JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 25, Number 4, October 2012, Pages 1119–1148
S 0894-0347(2012)00736-X
Article electronically published on April 11, 2012

SIEVE METHODS IN GROUP THEORY I: POWERS IN LINEAR GROUPS

ALEXANDER LUBOTZKY AND CHEN MEIRI

1. Introduction

The sieve method is a classic one in number theory (see, for example, [FI]). Recently it found some applications in a non-commutative setting. On the one hand, Bourgain-Gamburd-Sarnak [BGS1] applied it in studying almost-prime vectors in orbits of non-commutative groups acting on $\mathbb{Z}^n$. On the other hand, Rivin [Ri] and Kowalski [Ko] used it to study generic properties of elements in the mapping class group and arithmetic groups. Our formulation of the sieve method generalizes and simplifies the second one and usually falls under the name 'Large Sieve'. The goal of this introduction is to state the general large sieve setting with respect to group theory and to serve as a guideline for the proof of Theorem A below. We start by describing the algebraic problem and its background. After that, we explain how random walks and sieve methods are used in its solution.

A *virtually nilpotent group* is a group which contains a nilpotent subgroup of finite index. Mal′cev proved:

Theorem 1.1 (Mal′cev [Mal])**.** *Let Γ be a finitely generated virtually nilpotent group. Then, for every $m \geq 1$ the set of m-powers $\Gamma^m := \{g^m \mid g \in \Gamma\}$ contains a finite index subgroup of Γ.*

The converse is not true, not even for finitely generated groups: For every prime p, Golod and Shafarevich gave an example of a finitely generated residually finite infinite group Γ such that the order of every element of Γ is a power of p (see [Go] and [GS]). In particular, if m is coprime to p, then any element of Γ is an m-power.

Yet, in [HKLS], two kinds of partial converse results were proved:

Theorem 1.2 (Hrushovski-Kropholler-Lubotzky-Shalev [HKLS])**.** *Let Γ be a virtually solvable group. If $n \geq 2$ and $\bigcup_{m=2}^{n} \Gamma^m$ contains a finite index subgroup of Γ, then Γ is virtually nilpotent. On the other hand, there exists a solvable group Γ which is not virtually nilpotent and still there exists $m \geq 2$ such that Γ^m contains a coset of a finite index subgroup.*

Theorem 1.3 (Hrushovski-Kropholler-Lubotzky-Shalev [HKLS])**.** *Let Γ be a finitely generated linear group. If $n \geq 2$ and finitely many tessellates of $\bigcup_{m=2}^{n} \Gamma^m$ cover Γ, then Γ is virtually solvable.*

The formulation of the second theorem of [HKLS] suggests a stronger result; i.e., does the fact that finitely many tessellates of the set of **all** proper powers $\bigcup_{m=2}^{\infty} \Gamma^m$

Received by the editors July 19, 2011 and, in revised form, January 20, 2012.
2010 *Mathematics Subject Classification.* Primary 20Pxx.
Key words and phrases. Sieve, property-τ, powers, linear groups, finite groups of Lie type.

cover Γ imply that Γ is virtually solvable? But the methods of [HKLS] are not suitable for handling all proper powers together. The reason is that the proof uses only local data of Γ, i.e., the images of $\bigcup_{m=2}^{n}\Gamma^m$ in finite quotients of Γ, and it is clear that the image of $\bigcup_{m=2}^{\infty}\Gamma^m$ in such a quotient is the full quotient group (take m to be coprime to the size of the finite quotient). Thus, to extend the theorem to the case of all proper powers one need to combine the local data with some global data on the group and its elements. A way to do this is to use random walks, as we shall explain below.

A finite subset Σ of Γ is called *admissible* if it is symmetric, i.e. $\Sigma=\Sigma^{-1}$, and the Cayley graph $\mathrm{Cay}(\Gamma,\Sigma)$ is not bi-partite. Let Σ be an admissible generating subset of Γ. Random walks on $\mathrm{Cay}(\Gamma,\Sigma)$ can be used to 'measure' a subset $Z\subseteq\Gamma$ by estimating the probability $\mathrm{Prob}_\Sigma(w_k\in Z)$ that the k^{th}-step of a random walk belongs to Z for larger and larger values of k. We say that Z is *exponentially small with respect to* Σ if there exist constants $c,\alpha>0$ such that $\mathrm{Prob}_\Sigma(w_k\in Z)\le ce^{-\alpha k}$ for all $k\in\mathbb{N}$. The set Z is called *exponentially small* if it is exponentially small with respect to all admissible generating subsets. It is not hard to see that if a subset is exponentially small, then finitely many tessellates of it cannot cover Γ. Thus, our first theorem is the desired extension:

Theorem A. *Let Γ be a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{C})$ which is not virtually solvable. Then the set of proper powers $\bigcup_{m=2}^{\infty}\Gamma^m$ is exponentially small in Γ.*

Despite Theorem 1.3, Theorem A is somewhat surprising: The set $\bigcup_{m=2}^{\infty}\Gamma^m$ is dense in the profinite topology of Γ (as explained above) and still it is exponentially small.

A reduction process, given in subsection 5.1, shows that it is enough to prove the claim for a finitely generated subgroup Γ of $\mathrm{GL}_n(\mathbb{Q})$ whose Zariski-closure is semisimple. In order to avoid the technical difficulties, we will focus for now on the case where Γ is a Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Z})$. Fix such a subgroup Γ and some admissible generating subset Σ. For $k\in\mathbb{N}$ only the elements of Γ which belong to the ball of radius k, $\mathcal{B}_\Sigma(k)$, can occur as the k^{th}-step of a random walk on $\mathrm{Cay}(\Gamma,\Sigma)$. As in [LMR], we use in Lemma 4.3 arguments involving matrix norms and number theory to show that if k is large enough and $g\in\mathcal{B}_\Sigma(k)$ is a proper power, then g is either virtually unipotent (i.e. some positive power of g is unipotent) or g is an m-power for some $2\le m\le k^2$ (in fact, for some $2\le m\le ck$, where c is a constant depending on Σ).

The advantage in considering random walks is now clear. By considering only proper powers which can occur at the k^{th}-step of a random walk we only have to look at virtually unipotent elements and at finitely many powers. Thus, we can divide the proof into two parts, each of which can be proven by looking at the finite quotients.

The first part is to show that the set of all virtually unipotent elements (not necessarily proper powers) is exponentially small. Proposition 2.7 shows that if $V(\mathbb{C})$ is a proper subvariety of $\mathrm{SL}_n(\mathbb{C})$ defined over $\mathbb{Q}$, then $V(\mathbb{C})\cap\Gamma$ is exponentially small. In turn, Corollary 2.8 implies that the set of virtually unipotent elements of Γ is contained in a proper subvariety of $\mathrm{SL}_n(\mathbb{C})$ defined over $\mathbb{Q}$.

The second part is to find positive constants γ and r such that for every $k\ge r$ and every $2\le m\le k^2$ we have $\mathrm{Prob}_\Sigma(w_k\in\Gamma^m)\le e^{-\gamma k}$. Indeed, if such constants

exist and α is a positive constant strictly smaller than γ, then for large enough k,

$$\mathrm{Prob}_\Sigma(w_k \in \bigcup_{2\le m\le k^2} \Gamma^m) \le k^2 e^{-\gamma k} \le e^{-\alpha k}.$$

However, for every $m \ge 1$ the set of m-powers is Zariski-dense in $\mathrm{SL}_n(\mathbb{C})$, so we cannot use the same argument as for the first part. This brings us to the large sieve method. Theorem 3.3 gives the general quantitative statement of this method while Theorem B stated below is an easy consequence which is suitable for now (see Section 2 for the definition of property-τ).

Theorem B. *Let Γ be a group generated by a finite symmetric set Σ for which $\mathrm{Cay}(\Gamma,\Sigma)$ is not bi-partite. Let $(N_j)_{j\ge2}$ be a family of normal finite index subgroups. Let $Z \subseteq \Gamma$ and assume that:*

1. *Γ has property-τ w.r.t. the family $\{N_i \cap N_j \mid i,j \ge 2\}$.*
2. *The sequence $(|\Gamma/N_j|)_{j\ge2}$ grows polynomially in j.*
3. *$|\Gamma/N_i \cap N_j| = |\Gamma/N_i||\Gamma/N_j|$ for distinct i and j.*
4. *There exists $c > 0$ such that $|ZN_j/N_j| \le (1-c)|\Gamma/N_j|$ for every $j \ge 2$.*

Then there are positive constants γ and r depending only on Σ, c and the growth of $(|\Gamma/N_j|)_{j\ge2}$ such that $\mathrm{Prob}_\Sigma(w_k \in Z) \le e^{-\gamma k}$ for every $k \ge r$. In particular, Z is exponentially small.

Returning to our case, Γ is a Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Z})$. Fix $m \ge 2$ and define Z_m to be the set of m-powers. We start by verifying the conditions of Theorem B in order to bound $\mathrm{Prob}_\Sigma(w_k \in Z_m)$. For every prime p define $M_p := \ker \pi_p$, where $\pi_p : \Gamma \to \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ is the modulo-p homomorphism. Let $\mathcal{P}$ be the set of primes. Then, Γ has property-τ w.r.t. the family $\{M_p \cap M_q \mid p,q \in \mathcal{P}\}$ by the recent result of Salehi-Golsefidy and Varju [SGV]. In fact, for our special case, the work of Varju [Va] is enough. The Strong Approximation Theorem of Weisfeiler [We] and Nori [No] implies that if p and q are distinct large enough primes, then $\pi_{pq}(\Gamma) = \mathrm{SL}_n(\mathbb{Z}/pq\mathbb{Z})$. Condition 3 is satisfied since $\mathrm{SL}_n(\mathbb{Z}/pq\mathbb{Z})$ is isomorphic to $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}) \times \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$, so $|\Gamma/M_p \cap M_q| = |\Gamma/M_p||\Gamma/M_q|$ for distinct large enough primes p and q. Condition 4 is only true for a subset of $\{M_p \mid p \in \mathcal{P}\}$. Indeed, Lemma 4.1 shows that if p is a prime which belongs to the sequence $(1+mi)_{i\ge s}$, where $s := 3\binom{n}{2}$, then $|\pi_p(Z_m)| \le \left(1 - \frac{1}{6n!}\right)|\pi_p(\Gamma)|$. Thus, if $(p_i)_{i\ge2}$ is an ascending enumeration of the large enough primes which belong to the sequence $(1+mi)_{i\ge s}$ and $N_i := \ker \pi_{p_i}$, then conditions 1,3 and 4 are satisfied (with respect to $c := \frac{1}{6n!}$). The last condition left to verify is that $(|\Gamma/N_j|)_{j\ge2}$ grows polynomially. Since $|\Gamma/N_j| \le p_j^{n^2}$ the question about the growth of $(|\Gamma/N_j|)_{j\ge2}$ translates to a question about the density of the primes in the sequence $(1+mi)_{i\ge s}$. We use a quantitative version of Dirichlet's Theorem about primes in arithmetic progression (see Theorem 3.4 and Corollary 3.5 below) to estimate this density and to show that $(|\Gamma/N_j|)_{j\ge2}$ grows polynomially. Thus all the conditions of Theorem B hold and there are positive constants γ and r for which $\mathrm{Prob}_\Sigma(w_k \in Z_m) \le e^{-\gamma k}$ for every $k \ge r$. In fact, a more detailed study of the growth of $(|\Gamma/N_i|)_{i\ge2}$ shows that the γ and r are independent of m provided that $m \le k^2$. The (sketch of the) proof of the special case is now complete.

The main difficulty in the proof of the general case lies in proving the existence of the constant c needed in Theorem B. This requires a delicate analysis of the automorphism groups of almost simple groups. We dedicate Section 6 to this analysis,

which though quite technical, might be of interest on its on. A non-quantitative version of the main theorem of Section 6 (Theorem 6.16) is:

Theorem C. *Fix $d, l, r \in \mathbb{N}^+$. Then there are coprimes $a, b \in \mathbb{N}^+$ and a positive constant c such that for every prime p which belongs the arithmetic sequence $(a + bj)_{j\geq 1}$ the following claim holds:*

Let G be a finite group with a non-trivial normal subgroup H. Furthermore, assume that H is isomorphic to the direct product of at most r copies of finite simple groups of Lie type of rank l over the field $\mathbb{F}_{p^d}$ with p^d elements. Then for every coset L of H we have $|\{g^m \mid g \in L\}| \leq (1-c)|L|$.

The current paper is a first in a series of three (see [LuMe1] and [LuMe2]) in which the same sieve method is applied to obtain results on the mapping class group and on the automorphism group of a free group, respectively. It seems that Theorem B has the potential of having more applications in group theory (see also [Lu2]).

2. Random walks, expanders and unipotent elements

2.1. **Random walks.**

Definition. Let Γ be a group. A multi-subset Σ of Γ is called *symmetric* if for every $s \in \Sigma$ the number of times s occurs in Σ equals the number of times s^{-1} occurs in Σ. A finite symmetric multi-subset Σ of Γ is called *admissible* if the Cayley graph $\mathrm{Cay}(\Gamma, \Sigma)$ is not bi-partite, e.g. the identity belongs to Σ.

Fix an admissible generating multi-subset $\Sigma = [s_1, \ldots, s_{|\Sigma|}]$ of a group Γ. Since Σ is a multi-set, $\mathrm{Cay}(\Gamma, \Sigma)$ might contain self-loops and multiple edges. Let $\bar{\Sigma} \subseteq \Gamma$ consist of the elements which belong to Σ. Note that $\mathrm{Cay}(\Gamma, \Sigma)$ is connected if and only if $\bar{\Sigma}$ generates Γ and $\mathrm{Cay}(\Gamma, \Sigma)$ is not bi-partite if and only if $\bar{\Sigma}$ satisfies an odd relation, e.g. contains the identity.

A *walk on* $\mathrm{Cay}(\Gamma, \Sigma)$ is an infinite sequence of edges $(e_k)_{k\in\mathbb{N}^+}$ such that the initial vertex of e_1 is the identity and the terminal vertex of e_k is the initial vertex of e_{k+1} for every $k \in \mathbb{N}^+$. The initial vertex of e_{k+1}, denoted by w_k, is called the k^{th}-step of the walk; in particular, w_0 is the identity. The set of walks $\mathrm{W}(\Sigma)$ can be identified with $\{1, \ldots, |\Sigma|\}^{\mathbb{N}}$. Hence, the uniform probability measure of $\{1, \ldots, |\Sigma|\}$ induces a structure of a probability space on $\mathrm{W}(\Sigma)$. Once $\mathrm{W}(\Sigma)$ becomes a probability space, the term 'random walk' has a natural meaning. However, it is sometimes useful to think of a random walk on $\mathrm{Cay}(\Gamma, \Sigma)$ as constructed as follows: The random walk starts at the identity and if it arrives at a vertex v at some step, then in the next step it will use an edge which starts at v and every such edge has probability $\frac{1}{|\Sigma|}$ of being used.

