

Reporte de Seminario 1

Computación Cuántica

Lic. Julio A. Medina¹

¹ Universidad de San Carlos, Escuela de Ciencias Físicas y Matemáticas
Maestría en Física
julioantonio.medina@gmail.com

Durante el curso de Seminario 1 se han investigado los fundamentos teóricos de la computación cuántica. Se han repasado temas de mecánica estadística, como el concepto de ensambles, un tema recurrente en computación cuántica. La computación cuántica nace del deseo de Richard P. Feynman de querer analizar y simular sistemas cuánticos por medio de sistemas informáticos, esto llevo rápidamente a la realización que el problema crecía exponencialmente con respecto al número de partículas a simular, esto implicaba que el costo computacional crecía de la misma manera, esto imposibilitó de gran manera simular dichos sistemas cuánticos. Feynman[3] publicó en 1981 un artículo seminal en el que plantó la semilla para crear sistemas de computación cuántica para simular mas efectivamente sistemas de naturaleza cuántica.

Se han revisado conceptos fundamentales y básicos de la computación cuántica como:

- El concepto del bit cuántico, *qubit*.
- Entrelazamiento cuántico.
- Superposición de estados cuánticos.
- Producto tensorial.
- La esfera de Bloch.
- Compuertas lógicas cuánticas.
- Operador de Hadamard.
- Teletransportación cuántica.
- Transformada cuántica de Fourier.
- Circuitos cuánticos.
- Algoritmo de Shor.

Ademas de la investigación teórica se han aprendido conceptos prácticos a través de la API para computación cuántica creada por IBM, Qiskit [4]. Dicha API se usa como una biblioteca de python mediante la cual se pueden acceder a computadoras cuánticas reales en las instalaciones de IBM para poder probar y desarrollar circuitos cuánticos básicos. Este proyecto de seminario y tesis de maestría ha sido subido a un proyecto de GitHub donde también se han subido algunos scripts en python utilizando Qiskit donde se han desarrollado algoritmos como el de Deutch-Jozsa y otros, <https://github.com/Julio-Medina/Seminario>, esto con el fin de tener un historial claro del progreso de esta investigación.

1. Inicios de la computación cuántica

La computación cuántica nace del deseo de Richard P. Feynman de querer analizar y simular sistemas cuánticos por medio de sistemas informáticos, esto llevo rápidamente a la realización que el problema crecía exponencialmente con respecto al número de partículas a simular, esto implicaba que el costo computacional crecía de la misma manera, esto imposibilitó de gran manera simular dichos sistemas cuánticos. Feynman[3] publicó en 1981 un artículo seminal en el que plantó la semilla para crear sistemas de computación cuántica para simular mas efectivamente sistemas de naturaleza cuántica.

2. De bits a Qubits

En la computación clásica los estados o bits son 1 o 0, sin embargo en mecánica cuántica debido al principio de superposición de estados, se tiene que un qubit se puede encontrar en una superposición de estados i.e. simultáneamente estar en 1 y 0. Dichas superposiciones permiten realizar cálculos en varios estados simultáneamente, es decir se paralelizan los procesos de computo de una manera natural. Esto permite crear algoritmos cuánticos con mejoras exponenciales en el desempeño de computación. Sin embargo debido al colapso de la función de onda, cuando se hace una medición en los estados de superposición el estado colapsa en uno de los eigen-estados del operador que se utiliza para hacer la medición.

Debido a esto los algoritmos cuánticos se diseñan de tal manera que la respuesta correcta se amplifique, es decir que haya una resonancia de la respuesta correcta en la función de onda, esto hace que el diseño de algoritmos cuánticos sea una tarea poco trivial.

