Paralelismo cuántico: el problema de Deutsch

Por Andrés Sicard, Mario Vélez y Carlos Pérez

RESUMEN

Se define la unidad fundamental de información para la computación cuántica denominada qubit. Se define el proceso de evolución de la computación cuántica, realizada por medio de operadores de evolución. Se hace referencia a la reversibilidad de la evolución de la computación cuántica. Se presenta el paralelismo cuántico. Se indica como se realiza la medida sobre los qubits. Se presenta el problema de Deutsch y su solución. Finalmente, se presentan algunas conclusiones.

1. Introducción

A partir de los trabajos sobre computación reversible de Charles Bennnet (1973), de las compuertas universales reversibles construidas por Edward Fredkin y Tommaso Toffoli (1982), de las propuestas de computación cuántica de Richard Feynman (1996), del modelo de máquinas de Turing cuánticas (1985) y del modelo de circuitos cuánticos (1989) propuestos por David Deutsch; la computación cuántica obtuvo su resultado más importante en el área de la complejidad algorítmica.

El algoritmo de Peter Shor para factorizar un número en sus factores primos (1997), demostró que existe un algoritmo cuántico que resuelve un problema de manera más eficiente que el mejor algoritmo clásico conocido hasta el momento.

La reducción en la complejidad temporal de la computación cuántica respecto a la computación clásica, está sustentada en una característica de la primera llamada *paralelismo cuántico*.

Como un primer acercamiento a esta característica, se presenta la solución a un problema denominado *problema de Deutsch*.

Este problema fue inicialmente planteado por David Deutsch (1989) y la solución determinista que se presenta fue realizada por Cleve, Ekert, Macchiavello y Mosca (1998).

2. Qubits

El qubit (Schumacher, 1995) es la unidad fundamental de información en la computación cuántica al igual que el bit lo es en la computación clásica. Un qubit es un elemento de un espacio de Hilbert H_2 bidimensional. Los qubits se representan comúnmente en una base con la notación bra–ket de Dirac (1967), donde el ket $|0\rangle$ representa el qubit cero y el ket $|1\rangle$ representa el qubit uno.

Los qubits son vectores de H_2 y su forma más general está dada por [1]:

$$|x\rangle = c_0|0\rangle + c_1|1\rangle,$$

donde $c_0, c_1 \in C$ y $\sum_{i=0}^{1} |c_i|^2 = 1$. (1)

Los qubits $\{|0\rangle, |1\rangle\}$ forman una base para el espacio H_2 y son expresados de una manera más usual, llamada representación matricial como:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ y } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

A los kets o qubits se les asocia una forma lineal llamada bra. Una forma lineal es una función f que a todo vector $|x\rangle \in H_2$ le asocia $f(|x\rangle) \in C$. En la notación de Dirac, $\langle 0|$ es llamado bra cero y $\langle 1|$ es llamado bra uno. Estas formas lineales son inducidas mediante el producto interno definido de la siguiente manera:

$$\langle x|y\rangle = \delta_{xy} = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{si } x \neq y, \end{cases} \quad \text{es decir,}$$

[1] C : Números complejos.

$$\langle 0|0\rangle = \langle 1|1\rangle = 1 \text{ y } \langle 0|1\rangle = \langle 1|0\rangle = 0.$$

Los bras resultan ser entonces elementos del espacio dual del espacio de Hilbert H_2.

En forma matricial se representan como: $\langle 0| = (1 \;\; 0)$ y $\langle 1| = (0 \;\; 1)$. El vector bra asociado al vector ket $|x\rangle$ se escribe como $\langle x|$ y es el adjunto conjugado del vector ket, es decir, $\overline{|x\rangle} = \langle x|$ y $\overline{\langle x|} = |x\rangle$.

Los qubits por sí solos no son de mucha utilidad, por lo que se necesitan combinar para formar unidades de información más complejas.

La unidad de información que le sigue en complejidad al 1-qubit es el 2-qubit, el cual pertenece a un espacio de Hilbert 4-dimensional H_4 con base

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

Un 2-qubit se puede formar haciendo el producto tensorial entre dos 1-qubit.

