ISSN 0717-9103
ISSN Online 0718-8307

COMPUTABILIDAD Y COMPUTACIÓN CUÁNTICA: REVISIÓN DE MODELOS ALTERNATIVOS DE COMPUTACIÓN

COMPUTABILITY AND QUANTUM COMPUTING: A SURVEY OF ALTERNATIVE FORMAL COMPUTING MODELS

Guillermo Morales-Luna[1]
[1]Departamento de Computación Centro de Investigación y de Estudios Avanzados del IPN(CINVESTAV) México, D. F., México.

RESUMEN

Este es el primer ensayo, de una serie de dos, en los que se quiere presentar visiones panorámicas de la noción de computabilidad de dos nuevos paradigmas de computación. A saber, la computación cuántica y la computación basada en ADN o molecular, así como de los circuitos integrados tridimensionales que constituyen una alternativa para continuar con la miniaturización de procesadores hasta más allá del orden del nanómetro. Aquí se parte de la misma noción de computación, de sus limitaciones lógicas y se delinea el problema de decidir si acaso el determinismo y el no-determinismo coinciden en dispositivos de complejidades polinomiales en el tiempo. En cuanto a la computación cuántica, se presenta a sus elementos matemáticos básicos y a las ventajas que implican en comunicaciones y criptografía. Finalmente se menciona a algunas de las alternativas actuales para implementarlas. Esta presentación es una reseña del estado actual del área, y tan sólo es novedosa en cuanto a sus ejemplos; está escrita originalmente en lengua castellana, y está dirigida a un público extenso, conformado tanto por profesionistas como estudiantes de nivel universitario.

Palabras claves: Complejidad algorítmica, información, computación y criptografía cuánticas.

ABSTRACT

This is the first essay, in a series of two, devoted to review the new paradigms of Computing, namely quantum computing and molecular computing, as well as 3D integrated circuits aiming to miniaturization processes beyond nanometers. An analysis of the computability basics and its limits is realized and the essential P=NP problem is sketched. Quantum computing is introduced, and its implications in hard problems and in cryptography. Finally, some current implementation strategies are outlined. This is just a survey article, its novelty is the presentation suited to a wide audience.

Keywords: Algorithmic complexity, quantum information, computing and cryptography.

Autor para correspondencia: gmorales@cs.cinvestav.mx
Recibido: 22.12.2011 Aceptado: 12.03.2012

ESTADO DEL ARTE

Computabilidad

La noción de computación es propia del siglo XX. En la década de los 30 surgió naturalmente la pregunta de si acaso se podría construir máquinas que pudieran pensar, y en 1950 Alan Turing (Turing, 1950) planteó formalmente esta pregunta, desarrollando lo que se conocería posteriormente como la *prueba de Turing*: Dos partes, una humana y la otra, que puede ser un humano o una máquina, *dialogan* de manera libre, y la parte humana trata de determinar si su contraparte es o no humana. Una máquina *supera* la prueba si el humano no puede decidir que ésa es una máquina. En ese entonces, Turing asevera que para finales del siglo XX habrá computadoras que prácticamente habrían de superar la prueba. Se es testigo de que esta predicción se cumplió aproximadamente. Desde la década de los 90 se interactúa cotidianamente con máquinas en lenguaje natural, y muchas veces no se repara en que el interlocutor sea un autómata. Acaso se puede cuestionar todavía si la predicción de Turing se cumplió, pues, por lo general, los interlocutores automáticos son recognoscibles. Un problema de suma actualidad es una variante de la prueba de Turing: un autómata ha de reconocer que su interlocutor sea un humano y no un robot (CMU, 2000) -para fines de registro de cuentas de correo electrónico, por ejemplo.

Desde el final de la década de los 30 del siglo XX, las computadoras surgieron para realizar tareas de ordenamiento y de cálculo, las cuales evidentemente son de tipo mecánico. Sin embargo, las computadoras pueden mostrar algún comportamiento de tipo creativo. Por ejemplo, jugando ajedrez. En la actualidad son capaces de proporcionar servicios más cercanos a la inteligencia natural; por ejemplo, de traducción muy elemental. Sin embargo, aunque hagan traducciones entendibles, éstas serán al menos irrisorias (Humanitas, 2006), si no es que, de plano, ridículas. Pero, es evidente que las tareas realizadas por computadoras pueden dejar de parecer puramente mecánicas y acercarse más al terreno de la creatividad. Pero acaso esto es sólo una apariencia. Douglas Hofstadter enuncia un célebre teorema: *Cualquier función intelectual que realice una máquina, deja de ser considerada esencial para la inteligencia humana* (Hofstadter, 1979). La programación de computadoras se ha hecho siguiendo el paradigma de Von Neumann. Pero también puede hacerse a partir de ejemplos, que es el método de *programar humanos*. Sin embargo, para una colección finita de ejemplos y un programa que los genere, hay una infinidad de programas consistentes, en esos ejemplos, con el programa dado. Esta indeterminación hace poco plausible que se puedan generar programas automáticamente, pues para determinarlos de manera única hay que imponer presuposiciones arbitrarias, lo cual, a su vez, marca limitaciones a la inteligencia artificial. Ya Roger Penrose lo asevera de manera contundente: *Ningún programa, que se sepa que es correcto, puede simular toda la habilidad matemática de un humano*. Desde los inicios de la computación ha surgido la pregunta: ¿Pueden pensar las computadoras? El desarrollo tecnológico da evidencia de una respuesta positiva. Las limitaciones matemáticas -el teorema de Gödel, la no-computabilidad- y los cuestionamientos de tipo filosófico tienden a reforzar una posible respuesta negativa. En todo caso, la discusión de nociones como *mente* y *conciencia* atañe a áreas como sicología, filosofía, física y matemáticas (Harnad, 2000; Penrose, 1996), y lejos están de haber sido dilucidadas.

Las *máquinas de Turing* (Hodges, 2000) son el prototipo de la computación efectiva, y hay un acuerdo social llamado *Tesis de Church* respecto a ello. Cada máquina de Turing está definida sobre un alfabeto, actúa sobre una cinta lineal -infinita en ambos sentidos-, en blanco salvo para un número finito de localidades, y puede asumir un conjunto finito de estados. Toda vez que una máquina lee un símbolo en la cinta, dependiendo de su estado actual, substituye el símbolo leído por alguno otro, asume un nuevo estado y pasa a leer una de las dos casillas vecinas

