Mathematisches Forschungsinstitut Oberwolfach

Report No. 22/2016

DOI: 10.4171/OWR/2016/22

Combinatorics and Probability

Organised by
Béla Bollobás, Cambridge and Memphis
Michael Krivelevich, Tel Aviv
Oliver Riordan, Oxford
Emo Welzl, Zürich

17 April – 23 April 2016

Abstract. For the past few decades, Combinatorics and Probability Theory have had a fruitful symbiosis, each benefitting from and influencing developments in the other. Thus to prove the existence of designs, probabilistic methods are used, algorithms to factorize integers need combinatorics and probability theory (in addition to number theory), and the study of random matrices needs combinatorics. In the workshop a great variety of topics exemplifying this interaction were considered, including problems concerning designs, Cayley graphs, additive number theory, multiplicative number theory, noise sensitivity, random graphs, extremal graphs and random matrices.

Mathematics Subject Classification (2010): 05xx, 60xx.

Introduction by the Organisers

The workshop was organized by Béla Bollobás (Cambridge and Memphis), Michael Krivelevich (Tel Aviv), Oliver Riordan (Oxford) and Emo Welzl (Zürich). The meeting was extremely well attended, with 53 participants from 13 countries, including the US, Israel, Canada, Australia, Brazil, Korea, and various European countries. Many excellent mathematicians who would have loved to participate could not be invited, for lack of space. The programme consisted of 11 main lectures, 14 shorter talks, and a problem session, with plenty of time for discussion.

The timing of the workshop was very fortunate, because recently several major results have been proved in probabilistic combinatorics and combinatorial probability. The main lectures provided a very good overview of these great results. In particular, Peter Keevash talked about his solution of a problem of Steiner from

1853 concerning the existence of designs, József Balogh, Wojciech Samotij and Andrew Thomason gave interconnected lectures on their extremely powerful *method of containers* and its applications, and Paul Balister talked about a sharp result on an old problem of Pomerance related to the fastest known algorithms for factoring large integers. In addition, Noga Alon presented a probabilistic result answering a basic extremal question concerning 'universal' graphs, David Gamarnik and Van Vu presented recent developments in the theory of random matrices, Asaf Shapira described a new version of Szemerédi's regularity lemma (a fundamental tool in many areas of combinatorics and elsewhere), Mathias Schacht talked about a new class of extremal problems for hypergraphs, and Angelika Steger presented much simpler proofs of stronger forms of a number of results in randomized optimization. The shorter contributions, including several by younger researchers, covered a wide range topics. In the following we include the extended abstracts of all the talks, in the order they were given.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, "US Junior Oberwolfach Fellows".

Workshop: Combinatorics and Probability

Table of Contents

Abstracts

Counting designs

Peter Keevash

When does a graph G have a triangle decomposition? (By this we mean a partition of its edge set into triangles.) There are two obvious necessary ‘divisibility conditions’: the number of edges must be divisible by three, and the degree of any vertex must be even. We say that G is *tridivisible* if it satisfies these divisibility conditions. In 1847 Kirkman proved that any tridivisible complete graph has a triangle decomposition; equivalently, there is a Steiner Triple System on n vertices if n is 1 or 3 mod 6. In [5] we showed more generally that a tridivisible graph has a triangle decomposition if we assume a certain pseudorandomness condition. In fact, we proved a more general result on clique decompositions of simplicial complexes, which implies the Existence Conjecture for combinatorial designs.

In this extended abstract, we will outline estimates on the number of combinatorial designs, which prove (and generalise) a conjecture of Wilson from 1974 on the number of Steiner Triple Systems. We start by stating our result that tridivisible pseudorandom graphs have triangle decompositions. The pseudorandomness condition is as follows. Let G be a graph on n vertices. The *density* of G is $d(G) = |G|/\binom{n}{2}$. We say that G is *c-typical* if every vertex has $(1 \pm c)d(G)n$ neighbours and every pair of vertices have $(1 \pm c)d(G)^2 n$ common neighbours.

Theorem 1. *There exists $0 < c_0 < 1$ and $n_0 \in \mathbb{N}$ so that if $n \geq n_0$ and G is a c-typical tridivisible graph on n vertices with $d(G) > n^{-10^{-7}}$ and $c < c_0 d(G)^{10^6}$ then G has a triangle decomposition.*

One consequence of Theorem 1 is that the standard random graph model $G(n, 1/2)$ with high probability (whp) has a partial triangle decomposition that covers all but $(1 + o(1))n/4$ edges. Indeed, deleting a perfect matching on the set of vertices of odd degree and then at most two 4-cycles gives a graph satisfying the hypotheses of the theorem. This is asymptotically best possible, as whp there are $(1 + o(1))n/2$ vertices of odd degree, and any set of edge-disjoint triangles must leave at least one edge uncovered at each vertex of odd degree. We can also use Theorem 1 to prove the following conjecture of Wilson [12] on the number of Steiner Triple Systems on n vertices, i.e. triangle decompositions of the complete graph K_n; denote this by $STS(n)$.

Theorem 2. *If n is 1 or 3 mod 6, then $STS(n) = (n/e^2 + o(n))^{n^2/6}$.*

The upper bound in Theorem 2 was recently proved by Linial and Luria [8], who showed that $STS(n) \leq (n/e^2 + O(\sqrt{n}))^{n^2/6}$. Our lower bound will be $STS(n) \geq (n/e^2 + O(n^{1-a}))^{n^2/6}$ for some small $a > 0$, We use the following triangle removal process. We start with the complete graph K_n, and at each step we delete the edges of a uniformly random triangle in the current graph. It is shown in [2] that whp the process persists until only $O(n^{3/2+o(1)})$ edges remain, but we will stop at $n^{2-10^{-7}}$ edges (i.e. at the nearest multiple of 3 to this number) so that we can apply Theorem 1. We need the following additional facts from [2] about this stopped process: whp the final graph is $n^{-1/3}$-typical, and when $pn^2/2$ edges remain the number of choices for the deleted triangle is $(1 \pm n^{-2/3})(pn)^3/6$.

Proof of Theorem 2. Consider the following procedure for constructing a Steiner Triple System on n vertices: run the triangle removal process until $n^{2-10^{-7}}$ edges remain, then apply Theorem 1 (if its hypotheses are satisfied, which occurs in $1 - o(1)$ proportion of all instances of the process). Writing m for the number of steps and $p(i) = 1 - 6i/n^2$, the logarithm of the number of choices is

$$L_1 = \sum_{i=1}^{m} (\log(p(i)^3 n^3/6) \pm 2n^{-2/3}) = (n^2/6)(\log(n^3/6) - 3 \pm n^{-10^{-8}}),$$

since $\sum_{i=1}^{m} \log p(i) = (1 + O(n^{-10^{-7}} \log n))(n^2/6) \int_0^1 \log p \, dp$ and $\int_0^1 \log p \, dp = -1$. Also, for any fixed Steiner Triple System, the logarithm of the number of times it is counted by this procedure is at most

$$L_2 = \sum_{i=1}^{m} \log(p(i) n^2/6) = (n^2/6)(\log(n^2/6) - 1 \pm n^{-10^{-8}}).$$

Therefore $\log(STS(n)) \geq L_1 - L_2 = (n^2/6)(\log(n) - 2 \pm 2n^{-10^{-8}})$. □

The strategy of the proof of Theorem 1 is encapsulated by the following setup. We say that $J \subseteq G$ is *c-bounded* if $|J(v)| < c|V(G)|$ for every $v \in V(G)$, where $J(v) = \{u \in V(G) : uv \in J\}$ is the *neighbourhood* of v in J.

Setup 3. Suppose we have $G^* \subseteq G$ with a 'template' triangle decomposition T such that

Nibble: $G \setminus G^*$ contains a set N of edge-disjoint triangles with 'leave' $L := (G \setminus G^*) \setminus \cup N$ that is c_1-bounded,

Cover: For any $L \subseteq G \setminus G^*$ that is c_1-bounded, there is a set M^c of edge-disjoint triangles such that $L = (G \setminus G^*) \cap (\cup M^c)$ and the 'spill' $S := G^* \cap (\cup M^c)$ is c_2-bounded,

Hole: For any tridivisible $S \subseteq G^*$ that is c_2-bounded, there are 'outer' and 'inner' sets M^o, M^i of edge-disjoint triangles in G^* such that $\cup M^o$ is c_3-bounded and $(S, \cup M^i)$ is a partition of $\cup M^o$,

Completion: Given L, M^c, M^o and M^i as above, there are sets M_1, M_2, M_3, M_4 of edge-disjoint triangles in G^* such that $(L, \cup M_2)$ is a partition of $\cup M_1$, $\cup M_3 = \cup M_4$, $M_3 \subseteq T$ and $M_2 \subseteq M_4$.

The key step is choosing T (which determines G^*). We will use our method of Randomised Algebraic Construction, which takes a particularly simple form for triangle decompositions. To motivate the construction, suppose that $V(G)$ is an abelian group, and consider the set Σ of triples xyz such that $x + y + z = 0$. We note that Σ is a good 'model' for a triangle decomposition, as for any xy there is a unique z such that $x + y + z = 0$. However, we cannot simply take Σ, as not all such xyz are triangles of G; moreover, x, y, z may not even be pairwise distinct.

The idea of the construction is that a suitable random subset of Σ can act as a template, which covers a constant fraction of G. Next we find an approximate decomposition of the rest of G by random greedy algorithms: this is accomplished by steps **Nibble** and **Cover** of Setup 3. After these steps, every edge of G has been covered once or twice, and the spill S is the set of edges that have been covered twice. Finally, we use local modifications built into the template to turn the approximate decomposition into an exact decomposition: this is accomplished by steps **Hole** and **Completion** of Setup 3.

To motivate **Completion**, we imagine first that we have **Hole** and also $M^o \subseteq T$. Then we could delete M^o and take M^i instead, thus reducing by one the multiplicity of every edge in S, so that we have a triangle decomposition of G. However, specifying a triangle of T is very restrictive, as there are only order(n^2) such triangles out of a total of order(n^3) triangles in G. If we had chosen T uniformly at random it would be hopeless to obtain any useful configuration formed by triangles of T. However, the algebraic structure implies that certain configurations of triangles are dense within a sparse configuration space (described by linear constraints). This forms the basis of a modification procedure that replaces M^c, M^o and M^i by other sets of triangles with the same properties, where M_1 plays the role of $M^c \cup M^i$, M_2 of M^o, and each triangle f of M_2 can be embedded in a small subgraph that has one triangle decomposition (part of M_4) using f and another triangle decomposition (part of M_3) contained in T.

References

[1] P. Bennett and T. Bohman, A natural barrier in random greedy hypergraph matching, arXiv:1210.3581.

[2] T. Bohman, A. Frieze, E. Lubetzky, Random triangle removal, *Adv. Math.* **280** (2015), 379–438.

[3] D. A. Freedman, On tail probabilities for martingales, *Ann. Probability* 3:100–118 (1975).

[4] J. E. Graver and W. B. Jurkat, The module structure of integral designs, *J. Combinatorial Theory Ser. A* 15:75–90 (1973).

[5] P. Keevash, The existence of designs, arXiv:1401.3665.

[6] P. Keevash, A hypergraph regularity method for generalised Turán problems, *Random Struct. Alg.* 34:123–164 (2009).

[7] G. Kuperberg, S. Lovett and R. Peled, Probabilistic existence of regular combinatorial objects, Proc. 44th ACM STOC, (2012), 1091–1105.

[8] N. Linial and Z. Luria, Upper bounds on the number of Steiner triple systems and 1-factorizations, *Random Struct. Alg.* 43:399–406 (2013).

[9] B. D. McKay and N. C. Wormald, Asymptotic enumeration by degree sequence of graphs of high degree, *Europ. J. Combin.* 11:565–580 (1990).

[10] B. D. McKay and N. C. Wormald, Asymptotic enumeration by degree sequence of graphs with degrees $o(n^{1/2})$, *Combinatorica* 4:369–382 (1991).

[11] C. McDiarmid, Concentration, in: Probabilistic Methods for Algorithmic Discrete Mathematics, *Alg. Combin.* 16:195–248 (1998).

[12] R. M. Wilson, Nonisomorphic Steiner Triple Systems, *Math. Zeit.* 135:303–313 (1974).

[13] R. M. Wilson, The necessary conditions for t-designs are sufficient for something, *Utilitas Math.* 4:207–215 (1973).

[14] R. M. Wilson, Signed hypergraph designs and diagonal forms for some incidence matrices, *Designs, Codes and Cryptography*, 17:289–297 (1999).

High-dimensional discrepancy

Nati Linial
(joint work with Zur Luria)

The notion of *discrepancy* is central to all branches of discrete mathematics. Roughly speaking, one asks how well finite sets can approximate a uniform measure. A bit more concretely, the problem is defined in terms of a collection $\mathcal{F}$ of subsets in a probability space (Ω, μ). We seek the minimum of $\sup_{X \in \mathcal{F}} |\frac{|S \cap X|}{|S|} - \mu(X)|$ over all sets S of given cardinality. Such questions and their many variants make sense and are interesting in numerous contexts. An important example from graph theory is the *expander mixing lemma.* Let $G = (V, E)$ be a d-regular n-vertex graph. This lemma asserts that if G is an expander graph, then for every two subsets $A, B \subseteq V$ there holds $|e(A,B) - \frac{d}{n}|A||B|| \leq O(\sqrt{|A||B|})$ where $e(A,B)$ is the number of ordered pairs (a,b) with $a \in A, b \in B$ and $ab \in E$. The unspecified constant in the big-oh term depends on the spectrum of G's adjacency matrix.

A considerable body of recent research is aimed at developing a theory of *high-dimensional combinatorics.* Many basic combinatorial constructs have interesting high-dimensional counterparts, and it is natural to study discrepancy phenomena in these frameworks. Specifically we consider discrepancy in *high-dimensional permutations.* Let us briefly recall this concept [6]. We equate a (classical, i.e., one-dimensional) permutation with its permutation matrix, namely, an $n \times n$ array of zeros and ones where every row and every column contains exactly one 1. In analogy, a d-dimensional permutation A is an $[n]^{d+1} = n \times n \times \ldots n$ array of zeros and ones such that for every index $d+1 \geq i \geq 1$ and every choice of integers $\alpha_j \in [n]$ over $1 \leq j \neq i \leq d+1$ there is exactly one choice of $x \in [n]$ for which $A(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_{i+1}, \ldots, \alpha_{d+1}) = 1$. Note, in particular, that a two-dimensional permutation is synonymous with a Latin square.

The class $\mathcal{F}$ that defines our discrepancy problem is comprised of all boxes $\mathcal{T} = T_1 \times \ldots \times T_{d+1} \subseteq [n]^{d+1}$. The *volume* of this box is defined to be $\text{vol}(\mathcal{T}) := \prod |T_i|$. Our discrepancy problem is to find d-dimensional permutations A, such that for every box $\mathcal{T}$ it holds that $A(\mathcal{T}) := |\{\alpha \in \mathcal{T} : A(\alpha) = 1\}|$ is close to $\frac{\text{vol}(\mathcal{T})}{n}$. (Clearly this is what one would expect, since the density of 1 entries in a d-dimensional permutation is $\frac{1}{n}$). We propose the following conjecture.

Conjecture 1. *For every $d \geq 2$ there exist arbitrarily large d-dimensional permutations A such that for every box $\mathcal{T}$ we have*

$$\left| A(\mathcal{T}) - \frac{vol(\mathcal{T})}{n} \right| = O(\sqrt{vol(\mathcal{T})}).$$

There are at least two reasons why we expect this to be true. Consider the following "poor man's analog" of a random Latin square. It is a random $n \times n \times n$ array of zeros and ones whose entries are chosen independently with the same distribution, where 1 is chosen with probability $\frac{1}{n}$. It is easily verified that this relation holds in that model. In addition, a d-dimensional permutation may be viewed as a $(d+1)$-partite $(d+1)$-uniform hypergraph, and we find the similarity with the expander mixing lemma rather compelling.

We say that $\mathcal{T}$ is an *empty box* in A if $A(\mathcal{T}) = 0$, and denote by $\varepsilon(A)$ the maximal volume of an empty box in A. One consequence of the above conjecture is that there are d-dimensional permutations A such that $\varepsilon(A) = O(n^2)$. On the other hand, it is easy to see that $\varepsilon(A) = \Omega(n^2)$ for *every* d-dimensional permutation, since every (classical) permutation matrix contains a $\lfloor \frac{n}{2} \rfloor \times \lfloor \frac{n}{2} \rfloor$ block of zeros. Indeed, let A be an arbitrary d-dimensional permutation. Pick some $T_2 \subseteq [n]$ of cardinality $\lfloor \frac{n}{2} \rfloor$ and some $t_3, \ldots, t_{d+1} \in [n]$, and let $T_3 = \{t_3\}, \ldots, T_{d+1} = \{t_{d+1}\}$. We can find a subset $T_1 \subseteq [n]$ of cardinality $\lfloor \frac{n}{2} \rfloor$ for which $\mathcal{T} = T_1 \times \ldots \times T_{d+1} \subseteq [n]^{d+1}$ is an empty box in A. Indeed, for every $t \in T_2$, there is exactly one $x \in [n]$ for which $A(x, t, t_3, \ldots, t_{d+1}) = 1$ and clearly x cannot belong to T_1. But altogether only $\lfloor \frac{n}{2} \rfloor$ elements are ruled out from being in T_1, one per each element of T_2 so that at least $\lfloor \frac{n}{2} \rfloor$ are still acceptable and the claim follows.

We prove the following theorems in this spirit for 2-dimensional permutations, i.e., for Latin squares.

Theorem 2. *Asymptotically almost every order-n Latin square A satisfies $\varepsilon(A) = O(n^2 \log^2(n))$.*

Theorem 3. *There exist infinitely many order-n Latin squares satisfying $\varepsilon(A) = O(n^2)$ (and hence $\varepsilon(A) = \Theta(n^2)$).*

We tend to believe the following statement which subsumes both theorems:

Conjecture 4. *Asymptotically almost every order-n Latin square A satisfies $\varepsilon(A) = O(n^2)$.*

In fact, it is conceivable, that our discrepancy conjectures hold for asymptotically almost every d-dimensional permutation.

It is easy to see that the *multiplication table of a finite group* is a Latin square, and problems that we consider here have been previously addressed in the group theory literature. Babai and Sós [1], defined a subset $S \subset \Gamma$ of a finite group to be *product-free* if there are no three elements $x, y, z \in S$ with $xy = z$. Note that in our language this means that $S \times S \times S$ is an empty box in the Latin square L corresponding to Γ. Using the classification of finite simple groups, Babai and Sós showed that every finite group contains large product-free sets. Subsequently, Kedlaya [3] improved their bound. His result implies:

Theorem 5 (Kedlaya)**.** *If L is a Latin square that is the mutiplication table of an order-n group, then $\varepsilon(L) \geq cn^{\frac{33}{14}}$ for some fixed $c > 0$.*

On the other hand, Gowers [2] has exhibited order-n groups for which $\varepsilon(L) \leq Cn^{\frac{8}{3}}$ for some fixed $C > 0$.

These results show that a typical Latin square has substantially lower discrepancy than any group of the same order.

A *cube* is a box $A \times B \times C$ with $|A| = |B| = |C|$. It is easy to see that every order-n Latin square has an empty cube of side $\lfloor (n + 1/4)^{1/2} - 1/2 \rfloor$, and we can show:

Theorem 6. *There exist infinitely many order-n Latin squares L in which every empty cube has side $O((n \log n)^{1/2})$.*

As mentioned, Kedlaya finds an empty cube of side $\Omega(n^{11/14})$ in the Latin square of every order-n group.

Our proofs are based on two methods: (i) Our earlier work [6] in which we derived an upper bound on the number of d-dimensional permutations, (ii) Ideas developed by P. Keevash in his recent breakthrough work on the theory of combinatorial designs. He considers in [5] a random greedy process in which a set system evolves as sets are added to it in sequence. As he shows, with high probability the partial design that is obtained this way can be completed to a bona-fide design.

The full version of this note is [7].

References

[1] L. Babai and V. T. Sós, Sidon sets in groups and induced subgraphs of Cayley graphs, European J. Combin. 6 (1985), 101–114.

[2] W. T. Gowers, Quasirandom groups, Combinatorics, Probability and Computing 17 (2008), 363–387.

[3] K. S. Kedlaya, Large product-free subsets of finite groups, Journal of Combinatorial Theory, Ser. A 77 (1997), 339-343.

[4] P. Keevash, The existence of designs, arXiv:1401.3665.

[5] P. Keevash, Counting designs, arXiv:1504.02909.

[6] N. Linial and Z. Luria, An upper bound on the number of high-dimensional permutations, *Combinatorica* **34** (2014), 471–486.

[7] N. Linial and Z. Luria, Discrepancy of high-dimensional permutations, arXiv:1512.04123.

Counting sparse graphs with no induced 4-cycle

Wojciech Samotij

(joint work with Robert Morris, David Saxton)

In extremal and structural graph theory, two of the central objects of study are the family of H-free graphs and the family of induced-H-free graphs, where H is some fixed graph. More generally, it is natural to consider an arbitrary *monotone* or *hereditary* property of graphs, that is, a family of graphs that is closed under taking subgraphs or induced subgraphs, respectively. In recent years, the problem of understanding the typical behaviour of sparse graphs in monotone properties has attracted a great deal of attention and general techniques for attacking problems of this type have been developed, see [1, 2, 5, 6]. For example, it follows from the main results of these papers that (if H is not bipartite) a typical H-free graph with n vertices and m edges is 'structured' if $m \gg n^{2-1/m_2(H)}$ and 'random-like' if $m \ll n^{2-1/m_2(H)}$. More precisely, above (resp. below) the threshold almost all such graphs are close to (resp. far from) being $(\chi(H) - 1)$-partite. As usual, $m_2(H)$ denotes the 2-density of the graph H, that is, the maximum value of $(e(F) - 1)/(v(F) - 2)$ over all subgraphs $F \subseteq H$ with $v(F) \geq 3$. However, for induced-H-free graphs, these methods do not typically allow one to establish such a threshold, and its existence is unknown in all non-trivial cases.

We introduce a new 'asymmetric' version of the so-called 'method of hypergraph containers', which was introduced recently by Balogh, Morris, and Samotij [1] and independently by Saxton and Thomason [5] and use it to determine the structure of a typical graph with n vertices, m edges, and no induced copy of C_4 for all m satisfying $n^{4/3}(\log n)^2 \le m \ll n^2$. The lower bound on m is best possible up to a polylogarithmic factor, as we also show that if $m \ll n^{4/3}(\log n)^{1/3}$, then a typical such graph does not have such structure, and if $m \ll n^{4/3}$, then it is 'random-like'. We believe that the ideas contained in this work bring us closer towards determining analogous thresholds for families of graphs containing no induced copy of an arbitrary H.

Let us say that a graph G is *ε-close to being a split graph* if there exists a partition $V(G) = A \cup B$ such that $G[A]$ has at least $(1-\varepsilon)\binom{|A|}{2}$ edges and $G[B]$ has at most $\varepsilon e(G)$ edges. The main result of this work is the following theorem, which is motivated by a classical work of Prömel and Steger [4], who proved that almost every graph with n vertices (with no restriction on the number of edges) and no induced copy of C_4 is actually a split graph, i.e., 0-close to being a split graph.

Theorem 1. *Fix $\varepsilon > 0$ and let $m = m(n) \ge n^{4/3}(\log n)^2$. Then almost every graph with n vertices, m edges, and no induced copy of C_4 is ε-close to being a split graph.*

The proof of Theorem 1 relies on two new results: an 'asymmetric container lemma', which generalizes the main results of [1] and [5], and an analogue of (a 'supersaturated' version of) the Erdős–Simonovits stability theorem [3, 7] for sparse graphs with no induced copy of C_4.

References

[1] J. Balogh, R. Morris, and W. Samotij, *Independent sets in hypergraphs*, J. Amer. Math. Soc. **28** (2015), 669–709.

[2] D. Conlon and T. Gowers, *Combinatorial theorems in sparse random sets*, to appear in Ann. of Math.

[3] P. Erdős and M. Simonovits, *A limit theorem in graph theory*, Studia Sci. Math. Hungar. **1** (1966), 51–57.

[4] H. J. Prömel and A. Steger, *Excluding induced subgraphs: quadrilaterals*, Random Structures Algorithms **2** (1991), 55–71.

[5] D. Saxton and A. Thomason, *Hypergraph containers*, Invent. Math. **201** (2015), 925–992.

[6] M. Schacht, *Extremal results for random discrete structures*, to appear in Ann. of Math.

[7] M. Simonovits, *A method for solving extremal problems in graph theory, stability problems*, Theory of Graphs (Proc. Colloq., Tihany, 1966), Academic Press, New York, 1968, pp. 279–319.

