Algunos elementos introductorios acerca de la computación cuántica*

Andrés Sicard Ramírez
asr@eafit.edu.co

Mario Elkin Vélez Ruiz
mvelez@eafit.edu.co

Departamento de Ciencias Básicas
Universidad EAFIT
Medellín, Colombia

10 de junio de 1999

Resumen

Inicialmente se presenta una introducción y una motivación a la computación cuántica. Se ofrecen algunas definiciones y operaciones de la mecánica cuántica relevantes para la computación cuántica. Se muestran algunas compuertas cuánticas, sus matrices unitarias correspondientes y como operar con ellas para construir circuitos cuánticos. Se señalan dos características inherentes a la computación cuántica: la *reversibilidad* y los *estados enredados*. Se presenta el efecto llamado *paralelismo cuántico*. Finalmente, se muestra la transformada cuántica rápida de Fourier.

1. Introducción

Las máquinas de Turing cuánticas y los circuitos cuánticos son un modelo de la computación, tal como lo son las máquinas de Turing, las funciones recursivas y el λ-cálculo, entre otros. Estos modelos se inscriben dentro de un área conocida como computación cuántica y, como su nombre lo indica, hacen uso de las propiedades y efectos considerados por la mecánica cuántica. Esta área fue inicialmente sugerida por Richard Feymman en los años 80, formalizada por David Deutsch (en la forma de máquinas de Turing cuánticas en 1985 [7] y en la forma de circuitos cuánticos en 1989 [6]) y resaltada su potencialidad por Peter Shor en 1994 [14].

El trabajo de Shor señalo el aspecto fundamental en el cual se diferencian la computación clásica y la computación cuántica: *la complejidad algorítmica*. Esta diferencia consiste en que es posible definir algoritmos cuánticos cuya complejidad temporal sea menor que sus análogos clásicos (conocidos hasta el momento). En particular Shor realizó la descripción de un algoritmo cuántico de complejidad temporal de tipo polinomial para la factorización de números enteros. Más interesante—desde el punto de vista de los autores—es la pregunta por la potencia desde la perspectiva de la *computabilidad*, de la computación cuántica; algunos autores afirman que una máquina de Turing y una

*Este artículo fue realizado como parte del proyecto de investigación N_0. 817407 financiado por la Universidad EAFIT.

máquina de Turing cuántica son equipotentes en relación a las funciones que ellas pueden computar (cf. [7, 11]), otros autores por su parte, suponen que bajo ciertas circunstancias la computación cuántica pueda ofrecer características de «super-Turing» computación (cf. [15]), pero ésto hasta el momento es una cuestión abierta.

Este artículo espera proporcionar al lector algunos elementos necesarios para adquirir un breve panorama de la computación cuántica. Una de las principales dificultades con las que se han encontrado los autores, es que los *papers* (con algunas excepciones) que presentan el tema, no presentan el detalle del desarrollo de las operaciones realizadas, lo cual dificulta enormemente el seguimiento para el lector neófito. Por esta razón, los autores han hecho hincapié en este aspecto.

Inicialmente, la sección 2, presenta algunas definiciones y operaciones de la mecánica cuántica relevantes para la computación cuántica. En particular: se define el elemento básico de la computación cuántica denominado qubit; se indica el procedimiento de medida de los qubits, el cual involucra la probabilidad cuántica y se presenta el procedimiento de evolución temporal de los qubits, el cual es realizado por medio de un operador de evolución.

La sección 3 desarrolla los circuitos cuánticos. Inicialmente se muestran algunas compuertas y circuitos clásicos. Se presentan: algunas compuertas cuánticas de uno y dos qubits; el procedimiento para construir la matriz unitaria correspondiente a una compuerta cuántica, con base en su comportamiento entrada-salida; los procedimientos de manipulación de los *kets* y las matrices unitarias. Finalmente se realiza la construcción de un circuito cuántico a partir de algunas compuertas cuánticas definidas anteriormente.

La sección 4 presenta dos características inherentes a la computación cuántica: la *reversibilidad* y los *estados enredados*. La reversibilidad es una condición impuesta por la mecánica cuántica, ésta es ejemplarizada en la compuerta cuántica de Toffoli, para la cual se realiza un desarrollo completo de construcción en un circuito cuántico, esta compuerta además ofrece propiedades de computación universal y se constituye en una compuerta cuántica de uso general. Por otra parte, un estado enredado es una propiedad que no tiene un análogo clásico y, para la cual existe una relación estrecha con la medida cuántica, la cual es presentada.

La sección 5 presenta el efecto llamado *paralelismo cuántico*. Las ventajas ofrecidas por la computación cuántica en lo relacionado a la complejidad temporal son debidas a este efecto. Como ilustración, se presenta y soluciona un problema que hace uso de este paralelismo cuántico, conocido como el problema de Deutsch.

Finalmente, la sección 6 presenta la transformada cuántica rápida de Fourier. Esta transformada es utilizada con frecuencia por los algoritmos cuánticos en la preparación de los estados cuánticos para posibilitar el paralelismo cuántico.

2. Definiciones y operaciones preliminares

2.1. Qubits

La unidad fundamental de información cuántica es el *qubit* o bit cuántico, éste es un elemento del espacio de Hilbert de funciones de onda más simple no trivial de dos dimensiones, el cual es generado por los kets $\{|0\rangle, |1\rangle\}$, elementos de la base, y que convencionalmente pueden elegirse en una representación particular como,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}; \tag{1}$$

estos dos vectores son ortonormales, lo cual significa que bajo el producto escalar $\langle x \,|\, y \rangle$ definido en el espacio, los vectores base se comportan de la siguiente forma:

$$\langle 0 \,|\, 0 \rangle = \langle 1 \,|\, 1 \rangle = 1,$$

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

En las dos últimas ecuaciones los vectores bra $\langle 0 \,|$ y $\langle 1 \,|$, duales de los ket $|\, 0 \rangle$ y $|\, 1 \rangle$ respectivamente, se obtienen como los traspuestos hermíticos de los ket y se representan de la siguiente manera:

$$\langle 0 \,| = \begin{pmatrix} 1 & 0 \end{pmatrix}, \qquad \langle 1 \,| = \begin{pmatrix} 0 & 1 \end{pmatrix}.$$

El 1-qubit normalizado más general que se puede formar en este espacio es la superposición lineal de los dos elementos de la base, es decir:

$$|\, x \rangle = a_0 \,|\, 0 \rangle + a_1 \,|\, 1 \rangle, \quad \text{donde} \quad a_0, a_1 \in \mathbb{C}; \quad |a_0|^2 + |a_1|^2 = 1.$$

Ahora, ¿cuál es el estado de un sistema que consiste no solo de un qubit sino de un conjunto de n qubits cúanticos? La respuesta es que el estado en conjunto se describe como el producto tensorial de los n qubits individuales.

Inicialmente se presenta como ejemplo la situación cuántica para $n = 2$, es decir, dos qubits o un 2-qubit; la dimensión del espacio es $2^2 = 4$. La base de este espacio es:

$$|\, u_i \rangle \otimes |\, v_j \rangle = |\, u_i, v_j \rangle, \tag{2}$$

en esta última expresión $i, j = 0, 1$, entonces:

$$|\, u_0 \rangle = |\, 0 \rangle, \qquad |\, u_1 \rangle = |\, 1 \rangle, \qquad |\, v_0 \rangle = |\, 0 \rangle, \qquad |\, v_1 \rangle = |\, 1 \rangle; \tag{3}$$

las relaciones expresadas por las ecuaciones (2) y (3), permiten definir la base del espacio estado 4-dimensional como:

$$\{|\, 0 \rangle \otimes |\, 0 \rangle, |\, 0 \rangle \otimes |\, 1 \rangle, |\, 1 \rangle \otimes |\, 0 \rangle, |\, 1 \rangle \otimes |\, 1 \rangle\};$$

lo que puede ser escrito en una forma completamente equivalente como:

$$\{|\, 0, 0 \rangle, |\, 0, 1 \rangle, |\, 1, 0 \rangle, |\, 1, 1 \rangle\}.$$

El 2-qubit normalizado más general

$$|\, x_1, x_2 \rangle = |\, x_1 \rangle \otimes |\, x_2 \rangle,$$

que se puede formar en este espacio es la superposición lineal de los cuatro elementos de la base, es decir:

$$|\, x_1, x_2 \rangle = a_0 \,|\, 0, 0 \rangle + a_1 \,|\, 0, 1 \rangle + a_2 \,|\, 1, 0 \rangle + a_3 \,|\, 1, 1 \rangle, \quad \text{donde} \quad a_0, a_1, a_2, a_3 \in \mathbb{C}; \quad \sum_{i=0}^{2^2-1} |a_i|^2 = 1.$$

Una convención utilizada en computación cuántica es:

$$|\, x_1, x_2, \ldots, x_m \rangle \equiv |\, x \rangle, \tag{4}$$

donde $x_1, x_2, \ldots, x_m$ es la representación binaria del entero x, es decir

$$x = x_1 2^{m-1} + x_2 2^{m-2} + \cdots + x_{m-1} 2^1 + x_m 2^0. \tag{5}$$

De acuerdo con las ecuaciones (4) y (5) la base de un espacio formado por n qubits cuya dimensión es 2^n está formada por:

$$\{|\,0\rangle\,, |\,1\rangle\,, |\,2\rangle\,, \ldots, |\,2^n - 1\rangle\};$$

entonces el n-qubit normalizado más general

$$|\,x_1, \ldots, x_n\rangle = |\,x_1\rangle \otimes \cdots \otimes |\,x_n\rangle\,,$$

viene dado por la superposición lineal de los 2^n elementos de la base:

$$|\,x_1, x_2, \ldots, x_n\rangle = \sum_{i=0}^{2^n-1} a_i\,|\,i\rangle\,, \quad \text{donde} \quad a_0, \ldots a_{n-1} \in \mathbb{C}; \quad \sum_{i=0}^{2^n-1} |a_i|^2 = 1.$$

