

# Construyendo compuertas cuánticas con IBM's cloud quantum computer

## Building quantum gates with IBM's cloud quantum computer

H. E. Caicedo-Ortiz <sup>a,b,c</sup>, E. Santiago-Cortés <sup>a,d</sup>, D. A. Mantilla-Sandoval <sup>a</sup>

<sup>a</sup>Corporación Universitaria Autónoma del Cauca, Popayán, Colombia

<sup>b</sup>Instituto de Educación Media Superior de la Ciudad de México, México

<sup>c</sup>Departamento de Ciencias Básicas, Facultad de Ingeniería, Universidad Anahuac Norte, México

<sup>d</sup>Escuela Nacional de Ciencias Biológicas y Centro de Nanociencias y Micro y Nanotecnologías, Instituto Politécnico Nacional, México

Recibido: 08/03/2017; revisado: 18/05/2017; aceptado: 30/05/2017

**H. E. Caicedo-Ortiz, E. Santiago-Cortés, D. A. Mantilla-Sandoval:** Construyendo compuertas cuánticas con IBM's cloud quantum computer. *Jou.Cie.Ing.* 9 (1): 42-56, 2017. ISSN 2145-2628, e-ISSN 2539-066X.

### Resumen

En este artículo, se describe de manera didáctica los elementos esenciales que permiten realizar cálculos elementales en un computador cuántico. Revisamos las características de las compuertas cuánticas más relevantes de 1-qubit y 2-qubits, además de implementarlas en el computador cuántico de IBM.

**Keywords:** Compuertas cuánticas, IBM's cloud quantum computer, computación cuántica, información cuántica

### Abstract

In this article, we describe in a didactic way the essential elements that allow elementary calculations in a quantum computer. We reviewed the characteristics of the most relevant quantum gates of 1-qubit and 2-qubits in addition to implementing them in the IBM's quantum computer.

**Keywords:** Quantum gates, IBM's cloud quantum computer, quantum computing, quantum information

## 1. Introducción

La computación e información cuántica son una extensión de la teoría de la información [1–4], en las cuales se hace uso de los efectos de la mecánica cuántica [5] como una herramienta para procesar información. Este nuevo esquema fue propuesto por Richard Feynman y David Deutsch en la década de los años ochenta del siglo XX [5, 6], quienes imaginaron la idea de explotar los grados de libertad de sistemas cuánticos como una nueva forma para realizar el procesamiento de la información. Este escenario

de trabajo no se restringe a dos únicos estados de operación  $(0, 1)$ , por el contrario, se pueden obtener multitud de estados intermedios como resultado de la superposición de estas dos posibilidades. Al realizar cualquier operación, el sistema permite evaluar todas las posibilidades en un solo paso [6], realizando una computación en paralelo. El paralelismo cuántico se traduce en una reducción del tiempo y aumento en la velocidad de procesamiento de la información [2, 6]. En este artículo se presenta un enfoque didáctico en el cual se describen los elementos básicos que permiten realizar cálculos elementales en un computador cuántico. Se

implementan algunas compuertas cuánticas de 1-qubit y 2-qubits en el computador cuántico de IBM de 5 qubits, interpretando sus resultados y la forma en que estos son presentados.

## 2. Qubit

Al igual que en los sistemas clásicos de computo en los cuales la mínima unidad de información es el bit, en la teoría de la computación cuántica este elemento tiene su contraparte y se denomina bit cuántico ó qubit [1,2,7]. Aunque esta entidad se describe como un objeto matemático con ciertas propiedades específicas, tiene una realidad física, la cual se representa a través de un sistema cuántico de dos estados, pero en el cual todo su tratamiento es enteramente abstracto, dando libertad de generar una teoría general de la computación e información que no depende del sistema físico que se emplee para su implementación. Al considerar sistemas de esta clase como mínimas unidades de información, es necesario para su correcta descripción, implementar el formalismo matemático de la mecánica cuántica.

Existen varios esquemas que describen los estados de un sistema cuántico [8,9], siendo el más conveniente y conciso el descrito por la notación Dirac [9], la cual se ha convertido en un estándar en la física moderna. En este modelo, un estado cuántico es representado por un vector, denotado por  $|\rangle$  denominado ket y las operaciones sobre estos se realizan a través de operadores que son transformaciones lineales que actúan sobre el ket.

Los dos estados base posibles para un qubit son  $|0\rangle$  y  $|1\rangle$ , que corresponden en analogía al 0 y 1 de un bit clásico. La potencialidad de este esquema radica en que el qubit puede tomar otro valor diferente a los dos antes mencionados, debido a la combinación lineal de estados, por lo cual un qubit en su forma más general está representado de la forma:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle, \quad (1)$$

donde  $a_0$  y  $a_1$  son números complejos que satisfacen la relación de normalización  $|a_0|^2 + |a_1|^2 = 1$  y los kets  $|0\rangle$  y  $|1\rangle$  se representan por los vectores columna

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (2)$$

La habilidad de un sistema cuántico de existir simultáneamente en una mezcla de todos los estados permitidos es conocida como "Principio de Superposición" [2, 10–12] la cual es una característica completamente cuántica. Mientras en un sistema clásico el bit tiene una información concreta a la cual se puede

acceder sin perturbarla, el qubit siempre proporciona un resultado probabilístico y solo en aquellos casos en que  $a_0 = 0$  ó  $a_1 = 0$ , el estado del sistema permanece inalterado.

Consideremos ahora la situación en la cual hay más de un qubit, es decir, un registro de memoria cuántica. En tal situación, el espacio de estados es el resultado del producto tensorial de los espacios asociados a cada uno de los qubits. Si estos se representan por  $L_1^2$  y  $L_2^2$  de dimensiones  $n$  y  $m$  respectivamente, el nuevo espacio vectorial es  $L_{12}^2 = L_1^2 \otimes L_2^2$  de dimensión  $mn$  que a su vez es el número de elementos de la base. Tomando el caso particular de un sistema de registro cuántico de dos qubits ( $2-qubits$ ) en el cual la dimensión del espacio es  $2^2 = 4$ , su base natural esta constituida por 4 vectores. El qubit  $|\psi\rangle$  se describe de acuerdo a la superposición coherente

$$|\psi\rangle = a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |10\rangle + a_{11} |11\rangle, \quad (3)$$

donde  $a_{mn(ij)}$  es un número complejo. Para un sistema de  $N$  qubits, la base consta de  $2^N$  elementos de estados accesibles. En forma más general, tomando cada uno de los elementos de la base mediante el ket  $|x\rangle$  con  $x = 0, 1, 2, 3, \dots, 2^N - 1$ , el qubit se puede representar así

$$|\psi\rangle = \sum_{x=0}^{2^N-1} a_x |x\rangle \quad (4)$$

No es correcto tratar de dar una interpretación al qubit desde un punto de vista probabilístico de la teoría clásica de la computación, debido a que esa aparente complejidad en la descripción de estos sistemas es la encargada de presentar las mayores ventajas con respecto al modelo clásico.

