Introducción a la Información Cuántica

Autores: Andrés García Sandoval
Iván Fernando Valtierra Carranza
Omar Vladimir Macías Sandoval

Sexta Escuela de Verano de Matemáticas

2022

Introducción a la Información Cuántica

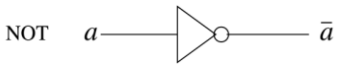
En este capítulo se busca mostrar la "extensión natural" de los conceptos básicos de la información clásica a la información cuántica. Con este objetivo en mente, se pretende abordar las analogías y diferencias que existen entre la información clásica y la información cuántica, destacando las ventajas que ofrece ésta última a partir del "entrelazamiento" de partículas. Aunque se pretende dar un acercamiento matemático a la información cuántica, será inevitable recurrir a algunas menciones "físicas" pero se evitará profundizar demasiado en ellas.

Bits y compuertas lógicas.

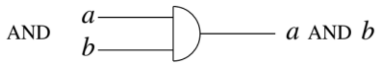
Para un ordenador clásico, la unidad elemental de información es el bit. Físicamente un bit puede ser implementado con un dispositivo electrónico de dos estados, por ejemplo, la dirección de corriente en un circuito de transistores, el estado de carga de una capacitancia, etcétera. Matemáticamente, la representación para un bit b es mediante un 0 o un 1, es decir $b \in \{0,1\}$. Si se consideran cadenas de n-bits, se disponen de 2^n valores diferentes $(00\cdots0, 00\cdots01, \dots, 11\cdots1)$, lo cual permite, por ejemplo, representar en lenguaje binario cualquier entero positivo x (o un símbolo asociado con él) en la forma $x \equiv x_1x_2\cdots x_n$ con $x_i \in \{0,1\},\ i = 1,\dots,n,$ donde $x = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n 2^0$. Utilizando esta representación, es fácil ver que con un byte de memoria (8 bits), se pueden almacenar números enteros en el rango de 0 a 255 (si el primer bit se usa para indicar signo, entonces el byte puede almacenar números en el rango de -127 a 127). Una vez que se consigue codificar la información en cadenas de bits, surge la necesidad de lograr un procesamiento o manejo adecuado de éstos (computación). El procesamiento de los bits se realiza mediante una secuencia de operaciones lógicas elementales lo cual puede ser esquematizado mediante circuitos. Los circuitos se componen de "cables" (que transportan bits) y de "compuertas lógicas". Una compuerta lógica es una función $f:\{0,1\}^n \to \{0,1\}^m$ que toma n bits de entrada y devuelve m bits de salida. A continuación, se muestran las compuertas lógicas elementales de la computación clásica:

1. Unity (unidad o identidad): $f:\{0,1\}\to\{0,1\}$ dada por $f(a)=a$.

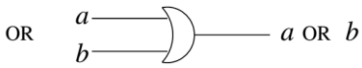
2. NOT: $f:\{0,1\}\to\{0,1\}$ dada por $f(a)=1\oplus a$ (en lo sucesivo, $\oplus$ representa suma módulo 2).



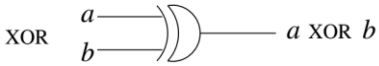
3. AND: $f:\{0,1\}^2\to\{0,1\}$ dada por $f(a,b)=\begin{cases}1 & \text{si } a=b=1\\ 0 & \text{en otro caso}\end{cases}$.



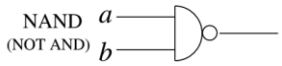
4. OR: $f:\{0,1\}^2\to\{0,1\}$ dada por $f(a,b)=\begin{cases}1 & \text{si } a=1 \text{ o } b=1\\ 0 & \text{en otro caso}\end{cases}$.



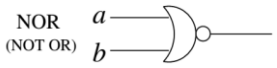
5. XOR: $f:\{0,1\}^2\to\{0,1\}$ dada por $f(a,b)=a\oplus b$.



6. NAND: $f:\{0,1\}^2\to\{0,1\}$ dada por $f(a,b)=\begin{cases}0 & \text{si } a=b=1\\ 1 & \text{en otro caso}\end{cases}$.



7. NOR: $f:\{0,1\}^2\to\{0,1\}$ dada por $f(a,b)=\begin{cases}0 & \text{si } a=1 \text{ o } b=1\\ 1 & \text{en otro caso}\end{cases}$.



Qubits y compuertas lógicas.

De forma análoga a la información clásica, la unidad básica de la información cuántica es el bit cuántico o simplemente qubit. Físicamente un qubit puede ser concebido, por ejemplo, con un átomo de dos niveles de energía, el spín del electrón ($\uparrow,\downarrow$), la polarización de un fotón, etc. Matemáticamente, un qubit $|\psi\rangle$ es un sistema mecánico-cuántico con dos estados ortogonales $|0\rangle$ y $|1\rangle$, los cuales forman una base (denominada base computacional) de $\mathbb{C}^2$. Un qubit $|\psi\rangle\in\mathbb{C}^2$ no sólo puede estar en alguno de los estados base, sino que puede estar en una combinación lineal (superposición) de ellos, es decir:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle, \tag{1}$$

donde $c_0, c_1 \in \mathbb{C}$ satisfacen $|c_0|^2 + |c_1|^2 = 1$ y

$$\mathfrak{B} = \left\{|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}\right\}. \tag{2}$$

La superposición de estados cuánticos marca una diferencia abismal entre la información cuántica y la clásica, pues mientras un bit solo puede almacenar dos valores reales (discretos), el qubit puede representar una infinidad de estados (un continuo de estados) mediante un vector unitario del espacio vectorial complejo $\mathbb{C}^2$. Si se consideran cadenas de n-qubits, se disponen de 2^n estados ortogonales que forman una base de $\mathbb{C}^{2^n}$ ($|00\cdots00\rangle, |00\cdots01\rangle, \ldots, |11\cdots11\rangle$), donde

$$|a_1 a_2 \cdots a_n\rangle = |a_1\rangle \otimes |a_2\rangle \cdots \otimes |a_n\rangle, \tag{3}$$

donde $a_i \in \{0,1\}$, $i = 1,2,\ldots,n$, y el símbolo $\otimes$ denota el producto de Kronecker (ver el siguiente ejemplo).