2.2. Medida cuántica

Sea $|\,x\rangle$ un qubit normalizado. Si se realiza una medida sobre la base $\{|\,u_0\rangle\,, |\,u_1\rangle\}$, la probabilidad de encontrar el qubit en el estado $|\,u_i\rangle$, denotada por $P(|\,u_i\rangle)$, está dada por:

$$P(|\,u_i\rangle) = |\,\langle u_i\,|\,x\rangle\,|^2. \tag{6}$$

Ejemplo 2.1. *La medición de un qubit* $|\,x\rangle = a_0\,|\,0\rangle + a_1\,|\,1\rangle$ *sobre la base* $\{|\,0\rangle\,, |\,1\rangle\}$*, genera las siguientes probabilidades:*

$$\begin{aligned} P(|\,0\rangle) &= |\,\langle 0\,|\,x\rangle\,|^2 \\ &= |\,\langle 0\,|\,(a_0\,|\,0\rangle + a_1\,|\,1\rangle)|^2 \\ &= |a_0\,\langle 0\,|\,0\rangle + a_1\,\langle 0\,|\,1\rangle\,|^2 \\ &= |a_0|^2, \end{aligned} \qquad \begin{aligned} P(|\,1\rangle) &= |\,\langle 1\,|\,x\rangle\,|^2 \\ &= |\,\langle 1\,|\,(a_0\,|\,0\rangle + a_1\,|\,1\rangle)|^2 \\ &= |a_0\,\langle 1\,|\,0\rangle + a_1\,\langle 1\,|\,1\rangle\,|^2 \\ &= |a_1|^2. \end{aligned}$$

Ejemplo 2.2. *La medición de un qubit* $|\,x\rangle = a_0\,|\,0\rangle + a_1\,|\,1\rangle$ *sobre la base* $\{|\,0\rangle + |\,1\rangle\,, |\,0\rangle - |\,1\rangle\}$*, genera las siguientes probabilidades:*

$$\begin{aligned} P(|\,0\rangle + |\,1\rangle) &= |(\langle 0\,| + \langle 1\,|)\,|\,x\rangle\,|^2 \\ &= |(\langle 0\,| + \langle 1\,|)(a_0\,|\,0\rangle + a_1\,|\,1\rangle)|^2 \\ &= |a_0\,\langle 0\,|\,0\rangle + a_1\,\langle 0\,|\,1\rangle + a_0\,\langle 1\,|\,0\rangle + a_1\,\langle 1\,|\,1\rangle\,|^2 \\ &= |a_0 + a_1|^2. \end{aligned} \tag{7}$$

$$\begin{aligned} P(|\,0\rangle - |\,1\rangle) &= |(\langle 0\,| - \langle 1\,|)\,|\,x\rangle\,|^2 \\ &= |(\langle 0\,| - \langle 1\,|)(a_0\,|\,0\rangle + a_1\,|\,1\rangle)|^2 \\ &= |a_0\,\langle 0\,|\,0\rangle + a_1\,\langle 0\,|\,1\rangle - a_0\,\langle 1\,|\,0\rangle - a_1\,\langle 1\,|\,1\rangle\,|^2 \\ &= |a_0 - a_1|^2. \end{aligned} \tag{8}$$

La medida de los qubits de un 2-qubit $|\,x_1, x_2\rangle = a_0\,|\,0,0\rangle + a_1\,|\,0,1\rangle + a_2\,|\,1,0\rangle + a_3\,|\,1,1\rangle$ sobre la base $\{|\,0\rangle\,, |\,1\rangle\}$ genera las siguientes probabilidades: la probabilidad de encontrar el primer qubit en el estado $|\,0\rangle$ denotada por $P_1(|\,0\rangle)$, la probabilidad de encontrar el primer qubit en el estado $|\,1\rangle$ denotada por $P_1(|\,1\rangle)$, la probabilidad de encontrar el segundo qubit en el estado $|\,0\rangle$ denotada por $P_2(|\,0\rangle)$ y la probabilidad de encontrar el segundo qubit en el estado $|\,1\rangle$ denotada por $P_2(|\,1\rangle)$. Estas probabilidades están dadas por:

$$\begin{aligned} P_1(|\,0\rangle) &= |a_0|^2 + |a_1|^2, \\ P_1(|\,1\rangle) &= |a_2|^2 + |a_3|^2, \\ P_2(|\,0\rangle) &= |a_0|^2 + |a_2|^2, \\ P_2(|\,1\rangle) &= |a_1|^2 + |a_3|^2. \end{aligned} \tag{9}$$

Sí, una vez realizada la medida sobre el primer qubit del 2-qubit $|\,x_1, x_2\rangle = a_0\,|\,0,0\rangle + a_1\,|\,0,1\rangle + a_2\,|\,1,0\rangle + a_3\,|\,1,1\rangle$, se obtiene que éste está en el estado $|\,0\rangle$, el 2-qubit evoluciona a un nuevo estado normalizado dado por:

$$|\,x', y'\rangle = \frac{a_0\,|\,0,0\rangle + a_1\,|\,0,1\rangle}{\sqrt{|a_0|^2 + |a_1|^2}}; \tag{10}$$

y se obtiene que éste está en el estado $|\,1\rangle$, el 2-qubit evoluciona a un nuevo estado normalizado dado por:

$$|\,x', y'\rangle = \frac{a_2\,|\,1,0\rangle + a_3\,|\,1,1\rangle}{\sqrt{|a_2|^2 + |a_3|^2}}. \tag{11}$$

Expresiones similares a las anteriores se obtienen para los resultados de la medida del segundo qubit del 2-qubit.

2.3. Evolución cuántica

La evolución o dinámica de un n-qubit es determinada por un operador unitario U sobre el espacio de Hilbert, este operador es denominado *operador de evolución*. Un operador es unitario si su adjunto es igual a su inverso, y puede expresarse como:

$$U^\dagger U = \mathbb{I}.$$

Sea $|\,\psi(t)\rangle = |\,x_1, \ldots, x_n\rangle$ un n-qubit, la evolución con base en el operador U de un paso de computación, está dada por:

$$U\,|\,\psi(0)\rangle \to |\,\psi(1)\rangle\,,$$

y en general, la evolución de m pasos de computación está dada por (cf. [7]):

$$U^m\,|\,\psi(0)\rangle \to |\,\psi(m)\rangle\,.$$

En el contexto de la computación cuántica un operador de evolución que opera sobre un n-qubit, corresponde a una matriz unitaria de dimensión 2^n. La próxima sección indica la construcción de estas matrices unitarias y su relación con las compuertas cuánticas.

x	y	$\neg x$	$x \wedge y$	$x \vee y$
0	0	1	0	0
0	1	1	0	1
1	0	0	0	1
1	1	0	1	1

Tabla 1: Operaciones lógicas *not*, *and* y *or*.

x	y	$x \uparrow y$	$x \downarrow y$	$x \oplus y$
0	0	0	1	0
0	1	0	0	1
1	0	0	0	1
1	1	1	0	0

Tabla 2: Operaciones lógicas *nand*, *nor* y *xor*.

3. Circuitos cuánticos

En la introducción se indicó que la computación cuántica ofrece dos modelos de computación: las máquinas de Turing cuánticas (MTQ) y los circuitos cuánticos. Para la presentación de un modelo de computación cuántica, se seleccionó el modelo de los circuitos cuánticos por considerarlos más cercanos a sus análogos, los circuitos clásicos. El modelo de las MTQ no será presentado, el lector interesado en éste, puede consultar [4, 1, 7].

3.1. Compuertas y circuitos lógicos

Las operaciones lógicas presentadas en la tabla 1, pueden ser representadas por compuertas lógicas, tal como lo indica la figura 1.

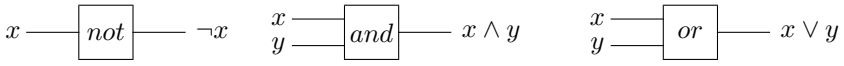


Figura 1: Compuerta lógicas *not*, *and* y *or*.

Con estas operaciones lógicas es posible construir otras operaciones lógicas, tales como el *nand* ($\uparrow$), *xor* ($\oplus$) y el *nor* ($\downarrow$) indicadas en la tabla 2. Estas nuevas operaciones lógicas pueden ser representadas por circuitos lógicos tal como lo indica la figura 2, en donde el símbolo '$\equiv$' significa que los circuitos son equivalentes. Se puede además, expresar las compuertas *nor* y *xor* en términos de las compuertas *not*, *and* y *or*.

Es posible también, combinando las diferentes compuertas lógicas obtener circuitos lógicos de mayor complejidad. Por convención en estos circuitos lógicos (también se aplicará a los circuitos cuánticos), el tiempo procede de izquierda a derecha, es decir, el orden de operación de las compuertas es de izquierda a derecha (cf. [2]).

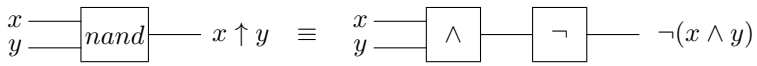


Figura 2: Compuerta lógica *nand* en términos de las compuertas lógicas *and* y *not*.

3.2. Compuertas cuánticas

A diferencia de las compuertas lógicas que pueden operar de n-bits en m-bits, las compuertas cuánticas deben operar de n-qubits en n-qubits. Esta es una condición necesaria pero no suficiente para satisfacer una propiedad (la reversivilidad) de las compuertas cuánticas que será presentada en una próxima sección. Cada compuerta cuántica de n-qubits puede ser representada por una matriz unitaria de dimensión 2^n, en donde la transformación realizada por la compuerta cuántica es realizada por el operador matriz asociado a ella.

