

los subconjuntos que transforman de manera única el vector $\mathbf{b}^{(k)}_{n_0 n_1 \cdots n_{k-1}}$ a un elemento en $B_{kk}$. Ya que $\text{card}(U^r_{m_0 m_1 \cdots m_{k-1}}) = k^k$, se logra enviar un mensaje de $\log_2 k^k$ bits clásicos empleando cualquier subconjunto $r$ para la codificación. En general para cualquier vector $\mathbf{b}^{(k)}_{n_0 n_1, \cdots n_{k-1}}$ cada subconjunto $r$ en $\left(\mathbf{1}_k \otimes \bigotimes_{\ell=1}^{k-1} U_{p_\ell q_\ell}\right)$ que transforma de manera única a un vector en $B_{kk}$ es tal que sus índices $p_\ell q_\ell$ son de la siguiente forma: para $p = \sum_{\ell=1}^{k-1} p_\ell$ fija, con $p \in [\![0, k-1]\!]$, los valores $q_\ell = q_1 q_2 \cdots q_{k-1}$ siguen un orden lexicográfico.

En la siguiente sección se propone un protocolo de varias partes basado en las transformaciones de Pauli que sigue las mismas ideas presentadas aquí.

## 4.2. Protocolo de varias partes usando transformaciones de Pauli

El protocolo de códigos superdensos [3] se basa en transformaciones de Pauli para transmitir 2 bits, y sólo considera un escenario de dos partes. Aquí se propone la extensión del protocolo a varias partes, comenzando con un protocolo de tres partes.

Sean los estados siguientes una base $\mathcal{B}_{Bell}$ en $\mathbb{H}_3 = \mathbb{C}^{2^3}$:

$$\begin{aligned}
\phi_0^{\pm} &= (1/\sqrt{2})(|000\rangle \pm |111\rangle) \\
\phi_1^{\pm} &= (1/\sqrt{2})(|001\rangle \pm |110\rangle) \\
\phi_2^{\pm} &= (1/\sqrt{2})(|010\rangle \pm |101\rangle) \\
\phi_3^{\pm} &= (1/\sqrt{2})(|011\rangle \pm |100\rangle)
\end{aligned} \tag{4.14}$$

De los cuales Alicia, Beto y Carolina tienen el primero, segundo y tercer qubit, respectivamente. Los dos últimos aplican transformaciones de Pauli de la forma $(\sigma_0 \otimes \sigma_b \otimes \sigma_c)$ donde Beto aplica $\sigma_b$ y Carolina aplica $\sigma_c$. Entonces para cualquier estado $\phi_n^{\pm}$, las posibles transformaciones que se pueden hacer se muestran en la tabla 4.2.

Por la simetría de la tabla 4.2 no es posible saber qué transformaciones producen un estado en particular. Considére la transformación $\theta : \sigma_b \otimes \sigma_c \mapsto bc$ donde $b, c \in \{0, 1, 2, 3\}$. Si se aplica $\theta$ de la siguiente forma:

$$\theta(\sigma_b \otimes \sigma_c) \to (b_1 \oplus b_2) \cdot (c_1 \oplus c_2) \tag{4.15}$$

Tabla 4.2: Resultado de aplicar transformaciones de Pauli ($\sigma_0 \otimes \sigma_b \otimes \sigma_c$) sobre el estado $\phi_n^{\pm}$. Los renglones corresponden a $\sigma_b$ y las columnas a $\sigma_c$.

| $\mathcal{B}_{Bell}\otimes$ | $\sigma_0$ | $\sigma_x$ | $\sigma_y$ | $\sigma_z$ |
|---|---|---|---|---|
| $\sigma_0$ | $\phi_n^{\pm}$ | $\phi_{(1+3n) \mod 4}^{\pm}$ | $\phi_{(1+3n) \mod 4}^{\mp}$ | $\phi_n^{\mp}$ |
| $\sigma_x$ | $\phi_{(n+2) \mod 4}^{\pm}$ | $\phi_{(3-n) \mod 4}^{\pm}$ | $\phi_{(3-n) \mod 4}^{\mp}$ | $\phi_{(n+2) \mod 4}^{\mp}$ |
| $\sigma_y$ | $\phi_{(n+2) \mod 4}^{\mp}$ | $\phi_{(3-n) \mod 4}^{\mp}$ | $\phi_{(3-n) \mod 4}^{\pm}$ | $\phi_{(n+2) \mod 4}^{\pm}$ |
| $\sigma_z$ | $\phi_n^{\mp}$ | $\phi_{(1+3n) \mod 4}^{\mp}$ | $\phi_{(1+3n) \mod 4}^{\pm}$ | $\phi_n^{\pm}$ |

donde $b_1 b_2$ y $c_1 c_2$ es la representación binaria de $b, c$. Entonces es posible codificar dos bits, sin importar que transformaciones se apliquen. Por ejemplo, para el estado $\phi_0^-$ la tabla de transformaciones es la siguiente:

| $\mathcal{B}_{Bell}\otimes$ | $\sigma_0$ | $\sigma_x$ | $\sigma_y$ | $\sigma_z$ |
|---|---|---|---|---|
| $\sigma_0$ | $\phi_0^-$ | $\phi_1^-$ | $\phi_1^+$ | $\phi_0^+$ |
| $\sigma_x$ | $\phi_2^-$ | $\phi_3^-$ | $\phi_3^+$ | $\phi_2^+$ |
| $\sigma_y$ | $\phi_2^+$ | $\phi_3^+$ | $\phi_3^-$ | $\phi_2^-$ |
| $\sigma_z$ | $\phi_0^+$ | $\phi_1^+$ | $\phi_1^-$ | $\phi_0^-$ |

Si el estado resultante es $(\sigma_0 \otimes \sigma_b \otimes \sigma_c)\phi_0^- \rightarrow \phi_3^-$, entonces Beto y Carolina aplicaron ya sea $\sigma_x \otimes \sigma_x$ ó $\sigma_y \otimes \sigma_y$. En ambos casos Alicia decodifica:

$$\begin{aligned} \theta(\sigma_x \otimes \sigma_x) &\rightarrow (0 \oplus 1) \cdot (0 \oplus 1) = 11 \\ \theta(\sigma_y \otimes \sigma_y) &\rightarrow (1 \oplus 0) \cdot (1 \oplus 0) = 11 \end{aligned} \tag{4.16}$$

Además, si se dispone de un canal de comunicación clásico, Beto podría enviar un bit a Alicia para indicarle que están usando ya sean las transformaciones $\sigma_0, \sigma_x$ ó $\sigma_y, \sigma_z$. De este modo Alicia puede distinguir que transformaciones se aplicaron, y recibir un mensaje de 4 bits. El protocolo es parecido al propuesto en [30] pero extendido a tres partes.