Ejemplo: Obtener los vectores de la base computacional para dos qubits.

Solución: El espacio vectorial correspondientes es $\mathbb{C}^{2^2}$, el cual tiene dimensión 4 y su base computacional estará formada por los cuatro estados $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Explícitamente los vectores se obtienen de la forma:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1 \cdot \begin{bmatrix}1\\0\end{bmatrix}\\ 0 \cdot \begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix},$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1 \cdot \begin{bmatrix}0\\1\end{bmatrix}\\ 0 \cdot \begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0 \cdot \begin{bmatrix}1\\0\end{bmatrix}\\ 1 \cdot \begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix},$$

$$|11\rangle = |1\rangle\otimes|1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0 \cdot \begin{bmatrix}0\\1\end{bmatrix}\\ 1 \cdot \begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}.$$

Entonces, un estado $|\psi\rangle$ de dos qubits podría ser representado con un vector de la forma:

$$|\psi\rangle = c_{00}|00\rangle + c_{01}\,|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \tag{4}$$

donde los $c_x \in \mathbb{C}$ satisfacen $\sum_x |c_x|^2 = 1, x \in \{00,01,10,11\}$. Cuando el estado de dos qubits se puede escribir como producto de dos qubits, se dice que es un estado producto, en otro caso, se dice que es un estado entrelazado.

Generalizando, un estado de n-qubits podría ser representado con un vector de la forma

$$|\psi\rangle = \sum_x c_x|x\rangle \tag{5}$$

con $\sum_x |c_x|^2 = 1,\ x \equiv x_1x_2\cdots x_n, x_i \in \{0,1\}, i = 1,\dots,n$. Cuando un estado de n-qubits se puede escribir como producto de n qubits, se dice que es un estado producto, en otro caso, se dice que es un estado entrelazado.

Ejemplo: Investigar si el siguiente estado es un estado producto o un estado entrelazado

$$|\psi\rangle = \tfrac{1}{2}|00\rangle - \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle.$$

Solución: El estado general de un qubit se estableció en la ecuación (1) y, por ende, el problema consiste en determinar si existe o no solución para la ecuación:

$$|\psi\rangle = (c_0|0\rangle + c_1|1\rangle)(c_0'|0\rangle + c_1'|1\rangle).$$

Si se desarrolla el producto del lado derecho:

$$\begin{aligned}(c_0|0\rangle + c_1|1\rangle)(c_0'|0\rangle + c_1'|1\rangle)&\\ = c_0c_0'|0\rangle\otimes|0\rangle + c_0c_1'|0\rangle\otimes|1\rangle + c_1c_0'|1\rangle\otimes|0\rangle + c_1c_1'|1\rangle\otimes|0\rangle&\\ = c_0c_0'|00\rangle + c_0c_1'|01\rangle + c_1c_0'|10\rangle + c_1c_0'|11\rangle,&\end{aligned}$$

la ecuación toma la forma

$$\tfrac{1}{2}|00\rangle - \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle = c_0c_0'|00\rangle + c_0c_0'|01\rangle + c_0c_0'|10\rangle + c_0c_0'|11\rangle,$$

de donde se obtiene el sistema de ecuaciones no lineales

$$\frac{1}{2} = c_0c_0',$$

$$-\frac{1}{2} = c_0c_1',$$

$$\frac{1}{2} = c_1c_0',$$

$$\tfrac{1}{2} = c_1c_1',$$

cuya solución existe y es fácil de determinar, a saber:

$$c_0 = \tfrac{1}{\sqrt{2}}, c_1 = \tfrac{1}{\sqrt{2}}, c_0' = \tfrac{1}{\sqrt{2}}, c_1' = -\tfrac{1}{\sqrt{2}}.$$

Por lo tanto, se ha demostrado que el estado $|\psi\rangle$ es un estado producto, pues se puede escribir como producto de dos estados de un solo qubit, es decir:

$$|\psi\rangle = \tfrac{1}{2}|00\rangle - \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle = \left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)\left(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle\right).$$

Ejemplo: Investigar si el siguiente estado es un estado producto o un estado entrelazado

$$|\psi\rangle = \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle.$$

Solución: De manera equivalente al ejemplo anterior, utilizamos la ecuación (1) y el problema queda planteado como "determinar si existe o no solución para la ecuación":

$$|\psi\rangle = (c_0|0\rangle + c_1|1\rangle)(c_0'|0\rangle + c_1'|1\rangle).$$

Si se desarrolla el producto del lado derecho:

$$(c_0|0\rangle + c_1|1\rangle)(c_0'|0\rangle + c_1'|1\rangle)$$
$$= c_0c_0'|0\rangle \otimes |0\rangle + c_0c_1'|0\rangle \otimes |1\rangle + c_1c_0'|1\rangle \otimes |0\rangle + c_1c_1'|1\rangle \otimes |0\rangle$$

$$= c_0c_0'|00\rangle + c_0c_1'|01\rangle + c_1c_0'|10\rangle + c_1c_0'|11\rangle,$$

la ecuación toma la forma

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = c_0c_0'|00\rangle + c_0c_0'|01\rangle + c_0c_0'|10\rangle + c_0c_0'|11\rangle,$$

de donde se obtiene el sistema de ecuaciones no lineales

$$\frac{1}{\sqrt{2}} = c_0c_0',$$

$$0 = c_0c_1',$$

$$0 = c_1c_0',$$

$$\frac{1}{\sqrt{2}} = c_1c_1'$$

de la segunda ecuación, se observa que $c_0 = 0$ y/o $c_1' = 0$. Si $c_0 = 0$ la primera ecuación no tiene solución, en otro caso, si $c_1' = 0$ la cuarta ecuación no tiene solución. Concluimos que el sistema no tiene solución y por lo tanto el estado es un estado entrelazado.

