XII Seminario de Matemática Discreta

8 - 10 de junio de 2011

Valladolid

Organizadores responsables de la serie de Seminarios de Matemática Discreta:
Jesús García López de Lacalle de la UPM
Gregorio Hernández Peñalver de la UPM
Carlos Marijuán López de la UVa

Entidades colaboradoras:
Dpto. de Matemática Aplicada de la EU de Informática de la UPM
Dpto. de Matemtica Aplicada de la Facultad de Informática de la UPM
Dpto. de Matemática Aplicada de la UVa
ETS de Ingeniería Informática de la UVa
Grupo de Investigación Singacom, GIR de la UVa
Vicerrectorado de Investigación de la UVa
Proyecto i-Math
Junta de Castilla y León

Los organizadores cuentan con la colaboración de un comité científico compuesto por expertos en cada una de las áreas temáticas del encuentro y representantes de las entidades científicas organizadoras:

Comité científico:
Manuel Abellanas Oar (Geometría Computacional, UPM)
Francesc Comellas Padró (Teoría de Grafos, UPC)
Jesús García López de Lacalle (Computación Cuántica, UPM)
Félix Delgado de la Mata (Singacom, UVa)

y de un comité para la organización local de esta edición de 2011 compuesto por investigadores de la Universidad de Valladolid:

Comité organizador local:
Carlos Marijuán López, Departamento de Matemática Aplicada, UVa
Belén Palop del Río, Departamento de Informática, UVa
Miriam Pisonero Pérez, Departamento de Matemática Aplicada, UVa

http://www.infor.uva.es/ b.palop/XII-SMD/Principal.html

XII Seminario de Matemática Discreta

8 - 10 de junio de 2011, Valladolid

El Seminario de Matemática Discreta es una reunión científica dirigida a investigadores en áreas temáticas de Matemática Discreta, básicas para el desarrollo de actividad investigadora en el estratégico sector de las TICs.

Estos encuentros tratan de ofrecer a investigadores del ámbito de la Matemática Discreta la oportunidad de difundir sus resultados de investigación, establecer colaboraciones con otros grupos que desarrollan líneas de investigación afines y potenciar la investigación multidisciplinar, la interrelación entre aspectos teóricos y prácticos, la orientación hacia problemas matemáticos con aplicaciones reales y el desarrollo e innovación tecnológica en las empresas.

El XII Seminario de Matemática Discreta se celebrará en el Aula Alan Turing de la ETS de Ingeniería Informática de la Universidad de Valladolid del 8 al 10 de junio de 2011.

El programa del encuentro se articula alrededor de las siguientes actividades:

- Doce conferencias en áreas temáticas de
  - **Geometría Computacional**,
  - **Teoría de Grafos** y
  - **Computación Cuántica**.

  A cada conferencia se le dedicará una hora de exposición y quince minutos de debate.
- Un curso de iniciación a la investigación en Computación Cuántica con una duración de cuatro horas y media.
- Una sesión final de conclusiones y de planificación de estrategias futuras relativas al propio encuentro.

Las actividades de este seminario se realizarán con arreglo al siguiente programa:

8 de junio	**9 de junio**	**10 de junio**
9:15 Recepción y entrega de documentación **9:30** Apertura		**9:00** Conferencia 9 Antonio Acín Inst. Ciènc. Fotòn.
9:45 Conferencia 1 Ferrán Hurtado UPC	**9:45** Conferencia 5 Oriol Serra UPC	**10:15** Conferencia 10 Vicente Martín UPM
11:00 Conferencia 2 Gregorio Hernández UPM	**11:00** Conferencia 6 Francesc Comellas UPC	**11:30** Pausa café
12:15 Pausa café	**12:15** Pausa café	**12:00** Conferencia 11 Miguel Ángel Martín UCM
12:45 Conferencia 3 Pedro Ramos U. de Alcalá	**12:45** Conferencia 7 Susana López UPC	**13:15** Conferencia 12 David Pérez UCM
14:00 Comida	**14:00** Comida	**14:30** Comida
15:30 Conferencia 4 Rodrigo Silveira UPC	**15:30** Conferencia 8 Carlos Marijuán UVa	**16:30** Curso Computación Cuántica 3 Jesús García, UPM
17:00 Curso Computación Cuántica 1 Jesús García, UPM	**17:00** Curso Computación Cuántica 2 Jesús García, UPM	**18:00** Conclusiones y planificación de estrategias
	21:00 Cena Seminario	**19:00** Clausura

