BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 52, Number 3, July 2015, Pages 503–514
http://dx.doi.org/10.1090/bull/1494
Article electronically published on April 3, 2015

# SELECTED MATHEMATICAL REVIEWS

related to the paper in the previous section by
H. A. HELFGOTT

**MR1308046 (96g:22018)** 22E40; 05C25, 11F70, 28C10, 43A07

**Lubotzky, Alexander**

**Discrete groups, expanding graphs and invariant measures.**
With an appendix by Jonathan D. Rogawski.

Progress in Mathematics, 125.
*Birkhauser Verlag*, *Basel*, 1994, xii+195 pp., $49.50, ISBN 3-7643-5075-X

This monograph was the first to receive the recently established Ferran Sunyer i Balaguer Prize. It guides an exciting tour through several areas of mathematics, such as graph theory, real and $p$-adic Lie groups, differential geometry, measure theory and analytic number theory. At the center are the solutions of two seemingly unrelated problems. One is the Ruziewicz problem, asking whether Lebesgue measure is the only finitely additive probability measure defined on the Lebesgue subsets of the unit sphere $\mathbf{S}^n$ in $\mathbf{R}^{n+1}$. This is closely related with the the Hausdorff-Banach-Tarski paradox; see the book by S. Wagon [*The Banach-Tarski paradox*, Cambridge Univ. Press, Cambridge, 1985; MR0803509 (87e:04007)]. The other problem is the explicit construction of so-called expanders: an $(n, k, c)$-expander is a $k$-regular graph $X$ with $n$ vertices such that for every subset $A$ of vertices, $|\partial A| \geq c|A|(1 - |A|/n)$. Here, $\partial A$ is the set of neighbours of $A$ in $X \setminus A$. More precisely, one wants to construct sequences of expanders with $c > 0$ (and possibly also $k$) fixed, while $n \to \infty$. Expanders are of big interest in various applications with an algorithmic flavour, such as sorting networks, Monte Carlo algorithms, or telephone networks [see, e.g., F. V. Bien, Notices Amer. Math. Soc. **36** (1989), no. 1, 5–22; MR0972207 (90a:90052)]. It should be noted that essentially the same problems are discussed, under a very different perspective with a more number theoretical flavour, in the book by P. C. Sarnak [*Some applications of modular forms*, Cambridge Univ. Press, Cambridge, 1990; MR1102679 (92k:11045)].

Chapters 1–2 present these two problems and give a first set of related results. For example, the expanding constant $c$ of a graph can be compared with its isoperimetric number (Cheeger constant), up to bounded factors involving only $k$. Chapter 2 contains, among other things, the negative answer to the Ruziewicz problem for the circle $\mathbf{S}^1$, a theorem due to Banach.

Representation theory plays an important role throughout this book. Of particular interest here is Kazdhan's property (T), the central theme of Chapter 3. A locally compact group $G$ is said to have this property if the trivial representation is isolated in the Fell topology of the unitary dual of $G$. A lattice (discrete subgroup with finite co-volume) has property (T) if and only if $G$ does. Borel's theorem on lattices in products of semisimple algebraic groups over the reals and $p$-adics can be used to construct many discrete groups $\Gamma$ with property (T). Examples are $\Gamma = \mathrm{SL}_n(\mathbf{Z})$ for $n \geq 3$ or $\mathrm{SO}(n, \mathbf{Z}[\frac{1}{5}])$ for $n \geq 5$. This allows a first method of construction of expanders, going back to Margulis: one can take the finite homomorphic images of $\Gamma$ and their Cayley graphs with respect to a fixed set of generators. On the other hand, it is shown how the Ruziewicz problem for

$n \geq 4$ has been solved by Margulis and by Sullivan, exhibiting a finitely generated subgroup with property (T) which is dense in $\mathrm{SO}(n+1, \mathbf{R})$.

This leaves the Ruziewicz problem for $n = 2, 3$. Also, the expanders constructed via property (T) are not best possible. The next three chapters prepare for the final solution. Chapter 4 is on the Laplacian and its eigenvalues, both for compact Riemannian manifolds and for graphs, where the Laplacian is a natural difference operator. Cheeger's inequality relates the smallest positive eigenvalue $\lambda_1$ with the isoperimetric constant of a manifold, and results of Dodziuk, Alon and others carry this over to graphs. This links $\lambda_1$ with expanders and suggests how to modify property (T) for a finitely generated group in order to obtain expanders from its finite homomorphic images. Now Selberg's theorem, which says that $\lambda_1(\Gamma(m)\backslash\mathbf{H}) \geq \frac{3}{16}$ for congruence subgroups $\Gamma(m)$ of $\Gamma = \mathrm{SL}_2(\mathbf{Z})$, enters upon the scene: the standard Cayley graphs of $\Gamma/\Gamma(m)$ must satisfy $\lambda_1 \geq$ an explicit positive constant. A slight modification yields a family of expanders with $k = 3$ and $c = 0.01$. Working with the discrete Laplacian amounts to working with the adjacency matrix. The graph is called Ramanujan if the eigenvalues of the latter other than $\pm k$ satisfy $|\lambda| \leq 2\sqrt{k-1}$, which is the best possible bound. Ramanujan graphs are expanders, but the converse is in general not true.

