UNIVERSIDAD ABIERTA INTERAMERICANA
Facultad de Tecnología Informática



Carrera: Licenciatura en Matemática

Cálculo de logaritmos discretos en una computadora cuántica.

Autor: Ariel Savarese
Directora: Dra. Samira Abdel Masih

TESIS PRESENTADA PARA OPTAR AL TÍTULO DE LICENCIADO EN MATEMÁTICA

- Septiembre de 2020 –

Firmas del jurado

Agradecimientos

Esta tesis está dedicada a mi padre, Jose Juan Savarese, quien me enseñó que el mejor conocimiento que se puede tener es aquél que se aprende por sí mismo.

A mi madre, Marta Savarese, y Rosita, quienes con sus litros de café, cariño y paciencia me enseñaron que incluso la tarea más grande se puede lograr si se hace un paso a la vez.

A mi hermano Salvador, quien con su predisposición a ayudarme en otros temas permitió que me concentre en mi carrera.

A Andrea, Roberto y toda la Administración Portuaria Puerto Barranqueras, donde pude ver aplicados los temas que aprendí en el pizarrón del aula, creciendo junto a ellos.

A todos mis amigos, los que están cerca y los que viven en el exterior, que siempre entendieron mis tiempos y faltazos a encuentros o salidas, gracias infinitas por todo su apoyo y buena voluntad.

A mis compañeros de cursada, alumnos y ex alumnos, quienes siempre me ayudaron sin pedirme nada a cambio.

A la Universidad Abierta Interamericana y sus profesores, por ser la sede de todo el conocimiento adquirido en estos años. De igual forma agradezco especialmente a mi Directora de Tesis, Dra. Samira Abdel Masih, gracias a sus consejos y correcciones pude realizar este trabajo.

A Cintia, sin ella nada de esto hubiera sido posible.

Resumen

El presente trabajo desarrolla matemáticamente la publicación presentada por Peter Shor en 1995 ([1], págs. 19-24), donde propone un algoritmo cuántico para el cálculo de logaritmos discretos.
Dicho algoritmo, ideado para ser implementado en una computadora cuántica, es exponencialmente más rápido que cualquier algoritmo clásico conocido hasta ahora.
Pero ¿a qué se debe el interés en calcular eficientemente un logaritmo discreto?
Se debe a que numerosos criptosistemas utilizan los logaritmos discretos como técnica para garantizar la seguridad de la información transmitida por un determinado canal.
Así, muchas criptografías de clave pública, como por ejemplo el Protocolo de Intercambio de Diffie-Hellman, que se aplica para acordar una clave secreta entre dos máquinas, o el Algoritmo ElGamal, utilizado para autenticar firmas digitales, llegarían a ser obsoletas si el algoritmo propuesto por Shor fuera ejecutado en una computadora cuántica.
Es decir, que dicho algoritmo podría ser empleado para atacar las bases de seguridad en el tránsito de la información, reduciendo drásticamente el tiempo que se necesita para descubrir numerosas claves de seguridad informática.
Por otro lado, en este trabajo de tesis planteamos el desafío de mostrar al lector que la Algoritmia Cuántica, una ciencia que se encuentra en sus inicios, puede ser entendida sin dificultad aplicando conocimientos básicos de Números Complejos, Álgebra Lineal y Probabilidad. En este sentido, y para facilitar la comprensión de los temas, hemos desarrollado numerosos ejemplos que aclararán los conceptos y resultados obtenidos.

Palabras claves:

Logaritmos Discretos, Algoritmo de Shor, Computación Cuántica, Transformada Cuántica de Fourier.

Índice General

Contenido

INTRODUCCIÓN....7

ORIGEN DE LA COMPUTACIÓN CUÁNTICA....7
QUÉ ES Y CÓMO FUNCIONA UNA COMPUTADORA CUÁNTICA....8
LAS PRIMERAS COMPUTADORAS CUÁNTICAS....9

NOCIONES MATEMÁTICAS PREVIAS....10

1.1 LOS NÚMEROS COMPLEJOS....10
1.2 PRODUCTO INTERNO DE VECTORES....12
1.3 PRODUCTO TENSORIAL DE VECTORES....14
1.4 NOCIONES DE ARITMÉTICA MODULAR....16
1.5 POTENCIA MODULAR....21
1.6 ECUACIONES LINEALES DE CONGRUENCIA....24
1.7 GRUPOS, SUBGRUPOS Y GRUPOS CÍCLICOS....25
1.8 NOCIONES BÁSICAS DE PROBABILIDAD....29

LOGARITMOS DISCRETOS....37

2.1 ¿EXISTEN ALGORITMOS EFICIENTES PARA EL CÁLCULO DE UN LOGARITMO DISCRETO? 40
2.2 CÁLCULO DE LOGARITMOS DISCRETOS MEDIANTE WOLFRAM MATHEMATICA 10.0....40
2.3 LOS LOGARITMOS DISCRETOS APLICADOS A LA CRIPTOGRAFÍA....41

LOS QUBITS....46

3.1 SISTEMAS FORMADOS POR UN QUBIT....46
3.2 SISTEMAS FORMADOS POR VARIOS QUBITS....50
3.2.1 Sistemas formados por dos qubits....51
3.2.2 Sistemas formados por tres qubits....54
3.2.3 Sistemas formados por n qubits....57
3.2.4 Diferencias entre bits y qubits....63

COMPUERTAS, CIRCUITOS Y ALGORITMOS CUÁNTICOS....64

4.1 DEFINICIÓN Y CARACTERÍSTICAS DE UNA COMPUERTA CUÁNTICA....64
4.2 CIRCUITOS CUÁNTICOS....67
4.3 COMPUERTAS CUÁNTICAS DE UN QUBIT....68
4.3.1 La compuerta de Identidad....68
4.3.2 La compuerta de Hadamard....68
4.3.3 La compuerta R o de desplazamiento de fase....69
4.3.4 Representación gráfica del efecto de una compuerta cuántica sobre un qubit....72
4.4 COMPUERTAS CUÁNTICAS DE DOS QUBITS....76
4.4.1 La compuerta Swap....77
4.4.2 La compuerta Xor....77
4.5 ALGORITMOS CUÁNTICOS....84

LA TRANSFORMADA CUÁNTICA DE FOURIER....90

5.1 REPRESENTACIÓN MATRICIAL DE LA TRANSFORMADA CUÁNTICA DE FOURIER....92
5.2 DISEÑO DEL CIRCUITO CUÁNTICO PARA LA TRANSFORMADA CUÁNTICA DE FOURIER....94
5.3 CIRCUITO CUÁNTICO PARA LA TRANSFORMADA CUÁNTICA DE FOURIER....96
5.3.1 Circuito Cuántico de la QFT de 1-qubit....96
5.3.2 Circuito Cuántico de la QFT de 2-qubits....97
5.3.3 Circuito Cuántico de la QFT de 3-qubits....98
5.3.4 Circuito Cuántico de la QFT de n-qubits (caso general)....101

LA FUNCIÓN POTENCIA MODULAR Y SU COMPUERTA 104

ALGORITMO CUÁNTICO PARA EL CÁLCULO DE LOGARITMOS DISCRETOS.....114

7. 1 RESULTADOS MATEMÁTICOS PREVIOS.....115
7. 2 PARTE CUÁNTICA DEL ALGORITMO QUE CALCULA UN LOGARITMO DISCRETO.....122
7.3. NOCIÓN DE UN BUEN PAR (c, d) 127
7. 3 PARTE CLÁSICA DEL ALGORITMO QUE CALCULA UN LOGARITMO DISCRETO 141
7.3.1 IMPLEMENTACIÓN DE LA PARTE CLÁSICA DEL ALGORITMO CUÁNTICO MEDIANTE WOLFRAM MATHEMATICA 10.0 147

CONCLUSIONES.....149

REFERENCIAS 150

Introducción

La Computación Cuántica, también llamada Informática Cuántica, es un paradigma de Computación que utiliza como unidad de almacenamiento de datos los qubits, en lugar de bits.
A diferencia del bit, que puede estar en estado *0* o bien en estado *1*, el qubit puede estar en ambos estados al mismo tiempo. Esta propiedad otorga a la Computación Cuántica un mayor potencial para implementar algoritmos mucho más eficientes que los ejecutados por un ordenador convencional.

Origen de la Computación Cuántica

El avance acelerado de la Computación en las últimas décadas está ligado al uso de transistores con microchips cada vez más pequeños, que producen mayor velocidad de procesamiento.
Sin embargo, no se pueden fabricar microchips tan pequeños como se quisiera, ya que existe un límite después del cual dejan de funcionar correctamente. Ello se debe a que cuando se llega a la escala de nanómetros, algunos electrones se escapan de los canales por donde deben circular, ya que pueden atravesar las paredes si éstas son lo suficientemente delgadas. De este modo la señal transitaría por conductos erróneos, provocando una pérdida de información.
Es así como surge la necesidad de descubrir nuevas tecnologías basadas en las leyes de la Mecánica Cuántica.
La idea de la Computación Cuántica surgió en 1981, cuando Richard Feynman (1918-1988), Premio Nobel de Física en 1965, presentó una ponencia en la que proponía el uso de fenómenos cuánticos para realizar cálculos computacionales. Él afirmaba que algunos cálculos de gran complejidad se realizarían más rápidamente en un ordenador cuántico.



Richard Feynman.
Fuente: https://flagellum.wordpress.com/2018/05/11/richard-feynman

En la década de los 90 esta teoría comenzó a plasmarse: aparecieron los primeros algoritmos cuánticos y las primeras máquinas capaces de realizar cálculos cuánticos.

Este nuevo paradigma llegó a su auge en 1995, cuando Peter Shor (1959-), un científico estadounidense, desarrolló un algoritmo que lleva su nombre. Dicho algoritmo permite calcular logaritmos discretos y hallar los factores primos de números enteros en una computadora cuántica, a una velocidad considerablemente mayor que la de cualquier ordenador tradicional.

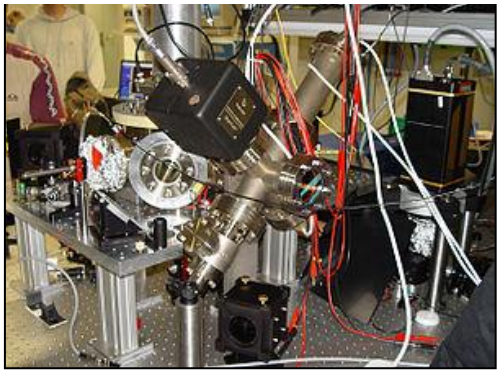


Peter Shor.
Fuente: ews.mit.edu/2019/mit-professor-peter-shor

Su algoritmo causó alto impacto, ya que podría romper muchos de los sistemas criptográficos utilizados actualmente. Además, sirvió para demostrar a una gran parte de la comunidad científica que observaba incrédula las posibilidades de la Computación Cuántica, que se trataba de un campo de investigación de gran potencial.

Qué es y cómo funciona una computadora cuántica

La computadora cuántica es un dispositivo que utiliza los qubits como unidad mínima de almacenamiento de datos. Un qubit representa el estado de una partícula subatómica (electrón, protón, neutrón, fotón, etc.). Como veremos más detalladamente en el Capítulo *3*, el qubit puede estar en estado 0, en estado 1 o en ambos estados al mismo tiempo. Cuando esto último ocurre, se dice que el qubit está en *estado de superposición*. Gracias a esta propiedad, las computadoras cuánticas pueden procesar datos en forma paralela, a diferencia de los ordenadores actuales que lo hacen en forma secuencial. A mayor cantidad de qubits, más rápido funcionará un ordenador cuántico.
Por lo general, la tecnología que se utiliza para manipular los qubits es *una trampa de iones*, que es una combinación de campos eléctricos y magnéticos que captura iones en un tubo al vacío.

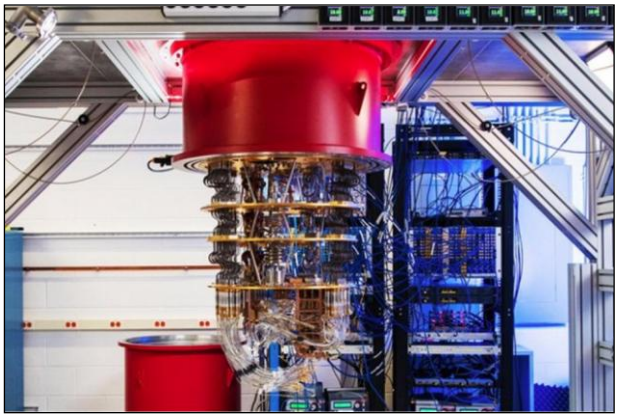


Trampa de iones en una computadora cuántica
Fuente: https://es.wikipedia.org/wiki/Trampa_i%C3%B3nica

Los ordenadores cuánticos no utilizan monitores, ni discos duros.
Todo sucede en la unidad de procesamiento que debe permanecer en unas condiciones de absoluto aislamiento, ya que los estados cuánticos de las partículas subatómicas son extremadamente frágiles y la superposición de los estados, que se produce durante los procesos de cálculo, puede perturbarse ante la más mínima vibración o fluctuación de la temperatura. Esta eventual alteración provocaría errores de cálculo.
Por esta razón, los procesadores en los que se encuentran los qubits se colocan dentro de un criostato (un gran termo de $3\ m^2$) para enfriarse y mantenerse cercanos al cero absoluto (- 273.15 grados Celcius).
Los estados de cada qubit se observan mediante un láser, de donde se extraen los resultados de los cálculos y se procesan en ordenadores normales.

Las primeras computadoras cuánticas

La primera computadora cuántica surgió en 1998 en la Universidad de Berkeley (California) y funcionaba con sólo un qubit.
Un año más tarde, en 1999, en los laboratorios de IBM-Almaden, se creó la primera máquina de *3* qubits.
A comienzos de 2019, IBM anunció el lanzamiento de IBM Q SYSTEM ONE, el primer ordenador cuántico comercial, que opera con *20* qubits.
Además, esta empresa habilitó una computadora cuántica de *5* qubits, a la que uno se puede conectar en forma gratuita y operar a distancia.
Por otro lado, otras empresas como Google y la NASA también están implementando prototipos con esta tecnología.



Computadora cuántica de Google
Fuente: https://www.pagina12.com.ar/227559-que-es-y-como-funciona-la-computadora-cuantica

En realidad, es muy poco probable que en un futuro próximo podamos disponer de ordenadores cuánticos en los hogares. Por el momento, el futuro de las computadoras cuánticas será el de ayudar a las clásicas en algunas tareas especializadas.

CAPÍTULO 1

Nociones matemáticas previas

En este capítulo desarrollaremos los principales conceptos matemáticos que aplicaremos a lo largo de este trabajo.

1.1 Los números complejos

Definición 1.1 : *Un número complejo* ***z*** *es una expresión de la forma*

$$z = a + i\,b$$

Donde a y b son números reales, $i = \sqrt{-1}$ *.En este caso,*

$a = Re(z)$ *(parte real de z)* $\qquad b = Im(z)$ *(parte imaginaria de z)*

Llamaremos $\mathbb{C}$ al conjunto de los números complejos, es decir,

$$\mathbb{C} = \{\, a + i\ b \ / \ a, b \in \mathbb{R} \,\}$$

Representación gráfica de los números complejos

Los números complejos se representan en el "Plano Complejo" del siguiente modo:

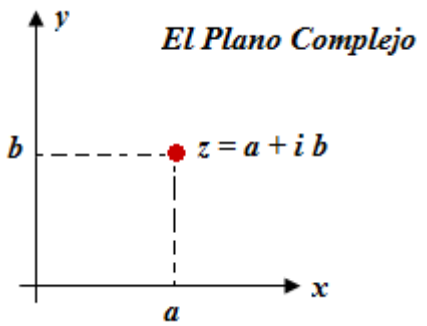


Figura 1.1: Representación gráfica de un número complejo

Otra representación posible de **z** en este plano es en forma de vector, con origen en el origen de coordenadas y extremo en el punto **z**.

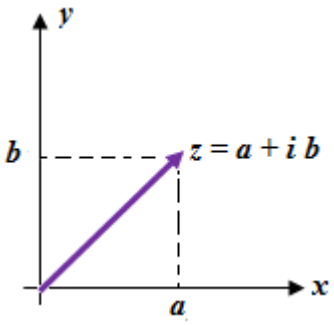


Figura 1.2: Representación vectorial de un número complejo.

Igualdad de números complejos

Dados dos números complejos $z_1 = a_1 + i\ b_1 \ \wedge\ z_2 = a_2 + i\ b_2$ entonces

$$z_1 = z_2 \ \Leftrightarrow a_1 = a_2 \ \wedge\ b_1 = b_2$$

Módulo o valor absoluto de un número complejo

Si ***z = a + i b*** , el módulo de ***z*** es

$$|\ z\ | = \sqrt{a^2 + b^2}\ .$$

Dicho número representa la distancia de ***z*** al origen de coordenadas.

El complejo conjugado

Si ***z = a + i b*** , el complejo conjugado de **z**, simbolizado por $\bar{z}$, es

$$\bar{z} = a - i\ b.$$

Forma exponencial de un número complejo.

Si ***z = a + i b*** es un complejo no nulo, podemos definir sus componentes usando coordenadas polares:

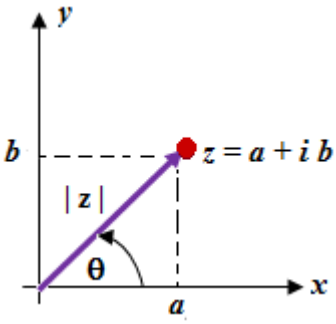


Figura 1.3: Representación de un número complejo aplicando coordenadas polares.

Donde

$|\ z\ | = \sqrt{a^2 + b^2}$

θ = ángulo, expresado en radianes, entre el vector de componentes (a, b) y el semieje x positivo, medido en sentido anti horario ($0 \le \theta < 2\pi$).

Por lo tanto, si $z \neq 0$ entonces

$$\begin{cases} cos\left(\theta\right)=\dfrac{a}{|z|} \\ sen\left(\theta\right)=\dfrac{b}{|z|} \end{cases} \Rightarrow \begin{cases} a=|z|\ cos\left(\theta\right) \\ b=|z|\ sen\left(\theta\right) \end{cases}$$

Luego, todo complejo no nulo puede expresarse como

$$z = a + i\,b = |z|\ cos\left(\theta\right)+i\ \ |z|\ sen\left(\theta\right)=|z|\ \left(cos\left(\theta\right)+i\ sen\left(\theta\right)\right).$$

Teniendo en cuenta la Fórmula de Euler:

$$e^{i\,\theta}=\left(cos\left(\theta\right)+i\ sen\left(\theta\right)\right)$$

Entonces podemos representar a un número complejo del siguiente modo:

Definición 1.2 : Forma exponencial de un número complejo

Dado un número complejo ***z = a + i b*** *, su representación en forma exponencial es*

$$z=|z|\ e^{i\,\theta}$$

Donde

$|z|=\sqrt{a^2+b^2}$

θ *= ángulo (en radianes) entre el vector de componentes (a, b) y el semieje x positivo.*

Igualdad de números complejos expresados en forma exponencial

Dados dos números complejos $z_1 \wedge z_2$ expresados en forma exponencial, es decir, $z_1=|z_1|\ e^{i\,\theta_1}\ \wedge\ z_2=|z_2|\ e^{i\,\theta_2}$ entonces

$$z_1=z_2\ \Leftrightarrow |z_1|=|z_2|\ \wedge\ \theta_1\ =\ \theta_2\ +2\,k\,\pi\ ,\ con\ k\in\mathbb{Z}$$

1.2 Producto interno de vectores

Definición 1.3: Producto interno de vectores

Sea **V** *un espacio vectorial sobre* $\mathbb{C}$*. Un "Producto interno" sobre* **V** *es una función que asigna, a cada par ordenado de vectores* (*v, w*)*, un escalar* $< v, w >$ *de* $\mathbb{C}$ *de modo tal que* $\forall\ v, w, u \in \mathbf{V}$ *y* $\forall\ \alpha \in \mathbb{C}$ *, se verifican las siguientes propiedades:*

1) $< v + w, u > = < v , u > + < w , u >$
2) $< \alpha\, v , w > = \alpha < v , w >$
3) $< v , w > = \overline{< w, v >}$ *donde la barra indica conjugación compleja.*
4) $< v , v > \geq 0\ \ \forall\ v \in \mathbf{V}$
5) $< v,\ v > > 0$ *si* $v \neq \mathbf{0}$ *y donde* **0** *representa el vector nulo.*

En lo que sigue supondremos que $\boldsymbol{V} = \mathbb{C}^n$ con $n \in \mathbb{N}$. En este espacio vectorial queda definido el producto interno canónico, como veremos a continuación:

Definición 1.4: Producto interno canónico

Sean $v, w \in \mathbb{C}^n$ *tales que* $v = (v_1, v_2, ..., v_n)^T$ *y* $w = (w_1, w_2, ..., w_n)^T$ *entonces el producto interno canónico es*

$$\langle v , w \rangle = \sum_{i=1}^{n} v_i \, . \overline{w}_i$$

Definición 1.5: Norma o módulo de un vector

Dado $v = (v_1, v_2, ..., v_n) \in \mathbb{C}^n$, *con el producto interno canónico. La norma o módulo de* v *es*

$$\| v \| = \sqrt{< v , v >} = \sqrt{\sum_{i=1}^{n} v_i \, . \overline{v}_i} = \sqrt{\sum_{i=1}^{n} | v_i |^2}$$

Teorema 1.6: Desigualdad de Cauchy-Schwarz

Sean $u = (u_1, u_2, ..., u_n)$, $v = (v_1, v_2, ..., v_n) \in \mathbb{C}^n$ *donde hay definido un producto interno. Entonces*

$$\left| \langle u , v \rangle \right|^2 \leq \langle u , u \rangle . \langle v , v \rangle$$

En particular, si el producto interno es el canónico entonces

$$\left| \sum_{i=1}^{n} u_i \, . \overline{v}_i \right|^2 \leq \sum_{i=1}^{n} | u_i |^2 . \sum_{i=1}^{n} | v_i |^2$$

Demostración

Véase Referencia [13]. ■

Ejemplo 1.7

Si $u = (u_1, u_2, ..., u_n) \in \mathbb{C}^n$, probar que $\left| \sum_{i=1}^{n} u_i \right|^2 \leq n \| u \|^2$

Solución

Aplicamos la desigualdad de Cauchy-Schwarz.
Para ello consideramos $v = (v_1, v_2, ..., v_n) = (1, 1, ..., 1)$. Por lo tanto

$$\left| \sum_{i=1}^{n} u_i \right|^2 = \left| \sum_{i=1}^{n} u_i .1 \right|^2 = \left| \sum_{i=1}^{n} u_i . \bar{1} \right|^2 \leq \sum_{i=1}^{n} |u_i|^2 . \sum_{i=1}^{n} |1|^2 = \sum_{i=1}^{n} |u_i|^2 . \sum_{i=1}^{n} 1 = \sum_{i=1}^{n} |u_i|^2 .n =$$

$$= \| u \|^2 .n$$

Por lo tanto $\left| \sum_{i=1}^{n} u_i \right|^2 \leq n \| u \|^2$.

1.3 Producto tensorial de vectores

Definición 1.8: Producto tensorial de vectores

Si $v = (v_1, v_2, ..., v_n) \in \mathbb{C}^n$ *y* $w = (w_1, w_2, ..., w_m) \in \mathbb{C}^m$ *entonces el producto tensorial* de *v con w , simbolizado por* $v \otimes w$ *es:*

$$v \otimes w = \begin{pmatrix} v_1 w \\ v_2 w \\ . \\ . \\ v_n w \end{pmatrix} = \begin{pmatrix} v_1 \begin{pmatrix} w_1 \\ w_2 \\ . \\ w_m \end{pmatrix} \\ v_2 \begin{pmatrix} w_1 \\ w_2 \\ . \\ w_m \end{pmatrix} \\ . \\ . \\ v_n \begin{pmatrix} w_1 \\ w_2 \\ . \\ w_m \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ . \\ v_1 w_m \end{pmatrix} \\ \begin{pmatrix} v_2 w_1 \\ v_2 w_2 \\ . \\ v_2 w_m \end{pmatrix} \\ . \\ . \\ \begin{pmatrix} v_n w_1 \\ v_n w_2 \\ . \\ v_n w_m \end{pmatrix} \end{pmatrix}$$

Claramente se puede verificar que el producto tensorial no es conmutativo. Es decir,

$$v \otimes w \neq w \otimes v$$

El siguiente ejemplo muestra cómo se calcula un producto tensorial.

Ejemplo 1.9

Si $v = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$ y $w = \begin{pmatrix} 3 \\ 5 \\ 4 \end{pmatrix}$, calcular $v \otimes w$ y $w \otimes v$.

Solución

$$v \otimes w = \begin{pmatrix} 2 \\ 5 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 5 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \begin{pmatrix} 3 \\ 5 \\ 4 \end{pmatrix} \\ 5 \begin{pmatrix} 3 \\ 5 \\ 4 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 6 \\ 10 \\ 8 \end{pmatrix} \\ \begin{pmatrix} 15 \\ 25 \\ 20 \end{pmatrix} \end{pmatrix}$$

Por otro lado,

$$w \otimes v = \begin{pmatrix} 3 \\ 5 \\ 4 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 \begin{pmatrix} 2 \\ 5 \end{pmatrix} \\ 5 \begin{pmatrix} 2 \\ 5 \end{pmatrix} \\ 4 \begin{pmatrix} 2 \\ 5 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 6 \\ 15 \end{pmatrix} \\ \begin{pmatrix} 10 \\ 25 \end{pmatrix} \\ \begin{pmatrix} 8 \\ 20 \end{pmatrix} \end{pmatrix}$$

Las propiedades básicas del producto tensorial se enumeran en la siguiente Proposición:

Proposición 1.10

1) Si $u \in \mathbb{C}^n$ *y* $v, w \in \mathbb{C}^m$ *entonces* $u \otimes (v + w) = (u \otimes v) + (u \otimes w)$

2) Si $u, v \in \mathbb{C}^n$ *y* $w \in \mathbb{C}^m$ *entonces* $(u + v) \otimes w = (u \otimes w) + (v \otimes w)$

3) Si $u \in \mathbb{C}^n$, $v \in \mathbb{C}^m$ *y* $\alpha \in \mathbb{C}$ *entonces*

$$(\alpha u) \otimes v = \alpha (u \otimes v)$$
$$u \otimes (\alpha v) = \alpha (u \otimes v)$$

4) Si $u \in \mathbb{C}^n$, $v \in \mathbb{C}^m$ *y* $\alpha > 0$ *entonces* $\alpha (u \otimes v) = (\sqrt{\alpha}\, u) \otimes (\sqrt{\alpha}\, v)$

Demostración

Véase Referencia [3], pág.16 ■

Observación 1.11

A fin de simplificar la notación, eliminaremos los paréntesis internos que figuran en el resultado de un producto tensorial.
Es decir, si $v = (v_1, v_2, \ldots, v_n)^T$ y $w = (w_1, w_2, \ldots, w_m)^T$ entonces

$$v \otimes w = \begin{pmatrix} \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ . \\ v_1 w_m \end{pmatrix} \\ \begin{pmatrix} v_2 w_1 \\ v_2 w_2 \\ . \\ v_2 w_m \end{pmatrix} \\ . \\ . \\ \begin{pmatrix} v_n w_1 \\ v_n w_2 \\ . \\ v_n w_m \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ . \\ v_1 w_m \\ v_2 w_1 \\ v_2 w_2 \\ . \\ v_2 w_m \\ . \\ . \\ v_n w_1 \\ v_n w_2 \\ . \\ v_n w_m \end{pmatrix}$$

De este modo, si $v \in \mathbb{C}^n$ y $w \in \mathbb{C}^m$ el producto tensorial $v \otimes w$ será identificado mediante un vector en $\mathbb{C}^{n.m}$.

Ejemplo 1.12

Si $v = \begin{pmatrix} 6i \\ 2 \end{pmatrix}$ y $w = \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}$ entonces

$$v \otimes w = \begin{pmatrix} 6i \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 6i \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} \\ 2 \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 18i \\ 24i \\ 30i \end{pmatrix} \\ \begin{pmatrix} 6 \\ 8 \\ 10 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 18i \\ 24i \\ 30i \\ 6 \\ 8 \\ 10 \end{pmatrix}$$

De este modo, $v \otimes w$ es identificado como un vector en $\mathbb{C}^6$.

1.4 Nociones de Aritmética Modular

La Aritmética Modular es la parte de la Aritmética que opera con números enteros, considerando el resto de la división de dichos números enteros por un número natural "*n*" fijo, llamado "*el módulo n*". Este concepto fue introducido por Carl F. Gauss (1777-1855), en su obra "*Disquisitiones Arithmeticae*", publicada en el año 1801. En esta sección daremos las nociones básicas de este tema, las cuales serán utilizadas a lo largo de este trabajo.

Definición 1.13: Divisibilidad

Sean $a,b \in \mathbb{Z}$ *con* $b \neq 0$ *Se dice que "b divide a a" y se escribe* $b \mid a$ *si* $a = k\ b$ *para algún* $k \in \mathbb{Z}$ *o equivalentemente, si al dividir a por b, el resto da 0.*

Definición 1.14: Máximo Común Divisor

Sean $a,b \in \mathbb{Z}$ *tales que no son simultáneamente nulos. Se dice que d es el máximo común divisor entre a y b, simbolizado por* $mcd\,(a,b)$*, si verifica:*

1) $d > 0$

2) $d \mid a \ \wedge\ d \mid b$

3) Si existe $c \in \mathbb{Z}$ *tal que* $c \mid a \ \wedge\ c \mid b \Rightarrow c \mid d$

Desde el punto de vista computacional, el Algoritmo de Euclides brinda una manera sencilla y eficiente de calcularlo (Véase Referencia [11]).

Definición 1.15: Congruencia

Dado un número natural n > 1 y dos números enteros a y b, se dice que a es congruente con b módulo n, y se escribe

$$a \equiv b \pmod{n}$$

Si

$$n \mid (a - b)$$

La siguiente Proposición enuncia las propiedades básicas de la congruencia:

Proposición 1.16

1) $a \equiv b \pmod{n} \ \Leftrightarrow$ *a y b tienen el mismo resto en la división entera por n.*
2) $a \equiv 0 \pmod{n} \ \Leftrightarrow\ n \mid a$
3) $a \equiv 0 \pmod{2} \ \Leftrightarrow$ *a es par.*
4) Si $a \equiv b \pmod{n} \ \wedge\ c \equiv d \pmod{n} \ \Rightarrow\ a\,c \equiv b\,d \pmod{n}$
5) Si $a \equiv b \pmod{n} \ \wedge\ c \equiv d \pmod{n} \ \Rightarrow\ a + c \equiv b + d \pmod{n}$
6) $a \equiv b \pmod{n} \ \wedge\ c \neq 0 \ \Rightarrow\ a\,c \equiv b\,c \pmod{n}$
7) $a \equiv b \pmod{n} \ \wedge\ k \in \mathbb{N} \ \Rightarrow\ a^k \equiv b^k \pmod{n}$
8) $a \equiv r_a \pmod{n}$ *donde* r_a *es el resto de la división entera de a por n.*
9) $a \equiv n + a \pmod{n}$

Demostración

Véase Referencia [11] ■

Definición 1.17: Suma modular

Sean $a, b \in \mathbb{Z}$ *y* $n \in \mathbb{N}$. *Entonces*

$a + b = c \pmod{n} \Leftrightarrow$ *c es el resto de dividir (a + b) por n.*

Definición 1.18: Suma "módulo 2"

Si n = 2 , la suma modular se la representa mediante el símbolo $\oplus$. *Es decir,*

$a \oplus b = c \Leftrightarrow$ *c es el resto de dividir (a + b) por 2.*

Definición 1.19: Producto modular

Sean $a, b \in \mathbb{Z}$ *y* $n \in \mathbb{N}$. *Entonces*

$a \cdot b = c \pmod{n} \Leftrightarrow$ *c es el resto de dividir (a . b) por n.*

Definición 1.20: Inverso multiplicativo modular

Dado $a \in \mathbb{Z}$ *y* $n \in \mathbb{N}$, *se dice que a tiene inverso multiplicativo (mod n) si* $\exists\, b \in \mathbb{Z}$ *tal que* $a.\, b \equiv 1 \pmod{n}$

De la Proposición 1.16 inciso 8), tenemos que si $a \in \mathbb{Z}$ y *n* es un natural mayor que 1, entonces $a \equiv r_a \pmod{n}$, donde r_a es el resto de la división entera de *a* por *n*. Esto permite clasificar a los números enteros según el resto de su división entera por *n*. De aquí surge la siguiente definición, teniendo en cuenta que los posibles restos de dicha división son $0, 1, \ldots, n-1$:

Definición 1.21: El conjunto $\mathbb{Z}_n$

Si n es un número natural mayor que 1, el conjunto $\mathbb{Z}_n$ *es*

$$\mathbb{Z}_n = \{\, 0\,,\ 1\,,\ 2\,, \ldots,\ n-1\ \}.$$

A dicho conjunto le definiremos ciertas operaciones, a fin de dotarlo de una estructura algebraica conveniente.

Definición 1.22: Suma y producto en $\mathbb{Z}_n$

Sean $a,\ b,\ c \in \mathbb{Z}_n$ *Entonces*

1) $a + b = c$ *en* $\mathbb{Z}_n \Leftrightarrow$ *c es el resto de la división entera de* $(a+b)$ *por n.*

2) $a.\, b = c$ *en* $\mathbb{Z}_n \Leftrightarrow$ *c es el resto de la división entera de* $(a.\, b)$ *por n.*

Definición 1.23: Elementos neutros para la suma y la multiplicación en $\mathbb{Z}_n$

1) El neutro para la suma es 0 pues $a+0 \equiv a \pmod{n}\ \forall a \in \mathbb{Z}_n$.

2) El neutro para el producto es 1 pues $a.1 \equiv a \pmod{n}\ \forall a \in \mathbb{Z}_n$.

Definición 1.24: El opuesto en $\mathbb{Z}_n$

Dado $a \in \mathbb{Z}_n$*, el opuesto de a es un número* $b \in \mathbb{Z}_n$ *tal que* $a + b = 0$ *en* $\mathbb{Z}_n$.

En este caso, el opuesto de a es $(n - a)$.

Definición 1.25: El inverso en $\mathbb{Z}_n$

Dado $a \in \mathbb{Z}_n$*, el inverso de a es un número* $b \in \mathbb{Z}_n$ *tal que* $a.b = 1$ *en* $\mathbb{Z}_n$.

Notación 1.26: al inverso de $a \in \mathbb{Z}_n$ lo simbolizaremos por a^{-1} , mientras que al opuesto de a lo representaremos por $-a$.

El siguiente teorema indica en qué casos un elemento de $\mathbb{Z}_n$ es invertible:

Teorema 1.27: Teorema de Invertibilidad en $\mathbb{Z}_n$

Un elemento $a \in \mathbb{Z}_n$ *es invertible* $\Leftrightarrow$ *mcd (a, n) = 1*

Donde $mcd(a,n)$ *es el máximo común divisor entre a y n.*

Demostración

Véase Referencia [4], pág. 21 ■

Corolario 1.28

Si n es primo entonces todo elemento no nulo de $\mathbb{Z}_n$ *es invertible.*

Demostración

Véase Referencia [4], pág. 22 ■

Ejemplo 1.29

Todo elemento de $\mathbb{Z}_{13}$ es invertible pues *13* es un número primo. Por otro lado, si *a=9* y *b= 11* entonces

a + b = 9 + 11 = 7 en $\mathbb{Z}_{13}$ pues el resto de dividir *a + b* por *13* es 7.

a. b = 9. (11) = 8 en $\mathbb{Z}_{13}$ pues el resto de dividir *a . b* por *13* es 8.

La siguiente proposición determinará cómo calcular el inverso de un elemento en $\mathbb{Z}_n$:

Proposición 1.30: Los inversos en $\mathbb{Z}_n$

Sea $a \in \mathbb{Z}_n$ *con* $a \neq 0$ *y tal que a es invertible en* $\mathbb{Z}_n$. *Entonces su inverso es*

$$a^{-1} = \frac{1 + n\ k}{a}$$

Para algún $k \in \mathbb{Z}$ *con* $0 \leq k \leq a$ *y tal que* $\frac{1 + n\ k}{a} \in \mathbb{Z}_n$.

Demostración

Véase Referencia [4], pág. 22 ■

Ejemplo 1.31

Calcular los siguientes inversos, en caso que existan, en el conjunto que se indica:

1) 5^{-1} en $\mathbb{Z}_{15}$

2) 7^{-1} en $\mathbb{Z}_{30}$

Solución

1) Como $mcd(5, 15) = 5 \neq 1$ por el Teorema 1.27 (Teorema de Invertibilidad) resulta que *5* no tiene inverso.

2) Como $mcd(7, 30) = 1$ entonces *7* tiene inverso en $\mathbb{Z}_{30}$. Por la Proposición 1.30,

$$7^{-1} = \frac{1 + 30k}{7}$$

Para algún $k \in \mathbb{Z}$ con $0 \leq k \leq 7$ y tal que $\frac{1 + 30k}{7} \in \mathbb{Z}_{30}$.

A fin de determinar cuál es el valor de *k*, diseñamos la siguiente tabla:

k	$\frac{\boldsymbol{1 + 30k}}{\boldsymbol{7}}$
0	$\frac{1}{7} \notin \mathbb{Z}_{30}$
1	$\frac{31}{7} \notin \mathbb{Z}_{30}$
2	$\frac{61}{7} \notin \mathbb{Z}_{30}$
3	$\frac{91}{7} = 13 \in \mathbb{Z}_{30}$

Luego, $7^{-1} = 13$ en $\mathbb{Z}_{30}$.

Ejemplo 1.32

Hallar los elementos invertibles en $\mathbb{Z}_4$.

Solución

Sea $a \in \mathbb{Z}_4$ invertible. Entonces, por el Teorema 1.27, $mcd\,(a\,,\,4) = 1$. Por lo tanto, el único elemento invertible es $a = 3$. Aplicando la Proposición *1.30*, resulta que $3^{-1} = 3$.

1.5 Potencia Modular

La potencia modular consiste en calcular

$$a^k \pmod n$$

Donde $k, a\,, n \in \mathbb{N}$.

Si "*a*" fuera un número entero muy grande y se intentara hallar $a^k \pmod n$ calculando primeramente a^k y luego efectuando su división entera por *n* para determinar el resto, resultaría bastante tedioso e ineficiente. Inclusive, si se hiciera este cálculo en un computador, se correría el riesgo de producirse *overflow* o *desbordamiento*. Este hecho ocurre cuando un cálculo con números enteros produce un resultado mayor a lo que puede almacenar el registro de un ordenador.
Por esta razón presentaremos el siguiente algoritmo que podrá ser implementado en una computadora clásica y que permitirá calcular $a^k \pmod n$ de un modo más sencillo y eficiente.

Algoritmo para el cálculo de la potencia modular

El procedimiento para calcular $a^k \pmod n$ se basa en el siguiente hecho:
Si se efectúa la división entera de k por *2*, se obtiene

$$k = 2\left[\frac{k}{2}\right] + r$$

Donde

$\left[\frac{k}{2}\right]$: Parte entera de $\frac{k}{2}$.

r : Resto de la división $(0 \le r \le 1)$.

En consecuencia,

$$a^k = a^{2\left[\frac{k}{2}\right]+r} = \left(a^2\right)^{\left[\frac{k}{2}\right]} . a^r$$

Esta expresión permite generar las siguientes sucesiones:

$\{a_0\ , a_1\ , a_2\ ,...\}$, $\{k_0\ , k_1\ , k_2\ ,...\}$, $\{c_0\ , c_1\ , c_2\ ,...\}$, $\{r_0\ , r_1\ , r_2\ ,...\}$

Donde

$$\begin{cases} a_0 = a \\ k_0 = k \\ c_0 = 1 \\ r_0 = r \end{cases}$$

Los demás términos de las sucesiones se definen del siguiente modo, aplicando las propiedades de congruencia enunciadas en los incisos 1), 4) y 7) de la Proposición 1.30:

$$a^k = a^{2\left[\frac{k}{2}\right]+r_0} = \left(a^2\right)^{\left[\frac{k}{2}\right]} . a^{r_0} \equiv a_1^{k_1} . c_1 = \left(a_1^2\right)^{\left[\frac{k_1}{2}\right]} . a_1^{r_1} . c_1 \equiv a_2^{k_2} . c_2 = \ldots.$$

$$\uparrow \qquad\qquad\qquad\qquad \uparrow$$

$$\begin{cases} a_1 \equiv a^2 \pmod n \\ k_1 = \left[\frac{k}{2}\right] \\ c_1 \equiv a^{r_0} = a^{r_0} . c_0 \pmod n \end{cases} \qquad \begin{cases} a_2 \equiv a_1^2 \pmod n \\ k_2 = \left[\frac{k_1}{2}\right] \\ c_2 \equiv a_1^{r_1} . c_1 \pmod n \end{cases}$$

El proceso sigue hasta que $k_i \leq 1$ para algún i. El pseudocódigo del algoritmo lo mostramos a continuación:

Algoritmo para calcular $\boldsymbol{a^k \pmod n}$

$a_0 = a$, $k_0 = k$, $c_0 = 1$, $i = 1$

Mientras $k_{i-1} > 1$ *hacer:*

$a_i \equiv a_{i-1}^2 \pmod n$

Si k_{i-1} *es par entonces*

$c_i = c_{i-1}$

Sino $c_i = a_{i-1} . c_{i-1} \pmod n$

Fin si

$k_i = \left[\frac{k_{i-1}}{2}\right]$

$i = i + 1$

Fin mientras

$a^k \equiv a_{i-1} . c_{i-1} \pmod n$

El siguiente ejemplo ilustrará cómo se aplica este algoritmo.

Ejemplo 1.33

Calcular $84^{41} \pmod{247}$

Solución

En este caso, $a_0 = 84$, $c_0 = 1$ y $k_0 = 41$. A fin de ordenar los cálculos, diseñamos la siguiente tabla:

i	a_i	c_i	k_i
0	84	1	41
1	140	84	20
2	87	84	10
3	159	84	5
4	87	18	2
5	159	18	1

Los detalles de los datos que figuran en la tabla los explicamos a continuación:

$$a_1 = a_0^2 = (84)^2 = 7056 \equiv 140 \pmod{247}$$
$$c_1 = a_0 . c_0 = 84.1 = 84 \pmod{247}$$
$$k_1 = \left[\frac{k_{i-1}}{2} \right] = \left[\frac{k_0}{2} \right] = \left[\frac{41}{2} \right] = 20$$

$$a_2 = a_1^2 = (140)^2 = 19600 \equiv 87 \pmod{247}$$
$$c_2 = c_1 = 84 \pmod{247}$$
$$k_2 = \left[\frac{k_1}{2} \right] = \left[\frac{20}{2} \right] = 10$$

$$a_3 = a_2^2 = (87)^2 = 7569 \equiv 159 \pmod{247}$$
$$c_3 = c_2 = 84 \pmod{247}$$
$$k_3 = \left[\frac{k_2}{2} \right] = \left[\frac{10}{2} \right] = 5$$

$$a_4 = a_3^2 = (159)^2 = 25281 \equiv 87 \pmod{247}$$
$$c_4 = a_3 . c_3 = 159.84 = 13356 \equiv 18 \pmod{247}$$
$$k_4 = \left[\frac{k_3}{2} \right] = \left[\frac{5}{2} \right] = 2$$

$$a_5 = a_4^2 = (87)^2 = 7569 \equiv 159 \pmod{247}$$
$$c_5 = c_4 = 18 \pmod{247}$$
$$k_5 = \left[\frac{k_4}{2} \right] = \left[\frac{2}{2} \right] = 1$$

Por lo tanto, $(84)^{41} \equiv a_5 . c_5 = (159).(18) = 2862 \equiv 145 \pmod{247}$

1.6 Ecuaciones lineales de congruencia

En esta sección veremos cómo resolver la ecuación de congruencias más sencilla: la congruencia lineal.

