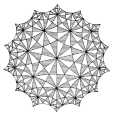
Rev. Mat. Iberoam. 38 (2022), no. 6, 1945–1973
DOI 10.4171/RMI/1344



Growth in Chevalley groups relatively to parabolic subgroups and some applications

Ilya D. Shkredov

Abstract. Given a Chevalley group $\mathbf{G}(q)$ and a parabolic subgroup $P \subset \mathbf{G}(q)$, we prove that for any set A there is a certain growth of A relatively to P, namely, either AP or PA is much larger than A. Also, we study a question about the intersection of A^n with parabolic subgroups P for large n. We apply our method to obtain some results on a modular form of Zaremba's conjecture from the theory of continued fractions, and make the first step towards Hensley's conjecture about some Cantor sets with Hausdorff dimension greater than $1/2$.

1. Introduction

In this paper we study some aspects of growth in Chevalley (i.e., untwisted, generated by its root subgroups and having trivial center) groups. Developing the ideas from [22], it was proved in [10,42] that any finite simple group of Lie type has growth in the following sense.

Theorem 1.1. *Let* $\mathbf{G}$ *be a finite simple group of Lie type with rank* r*, and let* A *be a generating subset of* $\mathbf{G}$*. Then either* $A^3 = \mathbf{G}$ *or*

$$|A^3| > |A|^{1+c},$$

where $c > 0$ *depends only on* r*.*

In particular, there is $n \ll (\log|\mathbf{G}|/\log|A|)^{C(r)}$ *such that* $A^n = \mathbf{G}$*.*

The theorem above gives an affirmative answer to the well-known Babai conjecture [4] for finite simple groups $\mathbf{G}$ of bounded rank. Modern questions on growth in groups are discussed in the excellent survey [23]. In our paper we consider two variants of Babai's problem for Chevalley groups $\mathbf{G}(q)$ defined over the field $\mathbb{F}_q$. The motivation for both of our problems goes back to a question from number theory, see [38] and Section 6. Let us describe the first problem. Let $P \subseteq \mathbf{G}(q)$ be any parabolic subgroup of $\mathbf{G}(q)$. First of all, what can we say about the size of the product of an arbitrary set $A \subseteq \mathbf{G}(q)$ by P? Of course, A can be a union of cosets of P, say, $x_1P, \dots, x_kP$, and thus AP

2020 Mathematics Subject Classification: Primary 11A55, 11J70, 11B30; Secondary 20G05, 20G40.
Keywords: Continued fractions, diophantine approximations, growth in groups, Chevalley groups.

does not grow. Similarly, if $A = \bigsqcup_j Py_j$, then $PA = A$. Nevertheless, we show that A must grow either after left multiplication or after right multiplication. It reminds the sum-product phenomenon, see, e.g., [50], Sections 8.3–8.5, and indeed our new application to continued fractions (see Section 6 below) is connected with this area, see the discussion of the main results in [37] (e.g., Remark 11 in [37]).

Let us formulate our first theorem in a simplified form (actually, the restriction $A \cap P = \emptyset$ can be relaxed hugely, see Theorem 5.1 from Section 5). Our regime throughout this paper: q tends to infinity and the rank is fixed.

Theorem 1.2. *Let $\mathbf{G}(q)$ be a Chevalley group and let $P \subset \mathbf{G}(q)$ be a parabolic subgroup. Then for any set $A \subseteq \mathbf{G}(q)$ with $A \cap P = \emptyset$, one has*

$$\max\{|AP|, |PA|\} \geq \frac{\sqrt{|A||P|q}}{2}. \tag{1.1}$$

For example, if $|A| \leq |P|$, then $\max\{|AP|, |PA|\} \gg |A|\sqrt{q}$, and this is larger than $|A|$.

Theorem 1.2 above helps us to study the second problem. Let A be an arbitrary subset of a group $\mathbf{G}$ and Γ be a subgroup of $\mathbf{G}$. Can we guarantee that for a certain reasonable n (say, n depends on $\log|\mathbf{G}|/\log|A|$ only) one has $A^n \cap \Gamma \neq \emptyset$? The representation theory (see Theorems 3.3, 5.6 in [14]) allows to show that *any* set $A \subset \mathbf{G}(q)$ of size at least $|\mathbf{G}(q)|q^{-r+\delta}$, where r is rank of $\mathbf{G}(q)$ and $\delta > 0$ is an arbitrary real number, effectively generates the whole group $\mathbf{G}(q)$, i.e., there is $n \ll_r \delta^{-1}$ such that $A^n = \mathbf{G}(q)$. In particular, $A^n \cap \Gamma \neq \emptyset$ for $n \ll_r \delta^{-1}$ (see, e.g., Theorem 5.3 of Section 5) and this bound is essentially sharp. We show that if one wants to find a non-trivial intersection with any parabolic subgroup of $\mathbf{G}(q)$, then it is possible to break this barrier.

Theorem 1.3. *Let q be an odd non-square, let $\mathbf{G}(q)$ be a Chevalley group, let $P \subset \mathbf{G}(q)$ be a parabolic subgroup, and let P_* be a proper parabolic subgroup of maximal size. Suppose that $A \subseteq \mathbf{G}(q)$ is a set with $|A| \geq |P_*|q^{-1+\delta}$, where $\delta > 0$ is a real number. Then there is n, $n \ll_r \delta^{-1}$, such that $A^n \cap P \neq \emptyset$.*

Roughly speaking, in Theorem 1.3 the usual assumption $|A| \gg |\mathbf{G}(q)|q^{-r+\delta}$ is replaced by $|A| \gg |\mathbf{G}(q)|q^{-r-1+\delta}$, and this improvement is crucial for us. Indeed, it turns out that the method of proof of Theorems 1.2 and 1.3 has some applications to the theory of continued fractions, namely, to Zaremba's conjecture. Roughly speaking, in a variant of this problem one should intersect small powers of a certain set $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ with an arbitrary Borel subgroup and in fact, this circle of problems motivated us to study the questions appearing in Theorems 1.2 and 1.3 above.

Let us recall the formulation of Zaremba's conjecture. Let a and q be two positive coprime integers, $0 < a < q$. By the Euclidean algorithm, a rational a/q can be uniquely represented as a regular continued fraction

$$\frac{a}{q} = [0; b_1, \dots, b_s] = \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \dots + \cfrac{1}{b_s}}}}, \qquad b_s \geq 2. \tag{1.2}$$

Zaremba's famous conjecture [52] posits that there is an absolute constant $\mathfrak{k}$ with the following property: for any positive integer q, there exists a coprime to q such that in the continued fraction expansion (1.2) all partial quotients are bounded:

$$b_j(a) \leq \mathfrak{k}, \quad 1 \leq j \leq s = s(a).$$

In fact, Zaremba conjectured that $\mathfrak{k} = 5$. For large prime q, even $\mathfrak{k} = 2$ should be enough, as conjectured by Hensley [20, 21]. Over the past years, this theme has become rather popular, see for instance [8, 19, 29], or the short surveys about this area in [37, 38]. We just mention a result of Korobov [30], who proved that one can always take growing $\mathfrak{k}$, namely, $\mathfrak{k} = O(\log q)$ for prime q (such result is also true for composite q, see [44]).

In [38], we have proved a "modular" version of Zaremba's conjecture.

Theorem 1.4. *There is an absolute constant $\mathfrak{k}$ such that for any prime number p there exists some positive integer $q = O(p^{30})$, $q \equiv 0 \pmod p$, and there exists $a < q$, with a coprime to q, such that a/q has partial quotients bounded by $\mathfrak{k}$.*

The first theorem in this direction was proved by Hensley in [20], and after that in [34, 35]. Now using results similar to Theorems 1.2 and 1.3 above and, of course, growth results in $\mathrm{SL}_2(\mathbb{F}_p)$ of Helfgott [22], we improve Theorem 1.4.

Theorem 1.5. *Let $\varepsilon \in (0, 1]$ be any real number. There is a constant $\mathfrak{k} = \mathfrak{k}(\varepsilon)$ such that for any prime number p there exist some positive integers $q = O(p^{1+\varepsilon})$, $q \equiv 0 \pmod p$, and $a < q$, a coprime to q, such that a/q has partial quotients bounded by $\mathfrak{k}$.*

Clearly, Theorem 1.5 is best possible up to ε and it is the limit of our method.

Another result on continued fractions (see Theorem 6.5 from Section 6) is even more interesting than Theorem 1.5 because its generality and because it is the first (weak) confirmation of Hensley's hypothesis (see Conjecture 3 in [21]). Namely, let now the partial quotients b_j belong to a finite set $\mathcal{A} \subset \mathbb{N}$, $|\mathcal{A}| \geq 2$, and suppose that the Hausdorff dimension of the correspondent Cantor set is strictly greater than $1/2$ (all the definitions are contained in Section 6). Then we show that a full analogue of Theorem 1.5 holds (with other constants, of course).

It is possible for a reader who is interested in Zaremba's conjecture but who does not want to deal with general Chevalley groups to skip Lemma 4.1 and all material of Section 4 before this result, as well as the third part of Theorem 5.5 from Section 5, in a first reading. The remaining information would be enough to understand the proof of Theorem 1.5.

We finish the introduction posing a weak version of Babai's conjecture. Even for sufficiently large subgroups Γ, the answer to our question is non-obvious (clearly, the difficulty increases when the size of Γ decreases).

Problem. *Let $\mathbf{G}$ be a finite simple non-abelian group, $\Gamma \subset \mathbf{G}$ a subgroup, and $A \subseteq \mathbf{G}$ an arbitrary (generating) set. Is it true that $A^n \cap \Gamma \neq \emptyset$ with $n \ll (\log|\mathbf{G}|/\log|A|)^C$, where $C > 0$ is an absolute constant?*

If $A = A^{-1}$, then the set $AA = AA^{-1}$ obviously contains the unit element and hence the answer to the problem is trivially affirmative (moreover, if $|A||\Gamma| > |\mathbf{G}|$, then the Dirichlet principle shows that $|AA^{-1} \cap \Gamma| > 1$ and hence we can find a non-trivial element

in AA^{-1}). Thus we cannot assume that $A = A^{-1}$ and, actually, this restriction is very important for some applications as for our modular version of Zaremba's conjecture.

2. Definitions

Let $\mathbf{G}$ be a finite group with the identity 1. Given two sets $A, B \subset \mathbf{G}$, define the *product set* of A and B as

$$AB := \{ab : a \in A,\ b \in B\}.$$

In a similar way we define higher product sets, e.g., A^3 is AAA. Let $A^{-1} := \{a^{-1} : a \in A\}$. As usual, given two subsets A, B of a group $\mathbf{G}$, we denote by

$$\mathsf{E}(A, B) = |\{(a, a_1, b, b_1) \in A^2 \times B^2 : a^{-1}b = a_1^{-1}b_1\}|$$

the *common energy* of A and B. Clearly, $\mathsf{E}(A, B) = \mathsf{E}(B, A) \geq |A||B|$, $\mathsf{E}(A) = \mathsf{E}(A^{-1})$ and by the Cauchy–Schwarz inequality,

$$\mathsf{E}(A, B)|A^{-1}B| \geq |A|^2|B|^2 \tag{2.1}$$

as well as

$$\mathsf{E}^2(A, B) \leq \mathsf{E}(A, A)\,\mathsf{E}(B, B). \tag{2.2}$$

We use representation function notations like $r_{AB}(x)$ or $r_{AB^{-1}}(x)$, which count the number of ways $x \in \mathbf{G}$ can be expressed as a product ab or ab^{-1} with $a \in A$, $b \in B$, respectively. In a similar way, $r_{ABC}(x)$ counts the number of ways $x \in \mathbf{G}$ can be expressed as a product abc, where $a \in A$, $b \in B$, $c \in C$, etc. For example, $|A| = r_{AA^{-1}}(1)$ and $\mathsf{E}(A, B) = r_{AA^{-1}BB^{-1}}(1) = \sum_x r^2_{A^{-1}B}(x)$. For any sets X, Y, Z, put

$$\sigma_X(Y, Z) := \sum_{x \in X} r_{YZ}(x).$$

In this paper, we use the same letter to denote a set $A \subseteq \mathbf{G}$ and its characteristic function $A\colon \mathbf{G} \to \{0, 1\}$. We write $\mathbb{F}_q^*$ for $\mathbb{F}_q \setminus \{0\}$, where $q = p^s$ and p is a prime number, and we denote by $(a_1, \dots, a_l)$ the greatest common divisor of some given positive integers $a_1, \dots, a_l$. If m divides n, then we write $m|n$.

Let $g \in \mathbf{G}$ and let $A \subseteq \mathbf{G}$ be any set. Then we write $A^g = gAg^{-1}$ and, similarly, we let $x^g := gxg^{-1}$, where $x \in \mathbf{G}$. We write $N(A)$ for the normalizer of a set A, that is, $N(A) = \{g \in \mathbf{G} : A^g = A\}$. If $H \subseteq \mathbf{G}$ is a subgroup, then we use the notation $H \leq \mathbf{G}$.

In the paper we consider the group $\mathrm{SL}_2(\mathbb{F}_q)$ of matrices

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ab|cd), \quad a, b, c, d \in \mathbb{F}_q, \quad ad - bc = 1,$$

as well as other *classical* groups as $\mathrm{PSL}_n(q)$, $\mathrm{SU}_n(q)$, $\mathrm{Sp}_n(q)$, $\Omega_n^{\varepsilon}(q)$ and so on. Also, we use the usual Lie notation $\mathrm{A}_n(q)$, $\mathrm{B}_n(q)$ and so on.

The signs $\ll$ and $\gg$ are the usual Vinogradov symbols. When the constants in the signs depend on a parameter M, we write $\ll_M$ and $\gg_M$. We write $x \sim y$ if $x \gg y$ and $x \ll y$. Similarly, for a parameter M, we use the symbol $x \sim_M y$ if and only if $x \gg_M y$ and $x \ll_M y$. All logarithms are to base 2.