Chapter 5 presents the main ingredients of the representation theories of $\mathrm{PGL}_2(\mathbf{R})^0$ and $\mathrm{PGL}_2(\mathbf{Q}_p)$ in terms of their action on the hyperbolic plane $\mathbf{H}$ and the regular tree $X_p$ with degree $p+1$, respectively. For a lattice $\Gamma$ in $\mathrm{PGL}_2(\mathbf{Q}_p)$, a criterion for $\Gamma\backslash X_p$ to be Ramanujan is given in terms of representations. Chapter 6 is an overview, quoting the work of Deligne and Jacquet-Langlands in the context of the spectral decomposition of $L^2(\mathrm{PGL}_2(\mathbf{Q})\backslash\mathrm{PGL}_2(\mathbf{A}))$, where $\mathbf{A}$ is the adèle ring of $\mathbf{Q}$. These are the deepest tools used here (leading among other things to the solution of the Petersson-Ramanujan conjecture).

All these ingredients are then merged in Chapter 7, containing the highlights of this book. A discrete, algebraic group over $\mathbf{Z}[1/p]$ is constructed, which is a lattice in $G = \mathrm{SO}(3, \mathbf{R}) \times \mathrm{PGL}_2(\mathbf{Q}_p)$ when diagonally imbedded. Via the spectral decomposition of $L^2(\Gamma\backslash G)$, the Ruziewicz problem is solved for $n = 2, 3$ by projecting a suitable subgroup of $\Gamma$ into $\mathrm{SO}(3, \mathbf{R})$. This result is originally due to Drinfel′d. On the other hand, by projecting the congruence subgroups $\Gamma(N)$ of $\Gamma$ into $\mathrm{PGL}_2(\mathbf{Q}_p)$ acting on the tree $X_p$, the same results on representations are used to construct the Ramanujan graphs $\Gamma(N)\backslash X_p$, giving rise to the best known expanders. This is a result obtained by the author with R. Phillips and Sarnak [Combinatorica **8** (1988), no. 3, 261–277; MR0963118 (89m:05099)].

The final three chapters bring together miscellaneous topics related with the above material, such as distributing points on a sphere, and conclude with a set of open problems. The Appendix, written by J. Rogawski, explains the Jacquet-Langlands theory and indicates Deligne's proof of the Petersson-Ramanujan conjecture. It would merit its own review.

In conclusion, this is a wonderful way of transmitting recent mathematical research directly "from the producer to the consumer". Sometimes one seems to feel a certain impatience on the part of the author: misspelling of names is chronic, not all items in the bibliography are cited, the index might be more comprehensive, and as the author says, "the choice of what to prove and what just to survey was very subjective": this is indeed true.

*Wolfgang Woess*

From MathSciNet, March 2015

**MR2415383 (2010b:20070)** 20F65; 05C25, 05E15, 11B30, 20G40

**Bourgain, Jean; Gamburd, Alex**

**Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$.**

*Annals of Mathematics. Second Series* **167** (2008), *no.* 2, 625–642.

This very interesting paper applies a wide range of techniques from additive combinatorics, representation theory and combinatorial group theory to study expansion properties of Cayley graphs. Suppose that $S$ is a finite set of elements in $\mathrm{SL}_2(\mathbb{Z})$ which is symmetric (closed under taking inverses) and generates a non-elementary subgroup of $\mathrm{SL}_2(\mathbb{Z})$, that is to say a subgroup which does not possess a solvable subgroup of finite index. Then by reducing (mod $p$) for each prime $p$ we obtain a finite set $S_p$ of elements of $\mathrm{SL}_2(\mathbb{F}_p)$. Using this, we may define the Cayley graph $\mathcal{G}_p = \mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ to be the graph which has the elements of $G = \mathrm{SL}_2(\mathbb{F}_p)$ as vertices, and in which two vertices corresponding to elements $x, y \in G$ are linked if $x = \sigma y$ for some $\sigma \in S$. This graph is, of course, $d$-regular where $d = |S|$.

The main result of this paper is that this family of Cayley graphs is a family of expanders. There are two equivalent ways to define what this means. The first is the one that gives the concept its name: there is some constant $c > 0$, independent of $p$, such that for any set $X$ consisting of at most one half the vertices of $\mathcal{G}_p$ the 1-neighbourhood $N_1(X) = X \cup \{y\colon xy \in E(\mathcal{G}_p)\}$ has size at least $(1 + c)|X|$. The second property, which is nontrivially equivalent to the first, is that the lim sup as $p \to \infty$ of the second largest eigenvalue $\lambda_1(\mathcal{G}_p)$ is strictly less than $d$. The expansion property, which has been extensively written about in many places, should be thought of as asserting that the family $\mathcal{G}_p$ is in a sense a family of pseudorandom graphs. A great deal more on expanders and their importance may be found in the article [S. Hoory, N. Linial and A. Wigderson, Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 4, 439–561; MR2247919 (2007h:68055)].

There is another interesting result in this paper, namely that by taking a random set of $2k$ generators $\{g_1^{\pm 1}, \dots, g_k^{\pm 1}\}$ for a Cayley graph on $\mathrm{SL}_2(\mathbb{F}_p)$, for each $p$, we almost surely get a family of graphs whose second largest eigenvalues are bounded away from $2k$ as $p \to \infty$.

