On Korobov bound concerning Zaremba's conjecture

N. Moshchevitin, B. Murphy and I. Shkredov

Zaremba's conjecture

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

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

Conjecture (Zaremba, 1972)

Let q be a positive integer. Then there exists a, $(a,q)=1$ such that

$$\frac{a}{q} = [c_1, c_2, \ldots, c_s]$$

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

Hensley (1994, 1996): for large q, even $\mathcal{M} = 2$ should be enough.

Motivation–I

Theorem (Koksma–Hlawka, 1961)

Let $f : [0,1]^d \to \mathbb{R}$ be a function of bounded variation $\mathrm{V}(f)$ and $X \subseteq [0,1]^d$ be a finite set. Then

$$\left| \int_{[0,1]^d} f(u)\, du - \frac{1}{|X|} \sum_{x \in X} f(x) \right| \le \mathrm{V}(f) \cdot \mathrm{Disc}(X)\,,$$

where

$$\mathrm{Disc}(X) := \sup_{R = \prod_{i=1}^{d} [a_i, b_i]} \left| \frac{|X \cap R|}{|X|} - \mu(R) \right| .$$

Theorem (Schmidt, 1972)

For any finite X one has $\mathrm{Disc}(X) \gg \frac{\log |X|}{|X|}$.

Motivation–II

Monte–Carlo gives $\mathrm{Disc}(X) \sim \frac{1}{|X|^{1/2}}$.

Now take winding of our two–dimensional torus

$$X = X(a,q) = \left\{ \left(\frac{j}{q}, \frac{aj}{q} \right) \right\}_{j=1}^{q} \subseteq [0,1]^2 \,.$$

Theorem (Zaremba, 1966)

Let $\frac{a}{q} = [c_1, \dots, c_s]$ and $M = \max_{j \le s} c_j$. Then

$$\mathrm{Disc}(X(a,q)) \le \left(\frac{4M}{\log(M+1)} + \frac{4M+1}{\log q} \right) \frac{\log q}{q} \,.$$

For the constant M this bound is essentially best possible.

Known bounds

Theorem (Korobov, 1963)

Let p be a prime number. Then there exists a s.t.

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

has all $c_j \le \mathcal{M} = O(\log p)$.

Theorem (Rukavishnikova, 2006)

The same holds for all q. Moreover,

$$\frac{1}{\varphi(q)} \left| \left\{ 1 \leqslant a \leqslant q,\, (a,q) = 1 \ :\ \max_{1 \leqslant j \leqslant s(a)} c_j(a) \geqslant T \right\} \right| \ll \frac{\log q}{T}$$

Niederreiter (1986): Zaremba's conjecture holds for $q = 2^n$, $q = 3^n$ with $\mathcal{M} = 4$ and for $q = 5^n$ with $\mathcal{M} = 5$.

Zaremba's conjecture for a.e. q

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

$$N - O(N^{1-c(\mathcal{M})/\log\log N}), \qquad c(\mathcal{M}) > 0 .$$

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.

Hensley's conjecture

Theorem (Hensley, 1989–1992)

For any M

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

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

$$w_2 = 0.5312805062772051416244686\ldots > \frac{1}{2}$$

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 a finite alphabet and

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

Then Zaremba's conjecture takes place: $\forall q \ge q_0$ there is a s.t.

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

Literally speaking, for general alphabet the Hensley's conjecture is wrong (Bourgain–Kontorovich, 2011).

Corollary (Hensley)

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

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

Then

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

We are interested in 1–parametric set (let $q = p$)

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

If we believe in the uniform distribution in v, then

Zaremba's conjecture, strong form

$$\forall p : \quad |\mathcal{Z}_M(p)| \sim_M \frac{p^{2w_M}}{p} = p^{2w_M - 1} \gg 1 \,, \quad \text{provided} \quad w_M > \frac{1}{2} .$$

Our results–I: upper bounds

Conjecture (Zaremba, again)

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

Theorem (Moshchevitin–Murphy–S., 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–S., 2019)

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

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

Our results–II: modular Zaremba

Theorem (S., 2020)

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

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

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

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

Thus, $\epsilon = 0$ gives Zaremba's conjecture.

