BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 49, Number 1, January 2012, Pages 113–162
S 0273-0979(2011)01359-3
Article electronically published on November 2, 2011

EXPANDER GRAPHS IN PURE AND APPLIED MATHEMATICS

ALEXANDER LUBOTZKY

Dedicated to the memory of Jonathan Rogawski

Abstract. Expander graphs are highly connected sparse finite graphs. They play an important role in computer science as basic building blocks for network constructions, error correcting codes, algorithms, and more. In recent years they have started to play an increasing role also in pure mathematics: number theory, group theory, geometry, and more. This expository article describes their constructions and various applications in pure and applied mathematics.

Contents

Introduction

Expander graphs are highly connected sparse finite graphs which play a basic role in various areas of computer science. A huge amount of research has been devoted to them in the computer science literature in the last four decades. (An excellent survey of these directions is [HLW].) But they also attracted the attention of mathematicians: their existence follows easily by random considerations (*à la* Erdős), but explicit constructions, which are very desirable for applications, are much more difficult. Various deep mathematical theories have been used to give

Received by the editors May 12, 2011, and, in revised form, June 7, 2011.
2010 *Mathematics Subject Classification.* Primary 01-02, 05C99.
This paper is based on notes prepared for the Colloquium Lectures at the Joint Annual Meeting of the American Mathematical Society (AMS) and the Mathematical Association of America (MAA), New Orleans, LA, January 6–9, 2011. The author is grateful to the AMS for the opportunity to present this material for a wide audience. He has benefited by responses and remarks which followed his lectures.

explicit constructions, e.g., the Kazhdan property (T) from representation theory of semisimple Lie groups and their discrete subgroups, the Ramanujan Conjecture (proved by Deligne) from the theory of automorphic forms, and more. All of these led to fascinating connections between pure mathematics and computer science and between pure mathematicians and computer scientists. For the first three decades—until approximately ten years ago—essentially all these connections went in one direction: methods of pure mathematics have been used to solve some problems arising from computer science (these are summarized in [L1] for example).

Something different has emerged in the last decade: computer science pays its debt to pure mathematics! The notion of expander graphs is starting to play a significant role in more and more areas of pure mathematics.

The goal of this article is to describe expander graphs and their applications in pure and applied mathematics. Rather than competing with the award winning manuscripts [L1] and [HLW] (the Ferran Sunyer i Balaguer prize and the Levi Conant prize, respectively), we will emphasize new directions: applications of expanders in pure mathematics. We will try to avoid repeating topics from [L1] and [HLW], though some intersection is unavoidable, especially in the first sections. The reader is strongly encouraged to consult these manuscripts for more background, as well as [LZu].

The article is organized as follows. We start with basic definitions of expander graphs, their properties, their eigenvalues, and random walks on them. In the second section we will give various examples, mainly of Cayley graphs, which are expanders. The reader should not be misled by this section's modest title, "examples". Some of the most remarkable developments in recent years are described there, e.g., the fact that all non-abelian finite simple groups are expanders in a uniform way and the result that congruence quotients of linear groups form a family of expanders. The last result is the crucial ingredient in some of the applications to number theory and to group theory.

Section 3 deals with applications to computing. Many are described in [HLW], so we chose to give a theoretical application to the product replacement algorithm and one for error correcting codes.

Section 4 deals with applications to number theory. There are several of these, but we will mainly describe a new direction of research for which the use of expanders is a dominant factor: the *affine sieve*. This method enables us to study primes and almost primes in orbits of groups acting on $\mathbb{Z}^n$. This is a far-reaching extension to a non-commutative world of Dirichlet's theorem about primes in arithmetic progression. This direction of research arose in response to the dramatic developments concerning Cayley graphs being expanders. It also sheds new light on classical subjects such as Apollonian circle packing and more.

The affine sieve method can also be modified to give a *group sieve*, which is a method to study various group-theoretical properties of *generic* elements in finitely generated groups. This method gives some new results about linear groups and the mapping class groups. These are described in Section 5.

Section 6 is devoted to applications to geometry. Most of the applications are for hyperbolic manifolds with some special attention to hyperbolic 3-manifolds.

In Section 7, we collected brief remarks on several topics which should fit into this article but for various reasons were left out.

We hope that the current notes will provide a panoramic view of the broad scope of mathematics which is connected with expander graphs. They have truly expanded into many different areas of mathematics!

This paper is dedicated to the memory of Jonathan Rogawski, an insightful mathematician, a loyal friend, and a wonderful human being. Jon helped me a lot when I took my first steps into the world of automorphic forms and generously contributed to [L1]. His friendship will be deeply missed.

1. Expander graphs

Expander graphs are highly connected sparse graphs. This property can be viewed from several different angles: eigenvalues, random walks, representation theory (if the graph is a Cayley graph), geometry, and more. In this section we briefly review these aspects (sending the reader to [L1] for a more comprehensive description). This leads to the highly relevant property (τ), described in §1.6, which will play a very important role in the sections to come.

1.1. **The basic definition.** Let X be a finite graph on a set V of n vertices and $A = A_X$ its adjacency matrix, i.e., A is an $n \times n$ matrix, where $A_{i,j}$ is the number of edges between vertex i and vertex j. So usually $A_{i,j} = 0$ or 1, but we also allow multiple edges ($A_{ij} > 1$) or loops ($A_{ii} > 0$). The graph X is *k-regular* if the valency of every vertex is k, i.e., for every i, $\sum_{j=1}^{n} A_{ij} = k$.

Definition 1.1. For $0 < \varepsilon \in \mathbb{R}$, X is an *ε-expander* if for every subset Y of V with

$$|Y| \leq \tfrac{1}{2}|V| = \frac{n}{2}, \quad |\partial Y| \geq \varepsilon |Y|,$$

where ∂Y is the boundary of Y, i.e., the set of vertices in V which are connected to (some vertices of) Y but are not in Y.

The largest ε for which X is an ε-expander will be denoted by $\varepsilon(X)$.

One easily sees that X is connected. So being an ε-expander for "large" ε (well, it is clear that ε cannot be larger than 1) means that X is "very much connected".

In most applications (real world applications as well as pure mathematical applications) what one wants is to find regular graphs with large n (say $n \to \infty$), fixed k (as small as possible), and a fixed ε (as large as possible). A family of k-regular graphs will be called a *family of expanders* or an *expanding family* if all of them are ε-expanders for the same $\varepsilon > 0$.

The first to define expander graphs was Pinsker [Pin] in 1973 who also coined the name. Recently, it has been noticed by Larry Guth that slightly earlier, Kolmogorov and Barzdin [KB] discussed a property of graphs which is equivalent to expanders. While Pinsker defined and studied expanders for their use in computer science (error correction codes, communication networks, and algorithms) Kolmogorov and Barzdin's motivation was very different: they studied the network of nerve cells of the human brain. This brought them to the question of realizing various networks in $\mathbb{R}^3$ and this way to graphs in which any two subsets have a large number of edges between them, a property which characterizes expanders (see [HLW, §2.4], and the historical notes in [GrGu]).

When k is fixed, ε (the expansion constant) is closely related to the *isoperimetric constant* $h(X)$, also called the *Cheeger constant*.

Definition 1.2. For X as above, let

$$h(X) := \min_{V=Y_1 \dot\cup Y_2} \frac{|E(Y_1, Y_2)|}{\min((|Y_1|, |Y_2|)},$$

where the minimum runs over all the ways to write V as a disjoint union of two subsets Y_1 and Y_2, and $E(Y_1, Y_2)$ is the set of edges between Y_1 and Y_2.

The following is a straightforward corollary of the definitions:

Proposition 1.3.

$$\frac{h(X)}{k} \leq \varepsilon(X) \leq h(X).$$

1.2. **Eigenvalues, random walks, and Ramanujan graphs.** Let X be as before, a k-regular graph on n vertices. As X is undirected, $A = A_X$ is a symmetric matrix with real eigenvalues. One can think of A as a linear operator on $L^2(X)$, the real (or complex) functions on V, where for $i \in V$ and $f \in L^2(X)$,

$$(Af)(i) = \sum_{j=1}^{n} A_{ij} f(j),$$

i.e., summing f on the neighbors. An easy argument shows that k is the largest eigenvalue of A (corresponding to the constant functions) and all the eigenvalues $\lambda_0 = k \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$ of A_X lie in the interval $[-k, k]$. The following are some well-known easy properties:

Proposition 1.4. *(a) X is connected iff $\lambda_1 < \lambda_0 = k$.*
(b) X is bipartite iff $\lambda_{n-1} = -k$.

Thus various combinatorial/geometric properties of X can be recovered from its spectrum (eigenvalues). This is also true of the expansion property:

Proposition 1.5.

$$\frac{k - \lambda_1}{2} \leq h(X) \leq \sqrt{(k + \lambda_1)(k - \lambda_1)}.$$

So for k-regular graphs (fixed k), being ε-expanders is equivalent to a spectral gap $\lambda_1 < k - \varepsilon'$.

This proposition is now well known and is attributed to various authors (see [L1] for more details and references about this result and others in this section).

For the original definition of an expander, one needs to bound the largest eigenvalue $\lambda_1 = \lambda_1(X)$ of X which is smaller than k. But for various other applications what is most relevant is

$$\lambda(X) := \max\{|\lambda| \big| \lambda \text{ an eigenvalue of } A \text{ and } |\lambda| \neq k\},$$

i.e., the largest eigenvalue in absolute value other than $\pm k$. This is not a crucial difference, but some care is needed as some authors define expanders by a bound on $\lambda(X)$.

For many applications the bound on the eigenvalues is even more relevant than the original definition since the eigenvalues control the random walk on X. Namely, assume $\mu \in L^2(X)$ is a probability measure on V, i.e., $0 \leq \mu(i) \leq 1$ for every $i \in V$ and $\sum_{i=1}^{n} \mu(i) = 1$. Then if a "little person" is in vertex i at step t with probability $\mu(i)$ and he walks a step over a randomly chosen edge coming out of i, then at step $t + 1$ he will be in $\frac{1}{k} A\mu$. In other words, the matrix $\triangle = \triangle_X = \frac{1}{k} A_X$ is the

bistochastic transition matrix of the Markov chain that is the random walk on X. If X is connected and not bipartite, then the random walk converges to the uniform distribution u, i.e., $u(i) = \frac{1}{n}$ for every $i \in V$. The rate of convergence depends on

$$\lambda(X) := \max\{|\lambda| \,\big|\, |\lambda| \neq k, \quad \lambda \text{ an eigenvalue of } A\}.$$

More precisely (cf. [HLW, Theorem 3.3]),

Proposition 1.6. *Let X be a non-bipartite k-regular graph with adjacency matrix A and normalized one $\Delta = \frac{1}{k}A$. Then for any distribution μ on the vertices of X and any $1 \leq t \in \mathbb{N}$,*

$$\|\Delta^t \mu - u\|_{L_2} \leq \big(\frac{\lambda(X)}{k}\big)^t$$

when u is the uniform distribution.

The non-bipartite issue is not crucial and can be avoided by considering the "lazy random walk"; cf. [LP]. One can also get similar types of bounds with the L^1-norm which is sometimes more relevant; see [HLW, §3.1].

There is a limit to what one can expect when trying to bound $\lambda(X)$. This is given by the Alon-Boppana result:

Proposition 1.7. *Let $X_{n,k}$ be an infinite family of k-regular connected graphs on n vertices where k is fixed and $n \to \infty$. Then $\lambda(X_{n,k}) \geq 2\sqrt{k-1} - o(1)$.*

This suggests the following definition:

Definition 1.8. A k-regular finite graph X is called a *Ramanujan graph* if $\lambda(X) \leq 2\sqrt{k-1}$.

So, Ramanujan graphs are, in some sense, optimal expanders. The most general known result gives for every k of the form $p^\alpha + 1$, where p is a prime and $\alpha \in \mathbb{N}$, an infinite family of k-regular Ramanujan graphs ([Mo], [LSV2]; see also [LPS1], [LPS2], [M2], [M3], and [Va2]). We mention in passing that for every k which is not of this form, it is not known if such an infinite family exists. The first open case is $k = 7$.

1.3. **Cayley graphs and representation theory.** A particularly nice way to construct graphs which are very symmetric is via Cayley graphs. Recall that if G is group and Σ a symmetric subset of G (i.e., $s \in \Sigma$ iff $s^{-1} \in \Sigma$), the Cayley graph $\mathrm{Cay}(G;\Sigma)$ of G w.r.t. Σ is the graph whose vertex set is G and $a \in G$ is connected to $\{sa | s \in \Sigma\}$. This is a k-regular graph with $k = |\Sigma|$. It is connected iff Σ generates G.

The expansion properties of $\mathrm{Cay}(G;\Sigma)$ can be reformulated in representation-theoretic terms. To this end, let us define:

Definition 1.9. Let G be a group, and let Σ be a subset of G. We say that $\varepsilon' > 0$ is a *Kazhdan constant* of G w.r.t. Σ if for every unitary representation $\rho : G \to U(H)$, where H is a Hilbert space and $U(H)$ the group of unitary operators, without a non-zero fixed vector, and for every $0 \neq v \in H$, there exists $s \in \Sigma$ such that $\|\rho(s)v - v\| \geq \varepsilon' \|v\|$.

One can see that in this case Σ generates G.

Definition 1.10. A discrete group Γ is said to have the *Kazhdan property* (T) if it has some finite set of generators Σ with Kazhdan constant $\varepsilon' > 0$.

One can prove that if this happens for one Σ, it is so for any set of generators, with possibly different ε'.

The Kazhdan constant is another way to express the expansion of Cayley graphs.

Proposition 1.11. *(i) For every $0 < \varepsilon' \in \mathbb{R}$, there exists $\varepsilon = f_1(\varepsilon') > 0$ s.t. if G is a finite group with a symmetric set of generators Σ and Kazhdan constant ε', then $\varepsilon(\mathrm{Cay}(G;\Sigma)) \geq \varepsilon$, i.e., $\mathrm{Cay}(G;\Sigma)$ is an ε-expander.*

(ii) For every $k \in \mathbb{N}$ and every $0 < \varepsilon \in \mathbb{R}$, there exists $\varepsilon' = f_2(k,\varepsilon)$ such that if G is a finite group with a symmetric set Σ of k generators with $\varepsilon(\mathrm{Cay}(G;\Sigma)) \geq \varepsilon$, then $\varepsilon' = f_2(k,\varepsilon)$ is a Kazhdan constant for G w.r.t. Σ.

So, at least as long as k is fixed, the expansion constant and the Kazhdan constant are closely related. Assume now that Γ is an infinite group generated by a finite symmetric set Σ and assume that $\mathcal{L} = \{N_i\}_{i\in I}$ is an infinite collection of finite index normal subgroups of Γ. We can deduce from Proposition 1.11:

Proposition 1.12 ([M1])**.** *If Γ has the Kazhdan property (T), i.e., there exists $\varepsilon' > 0$ which is a Kazhdan constant of Γ w.r.t. Σ, then all the finite quotients $\mathrm{Cay}(\Gamma/N_i;\Sigma)$, $i \in I$, are ε-expanders, where $\varepsilon > 0$ depends only on ε'.*

The fact that there are groups with property (T) is a non-trivial result due originally to Kazhdan (see §2.2 below for more). For example, $\Gamma = \mathrm{SL}_3(\mathbb{Z})$, the integral 3×3 matrices of determinant 1 is such a group and so the Cayley graphs of its quotients $\mathrm{SL}_3(\mathbb{Z}/m\mathbb{Z})$, $m \in \mathbb{N}$, form a family of ε-expanders w.r.t. a fixed set of generators coming from $\mathrm{SL}_3(\mathbb{Z})$, e.g., $\{A^{\pm 1}, B^{\pm 1}\}$, where

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

We will come back to many more examples of this kind in Section 2. Here we only observe that in order to deduce the conclusion of Proposition 1.12, we need a weaker property than (T), the so-called (τ). Due to its importance we will give the definition, repeating the notation again:

Definition 1.13. Let Γ be a group, with a collection $\mathcal{L} = \{\mathcal{N}_i\}_{i\in I}$ of finite index normal subgroups. We say that Γ has *property* $(\boldsymbol{\tau})$ w.r.t. $\mathcal{L}$ if there exists a symmetric subset Σ of Γ and an $0 < \varepsilon' \in \mathbb{R}$ such that for every finite quotient $G_i = \Gamma/N_i$, $i \in I$, ε' is a Kazhdan constant for G_i with respect to Σ (or more precisely w.r.t. $\Sigma N_i/N_i$). An equivalent way to say it is that for every unitary representation $\rho : \Gamma \to U(H)$, with $\mathrm{Ker}\rho \supset N_i$ for some i, without a non-zero fixed vector, and every $0 \neq v \in H$, there exists $s \in \Sigma$ such that $\|\rho(s)v - v\| > \varepsilon'\|v\|$. If $\mathcal{L}$ is the family of *all* finite index normal subgroups of Γ, we simply say that Γ has property (τ).

The equivalence of Proposition 1.11 shows:

Proposition 1.14. *The group Γ has property (τ) w.r.t. $\mathcal{L} = \{N_i\}_{i\in I}$ if and only if there exists a symmetric subset Σ of Γ and $\varepsilon > 0$, such that all the Cayley graphs $\mathrm{Cay}(\Gamma/N_i;\Sigma)$ are ε-expanders.*

There exist groups (e.g., $\Gamma = \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$) which have (τ) but not (T) while $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ has neither (T) nor (τ), but it has (τ) w.r.t. the family

$$\mathcal{L} = \{\Gamma(m) = \mathrm{Ker}\big(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\big)\}_{m\in\mathbb{N}},$$

the family of congruence subgroups; see §2.4 below.

Some of the recent breakthroughs are far-reaching extensions of this last fact; extensions which have some remarkable applications.

1.4. **Expanders and Riemannian manifolds.** Let M be an n-dimensional connected closed Riemannian manifold (i.e., compact with no boundary; much of the theory can be extended to a more general setting but for simplicity of the exposition we will stick to the closed case). Let $\Delta = -\mathrm{div}(\mathrm{grad})$ be the Laplacian operator of $L^2(M)$. Its eigenvalues $0 = \lambda_0(M) < \lambda_1(M) \leq \lambda_2(M) \leq \cdots$ form a discrete subset (with multiplicities) of $\mathbb{R}_+$, called the *spectrum* of M.

The spectrum of M is very much related to the geometry of M and these relations are the subject of *spectral geometry*. A more intuitive description of Δ is given by the formula,

$$(\Delta f)(p) = \lim_{r \to 0} \frac{2n}{r^2} \Big(\frac{\int_{S^r} f}{\mathrm{vol}(S_r)} - f(p) \Big),$$

where $n = \dim M$, $p \in M$, $f \in L^2(M)$, and S_r is the sphere of radius r around p. This description is similar to the combinatorial Laplacian as an averaging operator, as described in §1.2.

We will mainly be interested in $\lambda_1(M)$, which can be described directly without a reference to Δ.

Proposition 1.15.

$$\lambda_1(M) = \inf \left\{ \frac{\int_M \|df\|^2}{\int_M |f|^2} \Big| f \in C^\infty(M), \int_M f = 0 \right\}.$$

Another important geometric invariant of M, whose connection with expanders is even more evident, is the Cheeger constant:

Definition 1.16. The *Cheeger constant* $h(M)$ is

$$h(M) = \inf_E \frac{\mu(E)}{\min(\nu(A), \nu(B))},$$

where E runs over all the compact $(n-1)$-dimensional submanifolds of M which divide M into disjoint submanifolds A and B. Here $\mu(E)$ is the *area* of E, and ν is the volume form of M.

Just as for graphs, $h(M)$ is closely related to $\lambda_1(M)$. In fact, historically the relation between the expansion/Cheeger constant and λ_1 was discovered first for manifolds and only later on for graphs; see [L1] for historical notes.

Theorem 1.17 (Cheeger's inequality)**.** $\lambda_1(M) \geq \frac{h^2(M)}{4}$.

Buser proved a converse to this inequality, which depends on the Ricci curvature $R(M)$. We will not bother defining it here, but rather send the reader to [Bu], [L1] and the references therein. But let us quote:

Theorem 1.18. *If $R(M) \geq -(n-1)a^2$ for some $a \geq 0$, where $n = \dim M$, then $\lambda_1(M) \leq 2a(n-1)h(M) + 10h^2(M)$.*

What is important for us is that in the case of a bounded Ricci curvature, which will hold in all our considerations, $\lambda_1(M)$ is also bounded above by a function of $h(M)$.

The more precise connection between these notions and expander graphs will be given in Theorem 1.20 below. Let us point out here the basic intuition:

Let $\tilde{M}$ be the universal cover of M, $\Gamma = \pi_1(M)$ the fundamental group of M, and F a fundamental domain for the action of Γ on $\tilde{M}$, i.e., F is an open subset of $\tilde{M}$, whose closure $\bar{F}$ is compact and such that $\Gamma\bar{F} = \tilde{M}$ and for every $1 \neq \gamma \in \Gamma$, $\gamma(\bar{F}) \cap \bar{F} \subseteq \bar{F} \smallsetminus F$. Standard covering theory shows that the finite set $\Sigma = \{\gamma \in \Gamma \big| \gamma\bar{F} \cap \bar{F} \text{ is of codimension } 1\}$ is a symmetric set of generators for Γ. One can visualize $\mathrm{Cay}(\Gamma;\Sigma)$ in the following way: Fix $x_0 \in F$ and put a vertex at the interior point γx_0 of the tesselate γF of F (naturally this vertex will represent γ; note that γ is unique for the given tesselate). Now, draw an edge between $\gamma_1 x_0$ and $\gamma_2 x_0$ if $\overline{\gamma_1 F} \cap \overline{\gamma_2(F)}$ is of codimension 1. One can easily check that what we get is exactly a "drawing" of $\mathrm{Cay}(\Gamma;\Sigma)$ on $\tilde{M}$.

Moreover, if Γ_1 is a normal subgroup of Γ of finite index, then the "projection" of the above graph to $M_1 = \tilde{M}/\Gamma_1$ is exactly the Cayley graph $\mathrm{Cay}(\Gamma/\Gamma_1;\Sigma)$. We therefore get that the combinatorial graphs $\mathrm{Cay}(\Gamma/\Gamma_1;\Sigma)$ when Γ_1 runs over the finite index normal subgroups of Γ are "approximations" of the finite sheeted normal covers of M.

This enables us to relate the expansion properties of these Cayley graphs to the asymptotic expansion of $h(M_1)$ and similarly with λ_1 of the graphs and of the manifolds; see Theorem 1.20 below.

1.5. **Expanders and measure theory.** Let G be a compact group. A *mean* m on G is a linear functional $m : L^\infty(G) \to \mathbb{R}$ satisfying:

(i) $m(f) \geq 0$ if $f \geq 0$;
(ii) $m(\chi_G) = 1$, where χ_G is the constant function 1 on G.

We say that it is a **G**-*invariant mean* if it also satisfies:

(iii) $m(g.f) = m(f)$ for every $g \in G$ and $f \in L^\infty(G)$, where $g.f(x) = f(g^{-1}x)$, i.e., G-left invariant.

