The Erdős–Ginzburg–Ziv Problem in Discrete Geometry

Lisa Sauermann

University of Bonn

July 25, 2024

Introduction

The Erdős–Ginzburg–Ziv Problem is a classical extremal problem in discrete geometry.

Introduction

The Erdős–Ginzburg–Ziv Problem is a classical extremal problem in discrete geometry.

For given positive integers m and n it asks the following question.

Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Introduction

The Erdős–Ginzburg–Ziv Problem is a classical extremal problem in discrete geometry.

For given positive integers m and n it asks the following question.

Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Recall that the centroid of a collection of m points $p_1, \dots, p_m \in \mathbb{Z}^n$ is simply their average $(p_1 + \dots + p_m)/m \in \mathbb{R}^n$.

Introduction

The Erdős–Ginzburg–Ziv Problem is a classical extremal problem in discrete geometry.

For given positive integers m and n it asks the following question.

Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Recall that the centroid of a collection of m points $p_1, \dots, p_m \in \mathbb{Z}^n$ is simply their average $(p_1 + \dots + p_m)/m \in \mathbb{R}^n$.

We are looking for m points (among the given s points) such that $(p_1 + \dots + p_m)/m \in \mathbb{Z}^n$, i.e. such that all coordinates of the sum $p_1 + \dots + p_m$ are divisible by m.

Let n and m be given positive integers.

Erdős–Ginzburg–Ziv Problem

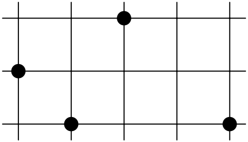
What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Let n and m be given positive integers.

Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Example for $n = 2$ and $m = 3$:

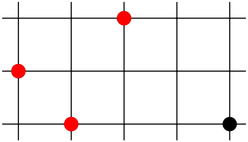


Let n and m be given positive integers.

Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Example for $n = 2$ and $m = 3$:

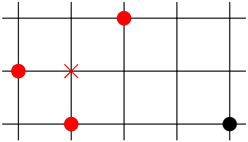


Let n and m be given positive integers.

Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Example for $n = 2$ and $m = 3$:

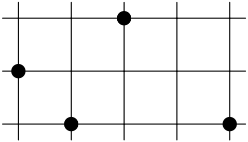


Let n and m be given positive integers.

Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Example for $n = 2$ and $m = 3$:



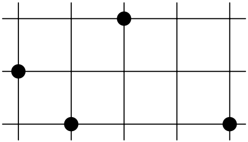
Among these four points in $\mathbb{Z}^2$ it is possible to find $m = 3$ points whose centroid is also a lattice point in $\mathbb{Z}^2$.

Let n and m be given positive integers.

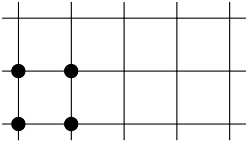
Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Example for $n = 2$ and $m = 3$:



Among these four points in $\mathbb{Z}^2$ it is possible to find $m = 3$ points whose centroid is also a lattice point in $\mathbb{Z}^2$.



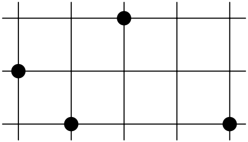
However, this is not always possible for four points in $\mathbb{Z}^2$.

Let n and m be given positive integers.

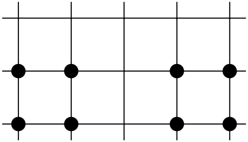
Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Example for $n = 2$ and $m = 3$:



Among these four points in $\mathbb{Z}^2$ it is possible to find $m = 3$ points whose centroid is also a lattice point in $\mathbb{Z}^2$.



However, this is not always possible for four points in $\mathbb{Z}^2$.

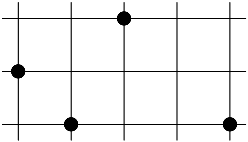
In fact this is not even always possible for eight points in $\mathbb{Z}^2$.

Let n and m be given positive integers.

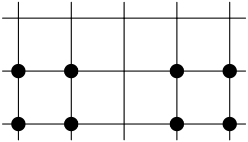
Erdős–Ginzburg–Ziv Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Example for $n = 2$ and $m = 3$:



Among these four points in $\mathbb{Z}^2$ it is possible to find $m = 3$ points whose centroid is also a lattice point in $\mathbb{Z}^2$.



However, this is not always possible for four points in $\mathbb{Z}^2$.

In fact this is not even always possible for eight points in $\mathbb{Z}^2$.

For $n = 2$ and $m = 3$, one needs $s = 9$ points.

Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

The answer to this question is called the Erdős–Ginzburg–Ziv constant $\mathfrak{s}(\mathbb{Z}_m^n)$.

Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

The answer to this question is called the Erdős–Ginzburg–Ziv constant $\mathfrak{s}(\mathbb{Z}_m^n)$.

(This notation reflects that this problem can be translated to a problem about sequences in $\mathbb{Z}_m^n$, since in fact only the remainders modulo m of the coordinates of the points are relevant.)

Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

The answer to this question is called the Erdős–Ginzburg–Ziv constant $\mathfrak{s}(\mathbb{Z}_m^n)$.