Definición 1.34: Ecuación lineal de congruencia

Una ecuación lineal de congruencia "módulo n" es una ecuación de la forma

$$a.x \equiv b \pmod{n}$$

Donde $a, x, b \in \mathbb{Z}$

x: incógnita

Nos interesa hallar las soluciones en $\mathbb{Z}_n$. En este caso, la ecuación lineal modular puede escribirse

$$a.\,x = b \ \ en \ \mathbb{Z}_n$$

Donde $a, b \in \mathbb{Z} \ \wedge \ x \in \mathbb{Z}_n$

El siguiente Teorema muestra en qué casos existe solución para este tipo de ecuaciones.

Teorema 1.35: Solución de una ecuación lineal de congruencia

Dada la ecuación lineal de congruencia

$$a.x \equiv b \pmod{n}$$

Entonces

1) Si $mcd(a,n) = 1 \Rightarrow$ *existe única solución en* $\mathbb{Z}_n$ *y es de la forma*

$$x = a^{-1}.\,b \ \ en \ \mathbb{Z}_n$$

2) Si $mcd(a,n) = m \neq 1 \ \wedge \ m \mid b \Rightarrow$ *existen m soluciones en* $\mathbb{Z}_n$*, y son de la forma*

$$x_1 + k\,\frac{n}{m} \text{ , con } k = 0,1,\ldots,(m-1)$$

Donde x_1 *es la única solución en* $\mathbb{Z}_{n/m}$ *de la ecuación de congruencia*

$$\frac{a}{m}.x \equiv \frac{b}{m} \pmod{\frac{n}{m}}$$

3) Si $mcd(a,n) = m \neq 1 \ \wedge \ m \nmid b \Rightarrow$ *no existe solución.*

Demostración

Véase Referencia [11] ■

Ejemplo 1.36

Resolver las siguientes ecuaciones modulares:

1) $3.x \equiv 8 \pmod{11}$

2) $12.x \equiv 9 \pmod{27}$ 3) $3.x \equiv 1 \pmod{6}$

Solución

1) Como $mcd(3,11)=1$ entonces, por el Teorema *1.35* inciso *1)*, la ecuación tiene única solución en $\mathbb{Z}_{11}$. Aplicando la Proposición *1.30* resulta

$x = 3^{-1}.8 = 4.(8) = 32 \equiv 10 \pmod{11}$. Luego, la solución en $\mathbb{Z}_{11}$ es *x = 10.*

2) Como $mcd(12,27)=3 \neq 1 \wedge 3 \mid 9$ entonces, por el Teorema *1.35* inciso *2)*, la ecuación tiene 3 soluciones en $\mathbb{Z}_{27}$ .Las mismas son de la forma

$$x_1 + k\,\frac{27}{3}\ , \text{con } k = 0,1,2$$

Donde x_1 es solución de la ecuación de congruencia

$$\frac{12}{3}.x \equiv \frac{9}{3} \quad \left(mod\ \frac{27}{3}\right)$$

Es decir

$$4.x \equiv 3 \pmod{9}$$

Luego $x = 4^{-1}.3 = 7.(3) = 21 \equiv 3 \pmod{9}$. En consecuencia, $x_1 = 3.$

Por lo tanto, las soluciones en $\mathbb{Z}_{27}$ son:

$$x_1 + k\,\frac{27}{3} = 3 + k\,9\ , \text{con } k = 0,1,2$$

Es decir, *x = 3* , *x = 12* y *x = 21.*

3) Como $mcd(3,6)=2 \neq 1 \wedge 2 \nmid 1$ entonces, por el Teorema *1.35* Inciso *3)*, la ecuación no tiene solución.

1.7 Grupos, Subgrupos y Grupos Cíclicos

Definición 1.37: Grupo

Sea G un conjunto no vacío y $*$ una operación binaria definida sobre los elementos de G. El par $(G,*)$ es un grupo si y sólo si verifica las siguientes propiedades:

1) $*$ es Ley de Composición Interna: Si $a,b \in G \Rightarrow a*b \in G$.

2) Propiedad asociativa: Si $a,b \in G \Rightarrow (a*b)*c = a*(b*c)$

3) Existencia de elemento neutro o Identidad: $\exists\, e \in G / a*e = e*a \ \ \forall a \in G$.

4) Existencia de inversos: $\forall a \in G\ \exists\, a^{-1} \in G / a * a^{-1} = a^{-1} * a = e$.

Definición 1.38: Grupo Abeliano

Un grupo $(G,*)$ es abeliano si verifica la Propiedad conmutativa. Es decir,

$$Si\ \ a,b \in G \Rightarrow a*b = b*a.$$

Ejemplo 1.39

Si $n \in \mathbb{N}$ es primo entonces, por el Corolario 1.28, $\left(\mathbb{Z}_n - \{0\},\ \bullet\right)$ es un Grupo.

Definición 1.40: Subgrupo

Sea $(G,*)$ un grupo y $\varnothing \neq H \subset G$. Se dice que $(H,*)$ es un subgrupo de $(G,*)$ sii $(H,*)$ es grupo.

Definición 1.41: Potencia de un elemento de un grupo

Sea $(G,*)$ un grupo y "e" su elemento neutro. Si $x \in G$ y $n \in \mathbb{N}$ entonces:

1) $x^n = \underbrace{x * x *.... * x}_{n \text{ veces}}$

2) $x^{-n} = \underbrace{x^{-1} * x^{-1} *.... * x^{-1}}_{n \text{ veces}}$

3) $x^0 = e$

La siguiente Proposición prueba algunas propiedades elementales de la potencia de un elemento de un Grupo.

Proposición 1.42

Sea $(G,*)$ un grupo. Si $a,b \in G$ y $m,n \in \mathbb{N}$ entonces:

1) $a^m * a^n = a^{m+n}$

2) $\left(a^m\right)^n = a^{m.n}$

3) $\left(a^{-m}\right)^n = a^{-m.n}$

4) $a^{-n} = \left(a^n\right)^{-1}$

5) $a^m * a^{-n} = a^{m-n}$

6) Si $(G,*)$ es abeliano entonces $(a*b)^n = a^n * b^n$

Demostración: Ver Referencia [4], pág. *30*. ■

Definición 1.43: Subgrupo generado por un elemento del grupo

Sea $(G,*)$ un grupo y $x \in G$. El "subgrupo generado por x", simbolizado por $\langle x \rangle$, es

$$\langle x \rangle = \left\{x^k \ / \ k \in \mathbb{Z}\right\}$$

La siguiente Proposición es útil para caracterizar al subgrupo generado por un elemento de un grupo:

Proposición 1.44

Sea $(G,*)$ *un grupo finito, e su elemento neutro y* $x \in G$. *Entonces*

1) $\langle x \rangle$ *es un subgrupo de G.*

2) $\exists\, n_0 \in \mathbb{N}$ *tal que* $n_0 = min\{n \in \mathbb{N} / \; x^n = e\}$

3) $\langle x \rangle = \{x^1, x^2, ..., x^{n_0} = e\}$ *o equivalentemente,* $\langle x \rangle = \{x^0, x^1, ..., x^{n_0 - 1}\}$

Demostración

Véase Referencia [12], pág.*31* ■

Ejemplo 1.45

Dado el grupo $(\mathbb{Z}_5 - \{0\}, \bullet)$, calcular $\langle 2 \rangle$.

Solución

Aplicamos la Proposición *1.44,* inciso *3),* calculando las sucesivas potencias de *2* con exponente natural:

$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8 \equiv 3 \pmod 5$$
$$2^4 = 16 \equiv 1 \pmod 5$$

Por lo tanto

$$\langle 2 \rangle = \{\, 2^1, 2^2, 2^3, 2^4 \,\} = \{\, 2, 4, 3, 1 \,\}$$

Es decir

$$\langle 2 \rangle = \mathbb{Z}_5 - \{0\}$$

Definición 1.46: Grupo cíclico

Sea $(G,*)$ *un grupo. Se dice que es un grupo cíclico si existe* $x \in G$ *tal que* $G = \langle x \rangle$.

En este caso, se dice que x es un generador de G.

El siguiente Teorema es sumamente importante para definir logaritmos discretos.

Teorema 1.47

$(\mathbb{Z}_p - \{0\}, \bullet)$ *es un grupo cíclico* $\Leftrightarrow$ *p es primo.*

Demostración

Véase Referencia [4], pág. 45. ■

Introducimos ahora la siguiente notación que será utilizada a lo largo de este trabajo:

Notación 1.48:

El conjunto $\mathbb{Z}_p - \{0\}$ *será simbolizado por* $\mathbb{Z}_p^*$ *. Es decir,* $\mathbb{Z}_p^* = \{1,\ 2,\ ...,\ p\ -1\}$

Ejemplo 1.49

Sea el conjunto $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

a) Justifique porqué $\mathbb{Z}_7^*$ es cíclico.

b) Hallar los generadores de $\mathbb{Z}_7^*$.

Solución

a) Por el Teorema *1.47*, como *7* es un número primo, resulta que $\mathbb{Z}_7^*$ es cíclico.

b) Los generadores de $\mathbb{Z}_7^*$ pueden ser *2, 3, 4, 5, 6.* Para hallarlos, calculamos las sucesivas potencias modulares de estos números. Veamos cuál es el mayor exponente que puede contener el conjunto $\langle x \rangle, \forall x \in \{2,3,4,5,6\}$. Como

$$\langle x \rangle \subseteq \mathbb{Z}_7^* \ \Rightarrow\ card\left(\langle x \rangle\right) \leq card\left(\mathbb{Z}_7^*\right)$$

Donde $card\left(\langle x \rangle\right)$ y $card\left(\mathbb{Z}_7^*\right)$ representan la cantidad de elementos que tienen los conjuntos $\langle x \rangle$ y $\mathbb{Z}_7^*$ respectivamente. Por lo tanto $card\left(\langle x \rangle\right) \leq 6$. Por la Proposición 1.44 inciso *3)*, tenemos que $\langle x \rangle = \left\{x^1, x^2, ..., x^{n_0} = 1\right\}$

Luego, $n_0 = card\left(\langle x \rangle\right) \leq 6$ La siguiente tabla contiene las potencias de estos números:

Valor de x / x^i	***2***	***3***	***4***	***5***	***6***
x^1	*2*	*3*	*4*	*5*	*6*
x^2	*4*	*2*	*2*	*4*	*1*
x^3	*1*	*6*	*1*	*6*	*6*
x^4	*2*	*4*	*4*	*2*	*1*
x^5	*4*	*5*	*2*	*3*	*6*
x^6	*1*	*1*	*1*	*1*	*1*

Los generadores serán los elementos de la tabla que encabezan las columnas que contienen a todos los elementos de $\mathbb{Z}_7^*$. De este modo, los generadores de $\mathbb{Z}_7^*$ son *3* y *5*. Es decir, $\langle 3 \rangle = \mathbb{Z}_7^*$ y $\langle 5 \rangle = \mathbb{Z}_7^*$.

1.8 Nociones básicas de Probabilidad

En esta sección recordaremos los conceptos de Probabilidad y sus propiedades básicas, a fin de introducir una distribución de probabilidad que aplicaremos en el Capítulo *7*: la Distribución Geométrica o de Pascal.

Definición 1.50: Experimento, Espacio muestral y Evento

Un experimento ε *es un proceso que genera un conjunto de datos.*

Un espacio muestral S es el conjunto formado por los posibles resultados del experimento.

Un evento es cualquier subconjunto del espacio muestral.

Ejemplo 1.51

Se lanza un dado y se anota el resultado obtenido. Indicar cuál es el experimento, el espacio muestral y mostrar un evento.

Solución

ε: Lanzar un dado y anotar el resultado obtenido. $S=\{1,2,3,4,5,6\}$.

Un evento *A* es cualquier subconjunto de *S*. Por ejemplo, $A=\{2,3,4\}$.

Definición 1.52: Probabilidad

Sea ε *un experimento y S su espacio muestral. Una Probabilidad es una función*

$$P:\{A \text{ tal que } A\subseteq S\}\to\mathbb{R}$$

que asigna a cada evento A un número real $P(A)$ *que mide la posibilidad de que el evento A ocurra cuando el experimento se realiza, y que verifica las siguientes propiedades:*

1) $0\le P(A)\le 1$

2) $P(S)=1$

3) Si A y B son eventos disjuntos entonces $P(A\cup B)=P(A)+P(B)$

4) Si $A_1, A_2, A_3, \ldots$ *son eventos disjuntos de par en par entonces*

$$P\left(\bigcup_{i=1}^{\infty}A_i\right)=\sum_{i=1}^{\infty}P(A_i)$$

Al número $P(A)$ lo llamaremos "*la probabilidad de que ocurra el evento A*".

De los incisos *2*) y *3*) de la Definición *1.52*, se demuestra sin dificultad de que si *A* es un evento y A^c es el complemento de *A* entonces

$$P(A^c)=1-P(A)$$

Cómo calcular Probabilidades

Según el enfoque clásico de Laplace (*1749-1827*), si todos los resultados del experimento tienen la misma chance de ocurrir y el espacio muestral *S* es finito entonces, si *A* es un evento, la probabilidad de que ocurra el evento *A* es

$$P(A) = \frac{card(A)}{card(S)}$$

Donde

$card(A)$: *Cantidad de elementos que tiene el evento A.*

$card(S)$: *Cantidad de elementos que tiene el espacio muestral S.*

En cambio, si todos los resultados del experimento no tienen la misma chance de ocurrir o si el espacio muestral *S* no es finito, la probabilidad de un evento *A* se calcula según la definición de Von Mises (*1883-1953*):

$$P(A) = \lim_{n \to \infty} \frac{n_A}{n}$$

Donde

n_A : *Cantidad de veces que ocurre el evento A.*

n : *Cantidad de veces que se repite el experimento.*

Como resulta imposible efectuar infinitas veces un experimento, en general se toma $n = 30$, $n = 50$ o bien $n = 100$ y se calcula

$$P(A) \cong \frac{n_A}{n}$$

Ejemplo 1.53

Una clase de Estadística para profesionales consta de *30* abogados, *20* médicos y *18* ingenieros. Ninguno de estos estudiantes tiene más de una profesión. Si el profesor elige a una persona al azar para que conteste una pregunta.

1) Hallar la probabilidad de que el profesional elegido sea médico.
2) Calcular la probabilidad de que el elegido sea abogado o ingeniero.
3) Hallar la probabilidad de que el profesional seleccionado no sea médico.

Solución

1) Definimos los eventos
A: El profesional elegido es abogado.
M: El profesional elegido es médico.
I: El profesional elegido es ingeniero.

El número total de profesionales en la clase es *68*, todos los cuales tienen la misma chance de ser seleccionados. Por lo tanto, aplicando la fórmula de Probabilidad según Laplace, obtenemos

$$P(M) = \frac{20}{68}$$

2) Como los eventos *A* e *I* son disjuntos resulta

$$P(A \cup I) = P(A) + P(I) = \frac{30}{68} + \frac{18}{68} = \frac{48}{68}$$

3) Calculamos

$$P(M^c) = 1 - P(M) = 1 - \frac{20}{68} = \frac{48}{68}$$

Definición 1.54: Eventos independientes

Dos eventos A y B son independientes si la probabilidad de que A ocurra no afecta ni influye sobre la probabilidad de que B ocurra. En este caso, se verifica que

$$P(A \cap B) = P(A).P(B)$$

En general, si los eventos $A_1, A_2, ..., A_n$ *son independientes entonces*

$$P(A_1 \cap A_2 \cap ..... \cap A_n) = P(A_1).P(A_2)....P(A_n)$$

Ejemplo 1.55

La probabilidad de que una lámpara falle es *0.3*. Se eligen al azar *3* lámparas. ¿Cuál es la probabilidad de que las tres lámparas fallen?

Solución

Definimos los eventos:

F_i : *Falló la i-ésima lámpara seleccionada, i =1, 2 ,3.*

Estos eventos son independientes, pues la probabilidad de que una lámpara seleccionada falle no afecta ni influye sobre la probabilidad de que otra lámpara escogida también falle. Por lo tanto

$P(F_1 \cap F_2 \cap F_3) = P(F_1).P(F_2).P(F_3) = (0.3)^3 = 0.027$.

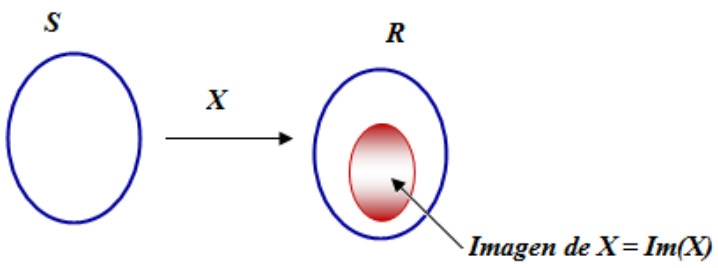
Siempre es importante asignar una descripción numérica a los resultados de un experimento, a fin de poder manipular matemáticamente los datos e inferir ciertos resultados. Por esta razón surge el siguiente concepto:

Definición 1.56: Variable aleatoria

Sea ε *un experimento y S su espacio muestral. Una Variable Aleatoria es una función*

$$X : S \to \mathbb{R}$$

que asigna a cada elemento del espacio muestral, un número real.



Por abuso de notación, se identifica a la variable aleatoria *X*, que es una función, con su imagen. Es decir,

$$X \equiv Im(X)$$

Ejemplo 1.57

Se lanza una moneda y se anota *1* punto si salió Cara (C) y *0* punto si salió Cruz (T). Indicar cuál es el experimento, el espacio muestral y la variable aleatoria.

Solución

ε: Lanzar una moneda. $S = \{C,T\}$

La variable aleatoria se define por

$$\begin{cases} X(C) = 1 \\ X(T) = 0 \end{cases}$$

En este caso, $Im(X) = \{0,1\}$ y se escribe $X = \{0,1\}$.

Definición 1.58: Clasificación de las variables aleatorias

Las variables aleatorias se clasifican en:

Discretas*: Cuando su imagen es un conjunto finito o infinito numerable.*
Continuas*: Cuando su imagen puede tomar todos los valores comprendidos en un intervalo.*

Ejemplo 1.59

Para los siguientes casos, indicar cuál es el experimento en análisis, la variable aleatoria generada y clasificarla.

1) En una universidad se extraerá una muestra al azar de 5 estudiantes y se establecerá cuántos de ellos trabajan.
2) En un banco, que atiende al público de *10* hs a *13* hs, se registrará la hora en que llega el primer cliente.

Solución

1) ε: Elegir al azar *5* estudiantes y establecer si trabaja.
   X: Cantidad de estudiantes de la muestra que trabajan.
   $X = \{0,1,2,3,4,5\}$ .Es una variable aleatoria discreta.

2) ε: Registrar la hora de llegada del primer cliente al banco.
   X: Hora de llegada del primer cliente al banco.
   $X = [10,13]$.Es una variable aleatoria continua.

Cuando se trabaja con una variable aleatoria discreta, es útil disponer del valor de las probabilidades para cada elemento de una variable aleatoria. Es así como surge la idea de Distribución de Probabilidad. Su definición es la siguiente:

Definición 1.60: Distribución de Probabilidad

Dada una variable aleatoria discreta $X = \{x_1, x_2, x_3, ...\}$, *la distribución de probabilidad de X es una función*

$$f : X \to \mathbb{R}$$

definida por $f(x_i) = P(X = x_i) =$ *probabilidad que la variable X tome el valor* x_i.

Dicha función verifica las siguientes propiedades:

1) $0 \leq f(x_i) \leq 1 \quad \forall i=1,2,....$

2) $\sum_i f(x_i) = 1$

Definición 1.61: Esperanza de una variable aleatoria discreta

Dada una variable aleatoria discreta $X = \{x_1, x_2, x_3, ...\}$, *la Esperanza de X es*

$$E[X] = \sum_{x_i \in X} x_i . P(X = x_i)$$

La Esperanza es un concepto análogo al promedio aritmético de un conjunto de datos. Su interpretación intuitiva o significado se corresponde con el valor medio de los posibles valores que pueda tomar la variable aleatoria.
También puede interpretarse como el valor que se "espera" que tome la variable aleatoria, cuando el experimento se repite un gran número de veces.

Ejemplo 1.62

Una urna contiene *4* bolas rojas y *3* blancas. Se extraen de manera sucesiva *2* bolas con sustitución (es decir, una vez extraída una bola, se la regresa a la urna) y se registra el número de bolas rojas extraídas.

1) Indicar cuál es la variable aleatoria en análisis.
2) Determinar su Distribución de Probabilidad.
3) Calcular la Esperanza.

Solución

1) La variable aleatoria es *X*: Cantidad de bolas rojas extraídas. Es decir,

$$X = \{0, 1, 2\}$$

2) Definimos los eventos:
R: salió la "bola roja".
B: salió la "bola blanca".

Teniendo en cuenta que estos eventos son independientes, la distribución de probabilidad la calculamos del siguiente modo:

$$f\left(0\right)=P\left(X=0\right)=P\left(B\cap B\right)=P\left(B\right).P\left(B\right)=\frac{3}{7}.\frac{3}{7}=\frac{9}{49}$$

$$f\left(1\right)=P\left(X=1\right)=P\left(\left(R\cap B\right)\cup\left(B\cap R\right)\right)=P\left(R\cap B\right)+P\left(B\cap R\right)=$$

$$=P\left(R\right).P\left(B\right)+P\left(B\right).P\left(R\right)=\frac{4}{7}.\frac{3}{7}+\frac{3}{7}.\frac{4}{7}=\frac{24}{49}$$

$$f\left(2\right)=P\left(X=2\right)=P\left(R\cap R\right)=P\left(R\right).P\left(R\right)=\frac{4}{7}.\frac{4}{7}=\frac{16}{49}$$

Los resultados obtenidos los resumimos en la siguiente tabla:

x	$f\left(x\right)$	$x.f\left(x\right)$
0	*9 / 49*	*0*
1	*24 / 49*	*24 / 49*
2	*16 / 49*	*32 / 49*

3) $E\left[X\right]=0.f\left(0\right)+1.f\left(1\right)+2.f\left(2\right)=0+\frac{24}{49}+\frac{32}{49}=\frac{56}{49}=1.14$

Como *1.14* está más próximo a *1* que al número *2*, se espera que al extraer *2* bolas de la urna, salga una sola bola roja.

La Distribución Geométrica o de Pascal

Una variable aleatoria tiene una Distribución de Pascal si responde a las siguientes características:

■ El experimento consiste en efectuar sucesivas pruebas, independientes una de otra.
■ Cada prueba produce dos resultados posibles, que se puede clasificar como *Éxito* o *Fracaso*.
■ La probabilidad de *Éxito*, que se denota por ***r***, permanece constante de una prueba a otra.
■ La prueba se repite hasta que aparece Éxito por primera vez.

Bajo estas condiciones, definimos la variable aleatoria *X* como el número de veces que repetimos la prueba hasta que se dé *Éxito* por primera vez. Es decir,

$$X=\left\{1,2,3,4,...\right\}$$

Cálculo de la Distribución de Pascal

Si definimos los eventos:

E_i : *Salió Éxito en la i-ésima prueba*.

F_i : *Salió Fracaso en la i-ésima prueba*.

Entonces

$$P\left(E_i\right)=r$$

$$P\left(F_i\right)=1-r \quad \forall i=1,2,....$$

Por hipótesis, estos eventos son independientes. Por lo tanto

$$f\left(1\right)=P\left(X\ =1\right)=P\left(E_1\right)=r$$

$$f\left(2\right)=P\left(X\ =2\right)=P\left(F_1\cap E_2\right)=P\left(F_1\right).P\left(E_2\right)=\left(1-r\right)r$$

En general,

$$f\left(n\right)=P\left(X\ =n\right)=P\left(F_1\cap F_2\cap\ldots\cap F_{n-1}\cap E_n\right)=P\left(F_1\right).P\left(F_2\right)\ldots P\left(F_{n-1}\right).P\left(E_n\right)=$$

$$=\left(1-r\right)^{n-1}\ r$$

Luego

$$f\left(n\right)=P\left(X\ =n\right)=\left(1-r\right)^{n-1}\ r\quad\forall n=1,2,....$$

Cálculo de la Esperanza de la Distribución de Pascal

La siguiente Proposición muestra la expresión de la Esperanza de una Distribución de Pascal.

Proposición 1.63

La Esperanza de una variable aleatoria X que sigue una Distribución de Pascal es

$$E\left[X\ \right]=\frac{1}{r}$$

Donde r es la probabilidad de Éxito de una prueba.

Demostración

Como $f\left(n\right)=\left(1-r\right)^{n-1}\ r\quad\forall n=1,2,....$ entonces

$$E\left[X\ \right]=\sum_{n\ =1}^{\infty}n.\ f\left(n\right)=\sum_{n\ =1}^{\infty}n.\ \left(1-r\right)^{n-1}\ r$$

Es decir

$$E\left[X\ \right]=r\sum_{n\ =1}^{\infty}n.\ \left(1-r\right)^{n-1}\qquad[I]$$

Por otro lado, consideremos la serie de potencias

$$\sum_{n\ =1}^{\infty}x^{\ n}\quad con\ x\ \in\mathbb{R}$$

Se puede probar que, si $\left|x\right|<1$, se verifica que

$$\sum_{n\ =1}^{\infty}x^{\ n}=\frac{x}{1-x}$$

Derivando miembro a miembro, y teniendo en cuenta que una serie de potencias puede derivarse término a término, obtenemos

$$\frac{d}{dx}\left(\sum_{n=1}^{\infty} x^n\right)=\frac{d}{dx}\left(\frac{x}{1-x}\right)\Rightarrow \sum_{n=1}^{\infty}\frac{d}{dx}\left(x^n\right)=\frac{1}{(1-x)^2}\Rightarrow \sum_{n=1}^{\infty} n\ .x^{n-1}=\frac{1}{(1-x)^2}$$

Por lo tanto, si $|x|<1$ entonces

$$\sum_{n=1}^{\infty} n\ .x^{n-1}=\frac{1}{(1-x)^2}$$

En particular, tomando $x = 1 - r$ resulta

$$\sum_{n=1}^{\infty} n\ .(1-r)^{n-1}=\frac{1}{(1-(1-r))^2}$$

Luego

$$\sum_{n=1}^{\infty} n\ .(1-r)^{n-1}=\frac{1}{r^2} \qquad \text{[II]}$$

Reemplazando [II] en [I] tenemos que

$$E[X]=r\sum_{n=1}^{\infty} n.\ (1-r)^{n-1}=r.\frac{1}{r^2}=\frac{1}{r} \quad \blacksquare$$

Ejemplo 1.64

Una fábrica comercializa sus productos enviando promotores a visitar los comercios minoristas. Se ha observado que el 30% de los comercios visitados efectúan alguna compra.

1) ¿Cuál es la probabilidad de tener que visitar *5* comercios para efectuar una venta?

2) ¿Cuántos comercios se espera tener que visitar para efectuar una venta?

Solución

Definimos la variable aleatoria

X: Cantidad de comercios a visitar hasta lograr una venta. Entonces

$$X=\{1,2,3,4,...\}$$

X responde a una Distribución de Pascal, con $r = 0.30$. En este caso, su función de Distribución de Probabilidad es

$$f(n)=P(X=n)=(1-r)^{n-1}\ r=(1-0.3)^{n-1}.(0.3) \quad \forall n=1,2,....$$

1) Calculamos

$$P(X=5)=(1-0.3)^{5-1}.(0.3)=(0.7)^4.(0.3)=0.072$$

2) La Esperanza de esta variable aleatoria es

$$E[X]=\frac{1}{r}=\frac{1}{0.3}=3.33$$

Luego, se espera tener que visitar 3 comercios hasta lograr una venta.

CAPÍTULO 2

Logaritmos Discretos

Los logaritmos discretos se definen para grupos cíclicos finitos y, en particular, para $\left(\mathbb{Z}_p^*, \bullet\right)$, donde *p es* un número primo. Su importancia radica en el hecho de que ciertos algoritmos criptográficos muy difundidos, como por ejemplo el de Diffie-Hellman, el Cifrado ElGamal o el Algoritmo de Firma Digital, basan su seguridad en la dificultad para resolver logaritmos discretos. Su definición la damos a continuación.

Definición 2.1: Logaritmo discreto

Sea $(\mathrm{G}, *)$ *un grupo cíclico finito de n elementos, y "g" un elemento generador de G. Es decir,*

$$G = \langle g \rangle = \left\{ g^0, g^1, ..., g^{n-1} \right\}$$

El logaritmo discreto en base "g" de un elemento $x \in G$ *es un número entero* $y \in \{0, 1, ..., n-1\}$ *que verifica*

$$\log_g (x) = y \iff g^y = x$$

Observación 2.2

En la definición de logaritmo discreto, se pide que la base "*g*" sea un elemento generador del grupo para que $\log_g (x)$ quede definido $\forall x \in G$. Por otro lado, en virtud del Teorema *1.47*, $\left(\mathbb{Z}_p^*, \bullet\right)$ es un grupo cíclico finito sii *p* es primo. Por lo tanto, si *p* es primo, el logaritmo discreto quedará definido en $\left(\mathbb{Z}_p^*, \bullet\right)$ del siguiente modo:

Definición 2.3: Logaritmo discreto en $\mathbb{Z}_p^*$

Sea $\left(\mathbb{Z}_p^*, \bullet\right)$ *con p un número primo y "g" un elemento generador de* $\mathbb{Z}_p^*$.

El logaritmo discreto en base "g" de un número $x \in \mathbb{Z}_p^*$ *es un número* $y \in \{0, 1, ..., p-1\} = \mathbb{Z}_p$ *que verifica:*

$$\log_g (x) = y \iff g^y = x \ en \ \mathbb{Z}_p$$

O equivalentemente,

$$\log_g (x) = y \iff g^y \equiv x \pmod{p}$$

Los siguientes ejemplos ilustrarán cómo calcular logaritmos discretos.

Ejemplo 2.4

Sea $\left(\mathbb{Z}_{13}^{*}, \bullet\right)$ donde $\mathbb{Z}_{13}^{*} = \{1, 2, 3, ..., 12\}$

1) Indicar si $log_7(x)$ queda definido en $\forall x \in \mathbb{Z}_{13}^{*}$

2) Determinar si $log_3(x)$ queda definido en $\forall x \in \mathbb{Z}_{13}^{*}$

Solución

1) Primeramente, observemos que $\left(\mathbb{Z}_{13}^{*}, \bullet\right)$ es un grupo cíclico pues, por el Teorema *1.47*, *13* es un número primo. Por otro lado, para que $log_7(x)$ quede definido, *7* debe ser un generador de $\mathbb{Z}_{13}^{*}$. Se verificará entonces si $\langle 7 \rangle = \mathbb{Z}_{13}^{*}$, calculando las potencias de *7* en $\mathbb{Z}_{13}^{*}$:

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
7^i	**1**	**7**	**10**	**5**	**9**	**11**	**12**	**6**	**3**	**8**	**4**	**2**

Por lo tanto, como las potencias de *7* generan todos los elementos de $\mathbb{Z}_{13}^{*}$, $log_7(x)$ queda definido $\forall x \in \mathbb{Z}_{13}^{*}$ del siguiente modo:

$log_7(1) = 0 \quad pues\ 7^0 = 1\ en\ \mathbb{Z}_{13}^{*}$

$log_7(2) = 11\ pues\ 7^{11} = 2\ en\ \mathbb{Z}_{13}^{*}$

$log_7(3) = 8 \quad pues\ 7^8 = 3\ en\ \mathbb{Z}_{13}^{*}$

$log_7(4) = 10\ pues\ 7^{10} = 4\ en\ \mathbb{Z}_{13}^{*}$

$log_7(5) = 3\ pues\ 7^3 = 5\ en\ \mathbb{Z}_{13}^{*}$

$log_7(6) = 7\ pues\ 7^7 = 6\ en\ \mathbb{Z}_{13}^{*}$

$log_7(7) = 1\ pues\ 7^1 = 7\ en\ \mathbb{Z}_{13}^{*}$

$log_7(8) = 9\ pues\ 7^9 = 8\ en\ \mathbb{Z}_{13}^{*}$

$log_7(9) = 4\ pues\ 7^4 = 9\ en\ \mathbb{Z}_{13}^{*}$

$log_7(10) = 2\ pues\ 7^2 = 10\ en\ \mathbb{Z}_{13}^{*}$

$log_7(11) = 5\ pues\ 7^5 = 11\ en\ \mathbb{Z}_{13}^{*}$

2) Se verificará primeramente si *3* es generador de $\mathbb{Z}_{13}^{*}$:

i	**0**	**1**	**2**	**3**
3^i	**1**	**3**	**9**	**1**

Como $\langle 3 \rangle = \{1,3,9\} \neq \mathbb{Z}_{13}^*$, concluimos que *3* no es generador de $\mathbb{Z}_{13}^*$ y, en consecuencia, $log_3(x)$ no queda definido $\forall x \in \mathbb{Z}_{13}^*$.

Ejemplo 2.5

---

1) Identificar los generadores de $\mathbb{Z}_{11}^*$.

2) Indicar para qué valores de "*g*" existe $log_g(x)\ \forall x \in \mathbb{Z}_{11}^*$

Solución

Los posibles generadores de $\mathbb{Z}_{11}^*$ pueden ser *2, 3, 4,… ,10*. Para hallarlos, diseñamos la siguiente tabla que contiene las potencias de estos números:

Valor de x / x^i	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
x^0	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*
x^1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
x^2	*4*	*9*	*5*	*3*	*3*	*5*	*9*	*4*	*1*
x^3	*8*	*5*	*9*	*4*	*7*	*2*	*6*	*3*	*10*
x^4	*5*	*4*	*3*	*9*	*9*	*3*	*4*	*5*	*1*
x^5	*10*	*1*	*1*	*1*	*10*	*10*	*10*	*1*	*10*
x^6	*9*	*3*	*4*	*5*	*5*	*4*	*3*	*9*	*1*
x^7	*7*	*9*	*5*	*3*	*8*	*6*	*2*	*4*	*10*
x^8	*3*	*5*	*9*	*4*	*4*	*9*	*5*	*3*	*1*
x^9	*6*	*4*	*3*	*9*	*2*	*8*	*7*	*5*	*10*

Los generadores serán los elementos de la tabla que encabezan las columnas que contienen a todos los elementos de $\mathbb{Z}_{11}^*$. De este modo, los generadores de $\mathbb{Z}_{11}^*$ son 2, 6, 7 y 8. Es decir,

$$\langle 2 \rangle = \mathbb{Z}_{11}^* \ , \ \langle 6 \rangle = \mathbb{Z}_{11}^* \ , \ \langle 7 \rangle = \mathbb{Z}_{11}^* \ , \ \langle 8 \rangle = \mathbb{Z}_{11}^* .$$

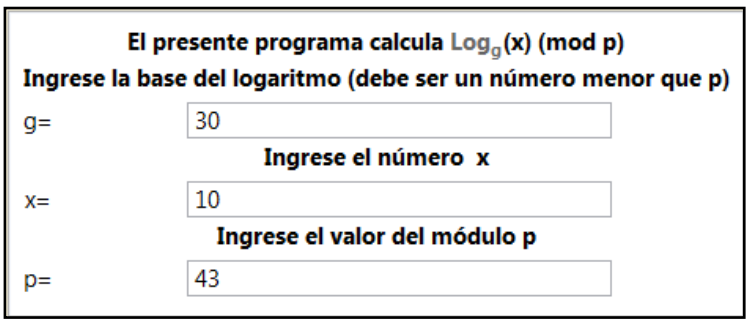
2) Como 2, 6, 7 y 8 son generadores de $\mathbb{Z}_{11}^*$, $log_2(x)$, $log_6(x)$, $log_7(x)$ y $log_8(x)$ quedan definidos $\forall x \in \mathbb{Z}_{11}^*$.

2.1 ¿Existen algoritmos eficientes para el cálculo de un logaritmo discreto?

Podemos afirmar con certeza que no existe un algoritmo, para ser ejecutado en una computadora clásica, que permita calcular logaritmos discretos de una manera eficiente. Se cree que el Problema de los Logaritmos Discretos es, computacionalmente, tan complejo como el problema de la factorización de números enteros grandes. Mientras más grande sea el módulo *p*, mayor será el tiempo que tome hallar el logaritmo.
Sin embargo, el algoritmo propuesto por Shor acelera considerablemente el tiempo de resolución de logaritmos discretos si se emplea una computadora cuántica. Es por esta razón que su propuesta despertó tanto interés en la comunidad científica, ya que pondría en jaque la seguridad de todos los sistemas criptográficos basados en logaritmos discretos y que son utilizados en la actualidad.

2.2 Cálculo de logaritmos discretos mediante Wolfram Mathematica 10.0

El siguiente programa, diseñado mediante el software Wolfram Mathematica 10.0, calcula $log_g(x)\ (mod\ p)$ aplicando el *Método de Fuerza Bruta*. Dicho método consiste en calcular las diferentes potencias modulares de *g*, hasta hallar $y \in \{0,1,...,p-1\}$ que verifique la condición $g^y = x \ \ en\ \mathbb{Z}_p$. Es decir, tal que $g^y \equiv x \pmod p$.
Para el cálculo de estas potencias modulares aplicamos el algoritmo descripto en el Capítulo *1*.
Para ejecutar el programa se ingresan la base *g*, el número $x \in \mathbb{Z}_p^*$ y el módulo *p*, en un cuadro de diálogo similar al de la figura:



Según los datos ingresados, el programa calcula

$$log_{30}(10)\ (mod\ 43)$$

O equivalentemente

$$log_{30}(10)\ en\ \mathbb{Z}_{43}$$

Al ejecutarlo, obtenemos por resultado *20*. El código fuente del programa lo mostramos a continuación.

Código fuente del programa que calcula $\log_g(x) \pmod p$

```
Interpretation[{g=18,x=11,p=43},Panel[Grid[{{Style ["El presente programa
calcula Log_g(x) (mod p)",Bold ], SpanFromLeft },{Style ["Ingrese la base del
logaritmo (debe ser un número menor que p)", Bold ], SpanFromLeft },
   {"g =", InputField [ Dynamic [ g ] ] },
   {Style ["Ingrese el número  x", Bold], SpanFromLeft },
   {"x =", InputField [ Dynamic[x] ] },
   {Style ["Ingrese el valor del módulo p",Bold], SpanFromLeft },
   {"p =", InputField [ Dynamic [ p] ] }
    }] ],
 a = 2;
 Encontrado = "Falso";
 While [ a < p-1 ,
  k = a;
  cc = 1;
  g1 = g;
  While [ k > 1,
   b= Mod [g1^2, p ];
   If [ Mod [ k, 2 ] != 0, cc= g1*cc ];
   g1 = b;
   k=IntegerPart [ k/2 ];
   ];
  If [ Mod [g1* cc, p] = =x, Encontrado="Verdadero"; resultado = a; Break[ ]
];
   a=a+1;
   ];
 If [Encontrado = ="Verdadero", Print ["Log",g,"(",x,") =", resultado, "  (mod
", p,")"] , "El Logaritmo no fue encontrado"]
 ]
```

Existen otros métodos que funcionan más rápido que el de *Fuerza Bruta*, como por ejemplo el *Método de Shanks* o el *Algoritmo de Pollard*. Sin embargo, no llegan a ser eficientes cuando el número primo *p* es muy grande. Más específicamente, cuando el número primo *p* tiene valores cercanos a los *1000* dígitos binarios, el cálculo del logaritmo discreto utilizando una computadora convencional se torna inmanejable.

2.3 Los logaritmos discretos aplicados a la Criptografía

Numerosos criptosistemas basan su seguridad en la dificultad para calcular logaritmos discretos. Entre los más difundidos, figuran el *Protocolo de Intercambio de Diffie-Hellman* y los *Algoritmos de ElGamal*.

Nos ocuparemos en describir el segundo de estos algoritmos, ya que el primero de ellos se encuentra detalladamente explicado en la Referencia [4].

Los Algoritmos de ElGamal

En *1985* el investigador egipcio, Thaer ElGamal, propone dos algoritmos criptográficos que llevan su nombre: "*El Algoritmo de Cifrado ElGamal*" y "*El Algoritmo de Firma Digital El Gamal*". Desarrollaremos a continuación cada uno de ellos.

El Algoritmo de Cifrado ElGamal

Es utilizado para cifrar y descifrar mensajes secretos, como por ejemplo, una clave de sesión por Internet. En este caso, cada usuario crea su propia clave pública (conocida por todos) y su correspondiente clave privada (mantenida en secreto) del siguiente modo:

1) Selecciona un número primo *p* grande y un generador *g* de $\mathbb{Z}_p^*$.

2) Elige aleatoriamente un entero a, tal que $1 \le a \le p-2$ y calcula $\beta = g^a \pmod p$.

3) La clave pública, que será conocida por los demás usuarios, es la terna (p, g, β).

La clave privada es a.

Clave pública	***Clave privada***
(p, g, β)	a

Supongamos que un usuario, al que llamaremos Bernardo, cifra un mensaje para enviárselo a otra usuaria, llamada Alicia. Entonces

Bernardo cifra un mensaje para Alicia

1) Bernardo obtiene la clave pública de Alicia: (p, g, β).

2) Representa un mensaje codificado numéricamente como un entero *m* en el intervalo $[0, p-1]$.

3) Elige al azar un entero *k* tal que $1 \le k \le p-2$.

4) Calcula $\gamma = g^k \pmod p$ y $\delta = m \,.\, \beta^k \pmod p$

5) Envía el par cifrado (γ, δ) a Alicia.

Alicia descifra el mensaje de Bernardo

Alicia utiliza su clave privada a para recuperar el mensaje *m*, del siguiente modo:

$$\gamma^{p-1-a} . \delta = m \pmod p$$

Justificación de porqué Alicia obtiene el mensaje m de Bernardo

El Teorema de Fermat afirma que si *p* es un número primo entonces

$$a^{p-1} \equiv 1 \pmod p \quad \forall a \in \mathbb{Z}_p^*$$

Por lo tanto

$\gamma^{p-1-a}.\ \delta = \gamma^{p-1}.\ \gamma^{-a}.\ \delta \equiv 1.\left(g^{k}\right)^{-a}.m\ .\ \beta^{k} = g^{-k.a}.m.\left(g^{a}\right)^{k} = g^{-k.a}.m.\ g^{k.a} =$

$= g^{-k.a}.\ g^{k.a}.m = 1.m = m \pmod{p}$

La seguridad del *Algoritmo de Cifrado ElGamal* se basa en la dificultad para descubrir la clave privada "*a*". Es decir, en hallar "*a*" tal que $\beta = g^{a} \pmod{p}$. O equivalentemente, en lo dificultoso que resulta resolver $log_{g}(\beta) \pmod{p}$ cuando el número primo *p* es muy grande.

Ejemplo 2.6

Alicia genera una clave privada *a= 33* y una clave pública $(p, g, \beta) = (151, 6, 60)$,

Donde $\beta = g^{a} = 6^{33} \equiv 60 \pmod{151}$.

Bernardo cifra un mensaje para Alicia

1) Bernardo obtiene la clave pública de Alicia: $(p, g, \beta) = (151, 6, 60)$.

2) Representa un mensaje codificado numéricamente como un entero *m=79.*

3) Elige al azar un entero *k =11*.

4) Calcula γ y δ del siguiente modo:

$\gamma = g^{k} \pmod{p}$. Es decir, $\gamma = 6^{11} \equiv 77 \pmod{151}$

$\delta = m\ .\ \beta^{k} \pmod{p}$. O sea, $\delta = 79\ .\ 60^{11} \equiv 8 \pmod{151}$

5) Envía el par cifrado $(\gamma, \delta) = (77, 8)$ a Alicia.

Alicia descifra el mensaje de Bernardo

Alicia utiliza su clave privada a para recuperar el mensaje *m*:

$\gamma^{p-1-a}.\ \delta = 77^{151-1-33}.(8) = 77^{117}.(8) \equiv 142.(8) = 1136 \equiv 79 \pmod{151}$

De este modo, Alicia descifra el mensaje *m=79* de Bernardo.

El Algoritmo de Firma Digital ElGamal

Este algoritmo permite que un verificador pueda confirmar la autenticidad de un mensaje que fue firmado y enviado por un emisor por un canal inseguro como es Internet. En este caso uno de los participantes, que llamaremos Alicia, quiere firmar los mensajes. Para ello procede del siguiente modo:

Alicia genera una clave

1) Selecciona un número primo *p* grande y un generador *g* de $\mathbb{Z}_{p}^{*}$.

2) Elige aleatoriamente un entero a, tal que $1 \le a \le p-2$ y calcula $\beta = g^{a} \pmod{p}$.

3) La clave pública, que será conocida por los demás usuarios, es la terna (p, g, β).
   La clave privada es a.

