sciendo

uniform distribution theory

DOI: 10.2478/UDT-2022-0005
Unif. Distrib. Theory **17** (2022), no.1, 1–10

BOUNDS ON THE SIZE OF PROGRESSION-FREE SETS IN $\mathbb{Z}_m^n$

Péter Pál Pach [1,2]

[1]Department of Computer Science and Information Theory, Budapest University of Technology and Economics, Budapest, HUNGARY

[2]MTA-BME Lendület Arithmetic Combinatorics Research Group, ELKH, Budapest, HUNGARY

Dedicated to The Seventh International Conference on the Uniform Distribution Theory (UDT 2021)

ABSTRACT. In this note we give an overview of the currently known best lower and upper bounds on the size of a subset of $\mathbb{Z}_m^n$ avoiding k-term arithmetic progression. We will focus on the case when the length of the forbidden progression is 3. We also formulate some open questions.

Communicated by László Mérai

1. Introduction

There has been great interest in finding progression-free sets in the group $\mathbb{Z}_m^n := \big(\mathbb{Z}/(m\mathbb{Z})\big)^n$, especially when $m{=}3$ or 4. This topic was studied in detail in very recent papers by the current author with Elsholtz (see [8]) and with Palincza (see [12]). Here, we summarize the results of those papers together with several further earlier results (from $[2, 4, 5, 7, 14]$) and finally we conclude with some open problems. We concentrate on sets $S \subseteq \mathbb{Z}_m^n$ of maximal size $|S| = r_k(\mathbb{Z}_m^n)$ with no k *distinct* elements in arithmetic progression. We are

2020 Mathematics Subject Classification: 11B25, 05D99.
Keywords: progression-free sets, cap set problem, polynomial method.
The author was supported by the Lendület program of the Hungarian Academy of Sciences (MTA), the National Research, Development and Innovation Office of Hungary (Grant Nr. K124171, K129335).

interested in the growth rate when k and m are fixed and $n \to \infty$, though other settings would also be interesting (and also studied, for instance, in finite geometry).

Let us formulate first some easy observations. It is well known that constructions can be lifted to higher dimensions and yield asymptotic results by a simple product construction:

Lemma 1.1. *Let us assume that either q is a prime power or $k = 3$.*

a) *Let $S_1 \subseteq \mathbb{Z}_q^{n_1}$ and $S_2 \subseteq \mathbb{Z}_q^{n_2}$ be k-progression-free sets, then $S_1 \times S_2 \subseteq \mathbb{Z}_q^{n_1+n_2}$ is also k-progression-free, consequently*

$$r_k(\mathbb{Z}_q^{n_1+n_2}) \geq r_k(\mathbb{Z}_q^{n_1})\, r_k(\mathbb{Z}_q^{n_2}).$$

b) *A repeated application of part a) gives:*

$$r_k(\mathbb{Z}_q^{nt}) \geq \big(r_k(\mathbb{Z}_q^n)\big)^t.$$

Lemma 1.1 directly implies (with the help of Fekete's lemma) the following proposition.

Proposition 1.2. *Let us assume that either q is a prime power or $k = 3$ such that $q \geq k \geq 3$. Then the limit*

$$\alpha_{k,q} := \lim_{n\to\infty} \big(r_k(\mathbb{Z}_q^n)\big)^{1/n} \quad \textit{exists.}$$

That is, for prime power q we have

$$r_k(\mathbb{Z}_q^n) = \big(\alpha_{k,q} - o(1)\big)^n,$$

where the sign in $-o(1)$ attempts to illustrate that in fact we must have

$$r_k(\mathbb{Z}_q^n) \leq \alpha_{k,q}^n \quad \text{for every} \quad n,$$

again, by Lemma 1.1. However, a priori it is not clear at all whether $\alpha_{k,q} < q$ holds for any pair of k and q. It is a major question (for any pair of $q \geq 3$ and $k \geq 3$) whether the quantity $\alpha_{k,q}$ is smaller than q (then we say that $r_k(\mathbb{Z}_q^n)$ is exponentially small), or $\alpha_{k,q} = q$.

In Section 2, we discuss the known bounds for $k = 3$, in Section 3 we mention some results about the case $k \geq 4$, finally several questions are posed in Section 4.