ISSN 0717-9103
ISSN Online 0718-8307

en la cinta. Pero la misma versatilidad de las máquinas de Turing conlleva sus limitaciones. En efecto, existen funciones no-computables. Por ejemplo, consideremos primeramente los llamados *castores atareados* (Marxen, 2006): Sea B_{2n} la colección de máquinas de Turing deterministas sobre el alfabeto (0+1), donde 0 hace las veces de símbolo blanco, con *n*+1 estados de los cuales el último es de paro. Hay exactamente $\left(4(n+1)\right)^{2n}$ máquinas en B_{2n} . Para cada máquina *M*, sean $\sigma(M)$ y $\tau(M)$ el número de 1's quequedan en la cinta y el número de movimientosrealizados, respectivamente, al pararse *M* habiendo comenzado su cómputo con la cinta en blanco. Se define a las funciones Σ y *T* como aquellas que a cada entero *n* le asocian los máximos valores que pueden asumir $\sigma(M)$ y $\tau(M)$, variando *M* en todo B_{2n} . Una máquina de Turing $M \in B_{2n}$ se dice ser un *castor atareado* si $\Sigma(n) = \sigma(M)$ o bien bien $T(n) = \tau(M)$. En otras palabras, para cada *n*, cada castor atareado calcula ya sea la máxima cadena que puede escribir una máquina en la clase B_{2n} o bien ocupa el máximo número de pasos que puede realizar una máquina en esa misma clase. El problema matemático de localizar castores atareados es sumamente difícil y se llevan recuentos de los *records* establecidos (Brady, 2006; Michel, 2006). De hecho, se tiene que ninguna de las funciones Σ y *T* es computable, es decir, no hay una máquina de Turing que las calcule, y esto último se demuestra mediante una variante del famoso *argumento diagonal* de Georg Cantor.

Turing mismo probó que el *Problema de la Parada* no es computable. Todo programa se escribe con reglas de buena formación, y la connotación de un programa queda determinado de manera única. Esta es la razón por la que es posible construir, puesto en su mayor generalidad, una *máquina de Turing universal*, o bien, en lo particular, compiladores de lenguajes de programación. En estos esquemas, los programas y los datos pueden codificarse mediante un mismo alfabeto: los programas y los datos son codificados por cadenas bien formadas respecto a reglas gramaticales específicas (Backus, 1978). Pero, al plantearse el Problema de la Parada, a saber, construir un programa tal que reconozca a las parejas programas-datos tales que los programas se paran, o convergen, al actuar en los datos resulta un problema irresoluble. Si existiese un programa que resuelva el Problema de la Parada, entonces se le podría modificar para obtener uno que reconozca a los programas que converjan con su propio código, y una nueva modificación produciría un programa que converge únicamente en los programas que no convergen con su código. Este último codifica la *paradoja del mentiroso*: ¡el programa ha de converger sobre su código cuando y sólo cuando no converge sobre su código! Por esto, es irresoluble el *problema de la parada* y lo es, también, cualquier otro problema que se reduzca a él. Por ejemplo, el llamado *de la correspondencia de Post*.

En la teoría de la complejidad es muy importante la noción de *indeterminismo*. En cualquier paradigma de programación se tiene un programa no-determinista cuando, ante una entrada particular, estando el dispositivo que ejecuta programas en un estado actual, se tiene la posibilidad de pasar a una, varias o a ningunas nuevas configuraciones. Por ejemplo, Teseo en su búsqueda por Ariadna en el laberinto de Creta; en cada recinto, si no ha encontrado a Ariadna ni al Minotauro, ha de continuar avanzando por cualquier nueva galería. ¿Por cuál en particular? En principio, la nueva galería queda indeterminada, aunque luego diversas maneras de precisarla -auxiliándose acaso del hilo de Ariadna- darán nuevos algoritmos, un tanto más determinados, todos derivados del algoritmo no-determinista.

La noción de indeterminismo corresponde naturalmente a la de *comprobación*: dada la instancia de un problema, se elige de alguna forma *indeterminada* una solución potencial en el espacio numerable de las soluciones posibles, y luego se verifica que, en efecto, la solución potencial sea una solución actual. En cambio, el determinismo corresponde a *resolución*: dada la instancia de un problema, se construye paso a paso una solución que efectivamente lo sea.

Todo algoritmo define una correspondencia entre el conjunto de entrada y el conjunto de

salida. Cada instancia de entrada está determinada por una cadena de bits, cuya longitud es precisamente el *tamaño* de la instancia. Ante una instancia de entrada, puede existir una cadena de salida tal que el algoritmo se para cuando la produce, es decir, el algoritmo *converge* o, en la situación contraria, se queda en un cómputo perenne, es decir *diverge*. En cualquier paradigma de programación, (las máquinas de Turing, por ejemplo), cada programa determina una función de *tiempo* y otra de *espacio*. A cada entero *n*, la primera le asocia el máximo número de transiciones primitivas que realiza el programa para arribar a una condición de paro, tomado sobre todas las instancias de entrada de tamaño *n*, y la segunda el máximo número de localidades de memoria examinadas por el programa para arribar a una condición de paro, tomado también sobre todas las instancias de entrada de tamaño *n*. Un problema *está en una clase determinista de funciones*, respecto al tiempo, si existe un programa determinista que lo resuelve, cuya función de tiempo está en esa clase y *está en una clase no-determinista de funciones*. Respecto al tiempo, si existe un programa no-determinista que comprueba soluciones del problema, cuya función de tiempo está en esa clase. Naturalmente se introducen definiciones similares respecto al espacio. Todo cómputo no-determinista posee en cada instante una variedad finita de posibilidades para proseguir, en otras palabras, posee una estructura arbórea, donde existe una cota para el número de ramas que emanan de cada nodo. Por esto, resulta que cuando el no-determinismo se simula exhaustivamente mediante programas o dispositivos deterministas, las funciones de tiempo se incrementan exponencialmente.

La *clase* P consta (Ausiello *et al.;* 1999) de los problemas resolubles en tiempo polinomial con máquinas de Turing deterministas, y la *clase* NP consta de los problemas resolubles en tiempo polinomial con máquinas de Turing no-deterministas, aunque en este segundo caso se abusa de la noción de "resolver", pues de hecho el cómputo de una solución en una máquina no-determinista consiste de dos etapas: en la primera se "adivina" una solución (y éste es el proceso no-determinista) y luego se "comprueba" que en efecto ésa es una solución (lo cual es plenamente determinista). Las clases análogas en cuanto a funciones de espacio se denotan convencionalmente como PSPACE y NPSPACE. Se dice, por ejemplo, que una función *f está en* P si el problema de encontrar, para una instancia *x*, una *y* tal que $f(x) = y$, está en la clase P. Para cualquiera de las clases P, NP, PSPACE y NPSPACE, se dice que un problema P_1 *se reduce* a un problema P_2 si existe una función *f* en P, del conjunto de instancias de P_1 en el conjunto de instancias de P_2 tal que para cualquier *x*, P_1 posee una solución para *x* cuando y sólo cuando P_2 posea una solución para $f(x)$. Un problema es *difícil* en una clase si cualquier otro problema en la clase se reduce a él, y es *completo* en esa clase si es difícil y además está en esa clase. De las definiciones se sigue directamente que P es una subclase de NP y ésta lo es de PSPACE. Mas, hoy en día se desconoce si algunas de ellas coinciden, y la conjetura P=NP se mantiene abierta y es uno de los problemas del Milenio del Instituto Clay de Matemáticas (CMI, 2006) galardonados con un millón de dólares cada uno. Este es un problema en el centro de las nociones fundamentales de la Computación. Si P=NP. Entonces, muchos problemas intratables a la fecha podrían resolverse eficientemente, y la prueba de este hecho ilustraría de manera impactante el nivel de ignorancia actual. Mas, si se probase que esas clases difieren, entonces se comprobaría formalmente la noción intuitiva de que comprobar es, en efecto, más fácil que resolver, y la localización de buenas soluciones a problemas difíciles continuaría más bien como un asunto de talento y de ensayo-y-error.

