Sets avoiding $p$-term arithmetic progressions in $\mathbb{Z}_q^n$ are exponentially small

Gábor Hegedűs
Óbudai Egyetem
Bécsi út 96, Budapest, Hungary, H-1037
hegedus.gabor@nik.uni-obuda.hu

December 16, 2020

Abstract

Pach and Palincza proved the following generalization of Ellenberg and Gijswijt’s bound for the size of $k$-term arithmetic progression-free subsets, where $k \in \{4, 5, 6\}$ in [4] Theorem 1.3:

Let $m > 0$ be an integer such that 6 divides $m$ and let $k \in \{4, 5, 6\}$. Then

$$r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$$

if $n$ is sufficiently large.

Building on the proof technique of Pach and Palincza’s upper bound we generalize the Ellenberg and Gijswijt’s bound in the following way:

Let $p > 2$ be any integer and let $q > 2$ be a prime. Suppose that $p \leq q$. Then there exists an $n_0 \in \mathbb{N}$ integer and a $0 < \delta(p,q) < 1$ real number such that

$$r_p(\mathbb{Z}_q^n) \leq (\delta(p,q)q)^n$$

for each $n > n_0$. 

1
1 Introduction

First we introduce some notations. Let $\mathbb{Z}_n^m$ denote the Abelian group $(\mathbb{Z}/(m\mathbb{Z}))^n$.

Let $G$ stand for a finite Abelian group. Then we denote by $r_k(G)$ the maximal size of a subset $A \subseteq G$ with no $k$ distinct elements in arithmetic progression.

Define $J(q) := \frac{1}{q} \left( \min_{0 < x < 1} \frac{1-x^q}{1-x} x^{-\frac{q-1}{3}} \right)$ for each $q > 1$.

This $J(q)$ constant appeared previously in Ellenberg and Gijswijt’s well-known upper bound for the size of three-term progression-free sets (see [3]).

**Theorem 1.1** Let $q > 2$ denote a prime power. Let $B \subseteq (\mathbb{Z}_q)^n$ be a three-term arithmetic progression-free subset. Then

$$|B| \leq 3 \left( J(q) q \right)^n.$$ 

It is easy to verify that $J(3) = 0.9184$.

Blasiak, Church, Cohn, Grochow and Umans proved in [1] Proposition 4.12 that $J(q)$ is a decreasing function of $q$ and

$$\lim_{q \to \infty} J(q) = \inf_{z > 3} \frac{z - z^{-2}}{3 \log(z)} = 0.8414 \ldots.$$ 

This means that $J(q)$ lies in the range

$$0.8414 \leq J(q) \leq 0.9184$$

for each $q \geq 3$.

Since $J(q) q < q$, we can interpret Theorem 1.1 in the following way: three-term arithmetic progression-free subsets in the group $\mathbb{Z}_q^n$ are exponentially small.

Pach and Palincza gave the following breakthrough upper bounds for the size of $k$-term arithmetic progression-free subsets in $\mathbb{Z}_q^n$ Theorem 1.3 and Theorem 1.4, where $k \in \{4, 5, 6\}$.

As the author knows, these bounds are the only existing exponentially small bounds for the size of $k$-term arithmetic progression-free subsets, where $k > 3$.

**Theorem 1.2** Let $m > 0$ be an integer such that 6 divides $m$ and let $k \in \{4, 5, 6\}$. Then

$$r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$$

if $n$ is sufficiently large.
Theorem 1.3 Let \( n \geq 1 \) be an integer. Then
\[
r_6(\mathbb{Z}_n^6) \leq 2^{n+1} \sqrt{3^n r_3(\mathbb{Z}_3^n)}
\]
These results inspired us to give the following definition. Let \( 3 \leq t \leq s \) be fixed integers. We say that the pair \((t, s)\) is small if there exists an \( n_0 \in \mathbb{N} \) integer and a \( 0 < \delta(t, s) < 1 \) real number such that
\[
r_t(\mathbb{Z}_s^n) \leq (\delta(t, s)s)^n
\]
for each \( n > n_0 \).

Our aim is to generalize the Ellenberg and Gijswijt’s bound and to give exponentially small upper bounds for the size of \( p \)-term arithmetic progression-free subsets, where \( p > 3 \) is arbitrary. Our proofs uses the same proof techniques as the proof of [4] Theorem 1.4. Pach and Palincza used the structural description of \( k \)-AP free subsets in \( \mathbb{Z}_6^n \) to prove their results (here \( k \in \{4, 5, 6\} \)). Our argument is a proof by the principle of complete induction, where we use a similar structural description of \( p \)-AP free subsets in \( \mathbb{Z}_2^q \) (where \( p \) and \( q \) are primes).

We state here our main results.

Theorem 1.4 Let \( 2 < p \leq q \) be primes. Then the pair \((p, q)\) is small.

We can easily verify the following Corollaries, which are the direct consequences of Theorem 1.4.

Corollary 1.5 Let \( p > 2 \) be an odd integer and let \( q > 2 \) be a prime. Suppose that \( p \leq q \). Then the pair \((p, q)\) is small.

