UNIVERSITY OF CALIFORNIA, SAN DIEGO

"Super-approximation" in Absolutely Almost Simple Groups Over the Field of Rational Functions with Coefficients in a Finite Field

A Dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Brian M. Longo

Committee in charge:

Professor Alireza Salehi Golsefidy, Chair
Professor Ronald Graham
Professor Schahar Lovett
Professor Jacques Verstraete
Professor Efim Zelmanov

2016

The Dissertation of Brian M. Longo is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

_____

_____

_____

_____

_____

Chair

University of California, San Diego

2016

DEDICATION

For Auntie.

EPIGRAPH

Do not fear the shrouded path.

The truth lies in darkness.

—Zed

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I must extend my gratitude to my advisor, Professor Alireza Salehi Golsefidy for the absolutely incredible amount of time he has spent teaching me over the years. His dedication to teaching is unbelievable, and at times he certainly met me more than halfway. I have yet to encounter any concept in math that he cannot explain on the spot. I would not have learned nearly half as much, nor would I have been half as motivated without him as a constant source of inspiration, encouragement, and frankly, a healthy amount of fear.

I also thank my family for their love and support over the years, even though I was often too stubborn to accept it. I am grateful for Cal Spicer, Daniel Smith, Zoe Smith, and Shaunak Das for often provideding useful and coherent insights into the world of algebraic geometry. I am also grateful for David Zimmermann and François Thilmany spent a considerable amount of time helping me edit this dissertation.

My good friends have played a large part in helping me stay sane during my graduate career. I thanks the following people for their friendship: Joe, Cesar, Hooman, David, Pandy, Wandy, Helen, James, Franklin, Mark, Janine, Janina and Corey. I owe Victoria Curreri and Susan Elle a debt of gratitude that I simply cannot repay.

Robert Won is the Ash Ketchum to my Gary Oak. He is the Hubert Farnsworth to my Ogden Wernstrom. He is the Ralph Macchio to my William Zabka. I have purposefully made this dissertation one page shorter than his, just so he can have the pleasure of one-upping me one last time. Cheers, friend.

Sa wakas, salamat si Mer, ang magandang babae ko. Dinala siya ako mas kaligayahan kaysa karapat-dapat ako. Mahal Kita.

I also extend my gratitude Peter Varjú for providing useful insights and advice for altering his product theorem for our purposes.

Chapter 3 contains material coauthored by Professor Alireza Salehi Golsefidy and is in preparation for publication under the title ""Super-approximation" in Absolutely Almost Simple Groups Over $\mathbb{F}_q(t)$". The author of this dissertation is a primary researcher and a primary author of the paper mentioned above.

Chapter 4 contains material coauthored by Professor Alireza Salehi Golsefidy and is in preparation for publication under the title ""Super-approximation" in Absolutely Almost Simple Groups Over $\mathbb{F}_q(t)$". The author of this dissertation is a primary researcher and a primary author of the paper mentioned above.

Chapter 5 contains material coauthored by Professor Alireza Salehi Golsefidy and is in preparation for publication under the title ""Super-approximation" in Absolutely Almost Simple Groups Over $\mathbb{F}_q(t)$". The author of this dissertation is a primary researcher and a primary author of the paper mentioned above.

VITA

2011	B. S. in Mathematics *summa cum laude*, University of California, Santa Cruz
2011-2016	Graduate Teaching Assistant, University of California, San Diego
2015	M. S. in Mathematics, University of California, San Diego
2015	C. Phil. in Mathematics, University of California, San Diego
2015	Graduate Associate Instructor, University of California, San Diego
2016	Ph. D. in Mathematics, University of California, San Diego

ABSTRACT OF THE DISSERTATION

"Super-approximation" in Absolutely Almost Simple Groups Over the Field of Rational Functions with Coefficients in a Finite Field

by

Brian M. Longo

Doctor of Philosophy in Mathematics

University of California, San Diego, 2016

Professor Alireza Salehi Golsefidy, Chair

Let p be a prime number greater than 5, and let q_0 be a fixed power of p. Let $\mathbb{F}_{q_0}(t)$ be the field of rational functions with coefficients in the finite field $\mathbb{F}_{q_0}$ of order q_0. Let $\Omega \subset \mathrm{GL}_n(\mathbb{F}_{q_0}(t))$ be a finite symmetric set and let Γ be the group generated by Ω. Suppose the Zariski closure, $\mathbb{G}$, of Γ is absolutely almost simple and simply connected, and that the ring generated by the set $\mathrm{Tr}(\mathrm{Ad}\,\Gamma)$ is all of $\mathbb{F}_{q_0}[t, 1/Q_0]$ where Q_0 is a common denominator of the entries of the matrices in Ω. Then there exists a

positive constant $\varepsilon > 0$ depending only on $\mathbb{G}$ such that the set of Cayley graphs,

$$\{\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega))\},$$

forms a family of ε-expander graphs as Q ranges through a suitable subset of the square free polynomials that are coprime to Q_0.

Chapter 1

Introduction

Let k be a positive integer. Let $\mathcal{G}$ be a finite, undirected, k-regular graph with vertex set $V(\mathcal{G})$ and edge set $E(\mathcal{G})$. For any two vertices v and w of $\mathcal{G}$, we say $w \sim v$ if and only if w is connected to v. For two subsets A and B of the vertices of $\mathcal{G}$, let

$$E(A, B) = \{e = \{v_1, v_2\} \in E(\mathcal{G}) | v_1 \in A,\ v_2 \in B\}$$

be the set of edges between A and B. Define the **Cheeger constant**, $h(\mathcal{G})$, of $\mathcal{G}$ by

$$h(\mathcal{G}) = \min_{\emptyset \neq X \subset V(\mathcal{G})} \frac{|E(X, V(\mathcal{G}) \setminus X)|}{\min\{|X|, |V(\mathcal{G}) \setminus X|\}}.$$

The Cheeger constant of a graph gives us a way to quantify the connectivity of a regular graph.

Definition 1. Let ε be a positive real number. Then $\mathcal{G}$ is called an **ε-expander graph** if $h(\mathcal{G}) > \varepsilon$. A family of regular graphs, $\{\mathcal{G}_i\}_{i \in I}$, is called a **family of ε-expander graphs**, or simply a **family of ε-expanders**, if $\inf_{i \in I} h(\mathcal{G}_i) > \varepsilon$. That is,

if the Cheeger constants $h(\mathcal{G}_i)$ are uniformly bounded away from zero by ε.

The notion of an expander graph was originally defined by Pinsker [Pin73] and who studied these graphs with applications in computer science. The notion of expander graphs has since gained popularity due to its wide reaching applications in both pure and applied mathematics. For an overview of expander graphs see [HLW06] and [Lub12].

1.1 Expander graphs and random walks

For our purposes, it will be more convenient to interpret the notion of ε-expander graphs in terms of random walks on the graphs. Let k be a fixed positive integer and let $\mathcal{G}$ be a finite k-regular undirected graph on n vertices. Fix an ordering $\{v_1, \ldots, v_n\}$ of the vertices of $\mathcal{G}$ and let $A_{\mathcal{G}} = (a_{i,j})$ be the corresponding **adjacency matrix** of $\mathcal{G}$. That is, $A_{\mathcal{G}}$ is the $n \times n$-matrix whose entry in the (i, j) position is equal to $|E(v_i, v_j)|$. We often view the matrix $\frac{1}{|V(\mathcal{G})|} A_{\mathcal{G}}$ as a linear operator $\mathrm{Ave}_{\mathcal{G}}$ on the space $L^2(V(\mathcal{G}))$ of real valued functions on the vertices of $\mathcal{G}$ by fixing the ordered basis $\{\delta_{v_i}\}_{i=1}^n$ of $L^2(V(\mathcal{G}))$, where for each $i = 1, \ldots n$, δ_{v_i} is the Kronecker delta function supported on v_i,

$$\delta_{v_i}(v) = \begin{cases} 1 & \text{if } v = v_i \\ 0 & \text{if } v \neq v_i. \end{cases}$$

The action of $\mathrm{Ave}_{\mathcal{G}}$ can be described by the formula

$$\mathrm{Ave}_{\mathcal{G}} f(v) = \frac{1}{|V(\mathcal{G})|} \sum_{w \sim v} f(w), \ \forall v \in V(\mathcal{G}), \ f \in L^2(V(\mathcal{G})).$$

In other words, $\mathrm{Ave}_{\mathcal{G}} f(v)$ is the average of f on the neighbors of v. For this reason, we call $\mathrm{Ave}_{\mathcal{G}}$ the **averaging operator** on $L^2(V(\mathcal{G}))$. Since $\mathcal{G}$ is undirected and k-regular, one sees that $\mathrm{Ave}_{\mathcal{G}}$ is a real, self adjoint operator. Therefore, $\mathrm{Ave}_{\mathcal{G}}$ has real eigenvalues

$$-1 \leq \lambda_{n-1} \leq \lambda_{n_2} \leq \cdots \leq \lambda_1 \leq \lambda_0 \leq 1.$$

It is easy to see (see for example [Chu97, Lem. 1.7]) that

1. $\lambda_0 = 1$ with corresponding eigenfunction $\mathbb{1}_{V(\mathcal{G})}$, where $\mathbb{1}_{V(\mathcal{G})}(v) = 1$ for all $v \in V(\mathcal{G})$.

2. $\lambda_1 < 1$ if and only if $\mathcal{G}$ is connected,

3. $\lambda_{n-1} = -1$ if and only if $\mathcal{G}$ is bipartite.

Keeping in mind that $h(\mathcal{G})$ quantifies the "connectedness" of $\mathcal{G}$, property 2 indicates a relationship between the spectrum of $\mathrm{Ave}_{\mathcal{G}}$ and $h(\mathcal{G})$. To understand this connection, we introduce the notion of a **uniform random walk** on $\mathcal{G}$.

Definition 2. [Chu97, §1.5] An **ℓ-step walk** w on $\mathcal{G}$ is a set of vertices $\{w_i\}_{i=1}^{\ell}$ with the property that $w_i \sim w_{i+1}$ for each $i = 1, \ldots, \ell$. A random walk on $\mathcal{G}$ is determined by the transitional probabilities $\mathbb{P}(w_{i+1} = u | w_i = v) = 1/k$.

A random walk on $\mathcal{G}$ is a Markov chain with Markov transition matrix $\mathrm{Ave}_{\mathcal{G}}$. In the special case that $\mathcal{G}$ is connected and nonbipartite, any random walk w with initial probability distribution μ converges to the uniform distribution and the speed of convergence is dictated by $\lambda_{\mathcal{G}} = \max_{i=0,\ldots,n-1:|\lambda_i|\neq 1}\{|\lambda_i|\}$. Note, however, that no random walk starting at a given vertex v on a bipartite graph can converge to the uniform distribution since consecutive steps in any walk lie in opposite of the

bipartition. Similary, no random walk starting at a given vertex v on a disconnected graph converges to the uniform probability measure since any step of a random walk on a disconnected graph is fully supported on only one connected component. For this reason, we will mainly focus on connected, nonbipartite graphs.

It is intuitively clear that if the graph $\mathcal{G}$ is "highly connected", then a random walk on $\mathcal{G}$ should equidistribute quickly since there are many ways to get from any one vertex to another. In other words, one should expect that if $h(\mathcal{G})$ is large, then $\lambda_{\mathcal{G}}$ is small. Figure 1.1 illustrates this principle. The diagram in Figure 1.1 shows the first four steps of a uniform random walk starting at the top vertex. The number in each vertex is the probability of landing on that vertex after a uniform random walk of the indicated number of steps. The graph on the left is cyclic while the graph on the right is complete. In this case, we see that after four steps the probability of landing at any given vertex after a four step uniform random walk on the complete graph is much closer to $1/5$ than on the cyclic graph.

In either of the cases in Figures 1.2 and 1.3, the l-step of a random walk cannot converge to equidistribution as l tends towards infinity.

In fact, the condition that $\mathcal{G}$ is an ε-expander graph is equivalent to the existence of a gap is the spectrum of the averaging operator. More precisely, a k-regular graph $\mathcal{G}$ is an ε-expander graph for some positive constant ε if and only if $\lambda_{\mathcal{G}} < 1 - \varepsilon'$ for some positive constant ε' (see [Dod84], [Alo86], [AM85]).

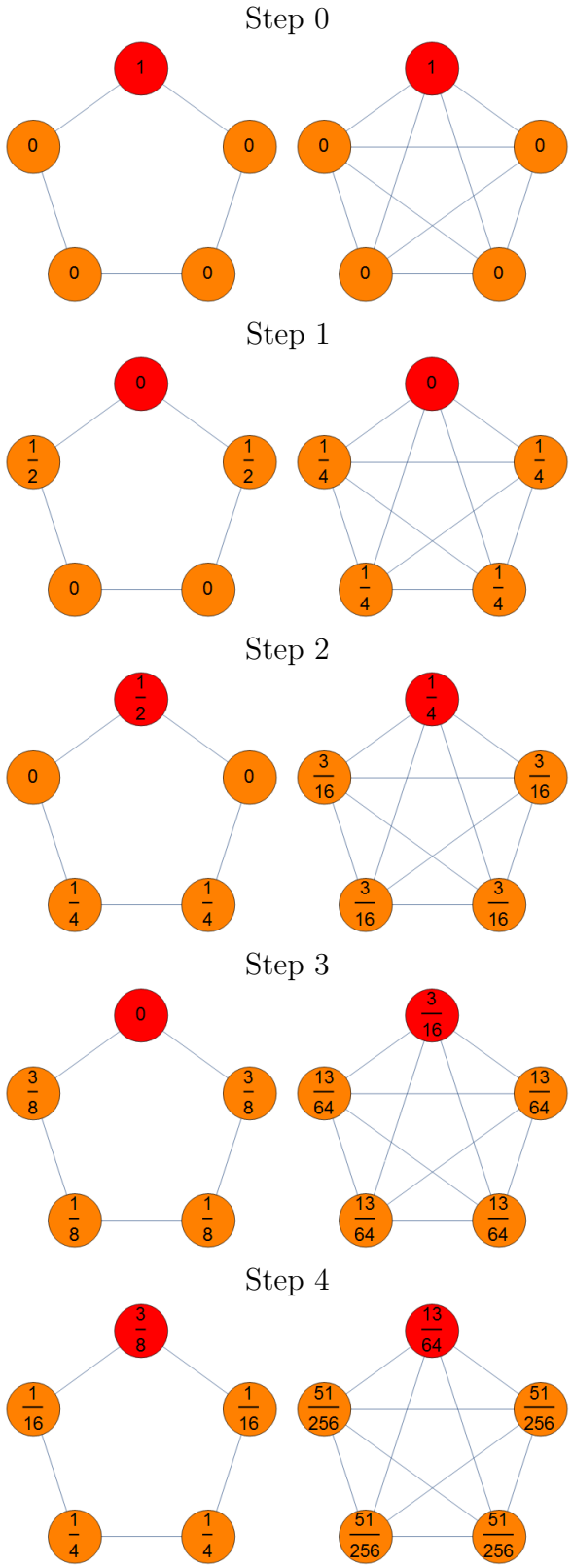


Figure 1.1: Connectivity and equidistribution of random walks

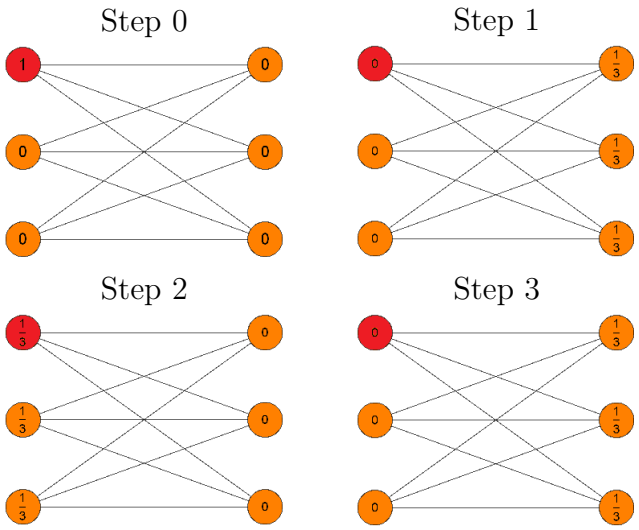


Figure 1.2: Random walk on a bipartite graph

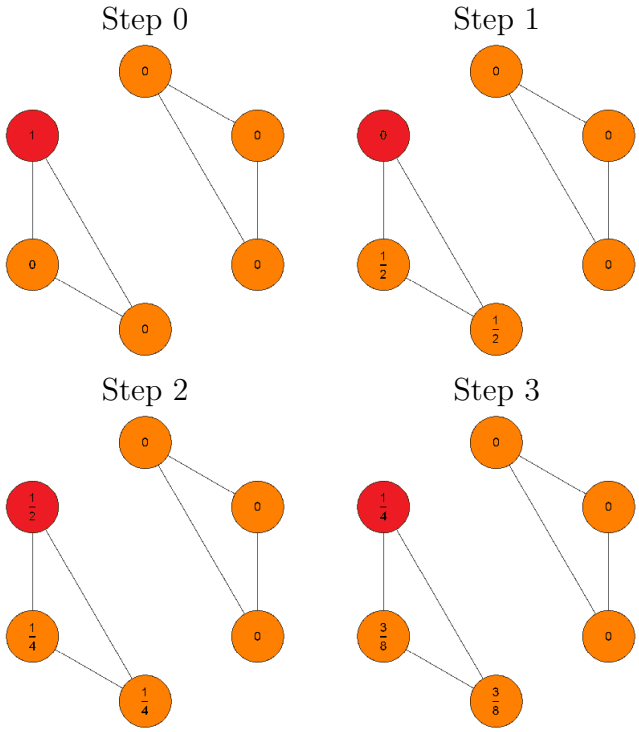


Figure 1.3: Random walk on a disconnected graph

1.2 Examples of families of k-regular ε-expander graphs

We consider the case where $\{\mathcal{G}_i\}_{i\geq 1}$ is a family of k-regular graphs where the sequence of positive integers $\{V(\mathcal{G}_i)\}_{i\geq 1}$ tends to infinity. It seems counter intuitive that any such family of graphs could be a family of expanders. On the one hand, we require that each graph has a high degree of connectivity, but on the other hand we are requiring the graph to be very sparse in the sense that each vertex has a bounded number of neighbors. However, the work of Pinsker [Pin73] and of Barzdin-Kolmogorov [BK67] provides a random model of k-regular graphs with the property that there exists a positive constant ε such that these graph are asymptotically almost surely ε-expanders. Historically, explicit examples of families of expander graphs have been difficult to construct. The earliest constructions, which are due to Margulis, arose as Cayley-Schreier graphs of lattices of Lie groups of higher rank. Let us state the following definitions:

Definition 3 (Cayley-Schreier Graphs)**.** Let G be a finite group, H a subgroup of G, and Ω a symmetric subset of G. The **Cayley-Schreier graph**, $\mathrm{Sch}(G, H, \Omega)$, of G with respect to H and Ω is defined to be the graph whose vertices coincides with the coset space G/H, where the vertices gH and $g'H$ are connected exactly when there exists an element $\omega \in \Omega$ satisfying $gH = \omega g'H$. The **Cayley** graph, $\mathrm{Cay}(G, \Omega)$, of G with respect to Ω is defined to be $\mathrm{Sch}(G, \langle id \rangle, \Omega)$.

Definition 4 (Kazhdan's Property (T) for discrete groups)**.** Let Γ be a finitely generated discrete group and $\Omega \subset \Gamma$ be a finite set of generators. Γ is said to have **Kazhdan Property (T)** if there exists a constant $\varepsilon > 0$ with the following property:

Let $\rho : \Gamma \to U(H)$ be a unitary representation of Γ on a Hilbert space H. Suppose for any nonzero vector $w \in H$ there exists $\gamma \in \Gamma$ such that $\rho(\gamma)w \neq w$. Let $v \in H$ be nonzero. Then there exists $\omega \in \Omega$ such that

$$\|\rho(\omega)v - v\| \geq \varepsilon\|v\|.$$

In 1973 ([Mar88]), Margulis proved that if $\Gamma = \langle\Omega\rangle$ is a group with Kazhdan property (T), then the family of Cayley graphs

$$\{\mathrm{Cay}(\Gamma/N_i, \Omega N_i/N_i)\}_{N_i \lhd \Gamma,\ [\Gamma:N_i]<\infty}$$

is a family of ε-expander graphs for some $\varepsilon > 0$. This, combined with Kazhdan's 1967 result which states that any lattice Γ in a simple Lie group of real rank at least 2 has property (T) ([Kaž67]), gave us a fairly rich source of examples.

The question then became: "What can we say about the rank 1 case?" It turns out that for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, we may only consider the "conguence quotients", $\mathrm{SL}_2(\mathbb{Z})/Ker(\pi_p)$ where

$$\pi_p \,\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$$

denotes the "reduction modulo p" map. Indeed, Selberg's $3/16^{th}$ theorem ([Sel67]) implies that if $\Omega \subset \mathrm{SL}_2(\mathbb{Z})$ is a finite symmetric subset which generates a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then there exists a positive number ε such that the family of graphs

$$\{\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p)), \pi_p(\Omega))\}_{p \text{ prime}}$$

is a family of ε-expander graphs. Analogous results were proved for any arithmetic

group. These results are due to a large number of mathematicians. Notably, Burger-Sarnak proved a sort of reduction process that implies the above statement for any arithmetic lattice of a simple algebraic $\mathbb{Q}$-group that contains a copy of SL_2 [BS91] and Clozel proved the result for the remaining cases [Clo03].

Lubotzky questioned whether or not the result is true when Ω generates a **thin** subgroup of $\mathrm{SL}_2(\mathbb{Z})$, i.e., a subgroup of infinite index which is dense in the Zariski topology. In particular, his famous "1-2-3" problem asks if families of graphs

$$\{\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), \pi_p(\Omega_i))\}_{p>3 \text{ prime}}$$

form a family of expanders where

$$\Omega_i := \left\{ \begin{pmatrix} 1 & \pm i \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm i & 1 \end{pmatrix} \right\}, \ i = 1, 2, 3.$$

Here, Ω_1 generates $\mathrm{SL}_2(\mathbb{Z})$ while Ω_2 generates a finite index subgroup. Ω_3, however, generates a thin subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The "1-2-3" problem was settled by the ground-breaking work of Bourgain and Gamburd in 2008 [BG08b] where they showed that for a subset Ω of $\mathrm{SL}_2(\mathbb{Z})$, the family of graphs

$$\{\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_p), \pi_p(\Omega)\}_{p \text{ prime}}$$

is a family of expanders if and only if $\langle \Omega \rangle$ is has no finite index solvable subgroups. Their method of proof, the so called "Bourgain-Gamburd Machine," has proven to be quite versitile and has since been used, for example, in [BG08a], [BG09], [BGS06], [BGS10], [Var12], and in [SGV12] where the last pair of authors found necessary

and sufficient conditions for such a contruction to yield a family of expander graphs. Namely, they proved the following:

Theorem 5 (Thm. 1 [SGV12]). *Let $\Gamma \subset \mathrm{GL}_d(\mathbb{Z}[1/q_0])$ be the group generated by a symmetric set Ω. Then*

$$\{\mathrm{Cay}(\Gamma/\Gamma(q), \Omega\Gamma(q)/\Gamma(q)\},$$

where $\Gamma(q) := Ker(\Gamma \to \Gamma(mod\ q))$ is the kernel of the reduction modulo q map, is a family of expander graphs as q ranges over the square free integers coprime to q_0 if and only if the connected component of the Zariski-closure of Γ is perfect.

This type of result has come to be known as "super-approximation"[1] as it is a quantitative version of strong approximation in the sense of [PR94, Ch. 7]. Its applications in mathematics have proven to be deep and diverse; including: Appolonian circle packing, homogeneous dynamics, Zaremba's conjecture, and affine sieving (see [BO14] for an overview).

To date, not much has been shown for the analogous "super approximation" question in positive characteristic (See [Bra15] for the case of SL_2).

1.3 Statement of the main result

Let $p > 5$ be a fixed prime number and let q_0 be a fixed power of p. Let $\mathbb{F}_{q_0}$ be a field of order q_0, $\mathbb{F}_{q_0}[t]$ the polynomial ring with coefficients in $\mathbb{F}_{q_0}$, and $\mathbb{F}_{q_0}(t)$ its field of fractions. For the remainder of this paper we fix a finite symmetric set $\Omega \subset \mathrm{GL}_{n_0}(\mathbb{F}_{q_0}(t))$, i.e., $|\Omega| < \infty$ and $\Omega = \Omega^{-1}$. We set Γ to be the subgroup of

[1] In the literature, this result is called "superstrong-approximation". Experts are trying to adopt the term "super-approximation".

$\mathrm{GL}_{n_0}(\mathbb{F}_{q_0}(t))$ generated by Ω and $\mathbb{G}$ the Zariski-closure of Γ. Since Ω is finite, there exists a common denominator, Q_0, of the entries of the matrices in Ω. Hence, Ω, and Γ are contained in $\mathrm{GL}_{n_0}(\mathbb{F}_{q_0}[t, 1/Q_0])$. If $Q \in \mathbb{F}_{q_0}[t]$ is coprime to Q_0, we obtain the "reduction modulo Q" homomorphism

$$\pi_Q : \Gamma \to \mathrm{GL}_{n_0}(\mathbb{F}_{q_0}[t, 1/Q_0]/(Q)) = \mathrm{GL}_{n_0}(\mathbb{F}_{q_0}[t]/(Q)).$$

By an abuse of notation, we will write $\pi_{(-)}$ to denote various reduction homomorphisms whose meaning will be clear in context.

Let Σ be the set of polynomials Q in $\mathbb{F}_{q_0}[t]$ with the following properties:

1. $Q = P_1 P_2 \dots P_k$ is square free with irreducible factors P_1, P_2, $\dots$, P_k and,
2. $\deg(P_i) \neq \deg(P_j)$ for $i \neq j$.

For any positive constant c, we define the set

$$\Sigma_c := \{Q = P_1 P_2 \dots P_k \in \Sigma \mid \forall 1 \leq i \leq k, \deg(P_i) \text{ has no divisor less than } c\}.$$

We will prove the following:

Theorem 6. *Let Ω, Γ and $\mathbb{G}$ be as above. Assume $\mathbb{G}$ is absolutely almost simple and simply connected. Assume further that the ring generated by the set $\mathrm{Tr}(\mathrm{Ad}(\Gamma))$ is all of $\mathbb{F}_{q_0}[t, 1/Q_0]$. Then there exist a square free multiple Q_1 of Q_0, and positive constants c and ε such that*

$$\{Cay(\pi_Q(\Gamma), \pi_Q(\Omega))\}_{Q \in \Sigma_c,\ (Q,Q_1)=1}$$

forms a family of ε-expander graphs.

1.4 Basic definitions

In this section we introduce the basic definitions that we will need in the paper.

1.4.1 Affine group schemes

Let R be a commutative Noetherian ring. Note that the definitions in this section are actually for affine group schemes of **finite type**. Since these are the only affine group schemes we will consider, we call them simple affine group schemes without ambiguity.