Optimal induced universal graphs

Noga Alon

Let $\mathbf{F}$ be a finite family of graphs. A graph G is *induced universal* for $\mathbf{F}$ if every member F of $\mathbf{F}$ is an induced subgraph of G. There is a vast literature about induced universal graphs since their introduction by Rado [7]. Let $\mathbf{F}(k)$ denote the family of k-vertex undirected graphs, and let $f(k)$ denote the smallest possible number of vertices of an induced universal graph for $\mathbf{F}(k)$. Moon [5] observed that a simple counting argument gives $f(k) \geq 2^{(k-1)/2}$ and proved that $f(k) \leq O(k2^{k/2})$. Alstrup, Kaplan, Thorup and Zwick [2] determined $f(k)$ up to a constant factor, showing that $f(k) \leq 16 \cdot 2^{k/2}$. Bollobás and Thomason [3] proved that the random graph $G(n, 0.5)$ on $n = k^2 2^{k/2}$ vertices is induced universal for $\mathbf{F}(k)$ with high probability, that is, with probability that tends to 1 as k tends to infinity. The question of finding tighter bounds for $f(k)$, suggested by the work of Moon, is mentioned by Vizing in [8] and by Alstrup et. al (despite the fact their work determines it up to a constant factor of $16\sqrt{2}$) in [2]. Here we show that the lower bound is tight, up to a lower order additive term.

Theorem 1.

$$f(k) = (1 + o(1))2^{(k-1)/2}.$$

The proof combines probabilistic and combinatorial arguments with some group theoretical facts about graphs with large automorphism groups. Similar arguments supply asymptotically tight estimates for the analogous questions for directed graphs, oriented graphs, tournaments, bipartite graphs or complete graphs with colored edges, improving results in [6], [4], [2].

As a byproduct of (a variant of) the first part of the proof we show that the minimum number of vertices n so that the random graph on n vertices is induced universal for $\mathbf{F}(k)$ with high probability is $(1 + o(1))\frac{k}{e}2^{(k-1)/2}$, improving the estimate in [3] (which was harder to improve in 1981, when [3] was written, but is simpler now, using some of the more recently developed high deviation inequalities.) Combining this argument with some group theoretic tools and the Stein-Chen method (as used in in [1]) we prove a more precise statement, as follows.

Theorem 2. *Let $n > k > 1$, let $G = G(n, 0.5)$ be the binomial random graph, and put*

$$\lambda = \binom{n}{k} 2^{-\binom{k}{2}}.$$

Then the probability that G is induced universal for $\mathbf{F}(k)$ is $(1 - e^{-\lambda})^2 + o(1)$, where the $o(1)$ tends to 0 (uniformly in $k = k(n)$) as n tends to infinity.

References

[1] N. Alon, Bipartite decomposition of random graphs, J. Combinatorial Theory, Ser. B 113 (2015), 220–235.

[2] S. Alstrup, H. Kaplan, M. Thorup and U. Zwick, Adjacency Labeling Schemes and Induced-Universal Graphs, Proc. STOC 2015, 625–634.

[3] B. Bollobás and A. Thomason, Graphs which contain all small graphs, European Journal of Combinatorics, 2(1) (1981), 13–15.

[4] V. V. Lozin and G. Rudolf, Minimal universal bipartite graphs, Ars Comb. 84 (2007), 345–356.

[5] J. W. Moon, On minimal n-universal graphs, Proceedings of the Glasgow Mathematical Association, 7(1) (1965), 32–33.

[6] J. W. Moon, *Topics on Tournaments*, New York, 1968.

[7] R. Rado, Universal graphs and universal functions, Acta. Arith. (1964), 331–340.

[8] V.G. Vizing, Some unsolved problems in graph theory, Russian Mathematical Surveys, 23(6) (1968), 125–141.

Quasirandom Cayley graphs

Yufei Zhao

(joint work with David Conlon)

A fundamental result of Chung, Graham, and Wilson [4], building on earlier work of Thomason [8, 9], states that for a sequence of graphs of constant edge-density, a number of seemingly distinct notions of quasirandomness are equivalent. In particular, for n-vertex, d-regular graphs, the following two properties are equivalent as long as $d = \Theta(n)$:

- *Discrepancy condition*: For all vertex subsets S and T,
$$e(S,T) = \frac{d}{n}|S||T| + o(nd);$$
- *Eigenvalue condition*: All eigenvalues of the the adjacency matrix, except the largest, are $o(d)$.

What about for sparse graphs, when $d = o(n)$?

The eigenvalue condition always implies the discrepancy condition. This is a consequence of the famous *expander mixing lemma*, which says that in an (n, d, λ)-*graph* (i.e., an n-vertex d-regular graph where all eigenvalues of the adjacency matrix, except the largest, are at most λ in absolute value), one has

$$\left| e(S,T) - \frac{d}{n}|S||T| \right| \le \lambda\sqrt{|S||T|} \tag{1}$$

for all vertex subsets S and T.

However, the discrepancy condition does not necessarily imply the eigenvalue condition when $d = o(n)$ [7, 3]. Consider the disjoint union of a large d-regular random graph and a copy of K_{d+1}. This graph satisfies the discrepancy condition since the copy of K_{d+1} does not significantly affect discrepancy. On the other hand, the eigenvalue d appears with multiplicity two (once for each connected component), so the graph does not satisfy the eigenvalue condition.

There have been some partial converses. For example, Bilu and Linial [2] gave a converse to the expander mixing lemma, showing that if (1) holds for all S and T, then the graph is an (n, d, λ')-graph with $\lambda' = O(\lambda \log d)$. The extra factor of $\log d$ cannot be removed. In a different direction, Alon et al. [1] showed that if the discrepancy condition is satisfied, then one can remove a $o(1)$-fraction of vertices from the graph so that remaining graph satisfies the eigenvalue condition.

A result of Kohayakawa, Rödl, and Schacht [6] (originally from 2003) comes as something of a surprise: the two properties are always equivalent for Cayley graphs of abelian groups. In our work [5], we extend their result to non-abelian groups, and more generally, all vertex-transitive graphs. Here is a precise statement of our theorem.

Theorem 1. *If an n-vertex d-regular Cayley graph (or more generally, a vertex-transitive graph) has the property that*

$$\left| e(S,T) - \frac{d}{n}|S||T| \right| \leq \epsilon dn \tag{2}$$

for all vertex subsets S and T, then it is an (n, d, λ)-graph with $\lambda \leq 8\epsilon d$.

The proof uses Grothendieck's inequality. We consider the cut norm for matrices, and show that its semidefinite relaxation equals the spectral norm when the matrix arises from a weighted Cayley graph. See our paper [5] for details.

References

[1] N. Alon, A. Coja-Oghlan, H. Hàn, M. Kang, V. Rödl and M. Schacht, Quasi-randomness and algorithmic regularity for graphs with general degree distributions, *SIAM J. Comput.* **39** (2010), 2336–2362.

[2] Y. Bilu and N. Linial, Lifts, discrepancy and nearly optimal spectral gap, *Combinatorica* **26** (2006), 495–519.

[3] B. Bollobás and V. Nikiforov, Hermitian matrices and graphs: singular values and discrepancy, *Discrete Math.* **285** (2004), 17–32.

[4] F. R. K. Chung, R. L. Graham, and R. M. Wilson, Quasi-random graphs, *Combinatorica* **9** (1989), 345–362.

[5] D. Conlon and Y. Zhao, Quasirandom Cayley graphs, *preprint*, available at arXiv:1603.03025 [math.CO].

[6] Y. Kohayakawa, V. Rödl, and M. Schacht, Discrepancy and eigenvalues of Cayley graphs, *preprint*, available at arXiv:1602.02291 [math.CO].

[7] M. Krivelevich and B. Sudakov, Pseudo-random graphs, in More sets, graphs and numbers, Bolyai Soc. Math. Stud., Vol. 15, 199–262, Springer, Berlin, 2006.

[8] A. G. Thomason, Pseudorandom graphs, in Random graphs '85 (Poznań, 1985), North-Holland Math. Stud., Vol. 144, 307–331, North-Holland, Amsterdam, 1987.

[9] A. G. Thomason, Random graphs, strongly regular graphs and pseudorandom graphs, in Surveys in Combinatorics 1987, London Math. Soc. Lecture Note Ser., Vol. 123, 173–195, Cambridge University Press, Cambridge, 1987.

Ways to build containers

Andrew Thomason

A collection $\mathcal{C}$ of subsets of the vertices of a hypergraph G is said to be a set of *containers* for G if, for every independent subset I in G (that is, I is a subset of the vertices that contains no edge), there is some $C \in \mathcal{C}$ with $I \subset C$. The existence of useful collections of containers was demonstrated recently by Balogh, Morris and Samotij [1] and by Saxton and Thomason [4]. Roughly speaking, $\mathcal{C}$ is useful if each $C \in \mathcal{C}$ is close to independent, and $|\mathcal{C}|$ is not very large — certainly much smaller than the number of independent sets. The collections described in [1] and [4] are in some senses optimal, and there have been quite a few applications. Wojciech Samotij in an earlier talk gave an overview of containers, together with some more recent developments, and József Balogh will discuss further new applications. In this talk we do not give new results but, rather, we attempt to give an idea of two ways in which containers can be built.

The first way is based on an older theorem of Saxton and Thomason [3], supplying containers for simple d-regular hypergraphs (simple means that no two edges share two common vertices). The containers in this theorem satisfied the bound $|C| \le (1-c)|G|$ for some constant c (in fact, $c = 1/4r^2$). It was subsequently noted that essentially the same argument gives containers satisfying $\mu(C) \le (1-c)$ in hypergraphs of average degree d. Here, $\mu(C) = (1/d|G|)\sum_{v\in C} d(v)$; it is readily checked that $\mu(C) \le (1-c)$ implies $|C| \le (1-c)|G|$ if G is regular, but also that $e(G[C]) \le \mu(C)e(G)$ whether or not G is regular. The great advantage of this latter inequality is that it allows the container construction process to be iterated: by applying the theorem to the hypergraph $G[C]$ we obtain $C' \subset C$ with $e(G[C']) \le (1-c)^2 e(G)$, and a few more iterations produces the following corollary, taken from [5].

Theorem 1. *Let G be a simple r-graph of average degree d. Let $0 < \delta < 1$. If d is large enough, then there is a collection of sets $\mathcal{C}$ of subsets of $V(G)$ satisfying*

- *if $I \subset V(G)$ is independent, there is some $C \in \mathcal{C}$ with $I \subset C$,*
- *$e(G[C]) < \delta e(G)$ for every $C \in \mathcal{C}$,*
- *$|\mathcal{C}| \le 2^{\alpha|G|}$ where $\alpha = (1/d)^{1/(2r-1)}$.*

The initial containers are built as follows. Given an integer $0 \le j < r$ and two disjoint subsets $X, Y \subset V(G)$, let $\Gamma_j(X,Y)$ be the set of vertices v for which there is an edge containing v, j vertices of X and $r-j-1$ vertices of Y. Then, given a third set Z, let $C_j(X,Y,Z)$ be the set $(V(G) \setminus \Gamma_j(X,Y)) \cup Z$, unless this set has measure more than $1-c$, in which case put $C_j(X,Y,Z) = \emptyset$. The collection $\mathcal{C}$ in the theorem is the collection of all $C_j(X,Y,Z)$ for all j and all small X, Y and Z (meaning, say, less than $\alpha|G|$). Every independent set I is in one of these containers, for the following reason. Given I, there are no edges with r vertices in I, but plenty of edges with no vertices in I. So there is some j such that there are many more edges with j vertices in I than with $j+1$. Pick $X \subset I$ and $Y \subset V(G) \setminus I$ randomly, and let $Z = I \cap \Gamma_j(X,Y)$. The hypotheses and the simplicity of G guarantee $\mu(\Gamma_j(X,Y))$ is large, and that Z is small, so we are done.

(For the sake of correctness it should be said that this method fails completely in the form stated, but the addition of an unexpected twist restores it to life — for details see [5]).

This method gives us a useful collection of containers for a simple hypergraph G. But it can nevertheless be applied to some denser hypergraphs, as follows. If G is dense, find a simple subgraph G_{simple} of G by randomly selecting a sparse set of edges and doing a bit of tidying up. We expect to find that, for every subset $C \subset V(G)$, if $e(G_{\text{simple}}[C]) < \delta e(G_{\text{simple}})$ holds then $e(G[C]) < 2\delta e(G)$ holds. Thus Theorem 1 can be applied to G_{simple} to obtain containers which are also useful containers for G. In this way, for example, a very short proof can be given that, if H is an ℓ-uniform hypergraph, then the number of H-free ℓ-uniform hypergraphs on n vertices is $2^{\pi(H)\binom{n}{\ell}+o(n^\ell)}$ (a result with a long pedigree described by Samotij in his talk, but in this form due to Nagle, Rödl and Schacht [2]).

Theorem 1 offers an easy way to build containers but the number of containers produced is more than necessary. The next theorem, similar to ones in [1] and [4], is more or less optimal.

Theorem 2. *Given $r \in \mathbb{N}$ and $\epsilon > 0$ there exists $c = c(r, \epsilon)$ as follows.*

Let G be an r-graph of average degree d. Let $0 < p \leq 1$ satisfy

$$(\dagger) \qquad d(T) \leq cp^{|T|-1}d \quad \text{holds for all } T,\ 2 \leq |T| \leq r$$

Then there is a function $C : \mathcal{P}V \to \mathcal{P}V$, such that, for every independent set $I \subset V$

(a) *there is some $S \subset V$ with $S \subset I \subset C(S)$,*
(b) *$|S| \leq p|V|$, and*
(c) *$e(G[C(S)]) \leq \epsilon e(G)$.*

In fact the above holds for all sets $I \subset V$ such that either $G[I]$ is $\lfloor cp^{r-1}d \rfloor$-degenerate or $e(G[I]) \leq cp^r e(G)$.

The reason why a condition like (†) is needed was discussed by Wojciech Samotij in his talk. We don't prove this theorem but try to give an indication of how it can be proved. The previously mentioned ideas of degree measure and iteration can be used here too, so we imagine that G is regular, and our job is to specify a small set $S \subset I$ whereby it is possible to identify a set C, with $I \subset C$ and $|C| \leq (1 - c)|G|$ for some positive c. The methods in [1] and [4] were algorithmic but the description here is non-algorithmic.

In the graph case, $r = 2$, when (†) reduces to $p \geq 1/cd$, the method used by Saphozhenko in several of his papers is to choose $S \subset I$ so that Γ, the set of neighbours of S, is as large as possible whilst S is kept small. Evidently $I \cap \Gamma = \emptyset$, so we can choose $C \subset V(G) \setminus \Gamma$. If G is d-regular we cannot achieve $|\Gamma| > d|S|$ but we aim for $|\Gamma| > \zeta d|S|$, for some small fixed constant ζ ($\zeta = 1/12r!$ is ok in general). One way to do this is to define a function $\psi(S) = -\zeta d|S| + |\Gamma|$, and to pick $S \subset I$ that maximises $\psi(S)$. Then define $C(S) = \{v \notin \Gamma : \psi(S \cup \{v\}) \leq \psi(S)\}$. Then $I \subset C(S)$ by the maximality of $\psi(S)$. Moreover, $\psi(S) \geq 0$ because $\psi(\emptyset) = 0$, and since $|\Gamma| \leq |V|$ this means $|S| \leq |V|/d\zeta$, which gives (b) if $c \leq \zeta$. Finally, note that the graph $G[C]$ has no vertex of degree exceeding ζd, for if v were such a vertex, then adding v to S would increase $|\Gamma|$ by more than ζd and thus $\psi(S \cup \{v\}) > \psi(S)$. Hence $G[C]$ is sparse relative to G, and since G is regular we know $|C|$ is not much more than $|V|/2$. This establishes the case $r = 2$.

To extend the argument to $r = 3$, we try to define a suitable function $\psi(S)$. We need $\psi(\emptyset) = 0$, and that $\psi(S) \geq 0$ implies $|S| \leq p|V|$. Again we define $C(S) = \{v \notin \Gamma : \psi(S \cup \{v\}) \leq \psi(S)\}$. It should be the case that $|C(S)|$ being close to $|V|$ implies that there are plenty of vertices $v \in C$ with $\psi(S \cup \{v\}) > \psi(S)$.

This time we define Γ to be the (possibly empty) set of vertices v for which there is an edge containing v and two vertices of S. We look too at the link graph of S. Observe that, loosely speaking, a vertex of large degree v in the link graph could be added to S to increase Γ. So we add a term to ψ to represent the link graph. But that term must be bounded in order that $\psi(S)$ is bounded (so we can bound $|S|$). We therefore use a subgraph P_2 of the link graph having a bounded number of edges. In order that we can infer the existence of lots of vertices v of large degree in P_2 when P_2 has many edges, we in fact bound, not the number of edges in P_2, but the maximum degree.

So we are led to define P_2 to be a set of edges of G, each having at least one vertex in S, such that $d_2(w) \leq qd$ where $d_2(w)$ is the number of edges in P_2 containing w and some (other) vertex of S. Here $q = 1/\sqrt{d}$, and since $p = 1/c\sqrt{d}$ typically satisfies (†), this means $q = cp$. Note $|P_2| \leq qd|V|/2$. We similarly define P_1 to be a set of edges with at least two vertices in S, such that $d_1(w) \leq q^2 d$, so $|P_1| \leq q^2 d|V|$. Define the linear function $\psi(S) = -3cd|S|/2q + |P_1|/q^2 + |P_2|/q$. Then $\psi(S) \geq 0$ implies $|S| \leq p|V|$. Moreover $|C(S)|$ cannot be close to $|V|$, for in that case *either* lots of vertices $w \in C$ have $d_2(w) = qd$, so $|P_2|$ is big and some $v \in C$ can be added to S to increase P_1 substantially, *or* few w have $d_2(w) = qd$, in which case lots of v in C lie in many edges not meeting these ws, and adding such a v to S increases P_2 substantially.

The description extends to $r \geq 4$. But this vague outline made no use of the condition (†). The condition comes in because, when adding v to S, the degrees $d_*(w)$ could potentially increase greatly, beyond the allotted bounds, due to the effect of overlapping edges. The condition (†) allows these overlaps to be accounted for and the calculations to be made correctly.

References

[1] J. Balogh, R. Morris and W. Samotij, *Independent sets in hypergraphs*, J. Amer. Math. Soc. **28** (2015), 669–709.

[2] B. Nagle, V. Rödl and M. Schacht, *Extremal hypergraph problems and the regularity method*, in "Topics in discrete mathematics", Algorithms Combin. **26** (2006), 247–278.

[3] D. Saxton and A. Thomason, *List colourings of regular hypergraphs*, Combinatorics, Probability and Computing **21** (2012), 315–322.

[4] D. Saxton and A. Thomason, *Hypergraph containers*, Inventiones Mathematicae **201** (2015), 925–992.

[5] D. Saxton and A. Thomason, *Simple containers for simple hypergraphs*, Combinatorics, Probability and Computing, **25** (2016), 448–459.

VC-dimension

János Pach

(joint work with Jacob Fox, Andrew Suk)

A graph G is said to have Vapnik-Chervonenkis dimension d (VC-dimension; see [4]), if the set system induced by the neighborhoods of each vertex has VC-dimension d. In this paper, we strengthen several classical results in extremal graph theory for graphs with bounded VC-dimension. In particular, we show that every such n-vertex graph contains a clique or an independent set of size $e^{(\log n)^{1-o(1)}}$. This improves upon the previous bound of $e^{c\sqrt{\log n}}$, which can be obtained by applying a classic result of Erdős and Hajnal.

We also strengthen and extend the Lovász-Szegedy [3], Alon-Fischer-Newman [1] ultra-strong regularity lemma for graphs with bounded VC-dimension, showing that it extends algorithmically to uniform hypergraphs and the number of parts in the partition can be taken to be $(1/\varepsilon)^{O(d)}$, which we show is tight up to the absolute constant factor in the exponent. Moreover, we give an $O(n^k)$-time algorithm for finding such a partition. We establish tight bounds on Ramsey-Turán number for graphs with bounded VC-dimension, and obtain several Ramsey-type results for hypergraphs with VC-dimension d.

References

[1] N. Alon, E. Fischer, and I. Newman, *Efficient testing of bipartite graphs for forbidden induced subgraphs*, SIAM J. Comput. **37** (2007), 959–976.

[2] P. Erdős and A. Hajnal, *Ramsey-type theorems*, Discrete Appl. Math. **25** (1989), 37–52.

[3] L. Lovász and B. Szegedy, *Regularity partitions and the topology of graphons,* in: *An Irregular Mind*, I. Bárány, J. Solymosi, and G. Sági, eds, Bolyai Society Mathematical Studies **21** (2010), 415–446.

[4] V. Vapnik and A. Chervonenkis, *On the uniform convergence of relative frequencies of events to their probabilities*, Theory Probab. Appl. **16** (1971), 264–280.

Regularity lemmas and applications

Jacob Fox

(joint work with László Miklós Lovász, Yufei Zhao)

Szemerédi's regularity lemma [14] is one of the most powerful tools in graph theory. To properly state the regularity lemma requires some terminology. Let G be a graph, and X and Y be (not necessarily disjoint) vertex subsets. Let $e(X,Y)$ denote the number of pairs vertices $(x,y) \in X \times Y$ that are edges of G. The *edge density* $d(X,Y) = e(X,Y)/(|X||Y|)$ between X and Y is the fraction of pairs in $X \times Y$ that are edges. The pair (X,Y) is *ϵ-regular* if for all $X' \subseteq X$ and $Y' \subseteq Y$ with $|X'| \geq \epsilon|X|$ and $|Y'| \geq \epsilon|Y|$, we have $|d(X',Y') - d(X,Y)| < \epsilon$. Qualitatively, a pair of parts is ϵ-regular with small ϵ if the edge densities between pairs of large subsets are all roughly the same. A vertex partition $V = V_1 \cup \ldots \cup V_k$ is *equitable* if the parts have size as equal as possible. An equitable vertex partition with k

parts is ϵ-*regular* if all but ϵk^2 pairs of parts (V_i, V_j) are ϵ-regular. The regularity lemma states that for every $\epsilon > 0$ there is a (least) integer $K(\epsilon)$ such that every graph has an ϵ-regular equitable vertex partition into at most $K(\epsilon)$ parts.

Arguably the main drawback of Szemerédi's regularity lemma is that the proof gives an enormous upper bound $K(\epsilon)$ on the number of parts, namely an exponential tower of twos of height $O(\epsilon^{-5})$. Eventually, Gowers [9] proved a lower bound on $K(\epsilon)$ which is an exponential tower of twos of height $\Omega(\epsilon^{-1/16})$. Conlon and Fox [3] determined the dependence on the number of irregular pairs, and Moshkovitz and Shapira [13] gave a simpler proof of Gowers' result. The first two authors [8] determine the order of the tower height in a version of the regularity lemma.

Due to the many applications of the regularity lemma, there has been considerable research on algorithmic versions of the regularity lemma. We would like to be able to find an ϵ-regular partition of a graph on n vertices in time polynomial in n. Szemerédi's proof of the regularity lemma was not algorithmic. The reason is that it needs to be able to check if a pair of parts is ϵ-regular, and if not, to use subsets of the parts that realize this. This is problematic because it is shown in [1] that determining whether a given pair of parts is ϵ-regular is co-NP-complete. They use this to show that checking whether a given partition is ϵ-regular is co-NP-complete.

However, Alon et al. [1] show how to find, if a given pair of vertex subsets of size n are not ϵ-regular, a pair of subsets which realize that the pair is not $\epsilon^4/16$-regular. The running time is $O_\epsilon(n^{\omega+o(1)})$, where $\omega < 2.373$ is the matrix multiplication exponent (multiplying two $n \times n$ matrices in $n^{\omega+o(1)}$ time) [12]. Here we use the subscript ϵ to mean that the hidden constants depend on ϵ. Finding a pair of subsets of vertices that detect irregularity is the key bottleneck for the algorithmic proof of the regularity lemma. It was shown [1] that one can find an ϵ-regular partition with the number of parts at most an exponential tower of height $O(\epsilon^{-20})$ in an n-vertex graph in time $O_\epsilon(n^{\omega+o(1)})$.

Kohayakawa, Rödl, and Thoma [11] gave a faster algorithmic regularity lemma with optimal running time of $O_\epsilon(n^2)$. Alon and Naor [2] develop an algorithm which approximates the cut norm of a graph within a factor 0.56 using Grothendieck's inequality and apply this to find a polynomial time algorithm which finds, for a given pair of vertex subsets of order n which is not ϵ-regular, a pair of subsets which realize that the pair is not $\epsilon^3/2$-regular. Their approach gives an improvement on the tower height in the algorithmic regularity lemma to $O(\epsilon^{-7})$.

However, due to the tower-type dependence for the number of parts on the regularity parameter, these are not practical algorithms. While most graphs have a small regularity partition, the previous algorithmic proofs would not necessarily find it and would only guarantee to find a regular partition with a tower-type number of parts. Addressing this issue, Fischer, Matsliah, and Shapira [7] give a probabilistic algorithm which runs in time $O_\epsilon(n)$ which with high probability finds, in a graph which has an $\epsilon/2$-regular partition with k parts, an ϵ-regular partition with at most k parts. Tao [15] gives a probabilistic algorithm which with high probability in constant time (depending on ϵ) produces an ϵ-regular partition. The algorithm takes a random sample of vertices (the number of which is also random) and outputs the common refinement of the neighborhoods.

Still, it is desirable to have a fast *deterministic* algorithm for finding a regularity partition, which we obtain here. An example theorem of this sort is the following.