Estos pasos son realizados una sola vez por el firmante, que en este caso es Alicia.

Alicia genera una firma

Para firmar un mensaje *m* que está codificado numéricamente, la firmante Alicia efectúa los siguientes pasos:

1) Elige un entero k tal que $1 \leq k \leq p-2$ y $mcd\left(k, p-1\right)=1$

2) Calcula $r = g^{k} \pmod{p}$

3) Calcula $s \equiv \left(m - a.\, r\right).\, k^{-1} \pmod{\left(p-1\right)}$

4) Si $s = 0$, volver al inciso 1).

El par $\left(r,s\right)$ así obtenido es la firma digital del mensaje *m*. La firmante procederá a repetir estos pasos para cada mensaje *m* que desee firmar.

Verificación de la autenticidad de la firma

Si un usuario quiere comprobar que un mensaje *m* procede efectivamente de Alicia, debe verificar que

$$g^{m} \equiv \beta^{r}.\, r^{s} \pmod{p}$$

El verificante acepta el mensaje únicamente si esta condición se cumple. Porque si efectivamente Alicia fue la emisora del mensaje, esta última expresión de congruencia es válida pues: como

$$s \equiv \left(m - a.\, r\right).\, k^{-1} \pmod{\left(p-1\right)} \Rightarrow m \equiv s.k + a.r \pmod{\left(p-1\right)} \Rightarrow \left(p-1\right) \mid \left(m - s.k - a.r\right)$$

Luego

$$m - s.k - a.r = k_1\left(p-1\right) \text{ para algún } k_1 \in \mathbb{Z}$$

Es decir

$$s.k + a.r = m - k_1\left(p-1\right)$$

Por lo tanto, aplicando el Teorema de Fermat resulta

$$\beta^{r}.\, r^{s} = \left(g^{a}\right)^{r}.\, \left(g^{k}\right)^{s} = g^{a.r}.\, g^{k.s} = g^{a.r+k.s} = g^{m-k_1(p-1)} = g^{m}.\, g^{-k_1(p-1)} =$$

$$= g^{m}.\, \left(g^{(p-1)}\right)^{-k1} = g^{m}.\, (1)^{-k1} = g^{m} \pmod{p}$$

Obviamente, si alguien fuese capaz de calcular logaritmos discretos y obtener el entero a a partir de β, es decir, si pudiera hallar $a = log_{g}\left(\beta\right) \pmod{p}$, podría firmar mensajes como si fuese la firmante Alicia, pero si se toma un numero primo *p* suficientemente grande, en la práctica es imposible encontrar a.

La importancia de este algoritmo reside en que es la base del actual sistema de firmas digitales, el DSA.

Finalizamos este Capítulo con el siguiente Ejemplo que implementa este último algoritmo.

Ejemplo 2.7

Alicia quiere firmar un mensaje *m= 300* para enviárselo a Bernardo a través de Internet. Para ello procede del siguiente modo:

Alicia genera una clave

1) Selecciona un número primo *p=6011* y un generador *g =13*.

2) Elige un entero $a = 20$ y calcula $\beta = g^a \pmod p$. Es decir,

$$\beta = 13^{20} = 2023 \pmod{6011}$$

3) La clave pública de Alicia es la terna $(p, g, \beta) = (6011, 13, 2023)$.
La clave privada es $a = 20$.

Alicia genera una firma

Para firmar el mensaje *m=300*, Alicia efectúa los siguientes pasos:

1) Elige el entero $k = 7$, el cual verifica que $mcd(k, p-1) = mcd(7, 6010) = 1$

2) Calcula $r = g^k \pmod p$.Es decir,

$$r = 13^7 \equiv 5699 \pmod{6011}$$

3) Calcula $s \equiv (m - a.r).k^{-1} \pmod{(p-1)}$. Es decir

$$s \equiv (300 - (20).5699).4293 = -488028240 \equiv 1790 \pmod{6010}$$

Así, el par $(r,s) = (5699, 1790)$ es la firma digital del mensaje *m=300*.

Bernardo verifica la autenticidad de la firma de Alicia

Bernardo deberá comprobar que

$$g^m \equiv \beta^r . r^s \pmod p$$

Es decir, chequeará si

$$13^{300} \equiv 2023^{5699} . 5699^{1790} \pmod{6011}$$

Entonces calcula

$$13^{300} \equiv 1329 \pmod{6011}$$

Por otro lado, calcula

$$2023^{5699} . 5699^{1790} \equiv (433).(1072) = 464176 \equiv 1329 \pmod{6011}$$

Luego, se verifica que $g^m \equiv \beta^r . r^s \pmod p$. En consecuencia, el mensaje *m=300* procede efectivamente de Alicia.

CAPÍTULO 3

Los Qubits

A diferencia de una computadora clásica, donde la unidad mínima de información es el ***bit***, en una computadora cuántica la unidad mínima de información es el ***qubit*** o ***bit cuántico*** (del inglés ***qu****antum* ***bit***).
En este capítulo definiremos el qubit para luego desarrollar sistemas cuánticos formados por dos o más qubits. Mencionaremos, además, la propiedad fundamental que los caracteriza: *la superposición*.

3.1 Sistemas formados por un qubit

Los sistemas computacionales cuánticos formados por un qubit procesan la información utilizando un qubit. Su definición matemática es la siguiente:

Definición 3.1: qubit
Un qubit es un vector $\boldsymbol{q} \in \mathbb{C}^2$ *de módulo 1. Es decir,*

$$\boldsymbol{q} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Donde $\alpha\ ,\ \beta\ \in \mathbb{C}$ *y tal que* $|\alpha|^2 + |\beta|^2 = 1$

Como un qubit se puede escribir de la forma

$$\boldsymbol{q} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Diremos que el conjunto $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ es una base ortonormal para el sistema formado por un qubit. Por otro lado, si establecemos la siguiente notación:

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

Entonces la Definición *3.1* se puede reformular de la siguiente manera:

Definición 3.2:

Un qubit es un vector $\boldsymbol{q}$ *de la forma*

$$\boldsymbol{q} = \alpha\ |0\rangle + \beta\ |1\rangle$$

Donde

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ y $\alpha\ ,\ \beta\ \in \mathbb{C}$ *con* $|\alpha|^2 + |\beta|^2 = 1$

En este caso, el conjunto $\{\ |0\rangle\ ,\ |1\rangle\ \}$ *constituye una base para el sistema formado por un qubit. Los vectores* $|0\rangle$ y $|1\rangle$ *se corresponden con el 0 y 1 del bit clásico.*

¿Qué representa físicamente un qubit?

Un qubit representa el estado de una partícula subatómica. En algunas computadoras cuánticas se toma como qubit al estado de polarización de un fotón. Pero en otras, y así lo supondremos a lo largo de este trabajo, se toma como partícula subatómica al electrón situado en la órbita más externa de un determinado átomo. En este caso, el estado que se considera es su *spin*. El *spin* (que significa giro en inglés), descubierto en 1925, es la facultad que tiene el electrón de poseer un *momento angular propio o intrínseco*.

Para hacer una analogía con la Mecánica Clásica y sólo por razones didácticas, imaginaremos que el electrón es un cuerpo que gira en torno a su eje. Su sentido de giro queda determinado por "La Regla de la mano derecha". Entonces el spin representa la posición del eje de rotación del electrón. Si el electrón está **spín arriba**, se encuentra en su mayor nivel de energía y se supone que está en estado **0**. Mientras que si está **spín abajo**, su nivel energético es el más bajo y se dice que está en estado **1**.

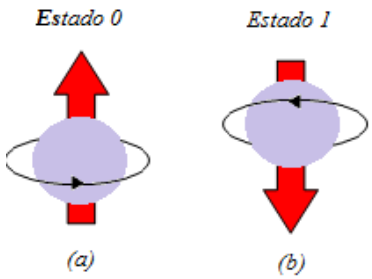


Figura 3.1: (a) Electrón girando spín arriba. En ese caso, se supone que hay almacenado un 0.
(b) Electrón girando spin abajo. Se asume que hay almacenado un 1.
Fuente: Referencia [3]

Pero el electrón también puede girar en cualquier otra posición comprendida entre el estado 0 y el estado 1. Es decir, puede rotar en una posición que es combinación lineal de ambos estados.

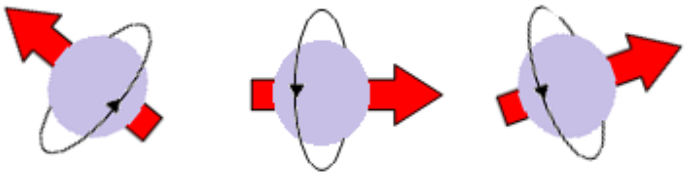


Figura 3.2: Distintas posiciones del eje de giro de un electrón
Fuente: Referencia [3]

Haciendo una analogía con el mundo visible a los ojos humanos, algunos comparan el spin del electrón con el eje de rotación de un trompo, el cual puede ir variando de posición.

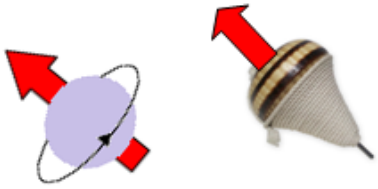


Figura 3.3: Analogía entre el giro de un electrón y el de un trompo.
Fuente: Referencia [3]

En caso de que el eje de rotación tome una posición distinta a la de spin arriba o spin abajo, se supone que el electrón está en ambos estados al mismo tiempo.
Por esta razón se afirma que un qubit puede adoptar simultáneamente los estados 0 y 1. Este hecho es lo que permite, a una computadora cuántica, procesar varios datos simultáneamente.

¿Por qué se define matemáticamente un qubit de este modo?

El hecho de que un qubit se modele matemáticamente como un vector de módulo *1* en el espacio vectorial complejo bidimensional se debe al Primer Postulado de la Física Cuántica, que afirma lo siguiente:

> ***Primer Postulado de la Mecánica Cuántica:***
>
> *Asociado a cada **sistema físico**, se encuentra un espacio de Hilbert **H**, conocido como **espacio de estados** del sistema. El sistema es completamente descripto por su **vector de estado**, el cual es un **vector unitario** en dicho espacio de estados.*

En este caso, el sistema físico que hace referencia este Postulado es el electrón de la órbita más externa de un determinado átomo. El espacio de Hilbert ***H*** es $\mathbb{C}^2$ y el estado que se estudia de este sistema es su spin. De este modo, el sistema queda completamente descripto mediante su vector de estado, que es un vector unitario en $\mathbb{C}^2$. Para más detalles acerca de la definición de espacio de Hilbert, puede consultarse la Referencia [3].

A continuación definiremos la propiedad de *superposición de un qubit*, gracias a la cual los computadores cuánticos pueden procesar información a una velocidad considerablemente mayor que la de los ordenadores clásicos.

> ***Definición 3.3: Estado de superposición de un qubit***
>
> *Dado un qubit*
>
> $$\boldsymbol{q} = \alpha \ |0\rangle + \beta \ |1\rangle$$
>
> *Entonces*
>
> *1) Si q = $|0\rangle$ se dice que el qubit está en estado 0 o "spin arriba".*
>
> *2) Si q = $|1\rangle$ se dice que el qubit está en estado 1 o "spin abajo".*
>
> *3) Si $\alpha \neq 0 \ \wedge \ \beta \neq 0$ se dice que el qubit está en **estado de superposición**, lo cual significa que se encuentra simultáneamente en los estados clásicos 1 y 0.*

Cabe destacar que el estado de superposición de un qubit sólo se logra bajo condiciones de absoluto aislamiento, ya que si entra en contacto con el medio ambiente, el qubit sólo puede estar en dos estados: estado *0* (*spin arriba*) o bien estado *1 (spin abajo)*.

Ejemplo 3.4

Indicar si los siguientes vectores complejos representan qubits y, en caso afirmativo, indicar si están en estado de superposición:

a) $q_1 = \begin{pmatrix} \frac{1+i}{\sqrt{3}} \\ \frac{i}{\sqrt{3}} \end{pmatrix}$ b) $q_2 = \begin{pmatrix} \frac{1}{2}i \\ \frac{1}{4} \end{pmatrix}$

Solución

Teniendo en cuenta que si $z = a + i\,b$ es un número complejo, el cuadrado de su módulo es $|z|^2 = a^2 + b^2$. Entonces

a) $\left|\frac{1+i}{\sqrt{3}}\right|^2 + \left|\frac{i}{\sqrt{3}}\right|^2 = \left(\frac{1}{\sqrt{3}}\right)^2 + \left(\frac{1}{\sqrt{3}}\right)^2 + \left(\frac{1}{\sqrt{3}}\right)^2 = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1$

Luego, q_1 representa un qubit. Por otro lado, q_1 está en estado de superposición ya que $\alpha = \frac{1+i}{\sqrt{3}} \neq 0$ y $\beta = \frac{i}{\sqrt{3}} \neq 0$.

b) $\left|\frac{1}{2}\,i\right|^2 + \left|\frac{1}{4}\right|^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{1}{4} + \frac{1}{16} = \frac{5}{16} \neq 1$

En consecuencia, q_2 no representa un qubit.

¿Cómo medir el estado de un qubit?

Según el Principio de Superposición de la Mecánica Cuántica, mientras una partícula subatómica no interactúa con su entorno, ésta puede estar en varios estados al mismo tiempo. En particular, un qubit $q = \alpha\ |0\rangle + \beta\ |1\rangle$ puede estar a la vez en estado *0* y en estado *1*, si $\alpha \neq 0 \wedge \beta \neq 0$. Sin embargo, en el instante en que es sometido a una medición mediante un láser, el qubit "colapsa" a uno de estos dos estados: *0* (spin arriba) o bien *1(spin abajo)*. Pero, ¿cómo saber a cuál de estos dos estados colapsará el qubit inmediatamente antes de efectuar la medición? Sólo se puede saber en términos de probabilidades y, para calcularlas, se aplica la siguiente definición, basada en el Tercer Postulado de la Mecánica Cuántica:

Definición 3.5: Medida de un qubit

Dado un sistema formado por un qubit, cuyo estado se describe mediante el vector

$$\boldsymbol{q} = \alpha\ |0\rangle + \beta\ |1\rangle$$

Si al qubit se lo somete a una observación entonces:

El número $|\alpha|^2$ *indica la probabilidad de encontrar el qubit del sistema en estado 0.*

Mientras que $|\beta|^2$ *da la probabilidad de encontrar el qubit del sistema en estado 1.*

Ejemplo 3.6

Dado el qubit $q = \left(\frac{1-i}{\sqrt{3}} \right) |0\rangle + \frac{1}{\sqrt{3}} |1\rangle$

a) ¿Cuál es la probabilidad de que, al ser sometido a una medición, éste se encuentre en estado 0 o spin arriba?

a) ¿Cuál es la probabilidad de que, al ser sometido a una medición, éste se encuentre en estado 1 o spin abajo?

c) ¿Es posible que al ser observado el qubit, se encuentre simultáneamente en estado 0 y en estado 1?

Solución

a) La probabilidad de que el qubit se encuentre en estado 0 es

$$\left| \frac{1-i}{\sqrt{3}} \right|^2 = \left(\frac{1}{\sqrt{3}} \right)^2 + \left(-\frac{1}{\sqrt{3}} \right)^2 = \frac{1}{3} + \frac{1}{3} = \frac{2}{3} .$$

b) La probabilidad de que el qubit se encuentre en estado 1 es

$$\left| \frac{1}{\sqrt{3}} \right|^2 = \left(\frac{1}{\sqrt{3}} \right)^2 = \frac{1}{3} .$$

c) No es posible que el qubit, al ser observado, se encuentre simultáneamente en los estados 0 y 1, ya que colapsará solamente a uno de estos dos estados.

Cabe preguntarse qué pasaría si las computadoras cuánticas utilizaran, para procesar los datos, más de un qubit. En estos casos los qubits comienzan a interactuar entre sí para generar un nuevo sistema físico. En la próxima sección mostraremos cómo describir su estado. Veremos que el producto tensorial desempeñará un rol importante, ya que permitirá modelar matemáticamente este tipo de sistemas.

3.2 Sistemas formados por varios qubits

Para describir el estado de un sistema formado por varios qubits, recurriremos al Cuarto Postulado de la Mecánica Cuántica:

Cuarto Postulado de la Mecánica Cuántica:

El espacio de estados de un sistema compuesto por dos o más sistemas físicos es el producto tensorial de los espacios de estado de cada uno de sus componentes.
Más específicamente, si los sistemas físicos están numerados de 1 a n y si el estado de cada sistema es q_i , con i = 1,…,n entonces el estado del sistema compuesto será

$$q_1 \otimes q_2 \otimes .... q_n$$

Por razones didácticas comenzaremos describiendo los sistemas formados por *2* qubits, luego por *3* qubits, para finalmente generalizarlos a *n* qubits.

3.2.1 Sistemas formados por dos qubits

Según el Cuarto Postulado de la Mecánica Cuántica el estado de un sistema formado por dos qubits q_1 y q_2 queda determinado por el producto tensorial $q_1 \otimes q_2$.
A fin de simplificar la expresión de los productos tensoriales, introduciremos la siguiente notación:

Notación 3.7:
Si $x, y \in \{ 0 , 1 \}$ *entonces se escribe*

$$|x\rangle \otimes |y\rangle = |x\ y\rangle \quad \textit{o bien} \quad |x\rangle \otimes |y\rangle = |x\ , y\rangle \quad \textit{o bien} \quad |x\rangle \otimes |y\rangle = |x\rangle\ |y\rangle$$

Por lo tanto, si

$$q_1 = \alpha_1 |0\rangle + \beta_1 |1\rangle \quad y \quad q_2 = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

Entonces, al aplicar las propiedades del producto tensorial resulta

$$q_1 \otimes q_2 = \left(\alpha_1 |0\rangle + \beta_1 |1\rangle\right) \otimes \left(\alpha_2 |0\rangle + \beta_2 |1\rangle\right) =$$

$$= \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle$$

Al calcular estos productos tensoriales obtenemos

$$|0\ 0\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|0\ 1\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|1\ 0\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|1\ 1\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} \approx \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

En consecuencia,

$$q_1 \otimes q_2 = \begin{pmatrix} \alpha_1 \ \alpha_2 \\ \alpha_1 \ \beta_2 \\ \beta_1 \ \alpha_2 \\ \beta_1 \ \beta_2 \end{pmatrix}$$

Como se puede comprobar, el producto tensorial de dos qubits genera un vector de 2^2 componentes. Por otro lado, según el Primer Postulado de la Mecánica Cuántica, el vector de estado del sistema debe ser de módulo *1*. Esto da lugar a definir un *2*-qubit de la siguiente manera:

Definición 3.8: 2-qubit

Un 2- qubit es un vector $\boldsymbol{q} \in \mathbb{C}^4$ *de módulo 1. Es decir,*

$$\boldsymbol{q} = (a_0, a_1, a_2, a_3)^T$$

Donde $a_0, a_1, a_2, a_3 \in \mathbb{C}$ *y verifican que* $\sum_{i=0}^{3} |a_i|^2 = 1$

Teniendo en cuenta que $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ es una base para el espacio de los *2*-qubits, la Definición 3.8 se puede reformular de la siguiente manera:

Definición 3.9:

Un 2- qubit es un vector $\boldsymbol{q}$ *de la forma*

$$\boldsymbol{q} = a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_2 |11\rangle$$

Donde

$a_0, a_1, a_2, a_3 \in \mathbb{C}$ *y* $\sum_{i=0}^{3} |a_i|^2 = 1$

En este caso, el conjunto $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ *constituye una base para el espacio de los 2- qubits*

De este modo, un *2*-qubit es un vector que describe el estado de un sistema formado por dos qubits. Nuevamente, del Tercer Postulado de la Mecánica Cuántica se deduce la siguiente definición:

Definición 3.10: Medida de un 2- qubit

Dado un sistema formado por dos qubits, cuyo estado se describe mediante el 2-qubit

$$\boldsymbol{q} = a_0 \ |00\rangle + a_1 \ |01\rangle + a_2 \ |10\rangle + a_2 \ |11\rangle$$

Si ambos qubits son observados entonces

$|\ a_0\ |^2$ *indica la probabilidad de encontrar el primer y segundo qubit del sistema en estado 0.*

$|\ a_1\ |^2$ *indica la probabilidad de encontrar el primer qubit del sistema en estado 0 y el segundo qubit del sistema en estado 1.*

$|\ a_2\ |^2$ *indica la probabilidad de encontrar el primer qubit del sistema en estado 1 y el segundo qubit del sistema en estado 0.*

$|\ a_3\ |^2$ *indica la probabilidad de encontrar el primer y segundo qubit del sistema en estado 1.*

Ejemplo 3.11

Se tiene un sistema cuántico formado por dos qubits, cuyo estado está definido mediante el 2-qubit $q = \frac{3}{5} i \ |00\rangle + \frac{1}{2} \ |10\rangle + \frac{\sqrt{39}}{10} \ |01\rangle$. Se ha decidido observar los dos qubits que componen el sistema.

a) ¿Cuál es la probabilidad de que ambos qubits estén en estado 0?
b) ¿Cuál es la probabilidad de que el primer qubit esté en estado 1 y el segundo en estado 0?
c) ¿Cuál es la probabilidad de que ambos qubits estén en estado 1?

Solución

a) La probabilidad de que ambos qubits estén en estado 0 es $\left| \frac{3}{5} i \right|^2 = \left(\frac{3}{5}\right)^2 = \frac{9}{25}$.

b) La probabilidad de que el primer qubit esté en estado *1* y el segundo en estado *0* es $\left| \frac{1}{2} \right|^2 = \left(\frac{1}{2}\right)^2 = \frac{1}{4}$.

c) La probabilidad de que ambos qubits estén en estado *1* es *0*.

Como mencionamos anteriormente, al medir el estado de un qubit del sistema, únicamente es posible obtener dos resultados: estado *0* o bien estado *1*. Además, antes de efectuar la medición, sólo se puede predecir en términos de probabilidades en qué estado se hallará dicho qubit. Así, el cálculo de probabilidades estará siempre presente a lo largo de este trabajo y por esta razón introduciremos la siguiente:

Notación 3.12:

$P\left(q_i = |0\rangle\right) = Prob\left(q_i = 0\right) =$ *Probabilidad de encontrar el i-ésimo qubit del sistema en estado 0.*

$P\left(q_i = |1\rangle\right) = Prob\left(q_i = 1\right) =$ *Probabilidad de encontrar el i-ésimo qubit del sistema en estado 1.*

Ejemplo 3.13

Se tiene un sistema cuántico formado por dos qubits, cuyo estado se describe mediante el *2*-qubit

$$q = \frac{1}{4} i\,|00\rangle + \left(\frac{1}{3} + \frac{1}{2} i\right)|01\rangle + \frac{1}{2}\,|10\rangle + \frac{\sqrt{47}}{12}|11\rangle .$$

Se ha decidido efectuar la medición de ambos qubits.

a) ¿Cuál es la probabilidad de que el primer qubit esté en estado 1 y el segundo en estado 0?
b) ¿Cuál es la probabilidad de que el segundo qubit esté en estado 1?

Solución

a) $P\left(q_1 = |1\rangle \wedge q_2 = |0\rangle\right) = \left|\frac{1}{2}\right|^2 = \left(\frac{1}{2}\right)^2 = \frac{1}{4}$.

b) Al aplicar las propiedades del cálculo de probabilidades resulta

$$P\left(q_2 = |1\rangle\right) = P\left(q_2 = |1\rangle \wedge \left(q_1 = |0\rangle \vee q_1 = |1\rangle\right)\right) =$$
$$P\left(\left(q_2 = |1\rangle \wedge q_1 = |0\rangle\right) \vee \left(q_2 = |1\rangle \wedge q_1 = |1\rangle\right)\right) =$$

$$= P\left(q_2 = |1\rangle \wedge q_1 = |0\rangle\right) + P\left(q_2 = |1\rangle \wedge q_1 = |1\rangle\right) =$$

$$= \left|\frac{1}{3} + \frac{1}{2} i\right|^2 + \left|\frac{\sqrt{47}}{12}\right|^2 = \left(\frac{1}{3}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{47}}{12}\right)^2 = \frac{1}{9} + \frac{1}{4} + \frac{47}{144} = \frac{11}{16} .$$

A continuación describiremos los sistemas cuánticos formados por *3* qubits, para luego generalizar a *n* qubits.

3.2.2 Sistemas formados por tres qubits

El estado de un sistema formado por tres qubits q_1 , q_2 y q_3 queda determinado, según el Cuarto Postulado de la Física Cuántica, por el producto tensorial $q_1 \otimes q_2 \otimes q_3$.
Nuevamente, a fin de simplificar la expresión de los productos tensoriales, introduciremos la siguiente:

Notación 3.14
Si $x, y, z \in \{ 0 , 1 \}$ *entonces se escribe*

$$|x\rangle \otimes |y\rangle \otimes |z\rangle = |x\ y\ z\rangle$$

O bien

$$|x\rangle \otimes |y\rangle \otimes |z\rangle = |x\ y\rangle\ |z\rangle$$

O bien

$$|x\rangle \otimes |y\rangle \otimes |z\rangle = |x\rangle |y\rangle |z\rangle$$

O bien

$$|x\rangle \otimes |y\rangle \otimes |z\rangle = |x , y , z\rangle$$

Por lo tanto, si

$$q_1 = \alpha_1 |0\rangle + \beta_1 |1\rangle,\ q_2 = \alpha_2 |0\rangle + \beta_2 |1\rangle \ \text{ y } \ q_3 = \alpha_3 |0\rangle + \beta_3 |1\rangle$$

Entonces, al aplicar las propiedades del producto tensorial obtenemos

$$q_1 \otimes q_2 \otimes q_3 = \left(\alpha_1 |0\rangle + \beta_1 |1\rangle\right) \otimes \left(\alpha_2 |0\rangle + \beta_2 |1\rangle\right) \otimes \left(\alpha_3 |0\rangle + \beta_3 |1\rangle\right) =$$

$$= \alpha_1\ \alpha_2\ \alpha_3 |000\rangle + \alpha_1\ \alpha_2\ \beta_3 |001\rangle + \alpha_1\ \beta_2\ \alpha_3 |010\rangle + \alpha_1\ \beta_2\ \beta_3 |011\rangle +$$

$$+ \beta_1\ \alpha_2\ \alpha_3 |100\rangle + \beta_1\ \alpha_2\ \beta_3 |101\rangle + \beta_1\ \beta_2\ \alpha_3 |110\rangle + \beta_1\ \beta_2\ \beta_3 |111\rangle$$

Al calcular estos productos tensoriales resulta

$$|\ 0\ 0\ 0\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \approx \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\begin{pmatrix}1\\0\end{pmatrix}\\0\begin{pmatrix}1\\0\end{pmatrix}\\0\begin{pmatrix}1\\0\end{pmatrix}\\0\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} =$$

$$= \begin{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\\\begin{pmatrix}0\\0\end{pmatrix}\\\begin{pmatrix}0\\0\end{pmatrix}\\\begin{pmatrix}0\\0\end{pmatrix}\end{pmatrix} \approx \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$$

Y así para los demás casos. Luego,

$$q_1 \otimes q_2 \otimes q_3 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1 & \alpha_2 & \beta_3 \\ \alpha_1 & \beta_2 & \alpha_3 \\ \alpha_1 & \beta_2 & \beta_3 \\ \beta_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \alpha_2 & \beta_3 \\ \beta_1 & \beta_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{pmatrix}$$

De este modo, el producto tensorial de *3* qubits genera un vector de 2^3 componentes. Además, por el Primer Postulado de la Física Cuántica, el vector de estado del sistema debe tener módulo *1*. Esto da lugar a definir un *3*-qubit de la siguiente manera:

Definición 3.15: 3-qubit

Un 3- qubit es un vector $\boldsymbol{q} \in \mathbb{C}^8$ *de módulo 1. Es decir,*

$$\boldsymbol{q} = (a_0 , a_1 , a_2 , a_3 , a_4 , a_5 , a_6 , a_7)^T$$

Donde $a_i \in \mathbb{C} \ \forall\, i = 0,...,7$ *y verifican que* $\sum_{i=0}^{7} | a_i |^2 = 1$

Teniendo en cuenta que

$$\{ |000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle \}$$

Es una base para el espacio de los *3*- qubits, la Definición *3.15* se reescribe de la siguiente manera:

Definición 3.16:

Un 3- qubit es un vector $\boldsymbol{q}$ *de la forma*

$$\boldsymbol{q} = a_0 |000\rangle + a_1 |001\rangle + a_2 |010\rangle + a_3 |011\rangle + a_4 |100\rangle + a_5 |101\rangle + a_6 |110\rangle + a_7 |111\rangle$$

Donde

$$a_i \in \mathbb{C} \ \forall\, i = 0,...,7 \quad y \quad \sum_{i=0}^{7} | a_i |^2 = 1$$

En este caso, el conjunto

$$\{ | 000 > , | 001 > , | 010 > , | 011 > , | 100 > , | 101 > , | 110 > , |111 > \}$$

Constituye una base para el espacio de los 3- qubits.

De este modo, un *3*-qubit es un vector que describe el estado de un sistema formado por tres qubits. La medida de un *3*-qubit se define de manera similar a las Definiciones *3.5*

y *3.10*. Por ejemplo, si los qubits son observados, entonces $|a_1|^2$ indica la probabilidad de encontrar el primer y segundo qubit del sistema en estado *0* y el tercer qubit del sistema en estado *1*.
A continuación definiremos los *n*- qubits, los cuales permitirán describir el estado de un sistema formado por *n* qubits.

3.2.3 Sistemas formados por n qubits

El estado de un sistema formado por *n* qubits se describe mediante un *n*-qubit. Su definición surge del Primer y Cuarto Postulado de la Mecánica Cuántica y es la siguiente:

Definición 3.17: n-qubit

Dado un número natural n, un n- qubit es un vector $q \in \mathbb{C}^{2^n}$ *de módulo 1. Es decir,*

$$q = \left(a_0 \ , a_1 \ , \ \dots \ , \ a_{2^n - 1} \right)^T$$

Donde $a_i \in \mathbb{C} \ \ \forall \ i = 0, \dots , 2^n - 1$ *y tales que* $\sum_{i=0}^{2^n - 1} |a_i|^2 = 1$

En este caso, una base del espacio de los *n*- qubits es

$$\left\{ |x_{n-1} \ x_{n-2} \ \dots . x_1 \ x_0\rangle \ \ con \ \ x_i = 0 \ \acute{o} \ 1 \ , \ \ i = 0, 1 \ ,\dots , n - 1 \right\}$$

Donde $|x_{n-1} \ x_{n-2} \ \dots . x_1 \ x_0\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \dots . \otimes |x_1\rangle \otimes |x_0\rangle$

Si quisiéramos representar un *n*-qubit como combinación lineal de los elementos de esta base (de una manera similar a la planteada en las Definiciones 3.9 y 3.16) entonces su expresión, con esta notación, se tornaría engorrosa si *n* fuera muy grande.
Por esta razón adoptaremos la siguiente convención:

Notación 3.18:

Si $x_i = 0 \ \acute{o} \ 1$ *con* $i = 0, 1 \ ,\dots , n - 1$ *entonces*

$$|x_{n-1} \ x_{n-2} \ \dots . x_1 \ x_0\rangle \equiv |x\rangle$$

Donde x es la representación en base 10 del número binario $x_{n-1} \ x_{n-2} \ \dots . x_1 \ x_0$ *. Es decir,*

$$x = 2^0 \ x_0 \ + 2^1 \ x_1 \ + \dots . + 2^{n-2} \ x_{n-2} \ + 2^{n-1} \ x_{n-1}$$

En el siguiente ejemplo mostraremos cómo aplicar esta notación.

Ejemplo 3.19

Dado el *3*-qubit

$$q = a_0\ |000\rangle + a_1\ |001\rangle + a_2\ |010\rangle + a_3\ |011\rangle + a_4\ |100\rangle + a_5\ |101\rangle + a_6\ |110\rangle + a_7\ |111\rangle$$

Expresarlo según la Notación *3.18*

Solución

El siguiente cuadro muestra cómo representar cada elemento de la base del espacio de los *3*-qubits:

Número binario	***Representación en base 10***
000	$0.\left(2^0\right)+0.\left(2^1\right)+0.\left(2^2\right)=0$
001	$1.\left(2^0\right)+0.\left(2^1\right)+0.\left(2^2\right)=1$
010	$0.\left(2^0\right)+1.\left(2^1\right)+0.\left(2^2\right)=2$
011	$1.\left(2^0\right)+1.\left(2^1\right)+0.\left(2^2\right)=3$
100	$0.\left(2^0\right)+0.\left(2^1\right)+1.\left(2^2\right)=4$
101	$1.\left(2^0\right)+0.\left(2^1\right)+1.\left(2^2\right)=5$
110	$0.\left(2^0\right)+1.\left(2^1\right)+1.\left(2^2\right)=6$
111	$1.\left(2^0\right)+1.\left(2^1\right)+1.\left(2^2\right)=7$

Por lo tanto

$$\begin{aligned}
|000\rangle &\equiv |0\rangle \\
|001\rangle &\equiv |1\rangle \\
|010\rangle &\equiv |2\rangle \\
|011\rangle &\equiv |3\rangle \\
|100\rangle &\equiv |4\rangle \\
|101\rangle &\equiv |5\rangle \\
|110\rangle &\equiv |6\rangle \\
|111\rangle &\equiv |7\rangle
\end{aligned}$$

En consecuencia, el *3*-qubit *q* se escribe

$$q = \sum_{i=0}^{7} a_i\ |i\rangle .$$

Con esta nueva notación para los elementos de la base del espacio de los *n*-qubits, se puede extender las Definiciones *3.9* y *3.16* del siguiente modo:

Definición 3.20:

Un n- qubit es un vector ***q*** *de la forma*

$$\boldsymbol{q} = \sum_{i=0}^{2^n-1} a_i \ |i\rangle$$

Donde

$a_i \in \mathbb{C} \ \forall\ i = 0,..., 2^n - 1$ *y* $\sum_{i=0}^{2^n-1} |\ a_i\ |^2 = 1$ *. En este caso, el conjunto*

$$\left\{ |0\rangle\ ,\ |1\rangle\ ,\ |2\rangle\ ,\ ....\ ,\ \left|2^n - 1\right\rangle \right\}$$

Constituye una base para el espacio de los n- qubits

Ejemplo 3.21

Se tiene un sistema cuántico formado por *5* qubits, cuyo estado se describe mediante el *5*-qubit

$$q = \left(\frac{1}{2} + \frac{1}{4}i\right)\ |1\rangle\ +\ \frac{1}{8}\ |5\rangle\ +\ \frac{1}{2}i\ |21\rangle\ +\ \frac{\sqrt{3}}{4}\ |25\rangle - \frac{1}{4}\ |30\rangle\ +\ \frac{\sqrt{11}}{8}i\ |31\rangle$$

a) Expresar el qubit *q* en notación binaria.
b) ¿Cuál es la probablidad de que, al observar todos los qubits, el quinto qubit esté en estado *1* y los restantes en estado 0?
c) ¿Cuál es la probabilidad de que, al medir todos los qubits, el quinto qubit esté en estado 1?

Solución

a) Primeramente se expresan $|1\rangle, |5\rangle, |21\rangle, |25\rangle, |30\rangle\ y\ |31\rangle$ en notación binaria:

Número decimal	***Representación binaria***
1	*00001*
5	*00101*
21	*10101*
25	*11001*
30	*11110*
31	*11111*

Por lo tanto

$$q = \left(\frac{1}{2} + \frac{1}{4}i\right)\ |00001\rangle + \frac{1}{8}\ |00101\rangle + \frac{1}{2}i\ |10101\rangle + \frac{\sqrt{3}}{4}\ |11001\rangle - \frac{1}{4}\ |11110\rangle + \frac{\sqrt{11}}{8}i\ |11111\rangle$$

b) $P\left(q_1 = |0\rangle \wedge q_2 = |0\rangle \wedge q_3 = |0\rangle \wedge q_4 = |0\rangle \wedge q_5 = |1\rangle\ \right) = \left|\frac{1}{2} + \frac{1}{4}i\right|^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{5}{16}$

c) $P\left(q_5 = |1\rangle\right) = \left|\frac{1}{2} + \frac{1}{4}i\right|^2 + \left|\frac{1}{8}\right|^2 + \left|\frac{1}{2}i\right|^2 + \left|\frac{\sqrt{3}}{4}\right|^2 + \left|\frac{\sqrt{11}}{8}i\right|^2 =$

$= \frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \frac{1}{4} + \frac{3}{16} + \frac{11}{64} = \frac{15}{16}$.

Cabe preguntarnos cómo evoluciona un sistema cuántico formado por dos o más qubits, cuando solamente algunos qubits son sometidos a observación. Las siguientes Proposiciones responden a esta pregunta, para el caso de sistemas formados por dos o tres qubits.

Proposición 3.22

Sea un sistema compuesto por dos qubits, y cuyo estado se describe mediante el 2-qubit

$$\boldsymbol{q} = a_0\ |00\rangle + a_1\ |01\rangle + a_2\ |10\rangle + a_2\ |11\rangle$$

Entonces

Si una vez realizada la medición sólo del primer qubit del sistema, se obtiene que éste está en estado 0, el 2-qubit evoluciona al siguiente estado:

$$\boldsymbol{q}' = \frac{a_0\ |00\rangle + a_1\ |01\rangle}{\sqrt{|a_0|^2 + |a_1|^2}}$$

Y si se obtiene que éste está en estado 1, el 2-qubit evoluciona a un nuevo estado dado por

$$\boldsymbol{q}' = \frac{a_2\ |10\rangle + a_3\ |11\rangle}{\sqrt{|a_2|^2 + |a_3|^2}}$$

Expresiones similares se obtienen para los resultados de la medida del segundo qubit del sistema.

Demostración: Véase Referencia [5] ■

Proposición 3.23

Sea un sistema compuesto por tres qubits, y cuyo estado se describe mediante el 3-qubit

$$\boldsymbol{q} = a_0\ |000\rangle + a_1\ |001\rangle + a_2\ |010\rangle + a_3\ |011\rangle + a_4\ |100\rangle + a_5\ |101\rangle + a_6\ |110\rangle + a_7\ |111\rangle$$

Entonces

Si una vez realizada la medición de los dos primeros qubits del sistema, se obtiene que ambos están en estado 0, el 3-qubit evoluciona al siguiente estado:

$$\boldsymbol{q}' = \frac{a_0\ |000\rangle + a_1\ |001\rangle}{\sqrt{|a_0|^2 + |a_1|^2}}$$

Expresiones similares se obtienen para las restantes mediciones.

Demostración: Véase Referencia [5] ■

Las Proposición anterior se puede generalizar para el caso de sistemas formados por *n* qubits.

Ejemplo 3.24

Se tiene el siguiente sistema cuántico formado por 2 qubits, cuyo estado se describe mediante el 2-qubit

$$q = 0.5\ |00\rangle + 0.5\ |01\rangle - 0.5\ |10\rangle - 0.5\ |11\rangle$$

Analizar cuál puede ser el estado resultante luego de medir el segundo qubit.

Solución

Sea *q'* el estado que resulta luego de medir el segundo qubit. Entonces

1) Si el segundo qubit quedó en estado 0 al ser observado, el estado resultante del sistema es

$$q' = \frac{0.5\ |00\rangle - 0.5\ |10\rangle}{\sqrt{|\,0.5|^2 + |-0.5|^2}} = \frac{0.5\ |00\rangle - 0.5\ |10\rangle}{\sqrt{0.5}} = \sqrt{0.5}\ |00\rangle - \sqrt{0.5}\ |10\rangle$$

Es decir

$$q' = \sqrt{0.5}\ |00\rangle - \sqrt{0.5}\ |10\rangle$$

2) Si el segundo qubit quedó en estado 1, el estado resultante del sistema es

$$q' = \frac{0.5\ |01\rangle - 0.5\ |11\rangle}{\sqrt{|\,0.5|^2 + |-0.5|^2}} = \frac{0.5\ |01\rangle - 0.5\ |11\rangle}{\sqrt{0.5}} = \sqrt{0.5}\ |01\rangle - \sqrt{0.5}\ |11\rangle$$

Por lo tanto

$$q' = \sqrt{0.5}\ |01\rangle - \sqrt{0.5}\ |11\rangle$$

Ejemplo 3.25

Se tiene el siguiente sistema cuántico formado por *5* qubits, cuyo estado se describe mediante el *5*-qubit

$$q = \left(\frac{1}{2} + \frac{1}{4}i\right)\ |00001\rangle + \frac{1}{8}\ |00101\rangle + \frac{1}{2}i\ |10101\rangle + \frac{\sqrt{3}}{4}\ |11001\rangle - \frac{1}{4}\ |11110\rangle + \frac{\sqrt{11}}{8}i\ |11111\rangle$$

a) Indicar el estado del sistema, tras medir el cuarto qubit y observando que éste quedó en estado 0.

b) Si a continuación se mide el primer qubit y se observa que está en estado 1 ¿en qué estado queda el sistema?

Solución

a) El estado del sistema quedará conformado por los términos de *q* cuyo cuarto qubit esté en estado 0. Es decir que, si llamamos *q'* al nuevo estado del sistema entonces

$$q' = \frac{\left(\frac{1}{2}+\frac{1}{4}i\right)\ |00001\rangle + \frac{1}{8}\ |00101\rangle + \frac{1}{2}i\ |10101\rangle + \frac{\sqrt{3}}{4}\ |11001\rangle}{\sqrt{\left|\frac{1}{2}+\frac{1}{4}i\right|^2 + \left|\frac{1}{8}\right|^2 + \left|\frac{1}{2}i\right|^2 + \left|\frac{\sqrt{3}}{4}\right|^2}} =$$

$$= \frac{\left(\frac{1}{2}+\frac{1}{4}i\right)\ |00001\rangle + \frac{1}{8}\ |00101\rangle + \frac{1}{2}i\ |10101\rangle + \frac{\sqrt{3}}{4}\ |11001\rangle}{\sqrt{\frac{1}{4}+\frac{1}{16}+\frac{1}{64}+\frac{1}{4}+\frac{3}{16}}} =$$

$$= \frac{\left(\frac{1}{2}+\frac{1}{4}i\right)\ |00001\rangle + \frac{1}{8}\ |00101\rangle + \frac{1}{2}i\ |10101\rangle + \frac{\sqrt{3}}{4}\ |11001\rangle}{\sqrt{\frac{49}{64}}} =$$

$$= \frac{\left(\frac{1}{2}+\frac{1}{4}i\right)\ |00001\rangle + \frac{1}{8}\ |00101\rangle + \frac{1}{2}i\ |10101\rangle + \frac{\sqrt{3}}{4}\ |11001\rangle}{\frac{7}{8}} =$$

$$\left(\frac{4}{7}+\frac{2}{7}i\right)\ |00001\rangle + \frac{1}{7}\ |00101\rangle + \frac{4}{7}i\ |10101\rangle + \frac{2\sqrt{3}}{7}\ |11001\rangle$$

Por lo tanto

$$q' = \left(\frac{4}{7}+\frac{2}{7}i\right)\ |00001\rangle + \frac{1}{7}\ |00101\rangle + \frac{4}{7}i\ |10101\rangle + \frac{2\sqrt{3}}{7}\ |11001\rangle$$

b) El estado del sistema quedará compuesto por los términos de *q'* cuyo primer qubit esté en estado 1. Es decir que, si llamamos *q''* al nuevo estado del sistema entonces

$$q'' = \frac{\frac{4}{7}i\ |10101\rangle + \frac{2\sqrt{3}}{7}\ |11001\rangle}{\sqrt{\left|\frac{4}{7}i\right|^2 + \left|\frac{2\sqrt{3}}{7}\right|^2}} = \frac{\frac{4}{7}i\ |10101\rangle + \frac{2\sqrt{3}}{7}\ |11001\rangle}{\sqrt{\frac{16}{49}+\frac{12}{49}}} =$$

$$= \frac{4}{\sqrt{28}}i\ |10101\rangle + \frac{2\sqrt{3}}{\sqrt{28}}\ |11001\rangle$$

Luego

$$q'' = \frac{4}{\sqrt{28}}i\ |10101\rangle + \frac{2\sqrt{3}}{\sqrt{28}}\ |11001\rangle$$

3.2.4 Diferencias entre bits y qubits

El siguiente cuadro resume las principales diferencias entre un bit y un qubit.