En 1971 se demostró el problema de decidir cuándo una forma booleana satisface un problema completo en la clase NP. A raíz de ello, ha crecido muy rápido el catálogo de problemas completos-NP. En general, problemas, por lo general de tipo combinatorio, que conllevan una revisión exhaustiva de posibilidades que crecen exponencialmente, tal como lo hace el número de subconjuntos respecto al número de elementos en un conjunto, vienen a dar problemas completos-NP. Asimismo, se ha clasificado una extensa variedad de clases de problemas en temas muy diversos (Aaronson & Kuperberg, 2006; Selman, 1994).

ISSN 0717-9103
ISSN Online 0718-8307

En 1965, Gordon E. Moore, cofundador de Intel, postuló su célebre *ley*: *Cada dos años se duplica la complejidad de las componentes en los dispositivos de costo mínimo*. Y aunque preveía que esa tendencia se mantendría en los siguientes 10 años, ésta ha sido vigente aún en la actualidad, y se ha visto que inclusive desde finales del S. XIX ya se mostraba esa tendencia. El crecimiento exponencial de la ley hace previsible que a la larga ocurra una "singularidad tecnológica", donde se interrumpa ese crecimiento, sea por limitaciones físicas (las velocidades de procesamiento no podrían exceder la de la luz) o lógicas (la complejidad computacional, referida al tiempo, de cada problema está bien definida y es independiente del dispositivo que lo resuelva). RayKurzweil ha estudiado con detalle la posibilidad real de esa singularidad (Kurzweil, 2006). Si bien el modelo de computación se ha ajustado a la Tesis de Church, en cuanto a implementaciones se han desarrollado variantes de circuitos de tipo molecular o cuántico, y con estos dispositivos altamente plausibles es probable que la Ley de Moore continue siendo vigente acaso un par de décadas más, al menos.

Cómputo cuántico

Existen textos ya clásicos presentando este tema con sumo detalle (Bouwmeester *et al*.; 2000; Nielsen&Chuang, 2000). El Cómputo Cuántico es el resultado de trabajos provenientes de la Física, la Matemática y la Teoría de la Información. Los diversos intentos hacia su implementación han repercutido en avances de la nanotecnología y sus principales aplicaciones están en la Seguridad Informática.

A diferencia de los conceptos básicos de información clásica, tales como el *bit* que puede asumir valores 0 o 1, y los registros que son arreglos de bits concatenados, en el cómputo cuántico, la unidad básica, el *qubit* puede estar en una superposición de valores 0 y 1 y al concatenar a los qubits se forman arreglos, llamados *quregistros*, de crecimiento exponencial. Esto dota al cómputo cuántico de un paralelismo inherente que permite acelerar notoriamente los procesos. Una breve cronología de la computación cuántica, cuya versión en extenso, junto con sus propias referencias a los trabajos originales, aparece en (Nielsen & Chuang, 2000), es la siguiente:

- 1961: Rolf Landauer plantea que la computación es física y analiza la generación de calor.
  1973: Charles Bennet estudia la noción de *reversibilidad* de las computaciones.
- 1981: Richard Feynman plantea que los sistemas físicos, incluidos los de nivel cuántico, pueden ser simulados de manera exacta por computadoras cuánticas.
- 1982: Peter Beniof presenta modelos lógicos de máquinas de Turing cuánticas.
- 1984: Charles Bennet y Gilles Brassard introducen las nociones básicas de criptografía cuántica.
- 1985: David Deutsch reinterpreta la llamada *tesis de Church-Turing*
- 1993: Bennet, Brassard, Crepeau, Josza, Peres, Wooters descubren la noción de *teleportación* .
- 1994: Peter Shor publica su algoritmo cuántico para factorizar enteros.

La unidad básica de información es pues el *qubit*, en contraposición del *bit clásico*. La noción de *superposición*, propia de los qubits, se describe formalmente en el ambiente de *espacios de Hilbert*. Los qubits son vectores unitarios en un espacio de dimensión 2 sobre los complejos, es decir, un qubit es un punto en la esfera unitaria del espacio vectorial C^2. Si $\mathbf{x} = x_0\mathbf{e}_0 + x_1\mathbf{e}_1$ es un qubit, $x_0, x_1 \in C$, con $|x_0|^2 + |x_1|^2 = 1$ y $\mathbf{e}_0, \mathbf{e}_1$ los vectores (1,0) y (0,1) de la base canónica de C^2, se escribe de acuerdo con la notación debida a Dirac, $\mathbf{x} = x_0|0\rangle + x_1|1\rangle$. Los bits clásicos se identifican, respectivamente, con los qubits $|0\rangle = \mathbf{e}_0$ y $|1\rangle = \mathbf{e}_1$. El conjunto de qubits, desde el punto de vista matemático, está en un espacio isomorfo al de cuatro dimensiones sobre los números reales.

Una manera de visualizarlo, considerando sólo valores reales en la primera coordenada, es mediante la llamada *esfera de Bloch*: A cada qubit $\mathbf{x} = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\text{sen}\frac{\theta}{2}|1\rangle$ se le asocia el punto $\text{sen}\theta\cos\varphi\,\mathbf{i} + \text{sen}\theta\,\text{sen}\varphi\,\mathbf{j} + cos\theta\cos\varphi\,\mathbf{k}$, donde los vectores $\mathbf{i},\mathbf{j},\mathbf{k}$ apuntan en las direcciones x,y,z. Así el polo norte corresponde al qubit $|0\rangle$ (el valor 0), el polo sur al qubit $|1\rangle$ (el valor 1) y el ecuador a los qubits de la forma $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right)$ (superposiciones con iguales probabilidades de asumir el valor 0 o el valor 1). El ángulo φ que determina meridianos en la esfera, corresponde a *desfasamientos* de qubits.

Al *tomar una medición*, el qubit **x** asumirá el valor $|0\rangle$ con probabilidad $|x_0|^2$ y el valor $|1\rangle$ con probabilidad $|x_1|^2 = 1 - |x_0|^2$. Así, la probabilidad de que el qubit asuma el valor "cero" es el cuadrado del valor absoluto de la primera coordenada, y la probabilidad de que asuma el valor "uno" es la complementaria. En tanto no se tome la medición, cada qubit es una superposición de los dos básicos $|0\rangle$ y $|1\rangle$.

