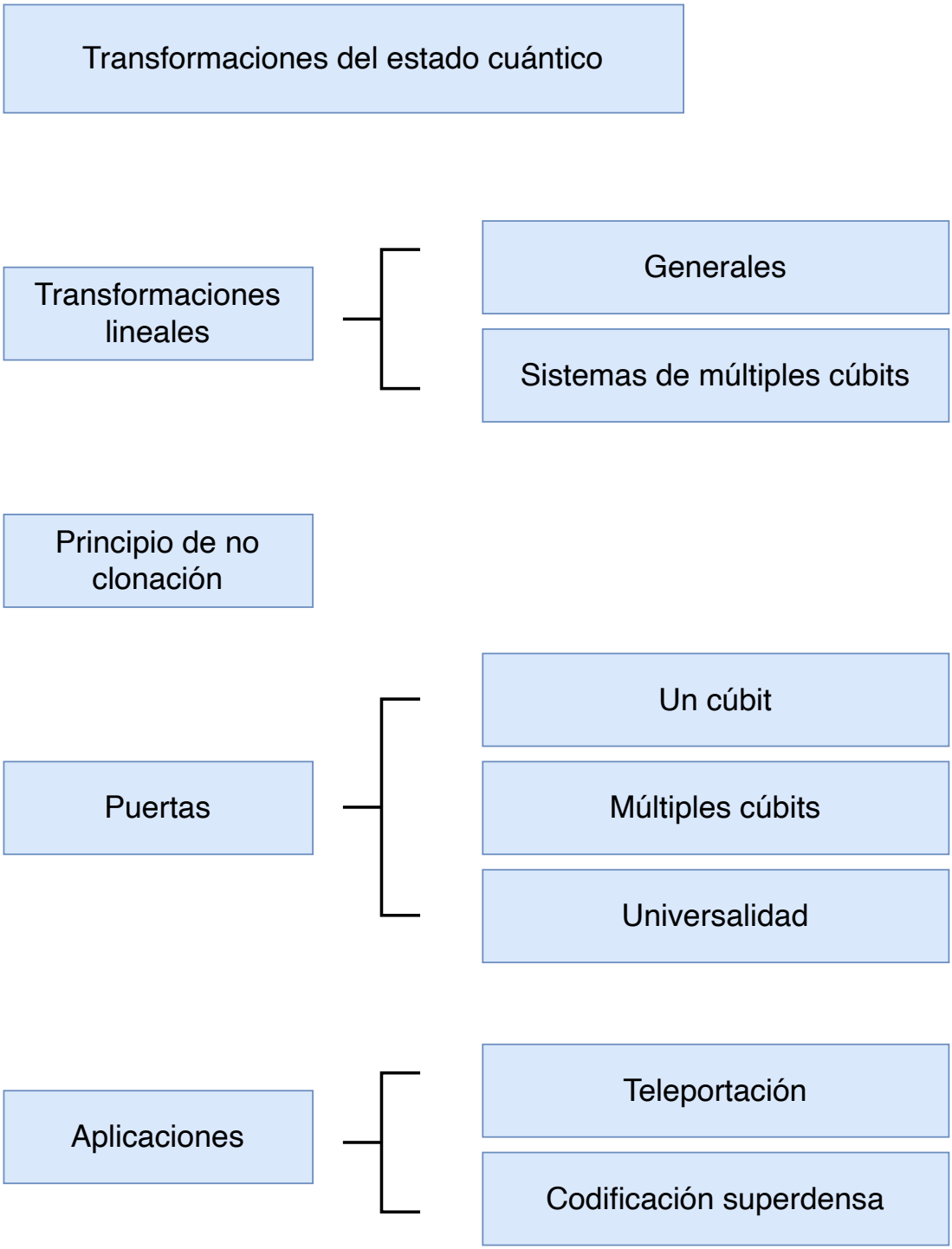
Computación Cuántica

Transformaciones

Índice

Esquema


Transformaciones del estado cuántico
Transformaciones lineales
Generales
Sistemas de múltiples cúbits
Principio de no clonación
Puertas
Un cúbit
Múltiples cúbits
Universalidad
Aplicaciones
Teleportación
Codificación superdensa

Ideas clave

6.1 Introducción y objetivos

El objetivo principal de este tema es estudiar los elementos básicos, los bloques de construcción, necesarios para poder realizar una computación cuántica.

El procesamiento de la información cuántica se realiza mediante la transformación dinámica del sistema. Por consiguiente, para entender la computación cuántica, se comenzará por entender que tipo de transformaciones son válidas en el contexto de la mecánica cuántica y para ello, se estudian las transformaciones de un sistema cuántico cerrado, que transforma un vector del espacio de estados en otro vector de ese mismo espacio de estados.

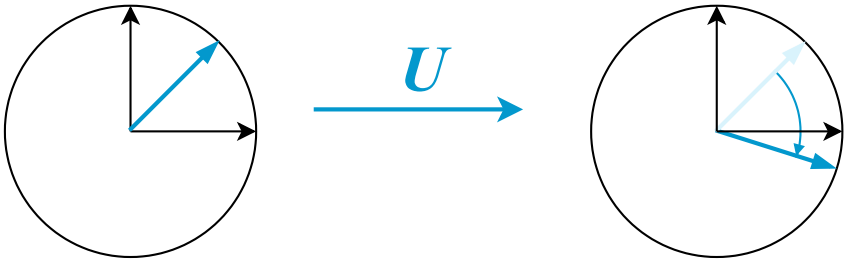


Figura 1: Geométricamente, la transformación unitaria es una rotación del espacio vectorial que no modifica la longitud del vector de estado, además asigna un vector del espacio de estados en otro vector dentro de ese mismo espacio vectorial. Elaboración propia.