Con base en la descripción de la tranformación que realiza una compuerta cuántica sobre los elementos de la base del espacio, la matriz unitaria asociada a ella se obtiene a partir del siguiente procedimiento: Las filas de la matriz corresponden a los vectores base de entrada y las columnas de la matriz corresponden a los vectores base de salida; la (j, i) posición de la matriz corresponde, cuando el i-ésimo vector base es la entrada a la compuerta, al coeficiente del j-ésimo vector base en la salida de la compuerta.

3.2.1. Compuertas cuánticas de 1-qubit

Las compuertas cuánticas que operan sobre un qubit (un qubit de entrada y un qubit de salida) tienen asociadas matrices 2×2. La convención utilizada en los cuatro ejemplos siguentes para representar vectorialmente el ket $|\,0\rangle$ y el ket $|\,1\rangle$ es la misma que la representada por la ecuación (1), es decir:

$$|\,0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |\,1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Inicialmente se presenta la compuerta cuántica *identidad*. Aunque su comportamiento—como su nombre lo indica—no modifica el qubit sobre el que actua, se busca con este ejemplo ilustrar el procedimiento de construcción de la matriz unitaria asociada a una compuerta cuántica.

Ejemplo 3.1 (Compuerta identidad)**.** *El comportamiento de la compuerta* identidad *está dado por*

$$U_{id}\,|\,x\rangle \to |\,x\rangle\,.$$

La transformación de los qubits que realiza la compuerta y su representación gráfica es:

$$\begin{aligned} U_{id}\,|\,0\rangle &\to |\,0\rangle\,, \\ U_{id}\,|\,1\rangle &\to |\,1\rangle\,, \end{aligned}$$

Entonces, la matriz unitaria correspondiente a la compuerta cuántica identidad, está dada por:

$$\begin{array}{c|cc} & |\,0\rangle & |\,1\rangle \\ |\,0\rangle & 1 & 0 \\ |\,1\rangle & 0 & 1 \end{array}, \quad \textit{la cual es representada por:} \quad U_{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{12}$$

El comportamiento de la compuerta cuántica identidad en términos de la matriz (12) es descrito por:

$$U_{id}\,|\,0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\,0\rangle\,,$$

$$U_{id}\,|\,1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\,1\rangle\,.$$

El siguiente ejemplo ilustra el comportamiento de una compuerta cuántica conocida como la compuerta de *Hadamard*. Esta compuerta transforma un qubit en una superposición de los elementos de la base $\{|\,0\rangle\,, |\,1\rangle\}$. Aunque no será ilustrado, es posible generalizar la compuerta de *Hadamard* para que opere sobre un n-qubit con un comportamiento similar al caso de 1-qubit, es decir, la compuerta de *Hadamard* sobre un n-qubit transforma éste en una superposición de los elementos de la base $\{|\,0\rangle\,, \ldots, |\,2^n - 1\rangle\}$.

Ejemplo 3.2 (Compuerta de Hadamard)**.** *La transformación de los qubits que realiza la compuerta de* Hadamard U_H *está dada por:*

$$U_H\,|\,0\rangle \to \frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle),$$
$$U_H\,|\,1\rangle \to \frac{1}{\sqrt{2}}(|\,0\rangle - |\,1\rangle).$$

La matriz para la compuerta de Hadamard está dada por:

$$\begin{array}{c|cc} & |\,0\rangle & |\,1\rangle \\ |\,0\rangle & \frac{1}{\sqrt{2}} & +\frac{1}{\sqrt{2}} \\ |\,1\rangle & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array}, \quad \textit{y se representa por:} \quad U_H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{13}$$

El comportamiento de la compuerta de Hadamard en términos de la matriz (13) es descrito por:

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

$$U_H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|\,0\rangle - |\,1\rangle).$$

El ejemplo siguiente—a diferencia de los ejemplos anteriores—ilustra como obtener la transformación que realiza una compuerta cuántica sobre los elementos de la base, a partir de la matriz unitaria asociada a ésta, además ilustra el uso de compuertas cuńticas parametrizadas.

Ejemplo 3.3 (Compuerta cuántica parametrizada)**.** *Una matriz unitaria parametrizada determina una compuerta cuántica parametrizda. A manera de ejemplo, sea*

$$U(\theta) = \begin{pmatrix} \cos(\theta/2) & \operatorname{sen}(\theta/2) \\ -\operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix}. \tag{14}$$

La matriz $U(\theta)$ tiene el siguiente comportamiento sobre los elementos de la base $\{|\,0\rangle\,, |\,1\rangle\}$:

$$U(\theta)\,|\,0\rangle = \begin{pmatrix} \cos(\theta/2) & \operatorname{sen}(\theta/2) \\ -\operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ -\operatorname{sen}(\theta/2) \end{pmatrix} = \cos(\theta/2)\,|\,0\rangle - \operatorname{sen}(\theta/2)\,|\,1\rangle\,. \quad (15)$$

$$U(\theta)\,|\,1\rangle = \begin{pmatrix} \cos(\theta/2) & \operatorname{sen}(\theta/2) \\ -\operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\operatorname{sen}(\theta/2) \\ \cos(\theta/2) \end{pmatrix} = \operatorname{sen}(\theta/2)\,|\,0\rangle + \cos(\theta/2)\,|\,1\rangle\,. \quad (16)$$

Con base en las ecuaciones (15) y (16), la transformación de la compuerta cuántica $U(\theta)$ está dada por:

$$U(\theta)\,|\,0\rangle \to \cos(\theta/2)\,|\,0\rangle - \operatorname{sen}(\theta/2)\,|\,1\rangle\,,$$
$$U(\theta)\,|\,1\rangle \to \operatorname{sen}(\theta/2)\,|\,0\rangle + \cos(\theta/2)\,|\,1\rangle\,.$$

Para la construcción de un circuito cuántico que será presentado en una sección próxima, es necesaria la siguiente transformación realizada por la compuerta $U(\theta)$:

$$U(\theta)(\cos(\theta/2)\,|\,0\rangle - \operatorname{sen}(\theta/2)\,|\,1\rangle) = \begin{pmatrix} \cos(\theta/2) & \operatorname{sen}(\theta/2) \\ -\operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} \cos(\theta/2) \\ -\operatorname{sen}(\theta/2) \end{pmatrix} = \begin{pmatrix} \cos(\theta) \\ -\operatorname{sen}(\theta) \end{pmatrix}$$

$$= \cos(\theta)\,|\,0\rangle - \operatorname{sen}(\theta)\,|\,1\rangle\,. \quad (17)$$

La unitariedad de la matriz M asociada a una compuerta cuántica M, permite construir una nueva compuerta cuántica $M^\dagger$ con base en la matriz hermítica conjugada $M^\dagger$ de M. La posibilidad de obtener una nueva compuerta $M^\dagger$ sustenta la propiedad de reversibilidad de las compuertas cuánticas, tal como será expuesto posteriormente. Se ilustra entonces, una compuerta $M^\dagger$.

Ejemplo 3.4 (Compuerta $M^\dagger$)**.** *La matriz hermítica conjugada de la matriz $U(\theta)$ representada por la ecuación (14) y las transformaciones que realiza la compuerta $U^\dagger(\theta)$ están dadas por:*

$$U^\dagger(\theta)\,|\,0\rangle \to \cos(\theta/2)\,|\,0\rangle + \operatorname{sen}(\theta/2)\,|\,1\rangle\,,$$
$$U^\dagger(\theta)\,|\,1\rangle \to -\operatorname{sen}(\theta/2)\,|\,0\rangle + \cos(\theta/2)\,|\,1\rangle\,,$$

$$U^\dagger(\theta) = \begin{pmatrix} \cos(\theta/2) & -\operatorname{sen}(\theta/2) \\ \operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix}.$$

Para la construcción de un circuito cuántico que será presentado en una sección próxima, son necesarias las siguientes transformaciones realizadas por la compuerta $U^\dagger(\theta)$:

$$\begin{aligned} U^\dagger(\theta)\,(\cos(\theta)\,|\,0\rangle - \operatorname{sen}(\theta)\,|\,1\rangle) &= \begin{pmatrix} \cos(\theta/2) & -\operatorname{sen}(\theta/2) \\ \operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} \cos(\theta) \\ -\operatorname{sen}(\theta) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta/2) \\ -\operatorname{sen}(\theta/2) \end{pmatrix}. \end{aligned} \quad (18)$$

$$U^{\dagger}(\theta)\left(\cos(\theta/2)\,|\,0\rangle - \operatorname{sen}(\theta/2)\,|\,1\rangle\right) = \begin{pmatrix} \cos(\theta/2) & -\operatorname{sen}(\theta/2) \\ \operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} \cos(\theta/2) \\ -\operatorname{sen}(\theta/2) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\,0\rangle\,. \tag{19}$$

3.2.2. Matriz unitaria 2×2 general

Cada matriz unitaria 2×2 es de la forma representada por la ecuación (20) y esta a su vez puede ser factorizada en cuatro matrices representadas por la ecuación (21).

$$U(\alpha,\beta,\delta,\theta) = \begin{pmatrix} e^{i\left(\delta+\frac{\alpha}{2}+\frac{\beta}{2}\right)}\cos(\theta/2) & e^{i\left(\delta+\frac{\alpha}{2}-\frac{\beta}{2}\right)}\operatorname{sen}(\theta/2) \\ -e^{i\left(\delta-\frac{\alpha}{2}+\frac{\beta}{2}\right)}\operatorname{sen}(\theta/2) & e^{i\left(\delta-\frac{\alpha}{2}-\frac{\beta}{2}\right)}\cos(\theta/2) \end{pmatrix}, \tag{20}$$

$$= \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix} \cdot \begin{pmatrix} e^{i\frac{\alpha}{2}} & 0 \\ 0 & e^{-i\frac{\alpha}{2}} \end{pmatrix} \cdot \begin{pmatrix} \cos(\theta/2) & \operatorname{sen}(\theta/2) \\ -\operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix} \cdot \begin{pmatrix} e^{i\frac{\beta}{2}} & 0 \\ 0 & e^{-i\frac{\beta}{2}} \end{pmatrix}. \tag{21}$$