Si $|x\rangle = a|0\rangle + b|1\rangle$, y $|y\rangle = c|0\rangle + d|1\rangle$ son dos 1-qubits, entonces el producto tensorial $|x\rangle \otimes |y\rangle$ está dado por:

$$|x\rangle \otimes |y\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|0,0\rangle + ad|0,1\rangle + bc|1,0\rangle + bd|1,1\rangle$$

y su representación matricial es:

$$|x\rangle \otimes |y\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = ac\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + ad\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + bc\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + bd\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Una representación matricial de los elementos de la base de H_4 es:

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

La forma más general de un 2-qubit está dada por:

$|x,y\rangle = c_0|0,0\rangle + c_1|0,1\rangle + c_2|1,0\rangle + c_3|1,1\rangle$, donde:

$$c_0, c_1, c_2, c_3 \in C \quad \text{y} \quad \sum_{i=0}^{3} |c_i|^2 = 1 \qquad (2)$$

Como se observa, un 2-qubit es un elemento de un espacio de Hilbert 4-dimensional y en general un n-qubit es un elemento de un espacio de Hilbert 2^n dimensional.

3. Operadores de evolución

La evolución o dinámica de un n-qubit es determinada por un operador lineal unitario sobre el espacio de Hilbert (Gruzka, 1989), este operador es denominado *operador de evolución*. Un operador unitario U es un operador que cumple que su adjunto conjugado $U^\dagger$ es igual a su inverso U^{-1}, es decir [2]:

$$UU^\dagger = U^\dagger U = I. \qquad (3)$$

Si $|\Psi(t)\rangle$ es un n-qubit, la evolución con base en el operador U de un paso de computación, está dada por:

$$U|\Psi(0)\rangle \rightarrow |\Psi(1)\rangle, \qquad (4)$$

y en general, la evolución de m pasos de computación está dada por (Deutsch, 1985)

$$U^m|\Psi(0)\rangle \rightarrow |\Psi(m)\rangle.$$

Ejemplo 1. Uno de los operadores de evolución más usados en la computación cuántica es el operador Hadamard (Rieffel y Polak, 1989) el cual realiza la siguiente operación sobre un 1-qubit:

$$H|x\rangle \rightarrow \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{si } |x\rangle = |0\rangle, \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{si } |x\rangle = |1\rangle. \end{cases}$$

Los operadores de evolución son expresados de manera más usual como matrices. La matriz $2x2$ que representa el operador de Hadamard es (Aharanov, 1989):

$$H_{2x2} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Para construir el operador de evolución Hadamard sobre un 2-qubit basta con hacer el producto tensorial

[2] I: Operador identidad, representado por la matriz identidad.

entre dos operadores Hadamard H_{2x2}. El producto tensorial entre dos matrices 2x2 es:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

Por lo tanto, el operador de evolución de Hadamard sobre un 2-qubit está definido por:

$$H_{4x4} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \qquad (5)$$

Ejemplo 2. Otro operador de evolución muy usado en computación cuántica es el operador XOR, el cual opera sobre un 2-qubit de la siguiente manera: $XOR|x,y\rangle \rightarrow |x, x \oplus y\rangle$, donde $\oplus$ es la suma módulo 2 o XOR clásico. La matriz correspondiente al XOR es:

$$XOR = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad (6)$$

4. Reversibilidad

La unitariedad de los operadores en la computación cuántica le proporcionan a ésta la reversibilidad. Si realizamos la operación indica por (4) y luego al estado resultado le aplicamos el operador adjunto conjugado de U, entonces por (3):

$$U^{\dagger}|\Psi(1)\rangle \rightarrow |\Psi(2)\rangle, \text{ donde}$$

$$|\Psi(2)\rangle = U^{\dagger}\left(U|\Psi(0)\rangle\right) = |\Psi(0)\rangle,$$

es decir, se obtiene de nuevo el estado inicial $|\Psi(0)\rangle$.

