ISRAEL JOURNAL OF MATHEMATICS **00** (XXXX), 1–24
DOI: 10.1007/s00000000000000000000000

EXPANSION, RANDOM WALKS AND SIEVING IN $SL_2(\mathbb{F}_p[t])$

BY

Henry Bradford
University of Oxford

ABSTRACT

We construct new examples of expander Cayley graphs of finite groups, arising as congruence quotients of non-elementary subgroups of $SL_2(\mathbb{F}_p[t])$ modulo certain square-free ideals. We describe some applications of our results to simple random walks on such subgroups, specifically giving bounds on the rate of escape of such walks from algebraic subvarieties, the set of squares and the set of elements with reducible characteristic polynomial in $SL_2(\mathbb{F}_p[t])$.

1. Introduction

The past few years have seen major developments in tools for constructing expanders as congruence images of linear groups. This programme was begun by the breakthrough paper of Bourgain and Gamburd [1], who studied expander congruence quotients of non-elementary subgroups of $SL_2(\mathbb{Z})$, but their approach was subsequently extended by many authors [5], [14]. We now have a fairly satisfying picture of the phenomenon of superstrong approximation (as it has come to be known) in linear groups over $\mathbb{Q}$. These results on expanders have in turn shed new light on problems in the geometry and analysis of infinite linear groups.

In spite of the major strides forward that have been made in this area, it is notable that the work of recent years has focused entirely on the characteristic zero case, with a theory of expansion in linear groups over fields of positive characteristic remaining largely undeveloped. In this paper we commence the development of such a theory.

1.1. Statement of Results. Fix a prime $p \geq 3$. Our main results concern the escape of random walks on $SL_2(\mathbb{F}_p[t])$ from subsets X of various types. All of the escape results are proved by the same broad strategy: an upper bound for the probability of the random walk lying in X is given by the probability of the random walk on a congruence quotient lying in the image of X. This in turn may be bounded above in terms of the *size* of the image of X, by our results on expander congruence quotients. Our first result on random walks demonstrates exponentially fast escape from proper algebraic subvarieties.

Theorem 1.1: *Let $S \subseteq SL_2(\mathbb{F}_p[t])$ be a finite symmetric subset, generating a non-elementary subgroup. Let $F : \mathbb{M}_2(\mathbb{F}_p[t])^r \to \mathbb{F}_p[t]$ be a polynomial over $\mathbb{F}_p[t]$ which does not vanish on $SL_2(\mathbb{F}_p[t])^r$. Then there exist $C_1(F), C_2(S) > 0$ such that, letting $V(F) \subseteq \mathbb{M}_2(\mathbb{F}_p[t])^r$ be the affine algebraic subvariety of $SL_2(\mathbb{F}_p[t])^r$ defined by F,*

$$(\times_{i=1}^r \mu_S^{(l)})(V(F)) \leq C_1 e^{-C_2 l}.$$

Here $\mu_S^{(l)}$ is the lth convolution power of the measure μ_S and $\times_{i=1}^r \mu_S^{(l)}$ is the product measure. We define these notions precisely below.

Second, we turn to proper powers in $SL_2(\mathbb{F}_p[t])$. In the characteristic zero case, a very general non-concentration result was provided by Lubotzky and Meiri [12]. In positive characteristic we have:

Theorem 1.2: *Let S be as in Theorem 1.1. There exist $C_1, C_2 > 0$ such that:*

$$\mu_S^{(l)}(\{g \in SL_2(\mathbb{F}_p[t]) : g = h^2 \text{ for some } h \in SL_2(\mathbb{F}_p[t])\}) \leq C_1 e^{-C_2\sqrt{l/\log(l)}}.$$

Remark 1.3: *More could be said about proper powers via the same method. We could, for instance, strengthen the proof of Theorem 1.2 to show that $\mu_S^{(l)}$ escapes from the sets of mth powers in $SL_2(\mathbb{F}_p[t])$, for all $m \in \mathbb{N}$ satisfying $p \equiv 1 \mod m$, simultaneously. However, absent an application, we shall not rehearse the details of such an argument.*

Finally we prove a non-concentration estimate for elements with reducible characteristic polynomial.

Theorem 1.4: *Let S be as in Theorem 1.1. There exist $C_1, C_2 > 0$ such that:*

$$\mu_S^{(l)}(\{g \in SL_2(\mathbb{F}_p[t]) : \chi_g \text{ is reducible } \}) \leq C_1 e^{-C_2\sqrt{l/\log(l)}}.$$

It is very likely that bounds on return probabilities of random walks to other subsets of $SL_2(\mathbb{F}_p[t])$ may be proved by the same method, and we emphasize that our results are best viewed as sample, rather than an exhaustive list, of the applications of this theory.

We now turn to our results on expanders.

DEFINITION 1.5: *For $M > 0$, an integer $n > 1$ will be called M-*admissible *if n has no prime factor less than M. A polynomial $f \in \mathbb{F}_p[t]$ will be called M-admissible if the degree of every irreducible factor of f is a M-admissible integer.*

EXAMPLE 1.6: *Let $M > 0$.*

(i) *Every prime $> M$ is M-admissible.*

(ii) *There is a sequence $(n_i)_i$ of M-admissible integers growing linearly in i. For, given M, let π be the set of all primes up to M. Let $n_i = Ni + 1$, where $N = \prod_{P \in \pi} P$. It will be significant in the applications in Section 3 that the set of admissible integers is sufficiently dense.*

Our main result on constructing expanders is:

THEOREM 1.7: *Let $S \subseteq SL_2(\mathbb{F}_p[t])$ be a finite symmetric subset, generating a non-elementary subgroup. Suppose every entry of every element of S has degree at most D. Let $(f_i)_i \subseteq \mathbb{F}_p[t]$ be a sequence of distinct polynomials. Then there exists $M > 0$ (depending on D and p) such that, if $(f_i)_i$ are M-admissible then for $i_0 \in \mathbb{N}$ sufficiently large (depending on D, p), $(SL_2(\mathbb{F}_p[t]/(f_i)), \pi_{f_i}(S))_{i \geq i_0}$ is a two-sided expander family, provided one of the following holds:*

(i) *The f_i are irreducible.*

(ii) *The f_i are square-free, every irreducible factor of every f_i has prime degree, and no two irreducible factors of any f_i have the same degree.*

We define the concept of a two-sided expander family in Section 1.2 below. Here, and throughout, for $\mathbb{G}$ a linear algebraic group defined over $\mathbb{F}_p$ and $f \in \mathbb{F}_p[t]$, $\pi_f : \mathbb{G}(\mathbb{F}_p[t]) \to \mathbb{G}(\mathbb{F}_p[t]/(f))$ shall denote the congruence map.

One of the keys to the proof of Theorem 1.7 shall be an analysis of Cayley graphs of large girth. For G a finite group generated by a subset S, recall that the girth of (G, S) is the length of the shortest non-trivial reduced word in S which equals 1 in G, or equivalently the length of the shortest non-trivial embedded loop in the Cayley graph $\mathrm{Cay}(G, S)$. In the course of our analysis,

we also obtain the following result, which applies to generating sets which may not be congruence images of a fixed subset in $SL_2(\mathbb{F}_p[t])$.

THEOREM 1.8: *For any $C_1 > 0$ and any $k \in \mathbb{N}$ with $k \geq 2$, there exists $C > 0$ (depending on k, p and C_1) such that, if $(n_i)_i$ a sequence of C-admissible positive integers, $S_{n_i} \subseteq SL_2(p^{n_i})$ is symmetric with $|S_{n_i}| = 2k$, and* girth$(SL_2(p^{n_i}), S_{n_i}) \geq C_1 n_i$, *for all $i \in \mathbb{N}$, then for i_0 sufficiently large (depending on C_1, k), $(SL_2(p^{n_i}), S_{n_i})_{i \geq i_0}$ is a two-sided expander family.*

The lower bound on girth is a natural hypothesis: for instance it is satisfied by *generic* subsets of $SL_2(p^n)$. Indeed large girth is a key component of the proof [5] that random pairs of generators in $SL_2(p^n)$ yield expanders.

