

Combinatorics, Groups, Algorithms, and Complexity

Conference in honor of Laci Babai's 60th birthday

The Ohio State University, March 21-25, 2010

ABSTRACTS

Arthur-Merlin and Black-Box Groups in Quantum Computing (Or, How Laci Did Quantum Stuff Without Knowing It)

Scott Aaronson

Massachusetts Institute of Technology

I'll discuss the black-box group membership problem studied by Babai in the 1980s, and how it ended up playing a central role in quantum computing theory over the last ten years. In particular, I'll discuss why Group Non-Membership is in Babai's complexity class AM (Arthur-Merlin), is not in MA (Merlin-Arthur), is in QMA (Quantum Merlin-Arthur), and is in QCMA (a "hybrid" of MA and QMA) assuming plausible conjectures related to the Classification of Finite Simple Groups. If time permits, I'll also make some general remarks about MA and AM, and why it's easy to construct an oracle relative to which BQP is not in MA but still open to construct an oracle relative to which BQP is not in AM.

On the geometry of Ramanujan graphs

Miklós Abért

Rényi Institute, Budapest

Some of my favorite problems

László Babai

University of Chicago

Metric dimension of distance-regular graphs

Robert Bailey

University of Regina, Canada

The metric dimension of a graph is the least size of a subset of vertices $\{v_1, v_2, \dots, v_k\}$ such that for any vertex w , the list of distances $(d(w, v_1), d(w, v_2), \dots, d(w, v_k))$ uniquely identifies w . Introduced in the 1970s, this parameter has seen a flurry of recent interest from a variety of authors.

We consider the case of distance-regular graphs, and in particular explain how Babai's 1981 paper "On the orders of uniprimitive permutation groups" is very useful in this context.

Polynomial-time Theory of Matrix Groups

Robert Beals

Center for Communications Research - Princeton

Suppose we are given a list T of $n \times n$ matrices over a finite field. How difficult is it to determine the order of the group $\langle T \rangle$ and (constructively) test membership in $\langle T \rangle$?

Hard number theoretic questions such as factoring and discrete log stand in the way of a polynomial-time solution; indeed, constructive membership testing in the case of 1×1 matrices is precisely the discrete log problem. So the reasonable question is whether these problems are solvable in randomized polynomial time using number theory oracles.

The new result we shall present is a positive answer in odd characteristic.

The complexity theoretic study of this problem was initiated by Babai and Szemerédi in 1984 [BSz]. Luks settled the solvable case in 1992 [Lu]. The nuts and bolts of the theory of *black box groups*, introduced in [BSz], were developed by Babai et al. [BCFLS] in the early 90s, and Babai gave a polynomial-time algorithm to produce nearly uniformly distributed random elements in a group, a fundamental algorithmic tool, in 1991 [Ba]. In a programmatic paper, Babai and the speaker outlined an approach to the general case in 1997 to a group theory audience [BB]. Subsequently, several groups of group theorists contributed algorithms in the black-box group context, based on new results of a statistical group theoretic nature about finite simple groups; these works, combined under the [BB] framework, eventually led to the result under discussion. Chief recent contributions include [AB], [BKPS], [BPS], [HLORW], [PW].

One of the ingredients of the new result is the following. A group is called *semisimple* if it has no abelian normal subgroups. For matrix groups over finite fields, we show that the order of the largest semisimple quotient can be determined in randomized polynomial time (no number theory oracles required and there is no restriction on the characteristic). The decision version of this problem then belongs to BPP and is not known to belong either to RP or to coRP.

The characteristic 2 bottleneck arises from the Parker-Wilson paper [PW] that analyses Bray's algorithm [Br] for finding centralizers of involutions. In characteristic 2, we don't even know how to find an involution in a simple matrix group.

Joint work with **László Babai** and **Ákos Seress**. Presented at STOC'09.

[AB] C. ALTSEIMER, A. V. BOROVIK: Probabilistic recognition of orthogonal and symplectic groups. *In: Groups and Computation III, OSU Workshop 1999*. deGruyter, 2001, pp. 1-20.

[Ba] L. BABAI: Local expansion of vertex-transitive graphs and random generation in finite groups. *In: STOC'91*, pp. 164–174.

[BB] L. BABAI, R. BEALS: A polynomial-time theory of black-box groups I. *In: Groups St Andrews 1997 in Bath, I*. Camb. U. Press, 1999, pp. 30–64.

[BBS] L. BABAI, R. BEALS, Á. SERESS: Polynomial-time Theory of Matrix Groups. *In: STOC'09*, pp. 55-64.

[BCFLS] L. BABAI, G. COOPERMAN, L. FINKELSTEIN, E. M. LUKS, Á. SERESS: Fast Monte Carlo algorithms for permutation groups. *J. Computer and System Sci.* **50** (1995), 296–307.

[BKPS] L. BABAI, W. M. KANTOR, P. P. PÁLFY, Á. SERESS: Black-box recognition of finite simple groups of Lie type by statistics of element orders. *J. Group Theory* **5** (2002), 383–401.

[BPS] L. BABAI, P. P. PÁLFY, J. SAXL: On the number of p -regular elements in simple groups. *LMS J. Computation and Mathematics* **12** (2009) 82–119.

[BSz] L. BABAI, E. SZEMERÉDI: On the complexity of matrix group problems I. *In: FOCS'84*, pp. 229–240.

[Br] J. BRAY: An improved method for generating the centralizer of an involution. *Arch. Math.* **74** (2000), 241–245.

[HLORW] P. E. HOLMES, S. A. LINTON, E. A. O'BRIEN, A. J. E. RYBA, R. A. WILSON: Constructive membership in black-box groups. *J. Group Theory* **11** (2008), 747–763.

[Lu] E. M. LUKS: Computing in solvable matrix groups. *In: FOCS'92*, pp. 111–120.

[PW] C. W. PARKER, R. A. WILSON: Recognising simplicity of black-box groups. Manuscript, 2004.

Transforming normal-generating n -tuples of a group into generating n -tuples

Robert Burns
York University, Toronto

The Andrews-Curtis conjecture suggests possible means for getting from a normal-generating n -tuple of a free group, i.e. one whose normal closure is the whole group, to a generating n -tuple. I will report on results of my student Daniel Oancea concerning the number of moves of a certain basic kind (arising from the AC-conjecture) needed to get from a normal-generating n -tuple of a finite or solvable group to a generating n -tuple.

Shuffling with ordered cards

Steven Butler
University of California, Los Angeles

We consider the problem of shuffling a deck with $N = kn$ labelled cards (with an ordering given on the labels). The shuffling is done by splitting the deck into k equally sized stacks of n cards and then taking the top card off each stack, sorting according to the labels and placing them in the newly shuffled stack. It is easy to see that given any stack we will eventually settle into a periodic shuffling (i.e., a deck of cards which returns to itself after several rounds of shuffling). We will consider the problem of determining what possible periods a deck might have. In particular, we will show that if $N = k^t q$ with $t \geq 1$ and $\gcd(k, q) = 1$ then the possible periods of a deck are the divisors of $\text{order}_k(N - q)$.

Joint work with **Ron Graham**.

Bases for permutation groups and combinatorial structures

Peter J. Cameron
Queen Mary, University of London

One of Laci Babai's many achievements was to introduce methods from probabilistic combinatorics into the problem of bounding the base size of a finite permutation group. The bound he obtained is essentially best possible (although use of the Classification of Finite Simple Groups does give more refined estimates).

In the meantime, a number of researchers in graph theory and related parts of combinatorics have introduced equivalents or variants of the base size, resulting in a confusion of terminology and results.

Perhaps it is time to revisit the area and see what has happened to Babai's ideas and how we might make further progress.

This is joint work with **Robert F. Bailey**.

Query Complexity Lower Bounds for Reconstruction of Codes

Sourav Chakraborty
Centrum Wiskunde & Informatica, Amsterdam

We investigate the problem of local reconstruction, as defined by Saks and Seshadhri (2008), in the context of error correcting codes.

The first problem we address is that of message reconstruction, where given an oracle access to an corrupted encoding $w \in \{0, 1\}^n$ of some message $x \in \{0, 1\}^k$ our goal is to probabilistically recover x (or some portion of it). This should be done by a procedure (reconstructor) that given an index i as input, probes w at few locations and outputs the value of x_i . The reconstructor can (and indeed must) be randomized, with all its randomness specified in advance by a single random seed, and the main requirement is that for most random seeds, all values x_1, \dots, x_k are reconstructed correctly (notice that if the for most and all quantifiers were swapped, the definition

would become equivalent to standard Local Decoding). Using the message reconstructor as a filter allows to evaluate certain classes of algorithms on x safely and efficiently. For instance, to run a parallel algorithm, one can initialize several copies of the reconstructor with the same random seed, and then they can autonomously handle decoding requests while producing outputs that are consistent with the original message x . Another example is that of adaptive querying algorithms, that need to know the value of some x_i before deciding which index should be decoded next.

The second problem that we address is codeword reconstruction, which is similarly defined, but instead of reconstructing the message our goal is to reconstruct the codeword itself, given an oracle access to its corrupted version.

Error correcting codes that admit message and codeword reconstruction can be obtained from Locally Decodable Codes (LDC) and Self Correctible Codes (SCC) respectively. The main contribution of this paper is a proof that in terms of query complexity, these are close to be the best possible constructions, even when we disregard the length of the encoding.