Con base en la ecuación (21) se define la matriz $R_y(\theta)$ por (a la cual se hará referencia en una sección posterior):

$$R_y(\theta) = \begin{pmatrix} \cos(\theta/2) & \operatorname{sen}(\theta/2) \\ -\operatorname{sen}(\theta/2) & \cos(\theta/2) \end{pmatrix}. \tag{22}$$

3.2.3. Compuertas cuánticas de 2-qubit

Se presentan ahora algunas compuertas que operan sobre dos qubits (dos qubits de entrada y dos qubits de salida) y sus matrices 4×4 correspondientes. La convención utilizada en los siguientes ejemplos, para representar vectorialmente los kets $|\,0,0\rangle$, $|\,0,1\rangle$, $|\,1,0\rangle$ y $|\,1,1\rangle$ es:

$$|\,0,0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad |\,0,1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \qquad |\,1,0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \qquad |\,1,1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Ejemplo 3.5. *Este ejemplo presenta una compuerta que realiza el intercambio de dos qubits, es decir la compuerta realiza la transformación*

$$U_{ic}\,|\,x,y\rangle \to |\,y,x\rangle\,.$$

La transformación de los dos qubits que realiza la compuerta y su representación gráfica estan dadas por:

$$\begin{aligned} U_{ic}\,|\,0,0\rangle &\to |\,0,0\rangle \\ U_{ic}\,|\,0,1\rangle &\to |\,1,0\rangle \\ U_{ic}\,|\,1,0\rangle &\to |\,0,1\rangle \\ U_{ic}\,|\,1,1\rangle &\to |\,1,1\rangle \end{aligned}$$

La matriz unitaria construida con base en el procedimiento descrito en el ejemplo 3.1 está dada por:

$$\begin{array}{c|cccc} & |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ \hline |00\rangle & 1 & 0 & 0 & 0 \\ |01\rangle & 0 & 0 & 1 & 0 \\ |10\rangle & 0 & 1 & 0 & 0 \\ |11\rangle & 0 & 0 & 0 & 1 \end{array},$$

representada por

$$U_{ic} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{23}$$

El comportamiento de la compuerta intercambio en términos de la matriz (23) es descrito por:

$$U_{ic}\,|\,0,0\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |\,0,0\rangle\,,$$

$$U_{ic}\,|\,0,1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |\,1,0\rangle\,,$$

$$U_{ic}\,|\,1,0\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |\,0,1\rangle\,,$$

$$U_{ic}\,|\,1,1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |\,1,1\rangle\,.$$

Ejemplo 3.6. *Para la compuerta que tiene el comportamiento $U_{xor}\,|\,x,y\rangle \to |\,x, x\oplus y\rangle$ corresponde la matriz:*

$$\begin{aligned} U_{xor}|0,0\rangle &\to |\,0,0\oplus 0\rangle = |0,0\rangle \\ U_{xor}|0,1\rangle &\to |\,0,0\oplus 1\rangle = |0,1\rangle \\ U_{xor}|1,0\rangle &\to |\,1,1\oplus 0\rangle = |1,1\rangle \\ U_{xor}|1,1\rangle &\to |\,1,1\oplus 1\rangle = |1,0\rangle \end{aligned} \qquad U_{xor} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{24}$$

El comportamiento de la compuerta U_{xor} en términos de la matriz (24) es descrito por

$$U_{xor}|0,0\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |0,0\rangle,$$

$$U_{xor}|0,1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |0,1\rangle,$$

$$U_{xor}|1,0\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |1,1\rangle,$$

$$U_{xor}|1,1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |1,0\rangle.$$

Esta compuerta corresponde a un xor *cuántico, también llamado* controlled-not. *Este* xor *cambia el segundo qubit si el primer qubit es* 1 *y deja sin cambiar el segundo qubit si el primero es* 0. *Esta compuerta es representada por el circuito de la figura 3.*

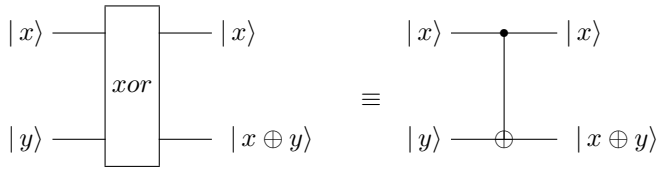


Figura 3: Compuerta *xor* cuántica.

La compuerta xor *también puede actuar sobre un qubit formado por cualquier combinación lineal y su comportamiento es similar al descrito anteriormente, el cambio o no del segundo qubit es controlado por el primer qubit y es desarrollado de la siguiente forma:*

$$\begin{aligned} U_{xor}\left(|\,0\rangle \otimes (a\,|\,0\rangle + b\,|\,1\rangle)\right) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} a \\ b \end{pmatrix} \right) \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} a \\ b \\ 0 \\ 0 \end{pmatrix} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} a \\ b \end{pmatrix} \right) \\ &= |\,0\rangle \otimes (a\,|\,0\rangle + b\,|\,1\rangle)\,, \end{aligned} \tag{25}$$

es decir, si el primer qubit es cero el segundo qubit no cambia; pero si el primer qubit es uno, se obtiene:

$$\begin{aligned} U_{xor}\left(|\,1\rangle \otimes (a\,|\,0\rangle + b\,|\,1\rangle)\right) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} a \\ b \end{pmatrix} \right) \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ a \\ b \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ b \\ a \end{pmatrix} = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} b \\ a \end{pmatrix} \right) \\ &= |\,1\rangle \otimes (b\,|\,0\rangle + a\,|\,1\rangle)\,, \end{aligned} \tag{26}$$

es decir, si el primer qubit es uno el segundo qubit intercambia sus coeficientes.

3.2.4. Construcción de circuitos cuánticos a partir de compuertas cuánticas

Se presenta la contrucción de un circuito cuántico que intercambia dos qubits por medio del uso de tres *xor* cuánticos, además se construye la matriz 4×4 correspondiente a dicho circuito. El circuito de intercambio de dos qubits, realiza la transformación $U_{ic}\,|\,x, y\rangle \to |\,y, x\rangle$ presentada en el ejemplo 3.5. Este circuito es representado por la figura 4 en la cual se utilizan tres *xor* cuánticos.

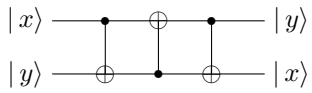


Figura 4: Circuito cuántico que intercambia dos qubits.

Siguiendo el circuito de la figura 4 de izquierda a derecha se obtiene la transformación que intercambia dos qubits:

$$\begin{aligned} |\,x, y\rangle &\to |\,x, x \oplus y\rangle && \text{(resultado primer } xor\text{)} \\ &\to |\,(x \oplus y) \oplus x, x \oplus y\rangle \\ &= |\,y, x \oplus y\rangle && \text{(resultado segundo } xor\text{)} \\ &\to |\,y, y \oplus (x \oplus y)\rangle \\ &= |\,y, x\rangle && \text{(resultado tercer } xor\text{).} \end{aligned}$$

Para construir la matriz unitaria 4×4 que representa el intercambio de dos qubits, se procede de la siguiente manera: El primer subcircuito del circuito de la figura 4 representado por la figura 5

realiza la transformación $|\,x,y\rangle \to |\,x,x\oplus y\rangle$ y corresponde a la compuerta *xor* cuántica presentada en el ejemplo 3.6 cuya matriz unitaria es:

$$m_1 = U_{xor} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

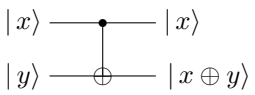


Figura 5: Primer subcircuito para el intercambio de dos qubits.

El segundo subcircuito del circuito de la figura 4 es representado por la figura 6 y realiza la transformación $|\,x,y\rangle \to |\,y\oplus x,y\rangle$. La transformación que realiza el subcircuito y la matriz unitaria asociada ella están dadas por:

$$\begin{aligned} &|\,0,0\rangle \to |\,0,0\rangle\,, \\ &|\,0,1\rangle \to |\,1,1\rangle\,, \\ &|\,1,0\rangle \to |\,1,0\rangle\,, \\ &|\,1,1\rangle \to |\,0,1\rangle\,, \end{aligned} \qquad m_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

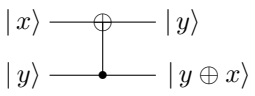


Figura 6: Segundo subcircuito para el intercambio de dos qubits.

El tercer subcircuito es similar al primer subcircuito por la tanto la matriz m_3 es igual a la matriz m_1.

La matriz U_{ic} correspondiente al circuito de intercambio de dos qubits está dada por:

$$\begin{aligned} U_{ic} &= (m_1 \times m_2) \times m_3 \\ &= \left[\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \right] \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

La verificación de que U_{ic} es la matriz unitaria correspondiente a la tranformación que realiza el intercambio de dos qubits fue presentada en el ejemplo 3.5 en donde se multiplica cada par de qubits $|\,0,0\rangle$, $|\,0,1\rangle$, $|\,1,0\rangle$ y $|\,1,1\rangle$ (en su representación vectorial) por la matriz U_{ic} y se obtiene los qubits $|\,0,0\rangle$, $|\,1,0\rangle$, $|\,0,1\rangle$ y $|\,1,1\rangle$ respectivamente (en su representación vectorial).