Compuertas de un qubit.

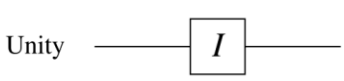
De manera similar a como ocurre con la información clásica, una vez que se dispone de cierta información codificada en un conjunto de n-qubits, será necesario su procesamiento, transmisión y/o manipulación; surge entonces la necesidad de definir compuertas cuánticas "adecuadas" y, por supuesto, circuitos cuánticos. Una compuerta cuántica será "adecuada" siempre que cumpla las siguientes características:

- El número de qubits de entrada y de salida debe coincidir (reversibilidad).
- Se debe preservar la norma $\sum_x |c_x|^2 = 1$ del estado correspondiente $|\psi\rangle$ (ver ecuación (5)).

Matemáticamente, las condiciones impuestas sobre las compuertas cuánticas implican que el operador correspondiente, que actuará en el "vector de estado" mediante multiplicación

matricial, debe ser un operador unitario U, es decir, $UU^{\dagger} = I$. A continuación, se muestran algunas de las compuertas más importantes de un qubit, es decir, transformaciones unitarias: $U: \mathbb{C}^2 \to \mathbb{C}^2$, cuya definición se da a partir de los vectores de la base computacional (2).

- Unity, $I|\psi\rangle = |\psi\rangle$, $|\psi\rangle \in \mathfrak{B} = \{|0\rangle, |1\rangle\}$ (ver (2)).



$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

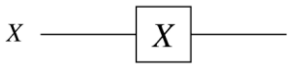
- Hadamard,

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \equiv |+\rangle,$$
$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \equiv |-\rangle.$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- $X \equiv NOT$,

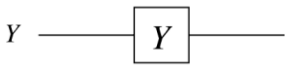
$$X|0\rangle = |1\rangle,$$
$$X|1\rangle = |0\rangle.$$



$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Y,

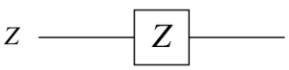
$$Y|0\rangle = i|1\rangle,$$
$$Y|1\rangle = -i|0\rangle.$$



$$Y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}$$

- Z,

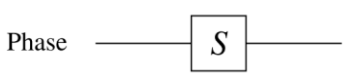
$$Z|0\rangle = |0\rangle,$$
$$Z|1\rangle = -|1\rangle.$$



$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Phase,

$$S|0\rangle = |0\rangle,$$
$$S|1\rangle = i|1\rangle.$$



$$S = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{bmatrix}$$

Ejercicio: Determine el resultado que se obtiene al aplicar cada una de las compuertas de un qubit al estado arbitrario (1); demuestre que se cumplen las identidades $H^2 = X^2 = Y^2 = Z^2 = I, S^2 = Z$.

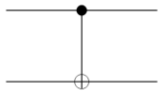
Compuertas de dos o más qubits.

A continuación, se muestran algunas de las compuertas más importantes de dos o más qubits.

- Controlled-NOT ($CNOT$, equivalente a XOR).

$$CNOT|00\rangle = |00\rangle,$$
$$CNOT|01\rangle = |01\rangle,$$
$$CNOT|10\rangle = |11\rangle,$$
$$CNOT|11\rangle = |10\rangle.$$

CNOT (XOR)



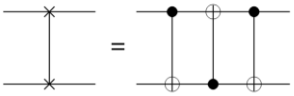
$$W_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

El funcionamiento (y el nombre) de la compuerta "Controlled-NOT" se puede aclarar utilizando la siguiente terminología: al primer qubit se le denomina "control" y al segundo "objetivo". Entonces, si el qubit de control es 0, el qubit objetivo no cambia, pero si el qubit de control es 1, se niega el qubit objetivo.

- SWAP,

$$SWAP|00\rangle = |00\rangle,$$
$$SWAP|01\rangle = |10\rangle,$$
$$SWAP|10\rangle = |01\rangle,$$
$$SWAP|11\rangle = |11\rangle.$$

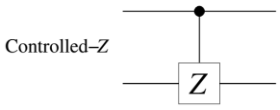
SWAP



$$W_{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

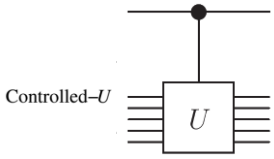
- Controlled-Z

$$Z|00\rangle = |00\rangle,$$
$$Z|01\rangle = |01\rangle,$$
$$Z|10\rangle = |10\rangle,$$
$$Z|11\rangle = -|11\rangle.$$



$$W_{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

- Controlled-U



$$W_{CU} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U & \\ 0 & 0 & & \end{bmatrix}$$

La última compuerta representa la generalización de cualquier transformación U controlada, el primer qubit es de "control" y, por lo tanto, U se aplica en los últimos n-qubits siempre que el primer qubit sea 1, en otro caso, no ocurre ningún cambio.

