J. Group Theory **14** (2011), 273–297
DOI 10.1515/JGT.2010.056

Journal of Group Theory

Growth in SL_2 over finite fields

Oren Dinai

(Communicated by R. Guralnick)

Abstract. By using tools from additive combinatorics, invariant theory and bounds on the size of the minimal generating sets of $\mathrm{PSL}_2(\mathbb{F}_q)$, we prove the following growth property. There exists $\varepsilon > 0$ such that the following holds for any finite field $\mathbb{F}_q$. Let G be the group $\mathrm{SL}_2(\mathbb{F}_q)$, or $\mathrm{PSL}_2(\mathbb{F}_q)$, and let A be a generating set of G. Then

$$|A \cdot A \cdot A| \geqslant \min\{|A|^{1+\varepsilon}, |G|\}.$$

Our work extends the work of Helfgott [26] who proved similar results for the family $\{\mathrm{SL}_2(\mathbb{F}_p) : p \text{ prime}\}$.

1 Introduction

1.1 Background. Let us define the *directed diameter* of a finite group G with respect to a set of generators S to be the minimal number l for which any element in G can be written as a product of at most l elements in S. We denote this number by $\mathrm{diam}^+(G,S)$. Define the (*undirected*) *diameter* of G with respect to S to be $\mathrm{diam}(G,S) := \mathrm{diam}^+(G, S \cup S^{-1})$.

The diameter of groups has many applications. Aside from group theory (see [3], [28], [29]) and combinatorics (see [17], [22], [23], [24]) the diameter of groups shows up in computer science e.g., in the context of computer networks (see [32], [36]), generalizations of Rubik's puzzles (see [20], [30]) and algorithms and complexity (see [21], [27]). For a detailed review see [2].

Since we are interested in the 'worst case generators', we define

$$\mathrm{diam}(G) := \max\{\mathrm{diam}(G,S) : G = \langle S \rangle\}.$$

A family of finite groups $\{G_n : n \in \mathbb{N}\}$ is said to have *poly-log diameter* (resp. *log diameter*) if for some $C, d > 0$ (resp. for $d = 1$), for any $n \in \mathbb{N}$ we have

$$\mathrm{diam}(G_n) \leqslant C \log^d(|G_n|).$$

In [15], the author showed (with an effective algorithm) that for any fixed $p, m \in \mathbb{N}$ with p a prime and $p > m \geqslant 2$, the family

$$\mathcal{G}_{m,p} := \{\mathrm{SL}_m(\mathbb{Z}/p^n\mathbb{Z}) : n \in \mathbb{N}\}$$

has poly-log diameter. Abért and Babai [1] showed that for any fixed prime p_0, the family $\{C_{p_0} \wr C_p : p \text{ prime}; p \neq p_0\}$ has logarithmic diameter.

A long-standing conjecture of Babai [7] asserts that the family of non-abelian finite simple groups has poly-logarithmic diameter. Very little is known about this conjecture. See [6] and [7] for some partial results concerning the alternating groups.

A breakthrough result of Helfgott [26] proves the conjecture for the family $\{\mathrm{SL}_2(\mathbb{F}_p) : p \text{ prime}\}$. The main goal of this paper is to extend Helfgott's work to the family $\{\mathrm{SL}_2(\mathbb{F}_{p^n}) : p \text{ prime}; n \in \mathbb{N}\}$. We follow the basic strategy of Helfgott (with some short cuts following [10]) and in particular we also appeal to additive combinatorics and sum-product theorems. The new difficulty is that unlike fields of prime order, general finite fields have subfields, and subsets which are 'almost' subfields, which are 'almost' stable with respect to sum and product.

1.2 Main results.

The following result extends the key proposition of Helfgott [26, Key Proposition in §1.2].

Theorem 1.1. *There exists $\varepsilon \in \mathbb{R}_+$ such that the following holds for any finite field $\mathbb{F}_q$. Let G be either the group $\mathrm{SL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$ and let A be a generating set of G. Then*

$$|A \cdot A \cdot A| \geqslant \min\{|A|^{1+\varepsilon}, |G|\}. \tag{1}$$

From this we get immediately the following corollary.

Corollary 1.2. *There exist $C, d \in \mathbb{R}_+$ such that the following holds for any finite field $\mathbb{F}_q$. Let A be generating set of $G = \mathrm{SL}_2(\mathbb{F}_q)$. Then*

$$\mathrm{diam}^+(G, A) < C \log^d(|G|)$$

and for any $\delta \in \mathbb{R}_+$ we have

$$|A| > |G|^\delta \quad \Rightarrow \quad \mathrm{diam}^+(G, A) < C\delta^{-d}.$$

1.3 Organization of the paper.

In Section 2 we introduce notation and definitions required for this work as well as mathematical background, and we prove some additional results that may be of interest. In Section 3 we prove the main results.

2 Preliminaries

2.1 Notation.

We write $\log x$ for $\log_2 x$, the logarithm to base 2. We will always use p for a prime number and q for a prime power. For a subset $A \subseteq B$ and $x \in B$ write

$A\backslash x$ for $A\backslash\{x\}$ and similarly $A \cup x := A \cup \{x\}$. For a field $\mathbb{F}$, denote by $\overline{\mathbb{F}}$ some fixed algebraic closure of $\mathbb{F}$. We write $(G, \cdot)$ for a multiplicative group which is not necessarily commutative and $(G, +)$ for a commutative additive group.

Definition 2.1. Let G be a group and let $A, B, A_1, \dots, A_n$ be non-empty subsets of G. Write $A^{\pm} := A \cup A^{-1}$ and for $k \in \mathbb{Z}$, write $A^k := \{a^k : a \in A\}$. Define the product set $A \cdot B := \{a \cdot b : a \in A, b \in B\}$, and for $x \in G$ define $x \cdot A := \{x\} \cdot A$ and $A \cdot x := A \cdot \{x\}$. Write

$$\prod_{i=1}^{n} A_i := \{a_1 \dots a_n : a_i \in A_i \text{ for all } i\}$$

for the product set of $A_1, \dots, A_n$ and $A^{(n)} := \prod_{i=1}^{n} A$ for the product of a set A with itself n times. The notation $A^{[0]} := \{1\}$, $A^{[1]} := A^{\pm} \cup 1$ and

$$A^{[n]} := (A^{[1]})^{(n)}$$

for the set of words of length at most n in $A^{\pm}$ will be important in this paper. In general we have only the containments $A^n \subseteq A^{(n)} \subseteq A^{[n]}$.

Since we have three possible operations on the subsets, $A^{[m]}$, $A^{(n)}$ and A^k, we use the following 'group action' notation: $A^{xyz} := ((A^x)^y)^z$ when x, y, z are any of these operations; e.g., $A^{k(n)[m]} := ((A^k)^{(n)})^{[m]}$.

Definition 2.2. Let G be a group and let $g, h \in G$. We write $g^h := h^{-1}gh$ and $[g, h] := g^{-1}g^h = g^{-1}h^{-1}gh$. For $A, B \subseteq G$ and $x \in G$ we write

$$A^B := \{a^b : a \in A, b \in B\} \quad \text{and} \quad x^B := x^B.$$

We write

$$[A, B]_{\text{set}} := \{[a, b] : a \in A; b \in B\}. \tag{2}$$

Note that $[A, B]_{\text{set}} \subseteq A^{-1}A^B \subseteq A^{-1}B^{-1}AB$. Note also that $A^{g(n)} = A^{(n)g}$ i.e., $(A^g)^{(n)} = (A^{(n)})^g$. Therefore conjugation, or any other automorphism, commutes with the operations $A^{[m]}$, $A^{(n)}$ and A^k.

Definition 2.3. Let G be a group and let $A, B \subseteq G$. Define

$$\mathrm{C}_B(A) := \{b \in B : a^b = a \text{ for all } a \in A\}.$$

We will use the generation notation $\langle A \rangle$ depending on the category we are using. The categories that will be involved in the paper will be groups and rings.

Definition 2.4. For positive real-valued functions, we write $f \ll g$ if $f = O(g)$. Similarly we write $f \gg g$ if $g \ll f$, and $f \approx g$ if $f \ll g \ll f$. We will use the dual notation $f = \Omega(g)$ for $g = O(f)$.

Denote the group of invertible elements of a commutative ring R by $R^{\times}$. If A is a subset of R, we will need different notation to distinguish the product set $A \cdot A = \{ab : a, b \in A\}$ and the sum set $A + A = \{a + b : a, b \in A\}$. Therefore we will need in some situations the following definitions.

Definition 2.5. Let A be a subset of an additive (semi-)group G and let $n \in \mathbb{N}$. Write

$$\sum_{n} A := \{a_1 + \cdots + a_n : a_i \in A \text{ for all } i\}.$$

Definition 2.6. Let $\Gamma \subseteq X \times Y$ be a directed graph. Denote the inverse graph $\Gamma^{-1} \subseteq Y \times X$ by $\Gamma^{-1} := \{(y, x) : (x, y) \in \Gamma\}$. Let $A \subseteq X$ and $a \in X$. Write $\Gamma_a := \{y \in Y : (a, y) \in \Gamma\}$ and $\Gamma(A) := \bigcup_{a \in A} \Gamma_a$ and $\deg(\Gamma) := \max\{|\Gamma_x| : x \in X\}$. We define the *multiplicity* of Γ to be

$$\operatorname{mult}(\Gamma) := \deg(\Gamma^{-1}).$$

Clearly if $\deg(\Gamma) \leqslant d$ then $|\Gamma(A)| \leqslant d|A|$ for any $A \subseteq X$. We will say that Γ is d-regular if $|\Gamma_x| = d$ for all $x \in X$. We will use the previous definition with the following simple observations. A function $f \in Y^X$ from X to Y is a directed graph which is 1-regular. Therefore if $\operatorname{mult}(f) \leqslant n$ then $|f(A)| \geqslant |A|/n$ for any $A \subseteq X$. For example, any non-zero one-variable polynomial $f(x) \in \mathbb{F}[x]$ of degree d defines a substitution map $f_s : \mathbb{F} \to \mathbb{F}$ such that $\operatorname{mult}(f_s) \leqslant \deg(f)$. Similarly if $0 \neq f(x, x^{-1}) \in \mathbb{F}[x, x^{-1}]$, with $\deg_x(f) + \deg_{x^{-1}}(f) = d$, then $\operatorname{mult}(f_s) \leqslant d$, where $f_s : \mathbb{F}^{\times} \to \mathbb{F}$. For example, $f(x) = x^2 + x^{-3}$ has multiplicity at most 5. By abuse of notation we write $\operatorname{mult}(f) := \operatorname{mult}(f_s)$.

2.2 Additive combinatorics.

The following lemma [26, Lemma 2.2] is a simple consequence of the Ruzsa triangular inequality [38, Lemma 2.6].

Lemma 2.7. *Let G be a group and let $A \subseteq G$ be a finite subset. Then whenever $3 \leqslant n \in \mathbb{N}$ and $1 \leqslant K \in \mathbb{R}$ we have*

$$|A^{[n]}| > K|A| \quad \Rightarrow \quad |A^{(3)}| > \frac{1}{2}\sqrt[3n]{K}|A|. \tag{3}$$

When dealing with fields one can use the following sum-product theorem which is a slight improvement of [11], [12] (cf. [38, §2.8]).

