Algoritmo de factorización para un computador cuántico

Hernando Efraín Caicedo-Ortiz
Escuela Superior de Física y Matemáticas, Instituto Politécnico Nacional,
Unidad Profesional "Adolfo López Mateos", Zacatenco, Delegación Gustavo A. Madero,
Edificio 9, CP 07738, México D. F.

E-mail: hecaicedo@esfm.ipn.mx, hecaicedo@gmail.com

(Recibido el 20 de Enero de 2010; aceptado el 6 de Mayo de 2010)

Resumen

En este artículo se realiza una revisión de uno de los algoritmos más importantes dentro de la teoría cuántica de la información, como es el algoritmo de Factorización de Shor. Se hace una pequeña introducción a la teoría cuántica de la información, se presentan las características más importantes del algoritmo de factorización, su implementación experimental, y por último se describen algunas de sus potenciales aplicaciones comerciales.

Palabras clave: Algoritmos Cuánticos, Computación e Información Cuántica, Algoritmo de Factorización de Shor.

Abstract

In this paper we review one of the most important algorithms in the quantum theory of information, such as Shor's factoring algorithm. A small introduction to quantum information theory, describing the features of the factoring algorithm, their experimental implementation and finally describes some of its potential commercial applications.

Keywords: Quantum Algorithm, Quantum Computing and Quantum Information, Shor's Factoring Algorithm.

PACS: 03.67.-a, 03.67.Ac, 03.67.Lx **ISSN 1870-9095**

I. INTRODUCCIÓN

Desde los trabajos fundacionales de Feynman [1] y Deutsch [2] en la década de los ochenta, la teoría de la computación cuántica se ha convertido en una de las áreas de investigación de mayor impacto en los últimos treinta años. Con la aparición de algoritmos que hacen uso de los efectos mecánico cuánticos, las velocidades de procesamiento de información han crecido exponencialmente, mientras que los tiempos asociados a estos procesos tienden a ser cada vez menores y de tipo polinomial.

Dentro de la gama de algoritmos existentes en esta nueva teoría, sobresale el algoritmo de Shor [3], el cual permite descomponer en factores primos un número N cualesquiera, por lo cual su potencial implementación en un dispositivo de computo cuántico traería como consecuencia que sistemas criptográficos basados en procesos de factorización como el sistema de clave pública RSA [4] fueran fácilmente quebrantados. Mientras los procesos asociados a los algoritmos de clave publica se realizan en tiempos superpolinómicos de la forma $\exp[c(In\,N)^{1/3}(In)^{2/3}]$, para el algoritmo cuántico de Shor, el tiempo necesario para realizar esta misma tarea es polinómico y de la forma $O(\mathrm{Log}(\mathrm{N})^3)$.

La gran fortaleza de cálculo que posee el algoritmo de Shor con respecto a los algoritmos implementados en ordenadores convencionales radica en el hecho de hacer uso de efectos cuánticos tales como la interferencia, potencializandolo y permitiendo un procesamiento de la información en forma paralela, lo cual se traduce computacionalmente en una disminución en el tiempo de procesamiento.

II. COMPUTACIÓN CUÁNTICA

La computación cuántica y la teoría cuántica de la información [5] no son otra cosa que una modificación de las ideas de computabilidad y en este contexto hacen uso de efectos mecánico-cuánticos [1] que rigen el mundo subatómico, como la superposición y el entrelazamiento de estados. Este nuevo esquema, en contraste con la computación clásica, presenta un escenario de trabajo que no solo se restringe a dos únicos estados de operación (0,1), al contrario, se pueden obtener multitud de estados intermedios como resultado de la superposición de estas dos posibilidades. Esto trae consigo que al llevar a cabo cualquier operación, el sistema permite evaluar todas las posibilidades en un solo paso, es decir, realiza una computación en paralelo de forma natural; mientras que clásicamente, este proceso de evaluación se realiza de

forma independiente una de otra y en pasos diferentes, es decir es de tipo secuencial o serial. Esta característica de paralelismo cuántico se traduce computacionalmente en una reducción del tiempo y aumento en la velocidad de procesamiento de la información.

