Annals of Mathematics **185** (2017), 339–343
http://dx.doi.org/10.4007/annals.2017.185.1.8

On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression

By Jordan S. Ellenberg and Dion Gijswijt

Abstract

In this note, we show that the method of Croot, Lev, and Pach can be used to bound the size of a subset of $\mathbb{F}_q^n$ with no three terms in arithmetic progression by c^n with $c < q$. For $q = 3$, the problem of finding the largest subset of $\mathbb{F}_3^n$ with no three terms in arithmetic progression is called the *cap set problem*. Previously the best known upper bound for the affine cap problem, due to Bateman and Katz, was on order $n^{-1-\varepsilon}3^n$.

The problem of finding large subsets of an abelian group G with no three-term arithmetic progression, or of finding upper bounds for the size of such a subset, has a long history in number theory. The most intense attention has centered on the cases where G is a cyclic group $\mathbb{Z}/N\mathbb{Z}$ or a vector space $(\mathbb{Z}/3\mathbb{Z})^n$, which are in some sense the extreme situations. We denote by $r_3(G)$ the maximal size of a subset of G with no three-term arithmetic progression. The fact that $r_3((\mathbb{Z}/3\mathbb{Z})^n)$ is $o(3^n)$ was first proved by Brown and Buhler [BB82], which was improved to $O(3^n/n)$ by Meshulam [Mes95]. The best known upper bound, $O(3^n/n^{1+\varepsilon})$, is due to Bateman and Katz [BK12]. The best lower bound, by contrast, is around 2.2^n [Ede04].

The problem of arithmetic progressions in $(\mathbb{Z}/3\mathbb{Z})^n$ has sometimes been seen as a model for the corresponding problem in $\mathbb{Z}/N\mathbb{Z}$. We know (for instance, by a construction of Behrend [Beh46]) that $r_3(\mathbb{Z}/N\mathbb{Z})$ grows more quickly than $N^{1-\varepsilon}$ for every $\varepsilon > 0$. Thus it is natural to ask whether $r_3((\mathbb{Z}/3\mathbb{Z})^n)$ grows more quickly than $(3-\varepsilon)^n$ for every $\varepsilon > 0$. In general, there has been no consensus on what the answer to this question should be.

In the present paper we settle the question, proving that for all odd primes p, $r_3((\mathbb{Z}/p\mathbb{Z})^n)^{1/n}$ is bounded away from p as n grows.

The first author is supported by NSF Grant DMS-1402620 and a Guggenheim Fellowship. We thank Terry Tao, Tim Gowers, and Seva Lev for useful discussions during the production of this paper.

The main tool used here is the polynomial method — in particular, the use of the polynomial method developed in the breakthrough paper of Croot, Lev, and Pach [CLP17], which drastically improved the best known upper bounds for $r_3((\mathbb{Z}/4\mathbb{Z})^n)$. In this case, they show that a subset of G with no three-term arithmetic progression has size at most c^n for some $c < 4$. In the present paper, we show that the ideas of their paper can be extended to vector spaces over a general finite field.

Remark 1. The ideas of this paper were developed independently and essentially simultaneously by the two authors. Since the arguments of our two papers were essentially identical, we present them as joint work.

We begin with a slight generalization of Lemma 1 of [CLP17]. Let $\mathbb{F}_q$ be a finite field, and let n be a positive integer. Let M_n be the set of monomials in $x_1, \dots, x_n$ whose degree in each variable is at most $q-1$, and let S_n be the $\mathbb{F}_q$-vector space they span.

Observe that the evaluation map $e : S_n \to \mathbb{F}_q^{\mathbb{F}_q^n}$ given by $e(p) := (p(a))_{a \in \mathbb{F}_q^n}$ is a linear isomorphism. Indeed, both spaces have dimension q^n, and the map e is surjective since for every $a \in \mathbb{F}_q^n$ the polynomial $\prod_{i=1}^n (1 - (x_i - a_i)^{q-1})$ is mapped to the indicator function of point a.

For any real number d in $[0, (q-1)n]$, let M_n^d be the set of monomials in M_n of degree at most d and S_n^d the subspace of S_n they span. Write m_d for the dimension of S_n^d. By a slight abuse of notation, we use "polynomial of degree at most d" to mean an element of S_n^d.

