AFFINE SIEVE AND EXPANDERS.

ALIREZA SALEHI GOLSEFIDY

Abstract. This note is based on my talk in the hot topics workshop at MSRI. My goals are to
(1) Describe affine sieve: its most general setting and the fundamental theorem in the subject.
(2) Convey the main ideas behind the proof of the fundamental theorem of affine sieve and its connection with expansion in linear groups.
(3) Give a survey of some of the results on the expansion in linear groups and briefly explain what goes into their proofs.
(4) Finish with some remarks, questions and conjectures.

1. Affine sieve

1.1. **What is affine sieve?** Lots of problems and theorems in number theory concern about the existence of *infinitely many* primes in a subset of integers.

(1) Dirichlet's theorem: *for any integers $a \neq 0$ and b, there are infinitely many integers x such that $ax+b$ is prime if there are no local obstructions, i.e.* $\gcd(a,b)=1$.
Instead of restricting ourselves to coprime pairs, we can work with $\mathbb{Z}[\frac{1}{\gcd(a,b)}]$ and say for any integers $a \neq 0$ and b there are infinitely many integers x such that $ax+b$ is prime in $\mathbb{Z}[\frac{1}{\gcd(a,b)}]$.

(2) Twin prime conjecture: *there are infinitely many positive integers x such that $x(x+2)$ has at most two prime factors.*
This is a well-known long standing open problem. If we relax it and ask for infinitely many *almost primes* instead, then we have an affirmative result. Brun developed a combinatorial sieve and in particular proved that there are infinitely many x such that $x(x+2)$ has at most 20 prime factors. Later more sophisticated sieve methods were developed. As a result Chen proved that there are infinitely many x such that $x(x+2)$ has at most *three* prime factors.
As we see in this example, in many problems, sieve methods can help us to see what should be expected and prove the existence of infinitely many *almost primes* instead of primes. [HR74]

(3) Mersenne prime conjecture: *there are infinitely many positive integers x such that 2^x-1 is prime.*
This set is too sparse and so sieve methods do not give us anything. In fact, here it is even open to prove that there are integers r and infinitely many positive integers x such that 2^x-1 has at most r prime factors.

In all of the mentioned examples, we are dealing with a one-parameter subset of integers. One can ask what happens in a multi-parameter setting. What should be the "right" question in this setting? In some sense it is not a good idea to just ask about existence of infinitely many desired values as one can just restrict to a one-parameter subset for that purpose. Bourgain, Gamburd and Sarnak [BGS09] nicely

Date: 1/25/2013.
1991 *Mathematics Subject Classification.* 22E40.
A. S-G. was partially supported by the NSF grant DMS-1160472 and Alfred P. Sloan Research Fellowship.

suggest to replace "infiniteness" with "Zariski-density"[1]. They also give the following reformulation of Hardy-Littlewood conjecture, which further convinces us that Zariski-density should be the right notion to seek in a multi-parameter setting.

Hardy-Littlewood conjecture: *let Λ be a subgroup of $\mathbb{Z}^n$ and $\vec{b}=(b_1,\dots,b_n)\in\mathbb{Z}^n$. Let*

$$\Lambda_{\vec{b}}:=\{\vec{\lambda}=(\lambda_1,\dots,\lambda_n)\in\Lambda|\ \prod_{i=1}^{n}(\lambda_i+b_i)\ \textit{has at most } n \textit{ prime factors.}\}.$$

Then the Zariski-closure $\overline{\Lambda_{\vec{b}}}$ of $\Lambda_{\vec{b}}$ is equal to the Zariski-closure $\overline{\Lambda}$ of Λ if there are no local obstructions, i.e. for any square-free integer q there is $\vec{\lambda}\in\Lambda$ such that $\gcd(f_{\vec{b}}(\vec{\lambda}),q)=1$, where $f_{\vec{b}}(\vec{\lambda})=\prod_{i=1}^{n}(\lambda_i+b_i)$.[2]

In the above formulation, we are looking at the action of $\mathbb{G}_a^n$ on $\mathbb{A}^n$ and investigating points in Λ where the value of $f_{\vec{b}}\in\mathbb{Q}[\mathbb{A}^n]$ has at most n prime factors. This point of view, makes us wonder what one should expect for an arbitrary algebraic $\mathbb{Q}$-group $\mathbb{G}$, equipped with an algebraic action on a $\mathbb{Q}$-variety $\mathbb{V}$ and a regular function f on $\mathbb{V}$. [3]

General setting of affine sieve, I: *let $\Gamma\Gamma\subseteq\mathbb{G}(\mathbb{Q})$ be a Zariski-dense subgroup of $\mathbb{G}$ where $\mathbb{G}$ is a linear algebraic group defined over $\mathbb{Q}$. Assume that $\mathbb{G}$ acts on a $\mathbb{Q}$-variety $\mathbb{V}$ and that the action is also defined over $\mathbb{Q}$. Let f be a regular function on $\mathbb{V}$ which is defined over $\mathbb{Q}$ and $x_0\in\mathbb{V}(\mathbb{Q})$. Under what conditions can we find a positive integer r and a finite set of primes S such that*

$$\{\gamma\in\Gamma|\ f(\gamma\cdot x_0)\ \textit{has at most } r \textit{ prime factors in } \mathbb{Z}_S\}$$

is Zariski-dense in $\mathbb{G}$?

Since the action is algebraic, $f\in\mathbb{Q}[\mathbb{V}]$ and $x_0\in\mathbb{V}(\mathbb{Q})$, we have that $f(g\cdot x_0)$ defines a regular function on $\mathbb{G}$ which is also defined over $\mathbb{Q}$. So without loss of generality, we can directly work with $\mathbb{G}$ and avoid introducing $\mathbb{V}$.

General setting of affine sieve, II: *let $\Gamma\subseteq\mathrm{GL}_n(\mathbb{Q})$ and $\mathbb{G}$ be its Zariski-closure. Let $f\in\mathbb{Q}[\mathbb{GL}_n]$. For a positive integer r and a finite set of primes S, let*

$$\Gamma_{r,S}(f):=\{\gamma\in\Gamma|\ f(\gamma)\ \textit{has at most } r \textit{ prime factors in } \mathbb{Z}_S\}.$$

Under what conditions can we find r and S such that $\Gamma_{r,S}(f)$ is Zariski-dense in $\mathbb{G}$?

Our goal here is to describe a general frame work. In a given problem, not only it is important to show the existence of r and S, but also to find the best possible r and the right conditions on f and Γ which guarantee that S is empty. (S will be called the set of ramified primes.) It should be added that this general setting was formulated in [BGS09] (slightly different notations are used in [BGS09] and the best possible r is called the saturation number.)

Before formulating and justifying the needed conditions, let us quickly reformulate the mentioned results and problems in terms of the above setting.

(1) Brun's fundamental theorem of sieves: let $\Gamma=\mathbb{Z}\subseteq\mathbb{G}_a(\mathbb{Q})$ and $f(x)\in\mathbb{Z}[x]$. Then $\Gamma_{r,\varnothing}(f)$ is Zariski-dense in $\mathbb{G}_a$ for some positive integer r.

[1] Of course, a subset of the affine line $\mathbb{A}^1$ is Zariski-dense if and only if it is infinite.

[2] It is worth mentioning that, if $\mathrm{rank}(\Lambda)$ is at least two, then this conjecture is proved as a result of works of Green and Tao [GT10, GT12] and Green, Tao and Ziegler [GTZ12].

