PROGRESSION-FREE SETS IN $\mathbb{Z}_4^n$ ARE EXPONENTIALLY SMALL

ERNIE CROOT, VSEVOLOD F. LEV, AND PÉTER PÁL PACH†

Abstract. We show that for integer $n \geq 1$, any subset $A \subseteq \mathbb{Z}_4^n$ free of three-term arithmetic progressions has size $|A| \leq 4^{\gamma n}$, with an absolute constant $\gamma \approx 0.926$.

1. Background and Motivation

In his influential papers [R52, R53], Roth has shown that if a set $A \subseteq \{1, 2, \dots, N\}$ does not contain three elements in an arithmetic progression, then $|A| = o(N)$ and indeed, $|A| = O(N/\log\log N)$ as N grows. Since then, estimating the largest possible size of such a set has become one of the central problems in additive combinatorics. Roth's original results were improved by Heath-Brown [H87], Szemerédi [S90], Bourgain [B99], Sanders [S12, S11], and Bloom [B], the current record due to Bloom being $|A| = O(N(\log\log N)^4/\log N)$.

It is easily seen that Roth's problem is essentially equivalent to estimating the largest possible size of a subset of the cyclic group $\mathbb{Z}_N$, free of three-term arithmetic progressions. This makes it natural to investigate other finite abelian groups.

We say that a subset A of an (additively written) abelian group G is *progression-free* if there do not exist pairwise distinct $a, b, c \in A$ with $a + b = 2c$, and we denote by $r_3(G)$ the largest size of a progression-free subset $A \subseteq G$. For abelian groups G of odd order, Brown and Buhler [BB82] and independently Frankl, Graham, and Rödl [FGR87] proved that $r_3(G) = o(|G|)$ as $|G|$ grows. Meshulam [M95], following the general lines of Roth's argument, has shown that if G is an abelian group of odd order, then $r_3(G) \leq 2|G|/\operatorname{rk}(G)$ (where we use the standard notation $\operatorname{rk}(G)$ for the rank of G); in particular, $r_3(\mathbb{Z}_m^n) \leq 2m^n/n$. Despite many efforts, no further progress was made for over 15 years, till Bateman and Katz in their ground-breaking paper [BK12] proved that $r_3(\mathbb{Z}_3^n) = O(3^n/n^{1+\varepsilon})$ with an absolute constant $\varepsilon > 0$.

Abelian groups of even order were first considered in [L04] where, as a further elaboration on the Roth-Meshulam proof, it is shown that $r_3(G) < 2|G|/\operatorname{rk}(2G)$ for any finite abelian group G; here $2G = \{2g \colon g \in G\}$. For the homocyclic groups of exponent 4 this

† Supported by the Hungarian Scientific Research Funds (Grant Nr. OTKA PD115978 and OTKA K108947) and the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

result was improved by Sanders [S11] who proved that $r_3(\mathbb{Z}_4^n) = O(4^n/n(\log n)^\varepsilon)$ with an absolute constant $\varepsilon > 0$. The goal of this paper is to further improve Sanders's result, as follows.

Let H denote the binary entropy function; that is,

$$H(x) = -x \log_2 x - (1-x)\log_2(1-x), \quad x \in (0,1),$$

where $\log_2 x$ is the base-2 logarithm of x. For the rest of the paper, we set

$$\gamma := \max\left\{\frac{1}{2}\big(H(0.5-\varepsilon) + H(2\varepsilon)\big) \colon 0 < \varepsilon < 0.25\right\} \approx 0.926.$$

Theorem 1. *If $n \ge 1$ and $A \subseteq \mathbb{Z}_4^n$ is progression-free, then $|A| \le 4^{\gamma n}$.*

The proof of Theorem 1 is presented in the next section.

We note that the exponential reduction in Theorem 1 is the first of its kind for problems of this sort.

Starting from Roth, the standard way to obtain quantitative estimates for $r_3(G)$ involves a combination of the Fourier analysis and the density increment technique; the only exception is [L12] where for the groups $G \cong \mathbb{Z}_q^n$ with a prime power q, the above-mentioned Meshulam's result is recovered using a completely elementary argument. In contrast, in the present paper we use the polynomial method, without resorting to the familiar Fourier analysis – density increment strategy.

For a finite abelian group $G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ with positive integer $m_1 \mid \cdots \mid m_k$, denote by $\mathrm{rk}_4(G)$ the number of indices $i \in [1,k]$ with $4 \mid m_i$. Since, writing $n := \mathrm{rk}_4(G)$, the group G is a union of $4^{-n}|G|$ cosets of a subgroup isomorphic to $\mathbb{Z}_4^n$, as a direct consequence of Theorem 1 we get the following corollary.

