Line-free sets in $\mathbb{F}_p^n$

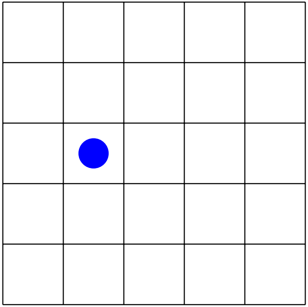
Jakob Führer
fuehrer@math.tugraz.at

joint work with
Christian Elsholtz, Erik Füredi, Benedek Kovács,
Péter Pál Pach, Dániel Gábor Simon and Nóra Velich

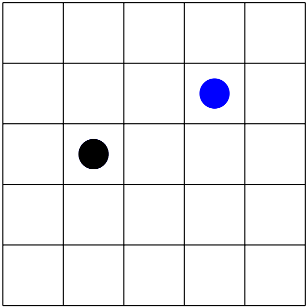
Graz University of Technology

20.09.2023

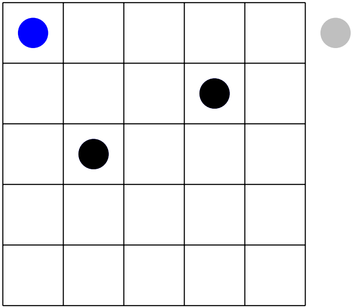
Introductory Example



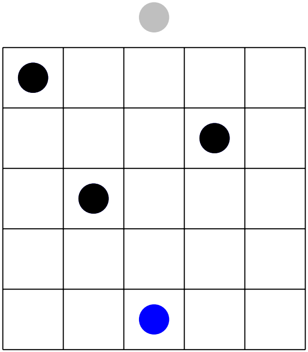
Introductory Example



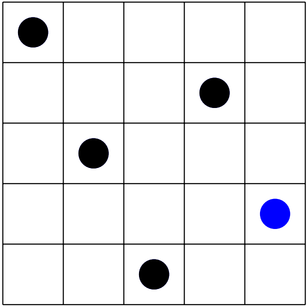
Introductory Example



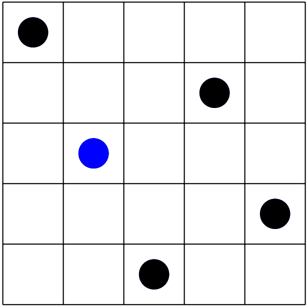
Introductory Example



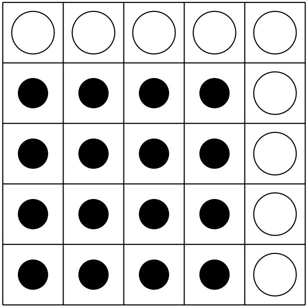
Introductory Example



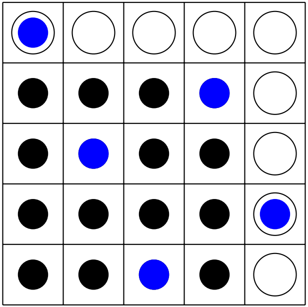
Introductory Example



Introductory Example



Introductory Example



Problem 1

Definition (progression-free sets)

Let $(A, +)$ be an abelian group and $k \in \mathbb{N}$. A subset $L \subseteq A$ with $|L| = k$ is called k-progression if there exist $a, b \in A$ such that

$$L = \{a + b \cdot i \mid i \in [0, k-1]\}.$$

A subset $S \subseteq A$ is called k-progression-free if it does not contain any k-progression.

Problem 1

Definition (progression-free sets)

Let $(A, +)$ be an abelian group and $k \in \mathbb{N}$. A subset $L \subseteq A$ with $|L| = k$ is called k-progression if there exist $a, b \in A$ such that

$$L = \{a + b \cdot i \mid i \in [0, k-1]\}.$$

A subset $S \subseteq A$ is called k-progression-free if it does not contain any k-progression.

Definition

Let $(A, +)$ be an abelian group and $k \in \mathbb{N}$. Let $\mathcal{S} := \{S \subseteq A \mid S \text{ is } k\text{-progression-free}\}$. We define

$$r_k(A) := \max_{S \in \mathcal{S}} |S|.$$

Problem 2

Definition

We call sets of the form $a + b\mathbb{F}_q = \{a + b \cdot i \mid i \in \mathbb{F}_q\}$ lines in $\mathbb{F}_q^n$.

Problem 2

Definition

We call sets of the form $a + b\mathbb{F}_q = \{a + b \cdot i \mid i \in \mathbb{F}_q\}$ lines in $\mathbb{F}_q^n$.