[3] We work with rational numbers instead of integers for simplicity. As a result we end up working with S-integers instead of integers. And similar to the above formulation of Dirichlet's theorem, we can avoid local obstructions.

(2) Dirichlet's theorem: let $\Gamma = \mathbb{Z} \subseteq \mathbb{G}_a(\mathbb{Q})$ and $0 \neq a, b \in \mathbb{Z}$. Let S be the set of prime factors of $\gcd(a, b)$. Then $\Gamma_{1,S}(ax + b)$ is Zariski-dense in $\mathbb{G}_a$.

(3) Twin prime conjecture: let $\Gamma = \mathbb{Z} \subseteq \mathbb{G}_a(\mathbb{Q})$ and $f(x) = x(x + 2)$. Then $\Gamma_{2,\varnothing}(f)$ should be Zariski-dense in $\mathbb{G}_a$. And Chen proved $\Gamma_{3,\varnothing}(f)$ is Zariski-dense in $\mathbb{G}_a$.

(4) Mersenne prime conjecture: let $\Gamma = \langle 2 \rangle \subseteq \mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^\times$ and $f(x) = x - 1$. Then $\Gamma_{1,\varnothing}(f)$ should be Zariski-dense in $\mathbb{G}_m$.

(5) Hardy-Littlewood conjecture: let $\Gamma \subseteq \mathbb{Z}^n$ and $f(\vec{x}) = \prod_{i=1}^n (x_i + b_i)$ where $b_i \in \mathbb{Z}$. Then $\Gamma_{n,\varnothing}(f)$ should be Zariski-dense in the Zariski-closure of Γ if there are no local obstructions.

(6) Bourgain-Gamburd-Sarnak's result: let $\Gamma = \langle \Omega \rangle \subseteq \mathrm{GL}_n(\mathbb{Z})$, $\mathcal{H}$ be its Zariski-closure in $(\mathcal{GL}_n)_{\mathbb{Z}}$ and $f \in \mathbb{Z}[\mathcal{H}]$. If $\mathcal{H}_{\mathbb{Q}}$ is isomorphic to $\mathbb{SL}_2$ and f is absolutely irreducible and primitive[4], then $\Gamma_{r,\varnothing}(f)$ is Zariski-dense in $\mathcal{H}$ for some positive integer r.

In fact, a much stronger result is proved in [BGS09]. In the above setting, assume that the family of Cayley graphs $\mathrm{Cay}(\pi_q(\Gamma), \pi_q(\Omega))$ form a family of expanders as q runs through square-free integers. Then if f is absolutely irreducible and primitive, then $\Gamma_{r,\varnothing}(f)$ is Zariski-dense in $\mathcal{H}$ for some positive integer r.

1.2. **What are the needed conditions? And the statement of the main result.** As we mentioned earlier, if $\Gamma = \langle 2 \rangle \subseteq \mathbb{G}_m(\mathbb{Q})$ and $f(x) = x - 1$, then we do not know whether $\Gamma_{r,S}(f)$ is Zariski-dense in $\mathbb{G}_m$ for some r and S. Sieve methods do not give us anything for this problem. In fact, heuristics [SGS, Appendix] suggest that it is not just the weakness of the method. And as Peter Sarnak says "*torus is the enemy*!" [Sar07-a]. Here we present two examples where conjecturally the answer to the general setting of affine sieve should be negative.

Isotropic torus[5]: heuristics suggest that the number of prime factors of $(2^n - 1)(2^{n-1} - 1)$ should go to infinity as n tends to infinity. This implies that if $\Gamma = \langle 2 \rangle \subseteq \mathbb{G}_m(\mathbb{Q})$ and $f(x) = (x - 1)(x - 2)$, then, for any r and S, $\Gamma_{r,S}(f)$ is not Zariski-dense in $\mathbb{G}_m$ (see [HW79, Page 15] or [SGS, Appendix] for this kind of heuristic considerations).

Anisotropic torus: let $\gamma = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Then for any integer n

$$\gamma^n = \begin{bmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{bmatrix},$$

where f_n is the n th Fibonacci number. Let $\Gamma = \langle \gamma^2 \rangle$. Note that the Zariski-closure $\mathbb{G}$ of Γ is isomorphic to the $\mathbb{Q}$-anisotropic torus $R^{(1)}_{\mathbb{Q}[\sqrt{5}]/\mathbb{Q}}(\mathbb{G}_m)$. Let $f(X_{ij}) = X_{12}$. Then conjecturally the number of prime factors of $f(\gamma^{2n})$ is going to infinity [BLMS05]. Hence again $\Gamma_{r,S}(f)$ cannot be Zariski-dense in $\mathbb{G}$ for any r and S.

In general, I believe the following question should have an affirmative answer (see [SGS, Appendix] for a heuristic consideration).

Question 1. *Let k be a Galois number field and H be a finitely generated subgroup of $k^\times$. Is there a polynomial $p_H(x) = p(x) \in k[x]$ such that for any positive integer r*

$$|\{h \in H |\ N_{k/\mathbb{Q}}(p(h)) \text{ has at most } r \text{ prime factors}\}| < \infty?$$

[4]We refer the reader to [BGS09] for the definition. This condition essentially takes care of local obstructions.

[5]Let $\mathbb{G}_m$ be the multiplicative group; so $\mathbb{G}_m(A)$ is the group of units of A for any commutative algebra A. A torus $\mathbb{T}$ defined over a field k is called k-isotropic if there is a non-trivial k-homomorphism from $\mathbb{T}$ to $\mathbb{G}_m$. It is called k-anisotropic otherwise. For instance, let l be a quadratic extension of k and let $\mathbb{T} = R^{(1)}_{l/k}(\mathbb{G}_m)$ be the kernel of the norm map. Then $\mathbb{T}$ is k-anisotropic and l-isotropic, e.g. $R^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)(\mathbb{R}) \simeq S^1$ and $R^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)(\mathbb{C}) \simeq \mathbb{C}^\times$.

If the answer to Question 1 is affirmative, then one can easily prove the following.

Proposition 2. *Assume Question 1 has an affirmative answer. Let $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Q})$, $\mathbb{G}$ be its Zariski-closure and $\mathbb{G}^\circ$ be its (Zariski) connected component of identity. If $X(\mathbb{G}^\circ) := \mathrm{Hom}(\mathbb{G}^\circ, \mathbb{G}_m)$ is non-trivial, then there is $f \in \mathbb{Q}[\mathbb{G}]$ (which is not constantly zero on a connected component of $\mathbb{G}$) such that $\Gamma_{r,S}(f)$ is not Zariski-dense in $\mathbb{G}$ for any r and S.*

The above discussion suggests that one has to assume that $X(\mathbb{G}^\circ) = \{1\}$. In [SGS], Sarnak and the author prove that this condition is sufficient.

Theorem 3 (Fundamental Theorem of Affine Sieve)**.** *Let $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Q})$, $\mathbb{G}$ be the Zariski-closure of Γ, and $f \in \mathbb{Q}[\mathbb{G}]$. If f is not constantly zero on a connected component of $\mathbb{G}$ and $X(\mathbb{G}^\circ) = \{1\}$, then $\Gamma_{r,S}(f)$ is Zariski-dense in $\mathbb{G}$ for some positive integer r and a finite set of primes S.*

It is worth mentioning that the following conditions are equivalent.