An example of an invariant mean is the Haar measure of G, which is also countably additive on subsets of G. In general, it is possible for G to have invariant means different than the (unique) Haar measure. For example, $G = S^1$ (the circle) has such means. But:

Theorem 1.19 ([Sh1])**.** *Let Γ be a finitely generated group, and let $\mathcal{L} = \{N_i\}_{i\in\mathbb{N}}$ be a decreasing chain of finite index normal subgroups of Γ. Let $G = \varprojlim_{i\in\mathbb{N}} \Gamma/N_i$ be the profinite completion of Γ w.r.t. $\mathcal{L}$. Then the following are equivalent:*

(i) *Γ has (τ) w.r.t. $\mathcal{L}$.*
(ii) *The Haar measure on G is the only Γ-invariant mean on G.*

So, we also have a measure-theoretic characterization of property (τ).

1.6. **A summary of property (τ).** Let Γ be a finitely generated group generated by a finite symmetric set Σ. Let $\mathcal{L} = \{N_i\}_{i\in\mathbb{N}}$ be a decreasing chain of finite index normal subgroups of Γ.

Theorem 1.20. *The following conditions are equivalent:*

(i) Γ has property (τ) w.r.t. $\mathcal{L}$; i.e., there exists $\varepsilon_1 > 0$ s.t. if $\rho : \Gamma \to U(H)$ is a unitary representation of Γ on a Hilbert space H without non-zero $\rho(\Gamma)$ fixed points and such that $\mathrm{Ker}(\rho) \geq N_i$ for some i, then for every $0 \neq v \in H$, there exists $s \in \Sigma$ with $\|\rho(s)v - v\| \geq \varepsilon_1\|v\|$.
(ii) There exists $\varepsilon_2 > 0$ such that all the Cayley graphs $\mathrm{Cay}(\Gamma/N_i;\Sigma)$ are ε_2-expanders.

(iii) *There exists* $\varepsilon_3 > 0$ *such that* $h(\mathrm{Cay}(\Gamma/N_i);\Sigma)) \geq \varepsilon_3$ *(see Definition* 1.2*).*

(iv) *There exists* $\varepsilon_4 > 0$ *such that* $\lambda_1(\mathrm{Cay}(\Gamma/N_i;\Sigma)) \leq k - \varepsilon_4$ *for every* $i \in \mathbb{N}$*, where* $k = |\Sigma|$*.*

(v) *The Haar measure of* $\hat{\Gamma}_{\mathcal{L}} = \varprojlim \Gamma/N_i$ *is the only* Γ*-invariant mean on* $L^\infty(\hat{\Gamma}_{\mathcal{L}})$*. If in addition* $\Gamma = \pi_1(M)$ *for some closed Riemannian manifold* M*, and* $\{M_i\}_{i\in\mathbb{N}}$ *are the finite sheeted Galois covers of* M *corresponding to* $\{N_i\}_{i\in\mathbb{N}}$*, then we also have*

(vi) *There exists* $\varepsilon_5 > 0$ *such that* $h(M_i) \geq \varepsilon_5$ *(see Definition* 1.16*) for every* $i \in \mathbb{N}$*.*

(vii) *There exists* $\varepsilon_6 > 0$ *such that* $\lambda_1(M_i) \geq \varepsilon_6$ *for every* $i \in \mathbb{N}$ *(see Proposition* 1.15*).*

The equivalence of all the properties except for (v) can be found in [L1, Theorem 4.3.2]. For (v) see [Sh1].

So property (τ) can be seen and expressed in many ways: combinatorial, representation theoretic, geometric and measure theoretic. This is what makes it so useful in a variety of applications as we will see in the next sections.

2. Examples of expanders

It is by no means clear that expander graphs exist, though it is not difficult to prove their existence by random considerations. Various deep mathematical tools have been used to give explicit constructions (Kazhdan property (T), Ramanujan Conjecture, etc.) We review these briefly here (again, more details can be found in [L1] and the references therein). Most of the current section is devoted to a description of the two important developments of the last decade:

(1) All non-abelian finite simple groups are expanders in a uniform way.
(2) Many linear groups have property (τ) with respect to congruence subgroups.

The second result has important applications to number theory, group theory, and geometry, which will be described in later sections.

2.1. **Random graphs and the Zig-Zag construction.** It is relatively easy to show that for a fixed $k \geq 3$ there exists an $\varepsilon > 0$ s.t. a random (n,k)-graph, i.e., a k-regular graph on n vertices, is an ε-expander with probability tending to 1 as n goes to infinity. The subtle issue (which we will ignore here) is how to describe a good model of random (n,k)-graphs. Anyway, this has been known for many years (see [L1] and §1.1 above). More recently a much deeper result (Alon's conjecture) has been proved by Friedman [Fr].

Theorem 2.1. *For every* $\varepsilon > 0$ *and* $k \geq 3$*,*

$$\mathrm{Prob}\big(\lambda(X) \leq 2\sqrt{k-1} + \varepsilon\big) = 1 - o_n(1)$$

when X *is a random* (n,k)*-graph; i.e., almost every such* X *is almost Ramanujan.*

It is interesting to repeat here the open question mentioned in §1.2, whether for *every* $k \geq 3$ there exist infinitely many Ramanujan graphs. While Theorem 2.1 hints toward a positive answer, it by no means implies that. Moreover, one may be tempted to conjecture, following Theorem 2.1, that almost every (n,k)-graph is Ramanujan. But quite a lot of computational data suggests the contrary, namely that the probability of a k-regular graph on n vertices to be Ramanujan tends,

when $n \to \infty$, to some constant strictly between 0 and 1. We do not know any result or even a conjecture that predicts what is this interesting number.

Of course, for many applications one wants explicit constructions. A lot of work has been dedicated to this goal, and various deep methods have been used. In a breakthrough paper, Reingold, Vadhan, and Wigderson [RVW] showed that there is an elementary combinatorial way to build expanders via the Zig-Zag product of graphs, which they introduced. We describe this subject here very briefly sending the reader to [RVW] for details (or to [HLW] for a very clear exposition).

The Zig-Zag product is a method that, given two graphs X and Y, where X is an (n, m) graph (i.e., m-regular graph on n vertices) and Y an (m, d)-graph, produces $X \circ Y$, an (mn, d^2)-graph. (This is *not* a commutative operation.) In [RVW], it is shown that one can bound the "spectral gap" of $X \circ Y$ by the spectral gaps of X and Y. They then start, for a small fixed integer d, with a (d^4, d)-graph $X = X_0$ with a good spectral gap (such a graph can be found by an exhaustive search in constant time) and define by induction $X_1 = X^2$ and $X_{n+1} = (X_n)^2 \circ X$ for $n \geq 1$. (If Y is a graph, we denote Y^2 to be the graph with the same vertex set as Y, putting an edge between the endpoints of any path of length 2 in the original graph.) Note that X_n is a (d^{4n}, d^2)-graph, so the family $\{X_n\}_{n=1}^{\infty}$ is a family of d^2-regular graphs (independent on n). Induction and the spectral control give that this is a family of expanders.

This construction turns out to be quite useful in various applications in computer science, sometimes giving better results than using the expanders constructed by the other methods. Still, as far as we know, it has not been used for applications in pure mathematics, which is our main interest in these notes. For the kind of applications we emphasize here, one usually needs expanders which are Cayley graphs (or at least somewhat symmetric). The Zig-Zag product has something to say about Cayley graphs of semidirect products of groups (see [ALW], [MW] and especially [RSW]), but one still needs the other approaches. These will be described in the next subsections.

2.2. **Kazhdan property (T) and finite simple groups.** The seminal work of Kazhdan [Ka] on property (T) of high-rank simple Lie groups and their lattices (= discrete subgroups of finite covolume) opened the door for Margulis to give the first explicit examples of expanders. Let us repeat what we already said in §1.3.

Proposition 2.2. *Let Γ be a group with property (T) generated by a finite symmetric set Σ, and let $\mathcal{L} = \{N \big| N \lhd \Gamma,\ [\Gamma : N] < \infty\}$ be the family of finite index normal subgroups of Γ. Then there exists an $\varepsilon > 0$ such that all $\mathrm{Cay}(\Gamma/N; \Sigma)$ are ε-expanders.*

So, the issue (which is non-trivial) is to show that such Γ's exist. This was done by Kazhdan and has been generalized substantially in recent years:

Theorem 2.3. *Let G be a simple Lie group (e.g., $G = \mathrm{SL}_n(\mathbb{R})$) of $\mathbb{R}$-rank ≥ 2 (e.g., $n \geq 3$). If Γ is a lattice in G (e.g., $\Gamma = \mathrm{SL}_n(\mathbb{Z})$), then Γ has property (T).*

Theorem 2.3 combined with Proposition 2.2 gives:

Corollary 2.4. *For a fixed n and a fixed finite symmetric set of generators Σ of $\mathrm{SL}_n(\mathbb{Z})$, the Cayley graphs $\mathrm{Cay}(\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}), \Sigma)$ are all k-regular ε-expanders for $k = |\Sigma|$ and some $\varepsilon = \varepsilon(n, \Sigma) > 0$.*

$\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ or more precisely $\mathrm{PSL}_n(\mathbb{Z}/p\mathbb{Z})$, the quotient by the center, is the prototype of finite simple groups of Lie type. Many more infinite families of finite simple groups can be deduced, by a similar method, to be expanders. But a more challenging conjecture was put forward in 1989 by Babai, Kantor, and Lubotzky [BKL]:

Conjecture 2.5. *There exist $k \in \mathbb{N}$ and $\varepsilon > 0$ such that every non-abelian finite simple group G has a symmetric set of generators Σ of size $\leq k$ such that $\mathrm{Cay}(G;\Sigma)$ is an ε-expander.*

For a number of years this conjecture has been open and even some suspicion arose (including by some of its proposers) that perhaps it is not true and expansion is a property restricted to "bounded rank". But it turned out that this conjecture is true, and it is now fully proved, and its proof required an ensemble of very different methods. The big breakthrough came with two works of Kassabov [K1] and [K2] ([K1] was very much influenced by [KN], which in turn was modeled on [Sh3]). Rather than being loyal to the historical development, let us start with an even more recent result (which was influenced by [KN]). To state the result, we first need a definition. Let R be a ring with an identity. For $n \geq 3$, define $E_n(R)$ to be the multiplicative subgroup of the ring of $n \times n$ matrices $M_n(R)$ generated by $E_{ij}(r)$ for all $1 \leq i \neq j \leq n$ and $r \in R$, where $E_{ij}(r)$ is the $n \times n$ matrix with ones on the diagonal, r at the (i,j)-entry, and zero otherwise. For many commutative rings, $E_n(R)$, at least for $n \geq 3$, is nothing more than $\mathrm{SL}_n(R)$. The groups $E_n(R)$ play an important role in algebraic K-theory.

If R is a finitely generated ring, then $E_n(R)$ is a finitely generated group (for $n \geq 3$). We can now state:

Theorem 2.6 (Ershov and Jaikin-Zapirain [EJ])**.** *Let R be the free ring $R = \mathbb{Z}\langle x_1, \ldots, x_r\rangle$ in the non-commutative free variables $x_1, \ldots, x_r$. Then for every $n \geq 3$, $E_n(R)$ has the Kazhdan property (T).*

Kassabov's basic idea was to use such a result (well, he proved a weaker version of it, which was sufficient) to deduce:

Corollary 2.7. *There exist $k \in \mathbb{N}$ and $\varepsilon > 0$ such that for every $n \in \mathbb{N}$ and every prime power $q \in \mathbb{N}$, the group $\mathrm{SL}_n(\mathbb{F}_q)$ has a set Σ of k generators for which $\mathrm{Cay}(\mathrm{SL}_n(\mathbb{F}_q), \Sigma)$ is an ε-expander. Here, $\mathbb{F}_q$ is the field with q elements.*

Indeed, take $R = \mathbb{Z}\langle x_1, x_2\rangle$. It is easy to see that $M_n(\mathbb{F}_q)$ is a (finite) quotient of R. Thus by Theorem 2.6 and Proposition 2.2,

$$\mathrm{Im}\big(E_3(R) \to E_3(M_n(\mathbb{F}_q)\big)$$

are expanders. But this latter group is

$$E_3\big(M_n(\mathbb{F}_q)\big) = \mathrm{SL}_{3n}(\mathbb{F}_q).$$

Now it is not difficult to deduce that $\mathrm{SL}_n(\mathbb{F}_q)$ are expanders in a uniform way (i.e., with the same k and ε for all q and for all $n \geq 3$) since $\mathrm{SL}_{3n+1}(\mathbb{F}_q)$ and $\mathrm{SL}_{3n+2}(\mathbb{F}_q)$ are bounded products of copies of $\mathrm{SL}_{3n}(\mathbb{F}_q)$:

Definition 2.8. Let $\mathsf{A} = \{A_i\}_{i\in I}$ and $\mathcal{B} = \{B_j\}_{j\in J}$ be two families of finite groups. We say that $\mathcal{B}$ is a *bounded product* of A if there exists a constant $m \in \mathbb{N}$ such that for every $B_j \in \mathcal{B}$, there exist $A_{i_1}, \ldots, A_{i_m}$ in A and homomorphisms $\varphi_{i_t} : A_{i_t} \to B$ such that B is the product (just as a set) $\varphi_{i_1}(A_{i_1}) \cdot \ldots \cdot \varphi_{i_m}(A_{i_m})$.

The following easy lemma is very useful:

Lemma 2.9. *In the notation above, if* A *are expanders in a uniform way (i.e., same* k *and* ε*) and* $\mathcal{B}$ *is a bounded product of* A*, then* $\mathcal{B}$ *are also expanders in a uniform way (for some* k' *and* ε' *which depend on* k *and* ε*).*

The next theorem says that we can go much further than SL_n:

Theorem 2.10 (Nikolov [Ni], Lubotzky [L6])**.** *Let*

$$\mathsf{A} = \{\mathrm{SL}_n(\mathbb{F}_q) \big| n \geq 2,\ q \text{ prime power}\}$$

and let $\mathcal{B}$ *be the family of all simple groups of Lie type excluding the Suzuki groups. Then* $\mathcal{B}$ *is a bounded product of* A*.*

One can check in the proof that if one allows the use of only SL_n with $n \geq 3$, the result remains true for those groups in $\mathcal{B}$ of rank ≥ 14. Thus Conjecture 2.5 is valid for these groups. To handle all finite simple groups of Lie type, one should handle $\mathrm{SL}_2(\mathbb{F}_q)$. This will be done in §2.4 by a completely different method. With the above results this will finish all groups of Lie type except the Suzuki groups. They will be handled in §2.6 again by a completely different method. But now we will consider first the case of symmetric and alternating groups, which is of special interest.

2.3. **The symmetric groups.** Making the symmetric groups (or equivalently the alternating groups) into a family of expanders in a uniform way has been a challenging problem for almost two decades, until it was solved by Kassabov [K2].

Theorem 2.11. *There exists* $k \in \mathbb{N}$ *and* $0 < \varepsilon \in \mathbb{R}$ *such that for every* $n \geq 5, \mathrm{Sym}(n)$ *has a symmetric generating subset* Σ *with* $|\Sigma| \leq k$ *for which* $\mathrm{Cay}(\mathrm{Sym}(n); \Sigma)$ *is an* ε*-expander.*

The same result holds also with $\mathrm{Alt}(n)$, the alternating group, instead of $\mathrm{Sym}(n)$. It suffices to prove the theorem for one of these two cases.

Now, one can show that while $\mathrm{Alt}(n)$ contains many copies of groups of Lie type it is not a bounded product of such groups, so the results of the previous section do not suffice. Still Kassabov looked at n's of the form $n = d^6$ for $d = 2^{3r} - 1$ for some $r \in \mathbb{N}$. Based on ideas similar to the ones in the previous section, he showed that the groups $\Delta_r = \mathrm{SL}_{3r}(\mathbb{F}_2)^{d^5}$ are ε_0-expanders w.r.t. generating sets F of size at most 40. He then embedded Δ_r in $\mathrm{Alt}(n)$ in six different ways which give six copies of F in $\mathrm{Alt}(n)$. He then showed that $\mathrm{Alt}(n)$ are uniformly expanders with respect to the union of these six sets. It should be stressed that $\mathrm{Alt}(n)$ is not a bounded product of these six copies and the argument is far more involved, working with the representation-theoretic version of expansion. One should work with the various irreducible representations of $\mathrm{Alt}(n)$, and Kassabov divided them into two classes, giving different arguments according to their Young diagrams. The reader is referred to [K2] for details and to [KLN] for a sketch of the proof.

2.4. **Property** (τ)**,** SL_2**, and groups of low rank.** As already mentioned in §1.3, one does not need the full power of property (T) to deduce that the finite quotients of the finitely generated group Γ give a family of expanders. Property (τ) (Definition 1.13) suffices.

The prototype of groups with (τ) w.r.t. some family is $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Let us set some notation: $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and for $m \in \mathbb{N}$, $\Gamma(m) = \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}))$—the congruence subgroup mod m. The group Γ acts on $\mathbb{H} = \{a + bi | a \in \mathbb{R}, 0 < b \in \mathbb{R}\}$ by Möbius transformations: $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $z \in \mathbb{H}$, then $\gamma(z) = \frac{az+b}{cz+d}$. The upper half-plane $\mathbb{H}$ is endowed with a Riemannian metric of constant curvature -1. This is the hyperbolic plane. The quotients $\Gamma(m) \setminus \mathbb{H}$ are (non-compact) Riemann surfaces of finite volume.

Theorem 2.12 (Selberg [Sel]). *For every $m \in \mathbb{N}$, $\lambda_1\big(\Gamma(m) \setminus \mathbb{H}\big) \geq \frac{3}{16}$.*

Selberg conjectured that $\frac{1}{4}$ is the right lower bound. The current world record is $\lambda_1 \geq 0.238$ due to Kim and Sarnak [Ki].

Anyway, Theorem 1.20 gives:

Corollary 2.13. *For a fixed set of generators Σ of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, e.g., $\Sigma = \left\{\left(\begin{smallmatrix} 1 & \pm 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ \pm 1 & 1 \end{smallmatrix}\right)\right\}$, the Cayley graphs $\mathrm{Cay}\big(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}); \Sigma\big)$ are all ε-expanders for some $\varepsilon > 0$ which may depend on Σ but not on m.*

It should be stressed that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ has negative solutions to the congruence subgroup problem and it has many more finite quotients than just $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. The family of *all* finite quotients of Γ does not form a family of expanders. So in the terminology of Definition 1.13 above, Γ does not have property (τ), but it has property (τ) w.r.t. the family of congruence subgroups.

The last corollary implies, in particular, that the groups $\{\mathrm{SL}_2(p) | p \text{ prime}\}$ can be made into a family of 4-regular Cayley graphs which are expanders uniformly (i.e., same ε).

Analogous results for arithmetic groups in positive characteristic such as $\mathrm{SL}_2(\mathbb{F}_p[t])$ or $\mathrm{SL}_2(\mathbb{F}_p[t, t^{-1}])$ (when this time a result of Drinfeld replaces the theorem of Selberg) can make, *for a fixed p*, the family $\{\mathrm{SL}_2(\mathbb{F}_{p^\alpha}) \big| \alpha \in \mathbb{N}\}$ into a family of expanders.

Can we make all of these families together $\{\mathrm{SL}_2(\mathbb{F}_{p^\alpha}) \big| p \text{ prime}, \alpha \in \mathbb{N}\}$ into a family of expanders?

The answer is yes, but the proof is more subtle. See [L6] (and a sketch in [KLN]). Here we only mention that the proof uses the *explicit* constructions of Ramanujan graphs (as a special case of Ramanujan complexes) in [LSV2] (see also [LSV1]). It is shown there that for a fixed p, $\mathrm{SL}_2(\mathbb{F}_{p^\alpha})$ are $(p+1)$-regular Ramanujan graphs. The $p+1$ generators involved are the conjugates of a fixed element $C_{p,\alpha}$ of $\mathrm{SL}_2(\mathbb{F}_{p^\alpha})$ by a fixed non-split torus $T \subseteq \mathrm{SL}_2(\mathbb{F}_p) \subseteq \mathrm{SL}_2(\mathbb{F}_{p^\alpha})$. Then we use the fact that $\mathrm{SL}_2(p)$ are expanders with respect to $\Sigma_0 = \left\{\left(\begin{smallmatrix} 1 & \pm 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ \pm 1 & 1 \end{smallmatrix}\right)\right\}$ to deduce that $\mathrm{SL}_2(\mathbb{F}_{p^\alpha})$ are expanders w.r.t. the symmetric set of six generators $\Sigma_0 \cup \{C_{p,\alpha}^{\pm 1}\}$ in a uniform way. So Selberg's Theorem and Drinfeld's solution to the positive characteristic Ramanujan Conjecture for GL_2 are both needed for that goal.

Now all the $\mathrm{SL}_2(\mathbb{F}_{p^\alpha})$ are expanders and so all $\{\mathrm{SL}_n(\mathbb{F}_{p^\alpha}) \big| p, n, \alpha \in \mathbb{N},\ p \text{ prime}\}$ are expanders in a uniform way (same k, same ε). We can appeal again to Theorem 2.10 and Lemma 2.9 to deduce that all finite simple groups of Lie type, with the possible exceptions of the Suzuki groups, are expanders in a uniform way.

Suzuki groups have to be excluded here as they do not contain copies of $\mathrm{SL}_n(\mathbb{F}_{p^\alpha})$. Indeed their order is not divisible by 3. (A classical result of Glauberman in the early days of the classification project of finite simple groups asserts that this property characterizes them! See [Gl].) But the Suzuki groups are not exceptional for our problem; i.e., they are also expanders. But this requires another method and has to wait for §2.7.

2.5. **Property (τ) with respect to congruence subgroups.** Selberg's Theorem 2.12 was a starting point for many works which extended it to general arithmetic groups. The results are of importance in number theory (automorphic forms), representation theory, and geometry. In this section, we will describe them from our perspective.

Let k be a global field, i.e., a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$. Let G be a simple algebraic group defined over k with a fixed embedding $\rho : G \hookrightarrow \mathrm{GL}_n$ for some n. Let θ be the ring of integers of k, and let S be a non-empty finite set of valuations of k containing S_∞, the set of Archimedean valuations. Let $\theta_S = \{x \in k \big| v(x) \geq 0,\ \forall v \notin S\}$ be the ring of S-integers, so $\theta_S = \theta$ if $S = S_\infty$. Let $\Gamma = \rho\big(G(k)\big) \cap \mathrm{GL}_n(\theta_S)$. A subgroup of G commensurable with Γ is called an *S-arithmetic subgroup* of G. For a non-zero ideal I of θ_S (which is always of finite index) we denote $\Gamma(I) = \mathrm{Ker}\big(\Gamma \to \mathrm{GL}_n(\theta_S/I)\big)$. An S-arithmetic subgroup of G containing $\Gamma(I)$ for some I is called a (S-) *congruence subgroup*.

While the definition of Γ may depend on the choice of the representation ρ, the classes of arithmetic and congruence subgroups do not.

Definition 2.14. We say that Γ has the Selberg property if it has property (τ) with respect to the congruence subgroups $\{\Gamma(I)\}_{0 \neq I \lhd \theta_S}$.