PROPOSITION 2. *Let $\mathbb{F}_q$ be a finite field and let A be a subset of $\mathbb{F}_q^n$. Let α, β, γ be three elements of $\mathbb{F}_q$ which sum to* 0.

Suppose $P \in S_n^d$ satisfies $P(\alpha a + \beta b) = 0$ for every pair a, b of distinct elements of A. Then the number of $a \in A$ for which $P(-\gamma a) \neq 0$ is at most $2m_{d/2}$.

Remark 3. The proof of Proposition 2 is essentially the same as that of Lemma 1 of Croot-Lev-Pach [CLP17], which proves the proposition in the case $(\alpha, \beta, \gamma) = (1, -1, 0)$. In the $\gamma = 0$ case, the conclusion of the proposition is that $P(0) = 0$ once $|A| > 2m_{d/2}$; it turns out to be essential for the present application to have the added flexibility of forcing P to vanish at a larger set of places.

Proof. Any $P \in S_n^d$ is a linear combination of monomials of degree at most d, so we can write

$$P(\alpha x + \beta y) = \sum_{m, m' \in M_n^d \,:\, \deg(mm') \leq d} c_{m,m'} m(x) m'(y). \tag{1}$$

In each summand of (1), at least one of m and m' has degree at most $d/2$. We can therefore write (not necessarily uniquely)

$$P(\alpha x + \beta y) = \sum_{m \in M_n^{d/2}} m(x) F_m(y) + \sum_{m \in M_n^{d/2}} m(y) G_m(x)$$

for some families of polynomials F_m, G_m indexed by $m \in M_n^{d/2}$.

Now let B be the $A \times A$ matrix whose a, b entry is $P(\alpha a + \beta b)$. Then

$$B_{ab} = \sum_{m \in M_n^{d/2}} m(a) F_m(b) + \sum_{m \in M_n^{d/2}} G_m(a) m(b).$$

This is an expression of B as a sum of $2m_{d/2}$ matrices, each one of which visibly has rank at most 1. Thus the rank of B is at most $2m_{d/2}$.

On the other hand, our hypothesis on P forces B to be a diagonal matrix. The bound on the rank of B now implies that at most $2m_{d/2}$ of the diagonal entries of B are nonzero. This completes the proof. □

THEOREM 4. *Let α, β, γ be elements of $\mathbb{F}_q$, not all zero, such that $\alpha + \beta + \gamma = 0$, and let A be a subset of $\mathbb{F}_q^n$ such that the equation*

$$\alpha a_1 + \beta a_2 + \gamma a_3 = 0$$

has no solutions $(a_1, a_2, a_3) \in A^3$ apart from those with $a_1 = a_2 = a_3$. As above, let m_d be the number of monomials in $x_1, \ldots, x_n$ with total degree at most d and in which each variable appears with degree at most $q - 1$.

Then $|A| \leq 3m_{(q-1)n/3}$.

Proof. Without loss of generality we may assume $\gamma \neq 0$.

Let $d \in [0, (q-1)n]$. The space V of polynomials in S_n^d vanishing on the complement of $-\gamma A$ has dimension at least $m_d - q^n + |A|$.

View the elements of V as functions on $\mathbb{F}_q^n$, and let $P \in V$ have maximal support. Let $\Sigma := \{a \in \mathbb{F}_q^n : P(a) \neq 0\}$ be the support of P. We have $|\Sigma| \geq \dim V$ for otherwise, there would exist a nonzero $Q \in V$ vanishing on Σ. But then the support of $P + Q$ would strictly contain Σ, contradicting the choice of P.

Write $\mathcal{S}(A)$ for the set of all elements of $\mathbb{F}_q$ of the form $\alpha a_1 + \beta a_2$, with a_1 and a_2 distinct elements of A. Then $\mathcal{S}(A)$ is disjoint from $-\gamma A$ by hypothesis, so P vanishes on $\mathcal{S}(A)$. By Proposition 2, we know that $P(-\gamma a)$ is nonzero for at most $2m_{d/2}$ points a of A, hence $|\Sigma| \leq 2m_{d/2}$.