2. Bounds on $r_3(\mathbb{Z}_m^n)$

The first nontrivial case is when the length of the forbidden arithmetic progression is $k = 3$. The multidimensional case of no 3 points in arithmetic progression has frequently been studied, especially modulo $m = 3$. Here the questions

of "no arithmetic progression $x_1+x_3=2x_2$" and "no zero sums $x_1+x_2+x_3=0$" turn out to be equivalent as $1 \equiv -2 \bmod 3$. This can also be formulated as there are "no three points on a (n affine) line", the problem is known as the "cap set problem". There were important contributions by Brown and Buhler [3], Frankl, Graham and Rödl [9], Meshulam [11], Lev [10], Bateman and Katz [1], Sanders [16], Croot, Lev and author of this note [4], Ellenberg and Gijswijt [7].

As it turns out that there are some differences between the cases when m is odd and when m is divisible by 4, since in case of $4 \mid m$ it may happen that in a non-constant 3-term arithmetic progression a, b, c we have $a = c$. Note that the case when m is an even number not divisible by 4 easily reduces to the odd case, in fact

$$r_3(\mathbb{Z}_m^n) = 2^n r_3(\mathbb{Z}_{m/2}^n)$$

for $m \equiv 2 \pmod 4$.

Let us start with summarizing the results in the case $m = 4$. Introducing an entirely new approach, based on the polynomial method rather than Fourier techniques, Croot, Lev and the present author [4] proved that

$$r_3(\mathbb{Z}_4^n) \le 4^{\gamma n} = 3.61\ldots^n,$$

where $\gamma \approx 0.926$.

As a lower bound Elsholtz and the present author [8] proved that for $n > 1$ we have

$$r_3(\mathbb{Z}_4^n) \ge \max_{0 \le t \le n} \sum_{i=t+1}^{n} \binom{n}{i} A(i, i-t), \tag{1}$$

where $A(m, d)$ denotes the largest possible size of a code in $\mathbb{F}_2^m$ with minimum distance at least d. Note that $A(m, 1) = 2^m$ (all vectors can be taken) and $A(m, 2) = 2^{m-1}$ (all codewords can be taken with even Hamming-weight).

As a consequence of this result the following lower bound can be obtained by choosing t in an optimal way (which satisfies $t \approx 2n/3$):

$$r_3(\mathbb{Z}_4^n) \gg \frac{3^n}{\sqrt{n}},$$

which implies that there exists a progression-free set $S \subseteq \mathbb{Z}_4^n$ with

$$|S| \gg 4^{0.7924n}.$$

In fact to get a lower bound for $r_3(\mathbb{Z}_m^n)$ one can look for constructions in small dimensions, however, finding exact values of $r_3(\mathbb{Z}_m^n)$ turns out to be difficult even in small dimensions. The following values are known [8] in case of $m = 4$:

$$r_3(\mathbb{Z}_4^1) = 2, r_3(\mathbb{Z}_4^2) = 6, r_3(\mathbb{Z}_4^3) = 16, r_3(\mathbb{Z}_4^4) = 42, r_3(\mathbb{Z}_4^5) = 124.$$

Note that lifting

$$r_3(\mathbb{Z}_4^5) = 124 \quad \text{only yields} \quad r_3(\mathbb{Z}_4^n) \geq \big(124^{1/5} - o(1)\big)^n = \big(2.622\ldots - o(1)\big)^n$$

which is considerably worse than the bound $3^n/\sqrt{n}$. It is also worth noting that for all the cases $n \leq 5$ the lower bound in (1) turns out to be the tight answer.