Again, if true for Γ, then it is true for all the arithmetic groups in its commensurability class.

The group $\Gamma = G(\theta_S)$ sits as an irreducible lattice in the Lie group $H = \prod_{v \in S} G(k_v)$, where k_v is the completion of k w.r.t. v.

Recall that a *lattice* Λ in H is a discrete subgroup, where $\Lambda \setminus H$ carries an H-invariant finite measure. It is *irreducible* if its projection to each proper subproduct is dense. In many cases, H has Kazhdan property (T):

Theorem 2.15 (Kazhdan)**.** *If k_v-rank $(G) \geq 2$ for every $v \in S$, then $H = \prod_{v \in S} G(k_v)$, and all its lattices have property (T).*

For having (τ) we need less:

Theorem 2.16 (Lubotzky and Zimmer [LZi])**.** *If one of the non-compact factors of H has property (T), then all irreducible lattices have property (τ).*

Selberg's Theorem 2.12 shows that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, which has neither (T) nor (τ), still has (τ) w.r.t. congruence subgroups. This has been extended to more general arithmetic groups. This is the work of many people. The most general method (and actually also the simplest!) is due to Burger and Sarnak [BS] who proved:

Theorem 2.17. *Let $L_1 \leq L_2$ be two non-compact simple Lie groups with arithmetic lattices $\Lambda_i \leq L_i, i = 1, 2$, and $\Lambda_1 = L_1 \cap \Lambda_2$. Then:*

(i) If Λ_1 has property (τ), so does Λ_2.
(ii) If Λ_1 has the Selberg property, so does Λ_2.

Many (in some sense "most") simple k-algebraic groups G contain a copy of SL_2, so Theorems 2.12 and 2.17 imply the Selberg property for the arithmetic subgroups of G. By the Galois cohomology method one can classify the arithmetic lattices for which this method does not apply. These need some other (more difficult) techniques. This was done by Clozel [Cl] using automorphic forms methods. As a result it is now known that all arithmetic lattices in semisimple groups over local fields of characteristic zero have the Selberg property. As far as we know this has not been completed yet for the positive characteristic case.

2.6. **Sum-products in finite fields and expanders.** The results described in the previous section gave a fairly complete picture of the congruence quotients of an arithmetic group of the form $\Gamma = G(\theta_S)$ described there, as being expanders with respect to generators coming from "the mother group" Γ. For example, the family

$$\{\mathrm{Cay}\big(\mathrm{SL}_2(\mathbb{F}_p); \left(\begin{smallmatrix}1 & \pm 1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ \pm 1 & 1\end{smallmatrix}\right)\big) | p \text{ prime}\}$$

forms a family of ε-expanders for some $\varepsilon > 0$ since $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ generate $\mathrm{SL}_2(\mathbb{Z})$. A similar conclusion (for a different $\varepsilon > 0$) is true for the family

$$\{\mathrm{Cay}\big(\mathrm{SL}_2(\mathbb{F}_p); \left(\begin{smallmatrix}1 & \pm 2\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ \pm 2 & 1\end{smallmatrix}\right)\big) | p > 2 \text{ prime}\}$$

even though Γ is not generated by $\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 2 & 1\end{smallmatrix}\right)$; these two matrices generate a finite index subgroup of Γ, and essentially the same arguments as before also apply for it.

But now what about

$$\{\mathrm{Cay}\big(\mathrm{SL}_2(\mathbb{F}_p); \left(\begin{smallmatrix}1 & \pm 3\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ \pm 3 & 1\end{smallmatrix}\right)\big) \mid p > 3 \text{ prime}\}?$$

Is this a family of ε-expanders for some $\varepsilon > 0$? The issue here is that the subgroup $\Lambda = \langle \left(\begin{smallmatrix}1 & 3\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 3 & 1\end{smallmatrix}\right)\rangle$ is of infinite index in $\mathrm{SL}_2(\mathbb{Z})$; still when taken mod p, the image of Λ generates $\mathrm{SL}_2(\mathbb{F}_p)$ for every $p > 3$. Combinatorially, one should expect a similar ε-expander conclusion for them, but the methods of the previous sections do not apply here. This problem was presented in 1992 in [L2] and was popularized under the nickname (given by Alex Gamburd) the "Lubotzky 1-2-3 problem".

In fact this 1-2-3 problem is just an attractive special case of a much more general problem: Let $\Gamma = G(\theta_S)$ as in the previous section, but for simplicity of notation, let us take $k = \mathbb{Q}$, $\theta = \mathbb{Z}$, and $S = S_\infty$, so $\Gamma = G(\mathbb{Z})$, e.g., $\Gamma = \mathrm{SL}_d(\mathbb{Z})$. Let Λ be a finitely generated subgroup of Γ, generated by a set Σ, which is Zariski dense in Γ. Note that being dense in the Zariski topology is quite a weak assumption. For example for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, every subgroup Λ which is not virtually cyclic, e.g., $\Lambda = \langle \left(\begin{smallmatrix}1 & 3\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 3 & 1\end{smallmatrix}\right)\rangle$, is Zariski dense. Assume further that G, as an algebraic group, is connected, simply connected, and simple (e.g., $G = \mathrm{SL}_d$). Then the *strong approximation theorem for linear groups* ([MVW], [No], [W], [Pi]; see [LS, Window 9] for an exposition) says that there exists $m_0 \in \mathbb{N}$ such that for every $m \in \mathbb{N}$ with $(m, m_0) = 1$, the projection of Λ to $G(\mathbb{Z}/m\mathbb{Z})$ is onto. In other words, it says that $\mathrm{Cay}\big(G(\mathbb{Z}/m\mathbb{Z}); \Sigma\big)$ is a connected graph. Being an expander is a very strong form of being connected. It thus naturally suggests the question whether these graphs form a family of ε-expanders. The so-called "Lubotzky 1-2-3 problem" is just a baby version of this much more general question.

The first steps and several interesting partial results toward the 1-2-3 problem were taken in [Ga1] and [Sh2]. But the main breakthroughs came in recent years, starting with the work of Helfgott and continued by others. We now turn to describe these developments.

Let us start by stating the main result of [H1]:

Theorem 2.18. *Let $G = \mathrm{SL}_2(\mathbb{F}_p)$, and let A be a generating subset of G. Let $0 < \delta < 1$ be a constant. Then:*

(a) *If $|A| < |G|^{1-\delta}$, then $|A \cdot A \cdot A| \geq C|A|^{1+\varepsilon}$, where C and ε depend only on δ.*

(b) *If* $|A| \geq |G|^{1-\delta}$, *then* $A \cdot \ldots \cdot A = G$, *i.e., the product of* k *copies of* A *is* G, *where* k *depends only on* δ.

Before elaborating on its importance for expanders, let us put it in a more general context.

The sum-product results form a body of various theorems asserting that if $F = \mathbb{F}_p$ is a finite field of a prime order p and A is a subset of $\mathbb{F}_p$, which is not too large, then either the set of products $A \cdot A = \{a \cdot b | a, b \in A\}$ or the set of sums $A + A = \{a + b | a, b \in A\}$ is significantly larger than A. Here is a typical result in this area, called also "additive combinatorics" ([TV]).

Theorem 2.19 ([BKT])**.** *If* A *is a subset of* $\mathbb{F}_p$, p *prime, with* $p^\delta \leq |A| \leq p^{1-\delta}$ *for some* $\delta > 0$, *then* $|A + A| + |A \cdot A| \geq c|A|^{1+\varepsilon}$, *where* c *and* ε *depend only on* δ.

The main idea of Helfgott was to convert the growth of a subset B of $\mathrm{SL}_2(\mathbb{F}_p)$ when taking the product $B \cdot B \cdot B$ with the growth of $A = \mathrm{tr}(B) = \{\mathrm{tr}(g) | g \in B\}$ as a subset of $\mathbb{F}_p$ under sums and products. He also showed that the sizes of B and A can teach a lot about each other. This enabled him to deduce Theorem 2.18 from Theorem 2.19. His work is quite complicated from a technical point of view. Some subsequent works simplified and extended his work (see below) and eventually made the conclusion free of the use of sum-products results. Still, various ideas of Helfgott are also crucial in those extensions.

An interesting corollary of Theorem 2.18 is that there exists a constant C such that for every set of generators Σ of $\mathrm{SL}_2(\mathbb{F}_p)$,

$$\mathrm{diam}(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); \Sigma)) \leq \log(p)^C.$$

This was the first infinite class of groups for which the following long-standing conjecture of Babai was proved:

Conjecture 2.20. *There exists a constant* C, *possibly* $C = 2$, *such that for every non-abelian finite simple group* G *and for every set of generators* Σ, *the diameter is polylogarithmic (i.e.,* $\mathrm{diam}\ \mathrm{Cay}(G; \Sigma)) = O((\log |G|)^C)$.

The example $\mathrm{Cay}(\mathrm{Sym}(n); \tau = (1, 2), \sigma^{\pm} = (1, 2, \ldots, n)^{\pm 1}\}$ and similar ones for $\mathrm{Alt}(n)$ show that one cannot expect better than $C = 2$ (see [L1]).

While Helfgott's result solved Babai's conjecture for $\mathrm{SL}_2(\mathbb{F}_p)$, it fell short of showing that these are expanders. (By the way, expanders give rise to logarithmic diameter, i.e., $C = 1$ in the last conjecture.) It did not solve the 1-2-3 problem either. But shortly afterwards Bourgain and Gamburd [BG1] made a second major breakthrough, establishing the desired expansion by introducing their fundamental flattening lemma technique and coupling it with more standard techniques from the representation theory of these finite simple groups.

Theorem 2.21. *For any* $0 < \delta \in \mathbb{R}$ *there exists* $\varepsilon = \varepsilon(\delta) \in \mathbb{R}$ *such that for every prime* p, *if* Σ *is a set of generators of* $\mathrm{SL}_2(\mathbb{F}_p)$ *such that* $\mathrm{girth}\left(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); \Sigma)\right) \geq \delta \log p$, *then* $\mathrm{Cay}\left(\mathrm{SL}_2(\mathbb{F}_p); \Sigma\right)$ *is an* ε*-expander.*

The girth of a graph is the length of the shortest non-trivial closed path in the graph.

This theorem solves, in particular, the 1-2-3 problem: an easy argument (going back to [M1]) shows that

$$\mathrm{girth}\left(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); \left(\begin{smallmatrix} 1 & \pm 3 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ \pm 3 & 1 \end{smallmatrix}\right))\right) \geq \delta \log p$$

for some $0 < \delta$ independent of p. Moreover, if Σ is a free set of generators of a non-abelian free subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then girth $\big(\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p);\Sigma)\big)$ is logarithmic in p and hence these are expanders. In fact, the last conclusion holds for every Zariski dense subgroup Λ of $\mathrm{SL}_2(\mathbb{Z})$ as every such subgroup contains a non-abelian free group. This is easy for $\mathrm{SL}_2(\mathbb{Z})$ but true also for the more general case of Λ, which concerns us, by a well-known result of Tits [Ti]. It actually implies that we can assume Λ is a non-abelian free group.

The reader may note that we have stopped discussing general congruence quotients $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ for $m \in \mathbb{N}$ and stuck to $m = p$ a prime and $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = \mathrm{SL}_2(\mathbb{F}_p)$. Well, the extension to general m required more effort. It was first done in [BGS2] for natural numbers m which are square-free and eventually for all $m \in \mathbb{N}$ in [BV]. We will come back to this issue later. The case of m square-free is especially important for the sieve methods in Sections 4 and 5.

The dramatic breakthroughs have continued even further: first in parallel by two groups of researchers Breuillard, Green, and Tao ([BGT1], [BGT2]) and Pyber and Szabó ([PS1], [PS2]) and secondly by Varju [V] (followed by [SGV]). The first two groups proved essentially the same result (there are some differences but for our impressionistic picture, we can ignore them).

Theorem 2.22. *Let $r \in \mathbb{N}$ be fixed. Then for every finite simple group G of Lie type of rank at most r and for every subset A of G which generates G, either $A \cdot A \cdot A = G$ or $|A \cdot A \cdot A| \geq |A|^{1+\varepsilon}$, where ε depends only on r.*

The reader may check that this generalizes Helfgott's result (Theorem 2.18) from $\mathrm{SL}_2(\mathbb{F}_p)$ to all finite simple groups of Lie type *of bounded rank*. It should be mentioned that shortly after Theorem 2.18 was proved, it was shown by Nikolov and Pyber [NiPy] that part (b) of that theorem follows quickly from a result of Gowers [Go] and in more general situations, i.e., finite simple groups of Lie rank at most r with $k = 3$ for some $\delta = \delta(r)$ depending only on r. (See [BNP] for more.) This handles the case of "large subsets", and the main novelty of Theorem 2.22 is the case when $|A| < |G|^{1-\delta(r)}$.

Theorem 2.22 extends Helfgott's result from SL_2 to any bounded rank finite simple group. In particular it proves the Babai conjecture for this case, namely:

Corollary 2.23. *For $r \in \mathbb{N}$, there is a constant $C = C(r)$ such that for every finite simple group of Lie type G of rank at most r and every symmetric set of generators Σ of G,*

$$\mathrm{diam}\big(\mathrm{Cay}(G;\Sigma)\big) \leq (\log|G|)^C.$$

The conjecture is still open for the unbounded rank case. It should be stressed that in Theorem 2.22, ε does depend on r. In fact, it is shown in [PS2] that $\varepsilon = O(\frac{1}{r})$. Still one can expect that C of Corollary 2.23 is independent of r. For the bounded rank case one may conjecture that the right bound is $C(r)(\log|G|)$ rather than $(\log|G|)^{C(r)}$; see more in §2.7.

Helfgott's result for SL_2 led to the Bourgain-Gamburd Theorem 2.21. It naturally suggests that we expect a similar result for bounded rank simple groups. The following theorem is the second breakthrough (proved first in [V] for SL_n and later in [SGV] in general). It is in one way weaker and in another way stronger than the expected analogue.

Theorem 2.24 (A. Salehi Golsefidy and P. Varju [SGV])**.** *Let Γ be a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Q})$, so $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Z}_S)$ for some finite set of primes S.*

Let $m_0 = \prod p_{p\in S}$. For every q prime to m_0, let $\Gamma(q) = \mathrm{Ker}\big(\Gamma \to \mathrm{GL}_n(\mathbb{Z}_S/q\mathbb{Z}_S)\big)$. Then Γ has property (τ) with respect to the family $\{\Gamma(q)\big|q \text{ is square} - \text{free}\}$ iff H^0, the connected component of the Zariski closure $H = \overline{\Gamma}^z$ is perfect (i.e., does not have an abelian quotient).

The "only if" part is easy. The main point is the "if" part. It does not exactly generalize Theorem 2.21 of Bourgain and Gamburd, but rather generalizes Bourgain, Gamburd, and Sarnak [BGS2], which gives expansion for square-free congruence quotients, but only for SL_2. As we will see in the next sections, this is an extremely useful result with important applications to number theory, group theory, and even geometry. The reader may note that even though we formulated the result over $\mathbb{Q}$, it holds over any number field by restriction of scalars and for most applications one can reduce anyway to $\mathbb{Q}$.

It will be desirable to know the above result for $\Gamma(q)$ for all q's without the restriction to square-free (see also [BG3] and [BG4]), though at this point we do not see applications to this more general statement. So far this was proved only for $\Gamma = \mathrm{SL}_n(\mathbb{Z})$ by Bourgain and Varju ([BV] using [BFLM]). One can fantasize on a much more general statement, which will be the ultimate generalization of the 1-2-3 problem:

Conjecture 2.25. *Let Γ be a finitely generated subgroup of $\mathrm{GL}_n(F)$, F a field. So, $\Gamma \subset \mathrm{GL}_n(R)$, R a finitely generated domain. Assume H^0 is perfect, where H is the Zariski closure of Γ and H^0 its connected component. Then Γ has (τ) w.r.t. to the family $\Gamma(I) = \mathrm{Ker}\big(\Gamma \to \mathrm{GL}_n(R/I)\big)$ when I runs over all the finite index ideals of R.*

A proof of the positive characteristic part of this conjecture will have new applications.

In light of Theorem 2.6 one can even speculate on a more general version of Conjecture 2.25, but this conjecture is general enough to cover any applications in sight.

2.7. **Random generators and worst-case generators.** In Sections 2.2, 2.3, and 2.4 we described how all the non-abelian finite simple groups, except for the Suzuki groups, can be made into a family of expanders uniformly. We showed that there exists $k \in \mathbb{N}$ and $0 < \varepsilon \in \mathbb{R}$ such that for every such G there exists an explicitly given symmetric subset Σ of G of size at most k such that $\mathrm{Cay}(G;\Sigma)$ is an ε-expander. We did not bother to write the sets Σ explicitly but the method was explicit and if one wants, such a Σ can be presented. Now, for the Suzuki groups such a Σ exists but in a non-explicit way.

Theorem 2.26 (Breuillard, Green, and Tao [BGT3])**.** *There exists an $0 < \varepsilon \in \mathbb{R}$ such that for every Suzuki group $G = Sz(2^{2\ell+1})$, for almost every pair of elements $(x, y) \in G \times G$, the Cayley graph $\mathrm{Cay}(G; \{x^{\pm 1}, y^{\pm 1}\})$ is an ε-expander.*

So altogether Conjecture 2.5 is now a theorem! This conjecture handles the "best-case scenario"; i.e., there exists a set of generators Σ of G with the desired property. What about random sets for general finite simple groups?

Recall the well-known result:

Theorem 2.27 ([D], [KL], [LiSh])**.** *Two random elements of a finite simple group G generate G with probability going to 1 when $|G|$ is going to infinity.*

Another way to state the last result is that a random pair of elements gives rise to a connected Cayley graph. Is this graph an expander? In a more precise formulation:

Open Problem 2.28. Is there a $0 < \varepsilon \in \mathbb{R}$, such that Prob(Cay$(G; \{x^{\pm 1}, y^{\pm 1}\})$ is an ε-expander) is going to one when G runs over the non-abelian finite simple groups with $|G| \to \infty$ and x and y are chosen randomly and uniformly from G?

It was recently proved by Breuillard, Green, Guralnick, and Tao ([BGGT1], [BGGT2]) that the answer to this problem is yes if one restricts oneself to groups of bounded Lie rank. This of course generalizes Theorem 2.26 as well as a similar result which was known before for SL_2 ([BG1] and [Di] using [GHSSV]). It can replace [L6] as a proof for the bounded case of Conjecture 2.5. (The proof in [L6] used deep results from automorphic forms such as Selberg's Theorem and Drinfeld's solution to the characteristic p Ramanujan Conjecture, but gave explicit generators.)

One can ask for even more: Is it possible that there exists $\varepsilon > 0$ such that Cay$(G; \{x^{\pm 1}, y^{\pm 1}\})$ is an ε-expander for *every* choice of generating set $\{x, y\}$ for G and any non-abelian finite simple group ("worst-case scenario"; compare to Babai Conjecture 2.20). In the general case the answer is certainly no! The family Alt(n) has generators which do not give rise to a family of expanders. (For Sym(n) one can take $\{\tau = (1,2), \sigma = (1,2,\ldots,n)\}$: Cay(Sym$(n); \{\tau, \sigma^{\pm 1}\}$) are not expanders (see [L1, Example 4.3.3(c)]) and from this one can deduce a similar result for Alt(n).) It seems likely that for a family of finite simple groups of unbounded rank, one can always find "worst-case generators" which are not expanders. But one may suggest:

Conjecture 2.29. *For every $r \in \mathbb{N}$, there exists $\varepsilon = \varepsilon(r)$ such that*

$$\mathrm{Cay}(G; \{x^{\pm 1}, y^{\pm 1}\})$$

is an ε-expander for every finite simple group G of Lie type and rank at most r and for every generating set $\{x, y\}$ of G.

One may want to compare Conjecture 2.29 with Corollary 2.23, which gives a weaker statement. An intermediate step would be to prove that

$$\mathrm{diam}\ \mathrm{Cay}(G; \{x^{\pm 1}, y^{\pm 1}\}) = O_r(\log |G|),$$

where the implied constant depends only on r.

As of now the only result concerning Conjecture 2.29 is:

Theorem 2.30 (Breuillard and Gamburd [BGa])**.** *There exists $0 < \varepsilon \in \mathbb{R}$ and an infinite set of primes $\mathcal{P}$ such that for every $p \in \mathcal{P}$ and* every *generating set $\{x, y\}$ of $\mathrm{SL}_2(\mathbb{F}_p)$, $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p); \{x^{\pm 1}, y^{\pm 1}\})$ is an ε-expander.*

Their interesting method is not explicit. They prove the existence of such a set $\mathcal{P}$ by a non-effective method.

3. Applications to computer science

Expander graphs play an important role in computer science with numerous applications in many subareas. They appear as basic building blocks of various networks, give error correcting codes, are used for derandomization of various probabilistic algorithms, and more. Many of the applications are presented in [HLW], and the reader is encouraged to consult them, either in detail or at least to get an

impression of the wide spectrum of applications. We chose to present one "real" application (to error correcting codes) and one theoretical application to the theory of computation (the analysis of the product replacement algorithm).

3.1. **Error correcting codes.** *Error correcting codes* is a collective name for various methods that enable sending messages of information through noisy channels. The most common model deals with sending a block of k bits of information, i.e., a vector v in $\mathbb{F}_2^k$. Instead of v, one sends $Tv \in \mathbb{F}_2^n$ when $n > k$, i.e., a longer vector, but with the hope that if the noise will cause t mistakes (i.e., switching 0 to 1 or vice versa, in t coordinates) the receiver will be able to correct it back to the right vector. This can happen if for every $v_1 \neq v_2 \in \mathbb{F}_2^k$, $\mathrm{dist}(Tv_1, Tv_2) > 2t$ where for $x, y \in \mathbb{F}_2^n$, we take $\mathrm{dist}(x, y) =$ the number of bits in which they are different.

It is usually convenient to use a linear transformation for T, in which case $C := T(\mathbb{F}_2^k)$ is a linear subspace of $\mathbb{F}_2^n$. Moreover, as $\mathrm{dist}(x, y) = \mathrm{dist}(x - y, \vec{0})$, this code can correct $\lfloor \frac{d-1}{2} \rfloor$ errors, when $d = d(C) = \min\{\mathrm{dist}(x, \vec{0}) \mid \vec{0} \neq x \in C\}$. This leads us to define:

Definition 3.1. An (n, k, d)-code is a linear subspace C of $\mathbb{F}_2^n$ of dimension k of distance $d(C) = d$.

In coding theory, one is interested in "good codes", i.e., a family of (n, k, d)-codes with dimension k and distance d both growing linearly with n. So let us denote $r(C) = \frac{k}{n}$ and $\delta(C) = \frac{d}{n}$, the rate and the relative distance of the code C. So, a family of codes, of dimensions going to infinity, is good if there exists $\varepsilon > 0$ such that $r(C)$ and $\delta(C)$ are both at least ε.