III EL QUBIT

De forma similar a los dispositivos de cómputo convencionales, en los cuales la mínima unidad de información es el bit, en la teoría de la computación cuántica este elemento tiene su contraparte y se denomina bit cuántico ó qubit [5]. Aunque esta entidad se describe como un objeto matemático con ciertas propiedades específicas, tiene una realidad física tangible, la cual se representa a través de un sistema cuántico de dos estados, pero en el cual todo su tratamiento es enteramente abstracto, dando libertad de generar una teoría general de la computación e información que no depende del sistema físico que se emplee para su implementación. Al considerar sistemas de esta clase como mínimas unidades de información, es necesario para su correcta descripción, implementar el formalismo matemático de la mecánica cuántica. Aunque existen varios esquemas que describen los estados de un sistema cuántico, el más conveniente y conciso es la notación de Dirac [6], la cual se ha convertido en un estándar en la física moderna, donde cualquier estado es representado por un vector ket, denotado por $|\psi\rangle$ y las operaciones sobre los estado se realizan a través de operadores que son transformaciones lineales que actúan sobre el ket.

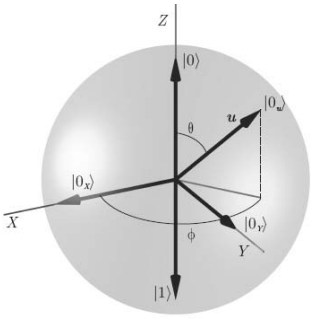

FIGURA 1. Representación tridimensional de un qubit en función de la esfera de Bloch**.**

Considerando esta representación, los dos estados posibles para un qubit son $|0\rangle$ y $|1\rangle$ ó matricialmente $\begin{pmatrix}1\\0\end{pmatrix}$ y $\begin{pmatrix}0\\1\end{pmatrix}$, que corresponden en analogía al 0 y 1 de un bit clásico, donde tales vectores pertenecen a un espacio de Hilbert L^2 [5].

Como se mencionó anteriormente, la potencialidad de este esquema radica en que el qubit puede tomar otro valor diferente a los dos antes mencionados, siendo esto posible debido a la combinación lineal de estados, por lo cual un qubit en su forma más general se representa como

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

donde a_0 y a_1 son números complejos que satisfacen la relación de normalización $|a_0|^2 + |a_1|^2 = 1$.

La habilidad de un sistema cuántico de existir simultáneamente en una mezcla de todos los estados permitidos es conocida como "Principio de Superposición" [1] y es una característica completamente cuántica. Esto significa que mientras en un sistema clásico el bit tiene una información concreta a la cual se puede acceder sin perturbarla, el qubit siempre proporciona un resultado probabilístico.

De la misma forma que en la electrónica convencional, en computación cuántica existen circuitos que realizan y llevan a cabo los procesos de cómputo. En este esquema, una compuerta lógico cuántica es una función que realiza un operador unitario en un conjunto de qubits seleccionados en un cierto periodo de tiempo. En la teoría clásica las compuertas lógicas constituyen un conjunto claramente finito, pero en el modelo cuántico esta característica se extiende y debido a que el espacio de estados de un qubit es continuo, el número de posibles transformaciones unitarias también lo es; en consecuencia, existen infinitas compuertas cuánticas. Sin embargo, es posible demostrar que cualquier transformación unitaria en un conjunto de *N* qubits puede realizarse mediante la aplicación sucesiva de tan sólo dos compuertas cuánticas universales [7].

IV. EL PROBLEMA DE FACTORIZACIÓN

El problema de factorización, al igual que los grandes problemas de las matemáticas como por ejemplo el teorema de Fermat, se enuncian de una manera muy sencilla: dado un número impar no primo *N*, es posible encontrar los dos factores primos de *N*, N_1 y N_2 tal que

$$N = N_1 * N_2. \quad (2)$$

Para *N* muy grande, no se conoce en la actualidad un algoritmo que resuelva eficientemente este problema; un intento reciente de factorizar un número de 200 dígitos (RSA-200) tardó 18 meses y consumió más de medio siglo de tiempo de cálculo. Esta dificultad para solventar el problema, es en la actualidad el núcleo de ciertos algoritmos criptográficos, como el RSA [4], ampliamente usado en la codificación de información transferida por internet.

V. IMPLEMENTACIÓN DEL ALGORITMO DE SHOR

Este algoritmo cimienta su potencia en determinar el periodo de una función adecuada. Aunque su estudio presenta un grado de complejidad relativamente alto, es muy interesante analizar el nuevo enfoque que la mecánica cuántica ofrece para solucionar el problema de factorización. La descripción paso a paso del mecanismo de operación del algoritmo desarrollado por Shor es el siguiente

[1] Se escoge inicialmente un número q (con pequeños números primos), tal que $2\,n^2 \le q \le 3n^2$.

