Mathematisches Forschungsinstitut Oberwolfach

Report No. 17/2024

DOI: 10.4171/OWR/2024/17

Mini-Workshop: Growth and Expansion in Groups

Organized by
Jitendra Bajpai, Kiel
Daniele Dona, Budapest

7 April – 12 April 2024

Abstract. The aim of the workshop was to give a panoramic view of the main lines of research on various aspects of growth and expansion in finite groups. The main topics included: diameter bounds for Cayley graphs of alternating and classical groups, with results for generating sets that can be arbitrary, random, or containing special elements; constructions of expander families of finite simple groups, with the use of property (T); and character bounds for finite simple groups, yielding applications to word map problems and random walks on Cayley graphs. A series of smaller topics explored connections and similarities to different problems in group theory.

Mathematics Subject Classification (2020): 20D60, 20F69.

Introduction by the Organizers

The Oberwolfach Mini-Workshop *Growth and expansion in groups* (2415a) was organized by Jitendra Bajpai (Kiel) and Daniele Dona (Budapest), and it was attended in total by 16 participants both senior and junior with a broad geographical distribution, all of whom came to Oberwolfach in person. The topic of the workshop was the phenomenon of growth and expansion of sets inside groups. The aim was to present the field's state of the art by gathering leading experts and passing the knowledge to the next generation. The program consisted of four mini-courses given by the main speakers, each made of four 1-hour lectures, and of seven individual lectures given by several other participants, of duration variable between 20 and 60 minutes.

The first main speaker was Sean Eberhard (Belfast), whose course was titled *Growth for special generating sets in high rank.* The course focused on finite simple groups of high rank, namely alternating groups and classical groups, and the diameter of their Cayley graphs with respect to generating sets that are either random or contain a special element of small support: such elements are 3-cycles in $\mathrm{Alt}(n)$, transvections in classical non-orthogonal groups, and long root elements in orthogonal groups. The speaker first showed the main techniques involved in the proof of results for $\mathrm{Alt}(n)$, going back to articles of Babai-Beals-Seress [1], Babai-Hayes [2], and Helfgott-Seress-Zuk [13] among others. Then he moved to the recent results for classical groups as in Halasi [10], Garonzi-Halasi-Somlai [7], Eberhard-Jezernik [6], and Eberhard [5].

The second main speaker was Harald Helfgott (Paris), whose course was titled *Strategies for growth in permutation groups.* The course focused on the proof of a uniform diameter bound for all the Cayley graphs of $\mathrm{Alt}(n)$. The speaker presented the methods adopted in the papers of Helfgott-Seress [12] and Helfgott [11]. One of the objectives of the course was to highlight which techniques could be potentially transferred to the case of classical groups, so the treatment was tailored to be general enough to cover both high-rank cases at once whenever possible.

The third main speaker was Martin Kassabov (Ithaca), whose course was titled *Kazhdan Property T, Kazhdan constants and expansion in finite groups.* The course focused on how to prove that certain groups have property (T), such as $\mathrm{SL}_{3k}(\mathbb{Z})$ and $\mathrm{Aut}(\mathbb{Z}[x_1, \ldots, x_n])$, which as a consequence provides families of expanders on finite groups of the form $\mathrm{SL}_{3k}(\mathbb{F}_p)$ and $\mathrm{Alt}(p^n - 1)$. The proofs are based on papers of Kassabov [14] and Caprace-Kassabov [4] and feature particularly explicit geometric constructions, giving in theory explicit bounds for the corresponding Kazhdan constants.

The fourth main speaker was Pham Huu Tiep (Piscataway), whose course was titled *Character bounds for finite simple groups and applications.* The course focused on giving bounds for the values of characters on non-central elements inside finite quasi-simple groups, either of the form $|\chi(g)| \leq \gamma\chi(1)$ or of the form $|\chi(g)| \leq \chi(1)^{\alpha}$. There is a variety of such results, both for symmetric groups and for groups of Lie type, due among others to Larsen-Shalev [15], Bezrukavnikov-Liebeck-Shalev-Tiep [3], Guralnick-Larsen-Tiep [8, 9], and Larsen-Tiep [16]. Particular emphasis was given to the theory of character levels and to the several applications of the resulting bounds, for example on Waring's problem, on random walks on Cayley graphs, and on Thompson's conjecture.

In addition, there were seven individual lectures distributed throughout the week. Vadim Alekseev (Dresden) presented some results concerning geometric property (T), and in particular connecting it to property (T) in the context of sofic groups. Michal Doucha (Prague) talked about the shadowing property of actions on compact metric spaces, according to which every pseudo-orbit closely traces the path of an actual orbit, and about the fact that hyperbolic groups acting on their border have the shadowing property. Daniele Garzoni (Los Angeles) gave a presentation of the group large sieve method, by which one can show that a random walk on a group with many quotients satisfying certain properties almost never ends in any given small set. Noam Lifshitz (Jerusalem) presented a Bogolyubov-type theorem for $\mathrm{SL}_n(\mathbb{F}_q)$, saying that for any subset A of positive density α there is a subgroup of density α^C contained in $(AA^{-1})^2$, where C is an absolute constant. Martin Nitsche (Karlsruhe) explained how to prove property (T) for $\mathrm{Aut}(F_n)$, with the use of a computer for n low and without for n large enough. Luca Sabatini (Belfast) showed that some results on diameter and expansion in Cayley graphs with random generating sets can be appropriately generalized to the setting of Schreier graphs as well. Katrin Tent (Münster) presented the main ideas of the proof that the free Burnside group $B(n, m)$ is infinite for $n \geq 557$ odd.

The workshop provided an inspiring environment in which the main speakers interacted with each other and with the younger audience, and stimulated discussion that resulted in a lot of open questions from the participants. We felt that the frontiers of the main lines of research on the topic of the workshop have been nicely presented to a potentially interested audience, and hope that in the future the event develops into a flurry of new ideas, results, and meetings.

Acknowledgement: The MFO and the workshop organizers would like to thank the Oberwolfach Foundation for supporting the participation of Subham Bhakta with the Oberwolfach Foundation Fellowship at the MFO.

References

[1] L. Babai, R. Beals, and Á. Seress. On the diameter of the symmetric group: polynomial bounds. In *Proceedings of the 15th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1108–1112. 2004.

[2] L. Babai and T. P. Hayes. Near-independence of permutations and an almost sure polynomial bound on the diameter of the symmetric group. In *Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1057–1066. 2005.

[3] R. Bezrukavnikov, M. W. Liebeck, A. Shalev, and P. H. Tiep. Character bounds for finite groups of Lie type. *Acta Math.*, 221(1):1–57, 2018.

[4] P.-E. Caprace and M. Kassabov. Tame automorphism groups of polynomial rings with property (T) and infinitely many alternating group quotients. *Trans. Amer. Math. Soc.*, 376(11):7983–8021, 2023.

[5] S. Eberhard. Diameter of classical groups generated by transvections. `arXiv:2308.07086`, 2023.

[6] S. Eberhard and U. Jezernik. Babai's conjecture for high-rank classical groups with random generators. *Invent. math.*, 227(1):149–210, 2022.

[7] M. Garonzi, Z. Halasi, and G. Somlai. On the diameter of Cayley graphs of classical groups with generating sets containing a transvection. *Israel J. Math.*, 2024. To appear.

[8] R. M. Guralnick, M. W. Larsen, and P. H. Tiep. Character levels and character bounds. *Forum Math. Pi*, 8, 2020. Article e2.

[9] R. M. Guralnick, M. W. Larsen, and P. H. Tiep. Character levels and character bounds for finite classical groups. *Invent. Math.*, 235(1):151–200, 2023.

[10] Z. Halasi. Diameter of Cayley graphs of $SL(n, p)$ with generating sets containing a transvection. *J. Algebra*, 569:195–219, 2021.

[11] H. A. Helfgott. Growth in linear algebraic groups and permutation groups: towards a unified perspective. In *Groups St Andrews 2017 in Birmingham*, volume 455 of *London Mathematical Society Lecture Note Series*, pages 300–345. Cambridge (UK), 2019.

[12] H. A. Helfgott and Á. Seress. On the diameter of permutation groups. *Ann. of Math. (2)*, 179:611–658, 2014.

[13] H. A. Helfgott, Á. Seress, and A. Zuk. Random generators of the symmetric group: Diameter, mixing time and spectral gap. *J. Algebra*, 421:349–368, 2015.

[14] M. Kassabov. Universal lattices and unbounded rank expanders. Invent. Math., 170:297–326, 2007.

[15] M. J. Larsen and A. Shalev. Characters of symmetric groups: sharp bounds and applications. *Invent. Math.*, 174(3):645–687, 2008.

[16] M. J. Larsen and P. H. Tiep. Uniform character bounds for finite classical groups. *Ann. of Math. (2)*, 2024. To appear.

Mini-Workshop: Growth and Expansion in Groups

Table of Contents

Abstracts

Sofic approximations and geometric property (T)

Vadim Alekseev
(joint work with Stefan Drigalla)

In the recent years, there has been substantial activity connecting graph theory and group theory via the concept of a metric approximation of an infinite group by finite objects (groups or graphs), particularly around sofic groups. This lead to numerous results which connect approximation properties of the group (for instance, amenability, Haagerup property) in terms of geometric properties of its approximations (e.g. hyperfiniteness, coarse embeddability into Hilbert space of a graph sequence). More precisely, we have the following results:

Theorem 1 ([1, Theorem 1.1]). *Let Γ be a sofic group, $\mathcal{X}$ a sofic approximation of Γ, and X be the space of graphs constructed from $\mathcal{X}$. Then:*

(1) If X has property A then Γ is amenable;
(2) If X admits an asymptotic coarse embedding into Hilbert space, then Γ is a-T-menable;
(3) If X has boundary geometric property (T) then Γ has property (T).

The philosophy of this result is exactly that interesting analytic properties of discrete groups are in some sense testable on a sofic approximation, but how these properties connect with the measures on the sofic boundary action as well as with their graph theoretic counterparts is yet to be fully understood, and it leads to the following question: to which extent do the converse statements to the one of Theorem 1 hold? In the case where the sofic approximation is coming from a sequence of finite quotients for a residually finite groups, the converses were known to hold true [2, 3, 4, 5], but as sofic approximations can be perturbed on sets of small density, it is easy to see that the converse implications can not hold "on the nose".

The question in the amenable case was partly answered by Tom Kaiser in [7] by introducing property almost-A which means that after throwing out asymptotically negligible pieces of a graph sequence one obtains a sequence with property A. Together with Leonardo Biz we were able to prove the following analogous statement in the a-T-menable setting:

Theorem 2 ([6, Theorem C]). *Let $\mathcal{X} = \{X_i\}_{i\in\mathbb{N}}$ be a sequence of finite graphs with bounded degree and X the related space of graphs. If the coarse boundary groupoid $(\partial G(X), \mu_\omega)$ is a measurably a-T-menable for every non-principal ultrafilter $\omega \in \partial\beta\mathbb{N}$, then, for every $\varepsilon > 0$, there exist $\{Z_i\}_{i\in\mathbb{N}} \subset \{X_i\}_{i\in\mathbb{N}}$ such that $\lim_{i\to\infty} \mu_i(Z_i) \leq \varepsilon$ and $\{X_i \backslash Z_i\}_{i\in\mathbb{N}}$ is asymptotically coarsely embeddable into a Hilbert space $\mathcal{H}$ when equipped with the same metric on X.*

This left the case of property (T) open. By the result of Gábor Kun, every sofic approximation of a property (T) group is asymptotically equivalent to an expander sequence, but in view of the above one would expect a stronger result here, namely that it should be asymptotically equivalent to a space with geometric property (T). This is indeed our main new result with Stefan Drigalla:

Theorem 3. *Let X be a space of graphs having almost boundary (T). Then there is a space of graphs X' which is approximately isomorphic to X and has geometric property (T).*

Here, almost boundary (T) is a condition which ensures spectral gap of the Laplacian of the graphs on a measure 1 subset of the Stone-Čech boundary of X. In particular, it is automatically satisfied for every sofic approximation of a property (T) group. As a consequence, we obtain the following result, completing the picture of converses to 1:

Theorem 4. *Let Γ be a finitely generated sofic group. The following are equivalent:*

(1) Γ has property (T),
(2) every sofic approximation of Γ has almost boundary (T),
(3) there is a sofic approximation of Γ with geometric property (T).