Increasing q we can choose $M = 2$.

Previously (Moshchevitin–S., 2019): $1+\epsilon \to 30$.

Our results–II: modular Hensley's conjecture

Theorem (S., 2020)

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

$$\mathcal{HD}(\mathcal{F}_\mathcal{A}) \geq \frac{1}{2} + \delta\,, \qquad \delta > 0\,.$$

There is $C = C_\mathcal{A}(\delta) > 0$ s.t. for any prime p there exists

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

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

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

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

New results

Theorem (Moshchevitin–Murphy–S., 2022+)

Let q be a positive integer with sufficiently large prime factors. Then there is a positive integer a, $(a, q) = 1$ and

$$M = O\left(\frac{\log q}{\log \log q}\right) \tag{1}$$

such that

$$\frac{a}{q} = [c_1, \dots, c_s]\,, \qquad c_j \le M\,, \qquad \forall j \in [s]\,. \tag{2}$$

Also, if q is a sufficiently large square–free number, then (1), (2) take place.

Thus we have improved Korobov's bound by $\log \log q$.

Ideas of the proof

Lemma (classical)

Let $(a,q)=1$ and $a/q=[c_1,\ldots,c_s]$. Consider the equation

$$ax \equiv y \pmod q\,, \qquad 1 \le x < q\,, \quad 1 \le |y| < q\,. \qquad (3)$$

• If for all solutions (x,y) of the equation above one has $x|y| \ge q/M$, then $c_j \le M$, $j \in [s]$.
• On the other hand, if for all $j \in [s]$ the following holds $c_j \le M$, then all solutions (x,y) of (3) satisfy $x|y| \ge q/4M$.

Symmetry $x \to x^{-1} \pmod q$:

$$\frac{a^{-1}}{q} = [c_s, c_{s-1}\ldots, c_1] \qquad \text{if } s \text{ is even}$$
$$\frac{a^{-1}}{q} = [1, c_s-1, c_{s-1}\ldots, c_1] \qquad \text{if } s \text{ is odd.}$$

Recall (let $t \le \sqrt{q}$ be a parameter)

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

and

$$\mathcal{Z}_M(t) = \left\{ a \ : \ \frac{a}{q} = [c_1, c_2, \dots, c_s], \forall c_j \le M, K(c_1, \dots, c_j) < t \right\} .$$

Also, let

$$\partial F_M(t) = \left\{ \frac{u}{v} = [c_1, c_2, \dots, c_s] \in F_M(t) \ : \ K(c_1, \dots, c_s, 1) \ge t \right\} .$$

Lemma (Moshchevitin, 2007)

Let $t \le \sqrt{q}$ and $T = |\partial F_M(t)|$. Then

$$\mathcal{Z}_M(t) = B_1 \bigsqcup \dots \bigsqcup B_T \,, \qquad c_1 t^{2w_M} \le T \le c_2 t^{2w_M} \,,$$

where B_j are some disjoint intervals and for all $j \in [T]$ the following holds $[q/t^2] \le |B_j|$.

Main lemma: prime case

Main lemma

Let p be a prime number, and $A, B \subseteq \mathbb{F}_p$ be sets. Then $\exists \kappa > 0$ such that

$$|\{(a+c)(b+c) = 1 \ : \ a \in A,\ b \in B,\ c \in 2 \cdot [N]\}| - \frac{N|A||B|}{p}$$

$$\ll \sqrt{|A||B|} N^{1-\kappa}\,.$$

Previously, Kloosterman sums were used and it gives the error term depending on p.

In our regime $N \sim (\log p)^C$ and such bounds are irrelevant.

