Constructions of Large Caps

Gabriel F. Lipnik

Joint Work with Christian Elsholtz

Additive Combinatorics in Marseille 2020

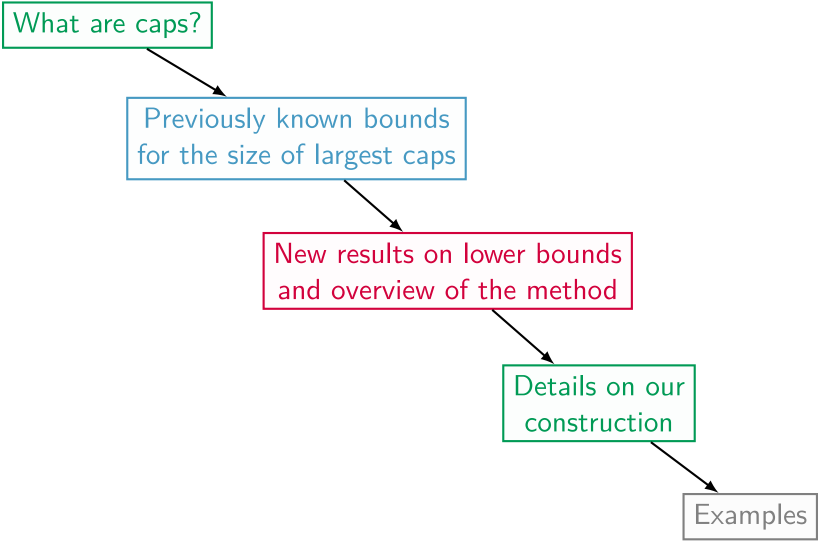
September 9, 2020

Graz University of Technology

DOCTORAL PROGRAM
DISCRETE MATHEMATICS

TU & KFU GRAZ • MU LEOBEN
AUSTRIA

Plan for the Following 30 Minutes



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

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

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.

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** $(|D| - o(1))^n$

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

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

It is known that both limits exist. Moreover, $c(p) \in [2, p)$ and $\mu(p) < 1$.

p	$p^{2/3}$	$(p^4 + p^2 - 1)^{1/6}$	new	improvement	$\mu(p)$
5	2.92401 . . .	2.94243 . . .	**3**	1.9562%	**0.6826 . . .**
7	3.65930 . . .	3.67139 . . .	3		0.5645 . . .
11	4.94608 . . .	4.95282 . . .	**5**	0.9526%	**0.6711 . . .**
13	5.52877 . . .	5.53418 . . .	4		0.5404 . . .
17	6.61148 . . .	6.61528 . . .	**7**	5.8156%	**0.6868 . . .**
19	7.12036 . . .	7.12364 . . .	6		0.6085 . . .
23	8.08757 . . .	8.09012 . . .	**9**	11.2468%	**0.7007 . . .**
29	9.43913 . . .	9.44099 . . .	$\geq$ **10**	$\geq$ 5.9210%	$\geq$ **0.6838 . . .**
31	9.86827 . . .	9.86998 . . .	≥ 8		$\geq$ 0.6055 . . .
37	11.10370 . . .	11.10505 . . .	≥ 10		$\geq$ 0.6376 . . .
41	11.89020 . . .	11.89138 . . .	$\geq$ **12**	$\geq$ 0.9134%	$\geq$ **0.6691 . . .**

Overview of the Construction

For a fixed prime p and

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

some set of **"fixed" digits** $D' \subseteq D$,

we consider the set

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

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

$$\left|S(D, D', n)\right| = \left(\prod_{\ell=0}^{|D'|-1} \binom{n - \frac{\ell n}{|D|}}{\frac{n}{|D|}} \right) \left(|D| - |D'|\right)^{n - \frac{|D'| n}{|D|}} \sim \frac{c|D|^n}{n^{\delta/2}}$$

with

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

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**

Finding Good Digit Sets (I)

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

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

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

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

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.,

$$\chi_v = \left|\left\{i \in \{1, \dots, n\} \,\middle|\, (x_i, y_i, z_i) = v\right\}\right|.$$

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)

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

$S(D, D', n)$ 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, D'), one has to ensure that

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

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

$\rightsquigarrow$ **integer programming**

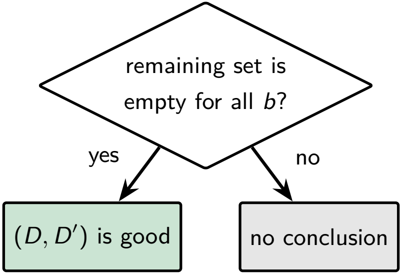
- Appropriate software is available. ☺
- Checking the emptiness of $\mathcal{P}$ is NP-complete. ☹

$\rightsquigarrow$ **simpler conditions required**

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

If there is some $r \in \{1,2,3\}$ and a digit $d \in D'$ such that
d' **does not occur in position** r **in any triple of** $P_b(D)$, then
remove all triples of $P_b(D)$ **which contain** d' **in any position**.
Proceed recursively with the remaining set.

Else: stop.



Equivalent Equations

We have already seen:

The "goodness" of (D, D') can be determined via $P_b(D)$.
The order of elements in $(x, y, z) \in P_b(D)$ does not matter.

- $(x, y, z) \in P_b(D) \iff (x, z, y) \in P_{-b-1}(D)$
  $\hookrightarrow$ **only one** of the equations

  $$x + by + (-b-1)z = 0 \quad \text{and} \quad x + (-b-1)y + bz = 0$$

  has to be considered
- $(x, y, z) \in P_b(D) \iff (z, y, x) \in P_{(-b-1)^{-1}b}(D)$
  $\hookrightarrow$ **only one** of the equations

  $$x + by + (-b-1)z = 0 \quad \text{and}$$

  $$x + (-b-1)^{-1}by + (-b-1)^{-1}z = 0$$

  has to be considered

$\rightsquigarrow$ **significant reduction** of the number of equations

Example: $p = 11$

We choose

- the digit set $D = \{0, 1, 3, 4, 5\}$ and "fixed" digits $D' = \{0, 1, 3\}$.

If (D, D') is good, then this implies

$$C(\mathbb{F}_{11}^n) \gg \frac{5^n}{n^{1.5}}.$$

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

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

We choose $D = D' = \{0, 1, 3, 4, 8, 9, 10, 12, 17\}$,
and we have **four non-equivalent equations**.

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

$$A = \begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\
0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & -1 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}$$

$$\vdots$$

Thank you for your attention!