3. Simple facts from the representation theory

First of all, we recall some notions and simple facts from the representation theory, see, e.g., [41] or [46]. For a finite group $\mathbf{G}$, let $\widehat{\mathbf{G}}$ be the set of all irreducible unitary representations of $\mathbf{G}$. It is well known that the size of $\widehat{\mathbf{G}}$ coincides with the number of conjugacy classes of $\mathbf{G}$. For $\rho \in \widehat{\mathbf{G}}$, denote by d_ρ the dimension of this representation. By $d_{\min}(\mathbf{G})$ we denote the quantity $\min_{\rho \neq 1} d_\rho$. We write $\langle \cdot, \cdot \rangle_{\mathrm{HS}}$ for the corresponding Hilbert–Schmidt scalar product $\langle A, B \rangle_{\mathrm{HS}} := \mathrm{tr}(AB^*)$, where A, B are two matrices of the same size. Put $\|A\| = \sqrt{\langle A, A \rangle_{\mathrm{HS}}}$. Clearly, $\langle \rho(g)A, \rho(g)B \rangle_{\mathrm{HS}} = \langle A, B \rangle_{\mathrm{HS}}$ and $\langle AX, Y \rangle_{\mathrm{HS}} = \langle X, A^*Y \rangle_{\mathrm{HS}}$. Also, we have $\sum_{\rho \in \widehat{\mathbf{G}}} d_\rho^2 = |\mathbf{G}|$.

For any function $f : \mathbf{G} \to \mathbb{C}$ and $\rho \in \widehat{\mathbf{G}}$, we define the matrix $\widehat{f}(\rho)$, which is called the Fourier transform of f at ρ, by the formula

$$\widehat{f}(\rho) = \sum_{g \in \mathbf{G}} f(g)\, \rho(g)\,. \tag{3.1}$$

Then the inverse formula reads

$$f(g) = \frac{1}{|\mathbf{G}|} \sum_{\rho \in \widehat{\mathbf{G}}} d_\rho \langle \widehat{f}(\rho), \rho(g) \rangle_{\mathrm{HS}}\,, \tag{3.2}$$

and the Parseval identity is

$$\sum_{g \in \mathbf{G}} |f(g)|^2 = \frac{1}{|\mathbf{G}|} \sum_{\rho \in \widehat{\mathbf{G}}} d_\rho \|\widehat{f}(\rho)\|^2\,. \tag{3.3}$$

The main property of the Fourier transform is the convolution formula

$$\widehat{f * g}(\rho) = \widehat{f}(\rho)\, \widehat{g}(\rho)\,, \tag{3.4}$$

where the convolution of two functions $f, g : \mathbf{G} \to \mathbb{C}$ is defined as

$$(f * g)(x) = \sum_{y \in \mathbf{G}} f(y)\, g(y^{-1}x)\,.$$

Finally, it is easy to check that for any matrices A, B one has $\|AB\| \leq \|A\|_o \|B\|$ and $\|A\|_o \leq \|A\|$, where the operator norm $\|A\|_o$ is just the maximal singular value of A (or, equivalently, the operator l^2-norm of A). In particular, this shows that $\|\cdot\|$ is indeed a matrix norm.

For any function $f : \mathbf{G} \to \mathbb{C}$, consider the Wiener norm of f defined as

$$\|f\|_W := \frac{1}{|\mathbf{G}|} \sum_{\rho \in \widehat{\mathbf{G}}} d_\rho \|\widehat{f}(\rho)\|\,. \tag{3.5}$$

Lemma 3.1. *Let* $\Gamma \leq \mathbf{G}$. *Then* $\|\Gamma\|_W \leq 1$.

Proof. Since Γ is a subgroup, we have for any $x \in \mathbf{G}$ that $\Gamma(x) = |\Gamma|^{-1}(\Gamma * \Gamma)(x) = |\Gamma|^{-1} r_{\Gamma\Gamma}(x)$. Hence using the last equality, formula (3.4), the submultiplicativity of the norm $\|\cdot\|$ and the Parseval identity (3.3), we obtain

$$\|\Gamma\|_W := \frac{1}{|\mathbf{G}|}\sum_{\rho\in\widehat{\mathbf{G}}} d_\rho \|\widehat{\Gamma}(\rho)\| = \frac{1}{|\Gamma||\mathbf{G}|}\sum_{\rho\in\widehat{\mathbf{G}}} d_\rho \|\widehat{\Gamma}^2(\rho)\| \le \frac{1}{|\Gamma||\mathbf{G}|}\sum_{\rho\in\widehat{\mathbf{G}}} d_\rho \|\widehat{\Gamma}(\rho)\|^2 = 1,$$

as required. ∎

Lemma 3.1 implies a result on growth in the affine group relatively to some subgroups. Namely, the following Corollary 3.2 can be considered as a "baby"-version of our main results on intersections of A^n with parabolic subgroups (see Theorem 5.5 below). For simplicity suppose that q is an odd number. Clearly, there is a group homomorphism φ of the standard Borel subgroup $B = \{(\lambda u\,|\,0\lambda^{-1}) : \lambda \in \mathbb{F}_q^*,\ u \in \mathbb{F}_q\}$ of the upper-triangular matrices onto an index two subgroup of $\mathrm{Aff}(\mathbb{F}_q)$, namely, $\varphi((\lambda u\,|\,0\lambda^{-1})) = (\lambda^2\,\lambda u\,|\,01)$ and $\mathrm{Ker}\varphi = \pm I$. The representation theory of B is similar to the representation theory of $\mathrm{Aff}(\mathbb{F}_q)$ (there are $q+3$ conjugacy classes, further, there exists $q-1$ one-dimensional representations and four representations of dimension $(q-1)/2$). Hence we can apply Corollary 3.2 (as in the first part of Theorem 5.5) in our study of the growth in $\mathrm{SL}_2(\mathbb{F}_q)$.

Corollary 3.2. *Let $A \subseteq \mathrm{Aff}(\mathbb{F}_q)$ be a set, and let $\Gamma \subseteq \mathrm{Aff}(\mathbb{F}_q)$ be a subgroup such that for every non-trivial multiplicative character χ, the restriction of χ to Γ is non-trivial. Also, let $z \in \mathrm{Aff}(\mathbb{F}_q)$ be an arbitrary element, let $n \ge 1$ be a positive integer, and let $|A|^n|\Gamma|^2 > q^{n+2}(q-1)^2$. Then $A^n \cap z\Gamma \ne \emptyset$ and $A^n \cap \Gamma z \ne \emptyset$.*

Proof. The representation theory of $\mathrm{Aff}(\mathbb{F}_q)$ is well known, see, e.g., [12]. Namely, there are $(q-1)$ one-dimensional representations ρ_χ, which are given by multiplicative characters χ, where $\rho_\chi((ab|01)) := \chi(a)$, and a certain $(q-1)$-dimensional representation π. Using formula (3.3) with $f = A$, we have

$$\|\widehat{A}(\pi)\|_o \le \|\widehat{A}(\pi)\| < \Big(\frac{|A|\,|\mathrm{Aff}(\mathbb{F}_q)|}{q-1}\Big)^{1/2} = (|A|q)^{1/2}. \tag{3.6}$$

Further, by the assumption, for any non-trivial multiplicative character χ there is $\gamma = (a,b) \in \Gamma$ such that $\chi(a) \ne 1$. This means that for any such χ one has $\rho_\chi(\Gamma) = 0$. Applying the bound (3.6), Lemma 3.1 and using formula (3.3) again, we obtain

$$\begin{aligned} r_{A^n\Gamma z^{-1}}(1) &= \frac{|A|^n|\Gamma|}{|\mathrm{Aff}(\mathbb{F}_q)|} + \frac{q-1}{|\mathrm{Aff}(\mathbb{F}_q)|}\,\langle \widehat{A}^n(\pi), \widehat{z\Gamma}(\pi)\rangle_{\mathrm{HS}} \\ &\ge \frac{|A|^n|\Gamma|}{|\mathrm{Aff}(\mathbb{F}_q)|} - \|\widehat{A}(\pi)\|_o^n\,\|z\Gamma\|_W \ge \frac{|A|^n|\Gamma|}{|\mathrm{Aff}(\mathbb{F}_q)|} - (|A|q)^{n/2} > 0, \end{aligned} \tag{3.7}$$

provided $|A|^n|\Gamma|^2 > q^{n+2}(q-1)^2$. This completes the proof. ∎

The condition $|A|^n|\Gamma|^2 > q^{n+2}(q-1)^2$ effectively works if, roughly, $|A| \gg q^{1+\varepsilon}$, where $\varepsilon > 0$ is a certain number. Further, an example of subgroup Γ from Corollary 3.2 is a torus $(\lambda 0|01)$, where λ runs over $\mathbb{F}_q^*$. Finally, notice that some assumptions on the

restriction of linear characters to Γ is needed. For instance, consider the unipotent subgroup U of $\mathrm{Aff}(\mathbb{F}_q)$. All linear characters of $\mathrm{Aff}(\mathbb{F}_q)$ restrict trivially to U, and one can easily construct a set A, $|A| \gg q^2/n$, such that $A^n \cap U = \emptyset$.

We shall use the arguments of the proof of Corollary 3.2 several times in this paper. For the convenience of the reader, we formulate a general lemma which we will apply later.

Lemma 3.3. *Let $\mathbf{G}$ be a finite group, let $\Gamma \le \mathbf{G}$, and let $z \in \mathbf{G}$ be an arbitrary element. Suppose that n is a positive integer such that $|A|^n|\Gamma|^2 d_{\min}^n > |\mathbf{G}|^{n+2}$. Then $A^n \cap z\Gamma \neq \emptyset$ and $A^n \cap \Gamma z \neq \emptyset$.*

Proof. Let $d = d_{\min}$. Using formula (3.3) with $f = A$, we have for any non-trivial representation ρ that

$$\|\widehat{A}(\rho)\|_o \le \|\widehat{A}(\rho)\| < \Big(\frac{|A||\mathbf{G}|}{d}\Big)^{1/2}. \tag{3.8}$$

Applying bound (3.8), Lemma 3.1 and using formula (3.3) again, we obtain

$$\begin{aligned} r_{A^n\Gamma z^{-1}}(1) &= \frac{|A|^n|\Gamma|}{|\mathbf{G}|} + \frac{1}{|\mathbf{G}|}\sum_{\rho\neq 1} d_\rho \langle \widehat{A}^n(\rho), \widehat{z\Gamma}(\rho)\rangle_{\mathrm{HS}} \\ &\ge \frac{|A|^n|\Gamma|}{|\mathbf{G}|} - \|z\Gamma\|_W \cdot \max_{\rho\neq 1}\|\widehat{A}(\rho)\|_o^n \ge \frac{|A|^n|\Gamma|}{|\mathbf{G}|} - \Big(\frac{|A||\mathbf{G}|}{d}\Big)^{n/2} > 0, \end{aligned}$$

provided $|A|^n|\Gamma|^2 d^n > |\mathbf{G}|^{n+2}$. This completes the proof. ∎

4. Some facts about Chevalley groups

We recall briefly some properties of (untwisted, generated by its root subgroups and having trivial center) Chevalley groups. The detailed description of such groups can be found in many books and papers, see, e.g., the classical book [48] and the paper [11]. Much of the notation that we use in this section will be freely used in the rest of the paper.

Let p be a prime number, let $q = p^s$, and let $\mathbb{F}_q$ be the finite field of size q. Also, let Φ be a root system, Π a fundamental subsystem, $\Pi \subseteq \Phi^+$, $\Phi = \Phi^+ \bigsqcup(-\Phi^+)$. Everything below depends on the root system Φ but we do not put emphasis on this. Let B be a Borel subgroup of $\mathbf{G} = \mathbf{G}(q)$, $U = O_p(B)$ (the unique largest normal p-subgroup of B), $B = UH$ (the product is semidirect and U is normal in B), $N = N(H)$ with H an abelian p'-group (Cartan subgroup). The unipotent subgroup U is the product of subgroups $\prod_{r\in\Phi^+} U_r$ and each U_r is isomorphic to the field $\mathbb{F}_q$. The Weyl group $W = N/H$ is a group generated by fundamental reflections $w_{r_1}, \dots, w_{r_l}$, $l = |\Pi|$, and W acts on the root system Φ. When there is no problem with coset representatives, we will consider $s \in W$ as an element of $\mathbf{G}(q)$. For $w \in W$, let $l(w)$ be the *length* of w, that is, the minimal n such that $w = w_{r_1} \dots w_{r_n}$ with $r_j \in \Pi$. Another description of $l(w)$ is $l(w) = |\Phi^+ \cap w^{-1}(-\Phi^+)|$ and it is clear that $l(w) = 0$ if and only if $w = 1$ (and if and only if $w(\Pi) = \Pi$, and if and only if $w(\Phi^+) = \Phi^+$). For any $J \subseteq \Pi$, let W_J be the

subgroup of W generated by w_r, where $r \in J$. It is well known that for any Chevalley group the Bruhat decomposition holds, namely,

$$\mathbf{G}(q) = \bigsqcup_{w \in W} BwB\,, \tag{4.1}$$

where the union in (4.1) is disjoint. This decomposition follows from the fact that, for any fundamental root r and an arbitrary $w \in W$, one has

$$w_r B w \subseteq BwB \cup Bw_r wB\,. \tag{4.2}$$

Decomposition (4.1) can be refined further. For $w \in W$, put

$$U'_w = \langle \{U_r \,:\, r \in \Phi^+, w(r) \in \Phi^+\}\rangle \quad \text{and} \quad U''_w = \langle \{U_r \,:\, r \in \Phi^+, w(r) \in -\Phi^+\}\rangle\,.$$

Then, clearly, $U = U'_w U''_w$, $B = HU'_w U''_w$ and $wU'_w w^{-1} \subseteq U$. Thus (4.1) can be rewritten as

$$\mathbf{G}(q) = \bigsqcup_{w \in W} BwU''_w\,, \tag{4.3}$$

and it turns out that every element of $\mathbf{G}(q)$ can be written in the form (4.3) uniquely. In particular,

$$|\mathbf{G}(q)| = |B| \sum_{w \in W} |U''_w| = |H||U| \sum_{w \in W} |U''_w| = |H| q^{|\Phi^+|} \sum_{w \in W} q^{l(w)} \tag{4.4}$$

and $|H| = (q-1)^{|\Pi|}/d$, where $d = (\Delta(\mathbf{G}(q)), q-1)$ if $\mathbf{G}(q)$ has no type D_l, and $d = (4, 4^l - 1)$ otherwise (it is known that the quantity $\Delta(\mathbf{G}(q))$ does not depend on q, see, e.g., Section 10 in [11]). From the Bruhat decomposition and the properties of Chevalley groups, it follows that all subgroups containing B are 2^l subgroups of the form $P_J := BW_J B$ and any conjugate of the subgroups P_J is called a *parabolic subgroup*. It is known that $N(P_J) = P_J$, and (see, e.g., Lemma 3 in [11])

$$P_J = \langle B, \{w_j\}_{j \in J}\rangle = \Big\langle B, \prod_{j=1}^{J} w_j \Big\rangle = \Big\langle B, \Big(\prod_{j=1}^{J} w_j\Big) B \Big(\prod_{j=1}^{J} w_j\Big)^{-1} \Big\rangle. \tag{4.5}$$

Put $W^J = \{w \in W : w(r) \in \Phi^+ \text{ for all } r \in J\}$. One can check (see, e.g., Proposition 2.4.4 in [5]) that any $w \in W$ can be decomposed uniquely as $w = w^J w_J$, where $w^J \in W^J$ and $w_J \in W_J$ and, moreover, $l(w) = l(w^J) + l(w_J)$. Any W_J (and W in particular) contains the unique *longest* element (that is, an element of maximal length) and this element is an involution. Formula (4.4) says, basically, that the length of the longest element of $\mathbf{G}(q)$ determines the size of $\mathbf{G}(q)$ and, similarly, writing

$$|P_J| = |B| \sum_{w \in W_J} |U''_w| = |H| q^{|\Phi^+|} \sum_{w \in W_J} q^{l(w)}, \tag{4.6}$$

we see that the length of the longest element of P_J determines its size up to $o(|P_J|)$ (for $|\Pi|$ fixed and $q \to \infty$).