Definition 7. A **commutative Hopf algebra** is a tuple $(A, m, e, \Delta, \epsilon, s)$ with the following properties:

(I) (A, m, e) is a commutative associative algebra:

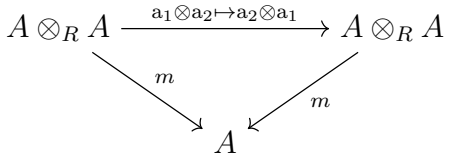
$$m : A \otimes_R A \to A, \text{ and } e : R \to A$$

are R-linear maps such that the following diagrams commute:

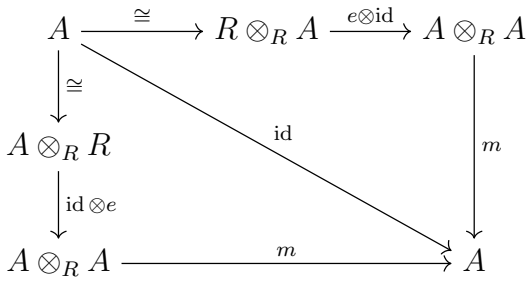
(i) Associativity:

$$\begin{array}{ccc} A \otimes_R A \otimes_R A & \xrightarrow{m\otimes \mathrm{id}} & A \otimes_R A \\ \downarrow{\scriptstyle \mathrm{id}\otimes m} & & \downarrow{\scriptstyle m} \\ A \otimes_R A & \xrightarrow{\quad m \quad} & A \end{array}$$

(ii) Commutativity:



(iii) Existence of identity element:



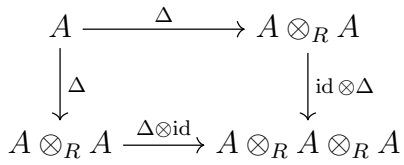
m is called **multiplication** and e is called the **identity**.

(II) (A, Δ, ϵ) is a **coassociative coalgebra**:

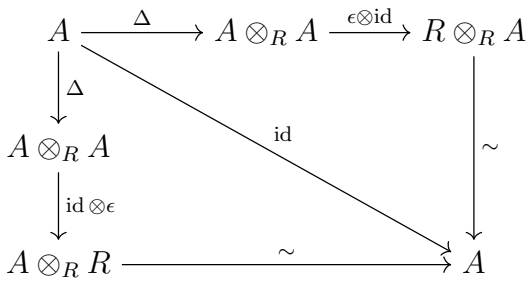
$$\Delta : A \to A \otimes_R A, \text{ and } \epsilon : A \to R$$

are R-linear maps such that the following diagrams commute.

(i) Coassociativity:



(ii) Existence of coidentity:



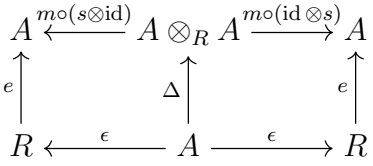
Δ is called **comultiplication** and ϵ is called the **coidentity**.

(III) Δ and ϵ are homomorphisms of R-algberas.

(IV) Existence of an antipodal map:

$$s : A \to A$$

is an R-algebra homomorphism that makes the following diagram commute:



s is called an antipodal map.

If A is a finitely generated commutative Hopf algebra over R, we consider the affine scheme $\mathscr{G} = \mathrm{Spec}(A)$ over $\mathrm{Spec}(R)$. The Hopf algbera structure of A gives $\mathscr{G}$ the structure of a group object in the category of affine schemes. We will call $\mathscr{G}$ an **affine group scheme** over R, or an **affine R-group scheme.**

Let $m : \mathscr{G} \times \mathscr{G} \to \mathscr{G}$ be the multiplication morphism on $\mathscr{G}$. For any R-algebra B, we set

$$\mathscr{G}(B) = \mathrm{Hom}_{R-alg}(A, B).$$

$\mathscr{G}(B)$ is called the set of B-points of $\mathscr{G}$. $\mathscr{G}(B)$ has a group structure where multiplication is defined by

$$\mathscr{G}(B) \times \mathscr{G}(B) \to \mathscr{G}(B) : (f, g) \mapsto (a \mapsto m_B((f \otimes g)\Delta(a)).$$

The assignment $B \rightsquigarrow \mathscr{G}(B)$ defines a functor from the category of R-algebras to the category of groups called the **functor of points of** $\mathscr{G}$.

If S is a commutative ring containing R, we can consider the extension of scalars of $\mathscr{G}$ to S,

$$\mathscr{G}_S = \mathscr{G} \times_{\mathrm{Spec}(R)} \mathrm{Spec}(S) = \mathrm{Spec}(S \otimes_R A).$$

Then $\mathscr{G}_S$ is an affine group scheme over S. We will sometimes write $\mathscr{G} \otimes S$ in place of $\mathscr{G}_S$.

1.4.2 Affine algebraic groups

We focus on the special case where $R = k$ is a field. Let A be a finitely generated commutative Hopf algebra over k, and $\mathbb{G} = \mathrm{Spec}(A)$. Then we say that $\mathbb{G}$ is an **affine algebraic group** over k, or that $\mathbb{G}$ is an affine algebraic k-group, if A is reduced and smooth. From now on, we will use blackboard bold characters to denote algebraic groups. Suppose S is a commutative ring and k is an S-algebra. Suppose there exists an affine group scheme $\mathcal{G}$ such that $\mathcal{G} \otimes_S k = \mathbb{G}$. Then we say that $\mathcal{G}$ is a **model of** $\mathbb{G}$ **over** S.

Since k is a field, Hilbert's Basis Theorem implies A is finitely presented. Therefore, $A = k[x_1, \ldots, x_n]/I$ for some finitely generated ideal I. $\mathbb{G}$ is called **connected**

if the underlying variety is irreducible. That is, if I is a prime ideal. $\mathbb{G}$ is called **simple** if it contains no nontrivial normal algebraic subgroup. If $\mathbb{G}$ is a simple group, then $\mathbb{G}(\overline{k})$ is an **almost simple group**. I.e., $Z(\mathbb{G}(\overline{k}))$ is finite and $\mathbb{G}(\overline{k})/Z((\mathbb{G}(\overline{k}))$ is simple as an abstract group. An algebraic k-group $\mathbb{G}$ is called absolutely almost simple if $\mathbb{G}(A)$ is almost simple for any k-algebra A.

Let $R(\mathbb{G})$ be the identity component of the maximal normal closed solvable subgroup of $\mathbb{G}$. $R(\mathbb{G})$ is called the **radical** of $\mathbb{G}$. If $R(\mathbb{G})$ is trivial, $\mathbb{G}$ is said to be **semisimple**.

Let $R_u(\mathbb{G})$ be the maximal connected unipotent normal subgroup of $\mathbb{G}$. $R_u(\mathbb{G})$ is called the **unipotent radical** of $\mathbb{G}$, and $\mathbb{G}$ is said to be **reductive** if $R_u(\mathbb{G})$ is trivial.

1.4.3 Galois descent

Suppose k is a perfect field.[2] Let $\mathbb{G}$ and $\mathbb{H}$ be two algebraic groups over k with corresponding Hopf algebras $A_{\mathbb{G}}$, $A_{\mathbb{H}}$ over k. Let

$$\phi : \mathbb{G} \otimes \overline{k} \to \mathbb{H} \otimes \overline{k}$$

be a morphism of $\overline{k}$-groups. Then ϕ arises from a $\overline{k}$-algebra homomorphism

$$\phi^* : A_{\mathbb{H}} \otimes \overline{k} \to A_{\mathbb{G}} \otimes \overline{k}.$$

[2]The statements in this section can be generalized to nonperfect fields, but we will not need them in this paper.

It is not necessarily true that there exists a k-algebra homomorphism

$$\phi_k^* : A_{\mathbb{H}} \to A_{\mathbb{G}}$$

such that $\phi_k^* \otimes \mathrm{id} = \phi^*$. When such a k-algebra homomorphism exists, then we have a homomorphism of affine k-schemes

$$\phi_k : \mathbb{G} \to \mathbb{H}.$$

In this case, we say that ϕ is **defined over** k or that ϕ is a k-morphism and we call ϕ_k a k**-descent of** ϕ. One can determine the field of definition of a morphism ϕ by means of the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$.

Notice that we have a natural semilinear Galois action on $A_{\mathbb{G}} \otimes \overline{k}$ given by the semilinear extension of the map

$$\sigma.(a \otimes c) = a \otimes \sigma(c),\ \forall a \in A_{\mathbb{G}}, c \in \overline{k},\ \text{and } \sigma \in \mathrm{Gal}(\overline{k}/k).$$

$\mathrm{Gal}(\overline{k}/k)$ acts on $A_{\mathbb{H}} \otimes \overline{k}$ similarly. Then ϕ is defined over k if and only if ϕ^* commutes with the Galois actions on $A_{\mathbb{G}} \otimes \overline{k}$ and $A_{\mathbb{G}} \otimes \overline{k}$. I.e., when $\sigma(\phi^*(a_1)) = \phi^*(\sigma(a_1))$ for each $a_1 \in A_{\mathbb{G}} \otimes \overline{k}$, and each $\sigma \in \mathrm{Gal}(\overline{k}/k)$.

1.5 Basic facts from algebraic group theory

1.5.1 The Lie algebra of an algebraic group and the Adjoint action

Let $\mathbb{G}$ be an affine algebraic group over a field k. Let $k[\epsilon] = k(X)/(X^2)$. $k[\epsilon]$ is called the ring of **dual numbers**. Let $\pi : \mathbb{G}(k[\epsilon]) \to \mathbb{G}(k)$ be the morphism induced from the morphism $k[\varepsilon] \to k$ that send ϵ to 0. Let $\mathrm{Lie}(\mathbb{G}) = \ker(\pi)$. $\mathrm{Lie}(\mathbb{G})$ is a Lie algebra over k and is called the **Lie algebra of** $\mathbb{G}$. For any field k' containing k, $\mathrm{Lie}(\mathbb{G}_{k'}) = k' \otimes_k \mathrm{Lie}(\mathbb{G})$. We will denote the Lie algebra of an algebraic group by the corresponding Fraktur letter, and we will denote $k' \otimes_k \mathfrak{g}$ by $\mathfrak{g}(k')$.

Notice that we have an exact sequence

$$0 \xrightarrow{i} k \to k[\epsilon] \xrightarrow{\pi} k \to 0.$$

This gives us an inclusion morphism $\tilde{i} : \mathbb{G}(k) \to \mathfrak{g}$. For any $g \in \mathbb{G}(k)$, let

$$\mathrm{Ad}(g) : \mathfrak{g} \to \mathfrak{g},$$

$$X \mapsto \tilde{i}(g) X \tilde{i}(g)^{-1}.$$

$\mathrm{Ad}(\mathbb{G}(A))$ can be defined similarly for any k-algebra A. The assignment $g \mapsto \mathrm{Ad}(g)$ for $g \in \mathbb{G}(A)$ defines an algebraic group homomorphism

$$\mathrm{Ad} : \mathbb{G} \to \mathbb{GL}(\mathfrak{g})$$

called the **adjoint representation of** $\mathbb{G}$.

1.5.2 Algebraic tori

Let $\mathbb{G}_m = \mathbb{GL}_1 = \mathrm{Spec}(\overline{k}[X, X^{-1}])$ be the **multiplicative group**. One sees that $\mathbb{G}_m$ has a $\mathbb{Z}$-scheme sctructure given by $(\mathbb{G}_m)_{\mathbb{Z}} = \mathrm{Spec}(\mathbb{Z}[X, X^{-1}])$. Let $\mathbb{G}$ be a k-group. An affine algebraic $\overline{k}$-subgroup $\mathbb{T}$ of $\mathbb{G}_{\overline{k}}$ is called an **algebraic torus** if there exists an isomorphism

$$\phi : \mathbb{T} \cong (\mathbb{G}_m)_{\overline{k}} \times (\mathbb{G}_m)_{\overline{k}} \times \cdots \times (\mathbb{G}_m)_{\overline{k}}.$$

If $\mathbb{T}$ is a torus defined over k, then we say that $\mathbb{T}$ is **k-split**, or that $\mathbb{T}$ splits over k if there exists an isomorphism

$$\phi : \mathbb{T}_k \cong (\mathbb{G}_m)_k \times (\mathbb{G}_m)_k \times \cdots \times (\mathbb{G}_m)_k.$$

Let $\mathbb{T}$ be a maximal torus of $\mathbb{G}$. Since $\mathbb{T}(\overline{k})$ evidently consists of mutually commuting semisimple elements, the $\mathrm{Ad}(\mathbb{T}(\overline{k}))$-module $\mathfrak{g}(\overline{k})$ has a basis of eigenvectors. In fact there exists a set $\Psi(\mathbb{G}, \mathbb{T})$ of nontrivial algebraic characters $\alpha : \mathbb{T} \to (\mathbb{G}_m)_{\overline{k}}$, $\alpha \in \Phi(\mathbb{G}, \mathbb{T})$ such that

$$\mathfrak{g}(\overline{k}) = \mathrm{Lie}(C_{\mathbb{G}}(\mathbb{T}))(\overline{k}) \oplus \left(\oplus_{\alpha \in \Phi(\mathbb{G}, \mathbb{T})} \mathfrak{g}_\alpha(\overline{k})\right)$$

where for each $\alpha \in \Phi(\mathbb{G}, \mathbb{T})$,

$$\mathfrak{g}_\alpha(\overline{k}) = \{x \in \mathfrak{g}(\overline{k}) |\, \mathrm{Ad}(t)x = \alpha(t)x \ \forall t \in \mathbb{T}(\overline{k})\}.$$

The set $\Phi(\mathbb{G}, \mathbb{T})$ is called the set of **roots** of $\mathbb{T}$. If $\mathbb{G}$ is reductive, then $\Phi(\mathbb{G}, \mathbb{T})$ is an

abstract root system in the vector space $X(\mathbb{T}) \otimes_{\mathbb{Z}} \mathbb{R}$ where

$$X(\mathbb{T}) = \{\phi : \mathbb{T} \to \mathbb{G}_m\}$$

is the group of all algebraic characters of $\mathbb{T}$. Furthermore, if $\mathbb{G}$ is reductive, then for each $\alpha \in \Phi(\mathbb{G}, \mathbb{T})$, $\dim \mathfrak{g}_\alpha = 1$.

Assume $\mathbb{G}$ is semisimple. Let Λ_1 be the $\mathbb{Z}$-span of $X(\mathbb{T})$ in $X(\mathbb{T}) \otimes_{\mathbb{Z}} \mathbb{R}$, and Λ_2 be the $\mathbb{Z}$-span of $\Phi(\mathbb{G}, \mathbb{T}) \subset X(\mathbb{T}) \otimes_{\mathbb{Z}} \mathbb{R}$. Then Λ_1 and Λ_2 are Abelian groups with $\Lambda_1 \subset \Lambda_2$. The **fundamental group**, $\pi_1(\mathbb{G})$, of $\mathbb{G}$ is defined to be the quotient Λ_2/Λ_1. $\mathbb{G}$ is said to be **simply connected** if $\pi_1(\mathbb{G})$ is trivial, and **adjoint** if $\pi_q(\mathbb{G})$ is "as large as possible," i.e., if Λ_2 is equal to the lattice of fundamental dominant weights of $\mathbb{T}$.

1.6 Notation

Throughout this paper for any group H and a subgroup H, $Z(G)$ is the center of G, $C_G(H)$ is the centralizer of H in G, and $N_G(H)$ is the normalizer of H in G as usual. If G and H are algebraic groups, then these notions are considered in the category of algebraic groups.

For a subset S of a finite group G, we denote by χ_S the uniform probability measure supported on S. I.e.

$$\chi_S(g) = \begin{cases} 1/|S| & : g \in S \\ 0 & : g \notin S \end{cases}$$

For any two measures μ, ν on G, $\mu * \nu$ denotes the convolution of μ and ν

$$(\mu * \nu)(g) = \sum_{h \in G} \mu(h)\nu(h^{-1}g),$$

$\mu^{(l)}$ denotes the l-fold convolution of μ with itself and $\widetilde{\mu}$ denotes the measure

$$\widetilde{\mu}(g) = \mu(g^{-1}).$$

For subsets $A, A_1, \ldots, A_n$ of a group G, we write

$$\Pi_{i=1}^{n} A_i := \{a_1 a_2 \ldots a_n | a_i \in A_i\}$$

for the product set of $A_1, \ldots, A_n$ and we write

$$\Pi_k A := \{a_1 a_2 \ldots a_k | a_i \in A,\ 1 \leq i \leq k\}$$

for the set consisting of products of k elements of A. We denote by

$$\times_{i=1}^{k} G_i,$$

the cartesian product of the groups $G_1, \ldots, G_k$. We use Vinogradov's notation $x \ll_A y$ to mean $|x| < Cy$ for some constant C depending on number the parameter A. For any constant δ, $K = \Theta_A(\delta)$ means $\delta \ll_A K \ll_A \delta$. The subscript will be omitted from the above notations if either the constant is universal, or if the dependencies are clear from context. If $G = \times_i G_i$ is a direct product of groups, we use pr_i to denote the projection of G to the i^{th} factor. If $J \subset I$, we identify the group $\times_{i \in J} G_i$ with its

natural inclusion in $\times_{i\in I} G_i$.

For any field k, we denote by $\overline{k}$ its algebraic closure. For any irreducible polynomial $P \in \mathbb{F}_{q_0}[t]$, we set $q_P := {q_0}^{\deg P} = |\mathbb{F}_{q_0}[t]/(P)|$. Throughout this paper Q_0 is a least common multiple of the entries of the matrices appearing in the set Ω in the statement of Theorem 6, and Q_1 is a square free polynomial divisible by Q_0 which has the property that the irreducible factors P of Q_1 are exactly the irreducible polynomials $P \in \mathbb{F}_{q_0}[t]$ with $\deg P \ll_\Omega 1$. Throughout the paper, Q_1 may be replaced by a square free multiple at different occurences. Lastly, we note that the bound of the degrees of the irreducible factors of Q_1 is effective.

Chapter 2

Outline of the proof of the main theorem

Let

$$\chi_\Omega(\gamma) = \begin{cases} \frac{1}{|\Omega|} & \text{if } \gamma \in \Omega \\ 0 & \text{if } \gamma \notin \Omega \end{cases}$$

be the uniform probability measure on Γ supported on Ω and for each square free polynomial $Q \in \mathbb{F}_{q_0}[t]$ coprime to Q_0 let $\pi_Q[\chi_\Omega]$ be the induced probability measure on $\pi_Q(\Gamma)$. For any probability measure ν on a group G, we denote by $\nu^{(\ell)}$ the ℓ-fold convolution of ν with itself. As mentioned in the introduction we follow the so called "Bourgain-Gamburd machine" which was first used in the proof of the main theorem in [BG08b]. The machine has three main components. First, one must show that a random walk on $\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega))$ has an exponentially small chance of landing in any coset of a proper subgroup of $\pi_Q(\Gamma)$. Applying this fact to the trivial subgroup gives us a nice upper bound on the ℓ^2 norm of $\pi_Q[\chi_\Omega]^{(l)}$ for $l \sim \log|\pi_Q(\Gamma)|$. Next, one shows that we can convolve $\pi_Q[\chi_\Omega]^{(l)}$ with itself a finite number of times independent

of Q so that the resulting measure is very close to equidistribution in the ℓ^2 norm. Finally, one can use the technique of Sarnak and Xue which first appeared in [SX91] in which one calculates a trace formula and exploits the fact that there exists a constant c_0 that does not depend on Q such that the groups $\pi_Q(\Gamma)$ are c_0-quasirandom in the sense of Gowers [Gow08] in order to achieve a uniform upper bound for the second largest eigenvalue in the spectrum of the adjacency matrices of the Cayley graphs. This was shown in [AM85] to be an equivalent condition for the family of graphs to be a family of ε-expander graphs for some fixed $\varepsilon > 0$.

There are two key differences in our problem compared to the previous work in characteristic zero: the subgroup structure of the groups $\pi_Q(\Gamma)$ and the fact that representations of $\mathbb{G}$ are not necessarily completely reducible. By Weisfeiler's Strong Approximation Theorem the first problem comes down to understanding subgroups of $\mathbb{G}_P(\mathbb{F}_{q_0}[t]/(P)) = \mathbb{G}_P(\mathbb{F}_{q_0^{\deg P}})$ where $\mathbb{G}_P$ is an absolutely almost simple algebraic $\mathbb{F}_{q_0^{\deg P}}$-group.

In the characteristic zero setting of [SGV12], one only needs to consider the subgroup structure of the $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ points of algebraic $\mathbb{F}_p$-groups. The subgroup structure of such groups is fully described by Madhav Nori in [Nor87] where it is shown that every subgroup can be approximated by the $\mathbb{F}_p$ points of a proper algebraic $\mathbb{F}_p$-subgroup. For larger fields, the correct classification is given by Larsen and Pink in [LP11]. As a corollary of their work we show that if $\mathbb{G}_0$ is an absolutely almost simple group of adjoint type defined over a finite field $\mathbb{F}_q$ and if $H \subset \mathbb{G}_0(\mathbb{F}_q)$ is a maximal proper subgroup then either there exists a proper algebraic subgroup $\mathbb{H}$ of $\mathbb{G}_0$ defined over the algebraic closure of $\mathbb{F}_q$ with $H \subset \mathbb{H}$, or there exists a subfield $\mathbb{F}_{q'}$ and a model

$\mathbb{G}_1$ of $\mathbb{G}_0$ defined over $\mathbb{F}_{q'}$ (i.e., $\mathbb{G}_1 \otimes_{\mathbb{F}_{q'}} \mathbb{F}_q = \mathbb{G}_0$) with

$$[\mathbb{G}_1(\mathbb{F}_{q'}) : \mathbb{G}_1(\mathbb{F}_{q'})] \subset H \subset \mathbb{G}_1(\mathbb{F}_{q'}).$$

Subgroups of the former type are called **structural subgroups** while subgroups of the latter type are called **subfield type subgroups**. In an attempt to establish the first step of the "Bourgain-Gamburd Machine" we show that if Q is "nice" and $H \subset \pi_Q(\Gamma)$ is a proper subgroup with the property that the image of H in $\pi_P(\Gamma) = \mathbb{G}_P(\mathbb{F}_{q_0^{\deg P}})$ for each irreducible factor P of Q is a structural subgroup, then the set of "small lifts" of H,

$$\mathcal{L}_\delta(H) := \{h \in \mathbb{G}(\mathbb{F}_{q_0}[t, 1/Q_0]) \mid \pi_Q(h) \in H \text{ and } \|h\| < [G : H]^\delta\}$$

is contained in a proper algebraic subgroup of $\mathbb{G}$. Then, we construct a finite set of irreducible representations of $\mathbb{G}$ with the property that any algebraic subgroup $\mathbb{H}$ of $\mathbb{G}$ fixes a line in at least one of these representations. It is clear that for any algebraic subgroup $\mathbb{H}$ of $\mathbb{G}$, the line spanned by $\wedge^{\dim \mathbb{H}} \mathfrak{h}$ in $\wedge^{\dim \mathbb{H}} \mathfrak{g}$ is stable under $\wedge^{\dim \mathbb{H}} \operatorname{Ad} \mathbb{H}$ but not all of $\wedge^{\dim \mathbb{H}} \operatorname{Ad} \mathbb{G}$. Unfortunately the representation $\wedge^{\dim \mathbb{H}} \operatorname{Ad}$ is not completely irreducible since $\mathbb{G}$ is defined over a field of positive characteristic. Nevertheless, using the classification of irreducible representations of reductive groups given in [Jan03] we show that one of the irreducible subquotients of a composition series of $\wedge^{\dim \mathbb{H}} \mathfrak{g}$ has the desired property. We then use a "ping-pong" argument to show that the probability that a word of length $l \sim \log |\pi_Q(\Gamma)|$ has an exponentially small chance of fixing a line in any of these representations and therefor the chance of landing in a subfield type subgroup after a random walk on $\operatorname{Cay}(\pi_P(\Gamma), \pi_P(\Omega))$ is exponentially small. Namely, we prove:

Proposition 8 (Escape from proper subgroups)**.** *Let Ω, Γ, and $\mathbb{G}$ be as in the hypotheses of Theorem 6. Then there is a symmetric set $\Omega' \subset \Gamma$, a square free polynomial Q_1 divisible by Q_0, and a constant ε depending only on Ω such that the following holds:*

Let $Q \in \Sigma$ and suppose $(Q, Q_1) = 1$. Let $H \leq \pi_Q(\Gamma)$ be a proper subgroup with the property that $\pi_P(H)$ is a ***structural subgroup*** *of $\pi_P(\Gamma)$ for every prime factor P of Q with $\deg(P) \gg 1$. Then for $\ell \gg \deg Q$ we have*

$$\pi_Q[\chi_{\Omega'}^{(l)}](H) \ll [\pi_Q(\Gamma) : H]^{-\varepsilon}.$$

Since the trivial subgroup is of structural type, we already get a nice bound on the ℓ^2-norm of $\pi_Q[\chi_\Omega]$. By adapting the proof of Varjú in [Var12], we show that second step of the "Bourgain-Gamburd machine" holds so long as the degrees of our polynomials have no small divisors. Namely:

Proposition 9 (l^2-flattening)**.** *Let Ω, Γ, and $\mathbb{G}$ be as in the hypotheses of Proposition 8. Then for any $\varepsilon > 0$ there exists positive constants δ and c depending on $\mathbb{G}$, Ω, and ε with the following property:*

Let $Q \in \Sigma_c$ and suppose (Q, Q_1). Let Ω' be the symmetric set given in Proposition 8. Suppose

$$|\pi_Q(\Gamma)|^{-1/2+\varepsilon} < \|\pi_Q[\chi_{\Omega'}^{(\ell)}]\|_2, \text{ and } \pi_Q[\chi_{\Omega'^{(\ell)}}](gH) < [\pi_Q(\Gamma) : H]^{-\varepsilon}$$

for all $g \in \pi_Q(\Gamma)$ and any proper subgroup $H < \pi_Q(\Gamma)$ with the property that $\pi_P(H)$

is a structural subgroup of $\pi_P(\Gamma)$ *for every irreducible factor* $P \mid Q$ *with. Then*

$$\|\pi_Q[\chi_{\Omega'}^{(2\ell)}]\|_2 < \|\pi_Q[\chi_{\Omega'}]\|_2^{1+\delta}.$$

The idea is that if we cannot get the ℓ^2-norm of $\pi_Q[\chi_\Omega]$ to "flatten out" in finitely many steps, then the results of [BGT12], [PS], and [BG08b] imply that the measure must concentrate on a coset of a large proper subgroup. The measure cannot concentrate on a coset of a proper structural subgroup since that contradicts what we have already shown. Therefore it must concentrate on a coset of a large subgroup whose image in $\pi_P(\Gamma)$ is of subfield type for some divisor P of Q. However, the restrictions on the degrees of the divisors of Q guarantee that no such subgroup exists. Finally, due to [LS04], we can use the trick of Sarnak and Xue to achieve a uniform bound on the second largest eigenvalues of the linear operators

$$T_{\pi_Q[\mu]} : L^2(\pi_Q(\Gamma)) \to L^2(\pi_Q(\Gamma)),$$

$$f \mapsto \pi_Q[\mu] * f,$$

which shows that the Cayley graphs indeed form a family of expander graphs.

