On rapid generation of $SL_2(\mathbb{F}_q)$

Jeremy Chapman and Alex Iosevich

Abstract. We prove that if $A \subset \mathbb{F}_q \backslash \{0\}$ with $|A| > Cq^{\frac{5}{6}}$, then $|R(A) \cdot R(A)| \geq C'q^3$, where

$$R(A) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(\mathbb{F}_q) : a_{11}, a_{12}, a_{21} \in A \right\}.$$

The proof relies on a result, previously established by D. Hart and the author ([3]) which implies that if $|A|$ is much larger than $q^{\frac{3}{4}}$ then

$$|\{(a_{11}, a_{12}, a_{21}, a_{22}) \in A \times A \times A \times A : a_{11}a_{22} - a_{12}a_{21} = 1\}| = |A|^4 q^{-1}(1 + o(1)).$$

1. Introduction

Let $SL_2(\mathbb{F}_q)$ denote the set of two by two matrices with determinant one over the finite field with q elements.

Definition 1.1. Given $A \subset \mathbb{F}_q$, let

$$R(A) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(\mathbb{F}_q) : a_{11}, a_{12}, a_{21} \in A \right\}.$$

Observe that the size of $R(A)$ is exactly $|A|^3$. The purpose of this paper is to determine how large A needs to be to ensure that the product set

$$R(A) \cdot R(A) = \{M \cdot M' : M, M' \in R(A)\}$$

contains a positive proportion of all the elements of $SL_2(\mathbb{F}_q)$. This question is partly motivated by the following result due to Harald Helfgott ([2]). See his paper for further background on this problem and related references.

Theorem 1.2. *(Helfgott) Let p be a prime. Let E be a subset of $SL_2(\mathbb{Z}/p\mathbb{Z})$ not contained in any proper subgroup.*

- *Assume that $|E| < p^{3-\delta}$ for some fixed $\delta > 0$. Then*
$$|E \cdot E \cdot E| > c|E|^{1+\epsilon},$$
where $c > 0$ and $\epsilon > 0$ depend only on δ.

- *Assume that $|E| > p^{\delta}$ for some fixed $\delta > 0$. Then there is an integer $k > 0$, depending only on δ, such that every element of $SL_2(\mathbb{Z}/p\mathbb{Z})$ can be expressed as a product of at most k elements of $E \cup E^{-1}$.*

Our main result is the following.

THEOREM 1.3. *Let $A \subset \mathbb{F}_q \backslash \{0\}$ with $|A| \geq Cq^{\frac{5}{6}}$. Then there exists $C' > 0$ such that*

$$|R(A) \cdot R(A)| \geq C'|SL_2(\mathbb{F}_q)| \geq C''q^3. \tag{1.1}$$

REMARK 1.4. Observe that if $q = p^2$, then $\mathbb{F}_q$ contains $\mathbb{F}_p$ as a sub-field. Since $R(\mathbb{F}_p)$ is a sub-group of $SL_2(\mathbb{F}_q)$ we see that the threshold assumption on the size of A in Theorem 1.3 cannot be improved beyond $|A| \geq q^{\frac{1}{2}}$.

We shall make use of the following result due to D. Hart and A. Iosevich ([3]).

THEOREM 1.5. *Let $E \subset \mathbb{F}_q^d$, $d \geq 2$, and define*

$$\nu(t) = |\{(x, y) \in E \times E : x \cdot y \equiv x_1y_1 + \cdots + x_dy_d = t\}|.$$