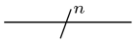
El procesamiento de los qubits se realiza mediante una secuencia de operaciones (compuertas cuánticas) y puede ser esquematizado mediante circuitos. Los circuitos se componen de "cables" (de arriba hacia abajo "transportan" el primero, segundo, …, n-ésimo qubit, de "izquierda a derecha"), y de "compuertas cuánticas" sobre los cables. A continuación, se especifican algunos símbolos más que se utilizan en un circuito cuántico:

- Medición:

- Qubit

- Bit clásico

- n-qubits



En este punto, es necesario aclarar que el "acto de medición" en información cuántica, provoca que un qubit colapse a un bit clásico, es decir, una vez que se lleva a cabo una medición se pasa de lo "cuántico" a lo "clásico" obteniéndose como resultado 0 o 1. Específicamente, medir el qubit $c_0|0\rangle + c_1|1\rangle$, producirá como salida el bit 0 con probabilidad $|c_0|^2$ y 1 con probabilidad $|c_1|^2$, y las probabilidades podrán determinarse

experimentalmente solo si se cuenta con un ensamble (conjunto) de copias del estado para realizar "muchas" mediciones que proporcionen los valores estadísticos necesarios. Se debe enfatizar que una sola medición no permitirá obtener las correspondientes amplitudes c_0 y c_1 del estado. En general no será posible acceder directamente a la información de los qubits, aunque sí de manera indirecta pues es factible manipularlos y transformarlos en formas que conducen a resultados de medición que dependen de las propiedades específicas del estado. Por lo tanto, estos estados cuánticos tienen propiedades reales y verificables experimentalmente.

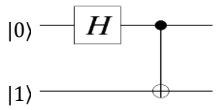
De manera similar al caso de un solo qubit, el resultado de la medición a un estado general de dos qubits (4) será $x \in \{00, 01, 10, 11\}$ el cual ocurrirá con probabilidad $|c_x|^2$. Es posible medir solo un subconjunto de los qubits, por ejemplo, si se mide el primer qubit del estado general (4), se obtendrá 0 con probabilidad igual a $|c_{00}|^2 + |c_{01}|^2$ y el estado colapsará a:

$$\frac{c_{00}|00\rangle + c_{01}|01\rangle}{\sqrt{|c_{00}|^2 + |c_{01}|^2}} = |0\rangle \frac{c_{00}|0\rangle + c_{01}|1\rangle}{\sqrt{|c_{00}|^2 + |c_{01}|^2}}$$

y 1 con probabilidad igual a $|c_{10}|^2 + |c_{11}|^2$ y el estado colapsará a:

$$\frac{c_{10}|10\rangle + c_{11}|11\rangle}{\sqrt{|c_{10}|^2 + |c_{11}|^2}} = |1\rangle \frac{c_{10}|0\rangle + c_{11}|1\rangle}{\sqrt{|c_{10}|^2 + |c_{11}|^2}}$$

Ejemplo: Determine el estado que se obtiene a partir del siguiente circuito:



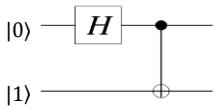
Solución: El circuito contempla dos qubits de entrada, el primero es $|0\rangle$ y el segundo $|1\rangle$. La primera operación que especifica el circuito es una Hadamard sobre el primer qubit, es decir,

$$H|01\rangle = H|0\rangle|1\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)(|1\rangle) = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Al qubit resultante se le aplica ahora una CNOT, es decir:

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

Ejemplo: Obtenga el estado que produce el siguiente circuito:



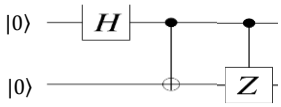
Solución: El circuito contempla dos qubits de entrada, el primero es $|1\rangle$ y el segundo $|0\rangle$. La primera operación que especifica el circuito es una Hadamard sobre el primer qubit, es decir,

$$H|10\rangle = H|1\rangle|0\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)(|0\rangle) = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Al qubit resultante se le aplica ahora una CNOT, es decir:

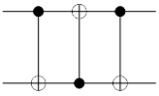
$$CNOT\left(\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle\right) = \frac{1}{\sqrt{2}}(CNOT|00\rangle - CNOT|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

Ejercicio: Calcular el estado que se obtiene a partir del siguiente circuito:



Solución: $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

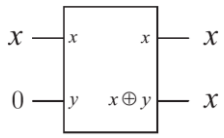
Ejercicio: Determine el estado que se obtiene a partir del siguiente circuito si la entrada es $|10\rangle$.



Solución: $|01\rangle$.

Teorema de la no-clonación.

Cuando se habla de información clásica, de manera "natural" concebimos que se puede reproducir, las veces que sea necesario y sin mayor problema. Específicamente, copiar un bit se puede llevar a cabo usando una compuerta clásica XOR, la cual toma el bit para copiar (en alguno estado desconocido x) y un bit auxiliar inicializado en cero. La salida que se obtiene son dos bits, ambos en el mismo estado x, es decir se logró clonar el estado:



Por otro lado, la situación para un qubit desconocido es completamente diferente, y es consecuencia de una característica fundamental de la mecánica cuántica: "la linealidad". Matemáticamente la linealidad garantiza que una compuerta cuántica representada por una transformación unitaria U satisface: $U(|\psi_1\rangle + |\psi_2\rangle) = U|\psi_1\rangle + U|\psi_2\rangle$. Utilizando esta propiedad, en el año 1982, Wootters y Zurek lograron probar que sería imposible clonar un estado cuántico desconocido y lo publicaron en su famoso artículo "A single quantum cannot be cloned". El sorprendente resultado publicado en dicho artículo se conoce hoy en día como "el teorema de la no-clonación" y a continuación proporcionamos una forma de demostrarlo:

Teorema de la No-clonación. El estado de un sistema cuántico desconocido, no se puede determinar con una medición realizada a una sola copia del sistema.