Así, pues, el hemisferio norte en la esfera de Bloch le da prioridad al valor 0, y el sur al valor 1.Un qubit es un vector unitario, o si se quiere, *normalizado*, en el espacio de Hilbert complejo de dimensión 2, y al ser multiplicado por un número complejo de valor absoluto 1, la distribución de probabilidad que determina no cambia. Es en este sentido que se dice que los *factores de fase* son irrelevantes.

Los *quregistros* se componen de varios qubits. Pero, a diferencia de sus análogos clásicos, no son meras concatenaciones de qubits, sino que se obtienen mediante productos tensoriales de ellos. Un *n*-quregistro "se compone" de *n* qubits y es formalmente un vector en la esfera unitaria del espacio complejo H_n de dimensión 2^n. Para cada $j = 0,\ldots,2^n - 1$, se escribe al *j*-ésimo vector básico en ese espacio como $\mathbf{e}_j = |(j)_2\rangle = |\varepsilon\rangle$ donde $\varepsilon = (j)_2$ es la representación en base 2 de *j*, de longitud *n*. La base canónica del espacio H_n es pues $\left(|\varepsilon\rangle\right)_{\varepsilon\in Q^n}$, donde Q^n consta de todas las cadenas de longitud *n* consistentes de bits clásicos 0,1. Por ejemplo, para *n*=3, el espacio $H_3 = C^8$ es de 8 dimensiones y su base canónica es

$$\{\mathbf{e}_j\}_{j=0}^{7} = \{|000\rangle,|001\rangle,|010\rangle,|011\rangle,|100\rangle,|101\rangle,|110\rangle,|111\rangle\}$$

Las operaciones básicas en el Cómputo Cuántico son matriciales y, así, en un solo paso de cómputo afectan a un número exponencial de componentes. Como deben de transformar quregistros en quregistros, necesariamente han de ser unitarias, es decir, han de aplicar la esfera unitaria en ella misma. Si $U: H_1 \to H_1$ es una transformación lineal unitaria, entonces se dice ser una *compuerta cuántica* o *qucompuerta*. Para dos qucompuertas $U,V: H_1 \to H_1$, su *producto tensorial* es $U\otimes V: H_2 \to H_2$ tal que $(U\otimes V)(\mathbf{x}\otimes\mathbf{y}) = U(\mathbf{x})\otimes V(\mathbf{y})$. Sucesivamente, se define $U^{\otimes 1} = U$ y $U^{\otimes(n+1)} = U\otimes U^{\otimes n}$. La composición de compuertas cuánticas, junto con procesos de toma de mediciones, forma a los algoritmos cuánticos.
Las siguientes son matrices unitarias:

$$\sigma_0 = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\ \sigma_x = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\ \sigma_y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix},\ \sigma_z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

donde $i = \sqrt{-1}$, y se dicen ser las *matrices de Pauli*. La primera es la matriz identidad $\mathbf{1}_2$, la segunda es una *negación*, la cuarta es un *cambio de fase*. La tercera hace las veces de una negación y de un cambio de fase.

Otra compuerta cuántica importante es la *transformación de Hadamard*: $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$, cuyo efecto es que si $\mathbf{x} = x_0|0\rangle + x_1|1\rangle$ entonces

$$H\mathbf{x} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}x_0\\ x_1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}x_0 + x_1\\ x_0 - x_1\end{bmatrix} = \frac{x_0 + x_1}{\sqrt{2}}|0\rangle + \frac{x_0 - x_1}{\sqrt{2}}|1\rangle$$

es decir, el operador de Hadamard "promedia" las coordenadas.

Una función booleana *f*, es decir, que transforma señales de 0's y 1's en otras señales de 0's y 1's, puede ser confundida con la transformación lineal tal que $|\boldsymbol{\varepsilon}\rangle|\boldsymbol{\delta}\rangle \mapsto |\boldsymbol{\varepsilon}\rangle|\boldsymbol{\delta} \oplus f(\boldsymbol{\varepsilon})\rangle$. Esta transformación actúa como una mera permutación de los vectores básicos y es por tanto unitaria. Si $n = m = 1$ entonces

$$U_f\left(H\mathbf{x}\otimes|0\rangle\right) = \frac{x_0 + x_1}{\sqrt{2}}U_f\left(|0\rangle\otimes|0\rangle\right) + \frac{x_0 - x_1}{\sqrt{2}}U_f\left(|1\rangle\otimes|0\rangle\right)$$
$$= \frac{x_0 + x_1}{\sqrt{2}}|0f(0)\rangle + \frac{x_0 - x_1}{\sqrt{2}}|1f(1)\rangle$$

en otras palabras, $U_f\left(H\mathbf{x}\otimes|0\rangle\right)$ está dando "sendos promedios de los valores de *f*". Para *n, m* cualesquiera, la matriz $H^{\otimes n}$ es de orden $\left(2^n \times 2^n\right)$, y se tiene similarmente que $U_f\left(H^{\otimes n}\mathbf{x}\otimes|\mathbf{0}\rangle\right)$ está dando "promedios de los valores de *f* ": cada valor $|\boldsymbol{\delta}\, f(\boldsymbol{\delta})\rangle$ será asumido con una probabilidad dada por el valor .

$$2^{-n}\left[\sum_{\boldsymbol{\varepsilon}\in{}_n} h_{\boldsymbol{\delta}\boldsymbol{\varepsilon}}x_{\boldsymbol{\varepsilon}}\right]^2 .$$

Así vemos que el cómputo cuántico en un número *lineal* de pasos conlleva la información de un número *exponencial* de posibles valores.

Las transformaciones de Pauli forman una base del espacio de matrices $2\text{x}2$, por lo que con ellas se puede constuir cualquier otra, de manera lineal. Las matrices unitarias pueden construirse en términos de las de Pauli y la que veremos a continuación.

En el espacio de los 2-quregistros H_2 , una compuerta muy importante es la llamada *NO-Controlado*, $C:|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |11\rangle, |10\rangle \mapsto |10\rangle, |11\rangle \mapsto |01\rangle$ la cual actúa de la forma siguiente: si el segundo bit es 0 deja el primero intacto, pero si es 1 "niega" al primero. De hecho, cualquier operación unitaria de relevancia en el Cómputo Cuántico puede escribirse como una composición de las transformaciones de Pauli y el NO-Controlado.