Programa detallado

Miércoles 8 de junio de 2011

9:15 - 9:30 Recepción de participantes y entrega de documentación.

9:30 - 9:45 Apertura.

9:45 - 11:00 Conferencia de Ferrán Hurtado Díaz (UPC)
On a Generalization of Convexity

11:00 - 12:15 Conferencia de Gregorio Hernández Peñalver (UPM)
Soluciones locales a problemas globales en redes geométricas

12:15 - 12:45 Pausa café.

12:45 - 14:00 Conferencia de Pedro Ramos Alonso (U. Alcalá de Henares)
j-facetas en el espacio: cotas y resultados estructurales

14:00 - 15:30 Comida.

15:30 - 16:45 Conferencia de Rodrigo Silveira (UPC)
Terrenos poliedrales imprecisos

17:00 - 18:30 Curso de Jesús García López de Lacalle (UPM)
Computación Cuántica 1: Introducción a la Información Cuántica

Jueves 9 de junio de 2011

9:45 - 11:00 Conferencia de Oriol Serra Albó (UPC)
Generalized Cromatic Numbers

11:00 - 12:15 Conferencia de Francesc Comellas Padró (UPC)
Modeling Topological and Dynamic Aspects of Complex Networks

12:15 - 12:45 Pausa café.

12:45 - 14:00 Conferencia de Susana Clara López Masip (UPC)
The $\bigotimes_h$-Product of Digraphs and its Application to Labelings

14:00 - 15:30 Comida.

15:30 - 16:45 Conferencia de Carlos Marijuán López (UVa)
Improving the PageRank of Local Websites

17:00 - 18:30 Curso de Jesús García López de Lacalle (UPM)
Computación Cuántica 2: Fundamentos de Criptografía Cuántica

21:00 Cena Seminario.

Programa detallado

Viernes 10 de junio de 2011

9:00 - 10:15 Conferencia de Antonio Acín Dal Maschio (ICF)
Quantum Correlations and Device-Independent Quantum Information Processing

10:15 - 11:30 Conferencia de Vicente Martín Ayuso (UPM)
Criptografía Cuántica y redes de comunicaciones

11:30 - 12:00 Pausa café.

12:00 - 13:15 Conferencia de Miguel Ángel Martín Delgado (UCM)
Entanglement Distillation Protocols and Number Theory

13:15 - 14:30 Conferencia de David Pérez García (U. Complutense)
A Quantum Version of Wielandt's Inequality

14:30 - 16:30 Comida.

16:30 - 18:00 Curso de Jesús García López de Lacalle (UPM)
Computación Cuántica 3: Resultados de la Computación Cuántica

18:00 - 19:00 Conclusiones y planificación de estrategias futuras.

19:00 Clausura.

On a Generalization of Convexity

Ferrán Hurtado Díaz

Universitat Politècnica de Catalunya

Abstract: In this talk we introduce a generalized notion of convexity, focusing on dimension two: a bidimensional set is k-convex if every line intersects its interior in at most k connected components. The usual notion of convexity coincides with 1-convexity under this definition. We mostly explore polygons in the plane that have this property. Polygons that are k-convex can be triangulated with fast yet simple algorithms. However, recognizing them in general is a 3SUM-hard problem. We give a characterization of 2-convex polygons, a particularly interesting class, and show how to recognize them in $O(n \log n)$ time, where n is the number of vertices. A description of their shape is given as well, which leads to Erdős-Szekeres type results regarding subconfigurations of their vertex sets. We also introduce the concept of generalized geometric permutations, and show that their number can be exponential in the number of 2-convex objects considered.