The subspace C is defined by linear equations. The code (or more precisely the family of codes) is called LDPC (low density parity check) if for some fixed constant ℓ, all these linear equations are ℓ-sparse, i.e., each such equation touches at most ℓ variables. Another way to say this is that the "parity check" matrix H defining C, i.e., the $(n-k) \times n$ matrix H with $C = \{x \in \mathbb{F}_2^n \mid Hx = \vec{0}\}$, has at most ℓ non-zero entries in each of its rows. (Of course, such an H is not unique; we say that C is LDPC if such an H exists.)

It has been known for a long time that LDPC good codes do exist. This was first shown by random considerations (see [HLW] and the references therein). In 1996, Sipser and Spielman [SiSp] gave an explicit construction based on expander graphs.

To describe their work, let us start with a simpler construction of codes based on graphs (sometimes called "cycle graph codes") as follows:

Let $X = (V, E)$ be a connected r-regular graph on m vertices. So $|E| = \frac{mr}{2}$. Let $\mathbb{F} = \mathbb{F}_2$ and $\mathbb{F}^E$ be the space of functions from E to $\mathbb{F}$. This can be thought of as the $\mathbb{F}$-vector space with basis E or also as the set of all subsets of E (where $A + B = (A \cup B) \backslash (A \cap B)$). Let C be the subspace of $\mathbb{F}^E$ spanned by all cycles of X. A simple argument shows that if we consider $\mathbb{F}^E$ as the space of functions, then $f \in C$ iff for every $v \in V$,

$$\sum_{v \in e \in E} f(e) = 0. \tag{3.1}$$

(In fact, this is the same argument which enabled Euler to prove that there is no Eulerian path in Königsberg; i.e., there is such a path iff the degree of every vertex is even.) This shows that $\dim(C) \geq |E| - |V|$. In fact, the sum of all the

defining equations is 0 and one can prove that $\dim(C) = |E| - |V| + 1$. Note that each one of the defining equations (3.1) has support exactly r, so if we take a family of r-regular graphs, we get a family of LDPS codes with rate $= 1 - \frac{2}{r}$. But, unfortunately, for these codes, the distance is logarithmic in the dimension rather than linear. Indeed, it is easy to see that the distance of this code is exactly $\mathrm{girth}(X)$, the girth of the graph X, i.e., the length of the shortest non-trivial closed cycle in X. By the well-known and easy Moore inequality, for an r-regular graph X on n vertices, $\mathrm{girth}(X) \leq 2\log_{r-1}(n)$, which implies that the cycle code cannot be good.

To overcome this, Sipser and Spielman used the following idea (which in some sense goes back to Tanner [Ta]). Choose a "small" code C_0 inside $\mathbb{F}^r$ with rate r_0 and relative distance δ_0. For every $v \in V$, give the edges coming out of v, labels $1, \ldots, r$, and denote them as $e_v(1), \ldots, e_v(k)$ (we do not require any compatibility here: the same edge can be labeled i when it comes out of v and j when it comes out of w). We now define $C(X, C_0)$ to be the subspace of all functions $f \in \mathbb{F}^E$ such that for every $v \in V$, $(f(e_v(1)), \ldots, f(e_v(k)))$ is a vector in C_0. Namely, these are the functions which are "locally" in C_0, i.e., what every vertex "sees" in its star is a vector of C_0.

Theorem 3.2 (Sipser and Spielman [SiSp])**.** *The code $C(X, C_0)$ has relative rate at least $2r_0 - 1$ and relative distance at least $(\frac{\delta_0 - \lambda}{1-\lambda})^2$, where $\lambda = \lambda(X) = \frac{1}{r}\max\{\mu \mid \mu \text{ an eigenvalue of } X, \mu \neq r\}$.*

The theorem gives an explicit construction of LDPC good codes. Indeed, let X be an r-regular Ramanujan graph, so $\lambda(X) \leq \frac{2\sqrt{r-1}}{r} \leq \frac{2}{\sqrt{r}}$. Pick a code C_0 in $\mathbb{F}^r$ with rate $> \frac{1}{2}$ and relative distance $> \frac{2}{\sqrt{r}}$. Such codes do exist as can be seen by either random consideration (and as r is fixed, we are allowed to pick one randomly) or by one of the many classical methods (note that we only ask the relative distance to be more than $\frac{2}{\sqrt{r}}$, so it does not have to be "good"). Theorem 3.2 now ensures that $C(X, C_0)$ is good. Finally, the code $C(X, C_0)$ is LDPC since every defining equation touches only the r edges adjacent to a vertex v (the equations which force it to be in C_0).

The proof of Theorem 3.1 is not difficult. As C_0 is defined by $(1-r_0)r$ equations, $C = C(X, C_0)$ is defined by $(1-r_0)rm$ equations on $|F| = \frac{rm}{2}$ variables, so $\dim C \geq \frac{rm}{2} - (1-r_0)rm = (2r_0 - 1)\frac{rm}{2} = (2r_0 - 1)|E|$. As $r_0 > \frac{1}{2}$, C has positive rate. To see that the relative distance of C is positive, one uses the following result of Alon and Chung [AC, Lemma 2.3].

Lemma 3.3. *In the notation of Theorem 3.2, if Y is a subset of the vertices of X of size γm, where $m = |X|$ and $0 < \gamma < 1$, then*

$$|e(Y) - \frac{1}{2}r\gamma^2 m| \;\leq\; \frac{r}{2}\;\lambda\;\gamma(1-\gamma)m,$$

where $e(Y)$ denotes the number of edges of X both of whose endpoints are in Y.

Remark 3.4. $\frac{1}{2}r\gamma^2 m$ is what one should expect "randomly".

Assume now that $0 \neq f \in C(X, C_0)$ with edge support D. We want to prove that $|D|$ is large. Assume the size of D is $\frac{rm}{2}(\gamma^2 + \lambda\gamma(1-\gamma))$ for some $0 < \gamma < 1$. Then by the lemma, D touches a set of vertices D_0 with at least γm vertices. As every edge touches two vertices, it means that on the average every vertex of D_0

sees at most $r(\gamma + \lambda(1-\gamma))$ edges. So one of them sees at most this size. But it sees a vector in C_0 whose support is at least $\delta_0 r$. Hence $\gamma + \lambda(1-\gamma) \geq \delta_0$, which implies $\gamma \geq \frac{\delta_0 - \lambda}{1-\lambda}$. Substituting into $|D|$ implies the theorem.

In [KaW] a version of Theorem 3.2 was shown for the case when the graph X is a Cayley graph of a group, in which case one can get a "symmetric code". This has been used in [KaL] to present *highly symmetric* LDPC good codes. These codes satisfy all the "gold standards" of coding theory: they have linear dimension (i.e., $r(C) \geq \varepsilon > 0$), linear distance (i.e., $\delta(C) \geq \varepsilon > 0$), they are LDPC, and there exists a group H acting transitively on the coordinates of $\mathbb{F}_2^n$ (i.e., acting on the Cayley graph which is edge transitive) such that the code C is invariant. Moreover, all the constraints ($\equiv$ equations) defining C are spanned by the orbit of one equation and this equation is of bounded ($\leq r$) support.

The key step for the construction of these highly symmetric codes are the edge transitive Ramanujan graphs constructed in ([LSV2]) as a special case of Ramanujan complexes ([LSV1]).

3.2. **The product replacement algorithm.** The last three decades have brought a great interest in computational group theory. This is usually divided in two directions: one is combinatorial group theory which usually deals with infinite groups. We will touch upon this direction briefly in §5.1. Here we mainly deal with the other direction: algorithms dealing with finite groups such as permutation groups or groups of matrices over finite fields. A typical problem in this theory is of the following type. Devise an algorithm that when given few explicit permutations in $\mathrm{Sym}(n)$ (or matrices in $\mathrm{GL}_n(\mathbb{F}_q)$) will find various properties of the group G generated by these elements, such as its order, its composition factors, etc. The computational theory of permutation groups is very developed where most problems have deterministic algorithms. On the other hand for matrix groups many of the practical algorithms are probabilistic.

Probabilistic algorithms very often need (pseudo-) random elements from the group G. Let us formulate this more formally. We need an algorithm that when explicit elements $g_1, \ldots, g_k$ (from a larger group such as $\mathrm{Sym}(n)$ or $\mathrm{GL}_n(\mathbb{F}_q)$) are given, it will provide us with a "pseudo-random" element from $G = \langle g_1, \ldots, g_k \rangle$, the group generated by $g_1, \ldots, g_k$.

One such algorithm is to take a random word of some length ℓ in the generators $g_1, \ldots, g_k$ and their inverses. This can be visualized as the random walk on the Cayley graph $\mathrm{Cay}\left(G; \left\{g_1^{\pm 1}, \ldots, g_k^{\pm 1}\right\}\right)$ when one stops after ℓ moves. This algorithm is a pretty good one if this Cayley graph is an expander, but this is not the case in general. The reader may think about the case $k = 1$, in which case G is cyclic, to see how slow the algorithm is in this case.

A different approach was suggested in 1995 in [CLMNO], and it very quickly became the standard way to generate random elements in finite groups in the various packages dealing with group computations such as MAGMA, GAP, etc. It is called the *product replacement algorithm*. The easiest way to describe it is also as a random walk on a graph. This time the vertex set of the graph is $\Omega_r(G) = \{(h_1, \ldots, h_r) \in G^r \mid G = \langle h_1, \ldots, h_r \rangle\}$, i.e., the r-tuples of generators of G. The edges correspond to the following "moves".

For $1 \leq i \neq j \leq r$:

$$\begin{aligned} L_{ij}^{\pm} &: (h_1, \ldots, h_i, \ldots, h_j, \ldots, h_r) \mapsto \left(h_1, \ldots, h_i, \ldots, h_i^{\pm 1} h_j, \ldots, h_r\right), \\ R_{ij}^{\pm} &: (h_1, \ldots, h_i, \ldots, h_j, \ldots, h_r) \mapsto \left(h_1, \ldots, h_i, \ldots, h_j h_i^{\pm 1}, \ldots, h_r\right). \end{aligned}$$

This makes $\Omega_r(G)$ into a $4r(r-1)$-regular graph. The algorithm is to take $r > k$ and a random walk, starting at $(g_1, \ldots, g_k, e, e, \ldots, e)$, of say, ℓ steps, then stop at a vertex of $\Omega_r(G)$ and pick up one of its coordinates randomly among the r possibilities. Unlike the previous Cayley graph, this graph is highly non-symmetric and contains many loops and double edges. The analysis of the algorithm is very complicated, but many simulations showed outstanding performances. For example for $G = \mathrm{Sym}(n)$, $\tau = (1,2)$ and $\sigma = (1, \ldots, n)$, the first algorithm needs (by theoretical and experimental data) approximately $n^2 \log n$ steps, so for $n = 52$ this is over 10,000. At the same time simulations with the product replacement algorithm for $n = 52$ and $r = 10$ showed that after approximately 160 steps one gets a random-like permutation.

What is needed is a theoretical explanation for these outstanding performances. The first steps in this analysis were taken in [DSC]. A more comprehensive explanation was suggested in [LP]. Here is the crucial observation: Think of $L_{ij}^{\pm}$ and $R_{ij}^{\pm}$ above as acting on the vector $(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_r)$ of r free generators of the free group F_r on $\{x_1, \ldots, x_r\}$. Let $A^+ = \mathrm{Aut}^+(F_r)$ be the subgroup of $A = \mathrm{Aut}(F_r)$ generated by these elements. By some well-known results, going back to Nielsen, A^+ is a subgroup of index 2 in A. Now, $\Omega_r(G)$ can be identified with the set $\mathrm{Epi}(F_r, G)$ of epimorphisms from F_r onto G, where such an epimorphism φ corresponds to $(\varphi(x_1), \ldots, \varphi(x_r))$. The group $\mathrm{Aut}(F_r)$ acts on $\mathrm{Epi}(F_r, G)$ by $\alpha.\varphi = \varphi \circ \alpha^{-1}$ for $\alpha \in A$. One can easily check now that the graph structure of $\Omega_r(G)$ defined above is the Schreier graph of $\mathrm{Aut}(F_r)$ acting on the set $\Omega_r(G)$ w.r.t. the generators $\left\{L_{ij}^{\pm}, R_{ij}^{\pm}\right\}$. (A Schreier graph of a group H generated by Σ and acting on a set X is the graph with vertex set X where $x \in X$ is connected to $\sigma.x$ for $\sigma \in \Sigma \cup \Sigma^{-1}$.)

If the group $A = \mathrm{Aut}(F_r)$ has Kazhdan property (T), then an argument similar to Proposition 1.11 would give that $\Omega_r(G)$ are expanders. The random walk on them converges then very fast to the uniform distribution. This would give a conceptual explanation for the great performances of the algorithm.

Unfortunately, it is still a (quite well-known) open problem whether $\mathrm{Aut}(F_r)$ has (T) (it does *not* for $r = 2, 3$; see [GL]). Still the approach presented here was sufficient to get some unconditional results for various classes of finite groups, for example, for abelian groups, or more generally, nilpotent groups of bounded class. It is shown in [LP] that the subgroup of $\mathrm{Aut}(F_r(c))$, the automorphism group of the free nilpotent group on r generators and class c, generated by the "Nielsen moves" (as above) has (T) if $r \geq 3$. One can therefore deduce a linear mixing time for the random walk on $\Omega_r(G)$ for G nilpotent (to be compared with the subexponential bound obtained in [DSC] without the use of expanders). This explains, at least for these groups, the outstanding performances of the product replacement algorithm. See [LP] for the details and a more general conjecture.

4. Expanders in number theory

As was mentioned (though briefly—for a more comprehensive treatment see [L1] and [S1]), the theory of expanders has been related to number theory in several

ways. But, traditionally, the direction was from number theory to graph theory: various deep results in number theory and the theory of automorphic forms have been used to give explicit constructions of expanders and of Ramanujan graphs. We now start to see applications in the opposite direction: from expander graphs to number theory. The most notable one is the development of the affine sieve method. This section will be devoted to its description and applications. For other applications, see [Ko1], [EHK] and [EMV].

4.1. **Primes on orbits.** Many results and problems in number theory are about the existence of primes. There are infinitely many primes in $\mathbb{Z}$, but Dirichlet's classical result says more:

Theorem 4.1. *If $b, q \in \mathbb{Z}$ with $(b, q) = 1$, then there are infinitely many primes on the arithmetic progression $b + q\mathbb{Z}$.*

If one wants to avoid the "local assumption" $(b, q) = 1$, the result can be restated as, for every b and $q \neq 0$ in $\mathbb{Z}$, the arithmetic sequence $b + q\mathbb{Z}$ has infinitely many numbers x with $\nu(x) \leq 1 + \nu((b, q))$. Here for $x \in \mathbb{Z}$, we write $\nu(x)$ for the number of prime factors of x.

Another well-known problem about primes is:

Conjecture 4.2 (Twin Prime Conjecture)**.** *There are infinitely many primes p, for which $p + 2$ is also a prime.*

Another way to state the conjecture is there are infinitely many $x \in \mathbb{Z}$ with $\nu(x(x + 2)) \leq 2$.

One also expects that the Twin Prime Conjecture is true along arithmetic progressions satisfying the "local condition" above.

A far-reaching generalization is the next conjecture of Schinzel and Sierpiński [SS], which needs some notation. Let Λ be an infinite subgroup of $\mathbb{Z}$, i.e., $\Lambda = q\mathbb{Z}$ for some $q \neq 0$, and $b \in \mathbb{Z}$. Let $\mathcal{O}$ be the orbit of b under the action of Λ on $\mathbb{Z}$, i.e., $\mathcal{O} = b + q\mathbb{Z}$. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial which is integral on $\mathcal{O}$. We say that the pair $(\mathcal{O}, f)$ is *primitive* if for every $2 \leq k \in \mathbb{Z}$ there exists $x \in \mathcal{O}$ such that $(f(x), k) = 1$.

Conjecture 4.3 (Schinzel and Sierpiński)**.** *If $f(x) \in \mathbb{Q}[x]$ is a product of t irreducible factors in $\mathbb{Q}[x]$, $\mathcal{O} = b + q\mathbb{Z}$ as above, f is integral on $\mathcal{O}$, and $(\mathcal{O}, f)$ is primitive, then there are infinitely many $x \in \mathcal{O}$ with $\nu(f(x)) \leq t$.*

Taking $f(x) = x$, one gets Dirichlet's Theorem and, for $f(x) = x(x + 2)$, the Twin Prime Conjecture in its generalized form (also along arithmetic progressions).

There are various high-dimensional conjectures generalizing Dirichlet's Theorem. Let us set some more notation:

Let Λ be a non-trivial subgroup of $\mathbb{Z}^n$, $b \in \mathbb{Z}^n$ and $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ which is integral on $\mathcal{O} = b + \Lambda$. For $r \in \mathbb{N}$, we denote by $\mathcal{O}(f, r)$ the set of $x \in \mathcal{O}$ for which $\nu(f(x)) \leq r$. We say that $(\mathcal{O}, f)$ *saturates* if for some $r < \infty$, $\mathcal{O}(f, r)$ is Zariski dense in (the Zariski closure of) $\mathcal{O}$. The smallest such r, if it exists at all, will be denoted by $r_0(\mathcal{O}, f)$.

Conjecture 4.4 (Hardy and Littlewood [HL])**.** *Let Λ be a subgroup of $\mathbb{Z}^n$. Assume that for each j, the jth coordinate function x_j is non-constant when restricted to Λ. Let $b \in \mathbb{Z}^n$, $\mathcal{O} = b + \Lambda$, and $f(x) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$, and assume $(\mathcal{O}, f)$ is primitive. Then $r_0(\mathcal{O}, f) = n$; i.e., the set of $x \in \mathcal{O}$ all of whose coordinates are simultaneously primes, is Zariski dense in $b + \mathbb{C}\Lambda$ and in particular, it is infinite.*

A recent breakthrough of Green, Tao, and Ziegler ([GTZ], [GT2]) has proved this conjecture for the case when $\mathrm{rank}(\Lambda) \geq 2$. The most difficult case is when $\mathrm{rank}(\Lambda) = 1$. For example, by looking at $b = (1,3) \in \mathbb{Z}^2$ and $\Lambda = \mathbb{Z}(1,1)$, we see that the Twin Prime Conjecture is a special case.

Another special case is the following famous result proved not long ago by Green and Tao [GT1]:

Theorem 4.5 (Arithmetic progressions of primes)**.** *For every $3 \leq k \in \mathbb{N}$, the set of primes contains an arithmetic progression of length k.*

To see that Theorem 4.5 is a special case of Conjecture 4.4, look at $\mathbb{Z}^k$ and let Λ be the 2-dimensional subgroup $\Lambda = \mathbb{Z}(1,1,1,\ldots,1) + \mathbb{Z}(0,1,2,3,\ldots,k-1)$. Then the orbit of $(1,1,\ldots,1)$ is Λ, which is the set $\{(m, m+n, m+2n, \ldots, m+(k-1)n | m,n \in \mathbb{Z}\}$. Conjecture 4.4 implies that there are infinitely many vectors of this kind whose entries are all primes.

The formulation of the Hardy-Littlewood Conjecture 4.4 naturally suggests studying the existence of prime vectors (i.e., vectors whose all coordinates are primes) in the orbit $\Lambda.b$ when this time Λ is a subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Somewhat surprisingly this has not been studied until recent years. It seems that counterexamples of the following kind led us to think that no real theory could be developed:

Example 4.6. *Let Λ be the cyclic subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by $\left(\begin{smallmatrix} 7 & 6 \\ 8 & 7 \end{smallmatrix}\right)$ and $b = (1,1)^t$. The orbit $\Lambda.b$ is contained in $\{(x,y) \in \mathbb{Z}^2 | 4x^2 - 3y^2 = 1\}$, from which one easily sees that no such y is a prime, in spite of the fact that for this problem there are no "local obstructions".*

Another example of a similar flavor is:

Example 4.7 ([S7], [BGS2])**.** *Let $\Lambda = \left\langle \left(\begin{smallmatrix} 3 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle \leq \mathrm{SL}_2(\mathbb{Z})$, $b = (2,1)^t$, and let $\mathcal{O}$ be the orbit $\Lambda.b$. The orbit lies on the hyperbola $\{(x,y) \in \mathbb{Z}^2 | x^2 - 3xy + y^2 = 1\}$ and for $n \in \mathbb{N}$ we get the pairs (f_{2n-2}, f_{2n}), where f_n is the nth Fibonacci number (one can define them for $n < 0$ as well). While it is conjectured that infinitely many of the f_n's are primes, the f_{2n} are not. In fact, $f_{2n} = f_n l_n$ when l_n is the nth Lucas number. Moreover, it is even expected that f_{2n} has an unbounded number of prime factors, when $n \to \infty$. (See* [BLMS]*.)*

The exciting fact, which came out only in recent years, is that these examples are exceptional, not typical. The Zariski closure in these cases is a torus. We will see below how conjectures and results (!) such as the Hardy-Littlewood Conjecture have non-abelian analogues when a torus is not involved. The key new ingredients for all this are the expanders combined with the classical combinatorial sieve of Brun. This will be our topic in the next section.

4.2. **Brun sieve and expanders.** For $0 < x \in \mathbb{R}$, denote by $\mathbb{P}(x)$ the set of primes smaller than or equal to x, $\pi(x) = |\mathbb{P}(x)|$ and $P(x) = \prod_{p \in \mathbb{P}(x)} p$. Evaluating $\pi(x)$ is one of the most important problems in mathematics, if not the most important. Well, the prime number theorem says that $\pi(x) \sim \frac{x}{\log x}$ and the Riemann hypothesis gives a sharp bound for the error term in this asymptotic result. In fact, one has an exact formula for $\pi(x)$, which was given by Legendre at the end of the 18th century.

Proposition 4.8.

$$\pi(x) - \pi(\sqrt{x}) = -1 + \sum_{S \subseteq \mathbb{P}(\sqrt{x})} (-1)^{|S|} \Big\lfloor \frac{x}{\prod_{p \in S} p} \Big\rfloor.$$

By current standards the proof is a simple application of the inclusion-exclusion formula: the primes between $\sqrt{x}$ and x are those integers $n \neq 1$ which are not divisible by any prime less than $\sqrt{x}$. So we count them by taking x, subtracting those divisible by one prime less than $\sqrt{x}$, adding the number of those divisible by two primes, etc. Basically, we are applying the classical Eratosthenes' sieve method.

While Proposition 4.8 gives an exact formula, it is not very useful. The error term, for example, between $\frac{x}{\prod_{p \in S} p}$ and its integral part is "small", bounded by 1. But there are so many summands (approximately $4^{\sqrt{x}/\log x}$), which makes the formula quite useless.

Various "sieve methods" have been developed for problems like that—the reader is referred to [FI] and [IK], for example. Let us say a few words about the combinatorial sieve developed by Brun. His main motivation was to handle the Twin Prime Conjecture 4.2. In a different language it says that if $f(x) = x(x+2)$, then for infinitely many n's in $\mathbb{N}$, $f(n)$ is a product of only two primes, i.e., $\nu(f(n)) \leq 2$. Let $f(x)$ be any integral polynomial $f(x) \in \mathbb{Z}[x]$, e.g., $f(x) = x(x+2)$. Let x be a large real number, and $z < x$. Denote:

$$S(f, z) := \sum_{\substack{n \leq x \\ (f(n), P(z)) = 1}} 1,$$

so $S(f, z)$ counts those n less than x such that $f(n)$ is not divisible by any prime less than z. Of course, we want z to be as large as possible.