We focus on the ideas behind the proof of the first theorem. Fix a prime $p$ and consider the probability measure $\mu_S(x) = |S|^{-1} \sum_{g \in S} \delta_g(x)$ which places equal mass on each point of $S$. The first main idea is to use the trace formula to conclude that $\frac{1}{N} \sum_{j=0}^{N-1} \lambda_j^{2m} = (2k)^{2m} \mu_S^{(2m)}(1)$, where the eigenvalues of $\mathcal{G}_p$ are listed as $2k = \lambda_0 > \lambda_1 \geq \cdots \geq \lambda_{N-1} \geq -2k$ and $\mu_S^{(j)}$ denotes the $j$th convolution power of $\mu_S$.

Thus the main business of the paper is to examine these convolution powers $\mu_S^{(j)}$. The first step (Proposition 4) is merely stated; the proof may be found in [A. Gamburd, Israel J. Math. **127** (2002), 157–200; MR1900698 (2003b:11050)]. The proposition claims that the graphs $\mathcal{G}_p$ have girth at least $c \log p$ for an appropriate constant $c > 0$. This means that if $l_0 < \frac{1}{2} c \log p$ then the measure $\mu_S^{(l_0)}$ (and hence all measures $\mu_S^{(l)}$ with $l \geq l_0$) is fairly "spread out", meaning that it does not resemble a $\delta$ peak too closely. More specifically we have a bound $\|\mu_S^{(l)}\|_\infty < p^\gamma$, which may be thought of as saying, roughly, that the support of $\mu_S^{(l)}$ behaves like a subset $\mathrm{SL}_2(\mathbb{F}_p)$ of size at least $p^\gamma$.

The next stage of the argument consists in bootstrapping this information rather considerably by looking at repeated convolution squares, that is to say by looking at the relationship between $\nu = \mu_S^{(j)}$ and $\nu * \nu = \mu_S^{(2j)}$. For each $j = l_0, 2l_0, 4l_0, \ldots$ one of two possibilities eventually occurs: either (i) $\nu * \nu$ is "not much more spread out" than $\nu$, meaning that $\|\nu * \nu\|_2 > p^{-\epsilon}\|\nu\|_2$, or (ii) $\nu$ is almost uniform in the sense that $\|\nu\|_2 < p^{-3/2+\epsilon}$ (note that $|\mathrm{SL}_2(\mathbb{F}_p)| \sim p^3$).

Suppose for the moment that (ii) holds, in which case we have a convolution power $\mu_S^{(l_1)}$, $l_1 \sim C_{\epsilon,k} \log p$, which is almost uniformly distributed in the sense that $\|\mu_S^{(l_1)}\|_2 < p^{-3/2+\epsilon}$. A little representation theory, specifically the fact that $\mathrm{SL}_2(\mathbb{F}_p)$ has no nontrivial representations of degree less than $(p-1)/2$, then allows one to conclude that still somewhat higher convolution powers $\mu_S^{(l_2)}$ are extremely uniform and hence to obtain a bound on an appropriate $\mu_S^{(2m)}(1)$ to use in the trace formula mentioned at the start of the review. This fact, that in groups with no small-dimensional representations convolution smoothes things out very dramatically, seems to have first been observed in a related context by P. C. Sarnak and X. X. Xue [Duke Math. J. **64** (1991), no. 1, 207–227; MR1131400 (92h:22026)]. More recently it has been elaborated upon and placed in a more general context by W. T. Gowers, who introduces the name "quasirandom group" for groups with this property [Combin. Probab. Comput. **17** (2008), no. 3, 363–387; MR2410393 (2009f:20105)].

It remains to rule out the possibility that (i) holds, and this is done using the techniques of additive combinatorics together with some combinatorial group theory. Here is a very brief summary. Supposing that $\|\nu * \nu\|_2 > p^{-\epsilon}\|\nu\|_2$, a rather tedious but essentially straightforward decomposition of $\nu$ into level sets produces a set $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ with $p^\gamma < |A| < p^{3-\gamma}$ with large "additive energy", that is to say with many solutions to $xy = zw$. By T. C. Tao's noncommutative version of the Balog-Szemerédi-Gowers theorem [Combinatorica **28** (2008), no. 5, 547–594; MR2010b:11017] one may locate an "approximate group" $H$ related to $A$. By the work of H. A. Helfgott [Ann. of Math. (2) **167** (2008), no. 2, 601–623; MR2415382 (2009i:20094)] any such approximate subgroup $H$ must fail to generate all of $\mathrm{SL}_2(\mathbb{F}_p)$. By classifying the proper subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$, one sees that $H$ must in fact be contained in a 2-step solvable group $G_0$. Working backwards, it follows that the measure $\nu$ concentrates near a coset of this solvable group $G_0$, and it is this possibility which must be ruled out in order to complete the argument. A result of Kesten concerning walks in the free group is applied to conclude that if this were the case then many different words of length $l_0$ in the generating set $S$ would lie in $G_0$. A combinatorial group theory argument is then applied to contradict this, essentially because the solvability forces too much commutation between the aforementioned words.