### 4.2.1. Extensión a varias partes

Dado un espacio de Hilbert $\mathbb{H}_n$ con base de Bell $\mathcal{B}_{Bell} = \{\phi_0, \ldots, \phi_{2^n-1}\}$, considérese las transformaciones aplicadas a $\phi_0$ de la siguiente forma:

$$\left( \sigma_0 \otimes \bigotimes_{i=1}^{n-1} \sigma_i \right) \phi_0 \in \mathcal{B}_{Bell} \tag{4.17}$$

Escritas como $U_i \phi_0 \sim \psi \in \mathcal{B}_{Bell}$. Aquí sucede lo mismo como en la ecuación (4.12) donde el número de matrices es mayor al número de elementos en la base de Bell. Por

Tabla 4.3: Subconjuntos $U_{k,i}^t$, para $n = 4$. Cada columna muestra los índices de las transformaciones de la forma $\sigma_0 \otimes \sigma_b \otimes \sigma_c \otimes \sigma_d$.

| $U_{k,0}^0$ | $U_{k,0}^1$ | $U_{k,0}^2$ | $U_{k,0}^3$ | |
|---|---|---|---|---|
| 0000 | 0033 | 0303 | 0330 | $\phi_0$ |
| 0001 | 0032 | 0302 | 0331 | $\phi_1$ |
| 0010 | 0023 | 0313 | 0320 | $\phi_2$ |
| 0011 | 0022 | 0312 | 0321 | $\phi_3$ |
| 0100 | 0133 | 0203 | 0230 | $\phi_4$ |
| 0101 | 0132 | 0202 | 0231 | $\phi_5$ |
| 0110 | 0123 | 0213 | 0220 | $\phi_6$ |
| 0111 | 0122 | 0212 | 0221 | $\phi_7$ |
| 0112 | 0121 | 0211 | 0222 | $\phi_8$ |
| 0113 | 0120 | 0210 | 0223 | $\phi_9$ |
| 0102 | 0131 | 0201 | 0232 | $\phi_{10}$ |
| 0103 | 0130 | 0200 | 0233 | $\phi_{11}$ |
| 0012 | 0021 | 0311 | 0322 | $\phi_{12}$ |
| 0013 | 0020 | 0310 | 0323 | $\phi_{13}$ |
| 0002 | 0031 | 0301 | 0332 | $\phi_{14}$ |
| 0003 | 0030 | 0300 | 0333 | $\phi_{15}$ |

Tabla 4.4: Algoritmo para construir los conjuntos $U_{k,0}^t$, dado $U_{k,0}^0$.

**Entrada.** $(n,\ n',\ \alpha,\ U_k^t,\ \Delta)$
**Salida.** índices de las matrices $U_{k_i}^0$, para
$t = 1, \ldots, 2^{n-2} - 1$ con $k$ fija
**Procedimiento.** Construye
{
`Indice`$(U_k^{\alpha+2^{n'-1}}) =$ `Indice`$(U_k^{\alpha})$
`Invierte`$(U_k^{\alpha+2^{n'-1}}, \Delta)$
`Invierte`$(U_k^{\alpha+2^{n'-1}}, n-1)$
Si $n' - 1 > 0$ entonces
Construye$(n, n' - 1, \alpha, U_k^t, \Delta + 1)$
Construye$(n, n' - 1, \alpha + 2^{n'-1}, U_k^t, \Delta + 1)$
}

lo que existen matrices que llevan a un mismo elemento en $\mathcal{B}_{Bell}$. Se puede ver que hay exactamente $2^{n-2}$ subconjuntos que satisfacen la siguiente relación:

$$U^t_{k,i}\phi_i \sim \phi_k, \quad \begin{array}{l} k,i \in [\![0, 2^n-1]\!] \\ t \in [\![0, 2^{n-2}-1]\!] \end{array} \tag{4.18}$$

Por ejemplo, la tabla 4.3 muestra los subconjuntos para $n = 4$ aplicados al estado $\phi_0$. En particular las matrices $U^0_{k,0}$ se pueden formar de la siguiente manera:

$$U^0_{k,0} = \begin{cases} \sigma_0 \otimes \sigma_{(k)_{2,0}} \otimes \sigma_{(k)_{2,1}} \otimes \cdots \otimes \sigma_{(k)_{2,n-1}} & \text{si } k < 2^{n-1} \\ \sigma_0 \otimes \sigma_{(r)_{2,0}} \otimes \cdots \otimes \sigma_{(r)_{2,n-2}} \otimes \sigma_{\neg((r)_{2,n-1})\cdot 1} & \text{si } 2^{n-1} \leq k < 2^n - 1 \end{cases} \tag{4.19}$$

donde $r = 2^n - k - 1$, y la notación $(k)_{2,j}$ quiere decir, el $j$-ésimo bit del número $k$ en base 2, representado con $n-1$ bits. Al formar las matrices $U_k$ se considera el valor decimal del índice $(k)_{2,j}$, y $j$ va del bit más significativo al menos significativo.