Recall the Möbius function

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 \cdot \ldots \cdot p_r \text{ with distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

The following is well known and easy to prove:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1, \\ 0 & n > 1. \end{cases}$$

One can therefore now write:

$$S(f, z) := \sum_{\substack{n \leq x \\ (f(n), P(z)) = 1}} 1 = \sum_{n \leq x} \sum_{d | (f(n), P(z))} \mu(d)$$

$$= \sum_{d | P(z)} \mu(d) \Bigg(\sum_{\substack{n \leq x \\ f(n) \equiv 0 (d)}} 1 \Bigg).$$

We now denote:

$$\beta(d) = |\{m \bmod d | f(m) \equiv 0 (d)\}|,$$

i.e., the number of solutions of f mod d. Running over all n's up to x, one then runs approximately $\frac{x}{d}$ times on all the residues mod d; approximately $\frac{x}{d}\beta(d)$ of them will

give zeros for f mod d. So, continuing the evaluation of $S(f,z)$ we have

$$S(f,z) = \sum_{d|P(z)} \mu(d)(\frac{\beta(d)}{d}x + r(d)),$$

where $r(d)$ is an error term. Note that $\frac{\beta(d)}{d}$ is a multiplicative function of d.

Brun developed a method to analyze such a sum with particular interest in the case $f(x) = x(x+2)$. He deduced that for δ small enough, if $z = x^\delta$, then $S(f,z) \geq c\frac{x}{\log(x)^2}$, which means that there are infinitely many n's with no prime divisor for $f(n)$ less than n^δ. For such n's, $\nu(f(n)) \leq \frac{\deg f}{\delta}$. So, while he fell short of proving the Twin Prime Conjecture, he was able to show that there are infinitely many n's with $\nu(f(n)) \leq 18$. His method has been refined; the current record is due to Chen [Ch] who replaced 18 by 3. Namely, there are infinitely many pairs $(n, n+2)$ such that one of them is a prime and the other is a product of at most two primes.

These "combinatorial sieve methods" have also been applied to the higher dimensional cases described in §4.1. For example, one gets a partial result toward the Hardy-Littlewood Conjecture: in the notation of Conjecture 4.4, one can prove that there exists $r \in \mathbb{N}$ such that $r_0(\mathcal{O}, f) \leq r$. In particular, the orbit $b + \Lambda$ contains infinitely many vectors, all of whose entries are products of a bounded number of primes. Moreover, it has even been proved that this r depends only on n and not on b or Λ (assuming, of course, no local obstructions, i.e., $(\mathcal{O}, f)$ is primitive).

All this is a quite deep (and quite technical) theory. The relevance for our story came from the insight of Sarnak who noticed that the machinery of the Brun sieve can be carried out also for a general non-commutative subgroup $\Lambda \leq \mathrm{GL}_n(\mathbb{Z})$ acting of $\mathbb{Z}^n$, *provided* Λ has property (τ) w.r.t. congruence subgroups. The orbit in this case of $b \in \mathbb{Z}^n$ is $\Lambda.b = \{\gamma.b | \gamma \in \Gamma\}$, and one can start the same kind of computation we illustrated above for the Twin Prime problem. This time, instead of summing over all $n \leq x$, one sums over the ball of radius at most k, with respect to a fixed set of generators Σ of Λ. The crucial point is that these balls $B(k) = \{\gamma \in \Lambda | \,\mathrm{length}_\Sigma(\gamma) \leq k\}$ when acting on $b \in \mathbb{Z}^n$ and reduced mod d, i.e., the set $B(k).b(\mathrm{mod}\ d)$, distribute almost uniformly over the vectors $\Gamma.b(\mathrm{mod}\ d)$, as a subset of $(\mathbb{Z}/d\mathbb{Z})^n$. This is exactly what the expander property gives us (compare with Proposition 1.6).

At first sight this connection with expanders may look counterintuitive: we want to extend sieve methods from abelian cases, such as the Hardy-Littlewood Conjecture, to a non-abelian setting. The abelian case *never* gives rise to expanders (see [LW]). Why should this be the needed property in the non-abelian case? The point is that in the abelian setting the number of integer points in arithmetic progressions which are contained in a large interval can be estimated quite accurately in the obvious way. But in the non-abelian setting, it is not clear what is the distribution of the points in a ball when taken mod d. Note also that such groups usually have exponential growth, and so when we move from ball $B(k)$ to $B(k+1)$ the boundary is as large as the original ball. The expanding property enables one to overcome this difficulty. In fact, one does not need that $\Lambda < \mathrm{GL}_n(\mathbb{Z})$ has (τ) with respect to all congruence subgroups; it suffices to know it with regard to congruence subgroups mod d when d is square-free.

All this machinery was put to work in the paper of Bourgain, Gamburd, and Sarnak ([BGS1], [BGS2]). At the time when the paper was written property (τ)

was known for such Λ's only when the Zariski closure of Γ was SL_2 (due to Helfgott [H1], Bourgain and Gamburd [BG1] and the extension to all square-free numbers in [BGS2]). But they also proved some conditional results, assuming an affirmative answer to some generalized form of the 1-2-3 problem (see §2.5 and §2.6). That work gave a push to efforts in this direction by a good number of authors ([BG3], [BG4], [BGS3], [BV], [B2], [BG2], [H2], [GH], [V], [BGT2], [PS2], [S7], [SGV]) as described in §2.6. The most general result for the "affine-sieve method" as it is now called, is given in a forthcoming paper of Salehi Golsefidy and Sarnak [SGS]:

Theorem 4.9. *Let $\Lambda \leq \mathrm{GL}_n(\mathbb{Z})$ be a finitely generated subgroup with Zariski closure G. Assume the reductive part of G^0 (the connected component of G) is semisimple. Let $b \in \mathbb{Z}^n$, $\mathcal{O} = \Gamma.b$ and $f \in \mathbb{Q}[x_1, \ldots, x_n]$, which is integral and not constant on $\mathcal{O}$. Then $(\mathcal{O}, f)$ saturates; namely, there exists $r \in \mathbb{N}$ such that the set of vectors in $\mathcal{O}$ for which $f(x)$ is a product of at most r primes is Zariski dense in $\mathcal{O}$.*

This theorem also covers cases when G is unipotent (and so various classical results) as well as completely new cases when G is semisimple. The method is called "affine sieve" as it also covers "affine transformations" of $\mathbb{Z}^n$ and not only linear. The affine case can be easily reduced to a linear case of higher dimensions. Some of the classical problems (e.g., the Hardy-Littlewood Conjecture) are naturally expressed as affine problems rather than linear.

The case which is not covered by the last general theorem is of a torus (or when one has a central torus in G). Some of the difficult problems in number theory can be presented in this language; e.g., the Mersenne Conjecture—there are infinitely many primes p with $2^p - 1$ also a prime, is such a problem (see [BGS2, §2.1]). But the set of primes is "too thin" to sieve over it. So the new method shed no new light on this conjecture. It is not even known if there are infinitely many almost primes of the form $2^n - 1$.

Still there are few concrete problems where the new method gives some fascinating results. Some of them will be described in the next section.

4.3. **Some applications to classical problems.** Theorem 4.9 above gives some results which are completely out of reach by other methods; e.g., if $\Lambda \leq \mathrm{GL}_n(\mathbb{Z})$ is a group as in the theorem, then the group itself contained infinitely many matrices which are almost primes, i.e., all their entries are products of a bounded number of primes. An example satisfying this is *any* non-virtually cyclic subgroup of $\mathrm{SL}_2(\mathbb{Z})$. But, here Theorem 4.9 answers questions which have not been asked before.

Let us now present (following [BGS2], [S5], [S8]) two applications to classical number-theoretic problems:

Pythagorian triangles. Look at right angle triangles with integral edges x_1, x_2, and x_3 such that $x_3^2 = x_1^2 + x_2^2$ and assume that g.c.d.$(x_1, x_2, x_3) = 1$. It is well known that in this case there exist $m, n \in \mathbb{Z}$, one odd, one even, and $(m, n) = 1$ s.t. $x_1 = m^2 - n^2$, $x_2 = 2mn$ and $x_3 = m^2 + n^2$. It follows that x_1 is divisible by 3 and x_2 is divisible by 4. So the area of the triangle $A = \frac{x_1 x_2}{2}$ is divisible by 6. All the Pythagorian triples (x_1, x_2, x_3) as above are obtained as the orbit $\mathcal{O}$ of the triples $(3, 4, 5)$ acted upon by $O_F(\mathbb{Z})$ when F is the quadratic form $x_1^2 + x_2^2 - x_3^2$ and $\Lambda = O_F(\mathbb{Z})$ is the group of 3×3 integral matrices preserving this form. The group Λ satisfies the conditions of Theorem 4.9, and $f = \frac{x_1 x_2}{2}$ is integral on $\mathcal{O}$ (and

even divisible by 6). We deduce that there are infinitely many triples whose areas are almost primes.

Now what is $r_0(\mathcal{O}, f)$—i.e., what is the minimal r for which the set of triples with $\nu(\text{area}) \leq r$ is Zariski dense? This is a more delicate question. Some elementary arguments show that it is at least 6 and some recent work of Green and Tao [GT2] implies that it is indeed 6. (See [BGS2] and the references therein for more information.)

Integral Apollonian Packing. A classical theorem of Apollonius asserts that given three mutually tangent circles C_1, C_2, and C_3, there are exactly two circles C_4 and C_4' tangent to all three. Descartes' Theorem says that the curvatures of these circles (i.e., the reciprocals of the radii) a_1, a_2, a_3, a_4 satisfy $F(a_1, a_2, a_3, a_4) = 0$ where

$$F(a_1, a_2, a_3, a_4) = 2(a_1^2 + a_2^2 + a_3^2 + a_4^2) - (a_1 + a_2 + a_3 + a_4)^2 \tag{1}$$

(a negative solution corresponds to a situation when one circle touches the others from the outside). An easy calculation using (1) shows that given C_1, C_2, C_3 with curvatures a_1, a_2, a_3, respectively, there are two solutions C_4 and C_4' with curvatures a_4 and a_4' satisfying

$$a_4' = 2a_1 + 2a_2 + 2a_3 - a_4. \tag{2}$$

It also shows that starting with an integral vector (a_1, a_2, a_3, a_4), the other quadruple (a_1, a_2, a_3, a_4') is also integral. This can be carried out with any subtriple of C_1, C_2, C_3, C_4. We deduce the following: let

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad S_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \text{ and } S_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix},$$

and let Λ be the subgroup generated by these four reflections. Then starting with any integral quadruple $b = (a_1, a_2, a_3, a_4)$ of integral curvatures of mutually touching circles, all elements in the orbit $\Lambda.b$ represent such quadruples. Moreover if $\gamma' = S_i\gamma$ in Λ, then the corresponding quadruple share a common triple. See Figure 1 for the starting stages of the orbit $(18, 23, 27, 146)$.

The subgroup Λ of $\mathrm{GL}_4(\mathbb{Z})$ preserves the quadratic form F of equation (1). It therefore lies within a conjugate of $SO(3, 1)$ and, in fact, it is Zariski dense there. One can therefore deduce from Theorem 4.9 various number-theoretic results on the orbit $\Lambda.b$.

But many more questions come up naturally. Are there infinitely many primes in the set of curvatures of the circles in the orbit? How many? One wishes to have a "prime number theorem" estimating the density of prime curvatures within the orbit of the ball of radius N in Λ (w.r.t. $\{S_i\}_{i=1}^4$). Are there infinitely many twin primes? That is, are there infinitely many kissing pairs of circles with prime curvatures?

A rich theory has started to emerge in recent years (cf. [GLMWY], [S5], [S8], [KO1], [Fu], [BK], [BF], [FS], [KO2], and the references therein). This is a fascinating crossroad of number theory, geometry, group theory, dynamics, ergodic theory, and expanders!

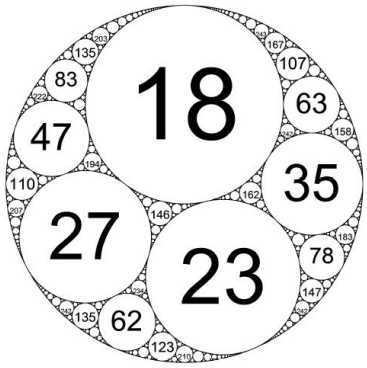

FIGURE 1. Apollonian packing

5. Applications to group theory

In the previous sections the connections between expander graphs and group theory have been illustrated over and over again. Many (in some sense "most") of the examples we gave for expander graphs were Cayley graphs of groups and being expanders says something quite deep on their group structure and/or their representation theory.

In this section we will describe several results about groups whose formulations do not mention expanders but expanders come out substantially in the proofs, sometimes in a somewhat surprising way. We will start with describing a new sieve method for finitely generated groups and indicate several applications to linear groups and to the mapping class groups. This is a new direction, and it can be expected that this sieve method will have further use in group theory.

We will also bring some applications to combinatorial group theory, a direction whose significance will be fully appreciated in the next section when we discuss geometric applications.

5.1. **Measuring subsets of finitely generated groups.** Let $G = \mathrm{GL}_n(\mathbb{C})$ be the group of $n \times n$ invertible complex matrices. A standard claim on G is, for generic $g \in G$, the centralizer $C_G(g)$ of g in G is abelian. What do we mean by this statement? What is meant by "generic"? Well, one can work in the Baire category setting, in the measure-theoretic language, or in the Zariski topology. Whatever setting we choose, the statement says that outside of a "meager" subset of G, the property of abelian centralizer is satisfied. The proof is easy: For almost every $g \in G$ the eigenvalues of g are all distinct (since the set of zeros of the discriminant is "meager"). Thus, with a suitable basis of $\mathbb{C}^n$, g is diagonal with n different eigenvalues, and the centralizer of such a g is just the diagonal matrices and hence abelian.

Let us now look at the finitely generated group $\Gamma = \mathrm{SL}_n(\mathbb{Z})$. Say we want to claim a similar statement about Γ: "For generic $g \in \Gamma$ the centralizer $C_\Gamma(g)$ is abelian". What does this mean? Is there a natural way to "measure" subsets of Γ to be "small" or "large"? On a countable set such as Γ one cannot take a "uniform distribution". This is a problem not only in group theory. The reader is referred to an interesting lecture by Barry Mazur [Maz] which illustrates, via various questions

in number theory, that one may have quite different answers to similar problems depending on the probabilistic model.

These types of questions have recently received attention also from another point of view. Complexity theory, i.e., the theory of algorithms, usually deals with "worst-case scenario", i.e., a problem is considered "difficult" if it is difficult for *some* inputs. But, in real life quite often we really care whether it is easy or difficult for "most" cases, for the "generic" inputs. These two different approaches to complexity theory can be very different. There are even "undecidable" problems which can be solved in polynomial time for "most" inputs. In recent years there have been a number of papers studying this direction in combinatorial group theory. Some of it was motivated by the proposal of various cryptosystems based on the braid groups.

This led to various approaches to the notion of "generic" elements in a finitely generated group (cf. [KMSS1], [KMSS2], [KS1], and [MR]). Let us call the reader's attention to [BMNVW], where it is shown that the answer to a problem can be very different in two different models of randomness, even if both are "natural".

Anyway, here is the model we will work with: Let Γ be a group generated by a finite symmetric set Σ. We will assume that Σ satisfies some relation of odd length. (This is a non-essential condition that simplifies the notation, avoiding bipartite graphs in what follows. It happens automatically if e—the identity element of Γ—is in Σ.) A walk w on Γ w.r.t. Σ is a function $w : \mathbb{N}^+ \to \Sigma$. The kth step of w is $w_k := w(1) \cdot \ldots \cdot w(k)$ (where $w_0 = e$). The uniform measure μ on Σ induces a product measure $\overline{\mu}$ on the set of Σ-walks $W_\Sigma := \Sigma^{\mathbb{N}^+}$. For a subset Z of Γ we denote the probability that the kth step of a walk belongs to Z by $\text{prob}(w_k \in Z)$. We say that Z is *exponentially small w.r.t.* Σ if there are constants $c, \alpha > 0$ s.t. $\text{prob}(w_k \in Z) \leq ce^{-\alpha k}$ for every $k \in \mathbb{N}$. If this happens w.r.t. every such Σ (where c and α may depend on Σ), Z is *exponentially small*. We will say that Z is *exponentially generic* if its complement in Γ is exponentially small.

Now, once there is a meaning to being "small" and "large", we can see that the set of g's in $\Gamma = \text{SL}_n(\mathbb{Z})$ for which $C_\Gamma(g)$ is not abelian is exponentially small. Indeed, fix a set Σ of generators for Γ and let $k \in \mathbb{N}$ and p be a prime of size exponential in k. The set Z_p of matrices in $\text{SL}_n(\mathbb{F}_p)$ with multiple eigenvalues (i.e., the discriminant equals zero) satisfies $\frac{|Z_p|}{|\text{SL}_n(\mathbb{F}_p)|} \sim \frac{1}{p}$. By Proposition 1.12 and Theorem 2.3, $Y = \text{Cay}(\text{SL}_n(\mathbb{F}_p); \Sigma)$ are ε-expanders for some ε depending on Σ but not on p. Thus by Proposition 1.6, the random walk on Y falls into Z_p at time k with probability approximately $\frac{1}{p}$, which is exponentially small in k.

The above argument illustrates how expanders play an important role in measuring subsets of Γ. Similar ideas can lead to results which at first sight look very different:

Theorem 5.1 ([BCLM]). *Let Γ be a linear group generated by a finite set Σ. If Γ is not virtually nilpotent, then Γ has exponential conjugacy growth; i.e., there exists a constant $C > 1$ such that for every $k \gg 0$, the ball of radius k around the identity in $\text{Cay}(\Gamma; \Sigma)$ intersects non-trivially at least C^k different conjugacy classes.*

Here the point of the proof is that in congruence quotients, each conjugacy class is "small". In the last result, and in the stronger forms of it in [BCLM], one does not really need the full power of expanders, and results such as Theorem 2.22 above suffice. That is why it also holds in positive characteristic. This is not the case for the more powerful method we will apply in the next section, which needs Theorem

2.24. At this point, this last result is known only in characteristic zero. It will be very useful to prove an analogous result for positive characteristic.

5.2. **Sieve method in group theory.** The results mentioned in the previous section "measure" a subset Z of $\Gamma = \mathrm{SL}_n(\mathbb{Z})$ (or more general linear groups) by projecting it to $\mathrm{SL}_n(\mathbb{F}_p)$ for one prime p, at a time, showing that the projection Z_p is "small" and, since $\mathrm{SL}_n(\mathbb{F}_p)$ is an expander, the random walk meets Z_p with exponentially small probability. This method works for sets Z for which the projections Z_p are small, e.g., when Z is an intersection of an algebraic variety V with Γ. In this case, indeed, the projection Z_p is "small" by the famous Lang–Weil Theorem. But for various natural problems, the projection Z_p of Z mod p is large (say, proportional to the size of $\mathrm{SL}_n(\mathbb{F}_p)$). For dealing with such problems, one needs the group sieve method, which is a group theoretical analogue of the "large sieve" in analytic number theory.

We can now formulate the general "group sieve method":

Theorem 5.2. *Let Γ be a finitely generated group. Let $(N_i)_{i\in I}$ be a series of finite index normal subgroups of Γ, where $I \subseteq \mathbb{N}$. Assume that there are constants $\gamma > 0$ and $d \in \mathbb{N}^+$ such that:*

1. *$|\{i \in I \mid i \le e^k\}| \ge e^{\gamma k}$ for every large enough $k \in \mathbb{N}$.*
2. *Γ has property (τ) w.r.t. the family of normal subgroups $(N_i \cap N_j)_{i,j\in I}$.*
3. *$|\Gamma_i| \le i^d$ for every $i \in I$, where $\Gamma_i := \Gamma/N_i$.*
4. *The natural map $\Gamma_{i,j} \to \Gamma_i \times \Gamma_j$ is an isomorphism for every distinct $i, j \in I$ where $\Gamma_{i,j} := \Gamma/N_i \cap N_j$.*

Then a subset $Z \subseteq \Gamma$ is exponentially small if there is $c > 0$ such that:

5. *$\frac{|Z_i|}{|\Gamma_i|} \le 1 - c$ for every $i \in I$, where $Z_i := ZN_i/N_i$.*

The above formulation is taken from [LM1]. This is a generalization (and simplification) of a method used by Rivin [Ri1], and by Kowalski [Ko1]. It has been greatly influenced by the "affine sieve" of Section 4.

The last theorem gives a very general result, but applying it for particular cases still requires a substantial amount of work. The more difficult part is establishing properties 2 and 5 in the theorem above. Property 2 is true for a large class of groups by Theorem 2.24. (This theorem is formulated for subgroups of $\mathrm{GL}_n(\mathbb{Q})$ but usually one can reduce questions about general finitely generated linear groups, over fields of characteristic zero, to this case by the method of specialization; cf. [LM1].) As mentioned in §5.1, it will be useful to have an analogue of Theorem 2.24 for fields of positive characteristic. Once this is done, the group sieve method should give various applications for these cases also.

Property 5 of Theorem 5.2 depends very much on each specific problem. Let us describe here the case where $Z \subseteq \Gamma$ is the subset of all proper powers in Γ, i.e., $Z = \bigcup_{m\ge 2} Z(m)$, where for $2 \le m \in \mathbb{N}$, we denote $Z(m) = \{\gamma^m \mid \gamma \in \Gamma\}$ the *set* of m-powers. The main result of [LM1] is the following:

Theorem 5.3. *Let Γ be a finitely generated linear group over a characteristic zero field. Assume Γ is not virtually solvable. Then*

$$Z = \bigcup_{2\le m\in\mathbb{N}} Z(m) = \bigcup_{2\le m\in\mathbb{N}} \{\gamma^m \mid \gamma \in \Gamma\}$$

is an exponentially small subset of Γ.

This theorem is a far-reaching straightening of the main result of [HKLS]. Not only does it give a quantitative result on Z, but it also deals with the union of all the $Z(m)$'s together. In [HKLS] only finitely many m's could be considered at a time. This is the power of the sieve which enables such a stronger result.

The proof of property 5 of Theorem 5.2 for this case also needs some careful treatment: the projection of Z is *onto* for *every* finite quotient. (This means that Z is dense in the profinite topology of Γ and still exponentially small!) Thus one has to treat each $Z(m)$ separately, getting quantitative results and then summing them together (see [LM1] for details).