This last paragraph, in particular, has been a very brief sketch. However, the reviewer hopes that it has adequately conveyed the amazingly rich array of ideas which have been brought to bear on this problem.

*Ben Joseph Green*

From MathSciNet, March 2015

**MR2415382** 20G40; 05C25, 20F69

**Helfgott, H. A.**

**Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.**

*Annals of Mathematics. Second Series* **167** (2008), *no.* 2, 601–623.

This paper represents a breakthrough in the asymptotic theory of Cayley graphs of finite groups, and their application to random walks and expander graphs. The main result concerns the group $G = \mathrm{SL}(2,p)$, where $p$ is prime. It is proved that if $A$ is any set of generators of $G$, and if $\Gamma(G,A)$ is the corresponding Cayley graph (i.e., the graph with vertex set $G$ and edges $\{g, ga\}$ for all $g \in G, a \in A$), then the diameter of $\Gamma(G,A)$ is $O((\log p)^c)$, where $c$ and the implied constant are absolute. This was a long-standing open problem, and part of a much more general conjecture of L. Babai that for any finite quasisimple group $G$ and generating set $A$, $\mathrm{diam}(\Gamma(G,A)) \ll (\log |G|)^c$.

A few special cases of the main result were known previously; for example, for the generating set

$$A = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

[see A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Progr. Math., 125, Birkhäuser, Basel, 1994; MR1308046 (96g:22018) (Theorem 4.4.2)]. That proof requires some deep number theory, namely Selberg's spectral gap theorem, and does not work for many other generating sets; for example, it does not work for the set

$$A = \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix} \right\}.$$

In contrast, Helfgott's proof is not based on such number theory, but rather on additive-combinatorial methods. These include recent sum-product estimates such as that of S. V. Konyagin ["A sum-product estimate in fields of prime order", preprint, `arxiv.org/abs/math/0304217`]: if $A \subseteq \mathrm{GF}(p)$ with $|A| < p^{1-\delta}$ $(\delta > 0)$, then either $|A \cdot A|$ or $|A + A|$ is greater than $|A|^{1+\epsilon}$, where $\epsilon > 0$ depends only on $\delta$. This and many other tools are used to establish the key proposition, from which the main result follows: if $A$ is a generating set for $\mathrm{SL}(2,p)$ and $|A| < p^{3-\delta}$ for some fixed $\delta > 0$, then $|A \cdot A \cdot A| > c|A|^{1+\epsilon}$, where $c, \epsilon > 0$ depend only on $\delta$.

The results of this paper have been applied a number of times already, for example, by J. Bourgain and A. Gamburd [Ann. of Math. (2) **167** (2008), no. 2, 625–642; MR2010b:20070] to prove that Cayley graphs of $\mathrm{SL}(2,p)$ are expanders with respect to the projection of any fixed elements in $\mathrm{SL}(2,\mathbb{Z})$ generating a non-elementary subgroup. In addition, the author ["Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$", preprint, `arxiv.org/abs/0807.2027`] has recently extended his results to $\mathrm{SL}(3,p)$.

*Martin W. Liebeck*

From MathSciNet, March 2015

**MR2813339 (2012f:20148)** 20H20; 20G20

**Larsen, Michael J.; Pink, Richard**

**Finite subgroups of algebraic groups.**

*Journal of the American Mathematical Society* **24** (2011), *no.* 4, 1105–1158.

This impressive article gives a generalization to arbitrary fields of Jordan's theorem concerning finite subgroups of $\mathrm{GL}_n$ over a field of characteristic zero, namely:

For every $n$ there exists a constant $J(n)$ such that any finite subgroup of $\mathrm{GL}_n$ possesses an abelian normal subgroup of index at most $J(n)$. The corresponding statement for fields of positive characteristic is false, but the authors prove the following result:

Theorem. For every $n$ there exists a constant $J'(n)$ such that any finite subgroup $\Gamma$ of $\mathrm{GL}_n$ over any field $k$ possesses normal subgroups $\Gamma_3 \subseteq \Gamma_2 \subseteq \Gamma_1$ such that:

(a) $[\Gamma : \Gamma_1] \leq J'(n)$.
(b) Either $\Gamma_1 = \Gamma_2$ or $p := \mathrm{char}(k) > 0$ and $\Gamma_1/\Gamma_2$ is a direct product of finite simple groups of Lie type in characteristic $p$.
(c) $\Gamma_2/\Gamma_3$ is abelian of order not divisible by $\mathrm{char}(k)$.
(d) Either $\Gamma_3 = \{1\}$ or $p := \mathrm{char}(k) > 0$ and $\Gamma_3$ is a $p$-group.

As with related earlier works, such as [M. V. Nori, Invent. Math. **88** (1987), no. 2, 257–275; MR0880952 (88d:20068)], $\Gamma$ is approximated by an algebraic group $G$ (though the context here is more general, and the method of approximation quite different). If $G_1$, $G_2$, and $G_3$ denote the identity component, the radical, and the unipotent radical of $G$, respectively, then the groups $\Gamma_i$ in the theorem are roughly equal to $\Gamma \cap G_i$. The least accessible part of $\Gamma$ is the image of $\Gamma \cap G_1$ in $G_1/G_2$, and a significant portion of the paper is devoted to describing this part. To that end, the authors introduce the notion of a *constructible family* of algebraic groups and frame many of their results in terms of *sufficiently general* finite subgroups of geometric fibers of such families.

