Computación cuántica: un esbozo de sus métodos y desarrollos

UNA VISIÓN PANORÁMICA DE LA NOCIÓN DE COMPUTACIÓN CUÁNTICA: SUS ELEMENTOS MATEMÁTICOS BÁSICOS, LAS VENTAJAS QUE IMPLICA EN COMUNICACIONES Y CRIPTOGRAFÍA, ASÍ COMO ALGUNAS OPCIONES ACTUALES PARA SU IMPLEMENTACIÓN.

Guillermo Morales-Luna

Ignoranti quem portum petat nullus suus ventus est.
(Nunca hay viento favorable para quien ignora hacia cuál puerto se dirige.)
Séneca

Elementos matemáticos básicos

En la mecánica cuántica, uno de los elementos más importantes es la noción de *estados de energía*. Estos son puntos en un espacio lineal generado por las funciones propias de un operador hamiltoniano, según lo describe la *ecuación de Schrödinger*, y son *unitarios*, es decir, su longitud euclidiana, vistos como elementos del espacio, es 1. Toda combinación lineal de las funciones propias, que sea unitaria, se ve como una superposición de las funciones propias y la probabilidad de que el estado asuma una de ellas es el cuadrado del valor absoluto de su coordenada en la dirección de esa función propia. En resumen, *la probabilidad de que el estado asuma una dirección es el cuadrado de su amplitud en esa dirección*.

Tal idea ha dado origen al *cómputo cuántico*. Los bits clásicos 0 y 1 se ponen en correspondencia con dos vectores unitarios en un espacio vectorial sobre los números complejos y cada vector unitario en ese espacio se ve como la superposición de esos dos bits. Se conviene en que, para una tal superposición, una *medición* la hará asumir uno de los dos valores, 0 ó 1, es decir, una de las dos direcciones básicas, con la probabilidad dada por el cuadrado de su amplitud en esa dirección.

Los *operadores primitivos* en el cómputo cuántico son las transformaciones unitarias; es decir, son transformaciones lineales cuyas inversas son sus propias transpuestas conjugadas, y en esto se sigue también una motivación de la mecánica cuántica. Un algoritmo cuántico es una lista de operadores primitivos, compuestos de manera consecutiva junto con toma de mediciones. Como todo paradigma de cómputo, el cómputo cuántico calcula funciones. Una función es *calculable* por un algoritmo cuántico si para cualquier entrada, es decir una cadena de bits, el algoritmo termina dando como salida el valor de

GUILLERMO MORALES-LUNA Es licenciado en Física y Matemáticas (ESFM-IPN), maestro en Ciencias con especialidad en Matemáticas (**Cinvestav**) y doctor en Ciencias Matemáticas (Instituto de Matemáticas, Academia Polaca de Ciencias). Ocupa el cargo de Investigador Titular en el Departamento de Computación del **Cinvestav**. Sus áreas de interés son: fundamentos matemáticos de computación; lógica y deducción automática; criptografía y teoría de la complejidad. Ha sido profesor en el IPN y en la B. Universidad Autónoma de Puebla. Ha realizado dos estancias sabáticas en el Instituto Mexicano del Petróleo. Es mexicano por nacimiento y también le fue conferida la ciudadanía polaca.
gmorales@cs.cinvestav.mx

la función en la entrada, codificada como una lista de bits, con una probabilidad 1.

Los textos clásicos en este tema son [2] y [10]. A diferencia de los conceptos básicos de información clásica, el bit que puede asumir valores 0 ó 1, y los bits pueden concatenarse para formar arreglos de crecimiento lineal, 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 de crecimiento exponencial. Esto dota al cómputo cuántico de un paralelismo inherente que permite acelerar notoriamente los procesos. A continuación se expone una breve cronología de la computación cuántica.