Corollary 1.6 Let \( p > 2 \) be any integer and let \( q > 2 \) be a prime. Suppose that \( p \leq q \). Then the pair \((p, q)\) is small.

The proof of Theorem 1.4 is based on the following Lemmas.

Lemma 1.7 Let \( p, r \geq 3 \), \( m \geq 1 \) be integers. Suppose that the pair \((p, r)\) is small. Then the pair \((p, rm)\) is small.

Lemma 1.8 Let \( s_1, s_2 \geq 2 \) be primes, let \( p \geq 3 \) be any integer. Suppose that \( s_1 < p \leq s_2 \) and the pair \((p, s_1s_2)\) is small. Then the pair \((p, s_2)\) is small.

Lemma 1.9 Let \( p > 2 \) be an odd integer and let \( m \geq p \) be an odd prime. Define \( q = 2m \). Suppose that the pair \((p, q)\) is small. Then the pair \((2p, q)\) is small.

We prove our results in Section 2.
2 Proofs of the main results

Proof of Lemma 1.7:
It is enough to prove that
\[ r_p(Z_{nrm}) \leq m^n r_p(Z^n_r). \]
Let \( A \) be a \( p \)-AP free subset of the group \( Z_{nrm}^n \). Clearly \( Z^n_r \) is a subgroup of the group \( Z_{nrm}^n \). Hence we can apply the upper bound \( r_p(Z^n_r) \) for each of the \( m^n \) cosets of this subgroup \( Z^n_r \). \hfill \square

Proof of Lemma 1.8:
It is enough to prove that
\[ (s_1)^n r_p(Z^n_{s_2}) \leq r_p(Z^n_{s_1 s_2}) \]
for each \( n \geq 1 \).
Let \( A \subseteq Z^n_{s_2} \) be a maximal \( p \)-AP free subset. This means that
\[ |A| = r_p(Z^n_{s_2}). \]
Then
\[ Z^n_{s_1} \times A \subseteq Z^n_{s_1} \times Z^n_{s_2} \cong Z^n_{s_1 s_2} \]
and
\[ |Z^n_{s_1} \times A| = (s_1)^n r_p(Z^n_{s_2}). \]
Hence it is enough to prove that \( Z^n_{s_1} \times A \) is \( p \)-AP free.
Indirectly, suppose that \((f_1, t_1), \ldots, (f_p, t_p) \in Z^n_{s_1} \times A \) is a \( p \)-AP, where the elements \((f_1, t_1), \ldots, (f_p, t_p) \) are distinct. Then \( t_1, \ldots, t_p \) is an AP, so it is enough to prove that \( t_1, \ldots, t_p \) are different elements of \( A \), since this contradicts to the fact that \( A \subseteq Z^n_{s_2} \) is a \( p \)-AP free subset.
Let \((d, v) := (f_2, t_2) - (f_1, t_1) \). If \( o(v) = s_2 \), then this means that \( t_1, \ldots, t_p \) are different elements, because \( s_2 \geq p \).
But \( s_2 \) is a prime, hence either \( o(v) = 1 \) or \( o(v) = s_2 \). If \( o(v) = 1 \), then \( o(d) = o(d, v) \) and either \( o(d) = 1 \) or \( o(d) = s_1 \). In both cases \( o(d, v) = o(d) < p \), which contradicts to the assumption that the elements \((f_1, t_1) \ldots (f_p, t_p) \in Z^n_{s_1} \times A \) are distinct. \hfill \square

Proof of Lemma 1.9:
In our proof we use the following Lemma.
Lemma 2.1 Let \( \mathcal{F} = \{A_1, \ldots, A_M\} \) be a collection of subsets of \([N] = \{1, 2, \ldots, N\}\). Suppose that
\[
|A_i \cap A_j| \leq t
\]
for each \(1 \leq i < j \leq M\). Then
\[
\sum_i |A_i| \leq M \sqrt{2Nt}.
\]

Proof of Lemma 2.1:
This follows easily from Cauchy–Schwartz inequality. The proof of this Lemma is essentially the same as that of Theorem 1.4. of [4]. \(\Box\)

Since the pair \((p, 2m)\) is small, hence it follows from Lemma 1.8 that the pair \((p, m)\) is small, too.
Clearly \(\mathbb{Z}_{2m}^n \simeq \mathbb{Z}_2^m \times \mathbb{Z}_m^n = \{(a, f) : a \in \mathbb{Z}_2^n, f \in \mathbb{Z}_m^n\}\).
Let \(A \subseteq \mathbb{Z}_2^m \times \mathbb{Z}_m^n\) be an arbitrary \(2p\)-AP free subset. Define
\[
A(a) := \{f \in \mathbb{Z}_m^n : (a, f) \in A\} \subseteq \mathbb{Z}_m^n
\]
for each \(a \in \mathbb{Z}_2^n\).

Consequently the following union gives a disjoint decomposition of the set \(A\):
\[
A = \bigcup_{a \in \mathbb{Z}_2^n} A(a).
\]

It follows that
\[
|A| = \sum_{a \in \mathbb{Z}_2^n} |A(a)|.
\]

It is easy to see that
\[
|A(r) \cap A(s)| \leq r_p(\mathbb{Z}_m^n)
\]
for each \(r, s \in \mathbb{Z}_2^n\), where \(r \neq s\).