References

[1] Vadim Alekseev and Martin Finn-Sell, *Sofic boundaries of groups and coarse geometry of sofic approximations*, Groups Geom. Dyn., **13(1)** (2019), 191–234.
[2] John Roe, *Lectures on coarse geometry*, American Mathematical Society, Providence, RI, 2003.
[3] Martin Finn-Sell, *Fibred coarse embeddings, a-T-menability and the coarse analogue of the Novikov conjecture*, J. Funct. Anal. **267(10)** (2014), 3758–3782.
[4] Rufus Willett, *Random graphs, weak coarse embeddings, and higher index theory*, J. Topol. Anal. **7(3)** (2015), 361–388.
[5] Rufus Willett and Guoliang Yu, *Geometric property (T)*, Chin. Ann. Math. Ser. B, **35(5)** (2014), 761–800.
[6] Vadim Alekseev and Leonardo Businhani Biz, *Sofic boundaries and a-T-menability,* arXiv 2112.14760.
[7] Tom Kaiser, Combinatorial cost: a coarse setting, Trans. Amer. Math. Soc., **372(4)** (2019), 2855–2874.
[8] Gabor Kun, *On sofic approximations of Property (T) groups*, arXiv:1606.04471, 2016.

Shadowing of actions of hyperbolic groups on their boundaries

Michal Doucha

Shadowing, also known as the pseudo-orbit tracing property, is a fundamental dynamical notion having its origins in smooth dynamics in the study of hyperbolic systems. A ε-pseudo-orbit of a homeomorphism $f : X \to X$ on a compact metric space X, for some $\varepsilon > 0$, is a sequence $(x_n)_{n\in\mathbb{Z}} \subseteq X$ such that for every $n \in \mathbb{Z}$, $f(x_n)$ is in a ε-neighborhood of x_{n+1}. A homeomorphism has the shadowing if each pseudo-orbit stays close to a true orbit; typical examples are uniformly hyperbolic dynamical systems.

The theory of shadowing has been eventually generalized to actions of more general groups (see [8])). Let a countable group G act continuously on a compact metric space X. Let $S \subseteq G$ be finite and let $\delta > 0$. A sequence $(x_g)_{g\in G}$ is a (S,δ)-pseudo-orbit if for every $g \in G$ and $s \in S$, $d(sx_g, x_{sg}) < \delta$. The action of G on X has the shadowing if for every $\varepsilon > 0$ there are a finite set $S \subseteq G$ and $\delta > 0$ such that for every (S,δ)-pseudo-orbit $(x_g)_{g\in G}$ there exists $x \in X$ so that for all $g \in G$ we have $d(gx, x_g) < \varepsilon$.

There are now a number of examples of group actions with the shadowing. For instance, Osipov and Tikhomirov in [8] show that an action of a finitely generated nilpotent group has the shadowing if and only if at least one element of the group acts expansively with the shadowing. Meyerovitch proves that expansive principal algebraic actions of countable groups have the shadowing, see [7]. Chung and Lee show that a subshift over a general countable group has the shadowing if and only if it is of finite type (see [1]) generalizing the result of Walters for the integer actions (see [9]). In general, subshifts of finite type approximate in a sense every action of a finitely generated group on a compact metrizable space with the shadowing, see [4, 3].

The following is our main result.

Theorem. *Let G be a hyperbolic group and denote by ∂G its Gromov boundary. Then the canonical action of G on ∂G has the shadowing.*

Let us mention some interesting consequences. Let G be a countable group and X a compact metric space. A continuous action $\alpha : G \times X \to X$ is called *topologically stable* if for every $\varepsilon > 0$ there exists an open neighborhood U of α in the space of all actions of G on X (this space can be identified with a closed subset of $\mathrm{Homeo}(X)^G$) such that for every action $\beta \in U$ there exists a continuous map $h : X \to X$ such that

- h intertwines between β and α, i.e. for every $x \in X$ and $g \in G$, $h(\beta(g,x)) = \alpha(g, h(x))$;
- $\sup_{x\in X} d(x, h(x)) \leq \varepsilon$.

Since expansive actions of finitely generated groups on compact metric spaces with the shadowing are topologically stable (see [9, 1]) and the canonical action of a hyperbolic group on its boundary is expansive (see [2, Chapter 3]), we recover the following recent results of Mann, Manning and Mann, Manning, Weisman.

Corollary[5, 6]. Let G be a hyperbolic group. Then the canonical action of G on ∂G is topologically stable.

References

[1] N.P. Chung and K. Lee, *Topological stability and pseudo-orbit tracing property of group actions*, Proc. Amer. Math. Soc., 146 (2018), pp. 1047–1057.

[2] M. Coornaert and A. Papadopoulos, *Symbolic dynamics and hyperbolic groups*, vol. 1539 of Lect. Notes Math., Berlin: Springer-Verlag, 1993.

[3] C. Good and J. Meddaugh, *Shifts of finite type as fundamental objects in the theory of shadowing*, Invent. Math., 220 (2020), pp. 715–736.

[4] Z. Lin, E. Chen, and X. Zhou, *Shadowing and mixing on systems of countable group actions*, Adv. Math., 405 (2022), pp. Paper No. 108521, 27.
[5] K. Mann and J. F. Manning, *Stability for hyperbolic groups acting on boundary spheres*, Forum Math. Sigma, 11 (2023), p. 25. Id/No e83.
[6] K. Mann, J. F. Manning, and T. Weisman, *Stability of hyperbolic groups acting on their boundaries*, arXiv:2206.14914, (2022).
[7] T. Meyerovitch, *Pseudo-orbit tracing and algebraic actions of countable amenable groups*, Ergodic Theory Dynam. Systems, 39 (2019), pp. 2570–2591.
[8] A. V. Osipov and S. B. Tikhomirov, *Shadowing for actions of some finitely generated groups*, Dyn. Syst., 29 (2014), pp. 337–351.
[9] P. Walters, *On the pseudo orbit tracing property and its relationship to stability*, Struct. Attract. dyn. Syst., Proc., North Dakota State Univ. 1977, Lect. Notes Math. 668, 231–244 (1978).

Growth for special generating sets in high rank

Sean Eberhard

The well-known conjecture of Babai predicts that Cayley graphs of simple groups have polylogarithmic diameter uniformly in the choice of generating set. This is now known for simple groups of Lie type of bounded rank, but it is still wide open for high-rank groups. For example, for A_n, the state of the art is still the 2014 result of Helfgott and Seress [10] that

$$\operatorname{diam}(A_n) \ll \exp O((\log n)^4 \log\log n),$$

i.e., *quasipolynomial* in $\log |A_n|$. For classical groups the situation is even worse.

The purpose of this short course is to consider the diameter with respect to generating sets containing "something special". We consider two particular meanings of "special": either "small support" or "random". We are particularly interested in random elements, which simply means we choose generators at random and hope to prove results with some probability estimate $1 - o(1)$. In other words, while Babai's conjecture strictly interpretated is a conjecture about diameters in the "worst case", we are now considering diameters in the "typical case". As ever, the case of symmetric and alternating groups is better studied and better understood. Our approach is to review what is known in this case and then see what analogues there are for classical groups if any.

The following table gives a representative sample of what is known for diameters of $G = S_n$ or A_n with respect to a generating set X containing something special.

If X contains...	$\operatorname{diam}(G; X) \ll$	Reference
a 3-cycle	n^4	folklore
$x \neq 1, \lvert\operatorname{supp}(x)\rvert \leq 0.33n$	$n^{8+o(1)}$	Babai–Beals–Seress, 2004 [1]
$x \neq 1, \lvert\operatorname{supp}(x)\rvert \leq 0.63n$	n^{78}	Bamberg–Gill–Hayes–Helfgott –Seress–Spiga, 2012 [3]
two random elements	$n^{7+o(1)}$	Babai–Hayes, 2004 [2]
	$n^{3+o(1)}$	Schlage-Puchta, 2012 [13]
	$n^{2+o(1)}$	Helfgott–Seress–Zuk, 2015 [11]
three random elements	$n^2 \log n$	Eberhard–Jezernik, 2022 [5]

Now let us turn to classical groups, say $G = \mathrm{SL}_n(q)$. Note that $|G| \approx q^{n^2}$, so ideally we want diameter bounds of the form

$$(\log |G|)^{O(1)} = (n \log q)^{O(1)},$$

i.e., polynomial in n and $\log q$. We will generally assume q is small (think $q = 2$, at least to begin with), so the goal is "polynomial in n" (just like for S_n).

The most important special kinds of elements in the symmetric group are elements of small support: transpositions, 3-cycles, etc. The closest analogues in classical groups are elements of small *degree*, where we define $\deg(g)$ to be the rank of $g - 1$. This quantity measures how close g is to being trivial. A *transvection* is an element of $\mathrm{SL}_n(q)$ of degree 1. Transvections are present in $\mathrm{SL}_n(q)$, $\mathrm{SU}_n(q)$, and $\mathrm{Sp}_{2n}(q)$, but not in $\Omega_n^\varepsilon(q)$. The elements of minimal degree in $\Omega_n^\varepsilon(q)$ (*long root elements*) have degree 2.

The following table summarizes the state of the art for special generating sets in classical groups.

If X contains...	$\mathrm{diam}(G; X) \ll$	Restrictions	Reference
a transvection	$(q \log n)^{O(1)}$	SL, $q = p$	Halasi, 2020 [9]
		q odd, $q \neq 9, 81$	Garonzi–Halasi–Somlai, 2023 [7]
		any q	Eberhard, 2024 [4]
$q^{O(1)}$ random			Eberhard–Jezernik, 2022 [5]
3 random		$q \ll 1$, not Ω	Eberhard, 2024 [4]

These results are all proved by combining (in varying amounts) only a few basic ingredients:

(0) the trivial diameter bound (i.e., diameter $\leq$ number of vertices),
(1) a random commutator argument (to shrink supports),
(2) the "xy^i trick" (to make a few random elements look like more),
(3) character bounds,
(4) spectral gaps for Schreier graphs.

The trivial diameter bound is used on suitable Schreier graphs, e.g., the Schreier graph for S_n acting on 3-cycles by conjugation. Here we rely on the fact that the symmetric group has comparatively small conjugacy classes. The random commutator argument is based on the observation that two elements of S_n of small support tend to have commutators of even smaller support. Neither of these facts seems to have a useful analogue for classical groups.

The "xy^i" trick is the idea that, if x and y are independent uniform random elements of a group G, the elements xy^i $(0 \leq i < L)$ behave in some ways like many independent uniform elements. Obviously this is not strictly true, but it is true that each element xy^i is uniformly distributed, and if we can show that the elements xy^i and xy^j are pairwise approximately uniform with respect to suitable events then we may be able to use the second moment method. This idea was first proposed by Babai–Beals–Seress [1] and implemented by Babai–Hayes [2].

The "xw trick" is more general, and also useful for classical groups. The idea is that if we have even more generators, say $k + 1$ generators $x_0, \ldots, x_k$, then we can consider not only the words $x_0x_1^i$ by also the words $x_0w(x_1,\dots,x_k)$ for any word w in k letters. If $k \ge 2$ we have exponentially words w, so this trick is exponentially more powerful. Here is a precise statement, based on characters. Let G be a finite group. Let $\mathcal{C} \subset G$ be a normal subset of density $\delta = |\mathcal{C}|/|G|$. Let $x_0 \in G$ be uniformly random and let $x_1,\dots,x_k \in G$ be fixed. Let $B_k(L) \subset F_k$ be the ball of radius L in the free group F_k. Let

$$E = \bigcap_{w \in B_k(L)} \{x_0w(x_1,\dots,x_k) \notin \mathcal{C}\}$$

be the event that $x_0w(x_1,\dots,x_k)$ fails to be in $\mathcal{C}$ for every word w of length at most L. Then

$$\operatorname{Prob}(E) \le \frac{1}{\delta|B_k(L)|} + \delta^{-1} \max_{\substack{1\ne\chi\in\operatorname{Irr}(G)\\ 1\ne w\in B_k(2L)}} \frac{|\chi(w(x_1,\dots,x_k))|}{\chi(1)}.$$

The message is that if we want to show that some $x_0w(x_1,\dots,x_k)$ lies in $\mathcal{C}$ with high probability, it suffices to (a) choose k and L so that $|B_k(L)|$ (which is $2L+1$ if $k=1$, and $\approx (k-1)^L$ if $k>1$) is much larger than δ^{-1}, and (b) bound character ratios $\chi(w)/\chi(1)$.