Isomorphism of hypergraphs of low rank in moderately exponential time

Paolo Codenotti
University of Chicago

Luks’s seminal 1980 paper, connecting the fine structure of permutation groups to the Graph Isomorphism Problem [4], combined with a combinatorial reduction by Zemlyachenko [6], led, in 1983, to an algorithm that tests graph isomorphism in moderately exponential, $\exp(\tilde{O}(\sqrt{n}))$ time [3], where n is the number of vertices and the tilde refers to a polylogarithmic factor. No significant improvement over this bound has been made during the intervening quarter century. It was pointed out in [3] that an $\exp(\tilde{O}(n^{1/2-c}))$ algorithm for graph isomorphism would yield a moderately exponential, $\exp(\tilde{O}(n^{1-2c}))$ algorithm for isomorphism of 4-hypergraphs.

In 1999, Luks gave a C^n upper bound for testing isomorphism of general hypergraphs [5], and prior to our paper, this was the best known bound even for $k = 3$.

In this paper, we give an algorithm to decide isomorphism of hypergraphs of rank k in time $\exp(\tilde{O}(k^2\sqrt{n}))$. (The rank is the maximum size of edges.) The case of bounded k removes the old obstacle mentioned above from improving the bound for Graph Isomorphism.

Our analysis combines combinatorial and group theoretic methods. For the purposes of recursion, we consider the more general problem of finding isomorphisms within a group G . The overall scheme of our procedure is gradual approximation. In each round we consider an invariant. If the invariant fails to yield isomorphism rejection, we bring the two hypergraphs X and Y “closer” to each other in the sense that X and Y look identical with respect to the invariant. We reduce G in the process by making it respect the invariant. The goal is to reach a point when G becomes a subgroup of the automorphism group $\text{Aut}(X)$. Once this is the case, we conclude that either $X = Y$ or X and Y are not G -isomorphic.

Our algorithm is recursive: if we find some irregularity in the hypergraphs, we split them into “more regular” parts, determine the isomorphism of the parts, and paste the results together using Coset Intersection, which Babai [1] showed can be computed in moderately exponential time.

Following Luks’s divide and conquer for permutation groups, we need to delve into the group structure to some depth. As in [1], the bottleneck arises from transitive groups with large alternating or symmetric group action on a set of blocks of imprimitivity (“giant action”); handling this case constitutes the principal technical contribution of this paper. We use combinatorial arguments to describe the structure of the hypergraphs if the actual automorphism group exhibits the “giant action;” and we find irregularities and recurse if we do not observe this structure.

Joint work with **László Babai**.

[1] L. BABAI: Coset Intersection in Moderately Exponential Time. *Chicago Journal of Theoretical Computer Science*, to appear. <http://cjtc.cs.uchicago.edu>

- [2] L. BABAI, P. CODENOTTI: Isomorphism of Hypergraphs of Low Rank in Moderately Exponential Time. In: *49th FOCS*, 2008, pp. 667–676
- [3] L. BABAI, E. M. LUKS: Canonical labeling of graphs. In: *15th ACM STOC*, 1983, pp. 171–183
- [4] E. M. LUKS: Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comp. Sys. Sci.* 25 (1982) 42–65
- [5] E. M. LUKS: Hypergraph Isomorphism and Structural Equivalence of Boolean Functions. In: *31st ACM STOC*, 1999, pp. 652–658
- [6] V. M. ZEMLYACHENKO, N. M. KORNIENKO, R. I. TYSHKEVICH: Graph isomorphism problem. *J. of Soviet Mathematics*, 29 (1985) 1426–1481. Russian original in *Zapiski LOMI* Vol. 118, 1982.

Sperner-type problems and results

Éva Czabarka
University of South Carolina

One of the central results in extremal set theory is Sperner’s theorem from 1928, and its generalizations, like the well-known BLYM-inequality. A Sperner family is a family of sets such that none of them is a proper subset of another. Sperner’s theorem asserts that the maximum size of a Sperner family on an n -element set is $\binom{n}{\lfloor n/2 \rfloor}$. G.O.H. Katona and D.J. Kleitman discovered independently and almost simultaneously that one can relax the condition of the Sperner theorem while keeping its conclusion. They relaxed the definition of Sperner families to more-part Sperner families, and showed that a maximum size 2-part Sperner family still has size $\binom{n}{\lfloor n/2 \rfloor}$. However, a 3-part Sperner family may be larger.

Since then the theory developed in several directions.

1. finding conditions under which the upper bound $\binom{n}{\lfloor n/2 \rfloor}$ still holds for the size of more-part Sperner families;
2. find the actual maximum size of more-part Sperner families;
3. find analogues of the Sperner and 2-part Sperner theorem for other structures.

In this talk we will see some new results about more-part Sperner families explore some old and new generalizations of the problem and present a new and interesting conjecture.

Joint work with **Harout Aydinian**, **P.L. Erdős**, and **L.A. Székely**.

Deciding finiteness in the class of finitely generated matrix groups

Alla Detinko
National University of Ireland, Galway

We present new methods for computing with matrix groups over infinite domains, based on the theory of finitely generated linear groups. Using those methods we have developed algorithms to solve a number of computational problems. One such problem, deciding finiteness, will be discussed in the talk. We present new, efficient algorithms which test finiteness of finitely generated matrix groups over a broad range of domains, both in zero and in positive characteristic. An implementation of the algorithms is publicly available in Magma. This is joint research with **Dane Flannery** and **Eamonn O’Brien**.

Growth in Some Finite Simple Groups of Lie Type of Rank One

Oren Dinai
University of Geneva

For any subset A of generators of $SL_2(p)$, where p is prime, the set $A \cdot A \cdot A$ is much larger than A , as was proven by Helfgott [2]. In this talk, we will review some of the algebraic tools used for a generalization [1] of this result to $SL_2(q)$, where q is a prime power. We will also discuss few ideas towards a further generalization of the result, with a focus on the case of Suzuki groups $Sz(q)$.

[1] Dinai, O.: *Expansion properties of finite simple groups*, Ph.D. thesis, Hebrew University (2009).

[2] Helfgott, H.: *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$* , Ann. of Math. 167 (2008), 601-623.

Finite group representations: from approximate to exact

John Dixon
Carleton University, Ottawa

In 2003 a report by Babai, Friedl and Lukács [2] (based in part on an earlier paper of Babai and Friedl [1]) considers the problem of working with “near-representations” of a finite group G (approximations to matrix representations over the complex field). They show how such representations can be handled computationally; for example, split stably into irreducible (near)-representations.

For many applications what is needed is an exact representation defined over a cyclotomic field $F := \mathbb{Q}(\omega)$ where ω is root of 1. At the same time it is often reasonable to assume that the character of the underlying representation is known exactly and that its value can be recognized from the matrix of the approximate representation. I shall show that in this case an exact representation can be constructed from an approximation to an absolutely irreducible representation if and only if we can construct an element in the group ring FG with a rank-1 image. I shall then explain how a rank-1 element can be constructed for suitable F using a Las Vegas algorithm.

[1] L. Babai and K. Friedl. Approximate representation theory of finite groups, in *32nd Annual Symp. FOCS (San Juan, PR, 1991)*, 733–742. IEEE Comput. Soc. Press, Los Alamitos, 1991.

[2] L. Babai, K. Friedl and A. Lukács. Near-representations of finite groups, 2003.

Babai, the Wizard, and the Power of Local Interaction

Lance Fortnow
Northwestern University

In the 80’s to classify certain group problems, László Babai developed Arthur-Merlin games, a model that would drive both computational complexity and algorithmic theory to this day. This talk will recount Babai’s contributions to the early days of interactive proof systems including the power of PCPs, holographic proofs and pseudo-random generators based on worst-case hardness.

Partition-critical hypergraphs

Zoltán Füredi
University of Illinois at Urbana-Champaign

A k -uniform hypergraph (X, \mathcal{E}) is 3-color critical if it is not 2-colorable, but for all $E \in \mathcal{E}$ the hypergraph $(X, \mathcal{E} \setminus \{E\})$ is 2-colorable. Lovász proved in 1976, that $|\mathcal{E}| \leq \binom{n}{k-1}$ for a 3-color critical k -uniform hypergraph with $|X| = n$. Here we prove an ordered version that is a sharpening of Lovász’ result. Let $\mathcal{E} \subseteq \binom{[n]}{k}$ be a k -uniform set system on an underlying set X of

n elements. Let us fix an ordering E_1, E_2, \dots, E_t of \mathcal{E} and a prescribed partition $A_i \cup B_i = E_i$ ($A_i \cap B_i = \emptyset$) for each member of \mathcal{E} . Assume that for all $i = 1, 2, \dots, t$ there exists a partition $C_i \cup D_i = X$ ($C_i \cap D_i = \emptyset$), such that $E_i \cap C_i = A_i$ and $E_i \cap D_i = B_i$, but $E_j \cap C_i \neq A_j$ and $E_j \cap D_i \neq B_j$ for all $j < i$. (That is, the i th partition cuts the i th set as it is prescribed, but does not cut any earlier set properly.) Then $t \leq \binom{n}{k-1} + \binom{n}{k-2} + \dots + \binom{n}{0} = \binom{n}{k-1} + O(n^{k-2})$. Furthermore, if $A_i = E_i$ and $B_i = \emptyset$ for all i , then $t \leq \binom{n}{k-1}$.

The proofs are algebraic.

This is a joint work with **Attila Sali**.

Combinatorial Methods for the Graph Isomorphism Problem

Martin Fürer

Pennsylvania State University

The strongest successes towards polynomial time isomorphism tests for significant classes of graphs come from group theory. Given the combinatorial flavor of the graph isomorphism problem, we are concerned here with the question of how much can be achieved in this area with combinatorial methods. We give a review of positive and negative results.