La computación cuántica proporciona además disminución de costos, en el sentido de complejidadcomputacional,debido al fenómeno de *entrelazamiento -entanglement*, en inglés-, el cual consiste en que, para ciertos registros formados como parejas de qubits, ellos no se factorizan como productos de los qubits involucrados; vale decir, el sistema de dos qubits no se expresa en términos de los qubits individuales de manera independiente: una vez que se determina mediante una medición el valor de un qubit, el valor del otro queda también determinado. Esto contradice el principio físico de localidad: Cuando dos partículas están en estados entrelazados, un cambio en una será manifestado instantáneamente por la otra. Formalmente, la colección de 2-quregistros es la esfera unitaria en $H_2 = C^4$. Dado un 2-quregistro $\mathbf{x}^{(2)} = x_{00}|00\rangle + x_{01}|01\rangle + x_{10}|10\rangle + x_{11}|11\rangle$ se tendrá que la probabilidad de que el quregistro asuma una de las cuatro posibles palabras de dos bits es $\Pr\left(\mathbf{x}^{(2)} \to |ij\rangle\right) = |x_{ij}|^2$, para cada $i, j \in \{0,1\}$. Sin embargo, si se tomaunamedición en el primer qubit y ésteasume el valor $i \in \{0,1\}$ entonces el 2-quregistrotomará el valor

$$\mathbf{x}^{(2)}\Big|_{\mathbf{x}_0 \to |i\rangle} = \frac{1}{\sqrt{|x_{i0}|^2 + |x_{i1}|^2}}\left(x_{i0}|i0\rangle + x_{i1}|i1\rangle\right)$$

es decir, el segundo qubit se mantiene en una superposición. Similarmente, si se mide al segundo qubit y éste asume el valor $j \in \{0,1\}$ entonces el 2-quregistro tomará el valor

$$\mathbf{x}^{(2)}\Big|_{\mathbf{x}_1 \to |j\rangle} = \frac{1}{\sqrt{|x_{0j}|^2 + |x_{1j}|^2}} \left(x_{0j}|0j\rangle + x_{1j}|1j\rangle \right)$$

es decir, el primer qubit se mantiene en una superposición. Sin embargo, supongamos

$$\begin{bmatrix} x_{00} & x_{01} & x_{10} & x_{11} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}. \quad (1)$$

Entonces, resulta $\mathbf{x}^{(2)}\Big|_{\mathbf{x}_0 \to |i\rangle} = |ii\rangle$ y $\mathbf{x}^{(2)}\Big|_{\mathbf{x}_1 \to |j\rangle} = |jj\rangle$, es decir, una vez que se determina un qubit, el otro queda también determinado, con el mismo valor. Similarmente, supongamos

$$\begin{bmatrix} x_{00} & x_{01} & x_{10} & x_{11} \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}. \quad (2)$$

Entonces, resulta $\mathbf{x}^{(2)}\Big|_{\mathbf{x}_0 \to |i\rangle} = |i\bar{i}\rangle$ y $\mathbf{x}^{(2)}\Big|_{\mathbf{x}_1 \to |j\rangle} = |j\bar{j}\rangle$, es decir, una vez que se determina un qubit, el otro queda también determinado, con el valor opuesto.

En estos casos se tiene que ambos qubits están *entrelazados*: El valor que asuma uno, determinará el que ha de asumir el otro.

Las listas de coeficientes (1) y (2) determinan estados entrelazados y, al cambiar en ellos el signo de la segunda componente no-nula, se obtiene a otros dos vectores entrelazados. Ellos cuatro generan al espacio de 2-quregistros, y forman la llamada *base de Bell*.

El entrelazamiento produce diferencias notorias respecto al cómputo clásico: Supongamos un protocolo que involucra dos partes *Alicia* y *Beto* que se han de comunicar bits clásicos. Ellos reciben sendos bits ε_A y ε_B y han de producir bits *a* y *b* tales que la conjunción (u operación "*and*") de los bits recibidos iguala la disyunción excluyente (u operación "*xor*") de los bits producidos: $\varepsilon_A \wedge \varepsilon_B = a \oplus b$. .

Por un lado, tenemos que $\varepsilon_A \wedge \varepsilon_B$ es 1 sólo en una de sus cuatro posibilidades, en tanto que $a \oplus b$ es 1 en dos de sus cuatro posibilidades. Así, la mejor estrategia de Alicia y Beto es lograr *a*=*b*, con lo cual $a \oplus b = 0$, y la probabilidad de éxito es entonces 3/4. Las partes necesitan pues comunicarseun bit clásicoparateneréxito con probabilidad 3/4. Por otro lado, para la implementación cuántica, consideremos el 2-quregistro $\mathbf{x}_0\mathbf{x}_1 = \mathbf{x}^{(2)} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$, que consta de dos qubits entrelazados: El valor que tome uno en una medición lo ha de tomar el otro. El primer qubit queda en posesión de Alicia y el segundo en el de Beto.Consideremos la matriz *G* correspondiente a una rotación de $\frac{\pi}{8}$ radianes, es decir, de 22.5 grados de la esfera unitaria en el espacio de los 2-quregistros. Alicia y Beto aplicarán sendas compuertas cuánticas en función del bit recibido. Sean

$$M_A = \begin{cases} \mathbf{1}_2 & \text{si } \varepsilon_A = 0 \\ G & \text{si } \varepsilon_A = 1 \end{cases}, \; M_B = \begin{cases} \mathbf{1}_2 & \text{si } \varepsilon_B = 0 \\ G^T & \text{si } \varepsilon_B = 1 \end{cases}.$$

ISSN 0717-9103
ISSN Online 0718-8307

Alicia produce su bit tomando como *a* el resultado de tomar medición a $M_A\mathbf{x}_0$ y Beto produce su bit tomando como *b* el resultado de tomar medición a $M_B\mathbf{x}_1$. Se puede ver que en este protocolo, la probabilidad de que $\varepsilon_A \wedge \varepsilon_B$ no coincida con $a \oplus b$ **es** $\frac{3-\sqrt{2}}{8}$, por tanto, la probabilidad de éxito en el protocolo es la complementaria, $1-\left(\frac{3-\sqrt{2}}{8}\right)=\frac{5+\sqrt{2}}{8}\approx 0.80177\ldots$ Así pues, con entrelazamiento solamente y sin necesidad de transmitir ningún bit, la probabilidad de éxito es mayor que en el enfoque clásico.

Otra aplicación importante del entrelazamiento es la llamada *Supercodificación*: Una parte, *Alicia*, ha de comunicar una pareja de bits clásicos $\varepsilon_0\varepsilon_1$ a otra parte, *Beto*. Supongamos que se prepara el 2- quregistro entrelazado $\mathbf{x}_0\mathbf{x}_1=\mathbf{b}_{00}=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)$ como el primer vector en la base de Bell, y se da el primer qubit $\mathbf{x}_0$ a Alicia y el segundo $\mathbf{x}_1$ a Beto. En función de la pareja $\varepsilon_0\varepsilon_1$, Alicia toma un operador U_A para aplicar sobre su qubit:

$$\begin{aligned}
\varepsilon_0\varepsilon_1 = 00 &\Rightarrow U_A=\sigma_0=\mathbf{1}_2\\
\varepsilon_0\varepsilon_1 = 01 &\Rightarrow U_A=\sigma_x\\
\varepsilon_0\varepsilon_1 = 10 &\Rightarrow U_A=\sigma_z\\
\varepsilon_0\varepsilon_1 = 11 &\Rightarrow U_A=\sigma_z\sigma_x
\end{aligned}$$

Alicia produce $\mathbf{y}_0=U_A\mathbf{x}_0$ y se lo envía a Beto. Observemos aquí que necesariamente se ha de tener que $(U_A\otimes\mathbf{1}_2)\mathbf{b}_{00}$ es uno de los vectores en la base de Bell. Beto entonces calcula $\mathbf{z}=(H\otimes\mathbf{1}_2)C(\mathbf{y}_0\otimes\mathbf{x}_1)$ y al tomar una medición respecto a la base de Bell recuperará $\varepsilon_0\varepsilon_1$ pues *a fortiori* *fortiori* $\mathbf{z}=\mathbf{b}_{\varepsilon_0\varepsilon_1}$.