Ahora considérese la construcción de las matrices $U^t_{k,0}$ para $t \in [\![0, 2^{n-2}-1]\!]$ y $k \in [\![0, 2^n - 1]\!]$. Para $k$ fija se obtienen todas la matrices aplicadas a $\phi_0$ que resultan en el estado $\phi_k$. Un algoritmo para construir las matrices se muestra en la tabla 4.4, donde la función $\texttt{Indice}(U^\alpha_k) = \texttt{Indice}(U^\beta_k)$, iguala los índices de las transformaciones de Pauli y la función $\texttt{Invierte}(U^t_k, i)$ invierte el índice de la $i$-ésima transformación de Pauli $\sigma_i$ en la matriz $U^t_k$, mediante las siguientes equivalencias:

$$\begin{aligned} \sigma_0 &\leftrightarrow \sigma_3 \\ \sigma_1 &\leftrightarrow \sigma_2 \end{aligned} \tag{4.20}$$

La llamada inicial al algoritmo se hace con $\alpha = 0$, $\Delta = 1$ y $n' = n-2$, para $\mathbb{H}_{n>3}$. El algoritmo de la tabla 4.4 se basa en el siguiente hecho:

**Proposición 4.2.1** *Para cualquier matriz de transformación $U^t_{k,i}$, tal que $U^t_{k,i}\phi_i \sim \phi_k$, si se intercambian dos índices $i, j \in [\![0, n-1]\!]$, $i \neq j$ según (4.20), entonces:*

$$(\sigma_{t_0} \otimes \sigma_{t_i} \otimes \cdots \otimes \sigma_{t_j} \otimes \sigma_{t_{n-1}})\phi_i \sim \phi_k. \tag{4.21}$$

Es fácil ver que la relación (4.21) se cumple escribiendo la matriz $U^t_k$ de la forma siguiente: $U^t_k = D \otimes (\sigma_{t_i} \otimes A) \otimes (\sigma_{t_j} \otimes B)$. Si se cambia sólo un índice digamos $G \otimes (\sigma_{t_j} \otimes B)$, se quita o introduce un signo, por lo que el estado $\phi_k$ cambia de fase. Entonces al cambiar el segundo índice balancea el primer cambio de índices. Esto se debe a que después de hacer cualquier cambio de índices la forma de la matriz no cambia salvo los signos y las entradas complejas.

### 4.2.2. Extensión con la transmisión de bits clásicos

Si se permite el envío de un bit $b$ por cada una de las $n-1$ partes transmisoras, indicando $b = 0$ si se aplica $\sigma_0$ ó $\sigma_1$ y $b = 1$ si se aplica $\sigma_2$ ó $\sigma_3$. Entonces es posible distinguir cada subconjunto de transformaciones dados en (4.18).

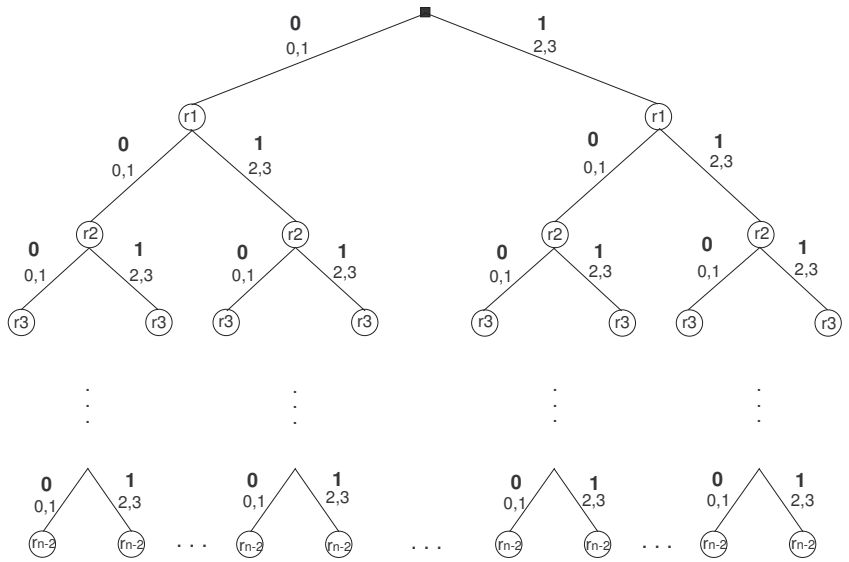


Figura 4.1: Estructura de árbol formada por las matrices $U_\alpha^t$. Las ramas izquierdas se recorren con 0 y las derechas con 1. Para un estado $\phi_\alpha$, las matrices $U_\alpha^t$ definen los pesos en el árbol.

Esto se puede ver de la siguiente forma. Para las matrices $U^t = \sigma_0 \otimes \sigma_{r_1} \otimes \cdots \otimes \sigma_{r_{n-1}}$ divídase en dos conjuntos $t \in [\![0, 2^{n-2} - 1]\!] = [\![0, 2^{n-3} - 1]\!] \cup [\![2^{n-3}, 2^{n-2} - 1]\!]$ para los cuales el índice $\sigma_{r_1} = \sigma_0, \sigma_1$ y $\sigma_{r_1} = \sigma_2, \sigma_3$, respectivamente. Hágase lo mismo para cada subconjunto, tal que se cumpla para $\sigma_{r_2}$. Y así sucesivamente hasta $\sigma_{r_{n-2}}$.

Este orden introducido induce una representación de árbol como se muestra en la figura 4.1. Donde cada nodo en el árbol indica un subconjunto de matrices. Los nodos en el nivel 1 del árbol de la figura 4.1 son dos subconjuntos (el nodo izquierdo y derecho), que tienen como índice $\sigma_{r_1} = \sigma_0, \sigma_1$ en el nodo izquierdo y $\sigma_{r_1} = \sigma_2, \sigma_3$ en el derecho.

Por ejemplo, los índices de las transformaciones en $\mathbb{H}_5$, tales que $U_{27,0}^t \phi_0 \sim \phi_{27}$ son: $U_{27,0}^t = \{00103, 00130, 00200, 00233, 03100, 03133, 03203, 03230\}$. Cada quinta es de la forma $(\sigma_0 \otimes \sigma_{r_1} \otimes \sigma_{r_2} \otimes \sigma_{r_3} \otimes \sigma_{r_4})$. La figura 4.2 muestra el árbol formado por las matrices $U_{27,0}^t$. Si la cadena de bits recibida es "1000"; existen 8 cadenas posibles al recorrer el árbol que son:

| | |
|---|---|
| 0200 | 0300 |
| 0201 | 0301 |
| 0210 | <u>0310</u> |
| 0211 | 0311 |

La cadena recuperada es 0310 que define al último índice que es 0. Así con la transmisión de un bit es posible obtener los índices de las transformaciones.

