BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 56, Number 2, April 2019, Pages 361–366
http://dx.doi.org/10.1090/bull/1610
Article electronically published on January 25, 2018

Expansion in finite simple groups of Lie type, by Terence Tao, Graduate Studies in Mathematics, Vol. 164, American Mathematical Society, Providence, RI, 2015, xiv+303 pp., ISBN 978-1-4704-2196-0

The beautiful book of Terry Tao starts with the following words:

> *Expander graphs* are a remarkable type of graph (or more precisely, a family of graphs) on finite sets of vertices that manage to simultaneously be both sparse (low-degree) and "highly connected" at the same time. They enjoy very strong mixing properties: if one starts at a fixed vertex of an (two-sided) expander graph and randomly traverses its edges, then the distribution of one's location will converge exponentially fast to the uniform distribution. For this and many other reasons, expander graphs are useful in a wide variety of areas of both pure and applied mathematics.

Indeed, expander graphs have emerged as the area with the most fruitful interactions between computer science and pure mathematics. In computer science, expanders appear everywhere as basic building blocks of (communication) networks, in algorithms, derandomization, error correcting codes, and much more. The reader is referred to [HLW] for an excellent survey (though in the last decade since it was written, so much more has been done that an updated version will be a welcome addition to the literature). The current book gives the story from a different angle: the importance of expander graphs in pure mathematics and the use of pure mathematics to further advance the theory of expanders. In this sense this book follows [L1], but so much has been done in the last twenty-five years, and the theory went to some totally unexpected directions, that except for some similarity in the early chapters, the books are very different.

Reviewing this book gives an opportunity to describe the fascinating development this area has made in the last decades. In spite of (or maybe because) I am personally involved in this process, going over this book was, for me, a wonderful journey in a beautiful interdisciplinary mathematics. Let me share some of this history.

Expander graph is a family $\{X_i\}_{i=1}^{\infty}$ of finite k-regular graphs (k-fixed) such that there exists a fixed $\varepsilon > 0$ with the following property: for every i and every subset Y of X_i, with $|Y| \leq \frac{1}{2}|X_i|$, $|\partial Y| \geq \varepsilon |Y|$, when ∂Y is the set of edges of X_i going from

2010 *Mathematics Subject Classification.* Primary 05C81, 11B30, 20C33, 20D06, 20G40.

Y to its complement. The nontrivial part is that the graphs are sparse (k fixed) and "very connected" (ε fixed). The first to define them and to prove their existence was Pinsker, though recently it was discovered that they had already appeared in the work of Kolmogorov and Barzdin. Chapter 1 of the book covers these aspects.

In any case it was Margulis who gave the first explicit and constructible examples. For this he used Kazhdan's property (T) from representation theory of Lie groups and their discrete subgroups: If Γ is a group with property (T) generated by a finite symmetric set S, then the family of Cayley graphs $\mathrm{Cay}(\Gamma/N; S)$, when N runs over the finite index normal subgroups of Γ, forms a family of k-regular expander graphs, with $k = |S|$. Recall that the Cayley graph of a group G with respect to a set of generators S is the graph with vertex set $V = G$ and edges $E = \{\{g, gs\} | g \in G,\ s \in S\}$. Examples of groups with property (T) are $\Gamma = \mathrm{SL}_n(\mathbb{Z})$ for $n \geq 3$. Thus, one gets many explicit examples of expanding graphs. This and more is covered in Chapter 2.

In the 1980s, Lubotzky, Phillips, and Sarnak observed that Selberg's $\lambda_1 \geq \frac{3}{16}$ theorem, which says that $\frac{3}{16}$ is a lower bound on the positive spectrum of the Laplacian on the hyperbolic arithmetic surfaces $\Gamma(p)\backslash\mathbb{H}$, also gives rise to expanders. Here $\mathbb{H} = \{z = x + iy | x, y \in \mathbb{R}, y > 0\}$ is the upper half-plane and for a prime p, $\Gamma(p) = \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$, where this group acts on $\mathbb{H}$ by the Möbius transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}.$$

In fact, Selberg's theorem can be translated to the language of representation theory, and it says that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ (which does not have property (T)!) has a "relative property (T)" (nowadays called property (τ)) with respect to the family $\{\Gamma(p) | p$ prime$\}$ and so Margulis's argument can also be applied here to get expanders. One may also argue directly from the geometric theorem of Selberg to the expansion of the graphs, and this is the way it is presented in Chapter 3.

The argument in the last paragraph produced some more expander graphs—this time Cayley graphs of the finite simple groups $(P)\,\mathrm{SL}_2(\mathbb{F}_p)$, but of no significant importance. (Well, they served at the time as an intermediate station for the important Ramanujan graphs, but this is a story in a different direction; see [L1].) However, an interesting new question arose. The set $S_1 = \{\left(\begin{smallmatrix} 1 & \pm 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ \pm 1 & 1 \end{smallmatrix}\right)\}$ generates $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, and by the discussion above we get

(1) $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); S_1)$ are expanders.