Then

$$\nu(t) = |E|^2q^{-1} + \mathcal{D}(t),$$

where for every $t > 0$,

$$|\mathcal{D}(t)| < |E|q^{\frac{d-1}{2}}.$$

In particular, if $|E| > q^{\frac{d+1}{2}}$, then $\nu(t) > 0$ and as E grows beyond this threshold,

$$\nu(t) = |E|^2q^{-1}(1 + o(1)).$$

REMARK 1.6. The proof of Theorem 1.5 goes through unchanged if $x \cdot y$ is replaced by any non-degenerate bi-linear form $B(x, y)$. In particular, we can replace $x_1y_1 + x_2y_2$ by $x_1y_1 - x_2y_2$ in the case $d = 2$ and this is what we actually use in this paper. More precisely, we shall use the fact that if $E = A \times A$ and the size of A is much greater than $q^{\frac{3}{4}}$, then

$$|\{(a, b, c, d) \in A \times A \times A \times A : ad - bc = 1\}| = |A|^4q^{-1}(1 + o(1)). \tag{1.2}$$

1.1. Structure of the proof of the estimate (1.1). The basic idea behind the argument below is the following. Let $T \in SL_2(\mathbb{F}_q)$ and define

$$\nu(T) = |\{(S, S') \in R(A) \times R(A) : S \cdot S' = T\}.$$

We prove below that

$$\sqrt{var(\nu)} \leq C|A|^3q^{-\frac{1}{2}},$$

where variance is defined, in the usual way as

$$\mathbb{E}\left((\nu - \mathbb{E}(\nu))^2\right),$$

with the expectation defined, also in the usual way, as

$$\mathbb{E}(\nu) = |SL_2(\mathbb{F}_q)|^{-1} \sum_{T \in SL_2(\mathbb{F}_q)} \nu(T) = |A|^6|SL_2(\mathbb{F}_q)|^{-1} = |A|^6q^{-3}(1 + o(1)).$$

One can then check by a direct computation that $\sqrt{var(\nu)}$ is much smaller than $\mathbb{E}(\nu)$ if $|A| \geq Cq^{\frac{5}{6}}$, with C sufficiently large, and we conclude that in this regime, $\nu(T)$ is concentrated around its expected value $\mathbb{E}(\nu) = |A|^6q^{-3}(1 + o(1))$.

1.2. Fourier analysis used in this paper. We shall make use of the following basic formulas of Fourier analysis on $\mathbb{F}_q^d$. Let $f : \mathbb{F}_q^d \to \mathbb{C}$ and let χ denote a non-trivial additive character on $\mathbb{F}_q$. Define

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) f(x).$$

It is not difficult to check that

$$(Inversion)\ f(x) = \sum_{m \in \mathbb{F}_q^d} \chi(x \cdot m) \widehat{f}(m)$$

and

$$(Plancherel)\ \sum_{m \in \mathbb{F}_q^d} |\widehat{f}(m)|^2 = q^{-d} \sum_{x \in \mathbb{F}_q^d} |f(x)|^2.$$

2. Proof of Theorem 1.3 (estimate 1.1)

We are looking to solve the equation

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & \frac{1+a_{12}a_{21}}{a_{11}} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{21} \\ b_{12} & \frac{1+b_{12}b_{21}}{b_{11}} \end{pmatrix} = \begin{pmatrix} t & \alpha \\ \beta & \frac{1+\alpha\beta}{t} \end{pmatrix},$$

which leads to equations

$$a_{11}b_{11} + a_{12}b_{12} = t, \tag{2.1}$$

$$\frac{b_{21}}{b_{11}} t + \frac{a_{12}}{b_{11}} = \alpha$$

and

$$\frac{a_{21}}{a_{11}} t + \frac{b_{12}}{a_{11}} = \beta.$$

Let D_t denote the characteristic function of the set

$$\{(a_{11}, b_{11}, a_{12}, b_{12}) \in A \times A \times A \times A : a_{11}b_{11} + a_{12}b_{12} = t\}$$

and let $E = A \times A$. Then the number of six-tuplets satisfying the equations (2.1) above equals