Theorem 2.8 ([38, Theorem 2.52]). *There exists an absolute constant $C > 0$ such that the following holds whenever $1 \leqslant K \in \mathbb{R}$ and for any field $\mathbb{F}$. Let $A \subseteq \mathbb{F}$ be a finite subset and suppose that*

$$|A + A| + |A \cdot A| \leqslant K|A|.$$

Then either $|A| < CK^C$, or for some subfield $\mathbb{E} \leqslant \mathbb{F}$ and $x \in \mathbb{F}^\times$ we have

$$|\mathbb{E}| \leqslant CK^C|A| \quad \textit{and} \quad |A \backslash x\mathbb{E}| \leqslant CK^C.$$

We introduce some notation and use it to restate the previous theorem.

Definition 2.9 (almost fields). Let $\mathbb{F}$ be a field and let $A \subseteq \mathbb{F}$ be a finite subset and let $\varepsilon \in \mathbb{R}_+$. We will say that A is *ε-almost field*, or *ε-field* for short, if for some subfield $\mathbb{E} \leqslant \mathbb{F}$ and $x \in \mathbb{F}^\times$ we have

$$|\mathbb{E}| \leqslant |A|^{1+\varepsilon} \quad \text{and} \quad |A \backslash x\mathbb{E}| \leqslant |A|^{\varepsilon}. \tag{4}$$

If the above holds then we will say that A is *ε-almost $x\mathbb{E}$*. Define A to be *pure* ε-field if

$$|\mathbb{E}| \leqslant |A|^{1+\varepsilon} \quad \text{and} \quad A \subseteq \mathbb{E}. \tag{5}$$

If (4) field holds but (5) does not hold then we will say that A is impure ε-field. In other words, A is *impure* ε-field if (4) field holds and also $|A \backslash \mathbb{E}| > 0$.

Definition 2.10 (almost stable). Let $\mathbb{F}$ be a field, $A \subseteq \mathbb{F}$ be a finite set and let $\varepsilon \in \mathbb{R}_+$. We will say that A is *ε-close*, or *ε-stable*, if

$$|A \cdot A| + |A + A| \leqslant |A|^{1+\varepsilon}. \tag{6}$$

Otherwise, we will say that A has *ε-expansion* or *ε-growth.*

Let us restate Theorem 2.8 using this terminology.

Theorem 2.11. *There exists $C > 0$ such that the following holds for any $\varepsilon \in \mathbb{R}_+$ with $\varepsilon < C^{-1}$. Let $\mathbb{F}$ be a field and let A be a finite subset of size $|A| > C^{1/\varepsilon}$.*

(a) *If A is an ε-field then A is $C\varepsilon$-stable.*

(b) *If A is ε-stable then A is a $C\varepsilon$-field.*

2.3 Expansion functions in fields.

Definition 2.12. Let $\mathbb{F}$ be a field, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F})$ and $t \in \mathbb{F}$. Let $x, y \in \mathbb{F}^\times$ and $X, Y \subseteq \mathbb{F}^\times$. Write

$$\operatorname{Prod}(g) := a \cdot d, \quad D_x := \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \quad \text{and} \quad D_X := \{D_x : x \in X\}.$$

Define $\mathrm{tr}(x) := \mathrm{Tr}(D_x) = x + x^{-1}$ and

$$\mathrm{tr}_g(x, y) := \mathrm{Tr}(D_x(D_y)^g) = ad \cdot \mathrm{tr}(xy) - bc \cdot \mathrm{tr}(x/y). \tag{7}$$

We extend these definitions to $\mathrm{tr}(X)$ and $\mathrm{tr}_g(X, Y)$ for subsets. Define

$$\mathrm{tr}_t(x, y) := t \cdot \mathrm{tr}(xy) + (1 - t) \cdot \mathrm{tr}(x/y).$$

So $\mathrm{tr}_g(x, y) = \mathrm{tr}_s(x, y)$ where $s = \mathrm{Prod}(g)$.

The following striking reduction of Helfgott allows one to gain large expansion from the non-commutativity in the group by twisting properly some commutative sets (cf. [26, §3] and [10, §4]). The proof is based on the following trick of Helfgott and [10, §4]: for any subset $Y \subseteq \mathbb{F}^\times$ we have

$$\{(t, s) : t, s \in Y^2\} \subseteq \{(xy, xy^{-1}) : x, y \in Y^{[2]}\}. \tag{8}$$

Theorem 2.13 (Helfgott). *There exists $C > 0$ such that the following holds for any field $\mathbb{F}$ and $1 \leqslant K \in \mathbb{R}$. Let $X \subseteq \mathbb{F}^\times$ be a finite subset and let $a_1, a_2 \in \mathbb{F}^\times$. Let $V \subseteq \mathrm{SL}_2(\mathbb{F})$ be a finite subset of diagonal matrices, $g \in \mathrm{SL}_2(\mathbb{F})$ with $\mathrm{Prod}(g) \notin \{0, 1\}$ (i.e., g has no zero entries) and let $\varepsilon \in \mathbb{R}_+$.*

If

$$|\{a_1 \cdot \mathrm{tr}(xy) + a_2 \cdot \mathrm{tr}(xy^{-1}) : x, y \in X^{[4]}\}| < K|\mathrm{tr}(X)|$$

then

$$|\mathrm{tr}(X^2)\,\mathrm{tr}(X^2)| + |\mathrm{tr}(X^2) + \mathrm{tr}(X^2)| < CK^C|\mathrm{tr}(X)|.$$

If $|\mathrm{Tr}(V^{[4]} \cdot V^{g[4]})| < |\mathrm{Tr}(V)|^{1+\varepsilon}$ then

$$|\mathrm{Tr}(V^2) \cdot \mathrm{Tr}(V^2)| + |\mathrm{Tr}(V^2) + \mathrm{Tr}(V^2)| < C|\mathrm{Tr}(V^2)|^{1+C\varepsilon}. \tag{9}$$

Now we make some simple observations that we will use later.

Lemma 2.14. *There exists $c > 0$ such that the following holds. Let $\mathbb{F}$ be a field and let $g \in \mathrm{SL}_2(\mathbb{F})$. Let $V \subseteq \mathrm{SL}_2(\mathbb{F})$ be a finite subset of diagonal matrices. Suppose that $\mathrm{Tr}(V^{[4]}) \subseteq \mathbb{E}$ for some subfield $\mathbb{E} \leqslant \mathbb{F}$. If $\mathrm{Prod}(g) \notin \mathbb{E}$ then*

$$|\mathrm{Tr}(V^{[4]} \cdot V^{[4]g})| > c|\mathrm{Tr}(V)|^2. \tag{10}$$

If $\mathrm{Prod}(g) \neq 1$ then

$$|\mathrm{Tr}([V, g])| > c|\mathrm{Tr}(V)|. \tag{11}$$

Proof. Write $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, set $X := \{x \in \mathbb{F} : D_x \in V\}$ and

$$T := \operatorname{Tr}(V^{[4]} V^{[4]g}) = \{ad \cdot \operatorname{tr}(xy) - bc \cdot \operatorname{tr}(x/y) : x, y \in X^{[4]}\},$$
$$T' := \{ad \cdot \operatorname{tr}(t) - bc \cdot \operatorname{tr}(s) : t, s \in X^{[2]2}\}.$$

By (8) we have $T' \subseteq T$. Set $f(z, w) := ad \cdot z + (1 - ad) \cdot w$. Since $ad - bc = 1$ we get $T' = f(\operatorname{tr}(X^{[2]2}), \operatorname{tr}(X^{[2]2}))$.

We claim that if $\operatorname{Prod}(g) = ad \notin \mathbb{E}$ then $f|_{\mathbb{E}\times\mathbb{E}}$ is injective. Indeed, writing $t = ad$ then by solving $tz + (1-t)w = tz' + (1-t)w'$, we get $t(z - z') = (1-t)(w' - w)$. Since $t \neq 0, 1$, either $z - z' = w' - w = 0$, or $(1-t)/t = t^{-1} - 1 \in \mathbb{E}$ which contradicts our assumption that $t = ad \notin \mathbb{E}$. Similarly we see that $f|_{x\mathbb{E}\times x\mathbb{E}}$ is injective for any coset of $\mathbb{E}$.

By the assumption $\operatorname{tr}(X^{[2]2}) \subseteq \operatorname{tr}(X^{[4]}) = \operatorname{Tr}(V^{[4]}) \subseteq \mathbb{E}$; therefore

$$|T| \geqslant |T'| = |\operatorname{tr}(X^{[2]2})|^2 \geqslant |\operatorname{tr}(X^2)|^2 \geqslant \left(\frac{1}{4}|\operatorname{tr}(X)|\right)^2$$

so we are done with (10). Now if $\operatorname{Prod}(g) = ad \neq 1$ then we get

$$\begin{aligned} |\operatorname{Tr}([V^{[4]}, g])| &= |\{\operatorname{Tr}(v^{-1}v^g) : v \in V^{[4]}\}| \\ &= |\{2ad + (1 - ad)\operatorname{tr}(x^2) : x \in X^{[4]}\}| \\ &= |\operatorname{tr}(X^{[4]2})| \geqslant \frac{1}{4}|X^{[4]}|. \quad \square \end{aligned}$$

Using the theorem of Frobenius on the characters of $\mathrm{SL}_2(\mathbb{F}_q)$, Babai, Nikolov and Pyber [4] obtained, after extending Gowers [25, Theorems 1.1, 1.2], the following result (cf. [31] and [5]).

Theorem 2.15. *There exist $C \in \mathbb{R}_+$ such that the following holds. Let $\mathbb{F}_q$ be a finite field and let A be a subset of $G = \mathrm{SL}_2(\mathbb{F}_q)$. Then*

$$|A| > Cq^{8/3} \quad \Rightarrow \quad A^{(3)} = \mathrm{SL}_2(\mathbb{F}_q). \tag{12}$$

2.4 Symbolic generation of traces. The invariant theory of tuples of matrices under various actions was developed over fields of zero characteristic. We are interested in the case of positive characteristic (cf. [14], [18], [33]).

Definition 2.16. For $m \geqslant 2$ denote by $\mathrm{R}_{2,m}$ the ring of invariants of m-tuples of 2×2 generic matrices $(X_1, \ldots, X_m)$ over a infinite field $\mathbb{F}$ under the simultaneous conjugation action of the general linear group. To be precise, we have $4m$ variables $x_1, y_1, z_1, w_1, \dots, x_m, y_m, z_m, w_m$ which we denote by $\overline{X_i} = (x_i, y_i, z_i, w_i)$ and $\overline{X} = (\overline{X_1}, \dots, \overline{X_m})$. Each

$$X_i = \begin{pmatrix} x_i & y_i \\ z_i & w_i \end{pmatrix}$$

is a formal matrix with four variables $\overline{X_i}$ for $1 \leqslant i \leqslant m$. We define an action of $g \in \mathrm{GL}_2(\mathbb{F})$ on $f(X_1, \dots, X_m) \in \mathbb{F}[\overline{X}]$ by

$$f^g(X_1, \dots, X_m) := f(X_1^g, \dots, X_m^g).$$

We define the algebra of invariants of this polynomial ring under the action of $\mathrm{GL}_2(\mathbb{F})$ by $\mathrm{R}_{2,m}(\mathbb{F}) := \{f \in \mathbb{F}[\overline{X}] : f^g = f \text{ for any } g \in \mathrm{GL}_2(\mathbb{F})\}$.