Namely indirectly, suppose that there exist \(r, s \in \mathbb{Z}_2^n\) such that both subsets \(A(r)\) and \(A(s)\) contain the same \(p\)-AP \(t_1, \ldots, t_p\) in \(\mathbb{Z}_m^n\). Then \((r, t_1), \ldots, (r, t_p), (s, t_1), \ldots, (s, t_p)\) \(A\) is a \(2p\)-AP in \(A \subseteq \mathbb{Z}_2^m \times \mathbb{Z}_m^n\), a contradiction.

Since the pair \((p, m)\) is small, hence there exists a real number \(0 < \delta(p, m) < 1\) and an \(n_0 \in \mathbb{N}\) such that
\[
|A(r) \cap A(s)| \leq (\delta(p, m)m)^n
\]
for each $n > n_0$.

Consider an arbitrary, but fixed ordering on the set $\mathbb{Z}_2^n$:

$$\mathbb{Z}_2^n = \{s_1, \ldots, s_{2^n}\}.$$

Define $A_i := A(s_i)$ for each $1 \leq i \leq 2^n$. We can apply Lemma 2.1 with the choices $M := 2^n$, $N := m^n$ and $t := (\delta(p, m)m)^n$. Hence we get from Lemma 2.1 that

$$|A| = \sum_{i=1}^{2^n} |A_i| \leq M\sqrt{2Nt} \leq \sqrt{2}(2m\sqrt{\delta(p, m)}))^n.$$

Consequently there exists an $\epsilon > 0$, where $\epsilon < 1 - \sqrt{\delta(p, m)}$ and $n_1 \in \mathbb{N}$ such that

$$|A| \leq (2m(\sqrt{\delta(p, m)} + \epsilon))^n$$

for each $n > n_1$. This means precisely that the pair $(2p, q)$ is small. \hfill \Box

**Proof of Theorem 1.4**

We prove our result by complete induction.

Consider the sequence of odd primes $(p_i)_{i=1}^\infty$.

1. Let $q \geq 3$ be an arbitrary prime. It follows from Theorem 1.1 that the pairs $(3, q)$ are small.

2. Let $t > 1$ be a fixed integer. Suppose that the pairs $(p_i, r)$ are small for each $1 \leq i \leq t - 1$ and for each $r \geq p_i$ prime. We prove that the pairs $(p_t, q)$ are small for each $q \geq p_t$ prime.

Define $p := p_t$.

It follows from Chebyshev’s Theorem that there exists a prime $s$ such that $s < p < 2s$. Since $s < p$, hence there exists an index $1 \leq j \leq t - 1$ such that $s = p_j$. Hence the pair $(s, q)$ is small by the induction hypothesis.

It follows from Lemma 1.7 that the pair $(s, 2q)$ is small, too. Then Lemma 1.9 gives that the pair $(2s, 2q)$ is small. But $p < 2s$, consequently the pair $(p, 2q)$ is small. Lemma 1.8 gives us the desired result that the pair $(p, q)$ is small. \hfill \Box

**Proof of Corollary 1.5:**
This proof is very similar to the proof of Theorem 1.4. Namely it follows from Chebishev’s Theorem that there exists a prime \( s \) such that \( s < p < 2s \). Then it follows from Theorem 1.4 that the pair \((s, q)\) is small. Hence the pair \((s, 2q)\) is small by Lemma 1.7. Lemma 1.9 implies that the pair \((2s, 2q)\) is small. Consequently the pair \((p, 2q)\) is small, since \( p < 2s \). But then Lemma 1.8 implies that the pair \((p, q)\) is small.

\[ \square \]

**Proof of Corollary 1.6:**

If \( p \) is an odd number, then Corollary 1.6 follows from Corollary 1.5. If \( p \) is even and \( q > p \) is a prime, then the pair \((q, q)\) is small by Corollary 1.5. Consequently the pair \((p, q)\) is small, because \( p < q \).

\[ \square \]

**References**

[1] J. Blasiak, T. Church, H. Cohn, J. A. Grochow, and C. Umans, On cap sets and the group-theoretic approach to matrix multiplication. *Discrete Analysis* 3, 27pp (2017).

[2] E. Croot, V. Lev and P. Pach, Progression-free sets in \( \mathbb{Z}_4^n \). *Annals of Math.*, 185, 331-337 (2017)

[3] J. S. Ellenberg and D. Gijswijt. On large subsets of \( \mathbb{F}_q^n \) with no three-term arithmetic progression. *Annals of Math.*, 185(1), 339-343 (2017).

[4] P. P. Pach and R. Palincza, Sets avoiding six-term arithmetic progressions in \( \mathbb{Z}_6^n \) are exponentially small. arXiv preprint [arXiv:2009.11897](https://arxiv.org/abs/2009.11897) (2020).

[5] T. Tao. A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound, 2016. URL:https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach-ellenberg-gijswijt-capset-bound