For a subset Z of Γ we denote the probability that the k^{th}-step of a walk belongs to Z by $\mathrm{Prob}_\Sigma(w_k \in Z)$. Of course, for a general Z the limit $\lim_{k\to\infty} \mathrm{Prob}_\Sigma(w_k \in Z)$ might not exist and even if it does, this limit might depend on Σ. However, in many natural cases this limit exists and does not depend on Σ. For example if Z is a finite index subgroup of Γ, then always $\lim_{k\to\infty} \mathrm{Prob}_\Sigma(w_k \in Z) = [\Gamma : Z]^{-1}$.

In the sequel we will present and apply the large sieve method which helps to show that certain subsets are 'very small'. More formally, a subset $Z \subseteq \Gamma$ is called *exponentially small with respect to* Σ if there are positive constants c and α such that $\mathrm{Prob}_\Sigma(w_k \in Z) \leq ce^{-\alpha k}$ for every $k \in \mathbb{N}$. This means not only that this limit

is zero but also that there is an 'exponentially fast' convergence to this limit. A set is *exponentially small* if it is exponentially small with respect to every admissible generating multi-subset of Γ.

The reason that we chose to work with multi-sets Σ instead of the underlying set $\bar{\Sigma}$ is that when passing from the group Γ to a quotient, where the image of Z is exponentially small, we want to deduce that Z is exponentially small. However, the quotient homomorphism does not have to be injective on the generating set, so we regard its image as a multi-set.

2.2. **Property-τ.** Let us now define expanders and property-τ. A more detailed discussion about these subjects can be found in [HLW] and [Lu1]. Let X be an undirected d-regular graph, where self-loops and multiple edges are allowed. Let n be the number of vertices of X. The normalized adjacency matrix of X, denoted by A_X, is an $n \times n$ matrix whose (v,u) entry is $\frac{d_{v,u}}{d}$, where $d_{v,u}$ is the number of edges in X between vertex u and vertex v. Being real and symmetric, the matrix A_X has n real eigenvalues which we denote by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. It is not difficult to see that all the eigenvalues of A_X lie between -1 and 1. More precisely, $\lambda_1 = 1$ and if the graph is connected, then $\lambda_2 < 1$. The *spectral gap* of X is defined to be $1 - \lambda_2$. A family of graphs is called an *ε-expander* if the spectral gap of every graph in this family is at least ε. It is called an *expander* if it is an ε-expander for some $\varepsilon > 0$

The following lemma is a group-theoretic formulation of Theorem 3.2 of [HLW].

Lemma 2.1. *Let Γ be a finite group with a finite symmetric generating multi-set Σ. Let A be the normalized adjacency metrix of the Cayley graph Cay(Γ, Σ) and denote the eigenvalues of A by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Define $\alpha := \max(|\lambda_2|, |\lambda_n|)$. Then for every subset $T \subseteq \Gamma$ and every $k \in \mathbb{N}^+$ we have:*

$$\left| \mathrm{Prob}_\Sigma(w_k \in T) - \frac{|T|}{|\Gamma|} \right| \leq \sqrt{|\Gamma|}\alpha^k.$$

□

Let Γ be a finitely generated group and let $\mathcal{N}$ be a family of finite index normal subgroups of Γ. The group Γ has *property-τ* w.r.t. $\mathcal{N}$ if for some finite symmetric generating multi-set Σ and some $\varepsilon > 0$ the family of Cayley graphs $\{\mathrm{Cay}(\Gamma_N, \Sigma_N) \mid N \in \mathcal{N}\}$ is an ε-expander, where Γ_N and Σ_N are the images of Γ and Σ under the quotient homomorphism $\Gamma \to \Gamma/N$ (Σ_N is a multi-set). It is not difficult to show that if Γ has property-τ w.r.t. $\mathcal{N}$, then for every finite symmetric generating multi-set Σ there is $\varepsilon > 0$ such that the family of Cayley graphs $\{\mathrm{Cay}(\Gamma_N, \Sigma_N) \mid N \in \mathcal{N}\}$ is an ε-expander; however, ε may depend on the generating multi-set. The maximal ε for which the family $\{\mathrm{Cay}(\Gamma_N, \Sigma_N) \mid N \in \mathcal{N}\}$ is an ε-expander is called the *expansion constant of* Σ.

We want to apply Lemma 2.1 to groups with property-τ. However, we have to be a little bit cautious. The expander property bounds the second largest eigenvalue of the normalized adjacency of the above graphs, but it does not tell us anything about the absolute value of the smallest eigenvalue. Still, in our case, this can be overcome.

Lemma 2.2. *Let Σ be a symmetric generating multi-set of Γ. If $\mathrm{Cay}(\Gamma, \Sigma)$ is not bi-partite, then there is some constant $c > -1$ such that for every finite index normal subgroup N of Γ, the smallest eigenvalue of the normalized adjacency matrix*

of $\mathrm{Cay}(\Gamma_N, \Sigma_N)$ *is greater than* c*. In fact,* c *depends only on the size of* Σ *and the length of the shortest odd cycle in* $\mathrm{Cay}(\Gamma, \Sigma)$*.*

Proof. Let N be a finite index normal subgroup of Γ. Let X be the Cayley graph of Γ_N with respect to Σ_N. Let $l \in \mathbb{N}$ be the length of the shortest odd cycle in $\mathrm{Cay}(\Gamma, \Sigma)$. The entries on the diagonal of A^l are positive and equal to each other. In fact, the value of the entries is at least $\frac{1}{|\Sigma|^l}$ since it is equal to the probability that a random walk on X starting at some vertex return to this vertex at the l^{th}-step. Hence, we can write A^l as $\alpha I + B$, where $\alpha \geq \frac{1}{|\Sigma|^l}$, I is the identity matrix and B is a real symmetric matrix with non-negative entries such that the sum of the entries in every row and column is $1 - \alpha$. Thus, the smallest eigenvalue of B is at least $\alpha - 1$, which implies that the smallest eigenvalue of A^l is at least $2\alpha - 1$. In turn, the smallest eigenvalue of A is at least $(2\alpha - 1)^{\frac{1}{l}} \geq (\frac{2}{|\Sigma|^l} - 1)^{\frac{1}{l}}$, which is a real number greater than -1 since l is odd. □

It is well known that a connected k-regular graph is bi-partite if and only if the smallest eigenvalue of the normalized adjacency matrix of this graph is -1. Thus, Lemma 2.2 shows that the condition that $\mathrm{Cay}(\Gamma, \Sigma)$ is not bi-partite does not only imply that the graphs in $\{\mathrm{Cay}(\Gamma_N, \Sigma_N) \mid N \in \mathcal{N}\}$ are not bi-partite but also that they are 'uniformly far' from being bi-partite.

A straightforward corollary of Lemmas 2.1 and 2.2 is:

Corollary 2.3. *Let* Γ *be a finitely generated group with an admissible generating multi-set* Σ*. Let* $\mathcal{N}$ *be a family of finite index normal subgroups of* Γ*. Assume that the family of Cayley graphs* $\{Cay(\Gamma_N, \Sigma_N) \mid N \in \mathcal{N}\}$ *is an* ε*-expander for some* $\varepsilon > 0$*. For every* $N \in \mathcal{N}$*, let* $\pi_N : \Gamma \to \Gamma_N$ *be the quotient homomorphism. Then there exists* $\delta > 0$*, depending only on* ε*, on the size of* Σ *and on the length of the shortest odd cycle in* $\mathrm{Cay}(\Gamma, \Sigma)$*, such that for every* $k \in \mathbb{N}$*, every* $N \in \mathcal{N}$ *and every* $T \subseteq \Gamma_N$ *the following holds:*

$$\left| \mathrm{Prob}_\Sigma(\pi_N(w_k) \in T) - \frac{|T|}{|\Gamma_N|} \right| \leq \sqrt{|\Gamma_N|} e^{-\delta k}.$$

2.3. **Linear groups.** Most of the upcoming applications of property-τ will be related to linear groups. We will mainly use the following result of Salehi-Golsefidy and Varju which is built on the work of Bourgain-Gamburd [BG1], [BG2] and [BG3], Bourgain-Gamburd-Sarnak [BGS1], Varju [Va] and on the Product Theorem of Breuillard-Green-Tao [BGT] and of Pyber-Szabó [PS] who followed and generalized Helfgott [He].

Theorem 2.4 (Salehi-Golsefidy-Varju [SGV])**.** *Fix* $q_0 \in \mathbb{N}^+$ *and let* $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Z}[\frac{1}{q_0}])$ *be a finitely generated subgroup such that the connected component of its Zariski-closure in* $\mathrm{GL}_n(\mathbb{C})$ *is perfect. There exists* $q_1 \in \mathbb{N}^+$ *divisible by* q_0 *such that* Γ *has property-*τ *with respect to the family*

$$\{N_d \mid d \text{ is a square-free positive integer coprime to } q_1\},$$

where N_d *is the kernel of the homomorphism* $\pi_d : \Gamma \to GL_n(\mathbb{Z}/d\mathbb{Z})$ *induced by the residue map* $\mathbb{Z}[\frac{1}{q_0}] \to \mathbb{Z}/d\mathbb{Z}$*.*

In practice, it is very helpful to know what is the image $\pi_d(\Gamma)$. Define

$$I_\Gamma := \{f \in \mathbb{Z}[t_{i,j}]_{1 \leq i.j \leq n} \mid \forall g \in \Gamma,\ f(g) = 0\}.$$

The Zariski-closure $\mathrm{G}(\mathbb{C})$ of Γ in $\mathrm{GL}_n(\mathbb{C})$ equals $\{g \in \mathrm{GL}_n(\mathbb{C}) \mid \forall f \in I_\Gamma.\ f(g) = 0\}$. Let $d \in \mathbb{N}^+$ and define

$$\mathrm{G}(\mathbb{Z}/d\mathbb{Z}) := \{g \in \mathrm{GL}_n(\mathbb{Z}/d\mathbb{Z}) \mid \forall f \in I_\Gamma.\ \bar{f}(g) = 0\},$$

where $\bar{f}$ is the image of f under the modulo-d homomorphism. Clearly, $\pi_d(\Gamma)$ is contained in $\mathrm{G}(\mathbb{Z}/d\mathbb{Z})$. The following Strong Approximation Theorem of Weisfeiler and Nori gives us sufficient conditions for equality to hold.

Theorem 2.5 (Weisfeiler [We], Nori [No])**.** *Let $q_0 \in \mathbb{N}^+$. Let Γ be a subgroup of $\mathrm{GL}_n(\mathbb{Z}[\frac{1}{q_0}])$ such that the Zariski-closure of it $\mathrm{G}(\mathbb{C})$ is semisimple, connected and simply connected. There is a number $q_2 \in \mathbb{N}^+$ divisible by q_0 such that $\pi_d(\Gamma) = \mathrm{G}(\mathbb{Z}/d\mathbb{Z})$ for every $d \in \mathbb{N}^+$ coprime to q_2.*

A finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Q})$ is contained in $\mathrm{GL}_n(\mathbb{Z}[\frac{1}{q_0}])$ for some $q_0 \in \mathbb{N}^+$. Thus, Corollary 2.3 together with Theorems 2.4 and 2.5 imply:

Corollary 2.6. *Let Γ be a finitely generated Zariski-dense subgroup of $SL_n(\mathbb{Q})$ and let Σ be an admissible generating multi-subset. There exist $q_3 \in \mathbb{N}^+$ and $\delta > 0$ such that for every square-free $d \leq e^{\delta k}$ coprime to q_3 and every $T \subseteq \mathrm{SL}_n(\mathbb{Z}/d\mathbb{Z})$, the probability $\mathrm{Prob}_\Sigma(\pi_d(w_k) \in T)$ is approximately $\frac{|T|}{|\mathrm{SL}_n(\mathbb{Z}/d\mathbb{Z})|}$ and the error term is smaller than $e^{-\delta k}$ (so it decays exponentially fast with k).*

The following proposition, which gives an example of a family consisting of exponentially small subsets, can be easily deduced from Proposition 3.2 of [BGS1].

Proposition 2.7 (Bourgain-Gamburd-Sarnak, [BGS1])**.** *Let Γ be a finitely generated Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Q})$. Let V be a proper subvariety of $\mathrm{SL}_n(\mathbb{C})$ defined over $\mathbb{Q}$. Then, $V(\mathbb{C}) \cap \Gamma$ is exponentially small.*

Proof. Fix an admissible generating multi-subset Σ and let δ be as in Corollary 2.6. Assume that k is large enough and pick a prime between $\frac{1}{2}e^{\delta k}$ and $e^{\delta k}$ coprime to q_3 for which $V(\mathbb{Z}/pZ)$ is defined. The dimension of V is at most $n^2 - 2$, so by the Lang-Weil estimates [LW], $|V(\mathbb{Z}/p\mathbb{Z})| \leq (c+1)p^{n^2-2}$, where c is the number of irreducible components of maximal dimension of V. Now, $|\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})| \geq \frac{1}{2}p^{n^2}$, so $\frac{|V(\mathbb{Z}/p\mathbb{Z})|}{|\mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z})|} \leq \frac{2c+2}{p}$. Corollary 2.6 shows that the probability $\mathrm{Prob}_\Sigma(\pi_p(w_k) \in V(\mathbb{Z}/p\mathbb{Z}))$ is at most $(4c+5)e^{-\delta k}$. □

Definition. An element $g \in \mathrm{SL}_n(\mathbb{Z})$ is called unipotent if all its eigenvalues are equal to 1. An element $g \in \mathrm{SL}_n(\mathbb{Z})$ is called virtually unipotent if for some $m \geq 1$ the element g^m is unipotent.

A straightforward corollary of Proposition 2.7 is:

Corollary 2.8. *Let Γ be a Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Q})$. Then, the set of virtually unipotent elements is exponentially small.*

Proof. An element $g \in \mathrm{SL}_n(\mathbb{Q})$ is virtually unipotent if and only if all its eigenvalues are roots of unity. There are only finitely many roots of unity which are roots of a monic polynomial of degree at most n over $\mathbb{Q}$. Hence, there is a constant $m \geq 2$, depending only on n, such that if $g \in \mathrm{SL}_n(\mathbb{Q})$ is virtually unipotent, then g^m is unipotent. The set of elements of $\mathrm{SL}_n(\mathbb{C})$ whose m^{th}-power is unipotent is a proper subvariety defined over $\mathbb{Z}$. Proposition 2.7 completes the proof. □

3. The large sieve

In the previous section we proved that the set U consisting of virtually unipotent elements of Γ is exponentially small, where Γ is a Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Z})$. For every large enough $k \in \mathbb{N}^+$ we picked a large prime p_k with two properties. The first is that the set $\pi_{p_k}(U)$ is exponentially small in $\pi_{p_k}(\Gamma)$, i.e., the ratio between the size of $\pi_{p_k}(\Gamma)$ and the size of $\pi_{p_k}(U)$ grows exponentially with k. The second is that the image of the k^{th}-step of a random walk is 'almost uniformly distributes' in $\pi_p(\Gamma)$.

There are some exponentially small sets for which an argument of that kind does not work. For example, it does not work for the set of proper powers or even for the set of m-powers for some fixed m. The reason is that there is a fixed positive proportion $\alpha > 0$ such that for every prime p the proportion of the set of m-powers in $\pi_p(\Gamma)$ is at least α. In order to overcome this problem one may look at the image of Γ under the modulo-d homomorphism, where d is a product of a linear number (as a function of k) of primes. This raises a new problem: the image of the k^{th}-step of a random walk is not 'almost uniformly distributes' in $\pi_d(\Gamma)$.