We will use the following results of Procesi [34] and Domokos, Kuzmin and Zubkov [19, Corollary 4.1].

Theorem 2.17. *If* $\mathrm{char}(\mathbb{F}) \neq 2$ *then*

$$\{\det(X_i), \mathrm{tr}(X_{i_1} \dots X_{i_s}) : 1 \leqslant i \leqslant m; 1 \leqslant s \leqslant 3; 1 \leqslant i_1 < \cdots < i_s \leqslant m\}$$

is a minimal system of generators of $\mathrm{R}_{2,m}(\mathbb{F})$. *If* $\mathrm{char}(\mathbb{F}) = 2$ *then*

$$\{\det(X_i), \mathrm{tr}(X_{i_1} \cdot \dots \cdot X_{i_s}) : 1 \leqslant i, s \leqslant m; 1 \leqslant i_1 < \cdots < i_s \leqslant m\}$$

is a minimal system of generators of $\mathrm{R}_{2,m}(\mathbb{F})$.

From this we get immediately the following result.

Lemma 2.18 (trace generation). *Let* $\mathbb{F}$ *be a field and let* $A \subseteq \mathrm{SL}_2(\mathbb{F})$ *be a subset with* $2 \leqslant |A| \leqslant m$. *Then we have the ring generation* $\langle \mathrm{Tr}(A^{[m]}) \rangle = \langle \mathrm{Tr}(\langle A \rangle) \rangle$. *Moreover if* $\mathrm{char}(\mathbb{F}) \neq 2$, *then we have the ring generation* $\langle \mathrm{Tr}(A^{[3]}) \rangle = \langle \mathrm{Tr}(\langle A \rangle) \rangle$.

Remark. There are various possible types of generation, depending on the category involved: groups, rings, algebras, vector spaces, modules and fields. In the invariant context, ring and group generation are involved. In the lemma, the meaning is ring generation in the outer bracket and group generation in the inner bracket. Explicitly, $\langle \mathrm{Tr}(A^{[m]}) \rangle_{\text{ring}} = \langle \mathrm{Tr}(\langle A \rangle_{\text{group}}) \rangle_{\text{ring}}$.

2.5 Size of minimal generating sets. By Lemma 2.18, for any finite field $\mathbb{F} = \mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}) \neq 2$ and any subset of generators A for $\mathrm{SL}_2(\mathbb{F}_q)$ we have 'bounded generation of trace generators'; indeed, $\langle \mathrm{Tr}(A^{[3]}) \rangle = \mathbb{F}$.

In this section we extend this to $\mathrm{char}(\mathbb{F}) = 2$. The main theorem of this section, and the only part used later, is Theorem 2.22 which asserts that $\langle \mathrm{Tr}(A^{[6]}) \rangle = \mathbb{F}$.

Definition 2.19. Let G be a finitely generated group. A subset A of G a *minimal generating set* if $\langle A\rangle = G$ but for any proper subset A' of A we have $\langle A'\rangle \neq G$. A subgroup H of $\mathrm{PSL}_2(\mathbb{F}_q)$ is called a *subfield subgroup* if $H \cong \mathrm{PSL}_2(q')$ for some subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_q$.

Saxl and Whiston proved the following result about the size of minimal generating sets of $\mathrm{PSL}_2(\mathbb{F}_q)$; cf. [35, Theorem 3 and Theorem 7 with its proof].

Theorem 2.20 ([35, Theorems 3, 7]). *Let $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with $q = p^r$ a prime power and let $A = \{g_1, \dots, g_m\}$ be a minimal generating set.*

If $r = 1$ then $|A| \leqslant 4$. If $r > 1$ then let $r = p_1^{e_1} \dots p_n^{e_n}$ be the prime decomposition of r and let $A_i := A\backslash g_i$ and $H_i := \langle A_i\rangle$. For $1 \leqslant j \leqslant n$, let S_j be the set of subfield subgroups H_i for which j is minimal subject to $H_i \leqslant G_j \cong \mathrm{PSL}_2(p^{r/p_j})$.

If $|A| > 6$ then after reordering of the elements g_i and the primes p_j one of the following holds.

(1) *For any $i \geqslant 3$, H_i is a subfield subgroup and there exists a unique j for which $H_i \leqslant G_j \cong \mathrm{PSL}_2(p^{r/p_j})$.*

(2) *For any $i \geqslant 2$, H_i is a subfield subgroup, $|S_1| \leqslant 2$ and $|S_j| \leqslant 1$ for any $j \geqslant 2$.*

(3) *For any $i \geqslant 1$, H_i is a subfield subgroup, $|S_1| \leqslant 3$ and $|S_j| \leqslant 1$ for any $j \geqslant 2$.*

As an immediate corollary we get the following claim.

Corollary 2.21. *Let q be a prime power, $G = \mathrm{PSL}_2(\mathbb{F}_q)$ and $A = \{g_1, \dots, g_m\}$ be a minimal generating set. Let $H_i := \langle A\backslash\{g_i\}\rangle$.*

If $|A| \geqslant 7$ then the subgroups H_i which are subfield subgroups $H_i \cong \mathrm{PSL}_2(\mathbb{F}_{q_i})$, satisfy that the subfields $\mathbb{F}_{q_i}$ generate $\mathbb{F}_q$.

Proof. We use the notation of the previous theorem. Let $q = p^r$ and $r = p_1^{e_1} \dots p_n^{e_n}$ be the prime decomposition of r. By the previous theorem we have three cases to consider. In all cases, for any S_j there exist $i = i_j$ and H_i and r_i such that $H_i \cong \mathrm{PSL}_2(p^{r_i}) \notin S_j$. In other words, for each j we have $r_{i_j} \nmid r/p_j$. Therefore $\mathrm{l.c.m}(r_{i_1}, \dots, r_{i_n}) = r$. □

Now let us use this corollary to prove the following theorem.

Theorem 2.22. *Let $q = p^r$ with p prime, let $G = \mathrm{SL}_2(\mathbb{F}_q)$ and let A be a generating set of G. Then $\langle \mathrm{Tr}(A^{[6]})\rangle = \mathbb{F}_q$.*

Proof. By Lemma 2.18, if $p \neq 2$ then $\langle \mathrm{Tr}(A^{[3]})\rangle = \mathbb{F}$. So assume that $p = 2$ and $G = \mathrm{SL}_2(\mathbb{F}_q) = \mathrm{PSL}_2(\mathbb{F}_q)$. Taking a subset A' of A if needed, we can assume that A is a minimal generating set. If $|A| \leqslant 6$ then by Lemma 2.18 we get $\langle \mathrm{Tr}(A^{[6]})\rangle = \mathbb{F}_q$.

Now by induction on r, and the previous theorem, if $r = 1$ then $|A| \leqslant 4$ and so $\langle \mathrm{Tr}(A^{[4]})\rangle = \mathbb{F}_q$. Otherwise, let $r = p_1^{e_1} \dots p_n^{e_n}$ be the prime decomposition of r. If $|A| \geqslant 7$ then by the previous corollary we get proper subfield subgroups

$H_i \cong \mathrm{SL}_2(2^{r_i})$, such that the subfields $\mathbb{F}_{2^{r_i}}$ generate $\mathbb{F}_{2^r}$. By the induction hypothesis on these H_i, which are generated by $A_i = A \backslash g_i$, we get $\langle \mathrm{Tr}(A_i^{[6]}) \rangle = \mathbb{F}_{2^{r_i}}$. Therefore $\langle \mathrm{Tr}(A^{[6]}) \rangle = \mathbb{F}_q$ as we wanted. □

2.6 Avoiding certain traces. We start with an identity that we will use many times.

Lemma 2.23. *Let* $\mathbb{F}$ *be a field and* $g, h \in \mathrm{SL}_2(\mathbb{F})$. *Then*

$$\mathrm{Tr}(g)\,\mathrm{Tr}(h) = \mathrm{Tr}(gh) + \mathrm{Tr}(gh^{-1}). \tag{13}$$

Proof. From the Cayley–Hamilton theorem $h^2 - \mathrm{Tr}(h)h + I = 0$, and we get by multiplying by gh^{-1} the matrix identity

$$gh - \mathrm{Tr}(h)g + gh^{-1} = 0.$$

Therefore by taking traces we are done. □

Definition 2.24. Let $\mathbb{F}$ be a field, G be a linear group and let $A \subseteq G(\mathbb{F})$ and $X \subseteq \mathbb{F}$. Write $A|_X := \{g \in A : \mathrm{Tr}(g) \in X\}$ and $A\not|_X := \{g \in A : \mathrm{Tr}(g) \notin X\}$. If $X = \{x\}$ we write x instead of X and $\pm x$ instead of $\{\pm x\}$; thus $A|_x := A|_{\{x\}}$, $A|_{\pm x} := A|_{\{\pm x\}}$ and similarly for $A\not|_x$ and $A\not|_{\pm x}$.

Definition 2.25. Let $\mathbb{F}$ be a field. Let $V(\mathbb{F}) := \mathbb{F}^2 \backslash \{0\}$ and let $\mathbb{P}(\mathbb{F}) := V(\mathbb{F})/\sim$ be the *projective line* over $\mathbb{F}$; thus for $v \in V(\mathbb{F})$, the equivalence class $\bar{v} \in P(\mathbb{F})$ is $\mathrm{span}(v) \backslash \{0\}$. Consider the projective line over the algebraic closure $\bar{F}$. The action of $G = \mathrm{SL}_2(\bar{\mathbb{F}})$ on $V(\bar{\mathbb{F}})$ by left multiplication induces an action on $\mathbb{P}(\bar{\mathbb{F}})$. For $g \in G$ write $\mathrm{Fix}(g) := \{\bar{v} \in \mathbb{P}(\bar{\mathbb{F}}) : g\bar{v} = \bar{v}\}$ for the *fixed-point set* of g. Note that if $v \in V(\mathbb{F})$ then $g\bar{v} = \bar{v}$ if and only if $gv = \lambda v$ for some $\lambda \in \bar{\mathbb{F}}^\times$. For a subset $V \subseteq \mathrm{SL}_2(\mathbb{F})$ write $\mathrm{Fix}(V) := \bigcap_{g \in V} \mathrm{Fix}(g)$.

Simple fact 2.26. Let $G = \mathrm{SL}_2(\mathbb{F})$. Denote by G_u the set of non-trivial $\pm$unipotent elements in G; thus $u \in G_u$ if and only if there exist $w \in \mathrm{SL}_2(\mathbb{F})$, $a \in \{\pm 1\}$ and $x \in \mathbb{F}^\times$ such that

$$u^w = a\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = a(I + xE_{12}).$$

If we denote the two columns of w by $w = (w_1, w_2)$ then $\mathrm{Fix}(u) = \{\bar{w}_1\}$. We have $G_u = G|_{\pm 2} \backslash \{\pm I\} = \{u \in G : |\mathrm{Fix}(u)| = 1\}$. For $A \subseteq G$ write $A_u := A \cap G_u$.