[2] Se toma al azar un número entero x, tal que sea co-primo a n.

[3] Los siguientes pasos desde (a) hasta (g) se repiten Log(q) veces, empleando el mismo número x en cada paso.

(a) Se crea un registro de memoria cuántica, dividiendo los qubits en dos conjuntos llamados registro 1 y registro. Si los qubits en el registro 1 se encuentran en el estado ***reg₁*** y aquellos que están en el registro 2 se encuentran en ***reg₂***, es posible representar el estado completo del sistema en notación Dirac como $|reg_1, reg_2\rangle$.

(b) Leer reg_1 con todos los enteros en el rango de *0* a *q-1* y leer reg_2 con todos los ceros. El estado del registro completo esta dado por

$$|\psi\rangle = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,0\rangle. \qquad (2)$$

(c) Aprovechando el paralelismo cuántico, se aplica la transformación $x^a \bmod n$ a cada número en registro 1 y poner el resultado en registro 2. El estado del registro completo se convierte en

$$|\psi\rangle = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a, x^2 \bmod n\rangle. \qquad (2)$$

(d) Al medir el estado del reg_2, se obtiene algún resultado k. Esto es el efecto de proyección por fuera del estado reg_1 para ser una superposición de justamente estos valores de a tal que $x^a \bmod n = k$. El estado del registro completo es

$$|\psi\rangle = \frac{1}{\sqrt{\|A\|}}\sum_{a\in A}|a, k\rangle, \qquad (3)$$

donde $A = \{a / x^a \bmod n = k\}$ y $\|A\|$ es el número de elementos en este lugar.

(e) A continuación se computa la transformada discreta de Fourier del estado proyectado en el reg_1. Esta transformada mapea cada estado en una superposición dada por

$$\text{a } |a\rangle \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1} e^{2\pi a c/q}|c\rangle. \qquad (4)$$

Así el efecto del costo neto de la transformada de Fourier es mapear el estado proyectado en reg_1 en la superposición dada por

$$|\psi\rangle = \frac{1}{\sqrt{\|A\|}}\sum_{a\in A}\frac{1}{\sqrt{q}}\sum_{c=0}^{q-1} e^{2\pi a c/q}|c, k\rangle. \qquad (5)$$

(f) Medir el estado de reg_1. Estos son ejemplos prácticos del la transformada de Fourier. Esto devuelve algún numero $c´$ que es algún múltiplo de λ siendo múltiplo de q/r donde r es el periodo; es decir, $c´/q = \lambda /r$ para algún entero positivo λ

(g) Para determinar el periodo r es necesario estimar λ. Esto es logrado por el cómputo de expansión de una fracción continúa $c´/q$ de tal forma que el denominador sea menor de n.

[4] Repitiendo los pasos de (a) al (g) se crea un juego de muestras de la transformada de Fourier en el reg_1. Esto da muestras de múltiplos de $1/r$ como λ_1/r, λ_2/r, λ_3/r... para varios enteros λ_i. Después de esto, el algoritmo se repite hasta obtener suficientes muestras de reg_1 que al computarlas por una técnica de continua fragmentación se obtienen los λ_i que permiten describir a r.

[5] Una vez conocido r, los factores de n pueden ser obtenido del $\text{mcd}(x^{r/2} - 1, n)$ y el $\text{mcd}(xr/2 + 1, n)$.

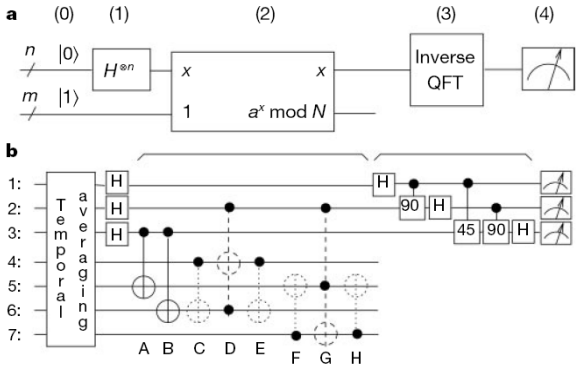

FIGURA. 2. Estructura del Circuito del Algoritmo de Shor.