Todas las transformaciones han de ser unitarias, esto es por imposición de las leyes de la mecánica cuántica. El proceso de medición no es una transformación unitaria, es irreversible, colapsa la función de onda y el estado cuántico deja de existir como tal, transformándose en un estado clásico.

Se comienza estudiando las transformaciones en sistemas cuánticos generales y luego se restringe a las transformaciones aplicadas a sistemas de múltiples cúbits y se

desarrolla el modelo de circuito de computación cuántica.

Se analiza la condición unitaria de las transformaciones de los estados cuánticos y el principio de no clonación que impone la imposibilidad de copiar de manera confiable el estado cuántico. Copiar no solo no produce una copia precisa, sino que también cambia el original de la misma manera que lo hace el proceso de medición. Esta limitación impuesta por el principio de no clonación tiene una importancia trascendental en la codificación de la información en forma de un estado cuántico, al impedir la copia, sin embargo, esta limitación, puede aprovecharse, por ejemplo, para garantizar la seguridad en los protocolos de cifrado.

Todas las transformaciones aplicadas a un sistema de múltiples cúbits pueden expresarse como una secuencia de transformaciones simples actuando sobre uno o dos cúbits, algunas de ellas son más simples de implementar y otras más costosas, el coste de una transformación se cuantifica en términos del número de puertas de uno y dos cúbits necesarias para su implementación.

Se estudia la aplicación de las puertas a dos problemas concretos, la teleportación y la codificación superdensa.

Se analizan los conjuntos finitos de puertas que pueden realizar cualquier transformación, es decir, su universalidad y se finaliza con una definición del modelo de circuito estándar para la computación cuántica.

- Transformaciones lineales generales
- Transformaciones lineales en sistemas de múltiples cúbits
- Principio de no clonación
- Transformaciones de un cúbit
- Transformaciones de múltiples cúbits
- Teleportación cuántica y codificación superdensa
- Universalidad

6.2 Transformaciones lineales

Una transformación cuántica asigna el espacio de estados de un sistema cuántico a sí mismo, es decir, las transformaciones asignarán un estado cuántico dentro de un espacio de estados a otro estado cuántico dentro de ese mismo espacio. En general, las transformaciones lineales no tiene porque tener esta restricción pero los sistemas cuánticos si la tienen.

En ese sentido, el proceso de medida no es una transformación, solo es posible un número finito de observables, y el resultado de aplicar una medición a un estado específico es solo probabilístico.

Las transformaciones que se tratarán en el tema son transformaciones de sistemas cuánticos cerrados, las leyes de la mecánica cuántica que gobiernan la naturaleza no permiten transformaciones arbitrarias, sino que deberán respetar las propiedades relativas a la medida del estado y la superposición.

Las transformaciones deben ser transformaciones lineales del espacio vectorial asociado al espacio de estados, de esa forma, un estado, superposición de otros estados, se transforma en la superposición de las transformaciones. Esta linealidad, se puede expresar de forma que cualquier transformación U actuando sobre cualquier superposición arbitraria: $|\psi\rangle = a_1|\psi_1\rangle + \cdots + a_k|\psi_k\rangle$, cumple:

$$U(a_1|\psi_1\rangle + \cdots + a_k|\psi_k\rangle) = a_1U|\psi_1\rangle + \cdots + a_kU|\psi_k\rangle$$

Los vectores de longitud unitaria mantendrán su longitud, lo que implica que los subespacios ortogonales serán transformados en subespacios ortogonales.

Estas propiedades aseguran que medir y luego aplicar una transformación al resultado, proporciona el mismo resultado que aplicar primero la transformación y luego medir en la base transformada. De forma específica, la probabilidad de obtener el resultado $U|\varphi\rangle$ aplicando primero U a $|\psi\rangle$ y luego midiendo con respecto a la descomposición $\oplus US_i$ es la misma que la probabilidad de obtener $U|\varphi\rangle$ midiendo $|\psi\rangle$ con respecto a la descomposición $\oplus S_i$ y luego aplicar U.

Estas propiedades se mantienen si U conserva el producto interno. Para cualquier $|\psi\rangle$

y $|\varphi\rangle$, el producto interno de sus transformaciones, $U|\psi\rangle$ y $U|\varphi\rangle$, debe ser el mismo que el producto interno entre $|\psi\rangle$ y $|\varphi\rangle$:

$$\langle\Phi|U^{\dagger}U|\psi\rangle = \langle\varphi|\psi\rangle.$$

Esta condición se cumple para todo $|\psi\rangle$ y $|\varphi\rangle$ solo si $U \dagger U = I$, en otras palabras, para cualquier transformación cuántica U, su adjunta $U^{\dagger}$(traspuesta conjugada de U), debe ser igual a su inversa, $U^{\dagger} = U^{-1}$, que es precisamente la condición para que una transformación lineal sea unitaria. Además, esta condición es suficiente, el conjunto de transformaciones permitidas de un sistema cuántico corresponde exactamente al conjunto de operadores unitarios en el espacio vectorial complejo asociado con el espacio de estados del sistema.

Dado que los operadores unitarios preservan el producto interno, asignan bases ortonormales a bases ortonormales, lo contrario es igualmente cierto, cualquier transformación lineal que asigne una base ortonormal a una base ortonormal, es unitaria.