En el estado cuántico que se describe por las ecuaciones (1) y (4), no solamente hay una combinación probabilística de cada estado, si no que adicionalmente se incorporan los efectos de interferencia y entrelazamiento, los cuales permiten realizar un masivo procesamiento de información que finalmente se traduce en un aumento exponencial en la velocidad de cálculo con respecto a los dispositivos clásicos.

## 3. Mediciones Cuánticas

A diferencia de las medidas realizadas a elementos macroscópicos en los cuales tales procesos arrojan una cantidad absoluta, en los sistemas microscópicos el proceso de medida de sus estados genera probabilidades de encontrarlo en cierta configuración. Inmediatamente después de ser realizada la medición, la mecánica

cuántica predice que el sistema evoluciona a otro estado normalizado. Para aclarar y enfatizar estas ideas es necesario retomar la ecuación (4) con su base natural  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ . Supongamos que se desea medir cuando el sistema se encuentra en cierto estado  $|\phi_n^m\rangle = \hat{A}|\psi\rangle$ , esto solo es posible determinando la probabilidad de encontrar el autovalor  $a_n$  de  $\hat{A}$  asociado a este estado, la cual esta dada por:

$$P_{a_n} = \sum_{m=1}^{g_n} |\langle \phi_n^m | \psi \rangle|^2, \quad (5)$$

donde  $g_n$  es el índice de degenerancia del autovalor  $a_n$ . Cuando el 2-qubit dado en la ecuación (3) es medido con respecto a la base, la probabilidad de encontrar un estado  $|0\rangle$  en el primer qubit del 2-qubit es:

$$P_{1|0} = |a_{00}|^2 + |a_{01}|^2, \quad (6)$$

de forma análoga, la probabilidad de encontrar un estado  $|1\rangle$  en el primer qubit del 2-qubit es:

$$P_{1|1} = |a_{10}|^2 + |a_{11}|^2. \quad (7)$$

Igualmente, para el segundo qubit es posible determinar la probabilidad de encontrar los estados  $|0\rangle$  y un  $|1\rangle$  en el 2-qubit, estan representadas por

$$P_{2|0} = |a_{00}|^2 + |a_{10}|^2, \quad P_{2|1} = |a_{01}|^2 + |a_{11}|^2. \quad (8)$$

Si el primer qubit esta en  $|1\rangle$ , el 2-qubit evoluciona al estado

$$|\psi^*\rangle = \frac{a_{10}|10\rangle + a_{11}|11\rangle}{\sqrt{|a_{10}|^2 + |a_{11}|^2}} \quad (9)$$

Si por el contrario, el primer qubit esta en  $|0\rangle$ , el 2-qubit evoluciona a un nuevo estado representado por

$$|\psi^*\rangle = \frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}} \quad (10)$$

Expresiones similares a las anteriores pueden ser determinadas para la medida del segundo qubit del 2-qubit, donde claramente queda representado el carácter probabilístico de estas entidades.

#### 4. Paralelismo Cuántico

La característica que convierte a la computación cuántica en una de las áreas más prometedoras, es el poder solventar en menor tiempo problemas intratables por la computación clásica, realizando para ello un procesamiento de información en paralelo de manera masiva. Esta idea, presentada por David Deutsch [6] en

1985 se esquematiza de la siguiente forma: Supóngase que se posee un computador cuántico que puede hacer evolucionar dos qubits cualesquiera según el operador unitario  $\hat{U}$  cuya transformación esta representada por

$$\hat{U} : |x\rangle |y\rangle \rightarrow |x\rangle |y \oplus f(x)\rangle. \quad (11)$$

Este operador cambia el segundo qubit  $|y\rangle$  a cero si  $f$  actuando en el primer qubit  $|x\rangle$  es 1 y no si  $f$  es 0<sup>1</sup>. Tomando  $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  se tiene

$$\begin{aligned} \hat{U} : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &\rightarrow |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \end{aligned} \quad (12)$$

donde se ha aislado la función  $f$  en una fase dependiente de  $x$ . Si  $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  y  $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  se comprueba de inmediato que

$$\begin{aligned} \hat{U} : \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &\rightarrow \\ \frac{1}{\sqrt{2}} \left[ (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right] \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \quad (13)$$

De esta manera, con solo realizar una proyección ortogonal del primer qubit en una base  $\{|+\rangle, |-\rangle\}$ , donde

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad (14)$$

ya se ha resuelto con una única computación el problema planteado en la ecuación (11). Esto es posible debido que al utilizar un dispositivo cuántico, este no se limita a evaluar  $f(0)$  ó  $f(1)$ , por el contrario, actúa sobre una superposición de los estados  $|0\rangle$  y  $|1\rangle$  permitiendo extraer información global de la función, es decir, información que depende de la combinación entre  $f(0)$  y  $f(1)$ . Esto es el paralelismo cuántico.

De igual manera, se puede utilizar el procesamiento en paralelo para conocer algunas propiedades de funciones más complejas. Así, si se desea calcular, para todas las posibles combinaciones de un conjunto de  $N$  bits, el valor de una función cualquiera  $f$ , un computador clásico necesitaría realizar  $2^N$  evaluaciones de la función. Sin embargo, utilizando uno cuántico, solamente se precisa efectuar, sobre un conjunto de  $N$  qubits, una transformación dada por el operador unitario  $\hat{U}_r$  tal que

$$\hat{U}_r : |x\rangle |0\rangle \rightarrow |x\rangle |f(x)\rangle, \quad (15)$$

<sup>1</sup> La operación  $\oplus$  denota la adición binaria o en modulo 2, la cual esta definida por  $0 \oplus 0 = 0$ ,  $0 \oplus 1 = 1$ ,  $1 \oplus 0 = 1$  y  $1 \oplus 1 = 0$

eligiendo que todos los registros de entrada se encuentren en el estado  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ , el estado del conjunto sería

$$\overbrace{\left[ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right] \otimes \cdots \otimes \left[ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right]}^N = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle, \quad (16)$$

el cual representa el producto tensorial de los  $N$  estados de entrada. Al aplicar sobre la ecuación (16) el operador  $\hat{U}_r$  se tiene

$$\frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle |f(x)\rangle, \quad (17)$$

y finalmente este estado recoge todas las propiedades globales de la función  $f$ .