In the paper [31], it was proved that Chevalley groups are quasi-random in the sense of Gowers [14] (also, see the first paper [45] where this concept was used). Namely, we have, by [31],

$$d_{\min}(\mathbf{G}(q)) \gg_r q^r, \tag{4.7}$$

where the rank r is the dimension of its maximal tori of $\mathbf{G}(q)$ or, in other words, $|\Pi|$ (in the case of a semisimple Chevalley group).

Let $\mathcal{P}_1(\mathbf{G}(q)) \geq \mathcal{P}_2(\mathbf{G}(q)) \geq \cdots$ be the sizes of maximal proper parabolic subgroups of $\mathbf{G}(q)$. Consider the quantity

$$\mathcal{P}(\mathbf{G}(q)) := \min\{t \,:\, \forall \Gamma \leq \mathbf{G}(q),\ |\Gamma| > t \implies \Gamma \text{ is parabolic}\}.$$

In other words, $\mathcal{P}(\mathbf{G}(q))$ coincides with the size of the largest (by cardinality) non-parabolic subgroup. The quantity depends on the concrete Chevalley group $\mathbf{G}(q)$ (e.g., $\mathrm{P}\Omega_8^+(q)$ contains the largest (by cardinality) parabolic subgroup P and also two large non-parabolic subgroups $\Omega_7(q)$, $\mathrm{Sp}_6(q)$, depending on the parity of q, $|\Omega_7(q)| \sim |\mathrm{Sp}_6(q)| \sim q^{-1}|\mathcal{P}_1(\mathrm{P}\Omega_8^+(q))|$, see Table 7 and Proposition 4.3.4 in [1]). Nevertheless, we give a simple upper bound for $\mathcal{P}(\mathbf{G}(q))$ in terms of $\mathcal{P}_1(\mathbf{G}(q))$, see Lemma 4.1 below. Initially, our proof is hugely based on the books [27] and [51] (which in turn use the famous Aschbacher classification theorem, [2], see the good survey [26] and also the paper [1]). We thank the reviewer for pointing us the papers [32] and [33], where all maximal (by size) proper subgroups of the finite classical/exceptional groups were found; this allows to obtain a shorter proof of Lemma 4.1. Our result is applicable for a slightly wider class of groups than our untwisted Chevalley groups, and we formulate a slightly more general statement because it does not increase the length of the proof significantly. Finally, due to the existence of isomorphisms between low-dimensional classical groups (see Proposition 2.9.1 in [27], for example), we may assume without loss of generality that n satisfies the stated lower bounds of Lemma 4.1, i.e., we can consider $n \geq 2$ for $\mathrm{PSL}_2(q)$, further $n \geq 3$ for $\mathrm{SU}_n(q)$, $n \geq 4$ for $\mathrm{PSp}_n(q)$, and $n \geq 7$ for $\Omega_n^\varepsilon(q)$, where $\varepsilon = \pm$ to cover all possible cases.

Lemma 4.1. *Let q be a sufficiently large odd non-square and let $\mathbf{G}(q)$ be a Chevalley group. Then we have $\mathcal{P}(\mathrm{PSL}_2(q)) \leq 2(q+1)$, $\mathcal{P}(\mathrm{PSL}_3(q)) \leq q^3$, and for $n \geq 4$, the following holds*: $\mathcal{P}(\mathrm{PSL}_n(q)) \leq q^{n(n+1)/2}$.

Further, we consider $n \geq 3$ for $\mathrm{SU}_n(q)$, $n \geq 4$ for $\mathrm{PSp}_n(q)$, $n \geq 7$ for $\Omega_n^\varepsilon(q)$, where $\varepsilon = \pm$. In all cases above and for all simple exceptional groups, one has

$$q\mathcal{P}(\mathbf{G}(q)) \ll \mathcal{P}_1(\mathbf{G}(q)) = \max\{|\Gamma| \,:\, \Gamma \leq \mathbf{G}(q),\ \Gamma \neq \mathbf{G}(q)\}. \tag{4.8}$$

Proof. The case $\mathrm{PSL}_n(q)$ for small n is simple and follows from the classification of subgroups of $\mathrm{PSL}_2(q)$ (see, e.g., [49], we use the assumption that q is a non-square to avoid the subgroup $\mathrm{PGL}_2(\sqrt{q}) \subset \mathrm{PSL}_2(q)$, say), further for $\mathrm{PSL}_3(q)$ (we apply the assumption that q is a non-square to avoid the subgroup $\mathrm{PSU}_3(q)$, say), see [36], for $\mathrm{PSU}_3(q)$, $\mathrm{PSp}_4(q)$ with odd q, again, see [36] and, finally, for $\mathrm{PSL}_4(q)$ with even q, see [40] (here we appeal to the fact that that $\mathrm{PSL}_4(q)$ contains $\mathrm{PSp}_4(q)$ having size less than $q^{4(4+1)/2}$).

Now let $n \geq 4$ and let us consider the general case. Put $d = (n, q-1)$, $\alpha = (2, q-1)$. We prove the inequality and the equality in (4.8) simultaneously. It is enough to check the

equality for all irreducible subgroups which are contained in Theorems 5.1–5.6 of [32] and in [33], or in [51] for exceptional groups. Let us, for example, consider the case $\mathrm{PSL}_n(q)$. It is known that the only subgroups belonging to the first Aschbacher class are maximal parabolic subgroups $\mathcal{P}_m(\mathrm{PSL}_n(q))$ with

$$|\mathcal{P}_m(\mathrm{PSL}_n(q))| = d^{-1}q^{m(n-m)}(q-1)\,|\mathrm{SL}_m(q)|\,|\mathrm{SL}_{n-m}(q)| \sim q^{n^2-nm+m^2-1} \geq q^{3n^2/4-1} > q^{n(n+1)/2}, \tag{4.9}$$

and by Theorem 5.1 of [32], the only irreducible subgroup Γ of minimal index has $\mathrm{soc}(\Gamma) = \Omega_n(q)$ or $\mathrm{PSp}_n(q)$ (recall that by our assumption q is a sufficiently large odd non-square) and hence these subgroups are too small. Also, using (4.9) one can check that the equality in (4.8) holds for all reducible subgroup (it is known that in the case of classical groups all reducible subgroups belong to the first Aschbacher class), as well as for both irreducible subgroups, and thus (4.8) holds for $\mathrm{PSL}_n(q)$. Similarly, for the remaining groups of Lie type we have analogous of formula (4.9), namely (see Propositions 4.1.18–4.1.20 in [27])

$$|\mathcal{P}_m(\mathrm{SU}_n(q))| \sim q^{2nm-3m^2+2}\,|\mathrm{L}_m(q^2)|\,|\mathrm{U}_{n-2m}(q)| \sim q^{n^2-2nm+3m^2-1}, \tag{4.10}$$

$$|\mathcal{P}_m(\mathrm{PSp}_n(q))| = q^{nm+m/2-3m^2/2}(q-1)\,|\mathrm{PGL}_m(q)|\,|\mathrm{PSp}_{n-2m}(q)| \sim q^{(n^2-2nm+n+3m^2-m)/2}, \tag{4.11}$$

and for $m \leq n/2$ (we do not consider smaller parabolic subgroups), one has

$$|\mathcal{P}_m(\Omega^{\varepsilon}_n(q))| \sim q^{nm-m/2-3m^2/2}|\mathrm{GL}_m(q)||\Omega^{\varepsilon}_{n-2m}(q)| \sim q^{(n^2-2nm-n+3m^2+m)/2}. \tag{4.12}$$

Again, we apply Theorems 5.2–5.6 of [32] and see that there are just irreducible subgroups of minimal index:

- $\mathrm{PSp}_m(q^2)\cdot 2$, $\mathrm{GU}_m(q)\cdot 2/Z$ and $\mathrm{PSL}_2(q^2)\cdot 2$ (for $\mathrm{PSp}_{2m}(q)$, $m>2$ and $m=2$, correspondingly),
- $\mathrm{PSp}_n(q)$ and $\mathrm{soc}(\Gamma) = \Omega_n(q)$ (for $\mathrm{PSU}_n(q)$),
- $\mathrm{GL}_m(q)\cdot 2/Z$, $\mathrm{GU}_m(q)\cdot 2/Z$ and $\mathrm{PO}_7(q)$ (for $\mathrm{PSO}^+_{2m}(q)$, $m\geq 6$ and $m=4$, correspondingly, and in a similar way for $\mathrm{P}\Omega^+_{2m}(q)$),
- $\mathrm{P}\Omega^-_m(q^2)$ and $\mathrm{GU}_m(q)\cdot a/Z$, where $a=1,2$ (for $\mathrm{P}\Omega^-_{2m}(q)$),
- $\Omega(2m+1,q_0)$, $q=q_0^c$, where c is a prime and $(O_a(q)\wr S_b)\cap\Omega(2m+1,q)$, where $ab=2m+1$ (for $\Omega_{2m+1}(q)$).

It is easy to check that in all such cases the equality in (4.8) takes place and moreover the inequality also holds true.

It remains to consider the exceptional groups. We should consider untwisted groups only, but formula (4.8) holds in a slightly more general context. In the case of the exceptional groups, we use Theorem 5 and Table 2 in [1] (an alternative way is to apply the results from [33], which say that any maximal subgroup Γ of $\mathbf{G}(q)$ of size $|\Gamma|\geq|\mathbf{G}(q)|^{1/3}$ is either a maximal parabolic subgroup or belongs to a certain list, see [1], Table 2 (again it is easy to check that the condition $q^{-1}\mathcal{P}_1(\mathbf{G}(q))\geq|\mathbf{G}(q)|^{1/3}$ holds). Analysing this table, one can see that the sizes of all non-parabolic subgroups of the exceptional groups

do not exceed $|B|$ with four exceptions: $\mathrm{F}_4(q)$ (the largest subgroups are $\mathrm{B}_4(q)$, $\mathrm{C}_4(q)$), further, $\mathrm{E}_6^{\varepsilon}(q)$ (the largest subgroup is $\mathrm{F}_4(q)$), $\mathrm{E}_7(q)$ (the largest subgroup is $(q-\varepsilon)\mathrm{E}_6^{\varepsilon}(q)$) and, finally, $\mathrm{E}_8(q)$ with the largest subgroup $\mathrm{A}_1(q)\mathrm{E}_7(q)$. For $\mathrm{F}_4(q)$, consult Section 4.5.9 in [51] to see that there is a parabolic subgroup $\Gamma \le \mathrm{F}_4(q)$ such that

$$\Gamma| = q^{15}(q-1)|\mathrm{Sp}_6(q)| \sim q^{37} \sim q\,|\mathrm{B}_4(q)| \sim q\,|\mathrm{C}_4(q)|\,.$$

Further, for $\mathrm{E}_6^{\varepsilon}(q)$ see Section 4.6.4 in [51] and [28], where it was proved that there exists a parabolic subgroup of size $q^{25}(q-1)|\mathrm{L}_2(q)||\mathrm{L}_5(q)| \sim q^{53} \sim q|\mathrm{F}_4(q)|$. Finally, if we consider $\mathrm{E}_8(q)$, then by [51], Section 4.7.2, this group contains a subgroup of size $\gg q^{58}|\mathrm{E}_7(q)|$ and this is much larger than $q|\mathrm{A}_1(q)||\mathrm{E}_7(q)|$. If we take $\mathrm{E}_7(q)$, then, similarly, by [51], Section 4.7.3, we see that $q^2|\mathrm{E}_6^{\varepsilon}(q)|$ is small. One can use another way to prove that the maximal (by size) parabolic subgroup is large: just analyse the Dynkin diagrams for $\mathrm{F}_4(q)$, $\mathrm{E}_6^{\varepsilon}(q)$, $\mathrm{E}_7(q)$ and $\mathrm{E}_8(q)$. This completes the proof. ∎

We need a simple general lemma (a similar result can be found in [16]).

Lemma 4.2. *Let* $\mathbf{G}$ *be a finite group and let* $\Gamma_1, \Gamma_2 \le \mathbf{G}$. *Then for* $x, y \in \mathbf{G}$, $x\Gamma_1 \cap \Gamma_2 y$ *is either empty or a translate of* $\Gamma_1^x \cap \Gamma_2$, $\Gamma_2^{y^{-1}} \cap \Gamma_1$. *In particular,*

$$\max_{x,y\in\mathbf{G}} |x\Gamma_1 \cap \Gamma_2 y| = \max_{x\in\mathbf{G}} |x\Gamma_1 \cap \Gamma_2 x|\,.$$

Also, we have $|\Gamma_1 \cap \Gamma_2| \ge |\Gamma_1||\Gamma_2|/|\mathbf{G}|$.

Proof. If the intersection $x\Gamma_1 \cap \Gamma_2 y$ is empty, then there is nothing to prove. Otherwise, for any $c \in x\Gamma_1 \cap \Gamma_2 y$ one has

$$x\Gamma_1 \cap \Gamma_2 y = ((x\Gamma_1 x^{-1}) \cap \Gamma_2)c = c((y^{-1}\Gamma_2 y) \cap \Gamma_1)$$

as required.

