Grupo de investigación en Computación Cuántica

Jesús García-López[1]

Resumen

La Teoría de la Información y la Computación Cuántica son áreas nuevas de investigación que prometen un importante avance en computación y dispositivos de tratamiento de la información. La representación físico-cuántica de la información ha permitido definir un nuevo modelo de computación que generaliza las máquinas de Turing tanto deterministas como probabilísticas. La demanda permanentemente creciente de potencia de cálculo en todos los ámbitos sociales ha originado la investigación de dispositivos microelectrónicos cada vez más pequeños, alcanzando eventualmente el límite cuántico. Áreas nuevas como la nanotecnología están alcanzando el punto en el que el control de dispositivos cuánticos se convierte en una necesidad. La Información y Computación Cuántica no sólo facilitará la transición hacia estos dispositivos cuánticos sino que proporciona formas radicalmente nuevas de representar y procesar la información que podrían resolver problemas clásicamente intratables.

En este artículo, además de presentar algunas ideas sobre el estado actual del arte en Computación Cuántica, se pretende dar a conocer el GQC (Group of Quantum Computation), con el objetivo de divulgar sus inquietudes y contactar con otros grupos de investigación en temas afines. El grupo, formado hace poco más de un año, tiene experiencia en campos afines como mecánica cuántica, teoría de la computación y simulación en ordenadores. También ha promovido actividades divulgativas (seminarios, cursos, material didáctico, etc.) sobre Información y Computación Cuántica. Su principal objetivo es la formación de los integrantes del grupo en este área y está especialmente interesado en códigos cuánticos y en la simulación del comportamiento de dispositivos reales en presencia de diferentes fuentes de ruido, áreas en las que el grupo confía aportar algún resultado relevante. Además de estos objetivos se han planificado otros, más exploratorios, como el control de estados cuánticos usando microscopía de campo cercano o el estudio de algoritmos cuánticos.

[1]Dpto. Matemática Aplicada. E.U. Informática. U. Politécnica Madrid. E-mail: jglopez@eui.upm.es

1 Introducción

La teoría de la información y la computación cuántica tienen como objetivo el estudio del tratamiento de la información mediante sistemas cuánticos. Si no ha surgido antes esta idea tan simple y a la vez tan profunda, es porque en este tema concurren muchos campos científicos: mecánica cuántica, computación, teoría de la información y criptografía.

Uno de los primeros resultados de la teoría cuántica de la información, descubierto a principios de los ochenta, es la imposibilidad de copiar estados cuánticos (no-cloning theorem). Es una propiedad que no tiene precedente en la teoría clásica de la información. Surgió al estudiar el uso de efectos cuánticos para transmitir señales a mayor velocidad que la de la luz y ha contribuido a entender mejor algunos aspectos de la mecánica cuántica.

La clave para el desarrollo de la teoría cuántica de la información está en las técnicas, desarrolladas a partir de los años setenta, para controlar sistemas cuánticos simples. Se consiguieron estudiar con gran precisión átomos aislados, confinados en trampas atómicas. Con el microscopio de efecto túnel se construyeron redes diseñadas a priori, colocando los átomos uno a uno. Se construyeron microscopios electrónicos que operaban con electrones individuales, etcétera. El objetivo de toda esta investigación, aparte de las aplicaciones tecnológicas, fue estudiar las leyes de la física en unas condiciones nunca controladas hasta ese momento.

La teoría de la información y la computación cuántica, si aspiran a convertirse en ciencias aplicadas, deben involucrarse plenamente en la consecución de esos objetivos. El resultado de las in-

vestigaciones en dispositivos en este campo, hasta la fecha, ha sido modesto. Pequeños ordenadores cuánticos capaces de realizar unas decenas de operaciones sobre unos pocos qubits (unidades de información cuántica) y prototipos experimentales de criptografía cuántica que podrían aplicarse incluso en aplicaciones reales. Sin embargo, es preciso desarrollar nuevas técnicas que permitan hacer realidad los sistemas de información cuántica y de computación cuántica a gran escala.