Definition (no k on a line)

Let $k \in \mathbb{N}$. Let $\mathcal{S} := \{S \subseteq \mathbb{F}_q^n \mid S$ does not contain k points on a line$\}$.
We define

$$\bar{r}_k(\mathbb{F}_q^n) := \max_{S \in \mathcal{S}} |S|.$$

Comparing the problems

- $\bar{r}_k(\mathbb{F}_p^n) \leq r_k(\mathbb{F}_p^n)$.

Comparing the problems

- $\bar{r}_k(\mathbb{F}_p^n) \leq r_k(\mathbb{F}_p^n)$.
- "order" does matter for Problem 1.

Comparing the problems

- $\bar{r}_k(\mathbb{F}_p^n) \leq r_k(\mathbb{F}_p^n)$.
- "order" does matter for Problem 1.
- Problem 1 can be studied in $(\mathbb{Z}/m\mathbb{Z})^n$ where m is no prime.

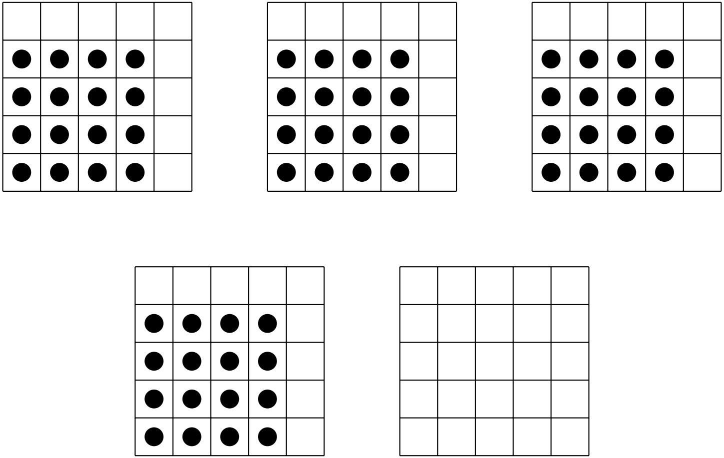
Comparing the problems

- $\bar{r}_k(\mathbb{F}_p^n) \leq r_k(\mathbb{F}_p^n)$.
- "order" does matter for Problem 1.
- Problem 1 can be studied in $(\mathbb{Z}/m\mathbb{Z})^n$ where m is no prime.
- Problem 2 can be studied in $\mathbb{F}_q^n$ where q is a prime power. Note that $\mathbb{F}_{p^\ell}^n \cong \mathbb{F}_p^{n\ell}$ as additive groups.

Comparing the problems

- $\bar{r}_k(\mathbb{F}_p^n) \leq r_k(\mathbb{F}_p^n)$.
- "order" does matter for Problem 1.
- Problem 1 can be studied in $(\mathbb{Z}/m\mathbb{Z})^n$ where m is no prime.
- Problem 2 can be studied in $\mathbb{F}_q^n$ where q is a prime power. Note that $\mathbb{F}_{p^\ell}^n \cong \mathbb{F}_p^{n\ell}$ as additive groups.
- $\bar{r}_p(\mathbb{F}_p^n) = r_p(\mathbb{F}_p^n)$ and the two problems coincide.

Trivial Lower Bounds



Trivial Lower Bound

Theorem

Let $p \in \mathbb{P}$ *and* $n \in \mathbb{N}$. *Then*

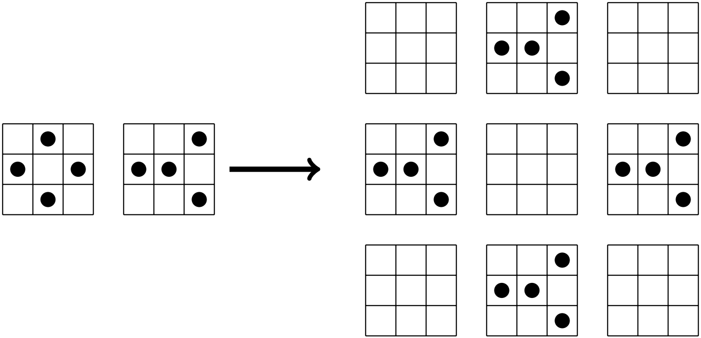
$$r_p(\mathbb{F}_p^n) \geq (p-1)^n.$$

Lifting To Higher Dimensions

Theorem

Let $p \in \mathbb{P}$ and $n_1, n_2 \in \mathbb{N}$. Then

$$r_p(\mathbb{F}_p^{n_1+n_2}) \geq r_p(\mathbb{F}_m^{n_1}) r_p(\mathbb{F}_m^{n_2}).$$