The large sieve method provides a way to deal with this situation. It implies that in order to show that a set $Z \subseteq \Gamma$ is exponentially small it is enough to find a constant $c > 0$ and exponentially many (as a function of k) primes p for which the following three conditions hold. The first is that $\frac{|\pi_p(Z)|}{|\pi_p(\Gamma)|} \leq 1 - c$ for every such prime p. The second is that the k^{th}-step of a random walk is 'almost uniformly distributes' in $\pi_p(\Gamma)$ for every such prime p. The third is that for every two distinct such primes p and q the images in $\pi_p(\Gamma)$ and $\pi_q(\Gamma)$ of the k^{th}-step of a random walk are 'almost independent'.

3.1. **The large sieve theorem.**

We start this section by stating a lemma which has nothing to do with property-τ nor with groups. Property-τ will come into the picture once we try to use this proposition in the context of group theory. We are thankful to Ron Peled who simplified the proof of the next lemma by suggesting the use of Chebyshev's inequality.

Lemma 3.1. *Let U be a probability space. Let $(A_i)_{1 \leq i \leq L}$ be a series of events. For $1 \leq i, j \leq L$ denote:*

$$W(i,j) := \mathrm{Prob}(A_i \cap A_j) - \mathrm{Prob}(A_i)\,\mathrm{Prob}(A_j),$$

$$\triangle := \max_{1 \leq i \neq j \leq L} |W(i,j)|,$$

and

$$M := \sum_{i=1}^{L} \mathrm{Prob}(A_i).$$

Then:

$$\mathrm{Prob}(U \setminus \bigcup_{1 \leq i \leq L} A_i) \leq \frac{L + L^2 \triangle}{M^2}.$$

Proof. Chebyshev's inequality says that if X is a random variable, then for $C \geq 0$:

$$\mathrm{Prob}(|X - \mathrm{E}(X)| \geq C) \leq \frac{\mathrm{Var}(X)}{C^2}.$$

In particular, if $C = \mathrm{E}(X)$, then:

$$\mathrm{Prob}(X = 0) \leq \mathrm{Prob}(|X - \mathrm{E}(X)| \geq \mathrm{E}(X)) \leq \frac{\mathrm{Var}(X)}{\mathrm{E}(X)^2}.$$

Define X_i to be the indicator function of A_i and set $X := \sum_{1 \leq i \leq L} X_i$. Then, $M = \mathrm{E}(X)$ while

$$\mathrm{Var}(X) := \mathrm{E}((X - \mathrm{E}(X))^2) = \sum_{1 \leq i,j \leq L} E(X_i X_j - 2X_i \,\mathrm{E}(X_j) + E(X_i)E(X_j))$$

$$= \sum_{1 \leq i,j \leq L} (E(X_i X_j) - E(X_i)E(X_j)) = \sum_{1 \leq i,j \leq L} W(i,j) \leq L + L^2 \triangle.$$

Thus,

$$\mathrm{Prob}(U \setminus \bigcup_{1 \leq i \leq L} A_i) = \mathrm{Prob}(X = 0) \leq \frac{L + L^2 \triangle}{M^2}.$$

□

Theorem 3.2. *Fix $s \geq 2$. Let Γ be a finitely generated group and let $\Sigma \subset \Gamma$ be an admissible multi-set. Let $(N_i)_{i \geq 2}$ be a series of finite index normal subgroups of Γ. For $i, j \geq 2$ denote $N_{i,j} := N_i \cap N_j$, $\Gamma_{i,j} := \Gamma / N_{i,j}$ and let $\pi_{i,j} : \Gamma \to \Gamma_{i,j}$ be the quotient homomorphism. Let $Z \subseteq \Gamma$ and assume that there are positive constants δ, c and d and a sequence $(T_i)_{i \geq 2}$ such that for every $i, j \geq s$ the following conditions hold:*

0. $T_i \subseteq \Gamma_{i,i} \setminus \pi_{i,i}(Z)$.
1. *For every $T \subseteq \Gamma_{i,j}$,* $\left|\mathrm{Prob}_\Sigma(\pi_{i,j}(w_k) \in T) - \frac{|T|}{|\Gamma_{i,j}|}\right| \leq \sqrt{|\Gamma_{i,j}|} e^{-\delta k}$.
2. $|\Gamma_{i,i}| \leq i^d$.
3. *If i and j are distinct, then* $\frac{|\{gN_{i,j} | gN_i \in T_i \ \wedge \ gN_j \in T_j\}|}{|\Gamma_{i,j}|} = \frac{|T_i||T_j|}{|\Gamma_{i,i}||\Gamma_{j,j}|}$.
4. $\frac{|T_i|}{|\Gamma_{i,i}|} \geq c$.

Then for every $k \geq \frac{d+1}{\delta} \log(2s)$, $\mathrm{Prob}_\Sigma(w_k \in Z) \leq \frac{20}{c^2} e^{-\frac{\delta k}{d+1}}$. In particular, Z is exponentially small w.r.t. Σ.

Proof. For every $i \in I$ denote $\Gamma_i := \Gamma_{i,i}$ and $\pi_i := \pi_{i,i}$. Conditions 1 and 3 imply that for every distinct $i, j \in I$ and $k \in \mathbb{N}^+$:

$$\left|\mathrm{Prob}_\Sigma(\pi_i(w_k) \in T_i) - \frac{|T_i|}{|\Gamma_i|}\right| \leq \sqrt{|\Gamma_i|} e^{-\delta k} \tag{1}$$

and

$$\left|\mathrm{Prob}_\Sigma(\pi_i(w_k) \in T_i \ \wedge \ \pi_j(w_k) \in T_j) - \frac{|T_i|}{|\Gamma_i|}\frac{|T_j|}{|\Gamma_j|}\right| \leq \sqrt{|\Gamma_i||\Gamma_j|} e^{-\delta k}. \tag{2}$$

Recall that the set of walks $\mathrm{W}(\Sigma)$ is a probability space. For $i \geq s$ and $k \geq 1$, denote $A_{i,k} := \{w \in \mathrm{W}(\Sigma) \mid \pi_i(w_k) \in T_i\}$. Note that if w is a walk and $w_k \in Z$, then $w \notin \bigcup_{i \geq s} A_{i,k}$. We can rewrite equations (1) and (2) in the form:

$$\left|\mathrm{Prob}(A_{i,k}) - \frac{|T_i|}{|\Gamma_i|}\right| \leq \sqrt{|\Gamma_i|} e^{-\delta k} \tag{3}$$

and

$$\left|\mathrm{Prob}(A_{i,k} \cap A_{j,k}) - \frac{|T_i|}{|\Gamma_i|}\frac{|T_j|}{|\Gamma_j|}\right| \leq \sqrt{|\Gamma_i||\Gamma_j|} e^{-\delta k}. \tag{4}$$

Thus, Equations 3 and 4 together with Condition 2 imply that for $i \neq j$:

$$|\mathrm{Prob}(A_{i,k} \cap A_{j,k}) - \mathrm{Prob}(A_{i,k})\mathrm{Prob}(A_{j,k})| \leq 4\max(i,j)^d e^{-\delta k}. \tag{5}$$

Define $L_k := e^{\frac{\delta k}{d+1}}$. Equation (5) shows that for every distinct $s \leq i, j \leq L_k$ we have $|W_k(i,j)| \leq 4e^{-\frac{\delta k}{d+1}}$, where $W_k(i,j)$ is defined in a similar manner to the definition in Lemma 3.1. Hence,

$$\Delta_k := \max_{s \leq i \neq j \leq L_k} |W_k(i,j)| \leq 4e^{-\frac{\delta k}{d+1}} = 4L_k^{-1}$$

while Condition 4 implies that

$$M_k := \sum_{s \leq i \leq L_k} \mathrm{Prob}(A_{i,k}) \geq c(L_k - s).$$

If $k \geq \frac{d+1}{\delta}\log(2s)$, then $L_k - s \geq \frac{1}{2}L_k$. Proposition 3.1 implies that for every $k \geq \frac{d+1}{\delta}\log(2s)$:

$$\mathrm{Prob}_\Sigma(w_k \in Z) \leq \mathrm{Prob}(\mathrm{W}(\Sigma) \setminus \bigcup_{s \leq i \leq L_k} A_{i,k}) \leq \frac{L_k + {L_k}^2\Delta_k}{M_k^2} \leq \frac{20}{c^2 L_k} = \frac{20}{c^2} e^{-\frac{\delta k}{d+1}}.$$

□

We are now ready to formulate the Group Large Sieve (GLS) method. The reader may note that Theorem B of the introduction is a special case of the following:

Theorem 3.3 (GLS)**.** *Fix $s \geq 2$. Let Γ be a finitely generated group and let Σ be an admissible multi-subset. Let Λ be a finite index subgroup of Γ and let $(N_i)_{i \geq 2}$ be a family of normal finite index subgroups of Γ which are contained in Λ. Let $Z \subseteq \Gamma$ and assume that the following conditions hold:*

1. *Γ has property-τ w.r.t. the family $\{N_i \cap N_j \mid i, j \geq s\}$.*
2. *There exists a constant d such that $|\Gamma/N_j| \leq j^d$ for every $j \geq s$.*
3. *$|\Lambda/N_i \cap N_j| = |\Lambda/N_i||\Lambda/N_j|$ for every distinct $i, j \geq s$.*
4. *There exists $c > 0$ such that for every coset $C \in \Gamma/\Lambda$ and every $j \geq s$,*

$$|(Z \cap C)N_j/N_j| \leq (1-c)|\Lambda/N_j|.$$

Then there are positive constants γ and t such that $\mathrm{Prob}_\Sigma(w_k \in Z) \leq e^{-\gamma k}$ for every $k \geq t\log s$. In particular, Z is exponentially small.

In fact, the constants γ and t depend only on the spectral gap of the family of Cayley graphs $\{\mathrm{Cay}(\Gamma/N_i, \Sigma N_i/N_i) \mid i \geq 2\}$, the size of Σ, the length of the shortest odd cycle in $\mathrm{Cay}(\Gamma, \Sigma)$ and the two constants c and d.

Proof. It is enough to verify the conditions of Theorem 3.2 with respect to Γ. The existence of constants δ and d for which Conditions 1 and 2 of Theorem 3.2 hold follows from Conditions 1 and 2 of the current theorem together with Corollary 2.3. Condition 4 of the current theorem allows us to choose for every $i \geq s$ a constant $b_i \geq c$ and a subset $T_i \subseteq \Gamma/N_i \setminus ZN_i/N_i$ such that $|T_i \cap C/N_j| = b_i|\Lambda/N_i|$ for every coset $C \in \Gamma/\Lambda$. Conditions 0 and 4 of Theorem 3.2 are readily satisfied by the definition of T_i. The definition also implies that for every $i \geq s$, $\frac{|T_i|}{|\Gamma_{i,i}|} = b_i$. In turn, Condition 3 of the current theorem ensures that for every distinct $i, j \geq s$, $\frac{|\{gN_{i,j} | gN_i \in T_i \ \wedge \ gN_j \in T_j\}|}{|\Gamma_{i,j}|} = b_i b_j$. Thus, Condition 3 of Theorem 3.2 also holds. □

Our next goal is to apply the group large sieve method in the situation where Γ is a subgroup of $\mathrm{SL}_n(\mathbb{Z})$. For every prime p, let $\pi_p : \Gamma \to \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ be the modulo-p homomorphism. We shall see that it is fruitful to define $N_i := \ker \pi_{p_i}$ where $p_2, p_3, \ldots$ is an ascending enumeration of the primes which belong to some arithmetic progression. In order to verify Condition 2 of Theorem 3.3 with respect to the sequence $(N_i)_{i\geq 2}$, we need the next theorem about the density of the primes in arithmetic progressions (for a proof, see Chapter 22 of [Da]).

Theorem 3.4 (Quantitative Dirichlet's Theorem)**.** *Let $0 \leq \varepsilon < 1$ and $t \geq 1$ be constants. Then there exists a constant $r > 0$ such that for every $k \geq r$, every $x \geq e^{\frac{k}{t}}$ and every two coprime numbers $1 \leq a, b \leq k^t$ the number of primes p which satisfy:*

- *$1 \leq p \leq x$*
- *p belongs to the series $(a + bj)_{j\geq 1}$*

is at least $\frac{1-\varepsilon}{\varphi(b)} \frac{x}{\log x}$, where φ is the Euler function.

A straightforward corollary of Theorem 3.4 is:

Corollary 3.5. *Let t_1 and t_2 be positive constants. Then there exists a positive constant r depending only on t_1 and t_2 such that for every $k \geq r$ and every two coprime natural numbers $a, b \leq k^{t_1}$, if $(p_i)_{i\geq 1}$ is an ascending enumeration of the primes which belong to the sequence $(a + bi)_{i\geq 1}$, then $p_i \leq i^2$ for every $i \geq e^{\frac{k}{t_2}}$.*

We can now deduce:

Proposition 3.6. *Fix $n \geq 2$ and $c > 0$. Let Γ be a Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Z})$ with an admissible multi-subset Σ. For every $q \in \mathbb{N}^+$, let $\pi_q : \Gamma \to \mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z})$ be the modulo-q homomorphism. Then, there exist two positive constants γ and r, depending only on Γ, Σ, and c such that the following statement holds:*

Let Z be a subset of Γ and let $k \geq r$ be a natural number. Assume that there are two coprime natural numbers $2 \leq a, b \leq k^2$ such that for every prime p which belongs to the arithmetic progression $(a + bj)_{j\geq 1}$, the size of $\pi_p(Z)$ is at most $(1 - c)|\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})|$. Then,

$$\mathrm{Prob}_\Sigma(w_k \in Z) \leq e^{-\gamma k}.$$

Proof. Let a ,b, c, k and Z be as in the statement. We need to show that there are positive constants γ and r depending only on Γ ,Σ and c such that if $k \geq r$, then

$$\mathrm{Prob}_\Sigma(w_k \in Z) \leq e^{-\gamma k}.$$

Denote $q_3 := q_1 q_2$, where q_1 is as in Theorem 2.4 and q_2 is as in Theorem 2.5. Note that q_3 depends only on Γ and Σ. Let $(p_i)_{i\geq 2}$ be an ascending enumeration of the primes which belong to the sequence $(\tilde{a} + bq_3 i)_{i\geq 1}$, where $a \leq \tilde{a} < a + bq_3$ is relatively prime to q_3 and $\tilde{a} \equiv a \pmod{b}$. Denote $N_i := \ker \pi_{p_i}$ for every $i \geq 2$. Theorem 2.4 implies that Γ has property-τ with respect to the family $(N_i \cap N_j)_{i,j\geq 2}$ and Theorem 2.5 (Strong Approximation) implies that if $q \in \mathbb{N}^+$ is a product of primes which belongs to $(\tilde{a} + bq_3 i)_{i\geq 1}$, then $\pi_q(\Gamma) = \mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z})$.