(1) $X(\mathbb{G}^\circ) = \{1\}$.
(2) No torus is a homomorphic image of $\mathbb{G}^\circ$.
(3) $X(R(\mathbb{G})) = \{1\}$ where $R(\mathbb{G})$ is the radical of $\mathbb{G}$.
(4) $\mathbb{G}/R_u(\mathbb{G})$ is semisimple where $R_u(\mathbb{G})$ is the unipotent radical of $\mathbb{G}$.
(5) $\mathbb{G} \simeq \mathbb{G}_{ss} \ltimes \mathbb{U}$, where $\mathbb{G}_{ss}$ is a semisimple group and $\mathbb{U}$ is a unipotent group.
(6) The Levi subgroup of $\mathbb{G}$ is semisimple.

A group is called *Levi-semisimple* if it satisfies the above conditions.

1.3. **Outline of the proof of Theorem 3.** From this point on, we work in the setting of Theorem 3.

Let us first remark that any unipotent group is a Levi-semisimple group. But the Cayley graphs of finite quotients of a unipotent group cannot form a family of expanders. So one cannot directly appeal to [BGS09] (see item (6) in page 3). In order to handle this difficulty, stronger results for unipotent groups and perfect groups[6] are proved.

In what follows let us also assume that $\mathbb{G}$ is Zariski-connected. So its derived subgroups $D^i(\mathbb{G})$ are also Zariski-connected. Let us recall that $D^0(\mathbb{G}) = \mathbb{G}$ and

$$D^{i+1}(\mathbb{G}) = [D^i(\mathbb{G}), D^i(\mathbb{G})].$$

Hence after $\dim \mathbb{G}$ steps, we get a perfect group $\mathbb{H} = D^{\dim \mathbb{G}}(\mathbb{G})$. We call it *the perfect core* of $\mathbb{G}$. Since $\mathbb{G}$ is Levi-semsimple, $\mathbb{G}/\mathbb{H}$ is a unipotent group $\mathbb{U}$ and we get the following diagram where each row is an exact sequence

$$\begin{array}{ccccccccc} 1 \to & & \mathbb{H} & \to & \mathbb{G} & \xrightarrow{\pi} & \mathbb{U} & \to 1 \\ & & \uparrow & & \uparrow & & \uparrow & \\ 1 \to & \mathbb{H}\cap\Gamma & \to & \Gamma & \xrightarrow{\pi} & \pi(\Gamma) & \to 1. & \end{array} \tag{1}$$

We also notice that $\Gamma_H := \Gamma \cap \mathbb{H}$ (resp. $\pi(\Gamma)$) is Zariski-dense in $\mathbb{H}$ (resp. $\mathbb{U}$). Furthermore since $\mathbb{U}$ is a unipotent $\mathbb{Q}$-group, there is a $\mathbb{Q}$-section $s : \mathbb{U} \to \mathbb{G}$ (alternatively $\mathbb{G}$ is isomorphic to $\mathbb{H} \times \mathbb{U}$ as a $\mathbb{Q}$-variety (and not as a $\mathbb{Q}$-group)). This way we view $\mathbb{G}$ as a fiber bundle over $\mathbb{U}$ and each fiber is a shifted copy of the perfect group $\mathbb{H}$.

The general idea is that in order to find "lots" of desirable points in Γ. First we find "lots" of desirable base points in $\pi(\Gamma)$ and then above each one of them in the fiber we find "lots" of desirable points. It is clear that for the above scheme to work we need to prove certain "uniformity" for the number of prime factors r and ramified primes S for the base points and the fibers.

[6] A group $\mathbb{G}$ is called perfect if $[\mathbb{G}, \mathbb{G}] = \mathbb{G}$.

Let us make these more precise. Since $\mathbb{G}$ as a $\mathbb{Q}$-variety is isomorphic to $\mathbb{H} \times \mathbb{U}$, there are $f_i \in \mathbb{Q}[\mathbb{H}]$ and $p_i \in \mathbb{Q}[\mathbb{U}]$ such that f_i are linearly independent over $\mathbb{Q}$ and $f = \sum f_i \otimes q_i$, i.e.

$$f(g) = \sum_i q_i(\pi(g)) f_i(s(\pi(g))^{-1} g),$$

for any $g \in \mathbb{G}$. Since $\mathbb{U}$ is unipotent, $\mathbb{Q}[\mathbb{U}]$ is isomorphic to the ring of polynomials in $\dim \mathbb{U}$ many variables. Let $p := \gcd q_i$ and $p_i = q_i/p$. So for any $\gamma \in \Gamma$,

$$f(\gamma) = p(\pi(\gamma)) \sum_i p_i(\pi(\gamma)) f_i(s(\pi(\gamma))^{-1}\gamma). \tag{2}$$

So if $f(\gamma)$ has few prime factors, then $p(\pi(\gamma))$ and $\gcd_i(p_i(\pi(\gamma)))$ also have few prime factors. Thus in the unipotent case, we need the following stronger result [SGS, Theorem 4].

Theorem 4. *Let Λ be a finitely generated Zariski-dense subgroup of $\mathbb{U}(\mathbb{Q})$ where $\mathbb{U}$ is a unipotent $\mathbb{Q}$-group. Let $p, p_1, \dots, p_k \in \mathbb{Q}[\mathbb{U}]$. Assume $\gcd(p_1, \dots, p_k) = 1$. Then there are a positive integer r and a finite set of primes S such that*

$$\Lambda_{r,S}(p; p_1, \dots, p_k) := \{\lambda \in \Lambda |\ p(\lambda) \text{ has at most } r \text{ prime factors in } \mathbb{Z}_S \text{ and } \gcd_i(p_i(\lambda)) = 1 \text{ in } \mathbb{Z}_S\}$$

is Zariski-dense in $\mathbb{U}$.

The main tools in the proof of Theorem 4 are Malcev theory of lattices in unipotent Lie groups [Rag72] and Brun's combinatorial sieve.

First we notice that Λ is a discrete subgroup of $\mathbb{U}(\mathbb{R})$. Then, by Malcev theorem, since Λ is discrete and Zariski-dense in $\mathbb{U}(\mathbb{R})$, it is a lattice in $\mathbb{U}(\mathbb{R})$. Thus $\log(\Lambda)$ contains a lattice of $\mathrm{Lie}(\mathbb{U})(\mathbb{Q})$. Since $\mathbb{U}$ is a unipotent group, the logarithm is a polynomial map. Hence it is enough to handle the vector group case. We handle this using Brun's combinatorial sieve and a careful induction on the dimension.

By Theorem 4, we have that $X = \pi(\Gamma)_{r,S}(p; (p_i)_i)$ is Zariski-dense in $\mathbb{U}$. We treat any $x \in X$ as a base point and look at the fiber above it. For any $x \in X$, let us also fix $\gamma_x \in \Gamma$ such that $\pi(\gamma_x) = x$. So by Equation (2), for any $\gamma_H \in \Gamma \cap \mathbb{H}$, we have

$$f(\gamma_x \gamma_H) = p(x) \sum_i p_i(x) f_i(s(x)^{-1}\gamma_x \gamma_H) = p(x) L_{\gamma_x s(x)^{-1}}(\sum_i p_i(x) f_i)(\gamma_H). \tag{3}$$

By Equation (3) and Theorem 4, one can easily prove Theorem 3 using the following [SGS, Theorem 6].