Bit	***Qubit***
Es la unidad mínima de información en una computadora clásica.	*Es la unidad mínima de información en una computadora cuántica.*
Sólo puede almacenar un valor: 0 ó 1. Este hecho permite realizar cómputos de a un valor por vez.	*Puede almacenar los valores 0 y 1 al mismo tiempo (Principio de Superposición). Esta propiedad permite realizar cómputos sobre ambos valores a la vez.*
Una computadora clásica que opere con n bits, puede almacenar y procesar n dígitos binarios al mismo tiempo.	*Una computadora cuántica que opere con n qubits, puede almacenar y procesar al mismo tiempo 2^n dígitos binarios (pues un qubit puede estar en estado 0 y 1 al mismo tiempo).*
Se puede medir el valor almacenado en un bit, sin que se altere luego su valor.	*En el momento en que el qubit es medido, éste colapsa en valor 0 o bien en valor 1.*

En base a estas comparaciones, si un ordenador convencional tiene un registro de *n* bits, dicho registro puede tomar 2^n valores posibles, pero el registro puede contener sólo uno de esos valores.
En cambio, si una computadora cuántica posee un registro de *n* qubits, dicho registro puede contener 2^n valores al mismo tiempo, gracias a la propiedad de superposición. Así, se podrán efectuar 2^n operaciones paralelas. De este modo, en una computadora cuántica tendríamos un avance exponencial en los cálculos y en la búsqueda de información en relación a un ordenador clásico.

CAPÍTULO 4

Compuertas, circuitos y algoritmos cuánticos

4.1 Definición y características de una compuerta cuántica

Para manipular la información almacenada en un conjunto de qubits se utilizan compuertas cuánticas. Éstas son para los ordenadores cuánticos lo que las puertas lógicas son para los ordenadores clásicos.
Desde el punto de vista de la Física, una compuerta cuántica es un dispositivo electromagnético que permite modificar el estado de los qubits que ingresan. Es decir, pueden modificar el spin de los electrones que componen el sistema.

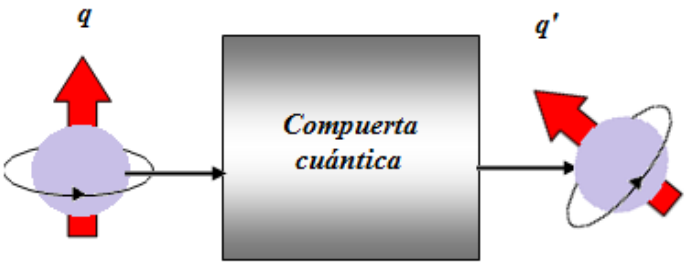


Figura 4.1: Representación gráfica de una compuerta cuántica. q' es el estado en que puede quedar el qubit q al atravesar una compuerta.Fuente: Referencia [12].

Tecnológicamente se la diseña mediante una trampa de iones, que genera campos magnéticos a lo largo de diferentes direcciones, los cuales permiten cambiar la orientación del spin de los electrones del sistema.

Características de las compuertas cuánticas

Las compuertas cuánticas tienen fundamentalmente las siguientes propiedades:

■ ***Reversibilidad***.

Una compuerta es reversible si a partir de los datos de salida se pueden recuperar los datos de entrada. Es decir, para cada compuerta debe haber otra que "deshaga" lo que hizo la primera.

■ ***El número de entradas es igual al número de salidas***

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. Si la compuerta cuántica tuviera menos salidas que entradas, se produciría una disipación de la energía que se transforma en calor y, por consiguiente, estos sistemas se calentarían. Como los estados cuánticos del átomo son extremadamente frágiles, la superposición podría verse afectada ante la más mínima fluctuación de la temperatura, lo que provocaría errores de cálculo. Por otro lado, si la compuerta tuviera más salidas que entradas, la compuerta encargada de recuperar los datos de entrada tendría menos salidas que entradas. Pero, por lo visto anteriormente, también se producirían errores de cálculo.

Cómo modelar matemáticamente una compuerta cuántica

Para modelar matemáticamente una compuerta cuántica, se recurre al Segundo Postulado de la Mecánica Cuántica:

> ***Segundo Postulado de la Mecánica Cuántica:***
>
> *La evolución de un sistema cuántico* ***cerrado*** *(totalmente aislado, sin intercambio de energía con su medio ambiente) se describe mediante una transformación lineal unitaria. Es decir que, si q_1 es el estado del sistema en el instante t_1 y q_2 es el estado en el instante t_2, entonces existe un operador unitario U de modo tal que $q_2 = U\, q_1$.*

El Segundo Postulado sugiere asociar, a cada compuerta cuántica, una transformación lineal unitaria definida en el espacio de los *n*-qubits, ya que éstos describen el estado del sistema. Por otro lado, como los *n*-qubits se identifican con vectores en $\mathbb{C}^{2n}$, la transformación unitaria quedará definida en $\mathbb{C}^{2n}$. Además, sabemos que toda transformación lineal unitaria lleva asociada una matriz unitaria. En base a estas observaciones surge la siguiente definición matemática de compuerta cuántica:

> ***Definición 4.1: Compuerta cuántica desde el punto de vista matemático***
>
> *Una compuerta cuántica, de n qubits de entrada y n qubits de salida, es una matriz unitaria U de orden 2^n, es decir, una matriz $U \in \mathbb{C}^{2n} \times \mathbb{C}^{2n}$ que verifica*
>
> $$U\,U^{+} = U^{+}\,U = I$$
>
> *Donde U^{+} es la traspuesta conjugada de U e I es la matriz Identidad de orden 2n.*

Ejemplo 4.2

Sea la matriz

$$U = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2}i \end{pmatrix}$$

1) Probar que *U* es unitaria.
2) Probar que *U* es una compuerta cuántica e indique sobre qué sistema cuántico opera.
3) Considere el qubit $q = |0\rangle$. ¿A qué estado evoluciona al atravesar la compuerta *U*?
4) ¿Queda el qubit *q* en estado de superposición al atravesar la compuerta *U*?
5) Si se decide observar el qubit *q* una vez que atravesó la compuerta *U*. ¿Cuál es la probabilidad de que éste se encuentre en estado *1*?
6) ¿Existe una compuerta cuántica que permita recuperar el estado inicial del qubit *q* luego de atravesar la compuerta *U*?

Solución

1) Para que U sea unitaria, deberemos verificar que $U.U^{+} = U^{+}.U = I$. Entonces

$$U.U^{+} = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2}i \end{pmatrix} . \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2}i \\ -\frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2}i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

De manera similar se prueba que $U^{+}.U = I$. Luego, U es unitaria.

2) U es una compuerta cuántica pues es una matriz unitaria de orden 2^n, con $n=1$. Luego, dicha compuerta opera sobre un sistema cuántico formado por *1* qubit.

3) Al atravesar la compuerta U, el qubit $q = |0\rangle$ evoluciona, por el Segundo Postulado de la Mecánica Cuántica, al estado

$$q' = U.q = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2}i \end{pmatrix} . \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2}i \end{pmatrix} = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{\sqrt{2}}{2}i\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Por lo tanto, el nuevo estado del sistema es

$$q' = \frac{\sqrt{2}}{2}\ |0\rangle + \frac{\sqrt{2}}{2}i\ \ |1\rangle$$

4) Al atravesar la compuerta U, el qubit quedó en estado de superposición pues los coeficientes que multiplican a son no nulos.

5) $P\left(q' = |1\rangle\right) = \left| \frac{\sqrt{2}}{2}i \right|^2 = \left(\frac{\sqrt{2}}{2}\right)^2 = \frac{1}{2}$

Luego, la probabilidad de que el qubit esté en estado *1* al ser observado es $\frac{1}{2}$.

6) Es posible recuperar el estado inicial del qubit aplicando a q' la compuerta representada por la matriz inversa de U, es decir, U^{+}. De este modo,

$$U^{+}.q' = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2}i \\ -\frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2}i \end{pmatrix} . \begin{pmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2}i \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle = q$$

4.2 Circuitos Cuánticos

Para cualquier cómputo cuántico se necesita diseñar un circuito cuántico, que se define del siguiente modo:

> ***Definición 4.3: Circuito cuántico***
>
> *Un circuito cuántico es un dispositivo que consta de los siguientes elementos:*
>
> *1)* ***Uno o más qubits de entrada****. Éstos sólo pueden estar inicializados en* $|0\rangle$ *o en* $|1\rangle$ *ya que el electrón, al interactuar con el medio ambiente, puede estar únicamente en dos estados: spin arriba o spin abajo.*
>
> *2)* ***Una o más compuertas cuánticas****. Éstas permiten modificar el estado de uno o más qubits que componen el sistema.*
>
> *3)* ***Uno o más qubits de salida****. Ellos son el resultado de los cómputos realizados por las compuertas cuánticas. La medición final se efectúa sobre algunos de los qubits de salida. La cantidad de qubits de salida debe ser igual a la de entrada.*

En la representación gráfica de un circuito cuántico, las compuertas cuánticas se simbolizan mediante rectángulos. Cada qubit de entrada o de salida debe ir acompañado de un segmento horizontal. Los distintos estados de un *n*-qubit al atravesar cada compuerta los simbolizaremos por q, q', q'', etc. El proceso de medición convierte el estado de un qubit $q = \alpha\,|0\rangle + \beta\,|1\rangle$ en un "bit clásico", que será *0* con una probabilidad $|\,\alpha\,|^2$ o bien *1* con una probabilidad $|\,\beta\,|^2$.

El procedimiento de medición de un qubit se lo simboliza así:

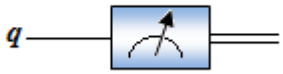


Figura 4.2: Representación gráfica del proceso de medición de un qubit q. Las líneas dobles se utilizan para simbolizar los dos únicos estados que puede tener el qubit al ser observado: 0 o bien 1.

El gráfico de un circuito se lee de izquierda a derecha. La siguiente figura muestra un circuito cuántico formado por dos qubits de entrada:

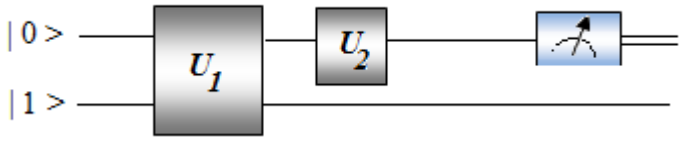


Figura 4.3: Un ejemplo de circuito cuántico.

Las compuertas cuánticas más utilizadas son las de un qubit y dos qubits. Ello se debe a que no siempre es posible implementar en un ordenador cuántico cualquier transformación unitaria. En general, es necesario descomponerla en transformaciones unitarias que operen sobre uno o dos qubits. En la siguiente sección describiremos las que aplicaremos en este trabajo.

4.3 Compuertas cuánticas de un qubit

Desde el punto de vista físico, las compuertas cuánticas que operan sobre un qubit son dispositivos que modifican el spin del electrón. Pero desde el punto de vista matemático, según la Definición *4.1*, las compuertas cuánticas que operan sobre un qubit son matrices unitarias de orden *2*. También se las suele llamar "*compuertas simples*". Las que utilizaremos en esta tesis son las siguientes:

4.3.1 La compuerta de Identidad

Su matriz asociada es la Identidad:

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

Esta compuerta no modifica el estado de los qubits de la base, pues

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

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

Sin embargo, es utilizada pues a partir de ella se pueden generar compuertas de dos o más qubits.

4.3.2 La compuerta de Hadamard

Esta compuerta es sumamente relevante y lleva este nombre en honor al matemático francés Jacques Hadamard (1865-1963). Su matriz asociada es la siguiente:

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

Veamos cómo actúa esta matriz sobre los qubits de la base:

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

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

Como podemos comprobar, la compuerta de Hadamard transforma los qubits $|0\rangle$ y $|1\rangle$ en estados de superposición, permitiendo estar en estado *0* y *1* al mismo tiempo. Por otro lado, los qubits transformados $H|0\rangle$ y $H|1\rangle$ tienen la misma probabilidad de que colapsen a estado 0 o a estado 1 en el instante en que entren en contacto con el medio ambiente (es decir, en el momento en que sean observados o sean sometidos a una medición). El valor de dicha probabilidad es $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$.

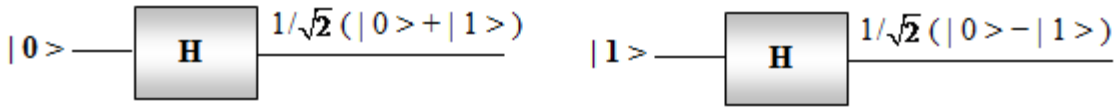


Figura 4.4: Efecto de la compuerta H sobre los qubits de la base.

El estado de superposición es muy difícil mantenerlo en el tiempo, ya que el electrón debe estar completamente aislado, porque si interactúa con el medio ambiente, el estado de superposición se destruye. Esta es una de las causas principales por la cual se torna muy dificultosa la construcción de computadoras cuánticas.

4.3.3 La compuerta R o de desplazamiento de fase

Dado un ángulo θ expresado en radianes, la compuerta de desplazamiento de fase R_θ tiene la siguiente forma matricial:

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

El efecto de esta compuerta sobre los qubits de la base es el siguiente:

$$R_\theta|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\,\theta} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$R_\theta|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\,\theta} \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ e^{i\,\theta} \end{pmatrix} = e^{i\,\theta}|1\rangle$$

Es decir que al qubit $|0\rangle$ lo deja intacto y al qubit $|1\rangle$ lo transforma en $e^{i\,\theta}\,|1\rangle$.

Un caso particular de compuerta R

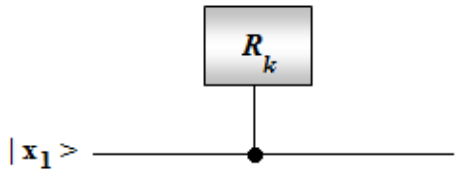
Si consideramos $\theta = \frac{2\,\pi}{2^k}$ con $k \in \mathbb{N}$ y definimos

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\,\pi\,i}{2^k}} \end{pmatrix}$$

Dicha compuerta opera sobre un determinado bit. Por ejemplo, si R_k opera sobre el bit x_1, entonces su expresión queda:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i x_1}{2^k}} \end{pmatrix}$$

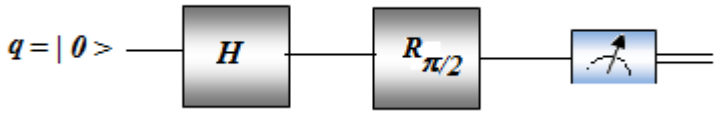
Y su representación gráfica es:



La compuerta de Desplazamiento de Fase, junto con la de Hadamard, serán utilizadas para diseñar el circuito cuántico para la Transformada Cuántica de Fourier.

Ejemplo 4.4

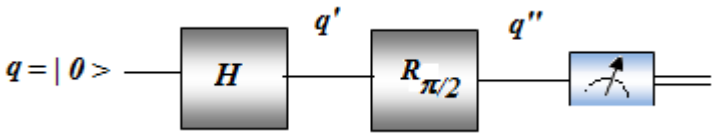
Sea el qubit de entrada $q = |0\rangle$ y el circuito:



1) Indicar el estado del qubit al atravesar cada compuerta.
2) ¿Cuál es la probabilidad de que, al observar el qubit de salida, esté en estado 1?

Solución

1) Simbolizaremos por q' y q'' a los estados del qubit q al atravesar las compuertas H y $R_{\pi/2}$ respectivamente.



Al aplicar el Segundo Postulado de la Mecánica Cuántica, los estados del qubit se obtienen del siguiente modo:

$q = |0\rangle$

$$q' = H\ q = H\ |0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$q'' = R_{\pi/2}\ q' = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & cos\left(\frac{\pi}{2}\right) + i\ sen\left(\frac{\pi}{2}\right) \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -i\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

2) Si $q = |0\rangle$, el qubit de salida del sistema es

$q'' = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -i\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - i\ \frac{1}{\sqrt{2}}|1\rangle$. Por lo tanto,

$$P\left(q'' = |1\rangle\right) = \left|-i\ \frac{1}{\sqrt{2}}\right|^2 = \left|-\ \frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Ejemplo 4.5

¿Existe una compuerta cuántica que lleve el qubit $|0\rangle$ al qubit $|1\rangle$ y el qubit $|1\rangle$ al qubit $\frac{1}{2}i\ |0\rangle + \frac{\sqrt{3}}{2}\ |1\rangle$?

Solución

Probaremos que no existe una matriz unitaria U de orden 2 tal que

$$\begin{cases} U.|0\rangle = |1\rangle \\ U.|1\rangle = \frac{1}{2}i\ |0\rangle + \frac{\sqrt{3}}{2}\ |1\rangle \end{cases}.$$

Supongamos por el absurdo que sí existe tal matriz. Por lo tanto, si

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Entonces

$$\begin{cases} U|0\rangle = |1\rangle \\ U|1\rangle = \frac{1}{2}i\ |0\rangle + \frac{\sqrt{3}}{2}\ |1\rangle \end{cases} \Rightarrow \begin{cases} \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}i \\ \frac{\sqrt{3}}{2} \end{pmatrix} \end{cases} \Rightarrow \begin{cases} \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} \frac{1}{2}i \\ \frac{\sqrt{3}}{2} \end{pmatrix} \end{cases} \Rightarrow \begin{cases} a = 0 \\ c = 1 \\ b = \frac{1}{2}i \\ d = \frac{\sqrt{3}}{2} \end{cases}$$

De aquí resulta que

$$U = \begin{pmatrix} 0 & \frac{1}{2}i \\ 1 & \frac{\sqrt{3}}{2} \end{pmatrix}$$

Por otro lado, como U es una matriz unitaria, entonces

$$U.U^{+} = I \Rightarrow U.\overline{U^{T}} = I \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & \frac{1}{2}i \\ 1 & \frac{\sqrt{3}}{2} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -\frac{1}{2}i & \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow$$

$$\Rightarrow \begin{pmatrix} \frac{1}{4} & \frac{\sqrt{3}}{4}i \\ -\frac{\sqrt{3}}{4}i & \frac{7}{4} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Al igualar los respectivos coeficientes de ambas matrices resulta

$$\begin{cases} \frac{1}{4} = 1 \\ \frac{\sqrt{3}}{4}i = 0 \\ -\frac{\sqrt{3}}{4}i = 0 \\ \frac{7}{4} = 1 \end{cases}$$

Lo cual es una contradicción. En consecuencia, no existe una compuerta cuántica que verifique la condición que indica el enunciado.

4.3.4 Representación gráfica del efecto de una compuerta cuántica sobre un qubit

Para representar gráficamente los qubits, se utiliza una esfera centrada en el origen y de radio 1, llamada *La Esfera de Bloch* (para más detalles, ver Referencia [3], pág. *27*). *La Esfera de Bloch* permite visualizar el estado de un qubit que, como mencionamos en el Capítulo *3*, supondremos que simboliza la posición del eje de rotación del electrón. De este modo, a cada qubit se le asigna un punto de la Esfera de Bloch, que representa al electrón, y un vector con origen en dicho punto de la esfera, que representará su eje de rotación.

En la *Esfera de Bloch* podemos visualizar también cómo cambia el estado de un qubit al atravesar una compuerta. Recurrimos al software Wolfram Mathematica *10.0* para llevar a cabo una simulación, a fin de mostrar estos conceptos.

Al ejecutar la simulación, aparece el siguiente cuadro de diálogo, donde se deberán ingresar las componentes del qubit q y los coeficientes de la matriz unitaria U:

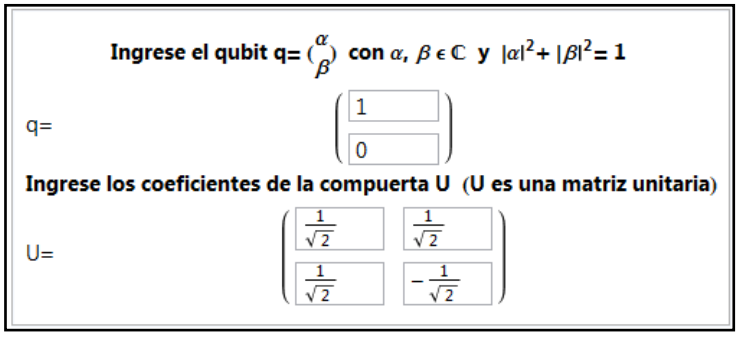


Figura 4.5: Datos a ingresar para ejecutar la simulación:
Las componentes del qubit q y los coeficientes de la matriz U.

Al ejecutar la simulación podemos visualizar cómo va cambiando la posición del eje de rotación del electrón, por la acción de una compuerta. En el siguiente gráfico mostramos la simulación obtenida, para el caso en que se ingresa el qubit $q = |0\rangle$ y la matriz de *Hadamard*

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

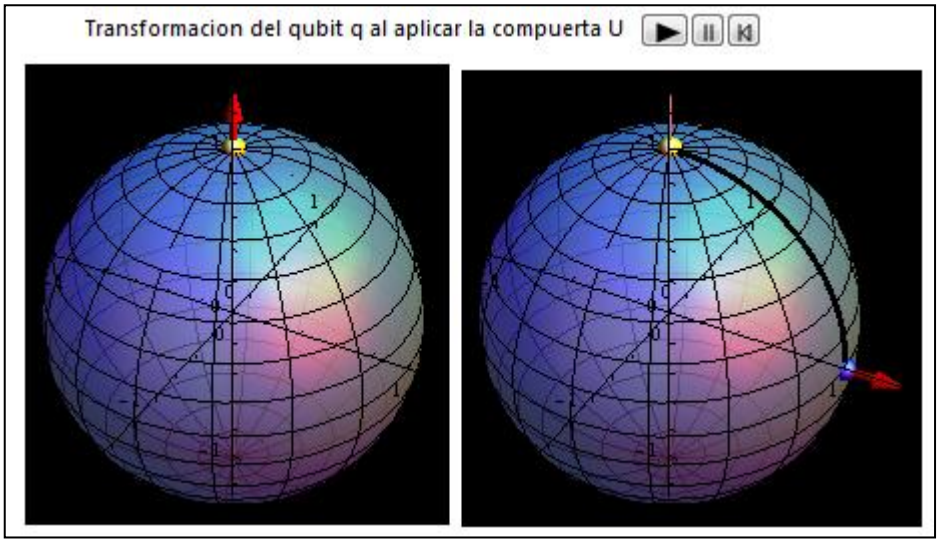


Figura 4.6: Simulación del efecto de una compuerta cuántica en la Esfera de Bloch.
Izquierda: Representación del qubit q= |0>. Derecha: Representación del qubit U.q, donde U es la compuerta de Hadamard.

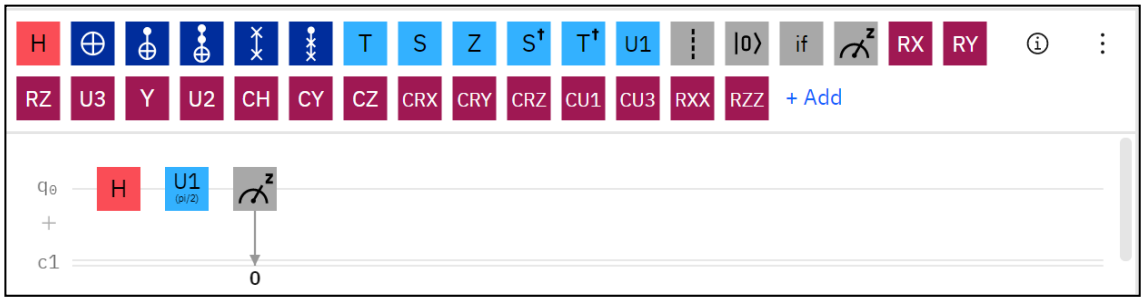
Código fuente del programa en Wolfram Mathematica 10.0

Mostramos a continuación el código fuente del programa que representa gráficamente un qubit en la Esfera de Bloch y cómo cambia su estado por la acción de una compuerta.

```
Interpretation[{α = 1, β = 0, a = 1/√2 , b = 1/√2 , c = 1/√2 , d = - 1/√2 },
 Panel[Grid[{{Style["Ingrese el qubit q= (α β) con α, β ∈ ℂ y |α|^2+ |β|^2= 1 ", Bold], SpanFromLeft},
    {"q=", MatrixForm[{InputField[Dynamic[α], FieldSize → 4], InputField[Dynamic[β], FieldSize → 4]}]},
    {Style["Ingrese los coeficientes de la compuerta U (U es una matriz unitaria)", Bold], SpanFromLeft},
    {"U=", MatrixForm[{{InputField[Dynamic[a], FieldSize → 4], InputField[Dynamic[b], FieldSize → 4]},
       {InputField[Dynamic[c], FieldSize → 4], InputField[Dynamic[d], FieldSize → 4] }}]}}]],
H = {{a, b}, {c, d}};
tita1 = Arg[α];
tita2 = Arg[β];
ro1 = Abs[α];
ro2 = Abs[β];
fi = If[ro1 ≠ 0, 2 ArcTan[ro2/ro1] , 2 Pi / 2];
tita = tita2 - tita1;
q = { Sin[fi] Cos[tita], Sin[ fi] Sin[tita], Cos[fi] };
Punto = Graphics3D[{Yellow, Specularity[White, 5], Sphere[q, 0.06] }];
αt = Extract[H.{α, β}, {1}];
βt = Extract[H.{α, β}, {2}];
tita11 = Arg[αt];
tita22 = Arg[βt];
ro11 = Abs[αt];
ro22 = Abs[βt];
fit = If[ro11 ≠ 0, 2 ArcTan[ro22/ro11] , 2 Pi / 2];
titat = tita22 - tita11;
Uqesfera = { Sin[fit] Cos[titat], Sin[ fit] Sin[titat], Cos[fit] };
Uq = {a * α + b * β, c * α + d * β};
Esfera = ParametricPlot3D[{ Sin[ϕ] Cos[θ], Sin[ ϕ] Sin[θ], Cos[ϕ] }, { ϕ, 0, Pi}, { θ, 0, 2 Pi} , Boxed → False, Axes → True, AxesOrigin → {0, 0, 0},
   PlotRange → {{-1.3, 1.3}, {-1.3, 1.3}, {-1.3, 1.3}}, ImageSize → {400, 400}, Background → Black,
   PlotStyle → Directive[RGBColor[0.482353, 0.705882, 0.74902], Opacity[0.8], Specularity[White, 20]]];
Ejez = Graphics3D[{White, Arrowheads[0.18], Arrow[Tube[{{0, 0, -2.5}, {0, 0, 2.5}}]]}];
Manipulate[
 Curva = ParametricPlot3D[If[ s <= 1 , { Sin[fi] Cos[tita + (titat - tita) s], Sin[ fi] Sin[tita + (titat - tita) s], Cos[fi] } ,
    { Sin[fi + (fit - fi) (s - 1)] Cos[titat], Sin[ fi + (fit - fi) (s - 1)] Sin[titat], Cos[fi + (fit - fi) (s - 1)] }], {s, 0, t}, PlotStyle → {Black, Thickness[0.008]}];
 Pt = If[ t <= 1 , { Sin[fi] Cos[tita + (titat - tita) t], Sin[ fi] Sin[tita + (titat - tita) t], Cos[fi] } ,
   { Sin[fi + (fit - fi) (t - 1)] Cos[titat], Sin[ fi + (fit - fi) (t - 1)] Sin[titat], Cos[fi + (fit - fi) (t - 1)] }];
Puntot = Graphics3D[{Blue, Specularity[White, 5], Sphere[Pt, 0.06] }];
  Ejev = Graphics3D[{Red, Arrowheads[0.04], Arrow[Tube[{Pt, Pt + 0.35 Pt/Norm[Pt]}, 0.02]] }];
  Show[Esfera, Curva, Puntot, Punto, Ejez, Ejev], Panel[" EFECTO DE UNA COMPUERTA CUÁNTICA SOBRE UN QUBIT EN LA ESFERA DE BLOCH "],
  {Uq},
  {{t, 0.00001, "Transformacion del qubit q al aplicar la compuerta U"}, 0.00001, 2, ControlType → Trigger }, SaveDefinitions -> True]
]
```

4.3.5 Codificación de un circuito cuántico en la plataforma IBM Quantum Experience

A partir del año *2017*, IBM puso a disposición del público en general una plataforma online que permite simular circuitos cuánticos y analizar sus resultados.
La plataforma lleva a cabo este tipo de simulaciones mediante bloques, tal como se observa en la siguiente figura



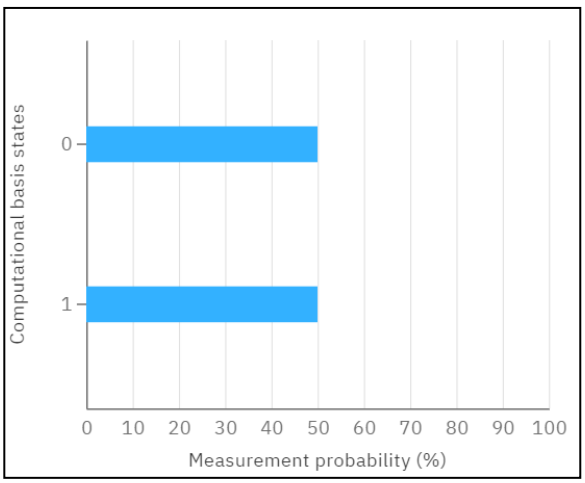
O mediante un código de programación utilizando el lenguaje QSAM o Qiskit. Así, la codificación del Ejemplo *4.4* es la siguiente:

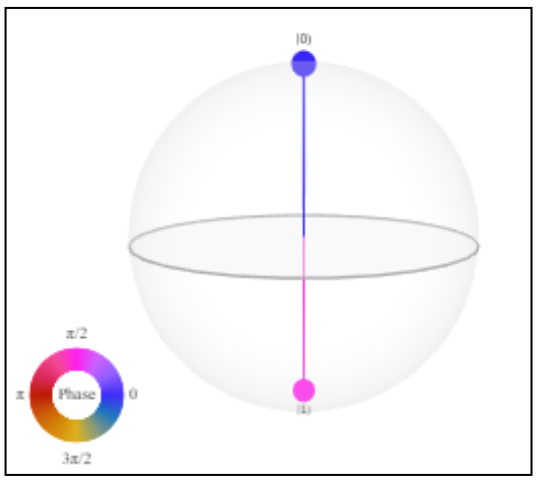
```
OPENQASM 2.0;
include "qelib1.inc";

qreg q[1];
creg c[1];

h q[0];
u1(pi/2) q[0];
measure q[0] -> c[0];
```

En el área de análisis de resultados, la plataforma muestra gráficos de barras que representan las probabilidades de encontrar un qubit en cierto estado. También nos da una visualización de la esfera de Bloch, donde se observan dichos estados. Es importante resaltar que, si se posiciona el mouse sobre el estado de un qubit, aparece una ventana con más datos sobre el mismo, como la probabilidad de que se encuentre en dicho estado.





4.4 Compuertas cuánticas de dos qubits

Según la Definición *4.1*, una compuerta cuántica que opera sobre un sistema formado por dos qubits es una matriz unitaria de orden 2^2. Como sabemos, una base ortonormal para el espacio de los *2*-qubits es

$$\{\ |00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle\ \}$$

Donde

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \approx \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \approx \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \approx \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \approx \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Luego, para definir la matriz unitaria *U* asociada a una compuerta cuántica, bastará con definir la transformación *U* sobre cada *2*-qubit de la base, expresándola como combinación lineal de los elementos de dicha base. Es decir, se especificará:

$$U|00\rangle = a_{11}\,|00\rangle + a_{12}\,|01\rangle + a_{13}\,|10\rangle + a_{14}\,|11\rangle$$

$$U|01\rangle = a_{21}\,|00\rangle + a_{22}\,|01\rangle + a_{23}\,|10\rangle + a_{24}\,|11\rangle$$

$$U|10\rangle = a_{31}\,|00\rangle + a_{32}\,|01\rangle + a_{33}\,|10\rangle + a_{34}\,|11\rangle$$

$$U|11\rangle = a_{41}\,|00\rangle + a_{42}\,|01\rangle + a_{43}\,|10\rangle + a_{44}\,|11\rangle$$

De este modo, la matriz unitaria *U* será

$$U = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

Describiremos a continuación dos de las compuertas de dos qubits que utilizaremos a lo largo de este trabajo: la compuerta *Swap* y la compuerta *Xor*.

4.4.1 La compuerta Swap

Esta compuerta intercambia dos qubits. Se la define por

$$\boldsymbol{Swap} \mid x\, y > = \mid y\, x > \text{ con } x, y \in \{0, 1\}.$$

La representación gráfica es la siguiente:



Figura 4.7: Representación gráfica de la compuerta Swap.

El efecto de esta compuerta sobre cada *2*-qubit de la base es:

$$Swap\ |00\rangle = |00\rangle = 1.\ |00\rangle + 0.\ |01\rangle + 0.\ |10\rangle + 0.\ |11\rangle$$

$$Swap|01\rangle = |10\rangle = 0.\ |00\rangle + 0.\ |01\rangle + 1.\ |10\rangle + 0.\ |11\rangle$$

$$Swap|10\rangle = |01\rangle = 0.\ |00\rangle + 1.\ |01\rangle + 0.\ |10\rangle + 0.\ |11\rangle$$

$$Swap|11\rangle = |11\rangle = 0.|00\rangle + 0.\ |01\rangle + 0.\ |10\rangle + 1.\ |11\rangle$$

Por lo tanto, la matriz asociada a esta compuerta es

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

En general, a la matriz asociada a una compuerta cuántica se la suele nombrar anteponiendo la letra "*U*".

4.4.2 La compuerta Xor

La compuerta cuántica *Xor* se la define por

$$\boldsymbol{Xor} \mid x\, y > = \mid x\, ,\, x \oplus y >$$

Donde $x, y \in \{0, 1\}$ y $\oplus$ representa la "*suma módulo 2*".

En este caso, el primer qubit recibe el nombre de "*qubit de control*", pues permanece inalterado. Mientras que el segundo qubit se lo llama "*qubit objetivo*". Observemos que si el qubit de control vale 0, el objetivo no cambia, mientras que si vale 1, se niega el objetivo.

La representación gráfica de esta compuerta es:

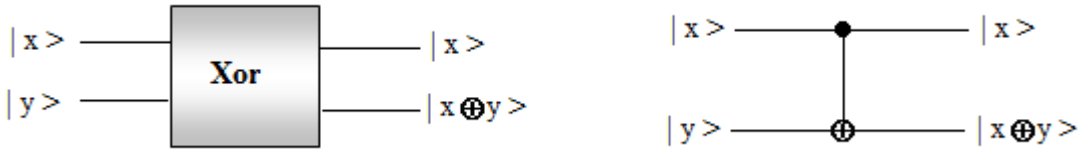


Figura 4.8: Dos representaciones gráficas de la compuerta Xor.

Por lo tanto

$Xor\ |00\rangle = |0,0 \oplus 0\rangle = |00\rangle$

$Xor\ |01\rangle = |0,0 \oplus 1\rangle = |01\rangle$

$Xor\ |10\rangle = |1,1 \oplus 0\rangle = |11\rangle$

$Xor\ |11\rangle = |1,1 \oplus 1\rangle = |10\rangle$

Su expresión matricial es entonces

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

Cómo definir compuertas de dos qubits a partir de compuertas de un qubit

Se pueden construir compuertas de dos qubits que sean producto tensorial de dos compuertas simples, que actúen separadamente en cada uno de los qubits. Su definición es la siguiente:

Definición 4.6: Producto tensorial de dos compuertas simples

Dadas dos compuertas de un qubit U y V, el producto tensorial $U \otimes V$ es una compuerta de dos qubits de la forma

$$U \otimes V\ |x\ y\rangle = U\,|x\rangle \otimes V\,|y\rangle$$

Con $x, y \in \{0,1\}$

Por lo tanto, este tipo de compuertas aplica *U* al primer qubit y *V* al segundo qubit. Se puede verificar que la matriz asociada es el producto tensorial de las matrices *U* y *V*. Su representación gráfica es la siguiente:

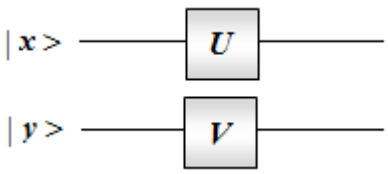


Figura 4.9: Representación gráfica del producto tensorial de dos compuertas simples.

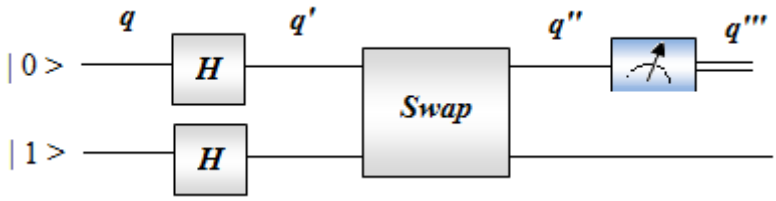
Si una de las compuertas *U* o *V* es la identidad, no aparece representada porque deja inalterado a uno de los qubits. Así, el producto tensorial de una compuerta simple por la identidad es una compuerta de dos qubits que consiste en modificar sólo uno de los qubits. Es decir,

$$U \otimes I \left| x\ y \right\rangle = U \left| x \right\rangle \otimes I \left| y \right\rangle = U \left| x \right\rangle \otimes \left| y \right\rangle$$

$$I \otimes V \left| x\ y \right\rangle = I \left| x \right\rangle \otimes V \left| y \right\rangle = \left| x \right\rangle \otimes V \left| y \right\rangle$$

Ejemplo 4.7

Dados los qubits de entrada $q_1 = |0\rangle$, $q_2 = |1\rangle$ y el siguiente circuito:



a) Indicar el estado del sistema al atravesar las compuertas *H* y *Swap*.
b) ¿Cuál es la probabilidad de que al medir el primer qubit del sistema, éste se encuentre en estado *1*?
c) ¿En qué estado queda el sistema luego de efectuar la medición del primer qubit, si éste quedó en estado *1*?
d) ¿Cuál es la probabilidad de que al observar el segundo qubit del sistema, éste se encuentre en estado 0?

Solución

a) Por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema se expresa mediante el producto tensorial de q_1 con q_2, es decir

$$q = q_1 \otimes q_2 = |0\rangle \otimes |1\rangle = |01\rangle$$

Al atravesar las compuertas de Hadamard *H*, el estado del sistema el sistema evoluciona al siguiente estado:

$$q' = H \otimes Hq = H \otimes H \left| 01 \right\rangle = H \left| 0 \right\rangle \otimes H \left| 1 \right\rangle = \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) =$$

$$= \frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle$$

Finalmente, al pasar por la compuerta *Swap*, el estado del sistema queda determinado por el siguiente *2*-qubit:

$$q'' = Swap.\ q' = Swap \left(\frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle \right) =$$

$$= \frac{1}{2} Swap\,|00\rangle - \frac{1}{2} Swap\,|01\rangle + \frac{1}{2} Swap\,|10\rangle - \frac{1}{2} Swap\,|11\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|11\rangle$$

Por lo tanto

$$q'' = \frac{1}{2}|00\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|11\rangle$$

b) Siguiendo el mismo procedimiento que en el Ejemplo 3.13, se tiene

$$P\left(q_1 = |1\rangle\right) = \left| -\frac{1}{2} \right|^2 + \left| -\frac{1}{2} \right|^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

c) Por la Proposición *3.23* se tiene que el sistema evoluciona al siguiente estado:

$$q''' = \frac{-\frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle}{\sqrt{\left|-\frac{1}{2}\right|^2 + \left|-\frac{1}{2}\right|^2}} = \frac{-\frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle}{\frac{1}{\sqrt{2}}} = -\frac{\sqrt{2}}{2}|10\rangle - \frac{\sqrt{2}}{2}|11\rangle$$

Luego

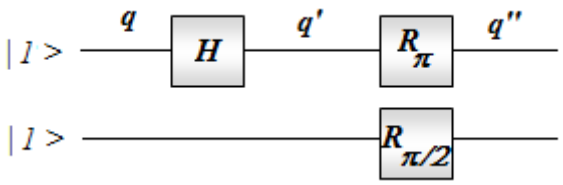
$$q''' = -\frac{\sqrt{2}}{2}|10\rangle - \frac{\sqrt{2}}{2}|11\rangle$$

d) $P\left(q_2 = |0\rangle\right) = \left| -\frac{\sqrt{2}}{2} \right|^2 = \frac{1}{2}$

Luego, la probabilidad de encontrar el segundo qubit en estado *0* es *0.5*.

Ejemplo 4.8

Dados los qubits de entrada $q_1 = |1\rangle$, $q_2 = |1\rangle$ y el siguiente circuito:



a) Hallar el estado final del sistema.

b) Se dice que dos qubits que componen un sistema cuántico están entrelazados si el *2*-qubit *q* que describe el estado de dicho sistema no puede expresarse como producto tensorial de dos qubits. Es decir, si

$$q \neq u \otimes v \quad \forall qubit\ u, v.$$

Por el contrario, si existen dos qubits *u*, *v* tales que

$$q = u \otimes v$$

Entonces se dice que los qubits que forman el sistema no están entrelazados. ¿Quedan entrelazados los qubits al atravesar todas las compuertas?

Solución

a) Nuevamente, por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema es

$$q = q_1 \otimes q_2 = |1\rangle \otimes |1\rangle = |11\rangle$$

Al atravesar la compuerta *H* el primer qubit, el sistema evoluciona al siguiente estado:

$$q' = H \otimes Iq = H \otimes I\,|11\rangle = H\,|1\rangle \otimes I\,|1\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |1\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

Finalmente, al atravesar las compuertas de desplazamiento de fase R_π **y** $R_{\pi/2}$, el estado final del sistema es

$$q'' = R_\pi \otimes R_{\pi/2}\, q' = R_\pi \otimes R_{\pi/2}\left(\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) =$$

$$= R_\pi \otimes R_{\pi/2}\left(\frac{1}{\sqrt{2}}|01\rangle\right) - R_\pi \otimes R_{\pi/2}\left(\frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{\sqrt{2}} R_\pi \otimes R_{\pi/2}\left(|01\rangle\right) - \frac{1}{\sqrt{2}} R_\pi \otimes R_{\pi/2}\left(|11\rangle\right) =$$

$$= \frac{1}{\sqrt{2}} R_\pi |0\rangle \otimes R_{\pi/2}\left(|1\rangle\right) - \frac{1}{\sqrt{2}} R_\pi |1\rangle \otimes R_{\pi/2}\left(|1\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle \otimes e^{i\frac{\pi}{2}}|1\rangle - \frac{1}{\sqrt{2}} e^{i\pi}|1\rangle \otimes e^{i\frac{\pi}{2}}|1\rangle =$$

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

Es decir

$$q'' = \frac{i}{\sqrt{2}}|01\rangle + \frac{i}{\sqrt{2}}|11\rangle$$

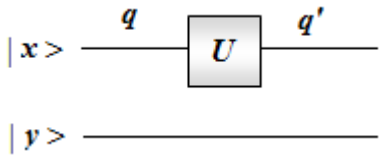
b) Como el estado final del sistema es

$$q'' = \frac{i}{\sqrt{2}}|01\rangle + \frac{i}{\sqrt{2}}|11\rangle = \underbrace{\left(\frac{i}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle\right)}_{\textit{Primer qubit}} \otimes \underbrace{|1\rangle}_{\textit{Segundo qubit}}$$

Entonces los qubits no quedan entrelazados porque q'' queda expresado como producto tensorial de dos qubits.

Notación 4.9

Si se tiene un circuito similar al de la figura:



Entonces sabemos que los estados del sistema son

$$q = |x\rangle \otimes |y\rangle = |x\ y\rangle$$

$$q' = U \otimes Iq = U \otimes I\,|x\ y\rangle = U\,|x\rangle \otimes I\,|y\rangle = U\,|x\rangle \otimes |y\rangle$$

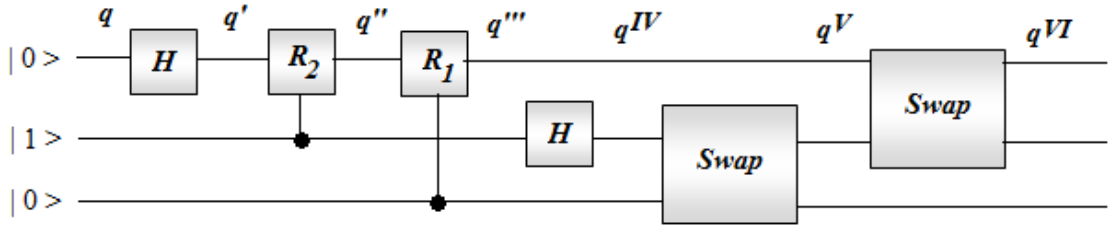
Para simplificar la notación, evitaremos expresar la compuerta Identidad y escribiremos simplemente

$$q' = U\,|x\rangle \otimes |y\rangle$$

Esta notación también la aplicaremos para sistemas de *3* o más qubits, en caso de que algunos de ellos permanezcan inalterados.