The k -dimensional Weisfeiler-Lehman algorithm (k -dim W-L) has established itself as an ultimate combinatorial approach to the graph isomorphism problem. Many properties based on the neighborhood of vertices have provided useful invariants distinguishing typical non-isomorphic graphs. Usually k -dim W-L can be shown to easily provide at least the same benefits.

Yet on the negative side, k -dim W-L is strictly weaker than the group theoretic approach. Nevertheless, from a practical point of view, k -dim W-L can speed up the group theoretic method significantly for typical graphs.

On the positive side, the 2-dimensional Weisfeiler-Lehman algorithm is able to replace the somewhat unnatural numerical approximations that come with a linear algebra approach to the graph isomorphism problem for graphs of bounded eigenvalue multiplicity. 2-dim W-L also provides invariants which are at least as strong as many spectral invariants based not just on eigenvalues, but also on angles among projections of standard basis vectors into eigenspaces.

On the limitations of 3-query linear locally decodable codes

Anna Gál

University of Texas at Austin

Locally decodable codes were introduced by Katz and Trevisan in 2000 [2]. These are error correcting codes with the extra property that, in order to retrieve the correct value of just one position of the input with high probability, it is sufficient to read a constant number of positions of the corresponding, possibly corrupted codeword. A breakthrough result by Yekhanin [4] showed that 3-query linear locally decodable codes may have subexponential length.

The construction of Yekhanin, and the 3-query constructions that followed e.g. [1], can achieve correctness only up to a certain limit which is $1 - 3\delta$ for nonbinary codes. The largest correctness for a subexponential size constant query binary code is achieved in a construction by Woodruff, and it is below $1 - 3\delta$, where an adversary is allowed to corrupt up to δ fraction of the codeword.

We show that achieving somewhat larger correctness (as a function of δ) requires exponential codeword length for 3-query linear codes. Previously, there were no larger than quadratic lower bounds known for locally decodable codes with more than 2 queries. Our lower bounds hold for linear codes over arbitrary finite fields.

Joint work with **Andrew Mills** (University of Texas at Austin).

[1] K. Efremenko: “3-query locally decodable codes of subexponential length”, In Proceedings of STOC 2009, pp. 39 - 44.

[2] J. Katz and L. Trevisan: “On the Efficiency of Local Decoding Procedures for Error-Correcting Codes”, In Proceedings of STOC 2000, pp. 80 - 86.

[3] D. Woodruff: “Corruption and Recovery-Efficient Locally Decodable Codes” In Proceedings of RANDOM 2008, pp. 584-595.

[4] S. Yekhanin: “Towards 3-query locally decodable codes of subexponential length”, In Proceedings of STOC 2007, pp. 266 - 274.

The product replacement algorithm graph of finite simple groups

Shelly Garion
Max Planck Institute, Bonn

The Product Replacement Algorithm (PRA) is a practical algorithm for generating random elements of a finite group G . Since its introduction in 1995, it quickly became popular and was included in the two commonly used computer algebra packages GAP and MAGMA.

One can describe this algorithm as a random walk on a certain graph, called the PRA graph, whose vertices are the generating k -tuples of G .

In the talk, I will discuss the connectivity properties of PRA graphs and present some new results concerning PRA graphs of finite simple groups.

Quantum Physics and Graph Spectra

Chris Godsil
University of Waterloo

As a graduate student, I was fascinated to learn that the eigenvalues of a graph could actually provide useful information about its structure. I started work on this topic, and never outgrew my interest in it—it seemed a harmless enough amusement. But recently I have been surprised to find that a number of questions arising in quantum computing could be profitably attacked using results and techniques from the theory of graph spectra. In my talk I will present some of these problems (in graph theoretic terms), and discuss what progress has been made.

Towards an approximation algorithm for the directed all-terminal network reliability problem

Igor Gorodezky
Cornell University

In the directed all-terminal network reliability problem, sometimes called the reachability problem, we are given a directed graph with root vertex r in which every edge has some probability of failure. The problem asks: if we allow edges to fail independently, what is the probability that there remains a directed path from every non-root vertex to r ? This canonical network reliability problem has long been known to be $\#P$ -complete, hence is most likely intractable. We give a randomized approximation algorithm (FPRAS) for reachability in the case of bi-directed graphs (i.e. graphs such that if there is an edge $u \rightarrow v$ then there must be an edge $v \rightarrow u$) in which all failure probabilities are $1/2$. We conjecture that our algorithm gives a FPRAS in the general case of arbitrary polynomially-bounded failure probabilities on a bi-directed graph.

Joint work with **Igor Pak**.

Paley-like uniform hypergraphs

Shonda Gosselin
University of Winnipeg

A k -uniform hypergraph X with vertex set V and edge set E is q -complementary if there is a permutation θ on V such that the sets $E, E^\theta, E^{\theta^2}, \dots, E^{\theta^{q-1}}$ partition the set of k -subsets of V . The 2-complementary 2-uniform hypergraphs are the self-complementary graphs, which

have been well studied due to their connection to the graph isomorphism problem. The vertex-transitive q -complementary k -uniform hypergraphs form examples of large sets of isomorphic designs which are point-transitive. These are important structures in combinatorial design theory which have useful applications in cryptography.

The well known Paley graphs are both vertex-transitive and self-complementary. These graphs have a high level of symmetry and many interesting properties. In this talk, we introduce Paley's construction and present some examples, and then we use Paley's algebraic technique to generalize this construction and find some 'Paley-like' vertex-transitive q -complementary k -uniform hypergraphs, for $k \geq 2$ and q prime. This will establish necessary and sufficient conditions on the order $|V|$ of these structures in the case where q is prime, for certain values of the rank k . In addition, we use group theoretic results due to Burnside and Zassenhaus to show that *every* vertex-transitive q -complementary k -uniform hypergraph of prime order can be obtained from some Paley-like uniform hypergraph by a switching operation.

Descents and Drops of a Permutation

Ronald L. Graham
University of California, San Diego

In this talk I will describe some recent results on the joint distribution of the descent and maximum drop statistics of a permutation. Several new identities for Eulerian numbers also follow from this analysis.

On the Shortest Identity in Finite Simple Groups of Lie Type

Uzy Hadad
Weizmann Institute and The Open University of Israel

We give bounds on the length of the shortest identity in finite simple groups of Lie type. We prove that the length of the shortest identity in a finite simple group of Lie type of rank r defined over \mathbb{F}_q , is bounded (from above and below) by explicit polynomials in q and r .

On long alternating non-crossing paths in 2-equicolored convex sets

Péter Hajnal
University of Szeged, Hungary

Let \mathcal{P} be an $2n$ -element planar point set in convex position. We arbitrarily divide \mathcal{P} into two halves and color the points of the first half red and the other half blue. This colored point set determines a longest path that is alternating between the two colors and non crossing (edges are straight lines). Erdős introduced the function $\ell(n)$, that is the largest length we can guarantee whatever the division/coloring was. He established the following basic bounds: $n \leq \ell(n) \leq 3/2n + 2$. Jan Kynčl, János Pach and Géza Tóth improved these bounds and proved that $n + \alpha\sqrt{n/\log n} \leq \ell(n) \leq 4/3n + \beta\sqrt{n}$. Their upper bound is exhibited by a sporadic coloring.

We improve the previous lower bound to $n + \alpha\sqrt{n}$. We also exhibit classes of colorings such that the Kynčl–Pach–Tóth upper bound is sharp (supporting the conjecture that the upper bound is the right order of magnitude for $\ell(n)$). We introduce other parameters of 2-equicolored convex point sets and consider their relation to $\ell(n)$.

Joint work with **Viola Mészáros**.

Liftings of Tree-Structured Markov Chains

Tom Hayes
University of New Mexico

A “lifting” of a Markov chain is a larger chain obtained by replacing each state of the original chain by a set of states, with transition probabilities defined in such a way that the lifted chain projects down exactly to the original one. It is well known that lifting can potentially speed up the mixing time substantially. However, essentially all examples of feasibly implementable liftings known to date require the original chain to possess a high degree of symmetry (i.e., random walk on a Cayley graph).

Addressing an open question of Chen, Lovász and Pak, we present apparently the first example of a successful lifting for a complex Markov chain that has been used in sampling algorithms. This chain, first introduced by Sinclair and Jerrum, samples a leaf uniformly at random in a large tree, given approximate counting information about the number of leaves in any subtree. It has been applied, among other things, to establish a general reduction from sampling to approximate counting for self-reducible problems in $\#\text{P}$, and is also a natural abstraction of the concept of importance sampling in Statistics.

Our lifting construction, based on flows, is systematic, and hopefully may be applicable to other Markov chains used in sampling algorithms.

This is joint work with **Alistair Sinclair**.

Growth in simple groups of Lie type

Harald Helfgott
University of Bristol, U.K.

Let G be a simple group of Lie type; let K be a finite field. Let A be a subset of $G(K)$ that generates $G(K)$. Assume that $|A| \leq |G(K)|^{1-\epsilon}$, $\epsilon > 0$, where $|S|$ denotes the number of elements of a set S .

In 2005, I proved that, for $G = SL_2$, $K = \mathbb{F}_p$, we always have $|AAA| \ll |A|^{1+\delta}$, where $\delta > 0$ and the implied constant depends only on ϵ . In other words, any set of generators that has room to grow does grow rapidly.