(This notation reflects that this problem can be translated to a problem about sequences in $\mathbb{Z}_m^n$, since in fact only the remainders modulo m of the coordinates of the points are relevant.)

Erdős–Ginzburg–Ziv constants have been studied intensively, but there are only few known exact values for $\mathfrak{s}(\mathbb{Z}_m^n)$:

Problem

What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

The answer to this question is called the Erdős–Ginzburg–Ziv constant $\mathfrak{s}(\mathbb{Z}_m^n)$.

(This notation reflects that this problem can be translated to a problem about sequences in $\mathbb{Z}_m^n$, since in fact only the remainders modulo m of the coordinates of the points are relevant.)

Erdős–Ginzburg–Ziv constants have been studied intensively, but there are only few known exact values for $\mathfrak{s}(\mathbb{Z}_m^n)$:

- $n = 1$: $\mathfrak{s}(\mathbb{Z}_m^1) = 2m - 1$ (Erdős–Ginzburg–Ziv, 1961).
- $n = 2$: $\mathfrak{s}(\mathbb{Z}_m^2) = 4m - 3$ (Reiher, 2007).
- $n = 3$ and m has only certain prime factors : $\mathfrak{s}(\mathbb{Z}_m^3) = 9m - 8$.
- $n = 4$ and m is a power of 3: $\mathfrak{s}(\mathbb{Z}_m^4) = 20m - 19$ (Edel et al., 2007).
- m is a power of 2: $\mathfrak{s}(\mathbb{Z}_m^n) = (m - 1)2^n + 1$ (Harborth, 1973).

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$.

Rather than aiming to determine $\mathfrak{s}(\mathbb{Z}_m^n)$ exactly, one might try to understand how $\mathfrak{s}(\mathbb{Z}_m^n)$ behaves as a function of m and n.

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$.

Rather than aiming to determine $\mathfrak{s}(\mathbb{Z}_m^n)$ exactly, one might try to understand how $\mathfrak{s}(\mathbb{Z}_m^n)$ behaves as a function of m and n.

Theorem (Alon, Dubiner, 1995)

For fixed dimension n, the function $\mathfrak{s}(\mathbb{Z}_m^n)$ grows linearly with m.

Alon and Dubiner gave the upper bound $\mathfrak{s}(\mathbb{Z}_m^n) \leq (cn \log n)^n \cdot m$ for some absolute constant c.

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$.

Rather than aiming to determine $\mathfrak{s}(\mathbb{Z}_m^n)$ exactly, one might try to understand how $\mathfrak{s}(\mathbb{Z}_m^n)$ behaves as a function of m and n.

Theorem (Alon, Dubiner, 1995)

For fixed dimension n, the function $\mathfrak{s}(\mathbb{Z}_m^n)$ grows linearly with m.

Alon and Dubiner gave the upper bound $\mathfrak{s}(\mathbb{Z}_m^n) \leq (cn \log n)^n \cdot m$ for some absolute constant c.

Zakharov (2020+) improved their bound to $\mathfrak{s}(\mathbb{Z}_m^n) \leq 4^n \cdot m$ in the case where m is a prime that is sufficiently large with respect to n.

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$.

Rather than aiming to determine $\mathfrak{s}(\mathbb{Z}_m^n)$ exactly, one might try to understand how $\mathfrak{s}(\mathbb{Z}_m^n)$ behaves as a function of m and n.

Theorem (Alon, Dubiner, 1995)

For fixed dimension n, the function $\mathfrak{s}(\mathbb{Z}_m^n)$ grows linearly with m.

Alon and Dubiner gave the upper bound $\mathfrak{s}(\mathbb{Z}_m^n) \leq (cn \log n)^n \cdot m$ for some absolute constant c.

Zakharov (2020+) improved their bound to $\mathfrak{s}(\mathbb{Z}_m^n) \leq 4^n \cdot m$ in the case where m is a prime that is sufficiently large with respect to n.

Open Problem

What happens in the opposite regime, when m is fixed and the dimension n is large?

Reducing to $m = p$ prime

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$.

Reducing to $m = p$ prime

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$.

If $m = k\ell$, the following lemma gives an upper bound for $\mathfrak{s}(\mathbb{Z}_m^n)$ in terms of $\mathfrak{s}(\mathbb{Z}_k^n)$ and $\mathfrak{s}(\mathbb{Z}_\ell^n)$.

Lemma

$\mathfrak{s}(\mathbb{Z}_{k\ell}^n) \leq \ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$.

Reducing to $m = p$ prime

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$.

If $m = k\ell$, the following lemma gives an upper bound for $\mathfrak{s}(\mathbb{Z}_m^n)$ in terms of $\mathfrak{s}(\mathbb{Z}_k^n)$ and $\mathfrak{s}(\mathbb{Z}_\ell^n)$.

Lemma

$\mathfrak{s}(\mathbb{Z}_{k\ell}^n) \leq \ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$.

This lemma can be used in all of the previously mentioned upper bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ in order to reduce to the case where m is a prime.

In other words, for these upper bounds it suffices to study $\mathfrak{s}(\mathbb{Z}_p^n) = \mathfrak{s}(\mathbb{F}_p^n)$ for a prime p.

Lemma

$\mathfrak{s}(\mathbb{Z}_{k\ell}^n) \leq \ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$.