4. Reversibilidad y estados enredados

4.1. Reversibilidad

Se puede clasificar los procesos de cómputo, además de que satisfacen las leyes fundamentales de la física, en aquellos para los que lo fundamental es una operación irreversible (disipativa), y del otro lado aquellos para los cuales eso no es fundamental. Las compuertas lógicas-cuánticas, materializadas en dispositivos de algún tipo, son las encargadas de realizar las operaciones, los cómputos. Una compuerta lógica cuya información de salida sea menor que la de entrada es irreversible (disipativa), pues tuvo que desechar información, lo cual se traduce en última instancia en una perdida de energía de algún tipo. Por el contrario, una compuerta lógica cuya información de salida sea igual a la información de entrada sera reversible (no disipativa), la información permanece invariante, lo cual lleva consigo una energía manifiestamente constante. Una compuerta de este tipo, más aún, un sistema de compuertas de este estilo, conectadas de alguna forma, capaz de realizar una operación lógica, es susceptible de que en ella se invierta el proceso de cómputo y al final se recupere las condiciones iniciales sin perdida alguna de energía. Una característica importante al estudiar las compuertas reversibles, es que Bennett en 1973 (cf. [3]) demostró que las compuertas irreversibles no son esenciales en los procesos de cómputo. Del mismo modo Fredkin con Toffoli y otros miembros del MIT, han demostrado que en particular la fricción no es esencial en los procesos de computo, según Fredkin, puede construirse un ordenador basado exclusivamente en un tipo de compuertas reversibles que llevan su nombre. Textualmente en [3], pág. 39, se concluye: «*Así, pues, según la termodinámica clásica, para realizar un cómputo no haría falta consumir, como mínimo, una cuota prefijada de energía.*».

Desde el punto de vista de las compuertas cuánticas, su reversibilidad es una consecuencia de la unitariedad de los operadores que las implementan. Sea U_f la matriz unitaria asociada a una compuerta f entonces para cualesquiera estados $|\,x\rangle\,, |\,y\rangle$ se obtiene:

$$\begin{aligned} U_f\,|\,x\rangle = |\,y\rangle &\Longrightarrow U_f^\dagger U_f\,|\,x\rangle = U_f^\dagger\,|\,y\rangle\,, \\ &\Longrightarrow |\,x\rangle = U_f^\dagger\,|\,y\rangle\,, \end{aligned}$$

es decir, desde la infomarción de salida (ket $|\,y\rangle$) es posible obtener la información de entrada (ket $|\,x\rangle$).

A partir de una función f de n bits en m bits se puede construir una función reversible $f_{\text{reversible}}$ de $m+n$ bits en $m+n$ bits dada por (cf. [1]):

$$f : x \to f(x) \quad \dashrightarrow \quad f_{\text{reversible}} : (x, y) \to (x, y \oplus f(x)); \tag{27}$$

entonces, una función f puede ser implementada por un circuito cuántico U_f, cumpliendo las condiciones de reversibilidad exigidas a éste, si U_f realiza la transformación:

$$U_f\,|\,x, y\rangle \to |\,x, y \oplus\ f(x)\rangle\,. \tag{28}$$

x	y	z	$z \oplus (x \wedge y)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Tabla 3: Comportamiento compuerta Toffoli.

Se presenta a continuación una compuerta lógica reversible conocida como compuerta de Toffoli y su implementación en un circuito cuántico. La importancia de esta compuerta radica en sus capacidades de computación universal, presentadas a continuación.

Las compuertas lógicas *and* y *not* son llamadas compuertas lógicas universales, porque cualquier función $f : \{0,1\}^n \to \{0,1\}^m$ puede ser implementada en un circuito lógico que utilice sólo estas compuertas. Por otro lado, no es posible obtener un conjunto de compuertas universales para funciones reversibles de la forma $f : \{0,1\}^n \to \{0,1\}^n$ con compuertas reversibles de 1-bit ni con compuertas reversibles de 2-bits; un conjunto de compuertas universales reversibles está formado por una compuerta de 3-bits llamada la compuerta de Toffoli e ilustrada en la figura 7 (cf. [12], capítulo 6).

Figura 7: Compuerta universal reversible: Compuerta de Toffoli.

Esta compuerta puede ser vista como un ejemplo de la aplicación de la ecuación (27) a la función *and* entre dos bits, es decir:

$$and : (x,y) \to x \wedge y \quad \dashrightarrow \quad toffoli : (x,y,z) \to (x,y,z \oplus (x \wedge y)).$$

El comportamiento de la compuerta de Toffoli es descrito por la tabla 3 y su caracter de compuerta universal es resumido por la ecuación (29) en donde se indica que dicha compuerta puede actuar como una compuerta *and* o una compuerta *not* o una compuerta *xor* o una compuerta *identidad*.

$$z \oplus (x \wedge y) = \begin{cases} x \wedge y & \text{sii } z = 0 \text{ (compuerta } and), \\ x \oplus z & \text{sii } y = 1 \text{ (compuerta } xor), \\ \neg z & \text{sii } x = y = 1 \text{ (compuerta } not), \\ x & \text{sii } x = 0; y = 1 \text{ (compuerta } identidad). \end{cases} \tag{29}$$

La compuerta de Toffoli puede ser vista como un circuito cuántico representado por la figura 8. A este circuito le corresponde la matriz unitaria dada por la ecuacion (30).

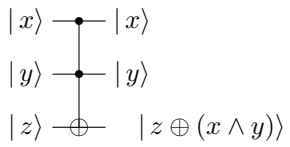
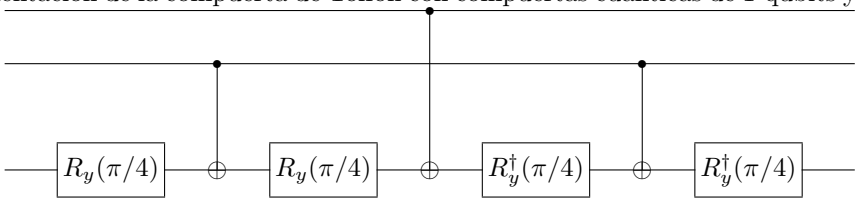


Figura 8: Circuito cuántico de Toffoli.

$$U_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{30}$$

Aunque la compuerta cuántica de Toffoli es un compuerta de 3-qubits, ésta puede ser implementada por un circuito cuántico que sólo utiliza compuertas cuánticas de 1-qubit y de 2-qubits. En particular, la compuerta cuántica de Toffoli puede ser descompuesta en un circuito cuántico formado con seis compuertas *xor* y ocho compuertas de 1-qubit ; pero sí, se es permitido un cambio de fase, la compuerta puede ser construída tal como lo indica la figura 9 (cf. [8, 2]), en la cual se han identificado cada una de las compuertas $R_y(\pi/4)$ con los nombres de compuerta$_1$ y compuerta$_2$, cada una de las compuertas $R_y^\dagger(\pi/4)$ con los nombres compuerta$_3$ y *compuerta*$_4$ y cada una de las compuertas *xor* con los nombres xor_1, xor_2 y xor_3.

La implementación de la compuerta de Toffoli con compuertas cuánticas de 1-qubits y 2-qubits, uti-



compuerta$_1$ xor_1 compuerta$_2$ xor_2 compuerta$_3$ xor_3 *compuerta*$_4$

Figura 9: Implementación de la compuerta de Toffoli con compuertas de 1-qubit y 2-qubits.

liza compuertas $R_y(\pi/4)$ cuya matriz unitaria fue descrita por la ecuación (22), compuertas $R_y^\dagger(\pi/4)$ cuya matriz unitaria es la conjugada transpuesta de la matriz anterior y compuertas *xor* cuánticas cuya matriz unitaria corresponde a la ecuación (24). La construcción de la matriz unitaria se realizará para tres ($|0,0,0\rangle, |1,0,0\rangle, |1,1,1\rangle$) de los ocho posibles casos.

1. Caso $|0,0,0\rangle$

Paso 0:
Los valores iniciales de los kets $|x\rangle, |y\rangle$ y $|z\rangle$ están dados por $|0\rangle, |0\rangle$ y $|0\rangle$ respectivamente, con lo cual se forma el estado cuántico inicial:

$$|0\rangle \otimes |0\rangle \otimes |0\rangle = |0,0,0\rangle . \tag{31}$$

Paso 1:
La compuerta$_1$ actua sobre el *ket* $|z\rangle = |0\rangle$ y el nuevo estado cuántico es (ejemplo 3.3, ecuación (15)):

$$|0\rangle \times |0\rangle \otimes (\cos(\pi/8)|0\rangle - \text{sen}(\pi/8)|1\rangle = \cos(\pi/8)|0,0,0\rangle - \text{sen}(\pi/8)|0,0,1\rangle . \tag{32}$$

Paso 2:
La compuerta xor_1 efectua un *xor* entre el *ket* $|y\rangle = |0\rangle$ y el *ket* $|z\rangle = \cos(\pi/8)|0\rangle - \text{sen}(\pi/8)|1\rangle$ y el nuevo estado cuántico es (ejemplo 3.6, ecuación (25)):

$$|0\rangle \times |0\rangle \otimes (\cos(\pi/8)|0 \oplus 0\rangle - \text{sen}(\pi/8)|0 \oplus 1\rangle) = \cos(\pi/8)|0,0,0\rangle - \text{sen}(\pi/8)|0,0,1\rangle . \tag{33}$$

Paso 3:
La compuerta$_2$ actua sobre el *ket* $|z\rangle = \cos(\pi/8)|0\rangle - \text{sen}(\pi/8)|1\rangle$ y el nuevo estado cuántico es (ejemplo 3.3, ecuación (17)):

$$|0\rangle \times |0\rangle \otimes (\cos(\pi/4)|0\rangle - \text{sen}(\pi/4)|1\rangle) = \cos(\pi/4)|0,0,0\rangle - \text{sen}(\pi/4)|0,0,1\rangle . \tag{34}$$