We now verify the four conditions of GLS (Theorem 3.3) for $\Lambda = \Gamma$. The above paragraph together with the fact that $\mathrm{SL}_n(\mathbb{Z}/p_1p_2\mathbb{Z}) \cong \mathrm{SL}_n(\mathbb{Z}/p_1\mathbb{Z}) \times \mathrm{SL}_n(\mathbb{Z}/p_2\mathbb{Z})$ for distinct primes p_1 and p_2 imply that Conditions 1 and 3 of GLS are satisfied for every $i, j \geq 2$. Condition 4 of GLS is true for every $j \geq 2$ by assumption.

Finally, we will show that Condition 2 of GLS holds for $d := 2n^2$. Let δ be the spectral gap of the family $\{\mathrm{Cay}(\Gamma/N_i, \Sigma N_i/N_i) \mid i \geq 2\}$. Let $\gamma := \gamma(\delta, |\Sigma|, c, d)$ and $t_2 := t(\delta, |\Sigma|, c, d)$ be the constants of GLS for $d = 2n^2$. Corollary 3.5 with respect to $t_1 := 3$ implies that there exists a constant r such that if $k \geq r$ and $j \geq e^{\frac{k}{2t_2}}$, then $p_j \leq j^2$, so $|\Gamma/N_j| \leq j^{2n^2}$. We can assume that $k \geq r$ and denote $s := e^{\frac{k}{2t_2}}$. Hence, Condition 2 of GLS holds for every $j \geq s$. We finished to verify all the conditions of GLS. Since $k \geq t_2 \log s$, GLS implies that $\mathrm{Prob}_\Sigma(w_k \in Z) \leq e^{-\gamma k}$. □

3.2. **An extension of Proposition 3.6.** This subsection is needed for the proof of the general case of Theorem A. A reader that is only interested in the special case (Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Z})$) can skip this subsection.

Proposition 3.7. *Let $\Gamma \leq \mathrm{GL}_n(\mathbb{Q})$ be a finitely generated group such that its Zariski-closure in $\mathrm{GL}_n(\mathbb{C})$ is semisimple. Then there are:*

- *A finite index normal subgroup Λ of Γ,*
- *A set $\mathcal{P}$ which contains almost all primes,*
- *For every prime $p \in \mathcal{P}$, an epimorphism $\pi_p : \Gamma \to \Gamma_p$ such that Γ_p is a non-trivial finite group and $N_p := \ker \pi_p$ is contained in Λ,*
- *Constants $d, l, s \in \mathbb{N}^+$,*

such that:

1. *Γ has property-τ with respect to the family $\{N_{p,q}\}_{p,q\in\mathcal{P}}$, where $N_{p,q} := N_p \cap N_q$.*
2. *$\Lambda_p := \pi_p(\Lambda)$ is a direct product of at most l finite simple groups of Lie type of rank at most l over finite extensions of $\mathbb{F}_p$ of degree at most l for every $p \in \mathcal{P}$. Furthermore, $\frac{1}{s}p^d \leq |\Lambda_p| \leq sp^d \leq p^{d+1}$.*
3. *The natural homomorphism $\pi_{p,q} : \Lambda_{p,q} \to \Lambda_p \times \Lambda_q$ is an isomorphism for all distinct $p, q \in \mathcal{P}$, where $\Lambda_{p,q} := \Lambda/N_{p,q}$.*

Proof. Since Γ is finitely generated it is contained in $\mathrm{GL}_n(\mathbb{Z}[\frac{1}{q_0}])$ for some $q_0 \in \mathbb{N}^+$. The connected component of the Zariski-closure of Γ in $\mathrm{GL}_n(\mathbb{C})$, denoted by $\mathrm{G}(\mathbb{C})$, is defined over $\mathbb{Q}$. Hence, for every large enough prime p the group $\mathrm{G}(\mathbb{F}_p)$ and the residue map $\Gamma^\circ \to \mathrm{G}(\mathbb{F}_p)$ are defined, where $\Gamma^\circ := \Gamma \cap \mathrm{G}(\mathbb{C})$.

We would like to apply the Strong Approximation Theorem to conclude that for every large enough prime p the residue map $\Gamma^\circ \to \mathrm{G}(\mathbb{F}_p)$ is an epimorphism. But we have a problem: our $\mathrm{G}(\mathbb{C})$ is connected and semisimple but not necessarily simply connected. To overcome this problem we let $\psi : \tilde{\mathrm{G}} \to \mathrm{G}$ be the universal cover of G. The algebraic group $\tilde{\mathrm{G}}$ and the rational homomorphism ψ are defined over $\mathbb{Q}$. The group $\psi(\tilde{\mathrm{G}}(\mathbb{Q}))$ is a normal coabelian subgroup of $\mathrm{G}(\mathbb{Q})$. This implies that there exists $\tilde{\Gamma}_1 \leq \tilde{\mathrm{G}}(\mathbb{Q})$, where $\psi|_{\tilde{\Gamma}_1}$ is an isomorphism onto a finite index subgroup Γ_1 of Γ° (see chapter 16 of [LuSe]). The image of Γ_1 under the residue map $\Gamma_1 \to \mathrm{G}(\mathbb{F}_p)$ is the same as the image of $\tilde{\Gamma}_1$ under the composition $\tilde{\Gamma}_1 \to \tilde{\mathrm{G}}(\mathbb{F}_p) \to \mathrm{G}(\mathbb{F}_p)$. The Strong Approximation Theorem (Theorem 2.5) says that for a large enough prime p the first homomorphism is an epimorphism. The kernel of the second homomorphism is contained in the center of $\tilde{\mathrm{G}}(\mathbb{F}_p)$ and the image is of index at most b in $\mathrm{G}(\mathbb{F}_p)$ where $b \in \mathbb{N}^+$ is some constant independent of p.

We define Λ to be the intersection of all subgroups of index at most b of Γ_1. For a large enough prime p we get a homomorphism $\pi_p : \Lambda \to \tilde{\mathrm{G}}(\mathbb{F}_p)/\mathrm{Z}(\tilde{\mathrm{G}}(\mathbb{F}_p))$ and we denote $N_p := \ker \pi_p$. The structure of $\tilde{\mathrm{G}}(\mathbb{F}_p)/\mathrm{Z}(\tilde{\mathrm{G}}(\mathbb{F}_p))$ is well known and there are $c, d, l \in \mathbb{N}^+$ such that the requirements of condition 2 are satisfied (see [JKZ]

and the references therein). In fact, $d := \dim(\tilde{\mathrm{G}}(\mathbb{C}))$. In particular, this structure assures that π_p is an epimorphism for a large enough prime p, so condition 2 is satisfied for the set $\mathcal{P}$ consisting of large enough primes. Condition 3 then follows since two finite simple Lie groups over a field of different characteristics are not isomorphic. Condition 1 follows from Theorem 2.4. □

The proof of the next proposition is identical to the proof of Proposition 3.6, so it is omitted.

Proposition 3.8. *Fix a positive constant c. Let Γ be as in Proposition 3.7 and let Σ be an admissible generating multi-set of Γ. Then, there exist two positive constants γ and r, depending only on Γ and Σ and c such that the following statement holds:*

Let Z be a subset of Γ and let $k \geq r$ be a natural number. Assume that there are two coprime natural numbers $2 \leq a, b \leq k^5$ such that for every prime p which belongs to the arithmetic progression $(a + bj)_{j\geq 1}$ and every coset $C \in \Gamma_p/\Lambda_p$, the size of $\pi_p(Z) \cap C$ is at most $(1 - c)|\Lambda_p|$. Then,

$$\mathrm{Prob}_\Sigma(w_k \in Z) \leq e^{-\gamma k}.$$

4. Proof of Theorem A for a Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Z})$

In this section, Γ denotes a Zariski-dense subgroup of $\mathrm{SL}_n(\mathbb{Z})$ and Σ is an admissible generating multi-subset of Γ.

Lemma 4.1. *Fix $m \geq 2$. Let p be a prime which satisfies:*

- $p \geq 3\binom{n}{2} + 1$,
- $p = 1 (\mathrm{mod}\, m)$.

Then $|\{g^m \mid g \in \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})\}| \leq (1 - \frac{1}{6n!})|\,\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})|$.

Proof. The subset T of diagonal matrices of $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ is a subgroup isomorphic to C_{p-1}^{n-1}, where C_{p-1} is a cyclic group of order $p - 1$. Since m divides $p - 1$ the map $x \mapsto x^m$ is m^{n-1}-to-1 on T, so

$$|\{t^m \mid t \in T\}| \leq \frac{1}{m^{n-1}}|T| \leq \frac{1}{2}|T|.$$

An element of T is called regular if all its non-zero entries are distinct. The size of the set S consisting of regular elements is at least $(p-1)^{n-1} - \binom{n}{2}(p-1)^{n-2}$. Thus, if $p \geq 1 + 3\binom{n}{2}$, then

$$|S| \geq \frac{2}{3}|T|,$$

while

$$|\{t^m \mid t \in S\}| \leq \frac{1}{2}|T|.$$

Let $s \in S$. Then the centralizer of s is T. If $g \in \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ and $gsg^{-1} \in T$, then gsg^{-1} is also regular, so its centralizer is also T. On the other hand, conjugation by g is an automorphism, so the centralizer of gsg^{-1} is gTg^{-1}. Thus, $T = gTg^{-1}$ and g belongs to the normalizer N of T. The normalizer N is the set of monomial matrices, so N/T is isomorphic to the symmetric group on n elements and $[N : T] = n!$.

Let R be a set of representatives of the left cosets of N. Then,

$$|R| = \frac{1}{n!}[\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}) : T].$$

If $r_1, r_2 \in R$ are distinct, then $r_1 S r_1^{-1}$ and $r_2 S r_2^{-1}$ are disjoint. Thus for $\bar{S} := \bigcup_{r\in R} rSr^{-1}$,

$$|\bar{S}| \geq \frac{2}{3}|T| \cdot \frac{1}{n!}\frac{|\operatorname{SL}_n(\mathbb{Z}/p\mathbb{Z})|}{|T|} = \frac{2}{3n!}|\operatorname{SL}_n(\mathbb{Z}/p\mathbb{Z})|$$

while

$$|\{s^m \mid s \in \bar{S}\}| \leq \frac{1}{2}|T| \cdot \frac{1}{n!}\frac{|\operatorname{SL}_n(\mathbb{Z}/p\mathbb{Z})|}{|T|} = \frac{1}{2n!}|\operatorname{SL}_n(\mathbb{Z}/p\mathbb{Z})|.$$

□

Combining Lemma 4.1 with Proposition 3.6 we get:

Corollary 4.2. *There exist two positive constants γ and r such that if $k, m \in \mathbb{N}^+$ with $k \geq r$ and $2 \leq m \leq k^2$, then*

$$\operatorname{Prob}_\Sigma(w_k \in \Gamma^m) \leq e^{-\gamma k}.$$

The next lemma shows what kind of m-powers are possible at the k^{th}-step of a random walk.

Lemma 4.3. *There is a constant $s \in \mathbb{N}^+$ such that if the k^{th}-step w_k of a random walk on $\operatorname{Cay}(\Gamma, \Sigma)$ is a proper power, then one of the following holds:*

- *w_k is virtually unipotent,*
- *$w_k = g^m$ for some element $g \in G$ and some prime number $m \leq sk$.*

Proof. For $x \in \mathbb{C}^n$ let $|x|$ be the L^2-norm of x. Recall that the operator norm of an element $g \in \Gamma$ is $||g|| := \max_{|x|=1} |gx|$. Note that if $g, h \in \Gamma$ and λ is an eigenvalue of g, then $||gh|| \leq ||g||||h||$ and $|\lambda| \leq ||g||$. Define $c := \max_{g\in\Sigma} ||g||$, so $||w_k|| \leq c^k$ for every walk w.

If a polynomial f of degree n with integer coefficients is not a product of cyclothymic polynomials, then it has a root with absolute value greater than $1 + \varepsilon$, where ε depends only on n (see for example Proposition 5.5 and Corollary 5.6 of [Mi]). Thus, if $g \in \operatorname{SL}_n(\mathbb{Z})$ is not virtually unipotent, then it has an eigenvalue λ with absolute value greater than $1 + \varepsilon$, so $||g^m|| \geq (1 + \varepsilon)^m$ for every $m \in \mathbb{N}$.

A power of a virtually unipotent element is virtually unipotent. Hence, if the k^{th}-step w_k of a walk is an m-power but not virtually unipotent, then $(1+\varepsilon)^m \leq c^k$ so $m \leq sk$ for $s := \frac{\log c}{\log(1+\varepsilon)}$. □

Our goal is to show that the set of proper powers in Γ is exponentially small. The set of virtually unipotent elements in Γ is exponentially small by Corollary 2.8. Thus, Lemma 4.3 implies that it is enough to show that the set $Z \subseteq \Gamma$ of elements which are proper powers but not virtually unipotent is exponentially small. Let s be as in Lemma 4.3 and let γ and r be as in Corollary 4.2. If $k \geq \max(r, s)$, then

$$\operatorname{Prob}_\Sigma(w_k \in Z) = \operatorname{Prob}_\Sigma(w_k \in \bigcup_{2\leq m\leq k^2} \Gamma^m) \leq k^2 e^{-\gamma k}.$$

If α is a positive constant smaller than γ, then for large enough k,

$$\operatorname{Prob}_\Sigma(w_k \in Z) \leq k^2 e^{-\gamma k} \leq e^{-\alpha k}.$$

Thus, Z is indeed exponentially small and the proof is complete.

5. Proof of Theorem A

5.1. **Reduction.** The next lemma shows that it is enough to prove Theorem A for a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Q})$ such that the connected component of its Zariski-closure is a non-trivial semisimple group.

Lemma 5.1. *Let $\Gamma \leq \mathrm{GL}_m(\mathbb{C})$ be a finitely generated group which is not virtually solvable. Then there is a positive integer n and a homomorphism $\alpha : \Gamma \to \mathrm{GL}_n(\mathbb{Q})$ such that the connected component of the Zariski-closure of $\alpha(\Gamma)$ is a non-trivial semisimple group.*

Proof. There is an $n_1 \in \mathbb{N}^+$ and a homomorphism $\alpha_1 : \Gamma \to \mathrm{GL}_{n_1}(\mathbb{Q})$ such that $\alpha(\Gamma)$ is not a virtually solvable group (see Proposition 16.4.13 of the window on strong approximation in [LuSe]). The connected component of the Zariski-closure of $\alpha(\Gamma)$ is not necessarily semisimple. However, we can divide it by its solvable radical, which is defined over $\mathbb{Q}$. Thus, there is $n_2 \in \mathbb{N}^+$ and a homomorphism $\alpha_2 : \alpha_1(\Gamma) \to \mathrm{GL}_{n_2}(\mathbb{Q})$ such that the connected component of the Zariski-closure of $\alpha_2 \circ \alpha_1(\Gamma)$ is semisimple. Define $\alpha := \alpha_2 \circ \alpha_1$ and $n := n_2$. □

5.2. **Virtually unipotent elements.** We start this section with an analog of Proposition 2.7.