Theorem (S., 2022+)

Let $N \geq 1$ be a sufficiently large integer, $N \leq p^{c\delta}$ for an absolute constant $c > 0$, $A, B \subseteq \mathbb{F}_p$ be sets, and $g \in \mathrm{SL}_2(\mathbb{F}_p)$ be a non–linear map.
Suppose that S is a set, $S \subseteq [N] \times [N]$, $|S| \geq N^{1+\delta}$.
Then $\exists \kappa = \kappa(\delta) > 0$ such that

$$|\{g(\alpha + a) = \beta + b \ : \ (\alpha, \beta) \in S,\ a \in A,\ b \in B\}| - \frac{|S||A||B|}{p}$$

$$\ll_g \sqrt{|A||B|}|S|^{1-\kappa}\,.$$

Exm. Taking $gx = -1/x$, we obtain the previous equation.

Lemmas imply the main result

We take $t = q^{1/2-\varepsilon}$, $\varepsilon > 0$ is a parameter.

By Moshchevitin's lemma $\mathcal{Z}_M(t) = B_1 \bigsqcup \dots \bigsqcup B_T$, $T \sim t^{2w_M}$ and hence

$$\mathcal{Z}_M(t) \approx I \dotplus S \,, \qquad |I| = N \,.$$

By $x \to x^{-1}$ symmetry we need to solve the equation

$$z_1 z_2 \equiv 1 \pmod q, \qquad z_1, z_2 \in \mathcal{Z}_M(t) \,,$$

and this is a consequence of

$$|\{(a+2i)(b+2i) = 1 \ : \ a, b \in S,\ i \in [N]\}|$$
$$\geq \frac{N|S|^2}{q} - C|S|N^{1-\kappa} > 0 \,.$$

The last inequality takes place if

$$\varepsilon \gg \frac{1}{M} \,.$$

Thus we have

$$ax \equiv y \pmod q$$

for all

$$x|y| \geq \frac{q}{4M} \qquad \text{for} \qquad x \in [t] \qquad \text{and} \qquad x \in \left[\frac{q}{4Mt}, q\right) .$$

Choosing $t = \frac{q}{4Mt}$ or, equivalently, $t = \sqrt{q/4M} = q^{1/2-\varepsilon}$, we get (recall that $\varepsilon \sim 1/M$)

$$M \log M \gg \log q$$

as required.

CF and SL_2, I

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

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

under the restrictions

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

By Hensley's lemma $t < p$

$$|\mathcal{C}| \sim t^{2w_M} = t^{2-O(1/M)}\,.$$

To compare: $|\mathrm{SL}_2(\mathbb{F}_p)| = p^3 - p$, so $\mathcal{C}$ is small.

CF and SL_2, II

We have

$$(a+c)(b+c) \equiv 1 \pmod{p}, \qquad a \in A,\ b \in B,\ c \in 2 \cdot [N].$$

The last equation is equivalent to

$$a = g_j b, \qquad a \in A,\ b \in B,\ j \in [N]$$

where

$$g_j = \begin{pmatrix} -2j & 1-4j^2 \\ 1 & 2j \end{pmatrix}, \qquad j \in [N] \tag{4}$$

with $\det(g_j) = -1$.

Our task is to study growth of the set

$$G = -\{g_j\}_{j=1}^{N} \subset \mathrm{SL}_2(\mathbb{F}_p).$$

Theorem (Helfgott, 2008)

Take $A \subset \mathrm{SL}_2(\mathbb{F}_p)$ such that A generates $\mathrm{SL}_2(\mathbb{F}_p)$. Then either $AAA = \mathrm{SL}_2(\mathbb{F}_p)$ or

$$|AAA| \geq |A|^{1+c}, \qquad c > 0 \quad \text{is an absolute}\,.$$

Theorem (Bourgain–Gamburd, 2008)