Los fundamentos de la computación moderna fueron establecidos por A. M. Turing en 1936, en su famoso artículo *"On computable numbers, with an application to the Entscheidungsproblem"* (Proc. London Math. Soc. 2, 42:230, 1936). Introdujo una definición matemática de ordenador programable, conocido ahora como máquina de Turing. Demostró la existencia de una máquina de Turing universal, capaz de simular cualquier máquina de Turing, y conjeturó que cualquier tarea que se pueda llevar a cabo sobre un dispositivo (por ejemplo un ordenador moderno) también puede realizarse con una máquina de Turing. Este resultado, conocido como tesis de Church-Turing, estableció la base para el espectacular desarrollo de la computación.

Poco después se construyeron los primeros ordenadores electrónicos. John von Neumann desarrolló un modelo teórico que reunía todos los elementos necesarios para poder construir un ordenador tan potente como una Máquina de Turing Universal. El hardware se desarrolló rápidamente a partir del descubrimiento del transistor en 1947, desarrollado por John Bardeen, Walter Brattain y Will Shockley. Desde entonces la potencia de los ordenadores ha crecido sin cesar, hasta tal punto que Gordon Moore en 1965 modelizó este crecimiento con la conocida ley de Moore que originalmente establecía que la potencia de los ordenadores se duplica cada dos años, intervalo que posteriormente tuvo que reducirse a 18 meses.

La ley de Moore se ha cumplido aproximadamente desde 1960. Sin embargo muchos investigadores esperan que esto no sea así en las primeras décadas del siglo XXI. Los efectos cuánticos empiezan a dificultar el funcionamiento de los dispositivos electrónicos a medida que se miniaturizan. Una posible solución al eventual fallo de la ley de Moore consiste en modificar el modelo de computación y una alternativa posible es el modelo cuántico de computación.

El elevado coste computacional del cálculo de la evolución de sistemas cuánticos en ordenadores clásicos hizo pensar a Benioff y Feynman que la evolución de estos sistemas se podría considerar como una herramienta de cálculo más que como un objeto a calcular. Con este planteamiento la ganancia de velocidad, debido al denominado paralelismo cuántico, es tan importante que muchos investigadores creen que el modelo cuántico de computación es más potente que el modelo clásico. Esto contradice la versión fuerte de la tesis de Church-Turing que asegura que *"cualquier proceso algorítmico se puede simular eficientemente en una máquina de Turing"*.

La idea de superar en eficiencia al modelo de computación clásico no es nueva. Muchos equipos de investigación hicieron notar que ciertos tipos de computación analógica pueden resolver eficientemente problemas que no tienen solución eficiente en una máquina de Turing. Desgraciadamente para la computación, consideraciones realistas sobre la presencia de ruido en los ordenadores analógicos hicieron inviable este modelo. For este motivo, uno de los primeros desafíos de la teoría cuántica de la información y de la computación cuántica fue desarrollar las teorías de códigos correctores cuánticos y de computación cuántica tolerante a fallos. A diferencia de lo que ocurrió con la computación analógica, la computación cuántica puede asumir una cantidad finita de ruido manteniendo sus ventajas sobre el modelo clásico.

El mayor reto a la tesis fuerte de Church-Turing apareció en los años setenta cuando Robert Solovay y Volker Strassen demostraron que era posible determinar si un número es primo o compuesto usando un algoritmo aleatorizado. Si el algoritmo determina que el número es compuesto el resultado es correcto pero si determina que el número es primo el resultado es probablemente correcto, con una probabilidad p independiente del número. Aplicando el algoritmo varias veces al mismo número se puede conseguir que la probabilidad de que el resultado sea correcto sea tan grande como se desee. Además, no se conoce ningún algoritmo determinista para resolver eficientemente este problema. Este ejemplo sugiere que existen problemas que se pueden resolver eficientemente con algoritmos aleatorizados y no se pueden resolver eficientemente con máquinas de Turing deterministas.