Some time later, I generalised this result to $G = SL_3$ and (jointly with N. Gill) to $G = SL_n$ (in the case of small sets A). In a very recent development, Breuillard, Green and Tao, on the one hand, and Pyber and E. Szabó, on the other, have announced general statements of the theorem valid for all finite simple groups of Lie type. We will discuss the program leading to the proofs of all of these results.

Bernoulli type truncation games and connected permutations

Gábor Hetyei
University of North Carolina at Charlotte

The number of connected permutations of order n is closely related to the probability that a random pair of permutations of order n from the alternating group A_n generates the entire subgroup A_n . Successively improving asymptotic estimates of this probability were given by Dixon (1969), Bovey and Williamson (1978), Babai (1989), and Dixon (2005). In this talk we present a class of truncation games on words, originally invented by the presenting author (2009) to provide a combinatorial model for the Bernoulli numbers of the second kind, introduced by Jordan (1979). We show that for a specific example of such a game the kernel positions are identifiable with the connected permutations, and finding the winning strategy is bijectively equivalent to the first phase of King’s (2006) algorithm, generating a Gray code of all connected permutations of fixed order.

[1] L. Babai, The probability of generating the symmetric group, *J. Combin. Theory Ser. A* **52** (1989), 148–153.

- [2] J. Bovey and A. Williamson, The probability of generating the symmetric group, *Bull. London Math. Soc.* **10** (1978), 91–96.
- [3] J. D. Dixon, The probability of generating the symmetric group. *Math. Z.* **110** (1969), 199–205.
- [4] J. D. Dixon, Asymptotics of generating the symmetric and alternating groups, *Electron. J. Combin.* **12** (2005), Research Paper 56, 5 pp.
- [5] G. Hetyei, Enumeration by Kernel Positions, *Adv. in Appl. Math.* **42** (2009), 445–470. doi:10.1016/j.aam.2008.11.001.
- [6] G. Hetyei, Enumeration by kernel positions for strongly Bernoulli type truncation games on words, preprint 2009, arXiv:0912.0573 [math.CO].
- [7] C. Jordan, “Calculus of finite differences”, Chelsea Publishing Company, New York, NY, 1979.
- [8] A. King, Generating indecomposable permutations, *Discrete Math.* **306** (2006), 508–518.

Products of Finite and Infinite Graphs

Wilfried Imrich

Montanuniversität Leoben, Austria

Products of finite and infinite graphs pose challenging algebraic, combinatorial and algorithmic problems. There are difficult open problems pertaining to the factorization of infinite graphs, the prime factorization of bipartite finite graphs with respect to the direct product, and the design of polynomial algorithms for the prime factorization of directed graphs with respect to the direct product. Recently new results have been obtained in all these areas.

This talk will focus on new results on the prime factorization of finite and infinite graphs with respect to the direct product and the relationship of these results with new, fast algorithms for the prime factorization of finite graphs with respect to the direct and the strong product.

It will also include a short survey of cancellation properties and results about the distinguishing number of finite and infinite graphs with respect to various products. The latter is made possible by the characterization of the automorphism groups of products by the groups of the factors.

Finally, a few words may be reserved for approximate graph products and applications in the modelling of large networks.

Modules and maximum rank matrix completion

Gábor Ivanyos

MTA SzTAKI, Budapest

In [2] Laci Babai and Lajos Rónyai suggested a deterministic polynomial time method for finding an element in a module over a simple algebra which generates a submodule of maximum possible dimension. In [3] the result was extended to semisimple modules and used to deciding and computing isomorphisms between modules through constructively testing cyclicity of not necessarily semisimple modules in deterministic polynomial time.

As the method of [3] was based on working with the semisimple parts of algebras and modules, it was limited to ground fields over which radicals of algebras can be efficiently computed. Unfortunately, there are base fields over which even deciding whether the radical is trivial is undecidable. In [1] Peter Brooksbank and Gene Luks presented a deterministic method for module isomorphism which has polynomial complexity over an arbitrary ground field.

Based on joint work with Marek Karpinski and Nitin Saxena [4], we show how to solve the stronger problem of constructively testing cyclicity of modules in deterministic polynomial time without any restriction on the base field. The method implicitly uses the original idea of Laci and Lajos [2] which is an extraordinary special instance of finding a maximum rank in linear spaces matrices. We also present hardness results which explain why this idea cannot be directly extended to non-semisimple modules.

- [1] P. A. Brooksbank, E. M. Luks, Testing Isomorphism of Modules, *J. Algebra* 320 (2008), 4020-4029, <http://dx.doi.org/10.1016/j.jalgebra.2008.07.014>.
- [2] L. Babai, L. Rónyai: Computing irreducible representations of finite groups, *Proc. 30th IEEE FOCS (1989)*, 93-98, also *Mathematics of Computation* 55 (1990), 705-722, <http://dx.doi.org/10.2307/2008443>.
- [3] A. Chistov, G. Ivanyos, M. Karpinski, Polynomial time algorithms for modules over finite dimensional algebras, *Proc. ISSAC'97*, 68-74, <http://doi.acm.org/10.1145/258726.258751>.
- [4] G. Ivanyos, M. Karpinski, N. Saxena, Deterministic polynomial time algorithms for matrix completion problems, *Preprint arXiv:0804.1974[cs.CC]*, <http://arxiv.org/abs/0907.0774>.

Aspects of Nonabelian Group Based Cryptography

Delaram Kahrobaei
City University of New York

Most common public key cryptosystems and public key exchange protocols presently in use, such as the RSA algorithm, Diffie-Hellman, and elliptic curve methods are number theory based and hence depend on the structure of abelian groups. The strength of computing machinery has made these techniques theoretically susceptible to attack and hence recently there has been an active line of research to develop cryptosystems and key exchange protocols using noncommutative cryptographic platforms. This line of investigation has been given the broad title of noncommutative algebraic cryptography. This was initiated by two public key protocols that used the braid groups, one by Ko, Lee et.al. and one by Anshel, Anshel and Goldfeld. The study of these protocols and the group theory surrounding them has had a large effect on research in infinite group theory. In this talk I survey some of these noncommutative group based methods and discuss several ideas in abstract infinite group theory that have arisen from them. I will mention about some new results and then present a set of open problems.

Short Presentations of Finite Simple Groups

William M. Kantor
University of Oregon

I'll discuss theorems such as the following, and why they are unexpected. All finite simple groups of Lie type of rank n over a field of size q , with the possible exception of the Ree groups ${}^2G_2(q)$, have presentations with at most 49 relations and bit-length $O(\log n + \log q)$. Moreover, A_n and S_n have presentations with 3 generators, 7 relations and bit-length $O(\log n)$.

Spectral gap of Cayley graphs of Coxeter groups

Martin Kassabov
Cornell University

In this talk I will use geometry of Hilbert spaces to show that the spectral gap of the Laplacian of Cayley graph of any finite Coxeter group can be computed by just looking at the defining representation. In the case of type A_n this result was proved by Bacher and de la Harpe using the representation theory of the symmetric groups.

Sharp kernel clustering algorithms and their associated Grothendieck inequalities

Subhash Khot
New York University

I will present an approximation algorithm for the kernel clustering problem which is defined as follows: fix a small $k \times k$ positive semidefinite matrix B . Now, assume that you are given a large

$n \times n$ positive semidefinite matrix A which is centered (i.e., normalized so that $\sum_{i,j=1}^n a_{ij} = 0$) and you wish to cluster it so that it will be most correlated with B . This means that you want to find a partition S_1, \dots, S_k of $\{1, \dots, n\}$ so that if you form the associated clustered version of A , i.e., set $c_{ij} = \sum_{(p,q) \in S_i \times S_j} a_{pq}$, then $\sum_{i,j=1}^k c_{ij} b_{ij}$ is as large as possible among all possible k -partitions of $\{1, \dots, n\}$. The problem arises in machine learning literature and generalizes problems such as Maximum Cut and Positive Semi-definite Grothendieck problem.

Our approximation ratio is a function of the test matrix B , and we show a matching hardness of approximation result assuming the Unique Games Conjecture. The analysis of our algorithm involves proving a new natural extension of the PSD Grothendieck inequality which is of independent interest. The Unique Games hardness is based on a new dictatorship test in which the underlying product distribution is non-uniform, and is induced by B via the geometric structure of the vectors in its Gram decomposition.

Joint work with **Assaf Naor**. Appeared in SODA'10.

Complexity of Scarf's Lemma and Fractional Stability Problems

Shiva Kintali

Georgia Institute of Technology

The notion of stability implies the absence of oscillations over time and encompasses the concepts of fixed points and equilibria. The study of stable solutions to combinatorial problems has a distinguished tradition dating back to, at least, the Gale-Shapley algorithm. The study of computational complexity of finding equilibrium points is of profound real-world significance. It is often the case, as with Nash's celebrated theorem, that fractional stable points are guaranteed to exist even when integral points don't.

Scarf's lemma is one of the fundamental results in combinatorics, originally introduced to study the core of an N -person game. Over the last four decades, the usefulness of Scarf's lemma has been demonstrated in several important combinatorial problems seeking fractional stable solutions.

In this talk I will define the complexity class PPAD, and mention several natural "fractional stability" problems that are PPAD-complete. I will introduce a simple game (called preference game) and prove that it is PPAD-complete.

I will discuss the computational version of Scarf's lemma and prove its PPAD-completeness along with its several practical applications :

- 1) Core of Balanced Games (Economics and Game theory),
- 2) Hypergraph Matching (Social Choice and Preference Systems),
- 3) Strong Fractional Kernel (Graph Theory) and
- 4) Fractional Stable Paths Problem (Internet routing).