En la figura 2 se observa una representación circuital en función de compuertas cuánticas y transformada cuántica de Fourier de la implementación del algoritmo de Shor.
En la parte a) se observa el contorno de el circuito cuántico. Los hilos representan los qubits y las cajas representan operaciones. El tiempo va de la izquierda a la

derecha (0) inicializa un primer registro de $n = 2[\log_2 n]$ qubits a $|0\rangle \otimes .... \otimes |0\rangle$ (para Shor $|0\rangle$) y el segundo registro de $m = \lceil \log_2 N \rceil$ qubits a $|0\rangle \otimes .... \otimes |0\rangle \otimes |1\rangle$

(1) Aplicando la transformada a los primeros n qubits hasta llegar a los primeros registros $\sum_{x=0}^{2^n 1} |x\rangle / \sqrt{2}^n$.

(2) Multiplicar el segundo registro por $f(x) = a^x \bmod N$ (para algún valor aleatorio $a \langle N$ el cual no tiene en común factores con N) obteniendo $|\Psi_2\rangle = \sum_{x=0}^{2^n 1} |x\rangle / 1 x a^x \bmod N \rangle / \sqrt{2^n}$ como el primer registro. Esta en una superposición de 2^n términos $|x\rangle$, el modulo exponencial esta computado para 2^n valores de *x* en paralelo.

(3) Ejecutar la inversa QFT del primer registro[19] dado por

$$|\psi_3\rangle = \sum_{y=0}^{2^n 1} \sum_{x=0}^{2^n 1} e^{2\pi |xy| 2^n} |y\rangle |a^x \bmod N \rangle / 2^n.$$

(4) En gran parte los qubits está en el primer registro sobre un computador cuántico ideal. La dimensión del resultado es $c2^n/r$ para algún c con gran probabilidad, y *r* pronto puede deducir de $c2^n/r$ en un computador clásico continua por los factores al cuadrado. En la parte b) de la figura 1 se detalla el circuito Cuántico para la situación $N = 15$ y $a = 7$. El control de los qubits es representado por $\otimes$ y describe una operación *NOT*, 90 y 45 representan Z rotaciones. Las compuertas vistas en las líneas utilizadas son reemplazadas por compuertas simples.

VI. IMPLEMENTACIÓN EXPERIMENTAL

En el año de 2001, el grupo de Computación Cuántica de IBM liderado por Isaac L. Chuang en conjunto con el Laboratorio de Estado Solidó y Fotónica de la Universidad de Stanford logró demostrar experimentalmente la propuesta de Shor [7].

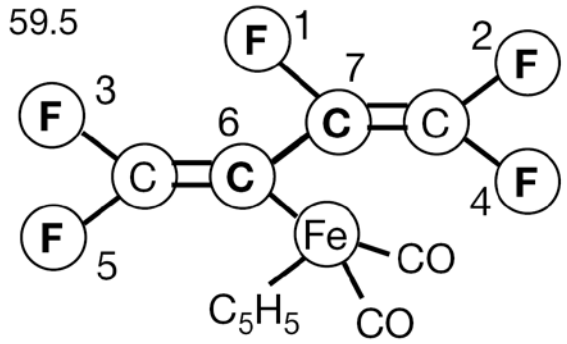

FIGURA 3. Estructura de la molécula de Fluor. Complejo penafluoro-butadienol ciclo-penta-dienil-dicarbonil-hierro.

En esta implementación, el numero a factorizar fue $N = 15$ (donde sus factores primos son 3 y 5). Para tal fin, se utilizo una molécula con 7 espines nucleares 1/2, los cuales representan en el contexto de la computación cuántica al qubit. La gran ventaja de este esquema radica en el hecho que puede ser manipulado a temperatura ambiente en el estado líquido a través de técnicas de resonancia magnética Nuclear (RMN). La estructura molecular escogida como sistema físico para la implementación hardware fue una molécula de cinco núcleos de ^{19}F y dos de ^{13}C especialmente diseñada de forma que los espines de los núcleos puedan interactuar entre ellos como unos qubits (Figura. 3). La molécula está sometida a un campo magnético estático, y los qubits se manipulan con pulsos de frecuencia de radio y se leen mediante técnicas de resonancia magnética nuclear (NMR) a temperatura ambiente.

Con este dispositivo cuántico, es posible determinar la solución al problema de calcular en un único paso el período de una función particular; lo cual claramente comprueba la validez del algoritmo de Shor.