A la vista de estos hechos se ha generalizado el modelo clásico de computación, sustituyendo la máquina de Turing por una máquina de Turing probabilística. En este modelo la tesis de Church-Turing dice que *"cualquier proceso algorítmico se puede simular eficientemente en una máquina de Turing probabilística"*. Motivado por estas cuestiones, David Deutsch propuso en 1985 utilizar las leyes de la física para obtener versiones todavía más fuertes de la tesis de Church-Turing. En concreto intentó definir un ordenador que fuera capaz de simular eficientemente un sistema físico arbitrario. Esta idea ha conducido a la concepción actual de ordenador cuántico.

En la década de los noventa muchos investigadores desarrollaron las ideas de Benioff, Feynman y Deutsch, culminando en 1994 con la demostración de Peter Shor de que la factorización de números enteros y el cálculo de logaritmos discretos se pueden resolver en tiempo polinomial en un ordenador cuántico. Este resultado es enormemente importante pues supone una ganancia de eficiencia exponencial respecto a los mejores algoritmos clásicos conocidos y parece indicar que la computación cuántica es más potente que las máquinas de Turing, incluso más que las máquinas de Turing probabilísticas. Se encontraron más evidencias de la potencia de la computación cuántica en 1995, año en el que Lov Grover probó que la localización en espacios de búsqueda no dirigida se puede acelerar en un ordenador cuántico. Aunque este resultado no supone una ganancia tan espectacular como la de los algoritmos de Shor atrajo la atención de muchos investigadores por las aplicaciones que tiene y por que establece una diferencia clara con el mejor algoritmo clásico posible.

Exceptuando problemas ad hoc no se conocen más problemas, aparte de los citados anteriormente y sus aplicaciones, que se puedan resolver más eficientemente en computación cuántica que en computación clásica. Preguntas como ¿qué es lo que hace que los ordenadores cuánticos sean más potentes que los clásicos? y ¿qué relación existe entre los conjuntos de problemas que se pueden resolver eficientemente en computación cuántica y en computación clásica respectivamente? son un gran desafío para el futuro.

Los fundamentos de la teoría de la información y la comunicación fueron establecidos por Claude Shannon en 1948. Definió matemáticamente el concepto de información, estableció los requisitos de un canal de comunicación sin ruido (noiseless channel coding theorem) y obtuvo una cota de la cantidad de información que se puede trasmitir a través de un canal de comunicación con ruido (noisy channel coding theorem). Demostró que para poder comunicarse a través de canales con ruido es preciso utilizar códigos correctores, que se desarrollaron posteriormente. Los fundamentos de la teoría cuántica de la información se han establecido de forma similar. En 1995 Ben Schumacher definió la unidad de información cuántica, el qubit, y demostró un teorema análogo al teorema de canales de comunicación sin ruido de Shannon.

Aunque en la teoría cuántica de la información no existe un teorema equivalente al teorema de canales de comunicación con ruido de Shannon, sí se ha desarrollado la teoría de códigos correctores cuánticos. En 1996 Robert Calderbank y Peter Shor e independientemente Andrew Steane descubrieron una importante tipo de códigos cuánticos, ahora conocidos como códigos CSS. Pertenecen a una clase más general de códigos, códigos estabilizadores, descubiertos independientemente por Robert Calderbank, Eric Rains, Peter Shor y Neil Sloane y por Daniel Gottesman.

La comunicación a través de canales cuánticos tiene propiedades importantes. Por ejemplo, la cantidad de información que necesitan intercambiar dos ordenadores que están resolviendo un problema concreto es exponencialmente más pequeña para ordenadores cuánticos que para ordenadores clásicos. Y, si se utiliza un canal cuántico para transmitir información clásica, el cociente entre la cantidad de información clásica trasmitida (información virtual) y la cantidad de información cuántica trasmitida (información real) es 2. Esto se consigue mediante la denominada codificación superdensa.