Let $A \subset \mathrm{SL}_2(\mathbb{F}_p)$ and $K \geq 1$. Suppose that for any proper subgroup $H \leq \mathrm{SL}_2(\mathbb{F}_p)$ and $\omega \in \mathrm{SL}_2(\mathbb{F}_p)$ one has

$$|A \cap \omega H| \leq |A|/K\,.$$

Then for any $s \in \mathrm{SL}_2(\mathbb{F}_p)$

$$|\{s = a_1 \dots a_{2^k} \ : \ a_j \in A\}| = \frac{|A|^{2^k}}{|\mathrm{SL}_2(\mathbb{F}_p)|} + O\left(\frac{|A|^{2^k}}{K^{ck}}\right)\,.$$

Main lemma: general case

Theorem (Bourgain–Gamburd–Sarnak, 2010)

Let q be a square–free number, $q = \prod_{p \in \mathcal{P}} p$. Also, let $A \subset \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ be a set, $\kappa_0, \kappa_1 > 0$ be constants such that $q^{\kappa_0} < |A| < q^{3-\kappa_0}$, further

$$|\pi_{q_1}(A)| > q_1^{\kappa_1}\,, \qquad \forall q_1 | q\,, \qquad q_1 > q^{\kappa_0/40}\,,$$

and for all $t \in \mathbb{Z}/q\mathbb{Z}$, for any $b \in \mathrm{Mat}_2(q)$, $\pi_p(b) \neq 0$, $p \in \mathcal{P}$ we have

$$|\{x \in A \;:\; \gcd(q, \mathrm{Tr}(bx) - t) > q^{\kappa_2}\}| = o(|A|)\,,$$

where $\kappa_2 = \kappa_2(\kappa_0, \kappa_1) > 0$. Then

$$|A^3| > q^{\kappa(\kappa_0,\kappa_1)}|A|\,.$$

Expansion for general q

Theorem (Bourgain–Varjú, 2012)

Let $S \subset \mathrm{SL}_d(\mathbb{Z})$ be a finite and symmetric set. Assume that S generates a subgroup $G < \mathrm{SL}_d(\mathbb{Z})$ which is Zariski dense in SL_d.
Then $\mathrm{Cay}(\pi_q(G), \pi_q(A))$ form a family of expanders, when S is fixed and q runs through the integers. Moreover, there is an integer q_0 such that $\pi_q(G) = \mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$ if q is coprime to q_0.

The proof uses a deep result from of Bourgain–Furman–Lindenstrauss–Mozes, 2011 which is irrelevant in our regime (roughly speaking, they consider just fixed N, plus the dependence on N is bad although computable).
In our case $d = 2$.

Theorem (Helfgott, 2008, again)

Take $A \subset \mathrm{SL}_2(\mathbb{F}_p)$ such that A generates $\mathrm{SL}_2(\mathbb{F}_p)$. Then either $AAA = \mathrm{SL}_2(\mathbb{F}_p)$ or

$$|AAA| \geq |A|^{1+c}\,, \qquad c > 0 \quad \text{is an absolute}\,.$$

Theorem (Kowalski, 2013)

Suppose that A is sufficiently large. Then one can take $c = \frac{1}{1526}$.

Theorem (Rudnev–S., 2018)

One can take $c = \frac{1}{20}$. Moreover, put $d = \log_{\frac{3}{2}} 8 \approx 5.13$. Then the Cayley graph $\mathrm{Cay}(A)$ relative to A, has diameter

$$O\left(\frac{\log|\mathrm{SL}_2(\mathbb{F}_p)|}{\log|A|}\right)^d.$$

Main lemma, general case

Using a more direct and more simple purely SL_2–method of Rudnev–S., 2018, we obtain

Main lemma, again

Let q be a positive integer with sufficiently large prime factors, and $A, B \subseteq \mathbb{Z}/q\mathbb{Z}$ be sets. Then $\exists \kappa > 0$ such that

$$|\{(a+c)(b+c) = 1 \ : \ a \in A,\ b \in B,\ c \in 2\cdot[N]\}| - \frac{N|A||B|}{q}$$

$$\ll \sqrt{|A||B|}N^{1-\kappa}\,.$$

Also, if q is a sufficiently large square–free number, then the same takes place.

Thank you for your attention!