## 5. Circuitos Cuánticos

### 5.1. Operadores Unitarios

Consideremos el comportamiento de sistemas cuánticos estáticos, es decir, sistemas que no cambian ni evolucionan a otro estado con el tiempo, pero que si lo hacen cuando un factor externo incide sobre ellos. Su dinámica esta descrita por la ecuación de Schrödinger y los cambios son debido a factores externos, expresados por transformaciones lineales u operadores representados por una matriz cuadrada, los cuales pueden tomarse estado a estado en un camino que preserve la ortogonalidad, siendo los operadores unitarios o transformaciones unitarias [2] los únicos elementos matemáticos que cumplen con este requisito. Para un conjunto de  $n$  sistemas cuánticos de 2 estados, el operador que actúa sobre este conjunto es una matriz de dimensión  $2^n \times 2^n$ . Por ejemplo, para un conjunto de dos sistemas cuánticos, sobre los cuales actúa un operador, se tiene

$$\begin{bmatrix} \alpha & \beta \\ \chi & \delta \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} \alpha a_0 + \beta a_1 \\ \chi a_0 + \delta a_1 \end{bmatrix}, \quad (18)$$

donde  $\hat{U} = \begin{bmatrix} \alpha & \beta \\ \chi & \delta \end{bmatrix}$ , es el operador evolución, el cual es unitario. Este tipo de operadores desempeñan un rol importante en el campo de la computación cuántica

ya que abren la posibilidad de crear esquemas de procesamiento de información reversibles.

### 5.2. Compuertas Cuánticas

Una compuerta cuántica es una función que realiza un operador unitario en un conjunto de qubits seleccionados en un cierto periodo de tiempo [13]. Clasicamente, las compuertas lógicas constituyen un conjunto finito [14], pero en computación cuántica, el número de posibles transformaciones unitarias no lo es y en consecuencia, existen infinitas compuertas cuánticas. Es posible demostrar que cualquier transformación unitaria en un conjunto de  $n$  qubits puede realizarse mediante la aplicación sucesiva de tan sólo dos compuertas cuánticas: la asociada a la operación  $XOR$ , y la rotación,  $\hat{R}(\theta, \phi)$  [13, 15–18].

El esquema más utilizado en computación cuántica, para representar una compuerta cuántica es el modelo circuital. Cada una de estas compuertas representan transformaciones y pueden actuar sobre un sistema cuántico. El repertorio de compuertas cuánticas reversibles está limitado a operadores unitarios, por lo cual es finito.

En las siguientes secciones presentamos el conjunto de compuertas cuánticas y circuitos cuánticos más relevante y su implementación en el computador cuántico de 5 qubits de IBM.

### 5.3. Compuertas de Pauli

Las matrices de Pauli representan el primer conjunto de compuertas cuánticas y están representadas por operadores unitarios hermiticos. Su representación en forma matricial y circuital es:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \text{---} \boxed{I} \text{---} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \text{---} \boxed{X} \text{---} \quad (19)$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \text{---} \boxed{Y} \text{---} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \text{---} \boxed{Z} \text{---} \quad (20)$$

La compuerta de  $X$  equivale en computación clásica a una compuerta de negación  $NOT$ . Su equivalente en la esfera de Bloch es una rotación alrededor del eje  $x$  en un ángulo de  $\pi$  radianes, tal como se presenta en la figura 1.

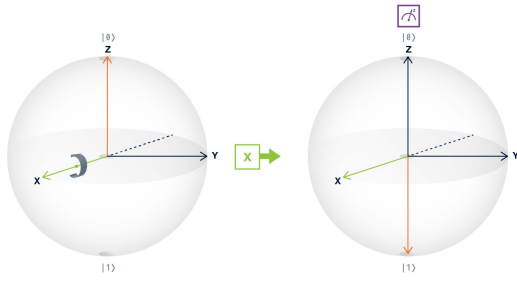


Figura 1. Representación de la acción de una compuerta de X (NOT) en un qubit [19].

Al actuar esta compuerta sobre el estado  $|0\rangle$  se mapea a  $|1\rangle$  y cuando actúa en  $|1\rangle$  lo convierte en el estado  $|0\rangle$ .

La compuerta de Y realiza una rotación de  $\pi$  radianes al estado cuántico respecto al eje  $y$  en la esfera de Bloch. El estado  $|0\rangle$  mapea a  $i|1\rangle$  y  $|1\rangle$  mapea a  $-i|0\rangle$ .

La compuerta de Z realiza una rotación de  $\pi$  radianes al estado cuántico respecto al eje  $z$ . El estado  $|0\rangle$  no cambia, mientras que el  $|1\rangle$  mapea a  $-|1\rangle$ . En la figura 2 se visualiza su representación en la esfera de Bloch.

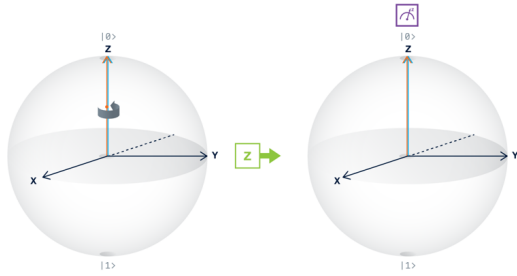


Figura 2. Representación de la acción de una compuerta de Z en un qubit [19].

#### 5.4. Compuerta $\sqrt{NOT}$

A diferencia de las compuertas de Pauli, la compuerta  $\sqrt{NOT}$  no tiene una contraparte clásica, pero se puede considerar que esta es una fracción de la compuerta NOT. Su representación matricial y circuital es:

$$\sqrt{NOT} = \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = -\boxed{\sqrt{\neg}} \quad (21)$$

Al aplicar de forma simultánea esta compuerta dos veces, se obtiene la compuerta NOT

$$\begin{aligned} \sqrt{NOT}\sqrt{NOT} &= \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \\ \sqrt{NOT}\sqrt{NOT} &= NOT = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (22) \end{aligned}$$

#### 5.5. Compuerta cambio de fase

La compuerta cambio de fase no realiza ningún cambio en el estado  $|0\rangle$ , pero  $|1\rangle$  mapea a  $e^{-i\theta}|1\rangle$ . En forma general, esta compuerta cambia la fase del estado cuántico. Su representación circuital y matricial es:

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} = -\boxed{R_\theta} \quad (23)$$

$R_\theta$  realiza una rotación en un ángulo  $\theta$  en la dirección contraria a las manecillas del reloj, sobre el eje  $z$  en su representación en la esfera de Bloch.