Chapter 3

Proof of Proposition 8

Let $\Omega \subset \mathrm{GL}_{n_0}(\mathbb{F}_{q_0}(t))$ be a finite symmetric set, and let $\Gamma = \langle \Omega \rangle$. Since Ω is finite, there exists a square free polynomial $Q_0 \in \mathbb{F}_{q_0}[t]$ such that $\Omega \subset \mathrm{GL}_{n_0}(\mathbb{F}_{q_0}[t, 1/Q_0])$. The set of polynomials in n_0^2 variables with coefficients in $\mathbb{F}_{q_0}(t)$ which vanish on Γ define a flat group scheme $\mathscr{G}$ of finite type over $\mathbb{F}_{q_0}[t, 1/Q_0]$. The Zariski closure $\mathbb{G}$ of Γ in $(\mathbb{GL}_{n_0})_{\mathbb{F}_{q_0}(t)}$ is defined to be the generic fibre

$$\mathscr{G} \otimes_{\mathbb{F}_{q_0}[t,1/Q_0]} \mathbb{F}_{q_0}(t). \tag{3.1}$$

After possibly enlarging Q_0, we may assume $\mathscr{G}$ is a smooth group scheme over $\mathbb{F}_{q_0}[t, 1/Q_0]$ and that all of its fibres are of constant type. For any polynomial $Q \in \mathbb{F}_{q_0}[t]$ that is coprime to Q_0, we obtain a "reduction modulo Q homomorphism"

$$\pi_Q : \mathscr{G}(\mathbb{F}_{q_0}[t, 1/Q_0]) \to (\mathscr{G} \otimes_{\mathbb{F}_{q_0}[t,1/Q_0]} \mathbb{F}_{q_0}[t]/(Q))(\mathbb{F}_{q_0}[t]/(Q)).$$

On Γ, π_Q is just the morphism that reduces the elements of the matrices in Γ modulo Q.

We will write $\mathbb{G}_Q(\mathbb{F}_{q_0}[t]/(Q))$ in place of

$$(\mathscr{G} \otimes_{\mathbb{F}_{q_0}[t,1/Q_0]} \mathbb{F}_{q_0}[t]/(Q))(\mathbb{F}_{q_0}[t]/(Q)).$$

By Weisfeiler's strong approximation theorem [Wei84], there exists a square free polynomial Q_1 divisible by Q_0 such that if Q is a square free polynomial coprime to Q_1, then

$$\pi_Q(\Gamma) = \mathbb{G}_Q(\mathbb{F}_{q_0}[t]/(Q)) \tag{3.2}$$

and

$$\mathbb{G}_Q(\mathbb{F}_{q_0}[t]/(Q)) = \prod_{P_{irred.}|Q} \mathbb{G}_P(\mathbb{F}_{q_0}[t]/(P)). \tag{3.3}$$

Throughout this paper, we may replace Q_1 by

$$\prod_{\substack{P_{irred.} \in \mathbb{F}_{q_0}[t] \\ \deg(P) < C}} P$$

where $C \ll_{\mathbb{G}} 1$ as necessary. For the remainder of this chapter, Q is a fixed square free polynomial coprime to Q_1.

In order to prove Proposition 8 we must understand proper subgroups of $\pi_Q(\Gamma)$. In light of (3.3) and (3.2), we must study proper subgroups of $\mathbb{G}_P(\mathbb{F}_{q_0}[t]/(P))$ as P ranges through all irreducible factors of Q.

3.1 Proper subgroups of $\pi_P(\Gamma)$

Let $\mathbb{T}$ be a maximal torus of $\mathbb{G}$ and let $\mathbb{L}$ be a minimal splitting field of $\mathbb{T}$. Then $\mathbb{L}$ is a finite extension of $\mathbb{F}_{q_0}(t)$ of degree say D'. Let $\mathscr{G}^{Che}$ be the simple, connected adjoint Chevalley $\mathbb{Z}$-group scheme of type Φ (See [Ste61]). Then there exists an $\mathbb{L}$-isogeny

$$\mathbb{G} \otimes_{\mathbb{F}_{q_0}(t)} \mathbb{L} \to \mathscr{G}^{Che} \otimes_{\mathbb{Z}} \mathbb{L}.$$

If $\mathscr{G}$ is the $\mathbb{F}_{q_0}[t, 1/Q_0]$-group scheme (3.1), then we have an isogeny

$$(\mathcal{G} \otimes_{\mathbb{F}_{q_0}[t,1/Q_0]} \mathbb{F}_{q_0}(t)) \otimes_{\mathbb{F}_{q_0}(t)} \mathbb{L} = \mathscr{G} \otimes_{\mathbb{F}_{q_0}[t,1/Q_0]} \mathbb{L} \to \mathscr{G}^{Che} \otimes_{\mathbb{Z}} \mathbb{L}.$$

Since $\mathbb{G}$ is finite dimensional, we may again enlarge Q_0 to get an isogeny

$$\phi : \mathscr{G} \otimes_{\mathbb{F}_{q_0}[t,1/Q_0]} \mathcal{O}_{\mathbb{L}}[1/Q_0] \to \mathscr{G}^{Che} \otimes_{\mathbb{Z}} \mathcal{O}_{\mathbb{L}}[1/Q_0]$$

where $\mathcal{O}_{\mathbb{L}}$ is the ring of integers of $\mathbb{L}$.

For any irreducible polynomial P coprime to Q_0, let $\mathfrak{p} \subset \mathcal{O}_{\mathbb{L}}[1/Q_0]$ be a prime ideal such that $\mathfrak{p} \cap \mathbb{F}_{q_0}[t] = (P)$. Then $\mathbb{F}_{q_P} = \mathbb{F}_{q_0}[t]/(P)$ embeds into the residue field $\mathbb{F}_{\mathfrak{p}}$ of $\mathfrak{p}$ and

$$[\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_{q_P}] < [\mathbb{L} : \mathbb{F}_{q_0}(t)] \ll_{\mathbb{G}} 1.$$

Hence, we obtain an induced isogeny

$$\phi_P : (\mathcal{G} \otimes_{\mathbb{F}_{q_0}[t,1/Q_0]} \mathbb{F}_{q_P}) \otimes \mathbb{F}_{\mathfrak{p}} = \mathbb{G}_P \otimes \mathbb{F}_{\mathfrak{p}} \to \mathscr{G}^{Che} \otimes \mathbb{F}_{\mathfrak{p}}.$$

Notice that by construction ϕ_P is determined by polynomial functions with coefficients

in a finite field $\mathbb{F}_{\mathfrak{p}}$ of $\mathbb{F}_{q_P}$ dimension $\ll 1$. Furthermore, the degrees of the polynomials defining ϕ_P are bounded by a constant $D \ll_{\mathbb{G}} 1$.

With this preparation, we need the following theorem of Larsen and Pink:

Theorem 10. *[LP11, Thm 0.5] Let $\mathscr{G}_0^{Che}$ be a split connected adjoint Chevalley $\mathbb{Z}$-group scheme with simple root system Φ_0. Then there exists a representation*

$$\rho : \mathscr{G}_0^{Che} \to \mathbb{GL}_{n_0'}$$

with the following property: Let H be a finite subgroup of $\mathscr{G}_{0,p}^{Che}(\overline{\mathbb{F}_p})$ where $\mathscr{G}_{0,p}^{Che} = \mathscr{G}_0 \otimes_{\mathbb{Z}} \mathbb{F}_p$ is the geometric fibre of $\mathscr{G}_0^{Che}$ over p. Then either there exists a proper subspace $W \subset (\overline{\mathbb{F}_p})^{n_0}$ that is stable under $\rho(H)$ but not $\rho(\mathscr{G}_{0,p}^{Che}(\overline{\mathbb{F}_p}))$, or there exists a finite field $\mathbb{F}_q \subset \overline{\mathbb{F}_p}$ and a model[1] $\mathbb{G}_0$ of $\mathscr{G}_{0,p}^{Che}$ over $\mathbb{F}_q$ such that the commutator subgroup of $\mathbb{G}_0(\mathbb{F}_q)$ is simple and

$$[\mathbb{G}_0(\mathbb{F}_q) : \mathbb{G}_0(\mathbb{F}_q)] \subset H \subset \mathbb{G}_0(\mathbb{F}_q). \tag{3.4}$$

Definition 11. Subgroups that satisfy the first condition are said to be of **structural type** while subgroups that satisfy the latter condition are said to be of **subfield type**. If the $H \subset \pi_P(\Gamma) = \mathbb{G}_P(\mathbb{F}_{q_P})$ is a subgroup such that $\phi_P(H)$ is a subfield type subgroup (resp. structural type subgroup) of $\mathscr{G}_p^{Che}(\overline{\mathbb{F}_p})$, then we call H a **subfield** (resp. **structural**) type subgroup of $\pi_P(\Gamma)$.

Since the isogeny ϕ_P is induced from a single global isogeny ϕ, we have the immediate

[1] I.e. an $\mathbb{F}_q$-group $\mathbb{G}_0$ such that $\mathbb{G}_0 \otimes \overline{\mathbb{F}_p} \cong \mathscr{G}_{0,p}^{Che}$.

Corollary 12. *Let $H \subset \pi_P(\Gamma)$ be a proper structural type subgroup. Then H is contained in the $\overline{\mathbb{F}_{q_P}}$ points a proper algebraic subgroup $\mathbb{H}_P \subset \mathbb{G}_P$ of complexity[2] at most a constant D, where D depends only on $\mathbb{G}$.*

We wish to apply Theorem 10 to subgroups of $\pi_P(\Gamma) = \mathbb{G}_P(\mathbb{F}_{q_P})$ to get a more accurate description of its subgroup structure. Suppose $\mathbb{G}'$ is a model of $\mathscr{G}_p^{Che}$ over a finite field $\mathbb{F}_q$, and H is a proper subgroup of $\mathbb{G}'(\mathbb{F}_q)$ which is of subfield type. Then by the above theorem there exists a model $\mathbb{G}_H$ of $\mathscr{G}_p^{Che}$ over a finite field $\mathbb{F}_{q_H}$ such that $H \approx \mathbb{G}_H(\mathbb{F}_{q_H})$. The following proposition implies that in fact $\mathbb{F}_{q_H}$ is a subfield of $\mathbb{F}_q$ and $\mathbb{G}_H$ is a model of $\mathbb{G}'$ over $\mathbb{F}_{q_H}$.

Proposition 13 (The case of nested subfield subgroups)**.** *For $i = 1, 2$, let $\mathbb{G}_i$ be an absolutely almost simple group defined over a finite field $\mathbb{F}_{q_i}$. Assume $char(\mathbb{F}_{q_1}) = char(\mathbb{F}_{q_2}) = p > 5$, $|\mathbb{F}_{q_1}| > 9$, and that $\mathbb{G}_2$ is of adjoint type. Let*

$$\widetilde{\phi} : \mathbb{G}_1 \otimes \overline{\mathbb{F}_p} \to \mathbb{G}_2 \otimes \overline{\mathbb{F}_p}$$

be an isogeny with the property that

$$\widetilde{\phi}(\mathbb{G}_1(\mathbb{F}_{q_1})) \subset \mathbb{G}_2(\mathbb{F}_{q_2}).$$

Then $\mathbb{F}_{q_1} \subset \mathbb{F}_{q_2}$ and there exists an isogeny

$$\phi : \mathbb{G}_1 \otimes \mathbb{F}_{q_2} \to \mathbb{G}_2$$

such that $\phi \otimes \mathrm{id}_{\overline{\mathbb{F}}_{q_1}} = \widetilde{\phi}$.

[2]The complexity of an algebraic group $\mathbb{H}$ is defined to be the maximum of the number of polynomials defining $\mathbb{H}$ and their degrees.

Remark 14. If $H \subset G \subset \mathscr{G}_p^{Che}(\overline{\mathbb{F}_p})$ are two finite subgroups of subfield type, then the proof of Theorem 10 produces a subfield $\mathbb{F}_{q_H}$ (resp. $\mathbb{F}_{q_G}$) of $\overline{\mathbb{F}_p}$ and a model $\mathbb{G}_1$ (resp. $\mathbb{G}_2$) such that equation 3.4 holds. By the construction given in the proof of Theorem 10, one sees that $\mathbb{F}_{q_H}$ is a subfield of $\mathbb{F}_{q_G}$ and $\mathbb{G}_1$ is a model of $\mathbb{G}_2$ over $\mathbb{F}_{q_H}$ as desired. The proof of Proposition 13 is independent of the proof of Theorem 10.

Remark 15. In the remainder of this paper it is only important that $\mathbb{F}_{q_1}$ divides $\mathbb{F}_{q_2}$, but Proposition 13 might be of independent interest.

By a theorem of Lang [Hum78, Thm. 35.2], $\mathbb{G}_{q_1}$ is quasisplit. Hence, any minimal $\mathbb{F}_{q_1}$-parabolic subgroup is a Borel subgroup. Let $\mathbb{B}_1$ be a Borel subgroup defined over $\mathbb{F}_{q_1}$. By [Bor66, §6.5 (3)], there is an $\mathbb{F}_{q_1}$-split torus $\mathbb{S}_1$ such that

$$\mathbb{B}_1 = C_{\mathbb{G}_1}(\mathbb{S}_1) \cdot R_u(\mathbb{B}_1).$$

Since $\mathbb{B}_1$ is a Borel subgroup, $\mathbb{T}_1 = C_{\mathbb{G}_1}(\mathbb{S}_1)$ is a maximal $\mathbb{F}_{q_1}$-torus, and $\mathbb{S}_1$ is a maximal $\mathbb{F}_{q_1}$-split torus.

Let $\widetilde{\mathbb{G}}_i = \mathbb{G}_i \otimes \overline{\mathbb{F}_p}$ for $i = 1, 2$, $\widetilde{\mathbb{S}_2} = \widetilde{\phi}(\mathbb{S}_1 \otimes \overline{\mathbb{F}_p})$, $\widetilde{\mathbb{T}_2} = \widetilde{\phi}(\mathbb{T}_1 \otimes \overline{\mathbb{F}_p})$, and $\widetilde{\mathbb{B}_2} = \widetilde{\phi}(\mathbb{B}_1 \otimes \overline{\mathbb{F}_p})$. Let $\mathfrak{g}_i = \mathrm{Lie}(\mathbb{G}_i)$ for $i = 1, 2$. Notice that since $\widetilde{\phi}$ is an isogeny, we have an isomorphism

$$d\widetilde{\phi} : \mathfrak{g}_1(\overline{\mathbb{F}_p}) \to \mathfrak{g}_2(\overline{\mathbb{F}_p})$$

which satisfies the identity

$$d\widetilde{\phi}(\mathrm{Ad}(g_1)(x_1)) = \mathrm{Ad}(\widetilde{\phi}(g_1))(d\widetilde{\phi}(x_1)), \tag{3.5}$$

for all $g_1 \in \mathbb{G}_1(\overline{\mathbb{F}_p})$ and $x_1 \in \mathfrak{g}_1(\overline{\mathbb{F}_p})$. To simplify notation, let $\widetilde{\mathbb{G}}_i = \mathbb{G}_i \otimes \overline{\mathbb{F}_p}$ for $i = 1, 2$. By [Bor91, Cors. 9.2, 11.12] and [CGP15, A.2.8], we have $\widetilde{\phi}(C_{\widetilde{\mathbb{G}_1}})(\mathbb{S}_1 \otimes \overline{\mathbb{F}_p}) = C_{\widetilde{\mathbb{G}_2}}(\widetilde{\mathbb{S}_2})$ is an $\overline{\mathbb{F}_p}$-torus, $\widetilde{\mathbb{T}_2} = C_{\widetilde{\mathbb{G}_2}}(\mathbb{S}_2)$ is a maximal $\overline{\mathbb{F}_p}$-torus, and $\mathrm{Lie}(\mathbb{T}_1) = C_{\mathfrak{g}_1}(\mathbb{S}_1)$.

We will first prove $\mathbb{F}_{q_1} \subset \mathbb{F}_{q_2}$.

Lemma 16. *$\widetilde{\phi}^*$ induces bijections*

$$\Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{S}_2}) \to \Phi(\widetilde{\mathbb{G}_1}, \widetilde{\mathbb{S}_1})$$

and

$$\Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{T}_2}) \to \Phi(\widetilde{\mathbb{G}_1}, \widetilde{\mathbb{T}_1}).$$

Moreover, $d\widetilde{\phi}$ induces isomorphisms

$$\mathfrak{g}_{1,\widetilde{\phi}^*\alpha}(\overline{\mathbb{F}_{q_1}}) \to \mathfrak{g}_{2,\alpha}(\overline{\mathbb{F}_{q_2}})$$

for $\alpha \in \Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{S}_2})$ or $\Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{T}_2})$.

Proof. Let

$$\mathfrak{g}_2(\overline{\mathbb{F}_{q_2}}) = \mathfrak{t}_2(\overline{\mathbb{F}_{q_2}}) \oplus \left(\oplus_{\phi \in \Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{S}_2})} \mathfrak{g}_{2,\phi}(\overline{\mathbb{F}_{q_2}})\right)$$

be a root space decomposition of $\mathfrak{g}_2(\overline{\mathbb{F}_{q_2}})$. Let $x_{2,\alpha} \in \mathfrak{g}_{2,\alpha}(\overline{\mathbb{F}_{q_2}})$, and let $x_1 \in \mathfrak{g}_1(\overline{\mathbb{F}_{q_1}})$ such that $d\widetilde{\phi}(x_1) = x_{2,\alpha}$. By equation 3.5 we have for every $s_1 \in \widetilde{\mathbb{S}_1}(\overline{\mathbb{F}_{q_1}})$, and $\alpha \in \Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{S}_2})$,

$$d\widetilde{\phi}(\mathrm{Ad}(s)(x_1)) = \mathrm{Ad}(\widetilde{\phi}(s_1))d\widetilde{\phi}(x_1) = (\widetilde{\phi}^*\alpha)(s_1)d\widetilde{\phi}(x_1) = d\widetilde{\phi}((\widetilde{\phi}^*\alpha)(s_1)x_1)$$

and hence $\widetilde{\phi}^*(\alpha)(s)x_1 = \mathrm{Ad}(s)x_1$ since $d\widetilde{\phi}$ is an isomorphism. Therefore, $\widetilde{\phi}^*(\alpha) \in \Phi(\widetilde{\mathbb{G}_1}, \widetilde{\mathbb{S}_1})$ and $d\widetilde{\phi}(\mathfrak{g}_{q,\widetilde{\phi}^*(\alpha)}(\overline{\mathbb{F}_{q_1}})) \subset \mathfrak{g}_{2,\alpha}(\overline{\mathbb{F}_{q_2}})$. By comparing dimensions, we see that $\widetilde{\phi}^*$ induces a bijection from $\Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{S}_2})$ to $\Phi(\widetilde{\mathbb{G}_1}, \widetilde{\mathbb{S}_1})$ and $d\widetilde{\phi}$ induces an isomorphism from $\mathfrak{g}_{1,\widetilde{\phi}^*(\alpha)}(\overline{\mathbb{F}_{q_1}})$ to $\mathfrak{g}_{2,\alpha}(\overline{\mathbb{F}_{q_2}})$. The argument is similar for the second assertion. □

Lemma 17. *For every $\alpha \in \Phi(\widetilde{\mathbb{G}_1}, \widetilde{\mathbb{S}_1})$, $\dim \mathfrak{g}_{1,\alpha} \leq 3$.*

Proof. By Lang's theorem [Hum78, Thm 35.2], $\mathbb{G}_i$ is quasisplit over $\mathbb{F}_{q_i}$ for $i = 1, 2$. Let $\mathbb{F}_1'$ be a splitting field for a maximal $\mathbb{F}_{q_1}$ torus of $\mathbb{G}_1$. For an arbitrary field k, the splitting field l of a quasisplit simple group over k is a Galois extension of k, and $\mathrm{Gal}(l/k)$ is isomorphic to the automorphism group of the Dynkin diagram of $\Phi(\widetilde{\mathbb{G}}_1, \widetilde{\mathbb{T}}_1)$. Hence $\mathrm{Gal}(l/k)$ is isomorphism to $\{1\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$, or $Sym(3)$. If k is a finite field, then $\mathrm{Gal}(l/k)$ is cyclic, and hence the last choice is not possible. We have for each $\alpha \in \Phi(\widetilde{\mathbb{G}_1}, \widetilde{\mathbb{S}_1})$,

$$\dim \mathfrak{g}_{1,\alpha} = |\{\widetilde{\alpha} \in \Phi(\widetilde{\mathbb{G}_1}, \widetilde{\mathbb{T}_1}) | \widetilde{\alpha}|_{\widetilde{\mathbb{S}_1}} = \alpha\}|$$

and $\mathrm{Gal}(\mathbb{F}_1'/\mathbb{F}_{q_1})$ acts transitively on the set

$$\{\widetilde{\alpha} \in \Phi(\widetilde{\mathbb{G}_1}, \widetilde{\mathbb{T}_1}) | \widetilde{\alpha}|_{\widetilde{\mathbb{S}_1}} = \alpha\}$$

which implies the lemma. □

Proposition 18. *With the notation as above, if $q_1 > 9$, then $\mathbb{F}_{q_1} \subset \mathbb{F}_{q_2}$.*

Proof. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ be a set of simple roots of $\mathbb{S}_1$, and $\{\alpha_1^\vee, \ldots, \alpha_r^\vee\}$ the corresponding coroots. Then for any $t_1, t_2, \ldots, t_r \in \mathbb{F}_{q_1}$,

$$\mathrm{Tr}(\mathrm{Ad}(\phi(\Pi_{i=1}^r \alpha_i^\vee(t_i))) \in \mathbb{F}_{q_2}$$

since $\widetilde{\phi}(\mathbb{G}_1(\mathbb{F}_{q_1})) \subset \mathbb{G}_2(\mathbb{F}_{q_2})$. Therefore,

$$\sum_{\beta \in \Phi(\mathbb{G}_1, \mathbb{S}_1)} \dim \mathfrak{g}_{q,\beta} \Pi_{i=1}^{r} t_1^{\langle \alpha_i^\vee, \beta \rangle} \in \mathbb{F}_{q_2}.$$

Notice that for each $i = 1, 2, \ldots, r$, and any root β, $\langle \alpha_i^\vee, \beta \rangle$ is a Cartan integer and hence is at most 3 in absolute value. By the discussion above, $\dim \mathfrak{g}_{1,\beta} < 3$. The proposition will be proved with the following series of lemmas:

Lemma 19. *Let $P(t) \in \mathbb{F}_p[t^{\pm}]$ be a nonconstant polynomial. If $P(\mathbb{F}_q) \subset \mathbb{F}_{q'}$, and $(\deg_t P + \deg_{t^{-1}} P)^2 < q$, then $\mathbb{F}_q \subset \mathbb{F}_{q'}$.*

Proof. For each $a \in \mathbb{F}_{q'}$, there are at most $(\deg_t P + \deg_{t^{-1}} P)$ elements $b \in \mathbb{F}_q$ such that $P(b) = a$. Hence, $|P(\mathbb{F}_q)| \geq q/(\deg_t P + \deg_{t^{-1}} P)$. If $\mathbb{F}'$ is the field generated by $P(\mathbb{F}_q)$, then $\log_p |\mathbb{F}'|$ divides $\log_p q$ and $\log_p q \leq \log_p |\mathbb{F}'| + \log_p((\deg_t P + \deg_{t^{-1}} P))$. If $\mathbb{F}' \neq \mathbb{F}_q$, then the above argument implies $\log_p q/2 \leq \log_p((\deg_t P + \deg_{t^{-1}} P))$. This contradicts the assumption that $q > ((\deg_t P + \deg_{t^{-1}} P))^2$.

□

Lemma 20. *Let $P \in \mathbb{F}_p[t_1^{\pm 1}, \ldots, t_r^{\pm 1}]$ be a nonzero polynomial. If $q > \max_i(\deg_{t_i} P + \deg_{t_i^{-1}}) + 1$, then $P(\mathbb{F}_q^\times, \ldots, \mathbb{F}_q^\times) \neq 0$.*

Proof. This can easily be proved by induction on r. □

Lemma 21. *Let $P \in \mathbb{F}_p[t_1^{\pm 1}, \ldots, t_r^{\pm 1}]$ be a nonzero polynomial such that $P(\mathbb{F}_q^\times, \ldots, \mathbb{F}_q^\times)$ is contained in $\mathbb{F}_{q'}$, and $\max_i(\deg_{t_i} P + \deg_{t_i^{-1}} P)^2 < q$. Then $\mathbb{F}_q \subset \mathbb{F}_{q'}$.*

Proof. Since P is nonconstant, there exists some index i_0 where $\deg_{t_{i_0}^{\pm 1}} \neq 0$. By the above lemma there is a choice of constants $t_1, \ldots, t_{r-1} \in \mathbb{F}_q$ such that $P(t_1, \ldots, t_{r-1})$ is a nonconstant polynomial in t_{i_0}. By Lemma 19, we are done. □

□

We must now prove the existence of the isogeny ϕ.

Proposition 22. *If $q_1 > 7$ and $p > 5$, then $d\widetilde{\phi}$ induces an isomorphism between $\mathfrak{g}_1(\mathbb{F}_{q_2})$ and $\mathfrak{g}_2(\mathbb{F}_{q_2})$.*

We distinguish two cases depending on whether or not $\mathfrak{g}_1$ has a nontrivial center.

Lemma 23. *Let $p > 5$. Suppose $\mathbb{G}$ is an absolutely almost simple $\mathbb{F}_q$ group and that $\mathbb{G}$ is not of type A_{np-1} for some positive integer n. Assume:*

1. *$M \subset \mathfrak{g}(\overline{\mathbb{F}_p})$ is an $\mathbb{F}_{q'}$-subspace where $\mathbb{F}_q \subset \mathbb{F}_{q'}$,*
2. *$\dim_{\mathbb{F}_{q'}} M = \dim_{\overline{\mathbb{F}_p}} \mathfrak{g}(\overline{\mathbb{F}_p})$, and*
3. *M is $\mathbb{G}(\mathbb{F}_q)$ invariant.*

Then there exists $0 \neq \lambda \in \overline{\mathbb{F}_p}$ such that $M = \lambda\mathfrak{g}(\overline{\mathbb{F}_p})$.

Proof. Since $\mathbb{G}$ is not of type A_{np-1}, $\mathfrak{g}(\overline{\mathbb{F}_p})$ is a simple $\mathbb{G}(\overline{\mathbb{F}_p})$-module. By [Wei84, Cor. 4.6], $\mathfrak{g}(\overline{\mathbb{F}_p})$ is a simple $\mathbb{G}(\mathbb{F}_q)$-module. Let $\{\alpha_i\}$ be an $\mathbb{F}_{q'}$-basis of $\overline{\mathbb{F}_p}$ so that

$$\mathfrak{g}(\overline{\mathbb{F}_p}) = \oplus_{i\geq 0}\alpha_i\mathfrak{g}(\mathbb{F}_{q'}).$$

Let $\mathrm{pr}_i : M \to \alpha_i\mathfrak{g}(\mathbb{F}_{q'})$ be the projection morphism onto the i^{th} component. Since M and $\mathfrak{g}(\mathbb{F}_{q'})$ are both $\mathbb{G}(\mathbb{F}_q)$-invariant, pr_i is an $\mathbb{F}_{q'}$-linear $\mathbb{G}(\mathbb{F}_q)$-module homomorphism. Again by [Wei84, Cor. 4.6], $\mathfrak{g}(\mathbb{F}_{q'})$ is a simple $\mathbb{F}_{q'}[\mathrm{Ad}(\mathbb{G}(\mathbb{F}_q))]$-module and hence pr_i is either trivial or surjective for each i. Since $\dim_{\mathbb{F}_{q'}} M = \dim_{\mathbb{F}_{q'}} \mathfrak{g}(\mathbb{G}_{q'})$, either $\mathrm{pr}_i = 0$ or pr_i is an isomorphism.

