Progression-free sets in $\mathbb{Z}_n^4$ are exponentially small. (English) Zbl 1425.11019

This paper represents without a doubt one of the most important breakthroughs in discrete mathematics in 2016. This is despite (or possibly to some extent because of) its relative brevity and elementary nature.

Given a finite abelian group $G$, let $r_k(G)$ denote the cardinality of a largest subset of $G$ containing no non-trivial $k$-term arithmetic progression. The case when $k = 3$ and $G$ is an $n$-dimensional vector space over a finite field of small fixed characteristic $p$ is considered a toy problem for Roth’s problem in the integers [B. Green, in: Surveys in combinatorics 2005, Lond. Math. Soc. Lect. Note Ser. 327, 1–27 (2005; Zbl 1155.11306)], but it is also of independent interest to the design theory and theoretical computer science communities, amongst others.


$$r_3(F_n^3) \ll 3^{n/3},$$

using a Fourier iteration argument going back to [K. F. Roth, J. Lond. Math. Soc. 28, 104–109 (1953; Zbl 0050.04002)] which is now considered standard in the field. Nudging this upper bound toward the lower bound of $3^{0.7245n} \approx 2.2174^n$ provided by a construction of Y. Edel [Des. Codes Cryptography 31, No. 1, 5–14 (2004; Zbl 1057.51005)] has proved surprisingly difficult. It was only in 2012 that M. D. Bateman and N. H. Katz [J. Am. Math. Soc. 25, No. 2, 585–613 (2012; Zbl 1262.11010)], in a paper that is by many considered a technical tour de force, managed to improve the exponent of the denominator from 1 to $1 + \varepsilon$ for some small but explicit $\varepsilon > 0$.

Finite abelian groups $G$ of even order were first considered by V. F. Lev J. Number Theory 104, No. 1, 162–169 (2004; Zbl 1043.11022), who adapted Meshulam’s proof to show that

$$r_3(G) < 2|G|/\text{rank}(2G).$$

T. Sanders [Anal. PDE 2, No. 2, 211–234 (2009; Zbl 1197.11017)] improved upon this for the specific group $G = (\mathbb{Z}/4\mathbb{Z})^n$, showing that

$$r_3((\mathbb{Z}/4\mathbb{Z})^n) \ll 4n/(n \log^\varepsilon n)$$

for some absolute constant $\varepsilon > 0$, using a more sophisticated (but still Fourier-analytic) iteration technique.

The main result of the present paper is the following.

**Theorem.** Let $n \geq 1$ and suppose that $A \subseteq (\mathbb{Z}/4\mathbb{Z})^n$ contains no non-trivial arithmetic progression of length 3. Then

$$|A| \leq 4^\gamma n$$

for a constant $0 < \gamma < 1$.

Specifically, the constant $\gamma \approx 0.926$ is obtained as the maximum over $0 < \varepsilon < 1/4$ of $\frac{1}{2}(H(0.5 - \varepsilon) + H(2\varepsilon))$, where $H$ is the binary entropy function.

This result is of significance for at least two reasons: first, it represents an exponential improvement over previous work, bringing the upper bound for the first time within reasonable reach of the lower bound; second, it spawned a flurry of further results in the immediate aftermath of its publication. Arguably the most important of these to date is the paper by J. S. Ellenberg and D. C. Gijswijt [Ann. Math. (2) 185, No. 1, 339–343 (2017; Zbl 1425.11020)], which reduces the upper bound on $r_3(F_n^3)$ to roughly $2.756^n$, alongside a handful of others that had not been formally published at the time that this review was written.

The core contribution of Croot, Lev and Pach is the realisation that a version of the polynomial method...
can be used to tackle Roth-type problems in certain finite abelian groups. For a comprehensive survey on the polynomial method, its variants and their applications, see [T. C. Tao, EMS Surv. Math. Sci. 1, No. 1, 1–46 (2014; Zbl 1294.05044)]. One recent application that stands out – having surfaced as unexpectedly as the result of the present paper – is the resolution of the finite-field Kakeya conjecture by Z. Dvir [J. Am. Math. Soc. 22, No. 4, 1093–1097 (2009; Zbl 1202.52021)].

The key ingredient in the proof of the above theorem is the following simple linear-algebraic lemma, also used in the aforementioned subsequent work of Ellenberg and Gijswijt: If \( P \) is a multilinear polynomial in \( n \) variables of total degree at most \( d \) over a field \( F \) such that \( P(a-b) = 0 \) for all \( a \neq b \in A \), then \( P(-a) \) cannot be non-zero for too many elements \( a \in A \).

This lemma can be used to prove that if \( A \) is a progression-free subset of \( (\mathbb{Z}/4\mathbb{Z})^n \) then there are few \( F_n \)-cosets containing many elements of \( A \), where \( F_n \) denotes the subgroup of \( (\mathbb{Z}/4\mathbb{Z})^n \) generated by its involutions (which is isomorphic to \( (\mathbb{Z}/4\mathbb{Z})^n \)). From this the bound on the size of \( A \) follows essentially by averaging and the tensor-power trick.

Reviewer: Julia Wolf

MSC:
11B25 Arithmetic progressions
11B13 Additive bases, including sumsets

Cited in 14 Reviews
Cited in 44 Documents

Keywords:
Roth’s theorem; Roth-Meshulam; capset; three-term arithmetic progressions

Full Text: DOI

References:
This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.