Simple fact 2.27. Let $G = \mathrm{SL}_2(\mathbb{F})$. Denote by G_s the semi-simple elements in G; thus $s \in G_s$ if and only if there exist $w \in \mathrm{SL}_2(\bar{\mathbb{F}})$ and $y \in \bar{\mathbb{F}} \backslash \{\pm 1\}$ such that

$$u^w = D_y = \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix}.$$

If $w = (w_1, w_2)$ then $\mathrm{Fix}(s) = \{\overline{w}_1, \overline{w}_2\}$. We have

$$G_s = G\nmid_{\pm 2} = \{s \in G : |\mathrm{Fix}(s)| = 2\}.$$

For $A \subseteq G$ write $A_s := A \cap G_s$.

Simple fact 2.28. Let $G = \mathrm{SL}_2(\mathbb{F})$. For $A \subseteq G$ we write for short,

$$\begin{aligned}\mathrm{C}(A) &:= \mathrm{C}_G(A) = \{g \in G : a^g = a \text{ for any } a \in A\},\\ \mathrm{N}(A) &:= \mathrm{N}_G(A) = \{g \in G : A^g = A\}.\end{aligned}$$

Let $s \in G_s$ and $u \in G_u$. Then

$$\begin{aligned}\mathrm{C}(s) &= \{s' \in G : \mathrm{Fix}(s') = \mathrm{Fix}(s)\} \cup \{\pm I\},\\ \mathrm{C}(u) &= \{u' \in G : \mathrm{Fix}(u') = \mathrm{Fix}(u)\} \cup \{\pm I\},\\ \mathrm{N}(\mathrm{C}(s)) &= \{g \in G : g(\mathrm{Fix}(s)) = \mathrm{Fix}(s)\},\\ \mathrm{N}(\mathrm{C}(u)) &= \{b \in G : \mathrm{Fix}(u) \subseteq \mathrm{Fix}(b)\}.\end{aligned}$$

The following lemma of Helfgott will yield many semi-simple elements (cf. [26, Lemma 4.2]).

Lemma 2.29 (Helfgott). *Let $\mathbb{F}$ be a field, let $G = \mathrm{SL}_2(\mathbb{F})$ and let A be a finite subset. If $\langle A \rangle$ is non-abelian, then $|A^{[3]} \cap G_s| \geqslant \frac{1}{4}|A|$.*

The following lemma is a slight variant of Lemma 2.29.

Lemma 2.30. *Let $\mathbb{F}$ be a finite field. Let A be a generating set of $G = \mathrm{SL}_2(\mathbb{F})$. Then $|A^{[3]}\nmid_0| \geqslant \frac{1}{4}|A|$.*

Proof. If $\mathrm{char}(\mathbb{F}) = 2$ then $G_s = G\nmid_0$ so we are done by Lemma 2.29. Otherwise $\mathrm{char}(\mathbb{F}) \neq 2$ and therefore $G|_0 \subseteq G_s$. If $0 \notin \mathrm{Tr}(A)$ then we are done. Otherwise fix $g \in A|_0$ and let $\omega \in \overline{\mathbb{F}}$ with $\omega^2 = -1$. Therefore[1] $\Lambda(g) = \mathrm{Spec}_{\overline{\mathbb{F}}}(g) = \{\pm\omega\}$. We have the implications

$$\mathrm{Tr}(g) = 0 \quad \Leftrightarrow \quad g^2 = -I \quad \Leftrightarrow \quad g^{-1} = -g. \tag{14}$$

Write $C = \mathrm{C}_G(g)$ and $N = \mathrm{N}_G(C)$. By the assumption and by Simple fact 2.28, $A \nsubseteq N$. Set $B := A \backslash N \neq \varnothing$ and let $h \in B$. If $\mathrm{Tr}(h) = 0$ then we have

$$\mathrm{Tr}(gh) = 0 \quad \Leftrightarrow \quad ghgh = -I \quad \Leftrightarrow \quad gg^h = I \quad \Leftrightarrow \quad g^h = g^{-1}. \tag{15}$$

[1] We write $\mathrm{Spec}_{\overline{\mathbb{F}}}(g)$ to emphasize that we take all eigenvalues in $\overline{\mathbb{F}}$.

Therefore if $\mathrm{Tr}(h) := \mathrm{Tr}(gh) = 0$ then $h \in N$, a contradiction (since we took $h \notin N$). Thus either $\mathrm{Tr}(h) \neq 0$ or $\mathrm{Tr}(gh) \neq 0$. So

$$|A^{[2]}\nmid_0| \geqslant \frac{1}{2}|B| = \frac{1}{2}(|A| - |A \cap N|). \tag{16}$$

On the other hand if $h \in A \backslash N$ then $h(A \cap N) \subseteq A^{[2]} \backslash N$, and so

$$|A^{[2]} \backslash N| \geqslant |A \cap N|.$$

Therefore by applying (16) with $B' = A^{[2]} \backslash N$ we get

$$|A^{[3]}\nmid_0| \geqslant \frac{1}{2}|B'| \geqslant \frac{1}{2}|A \cap N|. \tag{17}$$

Combining (16) and (17) we get $|A^{[3]}\nmid_0| \geqslant \frac{1}{4}|A|$. □

Lemma 2.31. *Let* $\mathbb{F}$ *be a finite field and* $\mathbb{E}$ *be a proper subfield. Let* A *be a generating set of* $G = \mathrm{SL}_2(\mathbb{F})$. *If* $|A\nmid_{\mathbb{E}}| > 0$ *then* $|A^{[4]}\nmid_{\mathbb{E}}| \geqslant \frac{1}{12}|A|$.

Proof. Write $B = A^{[3]}$. If $|B\nmid_{\mathbb{E}}| \geqslant \frac{1}{12}|A|$ then we are done. Assume that $|B\nmid_{\mathbb{E}}| < \frac{1}{12}|A|$. From Lemma 2.30 we get $|B\nmid_0| \geqslant \frac{1}{4}|A|$. Therefore $|B|_{\mathbb{E}^\times}| > \left(\frac{1}{4} - \frac{1}{12}\right)|A| = \frac{1}{6}|A|$. From Lemma 2.23 if $g \in G\nmid_{\mathbb{E}}$ and $h \in G|_{\mathbb{E}^\times}$ then either $\mathrm{Tr}(gh^{-1}) \notin \mathbb{E}$ or $\mathrm{Tr}(gh) \notin \mathbb{E}$. By the assumption there is some $g \in A\nmid_{\mathbb{E}}$. Therefore $B' := gB \subseteq A^{[4]}$ and so by (13)

$$|A^{[4]}\nmid_{\mathbb{E}}| \geqslant |B'\nmid_{\mathbb{E}}| \geqslant \frac{1}{2}|B|_{\mathbb{E}^\times}| > \frac{1}{12}|A|. \quad \square$$

Corollary 2.32. *Let* $\mathbb{F}$ *be a finite field and* $G = \mathrm{SL}_2(\mathbb{F})$. *Let* $A \subseteq G$ *and suppose that* $\langle A \rangle = G$ *and* $\langle \mathrm{Tr}(A) \rangle = \mathbb{F}$. *Then for any proper subfield* $\mathbb{E}$ *we have*

$$|A^{[4]}\nmid_{\mathbb{E}}| \geqslant \frac{1}{12}|A|.$$

Corollary 2.33. *Let* $\mathbb{F}$ *be a finite field and* $G = \mathrm{SL}_2(\mathbb{F})$. *Let* $A \subseteq G$ *and suppose that* $\langle A \rangle = G$. *Then for any proper subfield* $\mathbb{E}$ *we have*

$$|A^{[9]}\nmid_{\mathbb{E}}| \geqslant \frac{1}{12}|A|.$$

Proof. By Lemma 2.22, $\langle \mathrm{Tr}(A^{[6]}) \rangle = \mathbb{F}$ and therefore $|A^{[6]}\nmid_{\mathbb{E}}| > 0$. Now as in the proof of Lemma 2.31 either $|A^{[3]}\nmid_{\mathbb{E}}| \geqslant \frac{1}{12}|A|$ (and then we are done) or

$|A^{[3]}|_{\mathbb{E}^\times}| > \frac{1}{6}|A|$. Therefore taking $b \in A^{[6]}\not\chi_{\mathbb{E}}$, $B' := A^{[3]}|_{\mathbb{E}^\times}$ and $B'' := bB' \subseteq A^{[9]}$ and using (13) we get

$$|A^{[9]}\not\chi_{\mathbb{E}}| \geqslant |B''\not\chi_{\mathbb{E}}| \geqslant \frac{1}{2}|B'| > \frac{1}{12}|A|. \quad \square$$

2.7 Some useful growth properties.

Definition 2.34. Let G be a group and let $\sim$ be the equivalence relation of conjugacy in G. Given a subset $A \subseteq G$ write $\tilde{A} := A/\sim$. By abuse of notation we view $\tilde{A} \subseteq A$ as a set of representatives: thus for all $a \in A$ there is a unique $b \in \tilde{A}$ such that $a \sim b$.

The following useful lemma of Helfgott connects growth and commutativity.

Lemma 2.35 ([26, Proposition 4.1]). *Let G a finite group and let $\emptyset \neq A \subseteq G$. Then there exists $a \in A$ such that*

$$|\mathrm{C}_{A^{-1}A}(a)| \geqslant \frac{|\tilde{A}|\,|A|}{|A^{-1}AA|}. \tag{18}$$

If $\langle A\rangle = G$ then for any subgroups $H, K < G$ we have $|A^{[4]}\backslash(H \cup K)| > \frac{1}{4}|A|$.

The following corollary is a variant of [26, Corollary 4.3].

Corollary 2.36. *Let $\mathbb{F}$ be a field. Let G be a subgroup of $\mathrm{GL}_n(\mathbb{F})$ and let $A \subseteq G$ be a finite subset. Let $B \subseteq A$ with $|B| \geqslant c|A|$ for some $c \in \mathbb{R}_+$. Then there exists $b \in B$ such that*

$$|\mathrm{C}_{AA^{-1}}(b)| \geqslant c\frac{|\mathrm{Tr}(B)|\,|A|}{|A^{-1}AA|}. \tag{19}$$

Proof. Since conjugate elements have the same trace we get $|\tilde{A}| \geqslant |\mathrm{Tr}(A)|$. Therefore by Lemma 2.35 there exists $a \in A$ such that

$$|\mathrm{C}_{AA^{-1}}(a)| \geqslant \frac{|\mathrm{Tr}(A)|\,|A|}{|A^{-1}AA|}.$$

Hence if $B \subseteq A$ and $|B| \geqslant c|A|$ then there exists $b \in B$ such that[2],

$$|\mathrm{C}_{AA^{-1}}(b)| \geqslant |\mathrm{C}_{BB^{-1}}(b)| \geqslant \frac{|\mathrm{Tr}(B)|\,|B|}{|B^{-1}BB|} \geqslant c\frac{|\mathrm{Tr}(B)|\,|A|}{|A^{-1}AA|}. \quad \square$$

[2] The author thanks H. Helfgott for a helpful discussion concerning this variant.

A variant of the following lemma was proved in [26, Proposition 4.10]. Here, we give another proof.