Demostración

Por reducción al absurdo, supongamos que sí es posible determinar un estado desconocido con una sola medición (y una sola copia). Entonces, debe existir una transformación unitaria U tal que, para dos estados cualesquiera del sistema, $|\psi_1\rangle \neq |\psi_2\rangle$ se tiene:

$$U|\psi_1\rangle|e\rangle = |\psi_1\rangle|\psi_1\rangle$$

$$U|\psi_2\rangle|e\rangle = |\psi_2\rangle|\psi_2\rangle$$

donde $|e\rangle$ denota un estado auxiliar del sistema destino. Afirmamos entonces que U es capaz de reproducir cualquier estado desconocido, sin embargo, es posible construir un estado que no puede reproducir U, lo cual es la contradicción buscada, a saber:

$$U\left(\frac{|\psi_1\rangle|e\rangle + |\psi_2\rangle|e\rangle}{\sqrt{2}}\right) = |\psi_1\rangle|\psi_1\rangle + |\psi_2\rangle|\psi_2\rangle \neq \left(\frac{|\psi_1\rangle + |\psi_2\rangle}{\sqrt{2}}\right)\left(\frac{|\psi_1\rangle + |\psi_2\rangle}{\sqrt{2}}\right) \quad \blacksquare$$

Teleportación Cuántica.

La teleportación cuántica consiste en un protocolo que nos permite transferir un estado a un lugar distante utilizando un estado entrelazado (y comunicación clásica). El protocolo se puede describir de la siguiente manera: supongamos que un emisor (E) y un receptor (R) comparten previamente el estado entrelazado:

$$|\psi\rangle_{AB} = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

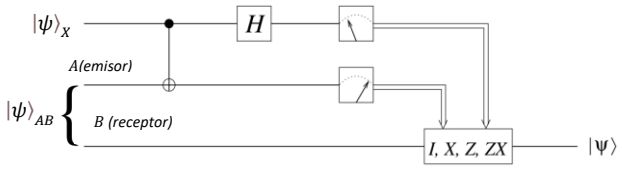
y que "E" desea enviar el estado de $|\psi\rangle_X = c_0|0\rangle_X + c_1|1\rangle_X$ a "R" sin utilizar ningún medio físico. De este estado ni "E" ni "R" conocen los valores de c_0 o c_1 (únicamente saben que, como es obvio, el estado debe estar normalizado). Como este estado lo tiene "E", tendrá tanto el qubit que tenía entrelazado con "R" como este qubit. Así, se tendrán en total tres qubits, en el que los dos primeros los tiene "E" y el tercero "R" y forma parte del estado compartido. El estado completo, considerando los tres qubits, puede ser reescrito en la forma:

$$|\psi\rangle_X \otimes |\psi\rangle_{AB} = \left(c_0|0\rangle_X + c_1|1\rangle_X\right) \otimes \left(\frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}\right) =$$

$$= \frac{1}{\sqrt{2}}\left[c_0|0\rangle_X\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) + c_1|1\rangle_X\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)\right]$$

Con esta preparación, "A" puede realizar la teleportación del estado $|\psi\rangle_X$ a "B" aplicando la siguiente sucesión de transformaciones: 1) CNOT a sus dos qubits, es decir a los primeros dos qubits, donde el qubit $|\psi\rangle_X$ es el qubit de control, 2) Hadamard al primer qubit, 3) mide sus dos qubits y comunica el resultado a "B" mediante un canal clásico. La información que

el receptor recibirá de "A" es una de las cuatro posibles parejas de bits clásicos resultados de la medición, 00, 01, 10, y 11 (los cuales están relacionados con los qubits $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, respectivamente). Para recuperar el estado, previamente "B" sabe que deberá realizar lo siguiente: 1) no realizar ninguna operación si recibe 00 (equivale a la compuerta I), 2) aplicar X si recibe 01, 3) aplicar Z si recibe 10 y 4) aplicar ZX si recibe 11. El protocolo descrito en este párrafo se puede describir con el circuito:



Explícitamente, los cálculos realizados por "A" son, respectivamente:

$$H_1\left[CNOT_{12}\left(|\psi\rangle_X \otimes |\psi\rangle_{AB}\right)\right]$$

$$= H_1\left\{\frac{1}{\sqrt{2}}\left[c_0\left(|0\rangle_X\right)\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) + c_1|1\rangle_X\left(|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B\right)\right]\right\}$$

$$= \frac{1}{2}\left[c_0\left(|0\rangle_X + |1\rangle_X\right)\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) + c_1\left(|0\rangle_X - |1\rangle_X\right)\left(|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B\right)\right]$$

$$= \frac{1}{2}\left[|0\rangle_X|0\rangle_A\left(c_0|0\rangle_B + c_1|1\rangle_B\right) + |0\rangle_X|1\rangle_A\left(c_0|1\rangle_B + c_1|0\rangle_B\right)\right.$$
$$\left. + |1\rangle_X|0\rangle_A\left(c_0|0\rangle_B - c_1|1\rangle_B\right) + |1\rangle_X|1\rangle_A\left(c_0|1\rangle_B - c_1|0\rangle_B\right)\right]$$

Observando esta última expresión, es claro que una vez que el receptor reciba el resultado de la medición, puede arreglar su estado para recuperar $|\psi\rangle_X$ aplicando la compuerta apropiada (I, X, Z o ZX), lo cual se resume en la siguiente tabla:

Resultado de la medición	Estado del Receptor	Compuerta por aplicar	Resultado
00	$c_0\|0\rangle_B + c_1\|1\rangle_B$	I	$c_0\|0\rangle_B + c_1\|1\rangle_B$
01	$c_0\|1\rangle_B + c_1\|0\rangle_B$	X	$c_0\|0\rangle_B + c_1\|1\rangle_B$
10	$c_0\|0\rangle_B - c_1\|1\rangle_B$	Z	$c_0\|0\rangle_B + c_1\|1\rangle_B$
11	$c_0\|1\rangle_B - c_1\|0\rangle_B$	ZX	$c_0\|0\rangle_B + c_1\|1\rangle_B$

Después de analizar lo logrado con la teleportación, surge una inquietud que parece contradecir la teoría de la relatividad: ¿es posible transmitir información cuántica a una rapidez superior a la de la luz? La respuesta es NO, pues como se vio explícitamente, es necesario utilizar un canal clásico para completar la teleportación, y cualquier canal clásico está limitado por la velocidad de la luz, por lo tanto, se concluye que la transmisión de información no se puede llevar a cabo a una rapidez superior a la de la luz.