Ejemplo 4.10

Dados el sistema formado por los qubits de entrada $q_1 = |0\rangle$, $q_2 = |1\rangle$, $q_3 = |0\rangle$ y el siguiente circuito cuántico:



a) Hallar el estado final del sistema luego de atravesar todas las compuertas.
b) ¿Cuál es la probabilidad de que al medir los qubits, el segundo y tercero se encuentren en estado 1?

Solución

a) Por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema se expresa mediante el producto tensorial

$$q = q_1 \otimes q_2 \otimes q_3 = |0\rangle \otimes |1\rangle \otimes |0\rangle = |010\rangle$$

Los otros estados que resultan al atravesar cada compuerta son:

$$q' = H\,|0\rangle \otimes |1\rangle \otimes |0\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle \otimes |0\rangle$$

Como

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\,\pi\,i\,1}{2^2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi\,i}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \cos\left(\frac{\pi}{2}\right) + i\ sen\left(\frac{\pi}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Entonces

$$R_2\,|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$R_2\,|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i\begin{pmatrix} 0 \\ 1 \end{pmatrix} = i\,|1\rangle$$

Luego

$$q'' = \frac{1}{\sqrt{2}} R_2 |0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} R_2 |1\rangle \otimes |1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}} |0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} i\, |1\rangle \otimes |1\rangle \otimes |0\rangle$$

Por otro lado, como

$$R_1 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\,\pi\, i\, 0}{2^1}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Entonces

$$R_1 |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$R_1 |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

Por lo tanto

$$q''' = \frac{1}{\sqrt{2}} R_1 |0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} i\ R_1 |1\rangle \otimes |1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}} |0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} i\, |1\rangle \otimes |1\rangle \otimes |0\rangle$$

Al atravesar el segundo qubit la compuerta *H* resulta

$$q^{IV} = \frac{1}{\sqrt{2}} |0\rangle \otimes H\, |1\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} i\, |1\rangle \otimes H\, |1\rangle \otimes |0\rangle =$$

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

$$= \frac{1}{2} |0\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} |0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{2} i\, |1\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} i\, |1\rangle \otimes |1\rangle \otimes |0\rangle$$

Luego

$$q^{IV} = \frac{1}{2} |0\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} |0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{2} i\, |1\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} i\, |1\rangle \otimes |1\rangle \otimes |0\rangle$$

Al pasar el segundo y tercer qubit por la compuerta *Swap* tenemos

$$q^{V} = \frac{1}{2} |0\rangle \otimes Swap\, |0\rangle \otimes |0\rangle - \frac{1}{2} |0\rangle \otimes Swap\, |1\rangle \otimes |0\rangle + \frac{1}{2} i\, |1\rangle \otimes Swap\, |0\rangle \otimes |0\rangle - \frac{1}{2} i\, |1\rangle \otimes Swap\, |1\rangle \otimes |0\rangle =$$

$$= \frac{1}{2} |0\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} |0\rangle \otimes |0\rangle \otimes |1\rangle + \frac{1}{2} i\, |1\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} i\, |1\rangle \otimes |0\rangle \otimes |1\rangle$$

Entonces

$$q^{V} = \frac{1}{2} |0\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} |0\rangle \otimes |0\rangle \otimes |1\rangle + \frac{1}{2} i\, |1\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} i\, |1\rangle \otimes |0\rangle \otimes |1\rangle$$

Finalmente, al atravesar el primer y segundo qubit por la compuerta Swap resulta

$$q^{VI} = \frac{1}{2} Swap\,|0\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} Swap\,|0\rangle \otimes |0\rangle \otimes |1\rangle + \frac{1}{2} i\ \ Swap\,|1\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2} i\ \ Swap\,|1\rangle \otimes |0\rangle \otimes |1\rangle =$$

$$= \frac{1}{2}|0\rangle \otimes |0\rangle \otimes |0\rangle - \frac{1}{2}|0\rangle \otimes |0\rangle \otimes |1\rangle + \frac{1}{2} i\ \ |0\rangle \otimes |1\rangle \otimes |0\rangle - \frac{1}{2} i\ \ |0\rangle \otimes |1\rangle \otimes |1\rangle$$

En consecuencia

$$q^{VI} = \frac{1}{2}|000\rangle - \frac{1}{2}|001\rangle + \frac{1}{2} i\ \ |010\rangle - \frac{1}{2} i\ \ |011\rangle$$

b) Observando el estado final del sistema, teniendo en cuenta la Definición *3.10* y haciendo un razonamiento similar al del Ejercicio *3.13* b), resulta que

$$P\left(q_2 = |1\rangle \ \wedge\ q_3 = |1\rangle\right) = \left| -\ \frac{1}{2} i \right|^2 = \left(-\ \frac{1}{2} \right)^2 = \frac{1}{4}.$$

4.5 Algoritmos cuánticos

Un algoritmo cuántico es un conjunto de instrucciones que se utilizan para realizar una determinada tarea en una computadora cuántica.
Los algoritmos cuánticos se llevan a cabo mediante una o más compuertas cuánticas, y muchos de ellos funcionan considerablemente mejor que los diseñados para ser ejecutados en un ordenador clásico.
Ello se debe a que los sistemas cuánticos gozan de una importante cualidad: *el paralelismo cuántico.*
El *paralelismo cuántico* es la propiedad que tienen los algoritmos cuánticos de efectuar varias operaciones al mismo tiempo, en virtud del estado de superposición que pueden adquirir las partículas subatómicas.
Sin embargo, sabemos que, al medir un qubit, éste colapsa a uno de los dos estados posibles: estado *0* (spin arriba) o estado *1* (spin abajo).
¿Dónde está, pues, la ventaja de utilizar algoritmos cuánticos? La ventaja radica en que se pueden manipular los qubits a través de compuertas cuánticas sin que colapsen sus estados. De este modo, se pueden manejar qubits en estado de superposición y en el momento apropiado, observarlos. En ese instante sus estados colapsarán, pero antes de ello sus estados darán la información necesaria para los propósitos del algoritmo.
En esta sección, a modo de ejemplo, desarrollaremos un algoritmo cuántico que suma dos dígitos binarios. Previamente definiremos la siguiente compuerta que opera sobre un qubit:

La compuerta U_θ

La compuerta cuántica U_θ, con $0 \le \theta < 2\pi$, llamada "*compuerta de rotación* θ ", está dada por la siguiente matriz unitaria

$$U_\theta = \begin{pmatrix} cos\left(\frac{\theta}{2}\right) & sen\left(\frac{\theta}{2}\right) \\ -sen\left(\frac{\theta}{2}\right) & cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

En este caso,

$$U_\theta|0\rangle = \begin{pmatrix} cos\left(\frac{\theta}{2}\right) & sen\left(\frac{\theta}{2}\right) \\ -sen\left(\frac{\theta}{2}\right) & cos\left(\frac{\theta}{2}\right) \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} cos\left(\frac{\theta}{2}\right) \\ -sen\left(\frac{\theta}{2}\right) \end{pmatrix} = cos\left(\frac{\theta}{2}\right)\ |0\rangle - sen\left(\frac{\theta}{2}\right)\ |1\rangle$$

$$U_\theta|1\rangle = \begin{pmatrix} cos\left(\frac{\theta}{2}\right) & sen\left(\frac{\theta}{2}\right) \\ -sen\left(\frac{\theta}{2}\right) & cos\left(\frac{\theta}{2}\right) \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} sen\left(\frac{\theta}{2}\right) \\ cos\left(\frac{\theta}{2}\right) \end{pmatrix} = sen\left(\frac{\theta}{2}\right)\ |0\rangle + cos\left(\frac{\theta}{2}\right)\ |1\rangle$$

Por otro lado, su matriz traspuesta conjugada es

$$U_\theta^+ = \begin{pmatrix} cos\left(\frac{\theta}{2}\right) & -sen\left(\frac{\theta}{2}\right) \\ sen\left(\frac{\theta}{2}\right) & cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

Entonces

$$U_\theta^+|0\rangle = cos\left(\frac{\theta}{2}\right)\ |0\rangle + sen\left(\frac{\theta}{2}\right)\ |1\rangle \qquad U_\theta^+|1\rangle = -\ sen\left(\frac{\theta}{2}\right)\ |0\rangle + cos\left(\frac{\theta}{2}\right)\ |1\rangle$$

Algoritmo cuántico para la suma de dos dígitos binarios

Primeramente recordemos cómo se efectúan las sumas de dos dígitos en base *2*:

Bit de acarreo

			1
0	***1***	***0***	***01***
+ ***0***	+ ***0***	+ ***1***	+ ***01***
0	***1***	***1***	***10***

El circuito cuántico que implementa el algoritmo tiene tres entradas:

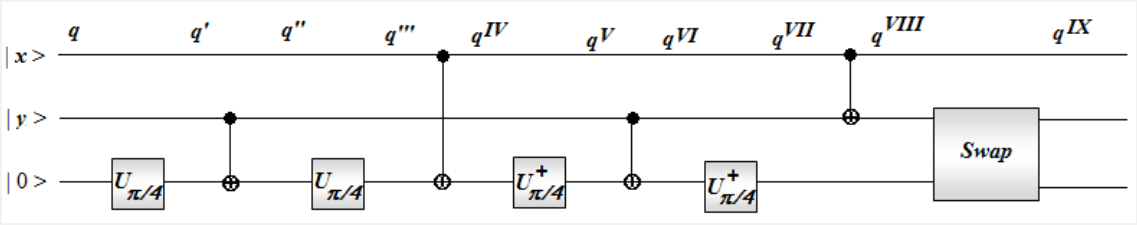
$$q_1 = |x\rangle,\ q_2 = |y\rangle,\ q_3 = |0\rangle$$

Con $x, y \in \{0,1\}$.

El circuito se diseña de modo tal que, al medir el estado final del sistema, el estado de q_2 indique el bit de acarreo, mientras que el estado de q_3 represente la suma (módulo *2*) de los bits *x* e *y*. La siguiente Proposición muestra dicho circuito y determina el estado final del sistema:

Proposición 4.11

Dado el siguiente circuito cuántico, con $x, y \in \{0,1\}$



Entonces

1) El estado final del sistema es

$$q^{IX} = \begin{cases} |x\,,\ x.y\,,\ x \oplus y\rangle & si\ (x = y = 0) \vee (x = y = 1) \\ -|x\,,\ x.y\,,\ x \oplus y\rangle & si\ (x = 1 \wedge y = 0) \vee (x = 0 \wedge y = 1) \end{cases}$$

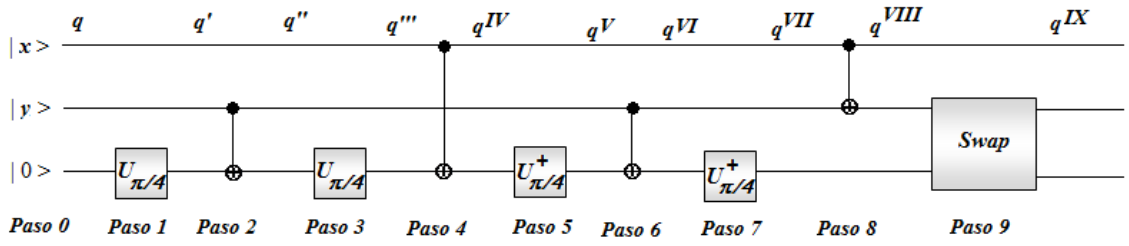
2) Al medir el estado final del sistema, los estados de los dos últimos qubits muestran, con probabilidad 1, el resultado de la suma binaria de ***x*** *e* ***y****.*

Demostración

1) Debemos hallar el estado final del sistema para los siguientes casos:

$$\begin{cases} x = 0\,,\ y = 0 \\ x = 0\,,\ y = 1 \\ x = 1\,,\ y = 0 \\ x = 1\,,\ y = 1 \end{cases}$$

Sólo analizaremos el caso en que *x= y=1*, ya que para los demás valores de *x* e *y* la demostración es similar. La evolución del sistema al atravesar cada compuerta la indicaremos paso a paso, según se muestra en la siguiente figura:



<u>Paso 0:</u>

Por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema es

$$q = q_1 \otimes q_2 \otimes q_3 = |1\rangle \otimes |1\rangle \otimes |0\rangle = |110\rangle$$

Paso 1:

Al aplicar la compuerta $U_{\pi/4}$ al tercer qubit, el sistema evoluciona al siguiente estado:

$$q' = |1\rangle \otimes |1\rangle \otimes U_{\pi/4} |0\rangle = |1\rangle \otimes |1\rangle \otimes \left(cos\left(\frac{\pi}{8}\right) |0\rangle - sen\left(\frac{\pi}{8}\right) |1\rangle \right)$$

Utilizando la Propiedad Distributiva del producto tensorial, resulta

$$q' = cos\left(\frac{\pi}{8}\right) |110\rangle - sen\left(\frac{\pi}{8}\right) |111\rangle$$

Paso 2:

Se aplica la compuerta *Xor* al segundo y tercer qubit del sistema. De este modo, el estado del sistema se transforma del siguiente modo:

$$q'' = cos\left(\frac{\pi}{8}\right) |1,1,1 \oplus 0\rangle - sen\left(\frac{\pi}{8}\right) |1,1,1 \oplus 1\rangle = cos\left(\frac{\pi}{8}\right) |1,1,1\rangle - sen\left(\frac{\pi}{8}\right) |1,1,0\rangle$$

Es decir

$$q'' = cos\left(\frac{\pi}{8}\right) |111\rangle - sen\left(\frac{\pi}{8}\right) |110\rangle$$

Paso 3:

Al atravesar la compuerta $U_{\pi/4}$ el tercer qubit, obtenemos

$$q''' = cos\left(\frac{\pi}{8}\right) |11\rangle \otimes U_{\pi/4} |1\rangle - sen\left(\frac{\pi}{8}\right) |11\rangle \otimes U_{\pi/4} |0\rangle =$$

$$= cos\left(\frac{\pi}{8}\right) |11\rangle \otimes \left(sen\left(\frac{\pi}{8}\right) |0\rangle + cos\left(\frac{\pi}{8}\right) |1\rangle \right) - sen\left(\frac{\pi}{8}\right) |11\rangle \otimes \left(cos\left(\frac{\pi}{8}\right) |0\rangle - sen\left(\frac{\pi}{8}\right) |1\rangle \right) =$$

$$= \left(cos\left(\frac{\pi}{8}\right) sen\left(\frac{\pi}{8}\right) - sen\left(\frac{\pi}{8}\right) cos\left(\frac{\pi}{8}\right) \right) |110\rangle + \left(cos^2\left(\frac{\pi}{8}\right) + sen^2\left(\frac{\pi}{8}\right) \right) |111\rangle = |111\rangle$$

Por lo tanto

$$q''' = |111\rangle$$

Paso 4:

Se aplica la compuerta *Xor* al primer y tercer qubit del sistema. Entonces, el sistema evoluciona al siguiente estado:

$$q^{IV} = |1,1,1 \oplus 1\rangle = |1,1,0\rangle$$

Luego

$$q^{IV} = |110\rangle$$

Paso 5:

Se aplica la compuerta $U^{+}_{\pi/4}$ al tercer qubit, con lo cual el sistema evoluciona al siguiente estado:

$$q^V = |11\rangle \otimes U^+_{\pi/4} |0\rangle = |11\rangle \otimes \left(cos\left(\frac{\pi}{8}\right) |0\rangle + sen\left(\frac{\pi}{8}\right) |1\rangle \right)$$

Nuevamente, haciendo uso de la propiedad distributiva, resulta

$$q^V = cos\left(\frac{\pi}{8}\right) |110\rangle + sen\left(\frac{\pi}{8}\right) |111\rangle$$

Paso 6:

Se aplica la compuerta *Xor* al segundo y tercer qubit del sistema. Entonces, el sistema evoluciona del siguiente modo:

$$q^{VI} = cos\left(\frac{\pi}{8}\right) |1,1,0 \oplus 1\rangle + sen\left(\frac{\pi}{8}\right) |1,1,1 \oplus 1\rangle = cos\left(\frac{\pi}{8}\right) |1,1,1\rangle + sen\left(\frac{\pi}{8}\right) |1,1,0\rangle$$

Es decir

$$q^{VI} = cos\left(\frac{\pi}{8}\right) |111\rangle + sen\left(\frac{\pi}{8}\right) |110\rangle$$

Paso 7:

Se aplica la compuerta $U^+_{\pi/4}$ al tercer qubit, con lo cual el sistema evoluciona al siguiente estado:

$$q^{VII} = cos\left(\frac{\pi}{8}\right) |11\rangle \otimes U^+_{\pi/4} |1\rangle + sen\left(\frac{\pi}{8}\right) |11\rangle \otimes U^+_{\pi/4} |0\rangle =$$

$$= cos\left(\frac{\pi}{8}\right) |11\rangle \otimes \left(-sen\left(\frac{\pi}{8}\right) |0\rangle + cos\left(\frac{\pi}{8}\right) |1\rangle \right) + sen\left(\frac{\pi}{8}\right) |11\rangle \otimes \left(cos\left(\frac{\pi}{8}\right) |0\rangle + sen\left(\frac{\pi}{8}\right) |1\rangle \right) =$$

$$= \left(-sen\left(\frac{\pi}{8}\right) cos\left(\frac{\pi}{8}\right) + sen\left(\frac{\pi}{8}\right) cos\left(\frac{\pi}{8}\right) \right) |110\rangle + \left(sen^2\left(\frac{\pi}{8}\right) + cos^2\left(\frac{\pi}{8}\right) \right) |111\rangle = |111\rangle$$

Por lo tanto

$$q^{VII} = |111\rangle$$

Paso 8:

Se aplica la compuerta *Xor* al primer y segundo qubit del sistema. Entonces, el sistema evoluciona al siguiente estado:

$$q^{VIII} = |1,1 \oplus 1,1\rangle = |1,0,1\rangle$$

Entonces

$$q^{VIII} = |101\rangle$$

Paso 9:

Se aplica la compuerta *Swap* al segundo y tercer qubit del sistema, obteniendo finalmente el estado:

$$q^{IX} = |1\rangle \otimes Swap\,|01\rangle = |1\rangle \otimes |10\rangle = |110\rangle$$

Es decir

$$q^{IX} = |110\rangle$$

En consecuencia, se verifica que $q^{IX} = |x\ ,\ x.y\ ,\ x \oplus y\rangle$ ya que si $x = y = 1$, que es el caso que estamos analizando, resulta

$$q^{IX} = |1\ ,\ 1\ ,\ 0\rangle = |1\ ,\ (1).(1)\ ,\ 1 \oplus 1\rangle = |x\ ,\ x.y\ ,\ x \oplus y\rangle$$

2) Si $x = y = 1$ entonces

$$x + y = 1 + 1 = 10 \text{ (en base 2)}$$

Por otro lado, del inciso *1)* se tiene que el estado final del sistema es

$$q^{IX} = |x\ ,\ x.y\ ,\ x \oplus y\rangle = |110\rangle$$

Por lo tanto, si se miden los dos últimos qubits del sistema, sus estados mostrarán, con probabilidad *1*, el resultado de la suma binaria $x + y$ pues, por la Definición *3.10* generalizada a tres qubits obtenemos

$$P\left(q_2 = |1\rangle \wedge\ q_3 = |0\rangle\right) = |\ 1\ |^2 = 1$$

De manera similar se demuestra para los demás valores de x e y. ■

Observación 4.12

El algoritmo anterior muestra que no se puede prescindir de las computadoras clásicas, ya que la suma binaria en este tipo de computadoras se realiza de una manera más sencilla y menos costosa que en un ordenador cuántico.
En general, las computadoras cuánticas llevan la ventaja cuando sus algoritmos hacen uso del *paralelismo cuántico*, pues los tiempos de ejecución de dichos algoritmos se reducen drásticamente en relación a los algoritmos clásicos. El efecto del *paralelismo cuántico* se pondrá en evidencia en el Ejemplo 6.7 del Capítulo *6* y en el Capítulo *7*, cuando desarrollemos el algoritmo para el cálculo de logaritmos discretos.

CAPÍTULO 5

La Transformada Cuántica de Fourier

En este capítulo presentaremos una transformación unitaria muy importante, que será utilizada en el Algoritmo de Shor para el cálculo de logaritmos discretos: *La Transformada Cuántica de Fourier* (En inglés ***Q**uantum **F**ourier **T**ransform*). Podríamos decir que es la analogía cuántica de la Transformada Discreta de Fourier. Veremos también que puede diseñarse eficientemente en un ordenador cuántico. Su definición es la siguiente:

Definición 5.1: La Transformada Cuántica de Fourier de n-qubits

Sea $|x\rangle \in \{ |0\rangle, |1\rangle, |2\rangle, ..., |2^n - 1\rangle \}$ *un elemento de la base del espacio de los n-qubits. La Transformada Cuántica de Fourier, simbolizada mediante la sigla QFT, es la transformación lineal definida por*

$$QFT\ |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n - 1} |y\rangle\ e^{\frac{2\ \pi\ i\ x.y}{2^n}}$$

Donde

$|x\rangle$ *es la representación en base 10 del n-qubit* $|x_{n-1}\ \ x_{n-2} \ldots x_1\ \ x_0\rangle$

$|y\rangle$ *es la representación en base 10 del n-qubit* $|y_{n-1}\ \ y_{n-2} \ldots y_1\ \ y_0\rangle$

Ejemplo 5.2

Probar que si *n = 1*, la Transformada Cuántica de Fourier es la compuerta de Hadamard.

Solución

Si *n=1* entonces $|x\rangle \in \{ |0\rangle, |1\rangle \}$. Es decir, $|x\rangle = |0\rangle$ o $|x\rangle = |1\rangle$. Luego

$$QFT\ |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n - 1} |y\rangle\ e^{\frac{2\ \pi\ i\ 0.y}{2^n}} = \frac{1}{\sqrt{2^1}} \sum_{y=0}^{2^1 - 1} |y\rangle\ e^{\frac{2\ \pi\ i\ 0.y}{2^1}} = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} |y\rangle\ e^0 =$$

$$\frac{1}{\sqrt{2}} \sum_{y=0}^{1} |y\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right)$$

Por lo tanto

$$QFT\ |0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right) \qquad [1]$$

Por otro lado

$$QFT\ |1\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} |y\rangle\ e^{\frac{2\ \pi\ i\ 1.y}{2^n}} = \frac{1}{\sqrt{2^1}} \sum_{y=0}^{2^1-1} |y\rangle\ e^{\frac{2\ \pi\ i\ 1.y}{2^1}} = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} |y\rangle\ e^{\pi\ i\ y} =$$

$$= \frac{1}{\sqrt{2}} \left(|0\rangle\ e^{\pi\ i\ 0} + |1\rangle\ e^{\pi\ i\ 1} \right) = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\ \left(cos\left(\pi\right) + i\ sen\left(\pi\right) \right) \right) = \frac{1}{\sqrt{2}}\ \left(|0\rangle - |1\rangle \right)$$

Luego

$$QFT\ |1\rangle = \frac{1}{\sqrt{2}}\ \left(|0\rangle - |1\rangle \right) \qquad [2]$$

De [1] y [2] resulta que efectivamente la Transformada Cuántica de Fourier, para el caso *n = 1*, coincide con la compuerta de *Hadamard*, según la definición dada en la sección *4.3* del Capítulo *4*.

Ejemplo 5.3

Sea *n =4*. Calcular $QFT\ |8\rangle$.

Solución

En este caso, la Transformada Cuántica de Fourier está definida para un sistema formado por *4* qubits. Luego

$$QFT\ |8\rangle = \frac{1}{\sqrt{2^4}} \sum_{y=0}^{2^4-1} |y\rangle\ e^{\frac{2\ \pi\ i\ 8.y}{2^4}} = \frac{1}{\sqrt{16}} \sum_{y=0}^{15} |y\rangle\ e^{\pi.y\ i} = \frac{1}{4} \sum_{y=0}^{15} |y\rangle\ \left(cos\left(\pi y\right) + i\ sen\left(\pi y\right) \right)$$

Teniendo en cuenta que $\forall y \in \mathbb{Z}$ se verifica que

$$\begin{cases} cos\left(\pi\ y\right) = \left(-1\right)^y \\ sen\left(\pi\ y\right) = 0 \end{cases}$$

Entonces

$$QFT\ |8\rangle = \frac{1}{4} \sum_{y=0}^{15} |y\rangle\ \left(-1\right)^y = \frac{1}{4} \left(|0\rangle - |1\rangle + |2\rangle - |3\rangle + |4\rangle - |5\rangle + |6\rangle - |7\rangle + |8\rangle - |9\rangle . + ... - |15\rangle \right)$$

O equivalentemente

$$QFT\ |1000\rangle = \frac{1}{4} \left(|0000\rangle - |0001\rangle + |0010\rangle - |0011\rangle + |0100\rangle - |0101\rangle + |0110\rangle - |0111\rangle + ... - |1111\rangle \right)$$

5.1 Representación matricial de la Transformada Cuántica de Fourier

La Transformada Cuántica de Fourier, por ser una transformación lineal, tiene una representación matricial. Para hallarla, valuaremos la Transformada en cada uno de los elementos de la siguiente base del espacio de los *n*-qubits expresados, para simplificar la escritura, en representación decimal: $\left\{ |0\rangle,\ |1\rangle\ ,\ |2\rangle,...,\ \left|2^n-1\right\rangle \right\}$.

Entonces, si definimos $w = e^{\frac{2\ \pi\ i}{2^n}}$, obtenemos

$$QFT\ |0\rangle = \frac{1}{\sqrt{2^n}}\left(\ 1.\ |0\rangle + 1.\ |1\rangle + 1.\ |2\rangle + ... + 1.\ \left|2^n-1\right\rangle\ \right)$$

$$QFT\ |1\rangle = \frac{1}{\sqrt{2^n}}\left(1\ |0\rangle\ +\ w\ |1\rangle\ +\ w^{\,2}\,|2\rangle\ +...+\ w^{\,2^n-1}\ \left|2^n-1\right\rangle\ \right)$$

$$QFT\ |2\rangle = \frac{1}{\sqrt{2^n}}\left(\ 1.\ |0\rangle + w^{\,2}\,|1\rangle + w^{\,4}\,|2\rangle + ... + w^{\,2\left(2^n-1\right)}\ \left|2^n-1\right\rangle\ \right)$$

…….

$$QFT\ \left|2^n-1\right\rangle = \frac{1}{\sqrt{2^n}}\left(1.|0\rangle\ +\ w^{\,2^n-1}\,|1\rangle + w^{\left(2^n-1\right).2}\ |2\rangle + ... + w^{\left(2^n-1\right).\left(2^n-1\right)}\left|2^n-1\right\rangle\ \right)$$

Por lo tanto, la matriz asociada a la Transformada Cuántica de Fourier sobre el espacio de los *n*-qubits es:

$$F_n = \frac{1}{\sqrt{2^n}}\begin{pmatrix} 1 & 1 & 1 & 1 & . \ . \ . & 1 \\ 1 & w & w^{\,2} & w^{\,3} & . \ . \ . & w^{\,2^n-1} \\ 1 & w^{\,2} & w^{\,4} & w^{\,6} & . \ . \ . & w^{\,2\left(2^n-1\right)} \\ 1 & w^{\,3} & w^{\,6} & w^{\,9} & . \ . \ . & w^{\,3\left(2^n-1\right)} \\ . & . & . & . & . \ . \ . & . \\ . & . & . & . & . \ . \ . & . \\ . & . & . & . & . \ . \ . & . \\ 1 & w^{\,2^n-1} & w^{\,2\left(2^n-1\right)} & w^{\,3\left(2^n-1\right)} & . \ . \ . & w^{\left(2^n-1\right)\left(2^n-1\right)} \end{pmatrix}$$

En la siguiente Proposición probaremos que F_n es efectivamente una matriz unitaria.

Proposición 5.4

Si F_n es la matriz asociada a la Transformada Cuántica de Fourier sobre el espacio de los n-qubits, entonces F_n es unitaria. Es decir, $F_n\ .\ F_n^{+} = I$

Demostración

Primeramente, observemos que los coeficientes de la matriz F_n pueden expresarse del siguiente modo:

$$\left(F_n\right)_{j\ k} = \frac{1}{\sqrt{2^n}}\ w^{(j-1)(k-1)}$$

Donde

$j,k = 1,2,...,2^n$, $w = e^{\frac{2\pi i}{2^n}}$

Además, $F_n\ .\ F_n^+ = I \Leftrightarrow \left(F_n\ .\ F_n^+\right)_{j\ k} = \begin{cases} 1 & si\ j = k \\ 0 & si\ j \neq k \end{cases} \quad \forall j, k = 1,...,2^n$

Entonces

$$\left(F_n\ .\ F_n^+\right)_{j\ k} = \sum_{m=1}^{2^n} \left(F_n\right)_{j\ m}\ \left(F_n^+\right)_{m\ k} = \sum_{m=1}^{2^n} \left(F_n\right)_{j\ m}\ \overline{\left(F_n\right)}_{k\ m} =$$

$$= \sum_{m=1}^{2^n} \frac{1}{\sqrt{2^n}}\ w^{(j-1)(m-1)}\ \overline{\frac{1}{\sqrt{2^n}} w^{(k-1)(m-1)}} = \frac{1}{2^n}\ \sum_{m=1}^{2^n} e^{\frac{2\pi i (j-1)(m-1)}{2^n}}\ e^{\overline{\frac{2\pi i (k-1)(m-1)}{2^n}}} =$$

$$= \frac{1}{2^n}\ \sum_{m=1}^{2^n} e^{\frac{2\pi i (j-1)(m-1)}{2^n}}\ e^{-\frac{2\pi i (k-1)(m-1)}{2^n}} = \frac{1}{2^n}\ \sum_{m=1}^{2^n} e^{\frac{2\pi i (j-k)(m-1)}{2^n}}$$

Por lo tanto

$$\left(F_n\ .\ F_n^+\right)_{j\ k} = \frac{1}{2^n}\ \sum_{m=1}^{2^n} e^{\frac{2\pi i (j-k)(m-1)}{2^n}}$$

Luego

<u>Si $j = k$</u>

Entonces

$$\left(F_n\ .\ F_n^+\right)_{j\ k} = \frac{1}{2^n}\ \sum_{m=1}^{2^n} e^{\frac{2\pi i (0)(m-1)}{2^n}} = \frac{1}{2^n}\ \sum_{m=1}^{2^n} e^0 = \frac{1}{2^n}\ \sum_{m=1}^{2^n} 1 = \frac{1}{2^n} 2^n = 1$$

<u>Si $j \neq k$</u>

En este caso, teniendo en cuenta que si $u \in \mathbb{C}$ con $u \neq 1 \Rightarrow \sum_{m=0}^{2^n-1} u^m = \frac{1-u^{2^n}}{1-u}$ entonces considerando $u = e^{\frac{2\pi i (j-k)}{2^n}}$ resulta

$$\left(F_n \,.\, F_n^{+}\right)_{j\ k} = \frac{1}{2^n} \sum_{m=1}^{2^n} e^{\frac{2\pi i\,(j-k)(m-1)}{2^n}} = \frac{1}{2^n} \sum_{m=1}^{2^n} \left(e^{\frac{2\pi i\,(j-k)}{2^n}} \right)^{(m-1)} =$$

$$= \frac{1}{2^n} \sum_{m=0}^{2^n-1} \left(e^{\frac{2\pi i\,(j-k)}{2^n}} \right)^{m} = \frac{1}{2^n} \frac{1-e^{\frac{2\pi i\,(j-k)}{2^n} 2^n}}{1-e^{\frac{2\pi i\,(j-k)}{2^n}}} = \frac{1}{2^n} \frac{1-e^{2\pi i\,(j-k)}}{1-e^{\frac{2\pi i\,(j-k)}{2^n}}} =$$

$$= \frac{1}{2^n} \frac{1-\left(\cos\left(2\pi(j-k)\right)+i\ sen\left(2\pi(j-k)\right)\right)}{1-e^{\frac{2\pi i\,(j-k)}{2^n}}} = \frac{1}{2^n} \frac{1-(1+i.0)}{1-e^{\frac{2\pi i\,(j-k)}{2^n}}} = 0$$

En consecuencia

$$\left(F_n \,.\, F_n^{+}\right)_{j\ k} = \begin{cases} 1 & si\ j = k \\ 0 & si\ j \neq k \end{cases} \quad \forall j, k = 1,\ldots,2^n$$

Por lo tanto, F_n es unitaria. ■

5.2 Diseño del circuito cuántico para la Transformada Cuántica de Fourier

Como mencionamos en el Capítulo anterior, no siempre es posible implementar en un ordenador cuántico cualquier transformación unitaria. Sin embargo, la Transformada Cuántica de Fourier puede ser diseñada eficientemente en un ordenador cuántico, utilizando tres tipos de compuertas: la compuerta de *Hadamard*, la compuerta de *Desplazamiento de Fase* y la compuerta *Swap*. En esta sección veremos cómo crear un circuito cuántico asociado a esta Transformada. Previamente recordaremos algunas definiciones y enunciaremos una Proposición que utilizaremos en el armado de dicho circuito.

Compuertas que intervienen en el circuito de la transformada cuántica de Fourier

Como se mencionó anteriormente, las compuertas que se emplearán para el diseño del circuito son tres:

1- La compuerta de Hadamard

Como se vio en el Capítulo 3, la matriz asociada a esta compuerta es:

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

Como

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

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

Entonces la compuerta de Hadamard puede expresarse del siguiente modo:

$$H\,|x\rangle = \frac{1}{\sqrt{2}}\ \left(\ |0\rangle\ + e^{2\ \pi\ i\ \ (0.x\ )}\ |1\rangle\ \right)$$

Donde

$x \in \{0,1\}$

$0.x$ es un número binario, cuya representación en base *10* es : $0.x = x\ .\ 2^{-1}$.

De este modo,

$$e^{2\ \pi\ i\ \ (0.x\ )} = e^{2\ \pi\ i\ x\ 2^{-1}} = e^{\pi\ i\ x} = cos\left(\pi\ x\ \right) + i\ \ sen\left(\pi\ x\ \right) = \begin{cases} 1 & si\ x = 0 \\ -1 & si\ x = 1 \end{cases}$$

Esta nueva manera de expresar la compuerta de Hadamard será utilizada en el diseño del circuito de la Transformada Cuántica de Fourier.

2- La compuerta R o de Desplazamiento de Fase

Dado un ángulo θ expresado en radianes, la representación matricial de esta compuerta es:

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

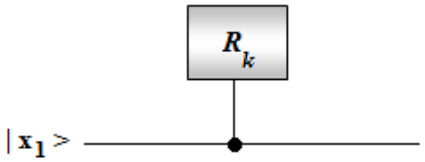
En particular, se define la siguiente compuerta, considerando $\theta = \frac{2\ \pi}{2^k}$:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\ \pi\ i}{2^k}} \end{pmatrix}$$

Dicha compuerta opera sobre un determinado bit. Por ejemplo, si R_k opera sobre el bit x_1, entonces su expresión queda:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\ \pi\ i\ x_1}{2^k}} \end{pmatrix}$$

Y su representación gráfica es:



3- La compuerta Swap

Esta compuerta intercambia dos qubits y se la define por

$$Swap\ |\ x\ y\ > = |\ y\ x\ >\ \ \text{con}\ x, y \in \{0,1\}\ .$$

La representación gráfica es:



A continuación probaremos otra forma de expresar la Transformada Cuántica de Fourier, que se utilizará para el diseño de su circuito cuántico.

Proposición 5.5

Si $x_i \in \{0,1\}\ \forall i = 0, 1,...,n-1$ *entonces*

$$QFT\,|x_{n-1}...x_0\rangle = \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{2\pi i 0.x_0}\,|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i 0.x_1x_0}\,|1\rangle\right)\otimes...\otimes\left(|0\rangle + e^{2\pi i 0.x_{n-1}...x_0}\,|1\rangle\right)$$

Es decir

$$QFT\,|x_{n-1}x_{n-2}...x_1x_0\rangle = \frac{1}{\sqrt{2^n}}\bigotimes_{l=1}^{n}\left(\,|0\rangle + e^{2\,\pi\, i\ 0.x_{l-1}x_{l-2}....x_0}\,|1\rangle\,\right)$$

Donde

$$0.x_{l-1}x_{l-2}...x_1x_0 = x_{l-1}.2^{-1} + x_{l-2}.2^{-2} + ... + x_l.2^{-(l-1)} + x_0.2^{-(l-0)}$$

O equivalentemente

$$0.x_{l-1}x_{l-2}...x_1x_0 = \sum_{k=1}^{l} x_{l-k}.2^{-k}$$

Demostración

Véase Referencia [12], pág.110. ■

5.3 Circuito cuántico para la Transformada Cuántica de Fourier

La Proposición *5.5* afirma que la Transformada Cuántica de Fourier puede ser "factorizada" como producto tensorial de *n* qubits. Este resultado permitirá diseñar el circuito cuántico asociado a dicha Transformada de una manera sencilla, empleando solamente compuertas de *Hadamard*, de *Desplazamiento de Fase* y compuertas *Swaps*. Por cuestiones didácticas mostraremos cómo crear dicho circuito para un qubit, luego para dos y tres qubits, para proceder finalmente a la generalización a *n*- qubits.

5.3.1 Circuito Cuántico de la QFT de 1-qubit

En este caso, *n =1*. Según la Proposición *5.4*, resulta que si $x_0 \in \{0,1\}$ entonces

$$QFT\,|x_0\rangle = \frac{1}{\sqrt{2^1}}\bigotimes_{l=1}^{1}\left(\,|0\rangle + e^{2\,\pi\, i\ 0.x_{l-1}x_{l-2}....x_0}\,|1\rangle\,\right) = \frac{1}{\sqrt{2}}\left(\,|0\rangle + e^{2\,\pi\, i\ 0.x_0}\,|1\rangle\,\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\ \pi i . x_0 . 2^{-1}} |1\rangle \right) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\ \pi i . x_0} |1\rangle \right) = \begin{cases} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle \right) & si\ x_0 = 0 \\ \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle \right) & si\ x_0 = 1 \end{cases} =$$

$$= H |x_0\rangle$$

En consecuencia, la *QFT* para *n = 1* es precisamente la compuerta de *Hadamard*.

5.3.2 Circuito Cuántico de la QFT de 2-qubits

En este caso, *n=2*. Aplicando la Proposición *5.5*, tenemos que si $x_0, x_1 \in \{ 0, 1 \}$ entonces

$$QFT\ |x_1 x_0\rangle = \frac{1}{\sqrt{2^2}} \bigotimes_{l=1}^{2} \left(|0\rangle + e^{2\ \pi i\ 0.x_{l-1} x_{l-2} .... x_0} |1\rangle \right) =$$

$$\frac{1}{\sqrt{2^2}} \left(|0\rangle + e^{2\ \pi i\ 0.x_0} |1\rangle \right) \otimes \left(|0\rangle + e^{2\ \pi i\ 0.x_1 x_0} |1\rangle \right)$$

Su circuito es el siguiente:

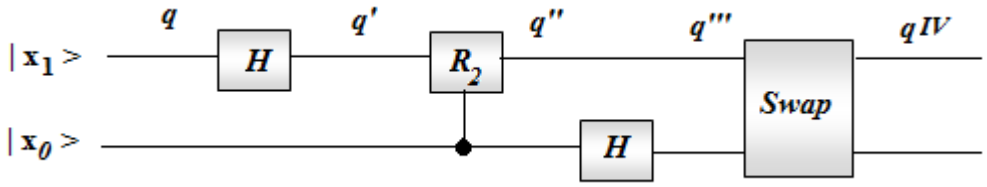


Figura 5.1: Circuito cuántico de la QFT para n = 2.

Probaremos que efectivamente este circuito genera la Transformada Cuántica de Fourier sobre el espacio de *2*-qubits.

Primeramente, el estado inicial del sistema es

$$q = |x_1\rangle \otimes |x_0\rangle$$

Los siguientes estados del sistema son:

$$q' = H |x_1\rangle \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\ \pi i\ 0.x_1} |1\rangle \right) \right) \otimes |x_0\rangle$$

Teniendo en cuenta que

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\ \pi i\ x_0}{2^2}} \end{pmatrix}$$

Entonces

$$q'' = R_2 \left(\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\ \pi i\ 0.x_1} |1\rangle \right) \right) \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}} \left(R_2 |0\rangle + e^{2\ \pi i\ 0.x_1} R_2 |1\rangle \right) \right) \otimes |x_0\rangle =$$

$$=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1}\;e^{\frac{2\,\pi\,i\;x_0}{2^2}}|1\rangle\right)\right)\otimes\;|x_0\rangle=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1}\;e^{2\,\pi\,i\;0.0x_0}\;|1\rangle\right)\right)\otimes\;|x_0\rangle=$$

$$=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;(0.x_1+0.0x_0)}\;|1\rangle\right)\right)\otimes\;|x_0\rangle=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)\otimes\;|x_0\rangle$$

El próximo paso consiste en aplicar la compuerta *H* al segundo qubit $|x_0\rangle$**:**

$$q'''=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)\otimes H\;|x_0\rangle=$$

$$=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)\otimes\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right)$$

Finalmente, al aplicar la compuerta *Swap* obtenemos

$$q^{IV}=Swap\left(\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)\otimes\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right)\right)=$$

$$=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right)\otimes\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)=$$

$$=\frac{1}{\sqrt{2^2}}\left(\;|0\rangle+e^{2\,\pi\,i\;0.x_0}\;|1\rangle\;\right)\otimes\left(\;|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\;\right)=$$

$$=\frac{1}{\sqrt{2^2}}\bigotimes_{l=1}^{2}\left(\;|0\rangle+e^{2\,\pi\,i\;0.x_{l-1}x_{l-2}....x_0}\;|1\rangle\;\right)=QFT\;|x_1x_0\rangle$$

5.3.3 Circuito Cuántico de la QFT de 3-qubits

En este caso, *n=3*. Aplicando nuevamente la Proposición *5.5*, tenemos que si $x_0,x_1,x_2\in\{0,1\}$ entonces

$$QFT\;|x_2x_1x_0\rangle=\frac{1}{\sqrt{2^3}}\bigotimes_{l=1}^{3}\left(\;|0\rangle+e^{2\,\pi\,i\;0.x_{l-1}x_{l-2}....x_0}\;|1\rangle\;\right)=$$

$$\frac{1}{\sqrt{2^3}}\left(\;|0\rangle+e^{2\,\pi\,i\;0.x_0}\;|1\rangle\;\right)\otimes\left(\;|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\;\right)\otimes\left(\;|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\;\right)$$

Su circuito es el siguiente:

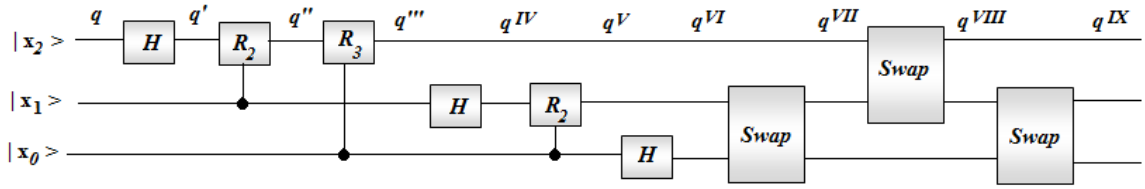


Figura 5.2: Circuito cuántico de la QFT para n = 3.