In view of the above results, and also of an upper bound in a relevant case Elsholtz and the present author [8] formulated the following conjecture:

Conjecture 1.

$$r_3(\mathbb{Z}_4^n) = \big(3 - o(1)\big)^n, \quad \text{i.e.,} \quad \alpha_{3,4} = 3.$$

To describe the case when the conjectured bound holds, let us give a reformulation of the problem of determining $r_3(\mathbb{Z}_4^n)$. Let us say that a system of subsets $A(x) \subseteq \mathbb{F}_2^n$ $(x \in \mathbb{F}_2^n)$ satisfies property $(*)$, if the following implication holds

$$\forall x \in \mathbb{F}_2^n \ (y \in x + A(x)\hat{+}A(x) \implies A(y) = \emptyset), \tag{$*$}$$

where $\hat{+}$ denotes the restricted sumset, that is,

$$x + A(x)\hat{+}A(x) = \{x + u + v : \ u, v \in A(x), \ u \neq v\}.$$

(Note that for $A(x) = \emptyset$, we define $x + A(x)\hat{+}A(x) := \emptyset$.) It can be shown that the maximal possible size of $\sum_{x \in \mathbb{F}_2^n} |A(x)|$ for a system of subsets $\{A(x) : x \in \mathbb{F}_2^n\}$ satisfying property $(*)$ is exactly $r_3(\mathbb{Z}_4^n)$, so property $(*)$ nicely captures the condition that the "corresponding" set $A \subseteq \mathbb{Z}_4^n$ is free of 3-term arithmetic progressions.

In [8] we proved the following

Theorem 2.1. *If the system of subsets $A(x)$ satisfies $(*)$ and all non-empty subsets $A(x)$ are subspaces, then*

$$\sum_{x \in \mathbb{F}_2^n} |A(x)| \leq 3^n.$$

For general even m we [8] proved the following lower bound.

Theorem 2.2. *Let $m \geq 4$ be even. There exists some $C_m > 0$ such that*

$$r_3(\mathbb{Z}_m^n) \geq \frac{C_m}{\sqrt{n}} \left(\frac{m+2}{2}\right)^n.$$

With

$$\sigma_m = \sqrt{\tfrac{m^4+8m^3+4m^2-48m}{2880}} \quad \text{one can choose} \quad C_m = \frac{1}{3\sqrt{3}\sigma_m}.$$

For large m one has that $C_m \sim \frac{8\sqrt{5}}{\sqrt{3}\, m^2}$.

Let us continue now with the odd case. The method introduced in [4] also led to the result

$$r_3(\mathbb{Z}_3^n) \le 2.756^n$$

by Ellenberg and Gijswijt [7].

More generally, for primes $p \ge 3$ and some positive constant δ_p

$$r_3(\mathbb{Z}_p^n) \le (p - \delta_p)^n.$$

Indeed the argument yields [2] the bound

$$r_3(\mathbb{Z}_p^n) \le \big(J(p)p\big)^n,$$

where

$$J(p) = \frac{1}{p} \min_{0<t<1} \frac{1 - t^p}{(1-t)\, t^{(p-1)/3}}. \tag{2}$$

As $J(p)$ is decreasing and $J(3) \le 0.9184$ one can conclude that for every $m \ge 3$ the following holds (see, e.g., [2] and [14]):

$$r_3(\mathbb{Z}_m^n) \le (0.9184m)^n \tag{3}$$

for every $m \ge 3$. To see this it suffices to notice that $r_3(\mathbb{Z}_{m_1 m_2}^n) \le m_1^n r_3(\mathbb{Z}_{m_2}^n)$ for every m_1 and m_2 and that each $3 \le m$ has 4 or an odd prime among its divisors.

For more on different interpretations of the proof of the upper bounds we refer the readers to [4, 7, 13, 18, 19].

We shall mention that although the method could be applied for any finite field $\mathbb{F}_q$ with $q = p^\alpha$, however, since $r_3(\mathbb{F}_q^n) = r_3(\mathbb{F}_p^{\alpha n})$ the relevant cases are those when the prime power q is a prime. (The resulting upper bound from the application to $\mathbb{F}_{p^\alpha}$ is worse than the bound coming from the case of $\mathbb{F}_p$.)

Lower bounds for progression-free sets in $G = \mathbb{Z}_3^n$ has also been studied in detail. It is known (see Edel [5] for the history and current record) that there is a set S with

$$|S| > 2.217389^n = |G|^\beta \quad \text{with} \quad \beta = \frac{\log 2.217389}{\log 3} \approx 0.724851.$$

The currently strongest lower bound example comes from a product construction, based on an example in dimension 480.