A partir de una función $f: x \rightarrow f(x)$ de n bits en m bits se construye una función reversible f_R de m+n bits en m+n bits dada por (Aharonovov, 1998) $f_R: (x,y) \rightarrow (x, y \oplus f(x))$, entonces, una función f puede ser implementada por un operador de evolución U_f si éste realiza la transformación:

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

Ejemplo 3. La función constante $f: \{0,1\} \rightarrow \{0,1\}$ donde $f(x) = 0$, implementada por un operador unitario U_1. La matriz para esta transformación es:

$$U_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Ejemplo 4. La función balanceada, es decir, con igual número de ceros y de unos, dada por $f: \{0,1\} \rightarrow \{0,1\}$, donde $f(x) = x$, implementada por un operador unitario U_f. La matriz para esta transformación es la matriz dada por (6).

5. Paralelismo cuántico

Una de las propiedades más importantes de la computación cuántica es el paralelismo cuántico. La posibilidad de esta propiedad se debe a que los operadores que determinan la evolución del sistema cuántico son lineales.

Así, si al 2-qubit $|\Phi\rangle = a|0,0\rangle + b|1,0\rangle$ se le aplica un operador U_f se obtiene:

$$U_f|\Phi\rangle = U_f\left(a|0,0\rangle + b|1,0\rangle\right) = U_f a|0,0\rangle + U_f b|1,0\rangle = a|0, f(0)\rangle + b|1, f(1)\rangle$$

El operador U_f es aplicado simultáneamente a todos los vectores bases que forman el estado superpuesto.

En este caso el estado superpuesto $|\Phi\rangle$ está formado por 2 estados de la base, sin embargo, esta situación se puede generalizar afirmando que en un sistema de n-qubits un operador lineal de evolución actúa simultáneamente sobre 2^n estados base. Es decir, un crecimiento lineal en el número de qubits produce un crecimiento exponencial en el número de estados base sobre los cuales se realiza la computación. En esto consiste el paralelismo cuántico.

6. Medida cuántica

De nada sirve computar sobre el sistema sino se puede medirlo para obtener información útil de él. Pero no se puede medir el sistema cuántico sin perturbarlo: después de medir el sistema, éste se colapsa a un único estado base. ¿Se puede conocer

a-priori exactamente a que estado colapsará el sistema? No, pero se puede conocer la probabilidad de que colapse a cualquiera de ellos.

La probabilidad de colapsar a un estado después de la medida está dada por los coeficientes de los vectores base. Entonces, si se mide el estado dado por (1), la probabilidad de colapsar al estado $|0\rangle$ es:

$$P(|0\rangle) = |c_0|^2 \text{, donde}$$

$$P(|0\rangle) = |\langle 0|(c_0|0\rangle + c_1|1\rangle)|^2 = |c_0\langle 0|0\rangle + c_1\langle 0|1\rangle|^2,$$

y la probabilidad de colapsar al estado $|1\rangle$ es:

$$P(|1\rangle) = |c_1|^2 \text{, donde}$$

$$P(|1\rangle) = |\langle 1|(c_0|0\rangle + c_1|1\rangle)|^2 = |c_0\langle 1|0\rangle + c_1\langle 1|1\rangle|^2.$$

La mayoría de las veces no se requiere medir todo el sistema. Si se tiene por ejemplo el 2–qubit representado por (2), se podría medir el primero o el segundo qubit. Si se decide medir el primer qubit, la probabilidad de que el primer qubit colapse a $|0\rangle$ es $|c_0|^2 + |c_1|^2$ y la probabilidad de que el primer qubit colapse a $|1\rangle$ es $|c_2|^2 + |c_3|^2$. El cálculo de estas probabilidades es como sigue a continuación. Si el primer qubit colapsa a $|0\rangle$, el sistema completo colapsa a una combinación lineal de $\{|0,0\rangle, |0,1\rangle\}$, es decir, $P(|0,i\rangle) = P(|0,0\rangle) + P(|0,1\rangle)$, donde

$$P(|0,0\rangle) = |\langle 0,0|(c_0|0,0\rangle + c_1|0,1\rangle + c_2|1,0\rangle + c_3|1,1\rangle)|^2$$
$$= |c_0\langle 0,0|0,0\rangle + c_1\langle 0,0|0,1\rangle + c_2\langle 0,0|1,0\rangle + c_3\langle 0,0|1,1\rangle|^2,$$

ecuación (7)

$$P(|0,1\rangle) = |\langle 0,1|(c_0|0,0\rangle + c_1|0,1\rangle + c_2|1,0\rangle + c_3|1,1\rangle)|^2$$
$$= |c_0\langle 0,1|0,0\rangle + c_1\langle 0,1|0,1\rangle + c_2\langle 0,1|1,0\rangle + c_3\langle 0,1|1,1\rangle|^2$$

ecuación (8)