$$\nu(t, \alpha, \beta) = \frac{1}{q^2} \sum_{u,v} \sum_{a_{11}, b_{11}, a_{12}, b_{12}, a_{21}, b_{21}} D_t(a_{11}, b_{11}, a_{12}, b_{12}) E(a_{21}, b_{21}) \chi(u(b_{21}t + a_{12} - \alpha b_{11})) \chi(v(a_{21}t + b_{12} - \beta a_{11})$$

$$= q^{-2}|D_t||E| + q^4 \sum_{\mathbb{F}_q^2 \setminus \{(0,0)\}} \widehat{D}_t(\beta v, \alpha u, -u, -v)\widehat{E}(tv, tu)$$
$$= \nu_0(t,\alpha,\beta) + \nu_{main}(t,\alpha,\beta).$$

By (1.2),

$$\nu_0(t,\alpha,\beta) = q^{-3}|A|^6(1+o(1)),$$

which implies that

$$\sum_{t,\alpha,\beta} \nu_0^2(t,\alpha,\beta) = q^{-3}|A|^{12}(1+o(1)).$$

We now estimate $\sum_{t,\alpha,\beta} \nu_{main}^2(t,\alpha,\beta)$. By Cauchy-Schwartz and Plancherel,

$$\nu_{main}^2(t,\alpha,\beta) \leq q^8 \sum_{u,v} \left|\widehat{D}_t(\beta v, \alpha u, -u, -v)\right|^2 \cdot \sum_{u,v} \left|\widehat{E}(tv,tu)\right|^2$$
$$\leq |E|q^6 \sum_{u,v} \left|\widehat{D}_t(\beta v, \alpha u, -u, -v)\right|^2.$$

Now,

$$|E|q^6 \sum_{\alpha,\beta}\sum_{u,v} \left|\widehat{D}_t(\beta v, \alpha u, -u, -v)\right|^2 = |E|q^6 q^{-4}|A|^4 q^{-1}(1+o(1))$$

as long as $|E|$ is much larger than $q^{\frac{3}{2}}$. It follows that

$$\sum_{t\neq 0,\alpha,\beta} \nu_{main}^2(t,\alpha,\beta) \leq |A|^6 q^2.$$

It follows that

$$\sum_{t,\alpha,\beta} \nu^2(t,\alpha,\beta) \leq C(|A|^{12}q^{-3} + |A|^6 q^2). \tag{2.2}$$

$$\left(|A|^6 - \sum_{\alpha,\beta} \nu(0,\alpha,\beta)\right)^2 = \left(\sum_{t\neq 0,\alpha,\beta} \nu(t,\alpha,\beta)\right)^2$$
$$\leq C|support(\nu)| \cdot (|A|^{12}q^{-3} + |A|^6 q^2)$$

in view of (2.2).

Suppose that we could show that

$$\sum_{\alpha,\beta} \nu(0,\alpha,\beta) \leq \frac{1}{2}|A|^6. \tag{2.3}$$

Then it would follow that

$$|support(\nu)| \gtrsim C \min\left\{q^3, \frac{|A|^6}{q^2}\right\}.$$

This expression is

$$\geq C|SL_2(\mathbb{F}_q)| = q^3(1+o(1))$$

if

$$|A| \geq Cq^{\frac{5}{6}},$$

as desired.

We are left to establish (2.3). Observe that if $t = 0$, then $\beta = -\alpha^{-1}$. Plugging this into (2.1) we see that this forces $a_{11} = -\alpha b_{12}$ and $a_{12} = \alpha b_{11}$ which implies that

$$\nu(0, \alpha, \beta) = \nu(0, \alpha, -\alpha^{-1}) \leq q^4,$$

which implies that

$$\sum_{\alpha,\beta} \nu(0, \alpha, \beta) = \sum_{\alpha} \nu(0, \alpha, -\alpha^{-1}) \leq q^5.$$

We have

$$q^5 \leq \frac{1}{2}|A|^6$$

if

$$|A| \geq Cq^{\frac{5}{6}},$$

which completes the proof.

