Sesión de Matemática Discreta y Algorítmica
MAT.ES 2005

Manuel Abellanas, Universidad Politécnica de Madrid
Moviendo discos en el plano

Dadas dos configuraciones de n discos disjuntos en el plano, se analiza si es posible transformar una en otra mediante traslaciones, y el número de éstas necesario. El problema consiste en medir la distancia entre dos configuraciones, entendiendo como tal el número de traslaciones necesarias. Este problema se puede considerar como una versión discreta del problema de movimiento de tierras. Un problema de este tipo aparece también al analizar la distancia tipográfica entre dos textos. En este trabajo se presentan distintas versiones del problema con muy diferentes resultados que abarcan desde soluciones algoritmicas eficientes a problemas de naturaleza NP-completa.

Simeon Ball, Universidad Politécnica de Cataluña
Los polinomios de Rédei y aplicaciones a la geometría finita

Un polinomio con coeficientes en un cuerpo finito $GF(q)$ que es el producto de polinomios lineares se llama un *polinomio de Rédei*. Por ejemplo,

$$R(T,S) = \prod_{(x,y)\in\mathcal{A}} (T - xS + y),$$

donde $\mathcal{A}$ es un subconjunto de $GF(q)^2$, es un polinomio de Rédei en dos variables. En el plano afín $AG(2,q)$ el punto (x,y) es incidente con la recta $Y = mX + \alpha$ si y solo si $\alpha = -mx + y$. Por lo tanto α es una raiz de $R(T,m)$ de multiplicidad k si y solo si la recta $Y = mX + \alpha$ es incidente con k puntos del conjunto $\mathcal{A}$. El problema por el cual Rédei introdujo el polinomio $R(T,S)$ fue la clasificación de las funciones sobre un cuerpo finito que determinan pocas direcciones. Es equivalente a hallar las funciones f sobre un cuerpo finito tal que la aplicación

$$x \mapsto f(x) + cx$$

es una permutación de $GF(q)$ para muchos elementos $c \in GF(q)$. Rédei demostró que si $\mathcal{A}$ es un conjunto de q puntos de $AG(2,q)$ que determina menos de $(q+3)/2$ direcciones entonces cada recta que es incidente con más de un punto de $\mathcal{A}$ es incidente con 0 mod p puntos de $\mathcal{A}$. En los ultimos años ha sido demostrado que las funciones que determinan menos de $(q+3)/2$ direcciones son lineares sobre un subcuerpo de $GF(q)$.

Esta conferencia se concentra en el problema en espacios de dimension más grande. Los resultados en el caso planar se pueden utilizar cuando el subconjunto de puntos determina muy pocas direcciones. No obstante, usando polinomios de Rédei con muchas variables, podemos deducir un teorema similar al teorema de Rédei pero en espacios de dimensión más grande que trata de subconjuntos de puntos que determina una cantidad bastante grande de direcciones.

Se expondrá algunos corolarios que tratan de ovoides de los cuadrangulos generalizados $T_2(O)$ y $T_2^*(O)$ y algunas cuestiones que aparecen en el caso de que q sea primo.

Josep Burillo, Universidad Politécnica de Cataluña
Árboles binarios y el grupo F de Thompson

Los grupos de R. Thompson aparecieron en los años 1960 en el estudio de propiedades lógicas y rápidamente ganaron interés con su utilización en la construcción de grupos infinitos simples finitamente presentados. En particular, el grupo F de Thompson ha sido estudiado hasta la saciedad en los últimos años. En esta charla se presentarán las propiedades más importantes de este grupo, su interpretación mediante pares de árboles binarios y la utilización de éstos para obtener propiedades algebraicas y geométricas del grupo.

Jesús García López, Universidad Politécnica de Madrid
Introducción a la algorítmica y criptografía cuánticas

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. Los tres argumentan 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 y proponen para la construcción de ordenadores cuánticos.

En un ordenador cuántico la capacidad de almacenamiento y cálculo crece exponencialmente con respecto a su tamaño. Este hecho, estrechamente relacionado con el principio de superposición de la mecánica cuántica, se denomina paralelismo cuántico. Sin embargo, la medición de estados cuánticos es un inconveniente importante. 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.

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.

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.

Alfredo García Olaverri, Universidad de Zaragoza
Rigidez combinatoria

El problema de rigidez combinatoria en R^d es el de determinar cuando un conjunto de nodos y de conexiones entre ellos (un grafo), al realizarlo en R^d, produce casi seguramente una estructura rígida. Sólo están caracterizados los grafos rígidos en R^2, pero no se conocen algoritmos polinomiales para decidir si un grafo es rígido o no en R^d para $d \geq 3$. Revisamos los conceptos de rigidez de estructuras, matriz de rigidez, rigidez combinatoria, rigidez en dos dimensiones, resultados parciales en $d \geq 3$ dimensiones y grafos redundantemente rígidos.