La idea de computación cuántica se desarrolló en la segunda mitad del siglo XX. Rolf Landauer, científico de origen alemán, radicado en los EUA desde la década de 1930, y que laboraba en IBM, planteó en 1961 que la información tiene una manifestación física: cuando se pierde en un circuito irreversible, la información se convierte en entropía y se disipa como calor. En contraposición, los circuitos reversibles, desde el punto de vista físico, son aquéllos que no incrementan la entropía, por lo que poseen una mayor eficiencia de la energía y, desde el punto de vista lógico, son aquéllos en los que cada operador primitivo actúa de manera inyectiva. Todo circuito reversible en el sentido lógico lo es en el sentido físico. Desde la década de 1970, Charles Bennet, también de IBM, en el centro Thomas Watson ha estudiado la noción de *reversibilidad* de las computaciones. En 1981, Richard Feynman planteó que los sistemas físicos, incluidos los de nivel cuántico, podían ser simulados de manera exacta por computadoras cuánticas. En 1982, Peter Beniof, del Laboratorio Nacional de Argonne, presentó modelos lógicos de máquinas de Turing cuánticas, y en 1984, Charles Bennet y Gilles Brassard, éste último de la Universidad de Montreal, introdujeron las nociones básicas de criptografía cuántica. En 1985, David Deutsch, de la Universidad de Oxford, reinterpretó la llamada Tesis de Church-Turing en el marco del cómputo cuántico y, desde 1993, Bennet, Brassard, Crepeau, Josza, Peres y Wooters han desarrollado el uso de la noción de *teleportación.* En 1994, Peter Shor, entonces en ATT, publicó su célebre algoritmo cuántico para factorizar enteros.

La unidad básica de información en el cómputo cuántico es, entonces, el *qubit*, en contraposición del *bit clásico*. Denotemos por Q al espacio de qubits y por $B = \{0,1\}$ al de los bits clásicos. La noción de *superposición* se realiza en el ambiente de *espacios de Hilbert*. Formalmente, los qubits son vectores unitarios en un espacio complejo

de dimensión 2 sobre los complejos, es decir, Q es la esfera unitaria del espacio vectorial C^2. Si $x = x_0\mathsf{e}_0 + x_1\mathsf{e}_1 = \begin{bmatrix} x_0 & x_1 \end{bmatrix}^{\mathrm{T}}$ es un qubit,

x_0, $x_1 \in \mathsf{Q}$, $|x_0|^2 + |x_1|^2 = 1$, se escribe de acuerdo con la notación debida a Dirac, $\mathsf{x} = x_0|0\rangle + x_1|1\rangle$. Los bits clásicos se identifican, respectivamente, con $0 \leftrightarrow |0\rangle = [1 \quad 0]^{\mathrm{T}}$ y $1 \leftrightarrow |1\rangle = [0 \quad 1]^{\mathrm{T}}$. Al *tomar una medición* el qubit **x** asumirá el valor $|0\rangle$ con probabilidad $|\mathsf{x}_0|^2$ y el valor $|1\rangle$ con probabilidad $|\mathsf{x}_1|^2 = 1 - |\mathsf{x}_0|^2$. Así, la probabilidad de que el qubit asuma el valor "cero" es el cuadrado del valor absoluto de la primera coordenada, $\Pr(\mathsf{x} \to |0\rangle) = |x_0|^2$ y la probabilidad de que asuma el valor "uno" es la complementaria, $\Pr(\mathsf{x} \to |1\rangle) = |x_1|^2$. En tanto que no se tome la medición, cada qubit es una superposición de los dos básicos $|0\rangle$ y $|1\rangle$.

La esfera unitaria del espacio complejo C^2 es una variedad de dimensión 3, sobre los números reales, por lo que puede ser parametrizada de manera alternativa considerando tres coordenadas, dos de los cuales son los ángulos θ y φ. Mediante las correspondencias

$$\begin{aligned} x_0 &\leftrightarrow \cos\frac{\theta}{2} \\ x_1 &\leftrightarrow e^{i\varphi}\operatorname{sen}\frac{\theta}{2} \\ \mathsf{x} = x_0|0\rangle + x_1|1\rangle &\leftrightarrow \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\operatorname{sen}\frac{\theta}{2}\,|1\rangle \end{aligned}$$

se identifica a la sección de la esfera de qubits correspondiente a abscisas con valores reales con la llamada *esfera de Bloch*. Ésta es una representación geométrica de uso común en cómputo cuántico.