Paso 4:
La compuerta xor_2 efectua un *xor* entre el *ket* $|x\rangle = |0\rangle$ y el *ket* $|z\rangle = \cos(\pi/4)|0\rangle - \text{sen}(\pi/4)|1\rangle$ y el nuevo estado cuántico es (ejemplo 3.6, ecuación (25)):

$$|0\rangle \times |0\rangle \otimes (\cos(\pi/4)|0 \oplus 0\rangle - \text{sen}(\pi/4)|0 \oplus 1\rangle) = \cos(\pi/4)|0,0,0\rangle - \text{sen}(\pi/4)|0,0,1\rangle . \tag{35}$$

Paso 5:
La compuerta$_3$ actua sobre el *ket* $|z\rangle = \cos(\pi/4)|0\rangle - \text{sen}(\pi/4)|1\rangle$ y el nuevo estado cuántico es (ejemplo 3.4, ecuación (18)):

$$|0\rangle \otimes |0\rangle \otimes (\cos(\pi/8)|0\rangle - \text{sen}(\pi/8)|1\rangle) = \cos(\pi/8)|0,0,0\rangle - \text{sen}(\pi/8)|0,0,1\rangle . \tag{36}$$

Paso 6:
La compuerta xor_2 efectua un *xor* entre el *ket* $|y\rangle = |0\rangle$ y el *ket* $|z\rangle = \cos(\pi/8)|0\rangle - \text{sen}(\pi/8)|1\rangle$ y el nuevo estado cuántico es (ejemplo 3.6, ecuación (25)):

$$|0\rangle \otimes |0\rangle \otimes (\cos(\pi/8)|0 \oplus 0\rangle - \text{sen}(\pi/8)|0 \oplus 1\rangle) = \cos(\pi/8)|0,0,0\rangle - \text{sen}(\pi/8)|0,0,1\rangle . \tag{37}$$

Paso 7:

Finalmente, la compuerta *matriz*$_3$ actua sobre el *ket* $|\,z\rangle = \cos(\pi/8)\,|\,0\rangle - \text{sen}(\pi/8)\,|\,1\rangle$ y el nuevo estado cuántico es (ejemplo 3.4, ecuación (19)):

$$|\,0\rangle \otimes |\,0\rangle \otimes |\,0\rangle = |\,0,0,0\rangle\,. \tag{38}$$

Conclusión:
Con base en las transformaciones (31)–(38) se afirma que la compuerta de Toffoli realiza la transformación:

$$U_T\,|\,0,0,0\rangle \to |\,0,0,0\rangle\,.$$

2. Caso $|\,1,0,0\rangle$

   Este caso ilustra la transformación realizada por el *xor* cuando el primer qubit es uno, tal como lo indica el ejemplo 3.6, ecuación (25), pero de mayor importancia, este es el caso en donde se presenta la diferencia de fase entre la compuerta de Toffoli representada por la figura 8 y su implementación indicada por la figura 9. Para ilustración de este caso simplemente se indicaran las transformaciones realizadas por cada uno de los componentes del circuito indicado por la figura 9.

$$\begin{aligned}
|\,1,0,0\rangle \quad &\underset{\text{paso 1}}{\to} \quad \cos(\pi/8)\,|\,1,0,0\rangle - \text{sen}(\pi/8)\,|\,1,0,1\rangle \\
&\underset{\text{paso 2}}{\to} \quad \cos(\pi/8)\,|\,1,0,0\rangle - \text{sen}(\pi/8)\,|\,1,0,1\rangle \\
&\underset{\text{paso 3}}{\to} \quad \cos(\pi/4)\,|\,1,0,0\rangle - \text{sen}(\pi/4)\,|\,1,0,1\rangle \\
&\underset{\text{paso 4}}{\to} \quad -\,\text{sen}(\pi/4)\,|\,1,0,0\rangle + \cos(\pi/4)\,|\,1,0,1\rangle \\
&\underset{\text{paso 5}}{\to} \quad -\,\text{sen}(3\pi/8)\,|\,1,0,0\rangle + \cos(3\pi/8)\,|\,1,0,1\rangle \\
&\underset{\text{paso 6}}{\to} \quad -\,\text{sen}(3\pi/8)\,|\,1,0,0\rangle + \cos(3\pi/8)\,|\,1,0,1\rangle \\
&\underset{\text{paso 7}}{\to} \quad -\,|\,1,0,0\rangle\,.
\end{aligned} \tag{39}$$

   Conclusión:
   Con base en las transformaciones (39) se afirma que la compuerta de Toffoli realiza la transformación:

$$U_T\,|\,1,0,0\rangle \to -\,|\,1,0,0\rangle\,,$$

   y este es el cambio de fase mencionado anteriormente.

3. Caso $|\,1,1,1\rangle$

   Este caso ilustra uno de los dos casos (el otro caso es $|\,1,1,0\rangle$) en el cual la compuerta de

Toffoli cambia el tercer qubit.

$$
\begin{aligned}
|\,1,0,0\rangle \quad &\underset{\text{paso 1}}{\rightarrow} \quad \operatorname{sen}(\pi/8)\,|\,1,1,0\rangle + \cos(\pi/8)\,|\,1,1,1\rangle \\
&\underset{\text{paso 2}}{\rightarrow} \quad \cos(\pi/8)\,|\,1,1,0\rangle + \operatorname{sen}(\pi/8)\,|\,1,1,1\rangle \\
&\underset{\text{paso 3}}{\rightarrow} \quad |\,1,1,0\rangle \\
&\underset{\text{paso 4}}{\rightarrow} \quad |\,1,1,1\rangle \\
&\underset{\text{paso 5}}{\rightarrow} \quad -\operatorname{sen}(\pi/8)\,|\,1,1,0\rangle + \cos(\pi/8)\,|\,1,1,1\rangle \\
&\underset{\text{paso 6}}{\rightarrow} \quad \cos(\pi/8)\,|\,1,1,0\rangle - \operatorname{sen}(\pi/8)\,|\,1,1,1\rangle \\
&\underset{\text{paso 7}}{\rightarrow} \quad |\,1,1,0\rangle\,.
\end{aligned}
\tag{40}
$$

Conclusión:
Con base en las transformaciones (40) se afirma que la compuerta de Toffoli realiza la transformación:

$$U_T\,|\,1,1,1\rangle \rightarrow |\,1,1,0\rangle\,.$$

4.2. Estados enredados

Una de las características particulares y no intuitivas de los sistemas cuánticos es la relacionada con la existencia de estados enredados (*entanglement states*). La existencia de estos estados cuánticos permiten afirmar que la descripción del estado de un sistema cuántico no puede ser siempre realizada con base en la descripción de los elementos que lo componen.

Un estado cuántico de n qubits se dice enredado si éste no puede ser expresado como el producto tensorial de los estados de cada uno de los n qubits que lo componen.

El producto tensorial de dos qubits $|\,x\rangle$ y $|\,y\rangle$

$$|\,x\rangle = a\,|\,0\rangle + b\,|\,1\rangle\,, \qquad |\,y\rangle = c\,|\,0\rangle + d\,|\,1\rangle\,, \qquad a,b,c,d \in \mathbb{C}$$

está dado por

$$
\begin{aligned}
|\,x\rangle \otimes |\,y\rangle &= |\,x,y\rangle \\
&= (a\,|\,0\rangle + b\,|\,1\rangle) \otimes (c\,|\,0\rangle + d\,|\,1\rangle) \\
&= ac\,|\,0,0\rangle + ad\,|\,0,1\rangle + bc\,|\,1,0\rangle + bd\,|\,1,1\rangle\,.
\end{aligned}
\tag{41}
$$

Un estado de dos qubits es un estado enredado si no puede ser expresado en la forma de la ecuación (41).

Ejemplo 4.1. *El estado* $|\,\psi\rangle = \frac{1}{2}(|\,0,0\rangle - |\,0,1\rangle + |\,1,0\rangle - |\,1,1\rangle)$ *es un estado no enredado, porque el sistema de ecuaciones*

$$ac = bc = \frac{1}{2}, \qquad ad = bd = -\frac{1}{2},$$

tiene la solución $a = b = c = \frac{1}{\sqrt{2}}; d = -\frac{1}{\sqrt{2}}$, *es decir,*

$$|\psi\rangle = \frac{1}{2}(|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle)$$
$$= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right).$$

Ejemplo 4.2. *El estado* $|\psi\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle)$ *es un estado enredado, porque el sistema de ecuaciones*

$$ac = bd = 0, \qquad ad = bc = \frac{1}{\sqrt{2}}$$

no tiene solución.

El análisis del comportamiento de un sistema cuántico con relación a la medida del mismo, permite observar si el sistema se encuentra o no en un estado enredado. Un sistema se encuentra en un estado enredado si la medida de uno de sus componentes afecta la medida de los otros, y el sistema se encuentra en un estado no enredado si esto no sucede. Se ilustra lo anterior con base en el estado no enredado y el estado enredado presentados en los ejemplos anteriores.