Now let us look at $S_2 = \{\left(\begin{smallmatrix} 1 & \pm 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ \pm 2 & 1 \end{smallmatrix}\right)\}$. The subgroup generated by them is $\Gamma(2)$ which is a finite index subgroup of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Still, Selberg's result applies and one can deduce

(2) $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); S_2)$, for $p \neq 2$, form a family of expanders.

But what about $S_3 = \{\left(\begin{smallmatrix} 1 & \pm 3 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ \pm 3 & 1 \end{smallmatrix}\right)\}$? The subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by S_3 is of infinite index and Selberg's theorem does not apply to it.

In the 1990s the following was one of my most favorite open problems:

(3) Is $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); S_3)$, $p \neq 3$, a family of expanders?

Alex Gamburd kindly coined this the"Lubotzky 1-2-3 problem" (a cute name which maybe made the problem even more popular...).

Let us put this problem in a more general perspective. Let G be a Chevalley group, and let $\Gamma = G(\mathbb{Z})$. The reader may think of the following examples: $G = \mathrm{SL}_n$ and $\Gamma = \mathrm{SL}_n(\mathbb{Z})$. The classical strong approximation theorem asserts that Γ is mapped onto $G(\mathbb{F}_p)$ for every prime p. For SL_n this is an exercise, since the elementary matrices generate $\mathrm{SL}_n(\mathbb{F}_p)$. In the 1980s and 1990s, "strong approximation theorems for linear groups" were proved by Nori, Weisfeiler, and others, claiming that if $S \subseteq \Gamma = G(\mathbb{Z})$ is a finite set generating a Zariski dense subgroup Λ of $G(\mathbb{Z})$, then for almost every prime p, the image of Λ under the "mod p map"

$$G(\mathbb{Z}) \to G(\mathbb{Z}/p\mathbb{Z}) = G(\mathbb{F}_p)$$

is onto. This theorem is of great importance and has many applications in "asymptotic group theory" (see [LS] and the references therein). In our context it can be reformulated as follows:

(A) If $S \subseteq G(\mathbb{Z})$ is a finite set generating a Zariski dense subgroup of G, then for almost every prime p, the Cayley graph $\mathrm{Cay}(G(\mathbb{F}_p); S)$ is connected.

This in particular applies for S_3 above (in fact, in SL_2 every nonvirtually abelian group is Zariski dense, which is always a pretty weak condition). The connectedness of $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); S_3)$ is easy to prove directly. Being an expander is a much stronger property than being connected. Question (3) was a "baby case" of a much more ambitious conjecture:

(B) If $S \subseteq G(\mathbb{Z})$ is a finite subset generating a Zariski dense subgroup, then the family $\mathrm{Cay}(G(\mathbb{F}_p); S)$ is a family of expanders outside a finite set of exceptional primes p.

The PhD theses of Alex Gamburd and of Yehuda Shalom in the 1990s proved some special cases of conjecture (B). The breakthrough toward the proof of conjecture (B) came in 2005 with a work of Harald Helfgott, who was interested in a somewhat different problem. Let us turn our attention to that problem for a moment.

Let F be a finite group, and let S be a symmetric set of generators of size d. The diameter $\triangle$ of $\mathrm{Cay}(F; S)$ is the largest possible distance between two vertices of the graph. It is easy to see that this is equal to $\max\{\ell_S(g) | g \in F\}$ when $\ell_S(g)$ is the length of the shortest possible word in S expressing g. Now let F be a finite simple group. If F is abelian (i.e., a cyclic group of order p), then it is not difficult to show that the diameter $\triangle$ is at least $p^{1/d} = |F|^{1/d}$. On the other hand, Babai, Kantor, and Lubotzky showed that for every *nonabelian* finite simple group F there exists a set of generators S of size 14 with respect to which $\mathrm{Cay}(F; S)$ has diameter $O(\log |F|)$, which, up to a constant factor, is optimal. So nonabelian finite simple groups have "optimal generators". An ambitious conjecture of Babai claims that even the "worst case generators" are not that bad, more precisely:

Babai Conjecture. *There exist constants c_1 and c_2 such that for every nonabelian finite simple group F and any set of generators S, the diameter of* $\mathrm{Cay}(F; S)$ *is at most* $c_1(\log |F|)^{c_2}$.

This conjecture is still wide open, though much progress has been made which is intimately connected with our main story; see below. Helfgott made the first breakthrough by proving it for an infinite family of finite simple groups $\{(P)\,\mathrm{SL}_2(p) | p$ prime$\}$.