Lemma 2.37. *Let* $\mathbb{F}$ *be a field and let* $G = \mathrm{SL}_2(\mathbb{F})$*. Let* $g \in G_s$ *be a semi-simple element. Let* $h \in G$ *and suppose that* $\mathrm{Fix}(g) \setminus \mathrm{Fix}(h) \neq \varnothing$*. Define* $F : \mathrm{SL}_2(\mathbb{F}) \to \mathbb{F}^3$ *by*

$$F(b) := (\mathrm{Tr}(b), \mathrm{Tr}(gb), \mathrm{Tr}(hb)).$$

Then $\mathrm{mult}(F) \leqslant 2$*. In particular, for any subset* $B \subseteq G$*,*

$$\frac{1}{2}|B| \leqslant |F(B)| \leqslant |\mathrm{Tr}(B)|\,|\mathrm{Tr}(gB)|\,|\mathrm{Tr}(hB)|. \tag{20}$$

Proof. There exists $w \in \mathrm{SL}_2(\overline{\mathbb{F}})$ such that

$$g = \begin{pmatrix} \alpha & a \\ 0 & \alpha^{-1} \end{pmatrix}^w, \quad h = \begin{pmatrix} \beta & 0 \\ b & \beta^{-1} \end{pmatrix}^w$$

with $b \in \overline{\mathbb{F}}^\times$ and $\alpha \notin \{\pm 1\}$. Let

$$g' = \begin{pmatrix} x & y \\ z & w \end{pmatrix}^w \in \mathrm{SL}_2(\mathbb{F}).$$

We need to show that for any c_1, c_2, c_3 there are at most two elements g' with

$$\det(g') = 1, \quad F(g') = (\mathrm{Tr}(g'), \mathrm{Tr}(gg'), \mathrm{Tr}(hg')) = (c_1, c_2, c_3).$$

By the opening trace equalities we get the equation

$$A\bar{x} = \bar{c}$$

where

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ \alpha & \alpha^{-1} & 0 & a \\ \beta & \beta^{-1} & b & 0 \end{pmatrix}, \quad \bar{x} = \begin{pmatrix} x \\ w \\ y \\ z \end{pmatrix} \quad \text{and} \quad \bar{c} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}.$$

Therefore, from our assumption on b and α, we have $\mathrm{rank}(A) = 3$. So the set of solutions $A^{-1}(\bar{c})$ is either empty or a one-dimensional affine linear subspace (i.e., a dilation of a one-dimensional linear subspace) of $\overline{\mathbb{F}}^4$. Note that for any z there is exactly one triple (x, w, y) such that g' is a solution. On the other hand, $g' \in \mathrm{SL}_2(\mathbb{F})$ so $xw - yz = 1$ and therefore there at most two solutions g' in the affine line $A^{-1}(\bar{c})$ with $\det(g') = 1$. In other words

$$|A^{-1}(\bar{c}) \cap \mathrm{SL}_2(\overline{\mathbb{F}})| \leqslant 2. \quad \square$$

2.8 Avoiding subvarieties.

Definition 2.38. Let $\mathbb{F}$ be a field. Let G be a group and let (V, ρ) be a finite-dimensional representation of G over $\mathbb{F}$. When the action will be clear from the context we will write the *linear action* on V simply by gv instead of $\rho(g)v$. Let $W_1, \ldots, W_m < V$ be proper subspaces of V and let $W = \bigcup_{i=1}^m W_i$. We will assume that the above union is *non-trivial* in the sense that $W_i \nleq W_j$ for $i \neq j$. We will call W a *linear variety* with *decomposition* $W = \bigcup_{i=1}^m W_i$. (If the union is non-trivial then the decomposition is unique.) Write

$$\mathrm{Stab}_G(W) = \{g \in G : gW = W\}.$$

For brevity we sometimes write $G_W = \mathrm{Stab}(W) = \mathrm{Stab}_G(W)$, when the group G is clear from the context. Write

$$\dim(W) := \max_i\{\dim(W_i)\},$$
$$\deg_d(W) := |\{i : \dim(W_i) = d\}| \quad \text{and} \quad \deg(W) := \deg_{\dim(W)}(W).$$

The following 'escaping lemma' of Helfgott will be useful.

Lemma 2.39 ([26, Lemma 4.4]). *For any $n, m \in \mathbb{N}_+$ there exists $k \in \mathbb{N}_+$ such that the following holds. Let G be a group and let (V, ρ) be a finite-dimensional representation of G over a field $\mathbb{F}$. Let $W_1, \ldots, W_m$ be subspaces of V and suppose that $W = \bigcup_i W_i$ is a linear variety with $\dim(W) \leqslant n$. Let A be a generating set of G. Let $0 \neq w \in V$, and write $O := Gw$ and $V_w := \mathbb{F}[G]w = \mathrm{span}(O)$.*

Suppose that $O \nsubseteq W$. Then for any $w' \in V_w \backslash \{0\}$ there exists $g \in A^{[k]}$ such that $gw' \notin W$. In particular for any $w' \in O$ there exists $g \in A^{[k]}$ such that $gw' \notin W$.

Now we will prove the following result (cf. [26, Corollary 4.5]). We give a different proof from Helfgott's original proof.

Corollary 2.40. *There exists $k \in \mathbb{N}_+$ such that the following holds for any finite field $\mathbb{F}$ of size $|\mathbb{F}| > 3$, and for any generating set A of $\mathrm{SL}_2(\mathbb{F})$. For any $u \in \mathrm{GL}_2(\overline{\mathbb{F}})$, there exists $a \in A^{[k]}$ such that a^u has no zero entries.*

Proof. Write $G := \mathrm{SL}_2(\mathbb{F})$ and $V := \mathrm{M}_2(\overline{\mathbb{F}})$ and for $1 \leqslant i, j \leqslant 2$ write

$$W_{ij} := \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in V : a_{ij} = 0 \right\}.$$

Write $W = \bigcup_{i,j} W_{ij}$. Equivalently, if $g = \begin{pmatrix} a_{21} & a_{22} \\ a_{11} & a_{12} \end{pmatrix} \in V$ then

$$a_{ij} = 0 \text{ if and only if } ge_j = \lambda e_i \text{ for some } \lambda \in \overline{\mathbb{F}}.$$

Now we use Lemma 2.39 with the group G^u and the orbit $O = G^u$ of $w' = I$ and the linear variety W. We can use Lemma 2.39 if we show that $G^u \nsubseteq W$. We will show that $|G^u \cap W| < |G|$ so $G^u \nsubseteq W$.

Let $u = (u_1, u_2)$ where u_i are the columns of u. Therefore for any $g \in G^u \cap W$ there exist $i, j \in \{1, 2\}$ such that $g\bar{u}_i = \bar{u}_j$; that is, $gu_i = \lambda u_j$ for some $\lambda \in \bar{\mathbb{F}}^\times$. Write

$$G_{ij} := \{g \in G : g\bar{u}_i = \bar{u}_j\}.$$

So $G^u \cap W = \bigcup_{i,j} G_{ij}$. In order to prove $|G^u \cap W| < |G|$ we will bound $|\bigcup_{i,j} G_{ij}|$ from above.

Choose for any $i \in \{1, 2\}$ some $u_i' \in \mathbb{F}^2 \backslash \{0\}$ with u_i, u_i' linearly independent. Now if $g, g' \in G_{ij}$ then $gu_i = \lambda u_j$ and $g'u_i = \lambda' u_j$ for some $\lambda, \lambda' \in \bar{\mathbb{F}}$. Note that gu_i' and gu_i determine g; therefore if $g, g' \in G_{ij}$ and $gu_i' = g'u_i' \in \mathbb{F}^2 \backslash \{0\}$ then we must have $\lambda = \lambda'$ since $\det(g) = \det(g') = 1$. We conclude that for any i, j we have $|G_{ij}| \leqslant |\mathbb{F}|^2 - 1$. Therefore $|G^u \cap W| = |\bigcup G_{ij}| \leqslant 4(|\mathbb{F}|^2 - 1) - 1$ since $I \in G_{11} \cap G_{22}$. So if $|\mathbb{F}| = q \geqslant 4$ then

$$|G^u| = |\mathrm{SL}_2(\mathbb{F})| = q(q^2 - 1) > 4(q^2 - 1) - 1 \geqslant |\bigcup G_{ij}|$$

and in particular $G^u \nsubseteq W$.

Therefore we can apply Lemma 2.39 to get the desired conclusion. □

2.9 Reduction from matrices to traces. Let us collect the properties that we will exploit (cf. [26, Propositions 4.8, 4.10]).

Theorem 2.41 (Helfgott). *There exist $k \in \mathbb{N}_+$ and $C \in \mathbb{R}_+$ such that the following holds for any finite field $\mathbb{F}$. Let A be a generating set of $\mathrm{SL}_2(\mathbb{F})$. Then*

$$|A^{[k]} \cap G_s| > \frac{1}{C}|A|, \quad |\mathrm{Tr}(A^{[k]})| > \frac{1}{C}|A|^{1/3}, \quad |\mathrm{Tr}(A)| < C\frac{|A^{[k]}|^{4/3}}{|A|}. \tag{21}$$

The following result reduces the growth of $A^{[k]}$ to the growth of $\mathrm{Tr}(A^{[k']})$ and then reduces the growth of traces to the growth of eigenvalues (cf. [26, §4.3]).

Theorem 2.42 (Helfgott). *There exist $k \in \mathbb{N}_+$ and $C \in \mathbb{R}_+$ such that for any $\varepsilon \in \mathbb{R}_+$ that following holds. Let $\mathbb{F}$ be a finite field and A a generating set of $\mathrm{SL}_2(\mathbb{F})$. Write $A_1 = A^{[k]}$ and $A_2 = A^{[k^2]}$. Suppose that $|A_2| < |A|^{1+\varepsilon}$. Then*

$$C^{-1}|A|^{1/3} < |\mathrm{Tr}(A_1)| < C|A|^{1/3+C\varepsilon} \tag{22}$$

and there exists an element $g \in A_1 \cap G_s$ with

$$|V| > C^{-1}|\mathrm{Tr}(A_1)|^{1-C\varepsilon} \quad \textit{where } V := \mathrm{C}_{A_2}(g). \tag{23}$$

Moreover, if

$$|A_2| < |A|^{1+\varepsilon} \quad \textit{and} \quad |\mathrm{Tr}(A_2)| < |\mathrm{Tr}(A_1)|^{1+\varepsilon} \tag{24}$$

then there exists an element $g \in A_1 \cap G_s$ *such that* (23) *holds and also*

$$|\mathrm{Tr}(V^2) \cdot \mathrm{Tr}(V^2)| + |\mathrm{Tr}(V^2) + \mathrm{Tr}(V^2)| < C|\mathrm{Tr}(V^2)|^{1+C\varepsilon}.$$

3 Main results

Proposition 3.1. *There exists* $C \in \mathbb{R}_+$ *such that the following holds. Let* $\mathbb{F}$ *be a finite field and* $G = \mathrm{SL}_2(\mathbb{F})$ *and let* $\varepsilon \in \mathbb{R}_+$ *with* $\varepsilon < C^{-1}$. *Let* $V \subseteq \mathrm{SL}_2(\mathbb{F})$ *be a set of diagonal matrices of size* $|V| > C$. *Suppose that*

$$\mathrm{Tr}(V) \textit{ is impure } \varepsilon\textit{-field} \tag{25}$$

and

$$|\mathrm{Tr}(V^{[2]})| < |\mathrm{Tr}(V)|^{1+\varepsilon}. \tag{26}$$

Then

$$\mathrm{Tr}(V^{[2]}) \textit{ is not } \varepsilon\textit{-field}. \tag{27}$$

Proof. Set $N := |\mathrm{Tr}(V)|$. By the assumption (25) there is some subfield $\mathbb{E} < \mathbb{F}$ and some $x \in \mathbb{F}^\times$ such that

$$|\mathrm{Tr}(V) \backslash x\mathbb{E}| < N^\varepsilon \quad \text{and} \quad |\mathbb{E}| < N^{1+\varepsilon}.$$

By the assumption (25), $\mathrm{Tr}(V)$ is impure subfield so $|\mathrm{Tr}(V) \backslash \mathbb{E}| > 0$.