Now from the Dirichlet principle there is $x \in \mathbf{G}$ such that $A := x\Gamma_1 \cap \Gamma_2$ has size at least $|\Gamma_1||\Gamma_2|/|\mathbf{G}|$. But $A \subseteq \Gamma_2$ and hence $A^{-1}A \subseteq \Gamma_1 \cap \Gamma_2$. It remains to notice that $|A^{-1}A| \ge |A| \ge |\Gamma_1||\Gamma_2|/|\mathbf{G}|$. An alternative way of the proof is just using the formula $|\Gamma_1 \cap \Gamma_2| = |\Gamma_1||\Gamma_2|/|\Gamma_1\Gamma_2| \ge |\Gamma_1||\Gamma_2|/|\mathbf{G}|$. This completes the proof. ∎

Now we are ready to prove a result on an upper bound for $|P \cap P^g|$ for parabolic subgroups P of $\mathbf{G}(q)$.

Lemma 4.3. *Let* $\mathbf{G}(q)$ *be a Chevalley group and let* $P \subset \mathbf{G}(q)$ *be a parabolic subgroup. Then for any* $g \notin P$ *one has*

$$r_{PgP}(x) \le \frac{2|P|}{q} \quad \textit{for all } x \in \mathbf{G}(q)\,. \tag{4.13}$$

Proof. In view of Lemma 4.2, it is enough to estimate $|P \cap P^g|$. Let $P = P_J$. From the Bruhat decomposition (4.1), we can assume that $g \in W$ and moreover we can assume that $g \in W^J$, $g \notin W_J$.

First of all, let us obtain (4.13) for the Borel subgroup B (in this case g must belong to W). The equation $Bg = gB$ can be rewritten as $Bg = gHU_g'U_g'' = HU_g'gU_g''$ (here we have used the definitions of the sets U_g', U_g'') and hence by (4.3) it has $|HU_g'| = |B|/|U_g''| = |B|q^{-l(g)}$ solutions. Clearly, $l(g) \ge 1$, and the result follows (in this case we do not even need the constant 2 in inequality (4.13)).

Now let $P = P_J$ be an arbitrary parabolic subgroup. Using the Bruhat decomposition and the arguments as in the case of the Borel subgroup, we obtain

$$|P \cap P^g| = \sum_{v_1,v_2 \in W_J} |gBv_1U''_{v_1} \cap Bv_2U''_{v_2}g|$$
$$\le \sum_{v_1,v_2 \in W_J,\, l(v_2) \le l(v_1)} |gBv_1U''_{v_1} \cap Bv_2U''_{v_2}g| + \sum_{v_1,v_2 \in W_J,\, l(v_1) \le l(v_2)} |gBv_1U''_{v_1} \cap Bv_2U''_{v_2}g|$$
$$= S_1 + S_2 .$$

Below we consider the first sum S_1; the second sum can be estimated similarly. We have

(4.14)
$$S_1 = |B|^{-2} \sum_{v_1,v_2 \in W_J,\, l(v_2) \le l(v_1)} q^{l(v_1)+l(v_2)} \cdot |\{(b_1,b_2,b_3,b_4) \in B^4 : gb_1v_1b_2 = b_3v_2b_4g\}|.$$

To obtain (4.14), we use that $gBv_1U''_{v_1} \cap Bv_2U''_{v_2}g = gBv_1B \cap Bv_2Bg$ and that the last set is not a direct product but contains any element of the set $gBv_1U''_{v_1} \cap Bv_2U''_{v_2}g$ with multiplicity $|B|^2 q^{-l(v_1)-l(v_2)}$. Now applying the inclusions (4.2), we see that for any $v \in W_J$ one has $gBv \subseteq BvB \cup BgvB$. Since $g \notin P$, we get $gBv \subseteq BgvB$ and hence any element gbv_j, $b \in B$, $j = 1,2$, can be written as $b_1gv_jb_2$, $b_1, b_2 \in B$. The same is true for vBg, of course. Whence recalling (4.14), we get

$$S_1 \le \sum_{v_1,v_2 \in W_J,\, l(v_2) \le l(v_1)} q^{l(v_1)+l(v_2)} |gv_1B \cap Bv_2g| .$$

Again, applying the Bruhat decomposition and transforming gv_1B as $HU'_{gv_1}gv_1U''_{gv_1}$, we derive

$$S_1 \le |B| \sum_{v_1,v_2 \in W_J,\, l(v_2) \le l(v_1),\, gv_1 = v_2g} q^{l(v_1)+l(v_2)-l(gv_1)}$$
$$\le |B| \sum_{v_1,v_2 \in W_J,\, l(v_2) \le l(v_1),\, gv_1 = v_2g} q^{2l(v_1)-l(gv_1)} .$$

But $g \in W^J$ and hence $l(gv_1) = l(g) + l(v_1)$. Clearly, $l(g) \ge 1$, because otherwise $g \in W_J$. In view of (4.4), this gives us

$$S_1 \le |B|q^{-1} \sum_{v_1,v_2 \in W_J,\, l(v_2) \le l(v_1),\, gv_1 = v_2g} q^{l(v_1)} \le |B|q^{-1} \sum_{v \in W_J} q^{l(v)} = |P|q^{-1}$$

as required. ∎

The argument given in the first part of the proof shows that the bound is tight for Borel subgroups (and we do not even need the factor 2).

We finish this section with a lemma in the spirit of the well-known result of Frobenius [13] on the representation of $\mathrm{SL}_n(\mathbb{F}_q)$. We thank the reviewer, who showed us a more simple way to obtain the result.

Lemma 4.4. *Let $\mathbf{G}(q)$ be a Chevalley group and let $P \subseteq \mathbf{G}(q)$ be a parabolic subgroup. Suppose that ρ is an arbitrary non-trivial irreducible representation of P such that $\widehat{H}(\rho) \ne 0$. Then $d_\rho \ge (q-1)/2$.*

Proof. Suppose that $\rho(u) \neq 1$ on the unipotent radical of B, in other words, U acts non-trivially. Then there is $r \in \Phi^+$ such that $\rho(U_r) \neq 1$. Since there is a canonical homomorphism from $\mathrm{SL}_2(\mathbb{F}_q)$ onto $\langle U_r, U_{-r}\rangle$, where $r \in \Phi$ is arbitrary and

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 1 & \lambda^2 t \\ 0 & 1 \end{pmatrix},$$

we see that, say, $g := (11|01)$ is conjugated with g^m, where m runs over all quadratic residues of $\mathbb{F}_q^*$. In other words, the operation $x \to x^m$ permutes all eigenvalues of $\rho(g)$ and hence the dimension d_ρ is at least $(q-1)/2$ (strictly speaking, the arguments above hold for $\mathbb{F}_p$ but it is easy to show that for $\mathbb{F}_q$ a similar method works, see, e.g., Proposition 8.10 in [9]).

Now assume, for a contradiction, that U acts trivially. By (4.5) we know that $P_J = \langle B, \{w_j\}_{j\in J}\rangle = \langle B, \prod_{j=1}^J w_j\rangle = \langle B, (\prod_{j=1}^J w_j)B(\prod_{j=1}^J w_j)^{-1}\rangle$. Our assumptions on ρ and the last formulae imply that the restriction of ρ to B is non-trivial and irreducible. Since $B/U \cong H$, it follows that ρ is one-dimensional. The condition $\widehat{H}(\rho) \neq 0$ and the fact that ρ is one-dimensional give us that the restriction of ρ to B is trivial, and this is a contradiction. ∎

5. Growth relatively to parabolic subgroups

Now let us obtain a result on growth of subsets from $\mathbf{G}(q)$ under left/right multiplications by parabolic subgroups.

Bounds in Theorem 5.1 below depend on the quantities $\sigma_P(A^{-1}, A)$, $\sigma_P(A, A^{-1})$, where A is an arbitrary subset of $\mathbf{G}(q)$ and P is a parabolic subgroup. The sense of these expressions is rather obvious, namely, $\sigma_P(A^{-1}, A)$ and $\sigma_P(A, A^{-1})$ are small if the intersection of A with left/right cosets of P is small in average.

Theorem 5.1. *Let $\mathbf{G}(q)$ be a Chevalley group and let $P \subset \mathbf{G}(q)$ be a parabolic subgroup. Then for any set $A \subseteq \mathbf{G}(q)$ one has either*

$$|AP||A \cap P| \geq \frac{|A|^2}{2}$$

or

$$|AP||PA| \geq \frac{|A||P|q}{4}. \tag{5.1}$$

In particular,

$$\max\{|AP|, |PA|\} \geq \frac{1}{2}\min\{|A|^2|A \cap P|^{-1}, (|A||P|q)^{1/2}\}. \tag{5.2}$$

Similarly,

$$|APA| \geq \frac{|P|}{4} \cdot \min\{q, |A|^4\sigma_P^{-1}(A^{-1}, A)\sigma_P^{-1}(A, A^{-1})\}, \tag{5.3}$$

and if A is not contained in P, then

$$|BAP| \geq q|P|. \tag{5.4}$$

Proof. Let $g \notin P$ and put $A_g = A \cap gP$. Also, let $\delta = \max_{g \notin P} |A_g|$. We have

$$\mathsf{E}(A^{-1}, P) = \sum_x r^2_{AP}(x) = \sum_{x \in P} r^2_{AP}(x) + \sum_{x \notin P} r^2_{AP}(x) \le |P| \sum_{x \in P} r_{AP}(x) + \delta |P||A|$$

$$= |P|^2 |A \cap P| + \delta |P||A|. \tag{5.5}$$

In view of (2.1), we get

$$|AP| \ge \frac{1}{2} \min\{|A||P|\Delta^{-1}, |A|^2 |A \cap P|^{-1}\}. \tag{5.6}$$

On the other hand, using Lemma 4.3, we derive

$$\mathsf{E}(P, A_g) = \sum_x r^2_{PA_g}(x) \le \sum_x r_{PA_g}(x)\, r_{PgP}(x) \le 2|P|^2 |A_g| q^{-1}, \tag{5.7}$$

and hence by the Cauchy–Schwarz inequality (2.1), we get

$$|PA| \ge |PA_g| \ge \frac{|P|^2 |A_g|^2}{\mathsf{E}(P, A_g)} \ge \frac{q|A_g|}{2} = \frac{q\Delta}{2}, \tag{5.8}$$

where we choose g such that $|A_g| = \Delta$. Combining (5.6) and (5.8), we arrive to (5.1) and (5.2) follows immediately.

Similarly, let us obtain (5.3). In view of Lemma 4.2 and Lemma 4.3, we have

$$\sigma := \sum_x r^2_{APA}(x) = \sum_{z,z'} r_{A^{-1}A}(z)\, r_{AA^{-1}}(z')\, |zP \cap Pz'|$$

$$= \sum_{z,z' \in P} r_{A^{-1}A}(z)\, r_{AA^{-1}}(z') |zP \cap Pz'| + \sum_{z,z' \notin P} r_{A^{-1}A}(z)\, r_{AA^{-1}}(z') |zP \cap Pz'|$$

$$\le |P| \sigma_P(A^{-1}, A) \sigma_P(A, A^{-1}) + 2|P| q^{-1} |A|^4. \tag{5.9}$$

By the Cauchy–Schwarz inequality, we know that $\sigma |APA| \ge |A|^4 |P|^2$ and combining this with (5.9), we obtain the required result.

It remains to obtain (5.4). Since A is not contained in $P = P_J$, it follows that there are $w_J \in W_J$, $1 \ne w^J \in W^J$, $b_1, b_2 \in B$, such that the product $b_1 w^J w_J b_2$ is an element from A. This follows easily from the Bruhat decomposition. Then $Bw^J w_J P \subseteq BAP$ and $w_J P = P$. Thus we see that BAP contains disjoint sets $Bw^J vB$ for any $v \in W_J$ and hence, by (4.4),

$$|BAP| \ge \sum_{v \in W_J} |Bw^J vB| = |B| \sum_{v \in W_J} q^{l(w^J v)} = |B| q^{l(w^J)} \sum_{v \in W_J} q^{l(v)}$$

$$\ge q|B| \sum_{v \in W_J} q^{l(v)} = q|P_J|.$$

This completes the proof. ∎

Remark 5.2. It is easy to see that the bound (5.2) is tight. Indeed, let $P = B$ be a Borel subgroup and let $A = B \bigsqcup Bw_r B$, where w_r is a fundamental reflection. In particular, $l(w_r) = 1$ and A is a parabolic subgroup. Then $AB = BA = A$, but by (4.6), we have $|A| \sim q|B| \sim \sqrt{|A||B|q}$.

Now we are ready to obtain a result on intersections of powers of A with parabolic subgroups. We use the quasi-random technique from [14, 45].

Theorem 5.3. *Let $\mathbf{G}(q)$ be a Chevalley group and let $P \subset \mathbf{G}(q)$ be a parabolic subgroup. Also, let $n \geq 1$ be a positive integer and let $X, Y_1, \dots, Y_n \subseteq \mathbf{G}(q)$ be nonempty sets such that $X \cap P = \emptyset$ and*

$$q\,|X|\,|P|^3\,d_{\min}^{n+2} \cdot \prod_{j=1}^{n} |Y_j| \geq 4|\mathbf{G}|^{n+4}\,. \tag{5.10}$$

Then $XY_1 \dots Y_n X \cap P \neq \emptyset$.