Now let us consider bounding character ratios $\chi(w)/\chi(1)$. Here w is a fixed word in k variables $x_1,\dots,x_k$ of length at most L, and ideally we wish to show that $|\chi(w)|/\chi(1)$ is very small with high probability. The character bound of Larsen and Shalev [12] states that, for $\chi \in \operatorname{Irr}(S_n)$,

$$|\chi(\sigma)| \le \chi(1)^{1-\frac{\log(n/f)}{2\log n}+o(1)},$$

where $f = \max(\operatorname{fix}(\sigma),1)$. For classical groups we rely on recent technology of Guralnick, Larsen, and Tiep [8]. For $g \in \mathrm{GL}_n(q)$, let $\operatorname{supp}(g)$ denote the minimum rank of $g-\lambda$ as λ ranges over the algebraic closure of $\mathbf{F}_q$. Then the GLT character bound implies that there exists $\delta > 0$ such that if $g \in G = \mathrm{SL}_n(q)$ (or another classical group) and $|\operatorname{supp}(g)| \ge (1-\delta)n$ then

$$|\chi(g)| \le \chi(1)^{1/2}.$$

for any irreducible character χ of G.

To apply these character bounds, we need to know that short words in random generators never have small support. To this end the following tail bounds are proved in this course.

(1) Let $G = S_n$ and $1 \ne w \in B_k(L)$. Let $x_1,\dots,x_k \in G$ be uniformly random. Then

$$\operatorname{Prob}(\operatorname{supp}(w(x_1,\dots,x_k)) \le n-f) \le 2\exp(-cf/L^2).$$

(2) Let $G = \mathrm{SL}_n(q)$ and $1 \ne w \in B_k(L)$. Let $x_1,\dots,x_k \in G$ be uniformly random. Let $\delta > 0$. Assume that $L < \delta^2 n/20$. Then

$$\operatorname{Prob}(\operatorname{supp}(w(x_1,\dots,x_k)) \le n-\delta n) \le 2q^{-c\delta^2n^2/L}.$$

Finally, all being well, the outcome of the above arguments is some element $g \in G$ of minimal support (or minimal degree, for a classical group) and of short length in the generators. To finish we use the fact that the Schreier graph defined by conjugation on 3-cycles (for A_n) or transvections (for SL) is actually an expander graph. For the symmetric group with two random generators this is a result of Friedman–Joux–Roichman–Stern–Tillich (1996) [6]. For classical groups, it turns out a similar argument works, but we must assume that the number of random generators is at least q^C for a certain constant C. This argument is sketched in the final lecture of this course. (Another approach for classical groups altogether is based on the "combinatorics of transvections": we do not have time to cover this unfortunately.)

We end by describing some related open problems.

(Q1) What is the length of the shortest "approximate law" on S_n? Here an *approximate law* is a word $w \in F_2$ such that $w(x, y) = 1$ for 99% of all pairs $x, y \in S_n$. The bound (1) above with $f = n$ shows that an approximate law must have length at least $cn^{1/2}$ for some $c > 0$. I can prove an upper bound of $n^{3+o(1)}$.

(Q2) What is the length of the shortest approximate law on $\mathrm{SL}_n(2)$? To put it in a particularly provocative way, is there an approximate law of length $\leq 10n$?

(Q3) Let $\Gamma_k(q)$ denote the Schreier graph of $G = \mathrm{SL}_n(q)$ acting on $\mathbf{F}_q^n \setminus \{0\}$ with k random generators $x_1, \ldots, x_k \in G$. In these lectures we sketch the proof that $\Gamma_k(2)$ is an expander with high probability provided $k \geq 32$. Show that $\Gamma_2(2)$ is an expander with high probability.

References

[1] Babai, L., Beals, R. & Seress, Á. On the diameter of the symmetric group: polynomial bounds. *Proceedings Of The Fifteenth Annual ACM-SIAM Symposium On Discrete Algorithms*. pp. 1108-1112 (2004)

[2] Babai, L. & Hayes, T. Near-independence of permutations and an almost sure polynomial bound on the diameter of the symmetric group. *Proceedings Of The Sixteenth Annual ACM-SIAM Symposium On Discrete Algorithms*. pp. 1057–1066 (2005)

[3] Bamberg, J., Gill, N., Hayes, T., Helfgott, H., Seress, Á. & Spiga, P. Bounds on the diameter of Cayley graphs of the symmetric group. *J. Algebraic Combin.*. **40**, 1–22 (2014)

[4] Eberhard, S. Diameter of classical groups generated by transvections. *ArXiv E-prints*. pp. earXiv:2308.07086 (2023,8)

[5] Eberhard, S. & Jezernik, U. Babai's conjecture for high-rank classical groups with random generators. *Invent. Math.*. **227**, 149–210 (2022)

[6] Friedman, J., Joux, A., Roichman, Y., Stern, J. & Tillich, J. The action of a few random permutations on r-tuples and an application to cryptography. *STACS 96 (Grenoble, 1996)*. **1046** pp. 375–386 (1996)

[7] Garonzi, M., Halasi, Z. & Somlai, G. On the diameter of Cayley graphs of classical groups with generating sets containing a transvection. *Israel Journal Of Mathematics*. (2024,4)

[8] Guralnick, R., Larsen, M. & Tiep, P. Character levels and character bounds for finite classical groups. *Invent. Math.*. **235**, 151–210 (2024)

[9] Halasi, Z. Diameter of Cayley graphs of $SL(n, p)$ with generating sets containing a transvection. *J. Algebra*. **569** pp. 195–219 (2021)

[10] Helfgott, H. & Seress, Á. On the diameter of permutation groups. *Ann. Of Math. (2)*. **179**, 611–658 (2014)

[11] Helfgott, H., Seress, Á. & Zuk, A. Random generators of the symmetric group: diameter, mixing time and spectral gap. *J. Algebra.* **421** pp. 349–368 (2015)
[12] Larsen, M. & Shalev, A. Characters of symmetric groups: sharp bounds and applications. *Invent. Math..* **174**, 645–687 (2008)
[13] Schlage-Puchta, J. Applications of character estimates to statistical problems for the symmetric group. *Combinatorica.* **32**, 309–323 (2012)

The group large sieve method and Hilbert's irreducibility theorem

Daniele Garzoni
(joint work with Lior Bary-Soroker)

Let $f(t_1, \dots, t_r, X) \in \mathbf{Q}[t_1, \dots, t_r, X]$ be irreducible. Hilbert's irreducibility theorem (HIT), proved by Hilbert in 1892, asserts that there exist $\underline{t_1}, \dots, \underline{t_r} \in \mathbf{Q}$ such that $f(\underline{t_1}, \dots, \underline{t_r}, X) \in \mathbf{Q}[X]$ is irreducible. In words, we can specialize the variables $t_1, \dots, t_r$ to rational numbers, preserving irreducibility. In fact, we can also find specializations that preserve the Galois group, which is to say, such that the Galois group of $f(\underline{t_1}, \dots, \underline{t_r}, X)$ over $\mathbf{Q}$ is isomorphic to the Galois group of $f(t_1, \dots, t_r, X)$ over $\mathbf{Q}(t_1, \dots, t_r)$.

HIT has had various applications, notably to the inverse Galois problem. Indeed, given HIT, in order to realize a group as Galois group over $\mathbf{Q}$, it is sufficient to realize it over $\mathbf{Q}(t_1, \dots, t_r)$, which is a more tractable problem that can be attacked with geometric methods.

Indeed, the connection of HIT with geometry is apparent and very fruitful: We can view f as a cover π of finite degree of the affine space $\mathbb{A}^n$ over $\mathbf{Q}$, and we are asking for rational points $\underline{t} = (\underline{t_1}, \dots, \underline{t_r}) \in \mathbb{A}^n(\mathbf{Q})$ such that the fiber $\pi^{-1}(\underline{t})$ is irreducible.

When HIT is stated in this way, the generalization to arbitrary algebraic varieties is inescapable. A variety V over a field K is said to have the *Hilbert Property* (HP) if it satisfies a suitable analogue of HIT, where $\mathbb{A}^n$ is replaced by V and $\mathbf{Q}$ by K. (In fact, the precise definition involves a finite number of covers $\pi_1, \dots, \pi_t$, and we are seeking points having irreducible fibers in each π_i.)

It is then an important problem to understand which varieties have HP. One of the main motivations is the following conjecture of Colliot-Thélène: Every unirational variety over $\mathbf{Q}$ has HP. If this were true, then the Inverse Galois Problem would have a positive solution.

One of the main examples of varieties (over $\mathbf{Q}$, say) having the HP are connected linear algebraic groups. This was proved by Sansuc [13].

Abelian varieties fail to have HP for an "obvious" reason, namely, because they admit isogenies. (In fact, this is obvious only if we are aware of the Mordell–Weyl theorem.) What if we exclude isogenies to begin with? Slightly more precisely, we only seek points with irreducible fibers under ramified covers. One defines the so-called *Weak Hilbert Property* (WHP) accordingly. This point of view, pioneered by Zannier [14] and Corvaja–Zannier [5] (though apparent also in earlier work of Dèbes [6]), has been subject of intense research in recent years.

If we restrict to ramified covers, then abelian varieties behave nicely (see [4]). What is more, one can obtain much stronger statements even for varieties having the usual HP, such as linear algebraic groups.

For example, a theorem of Corvaja [3] and Liu [9] asserts the following: If G is a connected linear algebraic group over $\mathbf{Q}$, Γ is a finitely generated Zariski dense subgroup of $G(\mathbf{Q})$ and $\pi\colon V \to G$ is a finite ramified cover of G, then there exists a coset C of a finite-index subgroup of Γ such that the fiber $\pi^{-1}(g)$ is irreducible for every $g \in C$. In particular, we can find "many" points of Γ with irreducible fiber. This fails if π is allowed to be an isogeny.

In joint work with Lior Bary-Soroker [1], we made this quantitative, showing that "almost all" points of Γ have irreducible fiber. We achieved this using random walks. Specifically, with notation as in the previous paragraph, we showed that, provided $G/\mathrm{R}_u(G)$ is trivial or semisimple, if we perform a random walk on any Cayley graph of Γ (with respect to a finite generating set), then almost surely we will only hit points whose fiber is irreducible. In fact, we also allow Γ to be an arithmetic group in positive characteristic, which is a setting of intrinsic interest in this context.

This way of counting is motivated and inspired by work of Rivin [12], Lubotzky–Meiri [10], Lubotzky–Rosenzweig [11], Jouve–Kowalski–Zywina [7]. Indeed, work by Jouve–Kowalski–Zywina on the characteristic polynomial of random elements of Γ can be seen as a special cases of the above result. Also, the case where G is semisimple and simply connected was addressed already by Kowalski [8].

The assumption that $G/\mathrm{R}_u(G)$ is trivial or semisimple is used crucially in the proof, as we will briefly explain below. In particular, groups such as tori or general linear groups are excluded by our analysis, though the statement could (and should) be true in these cases as well. There is some recent progress on tori, see [2].

The method of proof uses the so-called *group large sieve method*. This is motivated by the classical large sieve of analytic number theory. In the context of groups it was used by Rivin, and developed by Kowalski and Lubotzky–Meiri. We are given a finitely generated group Γ and a subset Z of Γ, and we want to show that Z is "small". Here we define "small" in the following way: If we fix a finite generating set of Γ and we perform a random walk on the corresponding Cayley graph, then at the n-th step the probability that we hit elements of Z decays to zero as $n \to \infty$, preferably exponentially fast. The large sieve gives conditions on Γ (more precisely, on a certain sequence of finite quotients of Γ) that ensure this conclusion.