Case 1. Suppose that

$$x \in \mathbb{E} \quad \text{and} \quad 0 < |\mathrm{Tr}(V) \backslash \mathbb{E}| < N^\varepsilon.$$

Choose $g \in V$ with $\mathrm{Tr}(g) \notin \mathbb{E}$. Since $g(V|_{\mathbb{E}^\times}) \subseteq V^{[2]}$ Lemma 2.23 gives

$$\begin{aligned} |V^{[2]} \not|_{\mathbb{E}}| &\geqslant |(g(V|_{\mathbb{E}^\times})) \not|_{\mathbb{E}}| \geqslant \frac{1}{2}|V|_{\mathbb{E}^\times}| \geqslant \frac{1}{2}(|V|_{\mathbb{E}}| - 2) \gg |V|_{\mathbb{E}}| \\ &\geqslant N - N^\varepsilon \gg N. \end{aligned} \tag{28}$$

By the assumption (26) we have $|\mathrm{Tr}(V^{[2]})| \leqslant N^{1+\varepsilon}$, so

$$\mathrm{Tr}(V^{[2]}) \text{ cannot be } \varepsilon\text{-field}. \tag{29}$$

Indeed, the bound (28) excludes the possibility that $\mathrm{Tr}(V^{[2]})$ is ε-almost $\mathbb{E}'$ where $\mathbb{E}'$ is either the subfield $\mathbb{E}$ or any other coset $x\mathbb{E}$ of $\mathbb{E}$. Now for any other field $\mathbb{E}' \neq \mathbb{E}$ if $|\mathbb{E}'| \leqslant |\mathrm{Tr}(V^{[2]})|^{1+\varepsilon}$ then

$$|\mathbb{E}'| \leqslant N^{1+O(\varepsilon)}$$

since $|\mathrm{Tr}(V^{[2]})| \leqslant N^{1+\varepsilon}$ by (26). Therefore the intersection of the field $\mathbb{E}$ with any coset $x'\mathbb{E}'$ satisfies

$$|\mathbb{E} \cap x'\mathbb{E}'| \leqslant |\mathbb{E} \cap \mathbb{E}'| \leqslant N^{O(\varepsilon)}.$$

So the intersection is too small to contain $\mathrm{Tr}(V|_{\mathbb{E}})$, since

$$|\mathrm{Tr}(V|_{\mathbb{E}})| \geqslant \frac{1}{2}|V|_{\mathbb{E}}| \geqslant N - N^{\varepsilon} \gg N.$$

Therefore (29) follows.

Case 2. Suppose that

$$\mathrm{Tr}(V) \subseteq x\mathbb{E} \quad \text{with } |\mathbb{E}| \leqslant N^{1+\varepsilon} \text{ and } x \notin \mathbb{E}.$$

This case is treated similarly to Case 1. By multiplying by some $g \in V|_{x\mathbb{E}}$ we get by Lemma 2.23 that at least $\frac{1}{2}|V|_{x(\mathbb{E}^{\times})}|$ elements in $V^{[2]}$ have trace not in $x\mathbb{E}$. Therefore, as was proved in (29) in Case 1, we find that $\mathrm{Tr}(V^{[2]})$ cannot be ε-field.

In both cases we get that $\mathrm{Tr}(V^{[2]})$ cannot be ε-field so we are done. □

Proposition 3.2. *There exist $C \in \mathbb{R}_+$ and $k \in \mathbb{N}_+$ with $k > C$ such that the following holds. Let $\mathbb{F}$ be a finite field, $G = \mathrm{SL}_2(\mathbb{F})$ and let $\varepsilon \in \mathbb{R}_+$ with $\varepsilon < C^{-1}$. Let $\mathbb{E}$ be a proper subfield and $A \subseteq \mathrm{SL}_2(\mathbb{F})$ with $\langle A \rangle = G$. For $i \in \{1, 2\}$ write $A_i = A^{[k^i]}$. Suppose that*

$$|A_3| < |A|^{1+\varepsilon}. \tag{30}$$

Then there exist an element $g \in A_1 \cap G_s$ and $V \subseteq \mathrm{C}_{A_2}(g)$ such that $\mathrm{Tr}(V) \subseteq \mathbb{F}\backslash\mathbb{E}$ *and* $|\mathrm{Tr}(V)| > C^{-1}|\mathrm{Tr}(A_2)|^{1-C\varepsilon}$.

Proof. To simplify the notation, we write $A_i := A^{[k^i]}$ and during the proof we will increase the value of k. By Lemma 2.33 there exists $k_1 \in \mathbb{N}_+$ such that for $k \geqslant k_1$ and $B := A_1{\nmid}_{\mathbb{E}}$ we have

$$|B| = |A_1{\nmid}_{\mathbb{E}}| \gg |A|. \tag{31}$$

Now let $g \in A_1 \cap G_s$ satisfy $\mathrm{Fix}(g) = \{x_1, x_2\} \subseteq \mathbb{P}(\overline{\mathbb{F}})$. Suppose that for any $h \in A$ we have $\mathrm{Fix}(h) \subseteq \mathrm{Fix}(g)$. Since $\langle A \rangle = G$ we have $\mathrm{Fix}(A) = \varnothing$, so we can find

$h_1, h_2 \in A$ such that $\mathrm{Fix}(h_i) = \{x_i\}$ and hence $\mathrm{Fix}(h_1h_2) \cap \mathrm{Fix}(g) = \varnothing$. Thus in any case there exists $h \in A^{[2]}$ such that $\mathrm{Fix}(h)\backslash\mathrm{Fix}(g) \neq \varnothing$.

Therefore by Lemma 2.37, if $k \geqslant \max\{k_1, 2\}$ then

$$|B| \ll |\mathrm{Tr}(B)|\,|\mathrm{Tr}(gB)|\,|\mathrm{Tr}(hB)| \leqslant |\mathrm{Tr}(B)|\,|\mathrm{Tr}(A_2)|^2. \tag{32}$$

Now by (20) and Theorem 2.41, there exists $k_2 \in \mathbb{N}_+$ such that if $k \geqslant \max\{2, k_1, k_2\}$ then

$$|\mathrm{Tr}(A_2)| \ll \frac{|A_2^{[k_2]}|^{4/3}}{|A_2|} \leqslant \frac{|A_3|^{4/3}}{|A|} \ll |A|^{1/3+O(\varepsilon)}. \tag{33}$$

We conclude from the above three inequalities that

$$|\mathrm{Tr}(A_2)|^{3-O(\varepsilon)} \ll |A| \ll |B| \leqslant |\mathrm{Tr}(B)|\,|\mathrm{Tr}(A_2)|^2 \leqslant |\mathrm{Tr}(A_2)|^3.$$

Therefore we get

$$|\mathrm{Tr}(B)| \gg |\mathrm{Tr}(A_2)|^{1-O(\varepsilon)}, \tag{34}$$

$$|\mathrm{Tr}(A_2)| \gg |A|^{1/3}. \tag{35}$$

Now suppose that $k \geqslant \max\{3, k_1, k_2\}$. Therefore by Corollary 2.36 and (30), (34), (35) there exists $b \in B$ such that

$$\begin{aligned}|\mathrm{C}_{B^{-1}B}(b)| &\gg \frac{|\mathrm{Tr}(B)|\,|A_1|}{|A_1^{-1}A_1A_1|} \geqslant \frac{|\mathrm{Tr}(B)|\,|A|}{|A_3|} \geqslant |\mathrm{Tr}(B)|\,|A|^{-\varepsilon}\\ &\gg |\mathrm{Tr}(B)|\,|\mathrm{Tr}(A_2)|^{-O(\varepsilon)} \gg |\mathrm{Tr}(A_2)|^{1-O(\varepsilon)}.\end{aligned} \tag{36}$$

Let b be as in (36) and set[3]

$$C := \mathrm{C}_{B^{-1}B}(b), \quad C' := C\nmid_0, \quad C'' := C' \cup bC' \quad \text{and} \quad V := C''\nmid_{\mathbb{E}}.$$

Note that $\mathrm{Tr}(b) \notin \mathbb{E}$, so b is semi-simple and the elements of $\mathrm{C}_G(b)$ are simultaneously diagonalizable; therefore $|C'| \geqslant |C| - 2$ and $|\mathrm{Tr}(V)| \geqslant \frac{1}{2}|V|$. Now by Lemma 2.23, we get that for any $c \in C'$ either $\mathrm{Tr}(c) \notin \mathbb{E}$ or $\mathrm{Tr}(bc) \notin \mathbb{E}$ or $\mathrm{Tr}(bc^{-1}) \notin \mathbb{E}$. Altogether we get that $V \subseteq \mathrm{C}_{A_2}(b)$, since $V \subseteq A_1^{[3]} \subseteq A_2$, and by (13) and (36) we get

$$|\mathrm{Tr}(V)| \gg |V| \geqslant \frac{1}{2}|C'| \geqslant \frac{1}{2}(|C| - 2) \gg |C| \gg |\mathrm{Tr}(A_2)|^{1-O(\varepsilon)}. \quad \square$$

[3] The author thanks H. Helfgott for very fruitful discussions related this argument.

Proof of Theorem 1.1. By Theorem 2.15 there exist $C_0, \delta_0 \in \mathbb{R}_+$ such that if $|A| \geqslant C_0 |G|^{1-\delta_0} > C_0 q^{2(2/3)}$ then $A^{(3)} = G$. Therefore if $|A| \geqslant C_0 |G|^{1-\delta_0}$ the conclusion follows. So we can assume from now that $|A| \ll |G|^{1-\delta_0}$. Let $3 \leqslant k \in \mathbb{N}$, $0 < \varepsilon_0 \in \mathbb{R}$ and $c_0 \in \mathbb{R}$ with $0 < c_0 \leqslant 1$. By Lemma 2.7 the following holds with $\varepsilon' = \varepsilon_0/3k$ and $c' = c_0/2$: for any group G and any finite subset A,

$$|A^{[k]}| > c_0 |A|^{1+\varepsilon_0} \quad \Rightarrow \quad |A^{(3)}| > c' |A|^{1+\varepsilon'}.$$

Now if $|A|^{\varepsilon'/2} < c'^{-1}$ then A is bounded; but if A is a generating set we get

$$|A^{(3)}| \geqslant |A| + 2 \geqslant |A|^{1+\varepsilon''}$$

for some $\varepsilon'' \in \mathbb{R}_+$. Therefore for any $\varepsilon < \min\{\varepsilon'/2, \varepsilon''\}$ we get

$$|A^{[k]}| > c_0 |A|^{1+\varepsilon_0} \quad \Rightarrow \quad |A^{(3)}| > |A|^{1+\varepsilon}.$$

In order to prove (1) it is now enough to prove that $|A^{[k]}| > c_0 |A|^{1+\varepsilon_0}$ for some absolute constants $3 \leqslant k \in \mathbb{N}_+$ and $c_0, \varepsilon_0 \in \mathbb{R}_+$. We will write $A_i := A^{[k^i]}$ and we will prove that there exist $C \in \mathbb{R}_+$ and $i \in \mathbb{N}_+$ such that the following holds. There exist $k \in \mathbb{N}$ and $\varepsilon \in \mathbb{R}_+$ with $k > C$ and $\varepsilon < C^{-1}$ such that if $|A| \leqslant C|G|^{1-\delta_0}$ then $|A_i| = |A^{[k^i]}| > \frac{1}{C} |A|^{1+\varepsilon^i}$.

