SESIONES ESPECIALES

Congreso RSME 2013

S4
Matemática Discreta

Jue 24, 17:00 - 18:00, Aula 3 – Gabor Lugosi:
Sobre la conectividad de algunos grafos aleatorios geométricos

Jue 24, 18:00 - 18:30, Aula 3 – José Ramón Portillo:
Grafos para la Mecánica Cuántica

Jue 24, 18:30 - 19:00, Aula 3 – Ignasi Sau:
Optimal Erdös-Pósa property for pumpkins

Jue 24, 19:00 - 19:30, Aula 3 – Juan Tena:
Curvas elípticas con $j = 0, 1728$ *y grado de inmersión pequeño*

Vie 25, 11:00 - 12:00, Aula 3 – María Angeles Hernández Cifre:
The Wills functional in the Geometry of Numbers

Vie 25, 12:00 - 12:30, Aula 3 – Sergio Cabello:
The Clique Problem in Ray Intersection Graphs

Vie 25, 12:30 - 13:00, Aula 3 – David Orden:
On the Fiedler value of large planar graphs

Vie 25, 13:00 - 13:30, Aula 3 – Pablo Soberón:
Particiones balanceadas de medidas en $\mathbb{R}^d$

Vie 25, 17:00 - 18:00, Aula 3 – Javier Cilleruelo:
Sucesiones de Sidon infinitas

Vie 25, 18:00 - 18:30, Aula 3 – Albert Atserias:
Semi-Algebraic Constraints, Gaussian Elimination, and Short Proofs of Unsatisfiability

Vie 25, 18:30 - 19:00, Aula 3 – Anna Lladó:
Algunas conjeturas sobre descomposiciones de grafos

Vie 25, 19:00 - 19:30, Aula 3 – Lander Ramos:
Núcleos planos aleatorios

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Sobre la conectividad de algunos grafos aleatorios geométricos

Nicolas Broutin[1], **Luc Devroye**[2], **Nicolas Fraiman**[2], **Gábor Lugosi**[3]

En esta charla se estudian las propiedades de conectividad del siguiente modelo de grafos aleatorios geométricos, denominados “redes de irrigación” o “grafos Bluetooth”. El grafo depende de dos parámetros: $r > 0$ y el número entero positivo c. Los vértices del grafo están representados por n puntos aleatorios distribuidos uniformemente en $[0, 1]^d$. Primero se forma un grafo aleatorio geométrico conectando los pares de puntos cuya distancia es menor que r. En el segundo paso de construcción cada vértice elije c de sus vecinos al azar, así se forman las aristas del grafo. Presentamos varias condiciones sobre los valores de los parámetros r y c que garantizan la conectividad del grafo con alta probabilidad.

Keywords: grafos aleatorios geométricos, conectividad

MSC 2010: 05C80

[1]INRIA París, Francia
`Nicolas.Broutin@inria.fr`

[2]School of Computer Science
McGill University
Montreal, Canada
`luc@cs.mcgill.ca, fraiman@math.mcgill.ca`

[3]ICREA y Universidad Pompeu Fabra
Barcelona
`gabor.lugosi@upf.edu`

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Grafos para la Mecánica Cuántica

José Ra. Portillo Fernández[1]

En este trabajo presentamos algunas aplicaciones de la Teoría de Grafos a la Mecánica Cuántica tales como entrelazamiento de estados–grafo [1] y correlaciones contextuales [2]. Para ello se hace uso de distintos parámetros numéricos (número de independencia, ϑ de Lovász, número de Rosenfeld, número de intersección, rango ortogonal y número e índice cromáticos, entre otros) exponiendo el significado de estos en relación con los valores máximos de correlación clásicos, cuánticos y genéricos en un experimento y las dimensiones mínimas de los espacios asociados al mismo. Finalmente expondremos una aplicación de ambas disciplinas al estudio de las redes sociales [3].