1.2. EXPANDERS. Let G be a finite group. For two functionals $\phi, \psi \in l^2(G)$, the *convolution* $\phi * \psi \in l^2(G)$ is given by:

$$(\phi * \psi)(g) = \sum_{h \in G} \phi(h)\psi(h^{-1}g).$$

For $l \in \mathbb{N}$, we define the *convolution power* $\phi^{(l)}$ recursively via:

$$\phi^{(0)} = \chi_e;\ \phi^{(l+1)} = \phi^{(l)} * \phi.$$

Here χ_e is the characteristic function of the identity element $e \in G$. For $S \subseteq G$ a symmetric subset, define a linear operator $A_S : l^2(G) \to l^2(G)$ (called the *adjacency operator*) by:

$$A_S(f) = (\tfrac{1}{|S|}\chi_S) * f.$$

A_S is self-adjoint of operator norm 1; let its spectrum be:

$$1 = \lambda_1 \geq \lambda_2 \geq \ldots \lambda_{|G|} \geq -1$$

with the eigenvalue $\lambda_1 = 1$ corresponding to the constant functionals on G. More generally, the 1-eigenspace of A_S is generated by the indicator functions of the right cosets of $\langle S \rangle \leq G$. In particular $\lambda_1 > \lambda_2$ iff S generates G. Let $l_0^2(G) \leq l^2(G)$ be the space of functions of mean zero on G (that is, the orthogonal complement of the constant functions), and note that $l_0^2(G)$ is preserved by A_S. Let $\rho = \max(|\lambda_2|, |\lambda_{|G|}|)$, the norm of the restriction $A_S \mid_{l_0^2(G)}$ in the Banach space $B(l_0^2(G))$ of bounded linear operators on $l_0^2(G)$.

DEFINITION 1.9: *For $\epsilon > 0$, the pair (G, S) is a (two-sided)* ϵ-expander *if $\rho \leq 1 - \epsilon$. A sequence $(G_n, S_n)_{n \in \mathbb{N}}$ is called an* ϵ-expander family *if (G_n, S_n) is an ϵ-expander for every $n \in \mathbb{N}$, or just an* expander family *if there exists $\epsilon > 0$ such that $(G_n, S_n)_{n \in \mathbb{N}}$ is an ϵ-expander family.*

The two-sided version of expansion (also known as *absolute expansion*) that we use here is stronger than the one-sided version which will be more familiar to many readers, and which is equivalent to the combinatorial notion of expansion defined in terms of the discrete Cheeger constant. For the most part, however, the distinction need not concern us, thanks to a recent result of Breuillard, Green, Guralnick and Tao [5]:

THEOREM 1.10: *For any $\epsilon > 0, k \in \mathbb{N}$, there exists $\delta_{\epsilon,k} > 0$ such that, if (G, S) is a one-sided ϵ-expander with $|S| = k$, then one of the following holds:*

(i) *(G, S) is a two-sided δ-expander;*
(ii) *There exists $H \leq G$ with $|G : H| = 2$ and $S \cap H = \emptyset$.*

We recall some facts about expanders which will be used in what follows. Those readers more familiar with the one-sided version of expansion may note that these results about two-sided expanders follow from their one-sided analogues together with Theorem 1.10. Note that condition (ii) of Theorem 1.10 is equivalent to $\mathrm{Cay}(G, S)$ being bipartite.

LEMMA 1.11: *Let Γ be a finitely generated group; $(K_n)_n$ be a sequence of finite index subgroups of Γ; $\pi_n : \Gamma \twoheadrightarrow \Gamma/K_n$ be the natural epimorphism. Let $S, T \subseteq \Gamma$ be finite symmetric subsets, with $\langle S \rangle = \langle T \rangle = \Gamma$. Suppose $\mathrm{Cay}(\Gamma/K_n, \pi_n(T))$ is not bipartite, for all $n \in \mathbb{N}$. If $(\Gamma/K_n, \pi_n(S))_n$ is an expander family then so is $(\Gamma/K_n, \pi_n(T))_n$.*

LEMMA 1.12: *Let Γ; $(K_n)_n$; π_n be as in Lemma 1.11 and let $H \leq \Gamma$ be a finitely generated subgroup. Suppose $\pi_n(H) = \Gamma/K_n$ for all $n \in \mathbb{N}$. Let $S \subseteq \Gamma$, $T \subseteq H$ be finite symmetric subsets, with $\langle S \rangle = \Gamma$, $\langle T \rangle = H$. If $(\Gamma/K_n, \pi_n(T))_n$ is an expander family, and $\mathrm{Cay}(\Gamma/K_n, \pi_n(S))$ is not bipartite, then $(\Gamma/K_n, \pi_n(S))_n$ is an expander family.*

In all cases in which we shall use these results, the finite groups concerned shall have no subgroups of index two, so the associated Cayley graphs shall never be bipartite.

The expander property for the pair (G, S) provides a logarithmic bound for the mixing times of random walks on G, given by a probability measure supported on S. This will be useful in the applications in Section 3.

LEMMA 1.13: *For any $l \in \mathbb{N}$; $g, h \in G$,*

$$|\langle A_S^l \chi_g, \chi_h \rangle - \tfrac{1}{|G|}| \leq \rho^l.$$

1.3. THE BOURGAIN-GAMBURD MACHINE. In [1] Bourgain and Gamburd developed a new method for constructing expanders, exploiting results from additive combinatorics. Much has been written about the possible formulations of the Bourgain-Gamburd Machine [3], [16], so we shall not rehearse the details of the proof, and give only a rough sketch of the most salient points.

The Machine tells us that the expansion of a pair (G, S) may be guaranteed by three hypotheses. The first is that G should be highly *quasirandom*, meaning that G has no small-dimensional non-trivial complex representations. There are good classical estimates of quasirandomness for many familiar families of finite groups, including finite simple groups of Lie type. The combinatorics of quasirandom groups was studied by Gowers [8], who coined the term, but its connection with expansion was first noted by Sarnak and Xue [15]. Suppose A_S has an eigenvalue λ of modulus close to 1, so that the expansion is weak. The eigenspace of λ is a subrepresentation of the right-regular representation of G, so by quasirandomness has large dimension. This places a substantial lower bound on $\mathrm{tr}(A_S^{2l})$.

Proving expansion therefore reduces to showing that $\mathrm{tr}(A_S^{2l})$ decays quickly. Sufficient conditions for such decay come from the non-commutative Balog-Szemerédi-Gowers Theorem, due to Tao [17], which tells us that if decay fails, the measure $\mu_S^{(2l)}$ must concentrate somewhat on a small *approximate subgroup* A of G (that is, a symmetric subset containing 1 such that AA is covered by a small number of translates of A). Some papers utilising the Bourgain-Gamburd Machine have tackled the problem of excluding this possibility head-on, but we can reduce the problem still further if G satisfies a *product theorem*. All finite groups have some obvious approximate subgroups: if A is already almost the whole of G, or is almost a proper subgroup of G, then A will not grow much under multiplication with itself. A product theorem says roughly that these are the only possibilities. Through much work by many authors in the past decade, product theorems are now known for many families of groups, including finite (quasi)simple groups of Lie type of fixed rank [4], [13].

Expansion is thereby reduced to showing that $\mu_S^{(2l)}$ escapes quickly from proper subgroups of G. It should be noted that this is the only point at which the set S enters the argument. We therefore usually expect some information

about the geometry of S to be crucially involved in proving escape from subgroups.

The general form of the Bourgain-Gamburd Machine admits many, related but distinct, formulations. The version which it shall be most convenient for us to consider shall be the following.

THEOREM 1.14: *Let G be a finite group; $S \subseteq G$ a symmetric generating set. Suppose:*

(i) *(Quasirandomness) There exists $\alpha > 0$ such that, for some finite groups $G_1, \ldots, G_n$, $G = \prod_{i=1}^{n} G_i$ and for every i, for any non-trivial representation $\rho : G_i \to GL_d(\mathbb{C})$,*

$$d \geq |G_i|^{\alpha}.$$

(ii) *(Product theorem) For all $\delta > 0$ there exists $\beta(\delta) > 0$ such that for any symmetric $A \subseteq G$ such that:*

$$|A| < |G|^{1-\delta} \text{ and } \mu_A(gH) < [G : H]^{-\delta}|G|^{\beta}$$

for any $g \in G$ and $H \lneq G$, then $|AAA| \gg |A|^{1+\beta}$.

(iii) *(Escape from subgroups) There exists $\gamma > 0$ and $C_0 > 0$ such that for some $l \leq C_0 \log|G|$ and every $H \lneq G$,*

$$\mu_S^{(2l)}(H) \leq |G : H|^{-\gamma}.$$

Then there exists $\epsilon(\alpha, \beta(\cdot), \gamma, C_0, |S|) > 0$ such that (G, S) is a two-sided ϵ-expander.