2.1. Notación de Dirac

Se utilizan para describir estados cuánticos. Son vectores en el espacio de Hilbert, pueden ser vectores con dimensiones finitas o describir cantidades continuas y ser vectores de dimensión infinita. El físico inglés Paul Dirac popularizó la llamada notación de Dirac para hacer los cálculos en mecánica cuántica mas compactos. Se define al ket como

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \quad (1)$$

donde $a_1, a_2 \in \mathbb{C}$. Y el bra se define como el vector fila, o vector en el espacio dual del ket definido como

$$\langle a| = (a_1^* \quad a_2^*) \quad (2)$$

donde $a_1^*, a_2^* \in \mathbb{C}$ son los complejos conjugados de a_1, a_2 . Los bra y los ket están relacionados de la siguiente manera

$$\langle a| = |a\rangle^\dagger \quad (3)$$

que equivale a

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}^\dagger = (a_1^* \quad a_2^*) \quad (4)$$

donde $a_1 = x + iy$ y $a_1^* = x - iy$ es el complejo conjugado, el operador \dagger da el transpuesto conjugado de un vector o matriz.

Se define al braket como el producto interno o producto escalar en el espacio de Hilbert.

$$\langle b|a\rangle = a_1 b_1^* + a_2 b_2^* = \langle a|b\rangle^* \in \mathbb{C} \quad (5)$$

. El ketbra o producto abierto se define como

$$|a\rangle\langle b| = \begin{pmatrix} a_1 b_1^* & a_1 b_2^* \\ a_2 b_1^* & a_2 b_2^* \end{pmatrix} \quad (6)$$

2.2. Representación de Qubit

La representación de un qubit viene dada naturalmente por los spinores utilizados para describir el experimento de Stern-Gerlach en el que se miden el spin de átomos de plata. Estos spinores se definen como

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (7)$$

como el análogo cuántico del estado 0 para un bit clásico, y para el estado clásico 1 se usa

$$|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (8)$$

estos estados cuánticos son evidentemente ortonormales $\langle 0|1\rangle = 0$ y $\langle 0|0\rangle = \langle 1|1\rangle = 1$. Se nota que estos dos estados forman una base. Todos los estados cuánticos están normalizados

$$\langle \psi|\psi\rangle = 1 \quad (9)$$

por ejemplo $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

3. Mediciones

Por lo general se utilizan bases ortonormales para describir y medir estados cuánticos, aquí se sigue esa convención. Durante una medición en la base $\{|0\rangle, |1\rangle\}$ el estado colapsara ya sea a $|0\rangle$ o $|1\rangle$, estos son los eigen-estados de σ_z la matriz Pauli-z(ver 4.1.1) a esto se le conoce como medición en z.

Hay infinitas bases distintas en las que se pueden realizar las mediciones pero otras bases comunes son $\{|+\rangle, |-\rangle\}$ definidas como:

$$|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (10)$$

$$|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (11)$$

que son los eigen-vectores de la matriz de Pauli x σ_x , y como se ha de esperar otra base comúnmente usada son los eigen-vectores de la matriz Pauli y , σ_y :

$$|+i\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad (12)$$

$$|-i\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \quad (13)$$

3.1. Regla de Born

La probabilidad que el estado $|\psi\rangle$ colapse durante una medición proyectiva en la base $\{|x\rangle, |x^+\rangle\}$ al estado $|x\rangle$ está dada por

$$P(x) = |\langle x|\psi\rangle|^2 \quad (14)$$

y del hecho que se está trabajando con estados normalizados se tiene, como es de esperarse que

$$\sum_i P(x_i) = 1 \quad (15)$$

Para ilustrar esto se presentan algunos ejemplos:

a. El estado $|\psi\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}|1\rangle)$ es medido en la base $\{|0\rangle, |1\rangle\}$ calcule las probabilidades correspondientes:

$$P(0) = \left| \langle 0 | \frac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}|1\rangle) \right|^2 = \left| \frac{1}{\sqrt{3}}\langle 0|0\rangle + \sqrt{\frac{2}{3}}\langle 0|1\rangle \right|^2$$

$$P(0) = \left| \frac{1}{\sqrt{3}} \right|^2 = \frac{1}{3}$$

$$P(1) = \left| \sqrt{\frac{2}{3}} \right|^2 = \frac{2}{3}$$

$$P(0) + P(1) = 1$$

b. El estado $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ es medido en la base $\{|+\rangle, |-\rangle\}$, encontrar las probabilidades correspondientes:

$$P(+) = \left| \langle + | \psi \rangle \right|^2 = \left| \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right|^2$$

$$P(+) = \frac{1}{4} \left| \langle 0|0\rangle - \langle 0|1\rangle + \langle 1|0\rangle - \langle 1|1\rangle \right|^2 = 0$$

$$P(-) = 1$$

Como es de esperarse ya que $\left| \langle - | \psi \rangle \right|^2 = \left| \langle - | - \rangle \right|^2 = 1$ y $\left| \langle + | - \rangle \right|^2 = 0$ por la propiedad de ortogonalidad de estas bases.