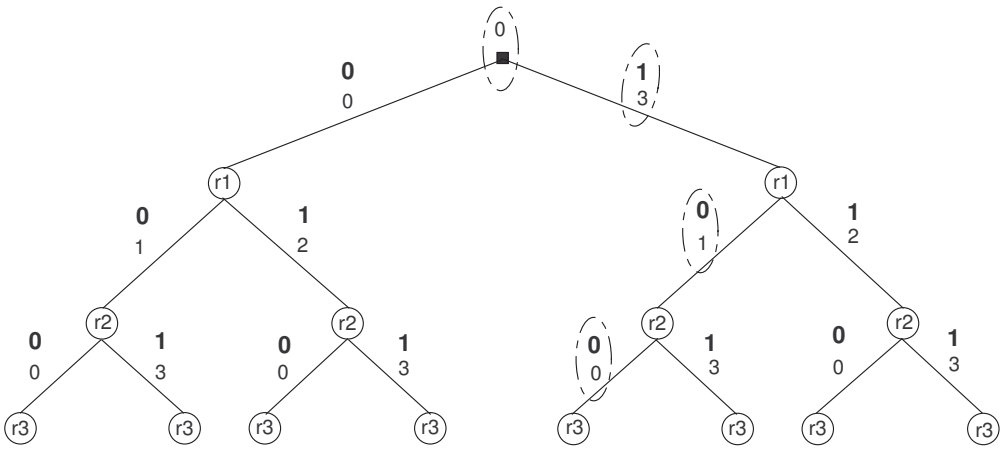


Figura 4.2: Árbol formado por las matrices $U^t_{27,0}$ en $\mathbb{H}_5$.

## 4.3. Comentarios finales

Desde el punto de vista de la implementación del protocolo de códigos superdensos de varias partes, es necesario preparar estados entrelazados con más de dos qubits. Se ha demostrado que preparar tales estados de más de dos qubits, a diferencia de las técnicas tradicionales para preparar estados entrelazados que emplean polarización de fotones, en [35] se explota el momento angular orbital de los fotones para preparar estados con alta dimensionalidad. Este resultado tiene implicaciones prácticas, como en la implementación de esquemas criptográficos y protocolos de comunicación como el que se propone en este trabajo. La aplicación de las transformaciones unitarias en el círculo unitario es más complejo que la aplicación de transformaciones de Pauli por lo que el protocolo propuesto con el uso de matrices de Pauli puede ser útil en una implementación física.

# Capítulo 5

# Implementación de protocolos cuánticos

En este capítulo se trata brevemente la implementación de los protocolos cuánticos propuestos. Siguiendo un esquema de comunicación de envío de mensajes usando *sockets* y memoria compartida, para simular un canal de comunicación cuántico. El propósito de la implementación es ilustrar un protocolo cuántico y mostrar la complejidad de la simulación del fenómeno de entrelazamiento.

## 5.1. Esquema de simulación con envío de mensajes

Para el envío de mensajes se propone el uso de sockets como medio de comunicación entre dos partes, por ejemplo Alicia y Beto que desean comunicarse de manera segura empleando un protocolo cuántico. El protocolo es el que se explica en el capítulo 3, donde se considera que Alicia crea a *priori* $n$ estados de Bell, $\psi_0 \otimes \psi_1 \otimes \cdots \otimes \psi_{n-1}$, de los cuales ella posee el primer qubit $q_A$ y Beto el segundo $q_B$. Alicia mide su qubit $q_A$ obteniendo un bit $a$ y envía su resultado a Beto por un canal de comunicación clásico; Beto también mide su qubit $q_B$, obteniendo un bit $b$. Según el estado creado por Alicia y su bit $a$, el resultado de la medición de Beto y la decodificación es: Si $\psi_i = \mathbf{b}_{00}$ entonces $a = b$ y Beto decodifica 0, si por el contrario $\psi_i = \mathbf{b}_{01}$ entonces $a \neq b$ y Beto decodifica 1.

El protocolo parece ser trivial ya que se envía un bit por un canal clásico, pero ya que cada uno posee un qubit, para cualquiera que tenga acceso al canal clásico, no podría ganar algún tipo de información si no tiene conocimiento del estado creado inicialmente por Alicia; y ya que el resultado de la medición de Alicia es totalmente aleatorio, lo único que obtendría es una cadena de bits aleatorios.

La simulación de entrelazamiento empleando el protocolo de Steiner considera lo siguiente: se comparte una sucesión $(t_n)_n$ de números aleatorios entre Alicia y Beto. Alicia conoce $y_0 \in [0, 1]$ y la sucesión $(s_n)_n$ de números aleatorios; entonces busca un $k_0 = \text{mín}(k|s_k \leq |\cos(2\pi(t_k - y_0))|)$ para calcular $a_0 = \text{Sgn}(\cos(2\pi(t_{k_0} - y_0)))$, y envía $k_0$ a Beto. Cuando Beto recibe $k_0$, calcula $a_1 = \text{Sgn}(\cos(2\pi(t_{k_0} - y_1)))$, donde $y_1$ es

