Growth in Chevalley groups and Zaremba's conjecture

I. D. Shkredov

Steklov Mathematical Institute

Chevalley groups

Theorem (CFSG)

Let **G** be a finite simple group. Then **G** belongs to three infinite families

1) $\mathbb{Z}/p\mathbb{Z}$, p is a prime number
2) A_n, $n \geq 5$
3) "groups of Lie type" or
4) 27 sporadic groups

Groups of Lie type for us are *Chevalley groups* (more or less).

Classical groups: $\mathrm{PSL_n}(\mathbb{F}_q)$, $\mathrm{U_n}(\mathbb{F}_q)$, $\mathrm{PSp_n}(\mathbb{F}_q)$, $\mathrm{P\Omega_n^{\pm}}(\mathbb{F}_q)$.
Others: E_6, E_7, E_8, F_4, G_2 + Steinberg and Suzuki–Ree groups.

Example: $\mathrm{SL}_n(\mathbb{F}_q)$

The standard *Borel subgroup*

$$\begin{pmatrix} \lambda_1 & * & * \\ 0 & \lambda_2 & * \\ \dots & \dots & \dots \\ 0 & \dots 0 & \lambda_n \end{pmatrix}, \qquad \lambda_1 \dots \lambda_n = 1\,.$$

Parabolic subgroups = containing a Borel subgroup

$$\begin{pmatrix} C_1 & * & * \\ 0 & C_2 & * \\ \dots & \dots & \dots \\ 0 & \dots 0 & C_n \end{pmatrix}, \qquad C_1, \dots, C_n \quad \text{are square blocks.}$$

There are 2^{n-1} of parabolic subgroups, containing a Borel subgroup, $(n-1)$ is *rank* of $\mathrm{SL}_n(\mathbb{F}_q)$.

Growth in finite simple groups

Conjecture (Babai, 1992)

Let $\mathbf{G}$ be a finite simple group and $\langle A \rangle = \mathbf{G}$. Then there is $n \ll (\log |\mathbf{G}| / \log |A|)^C$ such that $A^n = \mathbf{G}$.

Theorem (Helfgott, Breuillard–Green–Tao, Pyber–Szabó)

Let $\mathbf{G}$ be a finite simple group of Lie type with rank r and $\langle A \rangle = \mathbf{G}$. Then either $A^3 = \mathbf{G}$ or

$$\left|A^3\right| > |A|^{1+c(r)}.$$

In particular, there is

$$n \ll (\log |\mathbf{G}| / \log |A|)^{C(r)}$$

such that $A^n = \mathbf{G}$.

Growth relatively to parabolic subgroups, I

What about $A^n \cap H$, $H \leq \mathbf{G}(q)$?
E.g., H is a parabolic subgroup?

Theorem (Landazuri–Seitz, 1974)

Let $\mathbf{G}(q)$ be a Chevalley group. Then the minimal dimension $d_{\min}(\mathbf{G}(q))$ of any non–trivial representation is

$$d_{\min}(\mathbf{G}(q)) \gg q^r \, .$$

In other words Chevalley groups are *quasi–random* in the sense of Gowers (Sarnak–Xue, Huxley).

$d_{\min}(\mathbf{G}(q)) \gg q^r \sim |\mathbf{G}(q)|/|P|$, where P is a maximal (by size) parabolic subgroup.

Growth relatively to parabolic subgroups, II

Corollary

Let $A \subset \mathbf{G}(q)$ and for $\delta > 0$ one has

$$|A| \geq |\mathbf{G}(q)| q^{-r+\delta}.$$

Then $A^n = \mathbf{G}(q)$ for $n \ll_r \delta^{-1}$.

Theorem (S., 2020)

Let q be an odd number, $P \subset \mathbf{G}(q)$ be a parabolic subgroup. Suppose that for a $\delta > 0$

$$|A| \geq |\mathbf{G}(q)| q^{-r-1+\delta}.$$

Then $A^n \cap P \neq \emptyset$ for $n \ll_r \delta^{-1}$.

Growth relatively to parabolic subgroups, III

If $A = XP$, $X \subset \mathbf{G}(q)$, then $AP = A$.
If $A = PY$, then $PA = A$.