If pr_i and pr_j are isomorphisms, then $\mathrm{pr}_i \circ \mathrm{pr}_j{}^{-1} \in \mathrm{Aut}_{\mathbb{G}(\mathbb{F}_q)-Mod}(\mathfrak{g}(\mathbb{F}_{q'}))$. Then there exists a nonzero element $\alpha_{i,j} \in \mathbb{F}_{q'}$ such that $\mathrm{pr}_i \circ \mathrm{pr}_j{}^{-1}(x) = \lambda_{i,j}x$ for all $x \in \mathfrak{g}(\mathbb{F}_{q'})$. Hence if j_0 is a fixed index for which pr_{j_0} is an isomorphism, we have

$$M = \left(\sum_i \alpha_i \lambda_{i,j_0} \right) \mathfrak{g}(\mathbb{F}_{q'}).$$

□

In the case when $\mathbb{G}$ is of type A_{np-1} we have the following:

Lemma 24. *Suppose $p > 5$ and $\mathbb{G}$ is of type A_{np-1} for some positive integer n. Suppose $\mathbb{F}_q \subset \mathbb{F}_{q'}$ and suppose:*

1. *$M \subset \mathfrak{g}(\overline{\mathbb{F}_p})$ is an $\mathbb{F}_{q'}$-subspace,*
2. *M is $\mathbb{G}(\mathbb{F}_q)$-invariant, and*
3. *$\dim_{\mathbb{F}_{q'}}(M + \mathfrak{z}(\overline{\mathbb{F}_p}))/\mathfrak{z}(\overline{\mathbb{F}_p}) = \dim_{\overline{\mathbb{F}_p}} \mathfrak{g}(\overline{\mathbb{F}_p})/\mathfrak{z}(\overline{\mathbb{F}_p})$ where $\mathfrak{z}$ is the center of $\mathfrak{g}$.*

Then there exists $0 \neq \lambda \in \overline{\mathbb{F}_p}$, such that $M + \mathfrak{z}(\overline{\mathbb{F}_p}) = \lambda\mathfrak{g}(\mathbb{F}_{q'}) + \mathfrak{z}(\overline{\mathbb{F}_p})$.

Proof. In this case, $\mathfrak{g}(\overline{\mathbb{F}_p})/\mathfrak{z}(\overline{\mathbb{F}_p})$ is a simple $\mathbb{G}(\overline{\mathbb{F}_p})$-module. Again by [Wei84, Cor. 4.6], $\mathfrak{g}(\overline{\mathbb{F}_p})/\mathfrak{z}(\overline{\mathbb{F}_p})$ is a simple $\mathbb{G}(\mathbb{F}_q)$-module. An argument similar to the proof of the previous lemma establishes the claim. □

Proof of Proposition 22. Let $M = d\widetilde{\phi}^{-1}(\mathfrak{g}_2(\mathbb{F}_{q_2})) \subset \mathfrak{g}_1(\overline{\mathbb{F}_p})$. If $\mathbb{G}_1$ and $\mathbb{G}_2$ are not of type A_{np-1}, then Lemma 23 finishes the proof. So assume $\mathbb{G}_1$ is of type A_{np-1}. Then $\dim_{\mathbb{F}_{q_2}} M = \dim_{\overline{\mathbb{F}_p}} \mathfrak{g}_1(\overline{\mathbb{F}_p})$. Notice $d\widetilde{\phi}$ induces an isomorphism between $\mathfrak{z}_1(\overline{\mathbb{F}_p})$ and $\mathfrak{z}_2(\overline{\mathbb{F}_p})$, and

$$\dim_{\mathbb{F}_{q_2}} \mathfrak{g}_2(\mathbb{F}_{q_2}) + \mathfrak{z}_2(\overline{\mathbb{F}_p})/\mathfrak{z}_2(\overline{\mathbb{F}_p}) = \dim_{\overline{\mathbb{F}_p}} \mathfrak{g}_1(\overline{\mathbb{F}_p}) - 1$$

and hence

$$\dim_{\mathbb{F}_{q_2}} M + \mathfrak{z}_1(\overline{\mathbb{F}_p})/\mathfrak{z}_1(\overline{\mathbb{F}_p}) = \dim_{\overline{\mathbb{F}_p}} \mathfrak{g}_1(\overline{\mathbb{F}_p})/\mathfrak{z}_1(\overline{\mathbb{F}_p}).$$

By the previous lemma, there exists $0 \neq \lambda \in \mathbb{F}_{q_2}$ such that $M + \mathfrak{z}_1(\overline{\mathbb{F}_p}) = \lambda\mathfrak{g}_1(\mathbb{F}_{q_2}) + \mathfrak{z}_1(\overline{\mathbb{F}_p})$. Since $[\mathfrak{g}_i(\mathbb{F}_{q_2}), \mathfrak{g}_i(\mathbb{F}_{q_2})] = \mathfrak{g}_i(\mathbb{F}_{q_2})$ for $i = 1, 2$, we have $[M, M] = \lambda^2\mathfrak{g}_1(\mathbb{F}_{q_2})$ and

$$[M, M] = d\widetilde{\phi}^{-1}([\mathfrak{g}_2(\mathbb{F}_{q_2}), \mathfrak{g}_2(\mathbb{F}_{q_2})]) = d\widetilde{\phi}^{-1}(\mathfrak{g}_2(\mathbb{F}_{q_2})) = M.$$

Hence $M = [M, M] = \lambda^4\mathfrak{g}_1(\mathbb{F}_{q_2}) = \lambda^2\mathfrak{g}_1(\mathbb{F}_{q_2})$. This shows $\mathfrak{g}_1(\mathbb{F}_{q_2}) = \lambda^2\mathfrak{g}_1(\mathbb{F}_{q_2})$ and hence $M = \mathfrak{g}_1(\mathbb{F}_{q_2})$.

□

Corollary 25. *$d\widetilde{\phi}$ induces isomorphisms between*

$$\mathfrak{t}_1(\mathbb{F}_{q_2}) \text{ and } \mathfrak{g}_2(\mathbb{F}_{q_2}) \cap \widetilde{\mathfrak{t}}_2(\overline{\mathbb{F}_p}),$$

and

$$\mathfrak{g}_{1,\widetilde{\phi}^*(\beta)}(\mathbb{F}_{q_2}) \text{ and } \mathfrak{g}_2(\mathbb{F}_{q_2}) \cap \widetilde{\mathfrak{g}_{2,\beta}}(\overline{\mathbb{F}_p}),\ \forall\beta \in \Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{S}_2}).$$

Proof. By Proposition 22 we have,

$$d\widetilde{\phi}(\mathfrak{g}_{1,\widetilde{\phi}^*(\beta)}(\mathbb{F}_{q_2})) \subset \mathfrak{g}_2(\mathbb{F}_{q_2}) \cap \widetilde{\mathfrak{g}_{2,\beta}}(\overline{\mathbb{F}_p}),$$

and similarly

$$d\widetilde{\phi}(\mathfrak{t}_1(\mathbb{F}_{q_2})) \subset \mathfrak{g}_2(\mathbb{F}_{q_2}) \cap \widetilde{\mathfrak{t}}_2(\overline{\mathbb{F}_p}).$$

By comparing dimensions of $\mathfrak{g}_1(\mathbb{F}_{q_2})$ and

$$(\mathfrak{g}_2(\mathbb{F}_{q_2}) \cap \widetilde{\mathfrak{t}_2}(\overline{\mathbb{F}_p})) \oplus \left(\oplus_{\beta \in \Phi(\widetilde{\mathbb{G}_2}, \widetilde{\mathbb{T}_2})} (\mathfrak{g}_2(\mathbb{F}_{q_2}) \cap \widetilde{\mathfrak{g}_{2,\beta}}(\overline{\mathbb{F}_p}))\right)$$

the result follows easily. □

Proof of Proposition 13. Notice that the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_{q_2})$ acts naturally on $\mathbb{G}_1$, $\mathbb{G}_2$, and their Lie algebras. The existence of such an isogeny

$$\phi : \mathbb{G}_1 \otimes \mathbb{F}_{q_2} \to \mathbb{F}_2$$

is equivalent to $\widetilde{\phi}$ commuting with the action of $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_{q_2})$. More precisely, it suffices to show that for any $g_1 \in \mathbb{G}_1(\overline{\mathbb{F}_p})$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_{q_2})$, $\sigma(\widetilde{\phi}(g_1)) = \widetilde{\phi}(\sigma(g_1))$. Let $g_1 \in \mathbb{G}_{q_1}(\overline{\mathbb{F}_{q_1}})$ and $x_1 \in \mathfrak{g}(\overline{\mathbb{F}_{q_1}})$. Recall that we have the identity (3.5),

$$d\widetilde{\phi}(\mathrm{Ad}(g_1)(x_1)) = \mathrm{Ad}(\widetilde{\phi}(g_1))(d\widetilde{\phi}(x_1))$$

for every $x_1 \in \mathfrak{g}_1(\overline{\mathbb{F}_p})$.

Since $d\widetilde{\phi}$ restricts to an isomorphism from $\mathfrak{g}_1(\mathbb{F}_{q_2})$ to $\mathfrak{g}_2(\mathbb{F}_{q_2})$ by Proposition 22, we have

$$\sigma(d\widetilde{\phi}(\mathrm{Ad}(g_1)(x_1))) = d\widetilde{\phi}(\sigma(\mathrm{Ad}(g_1)(x_1))).$$

Since the adjoint representation of $\mathbb{G}_1$ is defined over $\mathbb{F}_{q_1} \subset \mathbb{F}_{q_2}$, we have

$$\sigma(\mathrm{Ad}(g_1)(x_1)) = \mathrm{Ad}(\sigma(g_1))(\sigma(x_1)).$$

The previous three equations imply

$$\begin{aligned}\sigma(d\widetilde{\phi}(\mathrm{Ad}(g_1)(x_1)) &= d\widetilde{\phi}(\mathrm{Ad}(\sigma(g_1))(\sigma(x_1)))\\ &= \mathrm{Ad}(\widetilde{\phi}(\sigma(g_1)))(d\widetilde{\phi}(\sigma(x_1))),\end{aligned}$$

and

$$\sigma(\mathrm{Ad}(\widetilde{\phi}(g_1))(d\widetilde{\phi}(x_1))) = \mathrm{Ad}(\sigma(\widetilde{\phi}(g_1)))(d\widetilde{\phi}(\sigma(x_1))).$$

Therefore we have

$$\mathrm{Ad}(\widetilde{\phi}(\sigma(g_1)))(d\widetilde{\phi}(\sigma(x_1))) = \mathrm{Ad}(\sigma(\widetilde{\phi}(g_1)))(d\widetilde{\phi}(\sigma(x_1)))$$

and hence

$$\mathrm{Ad}(\widetilde{\phi}(\sigma(g_1))) = \mathrm{Ad}(\sigma(\widetilde{\phi}(g_1))).$$

Since $\mathbb{G}_2 = \mathrm{Ad}\,\mathbb{G}_2$ is an adjoint group, $\widetilde{\phi}(\sigma(g_1)) = \sigma(\widetilde{\phi}(g_1))$ which proves the claim. $\square$

Now we can establish the following refinement of Theorem 10. Let $P \in \mathbb{F}_{q_0}[t]$ be coprime to Q_1 and let ρ'_P be the composition of ϕ_P and the representation ρ_P induced from the representation ρ (c.f., Theorem 10). Notice that by construction, ρ'_P is defined by polynomials of degree $\ll_{\mathbb{G}} 1$ with coefficients in a field $\mathbb{F}'_{q_P}$ of degree at most $[\mathbb{L} : \mathbb{F}_{q_0}(t)] \ll_{\mathbb{G}} 1$ over $\mathbb{F}_{q_P}$. Then

$$\rho'_P : \mathbb{G}_P(\overline{\mathbb{F}_{q_P}}) \to \mathrm{GL}_{n'_0}(V)$$

is a representation from $\mathbb{G}_P(\overline{\mathbb{F}_{q_P}})$ to the general linear group of an n_0 dimensional $\overline{\mathbb{F}_{q'_p}}$-vector space V, and V has a basis $\mathcal{B}$ consisting of elements in $(\mathbb{F}_{q'_P})^{n'_0}$. Let $V_{q'_p}$ be the $\mathbb{F}_{q'_P}$-linear span of the vectors in $\mathcal{B}$. Then we have

Proposition 26. *Let $P \in \mathbb{F}_{q_0}[t]$ be an irreducible polynomial coprime to Q_1 and let $H \subset \pi_P(\Gamma) = \mathbb{G}_P(\mathbb{F}_{q_P})$ be a proper subgroup of structural type. Then $\rho'_P(H)$ fixes a proper $\mathbb{F}_{q'_P}$-subspace W' of V that is not fixed by $\rho'_P(\mathbb{G}_P(\mathbb{F}_{q_P}))$.*

Proof. Let $H \subset \pi_P(\Gamma)$ be a proper subgroup of structural type. Then there exists a proper $\overline{\mathbb{F}_{q_P}}$-subspace $W \subset V$ that is stable under $\rho'_P(H)$ but not $\rho'_P(\mathbb{G}_P)$. By [LP11, Prop. 3.5], V is an absolutely irreducible $\rho'_P(\mathbb{G}_P(\mathbb{F}_{q'_P}))$-module if $q_P \gg 1$. After possibly enlarging Q_1, we may assume W is not stable under $\rho'_P(\mathbb{G}_P(\mathbb{F}_{q_P}))$.

Since W is finite dimensional, any basis $\mathcal{B}_W$ is contained in a finite field extension of $\mathbb{F}_{q'_P}$. Therefore, there exist a finite field $\mathbb{F}_{q''_P}$ containing $\mathbb{F}_{q'_P}$ and a $\rho'_P(H)$-stable $\mathbb{F}_{q''_P}$-vector space $W_{q''_P}$ such that $W_{q''_P} \otimes \overline{\mathbb{F}_{q_P}} = W$. Let $W' \subset W_{q''_P}$ be a simple $\mathbb{F}_{q'_P}[\rho'_P(H)]$-submodule. We may assume $V_{q'_P}$ has no $\rho'_P(H)$-stable $\mathbb{F}_{q'_P}$-subspaces since otherwise we are done. Let $\{\alpha_i\}_{i=1}^{[\mathbb{F}_{q''_P}:\mathbb{F}_{q'_P}]}$ be an $\mathbb{F}_{q'_P}$-basis of $\mathbb{F}_{q''_P}$ with $\alpha_1 = 1$. Let $V_{q''_P} = V_{q'_P} \otimes \mathbb{F}_{q''_P}$. Then

$$W' \subset V_{q''_P} = \bigoplus_{i=1}^{[\mathbb{F}_{q''_P}:\mathbb{F}_{q'_P}]} \alpha_i \otimes V_{q'_P}. \tag{3.6}$$

Set $V_i = \alpha_i \otimes V_{q'_P}$. Then for each $i_0 \in \{1, \ldots, [\mathbb{F}_{q''_P} : \mathbb{F}_{q'_P}]\}$, $\mathrm{pr}_i : W \to V_i$ is an $\mathbb{F}_{q'_P}$-linear $\rho'_P(H)$-module homomorphism. Since W' and V_i are simple $\mathbb{F}_{q'_P}[\rho'_P(H)]$-modules, each pr_i is either trivial or an isomorphism. We claim that there exists $\lambda \in \mathbb{F}_{q''_P}$ such that $W' = \lambda V_i$ for some i. Let I be the set of indices for which $\pi_i(W') \neq 0$.

If $|I| = 1$ then we are done. Fix an index $i_0 \in I$. Then for each $j \in I$, we have an isomorphism of $\mathbb{F}_{q'_P}[\rho'_P(H)]$-modules

$$V_{i_0} \xrightarrow{\mathrm{pr}_j \circ \mathrm{pr}_{i_0}^{-1}} V_j \xrightarrow{\ell_{\alpha_{i_0}} \circ \ell_{\alpha_j}^{-1}} V_{i_0}$$

where ℓ_α is given by left multiplication by α. Since V_{i_0} is a simple $\mathbb{F}_{q'_P}[\rho'_P(H)]$-module by assumption, there exists $\lambda_j \in \mathbb{F}_{q'_P}$ such that

$$\ell_{\alpha_{i_0}} \circ \ell_{\alpha_j}^{-1} \circ \mathrm{pr}_j \circ \mathrm{pr}_{i_0}^{-1} = \ell_{\lambda_j}.$$

This implies $W' = \lambda V_{q'_P}$ where $\lambda = \alpha_{i_0}^{-1} \sum \lambda_j \alpha_j$. Therefore, $W_{q''_P}$ contains an $\mathbb{F}_{q'_P}$ subspace $\lambda V_{q'_P}$. Hence $W = V$, which is a contradiction. Therefore $\rho'_P(H)$ stabilizes an $\mathbb{F}_{q'_P}$ subspace of $V_{q'_P}$. □

Corollary 27. *Let $H \subset \pi_P(\Gamma)$ be a proper subgroup of structural type. Then there exists an $\mathbb{F}_{q'_P}$-subgroup $\mathbb{H}_P$ of $\mathbb{G}_P$ such that H is contained in $\mathbb{H}_P(\overline{\mathbb{F}_{q_P}}) \cap \mathbb{G}_P(\mathbb{F}_{q_P})$. Moreover, $\mathbb{H}_P$ is of complexity $\ll_{\mathbb{G}} 1$.*

Proof. By Proposition 26, $\rho'_P(H)$ is contained in the stabilizer of an $\mathbb{F}_{q'_P}$ subspace W of V. Thus, $\rho'_P(H)$ is contained in the $\mathbb{F}_{q'_P}$-rational points of a proper algebraic $\mathbb{F}_{q'_P}$-group $\mathbb{H}' \subset \rho'_P(\mathbb{G}_P)$. $\mathbb{H}'$ is of bounded complexity by construction. Then $\mathbb{H}_P = \rho'^{-1}_P(\mathbb{H}')$ is the desired algebraic subgroup. □

We will also need the following corollary in the next section.

Corollary 28. *Let $H \subset \pi_P(\Gamma)$ be a proper subgroup of structural type. Then there exist a constant $D \ll_{\mathbb{G}} 1$ and polynomial $F_P \in \mathbb{F}_{q_P}[x_{11}, \ldots, x_{n_0,n_0}]$ of degree at most D such that H vanishes on F_P but $\pi_P(\Gamma)$ does not.*

Proof. Let $W_{q'_P}$ be a proper $\mathbb{F}_{q'_P}$-subspace of V that is stable under $\rho'_P(H)$ but not under $\rho'_P(\mathbb{G}_P(\mathbb{F}_{q_P}))$. Let $w \in W_{q'_P}$ and $v^* \in V^*_{q'_P}$ be a linear functional whose kernel is $W_{q'_P}$. After identifying $V^*_{q'_P}$ with $(\mathbb{F}_{q'_P})^{n'_0}$ we may view $\eta_{v,w}(g) = v^*(\rho'_P(g)w)$ as a polynomial with coefficients in $\mathbb{F}_{q'_P}$ whose degree is bounded by a constant $D \ll_{\mathbb{G}} 1$.

Moreover, since $W_{q'_P}$ is stable under H, $\eta_{v,w}(h) = 0$ for every $h \in H$ and yet there exists $\omega \in \Omega$ such that $\eta_{v,w}(\pi_P(\omega)) \neq 0$. Since the dimension of $\mathbb{F}_{q'_P}$ as an $\mathbb{F}_{q_P}$ vector space is at most $[\mathbb{L} : \mathbb{F}_{q_0}(t)] \ll_{\mathbb{G}} 1$ the claim follows.

□

3.2 Escaping certain proper subgroups

The goal of this section is to show that there exists a symmetric set $\Omega' \subset \Gamma$ with the following property: For any square free polynomial $Q \in \mathbb{F}_{q_0}[t]$ that is coprime to Q_1 and for any proper subgroup $H \subset \pi_Q(\Gamma)$ with the property that $\pi_P(H)$ is a structural subgroup for each irreducible factor P of Q, the probability that an $\ell \sim \deg(Q)$-step random walk lands in H is small. Let S be the set of irreducible polynomials appearing in the denominators of the matrices in Ω. For any $P_0 \in S$, let $\|\cdot\|_{P_0}$ be the P_0-adic norm of $\mathbb{F}_{q_0}(t)$ normalized so that $\|P_0(t)\|_{P_0} = (q_0^{|S| \max_{P \in S}\{\deg P\}})^{-1}$ and let $\|\cdot\|_{1/t}$ be the $1/t$-adic norm of $\mathbb{F}_{q_0}(t)$ normalized so that $\|t\|_{1/t} = q_0$. For any rational polynomial $a(t)$, let

$$\|a(t)\|_{S\cup\{1/t\}} = \max_{P \in S\cup\{1/t\}} \|a(t)\|_P.$$

If H is a proper subgroup of $\pi_Q(\Gamma)$ with the property that $\pi_P(H)$ is a structural subgroup of $\pi_P(\Gamma)$ for each irreducible factor P of Q, then we can lift the random walk on $\pi_Q(\Gamma)$ to a random walk on Γ. There we can show that the set of "small lifts" of H,

$$\mathcal{L}_\delta(H) := \{h = (h_{i,j}) \in \Gamma | \pi_Q(h) \in H \text{ and } \|h\| < [\pi_Q(\Gamma) : H]^\delta\},$$

where

$$\|h\| := \max_{1 \leq i,j \leq n_o} \{\|h_{i,j}\|_{S\cup\{1/t\}}\}, \tag{3.7}$$

lies in a proper algebraic subgroup of $\mathbb{G}$ if $\delta \ll_{\mathbb{G}} 1$. We then show that there is a finite collection of irreducible representations of $\mathbb{G}$ with the property that any proper algebraic subgroup of $\mathbb{G}$ fixes a line in one of these representations. Then we use the "ping-pong" argument from [SGV12] to show that there exists a symmetric subset $\Omega' \subset \Gamma$ such that the probability that a reduced word of length $\sim \deg Q$ in the alphabet Ω' fixes a line in one of these representations is exponentially small. This in turn implies that a random walk on the quotient graph has a small chance of landing in H.

Following the proof of [SGV12, Prop. 7], we first show that any subgroup H of $\pi_Q(\Gamma)$ can be approximated by a subgroup in product form. Let us record the following definition, which we will also need later on.

Definition 29 (Gowers [Gow08])**.** Let c be a positive constant and G be a finite group. G is said to be c**-quasirandom** if for any irreducible representation ρ of G we have $\dim \rho > |G|^c$.

Landazuri and Sietz proved in [LS74] that for any absolutely almost simple group $\mathbb{G}'$ over a finite field $\mathbb{F}_q$, there exists a constant $c' > 0$ depending only on $\mathbb{G}'$ such that the groups $\mathbb{G}'(k)$ are c'-quasirandom for any field k containing $\mathbb{F}_q$.

In this section, we again fix a square free polynomial Q coprime to Q_1. In order to use the subgroup dichotomy of $\pi_P(\Gamma)$ where P is an irreducible factor of Q, we will first take a subgroup $H \subset \pi_Q(\Gamma)$ and replace it with the product of subgroups $\pi_P(H)$ of $\pi_P(\Gamma)$ for irreducible $P \mid Q$. A priori, $\times_{P|Q:P_{irred.}} \pi_P(H)$ could be much larger than H. However, for us this is not the case.

Lemma 30. *Let G_{q_i} be a quasisimple group of Lie type over the field $\mathbb{F}_{q_i}$ of characteristic $p_i \geq 5$ for $i = 1, \ldots, k$. Assume $q_i \neq q_j$ for each $i \neq j$. Then there exists a*

positive constant δ such that

$$\Pi_i[G_{q_i} : \mathrm{pr}_i(H)] \geq [\times_i G_{q_i} : H]^{\delta}.$$

Furthermore, δ depends only on c where c is the minimum of the set

$$\{c' > 0 | G_{q_i} \text{ is } c'\text{-quasirandom } \forall i = 1, \ldots, k\}.$$

Remark 31. By the classification theorem of finite simple groups of Lie type and the result of Landazuri and Seitz mentioned above, the constant c in the statement of the lemma is nonzero and depends only on the absolute root systems of the G_{q_i}'s.

Proof. We proceed by induction on the size of $G := \times_i G_{q_i}$. Suppose $\mathrm{pr}_i(H)$ is a proper subgroup of G_{q_i} for each $1 \leq i \leq k$. Then

$$\Pi_i[G_{q_i} : \mathrm{pr}_i(H)] \geq \Pi_i |G_{q_i}|^c \geq [G : H]^c$$

and we are done. Partition the set $I = \{1, 2, \ldots, k\}$ into two sets I_1 and I_2 in such a way that $i \in I_1$ if and only if $\mathrm{pr}_i(H) = G_{q_i}$. By the above argument, we may assume I_1 is nonempty. For $i \in I_1$, $H \cap G_{q_i}$ is a proper normal subgroup of $G_{q_i} = \mathrm{pr}_i(H)$. Let

$$G'_{q_i} = \begin{cases} G_{q_i}/H \cap G_{q_i} & \text{if} \quad i \in I_1 \\ G_{q_i} & \text{if} \quad i \in I_2, \end{cases}$$

$$H' = H/\left(\times_{i \in I_1} H \cap G_{q_i}\right),$$

and

$$G' = \times_i G'_{q_i}.$$

If $H \cap G_{q_i}$ is a nontrivial for any $i \in I_1$, then $|G'| < |G|$ and G' clearly satisfies the hypothesis of the lemma. By the induction hypothesis we have

$$\Pi_i[G : \mathrm{pr}_i(H)] = \Pi_i[G' : \mathrm{pr}_i(H')] \geq [G' : H']^\delta = [G : H]^\delta$$

and again we are done.

Therefore we may assume $H \cap G_{q_i}$ is trivial for each index $i \in I_1$. For a fixed $j_0 \in I_1$, we have an isomorphism $G_{q_{j_0}} \cong H/N_{j_0}$ induced by pr_{j_0} where $N_{j_0} = H \cap \times_{i \neq j_0} G_{q_i}$. For each $i \neq j_0$, there exists a projection morphism

$$\phi_j : G_{q_{j_0}} \cong H/N_{j_0} \to \mathrm{pr}_i(H)/\,\mathrm{pr}_i(N_{j_0}).$$

By the induction hypothesis applied to $\times_{i \neq j_0} G_{q_i}$ and N_{j_0}, we have

$$\begin{aligned}
\Pi_i[G_{q_i} : \mathrm{pr}_i(N_{j_0})] &= \Pi_{i \neq j_0}[G_{q_i} : \mathrm{pr}_i\, N_{j_0}] \\
&\geq [\times_{i \neq j_0} G_{q_i} : N_{j_0}]^\delta \\
&= |\times_{i \neq j_0} G_{q_i}|^\delta \left(\tfrac{|G_{q_{j_0}}|}{|H|}\right)^\delta \\
&= [G : H]^\delta.
\end{aligned}$$

Therefore if $\mathrm{pr}_i(N_{j_0}) = \mathrm{pr}_i(H)$ for all $i \neq j_0$, we are done. So we may assume there exists $i_0 \neq j_0$ such that $\mathrm{pr}_{i_0} N_{j_0} \neq \mathrm{pr}_{i_0} H$.