Geométricamente, todas las transformaciones son rotaciones del espacio vectorial complejo asociado con el espacio de estados.

La columna i de la matriz correspondiente a la transformación U, es la transformación $U|i\rangle$ del vector base i, por lo que para una transformación unitaria dada en forma de matriz, U es unitaria, si y solo si, el conjunto de columnas de su representación matricial es ortonormal.

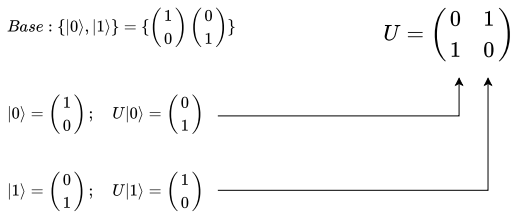


Figura 2: Matriz asociada a la transformación lineal Pauli X. Elaboración propia.

Dado que $U^{\dagger}$ es unitaria si y solo si U lo es, entonces U es unitaria si y solo si sus filas son ortonormales.

El resultado del producto U_1U_2 de dos transformaciones unitarias es una transformación unitaria.

El producto tensor $U_1 \otimes U_2$ es una transformación unitaria del espacio $V_1 \otimes V_2$ si U_1 y U_2 son transformaciones unitarias de V_1 y V_2 respectivamente.

Las combinaciones lineales de operadores unitarios no son unitarias en general. La condición unitaria simplemente asegura que el operador no viola ningún principio general de la teoría cuántica y no implica que una transformación se pueda implementar de manera eficiente, de hecho, la mayoría de los operadores unitarios no pueden implementarse de manera eficiente.

Una consecuencia de la condición unitaria es que toda transformación aplicada a un estado cuántico es reversible. Cualquier computación clásica puede implementarse de forma reversible con solo una pérdida insignificante de eficiencia. Por lo tanto, el requisito de reversibilidad no impone ninguna restricción a los algoritmos cuánticos.

En el modelo de circuito estándar de computación cuántica, toda la computación se lleva a cabo mediante transformaciones cuánticas, y la medición se usa solo al final para leer los resultados. Las transformaciones u operadores cuánticos, hacen referencia a operadores unitarios que actúan sobre el espacio de estados, no a operadores de medición. Si bien las mediciones son modeladas por operadores, el comportamiento de la medición no es modelado por la acción directa del operador hermítico de la medición en el espacio de estados, sino más bien por el procedimiento probabilístico indirecto descrito por el postulado de medición. Hay por tanto dos clases distintas de manipulación de un estado cuántico: las transformaciones cuánticas y la medición.

Una consecuencia simple, pero trascendental, de la condición unitaria, es el hecho de que los estados cuánticos desconocidos no se pueden copiar ni clonar, se puede derivar de la propia linealidad de las transformaciones unitarias. Sea U una transformación unitaria que realiza la clonación, de forma que:

$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$ para todos los estados cuánticos $|\psi\rangle$.

Sean $|\psi\rangle$ y $|\phi\rangle$ dos estados cuánticos ortogonales, si U es la transformación de clonación, entonces:

$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$ y

$U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle$

Si se define: $|\varphi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$, por linealidad:

$U(|\varphi\rangle|0\rangle) = \frac{1}{\sqrt{2}}(U(|\psi\rangle|0\rangle) + U(|\phi\rangle|0\rangle)) = \frac{1}{\sqrt{2}}(|\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle)$

Pero si U es la transformación de clonación, entonces:

$U(|\varphi\rangle|0\rangle) = |\varphi\rangle|\varphi\rangle = 1/2(|\psi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle) \neq \frac{1}{\sqrt{2}}(|\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle)$.

Por lo tanto, no existe una operación unitaria que pueda clonar de manera fiable todos los estados cuánticos.

El teorema de no clonación expone que es imposible clonar un estado cuántico desconocido específico de manera confiable, aunque no impide la construcción de un estado cuántico conocido a partir de un estado cuántico conocido.

6.3 Puertas cuánticas

Tanto en computación clásica como en computación cuántica, es posible realizar cómputos arbitrariamente complejos mediante la composición de elementos simples, es decir, las puertas lógicas en la computación clásica y las puertas cuánticas en computación cuántica.

Se denomina puerta cuántica a cualquier transformación de estado cuántico que actúa sobre un número reducido de cúbits. Las secuencias de puertas cuánticas se denominan circuitos cuánticos. Si el cúbit es la unidad de información en computación cuántica, el circuito es la unidad de cómputo.

Las puertas cuánticas son abstracciones matemáticas que resultan muy útiles para describir los algoritmos cuánticos pero que no se corresponden necesariamente con objetos físicos, como si ocurre en el caso clásico. Es por ello que el término puerta, así como su representación gráfica no deben tomarse literalmente. Para ciertas imple-

mentaciones, como el caso del procesador cuántico basado en fotones, puede haber puertas físicas reales, pero en otras, como las trampas de iones, la resonancia magnética nuclear o los circuitos superconductore, los cúbits son partículas estacionarias y las *puertas* son operaciones sobre ellas utilizando campos magnéticos, pulsos de láser o pulsos de microondas.

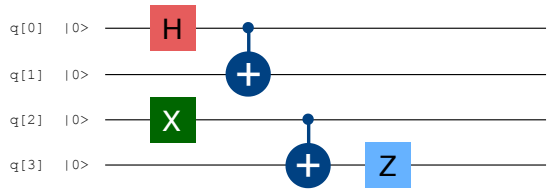


Figura 3: Circuito cuántico de cuatro cúbits formado por una composición de puertas cuánticas de uno y dos cúbits donde la ejecución siempre fluye de izquierda a derecha. Elaboración propia.

