# Asymptotic upper bounds on progression-free sets in $\mathbb{Z}_p^n$

Dion Gijswijt

June 7, 2016

**Abstract**

We show that any subset of $\mathbb{Z}_p^n$ ($p$ an odd prime) without 3-term arithmetic progression has size $O(p^{cn})$, where $c := 1 - \frac{1}{18 \log p} < 1$. In particular, we find an upper bound of $O(2.84^n)$ on the maximum size of an affine cap in $GF(3)^n$.

## Introduction

Given an abelian group $G$, a subset $A \subseteq G$ is *progression-free* if there are no disctinct $a, b, c \in A$ for which $a + b = 2c$. In their recent paper [2], Croot, Lev and Pach used the polynomial method to show an upper bound of $O(4^{0.926 \cdot n})$ on the size of progression-free sets in $\mathbb{Z}_4^n$. In this paper, we extend their method to progression-free sets in $\mathbb{Z}_p^n$, where $p$ is an odd prime. This improves the bound $O(\frac{p^n}{n})$ of Meshulam [8] and the bound $O(\frac{3^n}{n^{1+\epsilon}})$ (where $\epsilon > 0$ is a constant) in the case $p = 3$ due to Bateman and Katz [1].

**Remark 1.** *While submitting the paper, the author was informed that Jordan S. Ellenberg proved a similar result [4] three days ago. In their paper an upper bound of $O(2.756^n)$ for progression-free subsets of $\mathbb{Z}_3^n$ (and hence affine caps in $\mathbb{F}_3^n$ is proved. The paper also claims that their method gives an upper bound of $O(p^{cn})$ for some $c = c(p) < 1$ in the case of $\mathbb{Z}_p^n$.*
***Update v2:*** *Since the arguments of our two papers were essentially identical, we decided to publish our solutions as a joint paper [5].*

## Main theorem

Throughout, $\mathbb{F} = GF(p)$ will be a finite field, where $p$ is an odd prime. We denote by $L_n := \text{span}\{x^\alpha : \alpha \in \{0, 1 \ldots, p-1\}^n\}$ the linear space of polynomials over $\mathbb{F}$ in $n$ variables in which no variable occurs with exponent more than $p - 1$. Here we use the notation $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. Also, we denote $|\alpha| := \alpha_1 + \cdots + \alpha_n$. For $f \in L_n$, we denote by $Z(f) := \{a \in \mathbb{F}^n \mid f(a) = 0\}$ the zero set of $f$. For any integer $d \in \{0, \ldots, (p-1)n\}$ we denote by $L_{n,d}$ the subspace of $L_n$ consisting of polynomials of degree at most $d$. Observe that $\dim L_{n,d} + \dim L_{n,(p-1)n-d-1} = p^n$ since the map $(\alpha_1, \ldots, \alpha_n) \mapsto (p - 1 - \alpha_1, \ldots, p - 1 - \alpha_n)$ induces a bijection from the set of monomials in $L_n$ to itself. We will use the following estimate on the dimension of $L_{n,(p-1)n/3}$.

In order to bound the dimension of the subspaces $L_{n,d}$, we use the following inequality.

**Theorem 1** (Hoeffding inequality [7])**.** *Let $X_1, \ldots, X_n$ be independent random variables on $[a_i, b_i]$ and let $S = X_1 + \cdots + X_n$. Then*

$$\Pr(E[S] - S \geq t) \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right).$$

**Lemma 1.** *Let $c := 1 - \frac{1}{18 \log p} < 1$. For $n$ a positive multiple of 3, we have* $\dim L_{n,(p-1)n/3} \leq p^{cn}$.

*Proof.* Denote by $\binom{n}{k}_{p-1} := |\{a \in \{0,1,\ldots,p-1\}^n : |a| = k\}|$ the extended binomial coefficients (see e.g. [6]). So we have $\dim L_{n,d} = \sum_{k=0}^{d} \binom{n}{k}_{p-1}$. Let $X_1, \ldots, X_n$ be i.i.d. random variables with $\Pr[X_i = t] = \frac{1}{p}$ for $t = 0, \ldots, p-1$. Let $S := X_1 + \cdots + X_n$. It is easy to see that $\binom{n}{k}_{p-1} = p^n \Pr[X = k]$. The expected value of $S$ equals $\frac{1}{2}(p-1)n$.