Probaremos que efectivamente este circuito genera la Transformada Cuántica de Fourier sobre el espacio de *3*-qubits. Primeramente, el estado inicial del sistema es

$$q = |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle$$

Al aplicar la compuerta *H* al primer qubit resulta:

$$q' = H|x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x_2}|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle$$

Como

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i\, x_1}{2^2}} \end{pmatrix}$$

Entonces

$$q'' = R_2\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x_2}|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}}\left(R_2|0\rangle + e^{2\pi i\, 0.x_2} R_2|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle =$$

$$= \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x_2}\, e^{\frac{2\pi i\, x_1}{2^2}}|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle =$$

$$\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x_2}\, e^{2\pi i\, 0.0x_1}|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle =$$

$$= \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, (0.x_2 + 0.0x_1)}|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x_2x_1}|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle$$

Al aplicar la compuerta

$$R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i\, x_0}{2^3}} \end{pmatrix}$$

Obtenemos

$$q''' = R_3\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x_2x_1}|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle =$$

$$\left(\frac{1}{\sqrt{2}}\left(R_3|0\rangle + e^{2\pi i\, 0.x_2x_1} R_3|1\rangle\right)\right) \otimes |x_1\rangle \otimes |x_0\rangle =$$

$$\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1}\;e^{\frac{2\,\pi\,i\;x_0}{2^3}}|1\rangle\right)\right)\otimes\;|x_1\rangle\otimes|x_0\rangle=$$

$$\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1}\;e^{2\,\pi\,i\;0.00x_0}\,|1\rangle\right)\right)\otimes\;|x_1\rangle\otimes|x_0\rangle=$$

$$\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right)\otimes\;|x_1\rangle\otimes|x_0\rangle$$

Al aplicar la compuerta *H* al segundo qubit se obtiene el siguiente estado

$$q^{IV}=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right)\otimes\;H\,|x_1\rangle\otimes|x_0\rangle=$$

$$=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right)\otimes\;\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1}\;|1\rangle\right)\right)\otimes|x_0\rangle$$

A continuación se aplica al segundo qubit la compuerta

$$R_2=\begin{pmatrix}1 & 0\\ 0 & e^{\frac{2\,\pi\,i\;x_0}{2^2}}\end{pmatrix}$$

Con lo cual resulta el siguiente estado:

$$q^{V}=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right)\otimes\;R_2\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1}\;|1\rangle\right)\right)\otimes|x_0\rangle=$$

$$=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right)\otimes\;\left(\frac{1}{\sqrt{2}}\left(R_2\,|0\rangle+e^{2\,\pi\,i\;0.x_1}\;R_2\,|1\rangle\right)\right)\otimes|x_0\rangle=$$

$$=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right)\otimes\;\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)\otimes|x_0\rangle$$

Aplicando la compuerta *H* al tercer qubit resulta:

$$q^{VI}=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right)\otimes\;\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)\otimes H\,|x_0\rangle=$$

$$=\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right)\otimes\;\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)\otimes\left(\frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right)$$

A continuación se intercambian el Segundo y tercer qubit a través de la compuerta *Swap*:

$$q^{VII} = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right) \otimes Swap\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right) =$$

$$= \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)$$

Luego se intercambian el primer y segundo qubit para obtener el siguiente estado:

$$q^{VIII} = Swap\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right) =$$

$$= \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right)$$

Finalmente se intercambian el segundo y tercer qubit

$$q^{IX} = \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right) \otimes Swap\left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right) =$$

$$= \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_1x_0}\;|1\rangle\right)\right) \otimes \left(\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\,\pi\,i\;0.x_2x_1x_0}\;|1\rangle\right)\right) =$$

$$= \frac{1}{\sqrt{2^3}} \bigotimes_{l=1}^{3}\left(\;|0\rangle + e^{2\,\pi\,i\;0.x_{l-1}x_{l-2}\ldots.x_0}\;|1\rangle\;\right) = QFT\;|x_2x_1x_0\rangle$$

5.3.4 Circuito Cuántico de la QFT de n-qubits (caso general)

El circuito cuántico que implementa la Transformada Cuántica de Fourier de *n*-qubits utiliza compuertas de *Hadamard*, de *Desplazamiento de Fase* y compuertas *Swaps*. Para simplificar su representación gráfica, se omitirán las compuertas *Swaps*. El circuito se muestra a continuación:

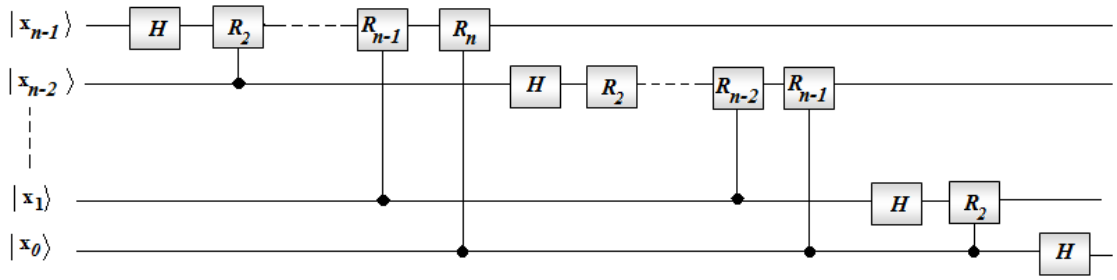


Figura 5.3: Circuito cuántico de la QFT de n qubits.

Como podemos comprobar, el qubit $|x_0\rangle$ requiere una compuerta de *Hadamard*, el qubit $|x_1\rangle$ requiere una compuerta de *Hadamard* y una de *Desplazamiento de Fase* y cada qubit que le antecede precisa una compuerta adicional de *Desplazamiento de Fase*.

En la próxima sección analizaremos el costo que demanda construir el circuito cuántico asociado a la Transformada Cuántica de Fourier, contando la cantidad de compuertas requeridas para su diseño.

Cantidad de compuertas requeridas para el circuito cuántico de la QFT de n-qubits

Primeramente enunciaremos la siguiente Proposición, que determina la cantidad de compuertas *Swaps* utilizadas en el circuito cuántico de la Transformada Cuántica de Fourier.

Proposición 5.6

La cantidad de compuertas Swaps que se necesitan en el circuito cuántico de la QFT de n-qubits es

$$\frac{n(n-1)}{2}$$

Demostración

Antes de ejecutar las compuertas *Swaps*, el estado del sistema es

$$a_n \otimes a_{n-1} \otimes .... \otimes a_1$$

Donde

$$a_k = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x_{k-1}....x_1x_0}\ |1\rangle\right),\ con\ k = 1, 2,...,n$$

Como debemos llegar al estado final, que es de la forma

$$a_1 \otimes a_2 \otimes .... \otimes a_n$$

Entonces probaremos, aplicando *El Principio de Inducción* sobre *n*, con $n \geq 2$, que se necesitan $\frac{n(n-1)}{2}$ compuertas *Swaps* para llevar un *n*-qubit $a_n \otimes a_{n-1} \otimes .... \otimes a_1$ a la forma $a_1 \otimes a_2 \otimes .... \otimes a_n$.

<u>*Para n = 2*</u>

Para llevar el *2*-qubit $a_2 \otimes a_1$ a la forma $a_1 \otimes a_2$ se necesita *1* compuerta *Swap*. Luego, la expresión es válida pues

$$\frac{n(n-1)}{2} = \frac{2(2-1)}{2} = 1$$

<u>*Hipótesis Inductiva:*</u>

Supongamos que la expresión es válida para *n*, es decir, se necesitan $\frac{n(n-1)}{2}$ compuertas *Swaps* para llevar un *n*-qubit $a_n \otimes a_{n-1} \otimes .... \otimes a_1$ a la forma $a_1 \otimes a_2 \otimes .... \otimes a_n$.

Verificación para $(n+1)$

Demostraremos que se precisan $\frac{n(n+1)}{2}$ compuertas *Swaps* para llevar un *(n+1)*-qubit $a_{n+1} \otimes a_n \otimes .... \otimes a_1$ a la forma $a_1 \otimes a_2 \otimes .... \otimes a_{n+1}$.

Primeramente ubicamos el qubit a_1 en la primera posición. Para ello se necesitan *n* compuertas *Swaps* que intercambien a_1 con a_k, para $k = 2,..., (n+1)$. De este modo, el *(n+1)*-qubit queda de la forma

$$a_1 \otimes \underbrace{a_{n+1} \otimes a_n \otimes .... \otimes a_3 \otimes a_2}$$

Aplicamos Hipótesis Inductiva

Por Hipótesis Inductiva, se necesitan $\frac{n(n-1)}{2}$ compuertas *Swaps* para llevar un *n*-qubit $a_{n+1} \otimes a_n \otimes .... \otimes a_3 \otimes a_2$ a la forma $a_2 \otimes a_3 \otimes .... \otimes a_{n+1}$.

En consecuencia, la cantidad de compuertas *Swaps* que se precisan para llevar un *(n+1)*-qubit $a_{n+1} \otimes a_n \otimes .... \otimes a_1$ a la forma $a_1 \otimes a_2 \otimes .... \otimes a_{n+1}$ es

$$n + \frac{n(n-1)}{2} = \frac{2n + n(n-1)}{2} = \frac{2n + n^2 - n}{2} = \frac{n + n^2}{2} = \frac{n(n+1)}{2} \quad \blacksquare$$

Se puede probar (Ver Referencia [12], pág. 118) que el circuito cuántico de la Transformada Cuántica de Fourier de *n*-qubits contiene un total de n^2 compuertas cuánticas.

Como mencionamos al inicio de este Capítulo, la Transformada Cuántica de Fourier desempeñará un rol importante en el diseño del circuito cuántico para el cálculo de un logaritmo discreto. Dicho circuito será explicado detalladamente en el Capítulo 7.

CAPÍTULO 6

La función potencia modular y su compuerta

En este capítulo presentaremos y desarrollaremos la función potencia modular y su compuerta, que serán utilizadas en el algoritmo cuántico para calcular un logaritmo discreto.
También mostraremos Ejemplos que ayudarán a comprender esta función.

Definición 6.1: La función potencia modular

Sea p un número primo, "g" un generador de $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$ *y* $x \in \mathbb{Z}_p^*$. *La función potencia modular asociada a "g" y "x" es la función* $f : \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \to \mathbb{Z}_p$ *definida por*

$$f(a,b) = g^a \cdot x^{-b} \pmod{p}$$

Observemos que el generador "*g*" existe, en virtud del Teorema *1.47*. El siguiente Ejemplo ilustrará esta Definición.

Ejemplo 6.2

Sea $p = 5$.

1) Verificar que $g = 2$ es un generador de $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.

2) Si $x = 3$, calcular x^{-1} en $\mathbb{Z}_5$.

3) Si $f(a,b) = g^a \cdot x^{-b} \pmod{p}$, calcular $f(a,b)$ $\forall a, b \in \mathbb{Z}_p$.

Solución

1) Verificaremos que $\langle 2 \rangle = \mathbb{Z}_5^*$ calculando las potencias de *2* en $\mathbb{Z}_5^*$:

i	**0**	**1**	**2**	**3**
2^i	**1**	**2**	**4**	**3**

Por lo tanto, las potencias de *2* generan todos los elementos de $\mathbb{Z}_5^*$. Luego $g = 2$ es un generador de $\mathbb{Z}_5^*$.

2) Por la Proposición *1.30*, tenemos que

$$3^{-1} = \frac{1+5k}{3}$$

Para algún $k \in \mathbb{Z}$ *con* $0 \leq k \leq 3$ *y tal que* $\frac{1+5k}{3} \in \mathbb{Z}_5$

Para hallar el valor de *k*, diseñamos la siguiente tabla:

k	$\frac{1+5k}{3}$
0	$\frac{1}{3} \notin \mathbb{Z}_5$
1	$\frac{6}{3} = 2 \in \mathbb{Z}_5$

Por lo tanto $3^{-1} = 2$ en $\mathbb{Z}_5$.

3) En este caso, $f(a,b) = g^a \cdot x^{-b} = 2^a \cdot 3^{-b} = 2^a \cdot \left(3^{-1}\right)^b = 2^a \cdot 2^b = 2^{a+b} \pmod 5$

Es decir,

$$f(a,b) = 2^{a+b} \pmod 5$$

En la siguiente tabla mostramos los valores de la función para todos los elementos de su dominio.

a	b	$f(a,b) = 2^{a+b} \pmod 5$	a	b	$f(a,b) = 2^{a+b} \pmod 5$
0	0	1	3	0	3
0	1	2	3	1	1
0	2	4	3	2	2
0	3	3	3	3	4
0	4	1	3	4	3
1	0	2	4	0	1
1	1	4	4	1	2
1	2	3	4	2	4
1	3	1	4	3	3
1	4	2	4	4	1
2	0	4			
2	1	3			
2	2	1			
2	3	2			
2	4	4			

Para explicar cómo se completó la tabla, calcularemos a modo de ejemplo $f(2,3)$.

En este caso,

$f(2,3) = 2^{2+3} = 2^5 = 32 \equiv 2 \pmod 5$.

A continuación definiremos la compuerta *f* asociada a la función potencia modular. Esta compuerta será la encargada de guardar los valores de dicha función.

Definición 6.3: La compuerta f de la función potencia modular

Sea p un número primo y $f : \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \to \mathbb{Z}_p$ *definida por*

$$f(a,b) = g^a \cdot x^{-b} \pmod{p}$$

Donde "g" es un generador de $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$ *y* $x \in \mathbb{Z}_p^*$. *Sea* m *el menor número natural tal que* $p \leq 2^m$. *La compuerta f de 3m-qubits, simbolizada por* U_f *,es la transformación lineal unitaria definida por*

$$U_f\left(|a\rangle\ |b\rangle\ |c\rangle\right) = |a\rangle\ |b\rangle\ |c \oplus f(a,b)\rangle$$

Donde $a,\ b,\ c \in \mathbb{Z}_{2^m}$

$|a\rangle$ *es la representación en base 10 del m-qubit* $|a_{m-1}\ a_{m-2}...a_1\ a_0\rangle$

$|b\rangle$ *es la representación en base 10 del m-qubit* $|b_{m-1}\ b_{m-2}...b_1\ b_0\rangle$

$|c\rangle$ *es la representación en base 10 del m-qubit* $|c_{m-1}\ c_{m-2}...c_1\ c_0\rangle$

$\oplus$ *es la suma módulo 2 bit a bit.*

Su representación gráfica es la siguiente:

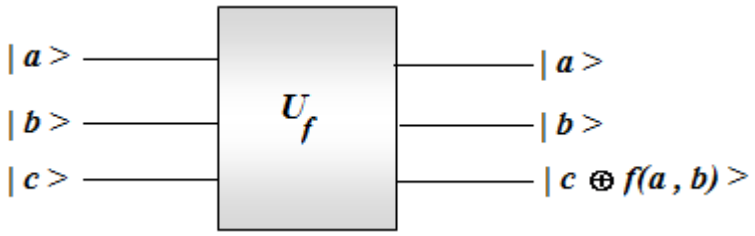


Figura 6.1: Representación gráfica de la compuerta f

El siguiente Ejemplo ilustrará cómo calcular esta compuerta.

Ejemplo 6.4

Sea $p = 7$, $g = 3$ un generador de $\mathbb{Z}_7^*$ y $x = 5$.

1) Hallar el menor número $m \in \mathbb{N}$ tal que $p \leq 2^m$.

2) Si $x = 5$, calcular x^{-1} en $\mathbb{Z}_7$.

3) Hallar la expresión de $f(a,b) = g^a \cdot x^{-b} \pmod{p}$.

4) Calcular $U_f\left(|2\rangle\ |1\rangle\ |3\rangle\right)$.

5) Calcular $U_f\left(|5\rangle\ |7\rangle\ |4\rangle\right)$.

Solución

1) Como

$$p \leq 2^m \Rightarrow \log_2(p) \leq \log_2\left(2^m\right) \Rightarrow \log_2(p) < \leq m \Rightarrow \log_2(7) \leq m\ .$$

Entonces

$$2.807 \leq m \Rightarrow m = 3.$$

2) Por la Proposición *1.30*, resulta

$$5^{-1} = \frac{1+7k}{5}$$

Para algún $k \in \mathbb{Z}$ *con* $0 \leq k \leq 5$ *y tal que* $\frac{1+7k}{5} \in \mathbb{Z}_7$.

Tomando *k = 2*, se verifica

$$\frac{1+7k}{5} = \frac{1+7(2)}{5} = 3 \in \mathbb{Z}_7$$

Luego

$$5^{-1} = 3 \text{ en } \mathbb{Z}_7 .$$

3) $f(a,b) = g^a \cdot x^{-b} = 3^a \cdot 5^{-b} = 3^a \cdot \left(5^{-1}\right)^b = 3^a \cdot 3^b = 3^{a+b} \pmod 7$

Es decir,

$$f(a,b) = 3^{a+b} \pmod 7$$

4) $U_f(|2\rangle\ |1\rangle\ |3\rangle) = |2\rangle\ |1\rangle\ |3 \oplus f(2,1)\rangle = |2\rangle\ |1\rangle\ |3 \oplus 3^{2+1} \pmod 7\rangle =$

$= |2\rangle\ |1\rangle\ |3 \oplus 3^3 \pmod 7\rangle = |2\rangle\ |1\rangle\ |3 \oplus 6\rangle = |2\rangle\ |1\rangle\ |011 \oplus 110\rangle = |2\rangle\ |1\rangle\ |101\rangle =$

$= |2\rangle\ |1\rangle\ |5\rangle .$

4) $U_f(|5\rangle\ |7\rangle\ |4\rangle) = |5\rangle\ |7\rangle\ |4 \oplus f(5,7)\rangle = |5\rangle\ |7\rangle\ |4 \oplus 3^{5+7} \pmod 7\rangle =$

$= |5\rangle\ |7\rangle\ |4 \oplus 3^{12} \pmod 7\rangle = |5\rangle\ |7\rangle\ |4 \oplus 1\rangle = |5\rangle\ |7\rangle\ |100 \oplus 001\rangle = |5\rangle\ |7\rangle\ |101\rangle =$

$= |5\rangle\ |7\rangle\ |5\rangle .$

Ejemplo 6.5

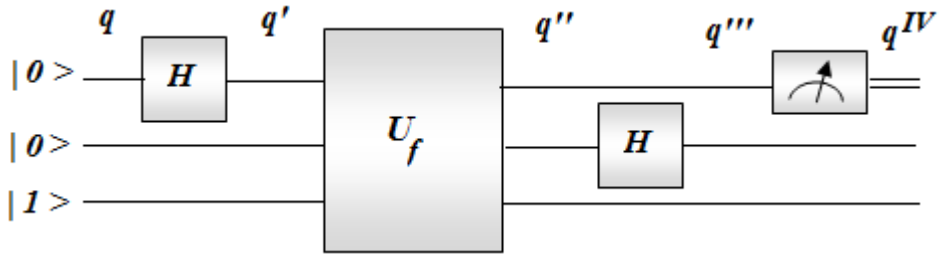
Sea *p = 2*.

1) Hallar la expresión de $f(a,b) = g^a \cdot x^{-b} \pmod p \ \ \forall a, b \in \mathbb{Z}_p$.

2) Calcular $U_f(|a\rangle\ |b\rangle\ |c\rangle) \ \ \forall a,\ b,\ c \in \mathbb{Z}_{2^m}$.

3) Hallar la representación matricial de la compuerta *f*.

4) Dado el siguiente circuito cuántico:



4.a) Determinar los estados del sistema q, q', q'' y q''' al atravesar cada compuerta.

4.b) Suponga que, al efectuar la medición del primer qubit, se obtuvo que éste se encuentra en estado *1*. Indicar a qué estado evoluciona el sistema.

4.c) ¿Cuál es la probabilidad de encontrar el tercer qubit del sistema en estado 0?

Solución

1) Como $p = 2$ entonces $\mathbb{Z}_p^* = \mathbb{Z}_2^* = \{ 1 \}$.

Por otro lado, como $g, x \in \mathbb{Z}_2^* = \{ 1 \}$ entonces $g = x = 1$.

En consecuencia $f(a,b) = g^a \cdot x^{-b} = 1^a \cdot 1^{-b} = 1 \ (mod\ 2)$. Luego

$$f(a,b) = 1 \quad \forall a, b \in \mathbb{Z}_2$$

2) En este caso, como

$$p \leq 2^m \Rightarrow log_2(p) \leq log_2\left(2^m\right) \Rightarrow log_2(p) \leq m \Rightarrow log_2(2) \leq m \Rightarrow 1 \leq m.$$

Luego, $m = 1$.

En la siguiente tabla se muestran los valores de $U_f\left(|a\rangle\ |b\rangle\ |c\rangle\right) \quad \forall a,\ b,\ c \in \mathbb{Z}_2$.

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

3) Observando los resultados de la tabla anterior tenemos:

$$U_f\ |000\rangle = |001\rangle = 0.\ |000\rangle + 1.|001\rangle + 0.|010\rangle + 0.|011\rangle + 0.|100\rangle + 0.|101\rangle + 0.|110\rangle + 0.|111\rangle$$

$$U_f\ |001\rangle = |000\rangle = 1.\ |000\rangle + 0.|001\rangle + 0.|010\rangle + 0.|011\rangle + 0.|100\rangle + 0.|101\rangle + 0.|110\rangle + 0.|111\rangle$$

$$U_f\ |010\rangle = |011\rangle = 0.\ |000\rangle + 0.|001\rangle + 0.|010\rangle + 1.|011\rangle + 0.|100\rangle + 0.|101\rangle + 0.|110\rangle + 0.|111\rangle$$

$$U_f\ |011\rangle = |010\rangle = 0.\ |000\rangle + 0.|001\rangle + 1.|010\rangle + 0.|011\rangle + 0.|100\rangle + 0.|101\rangle + 0.|110\rangle + 0.|111\rangle$$

$$U_f\ |100\rangle = |101\rangle = 0.\ |000\rangle + 0.|001\rangle + 0.|010\rangle + 0.|011\rangle + 0.|100\rangle + 1.|101\rangle + 0.|110\rangle + 0.|111\rangle$$

$$U_f\ |101\rangle = |100\rangle = 0.\ |000\rangle + 0.|001\rangle + 0.|010\rangle + 0.|011\rangle + 1.|100\rangle + 0.|101\rangle + 0.|110\rangle + 0.|111\rangle$$

$$U_f\ |110\rangle = |111\rangle = 0.\ |000\rangle + 0.|001\rangle + 0.|010\rangle + 0.|011\rangle + 0.|100\rangle + 0.|101\rangle + 0.|110\rangle + 1.|111\rangle$$

$$U_f\ |111\rangle = |110\rangle = 0.\ |000\rangle + 0.|001\rangle + 0.|010\rangle + 0.|011\rangle + 0.|100\rangle + 0.|101\rangle + 1.|110\rangle + 0.|111\rangle$$

Por lo tanto, la matriz asociada a la compuerta *f* es:

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

4.a) Por el Cuarto Postulado de la Mecánica Cuántica, el estado inicial del sistema es

$$q = |0\rangle \otimes |0\rangle \otimes |1\rangle$$

Al aplicar la compuerta *H* al primer qubit, el sistema evoluciona al siguiente estado:

$$q' = H\,|0\rangle \otimes |0\rangle \otimes |1\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |1\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |1\rangle$$

Es decir,

$$q' = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |1\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |1\rangle$$

Al atravesar la compuerta *f*, el sistema evoluciona del siguiente modo:

$$q'' = U_f\ \ q' = U_f\left(\frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |1\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |1\rangle\right) =$$

$$= \frac{1}{\sqrt{2}}U_f\left(|0\rangle \otimes |0\rangle \otimes |1\rangle\right) + \frac{1}{\sqrt{2}}U_f\left(|1\rangle \otimes |0\rangle \otimes |1\rangle\right) =$$

$$= \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |1 \oplus f\ (0,0)\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |1 \oplus f\ (1,0)\rangle =$$

$$= \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |1 \oplus 1\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |1 \oplus 1\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |0\rangle$$

Por lo tanto

$$q'' = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |0\rangle$$

Al aplicar la compuerta *H* al segundo qubit, el estado del sistema es

$$q''' = \frac{1}{\sqrt{2}}|0\rangle \otimes H\,|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes H\,|0\rangle \otimes |0\rangle =$$

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

$$= \frac{1}{2}|0\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{2}|0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{2}|1\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{2}|1\rangle \otimes |1\rangle \otimes |0\rangle$$

Luego

$$q''' = \frac{1}{2}|0\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{2}|0\rangle \otimes |1\rangle \otimes |0\rangle + \frac{1}{2}|1\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{2}|1\rangle \otimes |1\rangle \otimes |0\rangle$$

4.b) Si al medir el primer qubit se obtuvo que éste se encuentra en estado *1* entonces, por la Proposición *3.23* generalizada a sistemas de *3* qubits, el sistema evoluciona al siguiente estado:

$$q^{IV} = \frac{\frac{1}{2}|1\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{2}|1\rangle \otimes |1\rangle \otimes |0\rangle}{\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2}} = \frac{\frac{1}{2}|1\rangle \otimes |0\rangle \otimes |0\rangle + \frac{1}{2}|1\rangle \otimes |1\rangle \otimes |0\rangle}{\frac{1}{\sqrt{2}}}$$

Por lo tanto

$$q^{IV} = \frac{\sqrt{2}}{2}|1\rangle \otimes |0\rangle \otimes |0\rangle + \frac{\sqrt{2}}{2}|1\rangle \otimes |1\rangle \otimes |0\rangle$$

c) Observando el estado q^{IV} del sistema, resulta que

$$P\left(q_3 = |0\rangle\right) = \left|\frac{\sqrt{2}}{2}\right|^2 + \left|\frac{\sqrt{2}}{2}\right|^2 = \frac{1}{2} + \frac{1}{2} = 1$$

Luego, el tercer qubit del sistema estará en estado *0* con probabilidad *1*.

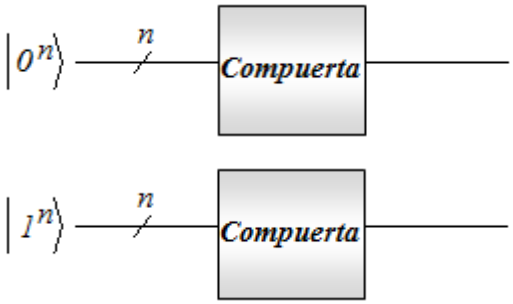
Notación 6.6

Al producto tensorial de *n* qubits, todos en estado *0* o bien todos en estado *1*, lo simbolizaremos por $|0^n\rangle$ y $|1^n\rangle$ respectivamente. Es decir,

$$|0^n\rangle = \underbrace{|0\rangle \otimes |0\rangle \otimes .... \otimes |0\rangle}_{n \text{ veces}}$$

$$|1^n\rangle = \underbrace{|1\rangle \otimes |1\rangle \otimes .... \otimes |1\rangle}_{n \text{ veces}}$$

En este caso, si a estos *n* qubits se les aplica una compuerta cuántica, su representación gráfica será la siguiente:

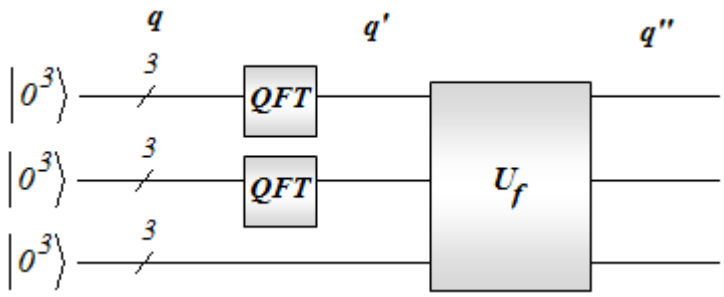


Ejemplo 6.7

Sea $p = 5$, $g = 2$ un generador de $\mathbb{Z}_5^* = \{1,2,3,4\}$ y $x = 3$. Según lo probado en el Ejemplo *6.2*, obtuvimos que $f(a,b) = g^a \cdot x^{-b} = 2^{a+b} \pmod 5 \ \forall a, b \in \mathbb{Z}_{\geq 0}$.

a) Definir la compuerta *f* de la función potencia modular.

b) Considere el siguiente circuito cuántico:



b.1) Hallar el estado final del sistema al atravesar cada compuerta.

b.2) Al medir todos los qubits del sistema luego de atravesar todas las compuertas, ¿cuál es la probabilidad de que el séptimo qubit esté en estado *1*, el octavo y noveno qubit estén en estado *0*?

b.3) Al medir el estado final del sistema, ¿cuál es la probabilidad de que los tres últimos qubits estén en estado *1*?

Solución

a) De acuerdo a la Definición *6.3*, primeramente hallamos el menor número natural *m* tal que $p \leq 2^m$. Es decir, $5 \leq 2^m \Rightarrow m = 3$. Por lo tanto

$$U_f\left(|a\rangle\ |b\rangle\ |c\rangle\right) = |a\rangle\ |b\rangle\ \left|c \oplus f\ (a,b)\right\rangle = |a\rangle\ |b\rangle\ \left|c \oplus 2^{a+b} \pmod 5\right\rangle$$

Donde $a,\ b,\ c \in \mathbb{Z}_{2^m} = \mathbb{Z}_8$

$|a\rangle$ *es la representación en base 10 del 3-qubit* $|a_2\ a_1\ \ a_0\rangle$

$|b\rangle$ *es la representación en base 10 del 3-qubit* $|b_2\ b_1\ \ b_0\rangle$

$|c\rangle$ *es la representación en base 10 del 3-qubit* $|c_2\ c_1\ \ c_0\rangle$

$\oplus$ *es la suma módulo 2 bit a bit.*

b.1) El estado inicial del sistema es

$$q = \left|0^3\right\rangle \otimes \left|0^3\right\rangle \otimes \left|0^3\right\rangle$$

Los primeros *3* qubits del sistema forman el primer registro, el cuarto, quinto y sexto qubit forman el segundo registro, mientras que los *3* últimos qubits constituyen el tercer registro del sistema. Al expresar cada registro en base *10*, el estado inicial se escribe

$$q = |0\rangle \otimes |0\rangle \otimes |0\rangle$$

Aplicamos la Transformada Cuántica de Fourier al primer y segundo registro. Luego, el sistema evoluciona al siguiente estado:

$$q' = QFT\ |0\rangle \otimes\ QFT\ |0\rangle \otimes\ |0\rangle = \left(\frac{1}{\sqrt{2^3}} \sum_{a=0}^{2^3-1} |a\rangle\ e^{\frac{2\ \pi\ i\ a.0}{2^3}} \right) \otimes \left(\frac{1}{\sqrt{2^3}} \sum_{b=0}^{2^3-1} |b\rangle\ e^{\frac{2\ \pi\ i\ b.0}{2^3}} \right) \otimes |0\rangle =$$

$$= \left(\frac{1}{\sqrt{2^3}} \sum_{a=0}^{2^3-1} |a\rangle \right) \otimes \left(\frac{1}{\sqrt{2^3}} \sum_{b=0}^{2^3-1} |b\rangle \right) \otimes |0\rangle = \frac{1}{2^3} \sum_{a=0}^{7} \sum_{b=0}^{7} |a\rangle \otimes |b\rangle \otimes |0\rangle$$

Es decir,

$$q' = \frac{1}{2^3} \sum_{a=0}^{7} \sum_{b=0}^{7} |a\rangle \otimes |b\rangle \otimes |0\rangle$$

Finalmente, al atravesar la compuerta U_f, el sistema evoluciona al siguiente estado:

$$q'' = U_f\ \ q' = U_f \left(\frac{1}{2^3} \sum_{a=0}^{7} \sum_{b=0}^{7} |a\rangle \otimes |b\rangle \otimes |0\rangle \right) = \frac{1}{2^3} \sum_{a=0}^{7} \sum_{b=0}^{7} U_f \left(|a\rangle \otimes |b\rangle \otimes |0\rangle \right) =$$

$$= \frac{1}{2^3} \sum_{a=0}^{7} \sum_{b=0}^{7} |a\rangle \otimes |b\rangle \otimes \left|0 \oplus f\ (a,b)\right\rangle = \frac{1}{2^3} \sum_{a=0}^{7} \sum_{b=0}^{7} |a\rangle \otimes |b\rangle \otimes \left|f\ (a,b)\right\rangle =$$

$$= \frac{1}{2^3} \sum_{a=0}^{7} \sum_{b=0}^{7} |a\rangle \otimes |b\rangle \otimes \left|2^{a+b}\ (mod\ 5\ )\right\rangle$$

Por lo tanto

$$q'' = \sum_{a=0}^{7} \sum_{b=0}^{7} \frac{1}{2^3}\ |a\rangle \otimes |b\rangle \otimes \underbrace{\left|2^{a+b}\ (mod\ 5\ )\right\rangle}_{\text{Tercer registro.}}$$

De esta manera hemos obtenido en forma simultánea, en el tercer registro, todos los valores de $f\ (a,b), \forall a,b \in \mathbb{Z}_8$. Es aquí donde se pone de manifiesto el paralelismo cuántico.

b.2) Para que, al efectuar la medición, el séptimo qubit esté en estado *1*, el octavo y noveno qubit estén en estado *0*, el tercer registro del sistema debe estar en estado $|100\rangle$. Dicho registro, expresado en base *10* es $|4\rangle$. Es decir, $\left|2^{a+b}\ (mod\ 5\ )\right\rangle = |4\rangle$.

Por lo tanto

$$P\left(q_7 = 1 \wedge q_8 = 0 \wedge q_9 = 0\right) = \sum_a \sum_b \left|\frac{1}{2^3}\right|^2$$

Donde la suma se efectúa sobre todos los pares (a,b) para los cuales $2^{a+b} \left(mod\ 5\right) = 4$

Los pares (a,b) que verifican esta condición figuran en la siguiente tabla, los cuales fueron obtenidos mediante un programa diseñado en Wolfram Mathematica *10.0*:

a	***b***	***a***	***b***
0	*2*	*4*	*2*
0	*6*	*4*	*6*
1	*1*	*5*	*1*
1	*5*	*5*	*5*
2	*0*	*6*	*0*
2	*4*	*6*	*4*
3	*3*	*7*	*3*
3	*7*	*7*	*7*

Observamos que hay *16* pares (a,b) que verifican que $\left|2^{a+b} \left(mod\ 5\right)\right\rangle = \left|4\right\rangle$. En consecuencia

$$P\left(q_7 = 1 \wedge q_8 = 0 \wedge q_9 = 0\right) = 16.\left|\frac{1}{2^3}\right|^2 = \frac{16}{2^6} = \frac{1}{4}$$

El código fuente del programa que calcula dichos pares (a,b) lo mostramos a continuación:

```
cont =0;
For [a = 0,  a ≤ 7,  a++, For [ b= 0,  b ≤ 7, b++, If [ Mod [ 2^(a+b) ,5] == 4, cont++;
Print [ a , b ] ] ] ;
Print [ "Total:", cont ]
```

b.3) En este caso, el tercer registro del sistema debe estar en estado $\left|111\right\rangle$ que, expresado en base *10*, es $\left|7\right\rangle$. Es decir, $\left|2^{a+b} \left(mod\ 5\right)\right\rangle = \left|7\right\rangle$. Por lo tanto

$$P\left(q_7 = 1 \wedge q_8 = 1 \wedge q_9 = 1\right) = \sum_a \sum_b \left|\frac{1}{2^3}\right|^2$$

Donde la suma se efectúa sobre todos los pares (a,b) para los cuales $2^{a+b} \left(mod\ 5\right) = 7$

Como esta ecuación no tiene solución (pues $2^{a+b} \left(mod\ 5\right)$ es un número perteneciente al conjunto $\mathbb{Z}_5 = \{0,1,2,3,4\}$), ningún par (a,b) verifica esta condición. En consecuencia

$$P\left(q_7 = 1 \wedge q_8 = 1 \wedge q_9 = 1\right) = 0$$

CAPÍTULO 7

Algoritmo cuántico para el cálculo de logaritmos discretos

En este capítulo desarrollaremos la parte de la publicación de Peter Shor, en la que describe el algoritmo cuántico para calcular un logaritmo discreto. Si bien el logaritmo discreto se define para cualquier grupo cíclico $(G,*)$, en este trabajo supondremos que $G=\mathbb{Z}_p^*$, con *p* un número primo. Previamente recordaremos su definición:

Definición 7.1: Logaritmo discreto en $\mathbb{Z}_p^*$

Sea $\left(\mathbb{Z}_p^*, \bullet\right)$ *con p un número primo y "g" un elemento generador de* $\mathbb{Z}_p^*$.

El logaritmo discreto en base "g" de un número $x \in \mathbb{Z}_p^*$ *es un número* $y \in \{0,1,...,p-1\} = \mathbb{Z}_p$ *que verifica:*

$$log_g(x) = y \Leftrightarrow g^y = x \ en \ \mathbb{Z}_p$$

O equivalentemente,

$$log_g(x) = y \Leftrightarrow g^y \equiv x \pmod{p}$$

Nuestro objetivo es entonces hallar el número $y \in \{0,1,...,p-1\}$ tal que $g^y = x \ en \ \mathbb{Z}_p$, dada la base "*g*" y el número $x \in \mathbb{Z}_p^*$. El algoritmo consta de dos partes:

Parte cuántica:

Es ejecutada por una computadora cuántica. Consiste en diseñar un circuito cuántico que tenga como dato al generador "*g*" y al número $x \in \mathbb{Z}_p^*$. El circuito debe producir como salida un par ordenado (c,d) y un elemento de la forma g^k, cuyo exponente "*k*" es desconocido. Luego identificaremos un subconjunto de tales pares que llamaremos "*buenos pares".*

Parte clásica:

Es ejecutada por una computadora convencional. Se encarga de hallar, a partir del par (c,d), el logaritmo discreto "*y*" en caso de que dicho par sea un "*buen par*" y si $c \neq 0$.

Los detalles de cada una de estas partes las describimos en la sección *7.2* y *7.3*, pero primeramente enunciaremos y demostraremos algunas Proposiciones que aplicaremos para justificar el Algoritmo que calcula un logaritmo discreto.

7. 1 Resultados matemáticos previos

Proposición 7.2

Sea p un número natural primo y "g" un generador de $\mathbb{Z}_p^*$ *. Entonces*

$$g^{p-1} \equiv 1 \pmod{p}$$

Además,

$$p-1 = min\left\{n \in \mathbb{N} / \; g^n \equiv 1 \pmod{p}\right\}$$

Demostración

Como "*g*" es un generador de $\mathbb{Z}_p^*$ entonces, por la Proposición *1.44* incisos *2*) y *3*) resulta

$$\mathbb{Z}_p^* = \langle g \rangle = \left\{g^1, g^2, ..., g^{n_0}\right\}$$

Donde

$$n_0 = min\left\{n \in \mathbb{N} / \; g^n = 1 \text{ en } \mathbb{Z}_p^*\right\} = min\left\{n \in \mathbb{N} / \; g^n \equiv 1 \pmod{p}\right\}$$

Por otro lado, como $card\left(\mathbb{Z}_p^*\right) = card\left(\langle g \rangle\right) \Rightarrow p-1 = n_0$. Es decir,

$$p-1 = min\left\{n \in \mathbb{N} / \; g^n \equiv 1 \pmod{p}\right\}$$

En consecuencia, $g^{p-1} \equiv 1 \pmod{p}$ ■

Proposición 7.3

Sean $a, b \in \mathbb{Z}_{\geq 0}$ *, p un número natural primo y "g" un generador de* $\mathbb{Z}_p^*$ *. Entonces*

$$g^a \equiv g^b \pmod{p} \Leftrightarrow a \equiv b \pmod{(p-1)}$$

Demostración

$\Rightarrow$) Sin pérdida de generalidad, podemos suponer que $a \geq b$. Entonces, como

$$g^a \equiv g^b \pmod{p} \Rightarrow g^{a-b} \equiv 1 \pmod{p} \qquad [I]$$

Luego, por la Proposición *7.2*, resulta

$$(p-1) \leq (a-b)$$

Por otro lado, por el Algoritmo de la División Entera, tenemos que

$$a-b = k(p-1) + r \qquad [II]$$

Con $k \in \mathbb{N} \wedge 0 \leq r < p-1$

Sustituyendo [II] en [I] y aplicando nuevamente la Proposición *7.2* obtenemos

$$g^{a-b} \equiv 1 \pmod{p} \Rightarrow g^{k(p-1)+r} \equiv 1 \pmod{p} \Rightarrow \left(g^{p-1}\right)^k . g^r \equiv 1 \pmod{p} \Rightarrow$$

$$\Rightarrow (1)^k . g^r \equiv 1 \pmod{p} \Rightarrow 1.g^r \equiv 1 \pmod{p} \Rightarrow g^r \equiv 1 \pmod{p}.$$

En consecuencia

$$r = 0 \qquad \text{[III]}$$

Sustituyendo [III] en [II] resulta

$$a - b = k\,(p-1)$$

Luego $(p-1) \mid (a-b) \Rightarrow a \equiv b \pmod{(p-1)}$.

$\Leftarrow$) Como $a \equiv b \pmod{(p-1)} \Rightarrow (p-1) \mid (a-b) \Rightarrow (a-b) = k\,(p-1)$

Para algún $k \in \mathbb{Z}$. Entonces $a = b + k\,(p-1)$. Por lo tanto, aplicando nuevamente la Proposición *7.2* obtenemos

$$g^a = g^{b+k(p-1)} = g^b . g^{k(p-1)} = g^b . \left(g^{(p-1)}\right)^k \equiv g^b . (1)^k \equiv g^b \pmod{p}$$

Luego $g^a \equiv g^b \pmod{p}$ ■

Definición 7.4: Parte entera, entero más próximo y residuo congruente

1) Si $a \in \mathbb{R}$ entonces "la parte entera de a" simbolizada por $[a]$, es el número entero que se obtiene de truncar la parte decimal del número a.

2) Si $a \in \mathbb{R}$ entonces $[\![a]\!]$ es el número entero que se encuentra más próximo al número a.

3) Si $u \geq 0$ y $n \in \mathbb{N}$ entonces "el residuo congruente con u módulo n", simbolizado por $\{u\}_n$ es

$$\{u\}_n = u - k.n$$

Donde $k \in \mathbb{Z}$ es tal que $-\frac{n}{2} < u - k.n \leq \frac{n}{2}$

Claramente se verifican las siguientes Propiedades:

1) $[a] = [\![a]\!] \quad \forall a \in \mathbb{Z}$

2) $[-a] = -[a] \quad \forall a \in \mathbb{R}$

3) $[\![-a]\!] = -[\![a]\!] \quad \forall a \in \mathbb{R}$.

El siguiente Ejemplo ayudará a aclarar estos conceptos.

Ejemplo 7.5

Calcular

1) $[1.7]$ 2) $[\![1.7]\!]$

3) $[-2.4]$ 4) $[\![-2.4]\!]$

5) $\{2000\}_{13}$

Solución

1) $\left[1.7\right]=1$

2) $[\![1.7]\!]=2$

3) $\left[-2.4\right]=-2$

4) $[\![-2.4]\!]=-2$

5) $\{2000\}_{13}=2000-k.13$

Donde *k* es tal que

$$-\frac{13}{2}<2000-k.13\leq\frac{13}{2}\ \Rightarrow-\frac{13}{2}-2000<-k.13\leq\frac{13}{2}-2000\Rightarrow-\frac{4013}{2}<-13k\leq-\frac{3987}{2}$$

$$\Rightarrow\frac{3987}{26}\leq k<\frac{4013}{26}\ \Rightarrow 153.34\leq k<154.34\Rightarrow k=154$$

Por lo tanto $\{2000\}_{13}=2000-k.13=2000-(154).13=2000-2002=-2$

Es decir

$$\{2000\}_{13}=-2$$

Proposición 7.6

Sean $a,b\in\mathbb{Z}_{\geq 0}$ *. Si* $a\equiv b\ (mod\ n)$ *entonces*

$$a=b\ -\left[\frac{b}{n}\right].n+k.n$$

Para algún $k\in\mathbb{Z}$

Demostración

Sea r_b es el resto de la división entera de *b* por *n*. Entonces, como

$a\equiv b\ (mod\ n)\ \wedge\ b\equiv r_b\ (mod\ n)\ \Rightarrow a\equiv r_b\ (mod\ n)\Rightarrow n\,|\,(a-r_b)$

Luego, $a-r_b=k.n$ para algún $k\in\mathbb{Z}$. Es decir

$$a=r_b+k.n \qquad \text{[I]}$$

Por otro lado, por el Algoritmo de la División Entera entre *b* y *n* se tiene que

$$b=\left[\frac{b}{n}\right]n+r_b$$

Entonces

$$r_b=b-\left[\frac{b}{n}\right]n \qquad \text{[II]}$$

Reemplazando [II] en [I] obtenemos finalmente

$$a=b\ -\left[\frac{b}{n}\right].n+k.n \qquad \blacksquare$$

Proposición 7.7

Sean $z_0 \in \mathbb{Z} \wedge b \in \mathbb{R}$. *. Entonces* $[\![z_0 + b]\!] = z_0 + [\![b]\!]$

Demostración

Consideramos los casos:

1) $z_0 \geq 0 \wedge b \geq 0.$

2) $z_0 \geq 0 \wedge b < 0.$

3) $z_0 < 0 \wedge b \geq 0.$

4) $z_0 < 0 \wedge b < 0.$

Sólo demostraremos la Proposición para el caso 1), ya que para los otros casos las demostraciones son similares.