La notación gráfica mostrada en la figura anterior, que representa una serie de transformaciones que actúan sobre varias combinaciones de cúbits, se utiliza normalmente para describir la secuencia de transformaciones y analizar los algoritmos. Las transformaciones simples se representan gráficamente mediante cajas debidamente etiquetadas que se conectan para formar circuitos más complejos, cada línea horizontal corresponde a un cúbit y el procesamiento procede de izquierda a derecha. Las puertas etiquetadas como H, X y Z corresponden a transformaciones de un solo cúbit, mientras que las dos restantes corresponde a una transformación de dos cúbit, una de ellas actuando sobre los cúbits $q[0]$ y $q[1]$ y la otra sobre los cúbits $q[2]$ y $q[3]$.

Al decir que se aplica el operador U al cúbit i de un sistema cuántico de n cúbit, significa que se aplica el siguiente operador a todo el sistema:

$$I \otimes \cdots \otimes I \otimes U \otimes I \otimes \cdots \otimes I,$$

donde I es el operador de identidad de un solo cúbit, aplicado a cada uno de los otros cúbits del sistema.

Puertas de Pauli

Las transformaciones de un solo cúbit más utilizadas son las transformaciones de Pau-

li. La transformación más simple posible es la transformación identidad I, cuya representación es la siguiente:

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Las otras tres transformaciones de Pauli son X, Y y Z:

Pauli X corresponde con una rotación de π alrededor del eje X en la esfera de Bloch:

$$X = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

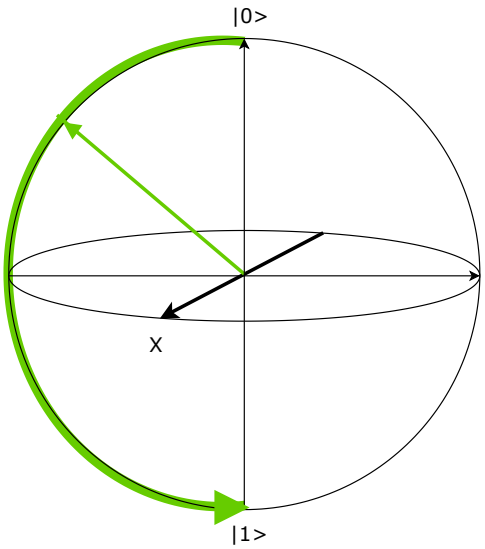


Figura 4: Puerta Pauli X como una rotación de π radianes alrededor del eje X.. Elaboración propia.

Pauli Y corresponde con una rotación de π alrededor del eje Y en la esfera de Bloch:

$$Y = \sigma_y = i|1\rangle\langle 0| - i|0\rangle\langle 1| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

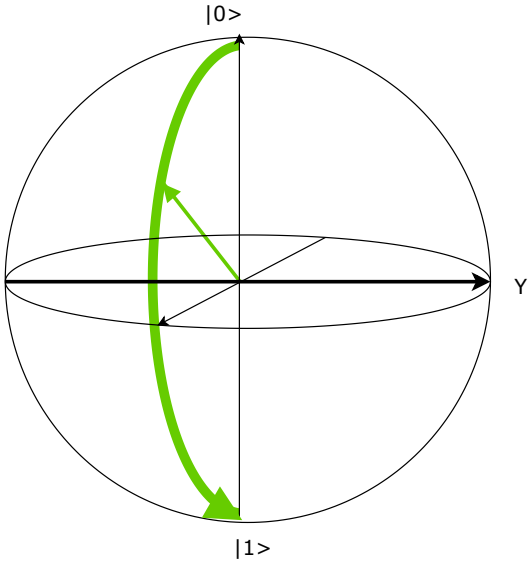


Figura 5: Puerta Pauli X como una rotación de π radianes alrededor del eje X.. Elaboración propia.

Pauli Z corresponde con una rotación de π alrededor del eje Z en la esfera de Bloch:

$$Z = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

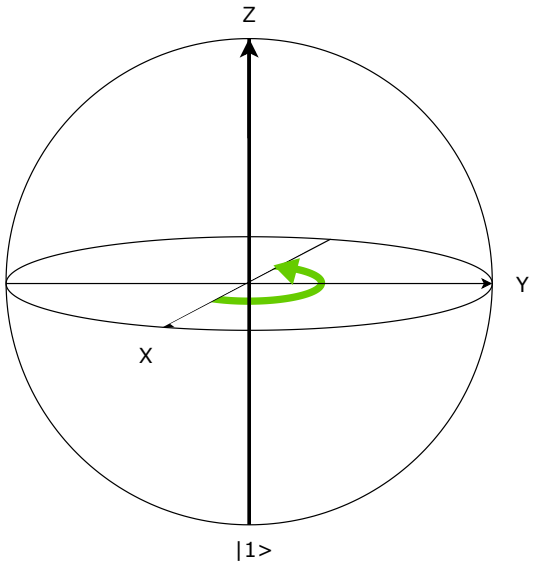


Figura 6: Puerta Pauli X como una rotación de π radianes alrededor del eje X.. Elaboración propia.

La transformación I no modifica el estado, Pauli X es la negación, equivalente a la operación clásica NOT, que intercambia los estados $|0\rangle$ y $|1\rangle$.

Pauli Z cambia la fase relativa de una superposición en la base estándar y finalmente, Pauli Y puede expresarse como: $Y = ZX$ es una combinación de negación y cambio de fase.