Theorem 5. *Let Γ be a finitely generated, Zariski-dense subgroup of a perfect, Zariski-connected $\mathbb{Q}$-group $\mathbb{G} \subseteq \mathbb{GL}_n$. Let S_0 be a finite set of primes and $f_1, \dots, f_m \in \mathbb{Q}[\mathbb{G}]$ be linearly independent over $\mathbb{Q}$. Then there are a positive integer r and a finite set of primes S such that $\Gamma_{r,S}(L_g(\sum_i v_i f_i))$ is Zariski-dense in $\mathbb{G}$ for any $g \in \mathbb{G} \cap \mathrm{GL}_n(\mathbb{Z}_{S_0})$ and primitive integer vector $(v_1, \dots, v_n)$.*

To prove Theorem 5, we start with a single regular function and describe how r and S depend on f and Γ. And then using our description, we uniformly control these parameters for $L_g(\sum_i v_i f_i)$.

We carefully define a set of ramified primes $S_{\Gamma,f}$ with respect to Γ and f. The set of ramified primes essentially consists of primes, where either $\pi_p(\Gamma)$ is "small" or $V(f)(\mathfrak{f}_p)$ [7] is "large" (here we are abusing the notation and $V(f)(\mathfrak{f}_p)$ denotes the set of solutions of f in $\mathbb{H}(\mathfrak{f}_p)$). Let us remark that by strong approximation [Nor89] one knows that $S_{\Gamma,f}$ is finite.

Using Bourgain-Gamburd-Sarnak sieve method, we prove the following [SGS, Theorem 5].

[7] In this article, π_q is the reduction map modulo q. And $\mathfrak{f}_q$ is the finite field of order q.

Theorem 6. *In the above setting if $\mathbb{H}$ is perfect and Zariski-connected and $f \in \mathbb{Q}[\mathbb{H}]$, then $\Gamma_{r,S_{\Gamma,f}}(f)$ is Zariski-dense for some positive integer r which depends on the spectral gap of the congruence quotients of Γ, the degree of $V(f)$ and $|S_{\Gamma,f}|$.*

It is worth mentioning that to execute Bourgain-Gamburd-Sarnak sieve method, one needs to estimate the number of elements of $V(f)(\mathfrak{f}_p)$. And this can be done using Lang-Weil [LW54] and Chebotarev density theorem (this is needed as $V(f)$ is not necessarily geometrically irreducible).

After proving Theorem 6, we can finish proof of Theorem 5 using the following (see [SGS, Proposition 29] and [SGV, Theorem 1]).

Proposition 7. *In the above setting,*

$$\bigcup_{g\in\mathbb{H}\cap\mathrm{GL}_n(\mathbb{Z}_{S_0}),\ \gcd_i v_i=1} S_{\Gamma,L_g(\sum_i v_i f_i)}$$

is finite.

Theorem 8. *Let Ω be a finite symmetric subset of $\mathrm{GL}_n(\mathbb{Z}_S)$ and $\Gamma = \langle\Omega\rangle$. Let $\mathbb{G}$ be its Zariski-closure and $\mathbb{G}^\circ$ be its Zariski-component of the identity. Then the Cayley graphs $\mathrm{Cay}(\pi_q(\Gamma), \pi_q(\Omega))$ form a family of expanders as q runs through square-free S-integers if and only if $\mathbb{G}^\circ$ is perfect.*

Theorem 8 is the main analytic tool in the proof of the fundamental theorem of affine sieve. In the next section, I explain very briefly the outline of proof of Theorem 8 and the groundbreaking results which are behind its proof.

2. Expansion properties of linear groups.

2.1. **Expanders, "thin" subgroups and triple-product: formulation and recent results.** In lots of problems in communication, one needs high connectivity and low cost. In other words, arbitrarily large highly connected sparse graphs. Such a family of finite graphs is called a family of expanders. Expanders have various interesting applications in computer science and number theory. I refer the reader to the beautiful surveys by A. Lubotzky [Lub12] and E. Kowalski [Kow]. Here I mostly discuss the recent breakthroughs related to Theorem 8.

The first explicit construction of expanders is due to Margulis. He made a remarkable observation that the Cayley graphs of finite quotients of a discrete group with property(T) form expanders. The same ideas show that using Selberg's theorem one can deduce that the Cayley graphs

$$\mathrm{Cay}\left(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}), \left\{\begin{bmatrix}1 & \pm1\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ \pm1 & 1\end{bmatrix}\right\}\right)$$

form expanders though $\mathrm{SL}_2(\mathbb{Z})$ does not have property (T) (in fact it is virtually free). As a result of works of many mathematicians (to name a few Kazhdan, Selberg, Margulis, Burger, Sarnak and Clozel) using automorphic forms and representation theory, the following is proved [Kaz67], [Mar73], [Sel65], [SX91], [BS91], [CO04], [Clo03].

Theorem 9. *Let $\mathbb{G} \subseteq \mathbb{GL}_n$ be a semisimple simply connected $\mathbb{Q}$-group. Assume $\Gamma = \mathbb{G} \cap \mathrm{GL}_n(\mathbb{Z}_S) = \langle\Omega\rangle$ is an infinite group. Then the Cayley graphs $\mathrm{Cay}(\pi_m(\Gamma), \pi_m(\Omega))$ form a family of expanders as m runs through positive integers.*

Lubotzky was the first to ask if a "thin group", i.e. a Zariski-dense subgroup of infinite index in an arithmetic lattice, has the same property. He asked if

$$\mathrm{Cay}\left(\mathrm{SL}_2(\mathfrak{f}_p), \left\{\begin{bmatrix}1 & \pm3\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ \pm3 & 1\end{bmatrix}\right\}\right)$$

form expanders or not.[8] Y. Shalom [Sha97],[Sha99] constructed the first thin group with *certain* finite quotients whose Cayley graphs form expanders (not congruence quotients). A. Gamburd [Gam02] is the first to prove Lubotzky's question for "large" thin subgroups of $\mathrm{SL}_2(\mathbb{Z})$. He proved that if the Hausdorff dimension of the limit set of a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is larger than $5/6$, then the Cayley graphs of its congruence quotients modulo primes form a family of expanders.

In 2008, Bourgain and Gamburd in a groundbreaking work [BG08-a] completely answered Lubotzky's question. They proved if $\Gamma = \langle \Omega \rangle \subseteq \mathrm{SL}_2(\mathbb{Q})$ is Zariski-dense in $\mathbb{SL}_2$, then $\mathrm{Cay}(\pi_p(\Gamma), \pi_p(\Omega))$ form expanders as p runs through large primes. The steps and the ideas of [BG08-a] also gave the general frame work of all the recent works on this area. One of the main tools in their proof is a breakthrough by Helfgott [Hel08]. Helfgott proved that if a symmetric generating set A of $\mathrm{SL}_2(\mathfrak{f}_p)$ is not very large (i.e. $|A| \leq |\mathrm{SL}_2(\mathfrak{f}_p)|^{1-\varepsilon}$), then its triple-product gets exponentially larger (i.e. $|A.A.A| \geq |A|^{1+\delta}$). Using this result coupled with Tao's non-commutative version of Balog-Szemerédi-Gowers [Tao08], Bourgain and Gamburd proved measure theoretic version of the triple-product theorem ("l^2-flattening phenomena"). (In the next section, I elaborate on this.) Then using Kesten's bound concerning the random-walk on a free group and the fact that any proper algebraic subgroup of $\mathbb{SL}_2$ is virtually solvable, they proved that the probability of being in a proper subgroup of $\mathrm{SL}_2(\mathfrak{f}_p)$ after an $l \sim \log(p)$-step random walk is small ("Escape from proper subgroups"). They finished the proof using a lower bound on the dimension of a non-trivial complex irreducible representation of $\mathrm{SL}_2(\mathfrak{f}_p)$ (this idea goes back to [SX91]).