Los *quregistros*, no son sólo concatenaciones de qubits, sino que son productos tensoriales de ellos, por lo que la dimensión de los quregistros crece exponencialmente respecto al número de qubits concatenados. Si $\mathsf{x}_0, \ldots, \mathsf{x}_{n-1} \in \mathsf{Q}$ son n qubits, su correspondiente *n-quregistro* es $\mathsf{x} = \mathsf{x}_0 \otimes \ldots \otimes \mathsf{x}_{n-1} \in \mathsf{C}^{2^n}$. Si Q^n es la colección de n-quregistros, entonces Q^n es la esfera unitaria del espacio complejo H_n de dimensión 2^n, la cual es precisamente la cardinalidad de B^n. Para cada $j = 0, \ldots, 2^n - 1$, se escribe $\mathsf{e}_j = |(j)_2\rangle = |\varepsilon\rangle$ donde $\varepsilon = (j)_2$ es la representación en base 2 de j, de longitud n. La base canónica del espacio H_n es pues $(|\varepsilon\rangle)_{\varepsilon \in \mathsf{B}^n}$. Por ejemplo, para n=3, $\mathsf{H}_3 = \mathsf{C}^8$ y su base canónica es

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

Las operaciones básicas son matriciales y 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. Si $U : \mathsf{H}_1 \to \mathsf{H}_1$ es una transformación lineal unitaria, es decir $U^{-1} = U^H$, donde esta última es la conjugada transpuesta, o *hermitiana*, de la matriz U, entonces se dice ser una *compuerta cuántica* o *qucompuerta*. Para dos qucompuertas $U, V : \mathsf{H}_1 \to \mathsf{H}_1$, su *producto tensorial* es $U \otimes V : \mathsf{H}_2 \to \mathsf{H}_2$ tal que $(U \otimes V)(\mathsf{x} \otimes \mathsf{y}) = U(\mathsf{x}) \otimes V(\mathsf{y})$.

Sucesivamente, se define $U^{\otimes 1} = U$ y $U^{\otimes(n+1)} = U \otimes U^{\otimes n}$.

Las siguientes son matrices unitarias:

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

donde $i = \sqrt{-1}$, y se dicen ser las *matrices de Pauli*. La primera es la matriz identidad 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*:

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

cuyo efecto es que si $\mathsf{x} = x_0|0\rangle + x_1|1\rangle$

entonces

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

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

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

$$\begin{aligned} U_f(H\mathsf{x} \otimes |0\rangle) &= \frac{x_0 + x_1}{\sqrt{2}}U_f(|0\rangle \otimes |0\rangle) + \frac{x_0 - x_1}{\sqrt{2}}U_f(|1\rangle \otimes |0\rangle) \\ &= \frac{x_0 + x_1}{\sqrt{2}}|0 f(0)\rangle + \frac{x_0 - x_1}{\sqrt{2}}|1 f(1)\rangle \end{aligned}$$

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

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

Procedimientos de comunicaciones y de criptografía

En comunicaciones, la computación cuántica proporciona, además, disminución de costos debido al fenómeno de entrelazamiento (*entanglement*, en inglés).

Entrelazamiento

La colección de 2-quregistros es la esfera unitaria en $\mathsf{H}_2 = \mathsf{C}^{2^2} = \mathsf{C}^4$. Dado un quregistro $\mathsf{x}^{(2)} = x_{00}|00\rangle + x_{01}|01\rangle + x_{10}|10\rangle + x_{11}|11\rangle \in \mathsf{Q}^2$ se tendrá que la probabilidad de que el quregistro asuma una de las cuatro posibles palabras de dos bits es $\Pr\left(\mathsf{x}^{(2)} \to |ij\rangle\right) = |x_{ij}|^2$, para cada $i, j \in \{0,1\}$. Sin embargo, si se toma una medición en el primer qubit y éste asume el valor $i \in \{0,1\}$ entonces el 2-quregistro tomará el valor

$$\mathsf{x}^{(2)}\Big|_{x_0 \to |i\rangle} = \frac{1}{\sqrt{|x_{i0}|^2 + |x_{i1}|^2}}\left(x_{i0}|i0\rangle + x_{i1}|i1\rangle\right),$$

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

$$\mathsf{x}^{(2)}\Big|_{x_1 \to |j\rangle} = \frac{1}{\sqrt{|x_{0j}|^2 + |x_{1j}|^2}}\left(x_{0j}|0j\rangle + x_{1j}|1j\rangle\right),$$

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

$$[x_{00} \quad x_{01} \quad x_{10} \quad x_{11}] = \left[\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}}\right].$$