En ocasiones se utiliza también la notación σ_x, σ_y, y σ_z para representar las puertas de Pauli, gráficamente se representan con cajas y la letra correspondiente, Pauli X en ocasiones se representa con el signo + rodeado de un círculo.

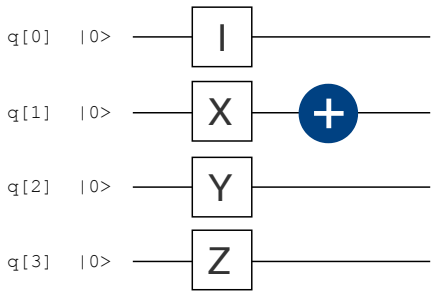


Figura 7: Representación gráfica de las puertas de Pauli. Elaboración propia.

Puerta de Hadamard

La transformación de Hadamard es otra de las transformaciones que actúan sobre un cúbit más importantes, produce una superposición uniforme de $|0\rangle$ y $|1\rangle$ a partir de cualquiera de los estados de la base computacional. Su representación es la siguiente:

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

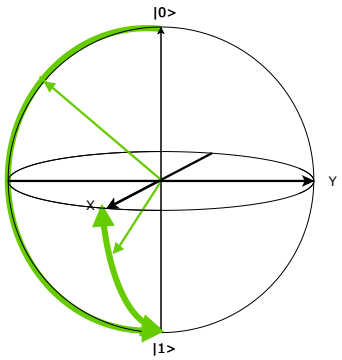


Figura 8: Puerta de Hadamard como una doble rotación de π radianes alrededor del eje X seguida de otra de $\pi/2$ radianes alrededor del eje Y. Elaboración propia.

La transformación de Hadamard, es su propia inversa, es Hermítica y por tanto, apli-

cada dos veces, corresponde con la identidad, $HH = I$ y asigna:

H :

$|0\rangle \rightarrow |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|1\rangle \rightarrow |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Las transformaciones que actúan sobre varios cúbits y que se pueden construir como productos tensoriales de transformaciones que actúan sobre un único cúbit. Estas transformaciones no son interesantes como transformaciones que aplican a múltiples cúbit ya que son equivalentes a realizar transformaciones de un solo cúbit en cada uno de los cúbits por separado en cierto orden. Por ejemplo, la transformación $U \otimes V$ se puede obtener aplicando primero $U \otimes I$ y luego $I \otimes V$.

Las transformaciones que modifican el entrelazamiento entre cúbits son de mayor interés. El entrelazamiento no es una propiedad local, las transformaciones que actúan por separado en dos o más subsistemas no pueden afectar al entrelazamiento entre esos subsistemas. De una forma más precisa, sea $|\psi\rangle$ un estado de dos cúbit y U y V dos transformaciones unitarias de un solo cúbit. Entonces $(U \otimes V)|\psi\rangle$ es un estado entrelazado si y solo si $|\psi\rangle$ es un estado entrelazado. A continuación se estudian las puertas controladas de dos cúbit y sus efectos sobre el entrelazamiento.

CNOT (Controled NOT). Puerta NOT controlada

La puerta CNOT actúa sobre dos cúbits: un cúbit de *control* y un cúbit *objetivo*. Aplica una puerta NOT al cúbit objetivo solo si el cúbit de control se encuentra en el estado $|1\rangle$, de lo contrario, lo deja sin cambios. Esta puerta, no puede descomponerse en un producto tensor de dos transformaciones de un solo cúbit.

La transformación CNOT tiene la siguiente representación:

$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) =$

$= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$

De esta forma, su efecto sobre los elementos de la base estándar sería:

$CNOT$:

$|00\rangle \rightarrow |00\rangle$

$|01\rangle \rightarrow |01\rangle$

$|10\rangle \rightarrow |11\rangle$

$|11\rangle \rightarrow |10\rangle$

Y su represetación matricial, en la base computacional, es la siguiente:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Graficamente, CNOT tiene las siguientes representaciones, donde el círculo pequeño indica el bit de control, la X o el circulo con el signo '+' la negación del bit objetivo y la línea entre ellos informa que la negación es condicional, dependiendo del valor del bit de control.

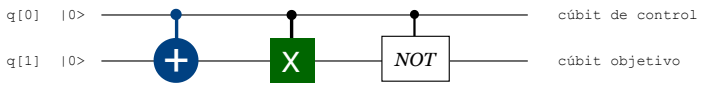


Figura 9: Representación gráfica de la puerta CNOT. Elaboración propia.

La importancia de esta puerta en computación cuántica radica en su capacidad de modificar el entrelazamiento entre dos cúbits. La puerta CNOT es, desde luego, unitaria y además, su propia inversa: $CNOT = CNOT^{-1}$, de este modo puede tanto generar entrelazamiento como eliminarlo.

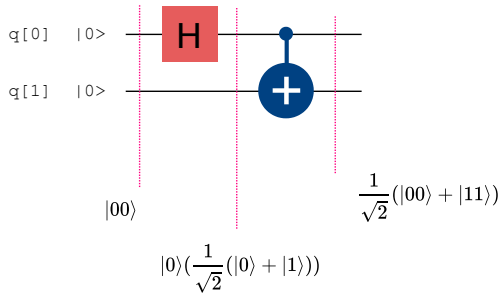


Figura 10: Circuito que genera entrelazamiento entre dos cúbits utilizando las puertas Hadamard y CNOT. Elaboración propia.