5.3. **The mapping class group.** In this section we will apply the group sieve method to $A = \mathrm{Aut}(F_n)$, the automorphism group of the free group on n generators and to $M = \mathrm{MCG}(g)$, the mapping class group of a closed surface S_g of genus g. The group M is isomorphic to $\mathrm{Out}\left(\prod_g\right) = \mathrm{Aut}\left(\prod_g\right)/\mathrm{Inn}\left(\prod_g\right)$, the group of outer automorphisms of $\prod_g = \pi_1(S_g)$, the fundamental group of S_g. The group $\prod_g$ has a presentation with $2g$ generators $a_1, \ldots, a_g, b_1, \ldots, b_g$ subject to one relation $\prod_{i=1}^{g}[a_i, b_i]$, where $[a,b] = a^{-1}b^{-1}ab$. The mapping class group is of great importance in topology and geometry and we will come back to these aspects in Section 6, where we will treat geometric applications of expanders. Here we mainly treat it from its algebraic description, though the major question comes from topology.

Thurston classified the elements of M into three kinds: (i) pseudo-Anosov, (ii) reducible, and (iii) elliptic. This is somewhat similar in spirit to the classification of elements of $\mathrm{MCG}(1) = \mathrm{SL}_2(\mathbb{Z})$ into hyperbolic, parabolic, and elliptic. We will not give the exact definitions, sending the reader to [Ri1], [Ko1], and the references therein for details. Thurston conjectured that "generic" elements of M are pseudo-Anosov. In one form (which is weaker and stronger than the following theorem) this was proved by Maher ([Ma1], [Ma2]). Rivin [Ri1] (see also Kowalski [Ko1]) proved, by using the sieve method:

Theorem 5.4. *The set of pseudo-Anosov elements of $M = \mathrm{MCG}(g)$ is exponentially generic.*

The proof uses the fact that $M = \mathrm{MCG}(g)$ is mapped onto the arithmetic group $\Gamma = \mathrm{Sp}(2g, \mathbb{Z})$. Now, a criterion due to Casson and Bleiler gives a sufficient condition for an element γ of M to be pseudo-Anosov in terms of some conditions on its image $\gamma' \in \Gamma$. Rivin showed that the set of those $\gamma' \in \Gamma$ which do not satisfy this condition is exponentially small and deduced that the non-pseudo-Anosov elements of M form an exponentially small set.

The proof sketched above gives no information on the subgroup

$$T = \ker\left(\mathrm{MCG}(g) \to \mathrm{Sp}(2g, \mathbb{Z})\right),$$

the Torelli subgroup of the mapping class group. It was asked by Kowalski [Ko1] whether a similar result to Theorem 5.4 holds also for T. In [LM2] and in [MS], independently, it was shown to be the case by using various representations of T onto $\mathrm{Sp}(2(g-1), \mathbb{Z})$ obtained by considering the action of T on the homology of the two-sheeted covers of the surface S_g (or equivalently on the commutator quotients of the index 2 subgroups of $\prod_g$) in the spirit of [Lo] and [GL].

The above-mentioned results have analogous results, proved also in [Ri1], [Ri2], [Ko1] and [LM3], for $\mathrm{Aut}(F_n)$ replacing $\mathrm{MCG}(g)$.The role of pseudo-Anosov is played by either the "fully irreducible" automorphisms (also called *irreducible with*

irreducible powers, or iwip, for short) or by the "hyperbolic" automorphisms. The first are the automorphisms $\alpha \in \mathrm{Aut}(F_n)$ such that no positive power of α sends a free factor H of F_n to a conjugate. The second are the automorphisms α such that for every $m \geq 1$, no conjugacy class of F_n is preserved by α^m. There are iwip automorphisms which are not hyperbolic and hyperbolic automorphisms which are not iwip. The conclusion is that the automorphisms which are iwip and hyperbolic are exponentially generic in $\mathrm{Aut}(F_n)$ as well as in $IA(n) = \ker(\mathrm{Aut}(F_n) \to \mathrm{GL}_n(\mathbb{Z}))$ when $n \geq 3$.

5.4. **The generic Galois group of linear groups.** The method of proof of the results in the previous section showed (when establishing the criterion of Casson and Bleiler mentioned there) something stronger which is of independent interest: for an exponentially generic matrix $A \in \mathrm{SL}_n(\mathbb{Z})$, the Galois group over $\mathbb{Q}$ of the splitting field of the characteristic polynomial of A is isomorphic to $\mathrm{Sym}(n)$, the full symmetric group on n letters. Similarly, for generic elements in $\mathrm{Sp}(2g, \mathbb{Z})$, the Galois group of the splitting polynomial is isomorphic to the Weyl group of the algebraic group $\mathrm{Sp}(2g)$. A common generalization was proved by Jouve, Kowalski and Zywina [JKZ].

Theorem 5.5. *Let k be a number field, and let $\mathbf{G}$ be a connected semisimple group defined and split over k with a faithful representation $\rho : \mathbf{G} \to \mathrm{GL}(m)$ defined over k. Let $\Gamma \subseteq \mathbf{G}(k)$ be an arithmetic subgroup. Then for exponentially generic elements A in Γ, the Galois group of the splitting field over k of the characteristic polynomial of A is isomorphic to the Weyl group $W(\mathbf{G})$ of the algebraic group $\mathbf{G}$.*

Although this statement seems to be asymptotic, the method is effective and enables one, for example, to find matrices whose characteristic polynomials have $W(E_8)$ as their Galois groups over k.

The reader is referred to [JKZ] for a more general result when $\mathbf{G}$ does not split and to [LR] for more general linear groups. (The results are somewhat different!)

Those results use heavily the fact that congruence quotients are expanders. But they also need an interesting use of the Chebotarev theorem which "provides" elements in conjugacy classes of the "target" Galois group. These elements are defined only up to conjugacy. This leads to the following interesting notion:

Definition 5.6. A subset S of a finite group G is said to generate G invariably if $G = \left\langle s^{g(s)} \,\middle|\, s \in S \right\rangle$ for *any* choice of $g(s) \in G$ (i.e., if every element of S is replaced by some conjugate of it, we still get a set of generators).

This is an interesting group-theoretic invariant of importance for computational group theory. For some basic properties of it, see [KLS] and the references therein. It illustrates once again how results and methods from pure mathematics and computer science enrich each other back and forth.

5.5. **Property (τ) in combinatorial group theory.** Let Γ be a discrete group. It is called *residually finite* if the intersection of the finite index subgroups is trivial. We say that Γ *splits* if Γ can be written as a free product with amalgamation $A \underset{C}{*} B$ or as an HNN-construction $A_{*_{C_1 = C_2}}$ in a non-trivial way, i.e., $C \lneqq A, B$. It is well known that Γ splits if and only if it acts on a simplicial tree without a (common) fixed point. Note that if Γ is finitely generated, then it is an HNN-construction

if and only if Γ is mapped surjectively onto the infinite cyclic group $\mathbb{Z}$, and this happens iff the commutator subgroup $[\Gamma, \Gamma]$ of Γ is of infinite index.

For a finitely generated group Λ, we denote by $d(\Lambda)$ the minimal number of generators of Λ. The *rank gradient* of Γ, $\mathrm{RG}(\Gamma)$ is defined as

$$\mathrm{RG}(\Gamma) = \inf \left\{ \frac{d(\Lambda) - 1}{[\Gamma : \Lambda]} \;\middle|\; \begin{array}{l} \Lambda \,\text{finite index} \\ \text{subgroup of } \Gamma \end{array} \right\}.$$

The following result of Lackenby [La1] gives a surprising connection between (τ), splitting, and $\mathrm{RG}(\Gamma)$.

Theorem 5.7. *Let Γ be a finitely presented residually finite group. Then Γ satisfies (at least) one of the following three properties:*

(*a*) *Γ virtually splits (i.e., has a finite index subgroup Λ which splits).*
(*b*) *Γ has property (τ).*
(*c*) *$\mathrm{RG}(\Gamma) = 0$.*

The method of proof is as follows: one assumes that Γ does not have (*b*) and (*c*), i.e., the quotient graphs of Γ are *not* expanders, and $\mathrm{RG}(\Gamma) > 0$, which means that the number of generators of finite index subgroups grows linearly with the index. These two pieces of information are used to deduce that a suitable finite cover Y of a two-dimensional complex X with $\pi_1(X) = \Gamma$ can be decomposed as $Y = Y_1 \cup Y_2$ in a non-trivial way that will enable us to apply the van Kampen Theorem to deduce that $\pi_1(Y)$ splits; see [La1] for details.

As we will see in the next section, it is of great importance in the theory of 3-manifolds to be able to show that $\pi_1(M)$ of such a manifold M virtually splits. So a result, such as Theorem 5.7 and various variants of it, is useful there as a tool to get the desired conclusion.

Another application is that for every finitely presented amenable group Γ, $\mathrm{RG}(\Gamma) = 0$ since such a Γ does not have τ ([LW]) and cannot split since groups which split contain non-abelian free groups (except for D_∞, the infinite dihedral group for which clearly $RG = 0$) while amenable groups cannot contain free groups. This last corollary was extended to all finitely generated amenable groups in [AJN].

6. Expanders and geometry

In this section we describe several ways in which expanders have appeared, somewhat unexpectedly, in geometry. Most of these applications are for hyperbolic manifolds. The background is given in §6.1. Then in §6.2 we will give the first application: a proof given in [L3] using expanders and property (τ) of a conjecture of Thurston and Waldhausen on positive virtual Betti numbers for arithmetic hyperbolic manifolds. Then in §6.3 we describe the attack of Lackenby on the "virtual Haken conjecture" for hyperbolic 3-manifolds using expanders (or more precisely the Lubotzky–Sarnak conjecture asserting that hyperbolic 3-manifolds hyperbolic do *not* have (τ)). While, as of now, this attack has not led to a complete solution of the virtual Haken conjecture, it has led to some partial results and opened exciting new directions. In particular, it shows connections between the Heegaard genus of 3-manifolds and expanders. This will be elaborated upon further in §6.4. There we will show another application of expanders to hyperbolic 3-manifolds. Moreover, the notion of cost from dynamics will be related to 3-manifolds via expanders!

6.1. **Hyperbolic manifolds.** Let M be an oriented n-dimensional hyperbolic manifold of finite volume. Such a manifold is obtained from the Lie group $G = \mathrm{SO}(n,1)$, the group of $(n+1)\times(n+1)$ real matrices preserving the quadratic form $X_1^2+\cdots+X_n^2-X_{n+1}^2$, in the following way: Let $K=\mathrm{SO}(n)$ sitting as a maximal compact subgroup of G and Γ a torsion-free lattice (i.e., discrete subgroup of finite covolume) in G. Then $\mathbb{H}^n = G/K$ is the n-dimensional hyperbolic space and $M=\Gamma\backslash G/K$ is a hyperbolic manifold of finite volume. All such manifolds are obtained in that way. Many geometric questions on such an M can be translated to group-theoretic questions about Γ, which is actually isomorphic to the fundamental group of M as $\mathbb{H}^n$ is contractible.

One of these questions is the following conjecture usually attributed to Thurston (though it probably goes back to Waldhausen):

Conjecture 6.1 (Thurston–Waldhausen conjecture)**.** *The manifold M has a finite sheeted cover $M_0 \twoheadrightarrow M$ with positive $\beta_1(M_0) := \dim H_1(M_0,\mathbb{R})$, i.e., non-trivial homology group. Or, equivalently, in group-theoretic terms: every lattice Γ in $\mathrm{SO}(n,1)$ has a finite index subgroup Γ_0 with $|\Gamma_0/[\Gamma_0,\Gamma_0]|=\infty$.*

The equivalence follows from two well-known facts: every lattice is finitely generated and has a torsion-free subgroup of finite index. The commutator quotient is infinite iff there is a surjective map $\Gamma_0 \twoheadrightarrow \mathbb{Z}$, and this happens iff the first real homology of $\Gamma_0\backslash G/K$ is non-trivial.

Let us mention right at the start another conjecture, due to Serre [Se] (which is now almost fully proved, see §6.2 below).

Conjecture 6.2 (Serre Conjecture)**.** *If Γ is an arithmetic lattice of $G=\mathrm{SO}(n,1)$, then Γ has a negative answer to the congruence subgroup property.*

It is well known that the Thurston–Waldhausen conjecture implies Serre's conjecture. This can be seen in one of the following ways:

(i) If Γ has the congruence subgroup property, then its profinite completion $\hat{\Gamma}$ is the same as the congruence completion. The latter is a product of compact p-adic analytic semisimple groups and as such, a finite index subgroup of it should have finite abelianization. Thus the same applies to $\hat{\Gamma}$ and Γ.

(ii) It is known that the congruence subgroup property for Γ implies superrigidity (cf. [Se]), but if Γ virtually maps onto $\mathbb{Z}$, it does not have superrigidity.

An intermediate step between these two conjectures is:

Conjecture 6.3 (Lubotzky–Sarnak conjecture)**.** *If Γ is a lattice in $SO(n,1)$, then Γ does not have property (τ).*

Now, Thurston–Waldhausen conjecture $\Rightarrow$ Lubotzky–Sarnak conjecture $\Rightarrow$ Serre conjecture. Indeed, if a finite index subgroup of Γ is mapped onto $\mathbb{Z}$, then it clearly does not have (τ) as $\mathbb{Z}$ does not have (τ). Also, we mentioned in §2.5 that an arithmetic lattice Γ always has (τ) with respect to congruence subgroups. Thus, if Γ does not have (τ), it must also have non-congruence subgroups.

This last observation was the key point in [L3] to be described in §6.2. But before going into these details, let us continue with another conjecture for the special case, $n=3$, which is the most interesting case:

Conjecture 6.4 (Virtual Haken conjecture)**.** *A finite volume hyperbolic* 3*-manifold* M *is virtually Haken, i.e., has a finite sheeted cover which is Haken (also known as "sufficiently large").*

Recall that Haken means that it contains an incompressible surface, i.e., a properly embedded orientable surface S (other than S^2) with $\pi_1(S)$ injecting into $\pi_1(M)$. It is known that M is Haken iff $\pi_1(M)$ is either mapped onto $\mathbb{Z}$ or $\pi_1(M)$ is a free product with amalgam in a non-trivial way, i.e., iff $\pi_1(M)$ splits, in the terminology of §5.5. From this it is clear that the Thurston–Waldhausen conjecture for $n = 3$ implies the virtual Haken conjecture.

6.2. **Thurston–Waldhausen conjecture for hyperbolic arithmetic manifolds.** The first use of expanders in geometry came out in the proof of the following result in [L3]:

Theorem 6.5. *Conjecture* 6.1 *is true for arithmetic lattices in* $\mathrm{SO}(n,1)$ *for* $n \neq 3, 7$*. Namely, every finite volume* n*-dimensional arithmetic hyperbolic manifold has a finite sheeted cover with a positive first Betti number if* $n \neq 3, 7$*.*

The result also covers "most" of the arithmetic lattices in $\mathrm{SO}(3,1)$ and $\mathrm{SO}(7,1)$. But these two cases are exceptional in having "more" arithmetic lattices than what one finds in $\mathrm{SO}(n,1)$ for other n's. The reasons are that $\mathrm{SO}(3,1)$ is locally isomorphic to $\mathrm{SL}_2(\mathbb{C})$ and as such it also has a complex structure, unlike all other n's. On the other hand, $\mathrm{SO}(7,1)$ is a real form of $\mathrm{SO}(8)$. The later has Dynkin diagram of type D_4 and as such it also has a graph automorphism of order 3 ("the triality of D_4") unlike the other D_n's which have only automorphisms of order 2. The theory of "Galois cohomology", which enables one to classify the arithmetic lattices in a given semisimple Lie group, shows that these anomalies give extra families of arithmetic lattices in $\mathrm{SO}(3,1)$ and $\mathrm{SO}(7,1)$ which do not exist for other n's. The method of proof of Theorem 6.5 does not apply to these extra families.

The connection between Conjecture 6.1 and expanders (or more precisely property (τ)) is best explained via the following:

Lemma 6.6 (The Sandwich Lemma)**.** *Assume* $G_1 \leq G_2 \leq G_3$ *are three non-compact simple Lie groups and for each* $i = 1, 2, 3$*,* Γ_i *is an arithmetic lattice in* G_i *such that* $\Gamma_1 \leq \Gamma_2 \leq \Gamma_3$*,* $\Gamma_2 = G_2 \cap \Gamma_3$ *and* $\Gamma_1 = G_1 \cap \Gamma_3 (= G_1 \cap \Gamma_2)$*. Then the following hold:*

- *(i) If* Γ_1 *has the Selberg property (i.e., property* (τ) *w.r.t. congruence subgroups; see Definition* 2.14*) and* Γ_3 *does not have* (τ)*, then* Γ_2 *has a negative answer to the congruence subgroup problem (i.e., has non-congruence subgroups).*
- *(ii) If* Γ_1 *has the Selberg property and* Γ_3 *has a congruence subgroup* Λ *with an infinite abelianization, then* Γ_2 *also has such a congruence subgroup.*

Part (i) of the lemma follows immediately from the Burger–Sarnak result (Theorem 2.17): indeed, the Selberg property of Γ_1 "lifts up" to Γ_2. On the other hand, Γ_2 does not have (τ), as otherwise Γ_3 would have. Thus, Γ_2 has (τ) but does not have Selberg. In other worlds, the quotients of Γ_2 modulo congruence subgroups give a family of expanders, while the family of all finite quotients does not. This shows (in a very non-constructive way!) that there are non-congruence subgroups in Γ_2! The proof of (ii) needs to go deeper into the actual proof of the Burger–Sarnak result (see [L3] and [BS]).

Anyway, the point is that when $n \neq 3, 7$, the arithmetic lattices in $\mathrm{SO}(n,1)$ can be put to be Γ_2 is such a sandwich: one takes $G_1 = \mathrm{SO}(2,1) \simeq \mathrm{SL}_2(\mathbb{R})$ or $G_1 = \mathrm{SO}(3,1) \simeq \mathrm{SL}_2(\mathbb{C})$ and one uses Jacquet–Langlands and Selberg results to ensure the Selberg property. On the other hand, $G_3 = \mathrm{SU}(n,1)$ and one uses results of Kazhdan, Shimura, and Borel and Wallach to ensure the needed properties of Γ_3; see [L3] and the references therein. These arguments show that if Γ is an arithmetic lattice in $\mathrm{SO}(n,1), n \neq 3, 7$, it has a congruence subgroup which is mapped onto $\mathbb{Z}$. In particular, it does not satisfy (τ) (so the Lubotzky and Sarnak Conjecture 6.3 is also valid) and does not have the congruence subgroup property (so Serre's conjecture 6.2 is also true for these cases).

All these three conjectures are still open for the lattices of $\mathrm{SO}(7,1)$ coming from the triality effect of D_4. The story of $n = 3$ is more involved and more important. This is our topic in the next section. We just mention in passing that the Thurston–Waldhausen conjecture has been proved for the *known* non-arithmetic lattices in $\mathrm{SO}(n,1)$ for $n \geq 4$ (see [L4]). It is still widely open for others (if they exist at all ...).

6.3. **Hyperbolic 3-manifolds.** A few years ago, Marc Lackenby initiated a program to prove the virtual Haken conjecture for hyperbolic 3-manifolds (Conjecture 6.4 above). In his program, expanders (or property τ) play a central role, as well as the notion of Heegaard splitting. Let us recall the definition of the latter.

Let M be a connected, closed, orientable, and irreducible (i.e., any two-dimensional sphere in M bounds a three-dimensional ball) 3-manifold. We will be mainly interested in hyperbolic 3-manifolds, i.e., the case when $M = \Gamma\backslash\mathbb{H}^3$, where Γ is a cocompact torsion-free lattice in $G = P\mathrm{SL}_2(\mathbb{C})$.

A classical result asserts that every such M can be decomposed as a union of two handle bodies $M = H_1 \cup H_2$ glued along their (isomorphic) boundaries, i.e., $H_1 \cap H_2 = \partial H_1 = \partial H_2$. This decomposition *(Heegaard splitting)* is not unique. The minimal number g of handles in H_1 (or H_2—they are isomorphic) in such a decomposition is called the *Heegaard genus* of M, denoted $g(M)$. Note that if H_1 has g handles, its boundary is a closed surface of genus g and Euler characteristic $2 - 2g$.

The following result of Lackenby [La3] shows a first connection between the Heegaard genus and the Cheeger constant $h(M)$ of M. See Definition 1.16 and Theorem 1.20 for the definition of Cheeger constant of M and its connection with expanders.

Theorem 6.7. *Let M be a closed Riemannian 3-manifold with supremal sectional curvature $K < 0$ (so $K = -1$ if M is hyperbolic). Then*

$$h(M) \leq \frac{8\pi(g(M) - 1)}{|K|\mathrm{vol}(M)}.$$

While this is a non-trivial result, the basic idea is simple: one proves that the Heegaard splitting (which is a topological decomposition) can be carried out in such a way that the two parts H_1 and H_2 have approximately equal volumes, half of the volume of M. Now, the area of the boundary, which is a surface of genus $g(M)$, is given by the Gauss-Bonnet formula as a linear function of $g(M)$ and the theorem can be deduced.

Given a Heegaard splitting of M one can write a presentation of M with g generators (say, pick a point on ∂H_1 and take as generators the generators of

$\pi_1(H_1)$, which is a free group on g generators) and g relations (obtained from non-trivial loops in H_1 which become homotopically trivial once H_2 is glued to H_1 along ∂H_2). In particular, one has:

Proposition 6.8. *$d(\pi_1(M)) \leq g(M)$; i.e., the number of generators of the fundamental group of M is bounded above by the Heegaard genus.*

For general 3-manifolds this can be a strict inequality, but:

Conjecture 6.9 (Heegaard genus versus rank conjecture)**.** *If M is a compact hyperbolic 3-manifold, then $d(\pi_1(M)) = g(M)$.*

Now, if M_0 is an r-sheeted cover of M, then the Heegaard splitting of M can be lifted to M_0 and one can deduce that $g(M_0) \leq rg(M)$. To "renormalize" this, define:

Definition 6.10. Let $\Gamma = \pi_1(M)$, let $\mathcal{L} = \{N_i\}$ be a family of finite index subgroups of Γ, and let $\{M_i\}$ be the corresponding finite sheeted covers. The *infimal Heegaard gradient* $\chi^h_{\mathcal{L}}(M)$ of M w.r.t. $\mathcal{L}$ is defined as $\chi^h_{\mathcal{L}}(M) = \inf_i \left\{ \frac{2g(M_i)-2}{[\Gamma:N_i]} \right\}$.

One uses $2g(M_i)-2$, the negative of the Euler characteristic, rather than $g(M_i)$, just for aesthetic reasons. The reader may note the connection with the rank gradient defined in §5.5, especially in light of Proposition 6.8.

There are many examples of M in which $\chi^h_{\mathcal{L}}(M) = 0$, where, say, $\mathcal{L}$ is a family of (all) finite index subgroups of $\pi_1(M)$. This happens for example if M fibres over a circle (or virtually fibres over a circle). There are many examples of such hyperbolic 3-manifolds. In fact, a conjecture attributed to Thurston suggests that every hyperbolic 3-manifold fibres over a circle after passing to a suitable finite sheeted cover. This is even stronger than Conjecture 6.1 above. In group-theoretic terms it is equivalent to the assertion that $\Gamma = \pi_1(M)$ has a finite index subgroup Γ_0 with an epimorphism $\pi : \Gamma_0 \twoheadrightarrow \mathbb{Z}$ whose kernel $\mathrm{Ker}(\pi)$ is finitely generated. In this case $\mathrm{Ker}(\pi)$ must be a surface group of genus g and going along the cyclic covers between Γ_0 and $\mathrm{Ker}(\pi)$ we get infinitely many covers with the same Heegaard genus. Hence $\chi^h_{\mathcal{L}}(M) = 0$.