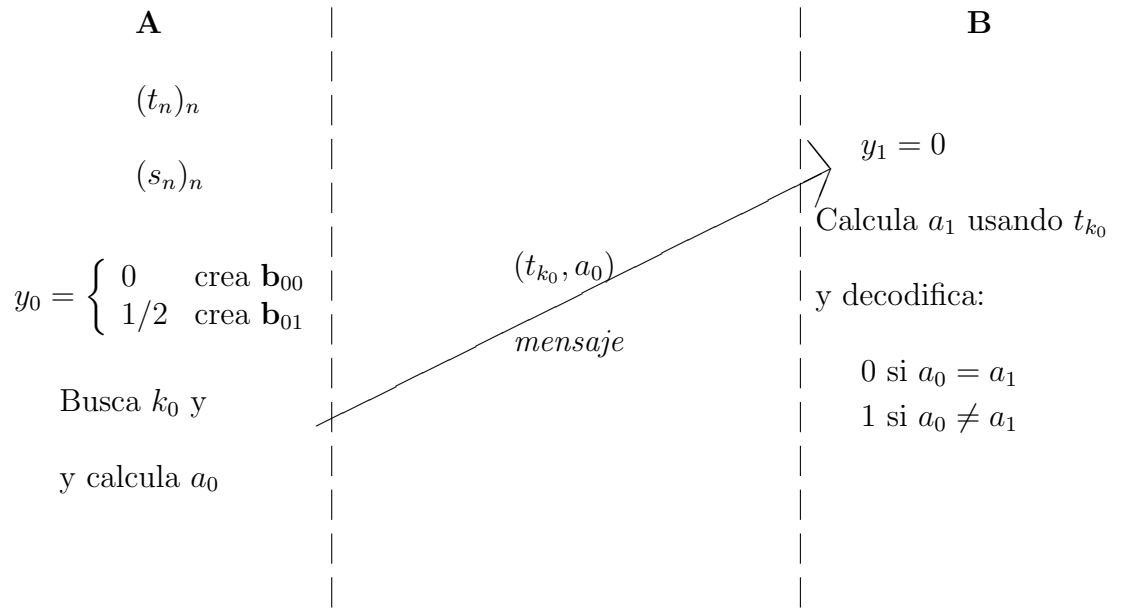


Figura 5.1: Esquema de simulación empleando el protocolo de Steiner con envío de mensajes. La línea transversal representa un canal de comunicación clásico.

de su conocimiento. Entonces si $y_0 = y_1$ el procedimiento anterior simula mediciones sobre el estado $\mathbf{b}_{00}$ y para $y_0 - y_1 = \pm\frac{2k-1}{2}$ con $k \in \mathbb{N}$, simula mediciones sobre $\mathbf{b}_{01}$.

Para implementar el protocolo no es necesario que ambas partes conozcan la sucesión de números aleatorios $(t_n)_n$; si Alicia genera la sucesión $(t_n)_n$ para encontrar $k_0$ y calcula $a_0$, entonces envía el par $(t_{k_0}, a)$ (un número real y un bit) a Beto, por medio de un mensaje. Así, cuando Beto recibe el par $(t_{k_0}, a_0)$ calcula $a_1$ empleando $t_{k_0}$ y decodifica 0 si $a_0 = a_1$ ó 1 si $a_0 \neq a_1$. Si Alicia desea comunicar un bit 0 a Beto crea el estado $\mathbf{b}_{00}$ usando $y_0 = 0$ y un bit 1 creando $\mathbf{b}_{01}$ con $y_0 = 1/2$, en ambos casos Beto siempre usa $y_1 = 0$ (los parámetros de medición $y_0, y_1$ se establecen antes de iniciar la comunicación). La figura 5.1 muestra este esquema de simulación

La simulación de entrelazamiento empleando el protocolo de Brassard considera lo siguiente: Alicia y Beto comparten una variable local oculta $c \in \{0, 1\}$, y acuerdan en un parámetro $t \in [0, \frac{3}{10}[$. Alicia conoce $x \in [0, 1]$ y Beto conoce $y \in [0, 1]$. Alicia calcula $\boldsymbol{\delta} = \boldsymbol{\varepsilon}(x, t)$ y lo envía a Beto (sólo son necesarios 4 bits), y obtiene el bit $a = c$. Cuando Beto recibe $\boldsymbol{\delta}$ sigue el procedimiento descrito en el protocolo (ver capítulo 3), obteniendo el bit $b$.

Para llevar a cabo la simulación Alicia genera la variable local oculta $c$, el parámetro $t$ y envía sus valores a Beto (antes de comenzar la transmisión). Así, cuando inicia la comunicación Alicia envía el par $(\boldsymbol{\delta}, a)$ (un número real y un bit) a Beto por medio de un mensaje. Cuando Beto recibe el mensaje de Alicia calcula el bit $b$ empleando $\boldsymbol{\delta}$ y decodifica el mensaje como 0 si $a = b$ ó 1 si $a \neq b$. De igual forma que en el protocolo de Steiner, Alicia comunica un bit 0 a Beto creando el estado $\mathbf{b}_{00}$ usando $x = 0$ y un bit 1 con el estado $\mathbf{b}_{01}$ con $x = \pi$ (ambos parámetros de medición $x, y$

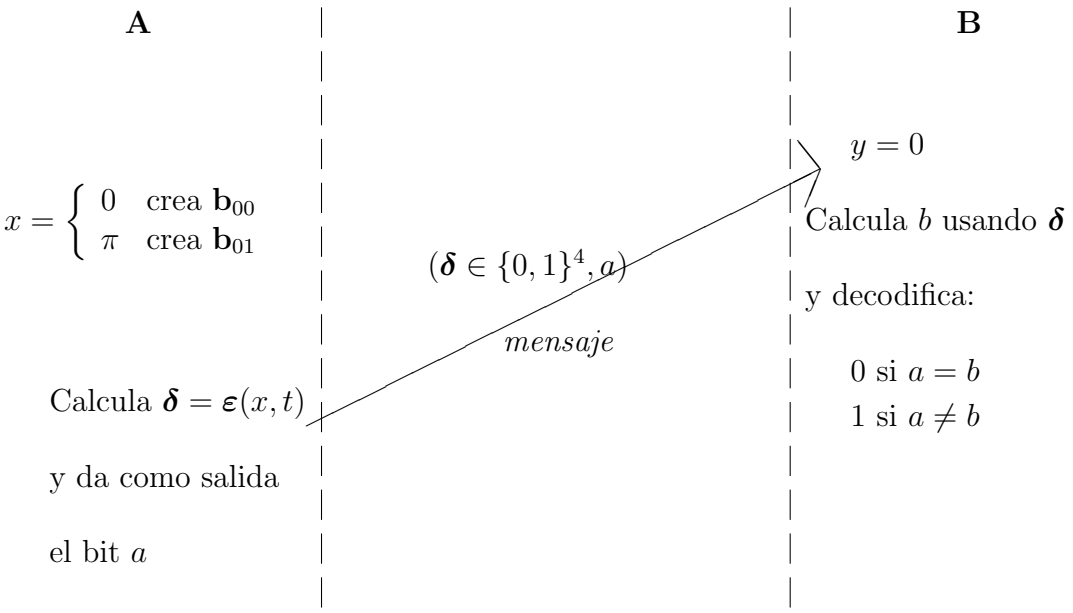


Figura 5.2: Esquema de simulación empleando el protocolo de Brassard con envío de mensajes. La línea transversal representa un canal de comunicación clásico.

son multiplicados por $2\pi$ y también se establecen antes de iniciar la comunicación). La figura 5.2 muestra este esquema de simulación.