4. Circuitos Cuánticos

Se utiliza el "modelo de circuitos", una secuencia de bloques básicos que realizan los cálculos elementales, a estos bloques básicos se les conoce como compuertas.

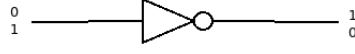


Figura 1: Compuerta NOT

4.1. Compuertas de un solo Qubit

Para hacer una analogía con las compuertas lógicas clásicas se presenta la compuerta lógica NOT, representada por 3, como se puede ver en la figura la operación que realiza el operador NOT en un bit es trivial, invierte el estado de bit de 0 a 1 y viceversa. Una de las características fundamentales de la teoría cuántica es el hecho que es unitaria, es decir que los operadores cuánticos, en este caso las compuertas cuánticas tienen que ser operadores unitarios (matrices unitarias), es decir que para un operador U se cumple que:

$$U^\dagger U = \mathbb{1} \quad (16)$$

esto implica que cuando un operador unitario actúa sobre un ket, no se cambia la magnitud del ket. De la notación de Dirac se puede representar a un operador unitario U como una combinación lineal de kets de la siguiente manera

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} = u_{00}|0\rangle\langle 0| + u_{01}|0\rangle\langle 1| + u_{10}|1\rangle\langle 0| + u_{11}|1\rangle\langle 1| \quad (17)$$

4.1.1. Matrices de Pauli

La matriz de Pauli x , σ_x esta definida como

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0| \quad (18)$$

esta matriz sirve como el análogo cuántico de la compuerta NOT, para ver esto basta con operar con la representación de los qubits definida en 7 y 8:

$$\sigma_x|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \quad (19)$$

De igual manera usando la notación de Dirac se tiene que

$$\sigma_x|1\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|)|1\rangle = |0\rangle \quad (20)$$

este comportamiento también se conoce como un bit-flip (intercambio de bit), también se puede actuar en superposiciones, los eigen-vectores de σ_x son los kets $|+\rangle, |-\rangle$.

La matriz de Pauli z , σ_z está definida como

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \quad (21)$$

el comportamiento de esta matriz se describe como un intercambio de fase (phase-flip), para visualizar esto actúa sobre la base $\{|+\rangle, |-\rangle\}$:

$$\sigma_z|+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle \quad (22)$$

en notación de Dirac se tiene

$$\sigma_z|-\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \quad (23)$$

Los eigen-vectores de la matriz σ_z son los kets $|0\rangle, |1\rangle$.

La matriz Pauli σ_y está definida por

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i|1\rangle\langle 0| - i|0\rangle\langle 1| \quad (24)$$

Se hace la observación que $\sigma_y = i\sigma_x\sigma_z$ por lo que se puede interpretar a esta compuerta como una sucesión de bit flip y phase flip.

Cualquiera de las matrices de Pauli $\sigma_x, \sigma_y, \sigma_z$ cumple con

$$\sigma_i^2 = \mathbb{1} \quad (25)$$

El conjunto de las matrices de Pauli y la matriz identidad forman una base de matrices de 2×2 .

4.1.2. Compuerta de Hadamard

La compuerta de Hadamard, H está definida por

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \quad (26)$$

la compuerta de Hadamard es muy útil ya que crea superposiciones de qubits, esto se ejemplifica de la siguiente manera

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (27)$$

$$H|0\rangle = |+\rangle \quad (28)$$

de igual manera se tiene que

$$H|1\rangle = |-\rangle \quad (29)$$

Debido que a que toda compuerta cuántica es unitaria y añadido al hecho que H es un operador Hermitico, i.e. $H^\dagger = H$, se tiene que

$$H|+\rangle = |0\rangle \quad (30)$$

$$H|-\rangle = |1\rangle \quad (31)$$

de esto que la compuerta de Hadamard pueda ser utilizada para cambiar entre las bases x y z .