Lemma

$\mathfrak{s}(\mathbb{Z}_{k\ell}^n) \leq \ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$.

Proof: Consider a set S of $\ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$ points in $\mathbb{Z}^n$.

We need to find $k\ell$ points in S whose centroid is a lattice point in $\mathbb{Z}^n$.

Lemma

$\mathfrak{s}(\mathbb{Z}_{k\ell}^n) \leq \ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$.

Proof: Consider a set S of $\ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$ points in $\mathbb{Z}^n$.

We need to find $k\ell$ points in S whose centroid is a lattice point in $\mathbb{Z}^n$.

First, we can find ℓ points in S whose centroid is a lattice point in $\mathbb{Z}^n$. Let us delete these ℓ points from S and repeat the process (again finding ℓ points whose centroid is in $\mathbb{Z}^n$).

Lemma

$\mathfrak{s}(\mathbb{Z}_{k\ell}^n) \leq \ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$.

Proof: Consider a set S of $\ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$ points in $\mathbb{Z}^n$.

We need to find $k\ell$ points in S whose centroid is a lattice point in $\mathbb{Z}^n$.

First, we can find ℓ points in S whose centroid is a lattice point in $\mathbb{Z}^n$. Let us delete these ℓ points from S and repeat the process (again finding ℓ points whose centroid is in $\mathbb{Z}^n$).

After having found $\mathfrak{s}(\mathbb{Z}_k^n) - 1$ groups of ℓ points, we still have $\mathfrak{s}(\mathbb{Z}_\ell^n)$ points left and can find another group of ℓ points.

Lemma

$\mathfrak{s}(\mathbb{Z}_{k\ell}^n) \leq \ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$.

Proof: Consider a set S of $\ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$ points in $\mathbb{Z}^n$.

We need to find $k\ell$ points in S whose centroid is a lattice point in $\mathbb{Z}^n$.

First, we can find ℓ points in S whose centroid is a lattice point in $\mathbb{Z}^n$. Let us delete these ℓ points from S and repeat the process (again finding ℓ points whose centroid is in $\mathbb{Z}^n$).

After having found $\mathfrak{s}(\mathbb{Z}_k^n) - 1$ groups of ℓ points, we still have $\mathfrak{s}(\mathbb{Z}_\ell^n)$ points left and can find another group of ℓ points.

In total, we have found $\mathfrak{s}(\mathbb{Z}_k^n)$ groups of ℓ points, so that each group has a centroid in $\mathbb{Z}^n$. Among these $\mathfrak{s}(\mathbb{Z}_k^n)$ centroid points, we can find k centroid points whose centroid is a lattice point in $\mathbb{Z}^n$.

Lemma

$\mathfrak{s}(\mathbb{Z}_{k\ell}^n) \leq \ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$.

Proof: Consider a set S of $\ell \cdot (\mathfrak{s}(\mathbb{Z}_k^n) - 1) + \mathfrak{s}(\mathbb{Z}_\ell^n)$ points in $\mathbb{Z}^n$.

We need to find $k\ell$ points in S whose centroid is a lattice point in $\mathbb{Z}^n$.

First, we can find ℓ points in S whose centroid is a lattice point in $\mathbb{Z}^n$. Let us delete these ℓ points from S and repeat the process (again finding ℓ points whose centroid is in $\mathbb{Z}^n$).

After having found $\mathfrak{s}(\mathbb{Z}_k^n) - 1$ groups of ℓ points, we still have $\mathfrak{s}(\mathbb{Z}_\ell^n)$ points left and can find another group of ℓ points.

In total, we have found $\mathfrak{s}(\mathbb{Z}_k^n)$ groups of ℓ points, so that each group has a centroid in $\mathbb{Z}^n$. Among these $\mathfrak{s}(\mathbb{Z}_k^n)$ centroid points, we can find k centroid points whose centroid is a lattice point in $\mathbb{Z}^n$.

Considering the corresponding k groups of size ℓ, gives $k\ell$ points in S whose centroid is a lattice point in $\mathbb{Z}^n$.

Proof techniques for small dimension n

All of the previously mentioned bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ can be reduced to the case where $m = p$ is a prime (with the lemma on the last slide).

Proof techniques for small dimension n

All of the previously mentioned bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ can be reduced to the case where $m = p$ is a prime (with the lemma on the last slide).

Theorem (Erdős, Ginzburg, Ziv, 1961)

For dimension $n = 1$, we have $\mathfrak{s}(\mathbb{F}_p^1) = 2p - 1$.

This can be proved as an easy application of the Combinatorial Nullstellensatz (due to Alon, 1999), although the original proof of Erdős, Ginzburg, and Ziv was different.

Proof techniques for small dimension n

All of the previously mentioned bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ can be reduced to the case where $m = p$ is a prime (with the lemma on the last slide).

Theorem (Erdős, Ginzburg, Ziv, 1961)

For dimension $n = 1$, we have $\mathfrak{s}(\mathbb{F}_p^1) = 2p - 1$.

This can be proved as an easy application of the Combinatorial Nullstellensatz (due to Alon, 1999), although the original proof of Erdős, Ginzburg, and Ziv was different.