In order to execute the affine sieve method, Bourgain, Gamburd and Sarnak [BGS09] considered square-free congruences. They proved that $\mathrm{Cay}(\pi_q(\Gamma), \pi_q(\Omega))$ form expanders as q runs through square-free integers if Γ is a Zariski-dense subgroup of $\mathrm{SL}_2(\mathbb{Z})$. They also conjectured that the if-part of Theorem 8 should hold if $\mathbb{G}$ is a semisimple group and $\Gamma \subseteq \mathbb{G} \cap \mathrm{GL}_n(\mathbb{Z})$. First they proved a sum-product theorem for $\mathbb{Z}/q\mathbb{Z}$, where q is a square-free integer. Then following Helfgott's argument they proved a triple-product theorem for $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ for a square-free integer q. They continued similar to [BG08-a]. Later P. Varjú [Var12] gave an elegant proof that if a family of finite quasi-simple groups satisfy a Helfgott-type triple-product property and some additional technical conditions, then any product of them also satisfies the triple-product property. He further showed how to use Tits's kind of argument to escape from proper subgroups when $\mathbb{G} \simeq R_{k/\mathbb{Q}}(\mathbb{SL}_n)$ (k is a number field) and $\Gamma \subseteq \mathrm{SL}_n(\mathcal{O}_k)$.

The next groundbreaking result is the generalization of Helfgott's result to any quasi-simple finite group due to independent works of Breuillard, Green and Tao [BGT11] and Pyber and Szabó [PS]. The main tools in their proofs are Helfgott's ideas (specially the ideas presented in [Hel11], where he proved that $\mathrm{SL}_3(\mathfrak{f}_p)$ has the triple-product property) and Larsen-Pink inequality [LP11].

Theorem 8 mostly relies on [BG08-a], [BGT11], [PS] and [Var12].

2.2. **Outline of proof of Theorem 8.** It is worth mentioning that for the only-if-part, it is enough to know that $\mathrm{Cay}(\pi_{q_i}(\Gamma), \pi_{q_i}(\Omega))$ form expanders for an infinite sequence of positive integers q_i. One can easily prove this using the following.

(1) $\Gamma \cap \mathbb{G}^\circ$ is a congruence subgroup of Γ. And so without loss of generality one can assume that $\mathbb{G}$ is Zariski-connected.
(2) There is a uniform upper bound for the order of the abelianization $|\pi_{q_i}(\Gamma)/[\pi_{q_i}(\Gamma), \pi_{q_i}(\Gamma)]|$ of $\pi_{q_i}(\Gamma)$.
(3) $\Gamma/[\Gamma, \Gamma]$ is a Zariski-dense finitely generated subgroup of $(\mathbb{G}/[\mathbb{G}, \mathbb{G}])(\mathbb{Q})$.
(4) π_{q_i} commutes with $\iota : \mathbb{G} \to \mathbb{G}/[\mathbb{G}, \mathbb{G}]$ when q_i has large enough prime factors.

[8] Now it is called "Lubotzky's 1-2-3 problem".

To prove the if-part , similar to all the recent works on this subject [BG08-a], [BG08-b], [BG09] and [BV12], we prove *Escape from proper subgroups* and *l^2-flattening*.

The general picture of random-walk on the Cayley graph of $\pi_q(\Gamma)$. Let us first remark that $\mathcal{G}_{q,\Omega} := \mathrm{Cay}(\pi_q(\Gamma), \pi_q(\Omega))$ form a family of expanders if and only if the random-walk on $\pi_q(\Gamma)$ with the probability law $\pi_q[\mathcal{P}_\Omega]$ gets arbitrarily close to the equidistribution in $l \sim \log q$-steps. So we essentially study this random-walk and the idea is that,

(1) if Ω is chosen carefully, then after $O(\log q)$-steps not only the probability law is not concentrated on any point but even it is not concentrated on any coset of a proper subgroup. This is called *escape from proper subgroups.*
(2) if we start with a probability law which is not concentrated on a coset of a proper subgroup, then either already the probability of being at the identity is pretty close to $1/|\pi_q(\Gamma)|$ or the probability of returning to identity gets much closer in the next step of the random-walk (we get a power-saving). This is called *l^2-flattening.*
(3) at this stage, we can appeal to [SX91] and use representation theory to say that in finitely many steps we get a flat probability law.

The precise formulation of *escape from proper subgroups* and the ideas behind its proof. First for simplicity, let us assume that Ω freely generates Γ. So $\mathrm{Cay}(\Gamma, \Omega)$ is a regular tree which is the covering space of all the finite graphs $\mathcal{G}_{q,\Omega}$. And the random-walk on $\pi_q(\Gamma)$ in $O(\log q)$-steps can be completely understood by the random-walk on the tree. This means in order to understand the behavior of the random-walk on $\pi_q(\Gamma)$ in $O(\log q)$-steps, one can focus on the behavior of the random on Γ and study "small" lifts of elements of $\pi_q(\Gamma)$ (here we view $\mathbb{Z}_S$ as a discrete subgroup of $\mathbb{R} \cdot \prod_{p\in S} \mathbb{Q}_p$ and use the S-norm).

On the other hand, notice that the weight of a proper subgroup H with respect to the normalized counting (probability) measure on $\pi_q(\Gamma)$ is equal to $[\pi_q(\Gamma) : H]^{-1}$. If we want to get arbitrarily close to this probability law in $l \sim \log q$-steps, we should be able to get $\pi_q[\mathcal{P}_\Omega^{(l)}](H) \ll [\pi_q(\Gamma) : H]^{-\delta}$ in $l = O(\log q)$-steps.

Proposition 10. *Let $\Omega \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a finite set and $\Gamma = \langle \Omega \rangle$. Assume the Zariski-closure $\mathbb{G}$ of Γ is Zariski-connected and perfect. Then there are $\delta > 0$ and a finite symmetric subset $\Omega' \subseteq \Gamma$ such that*

$$\pi_q[\mathcal{P}_{\Omega'}^{(l)}](H) \ll [\pi_q(\Gamma) : H]^{-\delta},$$

for any proper subgroup H of $\pi_q(\Gamma)$ and any even integer $l \sim \log q$.

Here $\mu^{(l)}$ is the l-fold convolution of μ with itself and for any S and q, π_q is either the quotient map from $\mathbb{Z}_S \to \mathbb{Z}_S/q\mathbb{Z}_S$ or any other similar map.

To prove Proposition 10, by the above discussion, we have to look at small lifts of elements of H. Using Nori's theorems [Nor89], we prove that small lifts of a large subgroup of H are in a proper algebraic subgroup of $\mathbb{G}$. So we have to prove that the weight of any proper algebraic subgroup of $\mathbb{G}$ in the random-walk on Γ with respect to the probability law $\mathcal{P}_{\Omega'}$ exponentially decays (for some choice of $\Omega' \subseteq \Gamma$).