Criptografía cuántica.

La criptografía es una disciplina de las matemáticas que busca lograr el intercambio seguro de información, a sabiendas de que se utilizan canales de comunicación inseguros. Uno de los protocolos de criptografía clásica más utilizado es el de clave privada. La "protección" de este tipo de protocolos se basa en que la inversión (obtener la clave por parte de un tercero), requeriría de la factorización de un número entero grande, lo cual es básicamente imposible para los ordenadores clásicos. Para describir el protocolo de clave privada, considere lo siguiente: un emisor (E) y un receptor (R) que comparten una clave privada constituida de N bits aleatorios que solo ellos conocen; si "E" requiere comunicarse con "R", le manda un mensaje secreto a través de un canal convirtiéndolo antes de enviarlo en una cadena de bits utilizando el código ASCII (cuya longitud es $M \leq N$) y luego usa la clave privada para cifrar el mensaje y enviárselo a "R". El procedimiento de cifrado consiste en agregar los bits aleatorios de la clave privada, uno por uno, a la cadena de mensaje usando suma módulo 2, es decir,

$$\overbrace{011101001\cdots}^{Mensaje\ (ASCCI)} \oplus \overbrace{110100101\cdots}^{Clave\ Privada} = \overbrace{101001100\cdots}^{Mensaje\ (encriptado)}$$

Al recibir el mensaje encriptado, "R" puede descifrarlo mediante la siguiente suma módulo 2:

$$\overbrace{101001100\cdots}^{Mensaje\ (encriptado)} \oplus \overbrace{110100101\cdots}^{Clave\ Privada} = \overbrace{011101001\cdots}^{Mensaje\ (ASCCI)}$$

A pesar de la seguridad que ofrecen estos códigos de encriptación, en 1999 Peter E. Shor mostró que, con un ordenador cuántico, la factorización de enteros sería factible (algoritmo

de Shor) y por lo tanto los protocolos de criptografía clásicos serían completamente vulnerables ante un intento de descifrado. Considerando esta problemática, si se logra el desarrollo de un ordenador cuántico, los protocolos de criptografía cuántica se convertirían en una mejor opción. A continuación, se describe el primer protocolo cuántico desarrollado el cual se conoce como BB84.

- Protocolo BB84

El nombre de este protocolo es debido a sus autores y al año en que fue desarrollado: Bennett y Brassard, 1984. El protocolo BB84 considera la construcción de una clave privada utilizando estados cuánticos. La construcción de la clave privada se puede explicar de la siguiente manera: suponga que un emisor (E) y un receptor (R) establecen dos canales de comunicación (uno cuántico y otro clásico). Si "E" le envía $2N$-qubits a "R" (por el canal cuántico), cada uno preparado en uno (elegido de manera aleatoria) de los cuatro estados: $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Si se considera que $\{|0\rangle, |+\rangle\}$, corresponde al valor 0 de "E" y los estados $\{|1\rangle, |-\}$ al valor 1. Una vez que "R" recibe los qubits enviados por "E", procede a medirlos (uno por uno) en cualquiera de las dos bases $\{|0\rangle, |1\rangle\}$ o $\{|+\rangle, |-\rangle\}$ (elegida al azar). Una vez que lleva a cabo la medición, asigna 0 a su bit aleatorio, si la medición produce $|0\rangle$ o $|+\rangle$, y 1, si es $|1\rangle$ o $|-\rangle$. Utilizando el canal clásico "E" y "R" se comunican entre sí para saber si alguno de los qubits se perdió y para cuales qubits "R" usó la base correcta para medir. En ausencia de pérdidas, de $2N$-qubits recibidos y medidos por Bob, en promedio en la mitad de los casos usó la base correcta. Si alguno de los qubits no llegaró a "R", "E" puede generar y enviar una nueva cadena de qubits para compensar las pérdidas. Después de comparar las bases, "E" y "R" descartan aquellas en las que no se pusieron de acuerdo en las bases y se quedan con una clave privada de N bits aleatorios.

Si algún intruso tratara de inferir la clave privada, dicho intruso, al igual que "R", debe medir los qubits con elección de la base al azar y registrar el resultado (por el teorema de la no-clonación, no puede clonar los qubits). Luego, debe generar cada qubit detectado en el estado medido y enviárselo a "R", ya que, de lo contrario, "E" descartará todos los

qubits perdidos y los sustituirá por otros. Cuando la base de elegida por el intruso resulta correcta, "R" recibe el qubit correcto. Pero cuando la base elegida por el intruso es incorrecta, en promedio en $N/2$ bases promedio, después de proyectar sobre la base correcta, la medición de "R" arroja en la mitad de esos casos un resultado incorrecto. Para detectar la presencia del intruso, "E" y "R" pueden elegir aleatoriamente $m < N$ bits de su cadena común y compararlos públicamente. Si los valores de unos $m/4$ bits no coinciden, se dan cuenta de la presencia del intruso, por lo que deben que borrar todos los bits y empezar de nuevo. Si, por otro lado, los m bits son iguales, entonces la probabilidad de que el intruso no sea detectado es de $(3/4)^m$, que, por ejemplo, con $m = 200$ es un número increíblemente pequeño, del orden de 10^{-25}.