4.2. Estados cuánticos de multipartículas

Para describir estados cuánticos de multipartículas se utiliza el producto tensorial, es decir que si tengo un estado para una partícula $|a\rangle$ y otro estado para una partícula distinta $|b\rangle$ se tiene que el estado bipartito se da por

$$|a\rangle \otimes |b\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix} \quad (32)$$

Para ejemplificar esto, supongamos que se tiene al sistema A en el estado $|1\rangle_A$ y al sistema B en el estado $|0\rangle_B$, entonces el estado total(híbrido) del sistema está dado por

$$|10\rangle_{AB} \equiv |1\rangle_A \otimes |0\rangle_B = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad (33)$$

como una observación importante de estos estados es que se les llama no correlacionados, también hay estados bipartitos que no pueden escribirse como $|\psi\rangle_A \otimes |\psi\rangle_B$, estos se conocen como estados correlacionados y para estados puros son estados entrelazados.

4.3. Compuertas de dos Qubits

Para hacer una analogía con compuertas lógicas clásicas se presenta a la compuerta lógica XOR, con una tabla de verdad dada por

x	y	$x \oplus y$
0	1	1
1	0	1
0	0	0
1	1	0

se nota que el operador XOR es un operador no reversible, sin embargo como ya se discutió anteriormente la teoría cuántica es unitaria y por lo tanto reversible. Para resolver este inconveniente se tiene la siguiente compuerta cuántica de dos qubits, llamada CNOT(controlled NOT), definida por

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| \quad (34)$$

para ver el efecto que la compuerta cuántica CNOT tiene se realizan los siguientes cálculos detalladamente:

$$\text{CNOT}|00\rangle_{xy} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)|00\rangle \quad (35)$$

$$\text{CNOT}|00\rangle = |00\rangle_{xy}$$

de igual manera se tiene que

$$\text{CNOT}|10\rangle_{xy} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)|10\rangle_{xy} \quad (36)$$

$$\text{CNOT}|10\rangle = |11\rangle_{xy}$$

$$\text{CNOT}|01\rangle_{xy} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)|01\rangle_{xy} \quad (37)$$

$$\text{CNOT}|01\rangle = |01\rangle_{xy}$$

$$\text{CNOT}|11\rangle_{xy} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)|11\rangle_{xy} \quad (38)$$

$$\text{CNOT}|11\rangle = |10\rangle_{xy}$$

Estos resultados se pueden resumir en la siguiente tabla, donde las dos primeras columnas representa la entrada y las últimas representan la salida de la operación, en este caso con el qubit de control, es decir el qubit del sistema x, se tiene un análogo de la compuerta XOR que en este caso es reversible como se puede ver en la tabla de verdad.

x	y	x	$x \oplus y$
0	1	0	1
1	0	1	1
0	0	0	0
1	1	1	0

Una representación gráfica de la compuerta CNOT realizada con la API de computación cuántica Qiskit se puede ver en la siguiente figura:

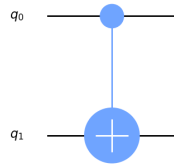


Figura 2: Compuerta cuántica CNOT

Es posible demostrar que los circuitos cuánticos pueden calcular cualquier función clásica de álgebra booleana, el fundamento de los circuitos digitales y por ende de toda computadora clásica.

5. Entrelazamiento cuántico

Si un estado puro $|\psi\rangle_{AB}$ de los sistemas A y B no puede escribirse como $|\phi\rangle_A \otimes |\gamma\rangle_B$ entonces el estado $|\psi\rangle_{AB}$ se conoce como un estado entrelazado, que es la definición para un estado correlacionado, pero ya que se está tratando solo con estados puros todo estado correlacionado es también un estado entrelazado.