Entonces, resulta $\mathsf{x}^{(2)}\Big|_{x_0 \to |i\rangle} = |i\bar{i}\rangle$

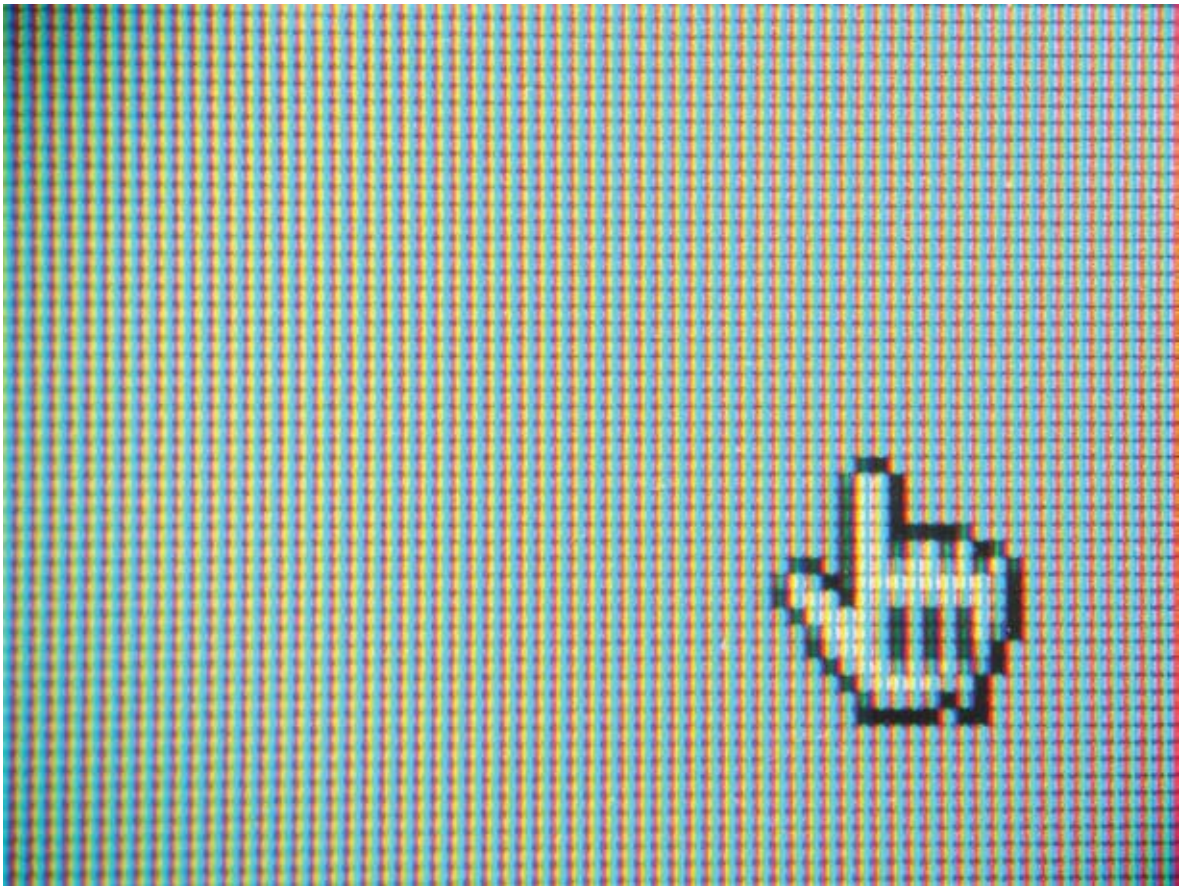
y $\mathsf{x}^{(2)}\Big|_{x_1 \to |j\rangle} = |j\bar{j}\rangle$, es decir, una vez que se determina un qubit, el otro queda también determinado, con el mismo valor. Similarmente, supongamos

$$[x_{00} \quad x_{01} \quad x_{10} \quad x_{11}] = \left[0 \quad \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}} \quad 0\right].$$

Entonces, resulta $\mathsf{x}^{(2)}\Big|_{x_0 \to |i\rangle} = |i\bar{i}\rangle$

y $\mathsf{x}^{(2)}\Big|_{x_1 \to |j\rangle} = |j\bar{j}\rangle$, 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.