We next generalize the notion of transversal k-convexity to finite point sets: A set of n points is considered k-convex if there exists a spanning polygonization such that the corresponding polygon is k-convex. As the main combinatorial result, we show that every point set of size n always contains a subset of $\Omega(\log^2 n)$ points that are in 2-convex position. This bound is tight. From an algorithmic point of view, we can show that 2-convexity of a point set can be decided using a polynomial-time algorithm, while the corresponding problem for a larger degree of convexity becomes NP-complete.

The results we overview have been developed in works with several coauthors: O. Aichholzer, F. Aurenhammer, E. Demaine, T. Hackl, A. Pilz, P.A. Ramos, J. Urrutia, P. Valtr, and B. Vogtenhuber.

Soluciones locales a problemas globales en redes geométricas

Gregorio Hernández Peñalver

Universidad Politécnica de Madrid

Resumen: Las redes de sensores o inalámbricas aparecen por doquier en el mundo actual. En la charla analizaremos algunos problemas sobre este tipo de redes que requieren soluciones locales, es decir, soluciones en las que la decisión en cada nodo se toma sólo en función de la información estrictamente local de la red que posee dicho nodo.

Responderemos a dos preguntas sobre estas cuestiones: ¿cómo se organiza la red de forma local? y ¿cómo se envían mensajes por la red? Estas preguntas corresponden a problemas de diseño de la red y estrategias de ruteo en la red, respectivamente.

Además presentaremos soluciones locales a algunos problemas sobre grafos geométricos, tales como dominación, coloración, etc., y mostraremos problemas para los que no existe ninguna solución local.

j-facetas en el espacio: cotas y resultados estructurales

Pedro Ramos Alonso

Universidad de Alcalá de Henares

Resumen: Sea S un conjunto de puntos en el espacio afín d-dimensional. Un conjunto de d puntos (independientes) es una j-faceta del conjunto si, en uno de los semiespacios abiertos delimitados por el hiperplano que definen, hay exactamente j puntos del conjunto.

El problema de dar cotas para el número de j-facetas que puede tener un conjunto de n puntos es uno de los más importantes, y difíciles, de la geometría discreta. En esta charla haremos un repaso de algunas propiedades conocidas del complejo simplicial formado por las j-facetas, y presentaremos algunos problemas abiertos.

Nos detendremos, en particular, en el "Generalized lower bound theorem" (GLBT) de la teoría de politopos. Dicho teorema es equivalente, via la transformada de Gale, a un teorema sobre conjuntos de puntos que involucra al complejo simplicial formado por las j-facetas. La demostración conocida del GLBT requiere técnicas de geometría algebraica avanzada y nuestro interés es encontrar una demostración puramente combinatoria para el caso de conjuntos de puntos. Para el caso $d = 2$ se conocen varias demostraciones, y presentaremos algún resultado que podría ser un primer paso para una demostración para el caso $d = 3$.

Terrenos poliedrales imprecisos

Rodrigo Ignacio Silveira

Universitat Politècnica de Catalunya

Resumen: Existen gran cantidad de aplicaciones relacionadas con sistemas de información geográfica (GIS) donde se utilizan terrenos poliedrales. Estos brindan una representación discreta de un terreno continuo, a través de puntos (muestras del terreno) que son interpoladas usando una triangulación en el plano.

Numerosos problemas algorítmicos han sido estudiados para terrenos poliedrales. Sin embargo, la asunción tácita de la mayoría de los algoritmos existentes es que los puntos (muestras) sobre los cuales se construye el terreno poliedral se conocen con exactitud. En la práctica esto rara vez es cierto, dado que para obtener los datos sobre esos puntos siempre se utilizan instrumentos de precisión limitada.

En esta charla se presentará un modelo de terreno poliedral en el que los vértices de la triangulación son imprecisos: las coordenadas x e y siguen considerándose exactas, pero la elevación pasa a ser imprecisa, siendo reemplazada por un intervalo continuo de posibles alturas. De esta forma, un terreno impreciso no representa una única superficie, sino un conjunto de infinitas superficies posibles, que contiene al terreno real.

Este modelo da lugar a muchos problemas de optimización sobre el conjunto de superficies representadas por un terreno impreciso. En esta charla se repasarán los problemas más importantes estudiados hasta el momento, como la obtención del terreno más suave, con menos mínimos locales, o el cómputo de cuencas hidrográficas, y se discutirán varios problemas abiertos.

Generalized Cromatic Numbers

Oriol Serra Albó

Universitat Politècnica de Catalunya

Abstract: The chromatic number of a graph is the minimum number of parts in a partition of the vertex set such that every part induces a graph with no edges. The acyclic chromatic number requires in addition that every two parts induce an acyclic graph. In the same way, for a given parameter h, the k-generalized chromatic number requires that every i parts induce a subgraph for which the value of the considered parameter is at most i, for i up to k. Treewidth or treedepth are parameters used in the literature in this context.

On the other hand, the list chromatic number restricts every vertex to belong to a prescribed list of parts. The distance between chromatic numbers and their list counterparts can be arbitrarily large, even within relatively simple classes of graphs. A conjecture by Ohba says that, if the chromatic number is at least half the number of vertices, then the ordinary and list chromatic numbers coincide. Bruce Reed and Benny Sudakov proved a weaker version of the conjecture, when the chromatic number is at least 3/5 the order of the graph, and an asymptotic version of the full conjecture. An extension of this result for the most general version of generalized chromatic numbers will be presented.

Modeling Topological and Dynamic Aspects of Complex Networks

Francesc Comellas Padró

Universitat Politècnica de Catalunya

Resumen: Áreas esenciales en nuestra sociedad como comunicaciones, procesado de información, biomedicina, economía, etc. se caracterizan por la dificultad de su estudio dado que numerosos elementos o unidades están interrelacionados y se influencian mutuamente de forma compleja. A pesar de su ubicuidad y relevancia, el estudio de estos sistemas complejos viene limitado por un escaso avance en el diseño de modelos matemáticos que permitan su comprensión y también la predicción de su evolución dinámica e incluso su manipulación para su optimización.

Una buena aproximación a estos sistemas lo constituye su estudio como redes complejas usando técnicas y avances recientes en teoría de grafos, juntamente con simulaciones por ordenador y tratamientos estadísticos.

En esta última década en la mayoría de los numerosos estudios realizados en este sentido se han abordado principalmente aspectos topológicos. Por ejemplo, se ha visto que el diámetro es bajo (logarítmico con el orden del grafo) o que la distribución de grados sigue a menudo una ley potencial. Estas propiedades pueden relacionarse con una estructura modular jerárquica que está implicada también en los procesos dinámicos y de comunicación que ocurren en los sistemas modelados. Más recientemente el interés se ha centrado en la consideración de técnicas espectrales para tratar estos aspectos. Así, por ejemplo, el espectro laplaciano ofrece información sobre características dinámicas de la red, como la sincronización, difusión de información, etc.

En este sentido, hemos desarrollado recientemente técnicas analíticas que permiten el cálculo exacto del MFPT (tiempo medio de primer paso en un paseo aleatorio) en el caso de familias infinitas de grafos acíclicos autosimilares que modelan redes reales. La técnica se basa en las propiedades recursivas de los grafos y la relación del MFPT con los autovalores de la matriz laplaciana del grafo, con la gran ventaja de que no es preciso la determinación explícita de estos autovalores. Las técnicas espectrales facilitan asimismo el estudio de los árboles generadores de grafos, de relevancia en la caracterización de sus propiedades de comunicación.