Suppose $i_0 \in I_1$. Then we have a morphism $G_{q_{j_0}} \to G_{q_{i_0}}/\,\mathrm{pr}_{i_0}(N_{j_0})$. Since $G_{q_{i_0}}$ and $G_{q_{j_0}}$ are quasisimple groups over nonisomorphic fields of order at least 5, this is impossible. Therefore $i_0 \in I_2$. By the above argument, we may assume for every

$j \in I_1$, there exists $i \in I_2$ such that $\mathrm{pr}_i(N_j) \neq \mathrm{pr}_i(H)$. After fixing such a choice of $i \in I_2$ for each $j \in I_1$, we get a function $F : I_1 \to I_2$ given by $F(j) = i$. We claim that for each $i \in F(I_1)$,

$$\prod_{j \in F^{-1}(i)} |G_{q_j}|^c \leq |G_{q_i}|.$$

For each $j \in F^{-1}(i)$, there exists a quotient morphism

$$\mathrm{pr}_i(H) \longrightarrow \mathrm{pr}_i(H)/\mathrm{pr}_i(N_j) \xrightarrow{\cong} G_{q_j}/\ker\phi_j \longrightarrow G_{q_j}/Z(G_{q_j}).$$

Since the groups $G_{q_j}/Z(G_{q_j})$ $1 \leq j \leq n$ are simple and mutually nonisomorphic, the Jordan-Hölder Theorem implies that $\mathrm{pr}_i(H)$ has a composition factor isomorphic to $G_{q_j}/Z(G_{q_j})$ for each $j \in F^{-1}(i)$. In particular,

$$|\mathrm{pr}_i(H)| \geq \pi_{j \in F^{-1}(i)} |G_{q_j}/Z(G_{q_j})|.$$

Therefore

$$|G_{q_i}| \geq |\mathrm{pr}_i(H)| \geq \prod_{j \in F^{-1}(i)} |G_{q_j}/Z(G_{q_j})| \geq \prod_{j \in F^{-1}(i)} |G_{q_j}|^c$$

as desired.

Since $\{F^{-1}(i)\}_{i \in I_2}$ partitions the set I_1, we have shown that

$$\Pi_{j \in I_1} |G_{q_j}|^c \leq \Pi_{i \in I_2} |G_{q_i}|,$$

and hence

$$\begin{aligned}\Pi_{i=1}^{n}[G_{q_i} : \mathrm{pr}_i(H)]^{c+1} &\geq \Pi_{i\in I_2}|G_{q_i}|^{1+\frac{1}{c}} \\ &\geq \left(\Pi_{j\in I_1}|G_{q_j}|\right)\left(\Pi_{i\in I_2}|G_{q_i}|\right) \\ &\geq [\times_{i=1}^{n} G_{q_i} : H]\end{aligned}$$

which completes the proof.

□

Proposition 32. *Fix an embedding of $\mathbb{G}$ into $(\mathbb{GL}_{n_0})_{\mathbb{F}_{q_0}(t)}$. Let $Q \in \Sigma$ be coprime to Q_1. Then there exists a constant δ such that the following holds: Let $H \subset \pi_Q(\Gamma)$ be a proper subgroup with the property that $\pi_P(H)$ is a structural subgroup of $\pi_P(\Gamma)$ for each irreducible factor P of Q. Then $\mathcal{L}_\delta(H)$ lies in a proper algebraic subgroup $\mathbb{H}$ of $\mathbb{G}$.*

Proof. Let $H \subsetneq \pi_Q(\Gamma)$ be as in the hypothesis of the proposition. By Lemma 30, there exists a positive constant δ' which depends only on $\mathbb{G}$ such that

$$[\pi_Q(\Gamma) : \underset{P_{irred.}|Q}{\times} \pi_P(H)] \geq [\pi_Q(\Gamma) : H]^{\delta'}.$$

If $\mathcal{L}_\delta(\times_{P_{ired.}|Q}\pi_P(H))$ lies in a proper algebraic subgroup of $\mathbb{G}$, then so does $\mathcal{L}_{\delta/\delta'}(H)$. Therefore we may replace H with $\times_{P|Q}\pi_P(H)$. Similarly, after replacing Q with the product of those irreducible factors satisfying $\pi_P(H) \neq \pi_P(\Gamma)$, we may assume $\pi_P(H)$ is a proper subgroup for each irreducible factor P of Q. By Corollary 28, there exists a constant $D \ll_{\mathbb{G}} 1$ and a polynomial of degree at most D that vanishes on $\pi_P(H)$. Consider the degree D monomial map

$$\Psi : \mathbb{GL}_{n_0} \to \mathbb{A}_{D'},$$

where

$$D' = \begin{pmatrix} n_0^2 + D \\ D \end{pmatrix}.$$

Let d be the dimension of the linear span of $\Phi(\mathbb{G}(\mathbb{F}_{q_0}(t)))$. It suffices to show that $\Phi(\mathcal{L}_\delta(H))$ spans a subspace of dimension less than d if δ is sufficiently small.

Assume for the sake of contradiction that the linear span of $\Phi(\mathcal{L}_\delta(H))$ is d dimensional. Pick a set of d linearly independent elements $h_1, h_2, \ldots, h_d$ of $\mathcal{L}_\delta(H)$. Recall that we have the inequality ([Nor87, Lem 3.5])

$$|\pi_Q(\Gamma)| = \prod_{P|Q} |\mathbb{G}_P(\mathbb{F}_{q_P})| < {q_0}^{(\dim \mathbb{G}+1)\deg Q}.$$

Since $\|h\| < |\pi_Q(\Gamma)|^\delta < {q_0}^{(\dim \mathbb{G}+1)\deg Q}$ (c.f. (3.7)), the entries of the vectors $h_1, h_2, \ldots, h_d$ are of the form

$$\frac{F}{\prod_{P\in S} P^{e_P}}$$

with $F \in \mathbb{F}_{q_0}[t]$ where

$$\deg F - \sum_{P|Q} e_P \deg P < \delta D(\dim \mathbb{G} + 1)\deg Q \tag{3.8}$$

and for each $P \in S$

$$\deg P^{e_P} < \delta D(\dim \mathbb{G} + 1)\deg Q/|S|. \tag{3.9}$$

By assumption, the matrix formed by the vectors h_1,h_2,...,h_d has a nonzero $d \times d$ subdeterminant. For $\delta < 1/2Dd(\dim \mathbb{G} + 1)$, equations 3.8 and 3.9 imply that any

subdeterminant, $s(t)$, has the form

$$\frac{F'}{\prod_{P\in S} P^{e'_P}}$$

with $\deg F < \deg Q$. Therefore there exists an irreducible factor P_0 of Q such that $s(t) \neq 0 \in \mathbb{F}_{q_0}[t, 1/Q_1]/(P)$ (recall $(Q, P) = 1$ for all $P \in S$.) This contradicts the existence of the polynomial given by Corollary 28. Therefore $\mathcal{L}_\delta(H)$ lies in the $\mathbb{F}_{q_0}(t)$ points of a proper subvariety $\mathbb{X}$ of $\mathbb{G}$. By [EMO05, Proposition 3.2] if $A \subset \mathbb{G}(\mathbb{F}_{q_0}(t))$ is a generating set, then there exists a positive integer N such that $\Pi_N A \neq \mathbb{X}(\mathbb{F}_{q_0}(t))$. We note that the statement of [EMO05, Proposition 3.2] is for algebraic varieties and groups over $\mathbb{C}$. However, one can replace the complex numbers in [EMO05, Thm. 3.1] with any algebraically closed field (See [Sch00, Pg. 519], [Ful98, Ex. 12.3.1], and [Dan94, III. Thm 2.2]) and the proof of [EMO05, Proposition 3.2] is valid for any algebraically closed field. In the proof of [EMO05, Proposition 3.2], N depends only on the dimension, degree and number of irreducible components of $\mathbb{X}$. These parameters are bounded by the constant D, which is independent of Q. Therefore since $\mathcal{L}_\delta(H) \subset \mathbb{X}(\mathbb{F}_{q_0}(t))$, $\mathcal{L}_{\delta/N}(H)$ does not generate $\mathbb{G}(\mathbb{F}_{q_0}(t))$ and therefore it lies in a proper algebraic subgroup of $\mathbb{G}$. □

3.3 Ping pong argument

Recall that the goal of this section is to show that if $H \subset \pi_Q(\Gamma)$ is a proper subgroup with the property that $\pi_P(H)$ is structural for each irreducible factor P of Q, then the probability of landing in H after a random walk of roughly $\deg(Q)$ steps on $\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega))$ is small. By Proposition 32, we can translate this problem to

random walks on $\mathrm{Cay}(\Gamma, \Omega)$.

For any subset $\Omega_0 \subset \Gamma$ let $B_\ell(\Omega_0)$ be the set of reduced words of length ℓ in the alphabet Ω_0. Using results in [SGV12], we find a symmetric set Ω_0 with the property that a random walk on on the Cayley graph $\mathrm{Cay}(\Gamma, \Omega_0)$ has an exponentially small chance of landing in a proper algebraic subgroup of $\mathbb{G}$. A key ingredient is the following proposition that holds more generally for any semisimple algebraic group over a field of positive characteristic.

Proposition 33. *Let $\mathbb{G}$ be a finite dimensional semisimple group over an algebraically closed field k of positive characteristic. Then there exists finitely many irreducible representations $\{\rho_i : \mathbb{G} \to (\mathbb{GL})_{\mathbb{V}_i}\}, i = 1 \ldots, d$ such that for every closed subgroup H of G, there exists an index $i \in \{1, 2, \ldots k\}$ and a vector $v \in \mathbb{V}_i(k)$ such that*

$$\rho_i(\mathbb{H}(k))[v] = [v]$$

but

$$\rho_i(\mathbb{G}(k))[v] \neq [v]$$

where $[v]$ denotes the line in V_i spanned by v.

Proof. Throughout this proof we let $G = \mathbb{G}(k)$, $H = \mathbb{H}(k)$, $V = \mathbb{V}(k)$, etc. It suffices to consider only maximal closed subgroups of $\mathbb{G}$. By Theorem 1 of [LS04], $\mathbb{G}$ has finitely many conjugacy classes of maximal closed subgroups of positive dimension. If $\mathbb{H}$ is a maximal closed subgroup, and if $\rho(H)[v] = [v]$ for some vector $v \in V_\rho$, then for any $g \in G$, $\rho(gHg^{-1})(\rho(g)[v]) = \rho(g)[v]$. Therefore, given a full set of representatives $\{\mathbb{H}_i\}_{i=1}^d$ of conjugacy classes of maximal closed subgroups of $\mathbb{G}$, it suffices to find d many representations $\{\rho_i\}_{i=1}^d$ such that for every $\mathbb{H}_i$ there exists a representation ρ_j

and a vector $v_j \in V_j$ such that v_j is $\rho_j(H_i)$-invariant but not $\rho_j(G)$-invariant.

Let us recall some facts about irreducible representations of $\mathbb{G}$. Fix a maximal torus $\mathbb{T}$ of $\mathbb{G}$. Let $\Phi = \Phi(G,T)$ be the system of roots of T and let Δ be a system of simple roots. Let B be the Borel subgroup containing T corresponding to Δ. Let $X(T)$ be the set of algebraic characters of $\mathbb{T}$ and fix an inner product $(-,-)$ on $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ that is invariant under the Weyl group, $W = N_G(T)/T$. For any two characters λ_1, λ_2 on T let $< \lambda_1, \lambda_2 >= 2(\lambda_1, \lambda_2)/(\lambda_2, \lambda_2)$. Note that we can extend any character $\lambda \in X(T)$ to a regular function on B. Let $k_\lambda = k$ be the B-module k where the action of B on k_λ is given by $b.x = \lambda(b)x$. Consider the G-module

$$\mathrm{Ind}_B^G(k_\lambda) = \{f : G \to k | f \text{ is regular, and } | \ f(gb) = \lambda(b)^{-1} f(g) \ \forall g \in G, b \in B\},$$

where G acts on $\mathrm{Ind}_B^G(k_\lambda)$ by left translation. By Chevalley's classification theorem of irreducible G-modules [Jan03, II.2.4], $\mathrm{Ind}_B^G(k_\lambda)$ contains a unique simple submodule $L(\lambda) = \mathrm{Soc}_G(k_\lambda)$ and every simple module of G arises this way.

Since $\mathbb{H}$ is a maximal closed subgroup of $\mathbb{G}$, either H is parabolic, or H° is reductive ([Hum78, Thm. 30.4]). If H is maximal and parabolic then there exists a simple root α such that H is conjugate to the maximal parabolic subgroup

$$P := P_{\Delta\setminus\{\alpha\}} = BW_{\Delta\setminus\{\alpha\}}B$$

where $W_{\Delta\setminus\{\alpha\}}$ is the group generated by $\{\sigma_\beta\}_{\beta\in\Delta\setminus\{\alpha\}}$ and σ_β is the reflection of $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ across the hyperplane orthogonal to α. Let $\lambda = \lambda_\alpha = 2\alpha/(\alpha,\alpha)$ be the fundamental dominant weight corresponding to α. As mentioned above, λ can be

extended to a character on B. Consider the G-module

$$\mathrm{Ind}_P^G(k_\lambda) = \{f : G \to k \mid f \text{ is regular, and } f(gp) = \lambda(p)^{-1} f(g)\ \forall p \in P, g \in G\}.$$

Let $U^- := R_u(B^-)$ be the unipotent radical of the Borel subgroup B^- opposite of B. Define the function f_λ on U^-B by $f_\lambda(u^-b) := \lambda(b)^{-1}$. By the calculation in [Jan03, 2.6], f_λ can be extended to an element of $\mathrm{Ind}_P^B \lambda$. The set $(P \cap U^-)B$ is an open dense subgroup of P and for any $u^- \in P \cap U^-$ and $b \in B$, we have

$$f_\lambda(u^-b) = \lambda(b)^{-1} = \lambda(u^-b)^{-1}.$$

Therefore for any $p \in P$, $f_\lambda(p) = \lambda(p)^{-1}$. This implies that the line spanned by f_λ in the unique simple module $L(\lambda)$ is invariant under P, which establishes the claim.

Now assume H° is reductive. Let $\mathfrak{g} = \mathfrak{g}(k)$ (resp. $\mathfrak{h} = \mathfrak{h}(k)$) be the Lie algebra of $\mathbb{G}$ (resp. $\mathbb{H}$). Since $\mathbb{G}$ is semisimple and $\mathbb{H}$ is maximal, $\mathbb{H}$ is not a normal subgroup and therefore $\mathfrak{h}$ is not invariant under the adjoint action of G. G acts on $\wedge^{\dim \mathfrak{h}} \mathfrak{g}$ via the representation $\wedge^{\dim \mathfrak{h}} \mathrm{Ad}$. By the above considerations the line $l_H = \wedge^{\dim \mathfrak{h}} \mathfrak{h}$ is H-invariant but not G-invariant. Let

$$0 =: V_0 \subset V_1 \subset V_2 \ldots V_m = \wedge^{\dim \mathfrak{h}} \mathfrak{g}$$

be a composition series of G-modules. It suffices to show that the image of l_H in one of the nontrivial composition factors is H-invariant but not G-invariant.

Let m' be the smallest index such that $l_H \subset V_{m'}$. Then

$$(l_H \oplus V_{m'-1})/V_{m'-1} \subset V_{m'}/V_{m'-1}$$

is an H-invariant line. Assume for the sake of contradiction that $V_{m'} = l_H \oplus V_{m'-1}$. Let m'' be the smallest integer such that $l_H \oplus V_{m''}$ is G-invariant. Then the line $l_H \oplus V_{m''-1}/V_{m''-1}$ is an H-invariant line inside the G-module $(l_H \oplus V_{m''})/V_{m''}$ that is not G-invariant.

By the classification theorem for simple G modules, there exists $\lambda \in X(T)$ such that $L(\lambda) \cong V_{m''}/V_{m''-1}$. We have an exact sequence of G-modules

$$0 \longrightarrow L(\lambda) = V_{m''}/V_{m''-1} \longrightarrow M = (l_H \oplus V_{m''})/V_{m''-1} \longrightarrow k \longrightarrow 0$$

which splits as a sequence of H-modules. For any group G over k, the fixed point functor from the category of left G-modules to the category of k-modules is left exact. Its i^{th} right derived functor, denoted by $H^i(G, -)$ is called the i^{th} cohomology functor. By [Jan03, Cor. 4.11] we have $H^0(G, k) = H^0(H, k) = k$. From the above short exact sequence we obtain a commutative diagram of long exact sequences:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & k & & \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & L(\lambda)^G & \longrightarrow & M^G & \longrightarrow & k^G & \longrightarrow & H^1(G, L(\lambda)) \longrightarrow \dots \\
 & & \downarrow{\scriptstyle \mathrm{Res}^G_H} & & \downarrow{\scriptstyle \mathrm{Res}^G_H} & & \downarrow{\scriptstyle \mathrm{Res}^G_H} & & \downarrow{\scriptstyle \mathrm{Res}^G_H} \\
0 & \longrightarrow & L(\lambda)^H & \longrightarrow & M^H & \longrightarrow & k^H & \xrightarrow{0} & H^1(H, L(\lambda)) \longrightarrow \dots \\
 & & \| & & \| & & \| & & \\
 & & 0 & & k & & k & &
\end{array}$$

We will arrive at a contradiction by showing that the restriction map

$$H^1(G, L(\lambda)) \to H^1(H, L(\lambda))$$

is injective. Since H° is reductive, G/H is an affine variety and hence the functor $Ind_H^G(-)$ is exact ([Jan03, Part I. Cor. 5.13]). By Shapiro's Lemma ([Jan03, Part I. Cor. 4.6]) $H^1(H, L(\lambda)) \cong H^1(G, \mathrm{Ind}_H^G L(\lambda))$. Therefore it suffices to show that the map $H^1(G, L(\lambda)) \to H^1(G, \mathrm{Ind}_H^G L(\lambda))$ is injective. To complete the proof we establish the following:

Lemma 34. *Let $\mathbb{G}$ be a semisimple algebraic group over an algebraically closed field k and let $\mathbb{H}$ be a maximal closed subgroup whose connected component is reductive. Let M be an irreducible H-module. Then the map*

$$H^1(G, M) \to H^1(G, \mathrm{Ind}_H^G M)$$

induced by the G-module monomorphism

$$M \to \mathrm{Ind}_H^G M : m \mapsto (g \mapsto g^{-1}m)$$

is injective.

Proof. The exact sequence of G-modules

$$0 \to M \to \mathrm{Ind}_H^G M \to (\mathrm{Ind}_H^G M)/M \to 0$$

gives rise to the long exact sequence of cohomologies

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M^G & \longrightarrow & (\mathrm{Ind}_H^G M)^G & \xrightarrow{\phi} & [(\mathrm{Ind}_H^G M)/M]^G & \longrightarrow & \dots \\ \dots & \longrightarrow & H^1(G,M) & \longrightarrow & H^1(G,\mathrm{Ind}_H^G M) & \longrightarrow & \dots. & & \end{array}$$

It suffices to show that ϕ is surjective. Let $f \in (\mathrm{Ind}_H^G M)^G \setminus M^G$ and let $[f]$ denote its image in $[(\mathrm{Ind}_H^G M)/M]^G$. After replacing $[f]$ by the function $[f - \widetilde{f(1)}]$, we may assume $f(1) = 0$. For every $g \in G$, $g.f = f - \widetilde{m}_g$ for some $m_g \in M^G$. Then

$$\begin{aligned} 0 &= f(1) \\ &= f(g^{-1}.g) \\ &= (g.f)(g) \\ &= f(g) - g^{-1}m_g. \end{aligned} \tag{3.10}$$

This implies $m_g = gf(g)$ for every $g \in G$. Therefore for every $g, g' \in G$,

$$\begin{aligned} f(g^{-1}g') &= (g.f)(g') \\ &= (f - \widetilde{gf(g)})(g') \\ &= f(g') - g'^{-1}gf(g). \end{aligned} \tag{3.11}$$

Let $X := \{g \in G \mid f(g) = 0\}$. For every $h \in H$, $f(h) = h^{-1}f(1) = 0$ and hence $H \subset X$. X is also a subgroup of G, since for any $g, g' \in X$, $f(g^{-1}g') = 0$ by the above calculation. If $f(g) = 0$ for all $g \in G$, then clearly $f = \widetilde{0_M}$ where 0_M is the zero element of M. Therefore X is a proper closed subgroup. By the maximality of H, $X = H$. We claim that the codimension of H in G is at least 2, which yields the desired contradiction.

Assume without loss of generality that H is connected. Let T_1 be a maximal

torus of H and T_2 a maximal torus of G containing T_1. Let $\Phi_H = \Phi(H, T_1)$ (resp. $\Phi_G = \Phi(G, T_2)$) be the root system of T_1 (resp. T_2). If $|\Phi_H| < |\Phi_G|$, then $|\Phi_H| \leq |\Phi_G| - 2$ since the size of any abstract root system is divisible by 2. This implies $\dim H = \dim T_1 + |\Phi_H|$ has codimension at least 2 in G. So we may assume $|\Phi_H| = |\phi_G|$.

Let

$$\mathfrak{h} = \mathrm{Lie}(T_1) \bigoplus \left(\bigoplus_{\beta \in \Phi_H} \mathfrak{h}_\beta \right), \ \mathfrak{g} = \mathrm{Lie}(T_2) \bigoplus \left(\bigoplus_{\alpha \in \Phi_G} \mathfrak{g}_\alpha \right)$$

be the root space decompositions of $\mathfrak{h}$ and $\mathfrak{g}$ with respect to Φ_H and Φ_G respectively. Let $\beta_0 \in \Phi_H$ and $0 \neq Y \in \mathfrak{h}_\beta \subset \mathfrak{g}$. Write

$$Y = Y_0 + \sum_{\alpha \in \Phi_G} Y_\alpha$$

where $Y_\alpha \in \mathfrak{g}_\alpha$ for each $\alpha \in \Phi_G$. Then for any $t_1 \in T_1$ we have

$$\mathrm{Ad}(t_1)Y - \mathrm{Ad}(t_1)Y_0 + \sum_{\alpha \in \Phi_G} Y_\alpha = (\beta_0(t_1) - 1)Y_0 + \sum_{\alpha \in \Phi_G} (\beta_0(t_1) - \alpha(t_1))Y_\alpha = 0.$$

This implies $Y_0 = 0$ and hence

$$\bigoplus_{\beta \in \Phi_H} \mathfrak{h}_\beta \subset \bigoplus_{\alpha \in \Phi_G} \mathfrak{g}_\alpha.$$

Since $|\Phi_H| = |\Phi_G|$ these vector spaces have the same dimension and therefore they must be equal. Since $\bigoplus_{\alpha \in \Phi_G} \mathfrak{g}_\alpha$ generates $\mathfrak{g}$ as a Lie algebra and $\bigoplus_{\alpha \in \Phi_G} \mathfrak{g}_\alpha \subset \mathfrak{h}$, $\mathfrak{g} = \mathfrak{h}$ which contradicts the fact that H is proper. □

□

The remainder of the proof of Proposition 8 follows the "ping-pong" argument given in [Var12] and [SGV12]. Parts of the proof their proof is included here for the sake of completion.

Proposition 35. *Let $\mathbb{G}, \Gamma$ and $\rho_1, \dots, \rho_m$ be as in the statement of Proposition 33. Then there exists a subset $\Omega' \subset \Gamma$ that freely generates a subgroup Γ' with the following property. For any $i = 1, \dots, m$ and for any nonzero vector $v \in V_i$*

$$|\{g \in B_\ell(\Omega') | \rho_i(g)([v]) = [v] \text{ where } v \in V_i\}| = |B_\ell(\Omega')|^{1-c'}$$

where c' is a constant depending only on Ω' and the representations.

In order to prove 35, we will need the following [SGV12, Prop. 21]

Proposition 36. *[SGV12, Prop. 21] Let $\mathbb{G}, \Gamma$ and $\rho_1, \dots, \rho_m$ be as above. Then there exists a symmetric set $\Omega' = \Omega'_0 \sqcup (\Omega')_0^{-1} \subset \Gamma$ such that Ω'_0 freely generates a subgroup $\Gamma' \subset \Gamma$, and for every $g \in \Omega'$ and $i = 1, \dots, m$ there exists sets $K_g^{(i)} \subset U_g^{(i)} \subset V_i$ such that for each i, the following properties hold:*

1. *For every $g \in \Omega'$, $\rho_i(g)(U_g^{(i)}) \subset K_g^{(i)}$,*
2. *For every nonzero vector $v \in V_i$, $v \in U_g^{(i)}$ for at least two elements $g \in \Omega'$,*
3. *For any $g_1, g_2 \in \Omega'$, $K_{g_1}^{(i)} \subset U_{g_2}^{(i)}$ unless $g_1 = g_2^{-1}$,*
4. *For any distinct $g_1, g_2 \in \Omega'$, $K_{g_1}^{(i)} \cap K_{g_2}^{(i)} = \emptyset$.*

The sets $K_g^{(i)}$ and $U_g^{(i)}$ are called the contracting and repelling sets of g with respect to ρ_i. These sets give strong restrictions on which words can possibly fix a given line in V_i which we exploit in the proof of Proposition 35.

Proof of Proposition 35. Let Ω' be the set given by Proposition 36 and for any $g \in \Omega'$ let $K_g^{(i)}$ and $U_g^{(i)}$ be the corresponding contracting and repelling sets. We fix an index i and omit the subscripts and superscripts for simplicity.

Fix a vector $v \in V$. For $k < \ell$ define X_k to be the set of words $g_\ell \dots g_1$ such that $\rho(g_k \dots g_1)v \in U_{g_{k+1}}$ and k is the minimal index with this property. Let X_ℓ be the complement of the union of the X_k's. Note that if $g_\ell \dots g_1$ is an element of X_k for $k < \ell$, then

$$\rho(g_{k+1})(\rho(g_k \dots g_1)) \in K_{g_{k+1}} \subset U_{g_{k+2}}.$$

By induction we see that

$$\rho(g_j \dots g_1)v \in U_{g_{j+1}}$$

for $j > k$. Suppose that $\rho(g_\ell \dots g_1)[v] = [v]$. Assume that $v \in K_{g'}$ for some $g' \in \Omega'$. Since $\rho(g_\ell \dots g_1)v = v \in K_{g_\ell}$ and since the contracting spaces for distinct elements of Ω' are disjoint, we see that $g_\ell = g'$ is determined uniquely by v. Continuing this way, we see that g_j is uniquely determined by v for all $j > k$.