## 5.2. Esquema de simulación empleando memoria compartida

La implementación del protocolo de comunicación empleando memoria compartida es similar al esquema de simulación presentado en la figuras 5.1 y 5.2, con la diferencia que la comunicación se lleva a cabo por medio de variables compartidas, tanto para el protocolo de Steiner como el de Brassard. En lo que sigue se presenta un esquema de simulación para el protocolo de códigos superdensos de varias partes empleando memoria compartida.

La figura 5.3 muestra el esquema de simulación, que consta de tres partes, donde en el lado izquierdo se muestra al receptor A; en el lado derecho se representa a los $n-1$ transmisores B, que aplican transformaciones de Pauli a sus qubits correspondientes y en la parte central se representa la memoria compartida, donde se guarda el estado entrelazado $\Psi = \sum a_i(e_{A_i} \otimes e_{B_i})$, al cual tienen acceso A y B.

Sea $\varphi_B = \sigma_{b_1} \otimes \cdots \otimes \sigma_{b_{n-1}}$ la composición o matriz de transformaciones de Pauli, donde $\sigma_{b_i}$ es la operación que aplica el transmisor $i \in [\![1, n-1]\!]$. Cuando se aplica $\varphi_B$ sobre $\Psi$, como $(\sigma_0 \otimes \varphi_B)\Psi$, el resultado se refleja en $\Psi$ (cambiando a otro estado en su base) y los $n-2$ qubits $f_B$ son enviados de regreso al receptor A (por medio de un canal cuántico). Entonces, A lleva a cabo una medición para conocer el nuevo estado

$\Phi$; generando números aleatorios para la medición (la tabla 5.1 muestra el algoritmo de medición) y simulando el entrelazamiento.

Para simular un canal cuántico se propone el uso de una memoria compartida. Ya que cuando se comparte un estado entrelazado, cada parte en el protocolo posee un qubit y cualquier transformación que se le aplique se refleja en $\Psi$. De este modo con una memoria compartida en común se puede modificar el estado $\Psi$ individualmente. Después de aplicar $\varphi_B$, la parte A tiene acceso a la memoria compartida y puede medir el nuevo estado $\Phi$. Finalmente cada transmisor en B envía un bit empleando algún esquema de envío de mensajes (por medio de una conexión con sockets).

En la medición se considera lo siguiente. Dada una base $\mathcal{B}_{Bell}$ en $\mathbb{H}_n$. Sea el operador de medición $M_i = |\psi_i\rangle\langle\psi_i|$ para $i \in [\![0, 2^n - 1]\!]$, se tiene que

$$p(\psi_i) = \langle\psi_i|M_i^\dagger M_i|\psi_i\rangle = 1 \tag{5.1}$$

Es decir, el estado $\psi_i$ es perfectamente identificable cuando se efectúa una medición con el operador $M_i$ correcto. En la implementación se puede evitar este paso, ya que resulta trivial buscar este operador leyendo la memoria compartida. Aunque el estado $\Psi$ es un estado entrelazado, su simulación no es necesaria, porque sólo se realizan transformaciones de Pauli y no mediciones sobre qubits individuales. Cabe mencionar que la comunicación en este esquema es de Beto hacia Alicia.

La realización práctica de los esquemas propuestos se realizaron en el lenguaje de programación `C++`. Para implementar sockets se siguió el modelo *cliente-servidor* donde Alicia es el cliente y Beto el servidor, cada uno ejecutándose como un proceso independiente, ya sea un una máquina local o nodos separados comunicándose a través de una red. Aquí sólo se experimento en una sola máquina, pero puede ser extendido fácilmente y llevarlo a una red. El tamaño en bytes de los mensajes en la comunicación requirieron enviar un número real y un entero corto; aunque se pueden enviar los bits necesarios, se eligió este modo.

Para implementar la memoria compartida se usaron las funciones de comunicación IPC en `C++`, que reservan un área de memoria por un proceso, a la cual pueden acceder otros procesos indicando su dirección (siempre y cuando tenga permisos de lectura o escritura). Así, la comunicación se realiza por medio de variables compartidas y los accesos a éstas se pueden controlar empleando semáforos o simplemente con otras variables usadas como banderas que indican si se puede escribir o leer. En el protocolo de códigos superdensos de varias partes se empleó ambos métodos de comunicación empleando sockets y la memoria compartida. En el apéndice se puede ver la lista completa de programas implementados así como sus versiones empleando sockets y memoria compartida.

Tabla 5.1: Algoritmo de medición.