Qubits "físicos"

En analogía al movimiento de rotación terrestre, en 1926 G. Uhlenbeck y S. Goudsmit propusieron que un electrón, además de girar alrededor del núcleo de un átomo, también gira sobre sí mismo. Los experimentos mostraron que el electrón no tiene un movimiento de rotación "equivalente" al de la tierra pero que sí existe una propiedad (intrínseca) debida a dicho movimiento a la cual se le llamó espín. La propiedad de espín quedó evidenciada en el famoso experimento de Stern-Gerlach, donde se observó que un haz de átomos de plata (el cual se hizo pasar por un campo magnético no uniforme) se dividía en dos trazas simétricas al eje x. La proyección del espín del electrón a lo largo de cualquiera de los ejes sólo toma dos valores posibles $\{\hbar/2, -\hbar/2\}$ lo que hace viable pensar en dicha propiedad como un ejemplo físico de qubits. Otro ejemplo físico de un sistema que puede representar un qubit sería la polarización de un fotón (con polarización lineal de un modo); suponiendo que el fotón se propaga en dirección del eje z, sus posibles polarizaciones serán dos, a lo largo de los ejes x e y, respectivamente.

Apéndice: notación de Dirac y postulados de mecánica cuántica.

Un sistema cuántico es un sistema físico en escala atómica o subatómica, pueden ser, por ejemplo, sistemas físicos de átomos, electrones, fotones, etc., pero también podrían ser sistemas que se centran en una característica particular de una partícula como el espín de un electrón o la polarización de un fotón. Un sistema físico compuesto de múltiples sistemas físicos se llama sistema compuesto. La caracterización de un sistema físico está determinada por cantidades físicas que son susceptibles a ser medidas las cuales se denominan observables, entre ellas están: la posición, cantidad de movimiento, energía, momento angular, polarización de un fotón, etc. Las herramientas necesarias para poder abordar la física que implica un sistema cuántico se pueden establecer a partir de los siguientes postulados:

1. Para cualquier sistema cuántico, existe un espacio de Hilbert (espacio vectorial con producto interno, completo y separable) asociado $\mathcal{H}$ de tal manera que un estado está representado por un vector unitario de $\mathcal{H}$. Un observable A está representado por un operador hermitiano $\hat{A}$ en $\mathcal{H}$ ($\hat{A} = \hat{A}^{\dagger}$) donde el resultado de la medición es uno de sus valores propios (los cuales son reales debido a la hermiticidad del operador correspondiente). Si medimos una cantidad física $A \in L(\mathcal{H})$ (operadores lineales en $\mathcal{H}$) por un estado $|\psi\rangle \in \mathcal{H}$, entonces la probabilidad de observar un resultado "a" está dada por

$$Pr(A = a||\psi\rangle) = \langle\psi|P_a\psi\rangle \qquad \text{(A1)}$$

   Aquí, P_a es la eigen-proyección correspondiente al valor propio a de A.

2. La evolución temporal del estado $|\psi(t)\rangle$ de un sistema cuántico está gobernada por la ecuación de Schrödinger:

$$i\hbar\frac{\partial|\psi(t)\rangle}{\partial t} = \hat{H}|\psi(t)\rangle$$

   donde $\hat{H}$ es el operador Hamiltoniano y corresponde a la energía total del sistema.

La notación utilizada en los postulados es debida a Dirac y consiste en lo siguiente:

a) a los elementos de $\mathcal{H}$ se les representa en la forma $|\psi\rangle$ y al objeto $|\psi\rangle$ se le denomina vector ket o simplemente ket;

b) a los elementos pertenecientes al espacio dual $\mathcal{H}^*$ se les denota por $\langle\psi|$ y al objeto $\langle\psi|$ se le llama vector bra o simplemente bra;

c) al producto interno se le denota con el símbolo $\langle|\rangle$ y se le llama bra-ket. Para el caso de información cuántica, nos interesan sistemas de qubits; el caso más simple, un sistema de un qubit, tendrá como espacio de Hilbert asociado a $\mathcal{H} \equiv \mathbb{C}^2$, donde las operaciones (que dan estructura de espacio vectorial) son la adición vectorial y multiplicación por un escalar estándar. El producto interno de $|\psi\rangle$ con $|\varphi\rangle$, donde:

$$|\psi\rangle = \begin{bmatrix} a_1 + b_1 i \\ a_2 + b_2 i \end{bmatrix}, |\varphi\rangle = \begin{bmatrix} c_1 + d_1 i \\ c_2 + d_2 i \end{bmatrix}$$

$$\langle\varphi|\psi\rangle = (c_1 - d_1 i)(a_1 + b_1 i) + (c_2 - d_2 i)(a_2 + b_2 i)$$

Técnicamente, el bra $\langle\varphi|$ es el transpuesto conjugado del ket $|\varphi\rangle$. En general, para cada ket $|\psi\rangle$ hay exactamente un bra $|\psi\rangle$ y en el caso de qubits, uno es el transpuesto conjugado del otro.

Ejemplo: Considere los siguientes kets de $\mathbb{C}^2$

$$|\psi\rangle = \begin{bmatrix} -3i \\ 2 + i \end{bmatrix}, |\varphi\rangle = \begin{bmatrix} 2 \\ -i \end{bmatrix},$$

Entonces, el bra correspondiente al ket $|\varphi\rangle$ está dado por el vector transpuesto conjugado, es decir, $\langle\varphi| = [2 \;\; i]$. De esta manera, el producto interno $\langle\varphi|\psi\rangle$ equivale al producto matricial correspondiente, es decir:

$$\langle\varphi|\psi\rangle = [2 \;\; i] \begin{bmatrix} -3i \\ 2 + i \end{bmatrix} = (2)(-3i) + (i)(2 + i) = -1 - 4i.$$

Ejemplo: Considere un sistema cuántico cuyo Hamiltoniano $\widehat{H}$ y estado inicial $|\psi_0\rangle$ están dados por

$$\widehat{H} = \omega \begin{bmatrix} 0 & i & 0 \\ -i & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, |\psi_0\rangle = \frac{1}{\sqrt{5}} \begin{bmatrix} 1-i \\ 1-i \\ 1 \end{bmatrix},$$

donde ω tiene dimensiones de energía.