Theorem. *There exists an $O_{\epsilon,\alpha,k}(n^2)$ time algorithm, which, given $0 < \epsilon, \alpha < 1$ and k, and a graph G on n vertices that admits an equitable ϵ-regular partition with k parts, outputs an equitable $(1+\alpha)\epsilon$-regular partition of G into k parts.*

Thus, if a graph has a regular partition with few parts, then we can quickly find a regular partition (with a slight regularity loss) with the same number of parts.

Counting the number of copies of a graph H in another graph G is a famous algorithmic problem. A special case of this problem is to determine the clique number of a graph. This is a well-known NP-complete problem. In fact, Håstad [10] and Zuckerman [16] proved that it is NP-hard to approximate the clique number of a n-vertex graph within a factor $n^{1-\epsilon}$ for any $\epsilon > 0$.

There is a fast *probabilistic* algorithm for approximating up to ϵ the fraction of k-tuples which make a copy of H. The algorithm takes $s = 10\epsilon^{-2}$ samples of k-tuples of vertices uniformly at random from G and outputs the fraction of them that make a copy of H. The number of copies of H is a binomial random variable with standard deviation at most $s^{1/2}/2$, and hence the fraction of k-tuples which make a copy of H in this random sample is likely within ϵ of the fraction of k-tuples which makes copies of H. However, this algorithm has no guarantee of success. It is therefore desirable to have a *deterministic* algorithm for counting copies which gives an approximation for the subgraph count with complete certainty.

The algorithmic regularity lemma is useful for deterministically approximating the number of copies of any fixed graph in a graph. Duke, Lefmann, and Rödl [6] gave a faster approximation algorithm for the number of copies of H in a graph G. They first develop a weak regularity lemma which has an exponential dependence instead of a tower-type dependence. This gives an algorithm which runs in time $2^{(k/\epsilon)^{O(1)}} n^{\omega+o(1)}$ which computes the number of copies of a graph H on k vertices in a graph on n vertices up to an additive error of ϵn^k.

We give a faster approximation algorithm for the subgraph counting problem, improving the dependence on the error parameter from exponential to polynomial.

Theorem. *Let H be a graph with v vertices and e edges, and let $\epsilon > 0$ be given. There is a deterministic algorithm that runs in time $O_H(\epsilon^{-O(1)} n^{\omega+o(1)} + \epsilon^{-O(e)} n)$ which finds the number of copies of H in G up to an error of at most ϵn^v.*

For example, we can count the number of cliques of order 1000 in an n-vertex graph up to an additive error $n^{1000-10^{-6}}$ in time $O(n^{2.4})$. The proofs of these new results utilize recent algorithmic version of the Frieze–Kannan weak regularity lemma due to Dellamonica, Kalyanasundaram, Martin, Rödl, and Shapira [4], [5].

References

[1] N. Alon, R. A. Duke, H. Lefmann, V. Rödl, and R. Yuster, *The algorithmic aspects of the regularity lemma*, J. Algorithms **16** (1994), 80–109.

[2] N. Alon and A. Naor, *Approximating the cut-norm via Grothendieck's inequality*, SIAM J. Comput. **35** (2006), 787–803 (electronic).

[3] D. Conlon and J. Fox, *Bounds for graph regularity and removal lemmas*, Geom. Funct. Anal. **22** (2012), 1191–1256.

[4] D. Dellamonica, S. Kalyanasundaram, D. Martin, V. Rödl, and A. Shapira, *A deterministic algorithm for the Frieze-Kannan regularity lemma*, SIAM J. Discrete Math. **26** (2012), 15–29.

[5] D. Dellamonica, Jr., S. Kalyanasundaram, D. M. Martin, V. Rödl, and A. Shapira, *An optimal algorithm for finding Frieze-Kannan regular partitions*, Combin. Probab. Comput. **24** (2015), 407–437.

[6] R. A. Duke, H. Lefmann, and V. Rödl, *A fast approximation algorithm for computing the frequencies of subgraphs in a given graph*, SIAM Journal on Computing **24** (1995), 598–620.

[7] E. Fischer, A. Matsliah, and A. Shapira, *Approximate hypergraph partitioning and applications*, SIAM Journal on Computing **39** (2010), 3155–3185.

[8] J. Fox and L. M. Lovász, *A tight lower bound for Szemerédi's regularity lemma*, arXiv:1403.1768.

[9] W. T. Gowers, *Lower bounds of tower type for Szemerédi's uniformity lemma*, Geom. Funct. Anal. **7** (1997), 322–337.

[10] J. Håstad, *Clique is hard to approximate within $n^{1-\epsilon}$*, Acta Mathematica **182** (1999), 105–142.

[11] Y. Kohayakawa, V. Rödl, and L. Thoma, *An optimal algorithm for checking regularity*, SIAM J. Comput. **32** (2003), 1210–1235.

[12] F. Le Gall, *Powers of tensors and fast matrix multiplication*, Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC '14, ACM, 2014, pp. 296–303.

[13] G. Moshkovitz and A. Shapira, *A short proof of Gowers' lower bound for the regularity lemma*, Combinatorica, to appear.

[14] E. Szemerédi, *Regular partitions of graphs*, Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976), Colloq. Internat. CNRS, vol. 260, CNRS, Paris, 1978, pp. 399–401.

[15] T. Tao, *An epsilon of room, II*, American Mathematical Society, Providence, RI, 2010.

[16] D. Zuckerman, *Linear degree extractors and the inapproximability of max clique and chromatic number*, Theory of computing **3** (2007), 103–128.

Ramsey goodness of paths

Benny Sudakov
(joint work with Alexey Pokrovskiy)

Given a pair of graphs G and H, the Ramsey number $R(G,H)$ is the smallest N such that every red-blue coloring of the edges of the complete graph K_N contains a red copy of G or a blue copy of H. It is a corollary of the celebrated theorem of Ramsey that these numbers are always finite. Let $\chi(H)$ be the chromatic number of H, i.e. the smallest number of colors needed to color the vertices of H so that no pair of adjacent vertices have the same colour, and $\sigma(H)$ be the the size of the smallest color class in a $\chi(H)$-colouring of H. It was observed by Burr [2] that for connected G with $|G| \geq \sigma(H)$ Ramsey numbers always satisfy the following easy lower bound

$$R(G,H) \geq (|G|-1)(\chi(H)-1)+\sigma(H). \tag{1}$$

To prove (1), consider a 2-edge-coloring of the complete graph on $N = (|G|-1)(\chi(H)-1)+\sigma(H)-1$ vertices consisting of $\chi(H)-1$ disjoint red cliques of size $|G|-1$ as well as one disjoint red clique of size $\sigma(H)-1$. This coloring has no red G because all red connected components have size $\leq |G|-1$, and there is no blue H since the partition of this H induced by red cliques would give a coloring of H by $\chi(H)$ colors with one color class smaller than $\sigma(H)$, contradicting the definition of $\sigma(H)$.

For some graphs the bound in (1) is quite far from the truth. For example Erdős [6] showed that $R(K_n,K_n) \geq \Omega(2^{n/2})$ which is much larger than the quadratic bound we get from (1). However there are many known pairs of graphs for which $R(G,H) = (|G|-1)(\chi(H)-1)+\sigma(H)$. In this case we say that *G is H-good*. The notion of Ramsey goodness was introduced by Burr and Erdős [3] in 1983 and was extensively studied since then, see, e.g., [1, 4, 5, 10, 8, 9] and their references.

In this short note we study the question of when the n-vertex path P_n is H-good, for some fixed graph H. This problem goes back to the work of Erdős, Faudree, Rousseau, and Schelp [7], who in 1985 proved that there is a function f such that P_n is H-good for all $n \geq f(|H|)$. The function $f(|H|)$ is not explicit in [7], but $f(H) = O(|H|^4)$ can be proved using their method. Häggkvist [11] (for $k = 2$) and later Pokrovskiy [13] obtained a general upper bound on the Ramsey number of path versus complete k-partite graphs, showing that $R(P_n, K_{m,\dots,m}) \leq (k-1)(n-1)+km-k+1$. Here and later, $K_{m_1,\dots,m_k}$ denotes a complete k-partite graph with parts of order $m_1,\dots,m_k$ together with all the edges connecting vertices in different parts. Although this bound is not strong enough to prove goodness, it holds for all values of the parameters. More recently, Pei and Li [12] showed that if $n \geq 8|H| + 3\sigma(H)^2 + c\chi^8(H)$, then P_n is H-good. For general H (e.g., when $H = K_{m,m}$) this result requires n to be quadratic in $|H|$. Allen, Brightwell, and Skokan [1] conjectured that P_n is H-good already when n is linear in $|H|$.

Conjecture 1 ([1])**.** *Let H be a fixed graph with chromatic number k and let $n \geq k|H|$. Then $R(P_n,H) = (n-1)(k-1)+\sigma(H)$.*

Let $R(C_{\geq n}, H)$ be the smallest N such that any 2-edge-coloring of K_N contains either a red cycle of length at least n or a blue H. Notice that we always have $R(P_n,H) \leq R(C_{\geq n},H)$. Motivated by the above conjecture, we prove the following theorem.

Theorem 2. *Given integers $m_1 \leq m_2 \leq \cdots \leq m_k$ and $n \geq 3m_k + 5m_{k-1}$, we have*

$$R(C_{\geq n}, K_{m_1,\dots,m_k}) = (k-1)(n-1)+m_1.$$

Notice that the vertices of a k-chromatic graph H can be partitioned into k independent sets of sizes $m_1, \dots, m_k$ with $\sigma(H) = m_1 \leq m_2 \leq \cdots \leq m_k$. This is equivalent to H being a subgraph of $K_{m_1,\dots,m_k}$. Since $4|H| \geq 4m_k + 4m_{k-1} \geq 3m_k + 5m_{k-1}$, Theorem 2 implies the following.

Corollary 3. *Let H be a fixed graph with chromatic number k and let $n \geq 4|H|$. Then $R(P_n, H) = (n-1)(k-1) + \sigma(H)$.*

For $k \geq 4$, this corollary proves Conjecture 1 in a very strong form, showing that the condition $n \geq \chi(H)|H|$ is unnecessary, and $n \geq 4|H|$ suffices. For $k \leq 3$, our result is slightly weaker than the conjecture, but is a large improvement on the best previously known [12] quadratic dependence of n on $|H|$. Moreover, for certain graphs H, Theorem 2 shows that P_n is H-good even when n is smaller than $4|H|$. For example if H is balanced (i.e. if $|H| = \sigma(H)\chi(H)$), then this theorem implies that P_n is H-good as long as $n \geq 8|H|/\chi(H)$.

References

[1] P. Allen, G. Brightwell and J. Skokan. Ramsey-goodness and otherwise. *Combinatorica* **33** (2013), 125–160.

[2] S. Burr. Ramsey numbers involving graphs with long suspended paths. *J. London Math. Soc.* **24** (1981), 405–413.

[3] S. Burr and P. Erdős. Generalizations of a Ramsey-theoretic result of Chvátal. *J. Graph Theory* **7** (1983), 39–51.

[4] V. Chvátal. Tree-complete graph Ramsey number. *J. Graph Theory* **1** (1977), 93.

[5] D. Conlon, J. Fox, C. Lee and B Sudakov. Ramsey numbers of cubes versus cliques. *Combinatorica*, to appear.

[6] P. Erdős. Some remarks on the theory of graphs. *Bull. Am. Math. Soc.* **53** (1947), 292–294.

[7] P. Erdős, R. Faudree, C. Rousseau and R. Schelp. Multipartite graph-sparse graph Ramsey numbers. *Combinatorica* **5** (1985), 311–318.

[8] V. Nikiforov. The cycle-complete graph Ramsey numbers. *Combin. Probab. Comput.* **14** (2005), 349–370.

[9] V. Nikiforov and C. Rousseau. Ramsey goodness and beyond. *Combinatorica* **29** (2009), 227–262.

[10] G. Fiz Pontiveros, S. Griffiths, R. Morris, D. Saxton and J. Skokan. The Ramsey number of the clique and the hypercube. *J. Lond. Math. Soc.* **89** (2014), 680–702.

[11] R. Häggkvist. On the path-complete bipartite Ramsey number. *Discrete Math.* **75** (1989), 243–245.

[12] C. Pei and Y. Li. Ramsey numbers involving a long path. *Discrete Math.* **339** (2016), 564–570.

[13] A. Pokrovskiy. Calculating Ramsey numbers by partitioning coloured graphs, preprint.

Finding a Large Submatrix of a Gaussian Random Matrix

David Gamarnik

(joint work with Quan Li)

We consider the algorithmic problem of finding a submatrix of a given random matrix such that the average value of the submatrix is appropriately large. Specifically, consider an $n \times n$ matrix $\mathbf{C}^n$ with i.i.d. standard Gaussian entries. Given

$k \leq n$, the goal is to find algorithmically a $k \times k$ submatrix $\mathbf{A}$ of $\mathbf{C}^n$ (not necessarily principal) with average entry as large as possible. The problem has motivations in several areas, including biomedicine, genomics and social networks [2, 3, 4].

The problem of finding asymptotically the largest average entry of $k \times k$ submatrices of $\mathbf{C}^n$ was recently studied by Bhamidi et.al. [1] (see also [5] for a related study) and questions arising in this paper constitute the motivation for our work. It was shown in [1] using a non-constructive method of moments that the largest achievable average entry of a $k \times k$ submatrix of $\mathbf{C}^n$ is asymptotically with high probability (w.h.p.) $(1 + o(1))2\sqrt{\log n/k}$ when $k = O(\log n/ \log\log n)$. Here $o(1)$ denotes a function converging to 0 as $n \to \infty$ regardless of k. Furthermore, the authors consider the asymptotic value and the number of so-called locally maximum matrices. A $k \times k$ matrix $\mathbf{A}$ is locally maximal if every $k \times k$ matrix of $\mathbf{C}^n$ with the same set of rows as $\mathbf{A}$ has a smaller average value than $\mathbf{A}$ and every $k \times k$ matrix of $\mathbf{C}^n$ with the same set of columns as $\mathbf{A}$ has a smaller average value than $\mathbf{A}$. Such local maxima are natural objects arising as terminal matrices produced by a simple iterative procedure called Large Average Submatrix ($\mathcal{LAS}$), designed for finding a matrix with a large average entry. $\mathcal{LAS}$ proceeds by starting with an arbitrary $k \times k$ submatrix $\mathbf{A}_0$ and finding a matrix $\mathbf{A}_1$ sharing the same set of rows with $\mathbf{A}_0$ which has the largest average value. The procedure is then repeated for $\mathbf{A}_1$ by searching through columns of $\mathbf{A}_1$ and identifying the best matrix $\mathbf{A}_2$. The iterations proceed while possible and at the end some locally maximum matrix $\mathbf{A}_{\mathcal{LAS}}$ is produced as the output. The authors show that when k is constant, the majority of locally maximum matrices of $\mathbf{C}^n$ have an asymptotic value $(1+o(1))\sqrt{2\log n/k}$ w.h.p., thus factor $\sqrt{2}$ smaller than the global optimum. Motivated by this finding, the authors suggest that the outcome of the $\mathcal{LAS}$ algorithm should be also factor $\sqrt{2}$ smaller than the global optimum, however one cannot deduce this from the result of [1] since it is not ruled out that $\mathcal{LAS}$ is clever enough to find a “rare” local maximum with a significantly larger average value than $\sqrt{2\log n/k}$.

In this paper [6] we show that the matrix produced by the $\mathcal{LAS}$ algorithm is indeed $(1 + o(1))\sqrt{2\log n/k}$ w.h.p. when k is constant and n grows. Then by drawing an analogy with the problem of finding cliques in random graphs, we propose a simple greedy algorithm which produces a $k \times k$ matrix with asymptotically the same average value $(1 + o(1))\sqrt{2\log n/k}$ w.h.p., for $k = o(\log n)$. Since the greedy algorithm is the best known algorithm for finding cliques in random graphs, it is tempting to believe that beating the factor $\sqrt{2}$ performance gap suffered by both algorithms might be very challenging. Surprisingly, we show the existence of a very simple algorithm which produces a $k \times k$ matrix with average value $(1 + o_k(1))(4/3)\sqrt{2\log n/k}$ for $k = O(\log n)$. Here $o_k(1)$ denotes a function decaying to zero as k increases.

To get an insight into the algorithmic hardness of this problem, and motivated by the so-called *Overlap Gap Property* (OGP) observed in several spin glass models, we study the OGP in the context of our problem in the following way. We fix $\alpha \in (1, \sqrt{2})$ and let $\mathcal{L}(\alpha)$ denote the set of matrices with average value asymptotically $\alpha\sqrt{2\log n/k}$. Thus α conveniently parametrizes the range between the achievable value on the one hand, namely $\alpha = 1$ for $\mathcal{LAS}$ and greedy algorithms, $\alpha = 4/3$ for the new algorithm we propose, and $\alpha = \sqrt{2}$ for the global optimum on the other hand. For every pair of matrices $\mathbf{A}_1$, $\mathbf{A}_2 \in \mathcal{L}(\alpha)$ with row sets I_1, I_2 and column sets J_1, J_2 respectively, let $x(\mathbf{A}_1, \mathbf{A}_2) = |I_1 \cap I_2|/k$, $y(\mathbf{A}_1, \mathbf{A}_2) = |J_1 \cap J_2|/k$. Namely x and y are the normalized counts of the common rows and common columns for the two matrices. For every $(x, y) \in [0, 1]^2$ we consider the expected number of pairs $\mathbf{A}_1$, $\mathbf{A}_2$ such that $x(\mathbf{A}_1, \mathbf{A}_2) \approx x$, $y(\mathbf{A}_1, \mathbf{A}_2) \approx y$ in some appropriate sense. We compute this expectation asymptotically. We define $R(x, y) = 0$ if such an expectation converges to zero as $n \to \infty$ and $= 1$ otherwise. Thus the set $\mathcal{R}(\alpha) = \{(x, y) : R(x, y) = 1\}$ describes the set of achievable in expectation overlaps of pairs of matrices with average value $\alpha\sqrt{2 \log n/k}$. At $\alpha^* = 5\sqrt{2}/(3\sqrt{3}) \approx 1.3608..$ we observe an interesting phase transition – the set $\mathcal{R}(\alpha)$ is connected for $\alpha < \alpha^*$, and is disconnected for $\alpha > \alpha^*$. For $\alpha > \alpha^*$, we say that the model exhibits the OGP. That is, the overlaps of two matrices belong to one of the two disconnected regions. We conjecture that OGP observed for $\alpha > \alpha^*$ also marks the onset of the algorithmic hardness - no polynomial time algorithm exists for finding matrices with average value at least $(1 + o(1))\alpha\sqrt{2 \log n/k}$, when $\alpha > \alpha^*$ and k is a growing function of n.

References

[1] S. Bhamidi, P. Dey and N. Andrew, *Energy Landscape for large average submatrix detection problems in Gaussian random matrices*, arXiv preprint arXiv:1211.2284 (2012).

[2] A. Shabalin, V. Weigman, P. Charles and N. Andrew, *Finding large average submatrices in high dimensional data*, The Annals of Applied Statistics (2009), 985–1012.

[3] S. Madeira and A. Oliveira, *Biclustering algorithms for biological data analysis: a survey*, IEEE/ACM Transactions on Computational Biology and Bioinformatics **1** (2004), 24–45.

[4] S. Fortunato, *Community detection in graphs*, Physics Reports **486** (2010), 75–174.

[5] X. Sun and A. Nobel, *On the maximal size of Large-Average and ANOVA-fit Submatrices in a Gaussian Random Matrix*, Bernoulli **19** (2013), 275-294.

[6] D. Gamarnik and Q. Li, *Finding a Large Submatrix of a Gaussian Random Matrix*, arXiv preprint arXiv:1602.08529 (2016).

A sparse regular approximation lemma

Asaf Shapira

(joint work with Guy Moshkovitz)

We introduce a new variant of Szemerédi's regularity lemma which we call the *sparse regular approximation lemma* (SRAL). The input to this lemma is a graph G of edge density p and parameters $\epsilon \ll \delta$. The goal is to construct an ϵ-regular partition of G while having the freedom to add/remove up to $\delta|E(G)|$ edges. As we show, this weaker variant of the regularity lemma already suffices for proving the graph removal lemma and the hypergraph regularity lemma, which are two of the main applications of the (standard) regularity lemma. This of course raises the following question: can one obtain quantitative bounds for SRAL that are significantly better than those associated with the regularity lemma?

Formally, for every ϵ, δ, $p > 0$ let $S = S(\epsilon, \delta, p)$ be the smallest integer so that if G is a graph of density at least p, and $\mathcal{P}_0$ is an equipartition of $V(G)$ of order at most $1/\epsilon$, then one can add/remove at most $\delta|E(G)|$ edges and thus turn G into a graph that has an ϵ-regular equipartition that refines $\mathcal{P}_0$ and has order at most S. Observe that if we allow δ to depend on ϵ, say if $\delta = \epsilon^4$, then $S(\epsilon, \epsilon^4, p) \geq M(2\epsilon) \geq \text{twr}(\text{poly}(1/\epsilon))$. Indeed, this follows from the simple observation that an ϵ-regular bipartite graph remains 2ϵ-regular if only ϵ^3-fraction of the possible edges are added/removed. Hence, the main interest in SRAL is when $\delta < 1$ is constant. As we show, even in this case SRAL has some unexpected applications. In fact, SRAL will be interesting even when $\epsilon = \text{poly}(p)$, hence our main interest will be in bounding the function $S(\text{poly}(p), \delta_0, p)$ for constant δ_0.

One of our main motivations for introducing SRAL is that one can in fact prove the *graph removal lemma* using SRAL. The celebrated graph removal lemma of Ruzsa and Szemerédi [11] states that for every fixed graph H there is a function $\text{Rem}_H(\epsilon)$ so that if one must remove from an n-vertex graph G at least ϵn^2 edges in order to make it H-free then G contains at least $n^h/\text{Rem}_H(\epsilon)$ copies of H, where $h = |V(H)|$. The standard proof of the removal lemma, via the regularity lemma, establishes the bound $\text{Rem}_H(\epsilon) \leq M(\text{poly}(\epsilon)) = \text{twr}(\text{poly}(1/\epsilon))$. The fact that SRAL implies the removal lemma is stated explicitly as follows.

Theorem 1. *For any graph H on $h \geq 3$ vertices we have*

$$\text{Rem}_H(\epsilon) \leq \left[S\big((\epsilon/h)^{h^2},\, 1/4h^4,\, \epsilon\big) \cdot (h/\epsilon)^{2h}\right]^h .$$

The proof of the Theorem 1 is much more delicate than the usual proof of the removal lemma via the standard regularity lemma, mainly due to having to work with a modified version of the input graph. In particular, we need to prove a counting lemma which is suitable for SRAL. This leads to the following question; can one obtain a significantly better bound for $S(\text{poly}(p), \delta, p)$ than $\text{twr}(\text{poly}(1/p))$?

Before describing our solution of the above problem, we first describe a related variant of the regularity lemma. As the name SRAL suggests, it is a variant of the so called *regular approximation lemma* (RAL for short). The RAL was introduced as part of the study of graph limits and of the hypergraph regularity lemma by Lovász and Szegedy [7] and Rödl and Schacht [9], respectively.

Let us define a special case of RAL. For $\epsilon, \delta > 0$ let $T = T(\epsilon, \delta)$ be defined similarly to $S(\epsilon, \delta, p)$, only that the number of allowed edge modification is δn^2 rather than $\delta|E(G)|$, and p, the density of G, is unconstrained. (The full-fledged RAL allows one to replace ϵ with an arbitrary function f, so that the equipartition $\mathcal{P}$ is such that all pairs are $f(|\mathcal{P}|)$-regular.) Notice we have the trivial relation

$$S(\epsilon, \delta, p) \leq T(\epsilon, \delta p) . \tag{1}$$

The upper bounds obtained in [7, 9], when specialized to the definition of $T(\epsilon, \delta)$, are no better than the trivial $T(\epsilon, \delta) \leq M(\epsilon) = \text{twr}(\text{poly}(1/\epsilon))$ bound that follows from the regularity lemma. A considerably better bound was given by Conlon and Fox [1] who showed that $T(\epsilon, \delta) \leq \text{twr}_{1/\epsilon}(\text{poly}(1/\delta))$, where $\text{twr}_y(x)$ denotes a tower of x exponents with y at the top. Note that for a fixed δ, this is a fixed number of exponents, which is significantly better than the $\mathrm{twr}(\mathrm{poly}(1/\epsilon))$ bound given by the regularity lemma. However, even this bound implies, via (1), that when δ is a fixed constant and $\epsilon = \mathrm{poly}(p)$ we have $S(\epsilon, \delta, p) \leq \mathrm{twr}_{1/\epsilon}(\mathrm{poly}(1/\delta p)) = \mathrm{twr}(\mathrm{poly}(1/\epsilon))$, which does not improve over the regularity lemma.

Our first bound shows one can improve the bound of the regularity lemma, even if the number of modifications allowed is relative to the graph's density.