En un reciente articulo, Alberto Politi, Jonathan C. F. Matthews y Jeremy L. O'Brien[10] de la Universidad de Bristol presentan una nueva comprobación experimental del algoritmo de Shor implementado en un chip basado en tecnología fotónica (Figura. 4), donde el algoritmo debe ser compilado, desarrollando todos su bucles de forma explícita, lo que para guarismos con un mayor número de qubits requiere un coste computacional muy alto, sin embargo, las tecnologías utilizadas para esta implementación parecen ofrecer una nueva vía para la escalabilidad de los ordenadores cuánticos.

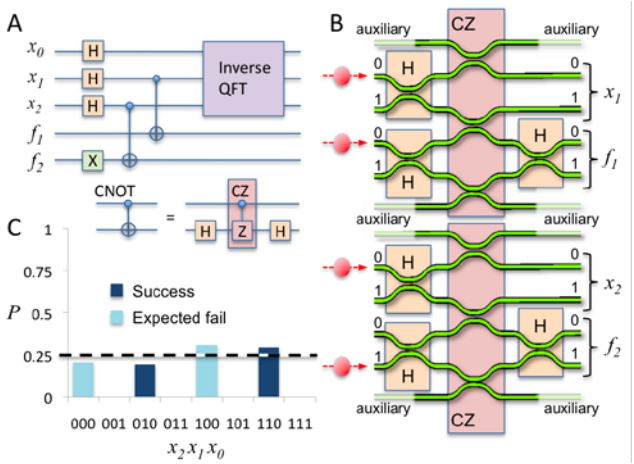

FIGURA 4. Implementación óptica integrada del algoritmo de factorización de Shor. (A) El circuito cuántico. (B) Esquema del chip sobre el cual se lleva a cabo el procesamiento cuántico del algoritmo. Los x_n qubits transportan el resultado del algoritmo; f_n son los qubits adicionales requeridos para que le proceso de computo se lleve a cabo. (C) La respuesta del algoritmo.

VII. APLICACIONES COMERCIALES

La más conocida aplicación de un dispositivo de cómputo cuántico usando el algoritmo de Shor es la capacidad de romper cualquier sistema criptográfico basada en RSA [4]. Esta aparente ventaja ha motivado a que especialmente en EE.UU y Europa el estudio de este algoritmo y la construcción de un ordenador cuántico sean apoyados fuertemente con fondos gubernamentales, catalogando estas investigaciones como clasificadas. Es muy claro que de ninguna manera habrá a mediano plazo un gran mercado para este tipo de dispositivos que descompone en factores: ya que la misma existencia de tal máquina conducirá a la total desaparición del esquema RSA, pero permitirá el surgimiento de sistemas de encriptación con tecnologías substitutas como la criptografía cuántica [9]. Tan solo el futuro lo dirá.

REFERENCIAS

[1] Feynman, R. P., *Simulating Physics With Computer*, Int. J. Theor. Phys. **21**, 467 (1982).

[2] Deutsch, D., *Quantum Theory, the Church-Turing principle and the universal quantum computer.* Proccedings of the Royal Society of London A 400, 97-117 (1985).

[3] Shor, P., *Algorithms for quantum computation: Discrete logarithms and Factoring.* Proceedings 35th Annual Symposium on Foundations of Computer Science, 124-134 (1994).

[4] Jiménez, R., Gordillo, E. y Rubiano, G., *Teoría de números para principiantes*, (Universidad Nacional de Colombia, Facultad de Ciencias, 2004).

[5] Nielsen, M. A. and Chuang, I., *Quantum Computation and Quantum Information*, (Cambridge University Press, United Kingdom, 2001).

[6] Dirac, P., *Principios de Mecánica Cuántica*, (Arial, Madrid, 1967).

[7] Galindo, A. y Martín-Delgado, M. A., *Information and Computation: Classical and Quantum Aspects*, Rev. Mod. Phys. 74, 347-423 (2002).

[8] Vandersypen, Lieven M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H. and Chuang, I. L. *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*, Nature 414, 883–887 (2001).

[9] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., *Quantum Cryptography*, Reviews of Modern Physics, 74, 145-195 (2002).

[10] Politi., A., Matthews, J C. F., and O'Brien, J L., *Shor's Quantum Factoring Algorithm on a Photonic Chip*, Science 325, 1221 (2009).