Proof. First of all, let us obtain a general upper bound for $\|A(\rho)\|_o$, where A is any subset of $\mathbf{G} = \mathbf{G}(q)$ and ρ is an arbitrary non-trivial representation of $\mathbf{G}$. Using formula (3.3) with $f = A$, we have

$$\|\widehat{A}(\rho)\|_o < \Big(\frac{|A|\,|\mathbf{G}|}{d_{\min}}\Big)^{1/2}\,. \tag{5.11}$$

Now if $XY_1 \dots Y_n X \cap P = \emptyset$, then $(PX)Y_1 \dots Y_n(XP) \cap P = \emptyset$. In terms of the representation theory, this can be rewritten as

$$0 = \frac{|PX||Y_1|\dots|Y_n||XP||P|}{|\mathbf{G}|} + \frac{1}{|\mathbf{G}|} \sum_{\rho \in \widehat{\mathbf{G}},\, \rho \neq 1} d_\rho \langle \widehat{PX}(\rho)\widehat{Y}_1(\rho)\dots\widehat{Y}_n(\rho)\widehat{XP}(\rho),\, \widehat{P}(\rho)\rangle_{\mathrm{HS}}.$$

Since $X \cap P = \emptyset$, by estimate (5.1) of Theorem 5.1 we have $|PX||XP| \geq 2^{-2}|X||P|q$. Using this fact and applying Lemma 3.1, combining with the bound (5.11) for the sets Y_j, we obtain

$$\begin{aligned}\frac{|PX||Y_1|\dots|Y_n||XP||P|}{|\mathbf{G}|} &< \|P\|_W \Big(\frac{|PX|\,|\mathbf{G}|}{d_{\min}}\Big)^{1/2} \Big(\frac{|XP|\,|\mathbf{G}|}{d_{\min}}\Big)^{1/2} \prod_{j=1}^{n} \Big(\frac{|Y_j|\,|\mathbf{G}|}{d_{\min}}\Big)^{1/2} \\ &\leq \Big(\frac{|\mathbf{G}|}{d_{\min}}\Big)^{(n+2)/2} \Big(|PX|\,|XP| \prod_{j=1}^{n} |Y_j|\Big)^{1/2}\end{aligned}$$

or, in other words,

$$q\,|X|\,|P|^3\,d_{\min}^{n+2} \cdot \prod_{j=1}^{n} |Y_j| < 4|\mathbf{G}|^{n+4}\,.$$

This completes the proof. ∎

Let P be a parabolic subgroup of size close to $|\mathbf{G}(q)|/d_{\min}$ and let $A \cap P = \emptyset$. Such parabolic subgroups exist, say, take $\mathbf{G}(q) = \mathrm{PSL}_n(q)$ (for precise results on $d_{\min}$, consult [31], page 419, or Table 4 in [15]). Then Theorem 5.3 says us that $A^{n+2} \cap P \neq \emptyset$, provided

$$|A| \geq \frac{C\,|\mathbf{G}(q)|}{d_{\min}} \cdot \Big(\frac{d_{\min}^2}{q}\Big)^{1/(n+1)}\,, \tag{5.12}$$

where $C > 0$ is an absolute constant.

The bound (5.12) is a natural barrier because any parabolic subgroup P of size $|P| \sim |\mathbf{G}(q)|/d_{\min}$ (recall that we just consider such subgroups) clearly does not generate the whole group (see also Example 5.6 below). Nevertheless, we do not want to generate the whole group but just to have a non-empty intersection of A^n with P for small n. In this case we will show that it is possible to relax the last condition (approximately by q). To do this, we consider the subgroup Γ generated by A. Then clearly $\emptyset \neq \Gamma \cap P =: Z < \mathbf{G}(q)$, but moreover, using Theorem 5.4 (for $\mathrm{PSL}_2(\mathbb{F}_p)$), Lemma 4.1, Theorem 5.3 and other tools, we show that $A^n \cap Z \neq \emptyset$ for a certain n and hence A^n intersects P. Indeed, one can show that the structure of Γ is simple, namely, for large A it must be another parabolic subgroup of $\mathbf{G}(q)$. Then Z contains a torus T and hence considering the representation theory of Γ (but not the whole group $\mathbf{G}(q)$) we derive that the orbit of A intersects T. Now if $\Gamma = \mathbf{G}(q)$, i.e., if A generates our group $\mathbf{G}(q)$, then one can apply some results on growth (e.g., Theorem 1.1) and this situation is even simpler.

In the particular case of $\mathrm{SL}_2(\mathbb{F}_q)$, we need a result which provides us some concrete bounds for the growth exponent, see Theorem 13 in [38] (which in turn develops the ideas of [22,43]). In the general case, we apply Lemma 4.1.

Theorem 5.4. *Let $q \geq 5$, let $A \subseteq \mathrm{SL}_2(\mathbb{F}_q)$ or $A \subseteq \mathrm{PSL}_2(\mathbb{F}_q)$ be a generating set, with $q^{2-\varepsilon} \leq |A| \leq q^{72/35}$, $0 < \varepsilon < 2/25$. Then $|AAA| \gg |A|^{25/24}$.*

More precisely, in Theorem 13 of [38] it was proved that, for any set A with $q^{2-\varepsilon} \leq |A| \leq q^{72/35}$, $0 < \varepsilon < 2/25$ and $K := |A^3|/|A|$, one has $K \gg \min\{|A|^{1/24}, p^{3/11}|A|^{-1/11}\}$. Thanks to our assumption $|A| \leq q^{72/35}$, we obtain that in any case $K \gg |A|^{1/24}$, as required.

Now we are ready to prove a result, which breaks the limit from (5.12). The absolute constants in (2) and (3) can be easily computed, but we do not specify them.

Theorem 5.5. *Let q be a sufficiently large odd non-square, let B be a Borel subgroup of $\mathrm{PSL}_2(\mathbb{F}_q)$, and let $A \subseteq \mathrm{PSL}_2(\mathbb{F}_q)$ be an arbitrary set. Then the following holds.*

(1) *If $|A| \geq q^{2-c}$, $c < 2/25$, then there is $n \leq \lceil \frac{24(1+c)}{2-25c} \rceil$ such that $A^{3n+2} \cap B \neq \emptyset$.*

(2) *If $|A| \geq q^{1+\delta}$, then there is $n \ll 1/\delta$ with $A^n \cap B \neq \emptyset$.*

(3) *In general, let $\mathbf{G}(q)$ be a Chevalley group and let $P \subset \mathbf{G}(q)$ be a parabolic subgroup. Suppose that $|A| \geq \mathcal{P}_1(\mathbf{G}(q))q^{-1+\delta}$. Then there exists n, $n \ll_r \delta^{-1}$, such that $A^n \cap P \neq \emptyset$.*

Proof. Let us start with (1). We can assume that $A \cap B = \emptyset$ because otherwise there is nothing to prove. Let $U := \{(1u|01) : u \in \mathbb{F}_q\}$. If A generates $\mathrm{PSL}_2(\mathbb{F}_q)$, then by Theorem 5.4 either $|A| \geq q^{72/35}$ or $|AAA| \gg |A|^{25/24} > q^{2+(2-25c)/24}$. In the last case, applying Theorem 5.3 with $P = B$, $X = A$, $Y_j = AAA$ and $d_{\min} = (q-1)/2$, we see that $A^{3n+2} \cap B \neq \emptyset$ provided $n \geq \lceil \frac{24(1+c)}{2-25c} \rceil$. If $|A| \geq q^{72/35}$, then Theorem 5.3 with $P = B$, $X = A$, $Y_j = A$ gives us even better upper bound for n.

Now suppose that A does not generate $\mathrm{PSL}_2(\mathbb{F}_q)$. By the well-known structure of the subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ see, e.g., Theorems 6.17 and 6.25 in [49], we have that A is a subset of a Borel subgroup and, by conjugating, we can assume that A is a subset of the standard Borel subgroup B_* of the upper-triangular matrices. Also, we have $B = g^{-1}B_*g$ for a certain $g \in \mathrm{PSL}_2(\mathbb{F}_q)$. We can assume that $g \notin B_*$ because otherwise $B_* = B$ and

hence $A = B_* \cap A = B \cap A \neq \emptyset$. One can carefully use inequalities (5.3), (5.4) of Theorem 5.1 and prove that $A^{-1}BA^{-1}$ has size at least $|\mathrm{PSL}_2(\mathbb{F}_q)| - (1 + o(1))|B|$. This is not enough for our purposes, and we consider A^n directly. We need the fact that the intersection of two Borel subgroups is a torus isomorphic to $\mathbb{F}_q^*$; in the case $\mathrm{PSL}_2(\mathbb{F}_q)$, this can be demonstrated rather easily. Indeed, by the Bruhat decomposition, the element g can be written as bwu, where $b \in B$, $u \in U$ and $w = (01|(-1)0)$. Then any element of $B = g^{-1}B_*g$ has the form

$$\begin{pmatrix} 1 & -v \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ \tilde{u} & \lambda^{-1} \end{pmatrix}\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda - v\tilde{u} & v(\lambda - \tilde{u}v) - v\lambda^{-1} \\ \tilde{u} & \tilde{u}v + \lambda^{-1} \end{pmatrix},$$

where the variables λ, $\tilde{u}$ run over $\mathbb{F}_q^*$, $\mathbb{F}_q$, respectively, and v is a fixed element. Since $A^n \subseteq B_*$, it follows that it is enough to find an element $(\lambda\ (v\lambda - v\lambda^{-1})|0\lambda^{-1}) \in B_* \cap B$ in A^n. The intersection $T := B_* \cap B$ is, clearly, a subgroup of size $q - 1$ (and T is, actually, a torus). Applying Corollary 3.2 (here we use the representation theory for B not $\mathrm{Aff}(\mathbb{F}_q)$), we obtain that $A^3 \cap T \neq \emptyset$, provided $|A| \gg q^{5/3}$.

Now let us prove that the condition $|A| \geq q^{1+\delta}$ implies that there is $n \ll 1/\delta$ such that $A^n \cap B \neq \emptyset$; in other words, let us obtain (2). Again, if A generates $\mathrm{PSL}_2(\mathbb{F}_q)$, then we consequently apply Theorem 1.1 (or just Theorem 5.4) and derive that $A^{3^{n+1}} = \mathrm{PSL}_2(\mathbb{F}_q)$ provided $(1 + c_*)^n(1 + \delta) > 3$, where $c_* > 0$ is an absolute constant. Hence $n = O(1)$ and in particular, $A^{3^{n+1}} \cap B \neq \emptyset$. Now if A does not generate $\mathrm{PSL}_2(\mathbb{F}_q)$, then by the structure of the subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$, we see that A is a subset of a Borel subgroup B_1. Put $T = B \cap B_1$. Then, as above, T is a torus, having size $q - 1$. Applying Corollary 3.2 again, we obtain $A^n \cap T \neq \emptyset$ provided $|A| > q^{1+2/n}$. Thus the restriction $n > 2/\delta$ is enough in this case.

It remains to prove the third part of our theorem. Again we can assume that $A \subseteq \Gamma \leq \mathbf{G}(q)$, $\Gamma \neq \mathbf{G}(q)$, because otherwise we consequently apply Theorem 1.1 to generate the whole $\mathbf{G}(q)$. By our assumption and Lemma 4.1, we have for sufficiently large q,

$$|\Gamma| \geq |A| \geq \mathcal{P}_1(\mathbf{G}(q))q^{-1+\delta} \gg \mathcal{P}(\mathbf{G}(q)),$$

and hence our subgroup Γ is a parabolic subgroup,

$$|\Gamma| \leq \mathcal{P}_1(\mathbf{G}(q)).$$

Recall that the intersection of two Borel subgroups contains a maximal torus of $\mathbf{G}(q)$. Indeed, by the Bruhat decomposition we have $B := gB_*g^{-1} = uwB_*w^{-1}u^{-1}$, where $u \in U$, $w \in W$ and hence $uHu^{-1} \subseteq B_* \cap B$ because $w^{-1}Hw = H \subseteq B_*$. In particular, the subgroup $P \cap \Gamma$ contains a torus T. Applying Lemma 3.3 for the group Γ, as well as Lemma 4.4, we see that $A^n \cap T \neq \emptyset$ if, for a sufficiently large constant C,

$$|A| \geq \frac{C\,\mathcal{P}_1(\mathbf{G}(q))}{q} \cdot \Big(\frac{\mathcal{P}_1(\mathbf{G}(q))}{|T|}\Big)^{2/n}. \tag{5.13}$$

To see this, one can use (3.7) replacing $|\Gamma|$ by $|T|$ and $|A|q$ by $2|A|\mathcal{P}_1(\mathbf{G}(q))/(q - 1)$ thanks to the first inequality from (3.6). Substituting, we get (5.13). Finally, by assumption, $|A| \geq \mathcal{P}_1(\mathbf{G}(q))q^{-1+\delta}$, and hence it is enough to choose $n \geq C(r)\delta^{-1}$ for a sufficiently large constant $C(r)$. This completes the proof. ∎

Example 5.6. Let B^+, B^- be the standard Borel subgroups of the upper/lower-triangular matrices from $\mathrm{PSL}_2(\mathbb{F}_p)$ and let $p \equiv -1 \pmod 4$. Also, let A be the set of all matrices $\subseteq B^+ \setminus B^-$ in which all entries are quadratic residues. It is easy to check that $|A| \gg p^2$. Further, one can see that $A \cap B^-$ and $A^2 \cap B^-$ are empty. It means that in Theorem 5.5 we need at least three multiplications even for sets A with $|A| \gg p^2$.

Remark 5.7. As the reviewer pointed out, the problem of finding n such that $A^n \cap P \neq \emptyset$, with P being a parabolic subgroup (of maximal size, say) can be treated as follows. Consider the permutation character χ of the canonical permutation representation $\rho\colon \mathbf{G} \to \mathbf{G}/P$ and the canonical action on the right cosets of P. Our task is to find $x \in A^n$ such that $\chi(x) \neq 0$. One can use the representation theory in the spirit of [3], Lemmas 3 and 4, to calculate L_2-norm of the character; but unfortunately, this way one can not gain the saving of size q, see Theorem 5.5. Nevertheless, it is an interesting new insight to the problem.

6. Two applications to Zaremba's conjecture

Using inequality (5.1) of Theorem 5.1, combining with Theorem 5.3, and applying the method from [38], one can decrease the constant 30 in Theorem 1.4 to 24. We go further, using the specifics of our problem and obtain Theorem 1.5 from the introduction. The results of this section can be considered as an "effective" form of strong approximation (see the definition in [7]). Namely, we answer in a particular case to the following question: given a semigroup from $\mathrm{SL}_2(\mathbb{Z})$) having strong approximation, how far (in the Archimedean norm) does one need to go in the semigroup to find a particular element modulo p?