The authors observe that some of their main results follow (with some work) from the classification of finite simple groups, but they provide completely independent proofs based on methods from the theory of algebraic groups rather than on those of finite groups. Since the first preprint of this article was circulated in 1998, several other related results have been published. In particular, using the classification of finite simple groups M. J. Collins gave optimal bounds for $J(n)$ [J. Group Theory **10** (2007), no. 4, 411–423; MR2334748 (2008g:20106)] and for $J'(n)$ [J. Reine Angew. Math. **624** (2008), 143–171; MR2456628 (2009j:20071)].

*Peter A. Brooksbank*

From MathSciNet, March 2015

**MR2869010 (2012m:05003)** 05-02; 05C40, 11N05, 11N35, 20F65, 68R10

**Lubotzky, Alexander**

**Expander graphs in pure and applied mathematics.**

*Bulletin of the American Mathematical Society. (New Series)* **49** (2012), *no.* 1, 113–162.

This paper is a survey based on notes prepared for the Colloquium Lectures at the Joint Annual Meeting of the American Mathematical Society and the Mathematical Association of America in January 2011. The notes were posted on the website of the AMS before the meeting.

The basic definition: Let $0 < \varepsilon \in \mathbb{R}$ and $X = (V, E)$ be a finite graph. The graph $X$ is an *$\varepsilon$-expander* if for every subset $Y$ of $V$ with $|Y| \leq \frac{1}{2}|V|$ the inequality $|\partial Y| \geq \varepsilon |Y|$ holds, where $\partial Y$ is the vertex boundary of $Y$, that is, the set of vertices in $V$ which are connected to some vertices of $Y$ but are not in $Y$.

A main goal of the theory of expanders is to construct and apply families of $\varepsilon$-expanders with fixed $\varepsilon$, uniformly bounded (usually constant) degrees and infinitely growing numbers of vertices. A probabilistic proof of the existence of such families was discovered simultaneously with the introduction of the notion of expanders. However, for applications it is important to have explicit constructions. Such constructions were first found using very advanced mathematical tools such as the Kazhdan property (T) from the representation theory of infinite groups and the Ramanujan Conjecture (proved by Deligne). For many years most of the applications of expanders were in computer science. Recently the situation has changed and expanders have found applications in algebra, geometry, and number theory. These applications, together with some of the recently discovered expander families, constitute the main contents of the survey.

The paper conforms to the established standards of survey papers for the Bulletin of the AMS, according to which "proofs should be at most briefly sketched". In this connection the reviewer does not intend to describe the contents of the survey in any detail and is only going to mention some of the topics found there.

The paper starts with a very short description of basic results and relatively classical constructions of expanders. The main purpose of this description is to introduce the necessary terminology, notation, and to state basic results used later in the paper. In this connection, in many cases, readers are referred to the author's book [*Discrete groups, expanding graphs and invariant measures*, Progr. Math., 125, Birkhäuser, Basel, 1994; MR1308046 (96g:22018)] and the survey [S. Hoory, N. Linial and A. Wigderson, Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 4, 439–561; MR2247919 (2007h:68055)] for details. (In connection with the discussion of zigzag products I would like to add two references: [N. Alon, O. Schwartz and A. Shapira, Combin. Probab. Comput. **17** (2008), no. 3, 319–327; MR2410389 (2009b:05070)], containing a simple zigzag type construction of expanders, and [M. Mendel and A. Naor, in *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms*, 236–255, SIAM, Philadelphia, PA, 2010; see MR2797147 (2012f:68008)], containing a significant simplification of the proof of expansion properties of zigzag products as well as applications of zigzag products in metric geometry.)

The next portion of the survey is devoted to a series of results proving the following conjecture of L. Babai, W. M. Kantor and A. Lubotzky [European J. Combin. **10** (1989), no. 6, 507–522; MR1022771 (91a:20038)]: There exist $k \in \mathbb{N}$ and $\varepsilon > 0$ such that every nonabelian finite simple group $G$ has a symmetric set of generators $\Sigma$ of size at most $k$ such that the Cayley graph of the group $G$ with respect to $\Sigma$ is an $\varepsilon$-expander.

Here we also find a description of some novel techniques of establishing the expander property of a family of graphs (Bourgain–Gamburd (2008) and further developments).

After that, the author turns to applications. A section on applications in computer science is relatively brief (in comparison with their number); this is justified by the fact that such applications have already been presented in other sources. Here we find the following two applications: (1) to error-correcting codes, Sipser–Spielman (1996) and some further developments; (2) to the product replacement algorithm. This is one of the algorithms used to produce a random element in a subgroup generated by explicitly given elements $g_1, \dots, g_k$ of some large group (for

example, the symmetric group). Expanders are used for the theoretical explanation of the experiments in which the algorithm shows outstanding performance.

A very rough description of the section "Expanders in number theory" is the following: We can regard the well-known result of Green and Tao (2008) about primes in arithmetic progressions as a result about primes in orbits of a commutative group. The applications discussed in the section are devoted to primes in orbits of noncommutative groups like $\mathrm{GL}_n(\mathbb{Z})$. This study is based on expander properties of Cayley graphs of some certain groups. It was initiated by Bourgain, Gamburd and Sarnak (2010) and developed rapidly.