#### 5.6. Compuerta Hadamard

Esta compuerta es ampliamente utilizada en la construcción de circuitos cuánticos y esta definida por el operador

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = -\boxed{H} \quad (24)$$

Una característica relevante de esta compuerta es que  $H^2 = I$  y  $H^{-1} = H$ . Cualquier operación unitaria sobre un solo qubit puede ser construida únicamente a partir de las compuertas de Hadamard y la compuerta de corrimiento de fase. Toda transformación unitaria mueve el estado de un qubit de un punto sobre la esfera de Bloch a otro punto de la misma. Esta compuerta juega un rol fundamental en la construcción de algoritmos cuánticos ya que permite crear una superposición de estados. Al actuar sobre el estado  $|0\rangle$ , se tiene:

$$|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (25)$$

Su representación en la esfera de Bloch se presenta en la figura 3.

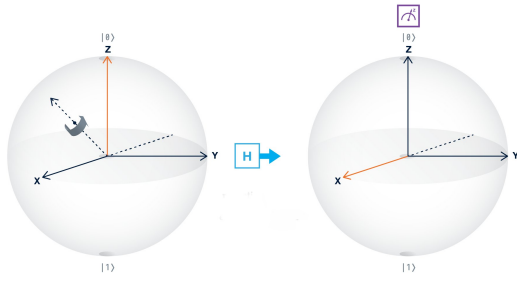


Figura 3. Representación de la acción de la compuerta Hadamar en el qubit  $|0\rangle$  [19].

Si la compuerta actúa sobre el estado  $|1\rangle$ , es necesario aplicar una compuerta de negación  $X$  al estado  $|0\rangle$  y posteriormente aplicar la compuerta hadamar, por lo tanto:

$$|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (26)$$

Su representación en la esfera de Bloch se describe en la figura 4.

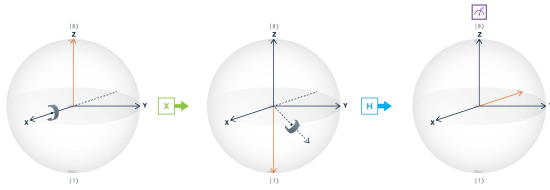


Figura 4. Representación de la acción de la compuerta Hadamar en el qubit  $|1\rangle$  [19].

### 5.7. Entrelazamiento

El entrelazamiento ó entanglement constituye probablemente el elemento clave que determina la gran diferencia entre las teorías cuántica y clásica de la información y en esta propiedad están basadas las compuertas cuánticas de 2-qubits. Considerando un sistema cuántico compuesto por dos subsistemas idénticos  $A$  y  $B$ , cuyos espacios de estados respectivos,  $L_1^2$  y  $L_2^2$ , se consideran bidimensionales. Si se supone que las bases de  $L_1^2$  y  $L_2^2$  están formadas por los kets  $|0\rangle$  y  $|1\rangle$  el espacio de estados del sistema compuesto,  $L_{12}^2 = L_1^2 \otimes L_2^2$ , tendrá como base natural el conjunto  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ . Sin embargo, no todos los estados pertenecientes a  $L_{12}^2$  tienen una interpretación física clara; así, mientras que, por ejemplo, en  $|01\rangle$  es evidente que  $A$  se encuentra en  $|0\rangle$  y  $B$  en  $|1\rangle$ , otras

situaciones, como la superposición  $1/2(|00\rangle + |01\rangle)$ , son más difíciles de interpretar, pues, aunque en este caso el estado de  $A$  es  $|0\rangle$ , el de  $B$  es una superposición de  $|0\rangle$  y  $|1\rangle$ . Finalmente, se pueden considerar ejemplos en los que no es posible asociar un estado cuántico a ninguno de los dos subsistemas de manera independiente: tal circunstancia se da, por ejemplo, en  $|\psi\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ . Este último tipo de estado, en el que no es posible una factorización de la forma  $|\psi_A\rangle \otimes |\psi_B\rangle$ , se denomina entrelazamiento.

Este tipo de estados tienen la característica de que si se realiza una media “local” en cualquiera de los dos subsistemas, no se adquiere ninguna información, es decir, el resultado es totalmente aleatorio (el estado se dice completamente mixto). La consecuencia inmediata de este hecho es que no se puede crear esta clase de estados mediante transformaciones realizadas por operadores unitarios del tipo  $U_A \otimes U_B$ ; la única manera de entrelazar dos sistemas es permitir que interactúen entre ellos.

Albert Einstein, Boris Podolsky y Nathan Rosen [20] fueron los primeros en percatarse de las consecuencias de la existencia de estos estados; pero, pareciéndoles del todo incompleta esta característica de “no localidad” de la Mecánica Cuántica, propusieron una teoría local de variables ocultas. Tres décadas más tarde, John Bell [21–23] consiguió probar que, mediante esquemas que supusiesen un comportamiento local de ambos subsistemas, es imposible imitar las correlaciones existentes entre los resultados obtenidos en la medida de dos subsistemas entrelazados. Los experimentos de Alan Aspect y su grupo [24–26] confirmaron las predicciones de la teoría cuántica y demostraron, por tanto, que el comportamiento de la naturaleza es “no local”.

### 5.8. Compuerta CNOT

Esta compuerta permite generar entrelazamiento entre qubits. A diferencia de las anteriores compuertas, esta actúa sobre un sistema 2-qubits, con una base de la forma  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ . La acción de la compuerta  $CNOT$  sobre un qubit genérico se representa como:

$$CNOT(|x, y\rangle) = |x, x \oplus y\rangle, \quad (27)$$

donde  $\oplus$  indica la adición modulo 2. La representación matricial y circuital de esta compuerta se presenta a continuación:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \text{---} \bullet \text{---} \oplus \text{---} \quad (28)$$

## 6. IBM Quantum Experience

En el mes de mayo de 2016, IBM anunció el lanzamiento de IBM Q [19], su primera computadora cuántica de 5 qubits de acceso libre a cualquier persona experta o no en el tema. Este puede ser considerado el primer paso hacia una masificación de la computación cuántica a través de la nube.



Figura 5. Hardware de la computadora cuántica QIBM [19].

Un año después, en mayo de 2017 [19], IBM anunció la introducción de dos nuevos procesadores en su computadora cuántica: uno de 16 qubit que permitirá realizar experimentos de mayor complejidad que en el procesador de 5 qubit disponible anteriormente. Aunque es de uso libre, el acceso Beta está disponible por solicitud a través de la plataforma de IBM Q. Su uso está enfocado a desarrolladores, programadores e investigadores, quienes buscan ejecutar algoritmos

cuánticos de mayor complejidad. El segundo es el prototipo de un procesador cuántico comercial de 17 qubits, diseñado con una arquitectura que garantice una potencia igual al doble de la disponible en la nube con acceso al público en la actualidad.