Así pues, basta con la transmisión de un solo qubit para enviar dos bits clásicos.

En Criptografía, el Cómputo Cuántico ha permitido diversos protocolos para el establecimiento de claves comunes. Una característica de ellos es que es incluso posible detectar la sola presencia de un intruso. De acuerdo al clásico protocolo BB84 (Bennett &Brassard, 1984) se tiene que:

Sea $E^0=\{\mathbf{e}_0^0,\mathbf{e}_1^0\}=\{|0\rangle,|1\rangle\}$ la base canónica de H_1 **y sea** $H(E^0)=E^1=\{\mathbf{e}_0^1,\mathbf{e}_1^1\}=\{H|0\rangle,H|1\rangle\}$ la base de H_1 obtenida al aplicar la transformación de Hadamard a E^0, la cual puede corresponder a un fotón con polarización *vertical-horizontal*, $E^0=\{\uparrow,\rightarrow\}$, **y** E^1, y a un fotón con polarización *oblicua*, *NO-NE*, $E^1=\{\text{?},\text{?}\}$

Dos partes, *Alicia* y *Beto*, han de establecer una clave común. Cuentan con dos canales de transmisión:

- **Canal cuántico:** Transmite de manera unidireccional, digamos de Alicia hacia Beto.
- **Canal clásico:** Transmite de manera bidireccional.

Supongamos que la transmisión a través de los canales está libre de cualquier ruido.

Protocolo sobre el canal cuántico

1. Alicia genera dos sucesiones de bits $\boldsymbol{\delta}=[\delta_i]_{i=1}^N$ **y** $\boldsymbol{\varepsilon}=[\varepsilon_i]_{i=1}^N$. Transmite por el canal cuántico

la sucesión de estados $S = \left[s_i = \mathbf{e}_{\delta_i}^{\varepsilon_i} \right]_{i=1}^{N}$.

2. Beto genera una sucesión de bits $\eta = [\eta_i]_{i=1}^{N}$ y realiza una medición de cada qubit s_i respecto a la base E^{η_i} para obtener así una sucesión de bits $\zeta = [\zeta_i]_{i=1}^{N}$. Toda vez que $\varepsilon_i = \eta_i$, se va a tener que $\delta_i = \zeta_i$, por lo que puede esperarse que en casi *N*/2 entradas van a coincidir las sucesiones δ y ζ.

Protocolo sobre el canal clásico

1. Beto le envía su sucesión ζ a Alicia.
2. Alicia calcula el conjunto $J = \{ i \leq N \mid \zeta_i = \varepsilon_i \}$ que corresponde a cuando Beto seleccionó la base correcta. Alicia le envía, de vuelta, *J* a Beto.
3. Necesariamente las restricciones de δ y de ζ a *J*, $\delta|_J$ y $\zeta|_J$, han de coincidir, para cada $j \in J : \delta_j = \zeta_j$, y por tanto esa sucesión, o una porción de ella, puede ser asumida como la llave en común. La única manera en la que δ y ζ podrían diferir sería mediante la intromisión de una tercera parte, la intrusa Isabel.
4. Para revisar si acaso hubo una intromisión, Alicia y Beto intercambian porciones de sus respectivas sucesiones $\delta|_J$ y $\zeta|_J$. Cada vez que intercambian una porción, la suprimen de sus sucesiones. Si en alguna pareja de porciones intercambiadas aparece una discrepancia, se detecta la intromisión de Isabel. De otra manera, se puede confiar con una muy alta probabilidad que la llave en común ya ha sido establecida.

Estos protocolos ya están siendo distribuidos comercialmente; por ejemplo, existe una compañía, MagiQ Technologies, Inc. con base en Boston que los anuncia en su página de Internet.

La teleportación es un fenómeno propio del Cómputo Cuántico y consiste en la transferencia de las propiedades de un sistema cuántico hacia otro sin que haya un contacto físico entre ellos, tales como la polaridad y el desfasamiento de efotónes, o los estados cuánticos, para ponerlo de la manera más general. La teleportación se realiza mediante el entrelazamiento y la corrección de errores. Por ejemplo, teniendo tres iones de berilio, con diámetros del orden de 10^{-8} m, a dos de ellos, digamos al primero y al tercero, se les prepara en estados entrelazados respecto a la polaridad y se les sitúa en lugares distintos. Si el segundo ión está junto al primero y se entrelaza con el primero respecto a desfasamiento, entonces al hacer una medición en los dos primeros, que dará un resultado de entre cuatro posibles, el tercero ha de manifestar ese resultado: el estado ha sido así teleportado.

La Computación Cuántica es un paradigma para acelerar procesos de cálculo y de comunicaciones y no de almacenamiento de la información. Evidentemente, en los procesos de cálculo es necesario inducir en quregistros los valores iniciales sobre los que han de actuar los procesos implementados, el almacenamiento de información en estados cuánticos coherentes es crucial y ha de durar lo suficiente para realizar los cálculos en el orden de microsegundos.En este punto también es esencial la noción de corrección de errores: Dado un qubit se le quiere codificar de manera que se recupere su valor independientemente del ruido en el ambiente o en los canales de transmisión. De manera típica, en el caso de bits clásicos, por ejemplo, a cada bit se le codifica mediante una palabra de bits. Cuando se recibe una palabra, o secuencia de bits, se revisa que ésa corresponda a una secuencia de los códigos asociados. Si no es el caso, entonces se detecta un error, y si a la secuencia recibida se le asocia la secuencia de códigos que esté más cercana a ella, entonces se corrige el error. Cuando los códigos asociados forman un espacio lineal (en el espacio vectorial consistente de palabras de bits de una dimensión fija sobre el campo formado por las señales 0 y 1), entonces el código se

dice ser lineal. Esta idea se ha extrapolado al caso de qubits. Por ejemplo, un qubit puede ser afectado por la aplicación de cualquiera de las matrices de Pauli. Pues bien, codificando mediante la repetición de valores, es decir cada qubit $\mathbf{x} = x_0|0\rangle + x_1|1\rangle$ se codifica mediante $\mathbf{y} = x_0|000\rangle + x_1|111\rangle$ entonces es posible contruir una transformación unitaria que dado **y**, aún con ruido, recupere **x**. Existen varios tipos de detección y corrección de errores, y el que acabamos de mencionar es muy elemental y sólo tiene propósitos de ejemplificación.