Theorem 2. *There is $c > 0$ such that $S(\epsilon, \delta, p) \leq \mathrm{twr}_{1/\epsilon}(c \log(1/p)/\delta^2)$. In particular, for every fixed $C, \delta_0 > 0$ we have*

$$S(p^C, \delta_0, p) \leq \mathrm{twr}(O(\log(1/p))) .$$

Since we trivially have $T(\epsilon, \delta) \leq S(\epsilon, \delta, 1/2)$, Theorem 2 immediately gives as a special case the bound $T(\epsilon, \delta) \leq \mathrm{twr}_{1/\epsilon}(\mathrm{poly}(1/\delta))$ for RAL, which was first proved in [1]. We note that, just like the full-fledged RAL, our proof of Theorem 2 gives a much more general result where the partition is such that all the pairs are ϵ-regular and where ϵ is a function of the order of the partition.

The proof of Theorem 2 is motivated by the one taken by Conlon and Fox [1], using an iterated version of the weak regularity lemma of Frieze and Kannan [4]. Our proof however differs in two important aspects. First, we use (and prove) a new variant of the weak regularity lemma which we need for our purposes. Second, we use the entropy potential function (first used by Fox [2]) together with Pinsker's inequality from information theory, in order to control the ℓ_1-distance, *relative to the graph's density*, between partitions with similar entropy potentials. An immediate application of Theorems 1 and 2 gives the following:

Corollary 3. *For every h-vertex graph H we have* $\mathrm{Rem}_H(\epsilon) \leq \mathrm{twr}(O(\log(1/\epsilon)))$.

As is of course well known, the above bound for the removal lemma was first obtained by Fox [2], who was the first to improve upon the $\mathrm{twr}(\mathrm{poly}(1/\epsilon))$ bound that follows from applying the regularity lemma. We think it is important to see that this result can be derived from an appropriate regularity lemma and not just from an ad-hoc argument.

The possibility of obtaining even better bounds for the removal lemma (via Theorem 1) naturally raises the question if one can obtain even better bounds for SRAL, say, $\mathrm{twr}_{1/\epsilon}(\mathrm{poly}(1/\delta))$ as the one obtained by Conlon and Fox [1] for RAL. As our second result shows, such an improvement is not possible, even when $\epsilon = p^5$ and δ is a fixed constant.

Theorem 4. *There are fixed constants $\delta_0, c > 0$ such that*

$$S(p^5, \delta_0, p) \geq \mathrm{twr}(c \log(1/p)) . \tag{2}$$

Furthermore, one can decompose the complete bipartite graph into $1/p$ graphs of density p so that each of them witnesses (2).

The proof of (2) is by far the most complicated part of this paper. While the construction has a (relatively) simple description, proving its correctness requires a very careful analysis, employing some ideas we used in [8], together with those of Gowers [5]. The main difficulty lies in handling an absolute constant δ_0 (we obtain $\delta_0 = 10^{-11}$ but make no effort to optimize it), i.e., even when the graph is very sparse and one is allowed to change a constant fraction of its edges!

Finally, we believe that an important aspect of Theorem 4 is in being a major step towards proving lower bounds for the *hypergraph* regularity lemma [6, 10, 12]. We have very strong evidence that the construction used to prove the "furthermore part" of Theorem 4 can be used as a key building block for proving a Wowzer-type lower bound for the 3-graph regularity lemma of Frankl and Rödl [3]. We intend to return to this subject in the near future.

References

[1] D. Conlon and J. Fox, *Bounds for graph regularity and removal lemmas*, GAFA **22** (2012), 1191–1256.

[2] J. Fox, *A new proof of the graph removal lemma*, Ann. of Math. **174** (2011), 561–579.

[3] P. Frankl and V. Rödl, *Extremal problems on set systems*, Random Struct. Algor. **20** (2002), no. 2, 131–164.

[4] A. Frieze and R. Kannan, *Quick approximation to matrices and applications*, Combinatorica **19** (1999), no. 2, 175–220.

[5] T. Gowers, *Lower bounds of tower type for Szemerédi's uniformity lemma*, GAFA **7** (1997), 322–337.

[6] T. Gowers, *Hypergraph regularity and the multidimensional Szemerédi theorem*, Ann. of Math. **166** (2007), 897–946.

[7] L. Lovász and B. Szegedy, *Szemerédi's lemma for the analyst*, Geom. Funct. Anal. **17** (2007), no. 1, 252–270.

[8] G. Moshkovitz and A. Shapira, *A short proof of Gowers's lower bound for the regularity lemma*, Combinatorica, to appear.

[9] V. Rödl and M. Schacht, *Regular partitions of hypergraphs: regularity lemmas*, Combin. Probab. Comput. **16** (2007), no. 6, 833–885.

[10] V. Rödl and J. Skokan, *Regularity lemma for uniform hypergraphs*, Random Struct. Algor. **25** (2004), 1–42.

[11] I. Z. Ruzsa and E. Szemerédi, *Triple systems with no six points carrying three triangles*, in Combinatorics (Keszthely, 1976), Coll. Math. Soc. J. Bolyai 18, Volume II, 939-945.

[12] T. Tao, *A variant of the hypergraph removal lemma*, J. Combin. Theory Ser. A **113** (2006), 1257–1280.

Problem Session

Nathan Linial (chair)

Zeev Dvir

Coloring the complete bipartite graph with no zero cycles

The following problem was communicated to me by Sergey Yekhanin. Let $K_{n,n}$ denote the complete bipartite graph on $2n$ vertices. Let $\mathbb{F}_2$ denote the field of two elements. Let $t(n)$ be the minimum integer $t \geq 1$ so that we can color the edges of $K_{n,n}$ with elements of $\mathbb{F}_2^t$ so that the sum over each cycle is non-zero (in $\mathbb{F}_2^t$). The problem is to determine $t(n)$ asymptotically as n tends to infinity. It is known that

$$\Omega(\log^2(n)) \leq t(n) \leq O(n \log(n)),$$

where the upper bound can be obtained from a random coloring (but also explicitly) and the lower bound requires a clever proof by induction. See [1] for the proofs and the motivation for the problem which comes from error correcting codes with local recovery properties.

References

[1] P. Gopalan, G. Hu, S. Saraf, C. Wang and S. Yekhanin, *Maximally Recoverable Codes*, Manuscript (2016).

Bhargav Narayanan

Laws for the symmetric group

A word w from the free group over two letters defines a map $f_w : S_n \times S_n \to S_n$ by composition: for example, if $w = aba^{-1}$, then $f_w(\pi, \sigma) = \pi \circ \sigma \circ \pi^{-1}$. A word w is a *law* for S_n if f_w maps every pair of permutations to the identity permutation. How long is the shortest non-trivial law for S_n?

There has been a lot of work on constructing short laws; the record belongs to Kozma and Thom who recently constructed laws of length $\exp((\log n)^{O(1)})$. However, we do not seem to know much about lower bounds. A lower bound of $n-1$ is an easy exercise. This almost trivial bound is pretty close to the state of the art; the best known lower bound is $2n-2$ and this is due to Buskin.

Ehud Friedgut

Partitioning the symmetric group into cosets

A t-coset of S_n is a coset of a subgroup which is the stabilizer of t points. Show that for every fixed t and sufficiently large n, any partition of S_n into t-cosets is a refinement of a partition into $(t-1)$-cosets.

This turns out to be false; a counterexample was found by Gábor Tardos.

Johannes Lengler

Diameter of Geometric Power Law Random Graphs

Consider the following random graph model with constant parameters $2 < \beta < 3$, $d \in \mathbb{N}$, and $\alpha > 1$. The graph has n vertices. Every vertex v draws independently

- a weight w_v from a power-law distribution with parameter β and minimum 1, i.e., $\mathbb{P}[w_v \geq w] = w^{1-\beta}$ for all $w \geq 1$.
- a position x_v u.a.r. from the d-dimensional torus $[0,1]^d$.

Then for each pair (u, v) of vertices we flip a coin, and we connect them with probability

$$p_{uv} = \min\left\{1, \left(\frac{w_u w_v}{n||x_u - x_v||^d}\right)^{\alpha}\right\}.$$

Details to the model can be found in [1, 2]. Here we just mention that the marginal edge probability is

$$\mathbb{P}_{x_u,x_v}[(u,v) \in E] = \Theta\left(\min\left\{1, \frac{w_u w_v}{n}\right\}\right),$$

as in Chung-Lu random graphs. Hence, $\deg(v)$ converges in distribution to $\mathrm{Poi}(\mu)$ for some $\mu = \Theta(w_v)$. Moreover, almost surely there is a giant component of linear size, all other components have size $(\log n)^{O(1)}$, and the average distance in the giant is $(2 + o(1))\frac{\log\log n}{|\log(\beta-2)|}$.

Conjecture. *Almost surely, every component of the graph has diameter $O(\log n)$.*

It should be mentioned that the giant component is easily seen to have diameter $\Omega(\log n)$ almost surely, and that an upper bound of $(\log n)^{O(1)}$ for the diameter is known. Moreover, the size of the second largest component is $(\log n)^{1+\Omega(1)}$, so the conjecture is nontrivial even for smaller components.

References

[1] K. Bringmann, R. Keusch, and J. Lengler. Geometric inhomogeneous random graphs. *arXiv:1511.00576 [cs.SI]*, 2015.

[2] K. Bringmann, R. Keusch, and J. Lengler. Average distance in a general class of scale-free networks with underlying geometry. *arXiv:1602.05712 [cs.DM]*, 2016.

Noga Alon

When are random permutations k-universal?

A sequence $(x_1, x_2, \dots, x_k)$ of distinct reals defines a permutation $\sigma \in S_k$ in a natural way: $\sigma(i) < \sigma(j)$ iff $x_i < x_j$. For $n > k$, a sequence $(x_1, x_2, \dots, x_n)$ of n distinct reals contains a permutation $\sigma \in S_k$ if there is a subsequence $(x_{i_1}, x_{i_2}, \dots, x_{i_k})$ defining σ. It is k-universal if it contains every $\sigma \in S_k$. Let $f(k)$ be the minimum $n = n(k)$ so that a random sequence of n reals in $[0, 1]$ chosen uniformly and independently is k universal with high probability.

Quite some time ago (see [1]) I conjectured that $f(k) = (\frac{1}{4} + o(1))k^2$, and observed that $f(k) \geq (\frac{1}{4}+o(1))k^2$ by the known results about the longest increasing subsequence of a random permutation. It is worth noting that this contradicts another (open) conjecture asserting that the minimum possible length of a k-universal sequence is $(1/2 + o(1))k^2$.

The following weaker version of the conjecture is also open:

Conjecture. *$f(k) \leq 1000k^2$.*

It is easy to show that $f(k) \leq O(k^2 \log k)$.

References

[1] R. Arratia, *On the Stanley-Wilf Conjecture for the Number of Permutations Avoiding a Given Pattern*, Elec. J. Combinatorics **6** (1999), N1.

Oliver Riordan

What can one say about three up-sets?

If A and B are up-sets (increasing events) in a (finite, say) product probability space, then Harris's Lemma says that $\mathbb{P}(A \cap B) \geq \mathbb{P}(A)\mathbb{P}(B)$. In this generality, there is of course nothing further to say: given real numbers $p_{00}, p_{01}, p_{10}, p_{11} \geq 0$ summing to 1, there exist increasing events in some product probability space with $\mathbb{P}(A^c \cap B^c) = p_{00}$, $\mathbb{P}(A^c \cap B) = p_{01}$, etc, if and only if $p_{11} \geq (p_{10} + p_{11})(p_{01} + p_{11})$.

What about three up-sets A, B and C? Applying Harris's Lemma to $A \cup B$ and C, etc, gives certain inequalities, but in terms of the 8 probabilities p_{000}, p_{001}, etc, these conditions turn out not to be sufficient for realisability by three up-sets. (For example, Jeff Kahn, Béla Bollobás and I, and Milanka Jankovic have found non-realisable examples.) Siddhartha Sahi [1] has conjectured (among other things) that the additional inequality $2\mathbb{P}(A \cap B \cap C) - \mathbb{P}(A \cap B)\mathbb{P}(C) - \mathbb{P}(A \cap C)\mathbb{P}(B) - \mathbb{P}(B \cap C)\mathbb{P}(A) + \mathbb{P}(A)\mathbb{P}(B)\mathbb{P}(C) \geq 0$ holds, but not that this is sufficient.

It seems conceivable that if the realisable subset of $[0,1]^8$ has a manageable description, this might be easier to prove by induction than any particular inequality or incomplete set of inequalities.

References

[1] S. Sahi, *Higher correlation inequalities*, Combinatorica **28** (2008), 209–227.

Van Vu

Tail bounds for the number of Hamiltonian cycles

The following problem came up in our recent studies with A. Ferber and D. Montelegre (both at Yale).

Problem. *Let $G(n,m)$ denote the random graph on n vertices and m edges, where $m = \Theta(n^2)$. Let H be the number of Hamiltonian cycles in the graph. Let μ be its expectation. The problem is to estimate the probability that $H \leq \frac{mu}{2}$.*

A variance computation shows that one can have a bound of order $1/n$. The truth is probably much smaller. Also notice that if we replace $G(n,m)$ by $G(n,p)$, the answer is $\Theta(1)$.

Nati Linial

Girth vs. Diameter

We consider here only graphs in which all vertex degrees are at least 3.

Consider the distance between two diametrically opposite vertices in a shortest cycle in a graph G to derive the well known fact that diameter$(G) \geq \frac{\text{girth}(G)-1}{2}$.

Question. *What is* $x = \limsup \frac{girth(G)}{diameter(G)}$ *(as diameter*$(G) \to \infty$*)?*

Clearly $2 \geq x$. It is also known (e.g., [1]) and can be shown in numerous ways that $x \geq 1$, but this is all I know. Most concretely, I wonder whether x is strictly bigger than 1.

References

[1] Erdős, Paul; Sachs, Horst *Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl.* (German) Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe **12** 1963 251–257.

Random graphs have simple spectrum

Van Vu

In the 1980s, Babai [1] posed the following conjecture

Conjecture 1. *$G(n, 1/2)$ has simple spectrum, with probability* $1 - o(1)$.

A (hermitian) matrix has simple spectrum if its eigenvalues are different. A graph has simple spectrum if its adjacency matrix does. $G(n, 1/2)$ is, as usual, the Erdős-Rényi graph with density 1/2.

In a recent paper [3], Tao and Vu proved Babai's conjectrure. Their proof holds for a large class of random matrices with independent (but not necessarily iid entries). As a matter of fact, the only condition required is that the entries are not concentrated on one point (in other words, they need to be truly random).

In a subsequent paper [4], Nguyen and the above two authors studied a harder problem of bounding the gaps between consecutive eigenvalues. Their results are near optimal and have applications in many areas, including the studies of nodal domains, numerical analysis, mathematical physics and control theory.

A key tool in the proof is the so-called Inverse Littlewood-Offord theorems, developed in the last 10 years or so. These theorems form a new and essential part of the theory of Anti-concentration; see [2] for a survey.

References

[1] L. Babai, Personal communication to the author, Chicago, 2012.

[2] H. Nguyen, V. Vu, *Small ball probability, inverse theorems, and applications,* Erdős centennial proceeding, 409–463, Bolyai Soc. Math. Stud., 25, János Bolyai Math. Soc., Budapest, 2013.

[3] T. Tao, V, Vu, *Random matrices have simple spectrum*, Combinatorica, *to appear.*

[4] H. Nguyen, T. Tao, V. Vu, *Random matrices: Tail bounds for gaps between eigenvalues*, Probability and Related Fields, *to appear.*

Rigorous Analysis of a Randomised Number Field Sieve

Jonathan Lee
(joint work with Ramarathnam Venkatesan)

For real numbers a, b, x, we write

$$L_x(a,b) = \exp\left(b(\log x)^a (\log\log x)^{1-a}\right).$$

Integer factorisation is of fundamental importance both in algorithmic number theory and in cryptography. In the latter setting, it is especially important to have effective bounds on the run time of existing algorithms, as many existing systems depend on being able to produce integers whose factorisations will remain unknown for decades, even allowing for the rapid increases in the cost-effectiveness of computational hardware. For example, an understanding of the factoring of numbers n with $\log_2 n \approx 4096$ is important in practice, while the public record for a factorisation of a general number stands at $\log_2 n \approx 768$. A uniform and effective bound will be useful in understanding the run time as $\log_2 n$ increases.

The Number Field Sieve (NFS) has been the state of the art algorithm for factorisation since its introduction nearly three decades ago [1]. Unfortunately, its analysis has been thus far entirely heuristic [6], with the claimed run time on an input n of $L_n\left(\frac{1}{3}, \sqrt[3]{\frac{64}{9}} + o(1)\right)$. This became of practical importance in the mid 1990s when it bettered the (also heuristic) $L_n\left(\frac{1}{2}, 1+o(1)\right)$ run time of the previous champion Quadratic Number Field Sieve.

Even assuming standard conjectures (e.g.; GRH), there is no analysis that any substantial part of the NFS will halt. In particular, the NFS and other algorithms critically depend on the existence of sufficient numbers of smooth elements among rational or algebraic integers on certain linear forms. This can not be be guaranteed, nor can one assure the reduction from smooth relations to a congruence of squares and so on. Our explicit randomisation allows us to get around these problems by analysing the average case as opposed to the worst case, influenced by the recent works on distribution of smooths on arithmetic progressions [7, 2, 3, 5] and the philosophy that sums of arithmetic functions are essentially determined by the part over smooths [4, 8]. In short, we make essential use and strengthening of these tools as well as probabilistic combinatorics, and it may explain why no analysis was available earlier.

For each n, we bound the expected time taken to form a congruence of squares modulo n by $L_n(1/3, 2.77)$ unconditionally. Assuming the GRH, we prove an upper bound of $L_n\left(1/3, \sqrt[3]{\frac{64}{9}}\right)$, matching the best known heuristic estimate. If n is randomised, we unconditionally bound the harmonic mean of the run time by $L_n\left(1/3, \sqrt[3]{\frac{64}{9}}\right)$.

References

[1] Joe P. Buhler, Jr. Hendrik W. Lenstra, and Carl Pomerance. Factoring integers with the number field sieve. In A. K. Lenstra and H. W. Lenstra, Jr., editors, *The development of the number field sieve*, number 1554 in Lecture Notes in Mathematics, pages 50–94. Springer-Verlag, 1993.

[2] Andrew Granville. Integers, without large prime factors, in arithmetic progressions. I. *Acta Mathematica*, 170:255–273, 1993.

[3] Andrew Granville. Integers, without large prime factors, in arithmetic progressions. II. *Philosophical Transactions of the Royal Society of London Series A*, 345:349–362, 1993.

[4] Andrew Granville and K. Soundararajan. Large character sums. *J. Amer. Math. Soc.*, 14(2):365–397, 2001.

[5] A. J. Harper. Bombieri–Vinogradov and Barban–Davenport–Halberstam type theorems for smooth numbers. *ArXiv e-prints*, August 2012.

[6] Carl Pomerance. A tale of two sieves. *Notices of the American Mathematical Society*, 43:1473–1485, 1996.

[7] Kannan Soundararajan. The distribution of smooth numbers in arithmetic progressions. In *Anatomy of integers*, volume 46 of *CRM Proc. Lecture Notes*, pages 115–128. Amer. Math. Soc., Providence, RI, 2008.

[8] Yitang Zhang. Bounded gaps between primes. *Ann. of Math.*, 179(3):1121–1174, 2014.

Bootstrap percolation on $G(n,p)$ revisited

Mihyun Kang
(joint work with Tamás Makai)

Bootstrap percolation on a graph with infection threshold $r \in \mathbb{N}$ is a deterministic infection process, which starts from a set of initially infected vertices and in each step every uninfected vertex becomes infected if it has at least r infected neighbours, otherwise it remains uninfected. Once a vertex has become infected, it remains infected forever.

Bootstrap percolation was introduced by Chalupa, Leath, and Reich [5], and since then it has been used to describe several complex phenomena from neuronal activity [1, 7] to the dynamics of the Ising model at zero temperature [9]. Several qualitative characteristics of bootstrap percolation have been studied on a variety of deterministic and random graphs, such as grids [3], hypercubes [2], random regular graphs [4, 6], random graphs with given degree sequence [10], and the binomial random graph $G(n,p)$ [11, 7, 8].

Consider bootstrap percolation on $G(n,p)$. For $r \geq 2$ and p satisfying both $p = \omega(n^{-1})$ and $p = o(n^{-1/r})$, Janson, Łuczak, Turova, and Vallier [11] showed, among other results, that with probability tending to one as $n \to \infty$ either only a few additional vertices are infected or almost every vertex becomes infected. We strengthen this result by showing that this happens with exponentially high probability. To achieve the result we introduce a martingale to show that the number of infected vertices is concentrated around its expectation with exponentially high probability. The martingale is similar to the one used in [11], however the maximal one step difference in our martingale is significantly lower and thus allows for tighter concentration. In the subcritical case, the expected number of infected vertices is 'small' and therefore the martingale argument alone implies the result. In the supercritical case, the martingale argument is not sufficient, however it still ensures that the number of infected vertices is 'large' with exponentially high probability. We show then that the subgraph spanned by the vertices with $r-1$ infected neighbours grows quite large to contain a giant component. The infection of just one vertex in this giant component leads to every vertex in the component becoming infected and we show that this in fact happens with exponentially high probability.

References

[1] H. Amini, *Bootstrap percolation in living neural networks*, Journal of Statistical Physics **141** (2010), 459–475.

[2] J. Balogh and B. Bollobás, *Bootstrap percolation on the hypercube*, Probab. Theory Related Fields **134** (2006), 624–648.

[3] J. Balogh, B. Bollobás, H. Duminil-Copin, and R. Morris, *The sharp threshold for bootstrap percolation in all dimensions*, Trans. Amer. Math. Soc. **364** (2012), 2667–2701.

[4] J. Balogh and B. Pittel, *Bootstrap percolation on the random regular graph*, Random Structures Algorithms **30** (2007), 257–286.

[5] J. Chalupa, P. Leath and G. Reich, *Bootstrap percolation on a Bethe lattice*, Journal of Physics C: Solid State Physics **12** (1979), L31-L35.

[6] A. Coja-Oghlan, U. Feige, M. Krivelevich, and D. Reichman, *Contagious sets in expanders*, Proceedings of the 26th Symposium on Discrete Algorithms (SODA'15), 1953–1987.

[7] H. Einarsson, J. Lengler, K. Panagiotou, F. Mousset, and A. Steger, *Bootstrap Percolation with Inhibition*, http://arxiv.org/abs/1410.3291.

[8] U. Feige, M. Krivelevich, and D. Reichman, *Contagious sets in random graphs*, http://arxiv.org/abs/1602.01751.

[9] L. Fontes, R. Schonmann, and V. Sidoravicius, *Stretched Exponential Fixation In Stochastic Ising Models At Zero Temperature*, Comm. Math. Phys **228** (2002), 495–518.

[10] S. Janson, *On percolation in random graphs with given degree sequence*, Electronic Journal of Probability **14** (2009), 86–118.

[11] S. Janson, T. Łuczak, T. Turova, and T. Vallier, *Bootstrap percolation on the random graph $G_{n,p}$*, The Annals of Applied Probability **22** (2012), 1989–2047.

Minimizing the number of pentagonal edges

Zoltán Füredi

(joint work with Zeinab Maleki)

Erdős, Faudree and Rousseau [3] proved that an n-vertex graph with $\lfloor n^2/4\rfloor+1$ edges contains:

(1) At least $2\lfloor n/2\rfloor+1$ edges in triangles.

(2) At least $11n^2/144$ edges on C_5 cycles ($n>n_0$).

In [4] we have considered a more general problem, where the number of edges may be larger than $\lfloor n^2/4\rfloor+1$. Given a graph G, denote by $\mathrm{Tr}(G)$ the number of edges of G contained in triangles, and let $\mathrm{Tr}(n,e) := \min\{\mathrm{Tr}(G) : |V(G)| = n,\ e(G)=e\}$. With this notation (1) can be reformulated as

$$\mathrm{Tr}(n, \lfloor n^2/4\rfloor+1) = 2\lfloor n/2\rfloor+1. \tag{1}$$

Note that $\mathrm{Tr}(n,e) = 0$ whenever $e \le n^2/4$, because in that case there exist triangle-free (even bipartite) graphs with n vertices and e edges.

Given integers a, b and c, $(a \ge 2)$, define a family of graphs $\mathbf{Tr}(a,b,c)$ as follows. The vertex set V of a graph G in this class has a partition $V = A \cup B \cup C$ where $|A| = a$, $|B| = b$, and $|C| = c$, such that B and C are independent sets, $B \cup C$ induces a complete bipartite graph $K_{b,c}$, the vertices of C have neighbors only in B, and $G[A]$ and $G[A,B]$ are 'almost complete graphs', namely, they span more than $\binom{|A|-1}{2} + |A||B|$ edges. The edges of $G[B,C]$ are the non-triangular edges.

Given integers $n \ge 3$ and $n^2/4 < e \le \binom{n}{2}$, we define a class of graphs, $\mathbf{Tr}(n,e)$, with many non-triangular edges as follows. Put a graph $G \in \mathbf{Tr}(a,b,c)$ into the class $\mathbf{Tr}(n,e)$ if it has n vertices and e edges and it has the minimum number of triangular edges among these type of graphs. Define $g(n,e)$ as $\min\{\mathrm{Tr}(G) : G \in \mathbf{Tr}(n,e)\}$. We have $\mathrm{Tr}(n,e) \le g(n,e)$, and

$$g(n,e) = \min\{e - bc : a+b+c = n,\ a,b,c \in \mathbb{N} \cup \{0\},\ \binom{a}{2} + ab + bc \ge e\}.$$

We believe that one can extend (1) as follows.