5.1. Estados de Bell

Hay cuatro estados llamados Estados de Bell, en honor al físico John Bell. Bell desarrolló las también llamadas desigualdades de Bell [1], con las que resolvió la paradoja de Einstein-Podolsky-Rosen. Los llamados estados de Bell están máximamente entrelazados, es decir que violan las desigualdades de Bell exactamente, aparte estos estados de Bell forman una base ortonormal. Se definen como

$$|\psi^{00}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (39)$$

$$|\psi^{01}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (40)$$

$$|\psi^{10}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (41)$$

$$|\psi^{11}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (42)$$

De manera general se puede escribir a los estados de Bell como:

$$|\psi^{ij}\rangle \equiv (\mathbb{1} \otimes \sigma_x^j \sigma_z^i) |\psi^{00}\rangle \quad (43)$$

La correlación no es atributo exclusivo de la mecánica cuántica esta correlación puede existir en sistemas clásicos, por ejemplo si se reparte un par de guantes a dos personas sin que las persona sepan la orientación del guante(se les da en un caja sin visibilidad a su interior), y después se les pide a las personas que se dirijan en trenes en dirección opuesta y abran la caja para revelar la orientación de los guantes media hora después, la persona que encuentre el guante derecho sabrá instantáneamente que la otra persona tiene el guante izquierdo. Sin embargo el entrelazamiento cuántico presenta una correlación mas fuerte ya que si se mide a un par de partículas entrelazada en una base distinta, se mantiene la correlación de los estados, es difícil hallar una analogía clásica para esta situación. Es decir que el estado de Bell se puede escribir como

$$|\psi^{00}\rangle = |++\rangle + |--\rangle \quad (44)$$

y hacer una medición en la base $\{|++\rangle, |--\rangle\}$ y se mantiene la correlación.

5.2. Creación de los estados de Bell

Para crear a los estado de Bell se puede crear un circuito cuántico

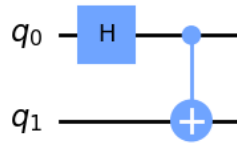


Figura 3: Circuito cuántico para la creación de estados de Bell

Esto equivale a

$$\text{CNOT} \left((H_A \otimes \mathbb{1}_B) |ij\rangle_{AB} \right) \quad (45)$$

con $i, j \in \{0, 1\}$, para entender paso a paso este circuito o cálculo se presenta la siguiente tabla en donde se desglosa la evolución de estado inicial a través del circuito cuántico

Estado Inicial $ ij\rangle_{AB}$	$(H_A \otimes \mathbb{1}_B) ij\rangle_{AB}$	Estados de Bell
$ 00\rangle$	$\frac{1}{\sqrt{2}}(00\rangle + 10\rangle)$	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$ 01\rangle$	$\frac{1}{\sqrt{2}}(01\rangle + 11\rangle)$	$\frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
$ 10\rangle$	$\frac{1}{\sqrt{2}}(00\rangle - 10\rangle)$	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$ 11\rangle$	$\frac{1}{\sqrt{2}}(01\rangle - 11\rangle)$	$\frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

5.3. Medición de Bell

Como se ha mencionado varias veces se tiene que los circuitos cuánticos son reversibles, por lo que para ir en el sentido contrario al circuito de creación de Bell que se presentó anteriormente se introduce un circuito cuántico conocido como medición de Bell, que revierte el proceso, el circuito esta definido como

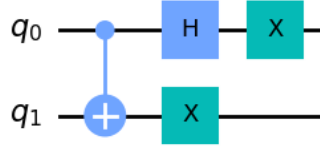


Figura 4: Circuito cuántico para la medición de Bell

Esto equivale a

$$(\sigma_x \otimes \sigma_x)(H \otimes \mathbb{1})(CNOT|\psi^{ij}\rangle) \quad (46)$$

6. Teletransportación cuántica

El objetivo del protocolo de teletransportación cuántica es el siguiente, Alice quiere enviar un estado cuántico $|\phi\rangle_S$ (desconocido por Alice)

$$|\phi\rangle_S = \alpha|0\rangle_S + \beta|1\rangle_S \quad (47)$$

a Bob, sin embargo solo puede enviar dos bit clásicos, aunque Alice supiera el estado es decir los valores reales de α y β , dos bits clásicos no son suficientes para codificar dos números reales. Sin embargo utilizando las propiedades cuánticas del entrelazamiento se puede lograr el objetivo de Alice. Supongamos que Alice y Bob comparten un estado de Bell máximamente entrelazado

$$|\psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \quad (48)$$

Con esto se tiene que el estado inicial del sistema es

$$|\phi\rangle_S \otimes |\psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(\alpha|000\rangle_{SAB} + \alpha|011\rangle_{SAB} + \beta|100\rangle_{SAB} + \beta|111\rangle_{SAB}) \quad (49)$$