This talk is based on joint work with **Laura Poplawski, Rajmohan Rajaraman, Ravi Sundaram** and **Shang-Hua Teng**.

Decision tree complexity, solvable groups, and the distribution of prime numbers.

Raghav Kulkarni

University of Chicago

A boolean function f on N variables is called "evasive" if its decision tree complexity is N , i.e., one must query *all* the variables (in worst case) in order to decide if $f(X) = 1$. A graph property of n -vertex graphs is a boolean function on $N = \binom{n}{2}$ variables which is invariant under relabeling of vertices. A graph property is called monotone if it is closed under deletion of edges, e.g., planarity, 3-colorability etc. The following conjecture due Aanderaa-Rosenberg-Karp is a longstanding (35+ years) open question: "every non-trivial monotone graph property must be evasive." An important special case is the class of properties given by a "forbidden subgraph," i.e., all n vertex graphs which do not contain a fixed subgraph H .

We confirm the evasiveness of several monotone graph properties under widely accepted number theoretic hypotheses (e.g. Generalized Riemann Hypothesis, Chowla's Conjecture on smallest Dirichlet primes etc). In particular, we show: (a) forbidden subgraph is evasive for all large enough n (b) any monotone property of sparse graphs ($< n^{3/2-\epsilon}$ edges) is evasive.

Even our weaker unconditional results rely on some deep and interesting properties of the integers such as Vinogradov's theorem on Goldbach conjecture asserting that every odd integer can be expressed as the sum of three primes. One of our main technical contribution here is in connecting the topological framework of Kahn, Saks, and Sturtevant 84, (further developed by Chakrabarti, Khot, and Shi 02), to analytic number theory via better analysis (derivable from Weil's character sum estimates) of the orbital structure of permutation groups and their connection to the distribution of prime numbers.

Joint work with **Laci Babai**, **Anandam Banerjee** and **Vipul Naik**.

Proof of the Bollobás-Catlin-Eldridge conjecture

Gábor Kun
DIMACS and IAS, Princeton

We say that the graphs G and H with n vertices *pack* if G and H can be embedded to the same vertex set with no overlapping edges. Bollobás, Eldridge and independently Catlin conjectured that if $(M(G)+1)(M(H)+1) < n+2$ holds for the maximal degrees then G and H pack. Aigner and Brandt and independently Alon and Fischer proved this in the case $M(G), M(H) < 3$, Csaba, Shokoufandeh and Szemerédi if $M(G), M(H) < 4$. Bollobás, Kostochka and Nakprasit settled the case when one of the graphs is degenerate. Kaul, Kostochka and Yu showed that if $M(G)M(H) < 3/5n$ and the maximal degrees are large enough then G and H pack. We prove the conjecture for graphs with at least 10^8 vertices.

Quantum interpolation of polynomials

Sandy Kutin
Center for Communications Research - Princeton

We consider quantum interpolation of polynomials. We imagine a quantum computer with black-box access to input/output pairs $(x_i, f(x_i))$, where f is a degree- d polynomial, and we wish to compute $f(0)$.

Classically, assuming we are not allowed to obtain $f(0)$ directly, the best strategy is to query $d+1$ values and interpolate. We show that a quantum computer requires at least $(d+1)/2$ queries to obtain even a single bit of information about $f(0)$. Our best general algorithm requires $d+1$ queries, but in some cases we show an exactly matching upper bound.

If there is an input i for which the black box returns the pair $(0, f(0))$, an alternate approach is to use Grover's search for such an i . In this case we again show an asymptotically tight lower bound: the number of queries required is the minimum of the Grover lower bound and $(d+1)/2$.

The proofs use the polynomial method of Beals, et al. [1], together with a little bit of probability theory. See our arXiv preprint [2] for more details.

Joint work with **Daniel Kane**.

[1] Robert Beals, Howard Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. quant-ph/9802049. IEEE Symposium on Foundations of Computer Science '98.

[2] Daniel Kane and Samuel Kutin. Quantum interpolation of polynomials. arXiv:0909.5683, September 2009. <http://arxiv.org/abs/0909.5683v1>.

Parameter testing with Borel Oracles

Gábor Lippner

Harvard University

The limit of a convergent sequence of bounded degree graphs can be considered as a Borel graph with an invariant measure. I will explain how to “pull back” measurable objects in the limit to construct certain combinatorial structures on the graph sequence. Applications include parameter testing and regularity type results.

Joint work with **Gábor Elek**.

Matrix Rigidity and Complexity of Linear Transformations

Satyanarayana V. Lokam
Microsoft Research India

A matrix A is said to be (k, r) -rigid if at least k entries of A must be altered to reduce its rank to a value $\leq r$. A counting/dimension argument shows that *almost all* matrices over an infinite field are $((n - r)^2, r)$ -rigid. The challenge is to construct *explicit* matrices that are $(n^{1+\delta}, \epsilon n)$ -rigid. Initial motivation for this goal comes from a result due to Valiant (1977), who introduced the notion of rigidity, that the linear transformation given by an $(n^{1+\delta}, \epsilon n)$ -rigid matrix requires superlinear size arithmetic circuits of logarithmic depth.

We will review some recent constructions of $(\Omega(n^2), \epsilon n)$ -rigid matrices with algebraic numbers as entries. While these matrices have a succinct mathematical description, e.g., entries are square roots of distinct primes, they are not explicit in the sense of being efficiently constructible by a Boolean model of computation. The techniques used to prove rigidity lower bounds on these matrices also help us prove nearly-quadratic lower bounds on the arithmetic complexity of the corresponding linear transformations. These are stronger bounds than implied by Valiant’s criterion. We will mention several remaining open questions.

- [1] Chapter 2 of *Complexity Lower Bounds using Linear Algebra*: Satyanarayana V. Lokam, Volume 4 (2009), Issue 1-2, in Foundations and Trends in Theoretical Computer Science.
<http://www.nowpublishers.com/product.aspx?product=TCS&doi=0400000011>.
- [2] *Using Elimination Theory to construct Rigid Matrices*: Abhinav Kumar, Satyanarayana V. Lokam, Vijay M. Patankar, and Jayalal Sarma. FSTTCS 2009
<http://drops.dagstuhl.de/portals/FSTTCS09/> and ECCC TR09-106
<http://eccc.hpi-web.de/report/2009/106/>.

Small presentations of finite simple groups

Alex Lubotzky
Hebrew University

We show that essentially all non-abelian finite simple groups have presentations which are at the same time small (i.e., small number of relations) and short (the relations are of short length). In the talk we will concentrate on the “small” part (leaving the “short” to Bill Kantor’s talks). Connections with discrete subgroups of Lie groups will be explained as well as some open problems.

The talk is based on:

- [1] R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: a quantitative approach*, Journal of the American Math. Soc. **21** (2008), 711–774.
- [2] R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: cohomological and profinite approach*, Groups, Geometry and Dynamics **1** (2007), 469–523.
- [3] R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky, *Presentations of finite simple groups: a computational approach*, J. of the European Math. Soc., to appear.

Permutation groups in parallel: canonical forms

Eugene M. Luks
University of Oregon

A significant portion of the polynomial-time library for permutation groups has been parallelized, bringing the problems into the complexity class NC. This effort has often involved replacing sequential methods with alternate approaches that make essential use of the group structure even for elementary problems such as testing membership. However, for some problems related to graph isomorphism, an isomorphism/canonization gap emerged. This is illustrated in the class BCC of vertex-colored graphs with bounded color-classes (as introduced in a classic paper of Babai). Isomorphism-testing for BCC was shown to be polynomial time (Babai; Furst-Hopcroft-Luks) and the method extended to canonical labeling. As the parallel machinery developed, isomorphism-testing for BCC was shown to be in NC. Yet, it seemed that the known canonical forms were inherently sequential, i.e., could not be computed in NC unless $P=NC$. We now remove the gap by offering an alternate canonical form for BCC that is computable in NC. The technique extends to several other problems where the sequential approaches relied on finding lexicographic leaders.

Rough structure theorem for symmetric graphs with small separations

Bojan Mohar
Simon Fraser University, British Columbia, Canada

Let $G = (V, E)$ be a vertex transitive (finite or infinite, directed or undirected) graph, let A be a finite set of vertices with $|A| \leq |V|/2$, and let k be the number of vertices that are not in A but have a neighbor in A . We show that whenever the diameter of G is at least $31(k+1)^2$, either $|A| \leq 2k^3$, or G has a (bounded) ring-like structure and A is efficiently contained in an interval. This result can be viewed as a rough structure theorem for small separations in symmetric graphs. Applications to the study of product sets, to expansion in groups, and to symmetries in minor-closed families will be presented.

Joint work with **Matt DeVos**.

Coloring simple hypergraphs

Dhruv Mubayi
University of Illinois, Chicago

Ajtai-Komlós-Pintz-Spencer-Szemerédi [1] proved the following fundamental result about the independence number of hypergraphs with no short cycles.

Theorem 1 ([1]). *Let $H = (V, E)$ be a k -uniform hypergraph of girth at least 5 with maximum degree D . Then it has an independent set of size at least $cn(\frac{\log D}{D})^{\frac{1}{k-1}}$, where c depends only on k .*

Spencer conjectured that Theorem 1 holds even for simple hypergraphs (those where every two edges share at most one vertex), and this was later proved by Duke-Lefmann-Rödl [2]. Theorem 1 has proved to be a seminal result in combinatorics, with many applications. Indeed, the result was first proved for $k = 3$ by Komlós-Pintz-Szemerédi [5] to disprove the famous Heilbronn conjecture, that among every set of n points in the unit square, there are three points that form a triangle whose area is at most $O(1/n^2)$. For applications of Theorem 1 to coding theory or combinatorics, see [6] or [4], respectively.

