Constructions of Large Caps and Progression-Free Sets

Gabriel F. Lipnik

Joint Work with Christian Elsholtz and Benjamin Klahn

Seminar of the Doctoral School

January 15, 2021

Graz University of Technology

DOCTORAL PROGRAM
DISCRETE MATHEMATICS
TU & KFU GRAZ • MU LEOBEN
AUSTRIA

Plan for the Following 25 Minutes

What are caps?

Previously known bounds for the size of largest caps

New results on lower bounds and overview of the method

Example

Details on our construction

Results on arithmetic progressions

additive combinatorics

Objects of Interest: Caps

Definition

An affine (resp. projective) **cap** is a
subset of the affine (resp. projective) space
in which **no three points lie on a line**.

We mainly consider *affine caps* in $\mathbb{F}_p^n = (\mathbb{Z}/p\mathbb{Z})^n$ for primes p, and we set

$$C(\mathbb{F}_p^n) := \max\{|S| \colon S \text{ is a cap in } \mathbb{F}_p^n\}.$$

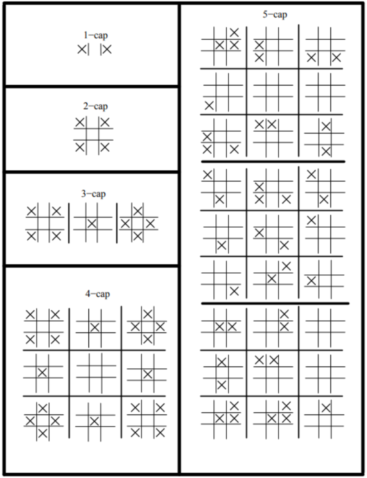
Aim:

construction of large caps in $\mathbb{F}_p^n$ for primes p and arbitrary dimension n

$\hookrightarrow$ **good lower bounds** for $C(\mathbb{F}_p^n)$

Since every subset of an affine space can be embedded into the projective space, our lower bounds also hold in the projective case.

Some Maximal Caps in $\mathbb{F}_3^n$ for $1 \leq n \leq 5$



- Situation gets complicated very fast.
- It is difficult to find maximal caps in high dimensions.

  $\rightsquigarrow$ **bounds**

Upper Bounds

For $p \in \{3,4,5\}$, we have

$$\text{“no three points on a line”} \iff \text{“no three points in AP”}.$$

Theorem

- Ellenberg–Gijswijt (2016): $C(\mathbb{F}_3^n) \leq 2.756^n$,
- Croot–Lev–Pach (2016): $C(\mathbb{Z}_4^n) \leq 3.611^n$.

Theorem (Blasiak–Church–Cohn et al. 2017)

We have

$$C(\mathbb{F}_p^n) \leq (J(p)p)^n,$$

where

$$J(p) = \frac{1}{p} \min_{0<t<1} \frac{1-t^p}{(1-t)t^{(p-1)/3}}.$$

Previously Known Lower Bounds

Best known general constructions so far are "**local**":

take the **tensor product of a large cap in small dimension**

For a fixed prime p, we have:

Theorem (Bose 1947)

$$C(\mathbb{F}_p^3) = p^2 \quad \text{and so} \quad C(\mathbb{F}_p^n) \gg p^{2n/3}.$$

Theorem (Edel–Bierbrauer 2004)

$$C(\mathbb{F}_p^6) \geq p^4 + p^2 - 1 \quad \text{and so} \quad C(\mathbb{F}_p^n) \gg (p^4 + p^2 - 1)^{n/6}.$$

Theorem (Elsholtz–Pach 2020)

$$C(\mathbb{Z}_4^n) \gg \frac{3^n}{\sqrt{n}} \quad \text{and} \quad C(\mathbb{F}_5^n) \gg \frac{3^n}{\sqrt{n}}.$$

Our Results

Theorem (Elsholtz–L 2020+)

$$C(\mathbb{F}_{11}^n) \gg \frac{5^n}{n^{1.5}}, \quad C(\mathbb{F}_{17}^n) \gg \frac{7^n}{n^{2.5}}, \quad C(\mathbb{F}_{23}^n) \gg \frac{9^n}{n^{3.5}},$$

$$C(\mathbb{F}_{29}^n) \gg \frac{10^n}{n^4}, \quad C(\mathbb{F}_{41}^n) \gg \frac{12^n}{n^5}.$$