Theorem (S., 2020)

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

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

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

Both growth results concerning parabolic subgroups are important in $\mathrm{SL}_2(\mathbb{F}_p)$ and hence for the continued fractions.

Zaremba's conjecture

Let $\alpha \in [0,1]$. The continued fraction expansion for α is

$$\alpha = \cfrac{1}{c_1 + \cfrac{1}{c_2 + \dots}} = [c_1, c_2, \dots], \qquad c_j \in \mathbb{N}.$$

Conjecture (Zaremba, 1972)

Let p be a prime number. Then there exists $1 \le a \le p-1$ such that

$$\frac{a}{p} = [c_1, c_2, \dots, c_s]$$

has all $c_j \le \mathcal{M} = 5$.

Known for $\mathcal{M} = \log p$, the prime $p \to q \in \mathbb{N}$, $(a,q) = 1$: Korobov, Hensley, Niederreiter, Bourgain–Kontorovich, Frolenkov–Kan, David–Shapira, Huang, Magge–Oh–Winter, ...

Zaremba's conjecture for a.e. p

Theorem (Bourgain–Kontorovich, 2011, 2014)

The number of $q \in \{1, \dots, N\}$ such that Zaremba's conjecture holds with $\mathcal{M}$ for this q is

$$N - O(N^{1-c/\log\log N}),$$

where $c = c(\mathcal{M}) > 0$.
Further if $\mathcal{M} = 50$, then there is a positive proportion of such q.

Decreasing $\mathcal{M}$: Frolenkov–Kan, Kan, Huang, Magge–Oh–Winter.

Theorem (Kan, 2016)

If $\mathcal{M} = 4$, then for all but $o(N)$ numbers $q \in \{1, \dots, N\}$ Zaremba's conjecture takes place.

Theorem (Hensley, 1989–1992)

For any M

$$w_M := \mathcal{HD}\left(\{\alpha = [c_1, c_2, \dots] \in [0,1] \ : \ \forall c_j \le M\}\right) =$$

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

$$w_2 = 0.531280506277205141624468 6\ldots > \frac{1}{2}$$

Thus $w_M = 1 - O(1/M)$, $M \to \infty$ (Khinchin).

$$w_M = \mathcal{HD}\left(\{\alpha = [c_1, c_2, \dots] \in [0,1] \ : \ \forall c_j \le M\}\right) =$$

$$= \mathcal{HD}(\mathcal{F}_M),$$

where $\mathcal{F}_M$ corresponds to the alphabet $\mathcal{A} = \{1, 2, \dots, M\}$.

Conjecture (Hensley, 1996)

Let $\mathcal{A} \subset \mathbb{N}$ be an alphabet and

$$\mathcal{HD}(\mathcal{F}_\mathcal{A}) > 1/2\,.$$

Then Zaremba's conjecture takes place: $\forall p \ge p_0$ there is a s.t.

$$\frac{a}{p} = [c_1, c_2, \dots, c_s]\,, \qquad c_j \in \mathcal{A}\,.$$

Corollary (Hensley)

Let $Q \in \mathbb{N}$. Consider the set $F_M(Q)$:

$$\left\{ \frac{u}{v} = [c_1, c_2, \dots, c_s] \ : \ (u,v) = 1, \, 1 \le u < v \le Q, \, \forall c_j \le M \right\} .$$

Then

$$|F_M(Q)| \sim Q^{2w_M} .$$

We are interested in 1–parametric set

$$\mathcal{Z}_M(p) = \left\{ 1 \le a \le p-1 \ : \ \frac{a}{p} = [c_1, c_2, \dots, c_s], \, \forall c_j \le M \right\} .$$

If we believe in the uniform distribution in v, then

Zaremba's conjecture, strong form

$$\forall p : \qquad |\mathcal{Z}_M(p)| \sim_M \frac{p^{2w_M}}{p} = p^{2w_M - 1} \sim p^{1 - O(1/M)} .$$

Conjecture (Zaremba, again)

$$\forall p: \qquad |\mathcal{Z}_M(p)| \sim_M p^{2w_M-1}\,.$$

Theorem (Moshchevitin–Murphy–Shkredov, 2019)