Lackenby conjectured that this is the only reason for the Heegaard gradient to vanish, i.e.,

Conjecture 6.11 (Heegaard gradient conjecture)**.** *If M has a family of covers $\mathcal{L}$ with $\chi^h_{\mathcal{L}}(M) = 0$, then M virtually fibres over a circle.*

He then proved:

Theorem 6.12. *Let M be a closed, orientable 3-manifold, and let $\mathcal{L} = \{N_i\}$ be a family finite index normal subgroups, with corresponding covers $\{M_i\}$. Assume:*

a) *$\chi^h_{\mathcal{L}}(M) > 0$;*
b) *$\Gamma = \pi_1(M)$ does* not *have property (τ) w.r.t $\mathcal{L}$.*

Then M is virtually Haken.

This last result implies:

Corollary 6.13. *The Lubotzky–Sarnak conjecture (Conjecture* 6.3*) and the Heegaard gradient conjecture (Conjecture* 6.11*) imply the virtual Haken conjecture (Conjecture* 6.4*).*

Indeed let M be a three-dimensional hyperbolic manifold, $\Gamma = \pi_1(M)$, and let $\mathcal{L}$ be the family of all its finite index normal subgroups. By the Lubotzky–Sarnak conjecture Γ does not have (τ), so condition (b) of Theorem 6.12 is satisfied. If $\chi^h_{\mathcal{L}}(M) > 0$, then M is virtually Haken by this theorem, while if $\chi^h_{\mathcal{L}}(M) = 0$, then by the Heegaard gradient conjecture, M virtually fibres over a circle and in particular, is virtually Haken.

This puts property (τ) and expanders at the heart of the theory of three-dimensional manifolds. As of now, the full virtual Haken conjecture has not been proven, but this approach, beside its intrinsic interest, led to some interesting unconditional results; cf. [La3], [La4], [LaLR1], [LaLR2].

6.4. **Heegaard splitting, property (τ), and cost.** In the previous section we saw the result of Lackenby, Theorem 6.7, which connects the Heegaard genus and the Cheeger constant. The Cheeger constant is the geometric way to express expanders (see Theorem 1.20). These connections enabled Long, Lubotzky, and Reid [LLR] to deduce the following geometric application of the theory of expanders.

Theorem 6.14. *Let M be a closed hyperbolic 3-manifold. Then there exists a sequence $\mathcal{L} = \{N_i\}_{i\in\mathbb{N}}$ of finite index normal subgroups of $\Gamma = \pi_1(M)$, with $N_1 \supseteq N_1 \supseteq \cdots$ and $\bigcap N_i = \{e\}$, and $\chi^h_{\mathcal{L}}(M) > 0$. Namely, there is a constant $c > 0$ such that for every $i \in \mathbb{N}$, the Heegaard genus $g(M_i) \geq c[M_i : M]$, where M_i is the cover of M corresponding to N_i of degree $[M_i : M] = [\Gamma : N_i]$.*

Remark 6.15. The formulation in [LLR] is slightly weaker than what is stated here. At that time we used the theory of sum-product results in finite fields and its applications to expanders in [BG1]. The more recent results (see Theorem 2.24 above) enable us to deduce the stronger version here.

It should be stressed that in many examples of M's as in Theorem 6.14, (and if the Thurston Conjecture is correct, then in all such M's!), one can also find a chain of normal subgroups $\mathcal{L}'$ in $\pi_1(M)$ with $\chi^h_{\mathcal{L}'}(M) = 0$. This shows that the Heegaard gradient does depend on the choice of chains of normal covers (even chains with trivial intersections).

This brings us to another fascinating connection: the notion of *cost*.

Let Γ be a countable group acting ergodically on X, a standard Borel space, by Borel automorphisms preserving a probability measure μ on X. Define the equivalence relation E on X by xEy iff x and y are on the same Γ-orbit. So E is a subset of $X \times X$, which can be thought of as defining a graph on X. For an arbitrary Borel subset S of $X \times X$ we denote $\deg_S(x) = |\{y \in X | (x, y) \in S\}|$ and $e(s) = \int_{x\in X} \deg_S(x) d\mu$ (see [Gab2]).

We say that S spans E if E is the minimal equivalence relation on X which contains S and define $\mathrm{cost}(E) = \mathrm{cost}(\Gamma, X)$ as $\inf e(S)$ when S runs over all the Borel subgraphs S spanning E.

One can easily see that if $\{\gamma_1, \ldots, \gamma_d\}$ generates Γ, then

$$S = \bigcup_{i=1}^{d} \bigcup_{x\in X} \{(x, \gamma_i x)\}$$

spans E and so always $\mathrm{cost}(\Gamma, X) \leq d(\Gamma)$, the number of generators of Γ.

This notion was introduced by Levitt [Le] and was used by Gaboriau [Gab1] to distinguish between equivalence relations of different group actions. Gaboriau conjectured:

Conjecture 6.16 (Fixed price conjecture)**.** *Given* Γ*, then* $\mathrm{cost}(\Gamma, X)$ *is the same number for all ergodic, essentially free actions of* Γ *on a standard Borel space* X*. (Essentially free means that the set of* $x \in X$ *with non-trivial stabilizer in* Γ *is of measure zero.)*

Gaboriau proved this conjecture for various groups, but it is still widely open for general Γ.

An interesting example in which the cost was computed explicitly is:

Theorem 6.17 (Abért and Nikolov [AN])**.** *Let* Γ *be a finitely generated group, let* $\mathcal{L} = \{N_i\}_{i\in\mathbb{N}}$ *be a chain of finite index normal subgroups* $N_1 \supseteq N_2 \supseteq \cdots$ *with* $\bigcap_I N_i = \{e\}$*, and let* $\bar{\Gamma} = \varprojlim \Gamma/N_i$*, the profinite completion of* Γ *w.r.t.* $\mathcal{L}$*. The group* Γ *acts freely on* $\bar{\Gamma}$ *and*

$$\mathrm{cost}(\Gamma, \bar{\Gamma}) = \mathrm{RG}_{\mathcal{L}}(\Gamma) + 1,$$

where $\mathrm{RG}_{\mathcal{L}}(\Gamma)$ *is the rank gradient of* Γ *(see §5.5) w.r.t.* $\mathcal{L}$*, i.e.,* $\lim_i \frac{d(N_i)-1}{[\Gamma:N_i]}$.

Now, if the fixed price conjecture were true, it would follow that the rank gradient of Γ does not depend on the chain $\mathcal{L}$ in the last theorem. On the other hand we saw above that for $\Gamma = \pi_1(M)$, M a three-dimensional hyperbolic compact manifold, the Heegaard genus gradient *does* depend on the choice of $\mathcal{L}$. This enabled Abért and Nikolov to deduce:

Theorem 6.18. *At least one of the two conjectures—the Heegaard genus versus rank conjecture (Conjecture 6.9) and the fixed price conjecture (Conjecture 6.16)—is not true!*

It is quite interesting how these two seemingly unrelated conjectures contradict each other and for our story it is also interesting how this contradiction is via property (τ).

Of course, it might be that both conjectures are false! One may even speculate that the fixed price conjecture is false in general but it is true for hyperbolic groups, just as it is true for free groups ([Gab1]). If this is the case, or even if it is true for the much smaller class of fundamental groups of compact hyperbolic 3-manifolds, then the Heegaard genus versus rank conjecture would be refuted.

Note added in proof. On June 30, 2011, Tao Li announced (see [Lit]) that there exists a compact hyperbolic 3-manifold M with $d(\pi_1(M)) \lneqq g(M)$ and so Conjecture 6.9 is not true. Still if the fixed cost conjecture is true, a stronger result would be deduced: the ration $\frac{d(\pi_1(M))}{g(M)}$ can be arbitrarily small. This is not known as of now.

7. Miscellaneous

As mentioned in the introduction, expander graphs have a huge number of applications in computer science which we have not even begun to mention here. We have focused on applications to pure mathematics. Even in this direction we were not able to give a comprehensive survey. In this final section we will just give a list of topics that, for lack of time, space or the author's expertise, have not found their way into the main sections.

(I) The Baum–Connes conjecture. This is a famous deep conjecture. For a user-friendly introduction, see [Va3]. Counterexamples to a generalized form of it were given in [Gro1] and [HLS]. The original conjecture is still open, though it

was proved for many classes of groups. The counterexamples were given by random groups constructed via expanders.

(II) Embedding metric spaces. There is great interest in embedding (finite) metric spaces into Hilbert spaces in a way that the metric is more or less preserved. In recent years this area has found many applications in computer science; see [HLW, Chap. 13] and [Li]. Expander graphs play the role of graphs whose metric is the farthest away from Euclidean.

(III) Dimension expanders. The notion of expander graphs has an analogue in vector spaces. For a fixed field F and $0 < \varepsilon$, we say that $T_1, \ldots, T_k \in \mathrm{End}_F(F^n)$, i.e., k linear transformations, form an *ε-dimension expander* if for every subspace W of F^n with $\dim(W) \leq \frac{n}{n}$, $\dim\left(\sum_{i=1}^k T_i(W)\right) \geq (1+\varepsilon)\dim W$. For motivation, see [DS]. Again, when one can talk about "probability" (e.g., if F is a finite or local field), "random" $T_1, \ldots, T_k \in \mathrm{End}_F(F^n) = M_n(F)$ will give rise to dimension expanders. Wigderson asked for explicit constructions, which are more difficult to construct. This was done in [LZ] for characteristic zero fields and in [B1] for the general case. This motivates the study of "algebras with property (τ)" such as the amenable algebras in [Ba] and [E].

(IV) High-dimensional expanders. A natural problem, which has been mentioned for a good number of years is: What is the natural definition for higher-dimensional expanders? A suggestion for such a definition was given in [Gro2] and [Gro3] (which formally speaking does not reduce to an expander for dimension one, but it still keeps the spirit of expanders). In [FGLNP], random and explicit constructions of such high dimensional expanders are given. The latter is based on [LSV2].

(V) The distribution of integer points on spheres. The set of integral solutions $H_d = \{(x,y,z) \in \mathbb{Z}^3 | x^2+y^2+z^2 = d\}$ can be normalized by dividing by $\sqrt{d}$ to give a subset of the sphere S^2. The distribution of these points on the sphere was studied by Linnik, and a modern treatment with stronger results is given in [EMV]. The modern approach makes use of random walks on expander graphs.

(VI) Counting rational solutions on curves. Expanders are used in a surprising way in [EHK] to show some strong finiteness results on the number of k-rational points on some families of curves over number fields of bounded degree. This is related to the notion of "gonality" of a curve X (i.e., the minimal degree of a meromorphic function on X, or the minimal d such that X is realized as a ramified cover of the plane). Zograf [Z1], [Z2] showed that if a family of covers of a fixed hyperbolic surface has (τ), then the gonality grows linearly with the volume.

(VII) C^*-algebras. For a Hilbert space H, denote by $B(H)$ the C^*-algebra of the bounded operators of H. In [Va1], Ramanujan graphs were used to study the different possible norms on $B(H) \otimes B(H)$. In [BeSz], property (τ) is used to give explicit examples of $n \times n$ matrices of norm 1 which cannot be well approximated by matrices that decompose into direct sums of smaller matrices.

In another direction, property (τ) has been used to study the question whether the set of finite-dimensional representations of the C^*-algebra $C^*(\Gamma)$ of a finitely generated group separates the points of $C^*(\Gamma)$ (see [Be] and [LSh]). Finally, we mention here [Bue], which describes property τ for von Neumann algebras.

(VIII) Random 3-manifolds. In [DT], Dunfield and Thurston presented a model for "random 3-manifolds". It is based on the fact (explained in §6.3) that every 3-manifold M has a (non-unique) Heegaard splitting, i.e., obtained by gluing

two handle-bodies along their boundaries. The elements of the mapping class group $\mathrm{MCG}(g)$ of a surface of genus g give rise to 3-manifolds of Heegaard genus at most g. Random walks on $\mathrm{MCG}(g)$ give therefore "random" 3-manifolds. The group sieve method presented in Section 5 has already been used for studying the group $\mathrm{MCG}(g)$ and in [Ko1] and [Ko2] it is used to give some results on the first homology of 3-manifolds. It seems to have a great potential for studying further properties of "random 3-manifolds".

We hope to return to this topic in the future.

Acknowledgments

The author is indebted to Peter Sarnak for many years of fruitful collaboration and friendship. Much of what is presented here was inspired by him and in particular in Section 4 we have made extensive use of material from his website. We are grateful to E. Kowalski, N. Linial, C. Meiri, and C. Elsholtz for helpful comments on an earlier draft. Thanks are also due to the ERC and ISF for partial support.

About the author

Alex Lubotzky is the Maurice and Clara Weil Professor of Mathematics at the Hebrew University of Jerusalem, Israel, and an adjunct professor at Yale University. He is a foreign honorary member of the American Academy of Arts and Sciences. In January 2011 he delivered the Colloquium Lectures at the Joint Meetings of the MAA and AMS, upon which this article is based.

References

[AJN] M. Abért, A. Jaikin-Zapirain and N, Nikolov, *The rank gradient from a combinatorial viewpoint*, Groups Geom. Dyn. 5 (2011) 213–230. MR2782170

[AN] M. Abért and N. Nikolov, *Rank gradient, cost of groups and the rank versus Heegaard genus problem*, J. Euro. Math. Soc., to appear. arXiv:math/0701361

[AC] N. Alon and Fan R.K. Chung, *Explicit construction of linear sized tolerant networks*, Discrete Mathematics 72 (1988), 15–19. MR0975519 (90f:05080)

[ALW] N. Alon, A. Lubotzky and A, Wigderson, *Semi-direct product in groups and zig-zag product in graphs: connections and applications* (extended abstract), 42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001), 630637, IEEE Computer Soc., Los Alamitos, CA, 2001. MR1948752

[BHKLS] L. Babai, G. Hetyei, W.M. Kantor, A. Lubotzky, and A. Seress, *On the diameter of finite groups*, 31st Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990), 857–865, IEEE Comput. Soc. Press, Los Alamitos, CA, 1990. MR1150735

[BKL] L. Babai, W.M. Kantor and A. Lubotzky, *Small-diameter Cayley graphs for finite simple groups*, European J. Combin. 10 (1989), no. 6, 507–522. MR1022771 (91a:20038)

[BNP] L. Babai, N. Nikolov and L. Pyber, *Product growth and mixing in finite groups*, Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms, 248–257, ACM, New York, 2008. MR2485310

[Ba] L. Bartholdi, *On amenability of group algebras. I*, Israel J. Math. 168 (2008), 153–165. MR2448055 (2010a:43001)

[BMNVW] F. Bassino, A. Martino, C. Nicaud, E. Ventura and P. Weil, *Statistical properties of subgroups of free groups*, arXiv:1001.4472

[Be] M.B. Bekka, *On the full C^*-algebras of arithmetic groups and the congruence subgroup problem*, Forum Math. 11 (1999), no. 6, 705–715. MR1725593 (2001f:22016)

[BeSz] E.J. Benveniste and S.J. Szarek, *Property T, property τ and irreducibility of matrices*, preprint.

[B1] J. Bourgain, *Expanders and dimensional expansion*, C. R. Math. Acad. Sci. Paris 347 (2009), no. 7-8, 357–362. MR2537230 (2010k:11012)

[B2] J. Bourgain, *New developments in combinatorial number theory and applications*, European Congress of Mathematics, 233–251, Eur. Math. Soc., Zurich, 2010. MR2648328 (2011d:11017)

[BF] J. Bourgain and E. Fuchs, *A proof of the positive density conjecture for integer Apollonian circle packings*, J. Amer. Math. Soc. 24 (2011), 945–967. arXiv:1001.3894 MR2813334

[BFLM] J. Bourgain, A. Furman, E. Lindenstrauss and S. Mozes, *Invariant measures and stiffness for non-abelian groups of toral automorphisms*, C. R. Math. Acad. Sci. Paris 344 (2007), no. 12, 737–742. MR2340439 (2008g:37005)

[BG1] J. Bourgain and A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. (2) 167 (2008), no. 2, 625–642. MR2415383 (2010b:20070)

[BG2] J. Bourgain and A. Gamburd, *On the spectral gap for finitely-generated subgroups of* SU(2), Invent. Math. 171 (2008), no. 1, 83–121. MR2358056 (2009g:22018)

[BG3] J. Bourgain and A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. *I*, J. Eur. Math. Soc. (JEMS) 10 (2008), no. 4, 987–1011. MR2443926 (2010a:05093)

[BG4] J. Bourgain and A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. *II*, with an appendix by J. Bourgain, J. Eur. Math. Soc. (JEMS) 11 (2009), no. 5, 1057–1103. MR2538500 (2011a:60021)

[BGS1] J. Bourgain, A. Gamburd and P. Sarnak, *Sieving and expanders*, C. R. Math. Acad. Sci. Paris 343 (2006), no. 3, 155–159. MR2246331 (2007b:11139)

[BGS2] J. Bourgain, A. Gamburd and P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. 179 (2010), no. 3, 559–644. MR2587341 (2011d:11018)

[BGS3] J. Bourgain, A. Gamburd and P. Sarnak, *Generalization of Selberg's* 3/16 *Theorem and Affine Sieve*, arXiv:0912.5021

[BKT] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. 14 (2004), no. 1, 27–57. MR2053599 (2005d:11028)

[BK] J. Bourgain and A. Kontorovich, *On representations of integers in thin subgroups of* $\mathrm{SL}_2\mathbb{Z}$, Geom. Funct. Anal. (GAFA) 20 (2010), 1144–1174. MR2746949

[BV] J. Bourgain and P.P. Varju, *Expansion in* $\mathrm{SL}_d(Z/qZ)$, *q arbitrary*, arXiv:1006.3365

[BCLM] E. Breuillard, Y. De Cornulier, A. Lubotzky and C. Meiri, *Conjugacy growth of linear groups*. arXiv:1106.4773

[BGa] E. Breuillard and A. Gamburd, *Strong uniform expansion in* $\mathrm{SL}(2,p)$, Geom. Funct. Anal. (GAFA) 20 (2010), 1201–1209. MR2746951

[BGT1] E. Breuillard, B. Green and T. Tao, *Linear Approximate Groups*, Electron. Res. Announc. Math. Sci. 17 (2010), 57–67. MR2718104 (2011g:11018)

[BGT2] E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*, arXiv:1005.1881

[BGT3] E. Breuillard, B. Green and T. Tao, *Suzuki groups as expanders*, Groups Geom. Dyn. 5 (2011), 281–299. MR2782174

[BGGT1] E. Breuillard, B. Green, R. Guralnick and T. Tao, *Strongly dense free subgroups of semisimple algebraic groups*, arXiv:1010.4259

[BGGT2] E. Breuillard, B. J. Green, R. Guralnick and T. C. Tao, *Expansion in finite simple groups of Lie type*, in preparation.

[Bue] M. R. Buettgens, *Property* τ *and von Neumann algebras*, Thesis, State University of New York at Buffalo, 2009. MR2712779

[BLMS] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, *On Fibonacci numbers with few prime divisors*, Proc. Japan Acad. Ser. A Math. Sci. 81 (2005), no. 2, 17–20. MR2126070 (2005k:11020)

[BS] M. Burger and P. Sarnak, *Ramanujan duals. II*, Invent. Math. 106 (1991), no. 1, 1–11. MR1123369 (92m:22005)

[Bu] Peter Buser, *Geometry and spectra of compact Riemann surfaces*, Progress in Mathematics, 106. Birkhäuser Boston, Inc., Boston, MA, 1992. xiv+454 pp. MR1183224 (93g:58149)

[CLMNO] F. Celler, C.R. Leedham-Green, S.H. Murray, A.C. Niemeyer and E.A. O'Brien, *Generating random elements of a finite group*, Comm. Algebra 23 (1995), no. 13, 4931–4948. MR1356111 (96h:20115)

[Ch] J.R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica 16 (1973), 157–176. MR0434997 (55:7959)

[Cl] L. Clozel, *Démonstration de la conjecture τ*, Invent. Math. 151 (2003), no. 2, 297–328. MR1953260 (2004f:11049)

[DSV] G. Davidoff, P. Sarnak and A. Valette, *Elementary number theory, group theory, and Ramanujan graphs*, London Mathematical Society Student Texts, 55. Cambridge University Press, Cambridge, 2003. x+144 pp. MR1989434 (2004f:11001)

[DSC] P. Diaconis and L. Saloff-Coste, *Walks on generating sets of groups*, Invent. Math. 134 (1998), no. 2, 251–299. MR1650316 (2000e:60013)

[Di] O. Dinai, *Growth in SL_2 over finite fields*, J. Group Theory, 14 (2011) 273–297. MR2788087

[D] J.D. Dixon, *The probability of generating the symmetric group*, Math. Z. 110 (1969), 199–205. MR0251758 (40:4985)

[DT] N.M. Dunfield and W.P. Thurston, *Finite covers of random 3-manifolds*, Invent. Math. 166 (2006), no. 3, 457–521. MR2257389 (2007f:57039)

[DS] Z. Dvir and A. Shpilka, *Towards dimension expanders over finite fields*, Twenty-Third Annual IEEE Conference on Computational Complexity, 304-310, IEEE Computer Soc., Los Alamitos, CA, 2008. MR2500345 (2010f:68069)

[E] G. Elek, *The amenability of affine algebras*, J. Algebra 264 (2003), no. 2, 469–478. MR1981416 (2004d:16043)

[EHK] J. Ellenberg, C. Hall and E. Kowalski, *Expander graphs, gonality and variation of Galois representations*, arXiv:1008.3675

[EMV] J. S. Ellenberg, P. Michel and A. Venkatesh, *Linnik's ergodic method and the distribution of integer points on spheres*, arXiv:1001.0897

[Er] M. Ershov, *Golod-Shafarevich groups with property (T) and Kac-Moody groups*, Duke Math. J. 145 (2008), no. 2, 309–339. MR2449949 (2009i:20060)

[EJ] M. Ershov and A. Jaikin-Zapirain, *Property (T) for noncommutative universal lattices*, Invent. Math. 179 (2010), no. 2, 303–347. MR2570119 (2011e:22010)

[FGLNP] J. Fox, M. Gromov, V. Lafforgue, A. Naor and J. Pach, *Overlap properties of geometric expanders*, arXiv:1005.1392

[FI] J. Friedlander and H. Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications, 57. American Mathematical Society, Providence, RI, 2010. xx+527 pp. MR2647984 (2011d:11227)

[Fr] J. Friedman, *A proof of Alon's second eigenvalue conjecture and related problems*, Mem. Amer. Math. Soc. 195 (2008), no. 910, viii+100 pp. MR2437174 (2010e:05181)

[Fu] E. Fuchs, Ph.D. Thesis, Princeton University.