In the spirit of Chevalley's theorem, we look for projective representations such that a proper algebraic subgroup fixes a point in one of them. If we had *finitely* many *irreducible* representations $\rho_i : \mathbb{G} \to \mathbb{GL}(\mathbb{V}_i)$ which satisfy the following:

(1) For any i, $\rho_i(\Gamma)$ contains *proximal* elements,
(2) Any proper connected algebraic subgroup fixes a point in $\mathbb{P}(\mathbb{V}_i)$ for some i,

then we could have used Tits's method to find "ping-pong players" which move around any projective point in all of these representations. And then finish the proof using Kesten's bounds for random-walks on a tree.

In fact, if $\Gamma \subseteq \mathbb{G} \cap \mathrm{GL}_n(\mathbb{Z})$ and $\mathbb{G}$ is semisimple, then it is relatively easy to construct such representations (using Goldsheid-Margulis [GM89]). However, if $\mathbb{G}$ is not semisimple, then the unipotent radical is in the kernel of any irreducible representation. So one needs another technique to detect proper subgroups of $\mathbb{G}$ which map onto the semisimple part of $\mathbb{G}$. Even when $\mathbb{G}$ is semisimple and we are in S-arithmetic setting, finding these representations would be still challenging (as [GM89] does not work over non-Archimedean fields).

To overcome these difficulties, we construct finitely many irreducible representations $\rho_i : \mathbb{G} \to \mathbb{GL}(\mathbb{V}_i)$ (which factor through the semisimple part of $\mathbb{G}$) and algebraic families $\{\phi_{i,w} : \mathbb{G} \to \mathrm{Aff}(\mathbb{V}_i)\}_{w \in \mathbb{W}_i}$ of affine representations defined over local fields K_i (the base parameter w changes in a vector group $\mathbb{W}_i$) such that

(1) The linear part of $\phi_{i,w}$ is ρ_i and $\mathbb{G}(K_i)$ does not fix any point in $\mathbb{V}_i(K_i)$ via $\phi_{i,w}$ for any $w \neq 0$ (the representations above 0 take care of proper subgroups which do not surject onto the semisimple part of $\mathbb{G}$).
(2) For any i, $\rho_i(\Gamma)$ is unbounded in $\mathrm{GL}(\mathbb{V}_i(K_i))$.
(3) Any proper connected algebraic subgroup $\mathbb{H}$ of $\mathbb{G}$ either
   (a) fixes a projective point in $\mathbb{P}(\mathbb{V}_i(K_i))$ via ρ_i for some i or
   (b) fixes a point v in $\mathbb{V}_i(K_i)$ via $\phi_{i,w}$ for some i and norm one vector $w \in \mathbb{W}_i(K_i)$.

We also give a somewhat new technique for constructing "ping-pong players" which does not rely on the existence of proximal elements.

We finish the proof of Proposition 10 studying random-walk in the affine spaces and proving that the probability of staying in a bounded set decays exponentially.

The precise statement of l^2-*flattening*. I have already given its formulation in item (2), page 8. Let us see the precise statement.

Proposition 11. *Let Γ and $\mathbb{G}$ be as in Proposition 10. Then for any $\varepsilon > 0$, there is $\delta > 0$ such that the following holds:*

Let μ be a probability measure on $\pi_q(\Gamma)$. Assume that

$$\|\mu\|_2 > |\pi_q(\Gamma)|^{-1/2+\varepsilon} \qquad \text{and} \qquad \mu(gH) < [\pi_q(\Gamma) : H]^{-\varepsilon},$$

for any $g \in \pi_q(\Gamma)$ and any proper subgroup $H < \pi_q(\Gamma)$. Then

$$\|\mu * \mu\|_2 < \|\mu\|_2^{1+\delta},$$

for any square-free integer q.

As I said earlier, [BG08-a] (also see [Var12]) used Tao's non-commutative version of Balog-Szemerédi-Gowers theorem to prove that, for a symmetric probability measure μ on a group, $\mu * \mu$ is not substantially flatter than μ only when $\mu * \mu$ is concentrated on an almost subgroup. So to prove Proposition 11, one has to understand almost subgroups of $\pi_q(\Gamma)$; or alternatively prove a triple-product theorem.

When $\mathbb{G}$ is semisimple, one can get such a result using works of Breuillard-Green-Tao [BGT11] or Pyber-Szabó [PS] (to get prime modulus for simple groups) and Varjú [Var12] (to extend it to square-free modulus for semisimple groups). (I refer the reader to a nice survey by B. Green [Gre10]).

To extend it to perfect groups, we prove a kind of bounded generation result and the general idea has some similarities with [ALW01].

3. Final remarks and questions.

Finding the best possible r (in [BGS09], it is called the saturation number) and S for a given Γ and f in the setting of Theorem 3 is an extremely hard task. I have already mentioned the connection of this question with twin prime and Hardy-Littlewood conjectures. In [BGS09], more interesting connections are mentioned, e.g. divisibility of area of Pythagorean triangles and integral Apollonian circle packings (ACP). And since then, there have been lots of works on integral ACP, e.g. [BF11], [KO11], [BK]. The main tool in the study of an integral ACP is its group $\mathcal{A}$ of symmetries. It is observed that $\mathcal{A}$ is a Kleinian group which is generated by a set of Möbius inversions $S = \{s_1, s_2, s_3, s_4\}$ (see [GLMWY] or [Sar07-b]). For instance, already in [Sar07-b], it is showed that in any primitive ACP there are infinitely many pairs of tangent circles with prime curvatures. In fact, much stronger result is proved. Sarnak considered the nerve $N(\mathcal{P})$ of a given ACP $\mathcal{P}$, i.e. a graph whose vertices are circles in $\mathcal{P}$ and, for $C_1, C_2 \in \mathcal{P}$, $\{C_1, C_2\}$ is an edge if and only if C_1 and C_2 are tangent. Then he considered the subgraph generated by vertices $N^P(\mathcal{P})$ with prime curvature and proved that this subgraph is a union of trees all of whose vertices are of infinite degree (in particular, there are arbitrarily large chain of circles).

Now I would like to add a bit more structure to the nerve $N(\mathcal{P})$ of $\mathcal{P}$. Let us attach 2-cells and 3-cells to $N(\mathcal{P})$ to get a contractible space and call it the simplicial complex $\mathcal{C}(\mathcal{P})$ of $\mathcal{P}$. For a given positive integer r, let $\mathcal{C}_r^P(\mathcal{P})$ be the contractible subcomplex generated by the vertices whose curvature has at most r prime factors, e.g. $\mathcal{C}_1^P(\mathcal{P}) = N^P(\mathcal{P})$. A corollary of Fuchs [Fuc10] result implies that $\mathcal{C}_{28}^P(\mathcal{P})$ has infinitely many 3-cells (her result even implies that the boundary of the nerve of the 3-cells in $\mathcal{C}_{28}^P(\mathcal{P})$ is also infinite). Conjecturally the same result should be true for $\mathcal{C}_2^P(\mathcal{P})$.

In light of the recent advancements, it seems interesting to study these complexes.