Keywords: Teoría de grafos, Mecánica cuántica

MSC 2010: 05C17, 05C62, 05C69, 05C72, 05C76, 81P13, 81P15, 81P40, 81Q99, 91D30, 81-05

Referencias

[1] A. Cabello, L. E. Danielsen, A. López-Tarrida y J.R. Portillo, Optimal preparation of graph states. *Physical Review A* **84**(4)042314, (2011).

[2] E. Amselem, L.E. Danielsen, A. López-Tarrida, M. Bourennane, J.R. Portillo y A. Cabello., Experimental fully contextual correlations. *Physical Review Letters* **108**(200405), (2012).

[3] A. Cabello, L. E. Danielsen, A. J. López-Tárrida, and José R. Portillo., Quantum Social Networks. *J. Phys. A: Math. Theor* **45**(285101), (2012).

[1]Matemática Aplicada 1
Universidad de Sevilla
E.T.S. Ing. Informática. Desp. B2-60
Avda Reina Mercedes s/n
41012 Sevilla
josera@us.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Optimal Erdős-Pósa property for pumpkins

Samuel Fiorini[1], **Gwenaël Joret**[2] and **Ignasi Sau**[3]

A class of graphs $\mathcal{H}$ satisfies the *Erdős-Pósa property* if there exists a function f such that, for every integer k and every graph G, either G contains k vertex-disjoint subgraphs each isomorphic to a graph in $\mathcal{H}$, or there is a set $S \subseteq V(G)$ of at most $f(k)$ vertices such that $G \setminus S$ has no subgraph in $\mathcal{H}$. Erdős and Pósa [2] proved that the set of all cycles satisfies this property with $f(k) = O(k \log k)$. Given a connected graph H, let $\mathcal{M}(H)$ be the class of graphs that can be contracted to H. Robertson and Seymour [5] proved that $\mathcal{M}(H)$ satisfies the Erdős-Pósa property if and only if H is planar. The best general upper bound for the function f is super-exponential [1], so it is interesting to find a smaller function for particular cases of the planar graph H. The *c-pumpkin* is the graph with two vertices linked by $c \geq 1$ parallel edges, and can be seen as a natural generalization of a cycle. Very recently, Fomin *et al*. [4] proved that the graphs that can be contracted to the c-pumpkin satisfy the Erdős-Pósa property with $f(k) = O(k^2)$. Using completely independent techniques, we improve this function to $f(k) = O(k \log k)$, which is asymptotically optimal [2, 3].

Keywords: Erdős-Pósa property; packing and covering; planar graphs; graph minors.

MSC 2010: 05C70, 05C83.

References

[1] R. DIESTEL, *Graph Theory*. volume 173. Springer-Verlag, 2005.

[2] P. ERDŐS; L. PÓSA, On independent circuits contained in a graph. *Canadian Journal of Mathematics* **17**, 347–352 (1965).

[3] S. FIORINI; G. JORET; D. R. WOOD, Excluded forest minors and the Erdős-Pósa property. Manuscript available at `http://arxiv.org/abs/1204.5192` (2012).

[4] F. V. FOMIN; D. LOKSHTANOV; N. MISRA; G. PHILIP; S. SAURABH, Quadratic Upper Bounds on the Erdős-Pósa property property for a generalization of Packing and Covering cycles. Manuscript available at `http://neeldhara.com/content/02-publications/FominLMPS2012.pdf` , to appear in *Journal of Graph Theory* (2012).

[5] N. ROBERTSON; P. D. SEYMOUR, Graph Minors. V. Excluding a Planar Graph. *Journal of Combinatorial Theory, Series B* **41**(1), 92–114 (1986).

[1]Département de Mathématique
Université Libre de Bruxelles
Brussels, Belgium
sfiorini@ulb.ac.be

[2]Département d'Informatique
Université Libre de Bruxelles
Brussels, Belgium
gjoret@ulb.ac.be

[3]AlGCo project-team
CNRS, LIRMM
Montpellier, France
sau@lirmm.fr

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Curvas elípticas con $j = 0, 1728$ y grado de inmersión pequeño

Juan Tena Ayuso[1]

Sea E una curva elíptica definida sobre un cuerpo finito F_q, y sea l el máximo orden de un subgrupo cíclico $< P >$ de orden primo (y diferente de la característica del cuerpo) de $E(F_q)$. Se denomina grado de inmersión de E al mínimo entero natural k para el que se verifica una de las condiciones equivalentes siguientes:

1. $l | q^k - 1$
2. $F^*_{q^k}$ contiene un subgrupo cíclico de orden l.