Corollary 1. *If A is a progression-free subset of a finite abelian group G then, writing $n := \mathrm{rk}_4(G)$, we have $|A| \le 4^{-(1-\gamma)n}|G|$.*

2. Proof of Theorem 1

We recall that the degree of a multivariate polynomial is the largest sum of the exponents of all of its monomials. The polynomial is *multilinear* if it is linear in every individual variable.

The proof of Theorem 1 is based on the following lemma.

Lemma 1. *Suppose that $n \ge 1$ and $d \ge 0$ are integers, P is a multilinear polynomial in n variables of total degree at most d over a field $\mathbb{F}$, and $A \subseteq \mathbb{F}^n$ is a set with $|A| > 2\sum_{0 \le i \le d/2} \binom{n}{i}$. If $P(a-b) = 0$ for all $a, b \in A$ with $a \ne b$, then also $P(0) = 0$.*

Proof. Let $m := \sum_{0\le i\le d/2}\binom{n}{i}$, and let $\mathcal{K}=\{K_1,\dots,K_m\}$ be the collection of all sets $K\subseteq[n]$ with $|K|\le d/2$. Writing for brevity

$$x^I := \prod_{i\in I} x_i, \quad x=(x_1,\dots,x_n)\in\mathbb{F}^n,\ I\subseteq[n],$$

there exist coefficients $C_{I,J}\in\mathbb{F}$ $(I,J\subseteq[n])$ depending only on the polynomial P, such that for all $x,y\in\mathbb{F}^n$ we have

$$\begin{aligned}P(x-y) &= \sum_{\substack{I,J\subseteq[n]\\ I\cap J=\varnothing\\ |I|+|J|\le d}} C_{I,J}\,x^I y^J\\ &= \sum_{I\in\mathcal{K}} x^I \sum_{\substack{J\subseteq[n]\setminus I\\ |J|\le d-|I|}} C_{I,J}\,y^J + \sum_{J\in\mathcal{K}}\Bigg(\sum_{\substack{I\subseteq[n]\setminus J\\ d/2<|I|\le d-|J|}} C_{I,J}\,x^I\Bigg) y^J.\end{aligned}$$

The right-hand side can be interpreted as the scalar product of the vectors $u(x),v(y)\in\mathbb{F}^{2m}$ defined by

$$u_i(x)=x^{K_i},\quad u_{m+i}(x)=\sum_{\substack{I\subseteq[n]\setminus K_i\\ d/2<|I|\le d-|K_i|}} C_{I,K_i}\,x^I$$

and

$$v_i(y)=\sum_{\substack{J\subseteq[n]\setminus K_i\\ |J|\le d-|K_i|}} C_{K_i,J}\,y^J,\quad v_{m+i}(y)=y^{K_i}$$

for all $1\le i\le m$. Consequently, if we had $P(a-b)=0$ for all $a,b\in A$ with $a\ne b$, while $P(0)\ne 0$, this would imply that the vectors $u(a)$ and $v(b)$ are orthogonal if and only if $a\ne b$. As a result, the vectors $u(a)$ would be linearly independent (an equality of the sort $\sum_{a\in A}\lambda_a u(a)=0$ with the coefficients $\lambda_a\in\mathbb{F}$ after a scalar multiplication by $v(b)$ yields $\lambda_b=0$, for any $b\in A$). Finally, the linear independence of $\{u(a)\colon a\in A\}\subseteq\mathbb{F}^{2m}$ implies $|A|\le 2m$, contrary to the assumptions of the lemma. □

Remark. It is easy to extend the lemma relaxing the multilinearity assumption to the assumption that P has bounded degree in each individual variable. Specifically, denoting by $f_\delta(n,d)$ the number of monomials $x_1^{i_1}\dots x_n^{i_n}$ with $0\le i_1,\dots,i_n\le\delta$ and $i_1+\dots+i_n\le d$, if P has all individual degrees not exceeding δ, and the total degree not exceeding d, then $|A|>2f_\delta(n,\lfloor d/2\rfloor)$ along with $P(a-b)=0$ $(a,b\in A,\ a\ne b)$ imply $P(0)=0$. Moreover, taking $\delta=d$, or $\delta=|\mathbb{F}|-1$ for $\mathbb{F}$ finite, one can drop the individual degree assumption altogether.

We will use the estimate

$$\sum_{0\le i\le z}\binom{n}{i} < 2^{nH(z/n)} \tag{1}$$

valid for all integer $n\ge 1$ and real $0<z\le n/2$; see, for instance, [McWS77, Ch. 10, §11, Lemma 8].