3. Proof of Theorem 1.5

To prove Theorem 1.5, we start out by observing that

$$\nu(t) = \sum_{x,y \in E} q^{-1} \sum_{s \in \mathbb{F}_q} \chi(s(x \cdot y - t)),$$

where χ is a non-trivial additive character on $\mathbb{F}_q$. It follows that

$$\nu(t) = |E|^2 q^{-1} + \mathcal{D},$$

where

$$\mathcal{D} = \sum_{x,y \in E} q^{-1} \sum_{s \neq 0} \chi(s(x \cdot y - t)).$$

Viewing $\mathcal{D}$ as a sum in x, applying the Cauchy-Schwartz inequality and dominating the sum over $x \in E$ by the sum over $x \in \mathbb{F}_q^d$, we see that

$$\mathcal{D}^2 \leq |E| \sum_{x \in \mathbb{F}_q^d} q^{-2} \sum_{s,s' \neq 0} \sum_{y,y' \in E} \chi(sx \cdot y - s'x \cdot y')\chi(t(s' - s)).$$

Orthogonality in the x variable yields

$$= |E|q^{d-2} \sum_{\substack{sy = s'y' \\ s,s' \neq 0}} \chi(t(s' - s))E(y)E(y').$$

If $s \neq s'$ we may set $a = s/s', b = s'$ and obtain

$$|E|q^{d-2} \sum_{\substack{y \neq y' \\ ay = y' \\ a \neq 1, b}} \chi(tb(1 - a))E(y)E(y')$$

$$= -|E|q^{d-2} \sum_{y \neq y', a \neq 1} E(y)E(ay),$$

and the absolute value of this quantity is

$$\leq |E|q^{d-2} \sum_{y \in E} |E \cap l_y|$$

$$\leq |E|^2 q^{d-1},$$

since

$$|E \cap l_y| \leq q$$

by the virtue of the fact that each line contains exactly q points.

If $s = s'$ we get

$$|E| q^{d-2} \sum_{s,y} E(y) = |E|^2 q^{d-1}.$$

It follows that

$$\nu(t) = |E|^2 q^{-1} + \mathcal{D}(t),$$

where

$$\mathcal{D}^2(t) \leq -Q(t) + |E|^2 q^{d-1},$$

with

$$Q(t) \geq 0.$$

It follows that

$$\mathcal{D}^2(t) \leq |E|^2 q^{d-1},$$

so

$$|\mathcal{D}(t)| \leq |E| q^{\frac{d-1}{2}}. \tag{3.1}$$

We conclude that

$$\nu(t) = |E|^2 q^{-1} + \mathcal{D}(t)$$

with $|\mathcal{D}(t)|$ bounded as in (3.1).

This quantity is strictly positive if $|E| > q^{\frac{d+1}{2}}$ with a sufficiently large constant $C > 0$. This completes the proof of Theorem 1.5.

4. Remarks and questions

- The Fourier analysis used in the proof of both the first and second assertions of Theorem 1.3 is almost entirely formal as no hard estimates are used, even on the level of Gauss sums. This suggests that the result should be generalizable to a much wider setting.

- A natural analog of the second part of Theorem 1.3 is proved in [3] in all dimensions. Thus in principle there is a launching mechanism to attack the second part, though it is certainly more difficult technically.

- One of the consequences of the main result of this paper is to give a quantitative version of Helfgott's result (Theorem 1.2) for a class of relatively large subsets of $SL_2(\mathbb{F}_q)$. In analogy with the results in [1] it should be possible to address the question of obtaining explicit exponents for relatively small sets as well.

References

[1] M. Garaev, *An explicit sum-product estimate in* $\mathbb{F}_p$, (preprint), (2007). 6
[2] H. Helfgott, *Growth and generation in* $SL_2(Z/pZ)$, Ann. of Math. **167** (2008), 601-623. 1
[3] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, Contemporary Mathematics, (to appear), (2007). 1, 2, 6