Los términos $\langle 0,0|0,0\rangle$, $\langle 0,0|0,1\rangle$, $\langle 0,0|1,0\rangle$ y $\langle 0,0|1,1\rangle$ de (7) y los términos $\langle 0,1|0,0\rangle$, $\langle 0,1|0,1\rangle$, $\langle 0,1|1,0\rangle$ y $\langle 0,1|1,1\rangle$ de (8), son calculados con base en la siguiente propiedad del producto tensorial (Rieffel y Polak, 1998): si A,B,X y Y son matrices, entonces:

$$(A \otimes B)\cdot(X \otimes Y) = AX \otimes BY. \qquad (9)$$

Con base en (9), $\langle a,b|x,y\rangle = \langle a|x\rangle \otimes \langle b|y\rangle$, luego (7) y (8) vienen a ser:

$$P(|0,0\rangle) = |c_0(\langle 0|0\rangle \otimes \langle 0|0\rangle) + c_1(\langle 0|0\rangle \otimes \langle 0|1\rangle)$$
$$+ c_2(\langle 0|1\rangle \otimes \langle 0|0\rangle) + c_3(\langle 0|1\rangle \otimes \langle 0|1\rangle)|^2 = |c_0|^2,$$

$$P(|0,1\rangle) = |c_0(\langle 0|0\rangle \otimes \langle 1|0\rangle) + c_1(\langle 0|0\rangle \otimes \langle 1|1\rangle)$$
$$+ c_2(\langle 0|1\rangle \otimes \langle 1|0\rangle) + c_3(\langle 0|1\rangle \otimes \langle 1|1\rangle)|^2 = |c_1|^2$$

Si el primer qubit colapsa a $|1\rangle$, el sistema completo colapsa a una combinación lineal de $\{|1,0\rangle, |1,1\rangle\}$, y un cálculo similar al anterior produce:

$$P(|1,i\rangle) = P(|1,0\rangle) + P(|1,1\rangle) = |c_2|^2 + |c_3|^2.$$

Si después de medir el primer qubit éste colapsa a $|0\rangle$, el sistema completo colapsará al estado (Rieffel y Polak, 1989):

$$|x'\rangle = \frac{1}{\sqrt{|c_0|^2 + |c_1|^2}}[c_0|0,0\rangle + c_1|0,1\rangle]$$

Pero si al medir el primer qubit éste colapsa a $|1\rangle$, el sistema completo colapsará al estado:

$$|x'\rangle = \frac{1}{\sqrt{|c_2|^2 + |c_3|^2}}[c_2|1,0\rangle + c_3|1,1\rangle]$$

Donde los términos $\frac{1}{\sqrt{|c_0|^2 + |c_1|^2}}$ y $\frac{1}{\sqrt{|c_2|^2 + |c_3|^2}}$ son para la normalización de los estados. Una situación similar sucede si se mide el segundo qubit.

7. Estados enredados

Una de las características particulares y no intuitivas de los sistemas cuánticos es la relacionada con la existencia de estados enredados o entrelazados (*entaglement*).

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.

Sean dos qubits $|x\rangle = a|0\rangle + b|1\rangle$ y $|x\rangle = c|0\rangle + d|1\rangle$

y su producto tensorial dado por:

$$|x\rangle \otimes |y\rangle = ac|0,0\rangle + ad|0,1\rangle + bc|1,0\rangle + bd|1,1\rangle ,$$

ecuación (10)

Entonces, un estado de dos qubits es un estado enredado si no puede ser expresado en la forma de la ecuación (10).

Ejemplo 5.