There are only very few explicit values known:

$$r_3(\mathbb{Z}_3^1) = 2, \qquad r_3(\mathbb{Z}_3^4) = 20,$$

$$r_3(\mathbb{Z}_3^2) = 4, \qquad r_3(\mathbb{Z}_3^5) = 45,$$

$$r_3(\mathbb{Z}_3^3) = 9, \qquad r_3(\mathbb{Z}_3^6) = 112.$$

The author of the 6-dimensional result (Potechin [15]), and the authors of the *classification* of the unique 5-dimensional extremal set [6] (required for the 6-dimensional case by Potechin) mentioned that they used computer calculations.

For general odd m we [8] proved the following lower bound:

Theorem 2.3. *Let $m \geq 5$ be odd. There exists some $C_m > 0$ such that*

$$r_3(\mathbb{Z}_m^n) \geq \frac{C_m}{\sqrt{n}} \left(\frac{m+1}{2}\right)^n.$$

Moreover, with

$$\sigma_m = \sqrt{\frac{1}{2880}\left(m^4 + 4m^3 - 14m^2 - 36m + 45\right)}$$

the value $C_m = \frac{1}{3\sqrt{3}\,\sigma_m}$ is admissible. For increasing odd m asymptotically

$$C_m \sim \frac{8\sqrt{5}}{\sqrt{3}\,m^2}$$

holds.

3. Bounds when $k \geq 4$

We have seen that $r_3(\mathbb{Z}_m^n)$ is exponentially small when $m \geq 3$, that is, $\alpha_{3,m} < m$. For longer progressions it has not yet been decided in the cases $4 \leq k \leq m$ whether $r_k(\mathbb{Z}_m^n)$ is also exponentially small or of order of magnitude $\big(m - o(1)\big)^n$ (as $n \to \infty$) with the exception of the case $6 \mid m$ and $k \in \{4, 5, 6\}$, when the quantity $r_k(\mathbb{Z}_m^n)$ is exponentially small, namely:

Theorem 3.1 ([12])**.** *If $6 \mid m$ and $k \in \{4, 5, 6\}$, then $r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$, if n is sufficiently large. Specially, $r_6(\mathbb{Z}_6^n) \leq 5.709^n$.*

As a lower bound we know only the following easy consequence of the lower bound for $r_3(\mathbb{Z}_3^n)$:

$$4.434^n \leq 2^n r_3(\mathbb{Z}_3^n) = r_3(\mathbb{Z}_6^n) \leq r_6(\mathbb{Z}_6^n).$$

Note that in case of non prime power m and longer progressions Lemma 1.1 is not applicable, furthermore, the product construction can indeed fail to work.

Let us illustrate this by the case $k = 6, m = 6$. In dimension 1 the set $A = \{0, 1, 2, 3, 4\}$ is free of 6-term arithmetic progressions. By taking

$$A \times A = \{0, 1, 2, 3, 4\} \times \{0, 1, 2, 3, 4\}$$

we obtain a 25-element subset of $\mathbb{Z}_6^2$ which contains the following 6-term arithmetic progression:

$$(0, 0), (2, 3), (4, 0), (0, 3), (2, 0), (4, 3).$$

Although the product construction is not applicable, the value of $r_6(\mathbb{Z}_6^2)$ still turns out to be $25 = 5^2$, however, we [12] showed that

$$r_6(\mathbb{Z}_6^3) < 125 = \big(r_6(\mathbb{Z}_6)\big)^3.$$

The lower bound constructions from Theorem 2.2 and Theorem 2.3 may be generalized in various ways, as an illustration we list some lower bounds obtained in similar manners.

Theorem 3.2 ([8]). *The following holds:*

$$r_4(\mathbb{Z}_{11}^n) \gg \frac{7^n}{n^3}.$$

Theorem 3.3 ([8]). *Let $m = p^s$ be a pure prime power, $s \geq 2$. Let $k = p^{s-1} + 1$. Then there exist constants $C_m > 0$ and $0 < c_m \leq m/2$ such that the following holds*

$$r_k(\mathbb{Z}_m^n) \geq C_m \frac{(m - p + 1)^n}{n^{c_m}}.$$

Corollary 3.4 ([8]). *There exist positive constants C_m and $c_m \leq m/2$ such that the following holds*