A proof of this result is contained in Sections 3.1 and 5 of [18]. See also Section 3 of [3] for a self-contained and accessible account of a related (though non-equivalent) version of the Machine.

REMARK 1.15: *For $H \leq G$, and $\phi \in l^2(G)$, define $\overline{\phi} \in l^2(G/H)$ by:*

$$\overline{\phi}(gH) = \textstyle\sum_{h \in H} \phi(gh).$$

Then since S is symmetric, for $l \in \mathbb{N}$,

$$\mu_S^{(2l)}(H) = \|\overline{\mu_S^{(l)}}\|_2^2.$$

Now define $\overline{A_S} : l^2(G/H) \to l^2(G/H)$ by:

$$\overline{A_S}(F)(gH) = \tfrac{1}{|S|} \textstyle\sum_{s \in S} F(sgH).$$

Then $\overline{A_S}$ is a linear operator; it is a contraction (being the adjacency operator on the Schreier graph of $(G/H, S)$) and satisfies, for $\phi \in l^2(G)$,

$$\overline{A_S}(\overline{\phi}) = \overline{\mu_S * \phi}.$$

It follows that $\mu_S^{(2l)}(H)$ is a decreasing function of l. Hypothesis (iii) of Theorem 1.14 therefore follows from an apparently weaker variant, in which our $l \leq C_0 \log|G|$ is permitted to depend on the subgroup H.

1.4. Further Questions and Structure of the Paper. It is natural to ask whether the admissibility hypothesis in Theorems 1.7 and 1.8 may be weakened. However there are some significant obstacles to doing so. For instance it is clear that Theorem 1.8 does not remain true for arbitrary sequences $(n_i)_i$:

Example 1.16: *Let $n_i = 2^i$. Then we may identify $\mathbb{F}_{p^{n_i}}$ with a proper subfield of $\mathbb{F}_{p^{n_{i+1}}}$, and hence embed $SL_2(p^{n_i}) \hookrightarrow SL_2(p^{n_{i+1}})$. For i even, let S_{n_i} be a generating set for $SL_2(p^{n_i})$ satisfying $\mathrm{girth}(SL_2(p^{n_i}), S_{n_i}) \gg n_i$. For i odd, let $S_{n_i} = S_{n_{i-1}}$, so that $\langle S_{n_i} \rangle \lneq SL_2(p^{n_i})$. Then for every i, $\mathrm{girth}(SL_2(p^{n_i}), S_{n_i}) \gg n_i$, but $\{(SL_2(p^{n_i}), S_{n_i})\}_{i \geq j}$ is not an expander family for any j.*

So the presence of large subfield subgroups presents a genuine obstruction to expansion of subsets. It should be noted however that Example 1.16 exhibits an obstruction to expansion which is *qualitative*, rather than *quantitative* in nature. That is to say, expansion in $(SL_2(p^{n_i}), S_{n_i})$ fails simply by virtue of the fact that $\langle S_{n_i} \rangle \neq SL_2(p^{n_i})$ for infinitely many i. This leads to the question of whether this is the *only* obstruction to expansion in these groups. Specifically:

Question 1.17: *Let $S_n \subseteq SL_2(p^n)$ with $\mathrm{girth}(SL_2(p^n), S_n) \gg n$. Does there exist $\epsilon > 0$ such that $(\langle S_n \rangle, S_n)$ is an ϵ-expander for all n sufficiently large?*

Question 1.18: *Let $S \subseteq SL_2(\mathbb{F}_p[t])$ be a finite symmetric set generating a non-elementary subgroup. Let $(f_i)_i \subseteq \mathbb{F}_p[t]$ be a sequence of distinct irreducible polynomials. Does there exist $\epsilon > 0$ such that $(\langle \pi_{f_i}(S) \rangle, \pi_{f_i}(S))$ is an ϵ-expander for all i sufficiently large?*

A second way in which Theorem 1.7 (ii) might be extended would be relax the assumption that no two irreducible factors of f_i have the same degree. As a model case, let $f, g \in \mathbb{F}_p[t]$ be distinct irreducibles of degree n, and consider the group $SL_2(\mathbb{F}_p[t]/(f \cdot g))$. By the Chinese Remainder Theorem, this may be identified with $SL_2(p^n) \times SL_2(p^n)$. A potential obstruction to expansion in this group comes from proper subdirect products of $SL_2(p^n) \times SL_2(p^n)$, which arise as the graphs of automorphisms of $SL_2(p^n)$. It remains an open question how to

demonstrate escape from such subgroups, as would be required for hypothesis (iii) of Theorem 1.14.

The primality assumption in Theorem 1.7 (ii) comes from hypothesis (ii) of Theorem 1.14, which in our setting is satisfied by results of Varjú [18]. The applicability of these results shall be discussed in more detail in Section 2. Roughly speaking though, for the product theorem to apply to reductions modulo polynomials with unboundedly many irreducible factors (so that the corresponding congruence quotients decompose as products with unboundedly many quasisimple factors), the subgroup structure of the quasisimple factors must be highly restricted. It seems plausible that a generalisation of Varjú's product theorem which relaxes these restrictions may be discovered, and the primality assumption thereby removed.

An expansion result for reductions modulo arbitrary square-free polynomials seems even further out of reach. For then the decompositions of the congruence quotients into products of quasisimple groups contain unboundedly many isomorphic factors, so Varjú's product theorem fails even more dramatically. It may be that the fastest route to a result on expansion in this general setting is to tackle the question of concentration in approximate subgroups directly.

Even an expansion result in the case of two irreducible factors of the same degree would have useful consequences for sieving in $SL_2(\mathbb{F}_p[t])$. For in the presence of such a result (and the relevant strengthening of the product theorem indicated above) we could substitute the group sieve of Lubotzky-Meiri for Proposition 3.3 in the proofs of Theorems 1.2 and 1.4, thereby improving the upper bounds in those two results from $e^{-C\sqrt{l/\log(l)}}$ to e^{-Cl}.

The paper is structured as follows: in Section 2 we prove Theorems 1.7 and 1.8. Specifically, Section 2.1 shall deal with hypotheses (i) and (ii) of Theorem 1.14 and further reduce Theorem 1.7 to the case of non-abelian free subgroups. We then turn to hypothesis (iii) of Theorem 1.14. In Section 2.2 it is verified for Cayley graphs of $SL_2(p^n)$ with large girth under the admissibility hypothesis. This yields Theorem 1.7 (i) and Theorem 1.8. The generalisation of this argument required for Theorem 1.7 (ii) is explained in Section 2.3.

We discuss the applications to random walks in $SL_2(\mathbb{F}_p[t])$ in Section 3. In Section 3.1 we explain in general terms how non-concentration results in infinite groups can be obtained using expansion results on finite quotients. Theorems 1.1, 1.2 and 1.4 are proved in the subsequent three Sections.

I would like to thank my supervisor, Marc Lackenby, for the abundance of support and sound advice he has given me in preparing this work, and his ongoing enthusiasm for my research in general. I am also grateful to Emmanuel Breuillard, Alireza Salehi-Golsefidy and Peter Varjú for enlightening conversations, and to the referee for careful reading of this manuscript. Finally, I would like to thank EPSRC for providing financial support during the undertaking of this work.

2. Constructing the Expanders

As a notational convenience, for $n \in \mathbb{N}$ we set $Q_n = SL_2(p^n)$.

2.1. Reduction to Escape for Free Generators. In this section we reduce the proof of Theorem 1.7 to the following Proposition:

Proposition 2.1: *Let $T \subseteq SL_2(\mathbb{F}_p[t])$ be the symmetric closure of a finite subset, freely generating a non-abelian free subgroup. Suppose every entry of every element of T has degree at most $\tilde{D}$. Then there exists $C, M, \gamma > 0$ (depending on $\tilde{D}$, $|T|$ and p) such that the following holds. Let $f \in \mathbb{F}_p[t]$ be an M-admissible square-free polynomial with no two irreducible factors having the same degree. Then for every $H \lneq G = SL_2(\mathbb{F}_p[t]/(f))$, there exists $l \leq C \log|G|$ such that:*

$$\mu_T^{(2l)}(H) \leq |G : H|^{-\gamma}.$$

The reduction shall be via Theorem 1.14. We reference known results which cover hypotheses (i) and (ii) of Theorem 1.14. We then use the general results about expanders from Section 1.2 to reduce the question of expansion for arbitrary sets S as in the Statement of Theorem 1.7 to expansion for finite sets $T \subseteq \langle S \rangle$ freely generating $\langle T \rangle$. This shall be via a Tits alternative.