Let M be a positive integer. Denote by $F_M(Q)$ the set of all *rational* numbers u/v, $(u,v)=1$, from $[0,1]$ with all partial quotients in (1.2) not exceeding M and with $v \le Q$:

$$F_M(Q) = \left\{ \frac{u}{v} = [0; b_1, \dots, b_s] \,:\, (u,v)=1, 0 \le u \le v \le Q,\, b_1, \dots, b_s \le M \right\}.$$

In other words, all partial quotients of $u/v \in F_M(Q)$ are bounded by the parameter M. At the end of our proof we will choose M to be a large but fixed number (in particular, M does not depend on all other parameters of this section). Further, by F_M we denote the set of all *irrational* numbers from $[0,1]$ with partial quotients less than or equal to M. From [19], Section 7, equation (7.11), we know that the Hausdorff dimension $w_M := \mathrm{HD}(F_M)$ of the set F_M satisfies

$$w_M = 1 - \frac{6}{\pi^2}\frac{1}{M} - \frac{72}{\pi^4}\frac{\log M}{M^2} + O\Big(\frac{1}{M^2}\Big), \quad M \to \infty.$$

Here it will be enough the simpler result from Theorem 1 in [18] (or see previous results in [17]), which states that

$$1 - w_M \sim 1/M \tag{6.1}$$

with some absolute constants in the sign $\sim$. Explicit estimates for dimensions of F_M for certain values of M can be found in [24, 25] and in other papers. For example (see p. 15 or Table on p. 16 in [25]),

$$w_2 = 0.531280506277205141624468 6\cdots > 1/2 \tag{6.2}$$

In Theorem 3 of [18], Hensley gives the bound

$$|F_M(Q)| \sim_M Q^{2w_M}. \tag{6.3}$$

More generally (see [21]), let $\mathcal{A} \subset \mathbb{N}$ be a finite set with at least two points and let $F_{\mathcal{A}}$ be the set of all irrational numbers such that $b_j \in \mathcal{A}$ (previously, $\mathcal{A} = \{1, \dots, M\}$). Then it is known that for the corresponding finite set $F_{\mathcal{A}}(Q)$, formula (6.3) holds with w_M replaced by $w_{\mathcal{A}} := \mathrm{HD}(F_{\mathcal{A}})$ (the constants there depend on $\mathcal{A}$ of course). The Hausdorff dimension $w_{\mathcal{A}}$ of the set $F_{\mathcal{A}}$ is known to exist and satisfies $0 < w_{\mathcal{A}} < 1$.

Let us make the first steps towards the proof of Theorem 1.5. Foremost, we associate a set of matrices from $\mathbf{G} = \mathrm{PSL}_2(\mathbb{F}_p)$ with the continued fractions. Here and below, p is a sufficiently large prime number (in particular, p is an odd integer). We begin with the set of the following products:

$$\begin{pmatrix} 0 & 1 \\ 1 & b_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & b_s \end{pmatrix} = \begin{pmatrix} p_{s-1} & p_s \\ q_{s-1} & q_s \end{pmatrix}, \tag{6.4}$$

where $p_s/q_s = [0; b_1, \dots, b_s]$ and $p_{s-1}/q_{s-1} = [0; b_1, \dots, b_{s-1}]$. Clearly, the determinant of any matrix from (6.4) is $p_{s-1}q_s - p_s q_{s-1} = (-1)^s$. Let $Q = p - 1$, $Q_1 \le Q$ and consider the set $F_M(Q_1)$ with a fixed integer $M \ge 2$. Any $u/v \in F_M(Q_1)$ corresponds to a matrix from $\mathrm{GL}_2(\mathbb{Z})$) of the form (6.4) with $b_j \le M$ by the rule $u/v = p_s/q_s$. By the uniqueness of the representation of a number as a continued fraction this correspondence is one-to-one. The set $F_M(Q_1)$ splits into ratios with even s and with odd s; in other words, $F_M(Q_1) = F_M^{\mathrm{even}}(Q_1) \bigsqcup F_M^{\mathrm{odd}}(Q_1)$. Let $A(Q_1)$ be the set of all matrices from (6.4) with even s. Since s is even, we have $A(Q_1) \subset \mathrm{PSL}_2(\mathbb{Z}))$, and because $Q_1 \le p - 1$, we can think of $A(Q_1)$ as about a subset of $\mathbf{G}$. It is easy to see from (6.3) that $|A(Q_1)| \gg_M Q_1^{2w_M}$. Indeed, it is obvious if $|F_M^{\mathrm{even}}(Q_1/(M+1))| \ge |F_M(Q_1)|/2 \gg_M Q_1^{2w_M}$, but if not, then $|F_M^{\mathrm{odd}}(Q_1/(M+1))| \ge |F_M(Q_1)|/2 \gg_M Q_1^{2w_M}$ and multiplying by $(01|1b)$, $1 \le b \le M$, we derive $|F_M^{\mathrm{even}}(Q_1)| \ge M|F_M^{\mathrm{odd}}(Q_1/(M+1))| \gg_M Q_1^{2w_M}$. Thus anyway $|A(Q_1)| = |F_M^{\mathrm{even}}(Q_1)| \gg_M Q_1^{2w_M}$ and $A(Q_1) \in \mathbf{G}$. Denote $A(Q)$ by A.

Now let B be the standard Borel subgroup of $\mathbf{G}$, i.e., the set of all upper-triangular matrices. It is easy to check that if for a certain n one has $A^n \cap B \ne \emptyset$ (the multiplication is considered modulo p), then any $g := (p_{s-1}p_s|q_{s-1}q_s) \in A^n \cap B$ has the form (6.4) and $q_{s-1} = q_{s-1}(g)$ equals zero modulo p. In other words, there is $u/v \in F_M((2p)^n)$ such that $v \equiv 0 \pmod p$. Actually, if we find any number from $p_s, q_s, p_{s-1}, q_{s-1}$ that equals zero modulo p, then we can do the same, see [20] (but we do not need this fact). Briefly, we consider A^n as a matrix of $\mathrm{PSL}_2(\mathbb{Z}))$ and after that taking a projection modulo p, we want to say something about the components of the projection. This is the spirit of the affine linear sieve, see [7].

The strategy of the proof of Theorem 1.5 is the following. Our task is to find the smallest n such that $A^n \cap B \ne \emptyset$. In Lemmas 6.1 and 6.3, as well as in other steps of the proof from Subsection 6.1, we will show that the set A is uniformly distributed in several senses, and the strongest sense is that for all non-trivial unitary representations ρ, one has $\|\widehat{A}\|_o \le |A|^{1-c}$, where $c > 0$ is an absolute constant. After that it is possible to use the methods of the previous sections (e.g., Theorem 5.5) to show that indeed $A^n \cap B \ne \emptyset$. This question about the intersection the orbit of A with the standard Borel subgroup B

motivates us to study growth of sets relatively to parabolic subgroups. Lemma 6.1 is rather general and it shows that A does not correlate with all Borel subgroups. Combining this lemma and some further combinatorial tools, we obtain Theorem 1.5 with constant 3. Lemma 6.3 uses the specifics of the set A more intensively, and it allows us to decrease the constant to $1+\varepsilon$.

Lemma 6.1. *We have*

$$\sigma_B(A,A^{-1}) \le p|A| \quad \text{and} \quad \sigma_B(A^{-1},A) \le Mp|A|\,.$$

Moreover,

$$\max_{g\in\mathbf{G}}\{|A\cap gB|,|A\cap Bg|\} \le Mp\,, \tag{6.5}$$

$$\max_{g,h\in\mathbf{G}} |A\cap gBh| \ll_M |A|\cdot p^{(1-2w_M)/4+o(1)}\,. \tag{6.6}$$

Proof. Let us begin with the estimation of $\sigma_B(A,A^{-1})$. We see that the product

$$\begin{pmatrix} p_{s-1} & p_s \\ q_{s-1} & q_s \end{pmatrix}\begin{pmatrix} q'_t & -p'_t \\ -q'_{t-1} & p'_{t-1} \end{pmatrix} \in B$$

if and only if $q'_t q_{s-1} \equiv q_s q'_{t-1} \pmod p$. It is well known that $q_s/q_{s-1}=[b_s;b_{s-1},\dots,b_1]$ and hence the number of pairs (q_{s-1},q_s) is at most $|A|$. Further, fixing q'_{t-1} (at most p choices), as well as a pair (q_{s-1},q_s) ($|A|$ choices), we find q'_t uniquely modulo p and hence we find q'_t because $q'_t \le p$. Thus $\sigma_B(A,A^{-1}) \le p|A|$. The argument showing that $\sigma_B(A^{-1},A) \le Mp|A|$ is even simpler because in this case we have the equation $p'_{t-1}q_{s-1} \equiv p_{s-1}q'_{t-1} \pmod p$ and any triple $(p_{s-1},q_{s-1},q'_{t-1})$ determines p'_{t-1}. It remains to notice that we can reconstruct (p_s,q_s) from (p_{s-1},q_{s-1}) in at most M ways. The bound (6.5) can be obtained exactly in the same way.

Finally, to get (6.6) we see that the inclusion

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} p_{s-1} & p_s \\ q_{s-1} & q_s \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in B \tag{6.7}$$

gives us

$$a(\gamma p_{s-1}+\delta q_{s-1}) \equiv -c(\gamma p_s+\delta q_s) \pmod p\,. \tag{6.8}$$

We can assume that $a,c\neq 0$ because this case was considered above, and the same situation for $\gamma=0$. If $\delta=0$, then $ap_{s-1}\equiv -cp_s \pmod p$ and fixing p_s we find p_{s-1} uniquely. But $p_s/p_{s-1}=[b_s;b_{s-1},\dots,b_2]$ and we determine the whole matrix, choosing b_1 in at most M ways. Thus suppose that all coefficients in (6.8) do not vanish. Dividing by $-c\gamma$, writing $\omega=a/c$ and redefining $\delta=-\delta/\gamma$, we obtain

$$\delta(q_s+\omega q_{s-1}) \equiv p_s+\omega p_{s-1} \pmod p\,. \tag{6.9}$$

Equation (6.9) can be interpreted easily: any Borel subgroup fixes a point (the standard Borel subgroup fixes ∞) and hence the inclusion (6.7) says that our set A transfers ω to δ. In other terms, the identity (6.9) says that the tuples $(q_s,q_{s-1},p_s,p_{s-1})$ belong to

a hyperspace with normal vector $(\delta, \delta\omega, -1, -\omega)$, and hence for some other solutions $(q'_s, q'_{s-1}, p'_s, p'_{s-1})$, $(q''_s, q''_{s-1}, p''_s, p''_{s-1})$, $(q'''_s, q'''_{s-1}, p'''_s, p'''_{s-1})$ of (6.9), we get

$$\begin{vmatrix} q_s & q_{s-1} & p_s & p_{s-1} \\ q'_s & q'_{s-1} & p'_s & p'_{s-1} \\ q''_s & q''_{s-1} & p''_s & p''_{s-1} \\ q'''_s & q'''_{s-1} & p'''_s & p'''_{s-1} \end{vmatrix} \equiv 0 \pmod{p}. \tag{6.10}$$

Now consider the set $\tilde{A} \subset A$, which is constructed exactly as A but with a smaller Q, which equals $2^{-5}Q^{1/k}$ (in the proof of Lemma 6.1, we will take $k = 4$). In other words, let $\tilde{A} = A(2^{-5}Q^{1/k})$. Our first task is to prove that, for any $k \geq 4$,

$$\max_{g,h \in \mathbf{G}} |\tilde{A} \cap gBh| \ll_M p^{1/k+o(1)}. \tag{6.11}$$

Clearly, $|\tilde{A}| \sim |A|^{1/k} \sim p^{2w_M/k}$, and hence (6.11) would give us an almost square-root saving as M tends to ∞. If we solve equation (6.10) with elements from $\tilde{A}$, then we arrive to an equation

$$Xq_s + Yq_{s-1} + Zp_s + Wp_{s-1} \equiv 0 \pmod{p}, \tag{6.12}$$

where $|X|, |Y|, |Z|, |W| < 2^{-2}p^{3/k}$ which is, actually, an equation in $\mathbb{Z}$. We can assume that not all integer coefficients X, Y, Z, W (these coefficients are some determinants of matrix from (6.10)) vanish because otherwise we obtain a similar equation with a smaller number of variables. Without loss of generality, assume that $X \neq 0$, and using (6.12) as well as the identity $q_s p_{s-1} - p_s q_{s-1} = (-1)^s = 1$, we derive

$$q_{s-1}p_s X = -p_{s-1}(Yq_{s-1} + Zp_s + Wp_{s-1}) - X$$

or, in other words,

$$(Xq_{s-1} + Zp_{s-1})(Xp_s + Yp_{s-1}) = YZp_{s-1}^2 - X(Wp_{s-1}^2 + 1) := f(p_{s-1}). \tag{6.13}$$

Fix $p_{s-1} < 2^{-5}p^{1/k}$ and suppose that $f(p_{s-1}) \neq 0$. Then the number of the solutions to equation (6.13) can be estimated in terms of the divisor function as $p^{o(1)}$. Further, if we know (q_{s-1}, p_s, p_{s-1}), then we determine q_s via (6.12) and hence the whole matrix from A. Now in the case $f(p_{s-1}) = 0$, we see that there are at most two choices for p_{s-1}, and fixing $q_s \leq 2^{-5}p^{1/k}$, we find the remaining variables using formulae (6.12), (6.13). Thus we have obtained (6.11).

To derive (6.6) from (6.11), notice that $A \subseteq \tilde{A}X$, where X is $A(2^5(M+1)Q^{1-1/k})$. Then, using (6.11), we get for any $g, h \in \mathbf{G}$ that

$$\begin{aligned} |A \cap gBh| &\leq \sum_{x \in X} |\tilde{A}x \cap gBh| \ll_M p^{1/k+o(1)}|X| \ll_M p^{2w_M + \frac{1}{k}(1-2w_M)+o(1)} \\ &\sim |A| \cdot p^{(1-2w_M)/4+o(1)}. \end{aligned}$$

This completes the proof of the lemma. ∎

Assume that $|A| \sim p^{2w_M} \gg p^{3/2}$. Using formula (5.3) of Theorem 5.1, as well as Lemma 6.1, we obtain an optimal lower bound for $|A^{-1}BA^{-1}|$.

Corollary 6.2. *Let $w_M > 3/4$. Then*

$$|ABA|, \ |A^{-1}BA^{-1}| \gg_M p^3.$$

6.1. Proof of Theorem 1.5

Now we are ready to prove Theorem 1.5. First of all we obtain the result with the constant equal to 5, that is, $q = O(p^{5+\varepsilon})$, and with the exact bounds (on M, say), and then subsequently refine the constant, using some additional arguments (which give worse dependence on M). The method of obtaining the constant 5 is more general and can be generalized further, see Theorem 6.5 below and the remarks after it. Once more, decreasing C in the condition $q = O(p^C)$ of Theorem 1.5, we increase the constant M). Let us say that Theorem 1.5 holds "with constant C" if it holds for $q = O(p^{C+\varepsilon})$ for any $\varepsilon > 0$.