- exponential improvements for **all primes** $p \leq 41$ **with** $p \equiv 5 \bmod 6$
- "**global**" and "**digit-based**" construction based on
  the method of Elsholtz and Pach for progression-free sets
- **basic idea** of the construction:
  For vectors in the cap,
  select a "good" set of digits $D \subseteq \mathbb{F}_p$
  and only use these digits for the vectors.
  $\hookrightarrow$ **caps of size** $(|D| - o(1))^n$

Comparison of the Lower Bounds

In order to get rid of the dimension in $C(\mathbb{F}_p^n)$, we define

$$c(p) := \lim_{n\to\infty} \left(C(\mathbb{F}_p^n)\right)^{1/n}.$$

It is known that the limit exists and $c(p) \in [2, p)$.

p	$p^{2/3}$	$(p^4 + p^2 - 1)^{1/6}$	new	improvement
5	2.92401...	2.94243...	**3**	1.9562%
7	3.65930...	3.67139...	3	
11	4.94608...	4.95282...	**5**	0.9526%
13	5.52877...	5.53418...	4	
17	6.61148...	6.61528...	**7**	5.8156%
19	7.12036...	7.12364...	6	
23	8.08757...	8.09012...	**9**	11.2468%
29	9.43913...	9.44099...	$\geq$ **10**	$\geq$ 5.9210%
31	9.86827...	9.86998...	≥ 8	
37	11.10370...	11.10505...	≥ 10	
41	11.89020...	11.89138...	$\geq$ **12**	$\geq$ 0.9134%

Overview of the Construction

For a fixed prime p and

some **set of digits** $D \subseteq \mathbb{F}_p$,

we consider the set

$$S(D,n) := \left\{ (a_1,\dots,a_n) \in D^n \;\middle|\; \forall d \in D\colon\, a_i = d \text{ for } \frac{n}{|D|} \text{ values of } i \right\}.$$

We call D **good** if $S(D,n)$ is a cap for all appropriate $n \in \mathbb{N}$.
By Stirling's formula, we obtain

$$|S(D,n)| = \prod_{\ell=0}^{|D|-1} \binom{n - \frac{\ell n}{|D|}}{\frac{n}{|D|}} \sim \frac{c|D|^n}{n^\delta}$$

with

$$\delta = \frac{|D|-1}{2} \quad \text{and} \quad c = \frac{1}{\sqrt{1-\delta/|D|}} \left(\frac{|D|}{2\pi}\right)^{\delta/2}.$$

Connection and Difference to APs

Three-term arithmetic progressions are solutions of the equation

$$x - 2y + z = 0. \qquad (\star)$$

Three points x, y, $z \in \mathbb{F}_p^n$ are **not collinear** if and only if

$$ax + by + cz \neq 0 \quad \text{for all } (a,b,c) \in \mathbb{F}_p^3 \setminus \{(0,0,0)\}$$

$$\text{with } a + b + c = 0.$$

Without loss of generality, we can assume $a = 1$ and $b \notin \{-1, 0\}$.

Three points x, y, $z \in \mathbb{F}_p^n$ are **not collinear** if and only if

$$x + by + (-b-1)z \neq 0 \quad \text{for all } b \in \mathbb{F}_p \setminus \{-1, 0\}. \qquad (\star\star)$$

$\hookrightarrow$ still $p - 2$ equations to consider

Idea: Apply the method of Elsholtz and Pach not only to $(\star)$, but also to the other equations $(\star\star)$ corresponding to "weighted progressions".

$\rightsquigarrow$ **much more involved**

Example: $p = 11$

We choose

- the digit set $D = \{0, 1, 3, 4, 5\}$.

If D is good, then this implies

$$C(\mathbb{F}_{11}^n) \gg \frac{5^n}{n^2}.$$

Equivalent equations:

- $\{x - 2y + z = 0, x - 10y + 9z = 0, x - 6y + 5z = 0\}$,
- $\{x - 3y + 2z = 0, x - 7y + 6z = 0, x - 9y + 8z = 0,$
  $x - 5y + 4z = 0, x - 8y + 7z = 0, x - 4y + 3z = 0\}$.