This method has been applied in a variety of problems [7, 10, 11]. The main examples of groups Γ satisfying the assumptions of the large sieve come from arithmetic: They are Zariski dense subgroups of semisimple simply connected linear algebraic groups over number fields. Here deep theorems, such as the *strong approximation theorem* and the *superstrong approximation theorem*, play a crucial role. (Strong approximation is really the reason why in [1] we require that $G/\mathrm{R}_u(G)$ be semisimple. The fact that it might not be simply connected can be amended via a geometric argument involving ramification. Moreover, in the aforementioned [2], we somehow remedy the failure of strong approximation for tori by invoking the Generalized Riemann Hypothesis.)

It is fair to say that these are essentially the only examples of groups to which the large sieve has been applied. In certain problems one can start with more general situations and reduce the problems to such groups (for example the so-called *Lubotzky's alternative* serves for this purpose).

In all previous applications of the large sieve, it has always been assumed that the aforementioned finite quotients of Γ be uniform expanders. However, it is not hard to remove this assumption, in order to make it amenable to more general contexts (notably, to arithmetic groups in positive characteristic), see [1]. There is a price to pay: One gets a decay in n which is polynomial rather than exponential (and this is really the best one can hope for.)

Further relaxations of the large sieve are easily obtained. For example, it has always been required that the finite quotients grow polynomially in size. One can remove this assumption, at the expense of getting some slower decay in n in the conclusion. Giving up on this condition is potentially very useful, as there are many groups satisfying the assumptions of the "relaxed" large sieve which do not come from arithmetic, so that applications in these novel contexts are possible.

References

[1] L. Bary-Soroker, D. Garzoni. *Hilbert's irreducibility theorem via random walks*, Int. Math. Res. Not. **2023** (2023), 12512–12537.

[2] L. Bary-Soroker, D. Garzoni., V. Matei, *On the irreducibility of $f(2^n, 3^m, X)$ and other such polynomials*, arXiv:2405.04058.

[3] P. Corvaja, *Rational fixed points for linear group actions* Ann. Sc. Norm. Super. Pisa Cl. Sc. **6** (2007), 561-597.

[4] P. Corvaja, J.L. Demeio, A. Javanpeykar, D. Lombardo, U. Zannier *On the distribution of rational points on ramified covers of abelian varieties*, Compos. Math. **158** (2022), 2109–2155.

[5] P. Corvaja, U. Zannier. *On the Hilbert property and the fundamental group of algebraic varieties*, Math. Z. **286** (2017), 579–602.

[6] P. Dèbes, *On the irreducibility of the polynomials $P(t^m, Y)$*, J. Number Theory **42** (1993) 141–157.

[7] F. Jouve, E. Kowalski, D. Zywina, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, Israel J. Math. **193** (2013), 263–307.

[8] E. Kowalski, *Sieve in expansion*, Sèminaire Bourbaki (2010).

[9] F. Liu, *On Hilbert's irreducibility theorem for linear algebraic groups*, Ann. Sc. Norm. Super. Pisa Cl. Sc. (2022), 1053-1089.

[10] A. Lubotzky, C. Meiri, *Sieve methods in group theory I: Powers in linear groups*, J. Amer. Math. Soc. **25** (2012), 1119–1148.

[11] A. Lubotzky, L. Rosenzweig, *The Galois group of random elements of linear groups*, Amer. J. Math. **136** (2014), 1347–1383.

[12] I. Rivin, *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. **142** (2008), 353–379.

[13] J.J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. Reine Angew. Math. **327** (1981), 12–80.

[14] U. Zannier, *Hilbert irreducibility above algebraic groups*, Duke Math. J. **153** (2010), 397–425.

Strategies for growth in permutation groups

Harald Andrés Helfgott

Consider the question of bounding the diameter of any Cayley graph $\Gamma(G, A)$ of a finite, simple, non-abelian group G. Here $A \subset G$ is any set generating G, and the diameter is just the smallest k such that every element of G can be written as a product $a_1 a_2 \cdots a_\ell$, $\ell \leq k$, $a_i \in A \cup A^{-1}$, where $A^{-1} = \{g^{-1} : g \in A\}$.

In the case of linear algebraic groups G, the dependence of bounds on the rank r of G was very poor until recently. Now it is exponential on r: for $G < \mathrm{GL}_N$ an untwisted classical group over a field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) > N$, and any subset $A \subset G(\mathbb{F})$ that generates $G(\mathbb{F})$,

$$\text{(1)} \qquad \mathrm{diam}(\Gamma(G(\mathbb{F}), A)) \leq (\log |G(\mathbb{F})|)^{O(r^4)} \qquad \text{(see [1], [3]).}$$

The technical assumptions here (untwisted group, high characteristic, etc.) are made mainly for simplicity; no doubt they will be removed eventually. What is more interesting is to compare this bound with what is believed to hold for all finite, simple, non-abelian groups G (Babai's conjecture: $\mathrm{diam}(\Gamma(G, A)) \ll (\log |G|)^{O(1)}$) and above all with what is already known for the alternating group Alt_n: for $G = \mathrm{Alt}_n$ and any set $A \subset G$ generating G,

$$\text{(2)} \qquad \mathrm{diam}(\Gamma(G, A)) \leq (\log |G|)^{O((\log n)^3 \log \log n)} \qquad \text{(see [5])}$$

Here n (or rather $n-1$) should be seen analogous to the rank r. In other words, we should aim at an improvement on (1) with $\log r$ in place of r; only then would we have a true analogue to (2).

One immediate objection (by those in the know) is that results such as (1) were originally corollaries of "product theorems" of the following kind:

$$\text{(3)} \qquad |A^3| \geq |A|^{1+\delta} \qquad \text{for } A \subset G \text{ generating } G$$

(where $A^k := \{a_1 a_2 \cdots a_k : a_1, \ldots, a_k\}$ and $|S|$ denotes the number of elements of a set S) and that it is known that such a theorem cannot hold in general with δ larger than $1/n$ or so, by a counterexample due to Pyber. However, exactly the same is true in Alt_n, and yet this was not a major obstacle to the proof of (2).

Our goal in this Oberwolfach minicourse was to go in detail over a newer proof of (2) – essentially as in [4], but streamlining the proof as much as possible, while keeping in mind some questions. How can Sym_n and Alt_n serve as a model for SL_n? What ideas from the proof may carry over to linear algebraic groups? What notions from existing proofs for permutation groups and linear algebraic groups can be put in a common framework?

1. There are some basic lemmas on growth that we can use whether we study linear algebraic groups or permutation groups, or any other group: growth in a subgroup implies growth in the group (by about the same factor), growth in a quotient implies growth in the group, etc. Many of them rest on an easy generalization of the orbit-stabilizer theorem (a result on actions familiar from any first course in group theory) to sets and their orbits (in place of subgroups and their orbits). The basic idea here can be applied elsewhere, in different ways, whether we speak

of SL_n or Alt_n: basic results in group theory whose proofs have a concrete or algorithmic flavor can often have their proofs "relaxed" so as to make the results to hold for arbitrary subsets A of a group G, rather than just for subgroups of G. (Typically, some instances of A are replaced by powers A^k, and some equalities become bounds.)

2. An idea that is productive both for linear algebraic groups and for Alt_n (but in different ways) is that of *quasitransversality*. In the case of linear algebraic groups G, the meaning is very simple: given an irreducible proper subvariety $V \subset G$ of dimension > 0 and a set of generators A of $G(\mathbb{F})$, we can find $g \in A$ such that $gVg^{-1} \neq V$; we then study the varieties $\overline{VgVg^{-1}}$ (of dimension $> \dim(V)$) and $V \cap gVg^{-1}$ (of dimension $< \dim(V)$). In the case of permutation groups such as Alt_n, we can consider, instead of V, sets whose orbits (not necessarily for the most obvious action) are constrained in some sense. It is in this way that we can prove a relaxation of Babai's splitting lemma, for instance.

3. At least one further basic tool in the proof of 2 has an obvious analogue for linear algebraic groups $G(\mathbb{F})$: (pointwise) stabilizer chains

$$A > A_{(\alpha_1)} > A_{(\alpha_1,\alpha_2)} > \dots$$

correspond to chains of stabilizers of flags. The latter do not play a role in current proofs of results such as (1), though it is natural to guess that they ought to be helpful, at least for the growth of relatively large subsets A (say, $A > |\mathbb{F}|$); otherwise it is not a priori clear how to obtain even two distinct elements of $A \subset \mathrm{SL}_n(\mathbb{F})$ stabilizing the same point in $\mathbb{A}^n(\mathbb{F})$ (though see our later discussion on lower bounds of intersections of the form $AA^{-1} \cap C(g)$).

4. Stepping back a little: linear algebraic groups $G(\mathbb{F})$ and permutation groups such as Alt_n are defined in terms of actions – a geometrically meaningful action on affine space $\mathbb{A}^n(\mathbb{F})$), in one case, and an action on a small, unstructured set $[n] = \{1, 2, \dots, n\}$, in the other. The strategies followed to prove 1 and 2 always reflect this similarity and this distinction: the action of $G = \mathrm{SL}_n$ (say) on $\mathbb{A}^n$ and on itself gives rise to subvarieties of G, whereas the fact that $[n]$ is small compared to Alt_n implies immediately that a random walk on any Schreier graph for the action $\mathrm{Alt}_n \curvearrowright [n]$ has small mixing time, and so probabilistic arguments are possible and in fact extremely fruitful. Is there a way to use probabilistic arguments to prove results on growth in linear algebraic groups? Small mixing time will no longer come for free.

Here are some challenges. First of all, let us try to do more or less the opposite of a transfer of a proof for Alt_n to linear algebraic groups.

Problem 1. *Let $G = SL_n$ (say), $\mathbb{F}$ a finite field. Let $A \subset G(\mathbb{F})$ be a set generating $G(\mathbb{F})$. Assume A contains all permutation matrices. Prove a good bound on diam$(\Gamma(G(\mathbb{F}), A))$.* (Perhaps $\ll (\log |G(\mathbb{F})|)^{O(1)}$?)

We can of course assume just that A contains a couple of permutation matrices that generate $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$ (as subgroups of SL_n) and then apply (2).

Problem 2. *Let G be a linear algebraic group of rank r defined over a finite field $\mathbb{F}$. Let $g \in G(\mathbb{F})$ be a regular semisimple element. Let $A \subset G(\mathbb{F})$ be a set generating $G(\mathbb{F})$. Prove that*

$$|A \cap \mathrm{Cl}(g)| \leq C|A^k|^{1-\frac{r}{\dim G}}. \tag{4}$$

for C, k as small as possible. (Is $C, k = r^{O(1)}$ doable?)

Here $\mathrm{Cl}(g)$ is the conjugacy class of g in $G(\mathbb{F})$ (or in $G(\overline{\mathbb{F}})$, if you prefer). We currently know how to prove (4) with $C, k = O(r)^{O(r^2)}$. The proof does use the fact that $\mathrm{Cl}(g)$ is a conjugacy class and not some other variety; otherwise, the dependence of C on r would be worse – that is, it is in fact worse in the best available bounds for intersections $A \cap V$ of subsets $A \subset G(\overline{\mathbb{F}})$ with arbitrary varieties V [2]. The motivation is that results of the form (4) are crucial in proofs of diameter bounds, product theorems, etc.: by the (relaxed) orbit-stabilizer theorem, (4) implies immediately a lower bound on the intersection $|AA^{-1} \cap C(g)|$, where $C(g)$ is the centralizer of g.

Let us conclude by pointing out that there are tools that are not currently being used in the proofs of results such as the above and probably should be. For instance - can character theory be used to address Problem 2? It also seems reasonable to venture that buildings ought to play a role in better bounds on growth and diameter in linear algebraic groups.

References

[1] J. Bajpai, D. Dona, H. A. Helfgott, *Growth estimates and diameter bounds for classical Chevalley groups*, preprint, https://arxiv.org/abs/2110.02942.

[2] J. Bajpai, D. Dona, H. A. Helfgott, *New dimensional estimates for subvarieties of linear algebraic groups*, Vietnam J. of Math. **52** (2024), 479–518.

[3] J. Bajpai, D. Dona, H. A. Helfgott, *Growth estimates and diameter bounds for untwisted classical groups*, in preparation.