El estado $|0\rangle(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle))$ no presenta entrelazamiento, si se aplica una puerta CNOT al estado anterior se genera un estado completamente entrelazado entre los dos cúbits: $CNOT(|0\rangle(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle))) = CNOT(\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ y si aplicamos de nuevo CNOT: $CNOT(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ que, como al principio, no presenta entrelazamiento esto es debido a que la puerta CNOT es su propia inversa.

Otras puertas controladas

Al igual que la puerta NOT puede controlarse, también es posible controlar otras puertas que realizan una transformación U sobre el cúbit objetivo cuando el cúbit de control es $|1\rangle$ y no actúan cuando es $|0\rangle$. Estas puertas controladas tienen una representación gráfica genérica como se muestra en la siguiente figura.

Figura 11: Representación gráfica de una puerta genérica U-controlada. Elaboración propia. p

Se utiliza la siguiente nomenclatura para estas transformaciones:

$$CU = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

Si U es una puerta que actúa sobre un cúbit con la siguiente representación matricial:

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$$

Entonces, la puerta U controlada es una puerta que opera sobre dos cúbits de forma que el cúbit de control determina si la puerta U se aplica o no sobre el cúbit objetivo. Asigna los estados de la base computacional de la siguiente forma:

$$|00\rangle \mapsto |00\rangle$$

$$|01\rangle \mapsto U|0\rangle \otimes |1\rangle = (u_{00}|0\rangle + u_{10}|1\rangle) \otimes |1\rangle$$

$$|10\rangle \mapsto |10\rangle$$

$$|11\rangle \mapsto U|1\rangle \otimes |1\rangle = (u_{01}|0\rangle + u_{11}|1\rangle) \otimes |1\rangle$$

En la base computacional, la transformación de dos cúbits CU se representa mediante una matriz cuadrada de dimensión cuatro.

$$CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}$$

Así, por ejemplo, CNOT:

$$CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Se puede generalizar una puerta de rotación, o cambio de fase, arbitraria, controlada. En la base estándar, el cambio de fase controlado cambia la fase del segundo bit si y solo si el bit de control es uno:

$$CP(\theta) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes P$$

Siendo P:

$$P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Y por tanto, su representación matricial:

$$CP(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$$

El cambio de fase controlado hace uso de una transformación de un solo cúbit que era un cambio de fase global, físicamente sin significado cuando se aplicaba a un sistema de un solo cúbit, pero cuando se usa como parte de una transformación condicional, este cambio de fase se vuelve no trivial, cambiando la fase relativa entre elementos de una superposición. Por ejemplo, asigna:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + e^{i\theta}|11\rangle)$$

Los elementos gráficos que se ha presentado pueden combinarse para crear circuitos cuánticos, el siguiente circuito, por ejemplo, realiza un intercambio de estado entre dos cúbits o puerta swap.

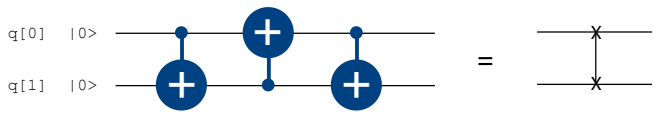


Figura 12: Circuito que intercambia el estado de dos cúbits. Elaboración propia.

Asignando:

$|00\rangle \mapsto |00\rangle$

$|01\rangle \mapsto |10\rangle$

$|10\rangle \mapsto |01\rangle$

$|11\rangle \mapsto |11\rangle$

O, en general, $|\psi\rangle|\varphi\rangle \rightarrow |\varphi\rangle|\psi\rangle$ para cualquiera estados $|\psi\rangle$ y $|\varphi\rangle$ de un cúbit.

Hay que tener en consideración que una transformación unitaria en el espacio vectorial complejo está completamente determinada por su acción sobre una base, sin embargo, en el espacio de estados, la transformación unitaria no está completamente determinada especificando qué estados resultan de hacer actuar la transformación sobre los estados de la base. Por ejemplo, el cambio de fase controlado transforma los cuatro estados cuánticos representados por $|00\rangle$, $|01\rangle$, $|10\rangle$, y $|11\rangle$ en sí mismos; $|10\rangle$ y $e^{i\theta}|10\rangle$ representan exactamente el mismo estado cuántico, al igual que $|11\rangle$ y $e^{i\theta}|11\rangle$. Sin embargo, como se mostró anteriormente, esta transformación no es la transformación identidad, ya que transforma $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + e^{i\theta}|11\rangle)$

Especificar que el vector $|0\rangle$ es asignado al vector $-|1\rangle$ es diferente a especificar que el vector $|0\rangle$ es asignado al vector $|1\rangle$ ya que ambos vectores $|1\rangle$ y $-|1\rangle$ son vectores diferentes, incluso si corresponden al mismo estado. La transformación en el espacio de estados se puede derivar fácilmente a partir de la transformación unitaria sobre el espacio vectorial complejo asociado.

Otro aspecto importante a considerar es que, si bien el comportamiento de la puerta $CNOT$ clásica nunca altera el estado del bit de control, esto no es cierto para todos los casos en su versión cuántica. Cuando los cúbits no se encuentran en un estado correspondiente a los elementos de la base estándar, el efecto de la puerta controlada puede no resultar intuitivo. Así, por ejemplo, en la especificación de la puerta $CNOT$ en la base de Hadamard $|+\rangle, |-\rangle$, es el estado del cúbit objetivo el que permanece sin cambio mientras que el estado del cúbit de control se invierte

$CNOT$:

$$|++\rangle \mapsto |++\rangle$$

$$|+-\rangle \mapsto |+-\rangle$$

$$|-+\rangle \mapsto |--\rangle$$

$$|--\rangle \mapsto |-+\rangle$$

Así, en la base de Hadamard, los roles del cúbit de control y objetivo se han invertido, sin embargo, la transformación es la misma.