Consideremos ahora, $\mathsf{b}_{00}=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)$,

$\mathsf{b}_{01}=\frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right)$,

$\mathsf{b}_{10}=\frac{1}{\sqrt{2}}\left(|00\rangle-|11\rangle\right)$ y

$\mathsf{b}_{11}=\frac{1}{\sqrt{2}}\left(|01\rangle-|10\rangle\right)$.

La colección $\{\mathsf{b}_{00},\mathsf{b}_{01},\mathsf{b}_{10},\mathsf{b}_{11}\}$ es una base ortonormal, llamada *de Bell*, del espacio de 2-quregistros H_2. De hecho, $\mathsf{b}_{ij}=C\left(H\otimes 1_2\right)\left(|i\rangle\otimes|j\rangle\right)=C\left(H|i\rangle\otimes|j\rangle\right)$, donde C es la compuerta *NO-Controlado*, $C:|00\rangle\mapsto|00\rangle,|01\rangle\mapsto|11\rangle,|10\rangle\mapsto|10\rangle,|11\rangle\mapsto|01\rangle$ (si el segundo bit es 0 deja el primero intacto, pero si es 1 "niega" al primero). Considerando las matrices de Pauli, se puede ver que también valen las igualdades: $\mathsf{b}_{00}=(1_2\otimes 1_2)\mathsf{b}_{00}$, $\mathsf{b}_{01}=(\sigma_x\otimes 1_2)\mathsf{b}_{00}$, $\mathsf{b}_{10}=(\sigma_z\otimes 1_2)\mathsf{b}_{00}$, $\mathsf{b}_{11}=(\sigma_z\sigma_x\otimes 1_2)\mathsf{b}_{00}$.

Protocolos de comunicación

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 $\varepsilon_A\wedge\varepsilon_B=a\oplus b$.

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 comunicarse un bit clásico para tener éxito con probabilidad 3/4.

Para la implementación cuántica, consideremos el 2-quregistro

$$\mathsf{x}_0\mathsf{x}_1=\mathsf{x}^{(2)}=\frac{1}{\sqrt{2}}\left(|00\rangle-|11\rangle\right)$$

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 correspondiente a la rotación de $\frac{\pi}{8}$ radianes:

$$G=\begin{bmatrix}\cos\left(\frac{\pi}{8}\right) & \operatorname{sen}\left(\frac{\pi}{8}\right)\\ -\operatorname{sen}\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right)\end{bmatrix}.$$

Sean $M_A=\begin{cases}1_2 & \text{si } \varepsilon_A=0\\ G & \text{si } \varepsilon_A=1\end{cases}$,

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

Alicia produce su bit tomando como a el resultado de tomar medición a $M_A\mathsf{x}_0$ y Beto produce su bit tomando como b el resultado de tomar medición a $M_B\mathsf{x}_1$. Se puede ver que

$$\Pr(a\oplus b\neq\varepsilon_A\wedge\varepsilon_B)=\sum_{\varepsilon_A,\varepsilon_B\in\mathsf{B}}\frac{1}{4}\Pr(a\oplus b\neq\varepsilon_A\wedge\varepsilon_B|\varepsilon_A,\varepsilon_B)=\frac{3-\sqrt{2}}{8},$$

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 $\varepsilon_0\varepsilon_1\in\mathsf{B}^2$ a otra parte, *Beto*. Supongamos que se prepara el 2-quregistro entrelazado

$$\mathsf{x}_0\mathsf{x}_1=\mathsf{b}_{00}=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right),$$

y se da el primer qubit x_0 a Alicia y el segundo x_1 a Beto. En función de la pareja $\varepsilon_0\varepsilon_1$, Alicia toma un operador U_A para aplicar sobre su qubit:

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

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

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

Procedimientos de criptografía

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.

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

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 $\delta = [\delta_i]_{i=1}^{N}$ y $\varepsilon = [\varepsilon_i]_{i=1}^{N}$.

   Transmite por el canal cuántico la sucesión de estados $S = \left[s_i = e_{\varepsilon_i}^{\delta_i}\right]_{i=1}^{N}$.

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, $\forall j \in J : \delta_j = \zeta_j$, 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, 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.

Implementaciones actuales

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 decoherencia excedan los de aplicación de las compuertas cuánticas primitivas.