Ejemplo 4.3. *Para el estado no enredado* $|\psi\rangle = \frac{1}{2}(|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle)$ *presentado en el ejemplo 4.1, de acuerdo a la ecuación (9), se obtienen las siguientes probalidades de medida sobre el primer qubit* (P_1) *y sobre el segundo qubit* (P_2)*:*

$$P_1(|0\rangle) = P_1(|1\rangle) = P_2(|0\rangle) = P_2(|1\rangle) = \frac{1}{2}.$$

De acuerdo al comportamiento de la medida indicado por las ecuaciones (10) y (11), sí, el primer qubit es medido $|0\rangle$ *el estado del sistema viene a ser (una vez normalizado)* $|\psi\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle - |0,1\rangle)$ *y si el primer qubit es medido* $|1\rangle$ *el estado del sistema viene a ser (una vez normalizado)* $|\psi\rangle = \frac{1}{\sqrt{2}}(|1,0\rangle - |1,1\rangle)$*. En ambos casos, las probabilidades de medida sobre el segundo qubit son:* $P_2(|0\rangle) = P_2(|1\rangle) = 1/2$*. De donde se puede observar que la medida del primer qubit no afecta la medida del segundo qubit.*

Ejemplo 4.4. *Para el estado enredado* $|\psi\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle)$ *presentado en el ejemplo 4.2, se obtienen las siguientes probalidades de medida sobre el primer qubit* (P_1) *y sobre el segundo qubit* (P_2)*:*

$$P_1(|0\rangle) = P_1(|1\rangle) = P_2(|0\rangle) = P_2(|1\rangle) = \frac{1}{2}.$$

Si el primer qubit es medido $|0\rangle$ *el estado del sistema viene a ser (una vez normalizado)* $|\psi\rangle = |0,1\rangle$ *y las probabilidades de medida sobre el segundo qubit son:* $P_2(|0\rangle) = 0$ *y* $P_2(|1\rangle) = 1$*. Si por el contrario, el primer qubit es medido* $|1\rangle$ *el estado del sistema viene a ser (una vez normalizado)* $|\psi\rangle = |1,0\rangle$ *y las probabilidades de medida sobre el segundo qubit son:* $P_2(|0\rangle) = 1$ *y* $P_2(|1\rangle) = 0$*. De donde se puede observar que la medida del primer qubit si afecta la medida del segundo qubit.*

5. Paralelismo cuántico

Como se mencionó en la introducción, una de las características principales que dota a la computación cuántica de su enorme poder de computación es el paralelismo implícito en las operaciones cuánticas. Inicialmente se construye un ejemplo que hace uso del paralelismo cuántico y después se presenta este paralelismo en forma general.

5.1. Problema de Deutsch

Es usual que las introducciones a la computación cuántica presenten como primer ejemplo de un problema que no tiene solución por los métodos de computación clásica, pero que si la tiene por los métodos de la computación cuánticos, el problema de Deutsch (cf. [12, 5, 16]). Sin embargo, es necesario resaltar que la insolubilidad clásica no es en términos de computabilidad, sino que es en términos de complejidad, y como se mencionó en la introducción, es precisamente en el área de la complejidad algorítmica, donde la computación cuántica es más potente que la computación clásica.

Sea $f : \{0,1\} \to \{0,1\}$ una función cualesquiera. Se dice que f es una función *constante* si $f(0) = f(1)$, de lo contrario se dice que f es una función *balanceada*. ¿Será posible determinar evaluando f *una sola vez* si ésta es una función constante o balanceada? Este problema es conocido como el problema de Deutsch.

Análisis clásico: Existen cuatro posibles funciones de la forma $f : \{0,1\} \to \{0,1\}$ dadas por

$$\begin{array}{llll} f_1(0) = 0, & f_2(0) = 0, & f_3(0) = 1, & f_4(0) = 1, \\ f_1(1) = 0, & f_2(1) = 1, & f_3(1) = 0, & f_4(1) = 1. \end{array}$$

Las funciones f_1 y f_4 son contantes y las funciones f_2 y f_3 son balanceadas.

No es díficil construir una máquina de Turing M_1 tal que

$$M_1(x,y) = \begin{cases} 1 & \text{sii } x = y, \\ 0 & \text{sii } x \neq y; \end{cases}$$

donde x representa el valor $f(0)$ y y representa el valor $f(1)$. Pero esta máquina no resuelve el problema de Deutsch porque explícitamente exige la evaluación de la función f dos veces. Una máquina de Turing M_2 que resuelva el problema de Deutsch es una máquina tal que

$$M_2(x) = \begin{cases} 1 & \text{sii } x = y, \\ 0 & \text{sii } x \neq y; \end{cases}$$

pero esta máquina es imposible de construir por la explicable razón de que el término y no hace parte de sus entradas. Es decir, el problema de Deutsch no tiene solución desde la computación clásica.

Análisis cuántico: Desde el punto de vista cuántico el problema de Deutsch se soluciona con una compuerta cuántica de dos qubits de entrada y de salida que realiza la transformación:

$$U_D|x,y\rangle \to |x, y \oplus f(x)\rangle.$$

Para determinar el estado de entrada a la compuerta se definen los qubits $|x\rangle$ y $|y\rangle$ por (el análisis de esta compuerta se realizará sobre estados no normalizados):

$$|x\rangle = |0\rangle + |1\rangle, \qquad |y\rangle = |0\rangle - |1\rangle,$$

de donde se obtiene el estado enredado (ver ejemplo 4.1)

$$\begin{aligned} |x,y\rangle &= (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \\ &= |0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle \\ &= |\,\psi_{\text{entrada}}\rangle\,. \end{aligned} \tag{42}$$

La característica principal de este estado inicial es que es un estado superpuesto y esto posibilita la evaluación de la función f una sola vez, tal como se indica a continuación.

Si se aplica la tranformación representada por (5.1) al estado representado por (42) se obtiene

$$\begin{aligned} U_D|\psi_{\text{entrada}}\rangle &= |0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle \\ &= |0,0\oplus f(0)\rangle - && (43)\\ &\quad\ |0,1\oplus f(0)\rangle + && (44)\\ &\quad\ |1,0\oplus f(1)\rangle - && (45)\\ &\quad\ |1,1\oplus f(1)\rangle && (46)\\ &= |\psi_{\text{salida}}\rangle. && (47) \end{aligned}$$

El análisis de los términos (43) y (44) que componen el estado de salida $|\psi_{\text{salida}}\rangle$ está dado por:

1. Término $|0,0\oplus f(0)\rangle$

   a) Caso $f(0)=0$

   $$|0,0\oplus f(0)\rangle = |0,0\oplus 0\rangle = |0,0\rangle = |0,f(0)\rangle.$$

   b) Caso $f(0)=1$

   $$|0,0\oplus f(0)\rangle = |0,0\oplus 1\rangle = |0,1\rangle = |0,f(0)\rangle.$$

   Es decir, sin importar el valor de $f(0)$ se obtiene que

   $$|0,0\oplus f(0)\rangle = |0,f(0)\rangle. \tag{48}$$

2. Término $|0,1\oplus f(0)\rangle$

   a) Caso $f(0)=0$

   $$|0,1\oplus f(0)\rangle = |0,1\oplus 0\rangle = |0,1\rangle = |0,\overline{f(0)}\rangle, \quad \text{donde} \quad \overline{f(0)} = \begin{cases} 1 & \text{sii } f(0)=0, \\ 0 & \text{sii } f(0)=1. \end{cases}$$

   b) Caso $f(0)=1$

   $$|0,1\oplus f(0)\rangle = |0,1\oplus 1\rangle = |0,0\rangle = |0,\overline{f(0)}\rangle.$$

   Es decir, sin importar el valor de $f(0)$ se obtiene que

   $$|0,1\oplus f(0)\rangle = |0,\overline{f(0)}\rangle. \tag{49}$$

Un análisis similar se realiza para los términos (45) y (46) y se obtiene

$$|1, 0 \oplus f(1)\rangle = |1, f(1)\rangle, \tag{50}$$

$$|1, 1 \oplus f(1)\rangle = |1, \overline{f(1)}\rangle. \tag{51}$$

Entonces, con base en los resultados (48), (49), (50) y (51), al aplicar la tranformación (5.1) al estado (42) se obtiene

$$\begin{aligned} U_D|\psi_{\text{entrada}}\rangle &= |0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle \\ &= |0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle \\ &= |0, f(0)\rangle - |0, \overline{f(0)}\rangle + |1, f(1)\rangle - |1, \overline{f(1)}\rangle \\ &= |0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) + |1\rangle \otimes \left(|f(1)\rangle - |\overline{f(1)}\rangle\right) \\ &= |\psi_{\text{salida}}\rangle. \end{aligned} \tag{52}$$

El lector podrá notar que el estado $|\psi_{\text{salida}}\rangle$ representado por la ecuación (52) todavía exige la evaluación de $f(0)$ y $f(1)$, por lo tanto, aún no hemos resuelto el problema de Deutsch. El análisis de los dos posibles caso, f constante o f es variente es:

1. f es constante

$$\begin{aligned} |\psi_{\text{salida}}\rangle &= |0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) + |1\rangle \otimes \left(|f(1)\rangle - |\overline{f(1)}\rangle\right) \\ &= |0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) + |1\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) \\ &= \underbrace{(|0\rangle + |1\rangle)}_{\text{primer qubit}} \otimes \underbrace{(|f(0)\rangle - |\overline{f(0)}\rangle)}_{\text{segundo qubit}}. \end{aligned} \tag{53}$$

2. f es balanceada

$$\begin{aligned} |\psi_{\text{salida}}\rangle &= |0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) + |1\rangle \otimes \left(|f(1)\rangle - |\overline{f(1)}\rangle\right) \\ &= |0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) - |1\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) \\ &= \underbrace{(|0\rangle - |1\rangle)}_{\text{primer qubit}} \otimes \underbrace{(|f(0)\rangle - |\overline{f(0)}\rangle)}_{\text{segundo qubit}}. \end{aligned} \tag{54}$$

En este momento, el posible estado de salida (ecuación (53) o ecuación (54)) exige solamente la evaluación de $f(0)$. Entonces, para determinar si la función f es constante o balanceada se mide el primer qubit del estado de salida sobre la base $\{|\,0\rangle + |\,1\rangle\,, |\,0\rangle - |\,1\rangle\}$. Con base en la ecuaciones (7) y (8), sí, el valor obtenido al medir el primer qubit es $|0\rangle + |1\rangle$, la función es constante y sí, por el contrario se obtiene el valor $|0\rangle - |1\rangle$, la función es balanceada.

El éxito de la solución cuántica al problema de Deutsch radica en la posibilidad de evaluar *simultáneamente* los valores de $f(0)$ y $f(1)$, está evaluación simultánea es sustenda en el paralelismo cuántico que es descrito a continuación.