We prove a result that is stronger than Theorem 1 (and also the accompanying result of [2]). Since the proof of our result does not use Theorem 1, it gives an alternative proof of all the applications of Theorem 1 as well. Our result states that not only can one find an independent set of the size guaranteed by Theorem 1, but in fact that the entire vertex set can be partitioned into independent sets with this average size. Recall that the chromatic number $\chi(H)$ of H is the minimum number of colors needed to partition the vertex set so that no edge is monochromatic.

Theorem 2 ([3]). Fix $k \geq 3$. Let $H = (V, E)$ be a simple k -uniform hypergraph with maximum degree D . Then $\chi(H) < c(\frac{D}{\log D})^{\frac{1}{k-1}}$, where c depends only on k .

Theorem 2 is sharp apart from the constant c . We conjecture the following:

Conjecture 3. Let F be a k -graph. There is a constant c_F depending only on F such that every F -free k -graph with maximum degree Δ has chromatic number at most $c_F(\frac{\Delta}{\log \Delta})^{\frac{1}{k-1}}$.

This is joint work with **Alan Frieze**.

[1] M. Ajtai, J. Komlós, J. Pintz, J. Spencer and E. Szemerédi, Extremal uncrowded hypergraphs, *Journal of Combinatorial Theory A* 32 (1982), no. 3, 321–335.

[2] R. Duke, H. Lefmann, V. Rödl, On uncrowded hypergraphs, *Random Structures and Algorithms*, **6**, 209–212, 1995.

[3] A. Frieze, D. Mubayi, Coloring Simple Hypergraphs, submitted. preprint available at <http://www.math.uic.edu/~mubayi/papers/ksimple.pdf>

[4] A. Kostochka, D. Mubayi, V. Rödl, P. Tetali, On the chromatic number of set systems, *Random Structures and Algorithms* 19 (2001), no. 2, 87–98.

[5] J. Komlós, J. Pintz and E. Szemerédi, A lower bound for Heilbronn’s problem, *J. London Math. Soc.* (2) 25 (1982), no. 1, 13–24.

[6] H. Lefmann, Sparse parity-check matrices over $\text{GF}(q)$. *Combin. Probab. Comput.* 14 (2005), no. 1-2, 147–169.

Small and Simple Representations

Jaroslav Nešetřil

Charles University, Prague

We show how the old topic of representations of groups, monoids and partial orders by special and small graphs leads in the new context to interesting problems and results.

Finite dualities by forbidding a clique minor

Yared Nigussie

East Tennessee State University

Let \mathcal{K} be a class of graphs. A pair (\mathcal{F}, U) is a finite duality in \mathcal{K} if $U \in \mathcal{K}$, \mathcal{F} is a finite set of graphs, and for any graph G in \mathcal{K} we have $G \leq U$ if and only if $F \not\leq G$ for all $F \in \mathcal{F}$ (“ \leq ” is the homomorphism order). We also say U is a dual graph in \mathcal{K} . Let \mathcal{G}/K_k denote the class of all graphs without a K_k minor. Using a theorem of Mader, the Four-color-theorem, and the Hadwiger conjecture for $k = 6$ result of Robertson, Seymour and Thomas, we prove that the only dual triangle-free graphs in \mathcal{G}/K_k are K_1 and K_{k-1} for $k \leq 6$. On the other hand, we show that for each $k \geq 4$, \mathcal{G}/K_k contains a proper subclass \mathcal{K}_k which contains infinitely many dual graphs in \mathcal{K}_k .

Joint work with **Jaroslav Nešetřil**.

On extremal cycle-free subgraphs of the hypercube

Lale Ozkahya

University of Illinois at Urbana-Champaign

Erdős conjectured that the size of the extremal 4-cycle-free subgraph of the n -dimensional hypercube, $ex(Q_n, C_4)$, is $(0.5 + o(1))e(Q_n)$, where $e(Q_n)$ is the number of edges of the n -dimensional hypercube. We consider the general Turan problem on Q_n for cycles of length $4k + 2$, $k \geq 3$, and show that $ex(Q_n, C_{4k+2})$ is $o(1)e(Q_n)$.

Joint work with **Zoltán Füredi**.

On the minimal distance of a polynomial near-ring code

Péter Pál Pach
Eötvös University

For a polynomial $f(x) \in \mathbb{Z}_2[x]$ it is natural to consider the near-ring code generated by the polynomials $f \circ x, f \circ x^2, \dots, f \circ x^k$ as a vectorspace. It is a 16 year old conjecture that for the polynomial $f(x) = x^n + x^{n-1} + \dots + x + 1$ the minimal distance of this code is n .

The conjecture is equivalent to the following purely number theoretical problem. Let $\underline{m} = \{1, 2, \dots, m\}$ and $A \subset \mathbb{N}$ be an arbitrary finite subset of \mathbb{N} . Show that the number of products that occur odd many times in $\underline{n} \cdot A$ is at least n . Among others we show that for $A = \underline{k}$ this number is at least n and that the distance of the code is at least $n/(\log n)^{0.223}$.

Generating random trees

Igor Pak
University of California, Los Angeles

I will present a generalization of the loop-erased random walk to (directed) hypergraphs. This allows a perfect sampling of random hyper-trees.

Joint work with **Igor Gorodezky**.

On the isomorphism problem of Cayley graphs

Péter P. Pálffy
Rényi Institute, Budapest

In 1977 Laci Babai defined the Cayley Isomorphism property for arbitrary finite groups and for arbitrary classes of relational structures. A group G is called a CI-group when two Cayley graphs of G are isomorphic only if there is an automorphism of the group G which is at the same time an isomorphism between the two Cayley graphs. There is an extensive literature concerning CI-groups, including important works by Muzychuk, Li, Praeger, Dobson, Godsil, and many others. In a joint work with Li and Lu we further restricted the structure of possible CI-groups. Concerning the CI property of elementary abelian p -groups recent advances were achieved by Muzychuk, Spiga, and Somlai.

Multipart Communication Complexity since Babai-Nisan-Szegedy

Toniann Pitassi
University of Toronto

The number-on-forehead (NOF) model of communication complexity is a fascinating model of communication where k players communicate to compute a joint function of their inputs. The twist is that in this setting, each player's input is placed metaphorically on his/her forehead, and thus each player actually sees all inputs except for his/her own. This model was defined in 1986 by Chandra, Furst and Lipton and has received considerable attention since then, due to its fundamental connections to central problems in complexity theory. In 1992, Babai, Nisan and Szegedy proved strong lower bounds in this model for up to sublogarithmic number of players, using the discrepancy method. To date this is the only method known for proving such strong lower bounds.

In this talk we will discuss several results obtained for the NOF model of communication complexity in the past few years. In particular we will discuss two relatively new separations. First a separation between randomized and deterministic communication complexity (Beame-David-Pitassi-Woelfel), and secondly, separations between nondeterministic and randomized complexity (Lee-Shraibman, Ada-Chattopadhyay, David-Pitassi-Viola, Beame-Huynh). We will conclude with open problems and future directions.

Islands on rectangular- and triangular grids

Gabriella Pluhár
Eötvös University

For each unit square of a square lattice a real number is given, its height. A rectangle on the lattice is called a rectangular island iff the height of every unit square of the rectangle is bigger than the height of the adjacent unit squares. In other words, if there exists a possible water-level by which the rectangle is an island in the usual sense. There are other cases when we assign numbers to cells; for example, a number may mean a colour on a gray-scale (before we convert the picture to black and white), transparency (against X-rays) or melting temperature.

We give lower and upper estimates for the maximum of the number of islands on the rectangular- and triangular grids. For example, if T_n denotes the maximum of the number of triangular islands on an equilateral triangle of sidelength n , then

$$\frac{n^2 + 3n}{5} \leq T_n \leq \frac{3n^2 + 9n + 2}{14},$$

and both values are attained infinitely many times.

Compatible functions on permutation groups

András Pongrácz
Central European University, Budapest

Let $S < G$ be a subgroup of the group G and $\Omega = \{Sg \mid g \in G\}$, and let G act on Ω on the usual way. A map $f : \Omega \rightarrow \Omega$ is called compatible with the above action if for any $H > S$ and $a, b \in G$ if $aH = bH$ then $f(a)H = f(b)H$. For example, constants and right translations are always compatible. The group action is called affine complete if these are the only compatible maps of Ω . A difficult open question of general algebraic systems is to characterize affine-complete permutation actions.

We investigate this notion for regular representations of groups. We call a group t -complete if it is affine complete with its regular representation. We show some examples of t -complete groups and a few necessary conditions for t -completeness. For example, dihedral groups and non-abelian finite simple groups are t -complete. From the two extraspecial groups of order p^3 one is t -complete, the other is not. Furthermore, we show that the product of t -complete subgroups of G forms a characteristic subgroup.

Serendipity, involutions and regular semisimple matrices

Cheryl E. Praeger
University of Western Australia

Key to studying finite simple groups is to study their involution centralisers, and this is true also in a computational setting. In a seminal paper, Chris Parker and Rob Wilson present and analyse a practical algorithm for computing the centraliser of an involution z in a finite classical group of odd characteristic. Fundamental to their approach, using Brays theorem and an observation of Richard Parker, is the estimation of the proportion of pairs of conjugates of z whose product has odd order – and is regular semisimple. They credit as inspiration for this work, a Monte Carlo algorithm published in 2001 by Christine Altseimer and Alexandre Borovik to distinguish finite simple classical groups of types B_n and C_n over a field of odd order at least 5. This algorithm also relies on constructing a particular involution, and a conjugate of it, such that the product is regular semisimple; their analysis utilises an estimate of $O(n^{-1})$ as the proportion of such pairs of conjugate involutions.