The quasirandomness condition in our setting is classical (see for instance [10]):

Theorem 2.2: *There is an absolute constant $C > 0$ such that every non-trivial complex representation of Q_n has dimension at least Cp^n.*

Let f be as in Proposition 2.1 and let $p_1, \ldots, p_N$ be the irreducible factors of f, of degrees $n_1, \ldots, n_N$ respectively. It follows from the Chinese Remainder

Theorem that:

LEMMA 2.3: *The natural map:*

$$(\prod_{j=1}^{N} \pi_{p_j}) : SL_2(\mathbb{F}_p[t]/(f)) \to \prod_{j=1}^{N} Q_{n_j}$$

is an isomorphism.

We turn next to the product theorem. In the setting of Theorem 1.7 (i), this is due to Dinai [6]. For Theorem 1.7 (ii) we use Proposition 14 of [18], which we quote in full:

THEOREM 2.4: *For all $\delta > 0$, $L \in \mathbb{N}$ and $\beta : \mathbb{R}^+ \to \mathbb{R}^+$ there exists $\beta'_{L,\beta}(\delta) > 0$ such that the following holds. Let G be a finite group, $G_1, \ldots, G_N$ be finite groups such that $G \cong G_1 \times \cdots \times G_N$. Suppose:*

(i) *For any finite group F, $|\{i \in \{1, \ldots, N\} : G_i \cong F\}| \leq L$.*
(ii) *For $1 \leq i \leq N$, G_i is quasisimple and $|Z(G_i)| \leq L$.*
(iii) *For $1 \leq i \leq N$, any non-trivial complex representation of G_i has dimension at least $|G_i|^{\frac{1}{L}}$.*
(iv) *For $1 \leq i \leq N$ and for some $m < L$, there are classes $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_m$ of subgroups of G_i satisfying:*
  (a) *$\mathcal{H}_0 = \{Z(G_i)\}$.*
  (b) *Each $\mathcal{H}_j$ is closed under conjugation in G_i.*
  (c) *For each $H < G_i$ there is $1 \leq j \leq m$ and $H^\sharp \in \mathcal{H}_j$ such that $|H : H \cap H^\sharp| \leq L$.*
  (d) *For $1 \leq j \leq m$ and for each $H_1, H_2 \in \mathcal{H}_j$ with $H_1 \neq H_2$, there exists $j' < j$ and $H^\sharp \in \mathcal{H}_{j'}$ such that $|H_1 \cap H_2 : H_1 \cap H_2 \cap H^\sharp| \leq L$.*

If $G_1, \ldots, G_N$ satisfy hypothesis (ii) of Theorem 1.14 with respect to the function β, then G satisfies hypothesis (ii) of Theorem 1.14 with respect to the function $\beta'_{L,\beta}$.

We check that this result applies to $G = SL_2(\mathbb{F}_p[t]/(f_i))$, for f_i as in Theorem 1.7 (ii). The decomposition as a product is given by Lemma 2.3. (i) follows from the assumption that no two irreducible factors of f_i have the same degree. (ii) is well-known for $G_i = Q_{n_i}$. (iii) is Theorem 2.2. For (iv), we recall the classification of subgroups of Q_n (see for instance [9]).

PROPOSITION 2.5: *For $\mathbb{F}_q$ the finite field of order q and characteristic $p \geq 3$, any proper subgroup H of $SL_2(\mathbb{F}_q)$ satisfies one of the following:*

(i) *H fixes a point in the projective line $\mathbb{F}_{q^2}\mathbb{P}^1$ over the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. In particular H is metabelian.*
(ii) *$H \leq S_5$.*
(iii) *H is conjugate in $SL_2(\mathbb{F}_q)$ to a subgroup of $SL_2(\mathbb{E})$ for some proper subfield $\mathbb{E}$ of $\mathbb{F}_q$.*

Define $\mathcal{H}_1$ to be the set of stabilisers in Q_n of pairs of distinct points in $\mathbb{F}_{p^{2n}}\mathbb{P}^1$, and $\mathcal{H}_2$ to be the set of stabilisers in Q_n of points in $\mathbb{F}_{p^{2n}}\mathbb{P}^1$. We check that the conditions of Theorem 2.4 (iv) are satisfied by $\mathcal{H}_0 = \{Z(Q_n)\}, \mathcal{H}_1, \mathcal{H}_2$, in the case for which n is prime. (a), (b) are obvious, and (c) is immediate from Proposition 2.5, since by primality of n, the only proper subfield subgroups of Q_n are the conjugates of Q_1, which are of bounded size. (d) is a consequence of the following elementary fact from linear algebra:

LEMMA 2.6: *Suppose $g \in Q_n$ has at least three distinct fixed points in $\mathbb{F}_{q^2}\mathbb{P}^1$. Then $g \in Z(Q_n)$.*

Now let S be as in the statement of Theorem 1.7. We produce a pair of words in S freely generating a non-abelian free subgroup. In the classical Tits alternative, the lengths of our free generators as words in S, and hence the degrees of their entries, depend on S and not just on D. However, we can obtain a bound depending only on D by utilising the following result of Breuillard:

THEOREM 2.7 (Uniform Tits Alternative [2]): *For every $d \geq 2$, there exists $N(d) > 0$ such that, for any field K, and $S \subseteq SL_d(K)$ finite symmetric, either $\langle S \rangle$ is virtually soluble or the ball $B_S(N(d))$ of radius $N(d)$ in the word metric contains two elements which freely generate a non-abelian free subgroup of $SL_d(K)$.*

Proof of Theorem 1.7. Let $N = N(2)$ be as in Theorem 2.7 and let $x, y \in B_S(N)$ freely generate a non-abelian free group. Every entry of every member of $T = \{x^{\pm 1}, y^{\pm 1}\}$ is expressible as a sum of monomials of degree at most N in the entries of the elements of S, hence has degree at most DN. We now apply Theorem 1.14 to $(SL_2(\mathbb{F}_p[t]/(f_i))), \pi_{f_i}(T))$.

We verify the conditions of Theorem 1.14. Hypothesis (i) is immediate from

Theorem 2.2 and Lemma 2.3. Hypothesis (ii) follows from [6] and Theorem 2.4. Hypothesis (iii) follows from Proposition 2.1, applied with $f = f_i$ and $\tilde{D} = DN$, and Remark 1.15.

We conclude that $(SL_2(\mathbb{F}_p[t]/(f_i)), \pi_{f_i}(T))_i$ is an expander family. By Lemma 1.12, $(SL_2(\mathbb{F}_p[t]/(f_i)), \pi_{f_i}(B_S(N)))_i$ is an expander family. The required result follows from Lemma 1.11, since $\langle S \rangle = \langle B_S(N) \rangle$. ∎

REMARK 2.8: *The constants M and i_0 in the statement of Theorem 1.7 could in principle be computed, by keeping track of the bounds arising in the proof of Proposition 2.1 below. They shall involve both the constant N from the statement of the Uniform Tits Alternative and the known spectral radius $\sqrt{8/9}$ for the simple random walk on $\{x^{\pm 1}, y^{\pm 1}\}$ in $F(x, y)$. Moreover, the proof of the Uniform Tits Alternative is effective, so N could in principle be computed (though to our knowledge this has not been done). Such a computation would yield an explicit description of the degrees of reductions which would give rise to families of expanders, in terms only of the degrees of the entries of elements of S, $|S|$ and p.*

2.2. ESCAPE FROM SUBGROUPS: THE IRREDUCIBLE CASE. In this section we warm up to the proof of Proposition 2.1 by examining the case for which the polynomials f_i are irreducible, so that $SL_2(\mathbb{F}_p[t]/(f_i)) = Q_{\deg(f_i)}$. The proof of this case shall contain all the key ideas of the general case (to be discussed in the following section) but is technically simpler. Indeed, more generally we shall prove:

PROPOSITION 2.9: *For any $C_1 > 0$ and any $k \in \mathbb{N}$ with $k \geq 2$, there exists $C_2, C_3, \gamma > 0$ (depending on $C_1, p, |S|$) such that, if n is a C_2-admissible positive integer, $S_n \subseteq Q_n$ is symmetric with $|S_n| = 2k$, and $\mathrm{girth}(Q_n, S_n) \geq C_1 n$, then for n sufficiently large and for all $H_n \lneq Q_n$, there exists $l \leq C_3 \log |Q_n|$ such that:*

$$\mu_{S_n}^{(2l)}(H_n) \leq |Q_n|^{-\gamma}.$$

The relevant case of Proposition 2.1 follows immediately from Proposition 2.9 and the following Lemma:

LEMMA 2.10: *let T be as in Proposition 2.1 and $f \in \mathbb{F}_p[t]$ be of degree n. Then:*

$$\mathrm{girth}(SL_2(\mathbb{F}_p[t]/(f)), \pi_f(T)) \geq n/\tilde{D}.$$

Proof. Let w be a non-trivial reduced word in T of length l. Every entry of every element of T has degree at most $\tilde{D}$, so every entry of w has degree at most $\tilde{D}l$. Now suppose $\pi_f(w) = 1$, so that $w \in (I_2 + f \cdot \mathbb{M}_2(\mathbb{F}_p[t])) \setminus \{I_2\}$. Then at least one entry of w has degree at least n, so $l \geq n/\tilde{D}$, as required. ∎

Given the discussion in Section 2.1, Proposition 2.9 also immediately implies Theorem 1.8.

Proof of Theorem 1.8. As in the proof of Theorem 1.7, we apply Theorem 1.14. Hypothesis (i) is Theorem 2.2; hypothesis (ii) is [6] and hypothesis (iii) follows from Proposition 2.9 and Remark 1.15. ∎

We now turn to the proof of Proposition 2.9. Once again we exploit the classification of subgroups of Q_n.

Informally, in all cases, the girth hypothesis and Kesten's Theorem will reduce the problem of bounding $\mu_{S_n}^{(2l)}(H_n)$ to providing an upper bound for $|H_n \cap B_{S_n}(2l)|$. For $H_n \leq S_4$ or A_5 this is immediate. The admissibility hypothesis on n will guarantee that any proper subfield subgroup is too small to fill $|B_{S_n}(2l)|$. Non-concentration in metabelian subgroups will be achieved by the same combinatorial argument as was used for the corresponding case in [1]: a metabelian group satisfies a short group law, so that if $|H_n \cap B_{S_n}(2l)|$ is large, there will be many short relations between the elements of S_n. However the girth hypothesis guarantees that this will not happen.

First we recall:

THEOREM 2.11 (Kesten): *Let X be a finite set. Then there exists $C_4(|X|) > 0$ such that $\mu_X \in l^2(F(X))$ satisfies:*

$$\mu_X^{(2l)}(g) \ll_{|X|} e^{-C_4 l}$$

for all $g \in F(X)$.

The technicalities of non-concentration in subgroups are contained in the following general Lemma.

LEMMA 2.12: *Let G be a finite group, $S \subseteq G$ symmetric with $|S| = 2k$ and let $C_1 > 0$ be such that $\mathrm{girth}(G, S) > C_1 \log|G|$. Let $C_4(k) > 0$ be the constant from Kesten's Theorem. Let $H \lneq G$. Let $\gamma > 0$ and let $C_5 \in (0, C_1)$. Suppose $|G|$ is sufficiently large.*

(i) *Suppose H is metabelian. Suppose $C_5 \log|G| \leq 2l \leq \frac{C_1}{32}\log|G|$. Suppose $\gamma < C_4C_5/2$. Then $\mu_S^{(2l)}(H) \leq |G|^{-\gamma}$.*

(ii) *Let $C_6 > 0$ and suppose $|H| \leq C_6|G|^{\frac{1}{C_2}}$ Suppose $C_5 \log|G| \leq 2l \leq C_1 \log|G|$. Suppose $\gamma + 1/C_2 < C_4C_5/2$. Then $\mu_S^{(2l)}(H) \leq |G|^{-\gamma}$.*

Proof. (i) Define a homomorphism $\theta : F \to G$ from a non-abelian free group F on free basis X, such that θ maps $X \cup X^{-1}$ bijectively onto S. Then θ maps $B_X(32l)$ bijectively onto $B_S(32l)$.

Consider $Y = B_X(2l) \cap \theta^{-1}(H)$. Then for any $a, b, c, d \in Y$, $\theta([[a, b], [c, d]]) = 1$ (since H is metabelian) so $[[a, b], [c, d]] = 1$ (since $[[a, b], [c, d]] \in B_X(32l)$).

Recall that the centraliser of every non-trivial element of a free group is cyclic. Hence there exists $x \in F$ such that for all $a, b \in Y$,

$$[a, b] \in Z := \langle x \rangle \cap B_X(8l) \tag{1}$$

so that $|Z| \leq 16l + 1$. Now for $a \in Y$ and $z \in Z$, define:

$$W_{a,z} = \{b \in Y : [a, b] = z\}.$$

Then $W_{a,z}$ is contained in a single coset of the centraliser of a, and in $B_X(2l)$, so that $|W_{a,z}| \leq 4l + 1$. Fix $a \in Y$. By (1),

$$Y \subseteq \bigcup_{z \in Z} W_{a,z}.$$

We conclude that:

$$|H \cap B_S(2l)| \leq |Y| \leq (16l + 1)(4l + 1).$$

By Kesten's Theorem and the girth hypothesis,

$$\mu_S^{(2l)}(H) \ll_k e^{-C_4 l}|H \cap B_S(2l)| \ll l^2 e^{-C_4 l},$$

so decays exponentially fast.

(ii) Suppose (for a contradiction) that for some $C_5 \log|G| \leq 2l \leq C_1 \log|G|$,

$$|G|^{-\gamma} < \mu_S^{(2l)}(H) \ll_k e^{-C_4 l}|H| \leq C_6 e^{-C_4 l}|G|^{\frac{1}{C_2}}.$$

(the second inequality being by Kesten's Theorem and the girth hypothesis). Hence:

$$|G|^{\frac{1}{C_2}+\gamma} \gg_{k,C_6} e^{C_4 l}.$$

But $e^{C_4 l} \geq |G|^{\frac{C_4 C_5}{2}}$ so we have the required contradiction by choice of C_2 and γ.

∎

Proof of Proposition 2.9. Suppose $C_5 n \leq 2l \leq \frac{C_1}{32} n$, for some $C_5 \in (0, \frac{C_1}{32})$. We consider each case of Proposition 2.5 separately:

(i) Suppose H_n is metabelian. Choosing $\gamma \in (0, C_4 C_5/2)$, the required result follows from Lemma 2.12 (i).

(ii) If $H_n \leq S_5$, then $|H_n| \leq 120$, so $\mu_{S_n}^{(2l)}(H_n) \ll_k e^{-C_4 l}$ for any $2l \leq C_1 n$, by Kesten's Theorem and the girth hypothesis.

(iii) Suppose that there exists a proper subfield $\mathbb{E} < \mathbb{F}_{p^n}$ such that H_n is contained in (some conjugate of) $SL_2(\mathbb{E})$. Recall that there exists $m \mid n$ such that $\mathbb{E} = \mathbb{F}_{p^m}$. By the admissibility hypothesis, $m \leq n/C_2$ so:

$$|H_n| \leq |Q_m| \leq p^{3m} \leq (p^{3n})^{\frac{1}{C_2}} \ll_p |Q_n|^{\frac{1}{C_2}}.$$

Choosing γ sufficiently small and C_2 sufficiently large, we may suppose $\gamma + 1/C_2 < C_4 C_5/2$, and the result follows from Lemma 2.12 (ii).

∎

2.3. Escape from Subgroups: The General Case. In this Section we complete the proof of Proposition 2.1. The proof shall be very similar in spirit to that of the special case discussed in Section 2.2: recall that there, Proposition 2.5 guaranteed that every proper subgroup of $SL_2(\mathbb{F}_p[t]/(f))$ was either metabelian (Case (i)) or small (Cases (ii) and (iii)), so fell within reach of Lemma 2.12. Something similar is true in general, but to apply Lemma 2.12 we first need to use the product decomposition of $SL_2(\mathbb{F}_p[t]/(f))$ from Lemma 2.3, and project down to either the factors on which the image of our proper subgroup is metabelian, or those on which it is small, depending on which make up the larger part of the product.