Conjecture 1. *Suppose that G is an n-vertex graph with e edges, such that $e > n^2/4$ and it has the minimum number of triangular edges. Then $G \in \mathbf{Tr}(n,e)$.*

In particular, we conjecture that $\mathrm{Tr}(n,e) = g(n,e)$. For $e > n^2/4$ we [4] have proved a slightly weaker result

$$g(n,e) - (3/2)n \le \mathrm{Tr}(n,e) \le g(n,e).$$

Our main tool was a new symmetrization method, a generalization of previous results by Zykov and Motzkin and Straus such that it can be applied to more than one graph simultaneously.

More recently, Gruslys and Letzter [6] using a refined version of the symmetrization method proved that there exists an n_0 such that $\mathrm{Tr}(n,e) = g(n,e)$ for all $n > n_0$. The second part of our Conjecture 1, namely that the extremal graph should be from a $\mathbf{Tr}(a,b,c)$, is still open.

In this talk we investigate these in an even more general setting. Given two graphs G and F let $h(G,F)$ denote the number of edges of G in subgraphs isomorphic to F, and let $h(n,e,F) = \min h(G,F)$ where $|V(G)| = n$ and $|E(G)| = e$. Obviously, $h(n,e,F) = 0$ if and only if $e \le \mathrm{ex}(n,F)$ (the Turán number).

Using new ideas and Szemerédi's Regularity Lemma we [5] asymptotically determine $h(n,e,F)$ for every given F with chromatic number $\chi(F) = 3$ as follows.

Theorem 2. *For every $1/4 < \lambda < 1/2$, $\lim_{n\to\infty} h(n,\lambda n^2,F)/n^2$ exists, and it equals to one of the (well described) functions $g_i(\lambda)$, $(1 \le i \le 13)$.*

We say that a graph G is of type (α,β,γ) (say $T_{\alpha,\beta,\gamma}$ for short), where $\alpha,\beta,\gamma \ge 0$ integers or ∞, if the vertex set $V(G)$ has a 5 partition $V(G) = U \cup V \cup A \cup B \cup C$ such that $U \ne \emptyset$, $V \ne \emptyset$ and U and V are independent sets, $K(U,V) \subset G$, $N(U) \subseteq V \cup A$, $N(V) \subseteq U \cup B$ (so $v \in V$ has neighbors only in U and B) and

$\chi(G[A]) \leq \alpha$, $\chi(G[B]) \leq \beta$, and $\chi(G[C]) \leq \gamma$. The edges between U and V are referred as special edges. If $\alpha = 0$ ($\beta = 0$, $\gamma = 0$) then $A = \emptyset$ ($B = \emptyset$, $C = \emptyset$, respectively). If $\alpha = 1$ ($\beta = 1$, $\gamma = 1$) then A is an independent set in G (B and C are independent, respectively). When α (β, or γ) is ∞ then we have no restriction on the chromatic number of $G[A]$ ($G[B]$ or $G[C]$). The graphs of $\mathbf{Tr}(n, e)$ have type $(\infty, 0, 0)$.

Let $\mathcal{G}(\alpha, \beta, \gamma)$ be the class of all graphs of type (α, β, γ). Let $\mathcal{G}_n(\alpha, \beta, \gamma)$ stand for the n-vertex members of $\mathcal{G}(\alpha, \beta, \gamma)$. A graph $G \in \mathcal{G}(\alpha, \beta, \gamma)$ is called F-feasible if for every n, for every possible $G \in \mathcal{G}_n(\alpha, \beta, \gamma)$ a special edge uv ($u \in U$, $v \in V$) can never be an F-edge. Also, for some $G \in \mathcal{G}(\alpha, \beta, \gamma)$ all other edges, except the special edges, are F-edges. So, G contains at most $e - |U||V|$ F-edges. Define

$$g_{\alpha\beta\gamma}(n, e) := \min\{e - |U||V| : G \in \mathcal{G}_n(\alpha, \beta, \gamma), |E(G)| = e\},$$

i.e., it is the solution of the following minimization problem. Minimize $e - uv$ for given integers n and e, $\binom{n}{2} \geq e \geq n^2/4$, subject to

$$n = u + v + \sum_{i=1}^{\alpha} a_i + \sum_{i=1}^{\beta} b_i + \sum_{i=1}^{\gamma} c_i,$$

where every variable is a non-negative integer and

$$uv + u\sum_{i=1}^{\alpha} a_i + v\sum_{i=1}^{\beta} b_i + (\sum_{i=1}^{\alpha} a_i + \sum_{i=1}^{\beta} b_i + \sum_{i=1}^{\gamma} c_i)^2/2 - (\sum_{i=1}^{\alpha} a_i^2 + \sum_{i=1}^{\beta} b_i^2 + \sum_{i=1}^{\gamma} c_i^2)/2 \geq e.$$

Our real result is the following:

Theorem 3. *For every graph F with $\chi(F) = 3$ and $\varepsilon > 0$ there exists an $n_0 = n_0(F, \varepsilon)$ such that for $1/4 + \varepsilon < \lambda < 1/2$, for $n > n_0$ there exists a type $(\alpha, \beta, \gamma) \in \{0, 1, 2, \infty\}^3$ such that*

$$h(n, e, F) = g_{\alpha\beta\gamma}(n, e) + o(n^2).$$

Especially, we got a counterexample for a conjecture of Erdős [2] regarding pentagonal edges asserting that $h(n, \lfloor n^2/4 \rfloor + 1, C_5) \geq (n^2/4) - n^2/36 + O(n)$. This value can be obtained by considering a graph having two components, a complete graph on $[2n/3] + 1$ vertices and a complete bipartite graph on the rest. (Type $(0, 0, \infty)$). This conjecture was mentioned in the papers of Erdős [2] and also in the problem book of Fan Chung and Graham [1]. However there are graphs of type $(1, 0, \infty)$ with $\lfloor n^2/4 \rfloor + 1$ edges and $n^2/8(2 + \sqrt{2}) + O(n) = n^2/27.31...$ non-pentagonal edges, disproving Erdős' conjecture.

On the other hand, Theorem 3 asymptotically verifies the conjecture of Erdős that for every $k \geq 3$, the maximum number of non-C_{2k+1} edges in a graph of size exceeding $(n^2/4) + o(n^2)$ is at most $n^2/36 + o(n^2)$ non-C_{2k+1} edges.

Grzesik, P. Hu, and Volec [7] using Razborov's flag algebra method showed that every n-vertex graph with $\lfloor n^2/4 \rfloor + 1$ edges has at least $(n^2/4) - n^2/8(2 + \sqrt{2}) - \varepsilon n^2$ pentagonal edges for $n > n_0(\varepsilon)$ for every $\varepsilon > 0$. They also proved that those graphs have at most $n^2/36 + \varepsilon n^2$ non-C_{2k+1}-edges for $n > n_k(\varepsilon)$ for every $\varepsilon > 0$ and $k \geq 3$. In Theorem 3 we were able to prove the same results only for graphs with $\lfloor n^2/4 \rfloor + \varepsilon n^2$ edges (for $n > n_0(k, \varepsilon)$, $k \geq 2$). Let's close with a slightly corrected version of Erdős conjecture.

Conjecture 4. *Suppose that G is an n-vertex graph with e edges, such that $e > n^2/4$ and it has the minimum number of C_{2k+1}-edges, $k \geq 3$, $n > n_k$. Then G is connected and has two blocks, one of them is a complete bipartite graph and the other one is almost complete.*

Many problems, e.g., an F with a higher chromatic number, or natural generalizations for hypergraphs remain open.

References

[1] F. Chung and R. Graham. *Erdős on graphs.* His legacy of unsolved problems. A. K. Peters, Ltd., Wellesley, MA, 1998.

[2] P. Erdős. Some recent problems and results in graph theory. *Discrete Mathematics* 164, 81–85, 1997.

[3] P. Erdős, R. J. Faudree, and C. C. Rousseau. Extremal problems involving vertices and edges on odd cycles. *Discrete Mathematics* 101, 23–31, 1992.

[4] Z. Füredi and Z. Maleki. The minimum number of triangular edges and a symmetrization for multiple graphs. `arXiv:1411.0771`, 8 pages. Posted on November 4, 2014.

[5] Z. Füredi and Z. Maleki. A proof and a counterexample for a conjecture of Erdős concerning the minimum number of edges in odd cycles. *Manuscript.*

[6] V. Gruslys and S. Letzter. Minimising the number of triangular edges. `arXiv:1605.00528`, 43 pages. Posted on May 2, 2016.

[7] A. Grzesik, P. Hu and J. Volec. Minimum number of edges that occur in odd cycles. *Manuscript*, 24 pages. May 2016.

[8] T. S. Motzkin and E. G. Straus. Maxima for graphs and a new proof of a theorem of Turán. *Canad. J. Math.* 17, 533–540, 1965.

The number of subsets of integers with no *k*-term arithmetic progression

József Balogh

(joint work with Hong Liu, Maryam Sharifzadeh)

Enumerating discrete objects in a given family with certain properties is one of the most fundamental problems in extremal combinatorics. In the context of graphs, this was initiated by Erdős, Kleitman and Rothschild [6] who studied the family of triangle-free graphs. Here, we investigate a counting problem in the arithmetic setting. A subset of $[n] := \{1, 2, \dots, n\}$ is *k-AP-free* if it does not contain a k-term arithmetic progression. Denote by $r_k(n)$ the maximum size of a k-AP-free subset of $[n]$. Cameron and Erdős [3] raised the following question:

Question 1. *Is it true that the number of k-AP-free subsets of $[n]$ is*

$$2^{(1+o(1))r_k(n)}?$$

Since every subset of a k-AP-free set is also k-AP-free, one can easily obtain $2^{r_k(n)}$ many k-AP-free subsets of $[n]$. In fact, Cameron and Erdős [3] slightly improved this obvious lower bound: writing $R_k(n)$ for the number of k-AP-free subsets of $[n]$, they proved that $\limsup_{n\to\infty} \frac{R_k(n)}{2^{r_k(n)}} = \infty$.

Until recently, the only progress on the upper bound in the last 30 years was improving the bounds on $r_k(n)$. Then Balogh, Morris and Samotij [1], and independently Saxton and Thomason [10], proved the following: for any $\beta > 0$ and integer $k \geq 3$, there exists $C > 0$ such that for $m \geq Cn^{1-1/(k-1)}$, the number of k-AP-free m-sets in $[n]$ is at most $\binom{\beta n}{m}$. This deep counting result implies the sparse random analogue of Szemerédi's theorem [12] which was proved earlier by Conlon and Gowers [4] and independently by Schacht [11]. However, this bound is far from settling Question 1.

One of the reasons for the difficulty in finding good upper bounds on $R_k(n)$ is our limited understanding of $r_k(n)$. Indeed, despite much effort, the gap between the current known lower and upper bounds on $r_3(n)$ is still rather large; closing this gap remains one of the most difficult problems in additive number theory. For the lower bound on $r_3(n)$, the celebrated construction of Behrend [2] shows that $r_3(n) = \Omega\left(n \cdot 2^{-2\sqrt{2}\sqrt{\log_2 n}}\right)$.

For $k \geq 4$ there exist $c_k, c'_k > 0$ such that

$$\frac{n}{2^{c_k(\log n)^{1/(k-1)}}} \leq r_k(n) \leq \frac{n}{(\log\log n)^{c'_k}}, \tag{1}$$

where the lower bound is due to Rankin [9] and the upper bound is by Gowers [8].

Notice that, using the lower bound in (1), we obtain the following trivial upper bound for $R_k(n)$:

$$R_k(n) \leq \sum_{i=0}^{r_k(n)} \binom{n}{i} < 2\binom{n}{r_k(n)} < 2\left(\frac{en}{r_k(n)}\right)^{r_k(n)} = 2^{O\left(r_k(n)\cdot(\log n)^{\frac{1}{k-1}}\right)}.$$

Our main result is removing the log-factor from the exponent.

Theorem 2. *The number of k-AP-free subsets of $[n]$ is $2^{O(r_k(n))}$ for infinitely many values of n.*

An immediate corollary of Theorem 2 is the following.

Corollary 3. *For every $\varepsilon > 0$, there exists a constant $b > 0$ such that the following holds. Let $A(b) \subseteq \mathbb{Z}$ consist of all integers n such that the number of k-AP-free subsets of $[n]$ is at most $2^{b\cdot r_k(n)}$. Then*

$$\limsup_{n\to\infty} \frac{|A(b) \cap [n]|}{n} \geq 1 - \varepsilon.$$

For all values of n, we obtain the following weaker counting estimate, which is nevertheless sufficient to improve previous transference theorems for Szemerédi's theorem, in particular implies Corollary 5.

Theorem 4. *If $r_k(n) \leq \frac{n}{h(n)}$, where $h(n) \leq (\log n)^c$ for some $c > 0$, then the number of k-AP-free subsets of $[n]$ is at most $2^{O(n/h(n))}$. Furthermore, for any*

$\gamma > 0$, there exists $C = C(k,c,\gamma) > 0$ such that for any $m \geq n^{1-\frac{1}{k-1}+\gamma}$, the number of k-AP-free m-subsets of $[n]$ is at most

$$\binom{Cn/h(n)}{m}.$$

We say that a set $A \subseteq \mathbb{N}$ is (δ, k)-*Szemerédi* if every subset of A of size at least $\delta|A|$ contains a k-AP. Denote by $[n]_p$ the p-random subset of $[n]$, where each element of $[n]$ is chosen with probability p independently of others. As mentioned earlier, the counting result of [1] and [10] implies the following sparse analogue of Szemerédi's theorem, which was only recently proved by a breakthrough transference theorem of Conlon and Gowers [4] and Schacht [11]: For any constant $\delta > 0$ and integer $k \geq 3$, there exists $C > 0$, such that almost surely $[n]_p$ is (δ, k)-Szemerédi for $p \geq Cn^{-\frac{1}{k-1}}$. As an easy corollary of Theorem 4, we obtain the following sharper version, in which δ could be taken as a function of n. In fact, it transfers the current best bounds on $r_k(n)$ of Gowers [8] to the random setting. Proving Corollary 5 from Theorem 4 is similar as in [1] and [10]. We remark that the bound on p is optimal up to the additive error term γ in the exponent.

Corollary 5. *If $r_k(n) \leq \frac{n}{h(n)}$, where $h(n) \leq (\log n)^c$ for some constant $c > 0$, then for any $\gamma > 0$, there exists $C = C(k,c,\gamma) > 0$ such that the following holds. If $p_n \geq n^{-\frac{1}{k-1}+\gamma}$ for all sufficiently large n, then*

$$\lim_{n\to\infty} \mathbb{P}\left([n]_{p_n} \textit{ is } \left(\frac{C}{h(n)}, k\right)\textit{-Szemerédi}\right) = 1.$$

The proof of Theorem 2 uses the hypergraph container method, developed by Balogh, Morris and Samotij [1], and independently by Saxton and Thomason [10]. In order to apply the hypergraph container method, we need a supersaturation result. Supersaturation problems are reasonably well-understood if the extremal family is of positive density. For example, the largest sum-free subset of $[n]$ has size $\lceil n/2 \rceil$, while any set of size $(\frac{1}{2}+\varepsilon)n$ has $\Omega(n^2)$ triples satisfying $x + y = z$. In the context of graphs, the Erdős-Stone theorem gives $\mathrm{ex}(n, G) = \left(1 - \frac{1}{\chi(G)-1} + o(1)\right)\frac{n^2}{2}$, while any n-vertex graph with $\left(1 - \frac{1}{\chi(G)-1} + \varepsilon\right)\frac{n^2}{2}$ edges contains $\Omega(n^{|V(G)|})$ copies of G. However, the degenerate case is significantly harder. Indeed, a famous unsolved conjecture of Erdős and Simonovits [7] in extremal graph theory asks whether an n-vertex graph with $\mathrm{ex}(n, C_4) + 1$ edges has at least two copies of C_4.

For arithmetic progressions Croot and Sisask [5] proved a nice formula, which is unfortunately not helping when $|A| \leq O(r_k(n))$ and $r_k(n) \ll n/f(n)$ where $f(n)$ is a polylogarithmic function. Their formula is that for every $A \subset [n]$, and every $1 \leq M \leq n$, the number of 3-APs in A is at least

$$\left(\frac{|A|}{n} - \frac{r_3(M)+1}{M}\right) \cdot \frac{n^2}{M^4}.$$

We need a supersaturation for sets of size $\Theta(r_k(n))$.

Theorem 6. *Given $k \geq 3$, there exists a constant $C' = C'(k) > 0$ and an infinite sequence $\{n_i\}_{i=1}^{\infty}$, such that the following holds. For any $n \in \{n_i\}_{i=1}^{\infty}$ and any $A \subseteq [n]$ of size $C'r_k(n)$, the number of k-APs in A is at least*

$$\log^{3k-2} n \cdot \left(\frac{n}{r_k(n)}\right)^{k-1} \cdot n.$$

Note that improving Theorem 6 could lead to solution of the question of Cameron and Erdős, Question 1.

References

[1] J. Balogh, R. Morris and W. Samotij, Independent sets in hypergraphs, *J. Amer. Math. Soc.*, (28) 2015, 669–709.

[2] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U.S.A.*, (32) 1946, 331–332.

[3] P. Cameron and P. Erdős, On the number of sets of integers with various properties, in Number Theory (R.A. Mollin, ed.), 61–79, Walter de Gruyter, Berlin, 1990.

[4] D. Conlon and W. T. Gowers, Combinatorial theorems in sparse random sets, *Ann. of Math.*, to appear.

[5] E. Croot and O. Sisask, A new proof of Roth's Theorem on Arithmetic progressions, *Proc. Amer. Math. Soc.*, (137) 2009, 805–809.

[6] P. Erdős, D. J. Kleitman and B. L. Rothschild, Asymptotic enumeration of K_n-free graphs, *Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), Tomo II* 19–27.

[7] P. Erdős, M. Simonovits, Cube-supersaturated graphs and related problems, Progress in graph theory (Waterloo, Ont., 1982), pp. 203–218, Academic Press, Toronto, ON, 1984.

[8] W. T. Gowers, A new proof of Szemerédi's theorem, *Geom. Func. Anal.*, (11) 2001, 465–588.

[9] R. A. Rankin, Sets of integers containing not more than a given number of terms in arithmetical progression, *Proc. Roy. Soc. Edinburgh Sect. A*, (65) 1960/1961, 332–344.

[10] D. Saxton and A. Thomason, Hypergraph containers, *Invent. Math.*, (201) 2015, 925–992.

[11] M. Schacht, Extremal results for random discrete structures, *Ann. of Math. (2)*, (184) 2016, 331–363.

[12] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.*, (27) 1975, 199–245.

Strong noise sensitivity and random graphs

Eyal Lubetzky
(joint work with Jeff Steif)

Noise sensitivity, a concept introduced by Benjamini, Kalai and Schramm [1], captures the notion that the value of a Boolean function of many i.i.d. variables would flip under small perturbations of its input. Consider a sequence of functions $f_n : \Omega_n \to \{0,1\}$ paired with a sequence of probabilities p_n, where each domain $\Omega_n = \{0,1\}^{\Lambda_n}$ is a product space of Bernoulli(p_n) variables, and the sets Λ_n are finite and increasing with n. Further assume (p_n) is *non-degenerate* in the sense that $\mathbb{P}(f_n = 1)$ is uniformly bounded away from 0 and 1. Given $\omega \in \Omega_n$ and some $\epsilon \in (0,1)$, let ω^ϵ denote the result of resampling the Bernoulli(p_n) variable ω_x

independently with probability ϵ for each $x \in \Lambda_n$. The sequence (f_n) is said to be *noise sensitive* (Sens) w.r.t. p_n and a given $\epsilon > 0$ if

$$\lim_{n\to\infty} \mathbb{P}\left(f_n(\omega^\epsilon) = 1 \mid f_n(\omega) = 1\right) - \mathbb{P}\left(f_n = 1\right) = 0\,, \tag{1}$$

or equivalently (recall that (f_n) is non-degenerate), $\mathrm{Cov}\left(f_n(\omega), f_n(\omega^\epsilon)\right) \to 0$. When a function (f_n) is Sens it is natural to further discuss *quantitative noise sensitivity*, i.e., how fast can $\epsilon \to 0$ with n such that (1) still holds.

In the setting where $p_n \equiv 1/2$ and the functions f_n are *monotone* w.r.t. the natural partial order on the hypercube Ω_n, a beautiful argument of [1] gave a criterion for noise sensitivity in terms of the first level of Fourier coefficients of f_n. Namely, (f_n) is noise sensitive if and only if $\lim_{n\to\infty} \sum_{x\in\Lambda_n} \hat{f}_n(x)^2 = 0$, where $\hat{f}_n(x)$ is the Fourier coefficient corresponding to the singleton $\{x\}$. Unfortunately, this criterion becomes invalid when $p_n \to 0$ (e.g., the indicator of a random graph being triangle-free satisfies the above condition and yet it is *not* noise sensitive; see [1, §6.4]), and determining noise sensitivity without it can be highly nontrivial.

Strong noise sensitivity. Going back to (1), this is known to be equivalent to having the average of $\left|\mathbb{P}\left(f_n(\omega^\epsilon) = 1 \mid \omega\right) - \mathbb{P}\left(f_n = 1\right)\right|$ over $\{\omega : f_n(\omega) = 1\}$ tend to 0 as $n \to \infty$. When dealing with monotone functions, however, it is in many cases more natural and useful to condition on a *witness* for $f_n(\omega) = 1$ instead of the entire configuration ω.

Definition 1. *A 1-*witness *for a monotone function $f : \{0,1\}^\Lambda \to \{0,1\}$ is a minimal subset $W \subset \Lambda$ such that $\omega_W \equiv 1$ implies $f(\omega) = 1$.*

Let $\mathcal{W}_1 = \mathcal{W}_1(f)$ be the set of 1-witnesses of a monotone Boolean function f, and let $\mathcal{W}_0 = \mathcal{W}_0(f)$ denote its analogously defined 0-witnesses.

Perhaps surprisingly, it can be the case that (f_n) is noise sensitive and yet the probability that $f_n(\omega^\epsilon) = 1$ substantially increases when we condition on *any particular* 1-witness in ω. This motivates the following definition.

Definition 2. *A sequence (f_n) of monotone increasing Boolean functions is said to be* 1-strongly noise sensitive *(*StrSens$_1$*) w.r.t. p_n and $\epsilon > 0$ if*

$$\lim_{n\to\infty} \max_{W\in\mathcal{W}_1} \mathbb{P}(f_n(\omega^\epsilon) = 1 \mid \omega_W \equiv 1) - \mathbb{P}(f_n = 1) = 0\,. \tag{2}$$

The notion of 0-strong noise sensitivity *(*StrSens$_0$*) is defined analogously. (Note that a sequence of increasing functions (f_n) is* StrSens$_0$ *if and only if its complement $(\overline{f_n})$ is* StrSens$_1$*, where $\overline{f_n}(\omega) = \overline{f_n(\overline{\omega})}$ with $\overline{x} = 1 - x$.)*

As suggested by its name, the notion of strong noise sensitivity, which addresses the subtler effect of conditioning on any *particular* witness (cf. (1) vs. (2)), indeed implies (even when $\epsilon \to 0$) the standard noise sensitivity but not vice versa.

Examples. *The next two examples of monotone noise sensitive functions, which were discussed in* [1]*, both trace back to Ben-Or and Linial in the related work* [2]*.*

(i) Tribes*: partition $\Lambda_n = \{x_1, \dots, x_n\}$ into blocks of $\log_2 n - \log_2 \log_2 n$ variables, let $p_n \equiv 1/2$ and set f_n to be 1 if there is an all-1 block. This function is non-degenerate and* Sens*(*[1, §6.1]*): A 1-witness W in ω is a full block, which the noise will destroy with probability approaching 1, and the probability of encountering another is $(1 - o(1))\mathbb{P}(f_n = 1)$. Indeed, tribes is* StrSens$_1$.

(ii) Recursive 3-Majority*: Index $n = 3^k$ variables by the leaves of a ternary tree, and iteratively set the value of each node to be the majority of its children. Take $p_n \equiv 1/2$ and define f_n to be the value at the root. Clearly non-degenerate, this function is* Sens*(*[1, §6.2]*): $\mathbb{P}\left(f_n(\omega^\epsilon) = 1 \mid f_n(\omega) = 1\right) \to 1/2$ as $n \to \infty$. A 1-witness W is a set of 2^k leaves (positioned in the obvious way to force the majority). One can verify that $\mathbb{P}\left(f_n(\omega^\epsilon) = 1 \mid \omega_W \equiv 1\right) = 1 - \epsilon/2$, and therefore this function is* not StrSens$_1$ *(nor* StrSens$_0$ *by symmetry).*

Notice the potentially different behaviors of 0-witnesses and 1-witnesses w.r.t. strong noise sensitivity, in contrast with standard noise sensitivity (which is closed under complements). E.g., the tribes function is StrSens$_1$ but *not* StrSens$_0$.