Motivated by the wish to improve on Parker and Wilson's algorithm by exploiting the pairs of conjugates of z whose product has even order, we were led by experimental evidence to estimate

the proportion of such pairs whose product is regular semisimple. Serendipity came to our rescue: we recognised the probability generating function for estimating such pairs as similar to one analysed by Jason Fulman, Peter Neumann and me for computing the proportion of separable matrices in unitary groups. A similar analysis enabled us to compute the limiting proportion as the dimension increases. This told us, for example, that the analogue of the Altseimer–Borovik proportion for general linear groups converges exponentially quickly to a limiting value depending only on the field size q .

Further work has given us good estimates for other involutions in general linear groups, and we have great hopes for the future of handling classical groups.

Joint work with **Ákos Seress**.

- [1] Christopher W. Parker and Robert A. Wilson, Recognising simplicity of black-box groups by constructing involutions and their centralisers, Submitted.
- [2] Christine Altseimer and Alexandre V. Borovik, Probabilistic recognition of orthogonal and symplectic groups, in *Groups and Computation III*, W. M. Kantor and Á. Seress (eds.), de Gruyter, Berlin/New York, 2001. pp. 120. With corrections in <http://www.ma.umist.ac.uk/avb/pdf/alt-avb4.pdf>.
- [3] J. E. Fulman, Peter M. Neumann and Cheryl E. Praeger, A Generating Function Approach to the Enumeration of Matrices in Classical Groups over Finite Fields, *Memoirs of the American Mathematical Society* 830, 2005.
- [4] Cheryl E. Praeger and Ákos Seress, Involutions and regular semisimple elements of finite general linear groups in odd characteristic.

Growth in finite simple groups of Lie type of bounded rank

László Pyber
Rényi Institute, Budapest

A Product Theorem in Free Groups

Alexander Razborov
University of Chicago and TTI-C

In inverse problems in arithmetic combinatorics, one is interested in describing internal properties of those finite subsets A of an algebraic structure that “barely expand” under its operations. One of the deepest results in the area is Freiman’s theorem providing a complete characterization of the sets A in abelian torsion-free groups for which $|A + A|$ is almost linear in $|A|$. Nothing non-trivial, however, is known already about sets of integers A with $|A + A| \leq A^{1+\delta}$.

Surprisingly, these questions have turned out to be easier for more complicated algebraic structures like commutative rings or, very recently, non-abelian groups. In particular, Chang (2006) proved that for some fixed δ , any set A in a free group with $|AAA| \leq A^{1+\delta}$ belongs to a cyclic subgroup.

We give a purely combinatorial proof of this result based on the theory of periodic words and their occurrences. Our proof also shows that δ can be chosen arbitrarily close to 1, and this is optimal. This further generalizes to arbitrary virtually free groups.

Polynomial functions on finite point sets

Lajos Rónyai
SzTAKI, Budapest

We discuss two results here. One is joint work with Laci Babai and M. K. Ganapathy [4], the other proves a conjecture by Laci and P. Frankl.

Let $\mathbf{f} = (f_1, \dots, f_m)$ be a sequence of polynomials of degree at most d in n variables ($m \geq n$) over a field F . The zero-pattern of \mathbf{f} at a point $u \in F^n$ is the set of indices i such that $f_i(u) = 0$. Denote by $Z_F(\mathbf{f})$ the number of zero-patterns of \mathbf{f} as u runs over F^n . We show that

$$Z_F(\mathbf{f}) \leq \sum_{j=0}^n \binom{m}{j}$$

for $d = 1$ and

$$Z_F(\mathbf{f}) \leq \binom{md}{n}$$

for $d > 1$. For $m \geq nd$ these bounds are optimal within a factor $(7.25)^n$. The result for $d > 1$ improves upon the bound $(1 + md)^n$ proved by J. Heintz using algebraic geometry. Our proof is very short, it employs the linear algebra bound. We have applications to the projective dimension of graphs and to the dimension of span programs.

Laci and P. Frankl conjectured the following in [1], p. 115. Let k, α be positive integers, p a prime and $q = p^\alpha$. Assume that $\mathcal{F} = \{A_1, \dots, A_m\}$ is a family of subsets of $[n]$ such that

$$\begin{aligned} |A_i| &\equiv k \pmod{q} \text{ for } i = 1, \dots, m, \text{ and} \\ |A_i \cap A_j| &\not\equiv k \pmod{q} \text{ for } 1 \leq i < j \leq m. \end{aligned}$$

Then

$$m \leq \binom{n}{q-1}.$$

We proved this with G. Hegedűs in [2], [3] for $2(q-1) \leq n$. We combined the linear algebra bound (developed for a related inequality in [1]) with an argument involving a Gröbner basis of a suitable ideal I in the polynomial ring $F_p[x_1, \dots, x_n]$.

[1] L. Babai, P. Frankl, *Linear algebra methods in combinatorics*, Preliminary Version 2, September 1992.

[2] G. Hegedűs, L. Rónyai, Gröbner bases for complete uniform families, *J. of Algebraic Combinatorics* **17** (2003), 171–180.

[3] G. Hegedűs, L. Rónyai, Standard monomials for q -uniform families and a conjecture of Babai and Frankl, *Central European Journal of Mathematics* **1** (2003), 198–207.

<http://www.cesj.com/mathematics.html>

[4] L. Rónyai, L. Babai, M. K. Ganapathy, On the number of zero-patterns of a sequence of polynomials, *Journal of the AMS* **14** (2001), 717–735.

Approximating the Permanent with Nonabelian Determinants

Alex Russell
University of Connecticut

Cellular Automata on Cayley Graphs and Amenability

Paul Schupp
Univ. Illinois, Urbana-Champaign

In 1929 John von Neumann defined the concept of amenability for groups, which has since been intensively studied. It is easy to see that the free group F_2 of rank 2 is not amenable and von Neumann raised the question of whether or not any finitely generated nonamenable discrete group had to contain a copy of F_2 . Examples of finitely generated amenable groups not containing F_2 have recently been given.

In the early 1950's, Ulam and von Neumann introduced cellular automata in the “classical case” of the grid of integer lattice points in the plane, that is, the Cayley graph of the free

abelian group, \mathbb{Z}^2 . However, all the relevant definitions are well-defined on the Cayley graph of any finitely generated group. A major question is whether or not the global transition function is surjective. Two important theorems in the classical case are the theorems of Moore and Myhill about “Garden of Eden patterns” and “mutually erasable patterns”.

Dave Muller pointed out that both the Moore and Myhill theorems are false on the Cayley graph of F_2 . In a series of papers Antonio Machi and colleagues proved that both the Moore and Myhill theorems hold for cellular automata on Cayley graphs of finitely generated amenable groups. Recently, Laurent Bartholdi proved the converse! Thus amenability is completely characterized by the cellular automaton properties of a group. We will also discuss decidability of surjectivity.

Cayley graphs of elementary Abelian p -groups

Gábor Somlai
Eötvös University, Budapest

A Cayley graph $\text{Cay}(G, S)$ is said to be a CI-graph if for each $T \subset G$ the Cayley graphs $\text{Cay}(G, S)$ and $\text{Cay}(G, T)$ are isomorphic if and only if there is an automorphism σ of the group G such that $S^\sigma = T$. Furthermore, a group G is called CI-group if every Cayley graph of G is a CI-graph.

Determining whether or not an elementary Abelian group \mathbb{Z}_p^n is CI is an important problem in the investigation of Cayley graphs. Muzychuk proved the essential fact that an elementary Abelian p -group of rank greater than or equal to $2p - 1 + \binom{2p-1}{p}$ is not a CI-group. In this talk I present an elementary construction that provides a uniform explanation for the recent works concerning the bound.

A graph polynomial for independent sets of bipartite graphs

Daniel Štefankovič
University of Rochester, New York

We introduce a new graph polynomial that encodes interesting properties of graphs, for example, the number of matchings and the number of perfect matchings. Most importantly, for bipartite graphs the polynomial encodes the number of independent sets ($\#BIS$).

We analyze the complexity of exact evaluation of the polynomial at rational points and show that for most points exact evaluation is $\#P$ -hard (assuming the generalized Riemann hypothesis) and for the rest of the points exact evaluation is trivial.

We conjecture that a natural Markov chain can be used to approximately evaluate the polynomial for a range of parameters. The conjecture, if true, would imply an approximate counting algorithm for $\#BIS$, a problem shown, by Dyer, Goldberg, Greenhill, and Jerrum to be complete (with respect to, so called, AP-reductions) for a rich logically defined sub-class of $\#P$.

We support our conjecture by proving that the Markov chain is rapidly mixing on trees. As a by-product we show that the “single bond flip” Markov chain for the random cluster model is rapidly mixing on constant tree-width graphs.

Joint work with **Qi Ge**.

Invariance in Property Testing

Madhu Sudan
Massachusetts Institute of Technology

Property testing considers the task of testing if some given data satisfies a desired property by sampling the data probabilistically in very few places. The “oldest” property test might be the use of polling to predict the outcome of an upcoming election. Modern research has extended the scope of property tests to a much richer class of properties including tests of linearity (“is

the data essentially linear with respect to some parameters”), multilinearity, low-degreeness, colorability (“is the data describing a graph with small chromatic number”) etc.