Recall the notation of Section 2.1: $f \in \mathbb{F}_p[t]$ is an M-admissible square-free polynomial with no two irreducible factors having the same degree. $G = SL_2(\mathbb{F}_p[t]/(f))$ and $H \lneq G$. Let $p_1, \ldots, p_N$ be the irreducible factors of f, of degrees $n_1, \ldots, n_N$ respectively. Recall (Lemma 2.3) that:

$$(\prod_{j=1}^N \pi_{p_j}) : SL_2(\mathbb{F}_p[t]/(f)) \to \prod_{j=1}^N Q_{n_j}$$

is an isomorphism.

COROLLARY 2.13: $\pi_{p_j}(H) \lneq Q_{n_j}$ *for some* $1 \leq j \leq N$.

Proof. We proceed by induction on N (the case $N = 1$ being trivial). Suppose (for a contradiction) that the projections π_{p_j} of H to Q_{n_j} are all surjective. Denote $F = \prod_{j=1}^{N-1} Q_{n_j}$, so that by Lemma 2.3, $G \cong F \times Q_{n_N}$. Define:

$$K_1 = \{g \in F : (g, e) \in H\},\ K_2 = \{g \in Q_{n_N} : (e, g) \in H\}.$$

By induction the projections of H to F and Q_{n_N} are surjective. By Goursat's Lemma, $K_1 \lhd F$, $K_2 \lhd Q_{n_N}$ and $F/K_1 \cong Q_{n_N}/K_2$.

If $K_2 \neq Q_{n_N}$ then F has $PSL_2(p^{n_N})$ as a composition factor. But this is not the case, as the n_j are all distinct. Hence $K_2 = Q_{n_N}$ and $K_1 = F$, so $H = G$. ∎

Up to a reordering of the p_i, there exist $k, m, n \in \mathbb{N}$ with $k+m+n = N$ such that:

(i) $\pi_{p_i}(H) = Q_{n_i}$ for $1 \leq i \leq k$;
(ii) $\pi_{p_i}(H)$ is metabelian for $k+1 \leq i \leq k+m$;
(iii) $\pi_{p_i}(H) \lneq Q_{n_i}$ is not metabelian for $k+m+1 \leq i \leq N$.

Let $C_2, \gamma > 0$ be constants satisfying the conditions of Lemma 2.12. For M sufficiently large, by the admissibility hypothesis and Proposition 2.5, $|\pi_{p_i}(H)| \leq |Q_{n_i}|^{\frac{1}{C_2}}$ for $k+m+1 \leq i \leq N$. Moreover by Corollary 2.13, at least one of m, n is non-zero.

Write $F_1 = \prod_{i=1}^{k} p_i$, $F_2 = \prod_{i=k+1}^{k+m} p_i$, $F_3 = \prod_{i=k+m+1}^{N} p_i$, so that $f = F_1 \cdot F_2 \cdot F_3$. Applying Lemma 2.3 with f replaced by F_1, F_2, F_3 respectively, we have:

LEMMA 2.14: (i) $\pi_{F_1}(H) = \prod_{i=1}^{k} SL_2(p^{n_i})$.
(ii) $\pi_{F_2}(H)$ *is metabelian.*
(iii) $|\pi_{F_3}(H)| \leq |\pi_{F_3}(G)|^{\frac{1}{C_2}}$.

Finally, we are ready to complete:

Proof of Proposition 2.1. $|H| \geq |\pi_{F_1}(H)| = |\pi_{F_1}(G)|$, so:

$$|G : H| \leq |G|/|\pi_{F_1}(G)| = |\pi_{F_2F_3}(G)|.$$

Case 1: $\deg(F_2) \geq \deg(F_3)$:

We have $|\pi_{F_2F_3}(G)|^{\frac{1}{2}} \ll_p |\pi_{F_2}(G)| \leq |\pi_{F_2F_3}(G)|$. By Lemma 2.10,

$$\text{girth}(\pi_{F_2}(G), S) \geq \tfrac{1}{\tilde{D}} \deg(F_2) \geq \tfrac{1}{3\tilde{D}\log(p)} \log|\pi_{F_2}(G)|,$$

so that by Lemma 2.12 (i), if:

$$C_5 \log|\pi_{F_2}(G)| \leq 2l \leq \tfrac{1}{96\tilde{D}\log(p)} \log|\pi_{F_2}(G)|,$$

then:

$$\mu_S^{(2l)}(H) \leq \mu_S^{(2l)}(\pi_{F_2}(H)) \leq |\pi_{F_2}(G)|^{-\gamma} \ll_p |\pi_{F_2F_3}(G)|^{\frac{-\gamma}{2}} \leq |G:H|^{\frac{-\gamma}{2}}$$

and

$$2l \leq \tfrac{1}{96\tilde{D}\log(p)} \log|\pi_{F_2}(G)| \leq \tfrac{1}{96\tilde{D}\log(p)} \log|\pi_{F_2F_3}(G)|.$$

Case 2: $\deg(F_3) \geq \deg(F_2)$:

We have $|\pi_{F_2F_3}(G)|^{\frac{1}{2}} \ll_p |\pi_{F_3}(G)| \leq |\pi_{F_2F_3}(G)|$. By Lemma 2.10,

$$\text{girth}(\pi_{F_3}(G), S) \geq \tfrac{1}{\tilde{D}} \deg(F_3) \geq \tfrac{1}{3\tilde{D}\log(p)} \log|\pi_{F_3}(G)|,$$

so that by Lemma 2.12 (ii), if:

$$C_5 \log|\pi_{F_3}(G)| \leq 2l \leq \tfrac{1}{3\tilde{D}\log(p)} \log|\pi_{F_3}(G)|,$$

then:

$$\mu_S^{(2l)}(H) \leq \mu_S^{(2l)}(\pi_{F_3}(H)) \leq |\pi_{F_3}(G)|^{-\gamma} \ll_p |\pi_{F_2F_3}(G)|^{\frac{-\gamma}{2}} \leq |G:H|^{\frac{-\gamma}{2}}$$

and

$$2l \leq \tfrac{1}{3\tilde{D}\log(p)} \log|\pi_{F_3}(G)| \leq \log|\pi_{F_2F_3}(G)|.$$

The required result follows. ∎

3. Non-Concentration Results

3.1. Two Different Sieves. We start with a simple observation:

Lemma 3.1: *Let G be a discrete countable group; H a finite group and $\phi : G \to H$ an epimorphism. Let ν be a probability measure on G and $X \subseteq G$. Then $\nu(X) \leq (\phi\nu)(\phi(X)) \leq |\phi(X)| \cdot \max_{x \in X}(\phi\nu)(\phi(x))$.*

Though straightforward, this bound can be very useful: when $\nu = \mu_S^{(l)}$, for $S \subseteq G$ symmetric, with $\phi(S)$ generating H, then for l sufficiently large and even, $\phi\nu$ is almost uniform on H, so that:

$$(\phi\nu)(\phi(X)) \ll |\phi(X)|/|H|. \tag{2}$$

Moreover if $(H, \phi(S))$ is a good expander, equidistribution occurs for l sufficiently *small* that (2) gives a non-trivial lower bound on the rate at which $\mu_S^{(l)}$ escapes from X.