Theorem (Reiher, 2007)

For dimension $n = 2$, we have $\mathfrak{s}(\mathbb{F}_p^2) = 4p - 3$.

This also be proved with the Combinatorial Nullstellensatz (or the Chevalley–Warning Theorem), but the proof is much more involved.

Theorem (Alon, Dubiner, 1995)

For fixed dimension n, the function $\mathfrak{s}(\mathbb{F}_p^n)$ grows linearly in p.

The proof is by induction on the dimension n. The induction step relies on results from additive combinatorics, as well as arguments using spectral graph theory (i.e. studying eigenvalues of certain matrices).

Theorem (Alon, Dubiner, 1995)

For fixed dimension n, the function $\mathfrak{s}(\mathbb{F}_p^n)$ grows linearly in p.

The proof is by induction on the dimension n. The induction step relies on results from additive combinatorics, as well as arguments using spectral graph theory (i.e. studying eigenvalues of certain matrices).

The proofs of all of these results for $\mathfrak{s}(\mathbb{F}_p^n)$ for small dimension n rely on algebraic techniques.

The techniques used for $n = 1$ and $n = 2$ are very different from the techniques for fixed $n > 2$ (even though all of these techniques are in some sense algebraic).

Theorem (Alon, Dubiner, 1995)

For fixed dimension n, the function $\mathfrak{s}(\mathbb{F}_p^n)$ grows linearly in p.

The proof is by induction on the dimension n. The induction step relies on results from additive combinatorics, as well as arguments using spectral graph theory (i.e. studying eigenvalues of certain matrices).

The proofs of all of these results for $\mathfrak{s}(\mathbb{F}_p^n)$ for small dimension n rely on algebraic techniques.

The techniques used for $n = 1$ and $n = 2$ are very different from the techniques for fixed $n > 2$ (even though all of these techniques are in some sense algebraic).

None of these approaches seems to work for large dimension n.

Open Problem

How large is $\mathfrak{s}(\mathbb{F}_p^n)$ for a fixed prime $p \geq 3$ and large dimension n?

$\mathfrak{s}(\mathbb{F}_p^n)$ for a fixed prime p

Assume from now on that $p \geq 3$ is a fixed prime and n is large.

Definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are p points whose centroid is also a lattice point in $\mathbb{Z}^n$.

$\mathfrak{s}(\mathbb{F}_p^n)$ for a fixed prime p

Assume from now on that $p \geq 3$ is a fixed prime and n is large.

Definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are p points whose centroid is also a lattice point in $\mathbb{Z}^n$.

Note that for p points in $\mathbb{Z}^n$, the centroid is a lattice point in $\mathbb{Z}^n$ precisely when the sum of the p points has all coordinates divisible by p.

$\mathfrak{s}(\mathbb{F}_p^n)$ for a fixed prime p

Assume from now on that $p \geq 3$ is a fixed prime and n is large.

Definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are p points whose centroid is also a lattice point in $\mathbb{Z}^n$.

Note that for p points in $\mathbb{Z}^n$, the centroid is a lattice point in $\mathbb{Z}^n$ precisely when the sum of the p points has all coordinates divisible by p.

We can consider the points as (possibly repeated) elements of $\mathbb{Z}_p^n = \mathbb{F}_p^n$. We are then trying to find p elements of $\mathbb{F}_p^n$ whose sum is the zero vector in $\mathbb{F}_p^n$.

$\mathfrak{s}(\mathbb{F}_p^n)$ for a fixed prime p

Assume from now on that $p \geq 3$ is a fixed prime and n is large.

Definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any s points in the lattice $\mathbb{Z}^n$ there are p points whose centroid is also a lattice point in $\mathbb{Z}^n$.

Note that for p points in $\mathbb{Z}^n$, the centroid is a lattice point in $\mathbb{Z}^n$ precisely when the sum of the p points has all coordinates divisible by p.

We can consider the points as (possibly repeated) elements of $\mathbb{Z}_p^n = \mathbb{F}_p^n$. We are then trying to find p elements of $\mathbb{F}_p^n$ whose sum is the zero vector in $\mathbb{F}_p^n$.

Equivalent definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any sequence of s elements of $\mathbb{F}_p^n$ there is a subsequence of length p whose elements have sum zero.

Definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any sequence of s elements of $\mathbb{F}_p^n$ there is a subsequence of length p whose elements have sum zero.

Definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any sequence of s elements of $\mathbb{F}_p^n$ there is a subsequence of length p whose elements have sum zero.

Equivalently, $\mathfrak{s}(\mathbb{F}_p^n) - 1$ is the answer to the following problem.

Problem

What is the maximum possible length of a sequence of elements of $\mathbb{F}_p^n$ without a subsequence of length p summing to zero?

Definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any sequence of s elements of $\mathbb{F}_p^n$ there is a subsequence of length p whose elements have sum zero.

Equivalently, $\mathfrak{s}(\mathbb{F}_p^n) - 1$ is the answer to the following problem.

Problem

What is the maximum possible length of a sequence of elements of $\mathbb{F}_p^n$ without a subsequence of length p summing to zero?