Primeramente, observemos que si $a \geq 0$ entonces

$$[\![a]\!] = \begin{cases} [a] & si \mid a - [a] \mid \leq 0.5 \\ [a] + 1 & si \mid a - [a] \mid > 0.5 \end{cases} \qquad [I]$$

Por otro lado,

$$[z_0 + b] = [z_0] + [b] \qquad [II]$$

Pues si expresamos como suma de potencias de *10* tenemos que

$$z_0 = \sum_{i=0}^{n_0} \alpha_i \ 10^i \ \wedge \ b = \sum_{i=0}^{n_1} \beta_i \ 10^i + \sum_{i=1}^{\infty} \gamma_i \ 10^{-i}$$

Con $0 \leq \alpha_i, \beta_i, \gamma_i \leq 9 \ \ \forall i$

Entonces

$$z_0 + b = \underbrace{\sum_{i=0}^{n_0} \alpha_i \ 10^i + \sum_{i=0}^{n_1} \beta_i \ 10^i}_{\text{Parte entera}} + \underbrace{\sum_{i=1}^{\infty} \gamma_i \ 10^{-i}}_{\text{Parte fraccionaria}}$$

Luego

$$[z_0 + b] = \sum_{i=0}^{n_0} \alpha_i \ 10^i + \sum_{i=0}^{n_1} \beta_i \ 10^i = z_0 + [b] = [z_0] + [b]$$

Teniendo en cuenta las expresiones [I] y [II] y que $[z_0] = [\![z_0]\!] = z_0$ resulta

$$[\![z_0 + b]\!] = \begin{cases} [z_0 + b] & si \mid z_0 + b - [z_0 + b] \mid \leq 0.5 \\ [z_0 + b] + 1 & si \mid z_0 + b - [z_0 + b] \mid > 0.5 \end{cases} =$$

$$= \begin{cases} [z_0] + [b] & si \mid z_0 + b - [z_0] - [b] \mid \leq 0.5 \\ [z_0] + [b] + 1 & si \mid z_0 + b - [z_0] - [b] \mid > 0.5 \end{cases} = \begin{cases} [z_0] + [b] & si \mid z_0 + b - z_0 - [b] \mid \leq 0.5 \\ [z_0] + [b] + 1 & si \mid z_0 + b - z_0 - [b] \mid > 0.5 \end{cases} =$$

$$= \begin{cases} [z_0]+[b] & si \mid b-[b] \mid \leq 0.5 \\ [z_0]+[b]+1 & si \mid b-[b] \mid > 0.5 \end{cases} = [z_0] + \begin{cases} [b] & si \mid b-[b] \mid \leq 0.5 \\ [b]+1 & si \mid b-[b] \mid > 0.5 \end{cases} = z_0 + [\![b]\!] \quad \blacksquare$$

Proposición 7.8

Sean $a,b \in \mathbb{R}$ *tales que* $a<0 \wedge b>1$. *Entonces en el intervalo* $[a,b)$ *hay al menos* $[b]$ *números enteros.*

Demostración

Como $a \leq [a]$, los números enteros existentes en el intervalo $[a,b)$ son de la forma $[a]+k$, con $k \in \mathbb{Z}_{\geq 0}$ tal que $[a]+k<b$. Observemos que

$$a-[a]+1>0 \qquad \text{[I]}$$

Pues, como $\mid a-[a] \mid <1$ entonces $-1<a-[a]<1 \Rightarrow -1<a-[a] \Rightarrow a-[a]+1>0$

De la desigualdad [I] resulta que

$$[a]+[b]-1<a+b \qquad \text{[II]}$$

Ya que

$$[a]+[b]-1<a+b \Leftrightarrow \underbrace{a-[a]+1}_{>0} + \underbrace{b-[b]}_{\geq 0} > 0$$

Por [I]

De la expresión [II] concluimos que los números enteros de la forma

$$[a]+k \text{, con } k=0,1,...,[b]-1$$

Están en el intervalo $[a,b)$. En consecuencia, hay al menos $[b]$ números enteros en dicho intervalo. $\blacksquare$

Proposición 7.9

Sean $k_0, y_0 \in \mathbb{Z}$, $m,p \in \mathbb{N}$ *con* $p<2^m$, *y el conjunto*

$$K_0 = \left\{ (a,b) \in \mathbb{Z}\times\mathbb{Z} \,/\, k_0 \equiv a-b.y_0 \pmod{(p-1)} \wedge 0 \leq a,b<2^m \right\}$$

Sea T_{k_0} *la cantidad de elementos del conjunto* K_0. *Entonces*

1) $T_{k_0} \geq 2^m \left[\frac{2^m}{(p-1)} \right]$

2) $\sum_{k_0=0}^{p-2} T_{k_0} \geq 2^m \left[\frac{2^m}{(p-1)} \right] (p-1)$

3) $\sum_{k_0=0}^{p-2} T_{k_0}^2 \geq 2^{2m} \left[\frac{2^m}{(p-1)} \right]^2 (p-1)$

Demostración

1) Como $k_0 \equiv a - b.y_0 \ \left(mod\left(p-1\right)\right)$ entonces

$$a = k_0 + b.y_0 \ + k\left(p-1\right) \qquad \text{[I]}$$

Para algún $k \in \mathbb{Z}$.

Por otro lado, como $0 \le a < 2^m$ entonces, aplicando la ecuación [I] obtenemos

$$0 \le k_0 + b.y_0 \ + k\left(p-1\right) < 2^m$$

Despejando *k* de estas desigualdades resulta

$$-\frac{\left(k_0 + b.y_0\ \right)}{\left(p-1\right)} \le k < -\frac{\left(k_0 + b.y_0\ \right)}{\left(p-1\right)} + \frac{2^m}{\left(p-1\right)} \qquad \text{[II]}$$

De las expresiones [I] y [II] podemos reescribir el conjunto K_0 del siguiente modo:

$$K_0 = \left\{\left(k_0 + b.y_0 + k\left(p-1\right), b\right) / \ 0 \le b < 2^m \wedge -\frac{\left(k_0 + b.y_0\ \right)}{\left(p-1\right)} \le k < -\frac{\left(k_0 + b.y_0\ \right)}{\left(p-1\right)} + \frac{2^m}{\left(p-1\right)}\right\}$$

Teniendo en cuenta que, por la Proposición *7.8*, hay al menos $\left[\frac{2^m}{\left(p-1\right)}\right]$ valores de *k*, y 2^m valores de *b* entonces, por el Principio de la Multiplicación resulta que el conjunto K_0 tiene al menos $2^m\left[\frac{2^m}{\left(p-1\right)}\right]$ elementos. Es decir, $T_{k_0} \ge 2^m\left[\frac{2^m}{\left(p-1\right)}\right]$

2) $\sum_{k_0=0}^{p-2} T_{k_0} \ge \sum_{k_0=0}^{p-2} 2^m\left[\frac{2^m}{\left(p-1\right)}\right] = 2^m\left[\frac{2^m}{\left(p-1\right)}\right]\sum_{k_0=0}^{p-2} 1 = 2^m\left[\frac{2^m}{\left(p-1\right)}\right]\left(p-1\right)$

3) Aplicando el inciso *2*) y la Desigualdad de Cauchy-Schwarz (Teorema *1.6*) resulta

$$\left(2^m\left[\frac{2^m}{\left(p-1\right)}\right]\left(p-1\right)\right)^2 \le \left(\sum_{k_0=0}^{p-2} T_{k_0}\right)^2 = \left(\sum_{k_0=0}^{p-2} T_{k_0}.1\right)^2 \le \left(\sum_{k_0=0}^{p-2} T_{k_0}^2\right).\left(\sum_{k_0=0}^{p-2} 1^2\right) =$$

$$= \left(\sum_{k_0=0}^{p-2} T_{k_0}^2\right).\left(p-1\right)$$

Por lo tanto

$$\left(2^m\left[\frac{2^m}{\left(p-1\right)}\right]\left(p-1\right)\right)^2 \le \left(\sum_{k_0=0}^{p-2} T_{k_0}^2\right).\left(p-1\right)$$

Luego

$$\left(\sum_{k_0=0}^{p-2} T_{k_0}^2\right) \ge 2^{2m}\left[\frac{2^m}{\left(p-1\right)}\right]^2\left(p-1\right) \qquad \blacksquare$$

Proposición 7.10

Sean $\theta_j \in \mathbb{R}$, *tales que* $\left|\theta_j\right| \leq \frac{\pi}{4}$ *con* $0 \leq j < N$. *Entonces*

$$\left| \sum_{j=0}^{N-1} e^{i\,\theta_j} \right|^2 \geq \frac{N^2}{2}$$

Demostración

Como $\left|\theta_j\right| \leq \frac{\pi}{4}$ entonces $-\frac{\pi}{4} \leq \theta_j \leq \frac{\pi}{4}$. Luego $\frac{1}{\sqrt{2}} \leq cos\left(\theta_j\right) \leq 1$. Por lo tanto

$$\left| \sum_{j=0}^{N-1} e^{i\,\theta_j} \right|^2 = \left| \sum_{j=0}^{N-1} \left(cos\left(\theta_j\right) + i\, cos\left(\theta_j\right) \right) \right|^2 = \left| \sum_{j=0}^{N-1} cos\left(\theta_j\right) + i \sum_{j=0}^{N-1} sen\left(\theta_j\right) \right|^2 =$$

$$= \left| \sum_{j=0}^{N-1} cos\left(\theta_j\right) \right|^2 + \left| \sum_{j=0}^{N-1} sen\left(\theta_j\right) \right|^2 \geq \left| \sum_{j=0}^{N-1} cos\left(\theta_j\right) \right|^2 \geq \left| \sum_{j=0}^{N-1} \frac{1}{\sqrt{2}} \right|^2 = \left| \frac{1}{\sqrt{2}} \sum_{j=0}^{N-1} 1 \right|^2 =$$

$$= \left| \frac{1}{\sqrt{2}} . N \right|^2 = \frac{N^2}{2}$$

En consecuencia

$$\left| \sum_{j=0}^{N-1} e^{i\,\theta_j} \right|^2 \geq \frac{N^2}{2} \quad \blacksquare$$

Como mencionamos anteriormente, estos resultados los aplicaremos en las próximas secciones para justificar matemáticamente el algoritmo cuántico que calcula un logaritmo discreto.

7. 2 Parte cuántica del algoritmo que calcula un logaritmo discreto

Primeramente se toma el menor número $m \in \mathbb{N}$ tal que $p \leq 2^m$.

Luego se diseña un circuito cuántico que contenga 3*m* entradas:

$$q_1 = q_2 = ... = q_m = q_{m+1} = ... = q_{3m} = |0\rangle$$

Los primeros *m* qubits forman el primer registro, los qubits $q_{m+1},..,q_{2m}$ constituyen el segundo registro, y los últimos *m* qubits integran el tercer registro del sistema. Al primero, segundo y tercer registro los llamaremos, respectivamente, R_1, R_2 y R_3.

La representación gráfica de dicho circuito es la siguiente:

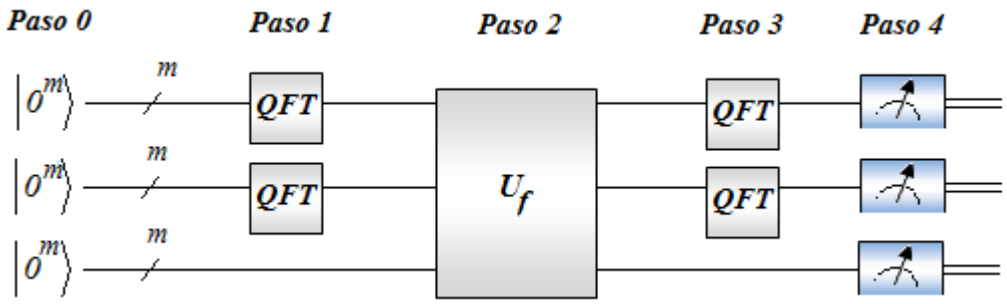


Figura 7.1: Circuito cuántico para el cálculo del logaritmo discreto.

Veamos cómo evoluciona el sistema al atravesar cada compuerta:

<u>*Paso 0*</u>

El estado inicial del sistema es

$$q = q_1 \otimes q_2 \otimes .... \otimes q_m \otimes q_{m+1} \ .... \otimes q_{3m} = |0\rangle \otimes |0\rangle \otimes .... \otimes |0\rangle ... \otimes |0\rangle = \left|0^m\right\rangle \otimes \left|0^m\right\rangle \otimes \left|0^m\right\rangle$$

Al expresar cada registro en base *10*, el estado inicial se escribe

$$q = |0\rangle \otimes |0\rangle \otimes |0\rangle$$

<u>*Paso 1*</u>

Se aplica la Transformada Cuántica de Fourier al primer y segundo registro, evolucionando el sistema al siguiente estado:

$$q' = (QFT \otimes QFT \otimes I)q = (QFT \otimes QFT \otimes I)(|0\rangle \otimes |0\rangle \otimes |0\rangle) = QFT\ |0\rangle \otimes QFT\ |0\rangle \otimes |0\rangle =$$

$$= \left(\frac{1}{\sqrt{2^m}} \sum_{a=0}^{2^m-1} |a\rangle\ e^{\frac{2\ \pi\ i\ a.0}{2^m}} \right) \otimes \left(\frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} |b\rangle\ e^{\frac{2\ \pi\ i\ b.0}{2^m}} \right) \otimes |0\rangle =$$

$$= \left(\frac{1}{\sqrt{2^m}} \sum_{a=0}^{2^m-1} |a\rangle \right) \otimes \left(\frac{1}{\sqrt{2^m}} \sum_{b=0}^{2^m-1} |b\rangle \right) \otimes |0\rangle = \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} |a\rangle \otimes |b\rangle \otimes |0\rangle$$

Es decir,

$$q' = \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} |a\rangle |b\rangle |0\rangle$$

Paso 2

Al atravesar la compuerta ***f***, el sistema evoluciona del siguiente modo:

$$q'' = U_f \cdot q' = U_f \left(\frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} |a\rangle|b\rangle|0\rangle \right) = \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} U_f \left(|a\rangle|b\rangle|0\rangle \right) =$$

$$= \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} |a\rangle|b\rangle|0 \oplus f\ (a,b)\rangle = \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} |a\rangle|b\rangle|\ f\ (a,b)\rangle =$$

$$\frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} |a\rangle\ |b\rangle \underbrace{|\ g^a.x^{-b}\ (mod\ p)\rangle}_{\text{Tercer registro.}}$$

Por lo tanto

$$q'' = \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} |a\rangle|b\rangle|\ g^a.x^{-b}\ (mod\ p)\rangle$$

Notemos que hemos obtenido en forma simultánea, en el tercer registro, todos los valores de $f\ (a,b), \forall a,b \in \mathbb{Z}_{2^m}$. Es aquí donde se evidencia el paralelismo cuántico.

Paso 3

Aplicamos nuevamente la Transformada Cuántica de Fourier al primer y segundo registro, evolucionando el sistema al siguiente estado:

$$q''' = (QFT \otimes QFT \otimes I) q'' = (QFT \otimes QFT \otimes I) \left(\frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} |a\rangle|b\rangle|\ g^a.x^{-b}\ (mod\ p)\rangle \right) =$$

$$= \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} QFT \otimes QFT \otimes I \left(|a\rangle\ |b\rangle\ |\ g^a.x^{-b}\ (mod\ p)\rangle \right) =$$

$$= \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} QFT\ |a\rangle \otimes QFT\ |b\rangle \otimes |\ g^a.x^{-b}\ (mod\ p)\rangle =$$

$$= \frac{1}{2^m} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} |c\rangle\ e^{\frac{2\pi i\ a.\ c}{2^m}} \otimes \frac{1}{\sqrt{2^m}} \sum_{d=0}^{2^m-1} |d\rangle\ e^{\frac{2\pi i\ b.\ d}{2^m}} \otimes |\ g^a.x^{-b}\ (mod\ p)\rangle =$$

$$= \frac{1}{2^{2m}} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} \sum_{c=0}^{2^m-1} \sum_{d=0}^{2^m-1} e^{\frac{2\pi i\ (a.\ c+b.\ d)}{2^m}} |c\rangle \otimes |d\rangle \otimes |\ g^a.x^{-b}\ (mod\ p)\rangle$$

Teniendo en cuenta que

$$g^{y} \equiv x \pmod{p}$$

Entonces, aplicando la Proposición *1.16*, incisos *6)* y *7)* resulta

$$g^{a}.x^{-b} \equiv g^{a}.\left(g^{y}\right)^{-b} = g^{a}.g^{-b.y} = g^{a-b.y} \pmod{p}$$

Es decir,

$$g^{a}.\, x^{-b} \equiv g^{a-b.y} \pmod{p}$$

Sustituyendo esta congruencia en la expresión de q''' obtenemos

$$q''' = \frac{1}{2^{2m}} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} \sum_{c=0}^{2^m-1} \sum_{d=0}^{2^m-1} e^{\frac{2\pi i\ (a.\,c+b.\,d)}{2^m}} |c\rangle \otimes |d\rangle \otimes \left| g^{a-b.y} \pmod{p} \right\rangle$$

En consecuencia

$$q''' = \frac{1}{2^{2m}} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} \sum_{c=0}^{2^m-1} \sum_{d=0}^{2^m-1} e^{\frac{2\pi i\ (a.\,c+b.\,d)}{2^m}} \left| c, d, g^{a-b.y} \pmod{p} \right\rangle$$

Observemos que el valor del logaritmo discreto que buscamos, es decir, el valor de $y = log_g(x)$ está "escondido" en el exponente del tercer registro.

<u>*Paso 4*</u>

Se efectúa la medición de los *3* registros, obteniendo un estado

$$|\, c_0, d_0, z_0 \rangle$$

Donde

$c_0,\ d_0 \in \{0,1,...,2^m-1\}$

$z_0 \in \mathbb{Z}_p^* = \{1,2,....,p-1\}$ *con* $z_0 \equiv g^{k_0} \pmod{p}$ *para algún* $k_0 \in \{0,1,...,p-2\}$.

En este caso, la probabilidad de obtener el estado $|\, c_0, d_0, z_0 \rangle$ se calcula considerando todos los coeficientes que multiplican a $|\, c_0, d_0, z_0 \rangle$. Más específicamente,

$$P\left(R_1 = c_0 \wedge R_2 = d_0 \wedge R_3 = z_0\right) = \left| \sum_{a} \sum_{b} \frac{1}{2^{2m}} e^{\frac{2\pi i\ (a.\,c_0+b.\,d_0)}{2^m}} \right|^2$$

Donde la suma se efectúa sobre todos los pares (a,b) para los cuales

$$z_0 \equiv g^{a-b.y} \pmod{p}$$

Es decir, tal que

$$g^{k_0} \equiv g^{a-b.y} \pmod{p}$$

Obviamente, esta fórmula de Probabilidad es meramente teórica, ya que involucra el valor del logaritmo discreto "*y*", que es nuestra incógnita. Sin embargo podremos obtener una cota inferior de dicha probabilidad, para ciertos pares (c_0 , d_0) que llamaremos "*buenos pares*". Pero previamente veremos el siguiente Ejemplo que ayudará a comprender lo desarrollado hasta ahora.

Ejemplo 7.11

Sea $p = 5$, $g = 2$ un generador de $\mathbb{Z}_5^* = \{1,2,3,4\}$ y $x = 3$.

a) Hallar el valor de *m* que indica el algoritmo cuántico descripto anteriormente.

b) Indicar el estado final del sistema al atravesar todas las compuertas del circuito cuántico.

c) Si se efectúa la medición de los qubits del sistema, ¿cuál es la probabilidad de obtener el estado $|\, c_0 , d_0 , z_0 \rangle = |1,4,2\rangle$?

d) ¿En qué estado se encuentra cada qubit que compone el sistema, si al efectuar la medición se obtuvo el *3m*-qubit $|1,4,2\rangle$?

Solución

a) Como *m* es el menor número natural que verifica:

$$p \le 2^m \Rightarrow 5 \le 2^m \Rightarrow m = 3$$

b) Teniendo en cuenta que $y = log_2(3) = 3 \ (mod\ 5)$ entonces, de acuerdo a lo obtenido en el *Paso 3* del Algoritmo Cuántico recientemente descripto, el estado final del sistema es

$$q''' = \frac{1}{2^{2m}} \sum_{a=0}^{2^m-1} \sum_{b=0}^{2^m-1} \sum_{c=0}^{2^m-1} \sum_{d=0}^{2^m-1} e^{\frac{2\pi i\ (a.\,c+b.\,d)}{2^m}} \left|\, c, d , g^{a-b.y} \ (mod\ p) \right\rangle =$$

$$= \frac{1}{2^6} \sum_{a=0}^{7} \sum_{b=0}^{7} \sum_{c=0}^{7} \sum_{d=0}^{7} e^{\frac{2\pi i\ (a.\,c+b.\,d)}{2^3}} \left|\, c, d , 2^{a-b.3} \ (mod\ 5) \right\rangle =$$

$$= \frac{1}{64} \sum_{a=0}^{7} \sum_{b=0}^{7} \sum_{c=0}^{7} \sum_{d=0}^{7} e^{\frac{\pi i\ (a.\,c+b.\,d)}{4}} \left|\, c, d , 2^{a-b.3} \ (mod\ 5) \right\rangle$$

Por lo tanto

$$q''' = \frac{1}{64} \sum_{a=0}^{7} \sum_{b=0}^{7} \sum_{c=0}^{7} \sum_{d=0}^{7} e^{\frac{\pi i\ (a.\,c+b.\,d)}{4}} \left|\, c, d , 2^{a-b.3} \ (mod\ 5) \right\rangle$$

c) La probabilidad de obtener el estado $|\, c_0 , d_0 , z_0 \rangle = |1,4,2\rangle$ es

$$P\left(\left|\, c_0\,,d_0\ ,z_0\,\right\rangle=\left|\,1,4\,,2\,\right\rangle\right)=\left|\sum_a\sum_b\ \frac{1}{2^{2m}}e^{\frac{2\pi i\ \left(a.\,c_0+b.\,d_0\right)}{2^m}}\right|^2=$$

$$=\left|\sum_a\sum_b\ \frac{1}{2^6}e^{\frac{2\pi i\ \left(a.\,1+b.\,4\right)}{2^3}}\right|^2=\frac{1}{2^{12}}\left|\sum_a\sum_b\ e^{\frac{\pi i\ \left(a+b.\,4\right)}{4}}\right|^2$$

Donde la suma se efectúa sobre todos los pares (a,b) para los cuales

$$z_0\equiv g^{a-b.y}\ (mod\ p)$$

Es decir

$$2\equiv 2^{a-b.3}\ (mod\ 5)$$

Los pares (a,b) que verifican esta condición figuran en la siguiente tabla, los cuales fueron obtenidos ejecutando un programa diseñado en Wolfram Mathematica *10.0* (similar al del Ejemplo *6.7*):

a	***b***
1	*0*
4	*1*
5	*0*
7	*2*

Por lo tanto

$$P\left(\left|\, c_0\,,d_0\ ,z_0\,\right\rangle=\left|\,1,4\,,2\,\right\rangle\right)=$$

$$=\frac{1}{2^{12}}\left|e^{\frac{\pi i\ \left(1+(0).\,4\right)}{4}}+e^{\frac{\pi i\ \left(4+(1)\,4\right)}{4}}+e^{\frac{\pi i\ \left(5+(0).\,4\right)}{4}}+e^{\frac{\pi i\ \left(7+(2).\,4\right)}{4}}\right|^2=$$

$$=\frac{1}{2^{12}}\left|e^{\frac{\pi i}{4}}+e^{2\pi i}+e^{\frac{5\pi i}{4}}+e^{\frac{15\pi i}{4}}\right|^2=$$

$$=\frac{1}{4096}\left|cos\left(\frac{\pi}{4}\right)+i\ sen\left(\frac{\pi}{4}\right)+cos\left(2\pi\right)+i\,sen\left(2\pi\right)+cos\left(\frac{5\pi}{4}\right)+i\ sen\left(\frac{5\pi}{4}\right)+cos\left(\frac{15\pi}{4}\right)+i\ sen\left(\frac{15\pi}{4}\right)\right|^2=$$

$$\frac{1}{4096}\left|\frac{\sqrt{2}}{2}+i\ \frac{\sqrt{2}}{2}+1-\frac{\sqrt{2}}{2}-i\ \frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}-i\ \frac{\sqrt{2}}{2}\right|^2=\frac{1}{4096}\left|1+\frac{\sqrt{2}}{2}-i\ \frac{\sqrt{2}}{2}\right|^2=$$

$$=\frac{1}{4096}\left(\left(1+\frac{\sqrt{2}}{2}\right)^2+\left(-\frac{\sqrt{2}}{2}\right)^2\right)=\frac{2+\sqrt{2}}{4096}=0.0008$$

En consecuencia

$$P\left(\left|\, c_0\,,d_0\ ,z_0\,\right\rangle=\left|\,1,4\,,2\,\right\rangle\right)=0.0008$$

d) Si al efectuarse la medición, se observa que el *3m*-qubit está en estado $|1,4,2\rangle$, significa que el primer registro se encuentra en estado $|1\rangle$, el segundo en estado $|4\rangle$ y el tercero en estado $|2\rangle$. Cada registro se compone de *m =3* qubits entonces, expresando los estados de cada registro en sistema binario resulta:

$$|1\rangle = |001\rangle$$
$$|4\rangle \equiv |100\rangle$$
$$|2\rangle \equiv |010\rangle$$

Entonces, al efectuar la medición, los qubits se encuentran en los siguientes estados:

Primer registro		***Segundo registro***		***Tercer registro***	
qubit	***estado***	***qubit***	***estado***	***qubit***	***estado***
primero	*0*	*cuarto*	*1*	*séptimo*	*0*
segundo	*0*	*quinto*	*0*	*octavo*	*1*
tercero	*1*	*sexto*	*0*	*noveno*	*0*

7.3. Noción de un buen par (c,d)

En esta sección introduciremos el concepto de "*un buen par* (c,d)" que se puede obtener luego de ejecutar el Circuito Cuántico y observar los *3* registros que componen el sistema.. Mostraremos que a partir de dicho "*buen par*" es posible hallar el valor del logaritmo discreto "*y*". Veamos su definición:

Definición 7.12: Un buen par (c,d)

Sea p un número primo, "m" el menor número natural tal que $p \le 2^m$. *Sea* $x \in \mathbb{Z}_p^*$ *e* $y = \log_g(x)$.

Se dice que un par (c,d), *con* $0 \le c,d \le 2^m - 1$ *es "un buen par" si verifica las siguientes condiciones:*

1) $\left| \{c(p-1)\}_{2^m} \right| \le 2^{m-4}$

2) $\left| \{c(p-1)\}_{2^m} \cdot \frac{y}{(p-1)} - f_j \right| \le 2^{-3}$

Para algún $f_j \in \mathbb{Z}$ *tal que* $d \equiv f_j - y.c \pmod{2^m}$

Por supuesto que, una vez ejecutado el Circuito Cuántico, es imposible chequear si el par (c,d) es un "*buen par*" ya que, en el inciso *2)* de la Definición *7.12,* figura el valor del logaritmo discreto "*y*" ", que es nuestra incógnita.

Puede que la definición de "*buen par*" resulte algo engorrosa, pero el siguiente Ejemplo ayudará a comprender el significado de las condiciones involucradas.

Ejemplo 7.13

Considere el Ejemplo *7.11*

a) ¿Es el par $(c,d)=(1,4)$ un "*buen par*"?

b) ¿Es el par $(c,d)=(4,4)$ un "*buen par*"?

Solución

De acuerdo al Ejemplo 7.*11*, tenemos que

$p = 5,\ g = 2\ ,\ m = 3\ ,\ x = 3$ e $y = log_g(x) = log_2(3) = 3$.

a) Veamos si $(c,d)=(1,4)$ verifica las dos condiciones para que sea un "*buen par*":

1)

$$\left| \{c(p-1)\}_{2^m} \right| \le 2^{m-4} \Leftrightarrow \left| \{1.(4)\}_{2^3} \right| \le 2^{3-4} \Leftrightarrow \left| \{4\}_8 \right| \le 2^{-1} \Leftrightarrow |4| \le 2^{-1} \Leftrightarrow 4 \le 0.5$$

Por lo tanto, como la última desigualdad es incorrecta, la condición *1*) no se verifica y en consecuencia $(1,4)$ no es un "*buen par*".

<u>*Cálculo auxiliar*</u>

$\{4\}_8 = 4 - k.8$

Donde $k \in \mathbb{Z}$ es tal que

$$-\frac{8}{2} < 4 - k.8 \le \frac{8}{2} \Rightarrow -4 < 4 - k.8 \le 4 \Rightarrow -8 < -k.8 \le 0 \Rightarrow 0 \le k < 1 \Rightarrow k = 0.$$

Luego

$\{4\}_8 = 4 - k.8 = 4 - 0.(8) = 4.$

b) Veamos ahora si $(c,d)=(4,4)$ es un "*buen par*":

1)

$$\left| \{c(p-1)\}_{2^m} \right| \le 2^{m-4} \Leftrightarrow \left| \{4.(4)\}_{2^3} \right| \le 2^{3-4} \Leftrightarrow \left| \{16\}_8 \right| \le 2^{-1} \Leftrightarrow |0| \le 2^{-1} \Leftrightarrow 0 \le 0.5$$

Como la última desigualdad es correcta, la condición *1*) se verifica.

<u>*Cálculo auxiliar*</u>

$\{16\}_8 = 16 - k.8$

Donde $k \in \mathbb{Z}$ es tal que

$$-\frac{8}{2} < 16 - k.8 \le \frac{8}{2} \Rightarrow -4 < 16 - k.8 \le 4 \Rightarrow -20 < -k.8 \le -12 \Rightarrow \frac{12}{8} \le k < \frac{20}{8} \Rightarrow$$

$$\Rightarrow 1.5 \le k < 2.5 \Rightarrow k = 2$$

Luego

$$\{16\}_8 = 16 - k.8 = 16 - 2.(8) = 0.$$

2)

$$\left| \{c(p-1)\}_{2^m} \cdot \frac{y}{(p-1)} - f_j \right| \leq 2^{-3} \Leftrightarrow \left| \{16\}_8 \cdot \frac{3}{4} - f_j \right| \leq 2^{-3} \Leftrightarrow \left| 0.\frac{3}{4} - f_j \right| \leq 2^{-3} \Leftrightarrow$$

$$\left| f_j \right| \leq \frac{1}{8}$$

Para algún $f_j \in \mathbb{Z}$ tal que $d \equiv f_j - y.c \pmod{2^m}$

Es decir, tal que

$$4 \equiv f_j - 3.(4) \pmod 8 \Rightarrow 4 \equiv f_j - 3.(4) \pmod 8 \Rightarrow f_j \equiv 16 \pmod 8$$

Luego,

$$f_j = 16 + 8k \text{ con } k \in \mathbb{Z}.$$

Por lo tanto, tomando $k = -2$ se verifica que $\left| f_j \right| \leq \frac{1}{8}$ pues

$$\left| f_j \right| = \left| 16 + 8(-2) \right| = 0 \leq \frac{1}{8}$$

Luego , la condición *2*) se satisface y en consecuencia $(4,4)$ es un "*buen par*".

Se puede comprobar fácilmente que $(0, 0)$ es "*un buen par*". Pero cabe preguntarnos cuántos buenos pares existen. La respuesta la da el siguiente Teorema:

Teorema 7.14

Sea p un número primo, "m" el menor número natural tal que $p \leq 2^m$ *. Entonces hay al menos* $2^{m-8} + 1$ *"buenos pares".*

Demostración

Véase Referencia [*5*], pág. *10*. ■

La siguiente Proposición afirma que el único "*buen par*" cuya primera coordenada es nula es el par $(0, 0)$.

Proposición 7.15

$$\left\{(c,d) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_{2^m} \;/\; (c,d) \text{ es buen par} \wedge c = 0\right\} = \left\{(0,0)\right\}$$

Demostración

Sea (c,d) un "*buen par*" tal que $c = 0$. Veamos que $d = 0$.

Como $c = 0$ entonces

$$\left\{c\left(p-1\right)\right\}_{2^m} = \left\{0\right\}_{2^m} = 0$$

Por otro lado, de acuerdo al inciso *2*) de la Definición *7.12*, tenemos que

$$\left| \left\{c\left(p-1\right)\right\}_{2^m} \cdot \frac{y}{\left(p-1\right)} - f_j \right| \leq 2^{-3} \Rightarrow \left| 0 - f_j \right| \leq 2^{-3} \Rightarrow \left| f_j \right| \leq 2^{-3} \Rightarrow -2^{-3} \leq f_j \leq 2^{-3}$$

De aquí resulta que, como $f_j \in \mathbb{Z}$, entonces $f_j = 0$. Además, como

$$d \equiv f_j - y.c \pmod{2^m} \Rightarrow d \equiv 0 - y.(0) \pmod{2^m} \Rightarrow d \equiv 0 \pmod{2^m}$$

Luego $d = 0 + k.2^m = k.2^m$ para algún $k \in \mathbb{Z}$.

Como $d \in \mathbb{Z}_{2^m} \Rightarrow 0 \leq d < 2^m \Rightarrow 0 \leq k.2^m < 2^m \Rightarrow 0 \leq k < 1 \Rightarrow k = 0.$

En consecuencia $d = k.2^m = (0).2^m = 0.$ ■

A continuación analizaremos cuál es la probabilidad de que, con una sola ejecución del Circuito Cuántico, podamos obtener un determinado "*buen par*". Como dijimos, la importancia de conseguir "*un buen par*" se debe a que a partir de él podremos hallar el valor del logaritmo discreto.

Teorema 7.16

La probabilidad de obtener "un buen par" específico a partir de una sola ejecución del Circuito Cuántico es al menos $\frac{1}{2^{2m+1}} \cdot \left[\frac{2^m}{\left(p-1\right)}\right]^2 \left(p-1\right)$.

Donde

p es un número primo.

m es el menor número natural tal que $p \leq 2^m$.

$\left[\frac{2^m}{\left(p-1\right)}\right]$ *es la parte entera de* $\frac{2^m}{\left(p-1\right)}$.

Demostración

Al ejecutar el Circuito Cuántico (pág. *124*), vimos que si $0 \leq c_0, d_0 \leq 2^m - 1$ y $z_0 \equiv g^{k_0} \pmod{p}$ con $k_0 \in \left\{0,1,...,p-2\right\}$, entonces la probabilidad de obtener el estado $\left| c_0, d_0, z_0 \right\rangle$ es

$$P\left(R_1 = c_0 \wedge R_2 = d_0 \wedge R_3 = z_0\right) = \left| \sum_a \sum_b \frac{1}{2^{2m}} e^{\frac{2\pi i \left(a.c_0 + b.d_0\right)}{2^m}} \right|^2$$

O equivalentemente

$$P\left(R_1 = c_0 \wedge R_2 = d_0 \wedge R_3 = g^{k_0} \ (mod\ p)\right) = \left| \sum_a \sum_b \ \frac{1}{2^{2m}} e^{\frac{2\pi i \ (a.\ c_0 + b.\ d_0)}{2^m}} \right|^2 \qquad [I]$$

Donde la suma se efectúa sobre todos los pares (a,b), con $0 \le a,b \le 2^m - 1$, para los cuales

$$z_0 \equiv g^{a - b.y} \ (mod\ p)$$

Es decir, tal que

$$g^{k_0} \equiv g^{a - b.y} \ (mod\ p)$$

Entonces, por la Proposición *7.3* resulta

$$k_0 \equiv a - b.y \ \left(mod\ (p-1)\right)$$

Luego

$$a \equiv k_0 + b.y \ \left(mod\ (p-1)\right)$$

Aplicando la Proposición *7.6* a esta última expresión, obtenemos

$$a = k_0 + b.y - \left[\frac{k_0 + b.y}{p-1}\right](p-1) + k_1 (p-1)$$

Para algún $k_1 \in \mathbb{Z}$. Por lo tanto

$$a.\ c_0 + b.\ d_0 = \left(k_0 + b.y - \left[\frac{k_0 + b.y}{p-1}\right](p-1) + k_1 (p-1)\right) c_0 + b.\ d_0 =$$

$$= k_0.\ c_0 + b.y.\ c_0 - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\ c_0 + k_1 (p-1).\ c_0 + b.\ d_0$$

Luego

$$a.\ c_0 + b.\ d_0 = k_0.\ c_0 + b.y.\ c_0 - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\ c_0 + k_1 (p-1).\ c_0 + b.\ d_0 \qquad [II]$$

Reemplazando [II] en [I] resulta

$$\left| \sum_a \sum_b \ \frac{1}{2^{2m}} e^{\frac{2\pi i \ (a.\ c_0 + b.\ d_0)}{2^m}} \right|^2 = \frac{1}{2^{4m}} \left| \sum_a \sum_b \ e^{\frac{2\pi i \ (a.\ c_0 + b.\ d_0)}{2^m}} \right| =$$

$$\frac{1}{2^{4m}} \left| \sum_b \ e^{\frac{2\pi i}{2^m}\left(k_0.\ c_0 + b.y.\ c_0 - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\ c_0 + k_1 (p-1).\ c_0 + b.\ d_0\right)} \right|^2 =$$

$$\frac{1}{2^{4m}} \left| \sum_b \ e^{\frac{2\pi i}{2^m}\left(k_0.\ c_0 + k_1 (p-1).\ c_0\right)} . e^{\frac{2\pi i}{2^m}\left(b.(y.\ c_0 + d_0) - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\ c_0\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \cdot \underbrace{\left| e^{\frac{2\pi i}{2^m}\left(k_0 \,.\, c_0 + k_1 (p-1).\, c_0\right)} \right|^2}_{=1 \text{ por la Fórmula de Euler}} \cdot \left| \sum_b e^{\frac{2\pi i}{2^m}\left(b.\,(y\,.\,c_0 + d_0) - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\, c_0\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \cdot \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b - 2^{m-1} + 2^{m-1}\right).\,(y\,.\,c_0 + d_0) - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\, c_0\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \cdot \left| \sum_b e^{\frac{2\pi i}{2^m}.2^{m-1}.\,(y\,.\,c_0 + d_0)} \,.\, e^{\frac{2\pi i}{2^m}\left(\left(b - 2^{m-1}\right).\,(y\,.\,c_0 + d_0) - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\, c_0\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \cdot \underbrace{\left| e^{\pi i\,.\,(y\,.\,c_0 + d_0)} \right|^2}_{=1 \text{ por la Fórmula de Euler}} \cdot \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b - 2^{m-1}\right).\,(y\,.\,c_0 + d_0) - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\, c_0\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b - 2^{m-1}\right).\,(y\,.\,c_0 + d_0) - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\, c_0\right)} \right|^2$$

Luego, la probabilidad de obtener el estado $\left| c_0 \,,\, d_0 \,,\, z_0 \right\rangle$ es

$$\frac{1}{2^{4m}} \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b - 2^{m-1}\right).\,(y\,.\,c_0 + d_0) - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\, c_0\right)} \right|^2 \qquad \text{[III]}$$

Por otro lado, como

$$\left\{(p-1).\, c_0\right\}_{2^m} = (p-1).\, c_0 - k_2 .\, 2^m$$

Con $k_2 \in \mathbb{Z}$ y tal que $-\frac{2^m}{2} < (p-1).\, c_0 - k_2 .\, 2^m \leq \frac{2^m}{2}$

Entonces

$$(p-1).\, c_0 = \left\{(p-1).\, c_0\right\}_{2^m} + k_2 .\, 2^m \qquad \text{[IV]}$$

Sustituyendo [IV] en [III] tenemos que

$$\frac{1}{2^{4m}} \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b - 2^{m-1}\right).\,(y\,.\,c_0 + d_0) - \left[\frac{k_0 + b.y}{p-1}\right](p-1).\, c_0\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b-2^{m-1}\right).\left(y.c_0+d_0\right)-\left[\frac{k_0+b.y}{p-1}\right]\left(\{(p-1).c_0\}_{2^m}+k_2.2^m\right)\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \left| \sum_b e^{-\frac{2\pi i}{2^m}\left[\frac{k_0+b.y}{p-1}\right]k_2.2^m} . e^{\frac{2\pi i}{2^m}\left(\left(b-2^{m-1}\right).\left(y.c_0+d_0\right)-\left[\frac{k_0+b.y}{p-1}\right]\{(p-1).c_0\}_{2^m}\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \left| \sum_b \underbrace{e^{-2\pi i\left[\frac{k_0+b.y}{p-1}\right]k_2}}_{=1 \text{ por la Fórmula de Euler}} . e^{\frac{2\pi i}{2^m}\left(\left(b-2^{m-1}\right).\left(y.c_0+d_0\right)-\left[\frac{k_0+b.y}{p-1}\right]\{(p-1).c_0\}_{2^m}\right)} \right|^2 =$$

Por lo tanto, la probabilidad queda expresada del siguiente modo:

$$P\left(R_1=c_0 \wedge R_2=d_0 \wedge R_3=g^{k_0}\ (mod\ p)\right)=$$

$$= \frac{1}{2^{4m}} \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b-2^{m-1}\right).\left(y.c_0+d_0\right)-\left[\frac{k_0+b.y}{p-1}\right]\{(p-1).c_0\}_{2^m}\right)} \right|^2 \qquad [V]$$

Ahora bien, como (c_0, d_0) es un "*buen par*" entonces, de acuerdo a la Definición *7.11* tenemos que

$$f_j \equiv y.c_0 + d_0 \ \left(mod\ 2^m\right)$$

Luego, la probabilidad [V] se reduce a la siguiente expresión:

$$\frac{1}{2^{4m}} \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b-2^{m-1}\right).f_j-\left[\frac{k_0+b.y}{p-1}\right]\{(p-1).c_0\}_{2^m}\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \underbrace{\left| e^{\pi i\ \{(p-1).c_0\}_{2^m}\frac{y}{(p-1)}} \right|^2}_{=1 \text{ por la Fórmula de Euler}} . \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b-2^{m-1}\right).f_j-\left[\frac{k_0+b.y}{p-1}\right]\{(p-1).c_0\}_{2^m}\right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \left| \sum_b e^{\frac{2\pi i}{2^m}\left(\left(b-2^{m-1}\right).f_j-\left[\frac{k_0+b.y}{p-1}\right]\{(p-1).c_0\}_{2^m}+2^{m-1}.\{(p-1).c_0\}_{2^m}\frac{y}{(p-1)}\right)} \right|^2$$

Es decir, la probabilidad de obtener el estado $|c_0, d_0, z_0\rangle$ con (c_0, d_0) "*un buen par*" es

$$P\left(R_1=c_0 \wedge R_2=d_0 \wedge R_3=g^{k_0}\ (mod\ p)\ \wedge\ (c_0, d_0)\ buen\ par\right)=$$

$$= \frac{1}{2^{4m}} \left| \sum_{b} e^{\frac{2\pi i}{2^m}\left(\left(b - 2^{m-1}\right).f_j \; - \left[\frac{k_0 + b.y}{p-1}\right] \left\{(p-1).c_0\right\}_{2^m} + 2^{m-1}.\left\{(p-1).c_0\right\}_{2^m} \frac{y}{(p-1)} \right)} \right|^2 \quad \text{[VI]}$$

A continuación hallaremos una cota superior para el exponente de la expresión [VI]. Primeramente, como $0 \le k_0 < (p-1)$ entonces

$$\frac{b.y}{p-1} - 1 \le \left[\frac{k_0 + b.y}{p-1}\right] \le \frac{b.y}{p-1} + 1$$

Por lo tanto

$$\left| \left[\frac{k_0 + b.y}{p-1}\right] - \frac{b.y}{p-1} \right| \le 1 \quad \text{[VII]}$$

Por otro lado, si (c_0 , d_0) es "*un buen par*", por la Definición *7.11* resulta:

$$\left| \left\{(p-1).c_0\right\}_{2^m} \right| \le 2^{m-4} \;\wedge\; \left| \left\{(p-1).c_0\right\}_{2^m} \frac{y}{(p-1)} - f_j \right| \le 2^{-3} \quad \text{[VIII]}$$

Además, como

$$0 \le b < 2^m \Rightarrow -2^{m-1} \le b - 2^{m-1} < 2^m - 2^{m-1} \Rightarrow -2^{m-1} \le b - 2^{m-1} < 2^{m-1}(2-1)$$

$$\Rightarrow -2^{m-1} \le b - 2^{m-1} < 2^{m-1}$$

En consecuencia

$$\left| b - 2^{m-1} \right| \le 2^{m-1} \quad \text{[IX]}$$

Aplicando las acotaciones [VII], [VIII], [IX] y utilizando la Desigualdad Triangular obtenemos

$$\left| \left[\frac{k_0 + b.y}{p-1}\right] \left\{(p-1).c_0\right\}_{2^m} - \left(b - 2^{m-1}\right).f_j \; - \; 2^{m-1}.\left\{(p-1).c_0\right\}_{2^m} \frac{y}{(p-1)} \right| =$$

$$\left| \left[\frac{k_0 + b.y}{p-1}\right] \left\{(p-1).c_0\right\}_{2^m} - \left(b - 2^{m-1}\right).f_j \; - \; 2^{m-1}.\left\{(p-1).c_0\right\}_{2^m} \frac{y}{(p-1)} + \left\{(p-1).c_0\right\}_{2^m} \frac{b.y}{(p-1)} - \left\{(p-1).c_0\right\}_{2^m} \frac{b.y}{(p-1)} \right| \le$$

$$\le \left| \left\{(p-1).c_0\right\}_{2^m} \left(\left[\frac{k_0 + b.y}{p-1}\right] - \frac{b.y}{(p-1)} \right) \right| + \left| \left(b - 2^{m-1}\right).\left(\left\{(p-1).c_0\right\}_{2^m} \frac{y}{(p-1)} - f_j \right) \right| \le$$

$$\le \left| \left\{(p-1).c_0\right\}_{2^m} \right| . \left| \left[\frac{k_0 + b.y}{p-1}\right] - \frac{b.y}{(p-1)} \right| + \left| b - 2^{m-1} \right| . \left| \left\{(p-1).c_0\right\}_{2^m} \frac{y}{(p-1)} - f_j \right| \le$$

$$\le 2^{m-4}.(1) + 2^{m-1}.2^{-3} = 2^{m-4} + 2^{m-4} = 2.\left(2^{m-4}\right) = 2^{m-3}$$

Entonces

$$\left| \left[\frac{k_0 + b.y}{p-1} \right] \left\{ (p-1).\, c_0 \right\}_{2^m} - \left(b - 2^{m-1} \right).\, f_j \; - \; 2^{m-1}.\left\{ (p-1).\, c_0 \right\}_{2^m} \frac{y}{(p-1)} \right| \leq 2^{m-3} \qquad [X]$$

Luego, si definimos

$$\theta_b = \frac{2\pi}{2^m} \left(\left(b - 2^{m-1} \right).\, f_j \; - \left[\frac{k_0 + b.y}{p-1} \right] \left\{ (p-1).\, c_0 \right\}_{2^m} + 2^{m-1}.\left\{ (p-1).\, c_0 \right\}_{2^m} \frac{y}{(p-1)} \right)$$

Entonces, por [X] tenemos que

$$\left| \theta_b \right| \leq \frac{2\pi}{2^m}.2^{m-3} = \frac{\pi}{4}$$

En consecuencia, utilizando la expresión [VI] y aplicando la Proposición *7.10*, la probabilidad de obtener el estado $\left| c_0 , d_0 , z_0 \right\rangle$ con (c_0 , d_0) "*buen par*", queda acotada inferiormente por:

$$\frac{1}{2^{4m}} \left| \sum_b e^{\frac{2\pi i}{2^m} \left(\left(b - 2^{m-1} \right).\, f_j \; - \left[\frac{k_0 + b.y}{p-1} \right] \left\{ (p-1).\, c_0 \right\}_{2^m} + 2^{m-1}.\left\{ (p-1).\, c_0 \right\}_{2^m} \frac{y}{(p-1)} \right)} \right|^2 =$$

$$= \frac{1}{2^{4m}} \left| \sum_b e^{i\ \theta_b} \right|^2 \geq \frac{1}{2^{4m}} . \frac{T_{k_0}^2}{2}$$

Donde T_{k_0} es el valor definido en la Proposición *7.9*. Luego

$$P\left(R_1 = c_0 \wedge R_2 = d_0 \wedge R_3 = g^{k_0} \ (mod\ p) \ \wedge \ (c_0 , d_0)\ buen\ par \right) \geq \frac{1}{2^{4m}} . \frac{T_{k_0}^2}{2}$$

En consecuencia, haciendo uso de la Proposición *7.9*, inciso *3)*, la probabilidad de obtener el buen par (c_0 , d_0) queda acotada inferiormente del siguiente modo:

$$P\left(obtener\ el\ buen\ par\ (c_0 , d_0) \right) = \sum_{k_0 = 0}^{p-2} P\left(R_1 = c_0 \wedge R_2 = d_0 \wedge R_3 = g^{k_0} \ (mod\ p) \wedge (c_0 , d_0)\ buen\ par \right) \geq$$

$$\geq \sum_{k_0 = 0}^{p-2} \frac{1}{2^{4m}} . \frac{T_{k_0}^2}{2} = \frac{1}{2^{4m+1}} \sum_{k_0 = 0}^{p-2} T_{k_0}^2 \geq \frac{1}{2^{4m+1}} .2^{2m} \left[\frac{2^m}{(p-1)} \right]^2 (p-1) = \frac{1}{2^{2m+1}} . \left[\frac{2^m}{(p-1)} \right]^2 (p-1)$$

Es decir

$$P\left(obtener\ el\ buen\ par\ (c_0 , d_0) \right) \geq \frac{1}{2^{2m+1}} . \left[\frac{2^m}{(p-1)} \right]^2 (p-1) \quad \blacksquare$$

Veamos un Ejemplo de aplicación de este Teorema.