[4] H. A. Helfgott, *Growth in linear algebraic groups and permutation groups: towards a unified perspective*, in: Groups St. Andrews 2017 in Birmingham. Selected papers of the conference, Birmingham, UK, August 5–13, 2017, Cambridge University Press, 2019.

[5] H. A. Helfgott, Á. Seress, *On the diameter of permutation groups*, Ann. of Math. **179** (2014), no. 2, 611–658.

Kazhdan Property T, Kazhdan constants and expansion in finite groups

Martin Kassabov

In this minicourse I will introduce Kazhdan property T and go over several methods for proving that a group has property T, which produce estimates for the relevant Kazhdan constants. Even though property T comes from representation theory and computing the Kazhdan constants requires deep understanding of all unitary representations of a group, it is possible to obtain surprisingly good estimates almost without any representation theory of "large groups". As an application I will go over several constructions of expanding generating sets in finite simple groups.

The outline of the minicourse is as follows.

1) Kazhdan Property T and
2) Dependance of Kazhdan constants on generating sets
3) Estimate of Kazhdan constants for $\mathrm{SL}_n(\mathbb{Z})$
4) Construction of expanding generating sets in finite simple groups of unbounded rank
5) Construction of expanding generating sets in alternating groups

Polynomial Bogolyubov in finite simple groups of Lie type

Noam Lifshitz
(joint work with Shai Evra, Guy Kindler, Nathan Linzey)

A well known open problem in additive combinatorics concerns showing that if $A \subseteq \mathbb{F}_p^n$, then $2A - 2A$ contains an affine subspace of codimension $O_p(\log(1/\alpha))$. Such a result is known as a polynomial Bogolyubov result because the density of the subspace $\frac{|H|}{p^n}$ is polynomial in the density $\frac{|A|}{p^n}$ of A. In the talk we discuss a nonabelian analogue for finite simple groups. We show that In my joint work with Evra, Kindler, and Lindzey [2] we show that if G is a finite simple group of Lie type, then $AA^{-1}AA^{-1}$ contains a subgroup whose density is polynomial in the density of A. Our work builds upon previous works due to Evra, Kindler, and Lifshitz [1] for special linear groups, Keevash–Lifshitz [3] for alternating groups, and the bounded rank case due to Nikolov and Pyber [5].

We present an approach based on the theory of Boolean functions. The study of the Boolean cube was initiated by Kahn, Kalai, and Linial [4] in 1988 and the theory that they developed has found remarkable applications across various domains. One of the central tools in the study of the Boolean cube is the hypercontractivity theorem of Bonami, Gross, and Beckner. For a function on the Boolean cube $\{-1,1\}^n$, its L_p-norms are given by

$$\|f\|_p^p = \mathbb{E}_{x\sim\{-1,1\}^n}[|f(x)|^p]$$

Bonami's lemma which is a well knon consequence of the hypercontractractivity theorem states that if f is a polynomial of degree $\leq d$ on the Boolean cube, and $r > 2$ then $\|f\|_r \leq \sqrt{r-1}\|f\|_2$. Kahn, Kalai and Linial used Bonami's lemma to prove their so called 'level d inequality'. Every function $f\colon \{-1,1\}^n \to \mathbb{R}$ has a Fourier expansion $f = \sum_{S\subseteq[n]} \hat{f}(S)\chi_S$, where $\chi_S = \prod_{i\in S} x_i$. The level d inequality states that if $f\colon \{-1,1\}^n \to \{0,1\}$ is the indicator of a set of density $\alpha \leq 1/2$, then $\sum_{|S|=d} |\hat{f}(S)|^2 \leq \alpha^2 \log^d(1/\alpha)$. When α is small, this is almost a quadratic improvement over the trivial L_2 bound, which states that the sum of the squares of the Fourier coefficients is $\|f\|_2^2 = \alpha$. It turns out that the KKL theorem has a representation theoretic interpretation. The hyperoctahedral group $S_n \rtimes \mathbb{Z}/2\mathbb{Z})^n$ acts on the Boolean cube and the spaces $\mathrm{span}\{\chi_S\}_{|S|=d}$ are the irreducible consituents of the module of real valued functions on the Boolean cube. The KKL theorem can then be reinterpreted as stating that most of the Fourier mass of a Boolean function is concentrated on the high dimensional representations.

The more classical approach of Sarnak–Xue, Gowers, and Nikolov–Pyber relies on the minimal dimension of an irreducible representation to obtain rowth results. When trying to adapt this approach to the high rank regime it fails due to the existence of low dimensional representations. We overcome this by proving level-d type inequalities showing that the Fourier mass of $\{0,1\}$-valued functions on finite simple groups are concentrated on the high dimensional representations.

References

[1] S. Evra, G. Kindler N. Lifshitz, *Polynomial Bogolyubov for special linear groups via tensor rank*, arXiv preprint arXiv:2404.00641 (2024).

[2] S. Evra, G. Kindler N. Lifshitz, N. Linzey *Polynomial Bogolyubov for finite classical groups*, in preparation.

[3] P. Keevash, N. Lifshitz *Sharp hypercontractivity for symmetric groups*, arXiv preprint arXiv:2307.15030 (2024)

[4] J. Kahn, G. Kalai, N. Linial *Proceedings of the 29th Annual Symposium on Foundations of Computer Science* Proceedings of the 29th Annual Symposium on Foundations of Computer Science (1988)

[5] N. Nikolov, L. Pyber *Product decompositions of quasirandom groups and a Jordan type theorem* Journal of the European Mathematical Society, (2011)

On property (T) for Aut(F_n)

Martin Nitsche

Ten years ago, Ozawa (cf. [6]) proposed a new method to prove property (T) for a given finitely generated group Γ. The centerpiece of this method is to decompose a certain element $\Delta \in \mathbb{R}[\Gamma]$ of the group algebra into a sum of squares, a task that can be formulated as an optimization problem and solved with the computer (see [3]). The most important application of this method, to date, is the proof that the automorphism groups of the free groups, $\mathrm{Aut}(F_n)$, have property (T) for $n \geq 4$ ([2, 1, 4]).

The main goal of this talk was to reinterpret Ozawa's method in a more geometrical way. The starting point for this is the following theorem of Shalom.

Theorem 1 (Shalom). *A finitely generated group Γ has property (T) exactly if its reduced cohomology $\bar{\mathrm{H}}^1(\Gamma,\pi)$ is trivial for any unitary representation π, i.e. if Γ does not allow any non-trivial harmonic 1-cocycle.*

If we fix a finite symmetric generating set $S = S^{-1}$ for Γ, then a non-trivial harmonic 1-cocycle (for some unitary representation π) is a map $c\colon \Gamma \to \mathcal{H}$ of Γ into some Hilbert space, such that

(1) $\|c(\gamma_1)-c(\gamma_2)\| = \|c(\gamma\gamma_1)-c(\gamma\gamma_2)\|$ for all $\gamma,\gamma_1,\gamma_2 \in \Gamma$ (cocycle condition)
(2) the "curvature" $\kappa(c) := \left\|c(\mathbf{1}) - 1/|S| \cdot \sum_{s\in S} c(s)\right\|^2$ is 0
(3) $c \neq 0$, we can assume that c is scaled such that $\sum_{s\in S} \|c(s)-c(\mathbf{1})\|^2 = 1$

To prove property (T) for a group Γ, one has to show that any non-trivial cocycle on Γ must have positive curvature. The key point now is that it suffices to look at partial cocycles $c_T\colon T \to \mathcal{H}$ that are defined only on a finite subset $T \subset \Gamma$. If one could find a partial harmonic cocycle for every finite subset T, one could obtain a full harmonic cocycle as a limit.

Since T is finite, the task of finding a lower bound for the curvature of a partial cocycle, under the constraints of Conditions 1 and 3, can be given to the computer. We get the following result (see [4]).

Theorem 2. *Let Γ be a finitely generated group with solvable word problem. If Γ has no non-trivial harmonic cocycles, the computer can (theoretically) always prove it by bounding the curvature of partially defined cocycles from below.*

The optimization problem of providing a lower bound for the curvature of a partially defined cocycle is equivalent to the optimization problem introduced by Ozawa and Netzer–Thom for proving property (T).

Unfortunately, the computer proofs for property (T) allow little insight into what makes them succeed for a particular group. But for $\Gamma = \mathrm{Aut}(F_n)$, if one allows n to be very big, one can also lead Conditions 1,2,3 to a contradiction by a purely human argument (see [5]). In the second part of the talk I sketched an example for how letting $n \to \infty$ can be exploited in such an argument.

References

[1] M. Kaluba, D. Kielak, and P. Nowak, *On property (T) for* $\mathrm{Aut}(F_n)$ *and* $\mathrm{SL}_n(\mathbb{Z})$, Ann. of Math. **193** (2021), 539–562.

[2] M. Kaluba, P. Nowak, and N. Ozawa, $\mathrm{Aut}(\mathbb{F}_5)$ *has property* (T), Math. Ann. **375** (2019), 1169–1191.

[3] T. Netzer and A. Thom, *Kazhdan's property (T) via semidefinite optimization*, Exp. Math. **24** (2015, 371–374.

[4] M. Nitsche, *Computer proofs for property (T), and SDP duality*, preprint.

[5] M. Nitsche, *A human property (T) proof for high-rank* $\mathrm{Aut}(F_n)$, preprint.

[6] N. Ozawa, *Noncommutative real algebraic geometry of Kazhdan's property* (T), J. Inst. Math. Jussieu **15** (2016), 85–90.

From Cayley graphs to Schreier graphs

Luca Sabatini

(joint work with Daniele Dona)

Let G be a finite group acting transitively on the set Ω, and let $S \subseteq G$. The Schreier graph $\Gamma = Sch(G \circlearrowleft \Omega, S)$ is the graph with vertex set $V(\Gamma) = \Omega$, and the edges are the pairs (ω, ω^s) for every $\omega \in \Omega$ and $s \in S$. This is a natural generalization of Cayley graphs, which arise when G is a regular permutation group on Ω. The general setting is much wilder, as there is no natural action of G on $V(\Gamma)$ that preserves the graph structure. For example, it is well known that every regular graph of even degree is a Schreier graph over $Sym(\Omega)$ [6].

In this seminar, we will discuss about the diameter of random Schreier graphs, where by random we mean that the action of G on Ω is fixed, and a set $S \subseteq G$ of size k is chosen uniformly at random. The value of k is allowed to depend on the size of Ω, which in turn is going to infinity (as well as the size of G). Of course, the results that we obtain depend on the particular group G and action, and on how large k is with respect to the cardinalities of G and Ω. For particularly "nice" actions, very strong results were obtained in [5, 4]. For example, for $Sym(\Omega)$ in its natural action, and for any fixed $k \geq 2$, the symmetrization of the resulting Schreier graph is a $2k$-regular expander graph with high probability. The situation turns out to be very different for a generic "bad" action: even just to obtain a connected graph, it is necessary for k to grow with the size of Ω. For instance, in the case of a Cayley graph, k has to be at least the minimal number of generators of G. In 1996, Roichman [7] proved the following theorem concerning the diameter of random Cayley graphs.

Theorem 1 (Roichman)**.** *Fix $\varepsilon > 0$, and let G be any group of cardinality n. Let $k = \lfloor (\log n)^{1+\varepsilon} \rfloor$, and let $S \subseteq G$ be a random multiset of k elements. Then*

$$\operatorname{diam}(\, Cay(G,S)\,) \;\leq\; \frac{2}{\varepsilon}\,\frac{\log n}{\log k}$$

with high probability.

Theorem 1 is sharp in three ways. First, it is clear that a bound of the type $O(\log_k n)$ is the best possible for the diameter of k-regular graph of size n. Second, it is not hard to see ([7, Proposition 5.7]) that, for an abelian group of order n, $(\log n)^{1+\varepsilon}$ elements are required to get such a bound $O(\log_k n)$. Third, even the constant $\frac{2}{\varepsilon}$ is close to the best possible.