Los sistemas criptográficos basados en el problema del logaritmo discreto sobre curvas elípticas con k pequeño son vulnerables (ataques MOV y FR), por lo que son desaconsejables para la implementación de tales sistemas. Sin embargo curvas con grado de inmersión pequeño son necesarias para la Criptografía basada en pairings. Las curvas elípticas supersingulares tienen grados de inmersión $k = 1, 2, 3, 4, 6$ mientras las ordinarias tienen, en general, grado muy grande.

Aplicación distorsión para un punto $P \in E(F_q)$ (generalmente de orden l, máximo divisor primo del orden de E) es un endomorfismo σ de E, definido sobre F_{q^k}, tal que los puntos $P, \sigma(P)$ son linealmente independientes (lo que implica que $e(P, \sigma(P)) \neq 1$ (donde e denota el pairing de Weil), condición deseable en la Criptografía basada en dicho pairing. Las curvas supersingulares admiten siempre una tal aplicación distorsión mientras que las curvas elípticas ordinarias solo la admiten cuando $k = 1$ y $E(F_q)$ contiene todos los puntos de l-torsión de E.

Se clasifican todas las curvas elípticas supersingulares con $j = 0, 1728$ definidas sobre un cuerpo finito F_q y se explicita en cada caso su grado de inmersión y una aplicación distorsión. Asimismo se muestran algunos casos de curvas ordinarias con tal invariante j y grado de inmersión pequeño y, en su caso, una aplicación distorsión.

Keywords: elliptic curves, j-invariant, pairings, embedding degree, distortion map

MSC 2010: 14H52; 94A60; 14G50

[1]Departamento de Algebra, Análisis Matemático, Geometría y Topología
Universidad de Valladolid
Facultad de Ciencias, Paseo de Belén 7, 47011 Valladolid
tena@agt.uva.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

The Wills functional in the Geometry of Numbers

María A. Hernández Cifre
(joint work with Jesús Yepes Nicolás) [1]

In 1973, J. M. Wills introduced and studied the functional

$$W(\lambda K) = \sum_{i=0}^{n} \mathrm{V}_i(K)\lambda^i$$

for a convex body K (compact and convex set) of the n-dimensional Euclidean space. Here, $\mathrm{V}_i(K)$ represents the so-called *i-th intrinsic volume* of K, i.e., the $(n-i)$-th coefficient (up to a constant) of the Steiner polynomial which is obtained when the volume $\mathrm{vol}(K + \lambda B_n)$ is computed. Wills was mainly interested in its possible relation with the lattice-point enumerator of K, $G(K) = \#(K \cap \mathbb{Z}^n)$, and conjectured that $G(K) \leq W(K)$ for any convex body K. (Un)fortunately, it turned out to be not always true, which has led to an increasing interest in this problem.

In this talk I will present a brief survey on the classical results on this topic, showing families of convex bodies for which the above conjecture holds as well as counterexamples. Then I will focus mainly in the geometric properties of the roots of the Wills functional, when it is considered as a formal polynomial in a complex variable. Its roots turn out to be closely related with another important concept in Discrete Geometry: the successive minima of a convex body with respect to a lattice.

[1]Departamento de Matemáticas,
Universidad de Murcia,
Campus de Espinardo, 30100-Murcia, Spain
mhcifre@um.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

The Clique Problem in Ray Intersection Graphs

Sergio Cabello[1], **Jean Cardinal**[2], **Stefan Langerman**[2]

Ray intersection graphs are intersection graphs of rays, or halflines, in the plane. We show that any planar graph has an even subdivision whose complement is a ray intersection graph. The construction can be done in polynomial time and implies that finding a maximum clique in a segment intersection graph is NP-hard. This solves a 21-year old open problem posed by Kratochvíl and Nešetřil.