This was deduced from the following product property, which he proved:

Theorem. *There exists a constant $\varepsilon > 0$ such that for every subset A which generates $G = \mathrm{SL}_2(\mathbb{F}_p)$, either $A^3 = G$ or $|A^3| \geq |A|^{1+\varepsilon}$, where $A^3 = \{abc \mid a, b, c \in A\}$.*

Note that such a product property implies the Babai Conjecture: Start with a set of generators S. Then within ℓ steps the sequence $S, S^3, S^9, \ldots, S^{3^\ell}$ must terminate for some ℓ with $|G| \geq |S|^{(1+\varepsilon)^\ell}$, $\ell \leq O(\log\log|G|)$, and every element of G can be written as a product of $3^\ell = (\log|G|)^{O(1)}$ elements of S.

Helfgott's proof was very interesting. He used the "sum product result" from additive combinatorics. This theorem vaguely says that if B is a subset of the field $\mathbb{F}_p$, which is not too large, then either $B+B$ or $B\cdot B$ are of size at least $|B|^{1+\varepsilon}$. Now, multiplication of matrices in $\mathrm{SL}_2(\mathbb{F}_p)$ involves both addition and multiplication of the entries, and Helfgott used it to deduce the product property.

Helfgott's manuscript came out in mid-2005—just in time. In the academic year 2005–06 the Institute for Advanced Study in Princeton ran a program on expanders, and during that program Bourgain and Gamburd took the additional step to show that if S is a symmetric set of generators of $G = \mathrm{SL}_2(\mathbb{F}_p)$ and $\mu = \frac{1}{|S|}\sum_{s\in S}\delta_s$, the measure with S as its support, then the convolutions μ^{*n} "do not concentrate" in a proper subgroup of G. We will not go into this deep and quite technical property (which is covered in Chapter 6 of the book under review). We only say that the proof also uses the known structure of the proper subgroups of $\mathrm{SL}_2(p)$, which are all either of bounded order or metabelian (and hence "amenable" if one thinks of them as versions of infinite groups). They also showed that if the girth of $\mathrm{Cay}(G; S)$ is logarithmic, then the nonconcentration property implies that $\mathrm{Cay}(G; S)$ are expanders. This enabled them to deduce that random S gives rise to expanders. Moreover, if S is coming from $\mathrm{SL}_2(\mathbb{Z})$ and $\Lambda = \langle S\rangle$, the group generated by S, is Zariski dense, then the family $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); S)$ is a family of expanders (except for finitely many p's), i.e., conjecture (B) above is proved for $G = \mathrm{SL}_2$, and in particular, they answered the Lubotzky 1-2-3 problem.

But another breakthrough was made during that year in Princeton: Sarnak realized that if one proves a stronger version of conjecture (B), it would have number theoretic applications.

(B′) With the same assumption as in conjecture (B), prove that there exists $m_0 \in \mathbb{N}$, such that $\mathrm{Cay}(G(\mathbb{Z}/m\mathbb{Z}); S)$ are expanders for every $m \in \mathbb{N}$, which is multiplicity free (i.e., for every prime p, $p^2 \nmid m$) and $(m, m_0) = 1$.

Indeed, Bourgain, Gamburd, and Sarnak proved this stronger version for $G = \mathrm{SL}_2$ and deduced some exciting number theoretical applications.

We will come back to this, but let us first complete the group theoretic story. The new results and the potential applications gave a lot of motivation to prove conjectures (B) and (B′) for general G. Two groups of authors, Breuillard, Green, and Tao and also Pyber and Szabo proved the analogous result of Helfgott for a general G rather than just SL_2. Once the product theorem was proved in general, Salehi-Golsefidy and Varju extended the Bourgain–Gamburd machinery to prove an even stronger form of conjecture (B′).

The proof for the general G is by far more complicated since $G(\mathbb{F}_p)$ has many more proper subgroups than $\mathrm{SL}_2(\mathbb{F}_p)$. An essential ingredient in these works is the result of Larsen and Pink who gave a "quantitative" description of the subgroups of $G(\mathbb{F}_p)$ for a fixed G and $p \to \infty$. Another important ingredient of the proof for general G is the notion of quasi-random groups. There are groups all of whose nontrivial irreducible representations are of large degree (and, in particular, they are far from being abelian). The product of subsets in such groups behaves somewhat like random. This applies to the sequence of groups $G(\mathbb{F}_p)$ where G is fixed and

$p \to \infty$. The product theorem is described in the book in Chapters 4 and 5. The author wisely chose to describe it for the special case of $G = \mathrm{SL}_d$ (arbitrary d) as all ideas already appear there and it is still readable by readers who are not familiar with the detailed structure of finite simple groups of Lie type.