What makes some properties testable so efficiently, that we do not have to look at the entire data in order to test for it? We suggest that for interesting properties, testability ought to be related to the “invariances” shown by the property: i.e., if the data is viewed as a function from some input to some output, then the “invariances” are given by a set (a group) of permutations of the input space under which the property is invariant. We then investigate this hypothesis in the context of “algebraic properties”. This leads to a rich unification of previous known works, as also some new properties and counterexamples to more optimistic conjectures.

Based on joint works with **Elena Grigorescu** and **Tali Kaufman** (MIT).

Paired Hanoi Towers Problem

Zoran Sunic
Texas A&M University

We provide a group theoretic model of the standard Hanoi Towers Problem by constructing a self-similar group H acting on a ternary rooted tree in such a way that its action on level n in the tree models the n -disk version of the Problem. Then we present a new version of the Hanoi Towers Problem and use the group H to provide an algorithm for solving it.

The computational complexity of solving equations over finite groups

Csaba Szabó
Eötvös University

It was always in the center of algebraic interest whether or not an equation can be solved. A similar problem is, whether or not two algebraic expressions agree at every substitution, or in other words whether or not an identity holds over an algebraic structure. In our talk we investigate the computational complexity of the above problems over finite groups. We show that for nilpotent and dihedral groups the problems are solvable in polynomial time and that for simple groups both problems are (co-)NP-complete. There are very few results known about solvable but non-nilpotent groups.

We show that extending a group with new operations might change the complexity. For example, for the alternating group $(A_4, \cdot, {}^{-1})$ both problems are in P, but if we add the commutator as basic operation, then for the (extended) group $(A_4, \cdot, {}^{-1}, [,])$ both problems become hard.

Price of Anarchy and Adword Auctions

Éva Tardos
Cornell University

An algorithmic proof of the Lovász Local Lemma

Gábor Tardos
Simon Fraser University, British Columbia, Canada & Rényi Institute, Budapest

The Lovász Local Lemma is a powerful tool to non-constructively prove the existence of combinatorial objects meeting a prescribed collection of criteria. In 1991 Beck gave an efficient algorithm that under certain more restrictive conditions found the desired object. Simplifications of his procedure and relaxations of its restrictions were subsequently exhibited in several publications. In this talk we present a very simple and natural polynomial time algorithm that can find the object guaranteed to exist by the Local Lemma in polynomial time. In contrast to all previous approaches, the new algorithm applies to almost all known applications of the lemma

and since the original non-constructive proofs are not invoked anymore, it can be regarded as a constructive proof variant.

Joint work with **Robin Moser**.

Horn Formulas or Directed Hypergraphs: Combinatorics and Complexity

György Turán

University of Illinois, Chicago and University of Szeged, Hungary

Horn formulas are conjunctions of clauses of the form $a, b \rightarrow c$, and can also be thought of as directed hypergraphs. We discuss some algorithmic and combinatorial problems for Horn formulas. A sublinear approximation algorithm and inapproximability results are given for the minimization of Horn formulas. The approximation algorithm is based on a decomposition of bipartite graphs into complete bipartite subgraphs. We also present extremal and threshold probability results for Horn formulas.

Joint work with **Amitava Bhattacharya, Bhasgar DasGupta, Marina Langlois, Dhruv Mubayi, and Bob Sloan**.

On the complexity of generating distributions

Emanuele Viola

Northeastern University, Boston

Complexity theory, with some notable exceptions, typically studies the complexity of computing a function $h(x)$ of a given input x . We advocate the study of the complexity of generating the output distribution $h(x)$ for random x , given random bits. While this question can be studied for a variety of computational models, here we focus on small bounded-depth circuits with unbounded fan-in (AC^0) or bounded fan-in (NC^0).

An interesting example of a function h for which computing $h(x)$ is harder than generating its output distribution is $h(x) := (x, \text{parity}(x))$, where $\text{parity}(x) := \sum_i x_i \pmod 2$. Whereas AC^0 circuits cannot compute parity, Babai [2] and Boppana and Lagarias [3] show an NC^0 circuit C whose output distribution equals that of $(x, \sum_i x_i \pmod 2)$ for random $x \in \{0, 1\}^n$:

$$C(x_1, x_2, \dots, x_n) := (x_1, x_1 + x_2, x_2 + x_3, \dots, x_{n-1} + x_n, x_n).$$

Our main results are:

(1) There are explicit AC^0 circuits of size $n^{O(1)}$ and depth $O(1)$ whose output distribution has statistical distance $1/2^n$ from the distribution $(X, \sum_i X_i) \in \{0, 1\}^n \times \{0, 1, \dots, n\}$ for uniform $X \in \{0, 1\}^n$, despite the inability of these circuits to compute $\sum_i x_i$ given x . We also prove a lower bound independent from n on the statistical distance between the output distribution of NC^0 circuits and the distribution $(X, \text{majority}(X))$. We show that $1 - o(1)$ lower bounds for related distributions yield lower bounds for succinct data structures.

(2) Uniform randomized AC^0 circuits of size $n^{O(1)}$ and depth $d = O(1)$ with error ϵ can be simulated by uniform randomized circuits of size $n^{O(1)}$ and depth $d + 1$ with error $\epsilon + o(1)$ using $\leq (\log n)^{O(\log \log n)}$ random bits. Previous derandomizations ([1],[4]) increase the depth by a constant factor, or else have poor seed length.

The paper is available at [5].

[1] Miklós Ajtai and Avi Wigderson. Deterministic simulation of probabilistic constant-depth circuits. *Advances in Computing Research - Randomness and Computation*, 5:199–223, 1989.

[2] László Babai. Random oracles separate PSPACE from the polynomial-time hierarchy. *Inform. Process. Lett.*, 26(1):51–53, 1987.

[3] Ravi Boppana and Jeffrey Lagarias. One-way functions and circuit complexity. *Inform. and Comput.*, 74(3):226–240, 1987.

[4] Noam Nisan. Pseudorandom bits for constant depth circuits. *Combinatorica*, 11(1):63–70, 1991.

[5] Emanuele Viola. Are all distributions easy?, 2009. <http://www.ccs.neu.edu/home/viola>

Self-dual and Self-Petrie-dual Regular Maps

Yan Wang
Yan Tai University

Regular maps are cellular decompositions of surfaces with the ‘highest level of symmetry’, not necessarily orientation-preserving. Such maps can be identified with three-generator presentations of groups G of the form $G = \langle a, b, c \mid a^2 = b^2 = c^2 = (bc)^2 = (ab)^n = (ca)^m = \dots = 1 \rangle$; the positive integers m and n are the vertex degree and the face length of the map. A regular map $(G; a, b, c)$ is *self-dual* if the assignment $a \mapsto a, b \mapsto c$ and $c \mapsto b$ extends to an automorphism of G , and *self-Petrie-dual* if G admits an automorphism fixing a and c and interchanging b with bc .

In this note we show that for infinitely many numbers m there exist finite, self-dual and self-Petrie-dual regular maps of degree and face length equal to m . We also prove that no such map with odd vertex degree is a normal Cayley map.

Joint work with **R. Bruce Richter** and **Jozef Širáň**.

Expanders, groups and irreducible representations

Avi Wigderson
Institute for Advanced Studies, Princeton

I will survey some work on iterative constructions of expanding Cayley graphs. I will also present some interesting open questions on different relationships between expansion and the irreducible representations in finite groups, motivated by this and other work.

Finding direct products of permutation groups is in P

James B. Wilson
Ohio State University

A polynomial-time algorithm is given which determines if a group generated by permutations is a direct product of proper nontrivial subgroups. The methods apply to groups of matrices and produce asymptotic estimates for the number, up to isomorphism, of finite groups which are indecomposable by direct products.

Vertex transitive tournaments of order pq

Jing Xu
Beijing

In this talk, we classify the vertex transitive tournaments of order pq where p and q are distinct odd primes. Moreover, we study 2-closed (in Wielandt’s sense) odd order transitive permutation groups of degree pq by using the classifications of vertex transitive tournaments of order pq . Actually, for each such 2-closed group we prove that it is the full automorphism group of some tournament.

The generalization of şiş kebab theorem and black box groups

Sükrü Yalcinkaya
University of Western Australia

In this talk, I will talk about the generalization of the Curtis-Tits presentation of Lie type groups and its application to black box recognition of finite groups.

Group Connectivity of Cayley Graphs

Taoye Zhang
Pennsylvania State University

Let G be a group and subset S of $G \setminus \{1\}$ such that $S^{-1} = S$. A Cayley graph $Cay(G; S)$ of the group G with symbol S is the graph with vertex set G and edge set $\{(g, gs) : g \in G, s \in S\}$.

Let G be a graph and G' be its orientation. For any vertex $v \in V(G)$, we denote the set of all edges with tails at v by $E^+(v)$ and heads at v by $E^-(v)$. G is said to be \mathbb{Z}_3 -connected if for every boundary $b : V(G) \rightarrow \mathbb{Z}_3$ with $\sum_{v \in V(G)} b(v) = 0$, there is a flow $f : E(G') \rightarrow \mathbb{Z}_3$ such that

$$\sum_{e \in E^+(v)} f(e) - \sum_{e \in E^-(v)} f(e) = b(v)$$

for every $v \in V(G)$.

We prove that every k -valent Cayley graph of an Abelian group, where $k \geq 5$, is \mathbb{Z}_3 -connected.