Keywords: Intersection graph, segment graph, planar graph, even subdivision

MSC 2010: 05C62, 68Q17

[1]Department of Mathematics, FMF
University of Ljubljana
Ljubljana, Slovenia
`sergio.cabello@fmf.uni-lj.si`

[2]Computer Science Department
Université Libre de Bruxelles (ULB)
Brussels, Belgium
`{jcardin,slanger}@ulb.ac.be`

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

On the Fiedler value of large planar graphs

Lali Barrière[1]
Clemens Huemer[1]
Dieter Mitsche[1]
David Orden[2]

The Fiedler value λ_2, also known as algebraic connectivity, is the second smallest Laplacian eigenvalue of a graph. We study the maximum Fiedler value among all planar graphs G with n vertices, denoted by $\lambda_{2\max}$, and we show the bounds $2 + \Theta(\frac{1}{n^2}) \leq \lambda_{2\max} \leq 2 + O(\frac{1}{n})$. We also provide bounds on the maximum Fiedler value for the following classes of planar graphs: Bipartite planar graphs, bipartite planar graphs with minimum vertex degree 3, and outerplanar graphs. Furthermore, we derive almost tight bounds on $\lambda_{2\max}$ for two more classes of graphs, those of bounded genus and K_h-minor-free graphs.

Keywords: Fiedler value, algebraic connectivity, Laplacian matrix, planar graph, bounded-genus graph, minor-free graph.

MSC 2010: 05C50

[1]Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
{lali,clemens,dieter.mitsche}@ma4.upc.edu

[2]Departamento de Física y Matemáticas
Universidad de Alcalá
david.orden@uah.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Particiones balanceadas de medidas en $\mathbb{R}^d$

Pablo Soberón[1]

En esta plática hablaremos sobre una generalización de un teorema clásico de Stone-Tukey [1] (conocido comunmente como el teorema del sándwich de jamón). Dado un entero positivo k y d medidas de probabilidad "buenas" $\mu_1, \mu_2, \ldots, \mu_d$ en $\mathbb{R}^d$, demostraremos que es posible partir $\mathbb{R}^d$ en k conjuntos convexos $C_1, C_2, \ldots, C_k$ de tal forma que $\mu_i(C_j) = \frac{1}{k}$ para todo i y todo j. El caso $k = 2$ es el teorema del sándwich de jamón.

Keywords: Conjuntos convexos, Particiones de medidas, Borsuk-Ulam

MSC 2010: 52A38, 28A75

Referencias

[1] A.H. STONES; J.W. TUKEY, Generalized "sandwich" theorems. *Duke Mathematical Journal* **9**(2),356–359 (1942).

[1]Department of Mathematics
University College London
Gower Street, WC1E 6BT London
pablo.soberon@ciencias.unam.mx

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Sucesiones de Sidon infinitas

Javier Cilleruelo[1]

S. Sidon preguntó a Erdős en 1932 sobre el crecimiento de sucesiones de enteros positivos con la propiedad de que todas las sumas de dos elementos de la sucesión son distintas. Erdős, que celebraría este año su centenario, llamó sucesiones de Sidon a estas sucesiones y fueron un tema recurrente en su investigación hasta que nos abandonase en busca de "El Libro".

El crecimiento de una sucesión infinita A se mide por el tamaño de su función contadora $A(x) = |A \cap [1, x]|$. Erdős observó que la sucesión avariciosa (se empieza en 1 y cada término se define como el menor que se puede añadir a la sucesión que no viole la condición de ser de Sidon) satisface que $A(x) > x^{1/3}$. Esta sucesión fue la más densa conocida hasta que Ajtai, Komlos y Szemeredi [1] demostraron en 1981 la existencia de una sucesión infinita con función contadora $A(x) \gg (x \log x)^{1/3}$. En 1998 I. Ruzsa [3] sorprendió a la comunidad matemática demostrando la existencia de una sucesión de Sidon con $A(x) \gg x^{\sqrt{2}-1+o(1)}$. Tanto la construcción de Ruzsa como la de Szemeredi y sus colaboradores son construcciones probabilísticas, no explícitas.