Lifting To Higher Dimensions

Theorem (Variation of Davis and Maclagan 2003)

Let $p \in \mathbb{P}$. Then the limit

$$\alpha_{p,p} := \lim_{n\to\infty} (r_p(\mathbb{F}_p^n))^{1/n}$$

exists and it holds that

$$p - 1 \leq \alpha_{p,p} \leq p.$$

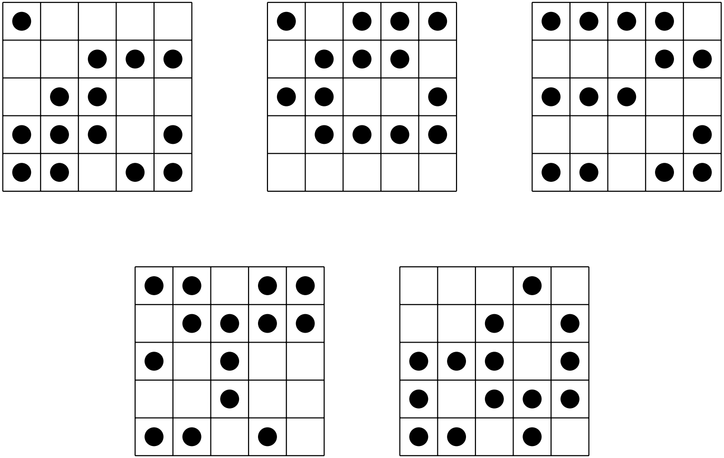
Moreover, if S is an p-progression-free set in $\mathbb{F}_p^{n'}$ then

$$\alpha_{p,p} \geq |S|^{1/n'},$$

i.e.

$$r_p(\mathbb{F}_p^n) \geq (|S|^{1/n'} + o(1))^n.$$

Approach 1: Computer based results



Approach 1: Computer based results

Theorem (E.F.F.K.P.S.V. 202?)

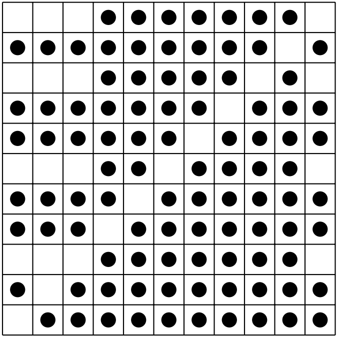
$r_5(\mathbb{F}_5^3) \geq 70,$

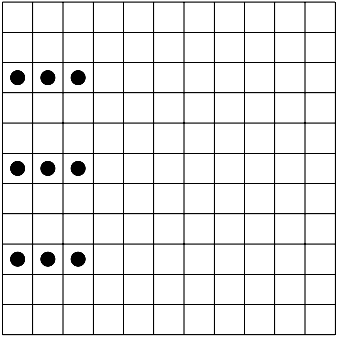
$$r_5(\mathbb{F}_5^n) \geq (4.121 + o(1))^n,$$

$r_7(\mathbb{F}_7^3) \geq 225,$

$$r_7(\mathbb{F}_7^n) \geq (6.082 + o(1))^n.$$

Approach 2: Combinatorial constructions





Approach 2: Combinatorial constructions

Theorem (E.F.F.K.P.S.V. 202?)

Let $p \in \mathbb{P} \setminus \{2\}$. *Then*

$$r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + p - 2\sqrt{p} + O(1).$$

Approach 2: Combinatorial constructions

Theorem (E.F.F.K.P.S.V. 202?)

Let $p \in \mathbb{P} \setminus \{2\}$. *Then*

$$r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + p - 2\sqrt{p} + O(1).$$

Theorem (E.F.F.K.P.S.V. 202?)

Let $p \in \mathbb{P} \setminus \{2\}$. *Then* $r_p(\mathbb{F}_p^n) \geq (p-1)^n + \frac{n-2}{2} \cdot (p-1)(p-2)^{n-3}$

Approach 3: Algebraic constructions

Use zero-sets of polynomials.

Approach 3: Algebraic constructions

Use zero-sets of polynomials.

Theorem (F. 202?)

Let q be a prime power and $k \in \mathbb{N}$ such that $k \leq q$ then

$$\bar{r}_k\left(\mathbb{F}_q^{(k^2-k)/2}\right) \geq q^{(k^2-k)/2-1}.$$

In particular,

$$r_p(\mathbb{F}_p^n) \geq \left(p^{1-\frac{2}{p^2-p}} + o(1)\right)^n,$$

and

$$r_p(\mathbb{F}_p^n) = (p + o(1))^n,$$

when both n and p tend to infinity.