One of the applications of expanders found in the section "Applications to group theory" is to the design of meaningful and useful notions of "small subsets", "large subsets" and "generic elements" of an infinite discrete group.

One of the results (Lackenby (2006)) presented in the section "Expanders and geometry" shows that the Lubotzky–Sarnak conjecture (about expansion properties of Cayley graphs of certain groups) has very close ties with conjectures on the topology of hyperbolic 3-manifolds such as the virtual Haken conjecture and the Heegard gradient conjecture.

The last section is described by the author as containing "brief remarks on several topics which should fit into these notes but for various reasons were left out".

In conclusion I would like to mention that this is a very interesting and readable survey containing much more than I described above. It should be also mentioned that in some parts of the survey the reader is expected to have a rather advanced knowledge of (mostly) algebraic terminology.

*Mikhail Ostrovskii*

From MathSciNet, March 2015

**MR2897695** 11B05; 11B75

**Bourgain, Jean; Varjú, Péter P.**

**Expansion in $SL_d(\mathbf{Z}/q\mathbf{Z})$, $q$ arbitrary.**

*Inventiones Mathematicæ* **188** (2012), *no.* 1, 151–173.

This impressive paper is a further installment in a series of papers by the authors and others on the expansion properties of finitely generated subgroups of linear groups under natural quotient maps. Let us begin by briefly recalling the context. Let $S$ be a finite symmetric subset of $\mathrm{SL}_d(\mathbf{Z})$, and consider the Cayley graph on $\mathrm{SL}_d(\mathbf{Z}/q\mathbf{Z})$ obtained by joining $x$ to $y$ iff $xy^{-1} \in S$. Then one is interested in whether this graph is an *expander*—that is, in whether there is some $\epsilon > 0$ such that the edge-boundary $\partial A$ satisfies $|\partial A| \geq \epsilon |A|$ whenever $|A| < \frac{1}{2}|\mathrm{SL}_d(\mathbf{Z}/q\mathbf{Z})|$. Typically, one wishes for $\epsilon$ to depend only on $S$, and not on $q$.

The construction of expander graphs as Cayley graphs in this way has a long history, and the reader is referred to the excellent survey of A. Lubotzky [Bull. Amer. Math. Soc. (N.S.) **49** (2012), no. 1, 113–162; MR2869010 (2012m:05003)] for more details.

Previous works of the authors, Gamburd and Sarnak, Helfgott, Pyber and Szabó, and Breuillard, Green, and Tao have established this expansion property when $S$ generates a Zariski-dense subgroup of $\mathrm{SL}_d(\mathbf{Z})$ as $q$ ranges over the square-free integers coprime to some fixed $q_0$. This has applications to the so-called affine sieve; see [J. Bourgain, A. Gamburd and P. C. Sarnak, Invent. Math. **179** (2010),

no. 3, 559–644; MR2587341 (2011d:11018)] and the review of that paper for more information.

The aim here is to dispense with the assumption that $q$ is squarefree in this result. The proof of this is difficult, and moreover relies on two substantial ingredients. Firstly, the aforementioned result about squarefree $q$ is used as a black box (Theorem A). Secondly, and quite surprisingly, a deep result of J. Bourgain et al. [J. Amer. Math. Soc. **24** (2011), no. 1, 231–280; MR2726604 (2011k:37008)] on the equidistribution of torus orbits of certain subgroups of $\mathrm{SL}_d(\mathbf{Z})$ is employed.

The broad scheme of the proof is the same as that of previous works in the series and goes back to the work of Bourgain and A. Gamburd [Ann. of Math. (2) **167** (2008), no. 2, 625–642; MR2415383 (2010b:20070)]. The key point is to obtain a certain product growth estimate for subsets of $\mathrm{SL}_d(\mathbf{Z}/q\mathbf{Z})$ (Proposition 2 of the paper under review), and this must now be done for arbitrary $q$.

Very roughly, the proof may be split into two extreme cases: (i) $q$ does not contain any prime to a large power, and (ii) every prime divisor of $q$ occurs to a high power. In case (i) the key ingredients are Theorem A, a pretty lemma (Lemma 4) about the nonexistence of an approximate inverse homomorphism to the projection from $\mathrm{SL}_d(\mathbf{Z}/p^2\mathbf{Z})$ to $\mathrm{SL}_d(\mathbf{Z}/p\mathbf{Z})$, the work of Gowers (extending work of Sarnak and Xue) on quasirandom groups, and various calculations in the Lie algebra $L = \mathrm{sl}_d(\mathbf{Z}/p\mathbf{Z})$. Case (ii) is deeper, and this is where Theorem B is brought into play in order to obtain some expansion properties in $L$ under addition and conjugation.

In very recent work [Geom. Funct. Anal. **22** (2012), no. 6, 1832–1891; MR3000503], A. S. Golsefidy and P. P. Varjú have weakened, in the case where $q$ is squarefree, the assumption that $\langle S\rangle$ is Zariski-dense to asking only that the connected component of the Zariski closure of $\langle S\rangle$ be perfect. This condition is also necessary. The next (and perhaps final) goal in this line of work would be to merge that result with the one in the paper under review, obtaining expansion for $q$ arbitrary assuming only that $\langle S\rangle$ has perfect Zariski closure.