By the construction of X_k we know that $\rho(g_{j-1} \dots g_1)v \notin U_{g_j}$ for $j \leq k$. Since $\rho(g_{j-1} \dots g_1)v$ is in at least two different repelling sets U_g, there are only $|\Omega'| - 2$ choices for g_j. Therefore,

$$|\{g \in B_\ell(\Omega') | \rho(g)[v] = [v]\} \cap X_k| \leq (|\Omega'| - 2)^k$$

for all $k = 1, 2, \dots \ell$. If $v \notin K_g$ for any $g \in \Omega'$, then certainly no element of X_k for $k < \ell$ will fix the line spanned by $[v]$ since $\rho(g_\ell g_{\ell-1} \dots g_1)(v) \in K_{g_\ell}$ for $g_\ell g_{\ell-1} \dots g_1 \in X_k$.

By the same argument as above we have

$$|\{g \in B_\ell(\Omega') | \rho(g)[v] = [v]\}| = |\{g \in B_\ell(\Omega') | \rho(g)[v] = [v]\} \cap X_\ell| \leq (|\Omega'| - 2)^\ell$$

which proves the claim. □

Proof of Proposition 8. Let Ω' be the set of generators given by Prop. 35. Let $Q \in \Sigma$ be coprime to Q_1. Let $H \subset \pi_Q(\Gamma)$ be a proper subgroup with the property that for each P dividing Q, $\pi_P(H)$ is a proper structural subgroup of $\pi_P(\Gamma)$.

By Proposition 32 there exists a constant δ with the property that $\mathcal{L}_\delta(H)$ lies in a proper algebraic subgroup of $\mathbb{G}$. Let $\ell \leq c' \log[\pi_Q(\Gamma) : H]$ for some constant c'. If $c' \ll_{\Omega'} 1$, if $h \in B_\ell(\Omega')$ and $\pi_Q(h) \in H$, then $\|h\| < [\pi_Q(\Gamma) : H]^\delta$. Then by definition

$$B_\ell(\Omega') \cap \{h \in \Gamma | \pi_Q(h) \in H\} \subset \mathcal{L}_\delta(H).$$

Combining Propositions 33 and 35, we have

$$|B_\ell(\Omega') \cap \mathcal{L}_\delta(H)| < |B_\ell(\Omega')|^{1-c''}$$

where c'' is the constant from 35.

Let $|\Omega'| = 2M$, so that $|B_\ell(\Omega')| = 2M(2M-1)^{\ell-1}$ for $\ell \geq 1$. Since Ω' generates a free group of Γ, for any k, $\chi^{(k)}_{\Omega'}(g) = \chi^{(k)}_{\Omega'}(g')$ for any $g, g' \in B_\ell(\Omega')$. In particular,

$$\chi^{(k)}(B_\ell \cap \mathcal{L}_\delta(H)) \leq |B_\ell|^{-\delta''} \chi^{(k)}_{\Omega'}(B_\ell) < (2M-1)^{-\delta''\ell} \chi^{(k)}_{\Omega'}(B_\ell).$$

Since the measure $\chi_{\Omega'}$ is symmetric, we have for any positive integer k,

$$\chi_{\Omega'}^{(k)}(0) \geq \chi_{\Omega'}^{(2k)}(0) = \sum_{g\in\Gamma} \chi_{\Omega'}^{(k)}(g)^2.$$

By the Cauchy-Schwarz inequality, $\chi_{\Omega'}^{(k)}(g) \leq \chi_{\Omega'}^{(k)}(0)$ for any $g \in \Gamma$.

By Kesten's result on recurrence to the origin for random walks on trees [Kes59], we have

$$\limsup_{k\to\infty} (P_k(0))^{1/k} = (2M-1)/M^2.$$

This implies $\chi_{\Omega'}^{(k)}(g) \leq ((2M-1)/M^2)^k$ for any positive integer k and any $g \in \Gamma$. We have,

$$\begin{aligned}
\chi_{\Omega'}^{(2k)}(\mathcal{L}_\delta(H)) &= \textstyle\sum_{\ell=1}^{2k} \chi_{\Omega'}^{(2k)}(\mathcal{L}_\delta(H)\cap B_\ell) \\
&= \textstyle\sum_{\ell\leq k/10} \chi_{\Omega'}^{(2k)}(\mathcal{L}_\delta(H)\cap B_\ell) + \sum_{\ell>k/10} \chi_{\Omega'}^{(2k)}(\mathcal{L}_\delta(H)\cap B_\ell) \\
&< \textstyle\sum_{\ell\leq k/10} |\mathcal{L}_\delta(H)\cap B_\ell| \chi_{\Omega'}^{(2k)}(0) + \sum_{\ell>k/10} (2M-1)^{-\delta''\ell} \chi_{\Omega'}^{(k)}(B_\ell) \\
&< (2M)^{k/10} \left(\tfrac{2M-1}{M^2}\right)^k + (2M-1)^{-\delta''k/10} \\
&< \left(\tfrac{(2M)^{11k/10+1}}{M^{2k}}\right) + (2M-1)^{-\delta''k/10},
\end{aligned} \tag{3.12}$$

as required.

□

Chapter 3 contains material coauthored by Professor Alireza Salehi Golsefidy and is in preparation for publication under the title ""Super-approximation" in Absolutely Almost Simple Groups Over $\mathbb{F}_q(t)$". The author of this dissertation is a primary researcher and a primary author of the paper mentioned above.

Chapter 4

ℓ^2-Flattening

This section is dedicated to the proof of Proposition 9. Recall that if $Q \in \mathbb{F}_{q_0}[t]$ is a square free polynomial coprime to Q_1, then $\pi_Q(\Gamma) = \times_{P_{irred.}|Q}\mathbb{G}(\mathbb{F}_{q_P})$ (Eqn. 3.3). We first prove a modified version of Varjú's Product Theorem [Var12, Prop. 14] to show that if each factor $\pi_P(\Gamma)$ exhibits a "triple product growth" phenomenon, then so does $\pi_Q(\Gamma)$. Then, following the methods of Bourgain and Gamburd [BG08b], we show that this implies Proposition 4.

4.1 A variation of Varjú's Product Theorem

Let L be a positive integer and δ' be a positive constant. We must introduce the following assumptions for a finite group G which depend on L and δ'. In what follows, $H \preceq_L H'$ denotes the inequality $[H' : H' \cap H] < L$.

Assumptions $\mathbf{(V1)}_{L,\delta'}$-$\mathbf{(V4)}_{L,\delta'}$

$(\mathrm{V1})_{L,\delta'}$: G is an almost simple group with $|Z(G)| < L$.

$(\mathrm{V2})_{L,\delta'}$: G is $1/L$-quasirandom (c.f. Definition 29).

$(\mathrm{V3})_{L,\delta'}$: There exists an integer $m < L$, and classes of subgroups $\mathcal{H}_0$, $\mathcal{H}_2$,..., $\mathcal{H}_m$ with the following properties:

(i) For each $i = 1, \ldots, m$, $\mathcal{H}_i$ is closed under conjugation by elements in G.

(ii) $\mathcal{H}_0 = \{Z(G)\}$.

(iii) For each subgroup H of G with $|H| > |G|^{\delta'}$ there exists an index $0 \leq i \leq m$, and a subgroup $H^\sharp \in \mathcal{H}_i$ such that $H \preceq_L H^\sharp$.

(iv) For each $i = 0, \ldots, m$, and for each pair of distinct subgroups H_1, $H_2 \in \mathcal{H}_i$, there exists $j < i$ and a subgroup $H^\sharp \in \mathcal{H}_j$ such that $H_1 \cap H_2 \preceq_L H^\sharp$.

$(\mathrm{V4})_{L,\delta'}$: There exists a constant C such that if $S \subset G_i$ is a generating set, then one of the following two statements holds:

(i) $|S| \gg |G_i|^{1-C/L}$,

(ii) $|\Pi_3 S| \geq |S|^{1+1/L}$.

Proposition 37. *Let L be a positive integer. Then for any $\varepsilon > 0$, there exists $\delta, \delta' > 0$ depending only on L and ε such that the following holds: Let $G_1, \ldots, G_n$ be mutually nonisomorphic groups that satisfy assumptions $(V1)_{L,\delta'}$-$(V4)_{L,\delta'}$. Then for any symmetric set $S \subset G = \times_{i=1}^n G_i$ satisfying*

$$|S| < |G|^{1-\varepsilon} \text{ and } \chi_S(gH) < [G:H]^{-\varepsilon}|G|^{\delta}, \tag{4.1}$$

we have

$$|\Pi_3 S| \gg_\varepsilon |S|^{1+\delta}.$$

Remark 38. More generally, in light of Inequality 4.5 below, we can replace the condition that the groups $G_1, \ldots, G_n$ are mutally nonisomorphic with the following: There are at most $M \ll_v are1$ groups amongst $G_1, \ldots, G_n$ of size $\ll_\varepsilon 1$. We do not need this statement here, but it would be useful if we remove the condition that the degrees of the irreducible factors of Q be distinct.

The key difference between Proposition 37 and [Var12, Prop. 14] is that we have a family of assumptions depending on a constant ε rather than a single set of assumptions. This will be sufficient for us since we need to apply Proposition 37 to a specific positive constant ε_0 which depends only on $\mathbb{G}$. Secondly, we use the assumption $(\mathrm{V4})_{L,\delta'}$ in place of assumption $(A4)$ in [Var12, Prop. 14]. Assumption $(\mathrm{V4})_{L,\delta'}$ implies (A4) by the work of [BG08b]. To our knowledge, it is not known whether or not these conditions are equivalent. Lastly, we note that the proof of [Var12, Cor. 14] has a mistake which our proof corrects. Varjú has also communicated to us a way to correct the proof without changing assumption $(A4)$.

Crucial to the proofs of Propositions 9 and 37 is the following lemma, which was implicitly proved by Bourgain and Gamburd in [BG08b] and is based on the noncommutative version of a theorem of Balog, Gowers, and Szméredi proved by Tao [Tao08]. The lemma in its current form is included in [Var12].

Lemma 39. *Let μ and ν be two probability measures on an arbitrary finite group G, and let K be a real number greater than 2. If*

$$\|\mu * \nu\|_2 > \frac{\|\mu\|_2^{1/2} \|\nu\|_2^{1/2}}{K}$$

then there is a symmetric set $A \in G$ with the following properties:

$$\frac{1}{K^R \|\mu\|_2^2} \ll |S| \ll \frac{K^R}{\|\mu\|_2^2} \tag{4.2}$$

$$|\Pi_3 S| \ll K^R |S| \tag{4.3}$$

$$\frac{K^- R}{|S|} \ll \min_{g \in S} (\widetilde{\mu} * \mu)(g) \tag{4.4}$$

where R and the implied constants are universal.

Proof of Proposition 37

The majority of this proof is due to Varjú [Var12, Prop. 14]. The necessary changes are found in the proofs of Corollary 43 and Proposition 40 to account for our modified assumptions. In particular, the proof of Proposition 44 remains unchanged. The full proof is included here for completeness.

Fix a positive constant ε and let δ and δ' be small constants. We will assume δ and δ' are sufficiently small in the sense that if $K > 0$ is a constant which only depends on ε, L, and the constants in assumptions $(\mathrm{V1})_{L,\delta'}$-$(\mathrm{V4})_{L,\delta'}$, then $\delta, \delta' < K$. Suppose we have n nonisomorphic groups $G_1, \ldots, G_n$ which satisfy assumptions $(\mathrm{V1})_{L,\delta'}$-$(\mathrm{V4})_{L,\delta'}$ and a subset $S \subset G = \times_{i=1}^n G_i$ as in the hypotheses of the proposition. We may assume the groups $|G_i|$ are sufficiently large in the sense that inequalities of the form

$$K \log |G_i| < |G|^{\delta\delta''} \tag{4.5}$$

hold where K and δ'' are constants depending only on ε and L. Indeed, let N be the product of those factors for which such an inequality fails. Then since each

group is distinct up to isomorphism, $|N|$ is bounded in terms of δ. For any subgroup $H \subset G/N$, $[G/N : H] = [G : HN]$. Furthermore, if S' is the projection of S mod N, $|\Pi_3 S| \geq |\Pi_3 S'|$ and $|S'| \geq |S|/|N|$. Therefore if the claim is true for G/N, we have

$$\chi_{S'}(g'H) = [G/N : H]^{-\varepsilon}|G/N|^{\delta} < [G : HN]^{-\varepsilon}|G|^{\delta}$$

satisfies the hypotheses of the proposition and we have

$$|\Pi_3 S| \geq |\Pi_3 S'| \gg_{\varepsilon} |S'|^{1+\delta} \geq (|S|/|N|)^{1+\delta} \gg_{\varepsilon} |S|^{1+\delta}.$$

If the proposition is true for the group G/N, then it is true for the group G with a worse implied constant depending on ε.

For $1 \leq i \leq n$ we set $\mathrm{pr}_{\leq i}$ to be the projection of G onto the first i factors and we set $\pi_0(G) = \langle 1 \rangle$. From the set S we obtain a tree with $n+1$ levels in the following way. The vertices on the i^{th} level are the elements of $\mathrm{pr}_{\leq i}(S)$, and a vertex $(s_j)_{j=1}^{i-1}$ on the $(i-1)^{th}$ level is connected to each vertex on the i^{th} level of the form $((s_j)_{j=1}^{i-1}, h)$ for each $h \in \mathrm{pr}_i(S)$. By [BGS10, Section 5] there exists a subset $A \subset S$ with the following property: For each $1 \leq i \leq n$, there exists a positive integer D_i such that for each $(a_j)_{j=1}^{i-1} \in \mathrm{pr}_{\leq i-1}(A)$

$$\{h \in \mathrm{pr}_i(A) \mid ((a_j)_{j=1}^{i-1}, h) \in \mathrm{pr}_{\leq i}(A)\} = D_i$$

and

$$|A| > (\Pi_{i=1}^{n} |G_i|^{\delta} \log |G_i|)^{-1} |S| > |G|^{-2\delta}|S|.$$

The last inequality is an inequality of the form (4.5). Furthermore for each i, $D_i > |G_i|^{\delta}$

or $D_i = 1$.

We partition the set $\{1, 2, \ldots, n\}$ into two sets I_s and I_ℓ. I_s is the set of indices i with the property that $D_i < |G_i|^{1-1/3L}$, and $I_\ell = \{1, 2, \ldots, M\} \setminus I_s$. We set pr_s and pr_ℓ to be the projections of G onto $\times_{i\in I_s} G_i$ and $\times_{i\in I_\ell} G_i$ respectively and set $G_s = \mathrm{pr}_s(G)$, $G_\ell = \mathrm{pr}_\ell(G)$. For $i \in I_s$, we hope to apply assumption $(\mathrm{V4})_{L,\delta'}$ to the fibres of A under the projection from the i^{th} factor to the to the $(i-1)^{th}$ factor to show $\mathrm{pr}_s(A)$ grows after taking the product with itself three times. However, we have little control over these sets. In particular we do not know if the fibres generate the group $G_i, i \in I_s$ so we cannot apply assumption $(\mathrm{V4})_{L,\delta'}$ directly. To deal with this, we multiply $\mathrm{pr}_i(A)$ by random elements in S and use assumption $(\mathrm{V4})_{L,\delta'}$ and Lemma 39 to obtain a probability measure λ supported on a bounded product of S which is small in the ℓ^2-norm. This in turn will imply growth in a bounded product of $\mathrm{pr}_s(A)$. For the indices $i \in I_l$, the fibres are too large and so after taking a product of itself three times, each fibre generates the group. Nevertheless, Varjú's argument using Farrah's notion of "approximate homomorphisms" shows that the projection of S to G_ℓ still contributes the growth of S after taking the product with itself three times.

We first prove the following version of proposition ([Var12, Prop. 16]) whose proof must be altered slightly to fit our needs.

Proposition 40. *There exists positive constants δ_s and Q depending only on ε and L such that*

$$|\Pi_{2^{m+1}} S| > |S||G|^{-Q\delta} \Pi_{i\in I_s} D_i^{\delta_s},$$

where m is the constant in $(V4)_{L,\delta'}$.

As mentioned in the previous section, the goal is to multiply the set

$$\{(b \in \mathrm{pr}_i(A) \mid ((a_j)_{j=1}^{i}, b) \in \mathrm{pr}_{\leq i}(A)\}$$

by suitably chosen random elements of G_i so that the resulting set is nicely distributed in G_i. In particular, we need to choose random elements from a subset B of S that has the property that $\pi_i(B)$ does accumulate on proper cosets of G_i for $i \in I_s$. The following lemma provides the required probability distribution.

Lemma 41. *There exists a subset $B \subset S$ and a partition of the set $\{1, 2, \ldots, n\} = J_g \sqcup J_b$ such that*

$$\Pi_{i \in J_b} |G_i| \leq |G|^{\delta/\delta''}, \tag{4.6}$$

and for any $i \in J_g$ and for any proper coset $gH \subset G_i$,

$$\chi_B(\{x \in G | \, \mathrm{pr}_i(x) \in gH\}) \leq |G_i|^{-\delta''}, \tag{4.7}$$

where $\delta'' > 0$ is a constant which only depends on ε and L.

Proof. B is constructed by the following algorithm: Initialize $B = S$, $J_g = \{1, 2, \ldots, n\}$, and $J_b = \emptyset$. If there exists an index i and a proper coset $gH \subset G_i$ with

$$\chi_B(\{x \in G | \, \mathrm{pr}_i(x) \in gH\} \geq |G_i|^{-\delta''},$$

then put i into J_b and replace B by

$$\{x \in B | \, \mathrm{pr}_i(x) \in gH\}.$$

When this property terminates, (4.7) holds. Note that by assumption $(\mathrm{V2})_{L,\delta'}$ applied to the induced representation, the index of any subgroup of G_i for any $1 \leq i \leq k$ is at least $|G_i|^{1/L}$. By construction B is contained in a coset of subgroup of G of index at least $\Pi_{i\in J_b}|G_i|^{1/L}$ and

$$\chi_S(B) \geq \Pi_{i\in J_b}|G_i|^{\delta''}.$$

By the second assumption on the set S in the hypotheses of Proposition 37,

$$\Pi_{i\in J_b}|G_i|^{-\delta''} < \left(\Pi_{i\in J_b}|G_i|^{1/L}\right)^{-\varepsilon}|G|^{\delta}.$$

The inequality (4.6) holds if $\delta'' < \varepsilon/2L$. □

Choose elements x_i, $1 \leq j \leq 2^m - 1$, independently at random according to the distribution χ_B. For an index $i \in J_g$ let $y_j := \mathrm{pr}_i(x_j)$ and let $A_1, A_2, \ldots, A_{2^m} \subset G_i$ be arbitrary subsets of constant size D where $|G_i|^{\delta} < D < |G_i|^{1-1/3L}$. Let

$$\lambda_m := \chi_{A_1} * \mathbb{1}_{y_1} * \chi_{A_2} * \mathbb{1}_{y_2} * \cdots * \chi_{A_{2^m-1}} * \mathbb{1}_{y_{2^m-1}} * \chi_{A_{2^m}}.$$

We will show that with high probability, λ_m does not accumulate on any proper coset. We need the following:

Lemma 42 (Lemma 18 [Var12])**.** *For every $i \in J_g$, there exists a constant δ'' depending only on ε and L such that the probability that*

$$\lambda_k(gH) < D^{-\delta''/10^k} \tag{4.8}$$

for any $g \in G_i$ and $H \in \cup_{l \leq k} \mathcal{H}_l$ is at least

$$1 - (2^k - 1)|G_i|^{-\delta''}$$

for any choice of sets $A_1, \ldots, A_{2^m}$.

Proof. Let δ'' be twice the δ'' from the previous lemma. We proceed by induction on k. If $k = 0$, then

$$\lambda_0(gZ(G_i)) = \chi_{A_1}(gZ(G_i)) \leq L/D_i < D^{-\delta''}$$

where the last inequality is an inequality of the form (4.5).

For the inductive step, assume the claim holds for $k > 1$. Write $\lambda_{k+1} = \lambda_k * \mathbb{1}_{y_{2^k}} * \nu_k$ where

$$\nu_k = \chi_{A_{2^k+1}} * \mathbb{1}_{y_{2^k+1}} * \cdots * \mathbb{1}_{y_{2^{k+1}-1}} * \chi_{A_{2^{k+1}}}.$$

By the induction hypothesis, the probability that

$$\lambda_k(gH) < D^{-\delta''/10^k} \text{ and } \nu_k(gH) < D^{-\delta''/10^k}$$

for all $H \in \mathcal{H}_k$ and $g \in G_i$ is at least $1 - (2^{k+1} - 2)|G_i|^{-\delta''}$. Assume that there exists $H \in \mathcal{H}_{k+1}$ and $g \in G_i$ such that $\lambda_{k+1}(gH) \geq D^{-\delta''/10^{k+1}}$. Fix a full set of coset representatives $\{g_j\}_{j=1}^{[G_P:H]}$ of H. Then

$$\lambda_{k+1}(gH) = \sum_{j=1}^{[G_P:H]} \lambda_k(gHg_j^{-1})\nu_k(y^{-1}h_jH) \tag{4.9}$$

where $y := y_{2^k}$.

Now for some index j, we have

$$\lambda_k(gHg_j^{-1}) \geq D^{-\delta'/10k}/2 \text{ and } \nu_k(yg_j^{-1}H) \geq D^{-\delta'/10k}/2, \tag{4.10}$$

for otherwise we have

$$\begin{aligned}\sum_{j=1}^{[G_P:H]} \lambda_k(gHg_j^{-1})\nu_k(y^{-1}h_jH) &= \sum_{j:\lambda_k(gHg_j^{-1})<D^{-\delta'/10k}/2} \lambda_k(gHg_j^{-1})\nu_k(y^{-1}h_jH) \\ &\quad + \sum_{j:\nu_k(yg_j^{-1}H)<D^{-\delta'/10k}/2} \lambda_k(gHg_j^{-1})\nu_k(y^{-1}h_jH) \\ &< D^{-\delta'/10^{k+1}}\end{aligned}$$

which is a contradiction.

Let j be an index satisfying (4.9). Then $(gHg_j^{-1})^{-1}gHg_j^{-1} \subset g_jHg_j^{-1}$ and $y^{-1}h_jH(y^{-1}h_jH)^{-1} \subset y_{-1}g_jHg_j^{-1}y$. Let $H_1 := g_jHg_j^{-1}$ and $H_2 := y_{-1}g_jHg_j^{-1}y = y^{-1}H_1y$. Since $\mathcal{H}_{k+1}$ is closed under conjugation, we have subgroups $H_1, H_2 \in \mathcal{H}_{k+1}$ such that

$$(\tilde{\lambda_k} * \lambda_k)(H_1) \geq D^{-2\delta'10^{k+1}}/4, \tag{4.11}$$

and

$$(\nu_k * \tilde{\nu_k})(H_2) \geq D^{-2\delta'10^{k+1}}/4. \tag{4.12}$$

Note that in this case y is in a fixed coset of $N_{G_i}(H_2)$, which by (4.7) has χ_B measure less than $|G_i|^{\delta''/2}$. We are done once we show the number of pairs H_1, H_2 for which (4.11) holds is also less than $|G_i|^{\delta''/2}$.

Let M be the number of subgroups which satisfy (4.11) and let $H_1, H_1' \in \mathcal{H}_{k+1}$

be two such subgroups. By assumption $(\mathrm{V3})_{L,\delta'}$(iv) and the inductive hypothesis, $\lambda_k(H_1 \cap H_1') < D^{-\delta''/10^k)}$. By the inclusion exclusion principle

$$MD^{-2\delta''/10^{k+1}}/4 - M^2 L D^{-\delta''/10^k} \leq 1.$$

If we assume $D^{\delta''}/2(10^{k+1}) > 4(1+L)$, which is an inequality of type (4.5), then $M < D^{\delta''/4(10^k)}$. Similarly, there are at most $D^{\delta''/4(10^k)}$ subgroups which satisfy (4.12), which completes the proof. □

Now with our modified assumptions we can prove the following corollary which is analogous to [Var12, Cor. 19].

Corollary 43. *Let $i \in J_g \cap I_s$, λ_m be the measure defined above and $A' \subset G_i$ be an arbitrary set of cardinality D_i. There exists a positive constant δ'' depending only on ε and L such that the probability that*

$$\|\lambda_m * \chi_{A'}\|_2 \ll D_i^{-1/2-\delta''}$$

is at least $1/2$.

Proof. By the previous lemma (and an inequality of the form (4.5)), there exists $\delta'' > 0$ such that with probability at least $1/2$ that $\lambda_m(gH) < LD^{-\delta_3}$ for every $g \in G_i$ and every proper subset H such that $|H| > |G|^{\delta'}$. We also have $L < D^{\delta''/2}$ which is an inequality of the form (4.5). If $\|\lambda_m\|_2 \leq |G_i|^{-1/2+1/12L}$, then the claim is trivial by Young's inequality. So suppose $\|\lambda_m\|_2 > |G_i|^{-1/2+1/12L}$ and assume for the sake of contradiction that

$$\begin{aligned} \|\lambda_m * \chi_{A'}\| &\gg D^{-1/2-\delta_3} \\ &= \|\lambda_m\|_2^{1/2} \|\chi_{A'}\|_2^{1/2} D^{-\delta_3} \end{aligned}$$

for every positive constant δ_3. Note that $D^{-1/4} = \|\chi_{A_1}\|_2 \geq \|\lambda_m\|_2$ by Young's inequality. Then by Lemma 39, there exists a symmetric set $X \subset G_i$ with the following properties:

$$\frac{1}{D^{\Theta(\delta_3)}\|\lambda_m\|_2^2} \ll |X| \ll \frac{D^{\Theta(\delta_3)}}{\|\lambda_m\|_2^2}, \tag{4.13}$$

$$|\Pi_3 X| \ll D^{\Theta(\delta_3)}|X|, \tag{4.14}$$

$$(\widetilde{\lambda_m} * \lambda_m)(X) \gg D^{-\Theta(\delta_3)}. \tag{4.15}$$

By (4.15)

$$(\widetilde{\lambda_m} * \lambda_m)(X) = \sum_{g \in G_i} \lambda_m(g)\lambda_m(g\langle X\rangle) \geq D^{-\Theta(\delta_3)} > D^{-\delta''/2}$$

where the last inequality holds if δ_3 is sufficiently small. Therefore either $|\langle X\rangle| < |G_i|^{\delta'}$ or $\langle X\rangle = G_i$. By (4.13),

$$|X| \geq \frac{1}{\|\lambda_m\|_2^2 D^{\Theta(\delta_3)}} \geq D^{1/2-\Theta(\delta)} > |G_i|^{\delta/4} > |G_i|^{\delta'}$$

where the last inequality holds if δ_3 is sufficiently small and $\delta' < \delta/4$. Therefore, X generates G_i. By assumption $(\mathrm{V4})_{L\delta'}$ and (4.14)

$$|X| > |G_i|^{1-\varepsilon_0}$$

for some positive constant ε_0 which depends on δ_3.

Again by (4.13),

$$\begin{aligned} |G_i|^{1-\varepsilon_0} &< |X| \\ &< D^{\Theta(\delta_3)}\|\lambda_2\|_2^{-2} \\ &< D^{\Theta(\delta_3)}|G_i|^{1-1/6L} \\ \Rightarrow D^{\Theta(\delta_3)}|G_i|^{\varepsilon_0} &> |G_i|^{1/6L}. \end{aligned}$$

Since $\varepsilon_0 \to 0$ as $\delta_3 \to 0$, this is a contradiction and the corollary is proven.