The present section contains two different instantiations of this philosophy for the group $SL_2(\mathbb{F}_p[t])$, taking (H, ϕ) to be one of the congruence quotients from Theorem 1.7. In the first of these it shall be sufficient to consider congruences modulo irreducible polynomials. We define, for G a countable discrete group and $\nu_1, \ldots, \nu_r$ finitely supported probability measures on G, the product measure $\times_{i=1}^r \nu_i$ on G by:

$$(\times_{i=1}^r \nu_i)(X) = \sum_{x \in X} \prod_{i=1}^r \nu_i(x), \text{ for } X \subseteq G.$$

PROPOSITION 3.2: *Let $S \subseteq SL_2(\mathbb{F}_p[t])$, $M > 0$ be as in Theorem 1.7; let $(n_i)_i$ be as in Example 1.6 (ii) and let $f_i \in \mathbb{F}_p[t]$ be irreducible of degree n_i. Let $X \subseteq SL_2(\mathbb{F}_p[t])^r$ and suppose there exists $\alpha, C > 0$ such that for all i sufficiently large,*

$$|\pi_{f_i}(X)|/|Q_{n_i}|^r \leq Cp^{-\alpha n_i}.$$

Then there exist $C_1(C, r), C_2(\alpha, p, S) > 0$ such that for all $l \in \mathbb{N}$,

$$(\times_{i=1}^r \mu_S^{(l)})(X) \leq C_1 e^{-C_2 l}.$$

Proof. By Theorem 1.7 and Lemma 1.13, there exists $c > 0$ such that, for $i \geq i_0$, $l \geq cn_i$ and any $x \in Q_{n_i}$, $(\pi_{f_i} \mu_S^{(l)})(x) \leq 2/|Q_{n_i}|$. Fix $\delta \in (0, 1)$, so that for l sufficiently large, $\exists i \geq i_0$ such that $l \geq cn_i \geq \delta l$. Then for i sufficiently large,

$$\begin{gathered}(\times_{j=1}^r \mu_S^{(l)})(X) \leq (\times_{j=1}^r \pi_{f_i} \mu_S^{(l)})(\pi_{f_i}(X)) \\ \leq 2^r |\pi_{f_i}(X)|/|Q_{n_i}|^r \text{ (by Lemma 3.1)} \\ \leq 2^r C p^{-\alpha n_i} \text{ (by hypothesis)} \\ \leq 2^r C e^{-\frac{\alpha \delta \log(p) l}{c}}\end{gathered}$$

as required. ∎

Proposition 3.2 is very useful for proving escape of the random walk from such subsets as proper algebraic subvarieties, which have small image in congruence quotients, as we shall see. However, Proposition 3.2 is powerless in the face of subsets X whose images modulo f_i are of order $\sim \gamma |Q_{n_i}|$, for $\gamma \in (0, 1)$, say. This difficulty may be partially resolved by considering, instead of individual congruence quotients Q_{n_i}, large products $Q_{n_i} \times \ldots \times Q_{n_{i+k}}$. The image of X in such a quotient will be of order $\sim \gamma^k |Q_{n_i}| \cdots |Q_{n_{i+k}}|$, so by allowing k to grow and applying Theorem 1.7, we may recover a good non-concentration estimate. As discussed in the Introduction, Theorem 1.7 is not powerful enough to retain exponentially fast escape from such X. However we still have:

PROPOSITION 3.3: *Let $S \subseteq SL_2(\mathbb{F}_p[t])$, $M > 0$ be as in Theorem 1.7; let $(n_i)_i$ be the sequence of all primes greater than M (arranged in ascending order) and let $f_i \in \mathbb{F}_p[t]$ be irreducible of degree n_i. Let $X \subseteq SL_2(\mathbb{F}_p[t])^r$ and suppose there exists $\gamma \in (0,1)$ and $i_1 \in \mathbb{N}$ such that for all $i \geq i_1$,*

$$|\pi_{f_i}(X)|/|Q_{n_i}|^r \leq \gamma.$$

Then there exist $C_1(r), C_2(\gamma, p, S) > 0$ such that for all $l \in \mathbb{N}$,

$$(\times_{i=1}^r \mu_S^{(l)})(X) \leq C_1 e^{-C_2\sqrt{l/\log(l)}}.$$

Proof. Define $g_i = \prod_{k=i_2}^{i_2+i-1} f_k \in \mathbb{F}_p[t]$, with i_2 sufficiently large (to be determined). Then:

$$|\pi_{g_i}(X)| \leq \gamma^i \prod_{k=i_2}^{i_2+i-1} |Q_{n_k}|^r$$

(provided $i_2 \geq i_1$). By Theorem 1.7, there exists $c > 0$ such that, provided i_2 is sufficiently large, for $l \geq c\sum_{k=i_2}^{i_2+i-1} n_k$ and for any $g \in SL_2(\mathbb{F}_p[t]/(g_i))$,

$$(\pi_{g_i}\mu_S^{(l)})(g) \leq 2/\prod_{k=i_2}^{i_2+i-1}|Q_{n_k}|.$$

For such l,

$$\begin{aligned}(\times_{j=1}^r \mu_S^{(l)})(X) &\leq (\times_{j=1}^r \pi_{g_i}\mu_S^{(l)})(\pi_{g_i}(X)) \\ &\leq |\pi_{g_i}(X)|(2/\prod_{k=i_2}^{i_2+i-1}|Q_{n_k}|)^r \\ &\leq 2^r\gamma^i.\end{aligned}$$

Recalling that n_k is of the order of $k\log(k)$, we have $\sum_{k=i_2}^{i_2+i-1} n_k \asymp i^2\log(i)$. Choosing $i \asymp \sqrt{l/\log(l)}$, $l \gg i^2\log(i)$ and the result follows. ∎

3.2. ESCAPE FROM SUBVARIETIES. We are now ready to prove Theorem 1.1. In view of Proposition 3.2, it will suffice to bound the size of projections of subvarieties to congruence quotients. We use:

THEOREM 3.4 (Schwarz-Zippel [11]): *Let $\mathbb{F}$ be a finite field; $\overline{\mathbb{F}}$ be its algebraic closure. Let V be an affine algebraic subvariety of $\mathbb{F}^d$, defined by A polynomials in $\overline{\mathbb{F}}[x_1, \ldots, x_d]$, each of total degree at most B. Then $|V| \ll_{A,B,d} |\mathbb{F}|^{\dim(V)}$.*

Proof of Theorem 1.1. SL_2^r is irreducible of dimension $3r$, so by Theorem 3.4,

$$|\pi_{f_i}(V(F))| \ll_F p^{(3r-1)n_i} \ll p^{-n_i}|Q_{n_i}|^r.$$

The result now follows from Proposition 3.2. ∎

EXAMPLE 3.5: *Under the hypotheses of Theorem 1.1:*

(i) *Zero entries are rare: let* $F_1 : \mathbb{M}_2(\mathbb{F}_p[t]) \to \mathbb{F}_p[t]$ *be given by* $F_1\begin{pmatrix} a & b \\ c & d \end{pmatrix} = abcd$. *Then there exist* $C_1, C_2 > 0$ *such that:*

$$\mu_S^{(l)}(\{g \in SL_2(\mathbb{F}_p[t]) : g \text{ has a zero entry}\}) = \mu_S^{(l)}(V(F_1)) \leq C_1 e^{-C_2 l}.$$

(ii) *Matrices with a particular trace are rare: fix* $\alpha \in \mathbb{F}_p[t]$ *and let* $F_\alpha : \mathbb{M}_2(\mathbb{F}_p[t]) \to \mathbb{F}_p[t]$ *be given by* $F_\alpha(A) = \mathrm{tr}(A) - \alpha$. *Then there exist* $C_1, C_2 > 0$ *such that:*

$$\mu_S^{(l)}(\{g \in SL_2(\mathbb{F}_p[t]) : \mathrm{tr}(g) = \alpha\}) = \mu_S^{(l)}(V(F_\alpha)) \leq C_1 e^{-C_2 l}.$$

(iii) *Torsion elements are rare: Let* $g \in SL_2(\mathbb{F}_p[t])$. *Conjugate* g, *possibly over a quadratic extension, to an upper triangular matrix* $\tilde{g} = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$. *Suppose there exists* $n \in \mathbb{N}$ *such that* $g^n = I_2$. *Then* $a^n = 1$. *This is only possible if* a *lies in a quadratic extension of* $\mathbb{F}_p$. *In particular* $\mathrm{tr}(g) \in \mathbb{F}_p$, *so* g *satisfies one of the bounded set of polynomials* F_α *as in (ii) above, for* $\alpha \in \mathbb{F}_p$. *Hence there exist* $C_1, C_2 > 0$ *such that:*

$$\mu_S^{(l)}(\{g \in SL_2(\mathbb{F}_p[t]) : g \text{ has finite order}\}) \leq \textstyle\sum_{\alpha \in \mathbb{F}_p} \mu_S^{(l)}(V(F_\alpha)) \leq C_1 e^{-C_2 l}.$$

(iv) *Elements fixing a point in the adjoint representation are rare: Recall that* $SL_2(\mathbb{F}_p[t])$ *acts linearly on* $\mathfrak{sl}_2(\mathbb{F}_p[t])$ *by conjugation. Given* $g \in SL_2(\mathbb{F}_p[t])$, *let* $\mathrm{Ad}(g) \in GL_3(\mathbb{F}_p[t])$ *be the matrix of the associated linear transformation with respect to some (fixed)* $\mathbb{F}_p[t]$*-basis for* $\mathfrak{sl}_2(\mathbb{F}_p[t])$.