Note that every element of $\mathbb{F}_p^n$ can occur in such a sequence at most $p-1$ times (otherwise, the p copies of the same element form a subsequence of length p summing to zero).

Definition

$\mathfrak{s}(\mathbb{F}_p^n)$ is the minimum integer s such that among any sequence of s elements of $\mathbb{F}_p^n$ there is a subsequence of length p whose elements have sum zero.

Equivalently, $\mathfrak{s}(\mathbb{F}_p^n) - 1$ is the answer to the following problem.

Problem

What is the maximum possible length of a sequence of elements of $\mathbb{F}_p^n$ without a subsequence of length p summing to zero?

Note that every element of $\mathbb{F}_p^n$ can occur in such a sequence at most $p-1$ times (otherwise, the p copies of the same element form a subsequence of length p summing to zero).

So, up to a factor of at most $p-1$, this problem is equivalent to:

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

Let $p \geq 3$ be a fixed prime and n large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

We have seen that $\mathfrak{s}(\mathbb{F}_p^n)$ agrees with the answer to this problem up to a constant factor (if p is fixed).

Let $p \geq 3$ be a fixed prime and n large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

We have seen that $\mathfrak{s}(\mathbb{F}_p^n)$ agrees with the answer to this problem up to a constant factor (if p is fixed).

An easy lower bound for the problem above is 2^n (consider the subset $\{0,1\}^n \subseteq \mathbb{F}_p^n$).

Let $p \geq 3$ be a fixed prime and n large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

We have seen that $\mathfrak{s}(\mathbb{F}_p^n)$ agrees with the answer to this problem up to a constant factor (if p is fixed).

An easy lower bound for the problem above is 2^n (consider the subset $\{0,1\}^n \subseteq \mathbb{F}_p^n$).

The best known lower bound is roughly 2.1398^n for $p \geq 5$ (Edel, 2008) and roughly 2.2202^n for $p = 3$ (Romera-Paredes et al., 2024).

Let $p \geq 3$ be a fixed prime and n large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

We have seen that $\mathfrak{s}(\mathbb{F}_p^n)$ agrees with the answer to this problem up to a constant factor (if p is fixed).

An easy lower bound for the problem above is 2^n (consider the subset $\{0,1\}^n \subseteq \mathbb{F}_p^n$).

The best known lower bound is roughly 2.1398^n for $p \geq 5$ (Edel, 2008) and roughly 2.2202^n for $p = 3$ (Romera-Paredes et al., 2024).

For $p = 3$, we are asking about the maximum size of a subset $A \subseteq \mathbb{F}_3^n$ not containing distinct vectors $x, y, z \in A$ with $x + y + z = 0$.

Let $p \geq 3$ be a fixed prime and n large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

We have seen that $\mathfrak{s}(\mathbb{F}_p^n)$ agrees with the answer to this problem up to a constant factor (if p is fixed).

An easy lower bound for the problem above is 2^n (consider the subset $\{0,1\}^n \subseteq \mathbb{F}_p^n$).

The best known lower bound is roughly 2.1398^n for $p \geq 5$ (Edel, 2008) and roughly 2.2202^n for $p = 3$ (Romera-Paredes et al., 2024).

For $p = 3$, we are asking about the maximum size of a subset $A \subseteq \mathbb{F}_3^n$ not containing distinct vectors $x, y, z \in A$ with $x + y + z = 0$.

In characteristic 3, having $x + y + z = 0$ is equivalent to $x - 2y + z = 0$, i.e. to x, y, z forming an arithmetic progression.

For $p = 3$, determining $\mathfrak{s}(\mathbb{F}_3^n)$ is equivalent to the following problem.

Problem

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

For $p = 3$, determining $\mathfrak{s}(\mathbb{F}_3^n)$ is equivalent to the following problem.

Problem

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

This is a famous problem, called the *Cap-Set Problem*.

For $p = 3$, determining $\mathfrak{s}(\mathbb{F}_3^n)$ is equivalent to the following problem.

Problem

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

This is a famous problem, called the *Cap-Set Problem*.

More generally, studying the maximum size of progression-free subsets of $\mathbb{F}_p^n$ or $\{1, \ldots, N\}$ is a fundamental problem in additive combinatorics.

For $p = 3$, determining $\mathfrak{s}(\mathbb{F}_3^n)$ is equivalent to the following problem.

Problem

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

This is a famous problem, called the *Cap-Set Problem*.

More generally, studying the maximum size of progression-free subsets of $\mathbb{F}_p^n$ or $\{1, \ldots, N\}$ is a fundamental problem in additive combinatorics.

Theorem (Szemerédi, 1975)

For any fixed $k \geq 3$, the maximum size of a subset of $\{1, \ldots, N\}$ without a k-term arithmetic progression is of the form $o(N)$.

This was the main result described in Szemerédi's 2012 Abel Prize citation.

For $p = 3$, determining $\mathfrak{s}(\mathbb{F}_3^n)$ is equivalent to the following problem.

Problem

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

This is a famous problem, called the *Cap-Set Problem*.

More generally, studying the maximum size of progression-free subsets of $\mathbb{F}_p^n$ or $\{1, \ldots, N\}$ is a fundamental problem in additive combinatorics.