□

Let

$$\lambda = \chi_A * \mathbb{1}_{x_1} * \chi_A * \mathbb{1}_{x_2} * \cdots * \mathbb{1}_{x_{2^m+1}} * \chi_A\chi_A.$$

For each $1 \leq i \leq n$, let

$$\mathrm{pr}_{i,i-1} : \times_{j=1}^{i} G \to \times_{j=1}^{i-1} G.$$

For $i \in I_s \cap J_g$ we will apply Corollary 43 to the sets $A_{i,g} = {\mathrm{pr}_{i,i-1}}^{-1}(g) \cap A$ for each $g \in \mathrm{pr}_{\leq i-1}(A)$ which are all sets of size D_i by construction. This will give us an upper bound on $\|\lambda\|_2$.

Proof of Proposition 40. For any collection of subsets $X_1, X_2, \ldots, X_k$ of a finite group G, it is easy to see that for any $g \in G$,

$$(\chi_{X_1} * \chi_{X_2} * \cdots * \chi_{X_k})(g) = \frac{|\{(x_j)_{j=1}^k \in \Pi_{j=1}^k X_j \mid x_1x_2\ldots x_k = g\}|}{|X_1||X_2|\ldots|X_k|}.$$

For each $1 \leq j \leq n$ let $\lambda_{\leq j}$ be the measure on $G_{\leq j}$ defined by

$$\lambda_{\leq j} = \chi_{A_{\leq j}} * \mathbb{1}_{\mathrm{pr}_{\leq j}(x_1)} * \chi_{A_{\leq j}} * \mathbb{1}_{\mathrm{pr}_{\leq j}(x_2)} * \cdots * \mathbb{1}_{\mathrm{pr}_{\leq j}(x_{2^m+1})} * \chi_{A_{\leq j}} * \chi_{A_{\leq j}}.$$

For each $g \in G_{\leq j}$ let $\lambda_{g,j}$ be the measure on G_j defined by

$$\lambda_{g,j} = \chi_{A_{g,j}} * \mathbb{1}_{\mathrm{pr}_j(x_1)} * \chi_{A_{g,j}} * \mathbb{1}_{\mathrm{pr}_j(x_2)} * \cdots * \mathbb{1}_{\mathrm{pr}_j(x_{2^m+1})} * \chi_{A_{g,j}} * \chi_{A_{g,j}}.$$

We prove by induction that for $1 \leq j \leq n$, the expected value of the random variable $\|\lambda_{\leq i}\|_2^2$ is less than

$$\left(\prod_{i \leq j : i \in I_s \cap J_g} C D_i^{-1-\delta''}\right)\left(\prod_{i \leq j : i \notin I_s \cap J_g} D_i^{-1}\right)$$

where C is the implied constant from Corollary 43.

The case when $i = 1$ follows directly from Corollary 43 and the inequality $\|\lambda_{1_G,1}\|_2 \leq \|\chi_{\mathrm{pr}_1(A)}\|_2 = D_1^{-1/2}$ which follows from Young's inequality. Now assume the claim is true for $1 < j < n$.

Then by computing the expected value of the random variable $\|\lambda\|_2^2$ we have,

$$\begin{aligned}
\mathbb{E}\left(\|\lambda\|_2^2\right) &= \mathbb{E}\left(\sum_{g \in G} (g)^2\right) \\
&= \mathbb{E}\left(\sum_{g_1 \in \mathrm{pr}_{j-1}(G)} \sum_{g_2 \in G_j} \lambda((g_1, g_2))^2\right) \\
&= \mathbb{E}\left(\sum_{g_1 \in \mathrm{pr}_{j-1}(G)} \sum_{g_2 \in G_j} \lambda_{\leq n-1}(g_1)^2 \lambda_{n,g_1}(g_2)^2\right) \\
&= \mathbb{E}\left(\sum_{g_1 \in \mathrm{pr}_{j-1}(G)} \lambda_{\leq j-1}(g_1)^2 \left(\sum_{g_2 \in G_n} \lambda_{n,g_1}(g_2)^2\right)\right) \\
&= \mathbb{E}\left(\sum_{g_1 \in \mathrm{pr}_{j-1}(G)} \lambda_{\leq j-1}(g_1)^2 \|\lambda_{j,g}\|_2^2\right) \\
&< \begin{cases} C D_j^{-1-\delta''} \mathbb{E}\left(\|\lambda_{\leq j-1}\|_2\right) & \text{if } j \in I_s \cap J_g \\ D_j^{-1}) \mathbb{E}\left(\|\lambda_{\leq j-1}\|_2\right) & \text{if } j \notin I_s \cap J_g \end{cases} \\
&< \left(\prod_{i \leq j : i \in I_s \cap J_g} C D_i^{-1-\delta''}\right)\left(\prod_{i \leq j : i \notin I_s \cap J_g} D_i^{-1}\right)
\end{aligned}$$

which proves the claim.

This implies that for some choice of $x_1, x_2, \ldots, x_{2^m+1}$, we have

$$\begin{aligned} |Ax_1Ax_2\ldots Ax_{2^m+1}AA| = |\operatorname{Supp}\lambda| &> \|\lambda\|_2^{-2} \\ &> \left(\prod_{i\in I_s\cap J_g} C^{-1}D_i^{1+2\delta''}\right)\left(\prod_{i\notin I_s\cap J_g} D_i\right) \\ &= |A|C^{-n}\left(\prod_{i\in I_s\cap J_g} D_i^{2\delta''}\right) \\ &> |A|C^{-n}|G|^{-\delta/2}\left(\prod_{i\in I_s} D_i^{2\delta''}\right) \\ &> |S||G|^{-Q\delta}\left(\prod_{i\in I_s} D_i^{2\delta''}\right) \end{aligned} \tag{4.16}$$

where we used the inequalities $|A| > |S||G|^{-2\delta}$, $C^n|G|^{\delta}$ which is of type (4.5), and Inequality (4.6). □

In order to deal with the indices of large degree, we use the following proposition whose proof, due to Varjú, is included here for the sake of completeness:

Proposition 44 (Proposition 20 [Var12])**.** *There exists a positive constant δ_l depending only on ε and L such that*

$$|\Pi_9 S| > |G|^{\delta_l-\delta}\Pi_{i\in I_l} D_i.$$

Recall that $G_s = \times_{i\in I_s} G_i$, $G_l = \times_{i\in I_l} G_i$ and let pr_s, pr_l be the projections to these subgroups. Nikolov and Pyber [NP11, Cor. 1] showed that a result of Gowers [Gow08, Thm. 3.3] implies that if $A, B, C \subset G_i$ are subsets that satisfy $|A||B||C| > |G_i|^{3-1/L}$ then $ABC = G_i$ where $|G_i|^{1/L}$ is a lower bound for the dimension of any nontrivial representation of G_i (assumption $(\mathrm{V2})_{L,\delta'}$.

Let $i_1, i_2, \ldots i_{n'}$ be the indices in I_l and for $1 \le k \le n'$ let $G_{\{1,2,\ldots i_k\}} = G_{i_1} \times G_{i_2} \times G_{i_k}$ and let $\mathrm{pr}_{\{1,2,\ldots,i_k\}}$ be the projection to this subgroup. We claim that

$\mathrm{pr}_{\{1,2,\ldots i_k\}}(\Pi_3 A) = G_{\{i_1,i_2,\ldots,i_k\}}$.

The base case $k = 1$ has already been mentioned. Assume the claim is true for $k > 1$ and let $g \in G_{\{i_1,\ldots,i_k\}}$. By the induction hypothesis, there exist $a_1, a_2, a_3 \in A$ such that $\mathrm{pr}_{\{1,2,\ldots,i_k\}}(a_1a_2a_3) = \mathrm{pr}_{\{1,2,\ldots,i_k\}}(g)$. Let

$$B_i = \{x \in A | \, \mathrm{pr}_{\{1,2,\ldots,i_k\}}(x) = \mathrm{pr}_{\{1,2,\ldots,i_k\}}(a_i)\}$$

and note that

$$\mathrm{pr}_{\{1,2,\ldots,i_{k+1}\}}(B_i) \supset \mathrm{pr}_{\{1,2,\ldots,i_{k+1}\}}(\{x \in A | \, \mathrm{pr}_{\leq i_{k+1}}(x) = \mathrm{pr}_{\leq i_{k+1}}(a_i)\})$$

and hence $|\,\mathrm{pr}_{\{1,2,\ldots,i_{k+1}\}}(B_i)| \geq D_{i_{k+1}} \geq |G_{i_{k+1}}|^{1-1/3L}$. Now apply [NP11, Cor. 1] to the sets $\mathrm{pr}_{\{1,2,\ldots,i_{k+1}\}}(B_i)$ to establish the claim.

Define a distance function on G_s by

$$d(g,h) = \sum_{i \in I_s | \mathrm{pr}_i(g) \neq \mathrm{pr}_i(h)} \log |G_i|.$$

Lemma 45. *If $|\Pi_3 S| \leq |G|^{1-\varepsilon+\delta}$ then there exists an element $g \in \Pi_6 S$ such that $\mathrm{pr}_l(g) = 1$ and*

$$d(\mathrm{pr}_s(g), 1) > \delta'' \log |G|,$$

where $\delta'' > 0$ is a constant depending on ε and L.

We introduce the notion of an approximate homomorphism that was given by Farah [Far00]. A function $\psi : G_l \to G_s$ is a δ''-approximate homomorphism if

$$d(\psi(g)\psi(h), \psi(gh)) \leq \delta''$$

and

$$d(\psi(g), \psi(g^{-1})^{-1}) \leq \delta''$$

for all $g, h \in G_l$.

By [Far00, Thm 2.1], if $\psi : G_l \to G_s$ is a δ''-approximate homomorphism, then there exists a homomorphism $\phi : G_l \to G_s$ such that

$$d(\psi(g), \phi(g)) \leq 24\delta'' \tag{4.17}$$

for all $g \in G_l$.

Proof of Lemma 45. Assume for the sake of contradiction that for any $g \in \Pi_6 S$ with $\mathrm{pr}_l(g) = 1$, $d(\mathrm{pr}_s(g), 1) \leq \delta'' \log |G|$. For each $g \in G_l$, we can find $h \in \Pi_6 S$ such that $\mathrm{pr}_l(h) = g$ by the above argument. Set $\psi(g) = \mathrm{pr}_s(h)$. If $h_1, h_2 \in \Pi_6 S$ such that $\mathrm{pr}_l(h_1) = \mathrm{pr}_2(h_2)$, then by the assumption we have

$$d(\mathrm{pr}_s(h_1), \mathrm{pr}_s(h_2)) = d(\mathrm{pr}_s(h_1 h_2^{-1}, 1) < \delta'' \log |G|.$$

If $g_1, g_2 \in G_l$, and if $h_1, h_2, h_3 \in \Pi_3 S$ satisfy $\psi(g_1) = \mathrm{pr}_s(h_1)$, $\psi(g_2) = \mathrm{pr}_s(h_2)$ and $\psi(g_1 g_2) = \mathrm{pr}_s(h3)$, then since $\mathrm{pr}_l(h_1 h_2) = \mathrm{pr}_l(h_3)$ we have

$$d(\psi(g_1 g_2), \psi(g_1)\psi(g_2)) = d(\mathrm{pr}_s(h_3), \mathrm{pr}_s(h_1 h_2)) < \delta'' \log |G|.$$

Similarly if $h_4 \in \Pi_3 S$ satisfies $\psi(g_1^{-1}) = \mathrm{pr}_s(h_4)$, then $\mathrm{pr}_l(h_1^{-1}) = \mathrm{pr}_l(h_4)$, whence

$$d(\psi(g_1^{-1}), \psi(g_1)^{-1}) = d(\mathrm{pr}_s(h_4), \mathrm{pr}_s(h_1^{-1})) < \delta'' \log |G|.$$

Therefore ψ is a $\delta'' \log |G|$-approximate homomorphism.

By [Far00, Thm. 2.1], there exists a homomorphism $\phi : G_l \to G_s$ such that $d(\psi(g), \phi(g)) \leq 24\delta'' \log |G|$ for any $g \in G_l$. Let H be the subgroup of G defined by

$$H = \{g \in G \mid \mathrm{pr}_s(g) = \phi(\mathrm{pr}_l(g))\}.$$

If $g \in G$, $h \in H$, we have

$$\begin{aligned} \mathrm{pr}_s(g)\phi(\mathrm{pr}_l(g))^{-1} &= \mathrm{pr}_s(g)\,\mathrm{pr}_s(h)\phi(\mathrm{pr}_l(h))^{-1}\phi(\mathrm{pr}_l(g))^{-1} \\ &= \mathrm{pr}_s(gh)\phi(\mathrm{pr}_l(gh))^{-1}. \end{aligned} \tag{4.18}$$

Clearly for $g_s \in G_s$, $\mathrm{pr}_s(g_s)\phi(\mathrm{pr}_l(g_s))^{-1} = g_s$. Therefore the cosets of H are in bijective correspondence with the elements of G_s and hence H has index $|G_s|$.

For any $h_1 \in \Pi_3 S$, the coset $h_1 H$ containing h_1 is represented by the element $g_1 = \mathrm{pr}_s(h_1)\phi(\mathrm{pr}_l(h_1))^{-1} \in G_s$. Since

$$\begin{aligned} d(\mathrm{pr}_s(h_1)\phi(\mathrm{pr}_l(h_1))^{-1}, 1) &= d(\mathrm{pr}_s(h_1), \phi(\mathrm{pr}_l(h_1))) \\ &\leq d(\mathrm{pr}_s(h_1), \psi(\mathrm{pr}_l(h_1))) + d(\psi(\mathrm{pr}_l(h_1)), \phi(\mathrm{pr}_l(h_1))) \\ &< 25\delta'' \log |G| \end{aligned} \tag{4.19}$$

there is a set of indices $I_{h_1} \subset I_s$ such that $g_1 \in \times_{i \in I_{h_1}} G_i$ and $|\times_{i \in I_{h_1}} G_i| < |G|^{25\delta''}$. Hence, there are at most $|G|^{25\delta''}$ choices for g_1. Since there are at most 2^n possibilities for I_{h_1}, $\Pi_3 S$ is contained in $2^n |G|^{25\delta''} < |G|^{26\delta''}$ cosets of H.

By the hypotheses on the set S, we have

$$1 = \sum_{gH \supset S.S.S \supset S} \chi_S(gH) < |G_s|^{-\varepsilon} |G|^{26\delta'' + \delta}.$$

Since $|G_l| \leq |\Pi_3 S| \leq |G|^{1-\varepsilon-\delta}$, $|G_s| \geq |G|^{\varepsilon-\delta}$. Therefore,

$$|G_s|^{-\varepsilon}|G|^{26\delta''+\delta} < |G|^{26\delta''+\delta+\varepsilon\delta-\varepsilon^2}.$$

This is a contradiction if $\delta < \varepsilon^2/4$ and $\delta'' < \varepsilon^2/26 \cdot 4$.

□

Proof of Proposition 44. Let g be the element found in Lemma 45. An element $h \in G$ commutes with g if and only if $\mathrm{pr}_i(h) \in C_{G_i}(\mathrm{pr}_i(g_i))$ for $1 \leq i \leq n$. If i is an index with $\mathrm{pr}_i(g) \neq 1$, then by assumption $(\mathrm{V2})_{L,\delta'}$ applied to the induced representation, we have $[G_i : C_{G_i}(g))] > |G_i|^{1/L}$. Recall that we assumed each G_i is simple, and hence $C_{G_i}(\mathrm{pr}_i(g)) \neq G_i$ since $Z(G_i)$ is trivial. This implies $[G : C_G(g)] > |G|^{\delta''/L}$ where δ'' is the constant found in Lemma 45. Let M be the number of cosets of $C_G(g)$ which have nontrivial intersection with S. Then by the hypotheses on S,

$$\begin{aligned} 1 &= M \textstyle\sum_{h:hC_G(g)\cap S\neq 0} \chi_S(hC_G(g)) \\ &< M[G : C_G(g)]^{\varepsilon}|G|^{\delta} \\ &< M|G|^{-\varepsilon\delta''/L-\delta} \\ \Rightarrow \quad M &> |G|^{\varepsilon\delta''/L-\delta}. \end{aligned}$$

This implies that the set

$$\{sgs^{-1} | s \in S\} \subset \Pi_8 S$$

contains at least $|G|^{\varepsilon\delta''/L-\delta}$ distinct elements h with $\mathrm{pr}_l(h) = 1$, which implies

$$|\Pi_9 S| \geq |G|^{\varepsilon\delta''/L-\delta}\Pi_{i\in I_l} D_i.$$

□

Proof of Proposition 37. By propositions 40 and 44 there exist constants δ_s, δ_l, and Q that are independent of δ such that

$$|\Pi_{2^m+1}S| > |S||G|^{-Q\delta_s}\Pi_{i\in I_s}D_i^{\delta_s}$$

and

$$|\Pi_9 S| > |G|^{\delta_l-\delta}\Pi_{i\in I_l}D_i.$$

Combining these equations we have

$$|\Pi_{2^m+1}S||\Pi_9 S|^{\delta_s} > |S||G|^{-\delta_s(Q+\delta)}|G|^{\delta_s\delta_l}\Pi_{i=1}^k D_i^{\delta_s}.$$

Since $|G| > |S|$ and $\Pi_{i=1}^n D_i = |A| > |S||G|^{-2\delta}$ we get

$$|\Pi_{2^m+1}S||\Pi_9 S|^{\delta_s} > |S|^{1+\delta_s+\delta_s\delta_l}|G|^{-Q\delta}.$$

By [Hel08, Lemma 2.2]

$$\frac{|\Pi_k S|}{|S|} \leq \left(\frac{|\Pi_3 S|}{|S|}\right)^{k-2}$$

and by the second hypothesis on the set S applied to the trivial subgroup we have $|S| > |G|^{\varepsilon-\delta}$. Therefore the claim is proven if δ is sufficiently small. □

4.1.1 Proof of Proposition 9

Proof of Proposition 9. We proceed in a similar manner as in the proof of Corollary 43. Let $Q \in \mathbb{F}_{q_0}[t]$ be a square free polynomial coprime to Q_1. Let $G_Q = \pi_Q(\Gamma)$. Assume that for each irreducible factor P of Q, $\deg(P)$ has no divisors smaller than a constant c which we will determine later. We will show in the next section that the groups $G_P = \pi_P(\Gamma)$ satisfy assumptions $(\mathrm{V4})_{L,\delta'}$ for some L that is independent of Q as long as $c < \delta'$. Let $\Omega' \subset \Gamma$ be the subset given by Proposition 8. Let $\mu = \chi_{\Omega'}$ and let $\mu_Q = \pi_Q[\mu]$. For any real number ε, let δ'_ε and δ_ε be the constants corresponding to ε in the statement of Proposition (37).

Assume for the sake of contradiction that there exists a positive constant ε such that for any positive real number δ,

$$\|\mu_Q\|_2 > |\pi_Q(\Gamma)|^{-1/2+\varepsilon} \text{ and } \mu_Q(gH) < [G:H]^{-\varepsilon} \tag{4.20}$$

for each $g \in G_Q$ and each proper subgroup H with the property that $\pi_P(H)$ is a structural subgroup of $\pi_P(\Gamma)$ for each irreducible factor P of Q. and yet

$$\|\mu_Q * \mu_Q\|_2 \geq \|\mu_Q\|^{1+\delta}.$$

Note that we may replace ε with another positive constant $\varepsilon' \ll \varepsilon$ freely. For if the claim is true for $\varepsilon' \ll \varepsilon$, and the inequalities (4.20) hold, then we also have

$$\|\mu_Q\|_2 > |\pi_Q(\Gamma)|^{-1/2+\varepsilon'} \text{ and } \mu_Q(gH) < [G:H]^{-\varepsilon'} \tag{4.21}$$

and the proposition implies itself. By Lemma 39 applied to $\mu = \nu = \mu_Q^{(\ell)}$, where

$\ell \ll \deg(Q)$ and $K = \|\mu_Q\|_2^{-\delta}$, there exists a symmetric set $S \subset G$ with the following properties:

$$\|\mu_Q^{(\ell)}\|_2^{-2+\Theta(\delta)} \ll |S| \ll \|\mu_Q^{(\ell)}\|_2^{-2-\Theta(\delta)}, \tag{4.22}$$

$$|\Pi_3 S| \ll \|\mu_Q^{(\ell)}\|_2^{-\Theta(\delta)}|S|, \tag{4.23}$$

$$\min_{s\in S}(\widetilde{\mu_Q^{(\ell)}} * \mu_Q^{(\ell)})(s) \gg \frac{\|\mu_Q\|_2^{\Theta(\delta)}}{|S|}. \tag{4.24}$$

Note that the implied constants in these equations are universal. We will show that the set S satisfies the hypotheses of Proposition 37 for the constant ε as long as c and δ are sufficiently small depending on ε. By Property (4.22), $|S| < |G|^{1-\varepsilon}$.

Let $g \in \pi_Q(\Gamma)$ and $H \subset \pi_Q(\Gamma)$ be a proper subgroup. Set

$$H' = \times_{P_{irred.}|Q}\pi_P(H).$$

Let G_s be the product of the factors G_P where P is an irreducible factor of Q and either $\pi_P(H) = G_P$ or $\pi_P(H)$ is a proper structural type subgroup of G_P, and let pr_s be the projection of G_Q to G_s. Let G_f be the product of the factors G_P where P is an irreducible factor of Q and $\pi_P(H)$ is a proper subfield type subgroup of G_P, and let pr_f be the projection of G_Q to G_f. Let $H'_s = \mathrm{pr}_s(H')$ and $H'_f = \mathrm{pr}_f(H')$ so that $H' = H'_s \times H'_f$ and $|\mathrm{pr}_f(H)| \leq |H'_f| < |G_f|$. We distinguish two cases. First assume $\mathrm{pr}_s(H) \neq G_s$. Then $\mathrm{pr}_s(H) \times \langle 1\rangle$ is a proper subgroup of G_Q such that for each irreducible factor P of Q, $\pi_P(H)$ is a structural subgroup.

Then we have,

$$\begin{aligned}\chi_S(gH) &\leq \chi_S(g(\mathrm{pr}_s(H)\times \mathrm{pr}_f(H)))\\ &= \textstyle\sum_{h_f\in \mathrm{pr}_f(H)} \chi_S((\mathrm{pr}_s(g),\mathrm{pr}_f(g)h_f)(\mathrm{pr}_s(H)\times\langle 1\rangle))\\ &\leq |\mathrm{pr}_f(H)|\max_{g'\in G_Q}\chi_S(g'(\mathrm{pr}_s(H)\times\langle 1\rangle)).\end{aligned} \tag{4.25}$$

By (4.24) and the second assumption in (4.20), we have for any $g'\in G_Q$

$$\begin{aligned}\chi_S(g'(\mathrm{pr}_s(H)\times\langle 1\rangle)) &\ll \|\mu_Q\|_2^{-\Theta(\delta)}(\widetilde{\mu_Q}^{(\ell)}*\mu_Q^{(\ell)})(g'(\mathrm{pr}_s(H)\times\langle 1\rangle))\\ &\leq \|\mu_Q^{(\ell)}\|_2^{-\Theta(\delta)}\max_{h\in G_Q}\mu_Q^{(\ell)}(h(\mathrm{pr}_s(H)\times\langle 1\rangle))\ .\\ &\ll |G_Q|^{\Theta(\delta)}[G_Q:\mathrm{pr}_s(H)\times\langle 1\rangle]^{-\varepsilon}.\end{aligned} \tag{4.26}$$

Combining equations (4.25) and (4.26), we have

$$\begin{aligned}\chi_S(gH) &\leq |\mathrm{pr}_f(H)||G_Q|^{\Theta(\delta)}[G_Q:\mathrm{pr}_s(H)\times\langle 1\rangle]^{-\varepsilon}\\ &< |G_f|^c|G_Q|^{\Theta(\delta)}[G_Q:\mathrm{pr}_s(H)\times\langle 1\rangle]^{-\varepsilon}\\ &\leq |G_f|^c|G_Q|^{\Theta(\delta)}[G_Q:H]^{-\varepsilon}\\ &\leq |G_Q|^{\delta_\varepsilon}[G_Q:H]^{-\varepsilon}\end{aligned} \tag{4.27}$$

Where the last inequality holds if say $c<\delta_\varepsilon/2$ and $\delta\ll\delta_\varepsilon/2$.

For the second case, we assume $\mathrm{pr}_s(H)=G_s$. Recall from Lemma 30, there exists a constant $\delta''>0$, depending only on $\mathbb{G}$ such that

$$[G_Q:H']\geq[G_Q:H]^{\delta''}.$$

Therefore, in order to show

$$\chi_S(gH) < [G_Q : H]^{-\varepsilon} |G_Q|^{\delta_\varepsilon},$$

it suffices to show

$$\chi_S(gH') < [G_Q : H']^{-\varepsilon/\delta''} |G_Q|^{\delta_\varepsilon}.$$

Note that if $\ell_0 < \ell$, then for any subset X of G and any constant M, $\chi_{\Omega'}^{(\ell_0)}(X) < M$ implies $\mu_Q^{(\ell)}(X) < M$. Let $Q' = \Pi_{P|Q:\pi_P(H)\neq G_P} P$. Since Ω' generates a free subgroup of Γ we have an upper bound on the probability of recurrence to the origin given by Kesten [Kes59, Thm. 3]:

$$\pi_{Q'}[\mu^{(\ell_0)}](1) < |G_{Q'}|^{-\Theta(1)}$$

where $G_{Q'} = \pi_{Q'}(\Gamma)$, and the implied constant depends only on the size of Ω'. If ℓ_0 is even, then by the Cauchy-Schwarz inequality and since Ω' is symmetric, we have

$$\pi_{Q'}[\mu^{(\ell_0)}(g') \leq \pi_{Q'}[\mu^{(\ell_0)}(1)$$

for any $g' \in G_{Q'}$.

Then on one hand we have for any $g' \in G_Q$,

$$\begin{aligned} \pi_{Q'}[\mu_Q^{\ell_0}](\mathrm{pr}_f(g')H'_f) &\leq |H'_f| \pi_{Q'}[\mu_Q^{\ell_0}](1) \\ &< |H'_f||G_f|^{-\Theta(1)} \\ &< |G_f|^{c-\Theta(1)} \\ &< |G_f|^{-\Theta(1)}, \end{aligned} \tag{4.28}$$

where the last inequality holds if $c \ll 1$. Therefore,

$$\pi_{Q'}[\mu_Q^{(\ell)}](\mathrm{pr}(f)H'_f) < |G_f|^{-\Theta(1)}.$$

On the other hand, we have

$$\pi_{Q'}[\mu_Q^{(\ell)}](\mathrm{pr}_f(g')H'_f) \quad = \mu_Q^{(\ell)}(g'(G_s \times H'_f)) \ . \tag{4.29}$$

By the calculation in equation (4.26) and by (4.28), we have

$$\begin{aligned}
\chi_S(gH') &\leq \chi_S(g(G_s \times H'_f) \\
&\ll \|\mu_Q^{(\ell)}\|_2^{-\Theta(\delta)} \max_{h \in G_Q} \mu_Q^{(\ell)}(h(G_s \times H'_f)) \\
&< |G_Q|^{\Theta(\delta)} |G_f|^{-\Theta(1)} \\
&< |G_Q|^{\Theta(\delta)} |G_f|^{-\varepsilon/\delta''} \\
&< |G_Q|^{\Theta(\delta)} |G_f|^{-\varepsilon/\delta''} |H'_f|^{\varepsilon/\delta''} \\
&= |G_Q|^{\Theta(\delta)} [G_Q : H']^{-\varepsilon/\delta''} \\
&< |G_Q|^{\delta_\varepsilon} [G_Q : H']^{-\varepsilon/\delta''}
\end{aligned} \tag{4.30}$$

where the fourth inequality holds if $\varepsilon \ll_{\Omega',\mathbb{G}} 1$ and the last inequality holds if $\delta \ll \varepsilon$.