### 6.1. Computadora QX 2

Esta es una computadora cuántica que opera con un procesador QX2 de 5 qubits superconductores (fig 5), inmersa en un refrigerador de dilución. Esta localizada en los cuarteles generales de IBM, en el Thomas J. Watson Research Center, Yorktown Heights, New York y se puede acceder a su servicio en la nube desde la web <https://www.research.ibm.com/ibm-q/>. A diferencia de proyectos similares, el acceso que provee IBM a su computadora es libre y para todo el público.

El procesador cuántico de IBM se basa en una red cuadrada de cinco qubits superconductores en un chip, como se presenta en la figura 6. Los qubits 0,1,3 y 4 se encuentran acoplados al qubit 2. Al realizar una operación con compuertas cuánticas de 2-qubits, estas involucran al qubit 2 de este circuito. De igual forma, en la compuerta CNOT, el qubit 2 actúa como target.

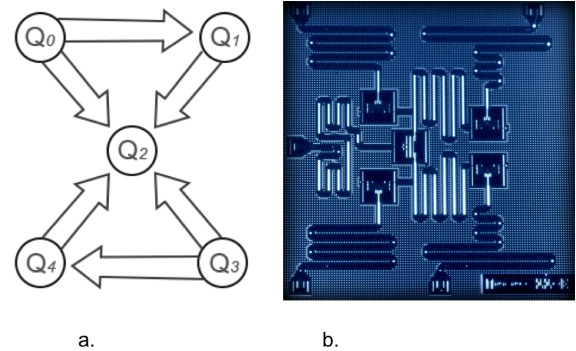


Figura 6. a. Arquitectura de conexiones y b. procesador cuántico de 5-qubits superconductores, disponible en la computadora cuántica de IBM [19].

Toda operación en un computador cuántico, se ve afectada por errores pueden ocurrir en los estados de superposición del qubit. Uno de ellos se denomina error de inversión del bit, que simplemente invierte un qubit del estado  $|0\rangle$  al estado  $|1\rangle$  y viceversa. Esto es similar a los errores clásicos de bit-flip. Para llevar a cabo una corrección de errores cuánticos, es necesario considerar adicionalmente los errores de cambio de fase (phase-flip), los cuales invierten el signo de la relación de fase entre  $|0\rangle$  y  $|1\rangle$  en un estado de superposición. La geometría cuadrada del circuito propuesto por IBM,



permite detectar de forma simultanea estos errores [27]. En este circuito fue posible implementar protocolos de corrección de errores, permitiendo que esta arquitectura

sea físicamente escalable a un sistema con un mayor número de qubits.



Figura 7. Interfaz gráfica del IBM Q denominada Quantum composer, sobre la cual es posible crear circuitos cuánticos utilizando una librería de compuertas lógicas y puntos de medición preestablecidos.

La interfaz de trabajo de esta computadora es llamada *IBM Q experience* [28] y ofrece una programación gráfica, empleando la representación circuital. La figura 7 muestra el Quantum Composer, que es la interfaz gráfica sobre la cual se construye el circuito cuántico a estudiar.

Las mediciones posibles que ofrece el computador cuántico son dos: La representación en la esfera de Bloch y la medición estándar Z. En la primera, se indica el estado final del qubit al ser proyectado en X, Y y Z, el cual se representa como un vector al interior de una esfera, tal como se presenta en las figuras 1 y 2 para las compuertas X y Z. La segunda opción de medición es una proyección sobre el eje Z de la esfera de Bloch, la cual es representada como un gráfico de barras, indicando la probabilidad normalizada de que el

resultado colapse en un cierto estado cuántico.

## 7. Compuertas Cuánticas en IBMQ

En esta sección se presentan cada una de los distintos circuitos que permiten representar el comportamiento de distintas compuertas cuánticas y que pueden ser ejecutadas o simuladas por el computador cuántico de IBM.

### 7.1. Compuerta X

La implementación circuital de la compuerta cuántica X en el entorno del computador cuántico de 5 qubits se puede observar en la figura 8.

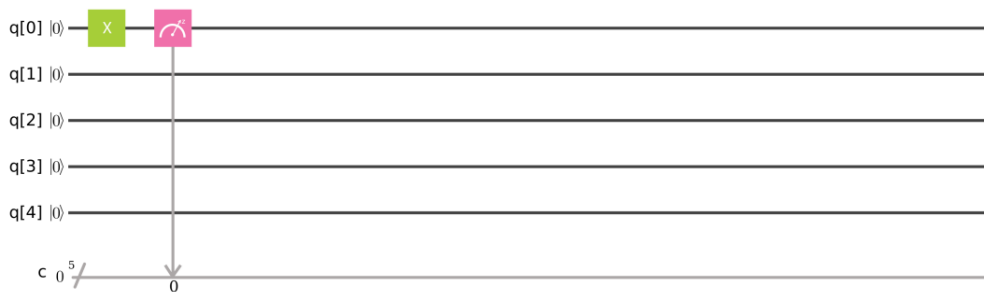


Figura 8. Representación circuital de la compuerta de negación X.



En las figuras 9 y 10 se presentan los resultados de la simulación y evaluación de esta compuerta en la medición estandar  $Z$ .

Al simular la compuerta, la probabilidad de obtener un cambio del estado  $|0\rangle$  a  $|1\rangle$  es de 100 % (normalizado a 1). Al ejecutar este circuito en el computador 1024

veces, en el 86.4 % el estado inicial de  $|0\rangle$  pasa a ser  $|1\rangle$ , mientras que en el 13.6 % el estado inicial de  $|1\rangle$  pasa a ser  $|0\rangle$ . En el computador cuántico de IBM, el qubit  $q[0]$  en el estado  $|0\rangle = |00000\rangle$ , mientras que el estado  $|1\rangle = |00001\rangle$ .

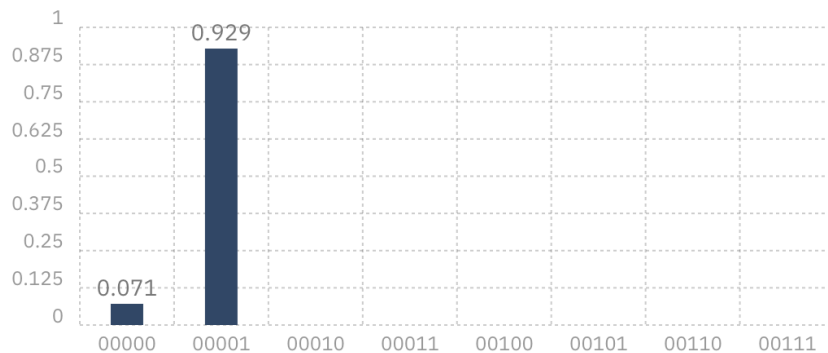


Figura 9. Resultado en la representación de la medición estandar  $Z$  al ejecutar el circuito de la compuerta de negación  $X$  1024 veces en el computador cuántico.