1. $x - 2y + z = 0$:

$$P_{-2}(D) = \{(1, 3, 5), (3, 4, 5), (5, 3, 1), (5, 4, 3)\}$$
$$\hookrightarrow \{(3, 4, 5), (5, 4, 3)\} \quad \to \emptyset$$

2. $x - 3y + 2z = 0$:

$$P_{-3}(D) = \{(1, 0, 5), (1, 3, 4), (1, 4, 0), (3, 0, 4),$$
$$(3, 1, 0), (4, 1, 5), (4, 5, 0), (5, 0, 3)\} \quad \to \emptyset$$

Finding Good Digit Sets (I)

We fix $b \in \mathbb{F}_p \setminus \{-1, 0\}$ and $D \subseteq \mathbb{F}_p$, and set

$$P_b(D) = \Big\{(x, y, z) \in D^3 \,\Big|\, x + by + (-b-1)z = 0\Big\} \setminus \Big\langle (1,1,1) \Big\rangle.$$

Assume that there is some $n \in \mathbb{N}$ with $|D| \mid n$ such that there are 3 points

$$x = (x_1, \ldots, x_n)^\top,\ \ y = (y_1, \ldots, y_n)^\top,\ \ z = (z_1, \ldots, z_n)^\top \in S(D, n)$$

which satisfy $x + by + (-b-1)z = 0$.
$\rightsquigarrow$ **introduce variable χ_v** for each $v = (v_1, v_2, v_3) \in P_b(D)$ which describes the number of occurrences of v in the components of x, y, z, i.e.,

$$\chi_v = \Big|\big\{i \in \{1, \ldots, n\} \,\big|\, (x_i, y_i, z_i) = v\big\}\Big|.$$

Since every digit d in D has to occur the same number of times, we find

$$\sum_{\substack{v \in P_b(D) \\ v_1 = d}} \chi_v = \sum_{\substack{v \in P_b(D) \\ v_2 = d}} \chi_v \quad \text{and} \quad \sum_{\substack{v \in P_b(D) \\ v_1 = d}} \chi_v = \sum_{\substack{v \in P_b(D) \\ v_3 = d}} \chi_v.$$

Finding Good Digit Sets (II)

$$\sum_{\substack{v \in P_b(D) \\ v_1 = d}} \chi_v = \sum_{\substack{v \in P_b(D) \\ v_2 = d}} \chi_v \quad \text{and} \quad \sum_{\substack{v \in P_b(D) \\ v_1 = d}} \chi_v = \sum_{\substack{v \in P_b(D) \\ v_3 = d}} \chi_v \qquad (\star)$$

$S(D, n)$ does not contain x, y, z with $x + by + (-b-1)z = 0$ for any appropriate n. $\iff$ System $(\star)$ has no non-trivial non-negative integral solution $\chi = (\chi_v \mid v \in P_b(D))$.

Hence, to show the "goodness" of some D, one has to ensure that

$$\mathcal{P} = \{\chi \in \mathbb{Z}^{\ell}_{\geq 0} \mid A \cdot \chi = 0\}$$

is empty, where the matrix A represents $(\star)$.

$\rightsquigarrow$ **integer programming**

- Appropriate software is available. ☺
- Checking the emptiness of $\mathcal{P}$ is NP-complete. ☹

$\rightsquigarrow$ **simpler conditions required**

Arithmetic Progressions

Let $r_k(\mathbb{F}_p^n)$ denote the size of the largest progression-free set in $\mathbb{F}_p^n$.

Theorem (Lin–Wolf 2010)

If $k \leq p$, then we have

$$r_k(\mathbb{F}_p^n) \geq \left(p^{2(k-1)} + p^{k-1} - 1\right)^{\frac{n}{2k}} \approx p^{\frac{(k-1)n}{k}}.$$

Theorem (Elsholtz–Pach 2020)

For $p \geq 5$ and some explicitly given constant d_p, we have

$$r_3(\mathbb{F}_p^n) \geq \frac{d_p}{\sqrt{n}}\left(\frac{p+1}{2}\right)^n.$$

Theorem (Elsholtz–Klahn–L 2020+)

$$r_5(\mathbb{F}_{23}^n) \gg (17 - o(1))^n \qquad \text{(improving on } 12.28^n\text{)}$$

$$r_7(\mathbb{F}_{29}^n) \gg (24 - o(1))^n \qquad \text{(improving on } 17.92^n\text{)}$$

Thank you for your attention!