El estado $|\Psi\rangle = \frac{1}{2}\left(|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle\right)$

es un estado no enredado, porque el sistema de ecuaciones:

$ac = bc = \frac{1}{2}$, $ad = bd = -\frac{1}{2}$, tiene la solución

$a = b = c = \frac{1}{\sqrt{2}}$, $d = -\frac{1}{\sqrt{2}}$, es decir,

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

Ejemplo 6. El estado $|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0,1\rangle + |1,0\rangle\right)$ es un estado enredado, porque el sistema de ecuaciones, ac=bd, $ad = bc = \frac{1}{\sqrt{2}}$, no tiene solución.

8. El problema de Deutsch

Un ejemplo común en las introducciones a la computación cuántica donde se demuestra su potencial es el problema de Deutsch. Éste consiste en determinar si una función $f: \{0,1\} \to \{0,1\}$ es constante o balanceada evaluando una sola vez la función. La función f es constante si $f(0) = f(1)$ y en caso contrario se dice que es balanceada.

No es posible desde la computación clásica determinar si la función f es constante o balanceada realizando una única evaluación de la función, pero desde la computación cuántica, si es posible determinar el tipo de función (Gruska, 1999). La estrategia consiste en emplear un estado superpuesto para que la función f se aplique simultáneamente sobre todos los estados base que forman la superposición.

Al comienzo el estado inicial es $|\Psi(0)\rangle = |0,1\rangle$.

Luego al aplicar el operador Hadamard representado por (5) se obtiene el estado no enredado (ver ejemplo 5):

$$H_{4\times4}|\Psi(0)\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$
$$= \frac{1}{2}\left(|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle\right)$$
$$= |\Psi(1)\rangle.$$

A continuación se aplica el operador de evolución U_f que implementa la función f y que está dado por: $U_f|x,y\rangle \to |x, y \oplus f(x)\rangle$. El estado del sistema es entonces:

$$U_f|\Psi(1)\rangle = U_f\left[\frac{1}{2}\left(|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle\right)\right]$$
$$= \frac{1}{2}\left(U_f|0,0\rangle - U_f|0,1\rangle + U_f|1,0\rangle - U_f|1,1\rangle\right)$$
$$= \frac{1}{2}\left(|0,0\oplus f(0)\rangle - |0,1\oplus f(0)\rangle + |1,0\oplus f(1)\rangle - |1,1\oplus f(1)\rangle\right)$$
$$= |\Psi(2)\rangle$$

Los términos $0 \oplus f(x)$ se simplifican a $f(x)$, ya que $0 \oplus 0 = 0$ y $0 \oplus 1 = 1$, es decir, sólo depende del valor de $f(x)$. Por otra parte, los términos $1 \oplus f(x)$ se simplifican a $\overline{f(x)}$, ya que $1 \oplus 0 = 1$ y $1 \oplus 1 = 0$, es decir, sólo depende del valor de $f(x)$ negado. Luego el estado del sistema puede expresarse como:

$$|\Psi(2)\rangle = \frac{1}{2}\left(|0, f(0)\rangle - |0, \overline{f(0)}\rangle + |1, f(1)\rangle - |1, \overline{f(1)}\rangle\right)$$
$$= \frac{1}{2}\left[\left(|0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) + |1\rangle \otimes \left(|f(1)\rangle - |\overline{f(1)}\rangle\right)\right]\right.$$

Ahora si f es constante:

$$|\Psi(2)\rangle = \frac{1}{2}\left[|0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) + |1\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right)\right]$$
$$= \frac{1}{2}\left[\left(|0\rangle + |1\rangle\right) \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right)\right]$$

Pero si f es balanceada:

$$|\Psi(2)\rangle = \frac{1}{2}\left[|0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) - |1\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right)\right]$$
$$= \frac{1}{2}\left[\left(|0\rangle - |1\rangle\right) \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right)\right]$$