For any prime p and $\varepsilon > 0$ there is $M = M(\varepsilon)$ such that

$$|\mathcal{Z}_M(p)| \ll_M p^{2w_M-1+\varepsilon(1-w_M)}\,.$$

Theorem (Moshchevitin–Murphy–Shkredov, 2019)

For any prime p and $\varepsilon > 0$ there is $M = M(\varepsilon)$ and $1 \le a < p$ such that

$$\frac{a}{p} = [c_1, \dots, c_s]\,, \quad c_j \le M\,, \quad \forall j \notin \left(\frac{(1-\varepsilon)s}{2}, \frac{(1+\varepsilon)s}{2}\right)\,.$$

A purely combinatorial consequences

Theorem (Shkredov, 2018, Moshchevitin–Murphy–Shkredov, 2018)

Let $A, B \subseteq \mathbb{F}_p$, and $|A+B| \leq K|A|$. Then for some $\delta > 0$ and any $\lambda \neq 0$ one has

$$|\{a_1 a_2 = \lambda \ : \ a_1, a_2 \in A\}| \leq \frac{K^2|A|^2}{p} + 2K|A||B|^{-\delta},$$

$$\left|\left\{\frac{1}{a_1} - \frac{1}{a_2} = \lambda \ : \ a_1, a_2 \in A\right\}\right| \leq \frac{K^2|A|^2}{p} + 2K|A||B|^{-\delta}.$$

The result does not hold for ratios: $|[N] \cap (2 \cdot [N])| \sim N/2$.

Exm. $A = \bigsqcup_j (B + x_j)$ is a disjoint union of an interval B.

Modular Zaremba

Theorem (Moshchevitin–S., 2019)

There is an absolute constant M s.t. $\forall p$ there is

$$q = O(p^{30}), \qquad q \equiv 0 \pmod{p}$$

with a, $(a, q) = 1$ s.t.

$$\frac{a}{q} = [c_1, \ldots, c_s], \quad c_j \leq M.$$

Theorem (Moshchevitin–S., 2019)

There is an absolute constant C s.t. $\forall p$ there is

$$q = O(p^C), \qquad q \equiv 0 \pmod{p}$$

with a, $(a, q) = 1$ s.t. c_j are bounded by two.

New results

Theorem (S., 2020)

Let $\epsilon \in (0, 1]$. There exists $M = M(\epsilon)$ s.t. $\forall p$ there is

$$q = O(p^{1+\epsilon}), \qquad q \equiv 0 \pmod{p}$$

with a, $(a, q) = 1$ s.t.

$$\frac{a}{q} = [c_1, \ldots, c_s], \quad c_j \leq M.$$

Thus, $\epsilon = 0$ gives the Zaremba conjecture.

Also, another proof of the Moshchevitin–S. result with $M = 2$.

New results: modular Hensley's hypothesis

Theorem (S., 2020)

Let $\mathcal{A} \subset \mathbb{N}$ be a finite set s.t.

$$\mathrm{HD}(\mathcal{F}_{\mathcal{A}}) > \frac{1}{2} + \delta\,.$$

There is $C = C_{\mathcal{A}}(\delta)$ s.t. $\forall p$ there exists

$$q = O_{\mathcal{A}}(p^C)\,, \qquad q \equiv 0 \pmod{p}$$

with a, $(a, q) = 1$ s.t.

$$\frac{a}{q} = [c_1, \ldots, c_s]\,, \quad c_j \in \mathcal{A}\,.$$

Thus the modular form of Hensley's conjecture takes place.