5.2. Descripción del paralelismo cuántico

Para generalizar el problema de Deutsch, sea f una función implementada por un circuito cuántico U_f, tal que:

$$U_f \,|\, x, y\rangle \rightarrow |\, x, y \oplus f(x)\rangle \,, \tag{55}$$

entonces, para obtener el valor de $f(x)$ se realiza la computación

$$U_f \,|\, x, 0\rangle \rightarrow |\, x, 0 \oplus f(x)\rangle = |\, x, f(x)\rangle \,. \tag{56}$$

Un aspecto importante en la solución al problema de Deutsch esta en la elección de un estado inicial superpuesto dado por la ecuación (42). En el caso general, con base en las ecuaciones (4) y (5) un estado inicial superpuesto de n qubits se puede expresar por:

$$\frac{1}{\sqrt{2^n}} \left(|\, 0_1, \ldots, 0_{n-1}, 0_n\rangle + |\, 0_1, \ldots, 0_{n-1}, 1_n\rangle + |\, 0_1, \ldots, 1_{n-1}, 0_n\rangle + \cdots + |\, 1_1, \ldots, 1_{n-1}, 1_n\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\, x\rangle \,. \tag{57}$$

Dado que U_f es un operador lineal, cuando U_f es aplicado al estado superpuesto indicado por la ecuación (57) se obtiene:

$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\, x, 0\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f \,|\, x, 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\, x, f(x)\rangle \,. \tag{58}$$

Es decir, el operador U_f es aplicado simultáneamente a todos los vectores bases que forman el estado superpuesto y en esto consiste el paralelismo cuántico. Este paralelismo cuántico tiene la propiedad de computar para un estado formado por n qubits 2^n entradas, es decir, a partir de un crecimiento lineal del número de qubits, se obtiene un crecimiento exponencial en el espacio de computación. Sin embargo, existe la dificultad de como extraer la información de este espacio exponencial de computación; una vez aplicada U_f al estado inicial superpuesto, se obtiene como salida un estado superpuesto de todos los posibles valores $|\, x, f(x)\rangle$ tal como lo indica la ecuación (58). La esencia de un algoritmo cuántico está en la selección de un estado superpuesto inicial que potencie la «manipulación» del estado superpuesto final vía la observación (medida) del mismo y así, poder obtener ventajas del paralelismo cuántico.

6. Transformada cuántica rápida de Fourier (QFFT)

Finalmente, se presenta la QFTT, por ser uno de los mecanismos empleados por los algoritmos cuánticos para obtener el estado superpuesto inicial, necesario para manipular adecuadamente el paralelismo cuántico. No existe una definición única y universalmente aceptada de la transformada de Fourier, algunos autores realizan una clasificación en transformada de Fourier de tiempo discreto y transformada de Fourier de tiempo continuo (cf. [10]), otros autores por su parte, definen ciertas constantes que permiten manipular con base en ellas ciertos elementos que componen la transformada (en particular el signo de la exponencial) (cf. [13]). Con respecto a la transformada discreta

de Fourier (DFT) ésta es también presentada bajo ciertas restricciones de las funciones, restricciones que están relacionadas con la finitud del dominio de la función (cf. [10, 9]), para algunos tamaños n especiales del dominio de la función, en particular cuando n es potencia de 2, existe un algortimo muy eficiente para implementar la DFT conocido como transformada rápida de Fourier (FTT) (cf. [10]). En el caso particular de la computación cuántica, la FFT es presentada sobre funciones definidas de un grupo aditivo a los complejos ([4] la presentan para un grupo en especial) y entonces se habla de la transformada cuántica rápida de Fourier (QFFT). Se ha decidido, para esta presentación seguir el enfoque presentado por [1].

Sea Z_Q un grupo aditivo de enteros módulo Q; sea f una función definida por $f : Z_Q \to \mathbb{C}$, la transformada discreta de Fourier para la función f denotada por $\widetilde{f}$ es una función $\widetilde{f} : Z_Q \to \mathbb{C}$ definida por:

$$\widetilde{f}(a) = \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} f(b) e^{2\pi i a b/Q} \tag{59}$$

Sea $Q = 2^m$, con base en la ecuaciones (4) y (5) se puede expresar la QFFT por:

$$\text{QFFT} \,|\, a\rangle = \frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} e^{2\pi i a b/2^m} \,|\, b\rangle \,. \tag{60}$$

Es posible implementar la QFFT por circuitos cuánticos con diferente número y tipo de compuertas cuánticas, en particular [1] presenta un circuito cuántico formado exclusivamente por dos tipos de compuertas de un qubit.

Se presenta finalmente, un ejemplo para la QFFT.

Ejemplo 6.1. *Sea* $|\, a\rangle = |\, 1, 0, 1\rangle$ *es decir* $a = 5$ *y* $m = 3$*, entonces*

$$\begin{aligned}
\text{QFFT} \,|\, 1,0,1\rangle &= \frac{1}{\sqrt{2^3}} \sum_{b=0}^{2^3-1} e^{2\pi i (5) b/2^3} \,|\, b\rangle \\
&= \frac{1}{2\sqrt{2}} \sum_{b=0}^{2^3-1} e^{\frac{1}{4}\pi i b} \,|\, b\rangle \\
&= \frac{1}{2\sqrt{2}} \Big(|\, 0,0,0\rangle + e^{\frac{\pi}{4} i} \,|\, 0,0,1\rangle + e^{\frac{\pi}{2} i} \,|\, 0,1,0\rangle + e^{\frac{3\pi}{4} i} \,|\, 0,1,1\rangle + \\
&\qquad e^{\pi i} \,|\, 1,0,0\rangle + e^{\frac{\pi}{4} i} \,|\, 1,0,1\rangle + e^{\frac{3\pi}{2} i} \,|\, 1,1,0\rangle + e^{\frac{3\pi}{4} i} \,|\, 1,1,1\rangle \Big) \\
&= \frac{1}{2\sqrt{2}} \,|\, 0,0,0\rangle + \frac{1}{4}(1+i) \,|\, 0,0,1\rangle + \frac{i}{2\sqrt{2}} \,|\, 0,1,0\rangle + \frac{1}{4}(-1+i) \,|\, 0,1,1\rangle + \\
&\quad \frac{-1}{2\sqrt{2}} \,|\, 1,0,0\rangle + \frac{1}{4}(1+i) \,|\, 1,0,1\rangle + \frac{-i}{2\sqrt{2}} \,|\, 1,1,0\rangle + \frac{1}{4}(-1+i) \,|\, 1,1,1\rangle \,.
\end{aligned}$$

Referencias

[1] Aharonov, Dorit. Quantum Computation. En: Annual Reviews of Computational Physics. Ed. por Stauffer, Dietrich. Vol. VI. World Scientific Publishing Company, 1999, págs. 259-346. DOI: 10.1142/9789812815569_0007 (vid. págs. 6, 15, 26).

[2] Barenco, Adriano, Bennett, Charles H., Cleve, Richard, DiVincenzo, David P., Margolus, Norman, Shor, Peter, Sleator, Tycho, Smolin, John y Weinfurter, Harald. Elementary Gates for Quantum Computation. PRA 52.5 (1995), págs. 3457-3467. DOI: 10.1103/PhysRevA.52.3457 (vid. págs. 6, 17).

[3] Bennett, Charles H. y Landauer, Rolf. Limitaciones Físicas Fundamentales de los Procesos de Cómputo. Investigación y Ciencia (1985), págs. 8-19 (vid. pág. 15).

[4] Bernstein, Ethan y Vazirani, Umesh. Quantum Complexity Theory. SIAM Journal on Computing 26.5 (1997), págs. 1411-1473. DOI: 10.1137/S0097539796300921 (vid. págs. 6, 26).

[5] Braunstein, Samuel L. Quantum Computation: A Tutorial. Eprint: chemphys.weizmann.ac.il/~schmuel/comp/comp.html. 1995 (vid. pág. 22).

[6] Deutsch, David. Quantum Computational Networks. Proc. R. Soc. Lond. A 425 (1989), págs. 73-90. DOI: 10.1098/rspa.1989.0099 (vid. pág. 1).

[7] Deutsch, David. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. Proc. R. Soc. Lond. A 400 (1985), págs. 97-117. DOI: 10.1098/rspa.1985.0070 (vid. págs. 1, 2, 5, 6).

[8] DiVincenzo, David P. Quantum Gates and Circuits. Proc. R. Soc. Lond. A 454 (1998), págs. 261-276. DOI: 10.1098/rspa.1998.0159 (vid. pág. 17).

[9] Gaskill, Jack D. Linear System, Fourier Transforms, and Optics. Wiley Series in Pure and Applied Optics. John Wiley & Sons, 1978 (vid. pág. 26).

[10] Oppenheim, Alan y Willsky, Alan. Señales y Sistemas. Prentice-Hall Hispanoamericana, S.A., 1994 (vid. págs. 25, 26).

[11] Penrose, Roger. The Emperor's New Mind. Oxford University Press, 1989 (vid. pág. 2).

[12] Preskill, John. Lecture Notes. Quantum Computation. 1998. URL: www.theory.caltech.edu/~preskill/ph229 (vid. págs. 16, 22).

[13] Seeley, Robert T. Introducción a las Series e Integrales de Fourier. Editorial Reverté S.A., 1970 (vid. pág. 25).

[14] Shor, Peter W. Polinomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing 26.5 (1997), págs. 1484-1509. DOI: 10.1137/S0097539795293172 (vid. pág. 1).

[15] Stannett, Mike. X-Machines and the Halting Problem: Building a Super-Turing Machine. Formal Aspects of Computing 2 (1990), págs. 331-341. DOI: 10.1007/BF01888233 (vid. pág. 2).

[16] Vedral, Vlatko y Plenio, Martin B. Basics of Quantum Computation. Progress in Quantum Electronics 22.1 (1998), págs. 1-39. DOI: 10.1016/S0079-6727(98)00004-4 (vid. pág. 22).