It follows that

$$m_d - q^n + |A| \leq \dim V \leq |\Sigma| \leq 2m_{d/2}$$

whence

$$|A| \leq 2m_{d/2} + (q^n - m_d).$$

We note that $q^n - m_d$ is the number of q-power-free monomials whose degree is *greater* than d; these are naturally in bijection with those monomials whose degree is less than $(q-1)n - d$, of which there are at most $m_{(q-1)n-d}$.

Taking $d = 2(q-1)n/3$, we thus have

$$|A| \leq 2m_{(q-1)n/3} + (q^n - m_{2(q-1)n/3}) \leq 3m_{(q-1)n/3}$$

as claimed. □

It is not hard to check that $m_{(q-1)n/3}/q^n$ is exponentially small as n grows with q fixed. We can be more precise. Let X be a variable which takes values $0, 1, \ldots, q-1$ with probability $1/q$ each. Then $m_{(q-1)n/3}/q^n$ is the probability that n independent copies of X have mean at most $(q-1)/3$. By symmetry, this equals the probability that n independent copies of X have mean at least $2(q-1)/3$. This is an example of a large deviation problem. By Cramér's theorem [RAS15, §2.4], we have

$$\lim_{n\to\infty} \frac{1}{n} \log(m_{(q-1)n/3}/q^n) = -I(2(q-1)/3),$$

where I is the *rate* function of the random variable X, calculated as follows: $I(x)$ is the supremum, over all θ in $\mathbb{R}$, of

$$\theta x - \log((1 + e^\theta + \cdots + e^{(q-1)\theta})/q). \tag{2}$$

We note that (2) takes the value 0 at $\theta = 0$ and has nonzero derivative at $\theta = 0$ unless $x = (q-1)/2$, so the supremum of (2) is positive; this shows that $m_{(q-1)n/3} = O(c^n)$ for some $c < q$.

Corollary 5. *Let A be a subset of $(\mathbb{Z}/3\mathbb{Z})^n$ containing no three-term arithmetic progression. Then $|A| = o(2.756^n)$.*

Proof. Taking $q = 3$ and $x = 4/3$, the supremum in (2) is attained when $e^\theta = (\sqrt{33} + 1)/4$ and we obtain the bound $3e^{-I(4/3)} < 2.756$. The theorem now follows by applying Theorem 4 with $\alpha = \beta = \gamma = 1$. □

References

[BK12] M. Bateman and N. H. Katz, New bounds on cap sets, *J. Amer. Math. Soc.* **25** (2012), 585–613. MR 2869028. Zbl 1262.11010. http://dx.doi.org/10.1090/S0894-0347-2011-00725-X.

[Beh46] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U. S. A.* **32** (1946), 331–332. MR 0018694. Zbl 0060.10302.

[BB82] T. C. Brown and J. P. Buhler, A density version of a geometric Ramsey theorem, *J. Combin. Theory, Ser. A* **32** (1982), 20–34. MR 0640624. Zbl 0476.51008. http://dx.doi.org/10.1016/0097-3165(82)90062-0.

[CLP17] E. Croot, V. F. Lev, and P. P. Pach, Progression-free sets in $\mathbf{z}_4^n$ are exponentially small, *Ann. of Math.* **185** (2017), 000–000. http://dx.doi.org/10.4007/annals.2017.185.1.

[Ede04] Y. Edel, Extensions of generalized product caps, *Des. Codes Cryptogr.* **31** (2004), 5–14. MR 2031694. Zbl 1057.51005. http://dx.doi.org/10.1023/A:1027365901231.

[Mes95] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, *J. Combin. Theory Ser. A* **71** (1995), 168–172. MR 1335785. Zbl 0832.11006. http://dx.doi.org/10.1016/0097-3165(95)90024-1.

[RAS15] F. Rassoul-Agha and T. Seppäläinen, *A Course on Large Deviations with an Introduction to Gibbs Measures*, *Grad. Stud. Math.* **162**, Amer. Math. Soc., Providence, RI, 2015. MR 3309619. Zbl 1330.60001.

(Received: May 31, 2016)

University of Wisconsin, Madison, WI
E-mail: ellenber@math.wisc.edu
http://www.math.wisc.edu/~ellenber/

Delft University of Technology, Delft, The Netherlands
E-mail: d.c.gijswijt@tudelft.nl
http://homepage.tudelft.nl/64a8q/