Ha habido varios modelos físicos [5]:

- **Resonancia nuclear magnética** *(Nuclear Magnetic Resonance, NMR).* Un conjunto de moléculas en una solución líquida en el que siete *espines* en cada molécula hacen las veces de siete qubits [12]. 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.
- **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. A fin de 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 [4]; también ha sido utilizado en protocolos de comunicación, destacándose en ello el grupo del profesor catalán J.I. Cirac [3] del Instituto Max Planck.
- **Trampas de iones** *(Ion Trap).* Se utilizan 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

La idea de computación cuántica se desarrolló en la segunda mitad del siglo XX. Rolf Landauer, científico de origen alemán, planteó en 1961 que la información tiene una manifestación física; es decir, cuando se pierde en un circuito irreversible, la información se convierte en entropía y se disipa como calor.

en tiempos adecuados para la aplicación de compuertas cuánticas [9]. Las trampas pueden realizarse como sistemas micro-electro-mecánicos o mediante técnicas de nanofabricación.

- **Átomos 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 que consiste de varios átomos que interactúan de manera controlada. En la actualidad existen niveles de control para producir condensados de Bose-Einstein [1] y gases degenerados de Fermi, con lo cual se ha previsto acoplar átomos.
- **Técnicas ópticas.** Comenzaron a utilizarse en protocolos criptográficos y para realizar el fenómeno de entrelazamiento [11] y han sido muy importantes en la investigación del procesamiento cuántico de la información. Aunque han mostrado se 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 [7]. La detección de efectos no-lineales entre fotones abre una posibilidad de "escalar" el modelo.
- **Superconductividad.** Aquí los qubits son circuitos de superconductividad operando a temperaturas de miligrados Kelvin [8]. 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 aplican las operaciones cuánticas. Se puede tener velocidades del orden de 700 GHz con muy poca disipación de potencia. Las mediciones respecto a diversas bases pueden ser realizadas mediante magnetómetros de interferencia cuántica de superconductividad.
- **Técnicas de estado sólido.** En éstas [6], los qubits son sistemas de dos niveles altamente coherentes correspondientes a estados de *espines* de electrones localizados o de núcleos atómicos. Las compuertas quedan dadas por interacciones recíprocas entre los *espines*. 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.

Un problema algorítmico abierto

Las comunicaciones actuales se han automatizado rápidamente y los procesos involucrados se utilizan de manera cada vez más extensa y compleja. Actividades como búsqueda de información, el intercambio de datos con el propósito de realizar protocolos, o la revisión de privilegios y autorizaciones otorgados por terceras partes, son comunes en transacciones comerciales, bancarias, contables, legales o de simple entretenimiento. Esto ha propiciado el desarrollo de

la seguridad informática. Los procesos electrónicos de autentificación y cifrado son de suma importancia en la sociedad moderna. Aunque éstos pueden dotar de una cierta "identidad" a los agentes informáticos y a sus propietarios (los métodos de autentificación conllevan procesos de no-repudio incontrovertibles), la autonomía de las partículas de *software* está aún muy restringida. La llamada criptografía de clave pública ha facilitado el establecimiento de claves privadas propias de cada transacción y se usa en el protocolo de comunicaciones SSL (*Secure Socket Layer*) de Internet. Sus protocolos se basan en problemas matemáticos de gran dificultad, tales como el de factorización de enteros, a saber, encontrar los factores primos de un número entero muy grande (del orden de 1 024 o 2 048 bits cuando se le escribe en binario), o del cálculo de logaritmos discretos, es decir, en un grupo cíclico, dado un generador de él, para un elemento cualquiera se trata de encontrar la mínima potencia del generador que lo representa. Las dificultades de estos problemas son aparentemente esenciales, por lo que nuevos dispositivos de cálculo sólo acelerarían en factores constantes el desempeño de los algoritmos para resolverlos. El cómputo cuántico, sin embargo, por la posibilidad de involucrar en un solo paso de cómputo una cantidad exponencial de información, podría disminuir la complejidad de los algoritmos para resolverlos. Por ejemplo, el mejor algoritmo para resolver el problema de factorización tiene una complejidad subexponencial (su orden es una potencia de la raíz cúbica del número de bits de la instancia), mientras que el algoritmo cuántico de Shor [10], para resolverlo, tiene una complejidad polinomial, de orden cúbico, pero involucra un orden lineal de qubits respecto al número de bits con los que se escriba el entero a factorizar. El modelo NMR de computadoras cuánticas [12] no significa ningún riesgo para los protocolos actuales. El problema de factorización, y su complemento, el decidir si un entero es un primo, están en la clase de problemas NP. Aún en la actualidad no se sabe si alguno de ellos es completo en esa clase, es decir, cualquier otro problema ahí se reduce procedimentalmente al problema de factorización, y se sospecha que no lo es, pues si lo fuera, se tendría que la clase NP sería cerrada por complementos, algo que la experiencia hace intuir que no es verdad, aunque esto último no ha sido tampoco demostrado.

El algoritmo de Shor, publicado hace ya 13 años, hace que la computación cuántica sea vista como un elemento que habrá de desafiar a los protocolos de comunicación en boga, cuando las limitaciones tecnológicas actuales hayan sido superadas. Luego de resolver el problema de factorización, el problema del logaritmo discreto también podría resolverse eficientemente mediante un algoritmo cuántico que utiliza la parte medular del algoritmo de Shor: el cálculo de órdenes de elementos en un grupo cíclico. Es, por tanto, del interés fundamental de la criptografía desarrollar métodos robustos ante los procedimientos para resolver los problemas de factorización y del logaritmo discreto. En el cómputo cuántico se ha planteado un problema matemático muy importante, el llamado *problema del subgrupo escondido*. Dado un grupo G y un subgrupo H contenido en él, una función f definida en G se dice que *separa clases* de H si dos elementos en G poseen una misma imagen bajo f si y sólo si sus clases módulo H coinciden, en símbolos: $\forall x_0, x_1 \in G$, $f(x_0) = f(x_1) \iff x_0 H = x_1 H$. El problema está en que, dada una función f que separa algún subgrupo (escondido), es necesario caracterizar a ese subgrupo (es decir, calcular un conjunto de generadores) utilizando el menor número de evaluaciones de la función f. Ambos problemas, el de factorización y el del logaritmo discreto, se reducen al problema del subgrupo escondido. En la actualidad se trabaja en diseñar un algoritmo cuántico de tiempo polinomial en la descripción del grupo y de la función.

La computación cuántica, entonces, es todavía un paradigma lógicamente viable que no ha sido implementado a plenitud debido a limitaciones tecnológicas. En un plazo de unas dos décadas seguramente presenciaremos avances notables en ello. ●

[Referencias]

[1] J.R. Anglin y W. Ketterle. Bose-Einstein condensation of atomic gases. *Nature*, 416:211-218, 2002.
[2] Dirk Bouwmeester, Artur Ekert, y Anton Zeilinger (eds.). *The Physics of Quantum Information*. Springer-Verlag, 2000.
[3] H.J. Briegel, J.I. Cirac, W. Dür, S.J. van Enk, H.J. Kimble, H. Mabuchi y P. Zoller. Physical implementations for quantum communication in quantum networks. *Quantum Computing and Quantum Communications*, 1509:373-382, 1999.
[4] L.M. Duan, A. Kuzmich, and H.J. Kimble. Cavity QED and quantum-information processing with "hot' trapped atoms. *Physical Review A*, 67:032305, 2003.
[5] Richard Hughes and Todd Heinrichs. Quantum information science and technology roadmap. 2004. disponible en http://qist.lanl.gov/.
[6] D. Loss y D.P. DiVincenzo. Quantum computation with quantum dots. *Physical Review A*, 57:120-126, 1998.
[7] M.D. Lukin y A. Imamoglu. Nonlinear optics and quantum entanglement of ultraslow single photons. *Physical Review Letters*, 84:1419-1422, 2000.
[8] Y. Maklin, G. Schön, y A. Shnirman. Quantum-state engineering with Josephson junction devices. *Reviews of Modern Physics*, 73:357, pp. 400, 2001.
[9] C. Monroe. Quantum information processing with atoms and photons. *Nature*, 416:238–246, 2002.
[10] Nielsen y Chuang. *Quantum Computation and Quantum Information*. Cambridge, 2000.
[11] N.A. Peters, T.C. Wei, y P.G. Kwiat. Mixed state sensitivity of several quantum information benchmarks. *Physical Review A*, 70:052309, 2004.
[12] Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood y Isaac L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883, 2001.