[FS] E. Fuchs and K. Sanden, *Some experiments with integral Apollonian circle packings*, arXiv:1001.1406

[Gab1] D. Gaboriau, *Coût des relations d'équivalence et des groupes*, Invent. Math. 139 (2000), no. 1, 41–98. MR1728876 (2001f:28030)

[Gab2] D. Gaboriau, *What is Cost?* Notices Amer. Math. Soc. 57 (2010), 1295–1296. MR2761803

[Ga1] A. Gamburd, *On the spectral gap for infinite index "congruence" subgroups of* $\mathrm{SL}_2(\mathbf{Z})$, Israel J. Math. 127 (2002), 157–200. MR1900698 (2003b:11050)

[Ga2] A. Gamburd, *Expander graphs, random matrices and quantum chaos*, Random walks and geometry, 109–140, Walter de Gruyter GmbH & Co. KG, Berlin, 2004. MR2087781 (2005k:81087)

[GHSSV] A. Gamburd, S. Hoory, M. Shahshahani. A. Shalev and B. Virg, *On the girth of random Cayley graphs*, Random Structures Algorithms 35 (2009), no. 1, 100–117. MR2532876 (2010i:05310)

[GJS] A. Gamburd, D. Jakobson and P. Sarnak, *Spectra of elements in the group ring of* SU(2), J. Eur. Math. Soc. (JEMS) 1 (1999), no. 1, 51–85. MR1677685 (2000e:11102)

[GH] N. Gill and H.A. Helfgott, *Growth of small generating sets in* $\mathrm{SL}_n(Z/pZ)$, arXiv:1002.1605

[Gl] G. Glauberman, *Factorizations in local subgroups of finite groups*, Regional Conference Series in Mathematics, No. 33. American Mathematical Society, Providence, RI, 1977. ix+74 pp. MR0470072 (57:9839)

[Go] W.T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. 17 (2008), no. 3, 363–387. MR2410393 (2009f:20105)

[GLMWY] R.L. Graham, J.C. Lagarias, C.L. Mallows, L. Colin, A.R. Wilks and C.H. Yan, *Apollonian circle packings: number theory*, J. Number Theory 100 (2003), no. 1, 1–45. MR1971245 (2004d:11055)

[Gr] B. Green, *Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak*, arXiv:0911.3354

[GT1] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) 167 (2008), no. 2, 481–547. MR2415379 (2009e:11181)

[GT2] B. Green and T. Tao, *Linear equations in primes*, Ann. of Math. (2) 171 (2010), no. 3, 1753–1850. MR2680398 (2011j:11177)

[GTZ] B. Green, T. Tao and T. Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$-norm*. arXiv:1009.3998

[Gro1] M. Gromov, *Random walk in random groups*, Geom. Funct. Anal. 13 (2003), no. 1, 73–146. MR1978492 (2004j:20088a)

[Gro2] M. Gromov, *Singularities, expanders and topology of maps. I. Homology versus volume in the spaces of cycles*, Geom. Funct. Anal. 19 (2009), no. 3, 743–841. MR2563769

[Gro3] M. Gromov, *Singularities, expanders and topology of maps. II. From combinatorics to topology via algebraic isoperimetry*, Geom. Funct. Anal. 20 (2010), 416–526. MR2671284

[GrGu] M. Gromov and L. Guth, *Generalizations of the Kolmogorov-Barzdin embedding estimates*, arXiv:1103.3423

[GL] F. Grunewald and A. Lubotzky, *Linear representations of the automorphism group of a free group*, Geom. Funct. Anal. 18 (2009), no. 5, 1564–1608. MR2481737 (2010i:20039)

[HL] G.H. Hardy and J.E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. 44 (1923), no. 1, 1–70. MR1555183

[H1] H.A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) 167 (2008), no. 2, 601–623. MR2415382 (2009i:20094)

[H2] H.A. Helfgott, *Growth in* $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, J. Eur. Math. Soc. 13 (2011), 761–851. MR2781932

[HLS] N. Higson, V. Lafforgue and G. Skandalis, *Counterexamples to the Baum-Connes conjecture*, Geom. Funct. Anal. 12 (2002), no. 2, 330–354. MR1911663 (2003g:19007)

[HLW] S. Hoory, N. Linial and A. Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. (N.S.) 43 (2006), no. 4, 439–561. MR2247919 (2007h:68055)

[HKLS] E. Hrushovski, P.H. Kropholler, A. Lubotzky and A. Shalev, *Powers in finitely generated groups*, Trans. Amer. Math. Soc. 348 (1996), no. 1, 291–304. MR1316851 (96f:20061)

[IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004. xii+615 pp. MR2061214 (2005h:11005)

[JKZ] F. Jouve, E. Kowalski and D. Zywina, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, Israel J. of Math., to appear. arXiv:1008.3662

[KL] W.M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata 36 (1990), no. 1, 67–87. MR1065213 (91j:20041)

[KLS] W. M. Kantor, A. Lubotzky and A. Shalev, *Invariable generation and the Chebotarev invariant of a finite group*, J. of Algebra, 348 (2011) 302–314.

[KMSS1] I. Kapovich, A. Miasnikov, P. Schupp and V. Shpilrain, *Generic-case complexity, decision problems in group theory, and random walks*, J. Algebra 264 (2003), no. 2, 665–694. MR1981427 (2005m:20080)

[KMSS2] I. Kapovich, A. Miasnikov, P. Schupp and V. Shpilrain, *Average-case complexity and decision problems in group theory*, Adv. Math. 190 (2005), no. 2, 343–359. MR2102661 (2005i:20053)

[KS1] I. Kapovich and P. Schupp, *On group-theoretic models of randomness and genericity*, Groups Geom. Dyn. 2 (2008), no. 3, 383–404. MR2415305 (2009k:20102)

[K1] M. Kassabov, *Universal lattices and unbounded rank expanders*, Invent. Math. 170 (2007), no. 2, 297–326. MR2342638 (2009b:20079)

[K2] M. Kassabov, *Symmetric groups and expander graphs*, Invent. Math. 170 (2007), no. 2, 327–354. MR2342639 (2008g:20009)

[KLN] M. Kassabov, A. Lubotzky and N. Nikolov, *Finite simple groups as expanders*, Proc. Natl. Acad. Sci. USA 103 (2006), no. 16, 6116–6119. MR2221038 (2007d:20025)

[KN] M. Kassabov and N. Nikolov, *Universal lattices and property tau*, Invent. Math. 165 (2006), no. 1, 209–224. MR2221141 (2007c:19002)

[KaL] T. Kaufman and A. Lubotzky, *Edge transitive Ramanujan graphs and highly symmetric LDPC good codes*, arXiv:1108.2960.

[KaW] T. Kaufman and A. Wigderson, *Symmetric LDPC and local Testing*, Innovations in Computer Science, 406–421, 2010.

[Ka] D.A. Kazhdan, *On the connection of the dual space of a group with the structure of its closed subgroups*, (Russian) Funkcional. Anal. i Priložen. 1 (1967), 71–74. MR0209390 (35:288)

[Ki] H.H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2, with appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak. J. Amer. Math. Soc. 16 (2003), no. 1, 139–183. MR1937203 (2003k:11083)

[KB] A. N. Kolmogorov and Y.M. Barzdin, *On the realization of nets in* 3*-dimensional space*, Probl. Cybernet, 8, 261–268, 1967. See also Selected Works of A.N. Kolmogorov, Vol. 3, pp. 194–202 (and a remark on page 245), Kluwer Academic Publishers, 1993. MR1228446 (94c:01040)

[KO1] A. Kontorovich and H. Oh, *Apollonian circle packings and closed horospheres on hyperbolic* 3*-manifolds*, J. Amer. Math. Soc. 24 (2011), 603–648. arXiv:0811.2236 MR2784325

[KO2] A. Kontorovich and H. Oh, *Almost prime Pythagorean triples in thin orbits*, arXiv:1001.0370

[Ko1] E. Kowalski, *The large sieve and its applications*, Arithmetic geometry, random walks and discrete groups. Cambridge Tracts in Mathematics, 175. Cambridge University Press, Cambridge, 2008. xxii+293 pp. MR2426239 (2009f:11123)

[Ko2] E. Kowalski, *Sieve in expansion*, Seminar Bourbaki Exp. no. 1028, November 2010. arXiv:1012:2793v1 MR2643980

[La1] M. Lackenby, *Expanders, rank and graphs of groups*, Israel J. Math. 146 (2005), 357–370. MR2151608 (2006c:20068)

[La2] M. Lackenby, *A characterisation of large finitely presented groups*, J. Algebra 287 (2005), no. 2, 458–473. MR2134155 (2006a:20048)

[La3] M. Lackenby, *Heegaard splittings, the virtually Haken conjecture and property* (τ), Invent. Math. 164 (2006), no. 2, 317–359. MR2218779 (2007c:57030)

[La4] M. Lackenby, *Large groups, property* (τ) *and the homology growth of subgroups*, Math. Proc. Cambridge Philos. Soc. 146 (2009), no. 3, 625–648. MR2496348 (2010g:20091)

[LaLR1] M. Lackenby, D.D. Long and A.W. Reid, *LERF and the Lubotzky-Sarnak conjecture*, Geom. Topol. 12 (2008), no. 4, 2047–2056. MR2431015 (2009j:57017)

[LaLR2] M. Lackenby, D.D. Long and A.W. Reid, *Covering spaces of arithmetic* 3*-orbifolds*, Int. Math. Res. Not. IMRN 2008, no. 12, Art. ID rnn036, 38 pp. MR2426753 (2009c:57031)

[Le] G. Levitt, *On the cost of generating an equivalence relation*, Ergodic Theory Dynam. Systems, 15(6) (1995), 1173–1181. MR1366313 (96i:58091)

[LiSh] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata 56 (1995), no. 1, 103–113. MR1338320 (96h:20116)

[Lit] T. Li, *Rank and genus of* 3*-manifolds*. arXiv:1106.6302v1

[Li] N. Linial, *Finite metric-spaces: combinatorics, geometry and algorithms*, Proceedings of the International Congress of Mathematicians, Vol. III (Beijing, 2002), 573–586, Higher Ed. Press, Beijing, 2002. MR1957562 (2003k:05045)

[LLR] D.D. Long, A. Lubotzky and A.W. Reid, *Heegaard genus and property* τ *for hyperbolic* 3*-manifolds*, J. Topol. 1 (2008), no. 1, 152–158. MR2365655 (2008j:57036)

[Lo] E. Looijenga, *Prym representations of mapping class groups*, Geom. Dedicata 64 (1997), no. 1, 69–83. MR1432535 (98m:57002)

[L1] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, with an appendix by Jonathan D. Rogawski. Reprint of the 1994 edition. Modern Birkhäuser Classics. Birkhäuser Verlag, Basel, 2010. iii+192 pp. MR2569682 (2010i:22011)

[L2] 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. MR1358635 (96k:05081)

[L3] A. Lubotzky, *Eigenvalues of the Laplacian, the first Betti number and the congruence subgroup problem*, Ann. of Math. (2) 144 (1996), no. 2, 441–452. MR1418904 (98h:22013)

[L4] A. Lubotzky, *Free quotients and the first Betti number of some hyperbolic manifolds*, Transform. Groups 1 (1996), no. 1-2, 71–82. MR1390750 (97d:57016)

[L5] A. Lubotzky, *What is... property* (τ), Notices Amer. Math. Soc. 52 (2005), no. 6, 626–627. MR2147485

[L6] A. Lubotzky, *Finite simple groups of Lie type as expanders*, J. Eur. Math. Soc. 13 (2011), 1331–1341.

[LM1] A. Lubotzky and C. Meiri, *Sieve methods in group theory: I. powers in linear groups*. Geom. Dedicata, to appear.arXiv:1107.3666

[LM2] A. Lubotzky and C. Meiri, *Sieve methods in group theory: II. The mapping class group*. arXiv:1104:2450

[LM3] A. Lubotzky and C. Meiri, *Sieve methods in group theory: III.* $Aut(F_n)$. arXiv:1104:2450

[LP] A. Lubotzky and I. Pak, *The product replacement algorithm and Kazhdan's property* (T), J. Amer. Math. Soc. 14 (2001), no. 2, 347–363. MR1815215 (2003d:60012)

[LPS1] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan conjecture and explicit construction of expanders*, Proc. STOC. 86 (1986), 240–246.

[LPS2] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica 8 (1988), no. 3, 261–277. MR963118 (89m:05099)

[LPS3] A. Lubotzky, R. Phillips and P. Sarnak, *Hecke operators and distributing points on the sphere. I*, Frontiers of the mathematical sciences: 1985 (New York, 1985). Comm. Pure Appl. Math. 39 (1986), no. S, suppl., 149–186. MR861487 (88m:11025a)

[LPS4] A. Lubotzky, R. Phillips and P. Sarnak, *Hecke operators and distributing points on* S^2*. II*, Comm. Pure Appl. Math. 40 (1987), no. 4, 401–420. MR890171 (88m:11025b)

[LR] A. Lubotzky and L. Rosenzweig, *The galois groups of random elements of linear groups*, in preparation.

[LSV1] A. Lubotzky, B. Samuels and U. Vishne, *Ramanujan complexes of type* $\tilde{A}_d$, Probability in Mathematics. Israel J. Math. 149 (2005), 267–299. MR2191217 (2006i:11134)

[LSV2] A. Lubotzky, B. Samuels and U. Vishne, *Explicit constructions of Ramanujan complexes of type* $\tilde{A}_d$, European J. Combin. 26 (2005), no. 6, 965–993. MR2143204 (2006g:20043)

[LS] A. Lubotzky and D. Segal, *Subgroup growth*, Progress in Mathematics, 212. Birkhäuser Verlag, Basel, 2003. xxii+453 pp. MR1978431 (2004k:20055)

[LSh] A. Lubotzky and Y. Shalom, *Finite representations in the unitary dual and Ramanujan groups*, Discrete geometric analysis, 173–189, Contemp. Math., 347, Amer. Math. Soc., Providence, RI, 2004. MR2077037 (2005e:22011)

[LW] A. Lubotzky and B. Weiss, *Groups and expanders*, Expanding graphs (Princeton, NJ, 1992), 95–109, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 10, Amer. Math. Soc., Providence, RI, 1993. MR1235570 (95b:05097)

[LZ] A. Lubotzky and E. Zelmanov, *Dimension expanders*, J. Algebra 319 (2008), no. 2, 730–738. MR2381805 (2008k:05098)

[LZi] A. Lubotzky and R.J. Zimmer, *Variants of Kazhdan's property for subgroups of semisimple groups*, Israel J. Math. 66 (1989), no. 1-3, 289–299. MR1017168 (90i:22020)

[LZu] A. Lubtozky and A. Zuk, *On property* (τ), monograph in preparation.

[Ma1] J. Maher, *Random walks on the mapping class group*, Duke Math. J. 156 (2011), 429–468. MR2772067

[Ma2] J. Maher, *Random Heegaard splittings*, J. Topology 3 (2010), 997–1025. MR2746344

[MS] J. Malestein and J. Souto, *On genericity of pseudo-Anosovs in the Torelli group*, arXiv:1102.0601

[M1] G.A. Margulis, *Explicit constructions of expanders*. (Russian) Problemy Peredači Informacii 9 (1973), no. 4, 71–80. English translation: Problems of Information Transmission 9 (1973), no. 4, 325–332 (1975). MR0484767 (58:4643)

[M2] G.A. Margulis, *Explicit constructions of graphs without short cycles and low density codes*, Combinatorica 2 (1982), no. 1, 71–78. MR671147 (83j:05053)

[M3] G.A. Margulis, *Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators*, Problems of Information Transmission, 24(1):39–46, 1988. MR939574 (89f:68054)

[MVW] C.R. Matthews, L.N. Vaserstein and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. (3) 48 (1984), no. 3, 514–532. MR735226 (85d:20040)

[Maz] B. Mazur, *It is a story*, A lecture given at Diaconis' 60th birthday. Available at http://www.math.ucsd.edu/ williams/diaconis/It.is.a.story.3.pdf

[MW] R. Meshulam and A. Wigderson, *Expanders in group algebras*, Combinatorica 24 (2004), no. 4, 659–680. MR2096820 (2005m:05114)

[Mo] M. Morgenstern, *Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q*, J. Combin. Theory Ser. B 62 (1994), 44–62. MR1290630 (95h:05089)

[MR] A.G. Myasnikov and A.N. Rybalov, *Generic complexity of undecidable problems*, J. Symbolic Logic 73 (2008), no. 2, 656–673. MR2414470 (2009g:03068)

[NS] A. Nevo and P. Sarnak, *Prime and almost prime integral points on principal homogeneous spaces*, Acta Math. 205 (2010), 361–402. MR2746350

[Ni] N. Nikolov, *A product of decomposition for the classical quasisimple groups*, J. Group Theory 10 (2007), no. 1, 43–53. MR2288458 (2007m:20073)

[NiPy] N. Nikolov and L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem*, arXiv:math/0703343

[No] M.V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. 88 (1987), no. 2, 257–275. MR880952 (88d:20068)

[Pi] R. Pink, *Strong approximation for Zariski dense subgroups over arbitrary global fields*, Comment. Math. Helv. 75 (2000), no. 4, 608–643. MR1789179 (2001k:20106)

[Pin] M.S. Pinsker, *On the complexity of a concentrator*, 7th International Teletraffic Conference, Stockholm, pages 318/1–318/4, June 1973.

[PS1] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type*, arXiv:1001.4556

[PS2] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type of bounded rank*, arXiv:1005.1858

[RVW] O. Reingold, S. Vadhan and A. Wigderson, *Entropy waves, the zig-zag graph product, and new constant-degree expanders*, Ann. of Math. (2) 155 (2002), no. 1, 157–187. MR1888797 (2003c:05145)

[Ri1] I. Rivin, *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. 142 (2008), no. 2, 353–379. MR2401624 (2009m:20077)

[Ri2] I. Rivin, *Zarisky density and genericity*, Int. Math. Res. Not. IMRN 19 (2010), 3649–3657. MR2725508

[RSW] E. Rozenman, A. Shalev and A. Wigderson, *Iterative construction of Cayley expander graphs*, Theory Comput. 2 (2006), 91–120. MR2322872 (2009b:05133)

[SGS] A. Salehi Golsefidy and P. Sarnak, *Affine linear sieve*, arXiv:1109.6432.

[SGV] A. Salehi Golsefidy and P. Varju, *Expansion in perfect groups*, arXiv:1108.4900.

[S1] P. Sarnak, *Some applications of modular forms*, Cambridge Tracts in Mathematics, 99. Cambridge University Press, Cambridge, 1990. x+111 pp. MR1102679 (92k:11045)

[S2] P. Sarnak, *Selberg's eigenvalue conjecture*, Notices Amer. Math. Soc. 42 (1995), no. 11, 1272–1277. MR1355461 (97c:11059)

[S3] P. Sarnak, *What is ... an expander?* Notices Amer. Math. Soc. 51 (2004), no. 7, 762–763. MR2072849

[S4] P. Sarnak, *Equidistribution and primes*, Géométrie differentielle, physique mathématiques, mathématiques et société. II. Astérisque No. 322 (2008), 225–240. MR2521658 (2010k:11146)

[S5] P. Sarnak, *Letter to Lagarias on integral Apollonian packings.* Available at http://www.math.princeton.edu/sarnak/

[S6] P. Sarnak, *Equidistribution and Primes*, (2007) PIMS Lecture. Available at http://www.math.princeton.edu/sarnak/

[S7] P. Sarnak, *Primes and orbits*, MAA Garden State lecture. Available at http://www.math.princeton.edu/sarnak/

[S8] P. Sarnak, *Integral Apollonian Packings* - MAA Lecture January 2009. Available at http://www.math.princeton

[SS] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, (French) Acta Arith. 4 (1958), 185–208; erratum 5 (1958) 259. MR0106202 (21:4936)

[SiSp] M. Sipser and D.A. Spielman, *Expander codes*, IEEE Trans. Inform. Theory 42 (1996), 1710–1722. MR1465731 (98d:94031)

[Sel] A. Selberg, *On the estimation of Fourier coefficients of modular forms*, 1965 Proc. Sympos. Pure Math., Vol. VIII, pp. 1–15, Amer. Math. Soc., Providence, RI MR0182610 (32:93)

[Se] J-P. Serre, *Le problème des groupes de congruence pour* SL_2, (French) Ann. of Math. (2) 92 (1970) 489–527. MR0272790 (42:7671)

[Sh1] Y. Shalom, *Expanding graphs and invariant means*, Combinatorica 17 (1997), no. 4, 555–575. MR1645694 (99h:05057)

[Sh2] Y. Shalom, *Expander graphs and amenable quotients*, Emerging applications of number theory (Minneapolis, MN, 1996), 571–581, IMA Vol. Math. Appl., 109, Springer, New York, 1999. MR1691549 (2000h:20059)

[Sh3] Y. Shalom, *Bounded generation and Kazhdan's property* (T), Inst. Hautes Études Sci. Publ. Math. No. 90 (1999), 145–168 (2001). MR1813225 (2001m:22030)

[Sh4] Y. Shalom, *The algebraization of Kazhdan's property* (T), International Congress of Mathematicians. Vol. II, 1283–1310, Eur. Math. Soc., Zurich, 2006. MR2275645 (2008a:22003)

[Ta] R. M. Tanner, *A recursive approach to low complexity codes*, IEEE Transactions on Information Theory 27 (1981), 533–547. MR650686 (83i:94017)

[TV] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006. xviii+512 pp. MR2289012 (2008a:11002)

[Ti] J. Tits, *Free subgroups in linear groups*, J. Algebra 20 (1972) 250–270. MR0286898 (44:4105)

[Va1] A. Valette, *An application of Ramanujan graphs to C -algebra tensor products*, 15th British Combinatorial Conference (Stirling, 1995). Discrete Math. 167/168 (1997), 597–603. MR1446777 (98d:46066)

[Va2] A. Valette, *Graphes de Ramanujan et applications*, (French) *Ramanujan graphs and applications*, Séminaire Bourbaki, Vol. 1996/97. Astérisque No. 245 (1997), Exp. No. 829, 4, 247–276. MR1627114 (99k:11079)

[Va3] A. Valette, *Introduction to the Baum-Connes conjecture*, Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 2002. MR1907596 (2003f:58047)

[V] P.O. Varju, *Expansion in* $\mathrm{SL}_d(O_K/I)$*, I square-free*, arXiv:1001.3664.

[W] B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Ann. of Math. (2) 120 (1984), no. 2, 271–315. MR763908 (86m:20053)

[Z1] P. Zograf, *Small eigenvalues of automorphic Laplacians in spaces of cusp forms*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 134 (1994), 157–168; translation in J. Math. Sciences 36, No. 1, 106–114. MR741858 (86a:58116)

[Z2] P. Zograf, *A spectral proof of Rademacher's conjecture for congruence subgroups of the modular group*, J. Reine Angew. Math. 414 (1991), 113–116. MR1092625 (92d:11041)

[Z] A. Zuk, *Property (T) and Kazhdan constants for discrete groups*, Geom. Funct. Anal. 13 (2003), no. 3, 643–670. MR1995802 (2004m:20079)

Einstein Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel
E-mail address: alexlub@math.huji.ac.il