Question 12. *In the above setting:*

1. *(Sarnak* [Sar07-b]*) Study the densities and the distributions of the connected components of* $N^P(\mathcal{P})$.
2. *What can we say about the 2-cells and the 3-cells of* $\mathcal{C}_r^P(\mathcal{P})$*?*
3. *Is there any* r *such that* $\mathcal{C}_r^P(\mathcal{P})$ *contains arbitrarily large chains of 3-cells?*

For each 3-cell C in $\mathcal{C}(\mathcal{P})$, let $p(C)$ be the product of the curvatures of its vertices. For any path $w = (1 = \gamma_1, \dots, \gamma_k)$ of length k in the Cayley graph $\mathrm{Cay}(\mathcal{A}, S)$ which starts from the identity and any 3-cell C, we can consider $f_w(C) := \prod_i p(\gamma_i \cdot C)$. So f_w is a polynomial of degree $4k$ which is a product of $4k$ linear functions. Then Theorem 3 (together with the bound on r given in the proof!) says that there is a positive integer r_0 such that $\Gamma_{r_0k^2,\varnothing}(f_w)$ is Zariski-dense in Γ; in particular, there are infinitely many chains of length k in $\mathcal{C}_{r_0k^2}^P(\mathcal{P})$. The third part of Question 12 (in average) asks if $\Gamma_{r_0k,\varnothing}(f_w)$ is infinite for some w.

Question 12 can be a test to see how much we can push the affine sieve methods and get better bounds for the saturation number. When Γ is a lattice in a semisimple Lie group, using best bounds toward Ramanujan conjecture, Nevo and Sarnak [NS10] gave sharp bounds on the saturation number which are similar to the bounds known for the classical case of one variable. I believe the next place to look for such bounds is where Γ is a thin group which contains a lattice in a subgroup (similar to the group of isometries of the ACP).

The general philosophy behind Lubotzky's 1-2-3 problem is that the Zariski-topology of Γ not only dictates the congruence topology on Γ (by strong approximation, when $\mathbb{G}$ is simply connected semisimple) but also tells us about the analytical behavior of the congruence quotients. Theorem 8 says that indeed this way of thinking is completely true if $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Q})$. To be precise, if Ω_1 and Ω_2 generate two Zariski-dense subgroups of $\mathbb{G} \cap \mathrm{GL}_n(\mathbb{Z}_S)$, then either both of the families $\{\mathcal{G}_{q,\Omega_1}\}$ and $\{\mathcal{G}_{q,\Omega_2}\}$ as q runs through square-free S-integers are expanders or neither of them are. However as soon as we enlarge $\mathbb{Q}$, Zariski-topology might not detect some of the properties of Γ (see [SGV, Example 5])[9]:

[9]This shows [Lub12, Conjecture 2.25] as written is not correct.

Example 13. *There are finite subsets Ω_1 and Ω_2 of $\mathrm{GL}_n(\mathbb{Z}[i])$ such that $\{\mathcal{G}_{\mathfrak{q},\Omega_1}\}$ is a family of expanders as $\mathfrak{q}$ runs through square-free Gaussian integers and $\{\mathcal{G}_{\mathfrak{q},\Omega_2}\}$ is NOT a family of expanders as $\mathfrak{q}$ runs through square-free Gaussian integers.*

Let $\mathcal{H}$ be the Heisenberg group scheme over $\mathbb{Z}$ and $\mathcal{C}$ be its scheme-theoretic center. Then it is well-known that the symplectic group scheme $\mathrm{Sp}(\mathcal{V})$ acts on $\mathcal{H}$ (where $\dim \mathcal{V}_{\mathbb{Q}} = \dim \mathcal{H}_{\mathbb{Q}} - 1$). Let $\mathcal{L} = \mathrm{Sp}(\mathcal{V}) \ltimes \mathcal{H}$. And let Γ_1 be the group generated by $\mathcal{L}(\mathbb{Z})$ and $\mathcal{C}(\mathbb{Z}[i])$ in $\Gamma_2 = \mathcal{L}(\mathbb{Z}[i])$. Then one can show that for any generating sets Ω_1 and Ω_2 of Γ_1 and Γ_2, respectively, we have:

(1) Γ_1 and Γ_2 are both Zariski-dense in $\mathcal{L}_{\mathbb{Q}[i]}$.
(2) $\{\mathrm{Cay}(\pi_{\mathfrak{q}}(\Gamma_1), \pi_{\mathfrak{q}}(\Omega_1))\}$ is not a family of expanders as $\mathfrak{q}$ runs through square-free Gaussian integers.
(3) $\{\mathrm{Cay}(\pi_{\mathfrak{q}}(\Gamma_2), \pi_{\mathfrak{q}}(\Omega_2))\}$ is a family of expanders as $\mathfrak{q}$ runs through square-free Gaussian integers.

Though Example 13 says that in general even over a number field one should be cautious, it should be said that if the Zariski-closure is semisimple we are in good shape [SGV, Corollary 6]:

Corollary 14. *If a finite set $\Omega \subseteq \mathrm{GL}_n(\overline{\mathbb{Q}})$ generates a Zariski-dense subgroup of an adjoint form semisimple group, then $\{\mathcal{G}_{\mathfrak{q},\Omega}\}$ is a family of expanders as $\mathfrak{q}$ runs through square-free ideals of $\mathcal{O}_k(S)$ for some S, where k is the trace-field of $\langle\Omega\rangle$.*

Now one can ask if Corollary 14 is true for a linear group over $\mathbb{C}$ (or any other field) and arbitrary finite index ideals. (This is a form of [Lub12, Conjecture 2.25] (also see [SGV, Question 4]).)

Question 15. *If a finite set $\Omega \subseteq \mathrm{GL}_n(\mathbb{C})$ generates a Zariski-dense subgroup of an adjoint form semisimple group, then is $\{\mathcal{G}_{\mathfrak{a},\Omega}\}$ a family of expanders as $\mathfrak{a}$ runs through finite index ideals of the trace ring of $\langle\Omega\rangle$?*

If one just wants to relax the square-free condition, then it should be true in the generality of Theorem 8:

Conjecture 16. *If a finite subset $\Omega \subseteq \mathrm{GL}_n(\mathbb{Q})$ generates a Zariski-dense subgroup of a perfect Zariski-connected group, then $\{\mathcal{G}_{m,\Omega}\}$ is a family of expanders as m runs through all the positive integers.*

Bourgain and Varjú [BV12] proved Conjecture 16 when $\Gamma \subseteq \mathrm{SL}_n(\mathbb{Z})$ is Zariski-dense in $\mathbb{SL}_n$ (earlier a similar result for powers of primes was proved by Bourgain and Gamburd [BG08-b] and [BG09]).

Another interesting question is if the positive characteristic analogue of Theorem 8 (or its generalizations to arbitrary modulus) holds [SGV, Question 3].

Question 17. *If a finite subset $\Omega \subseteq \mathrm{GL}_n(\mathfrak{f}_l(t))$ generates a Zariski-dense subgroup of a perfect Zariski-connected group, then is $\{\mathcal{G}_{q(t),\Omega}\}$ a family of expanders as $q(t)$ runs through square-free polynomials with large degree prime factors?*

Since Nori's theorems are extensively used in [SGV] and they do not hold over $\mathfrak{f}_l(t)$, one needs new ideas to handle Question 17. An affirmative answer to Question 17 have immediate applications to arithmetic over global function fields and sieve methods in group theory in the sense of [LM12].