*Ben Joseph Green*

From MathSciNet, March 2015

**MR3050711** 11N36; 11B05

**Kowalski, Emmanuel**

**Crible en expansion.**

Séminaire Bourbaki: Volume 2010/2011. Exposés 1027–1042.

*Astérisque*, *no.* 348 (2012), Exp. No. 1028, vii, 17–64. ISBN 978-2-85629-351-5.

The Bourbaki report under review describes new applications of classical sieving techniques made possible by recent breakthroughs in the understanding of the problem of growth in groups. One crucial aspect of sieve methods is that they can be thought of as local-to-global principles. In the classical case, one studies integers, i.e., subsets of $\mathbf{Z}$, by asking, e.g., that they avoid certain residue classes modulo primes. In this case there is an obvious underlying group homomorphism $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ for a set of selected primes $p$. In recent years many questions and applications arose where one was naturally led to generalize the above sieve setting to more general groups $G$, provided natural surjections $G \to G_p$ were still available for $p$ running over a certain index set $\mathcal{I}$ (in many cases this set would still be a subset of primes). Beyond the unavoidable problem of computing local densities

since one wants to avoid "generalized residue classes" in the groups $G_p$, the crucial question was to find a way to lift, in a strong quantitative way, the local information gathered from the $G_p$'s to the "global" elements investigated in $G$. This is where issues regarding expansion in groups (or, in a more combinatorial way, in some of the Cayley graphs naturally attached to the group one starts with) come into play.

In the introduction of the paper under review the following precise statement is given. Consider the subgroup $\Lambda$ of $\mathrm{SL}_2(\mathbf{Z})$ (known as the Lubotzky group) generated by the matrices

$$\begin{pmatrix} 1 & \pm 3 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ \pm 3 & 1 \end{pmatrix}.$$

It is Zariski dense in $\mathrm{SL}_2$ although it has infinite index in $\mathrm{SL}_2(\mathbf{Z})$.

Let $f$ be a nonconstant polynomial in $\mathbf{Z}[X, Y]$ and let $x_0 \in \mathbf{Z}^2 \backslash \{(0,0)\}$. Then there exists an integer $r \geq 1$ depending only on $f$ and $x_0$ such that $\{\gamma \in \Lambda : \Omega(f(\gamma \cdot x_0)) \leq r\}$ is Zariski dense in $\mathrm{SL}_2$ (in particular it is infinite). Here the function $\Omega$ counts the number of prime factors, counted with multiplicity.

This result is an instance of much more general statements of J. Bourgain, A. Gamburd and P. Sarnak [Acta Math. **207** (2011), no. 2, 255–290; MR2892611].

Besides explaining the strategy and describing the various ingredients needed for the proof of the above result (and of its generalizations) the report also discusses a different sieve method developed independently (and almost at the same time) by Kowalski and Rivin. The latter work also relies on spectral gap properties in groups though the sieve setting differs [see E. Kowalski, *The large sieve and its applications*, Cambridge Tracts in Math., 175, Cambridge Univ. Press, Cambridge, 2008; MR2426239 (2009f:11123); I. Rivin, Duke Math. J. **142** (2008), no. 2, 353–379; MR2401624 (2009m:20077)]. This other type of sieve produces applications where the group involved comes from yet a different context. The report mentions the application to the study of torsion in the homology of random 3-manifolds, in the sense of Dunfield and Thurston (details can be found in [E. Kowalski, op. cit.]).

This Bourbaki report is organized as follows. After a short introduction together with the description of a few motivating examples (e.g., applications to arithmetic properties of curvatures in Apollonian circle packings, or, as mentioned above, torsion in the homology of random 3-manifolds), the author gives a short account of classical sieve methods which are the ones used in some of the most striking applications (e.g., those obtained by Bourgain, Gamburd and Sarnak in [Invent. Math. **179** (2010), no. 3, 559–644; MR2587341 (2011d:11018); op. cit.; MR2892611]). The emphasis is put on the local/global aspects of the sieve. Then the heart of the report is devoted to the so-called *sieve in orbits* (also called affine linear sieve) of Bourgain, Gamburd and Sarnak. The general question can be summarized as follows. Let $m \geq 2$ and $\Lambda \subset \mathrm{GL}_m(\mathbf{Z})$ be a finitely generated subgroup. Given a vector $x_0 \in \mathbf{Z}^m$ one considers its orbit $\Lambda \cdot x_0 \subset \mathbf{Z}^m$. Now for a given polynomial $f \in \mathbf{Q}[X_1, \ldots, X_m]$ such that $f$ assumes only integral values on $\Lambda \cdot x_0$, a natural question is to measure the extent to which the integer $f(x)$ is "typical" as $x$ runs over $\Lambda \cdot x_0$ (the meaning of "typical" here is usefully discussed in an appendix to the paper under review). Since one would like to bring to bear sieve methods to answer questions of this type, important hypotheses have to be satisfied. A description of these conditions is given in the next section of the report. Here various deep results need to be used, e.g., strong approximation (in the context of the work of Matthews, Vaserstein, Weisfeiler, Nori, etc.) provides suitable surjectivity and