Recall, that for integer $n\ge d\ge 0$, the sum $\sum_{i=0}^{d}\binom{n}{i}$ is the dimension of the vector space of all multilinear polynomials in n variables of total degree at most d over the two-element field $\mathbb{F}_2$. In particular, the dimension of the vector space of *all* multilinear polynomials in n variables over $\mathbb{F}_2$ is equal to the dimension of the vector space of all $\mathbb{F}_2$-valued functions on $\mathbb{F}_2^n$, and it follows that any non-zero multilinear polynomial represents a non-zero function. These basic facts are used in the proof of Proposition 1 below.

For integer $n\ge 1$, denote by F_n the subgroup of the group $\mathbb{Z}_4^n$ generated by its involutions; thus, F_n is both the image and the kernel of the doubling endomorphism of $\mathbb{Z}_4^n$ defined by $g\mapsto 2g$ $(g\in\mathbb{Z}_4^n)$, and we have $F_n\cong\mathbb{Z}_2^n$.

Proposition 1. *Suppose that $n\ge 1$ and $A\subseteq\mathbb{Z}_4^n$ is progression-free. Then for every $0<\varepsilon<0.25$, the number of F_n-cosets containing at least $2^{nH(0.5-\varepsilon)+1}$ elements of A is less than $2^{nH(2\varepsilon)}$.*

Proof. Let $\mathcal{R}$ be the set of all those F_n-cosets containing at least $2^{nH(0.5-\varepsilon)+1}$ elements of A, and for each coset $R\in\mathcal{R}$ let $A_R:=A\cap R$; thus, $\cup_{R\in\mathcal{R}}A_R\subseteq A$ (where the union is disjoint), and

$$|A_R|\ge 2^{nH(0.5-\varepsilon)+1},\quad R\in\mathcal{R}. \tag{2}$$

For a subset $S\subseteq\mathbb{Z}_4^n$, write

$$2\cdot S:=\{s'+s''\colon (s',s'')\in S\times S,\ s'\ne s''\}\quad\text{and}\quad 2*S:=\{2s\colon s\in S\}.$$

The assumption that A is progression-free implies that the sets

$$B:=\cup_{R\in\mathcal{R}}(2\cdot A_R)\subseteq F_n\quad\text{and}\quad C:=\cup_{R\in\mathcal{R}}(2*R)\subseteq F_n$$

are disjoint: this follows by observing that if $2r\in 2\cdot A$ with some $r\in R$, then for each $a\in r+F_n$ we have $2a=2r\in 2\cdot A$. Furthermore, the sets $2*R$ are in fact pairwise distinct singletons (for $2r_1=2r_2$ is equivalent to $r_1-r_2\in F_n$ and thus to $r_1+F_n=r_2+F_n$), whence $|C|=|\mathcal{R}|$.

Let $d=n-\lceil 2\varepsilon n\rceil$ so that, in view of (2) and (1),

$$2\sum_{0\le i\le d/2}\binom{n}{i} < 2^{nH(0.5-\varepsilon)+1}\le |A_R|,\quad R\in\mathcal{R}. \tag{3}$$

Denoting by $\overline{C}$ the complement of C in F_n, and assuming, contrary to what we want to prove, that $|\mathcal{R}| \ge 2^{nH(2\varepsilon)}$, from (1) we get

$$\sum_{i=0}^{d} \binom{n}{i} = 2^n - \sum_{i=0}^{\lceil 2\varepsilon n\rceil -1} \binom{n}{i} > 2^n - 2^{nH(2\varepsilon)} \ge 2^n - |\mathcal{R}| = 2^n - |C| = |\overline{C}|.$$

(This is the computation where the assumption $\varepsilon < 0.25$ is used.) Consequently, identifying F_n with the additive group of the vector space $\mathbb{F}_2^n$, and accordingly considering B and C as subsets of $\mathbb{F}_2^n$, we conclude that the dimension of the vector space of all multilinear n-variate polynomials over the field $\mathbb{F}_2$ exceeds the dimension of the vector space of all $\mathbb{F}_2$-valued functions on $\overline{C}$. Thus, the evaluation map, associating with every polynomial the corresponding function, is degenerate. As a result, there exists a non-zero multilinear polynomial $P \in \mathbb{F}_2[x_1, \dots, x_n]$ of total degree $\deg P \le d$ such that P vanishes on $\overline{C}$. In particular, P vanishes on $B \subseteq \overline{C}$, and therefore on each set $2 \cdot A_R$, for all $R \in \mathcal{R}$. Fixing arbitrarily an element $r \in R$, the polynomial $P(2r + x)$ thus vanishes whenever $x \in 2 \cdot (A_R - r)$. Hence, also $P(2r) = 0$ by Lemma 1 (which is applicable in view of (3)); that is, P also vanishes on each singleton set $2 * A_R$, for all $R \in \mathcal{R}$. It follows that P vanishes on C. However, P was chosen to vanish on $\overline{C}$. Therefore, P vanishes on all of $\mathbb{F}_2^n$, and it follows that P is the zero polynomial. This is a contradiction showing that $|\mathcal{R}| < 2^{nH(2\varepsilon)}$, and thus completing the proof. □