Se nota que este estado inicial se puede reescribir como

$$\begin{aligned}
 |\phi\rangle_S \otimes |\psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}} \bigg[& (|00\rangle_{SA} + |11\rangle_{SA}) \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + (|01\rangle_{SA} + |10\rangle_{SA}) \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \\
 & + (|00\rangle_{SA} - |11\rangle_{SA}) \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) + (|01\rangle_{SA} - |10\rangle_{SA}) \otimes (\alpha|1\rangle_B - \beta|0\rangle_B) \bigg]
 \end{aligned}
 \tag{50}$$

Y esto equivale utilizando las definiciones de los estados de Bell(39, 40, 41, 42)
a

$$|\phi\rangle_S \otimes |\psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}} \bigg[|\psi^{00}\rangle_{SA} \otimes |\phi\rangle_B + |\psi^{01}\rangle_{SA} \otimes \sigma_x |\phi\rangle_B + |\psi^{10}\rangle_{SA} \otimes \sigma_z |\phi\rangle_B + |\psi^{11}\rangle_{SA} \otimes \sigma_x \sigma_z |\phi\rangle_B \bigg]
 \tag{51}$$

Con estos resultados es posible establecer un protocolo de teletransportación cuántica como se ve en la figura 5.

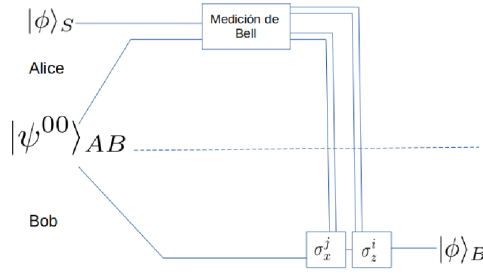


Figura 5: Protocolo de teletransportación cuántica.

Los pasos del protocolo son los siguientes:

1. Alice mide al sistema SA en la base de Bell, para ver como funciona esto se presenta la siguiente tabla

Alice Mide	Estado de Bob
$ \psi^{00}\rangle$	$ \phi\rangle_B$
$ \psi^{01}\rangle$	$\sigma_x \phi\rangle_B$
$ \psi^{10}\rangle$	$\sigma_z \phi\rangle_B$
$ \psi^{11}\rangle$	$\sigma_x\sigma_z \phi\rangle_B$

2. Alice envía el resultado de la medición de Bell a Bob, es decir le envía dos bits clásicos $i, j \in \{0, 1\}$.
3. Bob aplica $\sigma_z^i \sigma_x^j$ a su estado y obtiene $|\phi\rangle_B$

Hay que notar que cuando Alice hizo la medición de Bell su estado colapsó, por lo que ya no tiene al estado inicial $|\phi\rangle$, esto es de esperarse debido al teorema de no-clonación de la mecánica cuántica, no puede copiar su estado, solo puede enviarlo a Bob destruyendo su estado en el proceso.

Referencias

- [1] J.S. Bell. *On the Einstein Podolski Rosen Paradox*. https://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf
- [2] Michael A. Nielsen, Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press 2010. 10th. Anniversary Edition.
- [3] Richard P. Feynman. *Simulating Physics with Computers*. <https://doi.org/10.1007/BF02650179>.
- [4] *Qiskit Textbook*. <https://qiskit.org/textbook-beta>
- [5] N. David Mermin *Quantum Computer Science: An Introduction*. Cambridge University Press, 2007.
- [6] J.J. Sakurai *Modern Quantum Mechanics*. The Benjamin/Cummings Publishing Company, 1985.
- [7] Viktor Dotsenko. *An Introduction to the Theory of Spin Glasses and Neural Networks*. World Scientific 1994.
- [8] Yasaman Bahri, Jonathan Kadmon, Jeffrey Pennington, Sam S. Schoenholz, Jascha Sohl-Dickstein, Surya Ganguli. *Statistical Mechanics of Deep Learning*. <https://www.annualreviews.org/doi/pdf/10.1146/annurev-conmatphys-031119-050745>