Ejemplo 7.17

Considerando el Ejemplo *7.13* , se probó que el par $(c,d) = (4,4)$ es un "*buen par*".

¿Cuál es la probabilidad de obtener el "*buen par*" $(c,d) = (4,4)$ ejecutando una sola vez el Circuito Cuántico?

Solución

En este caso, $p = 5$ y $m = 3$. Por el Teorema *7.16*, tenemos que

$$P\left(\textit{obtener el buen par}\,(4,4)\right) \geq \frac{1}{2^{2m+1}} \cdot \left[\frac{2^m}{(p-1)}\right]^2 (p-1) = \frac{1}{2^7} \cdot \left[\frac{2^3}{4}\right]^2 (4) = \frac{1}{128} \cdot [2]^2 (4) =$$

$$= \frac{16}{128} = 0.125$$

Por lo tanto, la probabilidad de obtener el buen par $(4,4)$ es al menos *0.125*.

Cabe preguntarnos ahora cuál es la probabilidad de obtener cualquier "*buen par*" con una sola ejecución del Circuito Cuántico. El siguiente Teorema nos muestra una cota inferior de dicha probabilidad.

Teorema 7.18

La probabilidad de obtener "un buen par" con primera coordenada no nula, a partir de una sola ejecución del Circuito Cuántico, es al menos $\frac{1}{2^{m+9}} \cdot \left[\frac{2^m}{(p-1)}\right]^2 (p-1)$.

Donde

p es un número primo.

m es el menor número natural tal que $p \leq 2^m$.

$\left[\frac{2^m}{(p-1)}\right]$ *es la parte entera de* $\frac{2^m}{(p-1)}$.

Demostración

Consideremos el conjunto

$$A = \left\{(c,d) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_{2^m} \;/\; (c,d) \textit{ es buen par} \wedge c \neq 0\right\}$$

Entonces, por la Proposición *7.15* resulta

$$A = \left\{(c,d) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_{2^m} \;/\; (c,d) \textit{ es buen par}\right\} - \left\{(c,d) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_{2^m} \;/\; (c,d) \textit{ es buen par} \wedge c = 0\right\} =$$

$$= \left\{(c,d) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_{2^m} \;/\; (c,d) \textit{ es buen par}\right\} - \left\{(0,0)\right\}$$

Luego, por el Teorema 7.14 tenemos que

$$card\,(A) = card\left(\left\{(c,d) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_{2^m} \;/\; (c,d) \textit{ es buen par}\right\} - \left\{(0,0)\right\}\right) =$$

$$= card\left(\left\{(c,d) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_{2^m} \;/\; (c,d) \textit{ es buen par}\right\}\right) - 1 \geq 2^{m-8} + 1 - 1 = 2^{m-8}.$$

Es decir

$$card\,(A) \geq 2^{m-8}$$

Si numeramos a los elementos del conjunto *A* de la forma

$$(c_1,d_1),(c_2,d_2),\ldots,\left(c_{card(A)},d_{card(A)}\right)$$

Entonces, aplicando el Teorema 7. 16 y teniendo en cuenta que la probabilidad de la unión de eventos disjuntos es la suma de las probabilidades de dichos eventos, resulta

$$P\left(obtener\ un\ buen\ par\ (c,d)\ con\ c\neq 0\right)=P\left(obtener\ (c_1,d_1)\vee(c_2,d_2)\vee\ldots\vee\left(c_{card(A)},d_{card(A)}\right)\right)=$$

$$=P\left(obtener\ (c_1,d_1)\right)+\ldots+P\left(obtener\left(c_{card(A)},d_{card(A)}\right)\right)=$$

$$\sum_{k=1}^{card(A)}P\left(obtener\ (c_k,d_k)\right)\geq\sum_{k=1}^{card(A)}\frac{1}{2^{2m+1}}.\left[\frac{2^m}{(p-1)}\right]^2(p-1)=$$

$$=\frac{1}{2^{2m+1}}.\left[\frac{2^m}{(p-1)}\right]^2(p-1)\sum_{k=1}^{card(A)}1=\frac{1}{2^{2m+1}}.\left[\frac{2^m}{(p-1)}\right]^2(p-1).\ card\ (A)\geq$$

$$\geq\frac{1}{2^{2m+1}}.\left[\frac{2^m}{(p-1)}\right]^2(p-1)2^{m-8}=\frac{1}{2^{m+9}}.\left[\frac{2^m}{(p-1)}\right]^2(p-1)$$

En consecuencia

$$P\left(obtener\ un\ buen\ par\ (c,d)\ con\ c\neq 0\right)\geq\frac{1}{2^{m+9}}.\left[\frac{2^m}{(p-1)}\right]^2(p-1)$$

O equivalentemente

$$P\left(obtener\ un\ buen\ par\ no\ nulo\right)\geq\frac{1}{2^{m+9}}.\left[\frac{2^m}{(p-1)}\right]^2(p-1)\qquad\blacksquare$$

Ejemplo 7.19

Considere el número primo $p=10061$.

a) Hallar el menor número natural *m* tal que $p\leq 2^m$.

b) Aplicar el Teorema *7.18* para hallar la probabilidad de que, al ejecutar una vez el Algoritmo Cuántico, se obtenga un "*buen par*" no nulo.

Solución

a) Como

$$p\leq 2^m\Rightarrow 10061\leq 2^m\Rightarrow ln\left(10061\right)\leq ln\left(2^m\right)\Rightarrow ln\left(10061\right)\leq m\ ln\left(2\right)\Rightarrow m\geq\frac{ln\left(10061\right)}{ln\left(2\right)}$$

$$\Rightarrow m\geq\frac{9.126}{0.693}\Rightarrow m\geq 13.29\ .$$

Por lo tanto, *m= 14*.

b) Aplicando el Teorema *7.18* obtenemos

$$P\left(obtener\ un\ buen\ par\ no\ nulo\right)\geq\frac{1}{2^{m+9}}.\left[\frac{2^m}{(p-1)}\right]^2(p-1)=\frac{1}{2^{23}}.\left[\frac{2^{14}}{(10061-1)}\right]^2(10061-1)=$$

$$=0.0012$$

Luego, la probabilidad de obtener "*un buen par*" no nulo es de al menos *0.0012*.
Finalizamos esta sección con la siguiente pregunta, de gran importancia porque pondrá de manifiesto la eficiencia del Algoritmo Cuántico frente a otros Algoritmos Clásicos que calculan logaritmos discretos: ¿Cuántas veces habrá que ejecutar el Circuito Cuántico hasta lograr obtener un "*buen par*" no nulo? El siguiente Teorema nos da una respuesta.

Teorema 7.19

Se espera tener que ejecutar a lo sumo

$$\frac{2^{m+9}}{\left[\frac{2^m}{(p-1)}\right]^2 (p-1)}$$

veces el Circuito Cuántico hasta lograr obtener "un buen par" no nulo.

Donde
p es un número primo.

m es el menor número natural tal que $p \le 2^m$.

$\left[\frac{2^m}{(p-1)}\right]$ *es la parte entera de* $\frac{2^m}{(p-1)}$.

Demostración

Definamos la variable aleatoria *X* como el número de veces que debemos repetir, de manera independiente, la ejecución del Circuito Cuántico hasta obtener por primera vez "*un buen par*" no nulo. Entonces

$$X = \{1, 2, 3, \ldots\}$$

Bajo estas condiciones, la variable X sigue una Distribución Geométrica o de Pascal, de parámetro

$$r = P\left(\textit{obtener un buen par no nulo}\right)$$

Por el Teorema *7.18* tenemos que

$$r \ge \frac{1}{2^{m+9}} \cdot \left[\frac{2^m}{(p-1)}\right]^2 (p-1) \qquad \text{[I]}$$

Por otro lado, según la Proposición *1.63*, la Esperanza de esta variable aleatoria es

$$E[X] = \frac{1}{r}$$

Aplicando la desigualdad [I] obtenemos

$$E[X] = \frac{1}{r} \le \frac{1}{\frac{1}{2^{m+9}} \cdot \left[\frac{2^m}{(p-1)}\right]^2 (p-1)} = \frac{2^{m+9}}{\left[\frac{2^m}{(p-1)}\right]^2 (p-1)}$$

Luego, se espera tener que hacer a lo sumo

$$\frac{2^{m+9}}{\left[\frac{2^m}{(p-1)}\right]^2 (p-1)}$$

Ejecuciones del Circuito Cuántico hasta obtener *"un buen par"* no nulo. ■

Ejemplo 7.20

Considere el Ejemplo *7.19*, donde $p = 10061$ y $m = 14$. Entonces

$$\frac{2^{m+9}}{\left[\frac{2^m}{(p-1)}\right]^2 (p-1)} = \frac{2^{14+9}}{\left[\frac{2^{14}}{10060}\right]^2 (10060)} = \frac{2^{23}}{[1.62]^2 (10060)} =$$

$$= \frac{8388610}{(1)(10060)} = 833.85$$

Por lo tanto, se espera tener que ejecutar el Circuito Cuántico a lo sumo *833* veces hasta lograr obtener "*un buen par*" no nulo.

Finalmente, podemos aspirar a responder a la siguiente pregunta: ¿Cuántas veces deberemos ejecutar el Circuito Cuántico hasta obtener un "*buen par*" no nulo, independientemente del número primo *p*? La respuesta es de sumo interés, especialmente si el número *p* es muy grande, ya que los Algoritmos Criptográficos cuya seguridad se basa en la dificultad para calcular logaritmos discretos, consideran números primos muy grandes. En el siguiente Corolario presentamos una respuesta.

Corolario 7.21

Si el número primo p es grande, se espera tener que ejecutar a lo sumo 1024 veces el Circuito Cuántico hasta lograr obtener "un buen par" no nulo.

Demostración

Por el Teorema *7.19*, se espera tener que ejecutar a lo sumo

$$\frac{2^{m+9}}{\left[\frac{2^m}{(p-1)}\right]^2 (p-1)}$$

Veces el Circuito Cuántico, hasta obtener un "*buen par*" no nulo. Como

$$p \le 2^m \Rightarrow p-1 < 2^m \Rightarrow \frac{2^m}{p-1} > 1 \Rightarrow \left[\frac{2^m}{p-1}\right] \ge 1 \Rightarrow \left[\frac{2^m}{p-1}\right]^2 \ge 1$$

Luego

$$\frac{1}{\left[\frac{2^m}{p-1}\right]^2} \leq 1 \qquad \text{[I]}$$

Por otro lado, como m es el menor número natural tal que $p \leq 2^m$ entonces $2^{m-1} < p \leq 2^m$. Por lo tanto

$$2^{m-1} < p \leq 2^m \Rightarrow 2^{m-1} - 1 < p - 1 \leq 2^m - 1 \Rightarrow \frac{1}{2^m - 1} \leq \frac{1}{p-1} < \frac{1}{2^{m-1} - 1} \Rightarrow$$

$$\frac{1}{p-1} < \frac{1}{2^{m-1} - 1} \Rightarrow \frac{2^m}{p-1} < \frac{2^m}{2^{m-1} - 1} \Rightarrow \frac{2^m}{p-1} < \frac{2^m}{2^m\left(2^{-1} - \frac{1}{2^m}\right)}$$

En consecuencia

$$\frac{2^m}{p-1} < \frac{1}{\frac{1}{2} - \frac{1}{2^m}} \qquad \text{[II]}$$

Aplicando las desigualdades [I] , [II] y teniendo en cuenta que si p es grande, también m lo es, resulta

$$\frac{2^{m+9}}{\left[\frac{2^m}{(p-1)}\right]^2 (p-1)} = \frac{2^m . 2^9}{\left[\frac{2^m}{(p-1)}\right]^2 (p-1)} \leq \frac{2^m . 2^9}{(p-1)} < \frac{2^9}{\frac{1}{2} - \frac{1}{2^m}} \xrightarrow[m \to \infty]{} \frac{2^9}{\frac{1}{2}} =$$

$$= 2^{10} = 1024$$

Por lo tanto, se espera tener que ejecutar a lo sumo *1024* veces el Circuito Cuántico hasta lograr obtener "*un buen par*" no nulo. ■

Observación 7.22

La ejecución de un Circuito Cuántico puede llevarse a cabo tantas veces como se desea y sin dificultad, gracias a la propiedad de *Reversibilidad* que tienen las compuertas cuánticas.

7. 3 Parte clásica del algoritmo que calcula un logaritmo discreto

La parte clásica del algoritmo consiste en utilizar un ordenador clásico para hallar el valor de $y = log_g(x)$ a partir del *3m*-qubit $|\, c_0 , d_0 , z_0 \rangle$ que se obtuvo al ejecutar el Circuito Cuántico, en caso de que el par (c_0 , d_0) sea "*un buen par*" y $c_0 \neq 0$.

El valor de $y = log_g(x)$ se calcula resolviendo una ecuación lineal modular, como lo prueba el siguiente Teorema:

Teorema 7.23

Sea p un número primo, "m" el menor número natural tal que $p \leq 2^m$. *Sea* $x \in \mathbb{Z}_p^*$ *e* $y = log_g(x) \pmod p$.

Si (c_0 , d_0) *es* "*un buen par*" , *con* $c_0 \neq 0$ *entonces "y" es solución de la ecuación lineal de congruencia*

$$y \,.\, t \equiv [\![\frac{d_0 .(p-1)}{2^m}]\!] \pmod{(p-1)}$$

Donde

$t \in \mathbb{Z}$ *es tal que* $-\frac{c_0 (p-1)}{2^m} - \frac{1}{2} < t \leq -\frac{c_0 (p-1)}{2^m} + \frac{1}{2}$

$[\![\frac{d_0 .(p-1)}{2^m}]\!]$ es *el número entero que se encuentra más próximo a* $\frac{d_0 .(p-1)}{2^m}$.

Demostración

Como (c_0 , d_0) es un "*buen par*" tenemos que, por el inciso *2*) de la Definición *7.12*:

$$\left| \{c_0 (p-1)\}_{2^m} \cdot \frac{y}{(p-1)} - f_j \right| \leq 2^{-3} \qquad \text{[I]}$$

Para algún $f_j \in \mathbb{Z}$ tal que

$$d_0 \equiv f_j - y \,.\, c_0 \pmod{2^m}$$

Es decir,

$$f_j = d_0 + y \,.\, c_0 + k_1 \,.\, 2^m \qquad \text{[II]}$$

Para algún $k_1 \in \mathbb{Z}$.

Por lo tanto, si definimos

$$\delta = \{c_0 (p-1)\}_{2^m} \cdot \frac{y}{(p-1)} - f_j \qquad \text{[III]}$$

Entonces por [I] resulta

$$|\, \delta \,| \leq 2^{-3} \qquad \text{[IV]}$$

Sustituyendo [II] en [III] tenemos

$$\delta = \left\{c_0\,(p-1)\right\}_{2^m} . \frac{y}{(p-1)} - d_0 - y\,.\,c_0 - k_1\,.\,2^m$$

Multiplicando miembro a miembro esta última igualdad por $(p-1)$ obtenemos

$$\delta\,.(p-1) = \left\{c_0\,(p-1)\right\}_{2^m} .y - d_0.(p-1) - y\,.\,c_0.(p-1) - k_1\,.\,2^m.(p-1)$$

Dividiendo miembro a miembro por 2^m resulta

$$\frac{\delta\,.(p-1)}{2^m} = \left\{c_0\,(p-1)\right\}_{2^m} . \frac{y}{2^m} - d_0 . \frac{(p-1)}{2^m} - y\,.\,c_0 . \frac{(p-1)}{2^m} - k_1\,.\,(p-1)$$

Agrupando los términos, queda

$$y . \left(\frac{\left\{c_0\,(p-1)\right\}_{2^m} - c_0\,(p-1)}{2^m} \right) - d_0 . \frac{(p-1)}{2^m} - k_1\,.\,(p-1) = \frac{\delta\,.(p-1)}{2^m} \qquad [V]$$

Teniendo en cuenta la Definición *7.4* de residuo congruente, resulta

$$\left\{c_0\,(p-1)\right\}_{2^m} = c_0\,(p-1) - k\,.\,2^m \text{ con } k \in \mathbb{Z}$$

Por lo tanto

$$\frac{\left\{c_0\,(p-1)\right\}_{2^m} - c_0\,(p-1)}{2^m} = -k \in \mathbb{Z}$$

Luego, si definimos

$$t = -k = \frac{\left\{c_0\,(p-1)\right\}_{2^m} - c_0\,(p-1)}{2^m} \qquad [VI]$$

Entonces, reemplazando [VI] en [V] tenemos

$$y\,.t - d_0 . \frac{(p-1)}{2^m} - k_1\,.\,(p-1) = \frac{\delta\,.(p-1)}{2^m}$$

En consecuencia

$$[\![y\,.t - d_0 . \frac{(p-1)}{2^m} - k_1\,.\,(p-1)]\!] = [\![\frac{\delta\,.(p-1)}{2^m}]\!]$$

Aplicando la Proposición 7.7 en el miembro izquierdo, obtenemos

$$y\,.t - k_1\,.\,(p-1) + [\![- d_0 . \frac{(p-1)}{2^m}]\!] = [\![\frac{\delta\,.(p-1)}{2^m}]\!]$$

Teniendo en cuenta que $[\![-a]\!] = -[\![a]\!] \;\; \forall a \in \mathbb{R}$ entonces

$$y\,.t - k_1\,.\,(p-1) - [\![d_0 . \frac{(p-1)}{2^m}]\!] = [\![\frac{\delta\,.(p-1)}{2^m}]\!] \qquad [VII]$$

Por otro lado, como

$$p < 2^m \Rightarrow p-1 < 2^m \Rightarrow \frac{p-1}{2^m} < 1$$

Luego, haciendo uso de la expresión [IV] resulta

$$\left|\frac{\delta.(p-1)}{2^m}\right| = |\delta|.\left|\frac{(p-1)}{2^m}\right| < |\delta|.1 \le 2^{-3}$$

En consecuencia

$$-2^{-3} \le \frac{\delta.(p-1)}{2^m} \le 2^{-3} \Rightarrow -\frac{1}{8} \le \frac{\delta.(p-1)}{2^m} \le \frac{1}{8}$$

De aquí obtenemos que

$$[\![\frac{\delta.(p-1)}{2^m}]\!] = 0 \qquad \text{[VIII]}$$

Sustituyendo [VIII] en [VII] resulta

$$y.t - k_1.(p-1) - [\![d_0.\frac{(p-1)}{2^m}]\!] = 0$$

Luego

$$y.t = k_1.(p-1) + [\![d_0.\frac{(p-1)}{2^m}]\!]$$

Es decir

$$y.t \equiv [\![\frac{d_0.(p-1)}{2^m}]\!] \ (mod\,(p-1))$$

Además, de la expresión [VI] y de la Definición 7.4 se deduce que

$$-\frac{c_0(p-1)}{2^m} - \frac{1}{2} < t \le -\frac{c_0(p-1)}{2^m} + \frac{1}{2} \qquad \blacksquare$$

Observación 7.24

La ecuación lineal de congruencia que indica el Teorema *7.23* se resuelve aplicando el Teorema *1.35*.

Ejemplo 7.25

Sea $p = 5$, $g = 2$ un generador de $\mathbb{Z}_5^* = \{1,2,3,4\}$ y $x = 3$. En el Ejemplo *7.13* se probó que $(c_0, d_0) = (4,4)$ es un "*buen par*". Aplique el Teorema *7.23* para hallar $y = log_2(3)\ (mod\ 5)$.

Solución

En este caso, $m=3$. Como $(c_0, d_0) = (4,4)$ es "*un buen par*" y $c_0 \neq 0$ entonces, por el Teorema *7.23,"y"* es solución de la ecuación lineal de congruencia

$$y.t \equiv [\![\frac{d_0.(p-1)}{2^m}]\!] \ (mod\,(p-1)) \qquad \text{[I]}$$

Cálculo de t

$t \in \mathbb{Z}$ es tal que

$$-\frac{c_0(p-1)}{2^m}-\frac{1}{2}<t\leq-\frac{c_0(p-1)}{2^m}+\frac{1}{2} \Rightarrow -\frac{4(4)}{8}-\frac{1}{2}<t\leq-\frac{4(4)}{8}+\frac{1}{2}\Rightarrow -2.5<t\leq -1.5$$

Por lo tanto

$$t=-2$$

Por otro lado,

$$[\![\frac{d_0.(p-1)}{2^m}]\!]=[\![\frac{4.(4)}{8}]\!]=[\![\frac{16}{8}]\!]=[\![2]\!]=2$$

Sustituyendo estos valores calculados en [I] resulta que la ecuación a resolver es

$$-2y\equiv 2 \pmod 4$$

Por la Proposición *1.16* inciso *9)* se verifica que $-2\equiv -2+4=2 \pmod 4$. Entonces la ecuación anterior es equivalente a la ecuación:

$$2y\equiv 2 \pmod 4 \qquad \text{[II]}$$

Para resolver esta ecuación, aplicamos el Teorema *1.35*. En este caso, *a = b = 2* y *n = 4*. Como $mcd(a,n)=2\neq 1 \wedge mcd(a,n)\mid b$ entonces existen $mcd(a,n)$ soluciones en $\mathbb{Z}_n$ y son de la forma

$$x_1+k\frac{n}{mcd(a,n)}\text{ , con } k=0,1,...,(mcd(a,n)-1)$$

Es decir

$$x_1+k\,2\text{ , con } k=0,1 \qquad \text{[III]}$$

Donde x_1 es la única solución en $\mathbb{Z}_{n/\,mcd(a,n)}$ de la ecuación de congruencia

$$\frac{a}{mcd(a,n)}.x\equiv\frac{b}{mcd(a,n)}\left(mod\ \frac{n}{mcd(a,n)}\right)$$

O sea,

$$x\equiv 1 \pmod 2$$

Por lo tanto

$$x_1=1 \qquad \text{[IV]}$$

Reemplazando [IV] en [III] obtenemos que las soluciones de la ecuación [II] son

$$1+k\,2\text{ , con } k=0,1$$

Luego, los candidatos a ser $log_2(3) \pmod 5$ son: *1* y *3*.

Como $2^3=8\equiv 3 \pmod 5$, concluimos que $log_2(3)=3 \pmod 5$.

De todo lo expuesto en este Capítulo, podemos resumir el algoritmo para hallar un logaritmo discreto del siguiente modo:

Algoritmo para el cálculo de $\log_g(x) \pmod p$

Parte Cuántica

1) Ejecutar los Pasos 1 al 4 del Circuito Cuántico, para obtener un par (c_0, d_0) .

Parte Clásica

2) Si $c_0 = 0$ *entonces*

Volver al inciso 1)

Sino

Resolver, aplicando el Teorema 1.35, la ecuación lineal de congruencia

$$y.t = [\![\frac{d_0.(p-1)}{2^m}]\!] \pmod{(p-1)}$$

Donde

m es el menor número natural tal que $p \le 2^m$

$t \in \mathbb{Z}$ *es tal que* $-\frac{c_0(p-1)}{2^m} - \frac{1}{2} < t \le -\frac{c_0(p-1)}{2^m} + \frac{1}{2}$

$[\![\frac{d_0.(p-1)}{2^m}]\!]$ *es el entero que se encuentra más próximo a* $\frac{d_0.(p-1)}{2^m}$.

3) Si la ecuación no tiene solución entonces

Volver al inciso 1)

Sino

Chequear cuál de las soluciones resulta ser $\log_g(x) \pmod p$,

comprobando que

$$g^y \equiv x \pmod p$$

Si ninguna solución verifica esta expresión, volver al inciso 1).

Mostraremos un Ejemplo más que ayudará a comprender el funcionamiento de la Parte Clásica del Algoritmo Cuántico.

Ejemplo 7.26

Sea el número primo *p = 10099.*

a) Hallar el menor número natural *m* tal que $p \le 2^m$.

b) Al ejecutar el Circuito Cuántico, se obtuvo el par $(c_0, d_0) = (4, 16345)$. Aplique la Parte Clásica del Algoritmo Cuántico para hallar $\log_{50}(5512) \pmod p$.

Solución

a) Como

$$p \le 2^m \Rightarrow 10099 \le 2^m \Rightarrow \ln(10099) \le \ln(2^m) \Rightarrow \ln(10099) \le m.\ln(2) \Rightarrow m \ge \frac{\ln(10099)}{\ln(2)}$$

$$\Rightarrow m \ge 13.30 \Rightarrow m = 14$$

b) Para hallar $log_{50}(5512) \pmod p$, resolvemos la ecuación lineal de congruencia

$$y.t \equiv [\![\frac{d_0.(p-1)}{2^m}]\!] \pmod{(p-1)} \qquad [I]$$

Cálculo de t

$t \in \mathbb{Z}$ es tal que

$$-\frac{c_0(p-1)}{2^m}-\frac{1}{2}<t\leq-\frac{c_0(p-1)}{2^m}+\frac{1}{2} \Rightarrow -\frac{4(10098)}{2^{14}}-\frac{1}{2}<t\leq-\frac{4(10098)}{2^{14}}+\frac{1}{2}\Rightarrow$$

$$\Rightarrow -2.96 < t \leq -1.96$$

Por lo tanto

$$t = -2$$

Por otro lado,

$$[\![\frac{d_0.(p-1)}{2^m}]\!] = [\![\frac{16345.(10098)}{16384}]\!] = [\![10073.96]\!] = 10074$$

Sustituyendo estos valores calculados en [I] resulta que la ecuación a resolver es

$$-2y \equiv 10074 \pmod{10098}$$

Como $-2 \equiv -2+10098 = 10096 \pmod{10098}$ entonces la ecuación anterior es equivalente a la ecuación:

$$10096\,y \equiv 10074 \pmod{10098} \qquad [II]$$

Nuevamente, para resolver esta ecuación, aplicamos el Teorema *1.35*. En este caso, *a = 10096, b = 10074* y *n = 10098*.

Como $mcd(a,n) = 2 \neq 1 \ \wedge \ mcd(a,n) \mid b$ entonces existen $mcd(a,n)$ soluciones en $\mathbb{Z}_n$ y son de la forma

$$x_1 + k\,\frac{n}{mcd(a,n)}\ , con\ k = 0,1,...,(mcd(a,n)-1)$$

Es decir

$$x_1 + 5049k\ , con\ k = 0,1 \qquad [III]$$

Donde x_1 es la única solución en $\mathbb{Z}_{n/\,mcd(a,n)}$ de la ecuación de congruencia

$$\frac{a}{mcd(a,n)}.x \equiv \frac{b}{mcd(a,n)} \left(mod\ \frac{n}{mcd(a,n)}\right)$$

O sea,

$$5048x \equiv 5037 \pmod{5049}$$

Al resolver esta ecuación tenemos que

$$x \equiv (5048)^{-1}.5037 \pmod{5049}$$

Al aplicar la Proposición *1.30,* resulta que $(5048)^{-1} = 5048$ en $\mathbb{Z}_{5049}$. Por lo tanto

$$x \equiv (5048).5037 \pmod{5049}$$

Luego

$$x \equiv 25426776 \pmod{5049}$$

Por la Proposición *1.15* inciso *8*), resulta que $25426776 \equiv 12 \pmod{5049}$. Entonces

$$x \equiv 12 \pmod{5049}$$

En consecuencia,

$$x_1 = 12 \qquad \text{[IV]}$$

Reemplazando [IV] en [III] obtenemos que las soluciones de la ecuación [II] son

$$12 + 5049k \ , \text{con } k = 0,1$$

Luego, los candidatos a ser $log_{50}(5512) \pmod{10099}$ son: *12* y *5061*.

Aplicando el Algoritmo para el Cálculo de la Potencia Modular (pág. *19*), tenemos que

$50^{12} \equiv 5512 \pmod{10099}$

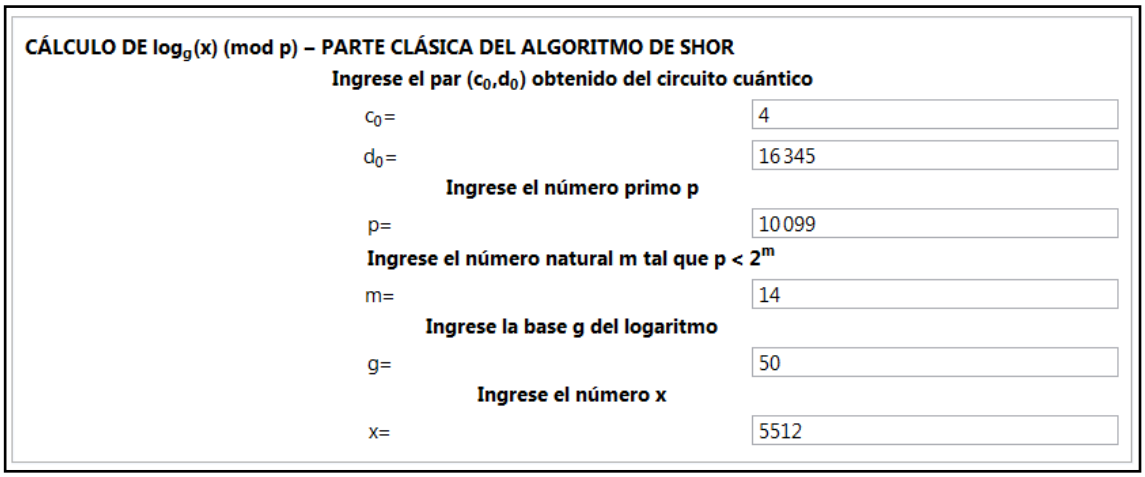
$50^{5061} \equiv 4587 \pmod{10099}$

Por lo tanto, concluimos que $log_{50}(5512) = 12 \pmod{10099}$.

Finalizamos este capítulo mostrando la implementación de la Parte Clásica del Algoritmo de Shor mediante el software Wolfram Mathematica.

7.3.1 Implementación de la Parte Clásica del Algoritmo Cuántico mediante Wolfram Mathematica 10.0

El siguiente programa, diseñado mediante el software Wolfram Mathematica *10.0*, implementa la Parte Clásica del Algoritmo de Shor para el cálculo de logaritmos discretos. Para ejecutar el programa se ingresan los datos en un cuadro de diálogo similar al de la figura:



Según los datos ingresados, el programa calcula, según el Ejemplo *7.26*,

$$log_{50}(5512) \pmod{10099}$$

Al ejecutarlo, obtenemos por resultado *12*. El código fuente del programa lo mostramos a continuación.

Código fuente de la parte clásica del Algoritmo de Shor que calcula $log_g(x) \pmod p$

```
Interpretation[{c0 = 4, d0 = 16345, p = 10099, m = 14, g = 50, x = 5512},
 Panel[Grid[{{Style["CÁLCULO DE log_g(x) (mod p) - PARTE CLÁSICA DEL ALGORITMO DE SHOR", Bold]},
    {Style["Ingrese el par (c0,d0) obtenido del circuito cuántico", Bold], SpanFromLeft},
    {"c0=", InputField[Dynamic[c0]]},
    {"d0=", InputField[Dynamic[d0]]},
    {Style["Ingrese el número primo p", Bold], SpanFromLeft},
    {"p=", InputField[Dynamic[p]]},
    {Style["Ingrese el número natural m tal que p < 2^m", Bold], SpanFromLeft},
    {"m=", InputField[Dynamic[m]]},
    {Style["Ingrese la base g del logaritmo", Bold], SpanFromLeft},
    {"g=", InputField[Dynamic[g]]},
    {Style["Ingrese el número x", Bold], SpanFromLeft},
    {"x=", InputField[Dynamic[x]]}

    }]],
If[Abs[IntegerPart[d0 (p - 1)/2^m] - d0 (p - 1)/2^m] ≥ 0.5, Residuo = IntegerPart[d0 (p - 1)/2^m] + 1, Residuo = IntegerPart[d0 (p - 1)/2^m]];
t = Mod[IntegerPart[-c0 (p - 1)/2^m - 1/2], p - 1];
If[Mod[Residuo, GCD[t, p - 1]] == 0, tt = t/GCD[t, p - 1]; RResiduo = Residuo/GCD[t, p - 1]; pp = (p - 1)/GCD[t, p - 1];

 Encontrado = 0;
  k++;
 ];
 ttinv = (1 + pp * (k - 1))/tt;
 x1 = Mod[ttinv * RResiduo, pp];

 Encontrado = 0;
 i = 0;
 While[i ≤ GCD[t, p - 1] - 1 && Encontrado == 0,
  g1 = g;
  cc = 1;
  k = x1 + pp * i;
  While[k > 1,
   b = Mod[g1^2, p];
   If[Mod[k, 2] ≠ 0, cc = g1 * cc];
   g1 = b;
   k = IntegerPart[k / 2];
  ];
  If[Mod[g1 * cc, p] == x, Encontrado = 1];
  i++;
 ];
 Print["El valor del logaritmo discreto es:"];
 Print["Log", g, "(", x, ") (mod ", p, ")=", x1 + pp * (i - 1)]
 ,
 Print["Lo siento, intente con otro par (c0,d0)"]

 ]
]
```

CAPÍTULO 8

Conclusiones

Una de las principales dificultades con la que nos hemos encontrado al desarrollar esta tesis, es que los papers (con algunas excepciones) que presentan este tipo de temas, no detallan ni demuestran los procedimientos matemáticos que se precisan para justificar los algoritmos empleados. Esto dificulta enormemente el seguimiento para el lector principiante. Por esta razón, en la tesis se ha hecho hincapié en este aspecto. En este sentido, brindamos un enfoque matemático, con demostraciones detalladas, de las propiedades cuánticas que se aplican para justificar, paso a paso, el procedimiento utilizado para el cálculo de un logaritmo discreto. El rigor matemático empleado contribuirá al entendimiento y servirá de complemento para otros temas de Computación Cuántica.

En cuanto al Algoritmo Cuántico propuesto por Shor y desarrollado en este trabajo, podemos concluir que su eficiencia supera a cualquier otro algoritmo clásico. La Parte Cuántica del Algoritmo requiere, para valores grandes del número primo *p*, a lo sumo *1024* ejecuciones del Circuito Cuántico para obtener "*un buen par*". La Parte Clásica tampoco precisa demasiado tiempo de ejecución, ya que consiste en resolver una ecuación lineal de congruencia. El cálculo de un logaritmo discreto que en un ordenador clásico podría tardar años en resolverlo, con el Algoritmo de Shor demandaría sólo unos minutos

A su vez, durante el proceso de investigación para esta tesis surgieron varias preguntas, como por ejemplo, si es posible físicamente desarrollar un computador cuántico capaz de ejecutar el Algoritmo de Shor, o si este desarrollo destruye toda la criptografía actual. Las respuestas no son alentadoras. En la actualidad, a pesar de los avances, el desarrollo de una computadora cuántica que supere a los superordenadores sigue siendo una promesa y ya existen equipos de trabajos dedicados específicamente al desarrollo de criptografía post – cuántica, como el proyecto PQCrypto de la UE.

¿Entonces, por qué dedicar la tesis a un tema cuya probabilidad de aplicación es una incógnita o no genere el cambio esperado? Porque lo importante de llegar a una meta, no es el arribo, sino lo que se aprende en el camino. Si bien la Computación Cuántica se encuentra en sus inicios, esta nueva rama de la Ciencia brinda un terreno sumamente fértil para investigar. Creemos que nuestro humilde aporte servirá de incentivo a otros estudiantes para incursionar en esta materia.

Referencias

[1] Peter W. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* . SIAM J.Sci.Statist.Comput, 1997.

[2] *https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17*

[3] Oviedo, Pablo Andrés. "*Fundamentos Matemáticos de Computación Cuántica en el Algoritmo de Shor, para la factorización prima de números enteros".* Tesis de Licenciatura en Matemática. Directora: Abdel Masih, Samira. Universidad Abierta Interamericana. Buenos Aires, 2017.

[4] Prieto, Cecilia Andrea."*Modelo compacto del algoritmo Diffie-Hellman utilizando cuaterniones".* Tesis de Licenciatura en Matemática. Directora: Abdel Masih, Samira. Universidad Abierta Interamericana. Buenos Aires, 2019.

[5] Martin Ekera. "*Modifying Shor's algorithm to compute short discrete logarithms*" *IACR Cryptol. ePrint Arch, 2016*.

[6] Nielsen, Michael & Chuang, Isaac.*"Quantum Computation and Quantum Information". Ed. Cambridge University Press, 2016.*

[7] McMahon, David Isaac.*"Quantum Computation Explained". John Wiley & Sons, 2008.*

[8] http://www.fisicafundamental.net/misterios/computacion.html#introduccion.

[9] D. Deutch and R. Jozsa. "*Rapid solution of problems by quantum computation". Proc. Roy Soc. London Ser.* pp 553-558, 1992

[10] Chris Bernhardt."*Quantum Computing for everyone". Ed. MIT Press* pp 157-167, *2019.*

[11] Granado Peralta, S. "*Matemática Discreta*". *Ed. CEIT. Buenos Aires, 2002*.

[12] Valente, Yésica. "*Descripción Matemática del Algoritmo de Shor, para la factorización prima de números enteros en una computadora cuántica".*
Tesis de Licenciatura en Matemática. Directora: Abdel Masih, Samira. Universidad Abierta Interamericana. Buenos Aires, 2020.

[13] Stanley Grossman. "*Álgebra Lineal con aplicaciones*". *Ed. Mc Graw Hill. México.1997*

[14] http://pimedios.es/2015/04/23/el-qubit-y-el-algoritmo-de-shor/

[15] Laverde Alfonso, Sebastián. *"Estudio comparativo y Evaluación de utilidad de protocolos de transmisión de datos usando Criptografía Cuántica, pág. 16-18"*. Trabajo de grado para optar al título de Ingeniero Electrónico. Director: González Jiménez, Edgar. Pontificia Universidad javeriana. Bogotá, 2016.

[16] J.W. Sanders and P. Zuliani. "*Quantum Programming*". *Ed. Oxford University Computing Laboratory. England. 2018.*

[17] Taher Elgamal." A public key cryptosystem and a signature scheme based on discrete logarithms". Lecture Notes in Comput. Sci., 196, Springer, Berlín, pág. 10-18, 1985.

[18] Fernández Santamaría, Jennifer. "El logaritmo discreto y sus aplicaciones en Criptografía". Trabajo de grado para optar al título de Licenciatura en Matemáticas. Director: Sadornil Renedo, Daniel. Universidad de Cantabria. Santander, España. 2013.

[19] La Criptografía Científica, entrevista al Dr. Hugo Daniel Scolnik https://www.youtube.com/watch?v=Oxt60h8YPYA

[20] https://santanderglobaltech.com

[21] https://quantum-computing.ibm.com/