There is another aspect of the story: Tao and Hrushovski studied "approximate subgroups" A of a group H. These are subsets A which are "almost" closed under multiplication; namely, $A \cdot A$ is contained in a bounded number of translations of A. The product theorem implies a classification of the approximate subgroups of $G(\mathbb{F}_p)$ for G fixed and $p \to \infty$. This concept later took Breuillard, Green and Tao to a fascinating connection between this and Hilbert's 5th problem, but this journey is not part of the current book.

Let us say something, as promised, about the number theoretic applications: The "affine sieve" method, described in Chapter 7 of the book, is a new noncommutative version of the classical sieve method due to Brun. Classically, this method was used to treat questions of the following type: Let $\mathbb{Z}$ act on $\mathbb{Z}^d$ by $n : \alpha \to \alpha + n\beta$ with $\alpha, \beta \in \mathbb{Z}^d$. The Hardy–Littlewood conjecture asserts that if the components of α and β are all relatively prime, then the orbit of this action will meet infinitely many prime vectors, i.e., vectors, all of whose components are prime numbers. The case $n = 1$ is Dirichlet's classical theorem on infinitely many primes in arithmetic progression. Note that if $d = 2$, $\alpha = (1, 3)$, and $\beta = (1, 1)$, this conjecture implies the twin primes conjecture. The classical combinatorial sieve method can be used to deduce that the orbit contains infinitely many "almost prime vectors", i.e., vectors whose entries have only a bounded number of prime factors. The new method can deal, for example, with similar problems for the action of a subgroup $\Lambda \leq \mathrm{SL}_d(\mathbb{Z})$, which is Zariski dense in SL_d, to imply that the orbit of a vector α under Λ contains infinitely many almost prime vectors. There are very interesting special cases, such as integral Appolonian packings and more. Let us just make one remark: At first sight, the connection between expanders and sieving looks strange. For years, sieving has been carried out in abelian situations, which are far from being expanders. Why are expanders needed in the nonabelian case? Let us recall that the basic idea of sieving is the following: Let us say that we are interested in $\pi(x)$—the number of primes less than x. We describe it by the inclusion-exclusion formula

$$\pi(x) = \sum_{\mathcal{P}} (-1)^{|\mathcal{P}|} \left[\frac{x}{\|\mathcal{P}\|} \right],$$

where $\mathcal{P}$ runs over all the subsets of the primes less than $\sqrt{x}$ and $\|\mathcal{P}\|$ is the product of the primes in $\mathcal{P}$. This formula is exact, and $\left[\frac{x}{\|\mathcal{P}\|}\right]$ is equal to $\frac{x}{\|\mathcal{P}\|}$ up to an error term at most 1. In the noncommutative setting, one would like to have such a starting formula. Namely, let us fix a set of generators S for Λ and try to estimate the number of "prime vectors" in the set $B_S(\ell) \cdot \alpha$, where $B_S(\ell)$ is the ball of radius ℓ in Λ with respect to S. This is a subset of $\mathbb{Z}^d$, and one can describe it by inclusion and exclusion. But here it is not clear that $B_S(\ell)\alpha$, when taken mod m, a product of primes $m = \|\mathcal{P}\|$ as before, is (almost) uniformly distributed. This is where the expansion property comes to help: if $\mathrm{Cay}(\mathrm{SL}_d(\mathbb{Z}/m\mathbb{Z}); S)$ are expanders, one can apply sieve methods to get some desirable estimates.

In summary, this wonderful book describes, in a readable fashion, an active area of mathematics whose beauty is also due to the fact that it is very interdisciplinary.

The author dedicates almost half of the 300 pages to six appendices on various subjects, where each one is a lovely, short course in itself which helps in reading the main part of the book.

I must end with a personal remark. The book appeared in the series Graduate Studies in Mathematics of the AMS, and as such it is indeed suitable for a pretty advanced graduate course. I have been involved in this area for the last thirty years, still I am learning a lot from this book. This is an outstanding exposition by one of the most outstanding mathematicians of our generation, which can be read at several different levels.

References

[HLW] Shlomo Hoory, Nathan Linial, and Avi Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 4, 439–561. MR2247919

[L1] Alexander Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Progress in Mathematics, vol. 125, Birkhäuser Verlag, Basel, 1994. With an appendix by Jonathan D. Rogawski. MR1308046

[LS] Alexander Lubotzky and Dan Segal, *Subgroup growth*, Progress in Mathematics, vol. 212, Birkhäuser Verlag, Basel, 2003. MR1978431

Alexander Lubotzky
Einstein Institute of Mathematics
Hebrew University
Jerusalem, Israel
Email address: alex.lubotzky@mail.huji.ac.il