It is natural to ask what happens in the realm of Schreier graphs [9]. It is remarkable that Roichman obtains his theorem starting from results on the mixing time of random random walks (see also [3]). The proofs of such results use many distinguished properties of Cayley graphs, in particular their vertex-transitivity. It follows that these ideas cannot be used in the general framework. In a recent work with D. Dona [2], we provide a direct combinatorial proof of the following:

Theorem 2. *For every $\varepsilon > 0$ there exists C such that the following holds. Let Ω be a set of cardinality n, and let G be any finite group acting transitively on Ω. Let k be an integer such that $(\log n)^{1+\varepsilon} \leq k \leq n$, and let $A \subseteq G$ be a random multiset of k elements. Then*

$$\operatorname{diam}(\, \mathrm{Sch}(G \circlearrowleft \Omega, A)\,) \;\leq\; C\,\frac{\log n}{\log k}$$

with high probability.

Our proof is based on the more modern philosophy of *growth in groups*. It consists of two main steps, which we explain in the two Propositions below. For $\omega \in \Omega$, $S \subseteq G$, and $t \in \mathbb{N}$, we write $sph_S(\omega, t)$ to denote the sphere of radius t in $Sch(G \circlearrowleft \Omega, S)$ and centered in ω. Moreover, we write $S \sim \mu_G(k)$ to say that $S \subseteq G$ is a random multiset of size k chosen with the uniform distribution.

Proposition 3 (Initial growth)**.** *For every $\varepsilon > 0$ there exists $C > 0$ such that the following holds. Let G be a finite group acting transitively on a set Ω with $|\Omega| = n$,* *and let k be any integer such that $(\log n)^{1+\varepsilon} \leq k \leq n$. Fix $\omega \in \Omega$. Then, for $A \sim \mu_G(k)$, we have*

$$|sph_A(\omega, \lfloor C \log_k n \rfloor)| \geq \frac{n}{k^{\varepsilon/2}}$$

with high probability.

Once we have a large sphere around a fixed point, we bound the diameter with the help of a few more random elements.

Proposition 4 (Filling the set)**.** *Suppose that, for some $\omega \in \Omega$, for $A \sim \mu_G(k)$ we have $|\omega^{A^t}| \geq |\Omega|/k^{\delta}$ with high probability. Then, for $B \sim \mu_G(k + 4k^{\delta} \log n)$, we have*

$$diam(Sch(G \circlearrowleft \Omega, B)) \leq 2t + 2$$

with high probability.

To use Proposition 4 in a effective way, it is important to notice that k is comparable to $k + 4k^{\delta} \log n$, when k is larger than $(\log n)^{1+\varepsilon}$ and δ is small enough with respect to ε.

We conclude the seminar with another question related to the diameter of Cayley graphs. We remark that a positive answer to Question 5 would imply the famous Babai's conjecture.

Question 5. *Fix $c \in \mathbb{N}$, and let $G = \langle S \rangle$ be a finite group. Suppose that $|S| \leq c$ and $diam(G, S) \leq (\log |G|)^c$. Does there exist $c'(c)$ such that $diam_{worst}(G) \leq (\log |G|)^{c'}$?*

Essentially, we are asking if polylogarithmic diameter is a group property. For comparison, it has been proved by Breuillard and Tointon [1] (see also [8]) that if $G = \langle S \rangle$ and $diam(G, S) \geq |G|^{\varepsilon}$ for some $\varepsilon > 0$, then $diam(G, S') \geq |G|^{\varepsilon'(\varepsilon, |S|)/|S'|}$ for every $S' \subseteq G$.

References

[1] E. Breuillard, M. Tointon, *Nilprogressions and groups with moderate growth*, Advances in Mathematics **289** (2016), 1008–1055.

[2] D. Dona, L. Sabatini, *The diameter of random Schreier graphs*, in preparation.

[3] C. Dou, M. Hildebrand, *Enumeration and random random walks on finite groups*, Annals of Probability **24(2)** (1996), 987–1000.

[4] S. Eberhard, U. Jezernik, *Babai's conjecture for high-rank classical groups with random generators*, Inventiones Mathematicae **227** (2022), 149–210.

[5] J. Friedman, A. Joux, Y. Roichman, J. Stern, J.P. Tillich, *The action of a few permutations on r-tuples is quickly transitive*, Random Structures and Algorithms **12(4)** (1998), 335–350.

[6] J.L. Gross, *Every connected regular graph of even degree is a Schreier coset graph*, Journal of Combinatorial Theory (B) **22** (1977), 227–232.

[7] Y. Roichman, *On random random walks*, Annals of Probability **24(2)** (1996), 1001–1011.

[8] L. Sabatini, *On finite groups with polynomial diameter*, https://arxiv.org/abs/2106.13577 (2021).

[9] L. Sabatini, *Random Schreier graphs and expanders*, Journal of Algebraic Combinatorics **56** (2022), 889–901.

Burnside groups of odd exponent and iterated small cancellation

Katrin Tent
(joint work with Agatha Atkarskaya, Eliyahu Rips)

Recall that a group G acts sharply n-transitively on a set X if for any two n-tuples $(x_1, \dots, x_n), (y_1, \dots, y_n)$ with $x_i \neq x_j, y_i \neq y_j, 1 \leq i \neq j \leq n$ there is a unique $g \in G$ such that $gx_i = y_i, i = 1, \dots n$.

For infinite groups it follows from results of Tits and Jordan that we have $n \leq 3$ and since for $n = 1$ any group can act regularly on itself, the cases to consider are $n = 2$ and 3.

It is easy to see that the set of involutions J in a sharply 2-transitive group is non-empty and forms a single conjugacy class. It follows that either involutions do not have fixed points or there is a G-equivariant bijection between the set of involutions and the underlying set X. In this case, the group G acts sharply 2-transitively on the set J and in particular, all translations, i.e. products of two distinct involutions, have the same order, either a prime p or infinite. Accordingly these groups are said to have characteristic p or 0. A long-standing conjecture stated that all sharply 2-transitive groups are of the form $K.K^*$ for some (near-)field K. In particular such groups contain a regular (and abelian) normal subgroup and are called *split*. For several classes of groups like e.g. finite groups, locally compact connected groups, groups having characteristic 3 and for subgroups of $GL(n, K)$ where $charK \neq 2$ the conjecture has been shown to hold by Zassenhaus, Tits, Kerby and Glasner-Gulko, respectively.

The first counterexamples were constructed by Rips, Segev and the speaker in [5]. In these examples, involutions have no fixed points and the set of translations does not necessarily form a conjugacy class. In a variant, this construction was extended in [7] to yield sharply 3-transitive groups in which the sharply 2-transitive point stabilizers are non-split (and their involutions have no fixed points). Then [6] presented the first examples of a group G acting sharply 2-transitively on the set of involutions. The construction proceeds via iterated HNN-extensions making translations conjugate. In this process translations are forced to have infinite order and in light of the result that sharply 2-transitive groups in characteristic 3 split, it is a particularly challenging problem to construct examples in positive characteristic.

In order to do so, one needs to take quotients of the HNN-extensions forcing translations to have a fixed finite order, much as is the case in the construction of free Burnside groups.

Recall that 1902, Burnside asked whether any finitely generated torsion group is finite. This has long been refuted, in particular by Adian and Novikov [1]. More precisely, Adian and Novikov show that the free Burnside group

$$B(n, m) = F_m / \langle\langle w^n : w \in F_m \rangle\rangle$$

is infinite for $m \geq 2$ and odd $n \geq 665$. However, the proof is based on a large number of induction assumptions and quite hard to follow. Shorter and more geometric proofs were obtained e.g. by Ol'shanski and Gromov at the expense of obtaining a very large lower bound for the exponent in order for the group to be infinite.

In order to construct sharply 2-transitive groups of positive characteristic, we needed a more managable approach. Hence we prove in [4]

Theorem: *The free Burnside group $B(n, m)$ is infinite for $m \geq 2$ and odd $n \geq 557$.*

The proof proceeds via iterated small cancellation theory, noting that for non-commuting reduced words $x, y \in F_m$ and any exponent $k \in \mathbb{N}$ the length of a common prefix of x^k, y^k is bounded in length by $|x| + |y|$. This yields a suitable small cancellation condition on power words, and hence on the relators for $B(n, m)$. Our proof proceeds roughly by ranking words in the free group by their nesting depth of power words, i.e. we fix a nesting constant $\tau = 15$ and put (roughly) $rk(x) = 1$ if $|x| = 1$. Then inductively we set $rk(x) \geq k + 1$ if x cyclically contains a subword u^τ with $rk(u) \geq k$.

Now let N_k denote the normal subgroup of F_m generated by x^n with $rk(x) \leq k$. Then $B(n, m) = F_m / \bigcup N_k$. Our proof proceeds by induction on the rank, constructing a section $can_k : F_m/N_k \longrightarrow F_m$. This section can_k thus defines for any element of F_m a *canonical form* of rank k, that is a canonical representative for its coset modulo N_k.

The idea is that we consider a word $w \in F_m$ which is already the canonical representative in rank $k - 1$. Now we decide for subwords of w of the form u^d with $rk(u) = k$ whether or not to turn them, i.e. to replace them by their complement in u^n. By the small cancellation condition for power words mentioned above the overlap between two different power subwords of the same rank is bounded by exponent $\tau + 1$. Hence we can bound the 'damage' that turning one such power subword creates on a neighbouring power subword.

If d is sufficiently small, we will never replace u^d and if d is sufficiently close to n we will always turn this occurrence. In all other cases, we use a *certification sequence* to decide whether or not to turn an occurrence. This ensures that we consider the whole word before making a turn which might have a ripple effect throughout the word.

Since words are finite strings, it is clear that the canonical forms stabilize for every word at some stage and this stage is defined as the canonical form of the given word. Also, by the size of the exponent, it is clear that words not containing cubic subwords are already in canonical form. The free Burnside group can now be considered as the collection of all canonical forms (with a suitable multiplication). Since there are infinitely many cube-free words in two generators, it follows that indeed the free Burnside groups $B(n, m)$ are infinite for odd $n \geq 557$ and $m \geq 2$.

We can now apply this to the construction of sharply 2-transitive groups in positive characteristic. Using results by Coulon, we already showed in [2] that sharply 2-transitive groups exist in all sufficiently large positive characteristics. However, the lower bound on the cahracteristic in these examples is extremely large and we thus expect to produce examples with a more reasonable lower bound on the characterstic using the methods from [4].

The existence of sharply 3-transitive groups with non-split point-stabilizers is still very much unresolved except for the examples in [7].

References

[1] S.I. Adian, P.S. Novikov, Infinite periodic groups. I–III, Izv. Akad. Nauk SSSR, Ser. Mat. 32(1–3), 212–244, 251–524, 709–731 (1968) [Math. USSR, Izv. 2, 209–236, 241–479, 665–685 (1968)]

[2] M. Amelio, S. André, K. Tent, Non-split sharply 2-transitive groups of odd positive characteristic, https://arxiv.org/pdf/2312.16992

[3] S. André, K. Tent, Simple sharply 2-transitive groups, Trans. AMS., Vol. 376, No 6, 3965–3993.

[4] A. Atkarskaya, E. Rips, K. Tent, The Burnside problem for odd exponent, https://arxiv.org/pdf/2303.15997

[5] Eliyahu Rips, Yoav Segev, Katrin Tent, A sharply 2-transitive group without a non-trivial abelian normal subgroup, J. Eur. Math. Soc. (JEMS) 19 (2017), no. 10, 2895–2910.

[6] Eliyahu Rips, Katrin Tent, Sharply 2-transitive groups in J. Reine Angew. Math. 750 (2019), 227–238. J. Reine Angew. Math. 750 (2019), 227–238.

[7] K. Tent, Sharply 3-transitive groups, Advances in Mathematics 286 (2016) 722–728.

[8] K. Tent, Infinite sharply multiply transitive groups. Jahresber. Dtsch. Math.-Ver. 118 (2016), no. 2, 75–85.