independence of $p$ properties, crucial for the sieve to apply. It is also at this point that recent results on expansion in groups enter the game. Starting with H. A. Helfgott's breakthrough [Ann. of Math. (2) **167** (2008), no. 2, 601–623; MR2415382 (2009i:20094)], this subject drew a lot of attention for a few years and culminated with the work of A. Salehi Golsefidy and P. P. Varjú [Geom. Funct. Anal. **22** (2012), no. 6, 1832–1891; MR3000503]. Let us quickly state their main result: let $G/\mathbf{Q}$ be a linear algebraic group which is connected, simply connected and absolutely almost simple. Up to fixing a faithful $\mathbf{Q}$-representation one may assume $G \subset \mathrm{GL}_m$, for some $m \geq 1$. Let $\Lambda \subset G(\mathbf{Q}) \cap \mathrm{GL}_m(\mathbf{Z})$ be a Zariski-dense (in $G$), finitely generated subgroup. Let $S$ be a symmetric generating system for $\Lambda$. Then the family of Cayley graphs obtained by reducing $\Lambda$ modulo $d$ with respect to the reduction of $S$ modulo $d$ is a family of expander graphs, as $d$ runs over the set of positive square-free integers.

The expansion property can be rephrased in terms of the existence of a uniform spectral gap for a natural set of Hecke operators attached to the Cayley graphs involved. It is this crucial property that enables the "transfer" of the local data to the global information in the sieving process. Three short sections end the report. Other applications of the affine linear sieve are mentioned, together with natural open questions that arise.

The report is written in a very clear and enlightening way, with many examples and discussions meant to introduce nonexperts to the subject.

*Florent Jouve*

From MathSciNet, March 2015

**MR3144176** 20F65; 05C25, 20G30, 20G40

**Kowalski, Emmanuel**

**Explicit growth and expansion for** $\mathrm{SL}_2$**.**

*International Mathematics Research Notices. IMRN* **2013**, *no.* 24, 5645–5708.

The purpose of this carefully written paper is to prove explicit versions of two well-known theorems, namely:

- the Bourgain-Gamburd argument for the expansion of Cayley graphs, modulo primes, of subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which are Zariski-dense in $\mathrm{SL}_2(\mathbb{Z})$ [J. Bourgain and A. Gamburd, Ann. of Math. (2) **167** (2008), no. 2, 625–642; MR2415383 (2010b:20070)];
- H. A. Helfgott's growth theorem for $\mathrm{SL}_2(\mathbb{F}_p)$ [Ann. of Math. (2) **167** (2008), no. 2, 601–623; MR2415382 (2009i:20094)].

In addition, the author obtains, as corollaries, an explicit solution to Babai's conjecture for $\mathrm{SL}_2(\mathbb{F}_p)$; explicit diameter bounds for Cayley graphs, modulo primes, of Zariski-dense subgroups of $\mathrm{SL}_2(\mathbb{Z})$; and explicit bounds for the largest eigenvalue and for the diameter of a third of the groups discussed in Lubotzky's famous 1-2-3 problem.

The value of these results is two-fold: firstly, given the acknowledged mathematical importance of the work of Bourgain-Gamburd and Helfgott (in particular to sieve methods), one would naturally like to have some indication of the size of the constants to which these results pertain. The author remarks that the original proofs of the two main results were effective, thus it is not surprising that one can obtain explicit versions; nonetheless, the gap between 'effective' and 'explicit' is

sometimes a large one, and the current paper bridges that gap for these results. No claim is made for the bounds being sharp—there is clearly a great deal of scope for further investigation in this direction.

Secondly, one can also see this paper as presenting a complete proof of the original qualitative forms of the results of Bourgain-Gamburd and Helfgott. As the author remarks, "when read in this light, ignoring the fussy technical details arising from trying to have explicit bounds, it may in fact be useful as a self-contained introduction to this area of research". Indeed, the author has clearly gone to some pains to make sure that the exposition of this paper is clear and accessible to those not already familiar with the area.

The proof of (an explicit version of) Helfgott's growth theorem given here has the flavour of the original proof of Helfgott, albeit modified in the light of subsequent work by a number of authors:

- firstly, Helfgott's work on $\mathrm{SL}_3(\mathbb{F}_p)$ demonstrated (for instance) how the geometry of maximal tori could be used in the proof [H. A. Helfgott, J. Eur. Math. Soc. (JEMS) **13** (2011), no. 3, 761–851; MR2781932];
- secondly, the subsequent generalization to all groups of Lie type (due independently to E. Breuillard, B. Green and T. C. Tao [Geom. Funct. Anal. **21** (2011), no. 4, 774–819; MR2827010] and L. Pyber and E. Szabó ["Growth in finite simple groups of Lie type of bounded rank", preprint, `arXiv:1005.1858`]) highlighted those ingredients which were truly key.

Indeed, a qualitative version of the proof given here is sketched out in the monograph of Pyber and Szabó [op. cit.].

The proof of the Bourgain-Gamburd argument is, again, reminiscent of the original. A central ingredient of the original proof is the $L^2$-flattening theorem, an explicit version of which is proved here for all finite groups.

*Nick Gill*

From MathSciNet, March 2015