**Entrada.** $\psi \in \mathcal{B}_{Bell}$
**Salida.** El índice $i$ tal que $p(\psi) = \langle\psi|M_i^\dagger M_i|\psi\rangle = 1$
**Procedimiento.** Medición
{
  Para cada $i \in [\![0, 2^n - 1]\!]$ hacer $\lambda_i = \langle\psi|\psi_i\rangle$
  $c_{-1} = 0$
  Para cada $i < 2^n$ hacer $c_i = c_{i-1} + |\lambda_i|^2$
  $x =$ `random`$([0, 1])$
  Encontrar $i$ tal que $c_{i-1} < x \leq c_i$
  salida $i$
}

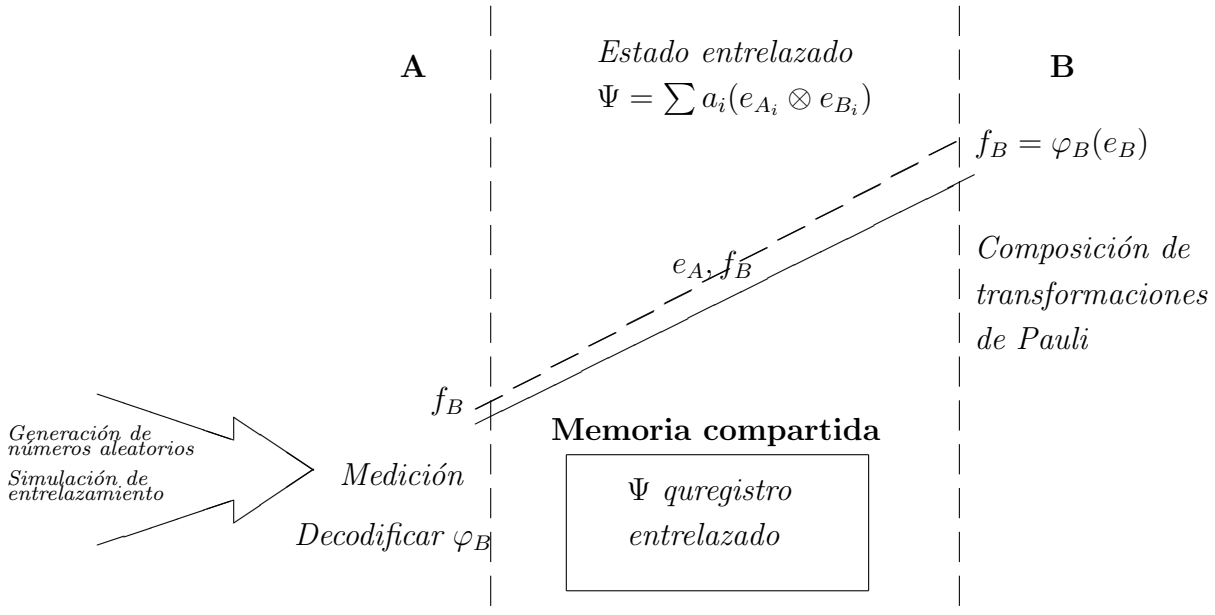


Figura 5.3: Esquema de simulación del protocolo cuántico de códigos superdensos empleando memoria compartida. La línea transversal superior representa un canal cuántico y la inferior un canal clásico.

# Capítulo 6

# Conclusiones y trabajo futuro

Son tres los problemas que se consideran en este trabajo de tesis: la separación de registros cuánticos, la simulación del entrelazamiento y el problema de la generalización del protocolo de códigos superdensos. Para el primero proponemos un algoritmo directo de orden polinomial con respecto a la longitud del quregistro, pero sin embargo la complejidad del problema crece de manera exponencial con respecto a la dimensión del quregistro. La solución propuesta decide si un quregistro es separable y en caso de que lo sea, recupera los factores que se tratan de vectores unitarios los cuales conservan las amplitudes para cada estado del quregistro, lo que no influye en la toma de mediciones. Para el segundo problema de la simulación del entrelazamiento se siguen de cerca dos protocolos conocidos, el de Steiner y de Brassard, ambos se basan en mediciones de tipo von Neumann y el esquema de variables locales ocultas. Por último se considera el problema de la generalización del protocolo de códigos superdensos, empleando estados de alta dimensionalidad con transformaciones en el círculo unitario y de matrices de Pauli. También se presenta algunos esquemas de simulación de protocolos cuánticos con el envío de mensajes y empleando memoria compartida.

Un problema que surge de la generalización del protocolo de códigos superdensos es la teletransportación cuántica, donde se demuestra que es posible enviar un qubit intacto con tan solo dos bits. En [36] se demuestra que si Alicia y Beto comparten un par EPR, si Alicia envía dos bits, entonces Beto puede reproducir el estado de un qubit que Alicia quiere transmitir. En particular el problema es la generalización de la teletransportación cuántica de estados multidimensionales como los vistos en el capítulo 4. Recientemente se ha propuesto la teletransportación cuántica empleando códigos superdensos [37] (*SuperDense Quantum Teleportation*). En [38, 39] se consideran los primeros enfoques de la teletransportación en términos de compuertas cuánticas de una forma más didáctica, por lo que es de interés considerar un método parecido para estados multidimensionales. De esta forma se puede construir un algoritmo cuántico para simular la teletransportación; ya que el enfoque tradicional sólo se consideran transformaciones unitarias como en el protocolo de códigos superdensos.

# Apéndice A

# Programas realizados

Desarrollamos los programas de separación de registros cuánticos y los protocolos de comunicación cuántico. El algoritmo de separación cuenta con una implementación en `C++` y en `Mathematica`. La versión en `C++` crea instancias aleatorias de un quregistro y busca su factorización completa, la versión en Mathematica sólo se implementó el algoritmo DescomParcial. Los programas implementados para los protocolos cuentan con dos versiones, el uso del esquema de memoria compartida para simular un canal cuántico y con el envío de mensajes empleando *Sockets*. Los programas que usan memoria compartida son los siguientes:

1. `Brassard-protocol-SM`
2. `Steiner-protocol-SM`
3. `Superdense-Coding-SM`

los programas que emplean envío de mensajes con sockets son:

1. `Brassard-sockets`
2. `Steiner-sockets`
3. `Superdense-Coding-sockets`

en cada uno de los casos se implementó el protocolo de Steiner, Brassard y el protocolo de códigos superdensos. Por último, se implementó el protocolo de varias partes de códigos superdensos:

1. `Multiparts-Densecoding`

éste emplea ambos esquemas de comunicación la memoria compartida y el envío de mensajes por medio de *sockets*. Los archivos conteniendo los originales en `C++` y sus correspondientes binarios para el sistema operativo basado en `UNIX`, la distribución de `Linux Red Hat 9.0` empleando en compilador `g++` versión 4.1, se pueden consultar en el disco compacto que acompaña este trabajo de tesis.