En esta charla presentamos la primera construcción explícita de una sucesión infinita de Sidon densa [2]. El crecimiento de esta sucesión es, de hecho, similar al de la sucesión de Ruzsa. Nuestra construcción utiliza un nuevo método, que explicaremos en detalle, basado en el logaritmo discreto. Este método se generaliza bien a las sucesiones B_h, aquellas con la propiedad de que todas las sumas de h elementos de la sucesión son distintas. En particular demostramos, para todo $h \geq 3$, la existencia de una sucesión B_h con función contadora $A(x) \gg x^{\sqrt{(h-1)^2+1}-(h-1)+o(1)}$.

Keywords: Sidon sequences, Discrete logarithm

MSC 2010: 11B13, 05B10

Referencias

[1] M. Ajtai, J. Komlós, and E. Szemerédi, A dense infinite Sidon sequence, *European J. Combin.* **2**, 1–11 (1981)

[2] J. Cilleruelo, Infinite Sidon sequences, *preprint.* Arxiv.

[3] I. Ruzsa, An infinite Sidon sequence, *J. Number Theory* **68** (1) 63-71 (1998).

[1]Departamento de Matemáticas y Instituto de Ciencias Matemáticas (ICMAT)
Universidad Autónoma de Madrid
28049-Madrid
franciscojavier.cilleruelo@uam.es

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Semi-Algebraic Constraints, Gaussian Elimination, and Short Proofs of Unsatisfiability

Albert Atserias[1]

Despite impressive recent progress in obtaining conditional complexity-theoretic results, one of the big remaining mysteries is why semi-definite programming appears to be the optimal polynomial-time algorithm for approximating constraint satisfaction problems (CSPs). The lack of a complete understanding is illustrated by the fact that a small generalization of semi-definite programming, the low-degree sum-of-squares method, remains still a candidate algorithm that could beat the UG-optimal Goemans-Williamson bound for max-cut. This raises the obvious question: how powerful low-degree sum-of-squares methods, or more generally low-degree semi-algebraic proofs, really are? A first observation we offer is that low-degree semi-algebraic dag-like proofs, unlike their tree-like versions, are able to simulate both Gaussian elimination over prime fields and bounded-width constraint propagation. Time permiting, we put the question in the more general context of characterizing which CSPs have polynomial-size proofs of unsatisfiability in a given proof system.

Keywords: Constraint satisfaction problem, semi-definite programming, maximum cut

MSC 2010: 68Q17 Computational difficulty of problems, 05C85 Graph algorithms

[1]Department de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya
Jordi Girona Salgado 1-3, 08034 Barcelona
atserias@lsi.upc.edu

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Algunas conjeturas sobre descomposiciones de grafos

Anna Lladó[1]

El objeto de la charla es describir algunos avances recientes en conjeturas sobre descomposiciones de grafos que llevan cerca de medio siglo abiertas. La conjetura de Ringel, de 1967, dice que las aristas de un grafo completo de orden impar $2m+1$ se pueden descomponer en copias isomorfas de un árbol arbitrario de m aristas. Una versión bipartita fué formulada en 1983 por Graham y Haggkvist, en el sentido que las aristas del grafo bipartito completo $K_{m,m}$ se pueden descomponer en copias isomorfas de un árbol dado de m aristas.