Proposition 5.2. *Let Γ be a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Q})$ whose Zariski-closure $\bar{\Gamma}$ is semisimple. Assume that $V(\mathbb{C})$ is a variety defined over $\mathbb{Q}$ and that $V(\mathbb{C})$ does not contain any coset of the connected component of $\bar{\Gamma}$. Then, $V(\mathbb{C}) \cap \Gamma$ is exponentially small.*

The proof of Proposition 5.2 is almost identical to that of Proposition 2.7, so we omit it. The next corollary is the main result of this subsection.

Corollary 5.3. *Let Γ be a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Q})$ whose Zariski-closure is semisimple. Then, the set of virtually unipotent elements is exponentially small.*

Proof. As in the proof of Corollary 2.8, there exists a positive integer t such that if $g \in \Gamma$ is virtually unipotent, then g^t is unipotent. Thus, the set of virtually unipotent elements is contained in a subvariety defined over $\mathbb{Q}$. Proposition 2.7 above and Lemma 5.4 below complete the proof. □

Lemma 5.4. *Let $t \in \mathbb{N}^+$. Let $\mathrm{G}(\mathbb{C})$ be an algebraic semisimple group. Then every coset of the identity component $\mathrm{G}(\mathbb{C})^\circ$ contains an element whose t-power is not unipotent.*

Proof. By replacing $\mathrm{G}(\mathbb{C})$ with its image in $\mathrm{G}(\mathbb{C})/\mathrm{Z}(\mathrm{G}(\mathbb{C})^\circ)$ we can assume that $\mathrm{G}(\mathbb{C})^\circ$ has a trivial center. Let C be some coset of $\mathrm{G}(\mathbb{C})^\circ$ and assume that for every $g \in C$ the power g^t is unipotent. Then the order of every element in C is either a divisor of t or equals infinity. Thus, in order to get a contradiction it is enough to show that every coset of $\mathrm{Inn}(\mathrm{G}(\mathbb{C})^\circ)$ in $\mathrm{Aut}(\mathrm{G}(\mathbb{C})^\circ)$ contains an element whose order is finite but greater than t.

If $\mathrm{G}(\mathbb{C})^\circ$ is a simple group of adjoint type, then every coset of $\mathrm{Inn}(\mathrm{G}(\mathbb{C})^\circ)$ in $\mathrm{Aut}(\mathrm{G}(\mathbb{C})^\circ)$ contains a graph automorphism α. The graph automorphism α fixes some root of the Dynkin diagram unless the diagram is of type A_{2n} and in that case the automorphism switches between the two roots at the ends. In any case, α pointwise fixes some torus T, so the set αT contains the desired element.

In the general case, $\mathrm{G}(\mathbb{C})^\circ$ has a characteristic subgroup $\mathrm{N}(\mathbb{C})$ such that $\mathrm{G}(\mathbb{C})^\circ/\mathrm{N}(\mathbb{C})$ is isomorphic to $\mathrm{H}(\mathbb{C})^k$, where $\mathrm{H}(\mathbb{C})$ is a connected simple group of adjoint type and $k \in \mathbb{N}^+$. It suffices to show that for every $\alpha \in \mathrm{Aut}(\mathrm{H}(\mathbb{C})^k)$ the set $\alpha\,\mathrm{Inn}(\mathrm{H}(\mathbb{C})^k)$ contains an element of finite order greater than t. As before, this will follow once we show that there is an element in $\alpha\,\mathrm{Inn}(\mathrm{H}(\mathbb{C})^k)$ which pointwise fixes a non-trivial torus. As $\alpha \in \mathrm{Aut}(\mathrm{H}(\mathbb{C})^k)$, there are $\alpha_1, \dots, \alpha_k \in \mathrm{Aut}(\mathrm{H}(\mathbb{C}))$ and a permutation $\sigma \in \mathrm{Sym}(k)$ such that for every $(x_1, \dots, x_k) \in \mathrm{H}(\mathbb{C})^k$ we have

$$\alpha(x_1, \dots, x_k) = (\alpha_1(x_{\sigma(1)}), \dots, \alpha_k(x_{\sigma(k)})).$$

If the type of $\mathrm{H}(\mathbb{C})$ is different from D_4, then there is only one non-identity graph automorphism, so by the previous paragraph we see that there is a non-trivial torus T which is pointwise fixed by all graph automorphisms. If the type of $\mathrm{H}(\mathbb{C})$ is D_4, then all the graph automorphisms fix the central root and thus pointwise fix the torus T corresponding to this root. By replacing α with another representative of the coset $\alpha\,\mathrm{Inn}(\mathrm{H}(\mathbb{C})^k)$ we can assume that α_i is a graph automorphism for every $1 \le i \le k$, so α pointwise fixes $T^* := \{(t, \dots, t) \mid t \in T\}$. □

5.3. **Completion of the proof of Theorem A.** Let Γ be a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Q})$ whose Zariski-closure $\bar{\Gamma}$ is semisimple. Then, there are finitely many primes $p_1, \dots, p_r$ such that Γ is contained in $\mathrm{GL}_n(\mathbb{Z}[\frac{1}{p_1 \cdots p_r}])$. Fix an admissible generating multi-subset Σ of Γ.

We start with some number-theoretic arguments. For every $1 \le i \le r$, let $|\cdot|_i$ be some extension of a p_i-adic valuation of $\mathbb{Q}$ to the algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$. Fix an embedding of $\tilde{\mathbb{Q}}$ in $\mathbb{C}$ and let $|\cdot|_0$ be the restriction to $\tilde{\mathbb{Q}}$ of the absolute value of $\mathbb{C}$. It is well known that for every $n \in \mathbb{N}^+$, there exists a constant $c > 1$ such that if x is an algebraic integer of degree at most n, then either x is a root of unity or some Galois conjugate y of x satisfies $|y|_0 \ge c$ (see Proposition 5.5 and Corollary 5.6 of [Mi]). The following lemma is a straightforward generalization of this fact.

Lemma 5.5. *Denote $R := \mathbb{Z}[\frac{1}{q}]$, where $q := p_1 \cdots p_r$. Then, for every $n \in \mathbb{N}^+$ there exists a constant $c > 1$ such that if $x \in \tilde{\mathbb{Q}}^*$ is integral over R of degree at most n, then either x is a root of unity or $|y|_i \ge c$ for some $0 \le i \le r$ and some Galois conjugate y of x.*

Proof. Let $x \in \tilde{\mathbb{Q}}^*$ be integral over R such that its minimal polynomial f over R has degree at most n. The roots of f are the Galois conjugates of x. The case where all the coefficients of f belong to $\mathbb{Z}$ is the classical case above. Thus, we can assume that some coefficient b of f does not belong to $\mathbb{Z}$. Define $d := \min_{1 \le i \le r} |p_i|_i^{-\frac{1}{n}}$ and note that $d > 1$. There is $1 \le j \le r$ such that p_j is a factor of the denominator of b, so $|b|_j \ge d^n$. The coefficient b is a symmetric polynomial of degree at most n in the Galois conjugates of x and $|\cdot|_j$ is non-Archimedean, so there is at least one Galois conjugate y of x with $|y|_j \ge d$. □

For $1 \le i \le r$ and $\bar{x} = (x_1, \dots, x_n) \in \tilde{\mathbb{Q}}^n$ define

$$|\bar{x}|_i := \max_{1 \le j \le n} |x_j|_i$$

and

$$|\bar{x}|_0 := \sqrt{\sum_{j=1}^{r} |x_j|_0^2}.$$

For an element $g \in \Gamma$ and $0 \leq i \leq r$, define:

$$|g|_i := \max_{\bar{x} \neq 0} \frac{|g\bar{x}|_i}{|x|_i}.$$

Note that if $g, h \in \Gamma$ and λ is an eigenvalue of g, then $|gh|_i \leq |g|_i |h|_i$ and $|\lambda|_i \leq |g|_i$.

Lemma 5.6. *There is a constant $t \in \mathbb{N}^+$ such that for every $k \in \mathbb{N}^+$ and every walk w on $\mathrm{Cay}(\Gamma, \Sigma)$, if w_k is a proper power, then one of the following holds:*

- *w_k is virtually unipotent,*
- *$w_k = g^m$ for some element $g \in G$ and some prime number $m \leq tk$.*

Proof. Fix $k \in \mathbb{N}$ and define:

$$b := \max_{g \in \Sigma \ \wedge \ 0 \leq i \leq r} |g|_i.$$

Then, $|w_k|_i \leq b^k$ for every walk w and every $0 \leq i \leq r$. Let $g \in \Gamma$. If λ is an eigenvalue of g, then so are all the Galois conjugates of it. Lemma 5.5 shows that there is a constant $c > 1$ such that if g is not virtually unipotent, then $|\lambda|_i \geq c$ for some eigenvalue λ of g and some $0 \leq i \leq r$. In the latter case for every $m \in \mathbb{N}^+$ we have that λ^m is an eigenvalue of g^m and $|g^m|_i \geq |\lambda^m|_i \geq c^m$. Thus, if w is a walk on $\mathrm{Cay}(\Gamma, \Sigma)$ and $w_k = g^m$ for some $g \in \Gamma$ and some $m \in \mathbb{N}^+$, then either w_k is virtually unipotent or $m \leq tk$, where $t := \frac{\log b}{\log c}$. □

Lemma 5.7. *There exist two positive constants α and r such that if $k \geq r$, then*

$$\mathrm{Prob}_\Sigma(w_k \in \bigcup_{2 \leq m \leq k^2} \Gamma^m) \leq e^{-\alpha k}.$$

Proof. We use the notation of Proposition 3.7. For every coset $D \in \Gamma/\Lambda$ and every $m \geq 2$ define $D^m := \{g^m \mid g \in D\}$. Proposition 3.8 together with Corollary 6.17 implies that there are positive constants γ and r such that for every $k \geq r$ and for every coset $D \in \Gamma/\Lambda$:

$$\mathrm{Prob}_\Sigma(w_k \in \bigcup_{2 \leq m \leq k^2} D^m) \leq k^2 e^{-\gamma k}.$$

The subgroup Λ is of finite index in Γ, so it has only finitely many cosets. Hence, if $0 < \alpha < \gamma$ and k is large enough, then:

$$\mathrm{Prob}_\Sigma(w_k \in \bigcup_{2 \leq m \leq k^2} \Gamma^m) \leq e^{-\alpha k}.$$

□

Corollary 5.3 together with Lemmas 5.6 and 5.7 completes the proof of Theorem A (modulo the proof of Theorem 6.16 and Corollary 6.17).

6. Powers in finite groups of Lie type

The goal of this section is to bound the number of powers in a finite extension of a direct product of finite groups of Lie type (see Theorem 6.16 below). This bound is needed for the proof of Theorem 1.1, but it might be interesting in its own right. While our primary interest is to get the estimates needed for the sieve method, it is worth mentioning that the results of this section are related to questions regarding the cardinality of definable sets over finite fields (since the set of m-powers is definable in the language of rings). A general description of

the possible cardinalities of definable sets was given by Chatzidakis-van den Dries-Macintyre [CvdDM] and by Fried-Haran-Jarden [FHJ]. The main result of this section shows that one of the (finitely many) C-vdD-M densities for the set of m-powers is strictly smaller than 1.

6.1. **Notation.** The letter p always denotes a prime number greater than 3 (sometimes further restrictions may apply). The letter q denotes some power of p. For a group G, a subgroup $T \subseteq G$ and an automorphism $\mu \in \mathrm{Aut}(G)$, we denote $T_\mu := \{t \in T \mid \mu(t) = t\}$. In most cases the group T will be abelian and μ will preserve T. In addition, if $n \in \mathbb{N}$, then $T_n := \{t \in T \mid \mathrm{Z}_G(t^n) = T\}$ is the centralizer of t^n in G and $T_{\mu,n} := T_\mu \cap T_n$.

We fix some root system $\Phi \subseteq \mathbb{R}^l$ and let $W(\Phi)$ be its Weyl group. The symbols G_q (G_q^*) represents the simply connected Chevalley (Steinberg) group of type Φ over the field with q elements $\mathbb{F}_q$. Unless otherwise mentioned, the term finite group of Lie type means a Chevalley or Steinberg group of adjoint type although the results apply to all finite groups of Lie type. A detailed description of these groups is given in later sections.

6.2. **Powers in arbitrary groups.** We start this section with three lemmas.

Lemma 6.1. *Let G be a finite group with a maximal abelian subgroup T. Assume $\mu \in \mathrm{Aut}(G)$ preserves T and denote $n := \mathrm{ord}(\mu)$. If $t \in T_{\mu,n}$, then*

$$T_\mu = \{g \in G \mid gt\mu(g)^{-1} = t\}.$$

Proof. The inclusion $\subseteq$ is clear. For the reverse inclusion assume that $gt = t\mu(g)$. The element t is fixed by μ, so $\mu^i(g)t = t\mu^{i+1}(g)$ for every $0 \leq i \leq n-1$. Hence,

$$gt^n = t\mu(g)t^{n-1} = t^2\mu^2(g)t^{n-2} = \cdots = t^n\mu^n(g) = t^n g.$$

This means that g centralizes t^n, so $g \in T$. Thus, $gt\mu(g)^{-1} = t = gtg^{-1}$, so $\mu(g) = g$, i.e. $g \in T_\mu$. □

Lemma 6.2. *Let G be a finite group with a maximal abelian subgroup T. Let $g \in G$ and $t \in T$. If $\mathrm{Z}_G(t) = T$ and $gtg^{-1} \in T$, then $g \in N$, where $N := N_G(T)$.*

Proof. Conjugation by g is an automorphism, so $\mathrm{Z}_G(gtg^{-1}) = g\,\mathrm{Z}_G(t)g^{-1} = gTg^{-1}$. But T is abelian and so $T \subseteq \mathrm{Z}_G(gtg^{-1}) = gTg^{-1}$, which implies that $T = gTg^{-1}$ and $g \in N$. □

Lemma 6.3. *Let G be a finite group with a maximal abelian subgroup T. Assume $\mu \in \mathrm{Aut}(G)$ preserves T and denote $n := \mathrm{ord}(\mu)$. Let c be the number of elements of T of order dividing n. If $|T_{\mu,n}| > \frac{1}{2}|T_\mu|$, then the set*

$$L := \{g \in G \mid \exists s \in T_{\mu,n} \text{ s.t. } gs\mu(g^{-1}) \in T_{\mu,n}\}$$

is a subgroup of G which contains T_μ as a subgroup of index at most $c[N : T]$, where $N := N_G(T)$.

Proof. Let $g \in L$. We start by showing that $gt\mu(g^{-1}) \in T_\mu$ for every $t \in T_\mu$. Choose $s \in T_{\mu,n}$ such that $gs\mu(g^{-1}) \in T_{\mu,n}$. Every element of T_μ is fixed by μ, so

$$gs\mu(g^{-1}) = \mu(g)s\mu^2(g^{-1}) \text{ and } \mu(g^{-1})gs\mu(g^{-1})\mu^2(g) = s.$$

Lemma 6.1 together with the fact that $\mu(\mu(g^{-1})g)^{-1} = \mu(g^{-1})\mu^2(g)$ implies that $u := \mu(g^{-1})g \in T_\mu$. The element u is fixed by μ, so

$$u = \mu^i(u) = \mu^{i+1}(g^{-1})\mu^i(g)$$

for every $0 \leq i \leq n-1$. Multiplying these equations we get that

$$u^n = \mu^{n-1}(u) \cdots \mu^1(u)u = 1,$$

which means that the order of u divides n.