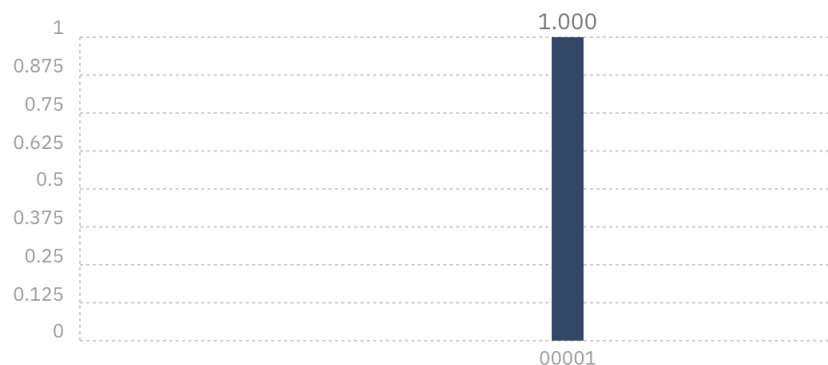


Figura 10. Resultado de la simulación de la medida en la representación estandar  $Z$  de la compuerta de negación  $X$  en el computador cuántico.

La aparente discrepancia entre el resultado experimental y el teórico radica en la naturaleza probabilista de las medidas en un sistema mecánico cuántico. El estado real cuantificado al realizar el experimento en el computador cuántico es la superposición de estos estados con la amplitud de probabilidad descrita en la figura 9.

## 7.2. Compuerta $Y$

La descripción circuital de la compuertas cuántica  $Y$  en el entorno composer se describe en la figura 11.

Los resultados de la evaluación y simulación de esta compuerta en la representación de medición estandar  $Z$  se presentan en las figuras 12 y 13.



Figura 11. Representación circuital de la compuerta de negación  $Y$ .

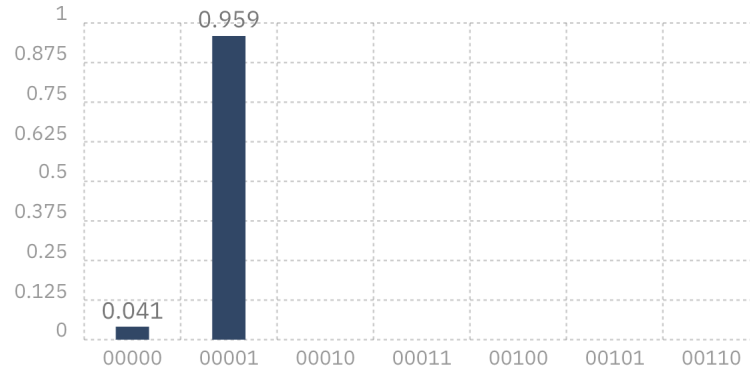


Figura 12. Resultado en la representación de la medición estándar  $Z$  al ejecutar el circuito de la compuerta de negación  $Y$  1024 veces en el computador cuántico.

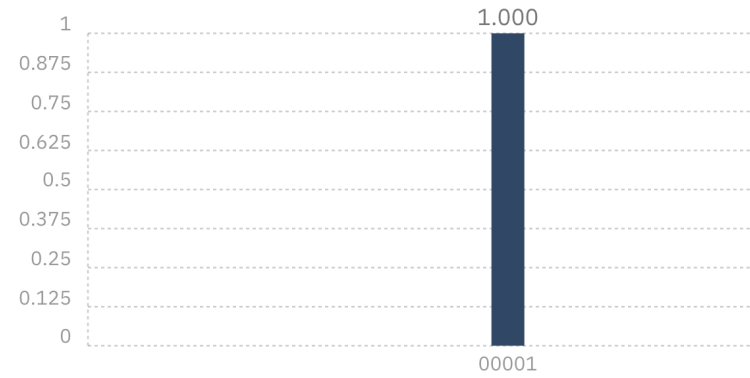


Figura 13. Resultado de la simulación de la medida en la representación estándar  $Z$  de la compuerta de negación  $Y$  en el computador cuántico.

### 7.3. Compuerta $Z$

La descripción circuital de la compuerta cuántica  $Z$  en el entorno composer se presenta en la figura 14.



Figura 14. Representación circuital de la compuerta de negación Z.

En las figuras 15 y 16 se presentan los resultados de la evaluación y simulación de esta compuerta en la representación de medición estandar Z.

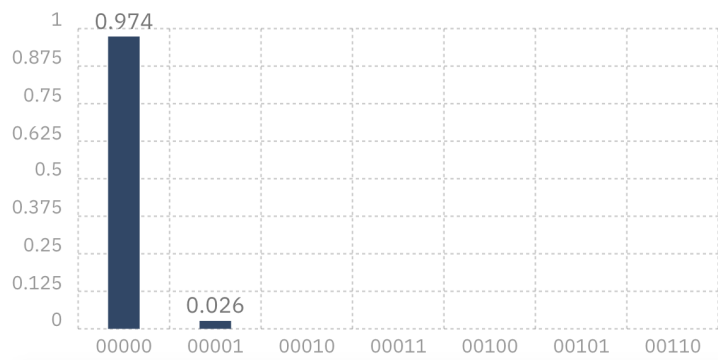


Figura 15. Resultado en la representación de la medición estandar Z al ejecutar el circuito de la compuerta de negación Z 1024 veces en el computador cuántico.

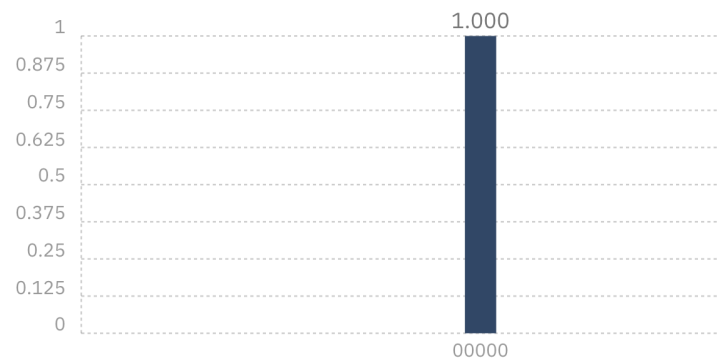


Figura 16. Resultado de la simulación de la medida en la representación estandar Z de la compuerta de negación Z en el computador cuántico.