Now recall that, given polynomials $F_1(X), F_2(X)$ *over some field* K, *there is a polynomial function* $\mathrm{Res}(F_1(X), F_2(X))$ *of their coefficients (defined over* $\mathbb{Z}$ *and depending only on the degrees of* F_1, F_2*) which vanishes precisely when* F_1, F_2 *have a common root in some extension of* K. *In particular,* $F(g) = \mathrm{Res}(\chi_{\mathrm{Ad}(g)}(X), X - 1)$ *is a polynomial in the entries of* g *which vanishes precisely when* g *has a non-zero fixed point in* $\mathfrak{sl}_2(\mathbb{F}_p[t])$. *Moreover* $F(g)$ *does not vanish identically on* $SL_2(\mathbb{F}_p[t])$:

$F\begin{pmatrix} 1+t & 2+t \\ t & 1+t \end{pmatrix} \neq 0$, *for instance. We conclude that there exist* $C_1, C_2 > 0$ *such that:*

$$\mu_S^{(l)}(\{g \in SL_2(\mathbb{F}_p[t]) : \exists X \in \mathfrak{sl}_2(\mathbb{F}_p[t]) \setminus \{0\} \text{ s.t. } X^g = X\}) \leq C_1 e^{-C_2 l}.$$

3.3. Squares in $SL_2(\mathbb{F}_p[t])$ are Rare. In this section we prove Theorem 1.2. Let $X \subseteq SL_2(\mathbb{F}_p[t])$ be the set of squares. In light of Proposition 3.3, it suffices to bound the sizes of images $\pi_{f_i}(X)$. We note some elementary facts about $SL_2(Q)$, for Q an arbitrary odd prime power. Let $D(Q) \leq SL_2(Q)$ be the subgroup of diagonal matrices. Recall that $D(Q)$ is cyclic of order $Q-1$.

Lemma 3.6: *Let $g \in D(Q)$ be non-central in $SL_2(Q)$. Then:*

(i) $C_{SL_2(Q)}(g) = D(Q)$.
(ii) $|\mathrm{ccl}_{SL_2(Q)}(g) \cap D(Q)| = 2$.
(iii) *If g is a square in $SL_2(Q)$ then it is a square in $D(Q)$.*

Now $2 \mid (Q-1)$, so the set of squares in $D(Q)$ is of order $\frac{Q-1}{2}$. $Z(SL_2(Q)) = \{\pm I_2\}$ consists of squares in $SL_2(Q)$, so that by Lemma 3.6 (iii), there is a subset $\{g_i\}_{i=1}^{\frac{Q-1}{2}} \subseteq D(Q)$ consisting entirely of non-squares in $SL_2(Q)$. If $g \in SL_2(Q)$ is not a square, then $\mathrm{ccl}_{SL_2(Q)}(g)$ consists entirely of non-squares, and by Lemma 3.6 (i), $|\mathrm{ccl}_{SL_2(Q)}(g)| = Q(Q+1)$. Hence:

$$\begin{aligned} |\{\text{non-squares in } SL_2(Q)\}| &\geq |\textstyle\bigcup_{i=1}^{\frac{Q-1}{2}} \mathrm{ccl}_{SL_2(Q)}(g_i)| \\ &\geq \tfrac{1}{2} \textstyle\sum_{i=1}^{\frac{Q-1}{2}} |\mathrm{ccl}_{SL_2(Q)}(g_i)| \text{ (by Lemma 3.6 (ii))} \\ &\geq \tfrac{1}{4}(Q-1)Q(Q+1) \\ &= \tfrac{1}{4}|SL_2(Q)|. \end{aligned}$$

Theorem 1.2 is now immediate from Proposition 3.3, taking $\gamma = \frac{3}{4}$.

3.4. Reducible Characteristic Polynomials in $SL_2(\mathbb{F}_p[t])$ are Rare. In this section we prove Theorem 1.4. Let $Y \subseteq SL_2(\mathbb{F}_p[t])$ be the set of elements with reducible characteristic polynomial. Once again, we bound $|\pi_{f_i}(Y)|$. Let $g \in Y$ and let $f \in \mathbb{F}_p[t]$ be irreducible of degree n. Since $\chi_g \in \mathbb{F}_p[t][X]$ splits over $\mathbb{F}_p[t]$, $\chi_{\pi_f(g)} \in \mathbb{F}_{p^n}[X]$ splits over $\mathbb{F}_{p^n}$. Let Q be an arbitrary odd prime power. It will suffice to bound the set of elements $g \in SL_2(Q)$ with reducible characteristic polynomial. We distinguish two cases and prove exponential decay in each:

Case 1: $\mathrm{tr}(g) \neq \pm 2$.

χ_g does not have a repeated root, so is diagonalisable in $SL_2(Q)$.

Hence there exists non-central $h \in D(Q)$ such that $\mathrm{ccl}_{SL_2(Q)}(g) = \mathrm{ccl}_{SL_2(Q)}(h)$. There are $Q-3$ non-central elements $h \in D(Q)$, and each has conjugacy class in $SL_2(Q)$ of order $Q(Q+1)$, by Lemma 3.6 (i). Therefore the number of non-central diagonalisable elements g is at most:

$$\begin{aligned} |\bigcup_{h \in D(Q) \setminus Z(SL_2(Q))} \mathrm{ccl}_{SL_2(Q)}(h)| &\leq \tfrac{1}{2} \sum_{h \in D(Q) \setminus Z(SL_2(Q))} |\mathrm{ccl}_{SL_2(Q)}(h)| \\ &\text{(by Lemma 3.6 (ii))} \\ &\leq \tfrac{1}{2}(Q-3)Q(Q+1) \\ &\leq \tfrac{1}{2}|SL_2(Q)|. \end{aligned}$$

Case 2: $\mathrm{tr}(g) = \pm 2$ is immediate from Example 3.5.

Theorem 1.4 follows from Proposition 3.3, with any $\gamma > \frac{1}{2}$.

References

[1] J. Bourgain, A. Gamburd. Uniform Expansion Bounds for Cayley Graphs of $SL_2(\mathbb{F}_p)$. Annals of Mathematics, **167** (2008), 625-642

[2] E. Breuillard. A Strong Tits Alternative. arXiv:0804.1395

[3] E. Breuillard. Approximate subgroups and super-strong approximation. arXiv:1407.3158

[4] E. Breuillard, B. Green, T. Tao. Approximate Subgroups of Linear Groups. Geom. Funct. Anal. Vol. 21 (2011) 774-819

[5] E. Breuillard, B. Green, R. Guralnick, T. Tao. Expansion in finite simple groups of Lie type. arXiv:1309.1975

[6] O. Dinai. Expansion properties of finite simple groups. Ph. D. thesis. The Hebrew University of Jerusalem (2009)

[7] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, B. Virág. On the girth of random Cayley graphs. Random Structures and Algorithms 35 (2009), no.1, 100-117

[8] W.T. Gowers. Quasirandom Groups. Combinatorics, Probability and Computing, Volume 17, Issue 03, May 2008, pp 363-387

[9] O.H. King. The subgroup structure of finite classical groups in terms of geometric configurations. Surveys in combinatorics, 2005. Edited by B. S. Webb.

[10] V. Landazuri, G. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. J. Algebra 32 (1974), 418-443

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

[12] A. Lubotzky, C. Meiri. Sieve methods in group theory I: Powers in linear groups. J. Amer. Math. Soc. 25 (2012), 1119-1148

[13] L. Pyber, E. Szabo. Growth in finite simple groups of Lie type of bounded rank. arXiv:1005.1858

[14] A. Salehi Golsefidy, P. P. Varjú. Expansion in Perfect Groups. Geom. Funct. Anal., 22 (6), 1832-1891 (2012)

[15] P. Sarnak, X. Xue. Bounds for multiplicities of automorphic representations. Duke Math. J. **64** (1991), 207-227

[16] T. Tao. Expansion in finite simple groups of Lie type. http://terrytao.files.wordpress.com/2014/04/expander-book.pdf

[17] T. Tao. Product set estimates for non-commutative groups. Combinatorica, September 2008, Volume 28, Issue 5, pp 547-594

[18] P. P. Varjú. Expansion in $SL_d(\mathcal{O}_K/I)$, I square free. J. Eur. Math. Soc. (JEMS) 14 (2012), no. 1, 273-305