En cuanto a la implementación, se tiene que cualquier sistema físico que realice la Computación Cuántica ha de cumplir con los criterios siguientes, llamados *de DiVicenzo*:

1. Tener caracterizada la noción de qubit y poder ensamblar varios de ellos
2. Contar con un conjunto de compuertas cuánticas primitivas que permitan realizar cualquier algoritmo
3. Poder inicializar una lista de qubits en estados puros determinados
4. Poder ejecutar la operación de toma de mediciones
5. Que los tiempos de coherencia excedan los de aplicación de las compuertas cuánticas primitivas

Ha habido varios modelos físicos (Hughes &Heinrichs, 2004):

1. *Resonancia nuclear magnética, nuclear magnetic resonance, NMR.* Un conjunto de moléculas en una solución líquida, en el que siete *efotónes* en cada molécula hacen las veces de siete qubits (Lieven*et al.;* 2001). Con esto, se puede factorizar a 15 como el producto de 3 por 5. Sin embargo, no podría extenderse el modelo a más de 10 qubits.
2. *Cavidad electrodinámica cuántica, cavity quantum electro-dynamics, Cavity QED*. Consiste de la interacción entre un qubit material -realizado como un átomo atrapado o un sistema puntual, *dot,* semiconductor- y un campo cuantizado -propiamente un fotón- de un resonador de microondas. Para conseguir una dinámica coherente se utiliza una *cavidad* para ampliar la frecuencia coherente de Rabi entre el átomo y el campo. Este modelo es apropiado para convertir estados de qubits materiales y qubits de fotones y es particularmente apto para protocolos de 2-quregistros (Duan*et al*.; 2003) y, también, ha sido utilizado en protocolos de comunicación, destacándose en esto el grupo del profesor catalán Cirac (Briegel *et al*.; 1999) del Instituto Max Planck.
3. *Trampas de iones, ion trap.* Se utiliza arreglos de trampas de iones interconectados por fotones, o por iones que hacen las veces de cabezas lectoras para transmitir la información entre arreglos, o por iones que transitan entre los arreglos. Los qubits dados como iones se mueven en diferentes zonas de trampas sin decoherencia en tiempos adecuados para la aplicación de compuertas cuánticas (Monroe, 2002). Las trampas pueden realizarse como sistemas micro-electro-mecánicos o mediante técnicas de nanofabricación.
4. *Atomos neutros(neutral atoms).* Un sistema de átomos neutros atrapados puede ser apropiado para el cómputo cuántico, debido a una estructura atómica simple al nivel cuántico, a que se mantienen aislados del medio ambiente y a su habilidad para atrapar e interactuar con una gran cantidad de átomos idénticos. Una computadora cuántica podría ser vista como un reloj atómico consistente de varios átomos interactuando de manera controlada. En la actualidad se tiene niveles de control para producir condensados de Bose-Einstein (Anglin & Ketterle, 2002) y gases degenerados de Fermi, con lo cual se ha previsto acoplar átomos.
5. *Técnicas ópticas.* Estas se comenzaron a utilizar en protocolos criptográficos y para realizar el fenómeno de entrelazamiento (Peters, 2004), y han sido muy importantes en la investigación del procesamiento cuántico de la información. Aunque han mostrado su eficacia en protocolos de comunicación, se tiene el problema de *escalabilidad*: hay limitaciones para formar ensambles de qubits fotónicos, aunque acaso éstas no sean esenciales (Lukin & Imamoglu, 2000). La detección de efectos no-lineales entre fotones

abre una posibilidad de *escalar* el modelo.

6. *Superconductividad*. Aquí los qubits son circuitos de superconductividad operando a temperaturas de miligrados Kelvin (Maklin*et al*.; 2001). Por ser de tipo eléctrico pueden interactuar con transistores consistentes de un solo electrón. Los qubits se inicializan enfriando los sistemas a su estado base. Entonces, mediante pulsos electromagnéticos de radio-frecuencia se aplica las operaciones cuánticas. Se puede tener velocidades del orden de 700GHz con muy poca disipación de potencia. Las mediciones respecto a diversas bases pueden ser realizadas mediante magnetómetros de interferencia cuántica de superconductividad.
7. *Técnicas de estado sólido.* En éstos (Loss & DiVincenzo, 1998), los qubits son sistemas de dos niveles altamente coherentes correspondientes a estados de *efotónes* de electrones localizados o de núcleos atómicos. Las compuertas quedan dadas por interacciones recíprocas entre los *efotónes*. Las transiciones excitónicas ortogonalmente polarizadas pueden realizar la noción de una pareja de qubits y el emparejamiento coulombiano de alto-orden, que conlleva la formación bi-excitónica, puede utilizarse para realizar la noción de entrelazamiento. Una limitación de este enfoque son los cortos tiempos de decoherencia.

Aplicaciones de Cómputo Cuántico

La Computación Cuántica tiene sus orígenes en campos muy especializados de la Física Teórica, pero en un futuro tendrá un impacto profundo en la vida cotidiana. En la actualidad se encuentra aún en una etapa de intenso desarrollo: Se está en una fase de transición entre experimentos que permiten observar los fenómenos y una etapa que permita controlar a los fenómenos. Diversos grupos en el mundo están involucrados en la implementación física de modelos de Computación Cuántica, entre los que se cuentan el Laboratorio Nacional de Los Alamos, el Instituto Tecnológico de Massachussets y el Tecnológico de California en los EUA, el Centro Europeo de Investigación Científica (CERN, por sus siglas en francés: *Centre Européen de la Recherche Nucléaire*), el grupo de centros de investigación participantes en el Consejo Europeo de Asesoría para la Iniciativa de Nanoelectrónica (ENIAC, por sus siglas en inglés: *European Nanoelectronics Initiative Advisory Council*) en Europa y la empresa NEC y otros institutos universitarios en Japón, entre muchos otros. Para esto se busca desarrollar tanto arquitecturas óptimas como algoritmos en este paradigma para diversos problemas. Entre las tecnologías de implementación están las trampas de iones, la electrodinámica cuántica de cavidades (QED) y la resonancia magnética nuclear (NMR), aunque aún las limitaciones son mayúsculas. Acaso las primeras computadoras cuánticas de uso generalizado serán muy distintas de sus modelos actuales.

Sus principales aplicaciones previstas están en las áreas de Criptografía (seguridad de la información, preservación de la privacidad y de la integridad de los mensajes), Bases de Datos (localización de registros en información poco estructurada, recolección de información de tipo militar o “de inteligencia”), Simulación de Fenómenos Cuánticos (estudio de diversos modelos de la Física de Partículas), Cómputo Masivo (de interés en ciencias como Física, Astronomía, Química, Meteorología, Oceanografía, Ciencias Forénsicas) y Simulación de Procesos Dinámicos (desde explosiones de diversos tipos hasta hidrodinámica de diversos fluidos). Naturalmente, en la administración y los negocios sus potencialidades son enormes en cuanto a la localización de información y sus posibilidades de pronóstico mediante la corrida de procesos. Acaso el desarrollo de cúmulos de computadoras se basará también en procesadores de tipo cuántico. La ingeniería a escalas atómicas y la interferometría atómica basada en la dualidad onda-partícula de la luz, constituyen también áreas de aplicación potencial de la Computación Cuántica. En Ciencia, además de la Física misma, se tiene que la corrección de errores, esencial para construir computadoras cuánticas robustas ante la decoherencia, ha mostrado grandes avances y ha tenido contribuciones importantes en la teoría matemática de

códigos.