Proof with $C = 5$. Take $n \geq 1$ and consider the equation $ay_1 \dots y_n a' = b$, where $y_j \in Y$, $a, a' \in A$, $b \in B$ and we will choose the set Y later. If this equation has no solutions, then the equation $sy_1 \dots y_n s' = b$, $s \in BA := S$, $s' \in AB := S'$ has no solutions either. Applying the second part of Lemma 6.1 (see formula (6.5)), we can estimate the energies $\mathsf{E}(A^{-1}, B)$, $\mathsf{E}(B, A)$ as $O(M|B||A|p)$. But then formula (2.1) gives us

$$|S|, |S'| \gg_M |A|p\,. \tag{6.14}$$

By arguments as those in the proof of Theorem 5.3, we obtain (recall that $d_{\min}(\mathrm{PSL}_2(\mathbb{F}_p)) \geq (p-1)/2$))

$$|Y|^n |S||S'||B| \ll |\mathbf{G}| \Big(\frac{|\mathbf{G}||S|}{p}\Big)^{1/2} \Big(\frac{|\mathbf{G}||S'|}{p}\Big)^{1/2} \Big(\frac{|\mathbf{G}||Y|}{p}\Big)^{n/2}$$

which implies

$$|Y|^n |A|^2 \ll p^{2n+4}\,. \tag{6.15}$$

It remains to choose Y. Let $K = |AAA|/|A|$ and $\tilde{K} = |AA|/|A|$. If $\tilde{K} \geq C_* p^6/|A|^3$ for a large constant C_*, then $|AA| \geq C_* p^6/|A|^2$ and this is a contradiction with inequality (6.15) for $Y = AA$, $n = 1$ and sufficiently large C_*. Suppose that $\tilde{K} \ll p^6/|A|^3$. In [38], inequality (31), using the Helfgott method [22,43], it was proved that

$$|A|^2 p^{-1} \ll_M K\tilde{K}|A| \cdot K^{2/3}|A|^{1/3}\,, \tag{6.16}$$

provided

$$|A| \gg p^{3/2} K^{5/2} \tag{6.17}$$

(the proof is standard: one should sum the Helfgott orbit-stabilizer inequality over the set of all possible traces $\mathrm{tr}(A)$ and use the trivial observation that $|\mathrm{tr}(A)| \geq |A|^2/p$, see details in [38]). Combining (6.16) with $\tilde{K} \ll p^6/|A|^3$, we get

$$K \gg_M \frac{|A|^{11/5}}{p^{21/5}}\,.$$

It is easy to check that if (6.17) does not hold, then we obtain even better lower bound for K. Applying inequality (6.15) with $Y = AAA$ and $n = 1$ we arrive to a contradiction, provided

$$|A| \geq C_* p^{2w_M} \gg p^{51/26}\,,$$

where $C_* > 0$ is a sufficiently large constant. In view of (6.1), the last condition can be satisfied taking M sufficiently large but fixed (not depending on p). Thus $A^5 \cap B \neq \emptyset$ and one can calculate the required M by formula (6.1).

Proof with $C = 3$. Let us obtain a non-trivial upper bound for the energy of A of the form $\mathsf{E}(A,A) \ll |A|^{3-c}$. In particular, in view of (2.1), the bound on the energy gives us $|AA| \gg |A|^{1+c}$ (indeed, by (2.2) one has $\mathsf{E}(A^{-1},A) \le \mathsf{E}(A,A)$). Suppose that, for a certain $T \ge 1$, $\mathsf{E}(A,A) = |A|^3/T$. By the non-commutative Balog–Szemerédi–Gowers theorem, see Theorem 32 in [39] or Proposition 2.43 and Corollary 2.46 in [50], there is $a \in A$ and $A_* \subseteq a^{-1}A$, $|A_*| \gg_T |A|$, such that $|A_*^3| \ll_T |A_*|$. Here the signs $\ll_T$ and $\gg_T$ mean that all dependences on T are polynomial. In view of the Helfgott growth result or Theorem 5.4, it is enough to show that A_* does not belong to a coset of a Borel subgroup. But this follows easily from the bound (6.6) of Lemma 6.1 (here we assume that $w_M > 1/2$) and from the lower bound for the size of A (and hence size of A_*). The Parseval identity (3.3) and formula (3.4) give us

$$\mathsf{E}(A,A) = \frac{1}{|\mathbf{G}|}\sum_{\rho\in\widehat{\mathbf{G}}} d_\rho \|\widehat{A}(\rho)\,\widehat{A^{-1}}(\rho)\|^2 = \frac{1}{|\mathbf{G}|}\sum_{\rho\in\widehat{\mathbf{G}}} d_\rho \|\widehat{A}(\rho)\,\widehat{A}(\rho)^*\|^2\,,$$

and hence by Lemma 4.4, we obtain

$$\max_{\rho\neq 1}\|\widehat{A}(\rho)\|_o^4 \le \sum_\rho \|\widehat{A}(\rho)\|_o^4 \ll \mathsf{E}(A,A)\cdot|\mathbf{G}|/p \ll |A|^{3-c}\,p^2\,. \tag{6.18}$$

Here $c > 0$ is an absolute constant and M is taken to be large enough. Hence we find a solution to the equation $sas' = b$ provided

$$\frac{|S||S'||A||B|}{|\mathbf{G}|} > \Big(\frac{|S||\mathbf{G}|}{p}\Big)^{1/2}\Big(\frac{|S'||\mathbf{G}|}{p}\Big)^{1/2}\|\widehat{A}\|_o\,. \tag{6.19}$$

Using (6.14) and the inequality

$$\max_{\rho\neq 1}\|\widehat{A}(\rho)\|_o \ll (|A|^{3-c}\,p^2)^{1/4},$$

which follows from the inequality in (6.18), we see that we are done provided $|A| \ge C_*\,p^{10/(5+c)}$, where C_* is a sufficiently large constant. In view of (6.1), the last condition is satisfied taking sufficiently large $M = M(c)$.

Finally, we shall decrease the constant C to 2 and further to 1. To do this. we introduce a very important new set Λ (from the point of view of Diophantine approximations, this set corresponds to all approximations with denominator at most $\sqrt{p}$. Such approximations play a crucial role in Zaremba's conjecture, see, e.g., Lemma 17 in [37]). Let $\Lambda \subset A$ be $\Lambda = A(\sqrt{Q}/2)$. Clearly, $|\Lambda| \sim p^{w_M} \sim \sqrt{|A|}$ and $\Lambda^2 \subseteq A$.

Lemma 6.3. *Let $X \subseteq B$ be an arbitrary set. We have*

$$\mathsf{E}(\Lambda,X) = |\Lambda||X| \quad \textit{and} \quad \mathsf{E}(\Lambda^{-1},X) \le M^4|\Lambda||X|.$$

In particular,

$$|B\Lambda| = |B||\Lambda| \quad \textit{and} \quad |\Lambda B| \ge |B||\Lambda|/M^4.$$

Proof. As in the proof of Lemma 6.1, we see that $\Lambda\Lambda^{-1} \cap B \neq \emptyset$ if and only if $q'_t q_{s-1} \equiv q_s q'_{t-1} \pmod p$ (we use the notation from the lemma). Since $\Lambda = A(\sqrt{Q}/2)$, it follows that $q'_t q_{s-1} = q_s q'_{t-1}$. Obviously, $(q_{s-1}, q_s) = (q'_{t-1}, q'_t) = 1$ and hence $q_s = q'_t$, $q_{s-1} = q'_{t-1}$. After that we reconstruct both matrices and obtain $\mathsf{E}(\Lambda, X) = |\Lambda||X|$.

Similarly, $\Lambda^{-1}\Lambda \cap B \neq \emptyset$ if and only if $p'_{t-1} q_{s-1} \equiv p_{s-1} q'_{t-1} \pmod p$ and whence $p'_{t-1} q_{s-1} = p_{s-1} q'_{t-1}$. Again, $(q_{s-1}, p_{s-1}) = (q'_{t-1}, p'_{t-1}) = 1$ and hence $p_{s-1} = p'_{t-1}$, $q_{s-1} = q'_{t-1}$. After that we reconstruct both matrices in at most M^2 ways. Whence we obtain $\mathsf{E}(\Lambda, X) \leq M^4 |\Lambda||X|$. This completes the proof of the lemma. ∎

Proof with $C = 2$. We redefine S and S' as $B\Lambda$, ΛB, respectively, and use the calculations from (6.19). This gives a solution to the equation $sas' = b$ provided

$$\frac{|S||S'||A||B|}{|\mathbf{G}|} > \Big(\frac{|S||\mathbf{G}|}{p}\Big)^{1/2} \Big(\frac{|S'||\mathbf{G}|}{p}\Big)^{1/2} \|\widehat{A}\|_o \,, \tag{6.20}$$

and using $\|A\|_o \ll (|A|^{3-c} p^2)^{1/4}$ as well as $|S|, |S'| \geq |B||\Lambda|/M^4$, we see that we are done provided

$$|A| \geq C_* M^{8/(3+c)} p^{6/(3+c)},$$

where C_* is a sufficiently large constant. In view of (6.1), the last condition can be satisfied taking sufficiently large M. Thus we have obtained the integer constant 2, but it is easy to see that this quantity is, actually, $2 - \tilde{c}$, where the absolute constant $\tilde{c}$ depends on c. Indeed, just replace $\sqrt{p-1}$ in the definition of the set Λ to $p^{(1-\varepsilon)/2}$ for sufficiently small $\varepsilon = \varepsilon(c) > 0$ and repeat the calculations above.

Proof with $C = 1$. In this last step we take an integer parameter $k \sim 1/\varepsilon$, $k \geq 4$, and consider $\Lambda_k \subset A$, $\Lambda_k = A(2^{-k} Q^{1/k})$. Letting $\tilde{A} = \Lambda_k^k \subset A$, we have $|\tilde{A}| \sim_k |A|$ (more precisely, $|A| \geq |\tilde{A}| \geq \eta^k |A|$, where $\eta < 1$ is an absolute constant). In other words, A and $\tilde{A}$ have comparable sizes. We will show later that there is a power saving for the operator norm of $\widehat{\Lambda}_k(\rho)$ of the form

$$\|\widehat{\Lambda}_k\|_o \ll_k |\Lambda_k|^{1-c_*(k)}, \quad \text{for a certain } c_*(k) > 0.$$

Calculations in (6.20) for the equation $s\lambda_k s' = b$, $\lambda_k \in \Lambda_k$, give us a solution provided

$$\frac{|S||S'||\Lambda_k||B|}{|\mathbf{G}|} > \Big(\frac{|S||\mathbf{G}|}{p}\Big)^{1/2} \Big(\frac{|S'||\mathbf{G}|}{p}\Big)^{1/2} \|\widehat{\Lambda}_k\|_o \,.$$

Since $\|\widehat{\Lambda}_k\|_o \ll_k |\Lambda_k|^{1-c_*(k)}$, and $|S|, |S'| \geq |B||\Lambda|/M^4$, the last equation is satisfied provided

$$|A||\Lambda_k|^{2c_*(k)} \geq \exp(C_* k) M^4 p^2 \,,$$

where $C_* > 0$ is a sufficiently large constant. In view of (6.3), it is enough to have

$$p^{w_M + 2c_*(k) w_M/k} \geq \exp(C'_* k) M^2 p \,, \tag{6.21}$$

where $C_* > 0$ is another sufficiently large constant. Taking $M = M(\varepsilon)$, $M \geq \tilde{C} k/c_*(k)$ for sufficiently large constant $\tilde{C}$, and using (6.3) again, we get (6.21).

To demonstrate the required power saving for the operator norm of $\widehat{\Lambda}_k(\rho)$, we first recall that the inequality (6.11) of Lemma 6.1 holds for any $k \geq 4$. An analogue of Lemma 6.1 for the set Λ_k holds. Hence we have the uniform bound $|\Lambda_k \cap gBh| \ll_M p^{1/k+o(1)}$ for all $g, h \in \mathbf{G}$. By Theorems 6.17 and 6.25 in [49], all other maximal subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$ are dihedral subgroups Γ. We consider the intersection of Λ_k with Γ, namely, with the set

$$\Gamma = \Gamma_\varepsilon := \left\{ \begin{pmatrix} u & \varepsilon v \\ v & u \end{pmatrix} : u, v \in \mathbb{F}_p,\ u^2 - \varepsilon v^2 = 1 \right\},$$

where ε is a primitive root. Our task is to show that for $k \geq 4$ one has

$$|\Lambda_k \cap g\Gamma h| \ll p^{1/k} \quad \text{for all } g, h \in \mathbf{G}.$$

Actually, this was done in Lemma 21 of [37] with even a stronger bound for the intersection (actually, the size of intersection is $O(1)$), but we briefly repeat the main steps of the argument. Writing $g = (xy|zw)$ and $h = (XY|ZW)^{-1}$, we want to estimate the number of the solutions in $u, v, p_{s-1}, q_{s-1}, p_s, q_s$ to the equation

$$\begin{pmatrix} xu + yv & \varepsilon xv + yu \\ zu + wv & \varepsilon zv + wu \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} u & \varepsilon v \\ v & u \end{pmatrix} = \begin{pmatrix} p_{s-1} & p_s \\ q_{s-1} & q_s \end{pmatrix} \begin{pmatrix} X & Y \\ Z & W \end{pmatrix}$$
$$= \begin{pmatrix} p_{s-1}X + p_sZ & p_{s-1}Y + p_sW \\ q_{s-1}X + q_sZ & q_{s-1}Y + q_sW \end{pmatrix}$$

with $xw - yz = XW - YZ = 1$. It follows that

$$X = q_s(xu + yv) - p_s(zu + wv) = (q_s x - p_s z)u + (q_s y - p_s w)v = Au + Bv$$

and

$$Y = q_s(\varepsilon xv + yu) - p_s(\varepsilon zv + wu) = (q_s y - p_s w)u + (q_s \varepsilon x - p_s \varepsilon z)v = Cu + Dv.$$

From $xw - yz = 1$, one has $(A, B) \neq (0, 0)$ and $(C, D) \neq (0, 0)$. For concreteness, let us assume that $A \neq 0$, $C \neq 0$. Using the last equations as well as the identity $u^2 - \varepsilon v^2 = 1$ and multiplying it by $A^2 \neq 0$ and $C^2 \neq 0$, correspondingly, we get

$$\alpha v^2 + \beta v + \gamma := (B^2 - \varepsilon A^2)v^2 - 2BXv + X^2 - A^2 = 0, \tag{6.22}$$

and similarly,

$$\alpha_* v^2 + \beta_* v + \gamma_* := (D^2 - \varepsilon C^2)v^2 - 2DYv + Y^2 - C^2 = 0. \tag{6.23}$$

Since ε is a primitive root and hence, in particular, ε is not a square, it follows that the quadratic equations are non-trivial. In other words, $\alpha \neq 0$ and $\alpha_* \neq 0$ for any (p_s, q_s). We can assume that $v \neq 0$ because it gives at most two points in our intersection. Now if $v \neq 0$, then excluding v from (6.22), (6.23), we arrive to a relation between p_s and q_s, namely,

$$(\alpha\gamma_* - \alpha_*\gamma)^2 = (\beta\gamma_* - \beta_*\gamma)(\alpha\beta_* - \beta\alpha_*).$$

One can check that this relation is non-trivial. Indeed, the homogeneous part of degree 8 of the last equation is $((BC)^2-(DA)^2)^2$ and hence it is zero if and only if

$$\varepsilon(q_sx-p_sz)^2=-(q_sy-p_sw)^2.$$

It follows that

$$y^2+\varepsilon x^2=w^2+\varepsilon z^2=0 \quad \text{and} \quad -\varepsilon xz=yw$$

(otherwise, we have a non-trivial equation in q_s, p_s). It is easy to check using $xy-zw=1$ that this is impossible because ε is not a square. Hence the number of our solutions is at most $2^{-k}Q^{1/k}$, as required. It remains to use the Bourgain–Gamburd machine [6], which we formulate here in a convenient form, referring to the survey [47], Section 6, see Theorem 49 and Corollary 50.