La imposibilidad de copiar estados cuánticos (no-cloning theorem) permite definir sistemas criptográficos cuánticos cuyas primeras ideas fueron propuestas por Stephen Wiesner a finales de la década de los sesenta. Desgraciadamente su trabajo no se publicó hasta 1983 (*"Conjugate Coding"*, Sigact News, 15, 1, 78-88, (1983)). En 1984 Charles Bennett y Gilles Brassard, basándose en el trabajo de Wiesner propusieron un protocolo cuántico de distribución de claves.

Los sistemas criptográficos de clave pública se empezaron a desarrollar a mediados de la década de los setenta, revolucionando la criptografía. Fueron propuestos independientemente por Whitfield Diffie y Martin Hellman y por Ralph Merkle. Poco más tarde Ronald Rivest, Adi Shamir y Leonard Adleman desarrollaron el sistema criptográfico RSA que en la actualidad es uno de los más extendidos. La seguridad de este sistema, basada en la imposibilidad práctica de factorizar números enteros grandes, se ha esfumado (de momento sólo teóricamente) por la existencia del algoritmo de factorización de Shor. Lo mismo ha ocurrido con otros sistemas criptográficos cuya seguridad se fundamentaba en la imposibilidad práctica de calcular logaritmos discretos.

El hecho de que los algoritmos de Shor hayan roto algunos sistemas criptográficos, en particular el sistema RSA, ha suscitado un enorme interés por la teoría cuántica de la información y por la computación cuántica.

2 Grupo de investigación en Computación Cuántica

El grupo de investigación GQC (Group of Quantum Computation), creado hace poco más de un año, está interesado en una disciplina nueva que, aunque se originó a principios de la década de los ochenta, se ha desarrollado fundamentalmente en los ocho últimos años, a partir del descubrimiento de Shor en 1994 [18]. Fue precisamente este trabajo, en el que P. W. Shor obtiene un algoritmo polinomial para factorizar números enteros en un ordenador cuántico, el que atrajo nuestra atención sobre la computación cuántica.

El primer paso para introducirnos en la computación cuántica consistió en impartir una conferencia en el III Seminario de Matemática Discreta, organizado por la Escuela Universitaria de Informática y la Facultad de Informática de la U. Politécnica de Madrid en el año 2001. En la preparación de esta conferencia pudimos comprobar que muchos de los problemas de computación cuántica se pueden abordar con técnicas matemáticas que van desde la computación clásica a la matemática discreta. Por este motivo pensamos que había posibilidades de obtener resultados de investigación en este campo y nos decidimos a formar un grupo.

La computación cuántica es una área en la que convergen muchas disciplinas por lo que era necesario introducir en el grupo personas de otras áreas, especialmente de física. Con este objetivo establecimos contacto con un profesor de la Facultad de Informática que daba un curso de doctorado sobre este tema que finalmente se integró en nuestro grupo. Además, por mediación de esta persona, se incorporó a nuestro grupo un investigador titular del CSIC. Para consolidar definitivamente el grupo programamos una sección de computación cuántica en el IV Seminario de Matemática Discreta, organizado por la Escuela Universitaria de Informática y la Facultad de Informática de la U. Politécnica de Madrid en el año 2002. En esta sección del seminario abordamos los siguientes temas:

- Introducción a la Computación Cuántica.
- Algoritmo polinómico de factorización de Shor.
- Algoritmos cuánticos de búsqueda.
- El problema del subgrupo escondido.
- Criptografía cuántica.
- Corrección cuántica de errores.
- Implementación de ordenadores cuánticos.