Theorem (Szemerédi, 1975)

For any fixed $k \geq 3$, the maximum size of a subset of $\{1, \ldots, N\}$ without a k-term arithmetic progression is of the form $o(N)$.

This was the main result described in Szemerédi's 2012 Abel Prize citation.

The behavior of the $o(N)$-term is still not understood, despite a lot of attention. For $k = 3$, a revolutionary new upper bound was shown by Kelley and Meka (2023+).

Problem (Cap-Set Problem)

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

Problem (Cap-Set Problem)

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

Upper bounds:

- trivial: 3^n

Problem (Cap-Set Problem)

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

Upper bounds:

- trivial: 3^n
- Pigeon-hole principle: $\frac{1}{2}(3^n + 1)$

Problem (Cap-Set Problem)

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

Upper bounds:

- trivial: 3^n
- Pigeon-hole principle: $\frac{1}{2}(3^n + 1)$
- Meshulam (1995): $O(3^n/n)$

Problem (Cap-Set Problem)

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

Upper bounds:

- trivial: 3^n
- Pigeon-hole principle: $\frac{1}{2}(3^n + 1)$
- Meshulam (1995): $O(3^n/n)$
- Bateman–Katz (2012): $O(3^n/n^{1+\varepsilon})$ for some constant $\varepsilon > 0$

Problem (Cap-Set Problem)

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

Upper bounds:

- trivial: 3^n
- Pigeon-hole principle: $\frac{1}{2}(3^n + 1)$
- Meshulam (1995): $O(3^n/n)$
- Bateman–Katz (2012): $O(3^n/n^{1+\varepsilon})$ for some constant $\varepsilon > 0$

Problem (Cap-Set Problem)

What is the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression
(i.e. without distinct vectors x, y, z with $x - 2y + z = 0$)?

Upper bounds:

- trivial: 3^n
- Pigeon-hole principle: $\frac{1}{2}(3^n + 1)$
- Meshulam (1995): $O(3^n/n)$
- Bateman–Katz (2012): $O(3^n/n^{1+\varepsilon})$ for some constant $\varepsilon > 0$

In 2017, Ellenberg and Gijswijt achieved a breakthrough on this problem, improving *exponentially* upon the trivial upper bound 3^n.

Theorem (Ellenberg, Gijswijt, 2017)

If $A \subseteq \mathbb{F}_3^n$ does not contain a three-term arithmetic progression, then $|A| \leq 2.756^n$.

Ellenberg and Gijswijt actually proved a more general result for $\mathbb{F}_p^n$ for any fixed prime $p \geq 3$:

Ellenberg and Gijswijt actually proved a more general result for $\mathbb{F}_p^n$ for any fixed prime $p \geq 3$:

Theorem (Ellenberg, Gijswijt, 2017)

Let $p \geq 3$ be prime. If $A \subseteq \mathbb{F}_p^n$ does not contain a three-term arithmetic progression, then $|A| \leq (\Gamma_p)^n$, for some $\Gamma_p < p$ (only depending on p).

Ellenberg and Gijswijt actually proved a more general result for $\mathbb{F}_p^n$ for any fixed prime $p \geq 3$:

Theorem (Ellenberg, Gijswijt, 2017)

Let $p \geq 3$ be prime. If $A \subseteq \mathbb{F}_p^n$ does not contain a three-term arithmetic progression, then $|A| \leq (\Gamma_p)^n$, for some $\Gamma_p < p$ (only depending on p).

The proof gives the the following value for Γ_p:

$$\Gamma_p = \min_{0<t<1} \frac{1 + t + \cdots + t^{p-1}}{t^{(p-1)/3}},$$

This Γ_p satisfies $0.8414p \leq \Gamma_p \leq 0.9184p$.

Ellenberg and Gijswijt actually proved a more general result for $\mathbb{F}_p^n$ for any fixed prime $p \geq 3$:

Theorem (Ellenberg, Gijswijt, 2017)

Let $p \geq 3$ be prime. If $A \subseteq \mathbb{F}_p^n$ does not contain a three-term arithmetic progression, then $|A| \leq (\Gamma_p)^n$, for some $\Gamma_p < p$ (only depending on p).

The proof gives the the following value for Γ_p:

$$\Gamma_p = \min_{0<t<1} \frac{1 + t + \cdots + t^{p-1}}{t^{(p-1)/3}},$$

This Γ_p satisfies $0.8414p \leq \Gamma_p \leq 0.9184p$.

For $p = 3$, we have $\Gamma_3 \approx 2.756$, giving the bound $|A| \leq 2.756^n$.

Ellenberg and Gijswijt actually proved a more general result for $\mathbb{F}_p^n$ for any fixed prime $p \geq 3$:

Theorem (Ellenberg, Gijswijt, 2017)

Let $p \geq 3$ be prime. If $A \subseteq \mathbb{F}_p^n$ does not contain a three-term arithmetic progression, then $|A| \leq (\Gamma_p)^n$, for some $\Gamma_p < p$ (only depending on p).

The proof gives the the following value for Γ_p:

$$\Gamma_p = \min_{0<t<1} \frac{1 + t + \cdots + t^{p-1}}{t^{(p-1)/3}},$$

This Γ_p satisfies $0.8414p \leq \Gamma_p \leq 0.9184p$.