Proof of Theorem 1. For $x \ge 0$, let $N(x)$ denote the number of F_n-cosets containing at least x elements of A; thus $N(x) = 0$ for $x > 2^n$, and we can write

$$|A| = \int_0^{2^{n+1}} N(x)\,dx. \tag{4}$$

Trivially, we have $N(x) \le 2^n$ for all $x \ge 0$, so that

$$\int_0^{2^{nH(1/4)+1}} N(x)\,dx \le 2^{(H(1/4)+1)n+1} < 2 \cdot 4^{\gamma n}. \tag{5}$$

On the other hand, the substitution $x = 2^{nH(0.5-\varepsilon)+1}$ gives

$$\int_{2^{nH(1/4)+1}}^{2^{n+1}} N(x)\,dx = n \int_0^{1/4} 2^{nH(0.5-\varepsilon)+1} N(2^{nH(0.5-\varepsilon)+1}) \log \frac{0.5+\varepsilon}{0.5-\varepsilon}\,d\varepsilon, \tag{6}$$

and applying Proposition 1, the integral in the right-hand side can be estimated as

$$2n \int_0^{1/4} 2^{n(H(0.5-\varepsilon)+H(2\varepsilon))} \log \frac{0.5+\varepsilon}{0.5-\varepsilon}\,d\varepsilon < 3n \int_0^{1/4} 2^{n(H(0.5-\varepsilon)+H(2\varepsilon))}\,d\varepsilon < n \cdot 4^{\gamma n}. \tag{7}$$

From (4)–(7) we get $|A| < (n+2) \cdot 4^{\gamma n}$, and to conclude the proof we use the tensor power trick: for integer $k \ge 1$, the set $A \times \dots \times A \subseteq \mathbb{Z}_4^{kn}$ is progression-free and therefore

$$|A|^k < (kn+2) \cdot 4^{\gamma k n}$$

by what we have just shown. This readily implies the result. □

References

[BK12] M. Bateman and N.H. Katz, New bounds on cap sets, *J. Amer. Math. Soc.* **25** (2012), no. 2, 585–613.

[B] T.F. Bloom, A quantitative improvement for Roth's theorem on arithmetic progressions, *submitted.*

[B99] J. Bourgain, On triples in arithmetic progression, *Geom. Funct. Anal.* **9** (1999), 968–984.

[BB82] T.C. Brown and J.C. Buhler, A density version of a geometric Ramsey theorem, *J. Combin. Theory, Ser. A* **32** (1982), 20–34.

[FGR87] P. Frankl, G Graham, and V. Rödl, On subsets of abelian groups with no 3-term arithmetic progression, *J. Combin. Theory, Ser. A* **45** (1987), 157–161.

[H87] D.R. Heath-Brown, Integer sets containing no arithmetic progressions, *J. London Math. Soc.* **35** (1987), 385–394.

[L04] V.F. Lev, Progression-free sets in finite abelian groups, *J. Number Theory* **104** (2004), no. 1, 162–169.

[L12] ———, Character-free approach to progression-free sets, *Finite Fields Appl.* **18** (2012), no. 2, 378–383.

[McWS77] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1977).

[M95] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, *J. Combin. Theory Ser. A* **71** (1995), no. 1, 168–172.

[R52] K. Roth, Sur quelques ensembles d'entiers, *C. R. Acad. Sci. Paris* **234** (1952), 388–390.

[R53] ———, On certain sets of integers, *J. London Math. Soc.* **28** (1953), 104–109.

[S09] T. Sanders, Roth's theorem in $\mathbb{Z}_n^4$, *Anal. PDE 2* (2009), no. 2, 211–234.

[S12] ———, On certain other sets of integers, *J. Anal. Math.* **116** (2012), 53–82.

[S11] ———, On Roth's theorem on progressions, *Ann. of Math. (2)* **174** (2011), no. 1, 619–636.

[S90] E. Szemerédi, Integer sets containing no arithmetic progressions, *Acta Math. Hungar.* **56** (1990), 155–158.

E-mail address: `ecroot@math.gatech.edu`

School of Mathematics, Georgia Institute of Technology, Atlanta, Georgia 30332, USA

E-mail address: `seva@math.haifa.ac.il`

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel

E-mail address: `ppp@cs.bme.hu`

Department of Computer Science and Information Theory, Budapest University of Technology and Economics, 1117 Budapest, Magyar tudósok körútja 2, Hungary