On large subsets of $\mathbb{F}_3^n$ with no three-term arithmetic progression

Jordan S. Ellenberg
University of Wisconsin-Madison

12 May 2016

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 $\mathbb{F}_3^n$ with no three terms in arithmetic progression by c^n with $c < 3$. Previously the best known upper bound, due to Bateman and Katz [BK], was on order $n^{-1-\epsilon}3^n$.

Let S_n be the $\mathbb{F}_3$-vector space spanned by cube-free monomials in $x_1, \dots, x_n$. We may think of this as the space of n-variable polynomials over $\mathbb{F}_3$, subject to the equivalence relation that equates polynomials when they take the same value at every point of $\mathbb{F}_3^n$. For any real number d in $[0, 2n]$, let M_n^d be the set of cube-free monomials 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 1. *Let d be an integer, let P be an element of S_n^d, and let A be a subset of $\mathbb{F}_3^n$. Suppose $P(a + a') = 0$ for every pair a, a' of distinct elements of A. Then the number of $a \in A$ for which $P(2a) \neq 0$ is at most $2m_{d/2}$.*

Proof. This is essentially the same as Lemma 1 of Croot-Lev-Pach [CLP].

If

$$M(x) = x_1^{a_1} \dots x_n^{a_n}$$

is a cube-free monomial of degree d, then we have

$$M(x + y) = \sum_{m \in M_n^d} c_m m(x)(M/m)(y)$$

for some sequence of constants $c_m \in \mathbb{F}_3$ indexed by $M_{d/2}$. Note that at least one of m and M/m lies in $M_{d/2}$.

More generally, any $P \in S_n^d$ is a linear combination of monomials of degree at most d, so we can write

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

In each summand of (1), at least one of m and m' has degree less than $d/2$. We can therefore write

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

for some family of polynomials F_m indexed by $m \in M_n^{d/2}$. Specifically, we can take $F_m = \sum'_{m,m'} c'_{m,m'} m'(y)$, where $c'_{m,m'} = c_{m,m'}$ if exactly one of m and m' has degree at most $d/2$, and $(1/2)c_{m,m'}$ if both do.

Let W be the space of functions from $M_n^{d/2}$ to $\mathbb{F}_3^2$. We can think of an element of W as a pair (a, b) of $\mathbb{F}_3$-valued functions on $M_n^{d/2}$. Then W carries a nondegenerate inner product structure given by

$$\langle (a,b), (a',b') \rangle = \sum_{m \in M_n^{d/2}} a(m)b'(m) + a'(m)b(m).$$

We define a (nonlinear) map $\Phi : \mathbb{F}_3^n \to W$ by the rule

$$\Phi(x)(m) = (m(x), F_m(x)).$$

Then, for any $x, y \in \mathbb{F}_3^n$, we have

$$P(x+y) = \langle \Phi(x), \Phi(y) \rangle.$$

It now follows from our hypothesis on $P(a+a')$ that $\Phi(a)$ and $\Phi(a')$ are orthogonal in W for any two distinct a, a' in A. On the other hand, the norm $\langle \Phi(a), \Phi(a) \rangle$ is just $P(a+a) = P(2a)$. If $\Phi(a_1), \ldots, \Phi(a_k)$ all have nonzero norm in W and are all mutually orthogonal, they must be linearly independent, so $k \leq \dim W = 2m_{d/2}$. This completes the proof. □

We will need some control of how m_d and $m_{d/2}$ vary.

Let I be the *rate function* of a trivalent random variable X taking values $0, 1, 2$ with probability $1/3$ each. Let $d = 2(1-\delta)n$ for some positive real number $\delta < 1/2$, By Cramér's theorem on large deviations, we have

$$3^n - m_d < 3^n e^{-I(2-2\delta)n}$$

and

$$m_{d/2} < 3^n e^{-I(1-\delta)n}$$

for all sufficiently large n.

Theorem 2. *Let A be a subset of $\mathbb{F}_3^n$ containing no a, b, c with $a+b+c = 0$, and let γ be a real number less than $I(2/3) = 0.085\ldots$. If n is sufficiently large, we have*

$$|A| < 3^n e^{-\gamma n}$$

In particular, $3e^{-I(2/3)} < 2.756$, so $|A| < (2.756)^n$ for n large enough. We also note that the upper bound for $|A|$ is roughly of the same order as the number of cube-free monomials in n variables of degree at most $(2/3)n$.

Proof. Let d be an integer such that $m_d \geq 3^n - |A|$. The space V of polynomials of degree at most d vanishing on the complement of $-A$ has dimension at least $m_d - 3^n + |A|$. On the other hand, $A + A$ is disjoint from $-A$, so any P vanishing on the complement of $-A$ vanishes on $A + A$. By Proposition 1, we know that $P(2a) = P(-a)$ is nonzero for at most $2m_{d/2}$ points a of A, for every P in V.

We say a point a of A is *active* if $P(-a)$ is nonzero for some P in V. The number of active points of A is evidently at least $\dim V$. On the other hand, at each active point a of V, the probability that a random element in V is nonzero is $2/3$. So the expected number of active points where a

random P in V takes a nonzero value is at least $(2/3)\dim V$, and in particular there is some P in V which takes nonzero values at $(2/3)\dim V = (2/3)(m_d - 3^n + |A|)$ points.[1]

We thus have the inequality

$$(2/3)(m_d - 3^n + |A|) \leq 2m_{d/2}. \tag{2}$$

Suppose $|A| > 3^n e^{-I(1-2\delta')n}$ for some positive real $\delta' < 1/2$. We can then take d to be $2(1-\delta)n$ for any $\delta < \delta'$, and the inequality $m_d \geq 3^n - |A|$ is satisfied, as long is n is sufficiently large. Moreover,

$$3^n - m_d < 3^n e^{-I(2-2\delta)n} < |A|^c$$

for some constant $c < 1$.

Now (2) becomes

$$(2/3)(|A| - |A|^c) < 2m_{d/2} < 2 \cdot 3^n e^{-I(1-\delta)n}.$$

This implies, for sufficiently large n, that $I(2-2\delta') > I(1-\delta)$. Since $I(x)$ is symmetric around the mean $x = 1$ of X, and is monotone increasing as x moves farther from 1 in either direction, this means that $1-2\delta' > \delta$. Since δ was an arbitrary real number less than δ', this yields a contradiction for every $\delta' > 1/3$. □

Remark 3. The same argument should give a similar exponential bound for the density of a subset of $\mathbb{F}_p^n$ with no three-term arithmetic progressions.

Acknowledgments

The author is supported by NSF Grant DMS-1402620 and a Guggenheim Fellowship.

References

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

[CLP] Croot, E. and Lev, V. and Pach, P.P., Progression-free sets in $\mathbf{Z}_4^n$ are exponentially small, arXiv preprint arXiv:1605.01506 (2016).

[1] We thank Terry Tao for this argument, which replaces a more complicated one in an earlier draft.