Properties of random graphs. The Erdős-Rényi random graph, $\mathcal{G}(n,p)$, is a probability distribution over graphs on n labeled vertices, where each undirected edge appears independently with probability $p = p(n)$. A monotone increasing graph property is a collection of graphs closed under isomorphism and the addition of edges, identified with its indicator function on the $\binom{n}{2}$ edge variables.

Theorem 1. *Fix $0 < a < b$ and let f_n be the property that the critical random graph $\mathcal{G}(n, 1/n)$ contains a cycle of length $\ell \in (an^{1/3}, bn^{1/3})$. Then (f_n) is non-degenerate and noise sensitive, and furthermore, it is* StrSens$_1$*.*

Moreover, the analogue of this conclusion for quantitative noise sensitivity holds if and only if the noise parameter $\epsilon = \epsilon(n)$ satisfies $\epsilon \gg n^{-1/3}$.

Theorem 1 holds throughout the critical window $p = \frac{1 \pm \xi}{n}$ with $\xi = O(n^{-1/3})$, around which the longest cycle grows from constant to linear (e.g., taking $\xi^3 n \to \infty$ still with $\xi = o(1)$, the maximum length of a cycle is $\Theta_{\mathrm{P}}(1/\xi)$ at $p = \frac{1-\xi}{n}$ and $\Theta_{\mathrm{P}}(\xi^2 n)$ at $p = \frac{1+\xi}{n}$; see [3, 4]).

Revisiting the quantitative conclusion of Theorem 1 now highlights an interesting phenomenon, where the $\epsilon \gg n^{-1/3}$ threshold for noise sensitivity coincides with the boundary of the critical window ($p = \frac{1 \pm \xi}{n}$ for $\xi \gg n^{-1/3}$). This phenomenon is best explained through the following equivalent process:

- Let ω be a uniform set of $N \sim \mathrm{Bin}(\binom{n}{2}, p)$ edges.
- Obtain $\bar{\omega}$ by deleting a uniform set of $\mathrm{Bin}(N, \epsilon(1-p))$ edges from ω.
- Add a uniform set of $\mathrm{Bin}(\binom{n}{2} - N, \epsilon p)$ edges missing from ω to get ω^ϵ.

As the edge probability in $\bar{\omega}$ is $p(1-\epsilon) + \epsilon p^2$, on a heuristic level we have:

(a) If $\epsilon = O(n^{-1/3})$ then $\bar{\omega}$ remains in the critical window, where (f_n) is non-degenerate, so $f_n(\omega), f_n(\bar{\omega})$ (thus $f_n(\omega), f_n(\omega^\epsilon)$) should be correlated.

(b) If $\epsilon \gg n^{-1/3}$ then $\bar{\omega}$ is subcritical whence $f_n(\bar{\omega})$ is degenerate, effectively decorrelating $f_n(\bar{\omega})$ from $f_n(\omega)$ (thus also $f_n(\omega), f_n(\omega^\epsilon)$) yielding Sens.

Intuitively, we expect a random graph property to be Sens when it has no bounded-size witnesses (thus none will survive the noise) and distinct witnesses are essentially independent (so surviving fragments of a witness will have negligible impact), as is the case in the theorem above. However, for various important graph properties the witnesses happen to be highly correlated, foiling this intuition. E.g., containing a Hamilton cycle is non-degenerate at $p \sim \frac{\log n}{n}$ yet the expected number of witnesses becomes exponentially large in n already at $p = O(1/n)$, and similarly for perfect matchings. Nevertheless, these are in fact noise sensitive:

Theorem 2. *Let f_n be the property that the minimum degree of $\mathcal{G}(n,p)$ is at least k for some fixed $k \geq 1$, and suppose $p = p(n)$ is such that (f_n) is non-degenerate. Then (f_n) is noise sensitive, and moreover, it is* StrSens$_0$.

As a result, the following properties of $\mathcal{G}(n,p)$ are noise sensitive:

(i) containing a Hamilton cycle,
(ii) containing a perfect matching (in general, an r-factor[1] *for r fixed),*
(iii) connectivity (in general, k-vertex and k-edge connectivity for k fixed),
(iv) having an isoperimetric constant[2] *of at least γ for some fixed $\gamma > 0$.*

Furthermore, each of these is quantitatively noise sensitive iff $\epsilon \gg \frac{1}{\log n}$.

Note that even the (non-strong) noise sensitivity in Theorems 1 or 2 *cannot* be obtained from the best known generalizations of the BKS criterion for varying p (see [5]), as these all require $1/p = n^{o(1)}$.

References

[1] I. Benjamini, G. Kalai, and O. Schramm, *Noise sensitivity of Boolean functions and applications to percolation*, Inst. Hautes Études Sci. Publ. Math. 90 (1999), 5–43.

[2] M. Ben-Or and N. Linial, *Collective coin flipping*, Randomness and Computation (S. Micali, ed.), Academic Press, 1990, pp. 91–115. Earlier version in FOCS 1985.

[3] B. Bollobás, *Random graphs*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 73, Cambridge University Press, Cambridge, 2001.

[4] S. Janson, T. Łuczak, and A. Rucinski, *Random graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley-Interscience, New York, 2000.

[5] N. Keller and G. Kindler, *Quantitative relation between noise sensitivity and influences*, Combinatorica 33 (2013), no. 1, 45–71.

[1] An r-factor of a graph is a spanning r-regular subgraph

[2] The isoperimetric constant of a graph is the minimum of $\frac{e(S,S^c)}{|S| \wedge |S^c|}$ over all subsets S of the vertices, where $e(S,S^c)$ is the number of edges between S and its complement.

Minimising the number of triangular edges

Shoham Letzter
(joint work with Vytautas Gruslys)

1. Introduction

We consider the following question: given n and e, what is the minimum number of *triangular edges* (i.e. edges on triangles) over n-vertex graphs with e edges? We note that a similar question, of minimising the number of triangles, was first considered by Rademacher [9], generalised by Erdős [1, 2], and subsequently studied by Lovász and Simonovits [6, 7] and by Razborov [10].

Erdős, Faudree and Rousseau [3] considered the first instance of the question: they showed that an n-vertex graph with $\lfloor n^2/4 \rfloor + 1$ edges has at least $2\lfloor n/2 \rfloor + 1$ triangular edges. We consider the question for general e. For convenience, we consider the following equivalent question: what is the maximum number of non-triangular edges among n-vertex graphs with at least e edges?

Let $G(a, b, c)$ be the graph that consists of a clique A of size a and two independent sets B and C of sizes b and c, such that B is joined to all of $A \cup C$ and there are no edges between A and C (see Figure 1). Let $s(G)$ be the number of non-triangular edges in G, and let $s(n, e)$ be the maximum of $s(G)$ over n-vertex graphs with at least e edges. Füredi and Maleki [4] made the following conjecture.

Conjecture 1 (Füredi and Maleki [4]). *For every n and e, there is a graph $H = G(a, b, c)$ with n vertices and at least e edges such that $s(H) = s(n, e)$.*

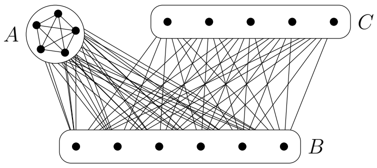

Figure 1. The graph $G(a, b, c)$

Note that the aforementioned result of Erdős, Faudree and Rousseau [3] confirms Conjecture 1 for $e = \lfloor n^2/4 \rfloor + 1$, (consider the graph $G(2, \lfloor n/2 \rfloor, \lceil n/2 \rceil - 2)$). Füredi and Maleki proved an approximate version of their conjecture.

Theorem 2 (Füredi and Maleki [4]). *For every n and e there is a graph $H = G(a, b, c)$ such that $|H| = n$, $e(H) \geq e$ and $s(H) \geq s(n, e) - 3n/2$.*

We prove the conjecture exactly, for large n.

Theorem 3. *There is n_0 such that for every $n \geq n_0$ and every e, there is a graph $H = G(a, b, c)$ such that $|H| = n$, $e(H) \geq e$ and $s(H) = s(n, e)$.*

The proof for e that is close to either $n^2/4$ or $\binom{n}{2}$ is easier; we discuss it briefly in the next section. The middle range, when e is bounded away from both $n^2/4$ and $\binom{n}{2}$, is the heart of the proof, and we elaborate more about it in Section 3.

2. The extremal ranges

The plan in each of the extremal ranges is the following. Let G be a graph with n vertices, at least e edges and $s(n,e)$ triangular edges. We first show that G is close to a graph $G(a,b,c)$ (e.g. when e is close to $n^2/4$, we show that G has an induced complete bipartite subgraph spanning almost all of the vertices). Then, using a lower bound on the number of triangular edges, we obtain sharper bounds on a,b,c. Finally, using edges-shifting operations we show that $G \cong G(a,b,c)$.

3. The middle range

Let G be an n-vertex graph with at least e edges and $s(n,e)$ non-triangular edges. In order to obtain information about the structure of G, we use the following two tools: compressed graphs - these are graphs with somewhat restrictive structure, and we show that G may be assumed to be compressed; and the continuity of $s(n,e)$, which enables us to extract information about G using operations of addition or deletion of edges. We discuss these two tools in more details in the next two subsections, and finish with a sketch of the proof.

3.1. **Compressed graphs.** We discuss briefly the notion of weighted graphs. A *weighted graph* G^w is a graph G with a non-negative weighting w of the vertices. $|G^w|$ is the sum of weights of the vertices; $e(G^w)$ is the sum of $w(u)w(v)$ over edges uv; $s(G^w)$ is defined similarly. Note that if w is integer valued, then G^w represents a blow-up of G, where a vertex u is replaced by an independent set of size $w(u)$.

As the first step in the proof of Theorem 2, Füredi and Maleki [4] show that every graph G has a subgraph H with weighting w such that $|H^w| = |G|$, $e(H^w) \geq e(G)$, $s(H^w) \geq s(G)$ and $\alpha(H) \leq 2$. With some effort, Theorem 2 follows. The main drawback in this approach is that w need not be integer valued, and thus H^w does not represent a graph. We are able to overcome this issue as follows: we show that every graph G has a subgraph H with integer weighting w, satisfying $|H^w| = |G|$, $e(H^w) \geq e(G)$ and $s(H^w) \geq s(G)$ and $\alpha(H) \leq 2\log n$. Since H has integer weights, we may think of it as a graph, and we call such a graph *compressed.*

Our main use of the fact that we can focus on compressed graph is the following observation: if G is compressed, then any independent set I contains a set of *clones* (i.e. vertices that have the same neighbourhood) J of size at least $|I|/(2\log n)$.

3.2. **Continuity.** We show that $s(n,e)$ is 'continuous': $s(n,e)-Cx \leq s(n,e+x) \leq s(n,e)-cx$. These inequalities hold for x not too large or too small and e bounded away from $n^2/4$ and $\binom{n}{2}$. This turns out to be very useful. For example, it allows us to conclude that if an addition of x edges to G reduces the number of non-triangular edges only slightly, then x cannot be very large.

3.3. **Sketch of the proof.** We may assume that G is compressed. We note that the proof of Füredi and Maleki [4] implies that G has a clique of size $\Omega(n)$, from which it follows, using the fact that G is compressed and the continuity of $s(n,e)$, that the set A of *triangular vertices* (i.e. vertices incident only with triangular edges) has size $\Omega(n)$. We note that we can assume that A spans a clique and its vertices have the same neighbourhood B outside A. Finally, let $C = V(G)\backslash(A\cup B)$. We further use the fact that G is compressed and the continuity of $s(n,e)$ to show that B and C may both be partitioned into $O(1)$ sets of clones and a small remainder (see Figure 2).

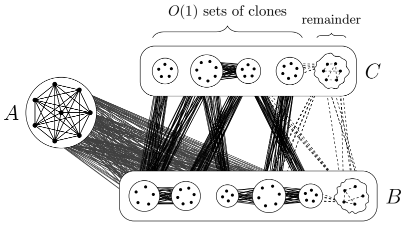

Figure 2. Structure of G

By running a weight shifting process on the graph (with the remainder removed), we show that the numbers of edges and non-triangular edges in G are close to those of a graph $G(|A|,|B|,|C|)$. It follows that almost all edges between B and C are present in G and are non-triangular. A sequence of edge shifting operations implies that $G = G(|A|,|B|,|C|)$.

4. Conclusion

The question of minimising the number of triangular edges can be generalised naturally: given any fixed H, one can ask for the minimum number of edges in copies of H. Two choices for the graph H seem particularly natural: $H = K_r$ and $H = C_{2r+1}$. We note that Erdős, Faudree and Rousseau [3] considered the number of pentagonal edges in n-vertex graphs with $\lfloor n^2/4\rfloor + 1$ edges. Furthermore, Füredi and Maleki [5] made progress on the above problem for any H with chromatic number 3 (so in particular for $H = C_{2l+1}$).

References

[1] P. Erdős, *Some theorems on graphs*, Riveon Lematematika **9** (1955), 13–17, in Hebrew.

[2] P. Erdős, *On a theorem of Rademacher-Turán*, Illinois J. Math **6** (1962), 122–127.

[3] P. Erdős, R. J. Faudree, and C. C. Rousseau, *Extremal problems involving vertices and edges on odd cycles*, Discr. Math. **101** (1992), 23–31.

[4] Z. Füredi, Z. Maleki, *The minimum number of triangular edges and a symmetrization for multiple graphs*, preprint, arXiv:1411.0771.

[5] Z. Fürdei, Z. Maleki, *A proof and a counterexample for a conjecture of Erdős concerning the minimum number of edges on odd cycles*, manuscript.

[6] L. Lovász, M. Simonovits, *On the number of complete subgraphs of a graph*, Proc. Fifth British Combinatorial Conference (Aberdeen) (1975), 431–442.

[7] L. Lovász, M. Simonovits, *On the number of complete subgraphs of a graph II*, Studies in pure mathematics, Birkhäuser, Basel, 1983, pp. 459–495.

[8] W. Mantel, Problem 28, Wiskundige Opaven **10** (1907), 60–61.

[9] H. Rademacher, (1941), unpublished.

[10] A. Razborov, *On the minimal density of triangles in graphs*, Combin. Probab. Comput. **17** (2008), 603–618.

On the chromatic number of random regular graphs

Samuel Hetterich
(joint work with Amin Coja-Oghlan, Charilaos Efthymiou)

Let $G(n, d)$ be the random d-regular graph on the vertex set $V = \{1, \ldots, n\}$. Determining the chromatic number of random graphs is one of the longest-standing challenges in probabilistic combinatorics. For the Erdős-Rényi model, which we denote by $G_{\mathrm{ER}}(n, m)$ the uniformly random graph on V with precisely m edges and which is the single most intensely studied model in the random graphs literature, the question dates back to the seminal 1960 paper that started the theory of random graphs [8]. Apart from that model, the one that has received the most attention certainly is the random regular graph $G(n, d)$ [4, 9]. We provide an almost complete solution to the chromatic number problem on $G(n, d)$, at least in the case that d remains fixed as $n \to \infty$. Our main result[1] is

Theorem 1. *There is a sequence $(\varepsilon_k)_{k\geq 3}$ with $\lim_{k\to\infty} \varepsilon_k = 0$ such that the following is true.*

(1) If $d \leq (2k-1)\ln k - 2\ln 2 - \varepsilon_k$, then $G(n, d)$ is k-colorable w.h.p.
(2) If $d \geq (2k-1)\ln k - 1 + \varepsilon_k$, then $G(n, d)$ fails to be k-colorable w.h.p.

Theorem 1 implies the following "threshold result".

Corollary 2. *There is a constant $k_0 > 0$ such that for any integer $k \geq k_0$ there exists a number $d_{k-\mathrm{col}}$ with the following two properties.*

- *If $d < d_{k-\mathrm{col}}$, then $G(n, d)$ is k-colorable w.h.p.*
- *If $d > d_{k-\mathrm{col}}$, then $G(n, d)$ fails to be k-colorable w.h.p.*

To obtain Corollary 2, let ε_k as in Theorem 1 and consider the interval $I_k = ((2k-1)\ln k - 2\ln 2 - \varepsilon_k, (2k-1)\ln k - 1 + \varepsilon_k)$. Then I_k has length $2\ln 2 - 1 + 2\varepsilon_k \approx 0.386 + 2\varepsilon_k$. Since $\varepsilon_k \to 0$, for sufficiently large k the interval I_k contains at most one integer. If it does, let $d_{k-\mathrm{col}}$ be equal to this integer. Otherwise, pick any $d_{k-\mathrm{col}}$ in I_k. For infinitely many values of k, $d_{k-\mathrm{col}}$ is not an integer, in which case Corollary 2 solves the k-colorability problem on $G(n, d)$ completely. In fact, we can make the following more precise quantitative statement. Since the sequence $((2k-1)\ln k \mod 1)_k$ is asymptotically uniform on $[0, 1]$ by Weyl's criterion [12], the set $\{k : d_{k-\mathrm{col}} \notin \mathbf{Z}\}$ has asymptotic density $2(1 - \ln 2) \approx 0.614$.

Another consequence of Theorem 1 is that it allows us to pin down the chromatic number $\chi(G(n, d))$ exactly for "almost all" d.

Corollary 3. *There exist a set $\mathcal{D} \subset \mathbf{Z}_{\geq 0}$ of asymptotic density 1 and a function $\mathcal{F} : \mathcal{D} \to \mathbf{Z}_{\geq 0}$ such that for all $d \in \mathcal{D}$ we have $\chi(G(n, d)) = \mathcal{F}(d)$ w.h.p.*

To obtain Corollary 3, let k_0, $(d_{k-\mathrm{col}})_{k\geq k_0}$ be as in Corollary 2, let $\mathcal{D} = \mathbf{Z}_{\geq 0} \setminus ([0, d_{k_0-\mathrm{col}}] \cup \{d_{k-\mathrm{col}} : k \geq k_0\})$ and define $\mathcal{F}(d)$ to be the smallest integer $k \geq k_0$

[1] The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 278857–PTCC

such that $d < d_{k-\mathrm{col}}$. Because $d_{(k+1)-\mathrm{col}} - d_{k-\mathrm{col}} \geq \ln k$ for large enough k, $\mathcal{D}$ has asymptotic density one.

The best current results on coloring $G_{\mathrm{ER}}(n,m)$ as well as the best prior result on $\chi(G(n,d))$ are obtained via the *second moment method* [3, 7, 10]. So are the present results. Generally, this is applying the *Paley-Zygmund inequality* to a random variable $Z \geq 0$ (s.t. $Z(G) > 0$ only if G is k-colorable) to obtain a lower bound on the probability that G is k-colorable if the second moment of Z is bounded from above by a constant times the square of the first moment of Z.

But what random variable Z might be suitable? A convenient choice is the number $Z_{k,\mathrm{bal}}$ of *balanced* k-colorings, in which all of the k color classes are the same size. Indeed, the core of the paper by Achlioptas and Naor [3] is to establish the second moment bound for the number $Z_{k,\mathrm{bal}}(G_{\mathrm{ER}}(n,m))$ of balanced k-colorings of $G_{\mathrm{ER}}(n,m)$ under the assumption that $d = 2m/n \leq (2k-2)\ln k - 2 + o_k(1)$. Achlioptas and Naor rephrase this problem as a non-convex optimization problem over the *Birkhoff polytope*, i.e., the set of doubly-stochastic $k \times k$ matrices, and establish the bound by solving a relaxation of this problem. This implies that $G_{\mathrm{ER}}(n,m)$ is k-colorable with a non-vanishing probability if $d \leq (2k-2)\ln k - 2 + o_k(1)$. The sharp threshold result of Achlioptas and Friedgut [1] leads to a probability of order $1 - o(1)$. A simple first moment argument shows that $G_{\mathrm{ER}}(n,m)$ is non-k-colorable w.h.p. if $d > (2k-1)\ln k$.

Achlioptas and Moore [2] use the same random variable $Z_{k,\mathrm{bal}}$ on $G(n,d)$ observing that the solution to the (relaxed) optimization problem over the Birkhoff polytope from [3] can be used as a “black box” to obtain the same results by using the second moment method. They prove that $G(n,d)$ is k-colorable with a *non-vanishing* probability if $d \leq (2k-2)\ln k - 2 + o_k(1)$. But unfortunately, in the case of random regular graphs there is no sharp threshold result to boost this probability to $1 - o(1)$. To get around this issue, Achlioptas and Moore instead adapt concentration arguments from [13, 16] to the random regular graph $G(n,d)$. However, these arguments inevitably require one extra “joker” color. Hence, Achlioptas and Moore obtain that $\chi(G(n,d)) \leq k+1$ w.h.p. for $d \leq (2k-2)\ln k - 2 + o_k(1)$.

Kemkes, Pérez-Giménez and Wormald [10] remove the need for this additional color, matching the result established in [3] for the Erdős-Rényi model. Instead of employing “abstract” concentration arguments, Kemkes, Pérez-Giménez and Wormald use the *small subgraph conditioning* technique [15].

Coja-Oghlan and Vilenchik [7] improved the result from [3] on the chromatic number of $G_{\mathrm{ER}}(n,m)$ recently. They showed that $G_{\mathrm{ER}}(n,m)$ is k-colorable w.h.p. if $d = 2m/n \leq (2k-1)\ln k - 2\ln 2 - o_k(1)$, gaining about an additive $\ln k$. They considered a different random variable, namely the number $Z_{k,\mathrm{good}}$ of “good” k-colorings, whose definition draws on intuition from non-rigorous statistical mechanics work on random graph coloring [11, 17]. Indeed, the concept of good colorings facilitates the computation of the second moment. The second moment method together with the sharp threshold result [1] leads to their improved lower bound on the k-colorabilty threshold.

Our main result matches [7] for $G(n, d)$. Following [10], we combine the second moment bound from [7] (which we can use largely as a "black box") with small subgraph conditioning. The main work in establishing the first part of Theorem 1 consists in computing the *first* moment of the number of good k-colorings in $G(n, d)$, a task that turns out to be technically quite non-trivial.

The previous *lower* bound on the chromatic number of $G(n, d)$ is based on a simple first moment argument over the number of k-colorings. The bound that can be obtained in this way, attributed to Molloy and Reed [14], is that $G(n, d)$ is non-k-colorable w.h.p. if $d > (2k-1) \ln k$. By contrast, the second assertion in Theorem 1 marks a strict improvement. The proof is via an adaptation of techniques developed in [6] for the random k-NAESAT problem. Extending this argument to the chromatic number problem on $G(n, d)$ requires substantial technical work. A matching improved lower bound on the chromatic number of $G_{\mathrm{ER}}(n, m)$ was recently obtained via a different argument [5].

References

[1] D. Achlioptas, E. Friedgut, *A sharp threshold for k-colorability*, Random Struct. Algorithms **14** (1999), 63–70.

[2] D. Achlioptas, C. Moore, *The chromatic number of random regular graphs*, Proc. 8th RANDOM (2004), 219–228.

[3] D. Achlioptas, A. Naor, *The two possible values of the chromatic number of a random graph*, Annals of Mathematics **162** (2005), 1333–1349.

[4] B. Bollobás, *Random graphs. 2nd edition*, Cambridge University Press (2001),.

[5] A. Coja-Oghlan, *Upper-bounding the k-colorability threshold by counting covers*, Electronic Journal of Combinatorics **20** (2013), P32.

[6] A. Coja-Oghlan, K. Panagiotou, *Catching the k-NAESAT threshold*, Proc. 44th STOC (2012), 899–908.

[7] A. Coja-Oghlan, D. Vilenchik, *Chasing the k-colorability threshold*, Proc. 54th FOCS (2013), 380-389.

[8] P. Erdős, A. Rényi, *On the evolution of random graphs*, Magayar Tud. Akad. Mat. Kutato Int. Kozl. **5** (1960), 17–61.

[9] S. Janson, T. Łuczak, A. Ruciński, *Random Graphs*, Wiley (2000).

[10] G. Kemkes, X. Pérez-Giménez, N. Wormald, *On the chromatic number of random d-regular graphs*, Advances in Mathematics **223** (2010), 300–328.

[11] F. Krzakala, A. Montanari, F. Ricci-Tersenghi, G. Semerjian, L. Zdeborova, *Gibbs states and the set of solutions of random constraint satisfaction problems*, Proc. National Academy of Sciences **104** (2007), 10318–10323.

[12] L. Kuipers, H. Niederreiter, *Uniform distribution of sequences*, Wiley (1974).

[13] T. Łuczak, *A note on the sharp concentration of the chromatic number of random graphs*, Combinatorica **11** (1991), 295–297.

[14] M. Molloy, B. A. Reed, *The chromatic number of sparse random graphs*, M. Math. Thesis, University of Waterloo (1992).

[15] R. Robinson, N. Wormald, *Almost all regular graphs are Hamiltonian*, Random Structures and Algorithms **5** (1994), 363–374.

[16] E. Shamir, J. Spencer, *Sharp concentration of the chromatic number of random graphs $G(n, p)$*, Combinatorica **7** (1987), 121–129.

[17] L. Zdeborová, F. Krzakala, *Phase transition in the coloring of random graphs*, Phys. Rev. E **76** (2007), 031131.