La representación gráfica de los circuitos cuánticos puede no interpretarse correctamente si no se analiza en detalle. Así, no se puede determinar el efecto que tiene una transformación sobre los cúbits de entrada, incluso si todos son estados de la base estándar, simplemente observando la línea en el diagrama correspondiente a ese cúbit. Por ejemplo, en el siguiente circuito, si el circuito actúa sobre el estado $|00\rangle$, puesto que la puerta Hadamard es su propia inversa, podría deducirse, incorrectamente, que el cúbit de arriba permancerá sin modificarse al atravesar el circuito, cuando en realidad si lo hace, ya que asigna:

$$|00\rangle \rightarrow \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle)$$

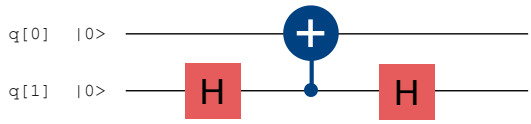


Figura 13: Ejemplo de circuito. Elaboración propia.

6.4 Aplicaciones

Durante muchos años, el entrelazamiento ha generado un interés meramente teórico, sin embargo, el procesamiento de la información cuántica cambia esa perspectiva mostrando aplicaciones prácticas del entrelazamiento como son, la codificación superdensa o la teleportación.

La codificación superdensa utiliza un bit cuántico junto con un par entrelazado, para el que suele escogerse entre uno de los estados de la base de Bell:$|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$, donde:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle$$

Este par entrelazado es compartido y se utiliza para codificar y transmitir dos bits clásicos.

Dado que los pares entrelazados se pueden distribuir con anticipación, solo se necesita transmitir físicamente un cúbit para comunicar dos bits de información, lo cual, resulta sorprendente, ya que, como se ha estudiado en temas anteriores, solo se puede extraer un bit clásico de información a partir de un cúbit.

La teleportación es el proceso inverso a la codificación superdensa en la cual se quiere teleportar un estado cuántico de un sistema a otro mediante la transmisión por un canal clásico de dos bits clásicos. La teleportación es igualmente sorprendente, por un lado, a pesar del principio de no clonación de la mecánica cuántica, este mecanismo permite la transmisión de un estado cuántico desconocido. Por otro, muestra que dos bits clásicos son suficientes para comunicar el estado de un cúbit que puede estar en cualquiera de un número infinito de estados posibles.

El elemento fundamental en ambos procesos es el entrelazamiento.

Teleportación cuántica

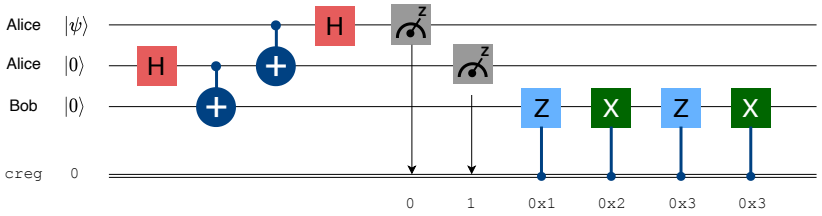


Figura 14: Circuito de teleportación cuántica. Elaboración propia.

El objetivo de la teleportación es transmitir información del estado cuántico de una partícula, utilizando bits clásicos, de forma que un receptor pueda reconstruir el estado cuántico exacto. Dado que el principio de no clonación de la mecánica cuántica significa que un estado cuántico no se puede copiar, el estado cuántico de la partícula original no se puede conservar. Es esta propiedad, que el estado original en la fuente debe ser destruido en el curso de la creación del estado en el objetivo, lo que le da a la teleportación cuántica su nombre.

Alice tiene un cúbit en un estado desconocido $|\psi\rangle = a|0\rangle + b|1\rangle$. Y quiere enviar dicho estado a Bob a través de un canal clásico. Alice y Bob poseen cada uno un cúbit de un par entrelazado $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

El estado inicial de los tres cúbits es $|00\psi\rangle$, como se observa en la figura anterior. Una vez el los cubits compartidos se entrelazan, el estado del sistema es el siguiente:

$$|\phi\rangle \otimes |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes (a|0\rangle + b|1\rangle) = \frac{1}{\sqrt{2}}(a|000\rangle + b|001\rangle + a|110\rangle + b|111\rangle)$$

A continuación Alice entrelaza su cúbit de la pareja compartida con el cúbit que contiene el estado que se quiere transmitir, y para ello aplica $I \otimes CNOT$ seguido de $I \otimes I \otimes H$, para obtener:

$$(I \otimes I \otimes H)(I \otimes CNOT)(|\phi\rangle \otimes |\psi\rangle) = (I \otimes I \otimes H)\frac{1}{\sqrt{2}}(a|000\rangle + b|011\rangle + a|110\rangle + b|101\rangle)$$

Aplicando ahora Hadamard al cúbit de arriba (el que inicialmente contenía el estado que queremos transmitir):

$$= \frac{1}{2}(a(|000\rangle + |001\rangle + |110\rangle + |111\rangle) + b(|010\rangle - |011\rangle + |100\rangle - |101\rangle))$$

y finalmente:

$$= \frac{1}{2}((a|0\rangle + b|1\rangle)|00\rangle + (a|0\rangle - b|1\rangle)|01\rangle + (a|1\rangle + b|0\rangle)|10\rangle + (a|1\rangle - b|0\rangle)|11\rangle)$$

Alice mide los dos primeros cúbits y obtiene uno de los cuatro posibles estados de la base $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$, con la misma probabilidad. En función del resultado, el estado cuántico del cúbit de Bob es proyectado a $a|0\rangle + b|1\rangle$, $a|1\rangle + b|0\rangle$, $a|0\rangle - b|1\rangle$ o $a|1\rangle - b|0\rangle$. Alice entonces envía el resultado de su medida a Bob utilizando un canal clásico.

Después de estas transformaciones, la información del estado original $|\psi\rangle$ está en el cúbit de Bob. Ya no es posible para Alice reconstruir el estado original de su cúbit. De hecho, el principio de no clonación implica que en cada momento dado, solo uno de ellos, Alice o Bob, puede reconstruir el estado cuántico original.

Cuando Bob recibe los dos bits clásicos de Alice, sabe cómo reconstruir el estado original del cúbit de Alice, $|\psi\rangle$, aplicando la transformación de *decodificación* correspon-

diente a su cúbit, originalmente parte del par entrelazado.

A continuación se muestra el operador de decodificación que debe aplicar Bob a su cúbit para recuperar el estado en función de la medida realizada por Alice.

Medida (Alice)	Acción (Bob)
$\|00\rangle$	No necesita aplicar ninguna transformación, su cúbit tiene el estado deseado
$\|01\rangle$	Aplicar la transformación Z
$\|10\rangle$	Aplicar la transformación X
$\|11\rangle$	Aplicar la transformación Y (ZX)

Codificación superdensa

En este caso, Alice desea transmitir el estado de dos bits clásicos (b_2, b_1) que codifican uno de los números del 0 al 3.

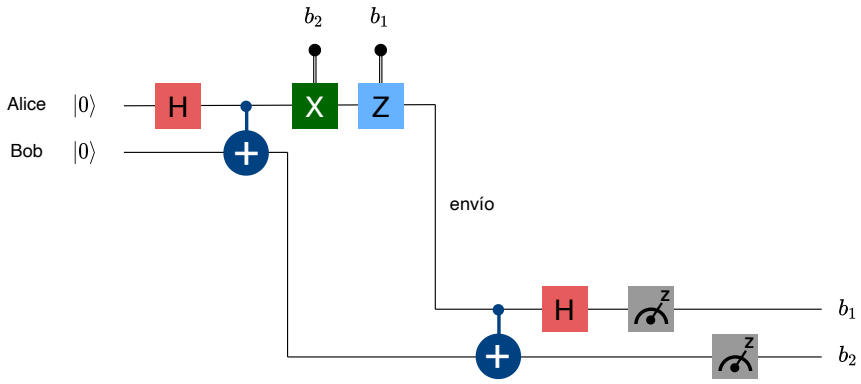


Figura 15: Circuito que implementa la codificación superdensa. Elaboración propia.

Tras el entrelazamiento el sistema se encuentra en el estado $|\psi\rangle$.

Dependiendo del numero que Alice desea transmitir, Alice realiza una de las transformaciones de Pauli I, X, Y, Z en su cúbit del par entrelazado.

El estado resultante será:

Valor a transmitir b_2b_1	Transformación aplicada	Estado resultante
00=0	$(I \otimes I)\|\psi\rangle$	$\|\Phi^+\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle$
01=1	$(I \otimes X)\|\psi\rangle$	$\|\Psi^+\rangle = \frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle$
10=1	$(I \otimes Z)\|\psi\rangle$	$\|\Phi^-\rangle = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle$
11=3	$(I \otimes Y)\|\psi\rangle = (I \otimes Z)(I \otimes X)\|\psi\rangle$	$\|\Psi^-\rangle = \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle$

A continuación Alice envía su cúbit a Bob.

Para decodificar la información, Bob aplica un no controlado a los dos cúbits del par entrelazado y luego aplica la puerta de Hadamard al primer cúbit con lo cual los cuatro posibles estados evolucionarían de la siguiente forma:

$$CNOT(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle + |1\rangle)$$

$$CNOT(\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}|1\rangle \otimes (|0\rangle + |1\rangle)$$

$$CNOT(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle) = \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle)$$

$$CNOT(\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|11\rangle - |10\rangle) = \frac{1}{\sqrt{2}}|1\rangle \otimes (|1\rangle - |0\rangle)$$

Aplicando Hadamard al cúbit de arriba:

$$(I \otimes H)(\frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle + |1\rangle)) = |00\rangle$$

$$(I \otimes H)(\frac{1}{\sqrt{2}}|1\rangle \otimes (|0\rangle + |1\rangle)) = |10\rangle$$

$$(I \otimes H)(\frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle)) = |01\rangle$$

$$(I \otimes H)(\frac{1}{\sqrt{2}}|1\rangle \otimes (|1\rangle - |0\rangle)) = |11\rangle$$

Finalmente Bob mide los dos cúbits en la base estándar para obtener la codificación binaria del número que Alice deseaba enviar.

6.5 Referencias bibliográficas

Nielsen and Chuang (2011) Quantum Computation and Quantum Information

Aaronson (2013), Quantum Computing Since Democritus

Eric R. Johnston, Nic Harrigan y Mercedes Gimeno-Segovia (2019), Programming Quantum Computers

Eleanor Rieffel and Wolfgang Polak (2011), Quantum Computing

Robert Sutor (2019), Dancing with cúbits