Character bounds for finite simple groups and applications

Pham Huu Tiep

In this minicourse, we discuss recent results, obtained in joint work of the speaker with various collaborators, on the following problem:

Problem 1. *Let G be a finite almost quasisimple group, $g \in G \smallsetminus Z(G)$.*

(A) *Find an explicit, and as small as possible, $0 < \gamma = \gamma(g) < 1$, such that*

$$\frac{|\chi(g)|}{\chi(1)} \leq \gamma, \ \forall \ \chi \in \mathrm{Irr}(G) \text{ with } \chi(1) > 1.$$

(B) *Find an explicit, and as small as possible, $0 < \alpha = \alpha(g) < 1$, such that*

$$|\chi(g)| \leq \chi(1)^{\alpha}, \ \forall \ \chi \in \mathrm{Irr}(G).$$

Results on Problem 1 will be useful for a number of applications, which usually involve using *Frobenius character formula*, and include

(i) *Ore conjecture* [17] and *Waring-type problems* [9, 13, 14] for finite simple groups;

(ii) Random generation of simple groups, and representation varieties $\mathrm{Hom}(\Gamma, G)$, where $G = \mathsf{S}_n$ or $G = \mathcal{G}(\mathcal{F})$ for a simple algebraic group $\mathcal{G}$, and Γ a Fuchsian group, see e.g. [20];

(iii) Random walks on Cayley graphs and McKay graphs [21, 22];

(iv) *Thompson conjecture* [11, Problem 9.24], [1]: *If G is a finite non-abelian simple group, then $G = C^2$ for some conjugacy class C of G.*

The most general result on Problem 1(A), which combines results of Gluck [5], Gluck and Magaard [6], and Guralnick and the author [10], says that one can take $\gamma = 79/80$, unless $E(G) = \mathsf{A}_n$. The first significant result on Problem 1(B) for *symmetric groups* was obtained by Fomin and Lulov [4]. It has been vastly generalized by Larsen and Shalev [12].

Our main focus will be on *finite classical groups* $G = \mathrm{Cl}(V)$, where $V = \mathbb{F}_q^n$. For any $g \in \mathrm{Cl}(V)$, the *support* $\mathsf{supp}(g)$ is defined to be.

$$\mathsf{supp}(g) = \inf_{\lambda \in \overline{\mathbb{F}_q}} \mathrm{codimKer}(g - \lambda \cdot 1_{\tilde{V}}),$$

where $\tilde{V} = V \otimes \overline{\mathbb{F}_q}$. A result of Larsen, Shalev, and the author [13] states that, for any classical group $G = \mathrm{Cl}(V)$, any irreducible character $1_G \neq \chi \in \mathrm{Irr}(G)$, and any $g \in G$

$$\frac{|\chi(g)|}{\chi(1)} \leq \frac{1}{q^{\sqrt{\mathsf{supp}(g)}/481}}. \tag{1}$$

Relying on *Howe's duality* and *Deligne-Lusztig theory*, an approach towards Problem 1(B) using the concept of *character level* has been developed in [7], [8]. This approach applies particularly well in the situation where either $\chi(1)$ or $|C_G(g)|$ is not too large, compared to $|G|$ logarithmically.

Theorem 2. [7, 8] *For any $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$ such that the following statement holds. For any finite quasisimple group G of Lie type, and for any $g \in G$ with $|C_G(g)| \leq |G|^\delta$,*

$$|\chi(g)| \leq \chi(1)^\varepsilon$$

for all $\chi \in \mathrm{Irr}(G)$.

For instance, if $G = \mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$, and $\varepsilon = 8/9$, one can take $\delta = 1/12$.

Building on [2, 7, 8, 25], we have recently proved the following uniform exponential character bound, which works for all elements in all finite quasisimple groups of Lie type:

Theorem 3. [15] *There exists an explicit constant $c > 0$ such that for all finite quasisimple groups G of Lie type, all $\chi \in \mathrm{Irr}(G)$, and all $g \in G$, we have*

$$|\chi(g)|/\chi(1) \leq \chi(1)^{-c\frac{\log|g^G|}{\log|G|}}.$$

Up to the factor c, the exponent in Theorem 3 is optimal.

Theorem 3 has a number of consequences.

- A linear upgrade of the LST-bound (1):
$$|\chi(g)/\chi(1)| \leq q^{-\sigma \cdot \mathsf{supp}(g)}$$
for a uniform constant $\sigma > 0$.
- One can "swap" ε and δ in Theorem 2 :
For any $0 < \delta < 1$, there is $0 < \varepsilon = \varepsilon(\delta) > 0$ such that the following statement holds. For any finite quasisimple group G of Lie type, and for any $g \in G$ with $|C_G(g)| \leq |G|^\delta$,
$$|\chi(g)| \leq \chi(1)^\varepsilon$$

for all $\chi \in \mathrm{Irr}(G)$.

- *Lubotzky's conjecture* (also of Shalev) [23, 24]: *If* G *is simple of Lie type, then the mixing time of the random walk on the Cayley graph* $\Gamma(G, g^G)$ *is of the same magnitude as its diameter; and it is* $\Omega(n/\mathsf{supp}(g))$ *if* $G = \mathrm{Cl}_n(q)$.
  The diameter part was established by [19].
- *Liebeck-Shalev-Tiep's conjecture* [20]: *If* G *is simple and* α *a faithful character of* G*, then the diameter of the McKay graph* $\mathcal{M}(G, \alpha)$ *is*
$$\Omega(\log |G| / \log \alpha^*(1)),$$
  where α^* *is the sum of distinct irreducible constituents of* α.

It was proved in [3] that Thompson's conjecture holds for all finite simple groups of Lie type over fields of at least 9 elements. Relying on Theorem 3 (and [17, 18]), we are able to make further progress on Thompson's conjecture:

Theorem 4. [15], [16] *Suppose* $G = \mathrm{Cl}_n(q)$ *is a simple classical group of large enough rank. If* $G = P\Omega_n^{\epsilon}(q)$ *and* $2 \nmid q$*, assume in addition that* $2|n$ *and* $\epsilon = (-1)^{n(q-1)/4}$*. Then Thompson's conjecture holds for* G*, i.e.* $G = C^2$ *for some conjugacy class* C *in* G.

Acknowledgements. The author gratefully acknowledges the support of the NSF (grant DMS-2200850), the Simons Foundation, and the Joshua Barlaz Chair in Mathematics.

References

[1] Z. Arad and M. Herzog, *Products of conjugacy classes in groups*, Lecture Notes in Mathematics, **1112**, Springer-Verlag, Berlin, 1985.

[2] R. Bezrukavnikov, M. W. Liebeck, A. Shalev, and Pham Huu Tiep, Character bounds for finite groups of Lie type, *Acta Math.* **221** (2018), 1–57.

[3] E.W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore. *Trans. Amer. Math. Soc.* **350** (1998), no. 9, 3657–3671.

[4] S. Fomin and N. Lulov, On the number of rim hook tableaux, *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)* **223** (1995), Teor. Predstav. Din. Sistemy, Kombin. i Algoritm. Metody. I, 219–226, 340; translation in *J. Math. Sci.* (New York) **87** (1997), 4118–4123.

[5] D. Gluck, Sharper character value estimates for groups of Lie type. *J. Algebra* **174** (1995), no. 1, 229–266.

[6] D. Gluck and K. Magaard, Base sizes and regular orbits for coprime affine permutation groups, *J. Lond. Math. Soc.* **58** (1998) 603–618.

[7] R. M. Guralnick, M. Larsen, and Pham Huu Tiep, Character levels and character bounds, *Forum Math. Pi* **8** (2020), e2, 81 pp.

[8] R. M. Guralnick, M. Larsen, and Pham Huu Tiep, Character levels and character bounds for finite classical groups, *Invent. Math.* **235** (2024), 151–210.

[9] R.M. Guralnick, M.W. Liebeck, E.A. O'Brien, A. Shalev, and Pham Huu Tiep, Surjective word maps and Burnside's $p^a q^b$ theorem. *Invent. Math.* **213** (2018), 589–695.

[10] R.M. Guralnick and Pham Huu Tiep, A problem of Kollár and Larsen on finite linear groups and crepant resolutions, *J. Eur. Math. Soc.* **14** (2012), 605–657.

[11] Kourovka Notebook, `https://kourovka-notebook.org/`

[12] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, *Invent. Math.* **174** (2008), 645–687.

[13] M. Larsen, A. Shalev and Pham Huu Tiep, The Waring problem for finite simple groups. *Ann. of Math.* **174** (2011), no. 3, 1885–1950.
[14] M. Larsen, A. Shalev and Pham Huu Tiep, Probabilistic Waring problems for finite simple groups. *Ann. of Math.* **190** (2019), no. 2, 561–608.
[15] M. Larsen and Pham Huu Tiep, Uniform character bounds for finite classical groups, *Annals of Math.* (to appear).
[16] M. Larsen and Pham Huu Tiep, Thompson's conjecture for large unitary groups, (submitted).
[17] M. W. Liebeck, E.A. O'Brien, A. Shalev, and Pham Huu Tiep, The Ore conjecture. *J. Eur. Math. Soc.* **12** (2010), no. 4, 939–1008.
[18] M. W. Liebeck, E.A. O'Brien, A. Shalev, and Pham Huu Tiep, Commutators in finite quasisimple groups. *Bull. Lond. Math. Soc.* **43** (2011), 1079–1092.
[19] M. W. Liebeck and A. Shalev, Diameters of simple groups: sharp bounds and applications. *Ann. of Math.* **154** (2001), 383–406.
[20] M. W. Liebeck, A. Shalev, and Pham Huu Tiep, Character ratios, representation varieties and random generation of finite groups of Lie type, *Adv. Math.* **374** (2020), 107386, 39 pp.
[21] M. W. Liebeck, A. Shalev, and Pham Huu Tiep, On the diameters of McKay graphs for finite simple groups, *Israel J. Math.* **241** (2021), 449–464.
[22] M. W. Liebeck, A. Shalev, and Pham Huu Tiep, McKay graphs for alternating groups and classical groups, *Trans. Amer. Math. Soc.* **374** (2021), 5651–5676.
[23] A. Lubotzky, Cayley graphs: eigenvalues, expanders and random walks, *Surveys in combinatorics*, 1995 (Stirling), 155–189, London Math. Soc. Lecture Note Ser. **218**, Cambridge Univ. Press, Cambridge, 1995.
[24] A. Shalev, Conjugacy classes, growth and complexity, *Finite simple groups: thirty years of the Atlas and beyond*, 209–221, Contemp. Math. **694**, Amer. Math. Soc., Providence, RI, 2017.
[25] J. Taylor and Pham Huu Tiep, Lusztig induction, unipotent support, and character bounds, *Trans. Amer. Math. Soc.* **373** (2020), 8637–8676.

Contributions to the open problem session

Questions by G. Arzhantseva.

An *expander* is an infinite sequence of finite graphs of uniformly bounded degree, size tending to infinity, and the Cheeger isoperimetric constant being uniformly isolated from zero.

Answering an old open question, Kassabov constructed, for each n, a bounded size generating set X_n of the symmetric group $Sym(n)$ such that the sequence of Cayley graphs $Cay(Sym(n), X_n)$ is an expander [13]. Equivalently, such generating sets exist for the alternating groups $Alt(n)$.

Using a strengthening of Kazhdan's property (T), V. Lafforgue provided the first examples of *super-expanders*, that is, expanders with respect to all uniformly convex Banach spaces [16]. A combinatorial construction of super-expanders was given in [18]. Every super-expander is an expander. Whether or not the converse holds is a major open question.

Question 1. *Can the sequence of symmetric groups $Sym(n)$ be made a super-expander using a bounded number of generators?*

Equivalently, the question arises for the sequence of alternating groups $Alt(n)$.

A famous open problem asks whether or not two almost commuting matrices are necessarily close to two commuting matrices. This is considered independently of the matrix sizes and the interpretation of "almost" and "close" is with respect to a given norm. The topic goes back to von Neumann (1929). There are numerious positive and negative answers in the literature, depending on the type of matrices, the matrix norm, and the underlying field.

In [2], we proved that almost commuting permutations are close to commuting permutations with respect to the normalised Hamming distance. We consider a finite number of permutations (two or more). The result is interesting in the setting of sofic approximations of groups. In [3], we have introduced *linear sofic approximations.* These are approximations by general linear groups $GL_n(F)$, over a field F, equipped with the normalised rank metric $d_{rk}(A, B) := \frac{1}{n}\text{rank}\,(A - B)$ for $A, B \in GL_n(F)$.

Question 2. *Are almost commuting invertible matrices close to commuting invertible matrices in the normalised rank metric?*

For $\mathbf{k} = \mathbb{C}$, a partial positive answer was obtained in [9].