By Lemma 2.22 there exists $k_0 \in \mathbb{N}_+$ such that if $k > k_0$ then $\mathrm{Tr}(A_1)$ is not contained in any proper subfield i.e., $\langle \mathrm{Tr}(A_1) \rangle = \mathbb{F}_q$. Set $\varepsilon_1 := \frac{1}{2}$. Note that if $0 < f < \varepsilon_1$, then

$$1 - f < \frac{1}{1+f} < 1 - \frac{1}{2} f < 1 - \Omega(f)$$

and similarly

$$1 + f < \frac{1}{1-f} < 1 + 2f < 1 + O(f).$$

By Theorem 2.42 there exists $k_1 \in \mathbb{N}_+$ (and an implicit constant $C_1 > 0$) such that for any $\varepsilon \in \mathbb{R}_+$ and $k > \max\{k_0, k_1\}$ we have either $|A_2| \geqslant |A|^{1+\varepsilon}$ (so we are done) or

$$|A|^{1/3} \ll |\mathrm{Tr}(A_1)| \ll |A|^{1/3+O(\varepsilon)}. \tag{37}$$

Explicitly,

$$\frac{1}{C_1} |A|^{1/3} < |\mathrm{Tr}(A_1)| < C_1 |A|^{1/3+C_1\varepsilon}.$$

Applying again Theorem 2.42, now for A_1, for any $k > \max\{k_0, k_1\}$ we have either $|A_3| \geqslant |A_1|^{1+\varepsilon^2}$ (so we are done) or

$$|A_1|^{1/3} \ll |\mathrm{Tr}(A_2)| \ll |A_1|^{1/3+O(\varepsilon^2)}. \tag{38}$$

Now if $|A_3| < |A|^{1+\varepsilon^2}$ and in addition $|\mathrm{Tr}(A_1)|^{1+\varepsilon} \leqslant |\mathrm{Tr}(A_2)|$ then both (37) and (38) hold and we get $|A| \ll |\mathrm{Tr}(A_1)|^3 < |\mathrm{Tr}(A_2)|^{3(1-(1/2)\varepsilon)} \ll |A_1|^{1-\Omega(\varepsilon)}$. In other words $|A|^{1+\Omega(\varepsilon)} \ll |A_1|$ and our conclusion holds.

We summarize what have proved so far: there exists $C \in \mathbb{R}_+$ such that whenever $0 < \varepsilon < C^{-1}$ and $k > C$ we have

$$|\mathrm{Tr}(A_2)| \geqslant |\mathrm{Tr}(A_1)|^{1+\varepsilon} \quad \Rightarrow \quad |A_3| \geqslant \frac{1}{C}|A|^{1+\varepsilon^2}. \tag{39}$$

Therefore in order to complete the proof we can assume from now that

$$|A_3| < |A|^{1+\varepsilon^2} \quad \text{and} \quad |\mathrm{Tr}(A_2)| < |\mathrm{Tr}(A_1)|^{1+\varepsilon^2}. \tag{40}$$

So we can apply Theorem 2.42. Thus there exists an element $g \in A_1 \cap G_s$ such that $V := \mathrm{C}_{A_2}(g)$ satisfies $|V| > C_1^{-1}|\mathrm{Tr}(A_1)|^{1-C_1\varepsilon^2}$ and

$$|\mathrm{Tr}(V^2)\cdot\mathrm{Tr}(V^2)| + |\mathrm{Tr}(V^2) + \mathrm{Tr}(V^2)| < C_1|\mathrm{Tr}(V^2)|^{1+C_1\varepsilon^2} \tag{41}$$

Hence using (40), (42) and (38) we get

$$|\mathrm{Tr}(V)| \geqslant \frac{1}{2}|V| \gg |\mathrm{Tr}(A_1)|^{1-O(\varepsilon^2)} \gg |\mathrm{Tr}(A_2)|^{1-O(\varepsilon^2)}, \tag{42}$$

$$|\mathrm{Tr}(V^2)| \geqslant \frac{1}{4}|V| \gg |\mathrm{Tr}(A_2)|^{1-O(\varepsilon^2)} \gg |A_1|^{1/3-O(\varepsilon^2)} \geqslant k^{1/3-O(\varepsilon^2)}. \tag{43}$$

Set $V_1 := V$, $U_1 := \mathrm{Tr}(V_1^2)$ and $K_1 := C_1|U_1|^{C_1\varepsilon}$. By (43), (41), for some absolute constant $C_3 \in \mathbb{R}_+$, $|U_1| \geqslant \frac{1}{C_3}k^{1/3-C_3\varepsilon}$ and $|U_1 \cdot U_1| + |U_1 + U_1| \ln K_1|U_1|$. Hence, by Theorem 2.8, for some absolute constant $C \in \mathbb{R}_+$, either $|U_1| < CK_1^C$ or for some subfield $\mathbb{E}_1 \leqslant \mathbb{F}$ and $x_1 \in \mathbb{F}^\times$ we have

$$|U_1 \backslash x_1\mathbb{E}_1| \leqslant CK_1^C \quad \text{and} \quad |\mathbb{E}| \leqslant CK_1^C|U_1| \tag{44}$$

Now set $C_4 := 2CC_1$ and $\varepsilon_3 = (3CC_1C_3)^{-1}$. Since $CK_1^C = CC_1|U_1|^{CC_1\varepsilon}$, for any $\varepsilon < \min\{\varepsilon_i\}$, there exists $k > \max\{k_i\}$, such that $CK_1^C < |U_1|^{C_4\varepsilon} < |U_1|$. Therefore the alternative (44) must hold and we get $|U_1\backslash x_1\mathbb{E}_1| \leqslant |U_1|^{C_4\varepsilon}$ and $|\mathbb{E}| \leqslant |U_1|^{1+C_4\varepsilon}$. In particular using (38) we have

$$|A_2| \gg \mathrm{Tr}(A_2)^{3-O(\varepsilon^2)} \gg |U_1|^{3-O(\varepsilon^2)} \geqslant |\mathbb{E}|^{3-O(\varepsilon)}.$$

Therefore for any $\delta_0 \in \mathbb{R}_+$ we can find $C_5 \in \mathbb{R}_+$ large enough (such that $C_5 > \max_i\{k_i\}$ and $C_5^{-1} < \min_i\{\varepsilon_i\}$) and we can find $\varepsilon < C_5^{-1}$ and $k > C_5$ such that $|A_2| > |\mathbb{E}|^{3-\delta_0}$. If $\mathbb{E} = \mathbb{F}$ then we are done by Theorem 2.15 which guarantees bounded generation for large subsets of $\mathrm{SL}_2(\mathbb{F})$.

Therefore in order to complete the proof of (1) we are left to treat the case that for some *proper* subfield $\mathbb{E} < \mathbb{F}$

$$\operatorname{Tr}(V^2) \text{ is } C_4\varepsilon\text{-field.} \tag{45}$$

Suppose first that

$$\operatorname{Tr}(V^2) \text{ is impure } O(\varepsilon)\text{-field.} \tag{46}$$

By Proposition 3.1 we get that $\operatorname{Tr}(V^{2[2]})$ is not $C_4\varepsilon$-field. Write

$$V_2 := V_1^{[2]}, \quad U_2 := \operatorname{Tr}(V_2^2), \quad K_2 := |U_2|^{C_4\varepsilon} \quad \text{and} \quad K_2' := (K_2/C)^{1/C} \gg |U_2|^{2C_1\varepsilon}.$$

Note that $V_2^2 = V^{[2]2} = V^{2[2]}$ since $\langle V \rangle$ is abelian. Therefore by Theorem 2.8 we get

$$|\operatorname{Tr}(V_2^2) \cdot \operatorname{Tr}(V_2^2)| + |\operatorname{Tr}(V_2^2) + \operatorname{Tr}(V_2^2)| \gg |\operatorname{Tr}(V_2^2)|^{1+2C_1\varepsilon}. \tag{47}$$

Now by Corollary 2.40 there exists $k_5 \in \mathbb{N}_+$ such that the following holds for any $k > k_5$. For any $w \in \mathrm{GL}_2(\overline{\mathbb{F}})$ there exists $g \in A_1$ such that g^w has no zero entries. In particular we can apply this for the basis $v \in \mathrm{GL}_2(\overline{\mathbb{F}})$ for which the set V^v is simultaneously diagonalizable.

Therefore by (47) we can apply Theorem 2.13, and using (43) we get that for some absolute $C_6 = k_6 \in \mathbb{N}_+$ and for $k > \max\{k_i\}$ we have

$$|\operatorname{Tr}(A_3)| \gg |\operatorname{Tr}(V_2^{[4]} V_2^{g[4]})| \gg |\operatorname{Tr}(V_2)|^{1+\Omega(\varepsilon)} \gg |\operatorname{Tr}(A_1)|^{1+\Omega(\varepsilon)}. \tag{48}$$

On the other hand, by what we have proved in (39), we get

$$|\operatorname{Tr}(A_3)| \gg |\operatorname{Tr}(A_1)|^{1+\Omega(\varepsilon)} \quad \Rightarrow \quad |A_4| \gg |A|^{1+\Omega(\varepsilon^2)}. \tag{49}$$

Therefore if (46) holds then by (48) the conclusion of the theorem holds.

We are left to treat the second subcase of (45):

$$\operatorname{Tr}(V^2) \text{ is a pure } O(\varepsilon)\text{-field} \tag{50}$$

for some proper subfield $\mathbb{E}$. Note that if $\operatorname{Tr}(V^{[4]}) \nsubseteq \mathbb{E}$ then the conclusion of the theorem holds by a similar argument to (46), which treated the case of impure $O(\varepsilon)$-field. Therefore using (43) we can assume in addition to (50) that

$$\operatorname{Tr}(V) \subseteq \operatorname{Tr}(V^{[4]}) \subseteq \mathbb{E}, \quad |\mathbb{E}| \ll |\operatorname{Tr}(V)|^{1+O(\varepsilon)} \ll |\operatorname{Tr}(A_1)|^{1+O(\varepsilon)}. \tag{51}$$

If we can find $g \in A_1$ such that $\operatorname{Prod}(g^v) \notin \mathbb{E}$ (v was a basis such that the set V^v is diagonal) then by Lemma 2.14 we get $|\operatorname{Tr}(V)|^{2-O(\varepsilon)} \ll |\operatorname{Tr}(VV^g)| \ll |\operatorname{Tr}(A_3)|$ and therefore $|\operatorname{Tr}(V)| \ll |\operatorname{Tr}(A_3)|^{1/2+O(\varepsilon)}$. On the other hand $|\operatorname{Tr}(A_1)| \ll |\operatorname{Tr}(A_3)|^{1-O(\varepsilon)}$ since $|\operatorname{Tr}(V)| \gg |\operatorname{Tr}(A_1)|^{1-O(\varepsilon)}$ by (43). Therefore by (49) we are done with (50).