Hoy en día, empresas como MITRE o MagicQ, ofrecen productos basados en Criptografía Cuántica, en particular para que varias partes establezcan de manera segura claves privadas a través de varios medios. La empresa canadiense D-Wave Systems, Inc., anunció a inicios de 2007 un propio modelo que simula el cómputo cuántico mediante una arquitectura "escalable" de procesadores convencionales. Esta utiliza una tecnología basada en la electrónica de superconductores, que son aluminio y niobio, ambos metales a temperatura ambiente. Pero, a temperaturas cercanas al cero absoluto, sus electrones se aparean en los llamados *pares de Cooper*, los cuales poseen el mismo estado cuántico y por las propiedades de superconductividad el efecto se amplifica. De esta manera se han construído coprocesadores que simulan el Cómputo Cuántico.

CONCLUSIONES

La Ciencia de la Computación se ha desarrollado plenamente como una propia ciencia. Ha planteado importantísimos problemas, tanto de ingeniería como físicos y matemáticos. Sus repercusiones en otras ciencias han sido tan relevantes que, en muchas de ellas, los métodos técnicos y formales de la Computación han resultado esenciales en sus avances. Pensemos en la biología celular, la lingüística, la medicina o la administración, por mencionar unos cuantos ejemplos. Así como el código genético significó un hito en la modelación de procesos biológicos mediante análisis de tipo sintáctico, propio de la teoría de autómatas finitos y de los lenguajes formales, en la actualidad esos métodos se usan en diversas teorías cosmogónicas para modelar interacciones entre partículas subatómicas y la misma teoría de cuerdas. Así, pues, la naturaleza en sí misma puede verse como un sistema de información. En el presente siglo la implementación de la Computación Cuántica seguro transformará esencialmente la explotación de problemas difíciles para la Computación Clásica, a fin de hacer más robustos los algoritmos de seguridad y para acelerar procesos de simulación.

REFERENCIAS

Aaronson, S. &Kuperberg, G. (2006). Complexity Zoo.[enlinea] [en linea] <http://qwiki.stanford.edu/index.php/Complexity_Zoo> [consultado : 17/03/12]

Anglin, J. &Ketterle, W. (2002). Bose-Einstein condensation of atomic gases.*Nature*. 416. pp 211-218.

Ausiello, G.; Crescenzi, P.; Gambosi, G.; Kann, V.; Marchetti-Spaccamela, A. &Protasi, M. (1999).*Complexity and Approximation*.Springer-Verlag, 1999. [en linea] <http://www.nada.kth.se/~viggo/approxbook/> [consultado :17/03/12]

Backus, J. (1978). Can programming be liberated from the von Neumann style*?Communications of the ACM*. Vol. 21. (8). pp. 613-641.

Bennett, C. H.; Brassard, G. (1984). Quantum Cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, p. 175

Bouwmeester, D.; Ekert, A. &Zeilinger, A. (Eds.). (2000).*The Physics of Quantum Information*. Springer-Verlag, 2000.

Brady, A. (2006). Latest results in search for large values. [en linea] <http://www.cse.unr.edu/~al/BusyBeaver.html> [consultado :17/03/12]

Briegel, H.; Cirac, J.; Dür, W.; Van Enk, S.; Kimble, H.; Mabuchi, H. & Zoller. P. (1999). Physical implementations for quantum communication in quantum networks.*Quantum Computing and Quantum Communications*. 1509, 373-382.

Clay Mathematics Institute. (2006). Millennium problems. [en linea] <http://www.claymath.org/millennium/> [consultado :17/03/12]

School of Computer Science at Carnegie Mellon University.(2000). The CAPTCHA Project. 2000. [en linea] <http://www.captcha.net/> [consultado :17/03/12]

Duan, L.; Kuzmich, A. & Kimble, H. (2003). Cavity QED and quantum-information processing with "hot' trapped atoms.*Physical Review A*. 67. (032305).

Harnad, S. (2000). Minds, machines and Turing: The indistinguishability of indistinguishables. *Journal of Logic, Language, and Information*. 9. (4), 425-445.

Hodges, A. (2000). Alan Turing Home Page. [en linea] <http://www.turing.org.uk/> [consultado :17/03/12]

Hofstadter, D. (1979). *Gödel, Escher, Bach: An Eternal Golden Braid*. Basic Books.

Hughes, R. &Heinrichs, T. (2004). Quantum information science and technology roadmap. <http://qist.lanl.gov/> [consultado :17/03/12]

Humanitas, Int. (2006). The original multilingual metanewstranslator.http://newstran.com.

Kurzweil, R. (2006). Kurzweilai.net. [en linea] <http://www.kurzweilai.net/> [consultado :17/03/12]

.

Lieven, M.; Vandersypen, M.; Steffen, M.; Breyta, G.; Yannoni, C.; Sherwood, M. & Chuang, I. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.*Nature*. 414. (883).

Loss, D. &DiVincenzo, D. (1998). Quantum computation with quantum dots.*Physical Review A*. 57, 120-126.

Lukin, M. &Imamoglu, A. (2000). Nonlinear optics and quantum entanglement of ultraslow single photons.*Physical Review Letters*. 84, 1419-1422.

Maklin, Y.; Schön, G. &Shnirman, A. (2001). Quantum-state engineering with Josephson junction devices.*Reviews of Modern Physics*. 73, 357-400.

Marxen, H. (2006). BusyBeaver. [en linea] <http://www.drb.insel.de/~heiner/BB/> [consultado : 17/03/12]

Michel, P. (2006). The busy beaver competitions.http://www.logique.jussieu. fr/~michel/bbc.html.

Monroe, C. (2002). Quantum information processing with atoms and photons. *Nature*. 416, 238-246.

Nielsen, M. & Chuang, I. (2000).*Quantum Computation and Quantum Information*. Cambridge, 2000.

Penrose, R. (1996). Beyond the doubting of a shadow. *Psyche.* Vol. 2. No. 23. [en linea] <http://psyche.cs.monash.edu.au/v2/psyche-2-23-penrose.html> [consultado : 17/03/12]

Peters, A.; Wei, T. &Kwiat, P. (2004). Mixed state sensitivity of several quantum information benchmarks. *Physical Review A*. 70, (052309).

Selman, A.(1994).A taxonomy of complexity classes of functions. *Journal of Computer and System Sciences*. 48, (2), 357-381.

Turing, A. (1950). Computing machinery and intelligence. *Mind, LIX*.pp433-460.