For $p = 3$, we have $\Gamma_3 \approx 2.756$, giving the bound $|A| \leq 2.756^n$.

It is not known whether the constant Γ_p defined above is tight. The best known general lower bound is $\Gamma_p \geq \sqrt{7/24}p \approx 0.54p$ (Elsholtz–Hunter–Proske–S., 2024+).

Ellenberg and Gijswijt actually proved a more general result for $\mathbb{F}_p^n$ for any fixed prime $p \geq 3$:

Theorem (Ellenberg, Gijswijt, 2017)

Let $p \geq 3$ be prime. If $A \subseteq \mathbb{F}_p^n$ does not contain a three-term arithmetic progression, then $|A| \leq (\Gamma_p)^n$, for some $\Gamma_p < p$ (only depending on p).

The proof gives the the following value for Γ_p:

$$\Gamma_p = \min_{0<t<1} \frac{1 + t + \cdots + t^{p-1}}{t^{(p-1)/3}},$$

This Γ_p satisfies $0.8414p \leq \Gamma_p \leq 0.9184p$.

For $p = 3$, we have $\Gamma_3 \approx 2.756$, giving the bound $|A| \leq 2.756^n$.

It is not known whether the constant Γ_p defined above is tight. The best known general lower bound is $\Gamma_p \geq \sqrt{7/24}p \approx 0.54p$ (Elsholtz–Hunter–Proske–S., 2024+).

However, Γ_p is tight for a certain "multi-colored" generalization of this result (Kleinberg–Sawin–Speyer, Norin, Pebody).

Theorem (Ellenberg, Gijswijt, 2017)

If $A \subseteq \mathbb{F}_3^n$ does not contain a three-term arithmetic progression, then $|A| \leq 2.756^n$.

The proof of Ellenberg and Gijswijt used a new polynomial method introduced by Croot, Lev and Pach only a few weeks earlier.

Theorem (Ellenberg, Gijswijt, 2017)

If $A \subseteq \mathbb{F}_3^n$ does not contain a three-term arithmetic progression, then $|A| \leq 2.756^n$.

The proof of Ellenberg and Gijswijt used a new polynomial method introduced by Croot, Lev and Pach only a few weeks earlier.

A few weeks later, Tao introduced a reformulation of this method, now called the *slice rank polynomial method*.

Theorem (Ellenberg, Gijswijt, 2017)

If $A \subseteq \mathbb{F}_3^n$ does not contain a three-term arithmetic progression, then $|A| \leq 2.756^n$.

The proof of Ellenberg and Gijswijt used a new polynomial method introduced by Croot, Lev and Pach only a few weeks earlier.

A few weeks later, Tao introduced a reformulation of this method, now called the *slice rank polynomial method*.

The result above gives the following corollary concerning $\mathfrak{s}(\mathbb{F}_3^n)$ for $p = 3$.

Corollary

$\mathfrak{s}(\mathbb{F}_3^n) \leq 1 + 2 \cdot 2.756^n$.

Theorem (Ellenberg, Gijswijt, 2017)

If $A \subseteq \mathbb{F}_3^n$ does not contain a three-term arithmetic progression, then $|A| \leq 2.756^n$.

The proof of Ellenberg and Gijswijt used a new polynomial method introduced by Croot, Lev and Pach only a few weeks earlier.

A few weeks later, Tao introduced a reformulation of this method, now called the *slice rank polynomial method*.

The result above gives the following corollary concerning $\mathfrak{s}(\mathbb{F}_3^n)$ for $p = 3$.

Corollary

$\mathfrak{s}(\mathbb{F}_3^n) \leq 1 + 2 \cdot 2.756^n$.

Again, the proof relies on an algebraic technique (using polynomials), but in a very different way than the results on $\mathfrak{s}(\mathbb{F}_p^n)$ for small dimension n.

For fixed $p \geq 3$, determining $\mathfrak{s}(\mathbb{F}_p^n)$ is equivalent to the following problem (up to constant factors depending on p).

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

For fixed $p \geq 3$, determining $\mathfrak{s}(\mathbb{F}_p^n)$ is equivalent to the following problem (up to constant factors depending on p).

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

For $p = 3$, this problem is the Cap-Set Problem, and by the result of Ellenberg–Gijswijt we have an upper bound of 2.756^n.

For fixed $p \geq 3$, determining $\mathfrak{s}(\mathbb{F}_p^n)$ is equivalent to the following problem (up to constant factors depending on p).

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

For $p = 3$, this problem is the Cap-Set Problem, and by the result of Ellenberg–Gijswijt we have an upper bound of 2.756^n.

It is natural to also try to apply the slice rank polynomial method to this problem for $p \geq 5$.

For fixed $p \geq 3$, determining $\mathfrak{s}(\mathbb{F}_p^n)$ is equivalent to the following problem (up to constant factors depending on p).

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

For $p = 3$, this problem is the Cap-Set Problem, and by the result of Ellenberg–Gijswijt we have an upper bound of 2.756^n.

It is natural to also try to apply the slice rank polynomial method to this problem for $p \geq 5$.