#### 7.4. Compuerta Hadamar

Esta compuerta permite crear superposición de estados con pesos iguales. El nuevo estado se representa por un signo y queda determinado por el estado sobre

el cual actúa la compuerta Hadamar. El estado  $|+\rangle$  es el resultado de aplicar  $H|0\rangle$ , por lo tanto

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (29)$$

Su representación circuital se presenta en la figura 17

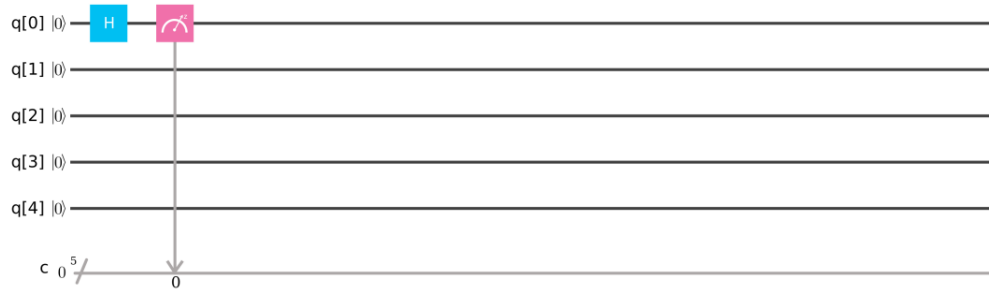


Figura 17. Implementación circuital de la compuerta Hadamar del estado (superior izquierda),  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ .

El estado  $|-\rangle$  queda representado como  $H|1\rangle$ , por lo tanto, el nuevo qubit es

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (30)$$

La representación circuital de esta compuerta se describe en la figura 22



Figura 18. Implementación circuital de la compuerta Hadamar del estado  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ .

#### 7.5. Compuerta CNOT

Para implementar la compuerta *CNOT*, es necesario considerar todas las posibles combinaciones de los

qubits de entrada, que para un sistemas de 2-bits son los estados  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ .

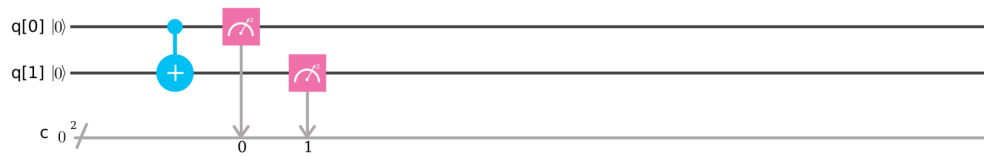


Figura 19. Implementación circuital de la compuerta  $CNOT$  en el estado  $|00\rangle$ .

En la figura 20 se presenta el circuito de la compuerta  $CNOT$  en el estado cuántico  $|01\rangle$

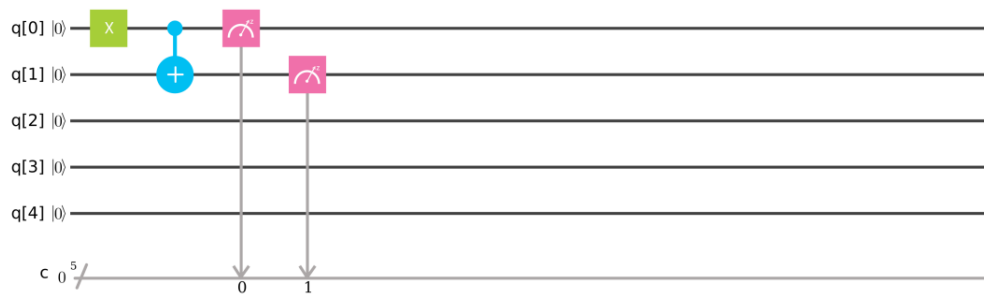


Figura 20. Implementación circuital de la compuerta  $CNOT$  en el estado  $|01\rangle$ .

En la figura 21 se presenta el circuito de la compuerta  $CNOT$  en el estado cuántico  $|10\rangle$ .

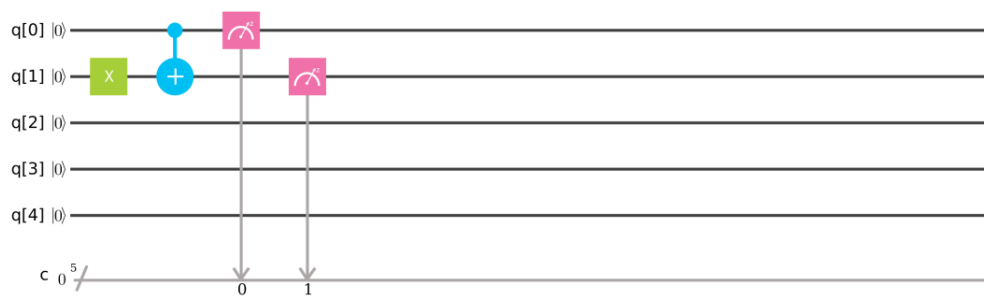


Figura 21. Implementación circuital de la compuerta  $CNOT$  en el estado  $|10\rangle$ .

En la figura 21 se presenta el circuito de la compuerta  $CNOT$  en el estado cuántico  $|11\rangle$ .

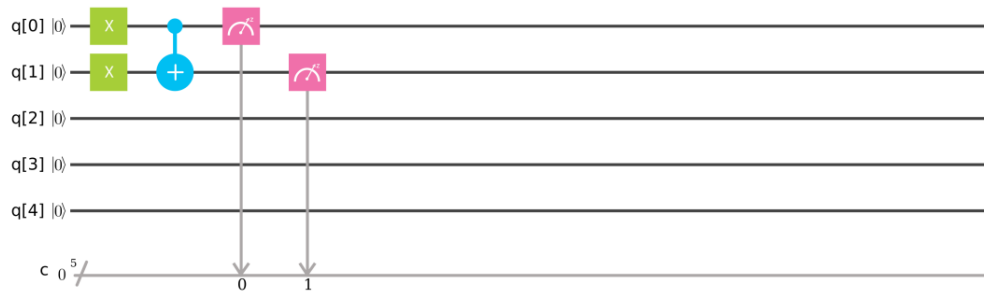


Figura 22. Implementación circuital de la compuerta  $CNOT$  en el estado  $|11\rangle$ .

En general, es necesario implementar un circuito para cada uno de los posibles estados cuánticos de entrada. A diferencia de los resultados obtenidos en un sistema clásico, en este tipo de ordenadores los resultados son distribuciones de probabilidad de posibles resultados en distintos escenarios.