The sharp threshold for making squares

Paul Balister
(joint work with Béla Bollobás, Robert Morris)

Many of the fastest known algorithms for factoring large integers rely on finding subsequences of randomly generated sequences of integers whose product is a perfect square. Examples include Dixon's algorithm [4], the quadratic sieve [9], and the number field sieve (see, e.g., [8]); an excellent elementary introduction to the area is given by Pomerance [11]. In each of these algorithms one generates a sequence of congruences of the form

$$a_i \equiv b_i^2 \pmod{n}, \qquad i = 1, 2, \dots$$

and then one aims to find subsets of the a_i whose product is a perfect square, say $\prod_{i\in I} a_i = X^2$, so then one has $X^2 \equiv Y^2 \pmod{n}$ with $Y = \prod_{i\in I} b_i$. If one is lucky then $X \not\equiv \pm Y \pmod{n}$, in which case one can generate non-trivial factors of n as $\gcd(X \pm Y, n)$.

A useful heuristic, suggested by Schroeppel in the 1970s (see [11]), is to imagine that the numbers a_i are chosen independently and uniformly at random from the set $\{1, \dots, x\}$, for some suitably chosen integer x. Motivated by this idea, Pomerance [10] posed the problem of determining the *threshold* for the event that such a collection of random numbers contains a subset whose product is a square. To be precise, given $x \in \mathbb{N}$, let us define a probability space $\Omega(x)$ by choosing $a_1, a_2, \dots$ independently and uniformly at random from $\{1, \dots, x\}$, and a random variable $T(x)$ by setting

$$T(x) := \min\left\{ N \in \mathbb{N} : \prod_{i\in I} a_i \text{ is a perfect square for some } I \subseteq \big\{1, \dots, N\big\},\, I \neq \emptyset \right\}.$$

Pomerance [12] proved that for all $\varepsilon > 0$,

$$\text{(1)} \qquad \exp\Big(\big(1-\varepsilon\big)\sqrt{2\log x \log\log x}\Big) \le T(x) \le \exp\Big(\big(1+\varepsilon\big)\sqrt{2\log x \log\log x}\Big)$$

with high probability[1], and conjectured that $T(x)$ in fact exhibits a *sharp threshold*, i.e., that there exists a function $f(x)$ such that $(1-\varepsilon)f(x) \le T(x) \le (1+\varepsilon)f(x)$ with high probability for all $\varepsilon > 0$. Croot, Granville, Pemantle and Tetali [3] significantly improved these bounds (see (3), below), and stated a conjecture as to the location of the threshold, i.e., the value of the function $f(x)$. Our main result proves these two conjectures.

In order to state the theorem and conjecture of Croot, Granville, Pemantle and Tetali, we need to recall some standard notation. Let $\pi(y)$ denote the number of primes less than or equal to y, let $\Psi(x, y)$ denote the number of y-*smooth* integers in $\{1, \dots, x\}$, that is, the number of integers with no prime factor strictly greater than y, and define

$$\text{(2)} \qquad J(x) = \min_{2\le y\le x} \frac{\pi(y)x}{\Psi(x, y)}.$$

[1] We use the term *with high probability* to mean with probability tending to 1 as $x \to \infty$.

It can be shown that the minimum in (2) occurs at

$$y_0 = y_0(x) = \exp\Big(\big(1+o(1)\big)\sqrt{\tfrac{1}{2}\log x \log\log x}\Big)$$

and that

$$J(x) = y_0^{2+o(1)} = \exp\Big(\big(1+o(1)\big)\sqrt{2\log x \log\log x}\Big).$$

We remark that a relatively straightforward argument, originally due to Schroeppel (see [12]), shows that, for all $\varepsilon > 0$,

$$T(x) \le \big(1+\varepsilon\big)J(x)$$

with high probability, which implies the upper bound in (1). Indeed, if $N \ge (1+\varepsilon)J(x)$ then with high probability at least $\pi(y_0)+1$ of the numbers $a_1,\dots,a_N$ will be y_0-smooth, since each a_i is y_0-smooth with probability $\Psi(x,y_0)/x = \pi(y_0)/J(x)$. Now, by simple linear algebra, it follows that the vectors encoding the primes that divide a_i an odd number of times are linearly dependent over $\mathbb{F}_2$, and hence there exists a subset whose product is a square, as required.

Pomerance's conjecture remained wide open for over ten years, until a fundamental breakthrough was obtained by Croot, Granville, Pemantle and Tetali [3], who used a combination of techniques from number theory, probability theory and combinatorics to show that

$$\frac{\pi}{4}\big(e^{-\gamma}-\varepsilon\big)J(x) \le T(x) \le \big(e^{-\gamma}+\varepsilon\big)J(x) \tag{3}$$

with high probability, where $\gamma \approx 0.5772$ is the Euler–Mascheroni constant.

The authors of [3] conjectured that the upper bound in (3) is sharp. Our main theorem confirms their conjecture.

Theorem 1. *For all $\varepsilon > 0$ we have with high probability*

$$\big(e^{-\gamma}-\varepsilon\big)J(x) \le T(x) \le \big(e^{-\gamma}+\varepsilon\big)J(x).$$

Since the upper bound in Theorem 1 was proved in [3], we are only required to prove the lower bound. However, we also obtain a new proof of the upper bound, quite different from that given in [3], as a simple consequence of our method. Another significant advantage of our proof is that it gives detailed structural information about the typical properties of the set of numbers that are left over after sieving and "singleton removal" (see, e.g., [7]).

The lower bound of Croot, Granville, Pemantle and Tetali [3] was obtained via the first moment method, by counting the expected number of non-empty subsets $I \subseteq \{1,\dots,N\}$ such that $\prod_{i\in I} a_i$ is a square. Unfortunately, we can show that there exists a constant $c > 0$ such that this expected number blows up when $N \ge (e^{-\gamma}-c)J(x)$, which implies that a sharp lower bound cannot be obtained by this method.

Instead, we use the method of self-correcting martingales, introduced recently in [5] (see also [1, 2]), to follow a random process which removes numbers from the set $\{a_1,\dots,a_N\}$ as soon as we can guarantee that they are not contained in a subset whose product is a square. This is in one sense very simple: a number a_i can be discarded if there exists a prime for which a_i is the only remaining number that it divides an odd number of times. However, this apparent simplicity is deceiving, and the technical challenges involved in tracking the process are substantial. For example, we need to reveal the random numbers $\{a_1, \dots, a_N\}$ gradually (roughly speaking, prime by prime, in decreasing order), and the amount of information we are allowed to reveal at each step is rather delicate. Moreover, the removal of a number can trigger an avalanche, causing many other numbers to be removed in the same step. Fortunately, however, self-correction (which is partly a result of these avalanches) allows us to show that the process remains subcritical (in a certain natural sense), which in turn allows us to control the upper tail of the size of the avalanches. In order to do so, we need good control over the dependence between the prime factors of the numbers $\{a_1, \dots, a_N\}$, conditioned on the information we have observed so far. This is obtained by a comparison theorem which gives strong bounds on the ratio between the (conditional) probability of certain 'basic' events, and the corresponding probabilities in a simpler independent model. These bounds require some number-theoretic estimates, most of which follow from the fundamental work of Hildebrand and Tenenbaum [6] on smooth numbers.

Using the method described above, we have shown that with high probability the number of 'active' numbers (i.e., elements of $\{a_1, \dots, a_N\}$ that we have not yet discarded) tracks a deterministic function until there are very few numbers remaining (roughly $e^{-C\sqrt{\log y_0}} y_0$ for some large constant C), at which point we can apply the first moment calculation from [3]. Finally, in order to prove the upper bound in Theorem 1, we observe that the ratio of the number of active numbers and active primes (that is, primes which could still appear in some square) approaches 1 when we have revealed primes down to y_0 and $N/J(x)$ approaches $e^{-\gamma}$. Thus, by adding just a few extra y_0-smooth numbers, we can apply the linear algebra approach of Schroeppel to obtain a subset whose product is a square, as required. We would like to thank Jonathan Lee for pointing out to us this particularly simple deduction from our proof.

References

[1] T. Bohman and P. Keevash, Dynamic Concentration of the Triangle-Free Process, submitted.

[2] T. Bohman, A. Frieze and E. Lubetzky, Random triangle removal, *Adv. Math.,* **280** (2015), 379–438.

[3] E. Croot, A. Granville, R. Pemantle and P. Tetali, Sharp Transitions in Making Squares, *Ann. Math,* **175** (2012), 1507–1550.

[4] J.D. Dixon, Asymptotically fast factorization of integers, *Math. Comp.* **36** (1981), 255–260.

[5] G. Fiz Pontiveros, S. Griffiths and R. Morris, The triangle-free process and $R(3, k)$, submitted.

[6] A. Hildebrand and G. Tenenbaum, On integers free of large prime factors. *Trans. Amer. Math. Soc.,* **296** (1986), 265–290.

[7] T. Kleinjung et al., Factorization of a 768-bit RSA modulus `https://eprint.iacr.org/2010/006.pdf`

[8] A.K. Lenstra and H.W. Lenstra Jr. (eds.), The development of the number field sieve, Lecture Notes in Math., **1554** , Springer–Verlag, Berlin and Heidelberg, 1993.

[9] Carl Pomerance, Analysis and Comparison of Some Integer Factoring Algorithms, in Computational Methods in Number Theory, Part I, H.W. Lenstra, Jr. and R. Tijdeman, eds., Math. Centre Tract 154, Amsterdam, 1982, pp. 89–139.

[10] C. Pomerance, The role of smooth numbers in number theoretic algorithms, *Proc. Intern. Congr. Math.,* (Zurich, 1994), Birkhaüser, Basel, 1995, pp. 411–422.

[11] C. Pomerance, A Tale of Two Sieves, *Notices Amer. Math. Soc.* **43** (1996), 1473–1485.

[12] C. Pomerance, Multiplicative independence for random integers, *Analytic Number Theory: Proceedings of a Conference in Honor of Heini Halberstam, Vol. 2,* B. Berndt, H. Diamond, A. Hildebrand, eds., Birkhäuser, Boston, 1996, 703–711.

Extremal problems for uniformly dense hypergraphs

Mathias Schacht
(joint work with Christian Reiher, Vojtěch Rödl)

1. Extremal problems for graphs and hypergraphs

Given a fixed graph F a typical problem in extremal graph theory asks for the maximum number of edges that a (large) graph G on n vertices containing no copy of F can have. More formally, for a fixed graph F let the *extremal number* $\mathrm{ex}(n, F)$ be the number $|E|$ of edges of an F-free graph $G = (V, E)$ on $|V| = n$ vertices with the maximum number of edges. It is well known and not hard to observe that the sequence $\mathrm{ex}(n, F)/\binom{n}{2}$ is decreasing. Consequently one may define the *Turán density*

$$\pi(F) = \lim_{n\to\infty} \frac{\mathrm{ex}(n, F)}{\binom{n}{2}}$$

which describes the maximum density of large F-free graphs. The systematic study of these extremal parameters was initiated by Turán [9], who determined $\mathrm{ex}(n, K_k)$ for complete graphs K_k. Thanks to his work and the results from [3] by Erdős and Stone it is known that the Turán density of any graph F with at least one edge can be explicitly computed using the formula

$$\pi(F) = \tfrac{\chi(F)-2}{\chi(F)-1}\,. \tag{1}$$

Already in his original work [9] Turán asked for hypergraph extensions of these extremal problems. We restrict ourselves to 3-*uniform hypergraphs* $H = (V, E)$, where V is a finite set of *vertices* and the set of *hyperedges* $E \subseteq \binom{V}{3}$ is a collection of 3-element sets of vertices. Here we shall only consider graphs and 3-uniform hypergraphs and when we are referring simply to a hypergraph we will always mean a 3-uniform hypergraph. Despite considerable effort no formula similar to (1) is known or conjectured to hold for general 3-uniform hypergraphs F. Determining the value of $\pi(F)$ is a well known and hard problem even for "simple" hypergraphs like the complete 3-uniform hypergraph $K_4^{(3)}$ on four vertices, which is also called the *tetrahedron.* Currently the best known bounds for its Turán density are

$$\frac{5}{9} \leq \pi(K_4^{(3)}) \leq 0.5616\,,$$

where the lower bounds is given by what is believed to be an optimal construction due to Turán (see, e.g., [2]). The upper bound is due to Razborov [6] (see also Baber and Talbot [1]) and its proof is based on the *flag algebra method* introduced by Razborov [5]. For a thorough discussion of Turán type results and problems for hypergraphs we refer to the recent survey of Keevash [4].

1.1. **Uniformly dense hypergraphs.** We consider a variant of Turán type questions in connection with uniformly dense hypergraphs. Roughly speaking, a uniformly dense hypergraph has the property that a specified class of witnesses always induces at least a given proportion of all possible hyperedges on these witnesses. Here we will consider the following notion.

Definition 1. *A* 3*-uniform hypergraph* $H = (V, E)$ *is* $(d, \eta, \therefore)$-dense *if for every subset* $X \subseteq V$ *of vertices and every subset of pairs of vertices* $P \subseteq V \times V$ *the number* $e_{\therefore}(X, P)$ *of pairs* $(x, (y, z)) \in X \times P$ *with* $\{x, y, z\} \in E$ *satisfies*

$$e_{\therefore}(X, P) \geq d\,|X|\,|P| - \eta\,|V|^3 \,.$$

We are interested in Turán densities for $\therefore$-dense hypergraphs given by the following function. For a 3-uniform hypergraph F we set

$$\pi_{\therefore}(F) = \sup\bigl\{d \in [0,1] \colon \text{for every } \eta > 0 \text{ and } n \in \mathbb{N} \text{ there exists an } F\text{-free}, \\ \text{3-uniform, } (d, \eta, \therefore)\text{-dense hypergraph } H \text{ with } |V(H)| \geq n\bigr\}\,.$$

The first interesting open case is, when F is the tetrahedron $K_4^{(3)}$. The following random construction from [8] establishes

$$\pi_{\therefore}(K_4^{(3)}) \geq \frac{1}{2}\,. \tag{2}$$

Example 1. Given any map $\varphi\colon \binom{[n]}{2} \to \{\text{red}, \text{green}\}$ we define the 3-uniform hypergraph H_φ with vertex set $[n] = \{1, \dots, n\}$ by putting a triple $\{i, j, k\}$ with $i < j < k$ into $E(H_\varphi)$ if and only if the colours of ij and ik differ.

Irrespective of the choice of the colouring φ, the hypergraph H_φ contains no tetrahedra: for if a, b, c, and d are any four distinct vertices, say with $a = \min(a, b, c, d)$, then it is impossible for all three of the pairs ab, ac, and ad to have distinct colours, whence not all three of the triples abc, abd, and acd can be hyperedges of H_φ.

Moreover, if the colouring φ is chosen uniformly at random, then for any $\eta > 0$ the hypergraph H_φ is with high probability $(1/2, \eta, \therefore)$-dense as n tends to infinity. This is easily checked using standard tail estimates for binomial distributions. Consequently, the lower bound (2) follows.

We provide a matching upper bound and show that for $K_3^{(4)}$-free $\therefore$-dense hypergraphs the construction given in Example 1 is best possible.

Theorem 2. *For every* $\varepsilon > 0$ *there exists an* $\eta > 0$ *and an integer* n_0 *such that every 3-uniform* $(\frac{1}{2} + \varepsilon, \eta, \therefore)$*-dense hypergraph* H *with at least* n_0 *vertices contains a tetrahedron. In particular, we have* $\pi_{\therefore}(K_4^{(3)}) = 1/2$.

The proof of Theorem 2 is based on the regularity method for 3-uniform hypergraphs combined with Ramsey-type arguments and ideas from extremal combinatorics. The details can be found in [7].

References

[1] R. Baber and J. Talbot, *Hypergraphs do jump*, Combin. Probab. Comput. **20**(2) (2011), 161–171.

[2] P. Erdős, *Paul Turán, 1910–1976: his work in graph theory*, J. Graph Theory **1** (1977), 97–101.

[3] P. Erdős and A. H. Stone, *On the structure of linear graphs*, Bull. Amer. Math. Soc. **52** (1946), 1087–1091.

[4] P. Keevash, *Hypergraph Turán problems* Surveys in combinatorics 2011, London Math. Soc. Lecture Note Ser. **392** (2011), 83–139.

[5] A. A. Razborov, *Flag algebras*, J. Symbolic Logic **72**(4) (2007), 1239–1282.

[6] A. A. Razborov, *On 3-hypergraphs with forbidden 4-vertex configurations*, SIAM J. Discrete Math. **24**(3) (2010), 946–963.

[7] Chr. Reiher, V. Rödl, and M. Schacht, *Embedding tetrahedra into quasirandom hypergraphs*, preprint.

[8] V. Rödl, *On universality of graphs with uniformly distributed edges*, Discrete Math. **59**(1-2) (1986), 125–134.

[9] P. Turán, *Eine Extremalaufgabe aus der Graphentheorie*, Mat. Fiz. Lapok **48** (1941), 436–452.

Drift Analysis Revisited

Angelika Steger
(joint work with Johannes Lengler)

One of the easiest randomized greedy optimization algorithms is the following evolutionary algorithm which aims at maximizing a boolean function $f : \{0,1\}^n \to \mathbb{R}$. This algorithm starts with a random search point $x \in \{0,1\}^n$, and in each round it flips each bit of x with probability (or *mutation rate*) c/n, where $c > 0$ is the *mutation parameter*. The thus created *offspring* x' replaces x if and only if $f(x') > f(x)$. We are interested in the *optimization time* of f, i.e., in the number of rounds until a maximum of f is found. Even for the seemingly trivial case that f is a strictly monotone function (that is, $f(x) > f(x')$ for all x, x' so that $x \neq x'$ and $x_i \geq x'_i$ for all $1 \leq i \leq n$) determining the asymptotic running time turned out to be far from trivial. One of the first rigorous results in this direction was [6] who determined the running time for the case that $f(x) = \sum_{i=1}^n x_i$. For general linear function it required substantial efforts [5, 7, 8, 4, 3] until Doerr and Goldberg [1] finally showed that the running time is $\Theta(n \log n)$ for all constants $c > 0$. For general linear functions it is easy to see, cf. e.g. [2], that the running time is also $\Theta(n \log n)$ for all $0 < c < 1$. However, as it turned out, this is not necessarily so for larger mutation parameters. Doerr et al. [2] showed that there are monotone function such that for $c > 16$ the algorithm takes exponential time.

In this talk we will provide short and elegant proofs for various drift theorem that will allow us to give proofs for the above statements which are simpler and stronger than previous results. The accompanying paper is completely self-contained.

References

[1] Benjamin Doerr and Leslie Goldberg. Adaptive drift analysis. *Algorithmica*, pages 1–27, 2011.

[2] Benjamin Doerr, Thomas Jansen, Dirk Sudholt, Carola Winzen, and Christine Zarges. Mutation rate matters even when optimizing monotonic functions. *Evolutionary computation*, 21(1):1–27, 2013.

[3] Benjamin Doerr, Daniel Johannsen, and Carola Winzen. Multiplicative drift analysis. *Algorithmica*, 64(4):673–697, 2012.

[4] Benjamin Doerr, Daniel Johannsen, and Carola Winzen. Non-existence of linear universal drift functions. *Theoretical Computer Science*, 436:71–86, 2012.

[5] Stefan Droste, Thomas Jansen, and Ingo Wegener. On the analysis of the (1+1) evolutionary algorithm. *Theoretical Computer Science*, 276:51–81, 2002.

[6] H. Mühlenbein, *How genetic algorithms really work: Mutation and Hillclimbing*, In: Parallel Problem Solving from Nature PPSN II, R. Männer, R. Manderick (eds.), North-Holland, Amsterdam (1992), pp. 15–25.

[7] Jun He and Xin Yao. A study of drift analysis for estimating computation time of evolutionary algorithms. *Natural Computing*, 3:21–35, 2004.

[8] Jens Jägersküpper. Combining markov-chain analysis and drift analysis. *Algorithmica*, 59(3):409–424, 2011.

The degree sequence of a random graph

Nick Wormald
(joint work with Anita Liebenau)

The degree sequence of a random graph has received considerable attention, and indeed was the first major topic dealt with in Bollobás' seminal book on random graphs [3]. Many interesting results are included there, for instance on the distribution of the k^{th} largest element d_k of the sequence was determined quite precisely when k is small. The book "Poisson Approximation" by Barbour, Holst and Janson [1] contained much information on the distribution of the number D_k of vertices of degree k.

Independently of this, the asymptotic numbers of graphs with given degrees were considered by various authors, culminating in papers giving asymptotic formulae for a wide range of degrees, provided the average degree d is in the range $d = o(\sqrt{n})$ (see McKay and Wormald [4]) or between $cn/\log n$ and $n/2$ for a certain c (see [5], and more recently [2] for a wider spread of degrees, but similar density). The complementary ranges larger than $n/2$ are automatically implied.

In [6], McKay and Wormald, found that the asymptotic formulae derived in both sparse and dense cases can be recast into a common form, and conjectured that this form holds for all densities (except in some trivial cases). To present the conjecture, we first make some definitions. Let A_n and B_n be two sequences of probability spaces with the same underlying set for each n. Suppose that for all events H_n having probability at least n^{-K} for all K, it is true that $\mathbb{P}_{A_n}(H) \sim \mathbb{P}_{B_n}(H)$. Then we say that A_n and B_n are *asymptotically quite equivalent* (a.q.e.). We assume that a graph on n vertices has vertex set $v_1, \ldots, v_n$ and degree sequence $(d_1, \ldots, d_n)$, so that $d(v_i) = d_i$. If $\mathcal{G}$ is a (random) graph, let $\mathcal{D}(\mathcal{G})$ be its (random) degree sequence, and define $B_p(n)$ to be the random sequence consisting of n independent binomial variables $\mathrm{Bin}(n-1, p)$.

Given m, set $p = m/\binom{n}{2}$. In [6] it was conjectured that for $p(1-p) = \omega(\log n/n^2)$,

(*i*) $\mathcal{D}(\mathcal{G}(n,m))$ and $B_p(n) \mid_{\Sigma=2m}$ are a.q.e.
(*ii*) $\mathcal{D}(\mathcal{G}(n,p))$ and $B_{\hat{p}}(n) \mid_{\Sigma \text{ is even}}$ are a.q.e.,

where Σ denotes the sum of the components of the random vector $B_p(n)$, and $\hat{p}$ has a randomly chosen value that is tightly concentrated near p. It is shown in [6] that, if true for a given function m (and p), (ii) implies that general classes of properties of $\mathcal{D}(\mathcal{G}(n,p))$ can be derived by transferring results from the independent binomial model $B_p(n)$. (This is done be showing how to deal with the conditioning on parity, and also the integration implicit in $\hat{p}$.) It is also observed, from the known asymptotic formulae, that (i) and (ii) hold when $p = o(1/\sqrt{n})$ or $p(1-p) > n/c\log n$.

The condition on p in both cases is just enough to ensure that the number of edges in both the graph and its complement grows somewhat faster than $\log n$.

The conjectures were actually made in a stronger form, in terms of the asymptotic numbers of graphs with degree sequences that have the degrees in the typical ranges for the random graphs.

Using methods that are quite different from those previously used for this problem, we prove that all of these conjectures hold by establishing them for all p in the gap. This shows that for instance the asymptotic formula for the number of d-regular graphs conjectured in [6] is valid for all functions d of n.

We outline some of the main elements of our approach. Let $d \le n$, let $\mathbf{d}$ denote a non-negative integer sequence of length n such that the entries sum to $2m = dn$. Let $\mathcal{G}(\mathbf{d})$ denote the set of graphs with degree sequence $\mathbf{d}$, and put $N(\mathbf{d}) = |\mathcal{G}(\mathbf{d})|$. We first compare $N(\mathbf{d})$ to $N(\mathbf{d} - \mathbf{e_i} + \mathbf{e_j})$, the degree sequence obtained by decreasing d_i by 1, and increasing d_j by 1, for $1 \le i, j \le n$.