By Hoeffding's inequality, we have

$$\Pr[S \leq \tfrac{1}{3}(p-1)n] = \Pr[S \leq \tfrac{1}{2}(p-1)n - \tfrac{1}{6}(p-1)n] \leq e^{-\frac{1}{18}n}.$$

It follows that

$$\dim L_{n,(p-1)n/3} \leq p^n \cdot e^{-\frac{1}{18}n} = p^{n\cdot(1-\frac{1}{18\log p})} = p^{cn}.$$

$\square$

**Proposition 1.** *The evaluation map $\phi : L_n \to \mathbb{F}^{\mathbb{F}^n}$ given by $\phi(f) = (f(a))_{a\in\mathbb{F}^n}$ is a linear bijection.*

*Proof.* The fact that $\phi$ is linear is clear. Since $\dim L_n = \mathbb{F}^n = \dim \mathbb{F}^{\mathbb{F}^n}$, it suffices to show that $\phi$ is injective. We will show this by induction on $n$. If $n = 1$, this follows since a nonzero polynomial $f = c_0 + c_1x_1 + \cdots + c_{p-1}x_1^{p-1}$ has at most $p - 1 < p$ roots in $\mathbb{F}$.

Now let $n \geq 2$ and let $f \in L_n$ be such that $Z(f) = \mathbb{F}^n$. We need to show that $f = 0$. Write $f = f_0 + x_nf_1 + x_n^2f_2 + \cdots + x_n^{p-1}f_{p-1}$, where $f_0, \ldots, f_{q-1} \in L_{n-1}$. Observe that for any $a_1, \ldots, a_{n-1} \in \mathbb{F}$ the univariate polynomial $g(x_n) := \sum_{i=0}^{p-1} x_n^i \cdot f_i(a_1, \ldots, a_{n-1})$ evaluates to zero on the whole of $\mathbb{F}$ and therefore is the zero polynomial. That is, for all $a_1, \ldots, a_{n-1}$ and all $i = 0, \ldots, p-1$ we have $f_i(a_1, \ldots, a_{n-1}) = 0$. By induction it follows that $f_i = 0$ for $i = 0, \ldots, p-1$ and hence that $f = 0$. $\square$

**Lemma 2.** *Let $g = \sum_{\alpha,\beta} C_{\alpha,\beta}\, x^\alpha y^\beta \in \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_m]$, where $C \in \mathbb{F}^{\mathbb{N}^n\times\mathbb{N}^m}$. Let $A \subseteq \mathbb{F}^n$ and $B \subseteq \mathbb{F}^m$. Define the matrix $M \in \mathbb{F}^{A\times B}$ by $M_{ab} := g(a,b)$. Then* $\operatorname{rank} M \leq \operatorname{rank} C$.

*Proof.* Let $M_A \in \mathbb{F}^{\mathbb{N}^n\times A}$, $M_B \in \mathbb{F}^{\mathbb{N}^m\times B}$ be defined by $(M_A)_{\alpha,a} := a^\alpha$ and $(M_B)_{\beta,b} := b^\beta$. It is easy to check that $M := M_A^{\mathsf{T}} C M_B$. Hence, $\operatorname{rank} M \leq \operatorname{rank} C$. $\square$

**Proposition 2.** *Let $f \in L_{n,2d}$ and let $A \subseteq \mathbb{F}^n$. Suppose that for all $a, b \in A$ we have: $f(a+b) = 0$ if and only if $a \neq b$. Then $|A| \leq 2\dim L_{n,d}$.*

*Proof.* Let $g \in \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ be defined by $g(x,y) := f(x+y)$. So $g$ has degree at most $2d$. Write $g = \sum_{\alpha,\beta} C_{\alpha,\beta}x^\alpha y^\beta$. Note that $C_{\alpha,\beta}$ is nonzero only if $|\alpha| \leq d$ or $|\beta| \leq d$. It follows that the support of $C$ is contained in the union of the rows indexed by monomials of degree at most $d$ and the columns indexed by monomials of degree at most $d$. Hence, $\operatorname{rank} C \leq 2\dim L_{n,d}$.

On the other hand, the $A \times A$ matrix $M$ defined by $M_{a,b} := g(a,b)$ is a diagonal matrix with nonzero diagonal elements and therefore has rank $|A|$. By Lemma 2, it follows that $|A| = \operatorname{rank} M \leq \operatorname{rank} C \leq 2\dim L_{n,d}$. $\square$

**Theorem 2** (Main theorem)**.** *Let $c := 1 - \frac{1}{18\log p} < 1$. For $A \subseteq \mathbb{F}^n$ progression free, we have $|A| = O(p^{cn})$.*

*Proof.* Let $n$ be a multiple of 3 and let $A \subseteq \mathbb{F}^n$ be progression free. It suffices to show that $|A| \leq 3p^{cn}$.