Theorem 6.4. *Let* $\mathbf{G}$ *be a group such that there is an absolute constant* $c_*>0$ *with the property that for any generating set* $X\subseteq\mathbf{G}$ *one has*

$$|X^3|\geq\min\{|\mathbf{G}|,|X|^{1+c_*}\}.$$

Also, let $A\subseteq\mathbf{G}$ *be a set such that*

$$\max_{g\in\mathbf{G},\,\Gamma<\mathbf{G}}|A\cap g\Gamma|\leq|A|/K.$$

Suppose that $\min\{d_{\min}(\mathbf{G}),K\}\geq|\mathbf{G}|^{\delta}$ *for a certain* $\delta>0$. *Then there is* $\varepsilon(\delta)>0$ *such that, for any unitary representation* $\rho\neq 1$, *one has*

$$\|\widehat{A}(\rho)\|_o\leq|A|^{1-\varepsilon(\delta)}.$$

Applying Theorem 6.4 for $\mathbf{G}=\mathrm{PSL}_2(\mathbb{F}_p)$ and our set A, we obtain Theorem 1.5.

Using the second part of Theorem 5.5 and the arguments of the proof of the result above (avoid using of Lemma 6.1 and Lemma 6.3 which appeal to the specific structure of the set $\mathcal{A}$), we obtain the following.

Theorem 6.5. *Let* $\mathcal{A}\subset\mathbb{N}$ *be a finite set,* $|\mathcal{A}|\geq 2$, *such that* $\mathrm{HD}(F_{\mathcal{A}})>1/2+\delta$, *where* $\delta>0$. *There is an integer constant* $C_{\mathcal{A}}(\delta)$ *such that for any prime number* p *there exist some positive integers* q *and* a, *with* $q=O_{\mathcal{A}}(p^{C_{\mathcal{A}}(\delta)})$, $q\equiv 0\pmod p$, *and* $(a,q)=1$, *such that* a/q *has partial quotients belonging to* $\mathcal{A}$.

Sketch of the proof. Let $Q=p-1$. We use the notation from the beginning of this section and recall that for $w_{\mathcal{A}}:=\mathrm{HD}(F_{\mathcal{A}})$ one has $F_{\mathcal{A}}(Q)\sim_{\mathcal{A}}Q^{2w_{\mathcal{A}}}$. As usual, the uniqueness of the continued fraction expansion implies that any ratio $u/v\in F_{\mathcal{A}}(Q)$ corresponds to a matrix from $\mathrm{GL}_2(\mathbb{Z})$) of the form (6.4) with $b_j\in\mathcal{A}$ by the rule $u/v=p_s/q_s$, and this correspondence is one-to-one. As above, we consider matrices of the form (6.4) with $b_j\in\mathcal{A}$ and $q_s<p$. As we have seen, the set of matrices A from (6.4) belonging to $\mathrm{PSL}_2(\mathbb{Z})$) has size $\Omega(F_{\mathcal{A}}(Q))$ and hence $|A|\gg_{\mathcal{A}}p^{2w_{\mathcal{A}}}\gg_{\mathcal{A}}p^{1+2\delta}$. We know that the theorem is proved if one finds an integer n, depending on δ and $\mathcal{A}$, such that $A^n\cap B\neq\emptyset$. But this follows from the second part of Theorem 5.5.

It is interesting to note (see Section 1 in [8]) that the original Hensley conjecture fails for general alphabet because of some local (modular) obstructions. Nevertheless, our modular Theorem 6.5 holds.

Thanks to (6.2), we see, in particular, that Theorem 6.5 holds for $\mathcal{A} = \{1, 2\}$. This fact was previously obtained in [38] by a different approach (although one can check that now our new constant $C_{\mathcal{A}}(\delta)$ is better). As the reader can see from the proof, our method is rather general and we do not even need, actually, restrictions of the form $b_j \in \mathcal{A}$, and it is possible to consider other (say, Markov-type) conditions for the partial quotients (of course, we still need that the Hausdorff dimension of the corresponding Cantor set is greater than $1/2$).

Acknowledgements. We thank Nikolai Vavilov and Misha Rudnev for useful discussions, and Nikolay Moshchevitin for valuable discussions and encouragement. Also, we are deeply grateful to the reviewers for valuable suggestions, remarks and very careful reading of our paper.

Funding. This work is supported by the Russian Science Foundation under grant 19-11-00001.

References

[1] Alavi, S. H. and Burness, T. C.: Large subgroups of simple groups. *J. Algebra* **421** (2015), 187–233.

[2] Aschbacher, M.: On the maximal subgroups of the finite classical groups. *Invent. Math.* **76** (1984), no. 3, 469–514.

[3] Austin, T.: Ajtai–Szemerédi theorems over quasirandom groups. In *Recent trends in combinatorics*, pp. 453–484. IMA Vol. Math. Appl. 159, Springer, Cham, 2016.

[4] Babai, L. and Seress, Á.: On the diameter of permutation groups. *European J. Combin.* **13** (1992), no. 4, 231–243.

[5] Björner, A. and Brenti, F.: *Combinatorics of Coxeter groups*. Graduate Texts in Mathematics 231, Springer, New York, 2005.

[6] Bourgain, J. and Gamburd, A.: Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. *Ann. of Math. (2)* **167** (2008), no. 2, 625–642.

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

[8] Bourgain, J. and Kontorovich, A.: On Zaremba's conjecture. *Ann. of Math. (2)* **180** (2014), no. 1, 137–196.

[9] Breuillard, E.: *Lectures on approximate groups*. IHP, Paris, February-March, 2011. Available at: www.imo.universite-paris-saclay.fr/~breuilla/ClermontLectures.pdf.

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

[11] Carter, R. W.: Simple groups and simple Lie algebras. *Matematika* **10** (1966), no. 5, 3–47.

[12] Celniker, N.: Eigenvalue bounds and girths of graphs of finite, upper half-planes. *Pacific J. Math.* **166** (1994), no. 1, 1–21.

[13] Frobenius, G.: Über Gruppencharaktere. *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1896), 985–1021.

[14] Gowers, W. T.: Quasirandom groups. *Combin. Probab. Comput.* **17** (2008), no. 3, 363–387.

[15] Guest, S., Morris, J., Praeger, C., and Spiga, P.: On the maximum orders of elements of finite almost simple groups and primitive permutation groups. *Trans. Amer. Math. Soc.* **367** (2015), no. 11, 7665–7694.

[16] Hamidoune, Y. O.: Two inverse results. *Combinatorica* **33** (2013), no. 2, 217–230.

[17] Hensley, D.: The distribution of badly approximable numbers and continuants with bounded digits. In *Théorie des nombres* (*Quebec, PQ, 1987*), pp. 371–385. De Gruyter, Berlin, 1989.

[18] Hensley, D.: The distribution of badly approximable rationals and continuants with bounded digits II. *J. Number Theory* **34** (1990) no. 3, 293–334.

[19] Hensley, D.: Continued fraction Cantor sets, Hausdorff dimension, and functional analysis. *J. Number Theory* **40** (1992), no. 3, 336–358.

[20] Hensley, D.: The distribution mod n of fractions with bounded partial quotients. *Pacific J. Math.* **166** (1994), no. 1, 43–54.

[21] Hensley, D.: A polynomial time algorithm for the Hausdorff dimension of continued fraction Cantor sets. *J. Number Theory* **58** (1996), no. 1, 9–45.

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

[23] Helfgott, H.: Growth in groups: ideas and perspectives. *Bull. Amer. Math. Soc.* **52** (2015), no. 3, 357–413.

[24] Jenkinson, O.: On the density of Hausdorff dimensions of bounded type continued fraction sets: the Texan conjecture. *Stoch. Dyn.* **4** (2004), no. 1, 63–76.

[25] Jenkinson, O. and Pollicott, M.: Computing the dimension of dynamically defined sets: E_2 and bounded continued fractions. *Ergodic Theory Dynam. Systems* **21** (2001), no. 5, 1429–1445.

[26] King, O. H.: The subgroup structure of finite classical groups in terms of geometric configurations. In *Surveys in combinatorics 2005*, pp. 29–56. London Math. Soc. Lecture Note Ser. 327, Cambridge Univ. Press, Cambridge, 2005.

[27] Kleidman, P. B. and Liebeck, M. W.: *The subgroup structure of the finite classical groups*. London Math. Soc. Lecture Note Series 129, Cambridge University Press, Cambridge, 1990.

[28] Kleidman, P. B. and Wilson, R. A.: The maximal subgroups of $E_6(2)$ and $\mathrm{Aut}(E_6(2))$. *Proc. London Math. Soc. (2)* **60** (1990), no. 2, 266–294.

[29] Kontorovich, A.: From Apollonius to Zaremba: local-global phenomena in thin orbits. *Bull. Amer. Math. Soc.* **50** (2013), no. 2, 187–228.

[30] Korobov, N. M.: *Number-theoretical methods in numerical analysis*. (Russian). Moscow, 1963.

[31] Landazuri, V. and Seitz, G. M.: On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443.

[32] Liebeck, M. W.: On the orders of maximal subgroups of the finite classical groups. *Proc. London Math. Soc. (3)* **50** (1985), no. 3, 426–446.

[33] Liebeck, M. W. and Saxl, J.: On the orders of maximal subgroups of the finite exceptional groups of Lie type. *Proc. London Math. Soc. (3)* **55** (1987), no. 2, 299–330.

[34] Magee, M., Oh, H. and Winter, D.: Expanding maps and continued fractions. Preprint 2015, arXiv: 1412.4284.

[35] Magee, M., Oh, H. and Winter, D.: Uniform congruence counting for Schottky semigroups in $\mathrm{SL}(\mathbb{Z})$. *J. Reine Angew. Math.* **753** (2019), 89–135.

[36] Mitchell, H. H.: Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.* **12** (1911), no. 2, 207–242.

[37] Moshchevitin, N. G., Murphy, B. and Shkredov, I. D.: Popular products and continued fractions. *Israel J. Math.* **238** (2020), no. 2, 807–835.

[38] Moshchevitin, N. G. and Shkredov, I. D.: On a modular form of Zaremba's conjecture. *Pacific J. Math.* **309** (2020), no. 1, 195–211.

[39] Murphy, B.: Upper and lower bounds for rich lines in grids. *Amer. J. Math.* **143** (2021), no. 2, 577–611.

[40] Mwene, B.: On the subgroups of the group $\mathrm{PSL}_4(2m)$. *J. Algebra* **41** (1976), 79–107.

[41] Naimark, M. A.: *Theory of group representations*. Fizmatlit., Moscow, 2010.

[42] Pyber, L. and Szabó, E.: Growth in finite simple groups of Lie type. *J. Amer. Math. Soc.* **29** (2016), no. 1, 95–146.

[43] Rudnev, M. and Shkredov, I. D.: On growth rate in $\mathrm{SL}_2(\mathbb{F}_p)$, the affine group and sum-product type implications. *Mathematika* **68** (2022), no. 3, 738–783.

[44] Rukavishnikova, M. G.: Probabilistic bound for the sum of partial quotients of fractions with a fixed denominator. *Chebyshevskii Sbornik* **7** (2006), 113–121.

[45] Sarnak, P. and Xue, X.: Bounds for multiplicities of automorphic representations. *Duke Math. J.* **64** (1991), no. 1, 207–227.

[46] Serre, J.-P.: *Représentations linéaires des groupes finis*. Collections Méthodes, Hermann, Paris, 1967.

[47] Shkredov, I. D.: Noncommutative methods in additive combinatorics and number theory. *Uspekhi Mat. Nauk* **76** (2021), no. 6 (462), 119–180.

[48] Steinberg, R. G.: *Lectures on Chevalley groups*. Yale University, New Haven, Conn., 1968.

[49] Suzuki, M.: *Group theory I*. Grundlehren der Mathematischen Wissenschaften 247, Springer-Verlag, Berlin-New York, 1982.

[50] Tao, T. and Vu, V.: *Additive combinatorics*. Cambridge Studies in Advanced Mathematics 105, Cambridge University Press, Cambridge, 2006.

[51] Wilson, R. A.: *The finite simple groups*. Graduate Texts in Mathematics 251, Springer-Verlag, London, 2009.

[52] Zaremba, S. K.: La méthode des "bons treillis" pour le calcul des intégrales multiples. In *Applications of number theory to numerical analysis* (*Proc. Sympos., Univ. Montreal, Montreal, Que., 1971*), pp. 39–119. Academic Press, New York, 1972.

Received February 23, 2021; revised February 10, 2022. Published online March 29, 2022.

Ilya D. Shkredov
Steklov Mathematical Institute, ul. Gubkina, 8, Moscow, Russia, 119991;
ilya.shkredov@gmail.com