It is clear that L is closed under inversion, so $g^{-1} \in L$ and the argument above assures that $v := \mu(g)g^{-1} \in T_\mu$. Since $gsg^{-1}v^{-1} = gs\mu(g^{-1}) \in T_{\mu,n}$ also $gsg^{-1} \in T_\mu$. The fact that $s \in T_{\mu,n}$ implies that $\mathrm{Z}_G(s) = T$, so Lemma 6.2 shows that $g \in N$. In particular, if $t \in T_\mu$, then $gt\mu(g^{-1}) = gtg^{-1}v^{-1} \in T$. In order to show that $gt\mu(g^{-1}) \in T_\mu$ we have to show that it is fixed by μ. Indeed,

$$\begin{aligned}\mu(gt\mu(g^{-1})) &= \mu(g)t\mu^2(g^{-1}) = gg^{-1}\mu(g)t\mu^2(g^{-1})\mu(g)\mu(g^{-1}) \\ &= gu^{-1}tu\mu(g^{-1}) = gt\mu(g^{-1}),\end{aligned}$$

where that last equality is true since T is commutative.

Define $Y := \{g \in G \mid gT_\mu\mu(g^{-1}) = T_\mu\}$; clearly Y is a subgroup of G. The previous two paragraphs show that $L \subseteq Y$ and in fact there is an equality. Indeed, the pigeon hole principle together with the fact that $|T_{\mu,n}| > \frac{1}{2}|T_\mu|$ shows that if $g \in Y$, then $gs\mu(g)^{-1} \in T_{\mu,n}$ for some $s \in T_{\mu,n}$.

We have established that L is a group contained in N and it is clear that $T_\mu \leq L$. Hence, in order to show that $[L : T_\mu] \leq c[N : T]$ we only have to prove that $[L \cap T : T_\mu] \leq c$. We showed that if $g \in L$, then $\mu(g)g^{-1}$ is an element of T_μ whose order divides n. The number of elements of T_μ of order dividing n is c, so it will be enough to show that if $t_1, t_2 \in L \cap T$ and $\mu(t_1)t_1^{-1} = \mu(t_2)t_2^{-1}$, then $t_1t_2^{-1} \in T_\mu$. Indeed, since T is abelian the equality $\mu(t_1)t_1^{-1} = \mu(t_2)t_2^{-1}$ implies that $t_1t_2^{-1} = \mu(t_1t_2^{-1})$, i.e., $t_1t_2^{-1} \in T_\mu$. □

Finally, we are ready to prove an analog of Lemma 4.1 for general groups.

Proposition 6.4. *Let m be a prime number. Let H be a finite group containing a normal subgroup G. Fix some $h \in H$ and let n be the order of the automorphism $\mu \in \mathrm{Aut}(G)$ induced by conjugation by h. Let T be a maximal abelian subgroup of G preserved by μ and denote by c the number of elements of T of order dividing n. Assume that:*

1. *m divides $|T_\mu|$,*
2. *$|T_{\mu,n}| \geq \frac{3}{4}|T_\mu|$.*

Then, for $N := N_G(T)$,

$$|\{x^m \mid x \in Gh\}| \leq \left(1 - \frac{1}{4c[N : T]}\right)|G|.$$

Proof. Choose an element $s \in T_\mu$ of order m. If $t \in T$, then $(th)^m = (tsh)^m$ since T is abelian and h commutes with s. Condition 2 implies that the number of elements $t \in T_{\mu,n}$ such that $ts \in T_{\mu,n}$ is at least $\frac{1}{2}|T_\mu|$. This shows that we can choose a set $A \subseteq T_{\mu,n}$ such that:

- The size of A is at least $\frac{1}{4}|T_\mu|$.
- The set $B := \{as \mid a \in A\}$ is contained in $T_{\mu,n}$.
- $A \cap B = \emptyset$.

Choose a set of representatives R for G/L, where L is defined in Lemma 6.3. If $t_1, t_2 \in A \cup B$ and $r_1, r_2 \in R$ satisfy $r_1t_1\mu(r_1^{-1}) = r_2t_2\mu(r_2^{-1})$, then $t_1 = t_2$ and $r_1 = r_2$. The equality $rthr^{-1} = rt\mu(r^{-1})h$ for $t \in T$ and $r \in R$ implies that

$$|\{rthr^{-1} \mid t \in A \cup B \ \wedge \ r \in R\}| = 2|A||R|$$

while

$$|\{(rthr^{-1})^m \mid t \in A \cup B \ \wedge \ r \in R\}| = |\{(rthr^{-1})^m \mid t \in A \ \wedge \ r \ \in R\}| \leq |A||R|.$$

Lemma 6.3 assures that $|R||A| \geq \frac{1}{4c[N:T]}|G|$, so

$$|\{x^m \mid x \in Gh\}| \leq |G| - |A||R| \leq \left(1 - \frac{1}{4c[N:T]}\right)|G|.$$

□

In the following subsections we will verify the conditions of Proposition 6.4 in the case where G is a direct product of finite groups of Lie type.

6.3. **Chevalley groups.** In this subsection we briefly describe the Chevalley groups and their basic properties. More details and proofs can be found in the classical book of Carter [Ca].

Let $\Phi \subseteq \mathbb{R}^l$ be an indecomposable root system and fix a fundamental system of roots $\Pi \subseteq \Phi$. Let $\mathcal{L}$ be the simple Lie algebra over $\mathbb{C}$ associated with Φ. We regard Φ as a subset of $\mathcal{L}$ and for every $r \in \Phi$ we define $h_r := \frac{2r}{(r,r)}$, where $(\cdot,\cdot)$ is the usual scalar product of $\mathbb{R}^l$. Finally we fix a Chevalley basis $\{h_r \mid r \in \Pi\} \cup \{e_r \mid r \in \Phi\}$ of $\mathcal{L}$. The multiplication of $\mathcal{L}$ satisfies:

1. $[h_r h_s] = 0$.
2. $[h_r e_s] = (h_r, s)e_s$.
3. $[e_r e_s] = h_r$ if $r + s = 0$.
4. $[e_r e_s] \in \mathbb{Z}e_{s+r}$ if $r + s \in \Phi$.
5. $[e_r e_s] = 0$ if $r + s \notin \Phi \cup \{0\}$.

In particular, the product of every two elements of the Chevalley basis is a linear combination with rational integer coefficients of the basis elements. Thus, there is a Lie algebra $\mathcal{L}_q$ over $\mathbb{F}_q$ with the same basis as $\mathcal{L}$ and a similar multiplication. The coefficients of the product of elements of the basis in $\mathcal{L}_q$ are equal modulo p to those of the product in $\mathcal{L}$.

The rules of the multiplication also show that for every $r \in \Phi$ the linear map $\operatorname{ad} e_r : \mathcal{L} \to \mathcal{L}$ is nilpotent and so $\exp(t \operatorname{ad} e_r)$ is an automorphism of $\mathcal{L}$ for every $t \in \mathbb{C}$. It turns out that $\exp(t \operatorname{ad} e_r)$ is in fact a finite power series of the form

$$\sum_{0 \leq k \leq n} a_k (t \operatorname{ad} e_r)^k,$$

where $a_k \in \mathbb{Z}$ for $0 \leq k \leq n$. Hence, this power series can be evaluated also for $t \in \mathbb{F}_q$ and the result is an automorphism of $\mathcal{L}_q$ denoted by $x_{r,t}$. The Chevalley group G_q associated to Φ is the subgroup of the automorphism group of $\mathcal{L}_q$ generated by the $x_{r,t}$ for $r \in \Phi$ and $t \in \mathbb{F}_q$.

In the next few paragraphs we will define certain subgroups of G_q. In order to keep the notation simple we will not insert the letter q in the symbols of these subgroups, but the reader should always remember that these groups depend on the group G_q, which in turn depends on q and the root system Φ.

For every root $r \in \Phi$ and an element $t \in \mathbb{F}_q^*$ there is an element $d_{r,t} \in G_q$ which satisfies $d_{r,t}(e_s) = t^{(h_r,s)}e_s$ and $d_{r,t}(h_s) = h_s$ for every $s \in \Phi$. The diagonal subgroup T is the group generated by these elements. The group T is a maximal abelian subgroup and, as the notation suggests, it will play the role of the maximal abelian subgroup of Section 6.1. As before, for an $n \in \mathbb{N}$ denote $T_n := \{t \in T \mid$

$\mathrm{Z}_{G_q}(t^n) = T\}$. Our first goal is to find a sufficient condition for an element of T to belong to T_n.

Every root $s \in \Phi$ can be written in a unique way as $s = \epsilon_s \sum_{r\in\Pi} n_{s,r} r$, where $\epsilon = \pm 1$ and the n_r's are natural numbers. The set of positive roots is $\Phi^+ := \{s \mid \epsilon_s = 1\}$ and the set of negative roots is $\Phi^- := \{s \mid \epsilon_s = -1\}$. The height of a root s is defined to be $\epsilon \sum_{r\in\Pi} n_{s,r}$. Let $\mathcal{L}_q^+$ ($\mathcal{L}_q^-$) be the subspace of $\mathcal{L}$ which is generated by the elements e_r, where r runs over the positive (negative) roots and let $\mathcal{L}_q^0$ be the subspace generated by the h_r, with $r \in \Pi$.

The upper unipotent subgroup U of G_q is the group generated by the elements $x_{r,t}$ for $r \in \Phi^+$ and $t \in \mathbb{F}_q$. Similarly, the lower unipotent subgroup V of G_q is the group generated by the elements $x_{r,t}$ for $r \in \Phi^-$ and $t \in \mathbb{F}_q$.Our first lemma is rather technical.

Lemma 6.5. *If $u \in U$ preserves $\mathcal{L}_q^0$, then u is the identity.*

Proof. Let $u \in U$ be a non-identity element. Fix an ordering $\succ$ of the roots such that $r \succ s$ implies that the height of r is greater than or equal to the height of s. There are unique $t_r \in \mathbb{F}_q$ such that

$$u = \prod_{r\in\Phi^+} x_{r,t_r},$$

where the product in taken in an increasing order of the roots. Let $r^* \in \Phi^+$ be the minimal root with respect to $\succ$ such that $t_{r^*} \neq 0$. The definition of $x_{r,t}$ for $r \in \Phi^+$ and $t \in \mathbb{F}_q$ implies that for $s \in \Phi$:

1. $x_{r,t}(h_s) = h_s - t_r(h_s, r)e_r$.
2. $x_{r,t}(e_s) = e_s + v$, where v is a linear combination of roots with height greater than the height of s.

Thus, $u(h_{r^*}) = h_{r*} - 2t_{r^*}e_{r*} + v$, where v is a linear combination of roots which are greater than r^* ($0 \neq 2 (\mathrm{mod}\, p)$ since $p \geq 5$). □

The last ingredient needed for the proof of Lemma 6.6 is the Bruhat decomposition. The diagonal group T normalizes U and so $B := TU$ is a subgroup of G_q. Let N be the normalizer of T in G; N is called the monomial group. Every $n \in N$ acts as a permutation on the set $\{\mathbb{C}e_r \mid r \in \Phi\}$. This action defines an epimorphism of N onto the Weyl group $W(\Phi)$ with kernel T. For every $w \in W(\Phi)$ choose a representative $n_w \in N$. The Bruhat decomposition says that

$$G_q = \bigcup_{w\in W(\Phi)} Bn_wB,$$

where the union is disjoint.

Lemma 6.6. *Assume that $d \in T$ satisfies:*

1. *If $r \in \Phi$, then $d(e_r) = \lambda_r e_r$, where $\lambda_r \neq 1$.*
2. *If $\lambda_r = \lambda_s$, then $r, s \in \Phi^+$ or $r, s \in \Phi^-$.*

Then T is the centralizer of d.

Proof. Note that $\mathcal{L}_q^0$ is exactly the eigenspace of d with eigenvalue 1. Assume $g \in G_q$ centralizes d. Conditions 1 and 2 imply that g preserves $\mathcal{L}_q^+$. Choose $b_1, b_2 \in B$ and $w \in W(\Phi)$ such that $g = b_1 n_w b_2$. The element $n_w = b_1^{-1} g b_2^{-1}$ also preserves $\mathcal{L}_q^+$ since B does. Thus, $w(\Phi^+) = \Phi^+$ since $n_w(\mathbb{C}e_r) = \mathbb{C}e_{w(r)}$ for every $r \in \Phi$. The

identity is the only element of the Weyl group which preserves Φ^+, so $w = \mathrm{id}$ and $g \in B$. Write $g = cu$ with $c \in T$ and $u \in U$. Since c centralizes d, also u centralizes it. Condition 1 shows that u preserves $\mathcal{L}_q^0$ and so $u = \mathrm{id}$ by Lemma 6.5. □

Corollary 6.7. *Let $n \in \mathbb{N}$. Assume that $d \in T$ satisfies:*

1. *If $r \in \Phi$, then $d(e_r) = \lambda_r e_r$, where $\lambda_r^n \neq 1$.*
2. *If $\lambda_r^n = \lambda_s^n$, then $r, s \in \Phi^+$ or $r, s \in \Phi^-$.*

Then $d \in T_n$.

Now that we have a sufficient criterion for an element to belong to T_n we want to show that a high proportion of the elements of T belong to T_n.

6.4. **Automorphisms of Chevalley groups.** The Chevalley group G_q has a trivial center, so it is isomorphic to the inner automorphism group and we shall identify these two groups. In general, G_q has non-inner automorphisms, which we shall now describe.

Let $\hat{T} \subseteq \mathrm{Aut}(\mathcal{L}_q)$ be the group consisting of automorphisms which have the elements of the Chevalley basis as eigenvectors and act as the identity on $\mathcal{L}_q^0$. The group $\hat{T}$ is abelian, has exponent $q-1$ and contains T. In addition, $\hat{T}$ normalizes G_q, so conjugation by its elements induces automorphisms of G_q. The automorphisms which are induced in this way are called diagonal automorphisms.

The second set of automorphisms are the graph automorphisms. These automorphisms arise from symmetry of the Dynkin diagram of Π. Since p is a prime greater than 3, the only Chevalley groups which have a non-identity graph automorphism are of type A_l for $l \geq 2$, D_l for $l \geq 4$ and E_6. We consider each case separately.

Type A_l with $l \geq 2$: In this case there is only one non-identity symmetry of the graph. The symmetry sends r_i to r_{l-i} for $1 \leq i \leq l$. The graph automorphism α_l associated with this symmetry has order 2, it preserves T and it satisfies $\alpha_l(d_{r_i,t}) = d_{r_{l-i},t}$ for $1 \leq i \leq l$ and $t \in \mathbb{F}_q^*$.

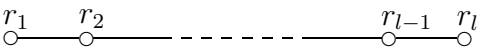

FIGURE 1. Dynkin diagram of type A_l.