En esta charla repasaremos algunos resultados recientes en este contexto.

The $\bigotimes_h$-Product of Digraphs and its Application to Labelings

Susana Clara López Masip

Universitat Politècnica de Catalunya

Resumen: Un etiquetado de un grafo es una asignación de elementos de cierto conjunto (normalmente el de los enteros) a los vértices, a las aristas, o a los vértices y a las aristas del grafo, que cumple ciertas propiedades. En 1967, Rosa introduce los etiquetados graciosos como una manera de atacar la conjetura de Ringel, que afirma que cualquier árbol T de orden p descompone al grafo completo K_{2p+1} en $2p+1$ copias de T. Hoy en día esta conjetura sigue abierta y solo han podido resolverse algunos casos particulares. Los etiquetados graciosos son el origen del área de los etiquetados de grafos y muchos otros etiquetados han surgido y han sido estudiados desde entonces. Entre ellos destacamos, por el número de artículos publicados, los etiquetados armónicos introducidos por Graham y Sloan en 1980. Asimismo destacamos, por sus conexiones con otros tipos, los etiquetados super edge-magic, introducidos en 1998 por Enomoto, Lladó, Nakamigawa y Ringel.

En 2008, Figueroa, Ichishima, Muntaner y Rius definen, para un digrafo D, una familia $\Gamma = \{F_i\}_{i=1}^m$ de digrafos con $V(F_i) = V$ y una función $h : E(D) \longrightarrow \Gamma$, el producto $D \otimes_h \Gamma$ como el digrafo con conjunto de vértices $V(D \bigotimes_h \Gamma) = V(D) \times V$ y conjunto de arcos $((a_1, b_1), (a_2, b_2)) \in E(D \bigotimes_h \Gamma) \Longleftrightarrow (a_1, a_2) \in E(D) \wedge (b_1, b_2) \in E(h(a_1, a_2))$.

Una gran parte de la bibliografía relacionada con los etiquetados se dedica a la construcción de familias de grafos que admiten determinado tipo de etiquetado, pero casi siempre desde un punto de vista local. Se da una asignación de etiquetas y se prueba que cumple la condición del etiquetado elegido. En esta charla trataremos el tema de los etiquetados desde un punto de vista diferente, utilizando el producto de digrafos $\bigotimes_h$ como herramienta clave. Aunque originalmente el uso de este producto se orienta al estudio de los etiquetados super edge-magic, trabajos recientes nos permiten extender su ámbito de aplicación a otros tipos, a la vez que se refuerzan las conexiones entre los distintos tipos de etiquetados. Después de hacer un breve repaso de los etiquetados mencionados e introducir el producto $\bigotimes_h$, con algunos de sus resultados estructurales, nos centraremos en la relación existente entre éste y los diferentes tipos de etiquetados. Terminaremos la charla con algunos resultados de tipo enumerativo y problemas relacionados.

Improving the PageRank of Local Websites

Carlos Marijuán López

Universidad de Valladolid

Abstract: This talk presents our studies on the rearrangement of links from the structure of websites for the purpose of improving the valuation of a page or group of pages as established by a ranking function as Google's PageRank. We build our topological taxonomy starting from unidirectional and bidirectional rooted trees, and up to more complex hierarchical structures as cyclical rooted trees (obtained by closing cycles on bidirectional trees) and PR–digraph rooted trees (digraphs whose condensation digraph is a rooted tree that behave like cyclical rooted trees). We give different modifications on the structure of these trees and its effect on the valuation given by the PageRank function. We derive closed formulas for the PageRank of the root of various types of trees, and establish a hierarchy of these topologies in terms of PageRank. We show that the PageRank of the root of cyclical and PR–digraph trees basically depends on the number of vertices per level and the number of cycles of distinct lengths among levels, and we give a closed vector formula to compute PageRank.