We are now left to treat the case that (50) and (51) hold and $\mathrm{Prod}(g^v) \in \mathbb{E}$ for any $g \in A_1$. Therefore $\mathrm{Tr}(VV^g) \subseteq \mathbb{E}$ for any $g \in A_1$ by (7). In particular by Definition 2.2, we get $\mathrm{Tr}([V, A_1]_{\mathrm{set}}) \subseteq \mathrm{Tr}(VV^{A_1}) \subseteq \mathbb{E}$. Therefore in order to complete (1) we can assume that

$$\mathrm{Tr}(VV^{A_1}) \subseteq \mathbb{E}, \quad |\mathbb{E}| \ll |\mathrm{Tr}(V)|^{1+O(\varepsilon)} \quad \text{and} \quad |\mathrm{Tr}(V)| \overset{(42)}{\gg} |\mathrm{Tr}(A_2)|^{1-O(\varepsilon)}. \tag{52}$$

Now by Proposition 3.2 there exists $C_7 \in \mathbb{R}_+$ such that the following holds with $k_7 = C_7$ and $\varepsilon_7 = C_7^{-1}$. Assume $k > \max\{k_i\}$ and $\varepsilon < \min\{\varepsilon_i\}$. Since $|A_3| \ln |A|^{1+\varepsilon}$ by (40), Proposition 3.2 yields an element $h \in A_1 \cap G_s$ and $U \subseteq \mathrm{C}_{A_2}(h)$ with $|\mathrm{Tr}(U)| \gg |\mathrm{Tr}(A_2)|^{1-O(\varepsilon)}$ and $\mathrm{Tr}(U) \subseteq \mathbb{F} \backslash \mathbb{E}$. Therefore there exists $u \in \mathrm{SL}_2(\mathbb{F}_{q^2})$ such that U^u is diagonal and

$$\mathrm{Tr}(U) \cap \mathbb{E} = \varnothing. \tag{53}$$

Repeating all steps before (52), but now with $\mathrm{Tr}(U)$ instead of $\mathrm{Tr}(V)$, we get that the only case that we need to treat, to complete the theorem, is that $\mathrm{Tr}(U)$ is $O(\varepsilon)$-field, for some proper field $\mathbb{E}' < \mathbb{F}$, and

$$\mathrm{Tr}(UU^{A_1}) \subseteq \mathbb{E}', \quad |\mathbb{E}'| \ll |\mathrm{Tr}(U)|^{1+O(\varepsilon)} \quad \text{and} \quad |\mathrm{Tr}(U)| \gg |\mathrm{Tr}(A_2)|^{1-O(\varepsilon)}. \tag{54}$$

Let us check what we have achieved so far. Write $N := |\mathrm{Tr}(A_2)|$ and $\mathbb{E}'' := \mathbb{E} \cap \mathbb{E}'$. By the construction of U in (53) we get that $\mathbb{E} \neq \mathbb{E}'$ and therefore

$$|\mathbb{E}''| \ll N^{O(\varepsilon)}, \tag{55}$$

since $|\mathbb{E}|, |\mathbb{E}'| \ll N^{1+O(\varepsilon)}$ and $N^{1-O(\varepsilon)} \ll |\mathbb{E}|, |\mathbb{E}'|$. Now by (52) and (54) we get

$$\mathrm{Tr}([U, V]_{\mathrm{set}}) \subseteq \mathbb{E}''. \tag{56}$$

On the one hand, if V and U have no common fixed point then by Lemma 2.14 we get $|\mathrm{Tr}([U, V]_{\mathrm{set}})| \gg |\mathrm{Tr}(V)| \gg N^{1-O(\varepsilon)}$. Therefore by (56) and (55) we get a contradiction for ε small enough.

On the other hand, if V and U do have a common fixed point, then denote their eigenvalues by X and Y respectively. Therefore $\mathrm{tr}(X^{[4]}) \subseteq \mathbb{E}$, $\mathrm{tr}(Y^{[4]}) \subseteq \mathbb{E}'$ and $X \subseteq \mathbb{K}$, $Y \subseteq \mathbb{K}'$ where $\mathbb{K}$ and $\mathbb{K}'$ are the two quadratic extensions of $\mathbb{E}$ and $\mathbb{E}'$ respectively. Write $\mathbb{K}'' := \mathbb{K} \cap \mathbb{K}'$. So we get $|\mathbb{K}''| = |\mathbb{E}''|^2 \ll N^{O(\varepsilon)}$. Hence

$$\begin{aligned} |\mathrm{Tr}(A_3)| &\geqslant |\mathrm{Tr}(UV)| = |\mathrm{tr}(XY)| \geqslant \frac{1}{2}|XY| \geqslant \frac{1}{2}\frac{|X|\,|Y|}{|\mathbb{K}''|} \\ &\gg N^{2-O(\varepsilon)} \gg |\mathrm{Tr}(A_2)|^{2-O(\varepsilon)}. \end{aligned}$$

Therefore by (49) we are done with (50), and the proof is complete. □

Acknowledgement. While writing the main results in this paper, the author was supported by a Fulbright Visiting Scholar grant, and was a visiting student at the Institute for Advance Study at Princeton. He would like to thank the Institute and Fulbright for their support. The author was also partially supported by the Swiss National Science Foundation Grant PP0022 118946.

This work is part of the author's Ph.D. thesis [16] written under the guidance of Alex Lubotzky, whom he thanks for his guidance and assistance in writing this work. The author wishes to thank also Michael Larsen who introduced him to the striking application of the invariant theory of §2.4 to his work. He is grateful to Harald Helfgott for his guidance and for many illuminating discussions.

References

[1] M. Abért and L. Babai. Finite groups of uniform logarithmic diameter. *Israel J. Math.* **158** (2007), 193–203.

[2] L. Babai, G. Hetyei, W. M. Kantor, A. Lubotzky and A. Seress. On the diameter of finite groups. In 31*st annual symposium on foundations of computer science* **II** (1990), 857–865.

[3] L. Babai, W. M. Kantor, and A. Lubotzky. Small diameter Cayley graphs for finite simple groups. *European J. Comb.* **10** (1989), 507–522.

[4] L. Babai, N. Nikolov and L. Pyber. Product growth and mixing in finite groups. In *Proc. 19th annual ACM-SIAM symposium on discrete algorithms* (SIAM, 2008), pp. 248–257.

[5] L. Babai, N. Nikolov and L. Pyber. Expansion and product decomposition of finite groups: variation on a theme of Gowers. Preprint.

[6] L. Babai and A. Seress. On the diameter of Cayley graphs of the symmetric group. *J. Combin. Theory Ser. A* **49** (1988), 175–179.

[7] L. Babai and A. Seress. On the diameter of permutation groups. *European J. Combin.* **13** (1992), 231–243.

[8] J. Bourgain and A. Gamburd. New results on expanders. *C. R. Math. Acad. Sci. Paris* **342** (2006), 717–721.

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

[10] J. Bourgain and A. Gamburd. On the spectral gap for finitely-generated subgroups of $\mathrm{SU}(2)$. *Invent. Math.* **171** (2008), 83–121.

[11] J. Bourgain, N. Katz and T. Tao. A sum-product estimate in finite fields and applications. *Geom. Funct. Anal.* **14** (2004), 27–57.

[12] J. Bourgain, A. Glibichuk and S. Konyagin. Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order. *J. London Math. Soc.* (2) **73** (2006), 380–398.

[13] T. C. Brown and J. P. Buhler. A density version of a geometric Ramsey theorem. *J. Combin. Theory Ser. A* **32** (1982), 20–34.

[14] C. de Concini and C. Procesi. A characteristic free approach to invariant theory. *Adv. in Math.* **21** (1976), 330–354.

[15] O. Dinai. Poly-log diameter bounds for some families of finite groups. *Proc. Amer. Math. Soc.* **134** (2006), 3137–3142.

[16] O. Dinai. Expansion properties of finite simple groups. Ph.D. thesis. The Hebrew University (2009). http://arxiv.org/abs/1001.5069.

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

[18] S. Donkin. Invariants of several matrices. *Invent. Math.* **110** (1992), 389–401.

[19] M. Domokos, S. G. Kuzmin and A. N. Zubkov. Rings of matrix invariants in positive characteristic. *J. Pure Appl. Algebra* **176** (2002), 61–80.

[20] J. R. Driscoll and M. L. Furst. Computing short generator sequences. *Inform. and Comput*. **72** (1987), 117–132.

[21] S. Even and O. Goldreich. The minimum length generator sequence is *NP*-hard. *J. Algorithms* **2** (1981), 311–313.

[22] P. Erdős and A. Renyi. Probabilistic methods in group theory. 3. *J. Anal. Math.* **14** (1965), 127–138.

[23] P. Erdős and P. Turan. On some problems of a statistical group theory. I. *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **4** (1965), 175–186.

[24] P. Erdős and P. Turan. On some problems of a statistical group theory. II. *Acta Math. Acad. Sci. Hung.* **18** (1967), 151–163.

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

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

[27] M. Jerrum. The complexity of finding minimum length generator sequences. *Theoret. Comput. Sci.* **36** (1985), 265–289.

[28] M. Larsen. Navigating the Cayley graph of $\mathrm{SL}_2(\mathbb{F}_p)$. *Internat. Math. Res. Notices* **27** (2003), 1465–1471.

[29] M. W. Liebeck and A. Shalev. Diameters of finite simple groups: sharp bounds and applications. *Ann. of Math.* (2) **154** (2001), 383–406.

[30] P. McKenzie. Permutations of bounded degree generate groups of polynomial diameter. *Info. Proc. Lett.* **19** (1984), 253–254.

[31] N. Nikolov and L. Pyber. Product decompositions of quasirandom groups and a Jordan type theorem. Preprint (2007). http://arxiv.org/abs/math/0703343.

[32] F. P. Preparata and J. Vuillemin. The cube connected cycles: a versatile network for parallel computation. *Comm. ACM* **24** (1981), 300–309.

[33] C. Procesi. Invariant theory of $n \times n$ matrices. *Adv. in Math.* **19** (1976), 306–381.

[34] C. Procesi. Computing with 2×2 matrices. *J. Algebra* **87** (1984), 342–359.

[35] J. Whiston and J. Saxl. On the maximal size of independent generating sets of $\mathrm{PSL}_2(q)$. *J. Algebra* **258** (2002), 651–657.

[36] H. S. Stone. Parallel processing with the perfect shuffle. *IEEE Trans. Comput.* **100** (1971), 153–161.

[37] T. Tao. The sum-product phenomenon in arbitrary rings. *Contrib. Discrete Math.* **4** (2009), 59–82.

[38] T. Tao and V. Vu. *Additive combinatorics* (Cambridge University Press, 2006).

Received 7 February, 2010; revised 8 May, 2010

Oren Dinai, Department of Mathematics, Pool Gruppe 1, ETH Zürich, Rämistr. 101, 8092 Zürich, Switzerland
E-mail: oren.dinai@math.ethz.ch