Actualmente el grupo está integrado por nueve personas, ha solicitado un Proyecto de Investigación Científica y Desarrollo Tecnológico en la convocatoria del MCYT del año 2002 y está desarrollando sus primeros trabajos de investigación. Toda la información acerca del grupo se encuentra en la página http://www.dma.eui.upm.es/CompCuant/ y la relación de sus miembros es la siguiente:

Coordinadores:

Jesús García López de Lacalle ($EUI - UPM$)
Vicente Martín Ayuso ($FI - UPM$)

Investigadores:

Gregoria Blanco Viejo ($EUI - UPM$)
José Juan Carreño Carreño ($EUI - UPM$)
José Ángel Martín Gago ($ICMM - CSIC$)
Alfonsa García López ($EUI - UPM$)
Francisco García Mazarío ($EUI - UPM$)
M. Ángeles Martínez Sánchez ($EUI - UPM$)
Julio Setién Villarán ($FI - UPM$)

Los objetivos inmediatos del grupo se centran en el estudio de protocolos de criptografía cuántica, códigos cuánticos y algoritmos cuánticos. En el primero de los puntos estamos analizando la seguridad de los protocolos criptográficos ante ataques con entrelazamiento de qubits y, en el segundo, estamos desarrollando modelos de distribución del error para determinar la eficacia de los códigos correctores y de la computación tolerante a fallos. También tenemos previsto abordar algunos problemas algorítmicos como la obtención de circuitos cuánticos para permutaciones y el estudio de algoritmos polinomiales de factorización con la estrategia de búsqueda de Grover [14]. Desde el punto de vista físico estamos analizando la posibilidad de controlar estados cuánticos con técnicas de microscopía tunel.

En la sección siguiente se enumeran los principales grupos de la red europea de excelencia *Quantum Information Processing and Communication* y algunas de las actividades llevadas a cabo en nuestro país. Finalmente se han incluido en las referencias los trabajos y las recopilaciones más importantes sobre el tema.

3 Grupos europeos de investigación en Computación Cuántica

Los proyectos europeos más importantes en teoría cuántica de la información y computación cuántica constituyen la red QIPC (Quantum Information Processing and Communication, ver http://www.cordis.lu/ist/fetgipc.htm, IST-1999-29064). Se trata de una red de excelencia (Networks of Excellence) del programa FET-IST (Future and Emerging Technologies - Information Society Technologies), amparado por el V Programa Marco de la Unión Europea, que agrupa a 33 universidades y centros tecnológicos y en el que se están desarrollando los siguientes proyectos:

- Atomics Chips For Quantum Information Research (IST-1999-11055).
- Active Teleportation and Entangled State Information Technology (IST-2000-29681).
- Entanglement in Quantum Information Processing and Communication (IST-1999-11053).
- Enabling Technologies for Quantum Information Systems (IST-1999-11594).
- Magnetic Systems as candidates for Quantum Computing Hardware (IST-1999-29110).
- Quantum computation: novel algorithms and their many body implementation (IST-1999-10596).
- Quantum Algorithms and Information Processing (IST-1999-11234).
- Study for the construction of a Quantum Information Processing Device using Doped Fullerenes (IST-1999-11617).
- Quantum Images (IST-2000-26019).
- Quantum Information Processing and transfer with with Single Atoms and Phonons (IST-1999-13021).
- Long Distance Photonic Quantum Communication (IST-1999-10033).
- Quantum information with continuous variables (IST-1999-13071).
- Solid State Sources for Single Photons (IST-1999-10243).
- Single electron source generating individual photons for secure optical communication (IST-2000-26020).
- Semiconductor-Based Implementation of Quantum Information Devices (IST-1999-11311).
- Superconducting Qubits: Quantum Computing with Josephson Junctions (IST-1999-10673).