Acknowledgments

I am grateful to Peter Sarnak and Peter Varjú for their collaborations. I am in debt to Peter Sarnak for pointing out his description of the "prime subgraph" of the nerve of an integral ACP. I would like to thank the anonymous referee for his comments and suggestions.

References

[ALW01] N. Alon, A. Lubotzky, A. Wigderson, *Semidirect products in groups and zig-zag product in graphs: connections and applications,* 42nd IEEE symposium on foundations of computer science (Las Vegas, NV, 2001), 630–637, IEEE computer soc., Los Alamitos, CA, 2001.

[BF11] J. Bourgain, E. Fuchs. *A proof of the positive density conjecture for integer Apollonian circle packings,* JAMS **24** (2011), no 4, 945–967.

[BK] J. Bourgain, A. Kontorovich, *On the strong density conjecture for integral Apollonian circle packings,*

[BG08-a] J. Bourgain, A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathfrak{f}_p)$*,* Ann. of Math. (2) **167** (2008), no. 2, 625–642.

[BG08-b] J. Bourgain, A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$*:I,* JEMS **10** (2008) 987–1011.

[BG09] J. Bourgain, A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$*:II,* With an appendix by J. Bourgain, JEMS **11** (2009), no. 5, 1057–1103.

[BGS09] J. Bourgain, A. Gamburd, P. Sarnak, *Affine linear sieve, expanders, and sum-product,* Invent. Math. **179** (2010), no. 3, 559–644.

[BV12] J. Bourgain, P. Varjú, *Expansion in* $\mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z})$*, q arbitrary,* Invent. Math. **188** (2012), no. 1, 151–173.

[BGT11] E. Breuillard, B. Green, T. Tao, *Approximate subgroups of Linear Groups,* GAFA **21** (2011), no. 4, 774–819.

[BLMS05] Y. Bugeaud, F. Luca, M. Mignotte, S. Siksek, *On Fibonacci numbers with few prime divisors,* Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 2, 17–20.

[BS91] M. Burger, P. Sarnak, *Ramanujan duals II,* Invent. Math. **106** (1991) 1–11.

[Clo03] L. Clozel, *Démonstration de la conjecture* τ*,* Invent. Math. **151** (2003), no. 2, 297–328.

[CO04] L. Clozel, E. Ullmo, *Équidistribution des points de Hecke,* in Contributions to Automorphic Forms, Geometry and Number theory, Johns Hopkins University Press, Baltimore, MD, 2004.

[Fuc10] E. Fuchs, *Arithmetic properties of Apollonian circle packings,* Ph.D. thesis, Princeton University, Princeton, NJ.

[Gam02] A. Gamburd, *On the spectral gap for infinite index "congruence" subgroups of* $\mathrm{SL}_2(\mathbb{Z})$*,* Israel J. Math. **127** (2002) 157–200.

[GM89] I. Goldsheid, G. Margulis, *Lyapunov exponents of a product of random matrices* (Russian), Uspekhi Mat. Nauk **44** (1989), no. 5, 13–60, translation in Russian Math. Surveys **44** (1989), no. 5, 11–71.

[GLMWY] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, *Apollonian circle packings: number theory,* Journal of Number Theory **100** (2003) 1–45.

[Gre10] B. Green, *Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak,* `http://www.ams.org/meetings/lectures/currentevents2010.pdf`.

[GT10] B. Green, T. Tao, *Linear equations in primes,* Annals of Mathematics **171** (2010) 1753–1850.

[GT12] B. Green, T. Tao, *The Möbius function is strongly orthogonal to nilsequences,* Annals of Mathematics **175** (2012) 541–566.

[GTZ12] B. Green, T. Tao, T. Ziegler, *An inverse theorem for the Gowers* $Us+1[N]$*-norm,* Annals of Mathematics **176** (2012) 1231–1372.

[HR74] H. Halberstam, H. Richert, Sieve method, Academic press, New York, 1974.

[HW79] G. H. Hardy, E. M. Wright, An introduction to the theory of numbers, Oxford University Press, fifth edition, New York, 1979.

[Hel08] H. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$*,* Ann. of Math. (2) **167** (2008), no. 2, 601–623.

[Hel11] H. Helfgott, *Growth in* $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$*,* JEMS **13** (2011), no. 3, 761–851.

[Hru12] E. Hrushovski, *Stable group theory and approximate subgroups,* JAMS **25** (2012), no. 1, 189–243.

[Kaz67] D. Kazhdan, *On the connection of the dual space of a group with the structure of its closed subgroups,* Functional analysis and its applications **1** (1967) (1) 63–65.

[KO11] A. Kontorovich, H. Oh, *Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds,* JAMS **24** 2011(3) 603–648.

[Kow] E. Kowalski, *Sieve in expansion,* Preprint.

[LW54] S. Lang, A. Weil, *Number of points of varieties in finite fields,* Amer. J. Math. **76** (1954) 819–827.

[LP11] M. Larsen, R. Pink, *Finite subgroups of algebraic groups,* JAMS **24** (2011) 1105–1158.

[Lub12] A. Lubotzky, *Expander graphs in pure and applied mathematics,* Bull. Amer. Math. Soc. **49** (2012) 113–162.

[LM12] A. Lubotzky, C. Meiri, *Sieve methods in group theory I: Powers in linear groups,* JAMS **25** (2012) 1119–1148.

[Mar73] G. Margulis, *Explicit construction of concentrators,* Problemy Peredachi Informatsii **9** (4) (1973) 71-80. (English translation Problems of Information Transmission, Plenum, New York (1975).)

[NS10] A. Nevo, P. Sarnak, *Prime and almost prime integral points on principal homogeneous spaces,* Acta Math. **205** (2010) 361–402.

[Nor89] M. V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathfrak{f}_p)$*,* Invent. Math. **88** (1987), no. 2, 257–275.

[PS] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type of bounded rank,* Preprint.

[Rag72] M. S. Raghunathan, Discrete subgroups of semisimple Lie groups, Springer, New York, 1972.

[SGS] A. Salehi Golsefidy, P. Sarnak, *Affine sieve,* Accepted for publication in JAMS.

[SGV] A. Salehi Golsefidy, P. Varjú, *Expansion in perfect groups,* Accepted for publication in GAFA.

[Sar07-a] P. Sarnak, personal communication, 2007.
[Sar07-b] P. Sarnak, *Letter to Lagarias about integral Apollonian packings,* `http://web.math.princeton.edu/sarnak/AppolonianPackings.pdf`
[SX91] P. Sarnak, X. Xue, *Bounds for multiplicities of automorphic representations,* Duke Math. J. **64** (1991) 207–227.
[Sel65] A. Selberg, *On the estimation of Fourier coefficients of modular forms,* Proc. Symp. Pure Math. VII, AMS (1965) 1–15.
[Sha97] Y. Shalom, *Expanding graphs and invariant means,* Combinatorica **17** (1997), no. 4, 555–575.
[Sha99] 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.
[Tao08] T. Tao, *Product set estimates for non-commutative groups,* Combinatorica **28** (2008), no. 5, 547–594.
[Var12] P. Varjú, *Expansion in* $\mathrm{SL}_d(\mathcal{O}_K/I)$*, I square-free,* JEMS **14** (2012), no. 1, 273–305.
[Wei84] B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups,* Ann. of Math. (2) **120** (1984), no. 2, 271–315.

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: `golsefidy@ucsd.edu`