Now as long as $c < \delta'_\varepsilon$, $\pi_Q(\Gamma)$, S, and $\mu_Q^{(\ell)}$ satisfy the hypotheses of Proposition 37. Therefore the conclusion of Proposition 37 contradicts (4.23) if δ is sufficiently small. $\square$

4.2 Satisfying assumptions $(\mathbf{V1})_{L,\delta'}$-$(\mathbf{V4})_{L,\delta'}$

Recall that if $Q = P_1 P_2 \dots P_k \in \Sigma$ is a square free polynomial coprime to Q_1, then $\pi_Q(\Gamma) = \mathbb{G}_Q(\mathbb{F}_p[t]/(Q)) = \times_{P_{irred.}|Q}\mathbb{G}_P(\mathbb{F}_{q_P})$. We claim that the groups $G_P = \mathbb{G}_P(\mathbb{F}_{q_P})$ satisfy assumptions $(\mathrm{V1})_{L,\delta'}$-$(\mathrm{V1})_{L,\delta'}$ for some L if $Q \in \Sigma_c$ for $c \ll \delta'$.

Assumptions $(\mathbf{V1})_{L,\delta'}$ and $(\mathbf{V2})_{L,\delta'}$

Since $\mathbb{G}$ is absolutely almost simple, G_P is almost simple and the center of G_P is bounded in terms of the absolute root system of $\mathbb{G}$. By the main theorem of [LS74] the groups G_P are known to be c-quasirandom for some constant c depending only on $\mathbb{G}$. Therefore assumptions $(\mathrm{V1})_{L,\delta'}$ and $(\mathrm{V2})_{L,\delta'}$ hold.

Assumption $(\mathbf{V3})_{L,\delta'}$

Let $H \subset G_P$ be a proper subgroup of G_P. Then by Proposition 26 either:

1. H is of subfield type. Then there exists a proper subfield $\mathbb{F}_{q'} \subset \mathbb{F}_{q_P}$ and model $\mathbb{G}_H$ of $\mathbb{G}_P$ over $\mathbb{F}_{q'}$ such that $[\mathbb{G}_H(\mathbb{F}_{q'}), \mathbb{G}_H(\mathbb{F}_{q'})]$ is simple and

$$[\mathbb{G}_H(\mathbb{F}_{q'}), \mathbb{G}_H(\mathbb{F}_{q'})] \subset \mathrm{Ad}(H) \subset \mathbb{G}_H(\mathbb{F}_{q'}),$$

   or,

2. H is of structural type. Then H lies in a proper algebraic subgroup $\mathbb{H} \subset \mathbb{G}_P$ of complexity $\ll 1$. I.e., $\mathbb{H}$ is defined by at most D polynomials of degree at most D (c.f., Proposition 26). Moreover, $\mathbb{H}$ is defined over a field $\mathbb{F}_{q'_P}$ of degree $\ll_{\mathbb{G}} 1$ over $\mathbb{F}_{q_P}$.

If $\deg(P)$ has no divisors smaller than a constant δ', then any subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_{q_P}$ has order less than $q_P^{\delta'}$. Therefore for any model $\mathbb{G}_0$ of $\mathbb{G}$ over a subfield $\mathbb{F}_{q'} \subset \mathbb{F}_{q_P}$, $|\mathbb{G}_0(\mathbb{F}_{q'})| < |G_P|^{\Theta(\delta')}$. Hence, if $P \in \mathcal{P}_c$ where $c \ll \delta'$ and $H \subset G_P$ is a subgroup such that $|H| > |G_P|^{\delta'}$, then H must be a subgroup of structural type.

It remains to describe the classes of subgroups $\mathcal{H}_1, \ldots, \mathcal{H}_m$. For $1 \leq i \leq m$, let

$$\mathcal{H}'_i := \{\mathbb{H} = \mathrm{Stab}_{\rho'_P(\mathbb{G}_P)}(W)(\mathbb{F}_{q'_P})^\circ \mid W \text{ is an } \mathbb{F}_{q'_P}\text{-subspace of } V_{q'_P},\ \dim \mathbb{H} = i\}$$

(c.f., §3.1) and let

$$\mathcal{H}_i := \{\rho'^{-1}_P(\mathbb{H})(\overline{\mathbb{F}_p}) \cap \mathbb{G}_P(\mathbb{F}_{q'_P}) \mid \mathbb{H} \in \mathcal{H}'_i\}.$$

Then we claim that the classes $\mathcal{H}_i$, $1 \leq i \leq \dim(\mathbb{G})$, satisfy the assumptions. Recall that by the construction of ρ'_P, $\mathbb{H}$ has complexity bounded by a constant $D \ll_{\mathbb{G}} 1$. By a refinement of Bézout's Theorem ([Ful98, Thm. 12.3]) the bound on the complexity of $\mathbb{H}$ yields a uniform bound on the number of irreducible components of $\mathbb{H}$. Therefore, $[\mathbb{H} : \mathbb{H}^\circ] < L$ if L is large enough. This implies that for any structural subgroup H of G_{q_P}, there exists an index $i_0 \in \{1, \ldots, \dim(\mathbb{G})$ and a subgroup $H^\# \in \mathcal{H}_{i_0}$ such that H is contained in at most L many cosets of $H^\#$.

For any index $i_0 \in \{1, \ldots, \dim(\mathbb{G})\}$, and any two subgroups $H_1, H_2 \in \mathcal{H}_{i_0}$ with say,

$$\rho'_P(H_1) \subset \mathrm{Stab}_{\rho_{P'}(\mathbb{G}_P)}(W_1)(\mathbb{F}_{q'_P})^\circ, \text{ and } \rho'_P(H_2) \subset \mathrm{Stab}_{\rho_{P'}(\mathbb{G}_P)}(W_2)(\mathbb{F}_{q'_P})^\circ,$$

we see that $\rho'_P(H_1 \cap H_2) \subset \mathrm{Stab}_{\rho_{P'}(\mathbb{G}_P)}(W_1 \cap W_2)(\mathbb{F}_{q'_P})$. Hence, $\rho'_P(H_1 \cap H_2)$ lies in at most L many cosets of $\mathrm{Stab}_{\rho_{P'}(\mathbb{G}_P)}(W_1 \cap W_2)^\circ(\mathbb{F}_{q'_P})$, and the last assumption is clear.

Assumption $(\mathrm{V4})_{L,\delta'}$

Assumption $(\mathrm{V4})_{L,\delta'}$ for the groups G_P is exactly the content of the following theorem that was proved independently by Breuillard-Green-Tao [BGT11, Cor. 2.4] and Pyber-Szabo [PS, Thm. 4]:

Theorem 46. *Let G be a simple group of Lie type of rank r, and X a set which generates G. Then either $|\Pi_3 X| \gg |X|^{1+\varepsilon_0}$ or $|X| \gg |G|^{1-\varepsilon_0}$ where ε_0 and the implied constant are universal.*

Chapter 4 contains material coauthored by Professor Alireza Salehi Golsefidy and is in preparation for publication under the title ""Super-approximation" in Absolutely Almost Simple Groups Over $\mathbb{F}_q(t)$". The author of this dissertation is a primary researcher and a primary author of the paper mentioned above.

Chapter 5

Proof of the main theorem

Proof of Theorem 6. The proof presented here is essentially identical to the proof of Theorem 1 of [SGV12] and is included for the sake of completeness. Let $\Omega' \subset \Gamma$ be the finite symmetric set given in Proposition 8. We will first show that there exists positive constants ε and c such that the family of graphs

$$\{\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega'))\}_{Q \in \Sigma_c}$$

is a family of ε-expander graphs.

For any polynomial $Q \in \Sigma$ with $\deg(Q) \gg 1$, let $\mu_Q := \pi_Q[\chi_{\Omega'}]$. Consider the "convolution by μ_Q" linear operator

$$\begin{aligned} *\mu_Q : \quad L^2(\pi_Q(\Gamma)) &\to L^2(\pi_Q(\Gamma)) \\ f &\mapsto f * \mu_Q. \end{aligned}$$

Note that if we fix an ordering of the elements of $\pi_Q(\Gamma)$, the matrix A_Q that represents $*\mu_Q$ in the basis of Dirac functions $\{\delta_\gamma\}_{\gamma \in \pi_Q(\Gamma)}$, where

$$\delta_\gamma(g) = \begin{cases} 1/|\Omega'| & g = \gamma \\ 0 & g \neq \gamma, \end{cases}$$

is equal to the normalized adjacency matrix of $\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega'))$. Since Ω' is a symmetric generating set of $\pi_Q(\Gamma)$ which contains the identity, we see that A_Q is a real, symmetric matrix with $|\Omega'|$ eigenvalues

$$1 = \lambda_{Q,0} > \lambda_{Q,1} \geq \lambda_{Q,2} \geq \cdots \geq \lambda_{Q,|\Omega'|-2} \geq \lambda_{Q,|\Omega'|-1} > -1.$$

It is well known (see [Dod84], [Alo86], [AM85]) that $\{\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega'))\}_{Q \in \Sigma_c}$ is a family of ε-expander graphs if and only if for each Q, we can bound the constants

$$\lambda_Q := \max\{|\lambda_{Q,1}|, |\lambda_{Q,|\Omega'|-2}|\}$$

uniformly away from 1.

In order to get the desired bound, we use the trick of Sarnak and Xue of bounding the multiplicity of the eigenvalues of A_Q in terms of the dimension of the irreducible representations of $\pi_Q(\Gamma)$. Let λ be an eigenvalue of $*\mu_Q$ and let $f \in L^2(\pi_Q(\Gamma))$ be an eigenfunction corresponding to λ. Note that the irreducible representations of $\pi_Q(\Gamma)$ are irreducible subspaces of $L^2(\pi_Q(\Gamma))$ that are stable under conjugation by μ_Q. Let ρ be the irreducible representation that contains f. We may assume that $\pi_P(\Gamma)$ is not contained in the kernel of ρ for any $P|Q$, since otherwise we can take the quotient $\pi_Q(\Gamma)/\pi_P(\Gamma)$ and replace Q by Q/P. Since $\pi_Q(\Gamma) = \times_{P|Q}\pi_P(\Gamma)$, ρ is a tensor product of irreducible representations of $\pi_P(\Gamma)$ for $P|Q$. By [LS74], the dimension of any irreducible representation of $\pi_P(\Gamma)$ is at least $|\Pi_P(\Gamma)|^{c_0}$ for some

constant c_0 which depends only on $\mathbb{G}$. Therefore the dimension of ρ, and hence the multiplicity of the eigenvalue λ, is at least $|\pi_Q(\Gamma)|^{c_0}$.

Let a positive integer ℓ be given. We compute the trace of $*\mu_Q^{(2\ell)}$ in two different ways.

On one hand,

$$\begin{aligned} \mathrm{Tr}(*\mu_Q^{(2\ell)}) &= \sum_{i=0}^{|\Omega'|-2} \lambda_{Q,i}^{2\ell} \\ &> \max\{\mathrm{mult}(\lambda_{Q,1}), \mathrm{mult}(\lambda_{Q,|\Omega'|-2})\}\lambda_Q^{2\ell} \\ &> |\pi_Q(\Gamma)|^{c_0}\lambda_Q^{2\ell}. \end{aligned} \tag{5.1}$$

On the other hand, if we compute $\mathrm{Tr}(*\mu_Q^{(2\ell)})$ in the basis of Dirac functions we have

$$\begin{aligned} \mathrm{Tr}(*\mu_Q^{(2\ell)}) &= |\pi_Q(\Gamma)|\mu_Q^{(2\ell)}(1) \\ &= |\pi_Q(\Gamma)| \sum_{g\in\pi_Q(\Gamma)} \mu_Q^{(\ell)}(g)^2 \text{ (since } \mu_Q \text{ is symmetric)} \\ &= |\pi_Q(\Gamma)|\|\mu_Q^{(\ell)}\|_2^2. \end{aligned} \tag{5.2}$$

Combining Equations (5.1) and (5.2), we see that it suffices to show

$$\|\mu_Q^{(\ell)}\|_2 \ll |\pi_Q(\Gamma)|^{-1/2+c_0/4} \tag{5.3}$$

for some $\ell \ll \deg(Q)$.

By Proposition 8 there exists a positive constant ε_1 such that if $\deg(Q) \gg 1$ and if $H \subset \pi_Q(\Gamma)$ has the property that $\pi_P(H)$ is structural for all irreducible factors

P of Q, then for $\ell \gg \deg Q$ we have

$$\pi_Q[\mu_{\Omega'}^{(l)}](H) \ll [\pi_Q(\Gamma) : H]^{-\varepsilon_1}. \tag{5.4}$$

By the Cauchy-Schwarz inequality and the fact that $\mu_Q^{(2\ell)}$ is symmetric, for any $g \in \pi_Q(\Gamma)$

$$\begin{aligned} \mu_Q^{(2\ell)}(g) &= \sum_{h \in \pi_Q(\Gamma)} \mu_Q^{(\ell)}(h)\mu_Q^{(\ell)}(hg) \\ &< \|\mu_Q^{(\ell)}\|_2^2 \\ &= \mu_Q^{(2\ell)}(1) \end{aligned} .$$

Since the trivial subgroup is clearly a structural subgroup of $\pi_P(\Gamma)$ for all irreducible polynomials P, we can apply Equation (5.4) to get

$$\|\mu_Q^{(2\ell)}\|_2 < |\pi_Q(\Gamma)|^{1/2}\mu_Q^{(2\ell)}(1) \ll |\pi_Q(\Gamma)|^{-\varepsilon_1/2}.$$

Now if we assume $Q \in \Sigma_c$ where c is the constant appearing in Proposition 9, we can apply Proposition 9 a finite number of times to the measures $\mu = \nu = \mu_Q^{(2^k\ell)}$ to obtain the desired inequality, which proves the first claim.

We now prove that the Cheeger constants of the Cayley graphs of $\pi_Q(\Gamma)$ with respect to Ω are uniformly bounded away from zero. Since Ω and Ω' are both finite generating sets of Γ, there exists a constant m such that $\Omega' \subset \Pi_m\Omega$. For a subset X of $\pi_Q(\Gamma)$, let $\partial_\Omega(X)$, $\partial_{\Omega'}(X)$ by the boundaries of X in the Cayley graphs of $\pi_Q(\Gamma)$ with respect to Ω and Ω' respectively. Suppose $|X| < |\pi_Q(\Gamma)|/2$. Recall that since

$\{\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega')\}_{Q\in\Sigma'}$ is a family of expander graphs, we have the inequality

$$\frac{|\partial_{\Omega'}(X)|}{|X|} > h_{\Omega'}$$

where $h_{\Omega'}$ is the Cheeger constant of the Cayley graph of $\pi_Q(\Gamma)$ with respect to Ω' (1). Then

$$\begin{aligned} |\Pi_m \Omega.X| &\geq |\Omega'.X| \\ &= |\partial_{\Omega'}(X)| + |X| \\ &> |X|h_{\Omega'} + |X|. \end{aligned} \tag{5.5}$$

On the other hand we have the obvious inequality

$$|\Pi_m \Omega.X| \leq |\Pi_{m-1}\Omega.\partial_\Omega(X)| + |X| \leq |\Omega'|^{m-1}||\partial_\Omega(X)| + |X|. \tag{5.6}$$

Combining (5.5) and (5.6), we have

$$|\partial_\Omega(X)| \geq |X| \left(\frac{h_{\Omega'}}{|\Omega|^{m-1}}\right).$$

Therefore,

$$\{\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega')\}_{Q\in\Sigma_c}$$

is a family of expander graphs with a smaller Cheeger constant. □

Chapter 5 contains material coauthored by Professor Alireza Salehi Golsefidy and is in preparation for publication under the title ""Super-approximation" in Absolutely Almost Simple Groups Over $\mathbb{F}_q(t)$". The author of this dissertation is a primary researcher and a primary author of the paper mentioned above.

Chapter 6

Questions

Theorem 6 naturally lends itself to several questions. The most crucial question is if we can prove expansion without the conditions on the irreducible factors of the square free polynomials in Σ. Namely,

Question 1 (Expansion without condition)**.** If Ω, Γ, $\mathbb{G}$, and Q_1 are as in the hypothesis of Theorem 6, then is the family of graphs

$$\{\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega))\}_{Q \text{ square free, } (Q,Q_1)=1}$$

a family of ε-expander graphs for some $\varepsilon > 0$?

We put the condition that irreducible factors of the polynomials in Σ_c be distinct in order to eliminate the possibility of subgroups of the form

$$H = \{g, \phi_1(g), \ldots, \phi_k(g)) \in \mathbb{G}_Q(\mathbb{F}_{q_0}[t]/(Q)) = \times_{i=0}^{k} \mathbb{G}_{Pi}(\mathbb{F}_{q_{P_i}})\}$$

where

$$\phi_i : \mathbb{G}_{P_0}(\mathbb{F}_{q_{P_0}}) \to \mathbb{G}_{P_i}(\mathbb{F}_{q_{P_i}})$$

is a group isomorphism arising from a field isomorphism from $\mathbb{F}_{q_{P_0}}$ to $\mathbb{F}_{q_{P_i}}$ for each $i = 1, \ldots, k$. For subgroups of this form, we cannot make use of Larsen and Pink's description of subgroups of $\mathbb{G}_P(\mathbb{F}_{q_P})$ since the projection to each factor is onto. Since the morphisms ϕ_i, $i = 1, \ldots, k$ are isomorphisms of abstract groups and not of an algebraic nature, it is not clear if the "small lifts" of the elements H lie in an algebraic subgroup of $\mathbb{G}$.

Seemingly related is the problem of getting rid of the assumption that the divisors of the irreducible factors of Q are large. In order to do this, one must prove that there is an exponentially small chance that a random walk on the Cayley graph lands in a subgroup H of $\pi_Q(\Gamma)$ that may have nontrivial subfield type projections. Again since those subgroups are not of an algebraic nature, a new idea is needed.

Question 2. Let $p \geq 5$ be a prime number, $\Omega \subset \mathrm{GL}_n(\mathbb{F}_{q_0}[t, 1/Q_0])$ be a finite symmetric set, $\Gamma = \langle \Omega \rangle$, and $\mathbb{G}$ be the Zariski-closure of Γ. Suppose $\mathbb{G}$ is semisimple and simply connected and let $pr_i : \mathbb{G} \to \mathbb{G}_i$ be the projection of $\mathbb{G}$ onto its i^{th} almost simple factor. Assume that $\mathrm{pr}_i(\Gamma)$ is Zariski dense for all i and that the ring generated by $\mathrm{Tr}(\mathrm{pr}_i(\mathrm{Ad}\,\Gamma)))$ is all of $\mathbb{F}_{q_0}[t, 1/Q_0]$. Then does there exist a positive constant $c > 0$ and a square free multiple Q_1 of Q_0 such that the family of graphs

$$\{\mathrm{Cay}(\pi_Q(\Gamma), \pi_Q(\Omega))\}_{Q \in \Sigma_c,\ (Q,Q_1)=1}$$

is a family of ε-expanders for some $\varepsilon > 0$?

A large portion of our proof still works in this setting so I suspect this question

of reasonable.

Aside from these questions, it may also be reasonable to answer the analogous positive characteristic version of the work of [BGS10]. Namely, can we take the reduction mod P^n map where P is a fixed irreducible polynomial in $\mathbb{F}_{q_0}[t]$ and n ranges through the positive integers? A modest start would be the following:

Question 3. Let Ω be a finite symmetric set of $\mathrm{SL}_2(\mathbb{F}_p[t])$ which generates a Zariski-dense subgroup Γ. Then is the family of graphs

$$\{\mathrm{Cay}(\pi_{t^n}(\Gamma), \pi_{t^n}(\Omega))\}_{n\geq 1}$$

a family of ε-expander graphs for some $\varepsilon > 0$?

Bibliography

[Alo86] N. Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):83–96, 1986. Theory of computing (Singer Island, Fla., 1984).

[AM85] N. Alon and V. D. Milman. λ_1, isoperimetric inequalities for graphs, and superconcentrators. *J. Combin. Theory Ser. B*, 38(1):73–88, 1985.

[BG08a] Jean Bourgain and Alex Gamburd. Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. I. *J. Eur. Math. Soc. (JEMS)*, 10(4):987–1011, 2008.

[BG08b] Jean Bourgain and Alex Gamburd. Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. *Ann. of Math. (2)*, 167(2):625–642, 2008.

[BG09] Jean Bourgain and Alex Gamburd. Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. II. *J. Eur. Math. Soc. (JEMS)*, 11(5):1057–1103, 2009. With an appendix by Bourgain.

[BGS06] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Sieving and expanders. *C. R. Math. Acad. Sci. Paris*, 343(3):155–159, 2006.

[BGS10] Jean Bourgain, Alex Gamburd, and Peter Sarnak. Affine linear sieve, expanders, and sum-product. *Invent. Math.*, 179(3):559–644, 2010.

[BGT11] Emmanuel Breuillard, Ben Green, and Terence Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.*, 21(4):774–819, 2011.

[BGT12] Emmanuel Breuillard, Ben Green, and Terence Tao. The structure of approximate groups. *Publ. Math. Inst. Hautes Études Sci.*, 116:115–221, 2012.

[BK67] Y. M. Barzdin and A. MN. Kolmogorov. On the realization of nets in 3-dimensional space. *Probl. Cybernet*, 8:261–268, 1967.

[BO14] Emmanuel Breuillard and Hee Oh, editors. *Thin groups and superstrong approximation*, volume 61 of *Mathematical Sciences Research Institute Publications*. Cambridge University Press, Cambridge, 2014. Selected expanded papers from the workshop held in Berkeley, CA, February 6–10, 2012.

[Bor66] Armand Borel. Linear algebraic groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 3–19. Amer. Math. Soc., Providence, R.I., 1966.

[Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[Bra15] Henry Bradford. Expansion, random walks and sieving in $sl_2(\mathbb{F}_p[t])$. 2015.

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

[CGP15] Brian Conrad, Ofer Gabber, and Gopal Prasad. *Pseudo-reductive groups*, volume 26 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, second edition, 2015.

[Chu97] Fan R. K. Chung. *Spectral graph theory*, volume 92 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1997.

[Clo03] Laurent Clozel. Démonstration de la conjecture τ. *Invent. Math.*, 151(2):297–328, 2003.

[Dan94] V. I. Danilov. Algebraic varieties and schemes. In *Algebraic geometry, I*, volume 23 of *Encyclopaedia Math. Sci.*, pages 167–297. Springer, Berlin, 1994.

[Dod84] Jozef Dodziuk. Difference equations, isoperimetric inequality and transience of certain random walks. *Trans. Amer. Math. Soc.*, 284(2):787–794, 1984.

[EMO05] Alex Eskin, Shahar Mozes, and Hee Oh. On uniform exponential growth for linear groups. *Invent. Math.*, 160(1):1–30, 2005.

[Far00] Ilijas Farah. Approximate homomorphisms. II. Group homomorphisms. *Combinatorica*, 20(1):47–60, 2000.

[Ful98] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 1998.

[Gow08] W. T. Gowers. Quasirandom groups. *Combin. Probab. Comput.*, 17(3):363–387, 2008.

[Hel08] H. A. Helfgott. Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math. (2)*, 167(2):601–623, 2008.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc. (N.S.)*, 43(4):439–561 (electronic), 2006.

[Hum78] James E. Humphreys. *Introduction to Lie algebras and representation theory*, volume 9 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1978. Second printing, revised.

[Jan03] Jens Carsten Jantzen. *Representations of algebraic groups*, volume 107 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, second edition, 2003.

[Kaž67] D. A. Každan. On the connection of the dual space of a group with the structure of its closed subgroups. *Funkcional. Anal. i Priložen.*, 1:71–74, 1967.

[Kes59] Harry Kesten. Symmetric random walks on groups. *Trans. Amer. Math. Soc.*, 92:336–354, 1959.

[LP11] Michael J. Larsen and Richard Pink. Finite subgroups of algebraic groups. *J. Amer. Math. Soc.*, 24(4):1105–1158, 2011.

[LS74] Vicente Landazuri and Gary M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra*, 32:418–443, 1974.

[LS04] Martin W. Liebeck and Gary M. Seitz. The maximal subgroups of positive dimension in exceptional algebraic groups. *Mem. Amer. Math. Soc.*, 169(802):vi+227, 2004.

[Lub12] Alexander Lubotzky. Expander graphs in pure and applied mathematics. *Bull. Amer. Math. Soc. (N.S.)*, 49(1):113–162, 2012.

[Mar88] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problemy Peredachi Informatsii*, 24(1):51–60, 1988.

[Nor87] Madhav V. Nori. On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$. *Invent. Math.*, 88(2):257–275, 1987.

[NP11] N. Nikolov and L. Pyber. Product decompositions of quasirandom groups and a Jordan type theorem. *J. Eur. Math. Soc. (JEMS)*, 13(4):1063–1077, 2011.

[Pin73] M.S. Pinsker. On the complexity of a concentrator. *7th International Teletraffic Conference*, Stockholm:318/1–318/4, June 1973.

[PR94] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

[PS] L. Pyber and E. Szabó. Growth in finite simple groups of lie type of bounded rank.

[Sch00] A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.

[Sel67] G. B. Seligman. *Modular Lie algebras*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 40. Springer-Verlag New York, Inc., New York, 1967.

[SGV12] Alireza Salehi Golsefidy and Péter P. Varjú. Expansion in perfect groups. *Geom. Funct. Anal.*, 22(6):1832–1891, 2012.

[Ste61] R. Steinberg. Lecture notes on chevalley groups, 1961. Prepared by John Faulkner and Robert Wilson.

[SX91] Peter Sarnak and Xiao Xi Xue. Bounds for multiplicities of automorphic representations. *Duke Math. J.*, 64(1):207–227, 1991.

[Tao08] Terence Tao. Product set estimates for non-commutative groups. *Combinatorica*, 28(5):547–594, 2008.

[Var12] Péter P. Varjú. Expansion in $SL_d(\mathcal{O}_K/I)$, I square-free. *J. Eur. Math. Soc. (JEMS)*, 14(1):273–305, 2012.

[Wei84] Boris Weisfeiler. Strong approximation for Zariski-dense subgroups of semisimple algebraic groups. *Ann. of Math. (2)*, 120(2):271–315, 1984.