El programa FET-IST sigue vigente y en estos momentos está abierta su segunda convocatoria de proyectos. Respecto a la participación española en la Universidad de Barcelona hay un grupo consolidado que desarrolla uno de los proyectos europeos mencionados anteriormente: Magnetic Systems as candidates for Quantum Computing Hardware (MAGQIP, IST-1999-29110, ver http://sophia.ecm.ub.es/qi-bcn/).

En España, además del grupo de la Universidad de Barcelona, hay otros investigadores que trabajan y publican artículos en teoría de la información y la computación cuántica y otras universidades que organizan eventos sobre este tema, por ejemplo:

- En la Universidad de Santiago de Compostela se imparten cursos sobre Información Cuántica (ver http://www-fp.usc.es/theory/escuela01/).
- En la Universidad de Oviedo se celebra la International Conference on Quantum Information: Conceptual Foundations, Developments ans Perspectives (ver http://www.unioni.es/Congresos/2001/QI/Welcome.html).

Referencias

[1] D. Aharonov. *Quantum Computation.* Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9812037. (1998).

[2] A. Barenco, T. A. Brun, R. Schak and T. P. Spiller. *Effects of noise on quantum error correction algorithms.* Phys. Rev. A, 56, 1177-1188, (1997).

[3] C. H. Bennett and G. Brassard. *Quantum cryptography: Public key distribution and coin tossing.* Proccedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179, IEEE, New York, 1984.

[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters. *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.* Phys. Rev. Lett., 70, 1895-1898, (1993).

[5] E. Bernstein and U. Vazirani. *Quantum complexity theory.* SIAM J. Comp., 26, 5, 1411-1473, (1997).

[6] A. Cabello. *Bibliographic guide to the foundations of quantum mechanics and quantum information.* Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/0012089, (2001).

[7] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. Sloane. *Quantum error correction and orthogonal geometry.* Phys. Rev. Lett., 78, 405-408, (1997).

[8] A. R. Calderbank and P. W. Shor. *Good quantum error-correcting codes exist.* Phys. Rev. A, 54, 1098-1105, (1996).

[9] I. L. Chuang and Y. Yamamoto. *Simple quantum computer.* Phys. Rev. A, 52, 3489-3496, (1995).

[10] J. I. Cirac and P. Zoller. *Quantum computation with cold trapped ions.* Phys. Rev. Lett., 74, 4091, (1995).

[11] D. G. Cory, A. F. Fahmy and T. F. Havel. *Ensemble quantum computing by NMR spectoscopy.* Proc .Nat. Acad. Sci. USA, 94, 1634-1639, (1997).

[12] D. Deutsch and R. Jozsa. *Rapid solution oj problems by quantum computation.* Proc. Roy. Soc. London A, 439, 553-558, (1992).

[13] A. Galindo and M. A. Martín-Delgado. *Information and Computation: Classical and Quantum Aspects.* Reviews of Modern Physics (to appear). Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/0112105, (2001).

[14] L K. Grover. *Quantum mechanics helps in searching for a needle in a haytack.* Phys. Rev. Lett., 79, 325-328, (1997).

[15] A. Yu Kitaev. *Quantum error correction with imperfect gates.* Quantum Communication, Computing and Measurement, (eds.) Hirota, Holevo and Caves, 181-188, Plenum Press, New York, 1997.

[16] M. A. Nielsen and L. I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press. 2000.

[17] E. Rieffel and W. Polak. *An Introduction to Quantum Computing for Non-Physicists.* Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9809016. (2000).

[18] P. W. Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM J. Comp., 26, 5, 1484-1509, (1997).

[19] P. W. Shor. *Scheme for reducing decoherence in quantum computer memory.* Phys. Rev. A, 52, 2493-2496, (1995).

[20] D. Simon. *On the power of quantum computation.* SIAM J. Comp., 26, 5, 1474-1483, (1997).

[21] A. Steane. *Quantum computing.* Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9708022. (1997).

[22] A. M. Steane. *Error correcting codes in quantum theory.* Phys. Rev. Lett., 77, 793-797, (1996).