$$r_5(\mathbb{Z}_8^n) \geq C_8 \frac{7^n}{n^{c_8}},$$

$$r_{10}(\mathbb{Z}_{27}^n) \geq C_{27} \frac{25^n}{n^{c_{27}}},$$

$$r_{26}(\mathbb{Z}_{125}^n) \geq C_{125} \frac{121^n}{n^{c_{125}}},$$

$$r_{102}(\mathbb{Z}_{101^2}^n) \geq C_{10201} \frac{10101^n}{n^{c_{10201}}}.$$

Theorem 3.5 ([8]). *Let $m = p^s$ be a pure prime power, $s \geq 3$. Let $k = p^{s-2} + 1$. Then there exist constants $C_m > 0$ and $0 < c_m \leq m/2$ such that the following holds:*

$$r_k(\mathbb{Z}_m^n) \geq C_m \frac{(m - 2p^2 + 2p)^n}{n^{c_m}}.$$

For $p = 2$, this is certainly not the best possible. By Theorem 2.2 for $m = 8$, $k = 3$ one can use 5 digits, rather than 4.

Corollary 3.6 ([8]). *There exist positive constants C_m and $c_m \le m/2$ such that the following holds:*

$$r_{p+1}(\mathbb{Z}_{p^3}^n) \ge C_{p+1}\frac{(p^3-2p^2+2p)^n}{n^{c_{p+1}}},$$

$$r_4(\mathbb{Z}_{27}^n) \ge C_{27}\frac{15^n}{n^{c_{27}}},$$

$$[r_{82}(\mathbb{Z}_{729}^n) \ge C_{729}\frac{717^n}{n^{c_{729}}},$$

$$[r_6(\mathbb{Z}_{125}^n) \ge C_{125}\frac{85^n}{n^{c_{125}}},$$

$$[r_{26}(\mathbb{Z}_{625}^n) \ge C_{625}\frac{585^n}{n^{c_{625}}}.$$

4. Questions

For prime power values of m there has been some improvements on the trivial corollaries of the prime case, like

$$r_3(\mathbb{Z}_9^n) \le 3^n r_3(\mathbb{Z}_3^n)$$

Namely, the method was adapted to odd prime powers [2,13,17] and also to the technically more difficult even case for $m = 2^3 = 8$. For $r_3(\mathbb{Z}_8^n)$ the trivial implication is

$$r_3(\mathbb{Z}_8^n) \le 2^n r_3(\mathbb{Z}_4^n) \le 7.222^n,$$

however, Petrov and Pohoata [14] could prove that

$$r_3(\mathbb{Z}_8^n) \le 7.09^n$$

also holds.

It would be interesting to see similar improvements for such composite m's that are not prime powers. For instance, it is clear that

$$r_3(\mathbb{Z}_{15}^n) \le \min\big(3^n r_3(\mathbb{Z}_5^n), 5^n r_3(\mathbb{Z}_3^n)\big),$$

but is it possible to improve on this bound?

Question 1. Is it true that $\alpha_{3,15} < \min(3\alpha_{3,5}, 5\alpha_{3,3})$?

According to Proposition 1.2 the quantity $\big(r_k(\mathbb{Z}_m^n)\big)^{1/n}$ converges when m is a prime power. This should also hold for an arbitrary integer m, however we do not see a proof of this statement.

Question 2. Does $\big(r_k(\mathbb{Z}_m^n)\big)^{1/n}$ converge? Specially, does $\big(r_6(\mathbb{Z}_6^n)\big)^{1/n}$ converge?

For $r_6(\mathbb{Z}_6^n)$ we gave only the trivial lower bound $2^n r_3(\mathbb{Z}_3^n) \le r_6(\mathbb{Z}_6^n)$. We ask whether this bound can be improved by an exponential factor:

Question 3. Is it true that $(2+\varepsilon)^n r_3(\mathbb{Z}_3^n) \le r_6(\mathbb{Z}_6^n)$ for some $\varepsilon > 0$ (not depending on n)?