The following well-known question is relevant to the present workshop.

Question 3. [20, Question 12.64, A. Yu. Ol'shanskiĭ] *Is it true that for a given number $k \geq 2$ and for any (prime) number n, there exists a number $N = N(k, n)$ such that every finite group with generators $A = \{a_1, \ldots, a_k\}$ has exponent $\leq n$ if $(x_1 \cdots x_N)^n = 1$ for any $x_1, \ldots, x_N \in A \cup \{1\}$?*

For given k and n, a negative answer implies, for example, the infiniteness of the free Burnside group $B(k, n)$, and a positive answer, in the case of sufficiently large n, gives, for example, an opportunity to find a hyperbolic group which is not residually finite (and in this group a hyperbolic subgroup of finite index which has no proper subgroups of finite index).

An affirmative answer is known for finite solvable groups and the general case of all finite groups reduces to the case of finite simple groups [17].

Questions by J. Bajpai.

Definition 1. *A subgroup Γ of $\mathrm{GL}_n(\mathbb{Z})$ is called* ***thin*** *if Γ is of infinite index in $G(\mathbb{Z})$ and* ***arithmetic*** *if Γ is of finite index in $G(\mathbb{Z})$, where G is the Zariski closure of Γ.*

For the past 15 years, thin groups have been a central object of research interest due to their connection with number theory, geometry, and computer science.

Following Tits alternative, we know that every finitely generated linear group which is not virtually solvable contains a free group on two generators. Classically, *ping-pong lemma* has been an important tool to construct free groups.

For $n \geq 3$, let A, B be any pair of matrices inside $\mathrm{GL}_n(\mathbb{Z})$, and a subgroup $\Gamma = \langle A, B\rangle$ generated by the matrices A and B. It has been a challenging task to determine the thinness of subgroup Γ, which to date, heavily relies on ping-pong lemma. That is, showing freeness by using ping-pong is the first major step towards thinness of Γ. Hence, the following is one of the most natural question to ask.

Question 4. *Can we classify all pairs of matrices A, B in $\mathrm{GL}_n(\mathbb{Z})$, for $n \geq 3$, such that the subgroup $\Gamma = \langle A, B\rangle \subset G(\mathbb{Z})$ is **thin**?*

In the last 12 years, lot of progress have been made in this direction. For quick introduction of the subject and recent developments, see [14, 1, 11].

For a special family of groups, namely hypergeometric groups $\Gamma = \Gamma(f, g) = \langle A, B\rangle \subset \mathrm{Sp}_{2n}(\mathbb{Z})$, $n \geq 1$, where $f, g \in \mathbb{Z}[x]$ be the polynomials of degree $2n$ and A and B are the companion matrices of the polynomials f respectively g, a nice criteria has been provided in [19] to determine *arithmeticity* of such Γ, that is, if highest nonzero coefficient of $f - g$ is either ± 1 or ± 2, then Γ is arithmetic inside Sp_{2n}. However, there is no such criteria available to determine *thinness* of these groups. In this direction, some progress has been done when the zariski closure G of Γ is $\mathrm{Sp}_4, \mathrm{Sp}_6$, and O_5, see [8, 10, 5, 6].

Questions by S. Eberhard.

There were four questions posed by Eberhard. Three of them are marked as (Q1), (Q2), (Q3) in his extended abstract. The fourth one goes as follows.

Question 5. *What is the length of the shortest law on S_n? It is known that a law must have length at least $2n - 1$, and at most $\exp(O((\log n)^4 \log\log n))$ by Kozma–Thom [15].*

Questions by H. Helfgott.

There were two questions posed by Helfgott, going as follows.

Question 6. *Can we prove better bounds for $\mathrm{diam}(G)$ with $G = SL_n(\mathbb{F}_q)$, say $(\log|G|)^{(\log n)^{O(1)}}$?*

The second question arises in the context of [12, §2.5]. Let $G = \mathrm{Sym}(n)$, $k \leq n$, $\Sigma = \{1, \ldots, k\}$, $O = \{k+1, \ldots, n\}$, and $A \subset G_\Sigma$ with $A|_\Sigma = \mathrm{Sym}(\Sigma)$. Note that $\langle (A^3)_{(\Sigma)}\rangle = \langle A\rangle_{(\Sigma)}$ by Schreier. Assume that $\langle A\rangle_{(\Sigma)}$ is non-trivial, it can be equal to $\mathrm{Sym}(O)$ if desired.

Question 7. *What can we say about $(A^{k^{100}})_{(\Sigma)}$? Is it big? What about its structure? If it is not big, is $(A^{k^{100}})_{(O)}$ non-trivial?*

Questions by M. Kassabov.

There were two questions posed by Kassabov, going as follows.

Question 8. *Does a random generating set in $\mathrm{Alt}(n)$ give expanders?*

Question 9. *For what function $f(n)$ does there exist an expanding generating set in $\mathrm{Alt}(n)^{f(n)}$?*

By [7, Cor. 15] there is such a set for $f(n) < \exp((\log n)^k)$ for any fixed k. There is no such set for $f(n) \gg n!$, because the minimal number of generators is unbounded. It may be possible to have $f(n) \approx \exp(n^{0.001})$.

A bottle of wine has been promised as reward for answering "yes" to Question 8 and "it must be $f(n) \lesssim \exp((\log n)^k)$" to Question 9.

Questions by N. Lifshitz.

There was one question posed by Lifshitz, going as follows.

In 1985, Babai and Sós [4] defined a set $A \subseteq G$ to be *product-free* if $xy \notin A$ for every $x, y \in A$. For instance, if G acts on a set X, for any $x \in X$ and $I \subseteq X$ the set $k_{x,I} = \{g \in G : g(x) \in I, g(I) \subseteq X \setminus I\}$ is product-free.

Question 10. *If the minimal dimension of an irreducible representation of G is $D > 1$, is there some X of size $D^{O(1)}$ such that a set $k_{x,I}$ is largest among the product-free sets of G?*

Questions by L. Sabatini.

There was one question posed by Sabatini. It is marked as Question 5 in his extended abstract.

References

[1] R. Aoun, *Random subgroups of linear groups are free*, Duke Math. J., **160** (2011), 117–173.

[2] G. Arzhantseva, L. Păunescu, *Almost commuting permutations are near commuting permutations*, J. Funct. Anal. **269** (2015), no. 3, 745–757.

[3] G. Arzhantseva, L. Păunescu, *Linear sofic groups and algebras*, Trans. Amer. Math. Soc. **369** (2017), no. 4, 2285–2310.

[4] L. Babai, V. T. Sós. *Sidon sets in group and induced subgraphs of Cayley graphs*, European J. Combin. **6** (1985), no. 2, 101–114.

[5] J. Bajpai, D. Dona, M. Nitsche, *Thin monodromy in* Sp(4) *and* Sp(6), arXiv, (2022).

[6] J. Bajpai, M. Nitsche, *Thin monodromy in* O(5), arXiv, (2022).

[7] L. Bartholdi, M. Kassabov, *Property (T) and many quotients*, `arXiv:2308.14529`, 2023.

[8] C. Brav, H. Thomas, *Thin monodromy in Sp(4)*, Compos. Math., **150** (2014), 333–343.

[9] G. Elek, L. Grabowski, *Almost commuting matrices with respect to the rank metric*, Groups Geom. Dyn. **15** (2021), no. 3, 1059–1083.

[10] E. Fuchs, C. Meiri, P. Sarnak, *Hyperbolic monodromy groups for the hypergeometric equation and Cartan involutions*, Journal of the European Mathematical Society (JEMS) **16** (2014), 1617–1671.

[11] E. Fuchs, I. Rivin, *Generic thinness in finitely generated subgroups of* $\mathrm{SL}_n(\mathbb{Z})$, Int. Math. Res. Not. IMRN, (2017), 5385–5414.

[12] H. A. Helfgott, *Growth in linear algebraic groups and permutation groups: towards a unified perspective*, in: Groups St. Andrews 2017 in Birmingham. Selected papers of the conference, Birmingham, UK, August 5–13, 2017, Cambridge University Press, 2019.

[13] M. Kassabov, *Symmetric groups and expander graphs*, Invent. Math. **170** (2007), no. 2, 327–354.

[14] A. Kontorovich, D. Long, A. Lubotzky, A. Reid, *What is ... a thin group?*, Notices Amer. Math. Soc., **66** (2019), 905–910.

[15] G. Kozma, A. Thom, *Divisibility and laws in finite simple groups*, Math. Ann. **364** (2016), no. 1–2, 79–95.

[16] V. Lafforgue, *Un renforcement de la propriété (T)*, Duke Math. J. **143** (2008), no. 3, 559–602.

[17] C. Martínez, *On power subgroups of profinite groups*, Trans. Amer. Math. Soc. **345** (1994), no. 2, 865–869.

[18] M. Mendel, A. Naor, *Nonlinear spectral calculus and super-expanders*, Publ. Math. Inst. Hautes Études Sci. **119** (2014), 1–95.

[19] S. Singh, T.N. Venkataramana, *Arithmeticity of certain symplectic hypergeometric groups*, Duke Math. J., **163** (2014), 591–617.

[20] *The Kourovka Notebook. Unsolved problems in group theory*, 20th edition, edited by E. I. Khukhro and V. D. Mazurov, Sobolev Institute of Mathematics. Russian Academy of Sciences. Siberian Branch, Novosibirsk, 2023. 270pp.

Reporter: Luca Sabatini

Participants

Dr. Vadim Alekseev
Institut für Geometrie
Technische Universität Dresden
01062 Dresden
GERMANY

Prof. Dr. Goulnara N. Arzhantseva
Fakultät für Mathematik
Universität Wien
Oskar-Morgenstern-Platz 1
1090 Wien
AUSTRIA

Dr. Jitendra Bajpai
Mathematisches Seminar
Christian-Albrechts-Universität Kiel
Heinrich-Hecht-Platz 6
24118 Kiel
GERMANY

Dr. Subham Bhakta
School of Mathematics
Indian Institute of Science Education
and Research Thiruvananthapuram
(IISER TVM)
Maruthamala PO, Vithura,
695551 Thiruvananthapuram Kerala
INDIA

Prof. Dr. Inna Capdeboscq
Mathematics Institute
University of Warwick
Zeeman Building
Coventry CV4 7AL
UNITED KINGDOM

Dr. Daniele Dona
Alfred Renyi Institute of Mathematics
Hungarian Academy of Sciences
Realtanoda utca 13-15
1053 Budapest
HUNGARY

Dr. Michal Doucha
Institute of Mathematics of the Czech
Academy of Sciences
Zitna 25
115 67 Praha
CZECH REPUBLIC

Dr. Sean Eberhard
Mathematical Sciences Research Centre
School of Mathematics and Physics
The Queen's University of Belfast
University Road
Belfast BT7 1NN
UNITED KINGDOM

Dr. Daniele Garzoni
Dept. of Mathematics, DRB 155
University of Southern California
1042 W 36th Place
Los Angeles, CA 90089-1113
UNITED STATES

Prof. Dr. Harald A. Helfgott
Université de Paris
Institut de Mathématiques de
Jussieu-Paris Rive Gauche
8 place Aurélie Nemours
P.O. Box 7012
75205 Paris Cedex 13
FRANCE

Prof. Dr. Martin Kassabov
Department of Mathematics
Cornell University
310 Malott Hall
Ithaca, NY 14853-4201
UNITED STATES

Dr. Noam Lifshitz
Einstein Institute of Mathematics,
The Hebrew University of Jerusalem
Givat Ram
Jerusalem 9190401
ISRAEL

Dr. Martin Nitsche
Fakultät für Mathematik
Institut für Algebra und Geometrie
Karlsruher Institut für Technologie
(KIT)
76128 Karlsruhe
GERMANY

Luca Sabatini
Queen's University Belfast
1364 Budapest
HUNGARY

Prof. Dr. Dr. Katrin Tent
Institut für Mathematische Logik und
Grundlagenforschung
Universität Münster
Einsteinstraße 62
48149 Münster
GERMANY

Prof. Dr. Pham Huu Tiep
Department of Mathematics
Rutgers University
Hill Center, Busch Campus
110 Frelinghuysen Road
Piscataway, NJ 08854-8019
UNITED STATES