(a) ¿Cuáles son los posibles valores que se pueden obtener si se mide la energía del sistema y con que probabilidades?

(b) Calcular el valor esperado del Hamiltoniano.

Solución:

(a) De acuerdo con el primer postulado de la mecánica cuántica, los posibles valores de la energía que se pueden obtener en una medición al sistema son precisamente los valores propios del operador de la energía o Hamiltoniano. Por lo tanto, daremos respuesta al inciso (a) obteniendo los valores propios, es decir resolviendo la ecuación algebraica:

$$det(H - \lambda I) = 0,$$

$$\begin{vmatrix} -\lambda & \omega i & 0 \\ -\omega i & -\lambda & 0 \\ 0 & 0 & -\omega - \lambda \end{vmatrix} = 0,$$

$$(-\omega - \lambda)(\lambda^2 - \omega^2) = 0,$$

$$(\lambda + \omega)(\lambda^2 - \omega^2) = 0,$$

$$(\lambda + \omega)^2(\lambda - \omega) = 0.$$

Entonces, de acuerdo con esto, los posibles valores de energía que se pueden obtener en una medición al sistema son: $E_1 = \omega$ y $E_{2,3} = -\omega$. Un cálculo sencillo produce los vectores propios correspondientes:

$$\omega \to |\varphi_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \\ 0 \end{bmatrix}, -\omega \to \left\{ |\varphi_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} -i \\ 1 \\ 0 \end{bmatrix}, |\varphi_3\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}.$$

Los vectores propios son ortonormales, $\langle \varphi_i | \varphi_j \rangle = \delta_{ij}$ y por forman una base para $\mathbb{C}^3$ lo que permite escribir el vector $|\psi_0\rangle$ como combinación lineal de ellos, explícitamente queda como:

$$|\psi_0\rangle = \frac{1}{\sqrt{5}}\begin{bmatrix}1-i\\1-i\\1\end{bmatrix} = \sqrt{\frac{2}{5}}|\varphi_1\rangle + \sqrt{\frac{2}{5}}|\varphi_2\rangle + \frac{1}{\sqrt{5}}|\varphi_3\rangle.$$

Entonces, la probabilidad de medir $E_1 = \omega$ se puede calcular como:

$$P(E_1 = \omega) = |\langle\varphi_1|\psi_0\rangle|^2 = \left|\sqrt{\frac{2}{5}}\right|^2 = \frac{2}{5}.$$

Por otro lado, para el valor propio degenerado $E_2 = E_3 = -\omega$ la probabilidad se puede calcular como:

$$P(E_2 = -\omega) = |\langle\varphi_2|\psi_0\rangle|^2 + |\langle\varphi_3|\psi_0\rangle|^2 = \left|\sqrt{\frac{2}{5}}\right|^2 + \left|\frac{1}{\sqrt{5}}\right|^2 = \frac{2}{5} + \frac{1}{5} = \frac{3}{5}$$

(b) En general, para obtener el valor esperado de un observable, se deben sumar (integrar para el caso continuo) todos los posibles valores permisibles a_n, con cada a_n multiplicado por su correspondiente probabilidad P_n. Por lo tanto, para obtener en este ejemplo el valor esperado del Hamiltoniano:

$$\langle\widehat{H}\rangle = P_1E_1 + P_2E_2 = \left(\frac{2}{5}\right)\omega + \left(\frac{3}{5}\right)(-\omega) = -\frac{1}{5}\omega.$$

Otra forma de obtener el valor esperado del Hamiltoniano es a partir d el vector inicial, es decir:

$$\langle\widehat{H}\rangle = \langle\psi_0|\widehat{H}|\psi_0\rangle = \left(\frac{1}{\sqrt{5}}[1-i \quad 1-i \quad 1]\right)\left(\omega\begin{bmatrix}0 & i & 0\\ i & 0 & 0\\ 0 & 0 & -1\end{bmatrix}\right)\left(\frac{1}{\sqrt{5}}\begin{bmatrix}1-i\\1-i\\1\end{bmatrix}\right)$$

$$= \frac{\omega}{5}([1-i \quad 1-i \quad 1])\left(\begin{bmatrix}0 & i & 0\\ i & 0 & 0\\ 0 & 0 & -1\end{bmatrix}\right)\left(\begin{bmatrix}1-i\\1-i\\1\end{bmatrix}\right)$$

$$= \frac{\omega}{5}([1-i \quad 1-i \quad 1])\left(\begin{bmatrix}i+1\\i+1\\-1\end{bmatrix}\right) = -\frac{1}{5}\omega.$$

Bibliografía

1. Nielsen, M. A., & Chuang, I. L. (2011). ***Quantum Computation and Quantum Information: 10th Anniversary Edition***. Cambridge University Press.
2. Lambropoulos, P., & Petrosyan, D. (2007). ***Fundamentals of Quantum Optics and Quantum Information***. Springer.
3. Masahito Hayashi, M., Ishizaka, S., Kawachi, A., Kimura, G., and Ogawa, T. (2015). ***Introduction to Quantum Information Science***. Springer.
4. Wilde, M. M. (2013). ***Quantum Information Theory***. Cambridge University Press.
5. Zettili, N. (2009). ***Quantum Mechanics: Concepts and Applications***. WILEY.