Quantum Correlations and Device-Independent Quantum Information Processing

Antonio Acín Dal Maschio

Institut de Ciènces Fotòniques (Barna)

Abstract: Device-independent quantum information processing aims to provide information protocols whose performance does not require any assumptions about the internal working of the devices used in the protocol. Crucial in the construction of these protocols is the characterization of non-local quantum correlations, that is, those correlations attainable by performing local measurements on quantum states that violate a Bell inequality. In this talk, a method to characterize the set of quantum correlations is first presented. It is then shown how this method can be applied to the construction of device-independent quantum key distribution and randomness generation protocols.

Criptografía Cuántica y redes de comunicaciones

Vicente Martín Ayuso

Universidad Politécnica de Madrid

Resumen: La criptografía cuántica es la primera tecnología derivada de la información cuántica que está siendo comercializada. Como toda tecnología nueva, tiene inconvenientes que pueden retrasar o incluso impedir su implantación. En esta charla haremos un breve repaso de los problemas y desafíos que presenta, para pasar a discutir los trabajos que estamos realizando en el marco de su implementación en redes cuánticas metropolitanas, un entorno mucho más complejo del que se ha utilizado en las pruebas y demostraciones habituales de la criptografía cuántica.

Entanglement Distillation Protocols and Number Theory

Miguel Ángel Martín Delgado

Universidad Complutense de Madrid

Abstract: We show that the analysis of entanglement distillation protocols for qudits of arbitrary dimension D benefits from applying basic concepts from number theory, since the set $\mathbb{Z}_n$ associated to Bell diagonal states is a module rather than a vector space. We find that a partition of $\mathbb{Z}_n$ into divisor classes characterizes the invariant properties of mixed Bell diagonal states under local permutations. We construct a very general class of recursion protocols by means of unitary operations implementing these local permutations. We study these distillation protocols depending on whether we use twirling operations in the intermediate steps or not, and we study them both analitically and numerically with Monte Carlo methods. In the absence of twirling operations, we construct extensions of the quantum privacy algorithms valid for secure communications with qudits of any dimension D. When D is a prime number, we show that distillation protocols are optimal both qualitatively and quantitatively.

A Quantum Version of Wielandt's Inequality

David Pérez García

Universidad Complutense de Madrid

Abstract: In this talk, Wielandt's inequality for classical channels is extended to quantum channels. That is, an upper bound to the number of times a channel must be applied, so that it maps any density operator to one with full rank, is found. Using this bound, dichotomy theorems for the zero–error capacity of quantum channels and for the Matrix Product State (MPS) dimension of ground states of frustration-free Hamiltonians are derived. The obtained inequalities also imply new bounds on the required interaction-range of Hamiltonians with unique MPS ground state.

Curso de Computación Cuántica

Jesús García López de Lacalle

Universidad Politécnica de Madrid

Resumen: La computación cuántica empezó a desarrollarse en la década de los ochenta a raíz de las propuestas de Paul Benioff, David Deutsch y Richard Feynman. En 1982, Benioff y Feynman sugirieron independientemente que, dado el elevado coste computacional del cálculo de la evolución de sistemas cuánticos, la evolución de estos sistemas se podría considerar como una herramienta de cálculo más que como un objeto a calcular. Poco después, en 1985, y también de forma independiente, Deutsch propone la búsqueda de un ordenador que sea capaz de simular eficientemente un sistema físico arbitrario. La conjunción de todas estas ideas ha conducido a la concepción actual de ordenador cuántico.