Idea of the proof

Having $\frac{p_s}{q_s} = [c_1, \dots, c_s]$, $\frac{p_{s-1}}{q_{s-1}} = [c_1, \dots, c_{s-1}]$

$$\begin{pmatrix} 0 & 1 \\ 1 & c_1 \end{pmatrix} \dots \begin{pmatrix} 0 & 1 \\ 1 & c_s \end{pmatrix} = \begin{pmatrix} p_{s-1} & p_s \\ q_{s-1} & q_s \end{pmatrix} \in A \subset \mathrm{SL}_2(\mathbb{F}_p)$$

under the restrictions

$$c_j \le M \qquad \text{and} \qquad q_s < p\,.$$

By Hensley's lemma

$$|A| \sim p^{2w_M} = p^{2-O(1/M)}\,.$$

To compare: $|\mathrm{SL}_2(\mathbb{F}_p)| = p^3 - p$.

$$A = \begin{pmatrix} p_{s-1} & p_s \\ q_{s-1} & q_s \end{pmatrix} \subset \mathrm{SL}_2(\mathbb{F}_p)\,, \quad q_s < p\,, \quad c_j \leq M\,.$$

Suppose that A^n contains zero, say, $q_s \equiv 0 \pmod{p}$.
Then $\frac{p_s}{q_s}$ has bounded partial quotients and $q_s = O((2p)^n)$.

Consider the standard Borel subgroup

$$B = \begin{pmatrix} \lambda & u \\ 0 & \lambda^{-1} \end{pmatrix}\,, \qquad \lambda \in \mathbb{F}_p \setminus \{0\}, \quad u \in \mathbb{F}_p\,.$$

Our problem is reduced to

$$A^n \cap B \neq \emptyset\,.$$

Again

$$A^n \cap B \neq \emptyset$$

or, equivalently,

$$(BA)A^{n-2}(AB) \cap B \neq \emptyset$$

and we know that

$$\max\{|AB|, |BA|\} \geq \frac{\sqrt{|A||B|p}}{2} \gg p^{3/2+w_M} \sim p^{5/2-O(1/M)}.$$

This and some growth–type results in the spirit of Helfgott give modular Zaremba's conjecture with some effective constants.

We have for $w_M > \frac{1}{2} + \delta$ that

$$|A| \sim p^{2w_M} > p^{1+2\delta}.$$

Theorem (Dickson, 1901)

Let $p \geq 5$ be a prime. Every proper subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$ is isomorphic to one of the following groups:

1. the standard Borel subgroup B and its subgroups,
2. the dihedral groups of order $p \pm 1$ and their subgroups,
3. A_4, S_4, A_5.

Thus, A (and hence A^n) avoids all subgroups excepting Borel subgroups.

Theorem (S., 2020, again)

Let q be an odd number, $P \subset \mathbf{G}(q)$ be a parabolic subgroup. Suppose that for a $\delta > 0$

$$|A| \geq |\mathbf{G}(q)| q^{-r-1+\delta}.$$

Then $A^n \cap P \neq \emptyset$ for $n \ll_r \delta^{-1}$.

For us $P = B$ (and its conjugates), $r = 1$ and

$$|A| > p^{1+\delta} \sim |\mathrm{SL}_2(q)| q^{-1-1+\delta}.$$

Hence $A^n \cap B \neq \emptyset$.

The result about intersecting of A with parabolic (Borel) subgroups gives modular Hensley's conjecture.

Theorem (S., 2020, again)

Let $\mathcal{A} \subset \mathbb{N}$ be a finite set s.t.

$$\mathrm{HD}(\mathcal{F}_{\mathcal{A}}) > \frac{1}{2} + \delta\,.$$

There is $C = C_{\mathcal{A}}(\delta)$ s.t. $\forall p$ there exists

$$q = O_{\mathcal{A}}(p^C)\,, \qquad q \equiv 0 \pmod{p}$$

with a, $(a,q) = 1$ s.t.

$$\frac{a}{q} = [c_1, \ldots, c_s]\,, \quad c_j \in \mathcal{A}\,.$$

This method plus a much more careful analysis concerning the representations of the set A and growth of the first products of A gives

Theorem (S., 2020, again)

Let $\epsilon \in (0, 1]$. There exists $M = M(\epsilon)$ s.t. $\forall p$ there is

$$q = O(p^{1+\varepsilon}), \qquad q \equiv 0 \pmod{p}$$

with a, $(a, q) = 1$ s.t.

$$\frac{a}{q} = [c_1, \ldots, c_s], \quad c_j \leq M.$$

Thank you for your attention!