## A.1. Estructura del disco compacto que acompaña esta tesis

```
|------------------- Directory
|
|------------------- readme.txt
|
|------------------- index.html : inicio de la navegacion
|
|------------------- tesis : directorio con la tesis en pdf
|
|------------------- presentaciones : algunas presentaciones%
|                    resultantes de este trabajo
|
|------------------- source files : programas en C++ y Mathematica
|
|------------------- binary files : ejecutables
```

# Referencias


[1] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.SCI.STATIST.COMPUT.*, 26:1484, 1997.

[2] Lov K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, pages 212–219, 1996.

[3] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phy. Rev. Lett.*, 69:2881–2884, November 1992.

[4] Richard Cleve, Wim van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. *Lecture Notes in Computer Science*, 1509:61–74, 1999.

[5] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 63–68, New York, NY, USA, 1998. ACM Press.

[6] Asher Peres. *Quantum Theory: concepts and methods*. Kluwer Academic Press, Dordrecht, 1993.

[7] Richard Jozsa. Entanglement and quantum computation. *The Geometric Universe, S Huggett, L Mason, K P Tod, S T Tsou and N Woodhouse, Oxford University Press*, Jan 1998.

[8] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.

[9] John S. Bell. On the Einstein–Podolsky–Rosen paradox. *Physics*, 1:195–200, 1964.

[10] M.Ñielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[11] Klaus Mattle, Harald Weinfurter, Paul G. Kwiat, and Anton Zeilinger. Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 76(25):4656–4659, Jun 1996.

[12] Ximing Fang, Xiwen Zhu, Mang Feng, Xi'an Mao, and Fei Du. Experimental implementation of dense coding using nuclear magnetic resonance. *Phys. Rev. A*, 61(2):022307, Jan 2000.

[13] G. Brassard, R. Cleve, and A. Tapp. The cost of exactly simulating quantum entanglement with classical communication. *Phys. Rev. Lett.*, 83(9):1874–1877, 1999.

[14] Harry Buhrman, Richard Cleve, and Wim van Dam. Quantum entanglement and communication complexity. *SIAM J. Comput.*, 30(6):1829–1841, 2000.

[15] Serge Massar, Dave Bacon, Nicolas Cerf, and Richard Cleve. Classical simulation of quantum entanglement without local hidden variables. *Physical Review A*, 63:052305, 2001.

[16] M. Steiner. Towards quantifying non-local information transfer: finite-bit non-locality. *Phy. Lett. A*, 270:239–244, June 2000.

[17] N. J. Cerf, N. Gisin, S. Massar, and S. Popescu. Quantum entanglement can be simulated without communication. *Physical Review Letters*, 94:220403, 2005.

[18] Sergio Albeverio, Shao-Ming Fei, and Debashish Goswami. Separability of rank two quantum states. *Physics Letters A*, 286:91, 2001.

[19] Jon Eakins and George Jaroszkiewicz. Factorization and entanglement in quantum systems. *Journal of Physics A: Mathematical and General*, 36:517–526, 2003.

[20] Artur Ekert and Peter Knight. Entangled quantum systems and the schmidt decomposition. *American Journal of Physics*, 63(5), 1995.

[21] S.-M. Fei, N. Jing, and B.-Z. Sun. Hermitian Tensor Product Approximation of Complex Matrices and Separability. *ArXiv Quantum Physics e-prints*, March 2006.

[22] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77(8):1413–1415, Aug 1996.

[23] Leonid Gurvits. Quantum matching theory (with new complexity theoretic, combinatorial and topological insights on the nature of the quantum entanglement). 2002.

[24] Leonid Gurvits. Classical deterministic complexity of edmonds'problem and quantum entanglement. In *STOC*, pages 10–19. ACM, 2003.

[25] Leonid Gurvits. Classical complexity and quantum entanglement. *J. Comput. Syst. Sci.*, 69(3):448–484, 2004.

[26] Leonid Gurvits and Howard Barnum. Separable balls around the maximally mixed multipartite quantum states. *Phys. Rev. A*, 68(4):042312, Oct 2003.

[27] Ian Glendinning and Bernhard Ömer. Parallelization of the qc-lib quantum computer simulator library. *Lecture Notes in Computer Science*, 3019/2004:461–468, 2004. Springer Berlin / Heidelberg.

[28] Jumpei Niwa, Keiji Matsumoto, and Hiroshi Imai. General-purpose parallel simulator for quantum computing. *Lecture Notes in Computer Science, in the Unconventional Models of Computation: Third International Conference, UMC 2002, Kobe, Japan, October 15-19, 2002. Proceedings*, 2509/2002:230–251, 2002. Springer Berlin / Heidelberg.

[29] Kim Boström and Timo Felbinger. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.*, 89(18):187902, Oct 2002.

[30] Kim Boström. Secure direct communication using entanglement. *quant-ph/0203064*, 2002.

[31] A. Cabello. Multiparty key distribution and secret sharing based on entanglement swapping. *ArXiv Quantum Physics e-prints*, September 2000.

[32] Zhang Zhanjun. Deterministic secure direct bidirectional communication protocol. arXiv:quant-ph/0403186v1.

[33] Andrzej Grudka and Antoni Wójcik. Symmetric scheme for superdense coding between multiparties. *Phys. Rev. A*, 66(1):014301, Jul 2002.

[34] X. S. Liu, G. L. Long, D. M. Tong, and Feng Li. General scheme for superdense coding between multiparties. *Phys. Rev. A*, 65(2):022304, Jan 2002.

[35] Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Entanglement of orbital angular momentum states of photons. *Nature*, 412:313–316, Jul 2001.

[36] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar 1993.

[37] Herbert J. Bernstein. Superdense quantum teleportation. *Quantum Information Processing*, 5(6):451–461, 2006.

[38] G. Brassard. Teleportation as a quantum computation. *preprint at quant-ph/9605035), Physica D120*, pages 43–47, 1998.

[39] Daniel Gottesman and Isaac L. Chuang. Quantum teleportation is a universal computational primitive. *Nature*, 402:390, 1999.