Type D_4: For every $\sigma \in \mathrm{Sym}\{1,2,3,4\}$ with $\sigma(1) = 1$, there is a graph symmetry which transforms r_i to $r_{\sigma(i)}$. The graph automorphism δ_σ associated with this symmetry has the same order as σ, it preserves T and it satisfies $\delta_\sigma(d_{r_i,t}) = d_{r_{\sigma(i)},t}$ for $1 \leq i \leq 4$ and $t \in \mathbb{F}_q^*$.

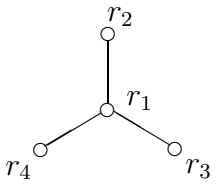

FIGURE 2. Dynkin diagram of type D_4.

Type D_l with $l \geq 5$: In this case there is only one non-identity symmetry of the graph. The symmetry switches between r_{l-1} and r_l and leaves the other fundamental roots fixed. The graph automorphism δ_l associated with this symmetry has order 2, it preserves T and it satisfies $\delta_l(d_{r_i,t}) = d_{r_i,t}$, $\delta_l(d_{r_{l-1},t}) = d_{r_l,t}$ and $\delta_l(d_{r_l,t}) = d_{r_{l-1},t}$ for $1 \leq i \leq l-2$ and $t \in \mathbb{F}_q^*$.

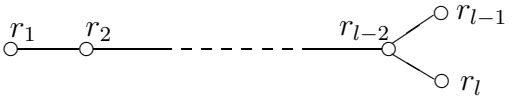

FIGURE 3. Dynkin diagram of type D_l.

Type E_6: Also in this case case there is only one non-identity symmetry of the graph. The symmetry sends r_i to r_{5-i} for $1 \leq i \leq 5$ and leaves r_6 fixed. The graph automorphism ε associated with this symmetry has order 2, it preserves T and it satisfies $\varepsilon(d_{r_1,t}) = d_{r_5,t}$, $\varepsilon(d_{r_2,t}) = d_{r_4,t}$, $\varepsilon(d_{r_3,t}) = d_{r_3,t}$ and $\varepsilon(d_{r_6,t}) = d_{r_6,t}$ for every $t \in \mathbb{F}_q^*$.

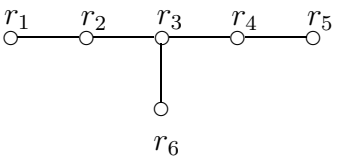

FIGURE 4. Dynkin diagram of type E_6.

The last set of automorphisms is the field automorphisms. Every $\varphi \in \mathrm{Aut}(\mathbb{F}_q)$ induces an automorphism $\bar{\varphi} \in \mathrm{Aut}(G_q)$, which is called a field automorphism, such that $\bar{\varphi}(x_{r,t}) := x_{r,\varphi(t)}$ and $\bar{\varphi}(d_{r,t}) = d_{r,\varphi(t)}$ for every $r \in \Phi$ and $t \in \mathbb{F}_q$.

Lemma 6.8. *Let $r_1, \ldots, r_l$ be the fundamental roots of Φ. Denote $d_t := d_{r_1,t} \cdots d_{r_l,t}$ for every $t \in \mathbb{F}_q^*$. The set $D := \{d_t \mid t \in \mathbb{F}_p^*\}$ is a subgroup of G_q which is pointwise fixed by every diagonal, graph or field automorphism. Furthermore, the size of D is $p-1$.*

Proof. All the assertions follow directly from the definitions except the one about the size of D. If $s \in \Phi$, then $d_t(e_s) = t^{m_s} e_s$, where $m_s := (h_{r_1} + \cdots + h_{r_l}, s)$. Inspection of the Dynkin diagrams of all root systems of rank l shows that there is always a fundamental root s such that $m_s := (h_{r_1} + \cdots + h_{r_l}, s) = -1$, so $d_t(s) = t^{-1}$. This implies that $|D| = p-1$. □

Lemma 6.9. *Fix $n \in \mathbb{N}^+$ and $\alpha \in (0,1)$ and define D as in the above lemma. There exists a constant c such that if $p \geq c$ and H is a subgroup of G_q such that $D \subseteq H \subseteq T$, then $|H_n| \geq \alpha |H|$, where $H_n := \{h \in H \mid \mathrm{Z}_{G_q}(h^n) = T\}$.*

Proof. Let $r_1, \ldots, r_l$ be the fundamental roots of Φ and d_t as in the above lemma. It suffices to show that if p is large enough, then for every $h \in H$ the number of $t \in \mathbb{F}_p^*$ such that $hd_t \in H_n$ is at least $\alpha(p-1)$. Fix $h \in H$ and assume $h(e_s) = \lambda_s e_s$ for every $s \in \Phi$. If $s \in \Phi$, then

$$hd_t(e_s) = \lambda_s t^{m_s} e_s,$$

where $m_s := (h_{r_1} + \cdots + h_{r_l}, s)$. Denote $m := \max |m_s|$, where the maximum is taken over $s \in \Phi$. Lemma 6.6 shows then if $t \in \mathbb{F}_p^*$, then $hd_t \in H_n$ whenever the following two conditions hold:

1. For every $s \in \Phi$ the product $\lambda_s^n t^{nm_s}$ is different from 1.
2. If $s_1 \in \Phi^+$ and $s_2 \in \Phi^-$, then $\lambda_{s_1}^n t^{nm_{s_1}} \neq \lambda_{s_2}^n t^{nm_{s_2}}$.

If $s \in \Phi^+$ ($s \in \Phi^-$), then s is a linear sum of elements of Π, where all the coefficients in this sum are non-negative (non-positive). In addition, the scalar product of any two distinct fundamental roots is non-positive and s cannot be orthogonal to all the fundamental roots. Hence, if $s \in \Phi^+$, then $m_s < 0$ while if $s \in \Phi^-$, then $m_s > 0$. Thus, for $s \in \Phi$ the number of $t \in \mathbb{F}_p^*$ which do not satisfy condition 1 is at most nm. Similarly, for $s_1 \in \Phi^+$ and $s_2 \in \Phi^-$ the number of $t \in \mathbb{F}_p^*$ which do not satisfy condition 2 is at most $2nm$. Therefore, the number of $t \in \mathbb{F}_p^*$ with $hd_t \in H_n$ is at least

$$(p-1) - nm|\Phi| - \frac{nm}{2}|\Phi|^2,$$

which is greater than $\alpha(p-1)$ for large enough p. □

The following is a first step to verify condition 2 of Proposition 6.4.

Corollary 6.10. *Let $n \in \mathbb{N}^+$ and $\alpha \in (0,1)$. There exists a constant w such that for every $p \geq w$ and every $\mu \in \mathrm{Aut}(G_q)$ the following holds:*

If μ stabilizes T and pointwise fixes D, then $|T_{\mu,n}| \geq \alpha |T_\mu|$. In particular, this is true for μ which is a product of field, graph and diagonal automorphisms.

We close this subsection with a further discussion about automorphisms. As before let p be a prime number greater than 3 and let $q := p^k$ for $k \in \mathbb{N}^+$. The group G_q is simple and we regard it as a normal subgroup of its automorphism group. Every automorphism of G_q is a product of the form $\varphi\eta\kappa\iota$, where ι is an inner automorphism, κ is a diagonal automorphism, η a graph automorphism and φ is a field automorphism. In Subsection 6.6 we will need a bound on the order of $\varphi\eta\kappa$, so we investigate this product. Graph and field automorphisms commute and both normalize the group of diagonal automorphisms $\hat{T}_q$. Hence, the order of $\varphi\eta\kappa$ is bounded by the product $\mathrm{ord}(\varphi)\,\mathrm{ord}(\eta)\,\mathrm{ord}(\kappa)$ since the group of diagonal automorphisms $\hat{T}$ is abelian. Thus, it is enough to bound the order of φ, η and κ separately. The order of a graph automorphism is at most 3, while the order of a field automorphism of G_q divides k (since $q = p^k$). However, a diagonal automorphism can have arbitrary large orders if p is large. To overcome this problem we note that $T \subseteq \hat{T}$, so in the presentation of an automorphism as a product $\varphi\eta\kappa\iota$ the diagonal automorphism κ can be replaced by other automorphisms of the coset κT. We need the following group-theoretic lemma:

Lemma 6.11. *Let G be a finite group which contains a normal subgroup H. Then every coset of H in G has a representative g such that every prime divisor of* $\mathrm{ord}(g)$ *also divides* $[G:H]$.

Proof. Let R be a set of representatives for H in G and let t be the largest natural number which divides $|G|$ and is coprime to $[G:H]$. It is enough to show that the set $R^t := \{g^t \mid g \in R\}$ is a set of representatives for H in G. This is true since if L is a finite group and t is coprime to the order of L, then the map $g \mapsto g^t$ is a bijection of L. □

The index $[\hat{T} : T]$ depends on the type of the root system and the field $\mathbb{F}_q$ and it is as follows:

A_l	B_l	C_l	D_l	G_2	F_4	E_6	E_7	E_8
$\gcd(l+1, q-1)$	2	2	$\gcd(4, q^l - 1)$	1	1	$\gcd(3, q-1)$	2	1

Lemma 6.12. *Let $k \in \mathbb{N}^+$ such that $q := p^k$. If $\xi \in \mathrm{Aut}(G_q)$, then there are: a field automorphism φ, a graph automorphism η, a diagonal automorphism κ and an inner automorphism ι such that $\xi := \varphi\eta\kappa\iota$ and the order of $\mu := \varphi\eta\kappa$ divides $6kz$, where z divides $q-1$ and every prime factor of z divides $6(l+1)$.*

Proof. The above discussion implies that it is enough to show that ξ can be written in the form $\xi = \eta\varphi\kappa\iota$ such that $z := \mathrm{ord}(\kappa)$ satisfies the required properties. The order of the elements of $\hat{T}$ divides $q-1$, and Lemma 6.11 shows that κ can be chosen such that the prime factors of its order divide $[\hat{T} : T]$. The above table shows that the primes which divide $[\hat{T} : T]$ also divide $6(l+1)$. □

The point of Lemma 6.12 is that for a given $r \in \mathbb{N}^+$ there is a suitable arithmetic progression $(a + bj)_{j\in\mathbb{N}}$ with coprimes a and b such that if $q = p^k$ where $k \leq r$ and p is a prime which belongs to the arithmetic progression, then the product $\varphi\eta\kappa$ has bounded order.

6.5. **Steinberg groups.** Assume that Φ has a non-trivial symmetry of the Dynkin diagram, i.e., Φ is of one of the types: A_l for $l \geq 2$, $D_l \geq 4$ or E_6. Let $\alpha \in \mathrm{Aut}(G_q)$ be the graph automorphism associated to such a symmetry. Then $\mathrm{ord}(\alpha) = 2$ unless Φ is of type D_4, where it is also possible that $\mathrm{ord}(\alpha) = 3$. Assume $q = p^k$, where $k \in \mathbb{N}^+$ is divisible by $\mathrm{ord}(\alpha)$, and let β be a field automorphism with the same order as α (recall that the automorphism group of $\mathbb{F}_{p^r}$ is cyclic of order r). Let $U_\gamma(V_\gamma)$ be the subgroup of the unipotent group U (V) of the elements fixed by $\gamma := \alpha\beta$. The Steinberg group G_q^* of type Φ over $\mathbb{F}_q$ is the subgroup of G_q generated by U_γ and V_γ. The group G_q^* is fixed by γ but it can be properly contained in the subgroup of fixed points. Note that for $p \geq 5$ the Steinberg groups are only defined when the root system is of type A_l for $l \geq 2$, $D_l \geq 4$ or E_6 and there is a field automorphism of $\mathbb{F}_q$ of the same order as a non-trivial graph automorphism. If Φ is of a type different than D_4, then there is just one non-trivial graph automorphism and its order is 2, so G_q^* is uniquely defined and q is a square. On the other hand, if the type is D_4, then there are 3 non-trivial graph automorphisms of order 2 and 2 graph automorphisms of order 3. However, it is easily verified that up to isomorphism the Steinberg group depends only on the order of the graph automorphism. Thus, if 6 divides k and $q = p^k$ the symbol G_q^* can represent two different Steinberg groups. This will not cause us problems since both groups share the properties we are concerned with.

A common notation for the Steinberg groups is ${}^2A_l(q^2)$, ${}^2D_l(q^2)$, ${}^3D_4(q^3)$ and ${}^2E_6(q^2)$, where for instance ${}^3D_4(q^3)$ is the Steinberg group corresponding to the graph automorphism of order 3 of G_{q^3}. We prefer not to use this notation since our arguments do not depend on the type of the root system. On the other hand, our arguments will depend on the fact that the Steinberg groups are subgroups of the Chevalley groups and the symbol G_q^* emphasizes this.

Let G_q^* be a Steinberg subgroup. Define $T^* := T \cap G_q^*$ and $N^* := N \cap G_q^*$, where T and N are the subgroups of G_q defined above. The proof of theorem 13.7.2 in [Ca] shows that D is a subgroup of T^*, where D is defined in Lemma 6.8. If p is large

enough, then Corollary 6.10 shows that D contains an element whose centralizer is T, so T^* is a maximal abelian subgroup of G_q^*. In turn, Lemma 6.2 implies that $N^* = N_{G_p^*}(T^*)$. In particular, we have $[N_{G_p^*}(T^*) : T^*] \leq [N : T] = |W(\Phi)|$, where $W(\Phi)$ is the Weyl group of Φ.

Next, we want to discuses the automorphisms of the Steinberg group G_q^* (see [St]). The group G_q^* has a trivial center (since $p \geq 5$), so we can view it as a subgroup of its automorphism group. The group of diagonal automorphisms $\hat{T}^*$ of G_q^* consists of the restrictions of the automorphisms which belong to $\hat{T}$ and stabilize G_q^*. Note that diagonal automorphisms of G_q^* fix T^* pointwise. The field automorphisms of G_q^* are the restrictions of the field automorphisms of G_q; they also stabilize T^*. Lemma 6.9 gives an analog of Corollary 6.10:

Corollary 6.13. *Let $n \in \mathbb{N}^+$ and $\alpha \in (0,1)$. There exists a constant c such that for every $p \geq c$ and every $\mu^* \in \mathrm{Aut}(G_q^*)$ the following holds:*

If μ^* stabilizes T^* and pointwise fixes D, then $|T^*_{\mu^*,n}| \geq \alpha |T^*_{\mu^*}|$. In particular, this is true for μ which is a product of field and diagonal automorphisms.