Ambas conjeturas estan verificadas para clases sencillas de árboles, como caminos, árboles de diàmetro a lo sumo 5 y otras variedades. Por otra parte se consideran resultados aproximados sobre el tamaño mínimo de un grafo completo que admite una descomposición en copias isomorfas de cualquier árbol de m aristas, o el menor árbol en el que se puede sumergir un árbol dado para obtener la descomposición deseada. La aplicación del llamado *método polinomial* de Alon [1] permite obtener este tipo de resultados aproximados a ambas conjeturas [2]. En algunas de estas aplicaciones se requiere que el número de aristas del árbol sea un número primo. Para el caso general se pueden utilizar métodos puramente combinatorios [3] que, aunque algo más débiles, permiten obtener resultados como el siguiente [4]: asintóticamente con alta probabilidad, un árbol de m aristas descompone las aristas del grafo completo $K_{2m,2m}$ y del grafo completo K_{cm^2} para cierta constante absoluta c. Las cotas menores conocidas hasta la fecha requieren órdenes del tipo K_{cm^2,cm^2} y K_{cm^3}.

Keywords: Descomposiciones de grafos, conjetura de Ringel, conjetura de Graham-Häggkvist

MSC 2010: 05C51

Referencias

[1] N. ALON, Combinatorial Nullstellensatz. *Combinatorics, Probability and Computing* **8** (1999), 7–29.

[2] M. CÀMARA, A. LLADÓ, J. MORAGAS, On a conjecture of Graham and Haggkvist with the polynomial method. *European J. Combin.* 30 (7) (2009), 1585–1592.

[3] R. L. HÄGGKVIST, Decompositions of Complete Bipartite Graphs. *Surveys in Combinatorics*, Johannes Siemons Ed., Cambridge University Press (1989), 115–146.

[4] A. LLADÓ, Almost every tree with n edges decomposes $K_{2n,2n}$. *Electronic Notes in Discrete Mathematics* 38 (2011), 571–574.

[1]Departament de matemàtica aplicada 4
Universitat Politècnica de Catalunya
Jordi Girona, 1 , 08034 Barcelona
`allado@ma4.upc.edu`

Congreso de la Real Sociedad Matemática Española
Santiago de Compostela, 21–25 enero 2013

Núcleos planos aleatorios

Marc Noy Serrano[1], **Lander Ramos Garrido**[2]

En este trabajo utilizaremos técnicas que nos permitan obtener nuevos resultados enumerativos sobre grafos planos. Recientemente ha sido hallada la función generadora que cuenta grafos planos [1], y a partir de ella se han obtenido ciertos resultados sobre parámetros en dichos grafos, como por ejemplo la distribución asintótica de grados [2]. En nuestro trabajo ampliamos el cálculo de parámetros asintótico a otras clases de grafos relacionadas. Principalmente nos centraremos en los 2-núcleos planos, que se definen como los grafos planos conexos que no contienen ningún vértice de grado menor que 2. Para ello definiremos una ecuación que relacione la función generadora obtenida en [1] sobre grafos planos con la función generadora sobre 2-núcleos planos, y a partir de ella obtendremos diversos parámetros asintóticos entre los que se incluyen:

- Número de grafos de un cierto tamaño
- Número esperado de aristas
- Distribución de los grados

Finalmente daremos algunas ideas sobre cómo extender estos resultados a 3-núcleos planos, y exhibiremos algunos resultados obtenidos, así como otros que faltan por obtener.

Keywords: Combinatoria Enumerativa, Teoría de grafos, Funciones generadoras

MSC 2010: 05C30

Referencias

[1] O. GIMÉNEZ; M. NOY, Asymptotic enumeration and limit laws of planar graphs. *J. Amer. Math. Soc.* 22, 309–329 (2009).

[2] M. DRMOTA; O GIMÉNEZ; M. NOY, Degree distribution in random planar graphs. *J. Combin. Theory Ser. A* 118, 2102–2130 (2011).

[1]Departamento de Matemática Aplicada II
Universitat Politècnica de Catalunya
Edifici Omega - Campus Nord C/ Jordi Girona, 1-3 CP 08034 BARCELONA
marc.noy@upc.edu

[2]Departamento de Matemática Aplicada II
Universitat Politècnica de Catalunya
Edifici Omega - Campus Nord C/ Jordi Girona, 1-3 CP 08034 BARCELONA
lander.ramos@upc.edu