## 8. Conclusiones

El avance en los procesos de miniaturización de los sistemas electrónicos, así como el procesamiento de la información está provocando la aparición de problemas relacionados con las limitaciones de trabajar a escala atómica en la que los efectos cuánticos tienen una gran relevancia. Al aplicar los modelos de la mecánica cuántica en la creación de un nuevo modelo de información se obtienen resultados que superan a los predichos por la teoría clásica de la información, conteniéndolos y siendo estos últimos un caso particular de los presentados en el modelo cuántico.

La computación cuántica es un nuevo y emergente campo de desarrollo que, tiene el potencial de cambiar dramáticamente el camino de como pensamos sobre computadores, programación y complejidad. Los desafíos que se presentan abarcan desde desarrollar nuevas técnicas de programación apropiadas para estos dispositivos hasta su implementación experimental en un sistema escalable.

Los modelos teóricos de la computación cuántica han logrado desarrollarse satisfactoriamente y en la actualidad tiene ampliamente definidos los fundamentos de las interacciones subatómicas, así como los esquemas del qubit, compuertas cuánticas, paralelismo cuántico, transporte y encriptación cuántica, sin embargo, no se ha logrado implementar hasta el momento un

computador cuántico totalmente operativo con una capacidad relevante de almacenamiento de información.

Una limitación en este esquema de procesamiento de información es visible en la implementación misma del dispositivo, en el cual se dificulta el manejo de sistemas de múltiples qubits donde sus interacciones afectan mutuamente sus estados. Otra requisito esta en las interacciones entre el sistema de medida y la partícula a medir, debido que no se puede realizar lectura sin producir cambios en el sistema, por lo que es necesario implementar complejos mecanismos de corrección de errores que agregan sobrecarga al procesamiento de información.

Con la creación de nuevos prototipos de estos computadores, como el desarrollado por IBM, se ha podido demostrar la funcionalidad de compuertas y algoritmos cuánticos de poca complejidad. La plataforma que ofrece el *IBM Q Experience* es una gran herramienta didáctica que permite aprender y aplicar los conceptos básicos de computación cuántica, mostrando las principales características de un computador cuántico, la forma en que se realiza su programación y la manera en que se interpretan los resultados.

## Referencias

- [1] H. E. Caicedo-Ortiz and E. Santiago-Cortés, "Overview of quantum computation," in *Theoretical and Computational Research in the 21st Century* (N. Islam, ed.), ch. 5, pp. 107–114, Toronto: Apple Academic Press, CRC Press, 2014.
- [2] N. Michael and t. Isaac, *Quantum Computation and Quantum Information*. Cambridge University Press, 1<sup>st</sup> ed., 2000.
- [3] E. G. Rieffel and W. H. Polak, *Quantum computing: A gentle introduction*. MIT Press, 2011.

- [4] C. P. Williams, *Explorations in quantum computing*. Texts in Computer Science, Springer, 2ed. ed., 2011.
- [5] R. Feynman, "Simulating physics with computer," *International Journal of Theoretical Physics*, vol. 21, no. 6/7, pp. 467–488, 1982.
- [6] D. Deutsch, "Quantum Theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London A*, vol. 400, no. 97, 1985.
- [7] W. Colin and C. Scott, *Explorations in Quantum Computing*. Springer-Verlag - TELOS, 1<sup>st</sup> ed., 1998.
- [8] R. Feynman and A. Hibbs, *Quantum Mechanics and Path Integrals*. McGraw-Hill, 1<sup>st</sup> ed., 1965.
- [9] P. Dirac, *Principios de Mecánica Cuántica*. Editorial Ariel, 1967.
- [10] W. Steeb, *Hilbert Spaces, Wavelets, Generalized Functions and Modern Quantum Mechanics, Mathematics and its applications*. Klumer Academics Publishers, 1<sup>st</sup> ed., 1998.
- [11] R. P. Feynman, R. B. Leighton, and M. Sands, *The Feynman Lectures on Physics, Desktop Edition Volume III*, vol. 3. Basic books, 2013.
- [12] C. Cohen-Tannoudji, B. Diu, and F. Laloe, *Quantum Mechanics Vol. I*. Hermann and John Wiley & Sons, 1<sup>st</sup> ed., 1977.
- [13] H. E. Caicedo-Ortiz and S. T. Pérez-Merchancano, "Simulación de un computador cuántico con óptica lineal," *Journal de Ciencia e Ingeniería*, vol. 1, no. 1, pp. 13–16, 2009.
- [14] P. Benioff, "Quantum mechanical hamiltonian models of turing machines," *J. Stat. Phys.*, vol. 29, p. 515, 1982.
- [15] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical review A*, vol. 52, no. 5, p. 3457, 1995.
- [16] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," *Phys. Rev. A.*, vol. 51, p. 1015, 1995.
- [17] A. Barenco, D. Deutsch, and E. Artur, "Universality in quantum computation," *Proceedings of the Royal Society of London A*, vol. 449, no. 1937, p. 669, 1995.
- [18] S. Lloyd, "Almost any quantum logic gate is universal," *Phys. Rev. Lett.*, vol. 75, no. 346-349, 1995.
- [19] C. Vu, "Ibm makes quantum computing available on ibm cloud to accelerate innovation." Accedido en 04-04-2016, <https://www-03.ibm.com/press/us/en/pressrelease/49661.wss>, 2016.
- [20] A. Podolsky, Boris; Einstein and R. Natan, "Can quantum mechanical description of physical reality be considered complete?," *Phys. Rev.*, vol. 47, p. 777, 1935.
- [21] J. S. Bell, "On the einstein-podolsky-rosen paradox," *Phys.*, vol. 1, p. 195, 1964.
- [22] J. S. Bell, "On the problem of hidden variables in quantum mechanics," *Rev. Mod. Phys.*, vol. 38, p. 447, 1966.
- [23] J. Colin, "Sherlock holmes investigates the epr paradox," *Physics World*, vol. 8, no. 4, p. 39, 1995.
- [24] t. Dalibard, J. and G. Roger., "Experimental test of bell's inequalities using timevarying analyzers," *Phys. Rev. Lett.*, vol. 49, p. 1804, 1982.
- [25] P. Grangier, A. Aspect, and G. Roger, "Experimental tests of realistic local theories via bell's theorem," *Phys. Rev. Lett.*, vol. 47, p. 460, 1981.
- [26] A. Aspect, "Testing bell's inequalities," *Europhys. News*, vol. 22, p. 73, 1991.
- [27] A. D. Córcoles, E. Magesan, S. J. Srinivasan, A. W. Cross, M. Steffen, J. M. Gambetta, and J. M. Chow, "Demonstration of a quantum error detection code using a square lattice of four superconducting qubits," *Nature communications*, vol. 6, 2015.
- [28] "Quantum experience: Ibm q." Accedido en 10-02-2017, <https://quantumexperience.ng.bluemix.net/qx/community>, 2017.