As for Chevalley groups, every automorphism of G_q^* is a product of the form $\varphi\kappa\iota$, where ι is an inner automorphism, κ is a diagonal automorphism and φ is a field automorphism (there in no need for graph automorphisms). Note that this fact does not follow directly from the equivalent fact for Chevalley groups and requires a separate proof, which can be found in [St]. The index of T^* in $\hat{T}^*$ is given in the following table:

${}^2A_l(q^2)$	${}^2D_l(q^2)$	${}^3D_4(q^3)$	${}^2E_6(q^2)$
$\gcd(l+1, q+1)$	$\gcd(4, q^l+1)$	1	$(3, q+1)$

We get an analog of Lemma 6.12:

Lemma 6.14. *Let $k \in \mathbb{N}^+$ such that $q = p^k$. If $\xi \in \mathrm{Aut}(G_q^*)$, then there are: a field automorphism φ, a diagonal automorphism κ and an inner automorphism ι such that $\xi := \varphi\kappa\iota$ and the order of $\mu^* := \varphi\kappa$ divides kz, where z divides $q-1$ and every prime factor of z divides $6(l+1)$.*

With the notation as above, we conclude:

Corollary 6.15. *Let $d \in \mathbb{N}^+$ and fix a prime number m. Assume that p is a large enough prime which belongs to the arithmetic progression $(a+bj)_{j\in\mathbb{N}}$ and $q = p^k$ for $k \leq d$, where $a := 1 + 6m(l+1)^2 d!^2$ and $b := 36m^2(l+1)^4 d!^4$. Then for every $\xi \in \mathrm{Aut}(G_q)$ and every $\xi^* \in \mathrm{Aut}(G_q^*)$ there are $\iota \in \mathrm{Inn}(G_q)$, $\iota^* \in \mathrm{Inn}(G_q^*)$, $\mu \in \mathrm{Aut}(G_q)$ and $\mu^* \in \mathrm{Aut}(G_q^*)$ such that:*

1. *$\xi = \mu\iota$ and $\xi^* = \mu^*\iota^*$.*
2. *$\mu(T) = T$ and $\mu^*(T^*) = T^*$.*
3. *Both μ and μ^* pointwise fix D.*
4. *m divides the order of D.*
5. *$\mathrm{ord}(\mu)$ and $\mathrm{ord}(\mu^*)$ divide $216(l+1)^3 d!^4$.*

Proof. Fix ξ and ξ^* and assume that $q = p^k$ for $k \leq d$. Lemmas 6.12 and 6.14 show that we can find $\iota \in \mathrm{Inn}(G_q)$, $\iota^* \in \mathrm{Inn}(G_q^*)$, $\mu \in \mathrm{Aut}(G_q)$ and $\mu^* \in \mathrm{Aut}(G_q^*)$ such that conditions 1,2,3 hold and the orders of μ and μ^* divide $6zk$, where z divides $q-1$ and every prime factor of z divides $6(l+1)$. The above arithmetic progression implies that

$$q - 1 = p^k - 1 \equiv 6mk(l+1)^2 d!^2 \pmod{36m^2(l+1)^4 d!^4}.$$

Thus, z divides $6mk(l+1)^2 d!^2$, so it also divides $36(l+1)^3 d!^3$. It follows that $\mathrm{ord}(\mu)$ and $\mathrm{ord}(\mu^*)$ divide $216(l+1)^3 d!^4$. Finally, the size of D is $p-1$, which is divisible by m. □

6.6. **Powers in extensions of finite simple groups of Lie type.** The main goal of this section is to prove Theorem 6.16 below. We start this section with a general discussion about powers in extension of finite groups. Let H be a finite group. Let G be a normal subgroup of H with a trivial center. Let K be a coset of G in H. Our goal is to bound the size of $\{k^m \mid k \in K\}$ for some $m \in \mathbb{N}^+$. Fix some $k \in K$ and let $\zeta \in \mathrm{Aut}(G)$ be the automorphism induced by conjugation by k. Then

$$|\{k^m \mid k \in K\}| = |\{(g\zeta)^m \mid g \in G\}|,$$

where in the right side G is viewed as a subgroup of $\mathrm{Aut}(G)$. Hence, we only have to deal with groups of the latter form, i.e., the case where $H = \mathrm{Aut}(G)$.

Next, we focus on the case $G = S^r$, where S is a non-abelian finite simple group and $r \in \mathbb{N}^+$. Every automorphism ζ of the direct product S^r is of the form:

$$\zeta(s_1, \dots, s_r) = (\xi_1(s_{\sigma(1)}), \dots, \xi_r(s_{\sigma(r)})) \tag{6}$$

where $\xi_1, \dots, \xi_r \in \mathrm{Aut}(S)$ and $\sigma \in \mathrm{Sym}(r)$. Every permutation is a product of disjoint cycles; say, σ is a product of k cycles of lengths $r_1, \dots, r_k$. By renumbering the copies of S^r and using the isomorphism $S^r \simeq S^{r_1} \times \cdots \times S^{r_k}$ we can assume that there are $\zeta_i \in \mathrm{Aut}(S^{r_i})$ and $\xi_{i,j} \in \mathrm{Aut}(S)$ for $1 \le i \le k$ and $1 \le j \le r_i$ such that

$$\zeta(\bar{s_1}, \dots, \bar{s_k}) = (\zeta_1(\bar{s}_1), \dots, \zeta_k(\bar{s}_k))$$

and

$$\zeta_i(s_{i,1}, \dots, s_{i,r_i}) = (\xi_{i,1}(s_{i,\sigma_i(1)}), \dots, \xi_{i,r_i}(s_{i,\sigma_i(r_i)})),$$

where $\bar{s}_i = (s_{i,1}, \dots, s_{i,r_i}) \in S^{r_i}$ and $\sigma_i = (r_i\ r_{i-1} \cdots 2\ 1) \in \mathrm{Sym}(r_i)$. Note that if

$$|\{(\bar{s}_1\zeta_1)^m \mid \bar{s}_1 \in S^{r_1}\}| \le c|S|^{r_1}$$

for some constant $c > 0$, then also

$$|\{(\bar{s}\zeta)^m \mid \bar{s} \in S^r\}| \le c|S|^r.$$

This allows us to restrict to the case where σ is a cyclic permutation.

Finally, let $\zeta \in \mathrm{Aut}(S^r)$ as in equation (6), where σ is the permutation $(r \cdots 1)$. Denote $\chi := (\rho_1, \rho_2, \dots, \rho_r) \in \mathrm{Aut}(S^r)$, where $\rho_j := \xi_j \cdots \xi_2$ for $j \ge 2$ and $\rho_1 := \mathrm{id}$. Conjugation by χ allows us to replace ζ with $\chi^{-1}\zeta\chi$, i.e. to assume that we have $\xi_2 = \cdots = \xi_r = \mathrm{id}$.

The main theorem of this section is:

Theorem 6.16. *Let $d, l, r \in \mathbb{N}^+$ be constants. There is a constant $c \in \mathbb{N}^+$ such that for every number $m \ge 2$ the following claim holds:*

Let $p \ge c$ be a prime which belongs to the arithmetic progression $(a + bj)_{j \ge 1}$, where

$$a := 1 + 6m(l+1)^2 d!^2 \text{ and } b := 36m^2(l+1)^4 d!^4.$$

Let Γ be a finite group with a non-trivial normal subgroup Λ. Furthermore, assume that Λ is isomorphic to a product of at most r finite quasi-simple groups of Lie type

(not necessarily of adjoint type) of rank at most l over extensions of $\mathbb{F}_p$ of degree at most d. Then for every coset Ψ of Λ the following inequality holds:

$$|\{g^m \mid g \in \Psi\}| \leq \left(1 - \frac{1}{4n^r {C_l}^r}\right)|\Psi|,$$

where $n := 216(l+1)^3 d!^4$ and C_l is the maximal size of a Weyl group of rank l.

Proof. We start with some reductions. The group Λ has a subgroup N normal in Γ such that Λ/N is isomorphic to a product of isomorphic finite simple Lie groups of adjoint type. We replace Λ with this quotient. We focus on the case where the finite simple Lie group is a Steinberg group G_q^* of type Φ over $\mathbb{F}_q$ with $q := p^d$ and $\Lambda = (G_q^*)^r$. The proofs of the other cases are similar. Furthermore, we can assume that m is a prime number.

Define $n = 216r(l+1)^3 d!^4$. Corollary 6.13 allows us to choose a constant c such that if p belongs to the above arithmetic progression, then $|T_{\mu^*,n}| \geq \frac{3}{4}^{\frac{1}{r}} |T_{\mu^*}|$ for every $\mu^* \in \mathrm{Aut}(G_q^*)$ which stabilizes T and pointwise fixes D. We can further assume that c is large enough so that T^* is a maximal abelian subgroup of G_q^* and $N_{G_{q^*}}(T^*) = N^*$.

The discussion before the proof shows that it is enough to deal with the case $\Gamma = \mathrm{Aut}(\Lambda)$ and $\Psi = \Lambda\zeta^*$, where

$$\zeta^*(s_1, \ldots, s_r) = (\xi^*(s_r), s_1, \ldots, s_{r-1})$$

for some $\xi^* \in \mathrm{Aut}(G_q^*)$. Corollary 6.15 allows us to replace ζ^* with some representative of $\Lambda\zeta^*$ such that the new representative, still denoted by ζ^*, satisfies

$$\zeta^*(s_1, \ldots, s_r) = (\mu^*(s_r), s_1, \ldots, s_{r-1}),$$

where $\mu^* \in \mathrm{Aut}(G_q^*)$ satisfies conditions 2, 3, 4 and 5 of that corollary. This implies that the order of ζ^* divides n.

We are in a position to verify that the requirements of Proposition 6.4 are fulfilled. The group $\tilde{T} := (T^*)^r$ is a maximal abelian subgroup of Λ and its normalizer is $\tilde{N} := N_\Lambda(\tilde{T}) = (N^*)^r$. In particular, $[\tilde{N} : \tilde{T}] \leq |W(\Phi)|^r$. Note that $\tilde{T}_{\zeta^*,\mathrm{ord}(\zeta^*)} \supseteq \tilde{T}_{\zeta^*,n}$ since $\mathrm{ord}(\zeta^*)$ divides n. Thus,

- $|\tilde{T}_{\zeta^*,\mathrm{ord}(\zeta^*)}| \geq \frac{3}{4}|\tilde{T}_{\zeta^*}|$ since $\tilde{T}_{\zeta^*} = (T_{\mu^*})^r$ and $\tilde{T}_{\zeta^*,n} = (T^*_{\mu^*,n})^r$.
- m divides the order of $\tilde{T}_{\zeta^*}$ since it contains the subgroup D^r and m divides $|D|$.

Proposition 6.4 together with the last two points shows that

$$|\{g^m \mid g \in \Psi\}| \leq \left(1 - \frac{1}{4c_n|W(\Phi)|^r}\right)|\Psi|,$$

where c_n is the number of elements of $\tilde{T}$ such that their orders divide n. However, $\tilde{T} = (T^*)^r \subseteq T^r \subseteq \hat{T}^r \simeq (\mathbb{F}_q^*)^r$, where $\mathbb{F}_q^*$ is the multiplicative group of $\mathbb{F}_q$, so $c_n \leq n^r$. □

The next corollary is stated with the notation of Proposition 3.7.

Corollary 6.17. *For every $n \geq 2$ there is a constant c for which the following claim holds:*

Let Γ be a subgroup of $\mathrm{GL}_n(\mathbb{Q})$ such that its Zariski-closure is semisimple. Let $k \in \mathbb{N}^+$ be large enough and let $2 \leq m \leq k^2$. Then there are two coprime natural numbers $2 \leq a, b \leq k^5$ such that for every prime p which belongs to the arithmetic

progression $(a + bj)_{j\geq 1}$ *and every two cosets* $C, D \in \Gamma_p/\Lambda_p$*, the size of* $\{g^m \mid g \in D\} \cap C$ *is at most* $(1 - c)|\Lambda_p|$.

Acknowledgments

The authors are grateful to the ERC and the ISF for partial support. They also want to thank Emmanuel Breuillard, Dorian Goldfeld, Emmanuel Kowalski and Ron Peled for useful conversations.

References

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

[BG2] 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)

[BG3] J. Bourgain and A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$.II. With an appendix by Bourgain. J. Eur. Math. Soc. (JEMS) 11 (2009), no. 5, 1057–1103. MR2538500 (2011a:60021)

[BGS1] 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)

[BGS2] J. Bourgain, A. Gamburd and P. Sarnak, *Generalization of Selberg's* 3/16 *Theorem and Affine Sieve*, arXiv:0912.5021

[BGT] E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal. 21 (2011), no. 4, 774–819. MR2827010

[Ca] R.W. Carter, *Simple groups of Lie type.* Pure and Applied Mathematics, Vol. 28. John Wiley & Sons, London-New York-Sydney, 1972. viii+331 pp. MR0407163 (53:10946)

[CvdDM] Z. Chatzidakis, L. van den Dries and A. Macintyre, *Definable sets over finite fields.* J. Reine Angew. Math. 427 (1992), 107–135. MR1162433 (94c:03049)

[Da] H. Davenport, *Multiplicative number theory, Second edition*, Revised by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York-Berlin, 1980. xiii+177 pp. MR606931 (82m:10001)

[FHJ] M.D. Fried, D. Haran, and M. Jarden, *Effective counting of the points of definable sets over finite fields.* Israel J. Math. 85 (1994), no. 1-3, 103–133. MR1264342 (95k:12016)

[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)

[Go] E.S. Golod, *On nil-algebras and finitely approximable p-groups.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964), 273–276. MR0161878 (28:5082)

[GS] E.S. Golod and I.R. Shafarevich, *On the class field tower.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964), 261–272. MR0161852 (28:5056)

[He] 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)

[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)

[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.

[Ko] 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)

[Lu1] 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)

[Lu2] A. Lubotzky, *Expander Graphs in Pure and Applied Mathematics.* Bull. Amer. Math. Soc. 49 (2012), 113–162.

[LuMa] A. Lubotzky and A. Mann, *On groups of polynomial subgroup growth.* Invent. Math. 104 (1991), no. 3, 521–533. MR1106747 (92d:20038)

[LuMe1] A. Lubotzky and C. Meiri, *Sieve methods in group theory II: The Mapping Class Group*, Geometriae Dedicata, to appear, arXiv:1104.2450 .

[LuMe2] A. Lubotzky and C. Meiri, *Sieve methods in group theory III*: $\mathrm{aut}(F_n)$, arXiv:1106.4637v1.

[LMR] A. Lubotzky, S. Mozes and M.S. Raghunathan, *The word and Riemannian metrics on lattices of semisimple groups.* Inst. Hautes Études Sci. Publ. Math. No. 91 (2000), 5–53 (2001). MR1828742 (2002e:22011)

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

[LW] S. Lang and A. Weil, *Number of points of varieties in finite fields.* Amer. J. Math. 76, (1954). 819–827. MR0065218 (16:398d)

[Mah] J. Maher, *Random walks on the mapping class group*, Duke Math. J. 156 (2011), no. 3, 429–468. MR2772067

[Mal] A.I. Mal′cev, *Homomorphisms onto finite groups.* Ivanov. Gos. Ped. Inst. Uchen. Zap. Fiz-Mat. Nauki 8 (1958), 49–60.

[Mi] J.S. Milne, *Algebraic number Theory.* Online: www.jmilne.org/math/CourseNotes/.

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

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

[Ri] 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)

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

[St] R. Steinberg, *Automorphisms of finite linear groups.* Canad. J. Math. 12 (1960), 606–615. MR0121427 (22:12165)

[Va] P. Varju, *Expansion in* $SL_d(O_K/I)$*, I square-free.* arXiv:1001.3664v1.

[We] 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)

Einstein Institute of Mathematics, Hebrew University, Jerusalem 90914, Israel
E-mail address: alexlub@math.huji.ac.il

Einstein Institute of Mathematics, Hebrew University, Jerusalem 90914, Israel
Current address: Institute for Advanced Study, Princeton, New Jersey 08540
E-mail address: chen7meiri@gmail.com