Alberto Márquez, Universidad de Sevilla
Grafos que son el borde de un mosaico

Tratamos de estudiar algunas de las relaciones existentes entre los mosaicos planos y los grafos. Más concretamente: dado un mosaico del plano, podemos considerar el borde de dicho mosaico como un grafo al que llamaremos grafo mosaico. El principal objetivo de esta charla es probar que se pueden caracterizar los grafos mosaicos, demostrando que todo grafo mosaico debe contener forzosamente a uno entre dos grafos obligatorios. Dicha demostración conlleva realizar un repaso a muchos de los conceptos fundamentales de la teoría de grafos topológicos.

Edgar Martínez-Moro, Universidad de Valladolid
Semisimple algebras and codes:* another turn of the screw *to cyclic codes

We study those codes defined as subalgebras of a semisimple algebra and derive some basic properties of their structure. We show how to compute a Groebner basis associated to such algebra and how to use it for deriving properties of the code and also decoding. This is a preliminar report on constructive study of those ideas on generalizations on cyclic codes by means of trivial results from Commutative Algebra.

Carlos Munuera, Universidad de Valladolid
Códigos correctores de errores

Uno de los principales problemas en la gestión y tratamiento de la información digital es el de los errores que aparecen en su manipulación. Para solucionarlo ha surgido una nueva rama de las matematicas: la teoria de códigos correctores de errores. En esta charla describiremos de manera informal sus propósitos, las herramientas y metodos que utiliza y su evolución desde sus orígenes hasta la actualidad.

Marc Noy, Universidad Politécnica de Cataluña
Enumeración asintótica y leyes límite de grafos planos

Sea G_n el número de grafos planos etiquetados con n vértices. En este trabajo probamos la estimación asintótica $G_n \sim cn^{-7/2}\gamma^n n!$, donde $\gamma = 27.2268777\cdots$ es una constante computable analíticamente. Como consecuencia, demostramos una conjectura de McDiarmid, Steger y Welsh sobre el número de vértices aislados en grafos planos aleatorios. Hallamos también leyes límite para el número de aristas (ley gaussiana) y para el número de componentes (ley de Poisson) en grafos planos aleatorios. En particular, demostramos que el número esperado de aristas es asintóticamente igual a μn para una constante μ calculable, y también que el número de aristas está concentrado alrededor del valor esperado.

Las demostraciones están basadas en la enumeración de grafos planos 2-conexos obtenida por Bender, Gao y Wormald, y en el análisis de singularidades de funciones generatrices.

Julian Pfeifle, Universidad de Barcelona
Coeficientes y raíces de polinomios de Ehrhart

Dado un politopo P cuyos vértices tienen todos coordenadas enteras, consideramos el número de puntos de la malla Z^n contenidos en la familia $\{kP : k \in N\}$ de sucesivas dilataciones de P. Es un resultado fundamental de Eugène Ehrhart que la función que asigna a cada k el número de puntos de Z^n en kP es un polinomio en la variable k.

En la conferencia hablaremos sobre qué tipo de información sobre el politopo P se puede extraer de la representación de este polinomio en diferentes bases, y daremos cotas para la ubicación

de los ceros complejos y reales de todos los polinomios de Ehrhart. Finalmente discutiremos los polinomios de Ehrhart de tetraedros de retícula con pocos puntos interiores.

Francisco Santos, Universidad de Cantabria
Pseudo-triangulaciones, grafos planos y rigidez

Las llamadas pseudo-triangulaciones de polígonos o de conjuntos de puntos en el plano generalizan a las triangulaciones, estudiadas profusamente en Geometría Computacional desde hace más de 25 años. Fueron propuestas a mediados de los 90 como objetos más fáciles de construir y, sobre todo, de mantener en un entorno dinámico, y casi tan buenas como las triangulaciones como objeto auxiliar en varios contextos algorítmicos (localización, visibilidad, trazado de rayos, etc).

Pero a partir del año 2000 el estudio de las pseudo-triangulaciones cobró nueva fuerza, debido sobre todo a que Ileana Streinu descubrió ciertas relaciones entre ellas y la teoría de la rigidez de grafos en el plano. Estas relaciones han sido exploradas desde entonces por varios autores, entre ellos el que suscribe, y llevan por ejemplo a resultados como el que sigue:

Teorema (Orden-Santos-Servatius-Servatius): Sea G un grafo finito. Son equivalentes: (a) G es plano y genéricamente rígido en el plano. (b) G puede ser dibujado como una pseudo-triangulación de un conjunto de puntos en posición general en el plano.

En esta charla se dará una introducción a los tres temas que conforman el título (planaridad de grafos, rigidez y pseudo-triangulaciones) y se hará un repaso de los resultados que los relacionan.