Lo siguiente es aplicar el operador Hadamard de un qubit sobre el primer qubit. Para ello se utilizará la propiedad (9). Por lo tanto, para aplicar Hadamard sobre el primer qubit y dejar el segundo qubit invariante, se debe aplicar el operador de evolución $H_{2\times 2} \otimes I$. Entonces al aplicar este operador en el caso de que la función sea constante, se obtiene:

$$H_{2\times 2} \otimes I|\Psi(2)\rangle = \frac{1}{2} H_{2\times 2}\left(|0\rangle + |1\rangle\right) \otimes I\left(|f(0)\rangle - |\overline{f(0)}\rangle\right)$$
$$= \frac{1}{2\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix} \otimes I\left(|f(0)\rangle - |\overline{f(0)}\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|0\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right)$$
$$= |\Psi(3)\rangle$$

pero si la función es balanceada, se obtiene:

$$H_{2\times 2} \otimes I|\Psi(2)\rangle = \frac{1}{2} H_{2\times 2}\left(|0\rangle - |1\rangle\right) \otimes I\left(|f(0)\rangle - |\overline{f(0)}\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|1\rangle \otimes \left(|f(0)\rangle - |\overline{f(0)}\rangle\right)$$
$$= |\Psi(3)\rangle$$

Como se puede observar, si la función es constante el primer qubit es $|0\rangle$ y si la función es balanceada el primer qubit es $|1\rangle$. Entonces sí se mide el primer qubit se puede saber si la función es constante o balanceada con probabilidad 1.

9. Conclusiones

Desde el punto de vista del número de evaluaciones de la función $f: \{0,1\} \rightarrow \{0,1\}$, el problema de Deutsch exige dos evaluaciones de la función desde la computación clásica y necesita sólo una evaluación de la función desde la computación cuántica. Esto representa una mejora (aunque no muy sustancial) de la complejidad algorítmica del problema.

Un generalización del problema de Deutsch es el problema denominado *The Deutsch-Jozsa promised problem*. En este problema se requiere evaluar la función $2^{n-1}+1$ veces desde la computación clásica y necesita sólo una evaluación de la función desde la computación cuántica (Gruzka, 1999). En esta situación la mejora en la complejidad algorítmica es muy sustancial. Esta es una situación similar a la ocurrida con el algoritmo de Shor para factorizar un número en sus factores primos.

Bibliografía

[1] Aharonov, Dorit. (1998). Quantum computation. Eprint: arXiv.org/abs/quant-ph/9812037.

[2] Bennet, Charles. (1973). Logical reversibility of computation. En: IBM Journal of Research and Development. Noviembre. pp. 525-532.

[3] Cleve, Richard et *al.* (1998). Quantum algorithms revisited. En: Proceeding Royal Society London. Tomo A454. pp. 339-354.

[4] Deutsch, David. (1985). Quantum theory, the Church – Turing principle and the universal quantum computer. En: Proceeding Royal Society London. Tomo A400. pp. 97-117.

[5] Deutsch, David. (1989). Quantum computational networks. En: Proceeding Royal Society London. Tomo A425. pp. 73-90.

[6] Dirac, P. A. M. (1967). Principios de mecánica cuántica. Barcelona: Ediciones Arial.

[7] Feynman, Richard. (1996). Feynman lectures on computation. Reading, Massachusetts: Addison-Wesley Publishing Company.

[8] Fredkin, Edward y Toffoli, Tommaso. (1982). Conservative logic. En: International Journal of Theoretical Physics. Tomo 21, No. 3 / 4. pp. 219-253.

[9] Gruska, Jozef. (1999). Quantum computing. Cambridge: McGraw-Hill International (UK) Limited.

[10] Rieffel, Eleanor y Polak, Wolfgang. (1998). An introduction to quantum computing for non – physicists. Eprint: arXiv.org/abs/quant-ph/9809016.

[11] Schumacher, Benjamin. (1995). Quantum Coding. En: Physical Review A. Tomo 51, No. 4. pp. 2738-2747.

[12] Shor, Peter W. (1997). Polynomial – time algorithms for prime factorization and discrete logarithms on a quantum computer. En: Siam Journal on Computing. Tomo 26, No. 5. pp. 1484-1509.

Andrés Sicard
Magister en Ingeniería Informática, Universidad EAFIT. Profesor Universidad EAFIT.

Mario Vélez
Magister en Física, Universidad de Antioquía. Profesor Universidad EAFIT.

Carlos Pérez
Estudiante Ingeniería de Sistemas, Universidad EAFIT. Grupo de Lógica y Computación, EAFIT.

Este artículo fue financiado por la universidad EAFIT, bajo el proyecto de investigación número 817424.