For simplicity of notation, fix $i = 1, j = 2$, and let G be a graph in $\mathcal{G}(\mathbf{d})$ with a distinguished edge incident to v_1. The number of such objects is $d_1 N(\mathbf{d})$. Disconnecting the distinguished edge from v_1 and reconnecting it to v_2 (i.e. if the edge is $v_1 v_i$, deleting it and adding $v_2 v_i$), produces a graph $G' \in \mathcal{G}(\mathbf{d} - \mathbf{e_1} + \mathbf{e_2})$ with a distinguished edge incident to v_2, unless this switching produces a loop (whence the distinguished edge is $v_1 v_2$) or a double edge (whence $v_2 v_i$ is already an edge in G). Let $\mathrm{Bad}(v_1, v_2, \mathbf{d})$ denote the probability that this happens when G is chosen uniformly at random from $\mathcal{G}(\mathbf{d})$ and the distinguished edge is chosen uniformly at random from all edges incident to v_1. Then the number of *admissible switchings* is

$$d_1 N(\mathbf{d})(1 - \mathrm{Bad}(v_1, v_2, \mathbf{d})).$$

Conversely, let $G' \in \mathcal{G}(\mathbf{d} - \mathbf{e_1} + \mathbf{e_2})$ with a distinguished edge incident to v_2, say $v_2 v_i$. Then G' is obtained through a switching as described above unless $v_1 v_i$ is an edge in G' or the distinguished edge is $v_1 v_2$. The number of such graphs with a distinguished edge, and hence the number of admissible switchings, is

$$(d_2+1)N(\mathbf{d}-\mathbf{e_1}+\mathbf{e_2})(1-\mathrm{Bad}(v_2,v_1,\mathbf{d}-\mathbf{e_1}+\mathbf{e_2})).$$

It follows that

$$R_{12}(\mathbf{d}) := \frac{N(\mathbf{d})}{N(\mathbf{d}-\mathbf{e_1}+\mathbf{e_2})} = \frac{d_2+1}{d_1}\cdot\frac{1-\mathrm{Bad}(v_2,v_1,\mathbf{d}-\mathbf{e_1}+\mathbf{e_2})}{1-\mathrm{Bad}(v_1,v_2,\mathbf{d})}. \tag{1}$$

The probability $\mathrm{Bad}(v_1,v_2,\mathbf{d})$ can be expressed in terms of various quantities $P_{ij}(\mathbf{d'})$, the probability of the edge v_iv_j in a graph G that is drawn uniformly at random from $\mathcal{G}(\mathbf{d'})$, where $\mathbf{d'}$ is a degree sequence quite similar to $\mathbf{d}$. Without loss of generality, we may focus on $P_{12}(\mathbf{d})$. We obtain the following identity by considering a distinguished edge incident to v_1:

$$P_{12}(\mathbf{d}) = d_1\left(\sum_{i=2}^{n} R_{2i}(\mathbf{d}-\mathbf{e_i})\frac{1-P_{1i}(\mathbf{d}-\mathbf{e_1}-\mathbf{e_i})}{1-P_{12}(\mathbf{d}-\mathbf{e_1}-\mathbf{e_2})}\right). \tag{2}$$

Using the recursive identities (1) and (2), we can eventually show, under suitable assumptions on $\mathbf{d}$, that

$$P_{12}(\mathbf{d}) = \frac{d_1d_2(n-d)}{(n-1)(dn-dd_1-dd_2+d_1d_2)} + O(\delta(n)\sigma^*/dn)$$

and

$$R_{12}(\mathbf{d}) = \frac{d_2(n-d_1)}{d_1(n-d_2)}\Big(1-\frac{d_1-d_2}{dn}\Big) + O(\delta(n)\sigma^*/dn), \tag{3}$$

where $\delta(n)$ is an upper bound on $\max_i |d_i-d|$, and $\sigma^* = \left|1-\frac{\sum_i(d_i-d)^2}{dn}\right|$.

For almost all degree sequences of the random graph $\mathcal{G}(n,p)$, under suitable assumptions on p, we have $\sum_i |d_i-d| = O(n\sqrt{d})$ and the relative error term in (3) is $o(1/n\sqrt{d})$. For such a degree sequence $\mathbf{d}$, the ratio of $N(\mathbf{d})$ to $N(\mathbf{d}_0)$, where $\mathbf{d}_0$ is nearly regular, is a product of $O(n\sqrt{d})$ separate ratios given by (3). Hence the relative error in the resultant ratio is $o(1)$. The conditions on p mentioned above are satisfied provided that

$$p = o(1/\sqrt{\log n})$$

and also that p grows sufficiently quickly. Hence, for all such p, the ratios agree with the binomial conjecture mentioned above. From this we are able to show that the conjecture holds in full.

More accurate estimates of the error terms allow us to find asymptotic formulae for the numbers of graphs of given degrees for a quite wide range of degree sequences. We also obtain similar results for bipartite graphs, directed graphs and r-uniform hypergraphs.

References

[1] A.D. Barbour, L. Holst and S. Janson, *Poisson Approximation*, Clarendon Press, Oxford, 1992.

[2] A. Barvinok and J.A. Hartigan, The number of graphs and a random graph with a given degree sequence, *Random Structures & Algorithms* **42**, no. 3 (2013), 301–348.

[3] B. Bollobás, *Random Graphs,* Academic Press, 1985 (Second Edition 2001).

[4] B.D. McKay and N.C. Wormald, Asymptotic enumeration by degree sequence of graphs with degrees $o(n^{1/2})$, *Combinatorica* **11** (1991) 369–382.

[5] B.D. McKay and N.C. Wormald, Asymptotic enumeration by degree sequence of graphs of high degree, *Europ. J. Combinatorics* **11** (1990), 565–580.

[6] B.D. McKay and N.C. Wormald, The degree sequence of a random graph. I. The models, *Random Structures& Algorithms* **11** (1997), 97–117.

Finite reflection groups and graph norms

David Conlon

(joint work with Joonkyung Lee)

Let H be a graph and $f : [0,1]^2 \to \mathbb{R}$ be a Lebesgue integrable function. Consider the integral

$$\int \prod_{ij \in E(H)} f(x_i, x_j) d\mu^{|V(H)|}, \tag{1}$$

where μ is the Lebesgue measure on $[0,1]$. If we choose f so as to model the adjacency matrix of a graph G, the integral above corresponds to the homomorphism density $t_H(G)$, which plays a key role in extremal graph theory. In particular, when H is a cycle of length 4, (1) becomes the fourth power of the Gowers uniformity norm, which measures the quasirandomness of f. More generally, when H is an even cycle, (1) corresponds to the well-known Schatten–von Neumann norms in operator theory, while a suitable hypergraph generalisation is related to Gowers' octahedral norms.

A natural question, proposed by Lovász, is to determine those graphs H for which the integral (1) gives a (semi-)norm. Formally, we say that a graph H is *norming* if the functional defined by

$$\|f\|_H := \left| \int \prod_{ij \in E(H)} f(x_i, x_j) d\mu^{|V(H)|} \right|^{1/|E(H)|} \tag{2}$$

is a semi-norm, and H is *weakly norming* if

$$\|f\|_{r(H)} := \left(\int \prod_{ij \in E(H)} |f(x_i, x_j)| d\mu^{|V(H)|} \right)^{1/|E(H)} \tag{3}$$

is a norm. It is easy to check that every norming graph is also weakly norming.

The study of (weakly) norming graphs was initiated by Hatami [2]. A moment's thought shows that H is necessarily bipartite whenever it is weakly norming. In [2], Hatami showed that hypercubes and complete bipartite graphs are weakly norming. He also observed that for even cycles, $\|\cdot\|_{C_{2k}}$ corresponds to the classical Schatten–von Neumann norms, and hence even cycles are norming. Subsequently, Lovász [3] showed that the complete bipartite graph $K_{n,n}$ minus a perfect matching is weakly norming.

We generalise these results, finding a much larger class of (weakly) norming graphs coming from finite reflection groups that includes all of the known examples. To give some indication of our results, suppose that k and r are integers with $k \leq r$ and $\mathcal{P}$ is a polytope. Consider the bipartite graph between k-faces and r-faces of $\mathcal{P}$ indicating their incidence. That is, we place an edge between a k-face and an r-face if one contains the other. We call this graph the (k, r)-incidence graph of the polytope $\mathcal{P}$. We then have the following theorem:

Theorem 1. *A bipartite graph H is weakly norming whenever it is the (k, r)-incidence graph of a regular polytope for some k and r.*

For example, in an n-dimensional simplex, the k-faces and r-faces naturally correspond to $(k+1)$-element and $(r+1)$-element subsets of $[n]$. Therefore, the (k, r)-incidence graph of an n-simplex is the inclusion graph between $(k+1)$-sets and $(r+1)$-sets. In particular, the $(0,1)$-incidence graph is the 1-subdivision of K_n, the $(0, n-2)$-incidence graph is $K_{n,n}$ minus a perfect matching, and the $(0, n-1)$-incidence graph is the star $K_{1,n}$, which by tensor powering shows that $K_{m,n}$ is also weakly norming. Even cycles C_{2k} are the $(0,1)$-incidence graphs of regular k-gons and thus are weakly norming. More generally, by considering the $(0,1)$-incidence graph of any regular polytope, such as hypercubes, the icosahedron, or the dodecahedron, we see that their 1-subdivisions are weakly norming.

When proving that $\|\cdot\|_{r(H)}$ is a norm, all of the difficulties lie in proving the triangle inequality. Hatami's work in [2] started from the observation that a Hölder-like inequality is equivalent to the triangle inequality for $\|\cdot\|_{r(H)}$. To state his condition, we have to introduce some notation that slightly generalises (2) and (3). Let $m = |E(H)|$ and let $\chi : E(G) \to [m]$ be a (not necessarily proper) edge colouring of H. Consider a family $\mathcal{F} = \{f_1, f_2, \cdots, f_m\}$ of integrable functions on $[0,1]^2$, indexed by $1, 2, \cdots, m$. Now define a multilinear product $\langle \cdot \rangle_H$ of m functions with respect to χ by

$$\langle \mathcal{F}; \chi \rangle_H := \int \prod_{e=ij \in E(H)} f_{\chi(e)}(x_i, x_j) d\mu^{|V(H)|}. \tag{4}$$

Note that if $f_i = |f|$ for all $i = 1, 2, \cdots, m$, then $\langle \mathcal{F}; \chi \rangle_H = \|f\|_{r(H)}^{|E(H)|}$, while if $f_i = f$, then $|\langle \mathcal{F}; \chi \rangle_H| = \|f\|_H^{|E(H)|}$. In [2], it was shown that the triangle inequality for $\|\cdot\|_{r(H)}$ is equivalent to showing that the following inequality is true for all choices of $\mathcal{F}$ and χ:

$$\langle \mathcal{F}; \chi \rangle_H \leq \prod_{e \in E(H)} \|f_{\chi(e)}\|_{r(H)}. \tag{5}$$

Furthermore, $\|\cdot\|_H$ is a semi-norm if and only if the inequality obtained by replacing $\|f_{\chi(e)}\|_{r(H)}$ with $\|f_{\chi(e)}\|_H$ holds.

Suppose the functions $f_1, \cdots, f_m$ correspond to m distinct graphs on the same vertex set and imagine each edge of f_i has the colour i. Then $\langle \mathcal{F}; \chi \rangle_H$ is the number of (homomorphic) copies of H which are coloured according to χ, i.e., each edge $e \in E(H)$ receives the colour $\chi(e)$. In particular, if χ is a one-to-one map then

$\langle \mathcal{F}; \chi \rangle_H$ counts the number of 'rainbow' copies of H, while $\|f_i\|_{r(H)}^{|E(H)|}$ counts the number of monochromatic copies of H in colour i. Thus, (5) is equivalent to the statement that the number of rainbow copies of H is bounded above by the geometric mean of the number of monochromatic copies in each colour.

Let f be a function on $[0,1]^2$, fix an edge e^* of H, and put $\chi(e^*) = 1$, $f_1 = |f|$, and $f_2 = f_3 = \cdots = f_m = 1$. Then $\langle \mathcal{F}; \chi \rangle_H = \|f\|_{r(K_2)}$, where K_2 is just a single edge, so (5) implies that

$$\|f\|_{r(K_2)} \leq \|f\|_{r(H)}. \tag{6}$$

That is, when H is weakly norming, H satisfies Sidorenko's conjecture, which says exactly that for any bipartite graph H and any f an inequality of the form (6) holds. Sidorenko's conjecture is one of the major open problems in extremal graph theory, and there has been much recent work verifying the conjecture for a widening class of graphs. As noted above, all weakly norming graphs also satisfy Sidorenko's conjecture. However, this is not the only application of our results to Sidorenko's conjecture. By applying the entropy techniques developed in [1, 4], weakly norming graphs can also be used as building blocks for constructing new graphs that satisfy the conjecture.

References

[1] D. Conlon, J. H. Kim, C. Lee and J. Lee, *Some advances on Sidorenko's conjecture*, arXiv:1510.06533 [math.CO].

[2] H. Hatami, *Graph norms and Sidorenko's conjecture*, Israel J. Math. **175** (2010), 125–150.

[3] L. Lovász, *Large Networks and Graph Limits*, Amer. Math. Soc. Colloq. Publ., American Mathematical Society, 2012.

[4] B. Szegedy, *An information theoretic approach to Sidorenko's conjecture*, arXiv:1406.6738 [math.CO].

Successive minimum spanning trees

Svante Janson
(joint work with Gregory Sorkin)

Consider the complete graph K_n with edge costs that are i.i.d. random variables, with a uniform distribution $U(0,1)$ (or, alternatively, an exponential distribution $\mathrm{Exp}(1)$). A well-known problem is to find the minimum (cost) spanning tree T_1, and its cost $c(T_1)$. A famous result by Frieze [2] shows that as $n \to \infty$, $c(T_1)$ converges in probability to $\zeta(3)$. (In both the uniform and exponential cases.)

Suppose now that we want a second spanning tree T_2, edge-disjoint from the first, and that we select it in a greedy fashion by first finding the minimum spanning tree T_1, and then the minimum spanning tree T_2 using only the remaining edges. (I.e., the minimum spanning tree in $K_n \setminus T_1$, meaning the graph with edge set $E(K_n) \setminus E(T_1)$.) We then continue and define T_3 as the minimum spanning tree in $K_n \setminus (T_1 \cup T_2)$, and so on. We show that the costs $c(T_2)$, $c(T_3)$, ... also converge in probability to some constants.

Theorem 1. *For each $k \geq 1$, there exists a constant γ_k such that, as $n \to \infty$, $c(T_k) \xrightarrow{\text{p}} \gamma_k$ (for both uniform and exponential cost distributions).*

The result extends easily to other distributions of the edge costs, by standard arguments, but we consider in here only the uniform and exponential cases.

By Frieze [2], $\gamma_1 = \zeta(3)$. The constants γ_k for larger k are given by some expressions in the proof, but not in a form that is easily evaluated since they involve solutions of some non-linear functional equations (which furthermore involve a parameter). We can show the following bounds, which imply that γ_k is roughly $2k$ for large k:

$$k^2 \leq \sum_{i=1}^{k} \gamma_i \leq k^2 + k, \qquad k \geq 1 \tag{1}$$

and

$$2k - 2k^{1/2} < \gamma_k < 2k + 2k^{1/2}, \qquad k \geq 1. \tag{2}$$

A minor technical problem is that T_2 (and $T_3, \dots$) does not always exist; it may happen that T_1 is a star and then $K_n \setminus T_1$ is disconnected. This happens only with a small probability, and w.h.p. (with high probability, i.e., with probability $1-o(1)$ as $n \to \infty$), T_k is defined for every fixed k. However, we avoid this problem completely by modifying the model: we assume that we have a multigraph with an infinite number of copies of each edge in K_n, and that these have the costs given by the points in a Poisson process with intensity 1 on $[0, \infty)$. (The Poisson processes for different edges are, of course, independent.) Note that when finding T_1, we only care about the cheapest copy of each edge, and its cost has an Exp(1) distribution, so the problem for T_1 is the same as the original one. However, we now never run out of edges and we can define T_k for all integers $k = 1, 2, 3, \dots$. Asymptotically, the three models are equivalent, and Theorem 1 holds for any of the models.

The multigraph model, moreover, is useful in our proofs because of the added independence.

Frieze [2] also proved that the expectation $\mathbb{E}\, c(T_1)$ converges to $\zeta(3)$. For the multigraph model just described, this too extends.

Theorem 2. *For the multigraph model, $\mathbb{E}\, c(T_k) \to \gamma_k$ for each $k \geq 1$ as $n \to \infty$.*

Remark 3. However, for the simple graph K_n with, say, exponential costs, there is as said above a small but positive probability that T_k does not exist for $k \geq 2$. Hence, either $\mathbb{E}\, c(T_k)$ is undefined for $k \geq 2$, or (better) we define $c(T_k) = \infty$ when T_k does not exist, and then $\mathbb{E}\, c(T_k) = \infty$ for $k \geq 2$ and every n. Hence Theorem 2 does not hold for simple graphs, and the multigraph model is essential for studying the expectation.

Remark 4. Frieze and Johansson [3] recently considered a related problem, where instead of choosing spanning trees $T_1, T_2, \dots$ greedily one by one, they choose k edge-disjoint spanning trees with minimum total cost. It is easy to see, by small examples, that selecting k spanning trees greedily one by one does not always give a set of k edge-disjoint spanning trees with minimum cost, so the problems are different. We can also show that, at least for $k = 2$, the two problems also asymptotically have different answers, in the sense that the limiting values of the minimum cost (which exist for both problems) are different.

The proofs are, as in many other previous papers on the random minimum spanning tree problem, based on *Kruskal's algorithm* which processes the edges in order of increasing cost and keeps the ones that join two different components in the forest obtained so far. (I.e., it keeps the edges that do not form a cycle together with some previously chosen edges.) The second minimum spanning tree can then be found by another application of the same algorithm to the remaining edges, and so on.

The results are proved by considering a random (multi)graph process, where copies of each edge ij arrive as a Poisson process with intensity $1/n$; an edge arriving at time t has cost t/n. We let $G_1(t)$ be the multigraph formed by the edges that have arrived at time t. We run Kruskal's algorithm and let $F_1(t)$ be the forest formed by the edges selected up to time t for the minimum spanning tree T_1. We let $G_2(t)$ be the multigraph consisting of the edges in $G_1(t) \setminus F_1(t)$, and let $F_2(t)$ be the forest formed by the edges selected up to time t by Kruskal's algorithm applied to $G_2(t)$, and so on. We show, by induction in k, that each $G_k(t)$ is an example of an inhomogeneous random graph of the type studied in [1]; results from [1] thus yield results on the (asymptotic) structure of $G_k(t)$, in particular on the existence and size of a giant component, and these structural results are used to show the theorems above on the cost $c(T_k)$.

References

[1] Béla Bollobás, Svante Janson and Oliver Riordan, The phase transition in inhomogeneous random graphs. *Random Struct. Alg.* **31** (2007), 3–122.

[2] Alan M. Frieze, On the value of a random minimum spanning tree problem, *Discrete Applied Mathematics* **10** (1985), 47–56.

[3] Alan Frieze and Tony Johansson, On edge disjoint spanning trees in a randomly weighted complete graph. Preprint, 2015, `arXiv:1505.03429`.

Reporter: Karen Gunderson

Participants

Prof. Dr. Noga Alon
Department of Mathematics
Sackler Faculty of Exact Sciences
Tel Aviv University
Tel Aviv 69978
ISRAEL

Prof. Dr. Paul Balister
Department of Mathematical Sciences
The University of Memphis
331 Dunn Hall
Memphis TN 38152-3240
UNITED STATES

Prof. Dr. Jozsef Balogh
Department of Mathematics
University of Illinois at
Urbana-Champaign
1409 West Green Street
Urbana IL 61801
UNITED STATES

Prof. Dr. Imre Barany
Alfred Renyi Institute of Mathematics
Hungarian Academy of Sciences
P.O.Box 127
1364 Budapest
HUNGARY

Prof. Dr. Thomas A. Bohman
Department of Mathematical Sciences
Carnegie Mellon University
Pittsburgh, PA 15213-3890
UNITED STATES

Prof. Dr. Béla Bollobás
Department of Pure Mathematics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Amin Coja-Oghlan
Institut für Mathematik
Goethe-Universität Frankfurt
Robert-Mayer-Straße 6-10
60325 Frankfurt am Main
GERMANY

Dr. David Conlon
Mathematical Institute
Oxford University
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Zeev Dvir
Department of Computer Science
Princeton University
35 Olden Street
Princeton, NJ 08544-5233
UNITED STATES

Prof. Dr. Jacob Fox
Department of Mathematics
Stanford University
Stanford, CA 94305-2125
UNITED STATES

Prof. Dr. Ehud Friedgut
Department of Mathematics
The Weizmann Institute of Science
P. O. Box 26
Rehovot 76100
ISRAEL

Prof. Dr. Zoltan Furedi
Alfred Renyi Institute of Mathematics
Hungarian Academy of Sciences
P.O.Box 127
1364 Budapest
HUNGARY

Prof. Dr. David Gamarnik
Massachusetts Institute of Technology
Sloan School of Management
E 53 - BS 7
77 Massachusetts Avenue
Cambridge MA 02139-4307
UNITED STATES

Dr. Karen Gunderson
Department of Mathematics
University of Manitoba
Winnipeg, MB R3T 2N2
CANADA

Prof. Dr. Penny E. Haxell
Department of Combinatorics
and Optimization
University of Waterloo
Waterloo, ONT N2L 3G1
CANADA

Samuel Hetterich
Institut für Mathematik
Goethe-Universität Frankfurt
Postfach 111932
60054 Frankfurt am Main
GERMANY

Dr. Cecilia Holmgren
Matematiska Institutionen
Uppsala Universitet
Box 480
751 06 Uppsala
SWEDEN

Prof. Dr. Svante Janson
Matematiska Institutionen
Uppsala Universitet
Box 480
751 06 Uppsala
SWEDEN

Prof. Dr. Jeff Kahn
Department of Mathematics
Rutgers University
Piscataway NJ 08854-8019
UNITED STATES

Prof. Dr. Mihyun Kang
Institut für Diskrete Mathematik
Technische Universität Graz
Steyrergasse 30
8010 Graz
AUSTRIA

Prof. Dr. Peter Keevash
Mathematical Institute
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Dr. Jeong Han Kim
Department of Mathematics
Yonsei University Graduate School
50 Yonsei-Ro, Seodaemun-Gu
Seoul 120-749
KOREA, REPUBLIC OF

Prof. Dr. Yoshiharu Kohayakawa
Instituto de Matematica e
Estatistica
Universidade de Sao Paulo (IME-USP)
Rua do Matao 1010
Sao Paulo 05508-090 - SP
BRAZIL

Prof. Dr. Michael Krivelevich
School of Mathematical Sciences
Sackler Faculty of Exact Sciences
Tel Aviv University
Tel Aviv 69978
ISRAEL

Dr. Jonathan D. Lee
Merton College
Oxford University
Oxford OX1 4JD
UNITED KINGDOM

Dr. Johannes Lengler
Institut für Theoretische Informatik
ETH Zürich
CAB G 36.2
8092 Zürich
SWITZERLAND

Dr. Shoham Letzter
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Nathan Linial
School of Computer Science &
Engineering
The Hebrew University
Givat Ram
Jerusalem 91904
ISRAEL

Dr. Eoin Patrick Long
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
ISRAEL

Dr. Eyal Lubetzky
Courant Institute of Mathematical
Sciences
New York University
251, Mercer Street
New York, NY 10012-1110
UNITED STATES

Prof. Dr. Tomasz Luczak
Wydzial Matematyki i Informatyki
Uniwersytet im. Adama Mickiewicza
Umultowska 87
61-614 Poznan
POLAND

Dr. Bhargav P. Narayanan
St. John's College
Department of Mathematics
Cambridge CB2 1TP
UNITED KINGDOM

Prof. Dr. Janos Pach
E.P.F.L. SB MATHGEOM DCG
MA C1 577
Station 8
1015 Lausanne
SWITZERLAND

Prof. Dr. Konstantinos Panagiotou
Mathematisches Institut
Universität München
Theresienstrasse 39
80333 München
GERMANY

Prof. Dr. Oliver M. Riordan
Mathematical Institute
Oxford University
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Dr. Vojtech Rödl
Department of Mathematics and
Computer Science
Emory University
400 Dowman Dr.
Atlanta, GA 30322
UNITED STATES

Prof. Dr. Andrzej Rucinski
Faculty of Mathematics & Computer Science
Adama Mickiewicz University
ul. Umultowska 87
61-614 Poznan
POLAND

Dr. Wojciech Samotij
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL

Prof. Dr. Mathias Schacht
Fachbereich Mathematik
Universität Hamburg
Bundesstrasse 55
20146 Hamburg
GERMANY

Prof. Dr. Alexander Scott
Mathematical Institute
University of Oxford
Andrew Wiles Building
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Dr. Asaf Shapira
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
ISRAEL

Prof. Dr. József Solymosi
Department of Mathematics
University of British Columbia
1984 Mathematics Road
Vancouver BC V6T 1Z2
CANADA

Prof. Dr. Angelika Steger
Institut für Theoretische Informatik
ETH Zürich
CAB G 38
Universitätsstrasse 6
8092 Zürich
SWITZERLAND

Prof. Dr. Benjamin Sudakov
Department of Mathematics
ETH Zürich, HG G 65.1
Rämistrasse 101
8092 Zürich
SWITZERLAND

Prof. Dr. Tibor Szabo
Institut für Mathematik & Informatik
Freie Universität Berlin
Arnimallee 6
14195 Berlin
GERMANY

Prof. Dr. Anusch Taraz
Institut für Mathematik (E-10)
Technische Universität Hamburg
Am Schwarzenberg Campus 3
21073 Hamburg
GERMANY

Prof. Dr. Gábor Tardos
Alfred Renyi Institute of Mathematics
Hungarian Academy of Sciences
Realtanoda u. 13-15
1053 Budapest
HUNGARY

Prof. Dr. Andrew Thomason
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Van H. Vu
Department of Mathematics
Yale University
Box 20 82 83
New Haven, CT 06520
UNITED STATES

Dr. Lutz Warnke
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Emo Welzl
Institut für Theoretische Informatik
ETH Zürich, CAB G 39.2
8092 Zürich
SWITZERLAND

Prof. Dr. Nicholas Wormald
School of Mathematical Sciences
Monash University
Clayton, Victoria 3800
AUSTRALIA

Dr. Yufei Zhao
Mathematical Institute
Oxford University
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM