Alicia y Beto se comunican. Introducción a la comunicación cuántica

EL ESTILO DE VIDA ACTUAL DEPENDE DE UN INTERCAMBIO CONTINUO DE INFORMACIÓN POR LO QUE ES NECESARIO GARANTIZAR TRANSMISIONES EFICIENTES Y SEGURAS. SIN ESTE PAR DE GARANTÍAS, LAS TRANSACCIONES FINANCIERAS SE VOLVERÍAN CAÓTICAS PONIENDO EN PELIGRO LA ECONOMÍA MUNDIAL. EN LA BÚSQUEDA DE SOLUCIONES AL PROBLEMA DE LA PRIVACIDAD EN LAS COMUNICACIONES, LA CIENCIA ACTUAL ESTÁ FORMULANDO MODELOS CUÁNTICOS DE CIFRADO. CON ELLO SE ESTÁ PREPARANDO TERRENO PARA INAUGURAR LA ERA DE LA COMUNICACIÓN CUÁNTICA.

Blas Manuel Rodríguez Lara

En este artículo se tratará el problema de Alicia y Roberto –Beto para los amigos– habitantes de un mundo ideal. Alicia desea compartir información cuántica generada en su laboratorio, por ejemplo un bit cuántico o qubit, con Beto, cuyo laboratorio se encuentra en una locación diferente. Ella quiere que la información sea transmitida de manera eficaz y eficiente. En caso de existir errores en la transmisión, necesita que él esté consciente de la existencia de esos errores y sea capaz de resarcirlos. Para lograr esta tarea, Alicia y Beto cuentan con un canal clásico de comunicación y un proveedor de qubits entrelazados. Utilizando estos recursos se establecerá un canal cuántico de transmisión de información entre ellos y se analizará una forma de codificar y corregir los posibles errores inducidos por ruido –ideal como su mundo– en dicho canal.

¿Por qué comunicaciones cuánticas?

El problema de las transmisiones eficientes y seguras es de vital importancia en nuestra sociedad. El estilo de vida moderno depende de un intercambio continuo de información con fidelidad y privacidad garantizadas. Sin este par de garantías en sus transacciones, el mundo financiero, por ejemplo, sería un caos y con él, las economías mundiales.

Más de alguno podría preguntarse: ¿por qué, si la información que manejamos cotidianamente

BLAS MANUEL RODRÍGUEZ LARA (D.C. INAOE 05, SNI-Candidato) Investigador becario postdoctoral, Departamento de Física Teórica, Instituto de Física, Universidad Nacional Autónoma de México. Entre sus intereses se encuentran la docencia de la óptica e informática cuántica y la investigación de la interacción radiación-materia y sus posibles aplicaciones para el cómputo cuántico. Ha trabajado en caracterización de correlaciones cuánticas, reversión de dinámica y caracterización de objetos mesoscópicos en modelos de interacción radiación-materia.
bmlara@fisica.unam.mx

es clásica, nos metemos en problemas trabajando con información cuántica? ¿Por qué utilizar comunicaciones cuánticas? Tres razones, suficientes para contestar la primera pregunta, son expuestas por Kamil Bradler en su contribución a este volumen, relacionada con la búsqueda de soluciones al problema de la privacidad en las comunicaciones. Un ejemplo muy particular de esas razones es el siguiente:

La criptografía clásica, utilizada actualmente para proteger la información transmitida por los canales de comunicación existentes, se basa en la especulación acerca de la imposibilidad de descomponer eficientemente números enteros grandes en sus factores primos utilizando un algoritmo clásico. En 1994, Peter Shor (Massachusetts Institute of Technology, EUA) demostró que encontrar los factores primos de un número entero puede realizarse de manera eficiente con un algoritmo cuántico. El día en que sea posible implementar el algoritmo de factorización en primos de Shor, las comunicaciones clásicas, con los modelos de cifrado que conocemos, dejarán de ser seguras. Si ese día llegare, será necesario tener una criptografía cuántica lista, que permita recuperar la privacidad en los procesos de transferencia de información.

La segunda pregunta, que funge como título de esta sección, puede justificarse en función de la respuesta anterior. Si es necesario utilizar modelos de criptografía cuántica para garantizar la privacidad de las comunicaciones, entonces será de vital importancia contar con canales de comunicación que permitan transmitir información cuántica.

Canal cuántico

Al medio capaz de transferir uno o más qubits se le llama canal cuántico. Establecer un canal de este tipo entre Alicia y Beto soluciona su primer problema: ¿cómo transmitir un qubit entre ellos?

Alicia y Beto cuentan con un proveedor de pares de qubits entrelazados, *deus ex machina*. Este proveedor les asegura que cada uno recibirá un qubit perteneciente a un par entrelazado, que es la superposición coherente con igual amplitud de los dos qubits en el estado cero y los dos qubits en el estado uno. Esto significa que si Alicia y Beto realizan la misma medición proyectiva en su respectivo qubit, encontrarán que los dos bit clásicos, resultado de sus mediciones, tendrán el mismo valor. Además, Alicia cuenta con un qubit adicional en un estado cualquiera que desea transferir a Beto; a este qubit se le llamará qubit mensaje.

Para realizar la transferencia, Alicia debe entrelazar el qubit mensaje con su qubit, perteneciente al par distribuido por el proveedor, y asegurarse que la información que contiene se transfiera al qubit de Beto. Esto lo puede lograr mediante dos pasos: una compuerta de negación controlada (CNOT) seguida de una compuerta Hadamard. Una vez realizadas este par de operaciones locales en el laboratorio de Alicia, existe una posibilidad de uno en cuatro que el qubit localizado en el laboratorio de Beto sea igual al qubit mensaje.

Alicia puede realizar una medición proyectiva en su qubit; dicha medición puede resultar en una de cuatro opciones de dos bits clásicos con igual probabilidad de ocurrencia: 00, 01, 10, 11. A cada uno

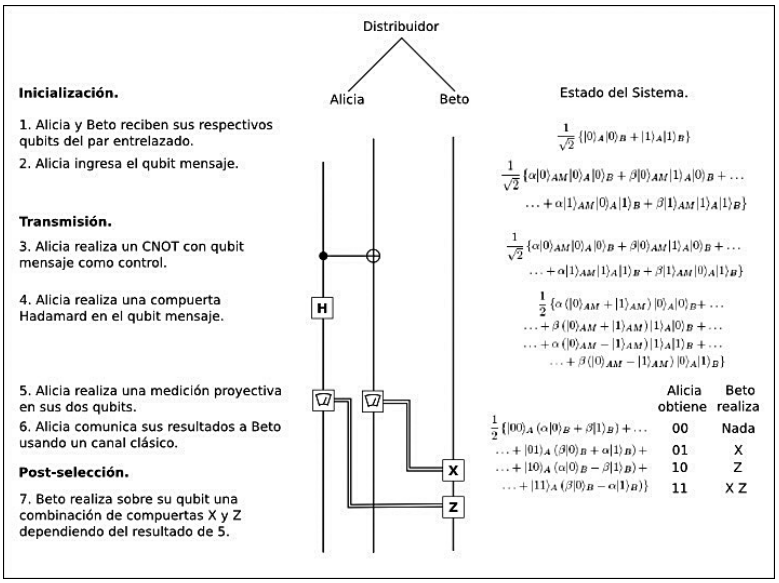

Figura 1. Este esquema muestra los pasos y el circuito cuántico para establecer el protocolo de teletransportación cuántica.

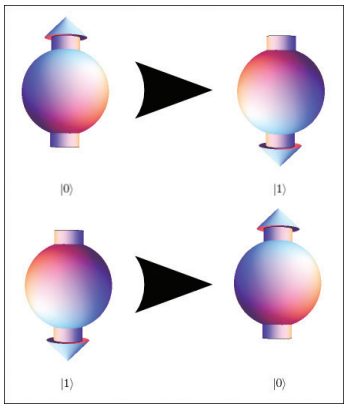

Figura 2. Representación en la esfera de Bloch de un error de tipo cambio de qubit.

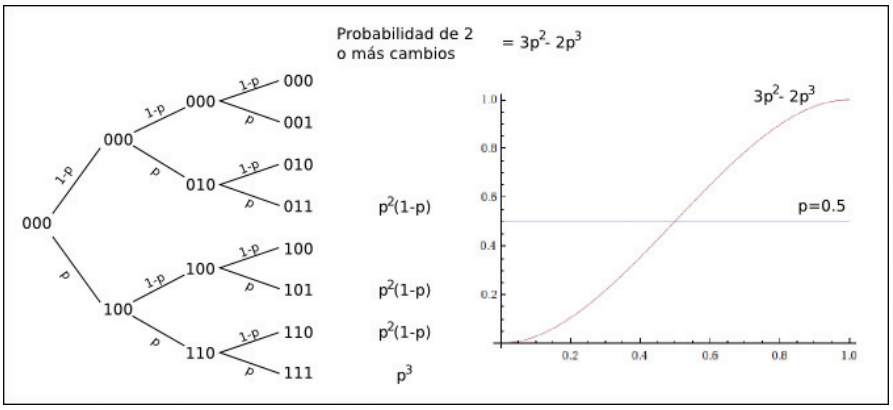

Figura 3. ¿Por qué funciona el cifrado por redundancia en comunicaciones clásicas?

de estos resultados corresponde un estado particular en el qubit de Beto. Por ejemplo, el qubit de Beto es idéntico al qubit mensaje si y sólo si Alicia obtiene como resultado de su medición los bits clásicos 00. Entonces, cuando Alicia obtiene este resultado, puede anunciarle a Beto que tiene el bit correcto utilizando el canal clásico. Esto es efectivo, pero no eficiente.

Para solucionar este problema de optimización, es posible asociar tres conjuntos de operaciones específicas a realizar en el laboratorio de Beto a fin de llevar el estado de su qubit al estado original del qubit mensaje de Alicia. Cada uno de estos conjuntos de operaciones estará relacionado con cada uno de los otros tres resultados restantes, que Alicia puede obtener en su medición proyectiva. De esta forma se asegura que la transmisión del estado del qubit mensaje del laboratorio de Alicia al qubit del laboratorio de Beto se realiza siempre, contando con que Alicia comparta cada vez, utilizando el canal clásico, los dos bits clásicos resultado de las mediciones proyectivas sobre sus dos qubits, y Beto realice las operaciones correspondientes para recuperar el qubit mensaje.

A este protocolo se le conoce como teletransportación cuántica, pues en ningún momento se transfiere un sistema físico de un laboratorio a otro. La información cuántica simplemente es transportada a la distancia utilizando el entrelazamiento que existe en el par de qubits, que originalmente comparten las partes. Cabe resaltar que la información en el qubit mensaje se pierde mientras se transfiere al qubit receptor. El protocolo de teletransportación constituye un canal de comunicación cuántico. Es importante mencionar que el canal cuántico se destruye en el momento en que Alicia realiza sus mediciones proyectivas. Para transmitir un segundo qubit de información es necesario que el proveedor distribuya a Alicia y a Beto un nuevo par de qubits entrelazados, lo cual permite ver al proveedor como un canal cuántico *per se*.

Canal cuántico con ruido

El problema de Alicia y Beto se ha resuelto en teoría. Los primeros contratiempos aparecen con las pruebas del sistema. Ellos deciden probar su canal de comunicación y realizan las mismas mediciones proyectivas en cada uno de sus laboratorios utilizando qubits mensaje bien caracterizados y el canal de comunicación clásico para compartir sus resultados. Alicia y Beto se dan cuenta que los bits clásicos que obtienen como resultado de su prueba, algunas veces no son los correctos. Es más, se dan cuenta que p veces de cada cien los resultados que obtienen son opuestos entre sí; q veces de cada cien el resultado que obtienen es el mismo pero con signo contrario; y pq veces de cada cien obtienen el resultado opuesto y con signo contrario. Estos resultados les hacen concluir que su canal cuántico presenta dos tipos de ruido:

1. Cambio de qubit (*qubit flip*). Los componentes del estado de un qubit se intercambian por el componente ortogonal de la base: el estado cero de un qubit pasa a ser un estado uno y viceversa.
2. Cambio de fase (*phase flip*). Este tipo de ruido corresponde a un cambio de signo en el componente en el estado uno del qubit.

Este par de errores discretos son los modelos ideales de errores que pueden ocurrir en un canal

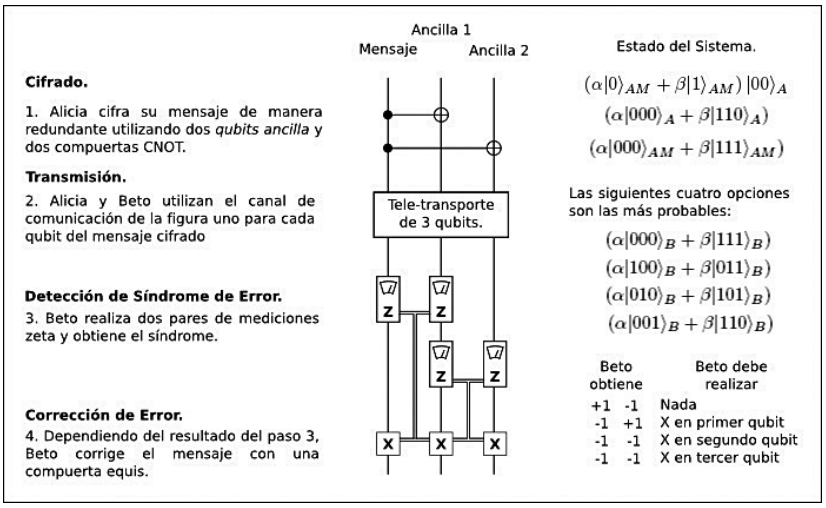

Figura 4. Circuito cuántico para corregir errores de cambio de qubit.

cuántico. Un error real es continuo y corresponde a una rotación aleatoria de un qubit, la cual puede ser tan pequeña que la diferencia entre el qubit original y el qubit con error sea casi imperceptible. Es posible demostrar, aunque queda fuera de los objetivos de este documento, que los métodos de corrección de errores que se presentarán a continuación protegen la información cuántica de rotaciones aleatorias.

Corrección de errores: cambio de qubit

Del par de errores encontrados por Alicia y Beto, el correspondiente a cambio de qubit existe en comunicaciones clásicas. De hecho, recibe un nombre análogo. La forma de corregirlo clásicamente es por redundancia, es decir, cifrar el mensaje original utilizando repetición del bit. Esto es, un bit cero se cifra en un bit lógico que contiene un número impar, al menos tres, de bits cero y un bit uno se cifra en un bit lógico compuesto por el mismo número impar que antes de bits uno.

Tal vez alguno se pregunte ¿por qué se repite el valor de un número impar mayor o igual que tres veces? o ¿qué tan seguro es cifrar por redundancia? El cifrado debe ser una repetición impar para dar lugar a un voto de mayoría. En el caso de redundancia triple, si dos bits del bit lógico son iguales y uno diferente, entonces por mayoría se decide que el bit correcto es el que aparece dos veces y se cambia el valor del bit diferente. Esto sólo se puede hacer cuando el número total de repeticiones es impar, con números pares existe la oportunidad de empate. Si la probabilidad de que ocurra uno y sólo un cambio de bit es menor de 50%, esta forma de cifrado tiene una probabilidad mayor a 50% de un voto de mayoría correcto.

Esta estrategia de corrección de errores puede extenderse al caso de información cuántica. Si la probabilidad de que ocurra un cambio de más de un qubit a la vez es muy pequeña, es posible utilizar un cifrado por repetición, donde Alicia cifre el qubit cero de su mensaje en un qubit lógico 000 y el qubit uno en un qubit lógico 111. Beto debe conocer en qué qubit suceden las cosas para intentar corregir el error, así que es importante conocer las variantes, o síndromes, de error ante el cifrado propuesto. A continuación se enumeran:

0. No pasa nada, no hay error.
1. Hay un cambio de qubit en el primer qubit.
2. Hay un cambio de qubit en el segundo qubit.
3. Hay un cambio de qubit en el tercer qubit.

Beto puede construir cuatro medidas proyectivas que diagnostiquen cada uno de estos síndromes. Cada una de las medidas entregaría un triplete de bits clásicos cero o uno dependiendo si el qubit tiene o no el tipo de error. En caso de que el triplete clásico resultado sea cero, el qubit lógico con el mensaje es destruido; en caso de que el triplete clásico resultado sea uno, el qubit lógico con el mensaje se mantiene igual y es posible corregirlo realizando un cambio de qubit en el qubit correspondiente. Nuevamente, Beto tiene en sus manos una primera estrategia efectiva, más no eficiente.

Es posible construir un par de operaciones de medición que no afecten el qubit lógico mensaje. Esto implica utilizar un medidor cuyos estados propios sean el qubit lógico cero y uno, por ejemplo, una compuerta zeta actuando en uno de los qubits. La compuerta zeta da como resultado un signo positivo, +1, si el estado del qubit es cero, y un signo negativo,

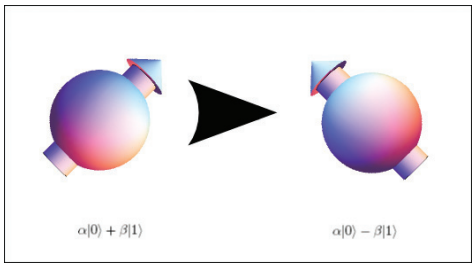

Figura 5. Representación en la esfera de Bloch de un error de tipo cambio de fase.

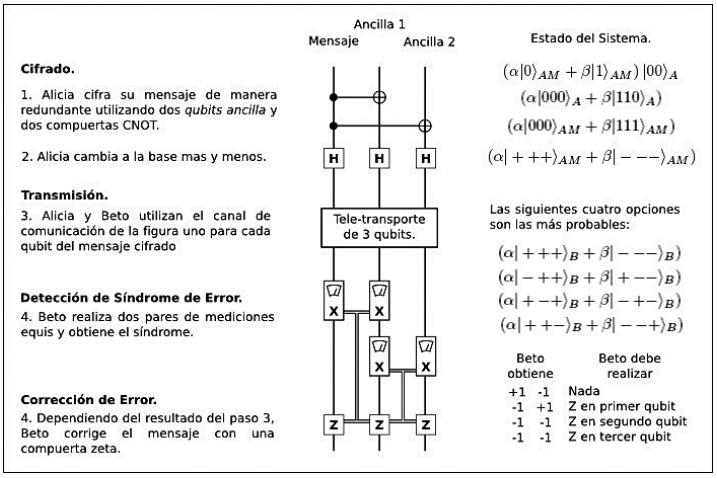

Figura 6. Circuito cuántico para corregir errores de cambio de fase.

-1, si el estado del qubit es uno dejando el qubit en el estado original. Si Beto mide con una compuerta zeta en el primer y segundo qubit del qubit lógico haciendo nada en el tercero, entonces obtendrá un signo positivo, si los dos qubits son iguales, y un signo negativo, si los dos qubits son diferentes. Si después Beto mide con una compuerta zeta en el segundo y tercer qubit del qubit lógico, entonces el resultado de las dos mediciones puede dar cuatro combinaciones:

0. Dos signos positivos. Es muy probable que los tres qubits son iguales, no tiene que corregir nada.
1. Primer signo negativo y segundo positivo. Es muy probable que el primer qubit es el diferente; para corregir, tiene que aplicar una compuerta equis, que realiza un cambio en el primer qubit.
2. Dos signos negativos. Es muy probable que el segundo qubit es el diferente; para corregir, tiene que aplicar una compuerta equis en el segundo qubit.
3. Primer signo positivo y segundo negativo. Es muy probable que el tercer qubit es el diferente y entonces se aplica una compuerta equis en el tercer qubit para corregir.

Ahora Beto tiene una estrategia de corrección del error de cambio de qubit de dos partes: la primer parte le permite diagnosticar, con una alta probabilidad de certeza, el síndrome de error presente en su qubit después de ser transmitido por el canal; en la segunda, según el diagnóstico, Beto puede no hacer nada o aplicar una compuerta equis en uno de los qubits para corregir el probable error.

Corrección de errores: cambio de fase

Por su parte, el cambio de fase no tiene un equivalente clásico. Esto puede hacer pensar que encontrar una estrategia de corrección para este error puede ser más difícil, pero no es así. El cambio de fase es de naturaleza cuántica y, precisamente, es la naturaleza cuántica lo que permite convertirlo en un error de cambio de qubit que ya se conoce y para el cual se tiene una estrategia de corrección.

Alicia puede realizar el cifrado utilizando el qubit lógico más, signo positivo, la superposición del qubit cero y el qubit uno y el qubit lógico menos, signo negativo, la superposición de qubit cero y el qubit uno con signo negativo. Utilizando este código, el error de cambio de fase cambia al qubit lógico más en el qubit

> La criptografía clásica, utilizada actualmente para proteger la información transmitida por los canales de comunicación existentes, se basa en la especulación acerca de la imposibilidad de descomponer eficientemente números enteros grandes en sus factores primos utilizando un algoritmo clásico.

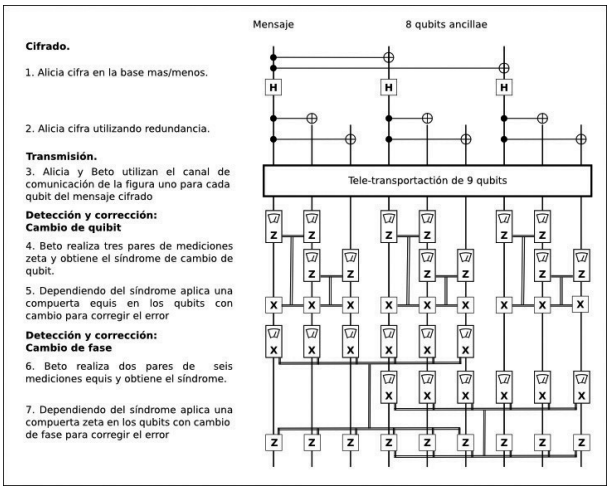

Figura 7. Circuito cuántico para realizar el cifrado de Shor.

lógico menos, y viceversa. Es decir, Alicia convierte un error de cambio de fase en un error de cambio de qubit. Alicia y Beto ya han desarrollado una estrategia para detectar y corregir este error utilizando redundancia. La diferencia con la estrategia previa se encuentra en la forma de diagnosticar el síndrome de error y corregirlo. En este caso, el diagnóstico se realiza utilizando la compuerta equis en el primero y el segundo qubit, y la compuerta equis en el segundo y tercer qubit. El síndrome resultado corresponde con las combinaciones de signo obtenidas anteriormente. La corrección se da aplicando la compuerta zeta en el qubit correspondiente.

Corrección de errores: cifrado de Shor

Es posible utilizar un cifrado combinado para combatir ambos tipos de errores. Primero, es necesario que Alicia cifre su qubit mensaje en la superposición definida para combatir el cambio de fase utilizando tres qubits y realizar un qubit lógico redundante en estados más y menos; después, ella debe cifrar el qubit lógico resultado utilizando el código para cambio de bit replicando el qubit lógico anterior tres veces. Este cifrado entrega un qubit lógico final compuesto por nueve qubits. A este código de cifrado se le conoce como *cifrado de Shor*. Es posible demostrar que dicho cifrado protege contra los efectos de un error arbitrario, pero eso rebasa los fines de este documento.

Así, pues, es altamente probable escapar de los efectos de un error arbitrario en el canal cuántico de comunicación utilizando nueve qubits para cifrar un qubit en un qubit lógico con el cifrado de Shor y realizando un total de seis operaciones zeta en pares –para analizar triadas de qubits y detectar los síndromes de cambios de qubit– y doce operaciones equis, en dos conjuntos de seis –para detectar el síndrome de cambio de fase ocurrido y entregar información a Beto sobre las operaciones que debe realizar para corregir el error introducido por el paso a través del canal.

Conclusiones

Se ha presentado un modelo de juguete de comunicación cuántica entre dos puntos con un protocolo específico de corrección de errores, el cifrado de Shor. Este protocolo permite ejemplificar de manera sencilla las ideas que subyacen en un código de corrección de errores cuántico: cifrado, detección de síndrome y recuperación del mensaje original.

Esto es sólo la punta del iceberg de un campo de investigación que utiliza el análisis funcional y la geometría diferencial como herramientas básicas.[1]

[Notas]

[1] Para personas interesadas en una presentación formal del tema con todas sus implicaciones, es recomendable revisar las siguientes fuentes disponibles de manera gratuita en Internet:
Notas del curso en computación cuántica de John Preskill (CalTech, EUA) en http://www.theory.caltech.edu/people/preskill/ph229/
Tesis doctoral en códigos estabilizadores y corrección de errores cuánticos de Daniel Gottesman bajo la supervisión de John Preskill en http://www.arxiv.org/abs/quant-ph/9705052
Para ampliar la información sobre cifrado cuántico y corrección cuántica de errores, el lector puede consultar, además, las siguientes publicaciones:
Quantum computation and quantum information de Michael Nielsen e Isaac Chuang.
The physics of quantum information, editada por Dirk Bowmeester, Artur Ekert y Anton Zeilinger. En esta última se hacen conexiones con sistemas físicos y sus implementaciones en laboratorio.
Finalmente, está disponible un par de bitácoras digitales, escritas por investigadores que desde hace varios años tratan el tema de la informática cuántica:
The Quantum Pontiff, bitácora de Dave Bacon (U.Washington, EUA):http://scienceblogs.com/pontiff/
Shtetl Optimized, bitácora de Scott Aaronson (MIT, EUA):
http://scottaaronson.com/blog/
Aquí se pueden encontrar comentarios sobre los últimos acontecimientos en las áreas de computación, informática y mecánica cuántica, además de vínculos a las bitácoras digitales de otros investigadores como David Deutsch, Michael Nielsen, Isaac Chuang, entre otros.