It is known that $r_k(\mathbb{Z}_m^n)$ is exponentially smaller than m^n when $k = 3$ or $6 \mid m$ and $k \in \{4,5,6\}$. It would be interesting to add further pairs of k and m into this list. On the other hand, as far as we know, no pair of $k \ge 3$ and $m \ge 3$ is known when $r_k(\mathbb{Z}_m^n)$ is *not* exponentially small, which motivates the question below:

Question 4. Does there exist $m \ge k \ge 3$ such that $r_k(\mathbb{Z}_m^n) = \big(m - o(1)\big)^n$?

REFERENCES

[1] BATEMAN, M.—KATZ, N. H.: *New bounds on cap sets*, J. Amer. Math. Soc. **25** (2012), no. 2, 585–613.

[2] BLASIAK, J. — CHURCH, T. — COHN, H. — GROCHOW, J. — NASLUND, E. – – SAWIN, W. — UMANS, C.: *On cap sets and the group-theoretic approach to matrix multiplication*, Discrete Anal. 2017, art. no. 3, 27 pp.

[3] BROWN, T. C.—BUHLER, J. P.: *A density version of a geometric Ramsey theorem*, J. Combin. Theory Ser. A **25** (1982), 20–34.

[4] CROOT, E.—LEV, V. F.—PACH, P. P.: *Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small*, Ann. of Math. (2) **185** (2017), no. 1, 331–337.

[5] EDEL, Y.: *Extensions of generalized product caps*, Des. Codes Cryptogr. **31** (2004), 5–14.

[6] EDEL, Y.—FERRET, S.—LANDJEV, I.—STORME, L.: *The classification of the largest caps in* AG$(5,3)$, J. Combin. Theory Ser. A **99** (2002), 95–110.

[7] ELLENBERG, J. S.—GIJSWIJT, D.: *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*, Ann. of Math. (2) **185** (2017), no. 1, 339–343.

[8] ELSHOLTZ, C.—PACH, P. P.: *Caps and progression-free sets in $\mathbb{Z}_m^n$*, Des. Codes Cryptogr. **88** (2020), 2133–2170.

[9] FRANKL, P.—GRAHAM, R. L.—RÖDL, V.: *On subsets of abelian groups with no 3- -term arithmetic progression*, J. Combin. Theory, Ser. A **45** (1987), no. 1, 157–161.

[10] LEV, V. F.: *Progression-free sets in finite abelian groups*, J. Number Theory **104** (2004), 162–169.

[11] MESHULAM, R.: *On subsets of finite abelian groups with no* 3*-term arithmetic progressions*, J. Comb. Theory, Ser. A **71** (1995), 168–172.

[12] PACH, P. P.—PALINCZA, R.: *Sets avoiding six-term arithmetic progressions in $\mathbb{Z}_6^n$ are exponentially small*, SIAM Journal Discrete Math. (to appear)

[13] PETROV, F.: *Combinatorial results implied by many zero divisors in a group ring*; https://doi.org/10.48550/arXiv.1606.03256

[14] PETROV, F.—POHOATA, C.: *Improved Bounds for Progression-Free Sets in C_8^n*, Israel J. Math. **236** (2020), no. 1, 345–363.

[15] POTECHIN, A.: *Maximal caps in $AG(6,3)$*, Des. Codes Cryptogr. **46** (2008), no. 3, 243–259.

[16] SANDERS, T.: *Roth's theorem in $\mathbb{Z}_4^n$*, Anal. PDE **2** (2009), no. 2, 211–234.

[17] SPEYER, D.: *Bounds for sum free sets in prime power cyclic groups — three ways*; https://sbseminar.wordpress.com/2016/07/08/bounds-for-sum-free-sets-inprime--power-cyclic-groups-three-ways

[18] SAWIN, W.—TAO, T.: *Notes on the slice rank of tensors*, (2016); https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-of-tensors

[19] TAO, T.: *A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound*, (2016); https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the--croot-lev-pach-ellenberg-gijswijt-capset-bound

Received June 30, 2021
Accepted November 18, 2021

Péter Pál Pach
Department of Computer Science and Information Theory
Budapest University of Technology and Economics
Műegyetem rkp. 3
HU-1111 Budapest
HUNGARY

MTA-BME Lendület Arithmetic Combinatorics Research Group, ELKH
Műegyetem rkp. 3
HU-1111 Budapest
HUNGARY

E-mail: ppp@cs.bme.hu