Define $B := \{a + b \mid a, b \in A \text{ with } a \neq b\}$ and $C := \{a + a \mid a \in A\}$. Since $A$ is progression-free we have $B \cap C = \emptyset$. Let

$$\begin{aligned} K &:= \{f \in L_n \mid (\mathbb{F}^n \setminus C) \subseteq Z(f)\}, \\ L &:= L_{n,\frac{2}{3}(p-1)n}. \end{aligned}$$

Note that $K$ is a linear space of dimension $|C|$ by Proposition 1. By Lemma 1, $L$ is a linear space of dimension

$$\dim L \geq p^n - \dim L_{n,\frac{1}{3}(p-1)n-1} \geq p^n - p^{cn}.$$

Denote $V := K \cap L$. We have

$$\dim V \geq \dim L + \dim K - p^n \geq |C| - p^{cn}. \tag{1}$$

In particular, we may assume that $V$ has positive dimension, for otherwise $|A| = |C| \leq p^{cn}$, and we would be done.

By Proposition 1, we can view $V$ as a linear subspace of $\mathbb{F}^C$. Hence, there is a subset $C' \subseteq C$ of size $\dim V$ such that the evaluation map $\phi : V \to \mathbb{F}^{C'}$ given by $\phi(f) := (f(c))_{c \in C'}$ is surjective. Hence, we can choose $f \in V$ such that $f(c) = 1$ for all $c \in C'$.

Let $A' := \{a \in A \mid a + a \in C'\}$. Since $p$ is odd, we have $|A'| = |C'|$. Since $f \in K$, we have $B \subseteq (\mathbb{F}^n \setminus C) \subseteq Z(f)$. This implies that $f(a+b) = 0$ for all $a, b \in A'$ distinct. By our choice of $f$ we also have $f(a+a) = 1$ for all $a \in A'$. Since $f$ has degree at most $\frac{2}{3}(p-1)n$, Proposition 2 implies that $|A'| \leq 2 \dim L_{n, \frac{1}{3}(p-1)n} = 2 \dim L$. Hence, $|C'| = |A'| \leq 2p^{cn}$. By (1), we obtain

$$|A| = |C| \leq p^{cn} + \dim V = p^{cn} + |C'| \leq 3p^{cn}.$$

$\square$

In the special case $p = 3$, progression-free sets correspond exactly to affine caps. The best known *lower* bound for affine caps in $\mathbb{F}_3^n$ is $\Omega(2.2174^n)$ due to Edel [3]. Since $3^{1 - \frac{1}{18 \log 3}} = 2.84\cdot$, Theorem 2 implies an *upper* bound of $O(2.84^n)$, improving the previous best upper bound of $O(\frac{3^n}{n^{1+\epsilon}})$ due to Bateman and Katz [1].

**Corollary 1.** *The maximum size of an affine cap in $\mathbb{F}_3^n$ is $O(2.84^n)$.*

# Acknowledgements

The author would like to thank Jop Briët, Viresh Patel, Guus Regts and Jeroen Zuiddam for very useful discussions on the polynomial method, which ultimately led to the current paper.

# References

[1] M. Bateman, N.H. Katz, New bounds on cap sets, *J. Math. Soc.* 25.2 (2012), 585–613.

[2] E. Croot, V. Lev, P. Pach, Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small, arXiv preprint arXiv:1605.01506.

[3] Y. Edel, Extensions of generalized product caps, *Designs, Codes and Cryptography* 31.1 (2004), 5–14.

[4] J.S. Ellenberg, On large subsets of $\mathbb{F}_3^n$ with no three-term arithmetic progression. `http://quomodocumque.files.wordpress.com/2016/05/cap-set.pdf`

[5] J.S. Ellenberg, D. Gijswijt, On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression, arXiv preprint arXiv:1605.09223.

[6] N.E. Fahssi, Polynomial triangles revisited, arXiv preprint arXiv:1202.0228.

[7] W. Hoeffding, Probability inequalities for sums of bounded random variables, *Journal of the American statistical association* 58.301 (1963), 13–30.

[8] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, *J. Combin. Theory Ser. A* 71.1 (1995), 168–172.