Cuestionar el sistema de computación clásico, que cuenta con una sólida base teórica y con el aval de infinidad de aplicaciones en todos los ámbitos de la vida cotidiana, sólo tiene sentido si el modelo que se propone como alternativo es potencialmente mejor que el actual. Efectivamente, así lo hacen Benioff, Deutsch y Feynman, fundamentando sus propuestas sobre la posibilidad de que los sistemas cuánticos tengan mayor potencia de cálculo que los clásicos. El argumento que todos utilizan para apuntar esta posibilidad es el hecho de que la simulación de un ordenador cuántico (sistema cuántico) en un ordenador clásico requiere una gran cantidad de operaciones.

El principal método para aumentar la capacidad de cálculo de un ordenador clásico es el procesamiento en paralelo. Los ordenadores que soportan este esquema de programación disponen de varios cientos o miles de procesadores. Sabemos que la capacidad de almacenamiento de información y la capacidad de cálculo de un ordenador son proporcionales al número de celdas de memoria y al número de procesadores respectivamente, es decir, al tamaño del ordenador. Entonces la capacidad de un ordenador clásico (de almacenamiento y de cálculo) crece linealmente con respecto a su tamaño.

En un ordenador cuántico la situación cambia por completo, hasta el punto de que su capacidad crece exponencialmente con respecto a su tamaño. Este hecho, estrechamente relacionado con el principio de superposición de la mecánica cuántica, se denomina paralelismo cuántico. Llamamos qubits o bits cuánticos a los sistemas cuánticos elementales, es decir, a los sistemas cuánticos obtenidos a partir de dos estados. Los

sistemas cuánticos de n qubits se describen mediante vectores de un espacio de Hilbert complejo de dimensión 2^n. Esto permite codificar una cantidad exponencial de información en el estado de un sistema cuántico de n qubits. Además, cualquier transformación del estado del sistema se traduce en la modificación simultánea de toda la información almacenada. Por tanto, la capacidad de un ordenador cuántico (tanto de almacenamiento como de cálculo) crece exponencialmente con respecto a su tamaño.

Sin embargo, la medición de estados cuánticos es un inconveniente importante para la computación cuántica. Hay que recordar que las medidas cuánticas no son deterministas. Esto quiere decir, por ejemplo, que si medimos dos estados iguales los resultados no tienen por qué ser iguales. El proceso de medida es, por tanto, un experimento aleatorio en el que la probabilidad de cada resultado está determinada por el estado del sistema.

Las dificultades para sacar provecho del paralelismo cuántico son tan notables que hubo que esperar más de una década para encontrar el primer gran resultado. En 1994 Peter W. Shor sorprendió a todos presentando sendos algoritmos polinomiales para factorizar números enteros y para calcular logaritmos discretos. Fueron los primeros problemas relevantes en los que se alcanzaba una aceleración exponencial con respecto a los mejores algoritmos clásicos conocidos. A raíz de este descubrimiento se generó una gran actividad, tanto en el desarrollo de la tecnología necesaria para la construcción de ordenadores cuánticos como en el estudio de algoritmos cuánticos.

El algoritmo de Shor rompió teóricamente el sistema criptográfico más difundido en la actualidad, el sistema RSA propuesto por Rivest, Shamir y Adleman en 1978. Este hecho contribuyó a su vez al desarrollo de los sistemas criptográficos cuánticos. Las técnicas que se utilizan para garantizar la confidencialidad de los canales cuánticos se apoyan en una propiedad característica de la mecánica cuántica: los estados cuánticos no se pueden copiar (clonar). En el área de las comunicaciones, además del estudio de la confidencialidad, se están investigando otros problemas como, por ejemplo, la codificación de información clásica en canales cuánticos y el teletransporte de estados cuánticos.

Desde el punto de vista algorítmico, sólo se ha podido hacer efectiva una ganancia exponencial en el cálculo de transformadas de Fourier y, en estos momentos, Esta es la herramienta más importante de la computación cuántica. Otra técnica que permite mejorar la complejidad de algunos algoritmos clásicos, aunque con ganancia solamente cuadrática, es el método de Grover de búsqueda en conjuntos desordenados.