However, this does not work. The problem is that the natural tensor associated with this problem is not a diagonal tensor, and so one does not have a good lower bound for its slice rank.

The fact that the tensor is not necessarily diagonal is due to the distinctness condition in the problem above.

Let $p \geq 5$ be a fixed prime, and let n be large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

Let $p \geq 5$ be a fixed prime, and let n be large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

In other words, we are asking for the maximum size of a subset $A \subseteq \mathbb{F}_p^n$ with no solution for $x_1 + \cdots + x_p = 0$ with $x_1, \ldots, x_p \in A$ being distinct.

Let $p \geq 5$ be a fixed prime, and let n be large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

In other words, we are asking for the maximum size of a subset $A \subseteq \mathbb{F}_p^n$ with no solution for $x_1 + \cdots + x_p = 0$ with $x_1, \ldots, x_p \in A$ being distinct.

Let $p \geq 5$ be a fixed prime, and let n be large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

In other words, we are asking for the maximum size of a subset $A \subseteq \mathbb{F}_p^n$ with no solution for $x_1 + \cdots + x_p = 0$ with $x_1, \ldots, x_p \in A$ being distinct.

Similar-looking problem

What is the maximum size of a subset of $A \subseteq \mathbb{F}_p^n$ with no solution for $x_1 + \cdots + x_p = 0$ with $x_1, \ldots, x_p \in A$ being not all equal.

Let $p \geq 5$ be a fixed prime, and let n be large.

Problem

What is the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero?

In other words, we are asking for the maximum size of a subset $A \subseteq \mathbb{F}_p^n$ with no solution for $x_1 + \cdots + x_p = 0$ with $x_1, \ldots, x_p \in A$ being distinct.

Similar-looking problem

What is the maximum size of a subset of $A \subseteq \mathbb{F}_p^n$ with no solution for $x_1 + \cdots + x_p = 0$ with $x_1, \ldots, x_p \in A$ being not all equal.

Here, we have $|A| < 4^n$. This is a straightforward application of the slice rank polynomial method.

However, this argument fails for the top problem because we do not have a diagonal tensor anymore.

Results for fixed $p \geq 5$ and large n

Let $p \geq 5$ be a fixed prime and n large.

Problem

What is the maximum size of a subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero?

Results for fixed $p \geq 5$ and large n

Let $p \geq 5$ be a fixed prime and n large.

Problem

What is the maximum size of a subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero?

Clearly, $|A| \leq p^n$.

Results for fixed $p \geq 5$ and large n

Let $p \geq 5$ be a fixed prime and n large.

Problem

What is the maximum size of a subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero?

Clearly, $|A| \leq p^n$. Naslund proved that $|A|$ must be *exponentially smaller* than p^n.

Theorem (Naslund, 2020)

If $A \subseteq \mathbb{F}_p^n$ does not contain p distinct elements summing to zero, then $|A| \leq (2^p - p - 2) \cdot \Gamma_p^n$.

Here, $\Gamma_p < p$ is the constant in the Ellenberg–Gijswijt bound for progression-free subsets of $\mathbb{F}_p^n$. It satisfies $0.8414p \leq \Gamma_p \leq 0.9184p$.

Results for fixed $p \geq 5$ and large n

Let $p \geq 5$ be a fixed prime and n large.

Problem

What is the maximum size of a subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero?

Clearly, $|A| \leq p^n$. Naslund proved that $|A|$ must be *exponentially smaller* than p^n.

Theorem (Naslund, 2020)

If $A \subseteq \mathbb{F}_p^n$ does not contain p distinct elements summing to zero, then $|A| \leq (2^p - p - 2) \cdot \Gamma_p^n$.

Here, $\Gamma_p < p$ is the constant in the Ellenberg–Gijswijt bound for progression-free subsets of $\mathbb{F}_p^n$. It satisfies $0.8414p \leq \Gamma_p \leq 0.9184p$.

So this bound is exponentially better than the trivial bound $|A| \leq p^n$, but the base Γ_p is still is linear in p.

Let $p \geq 5$ be a fixed prime and n large.

Theorem (S., 2021)

If $A \subseteq \mathbb{F}_p^n$ does not contain p distinct elements summing to zero, then $|A| \leq C_p \cdot \left(2\sqrt{p}\right)^n$ for some constant C_p only depending on p.

Let $p \geq 5$ be a fixed prime and n large.

Theorem (S., 2021)

If $A \subseteq \mathbb{F}_p^n$ does not contain p distinct elements summing to zero, then $|A| \leq C_p \cdot (2\sqrt{p})^n$ for some constant C_p only depending on p.

The proof combines the slice rank polynomial method with combinatorial ideas (in order to overcome the problem of the tensor not being diagonal).

Let $p \geq 5$ be a fixed prime and n large.

Theorem (S., 2021)

If $A \subseteq \mathbb{F}_p^n$ does not contain p distinct elements summing to zero, then $|A| \leq C_p \cdot \left(2\sqrt{p}\right)^n$ for some constant C_p only depending on p.

The proof combines the slice rank polynomial method with combinatorial ideas (in order to overcome the problem of the tensor not being diagonal).

The same proof gives a "multi-colored" generalization (which is somewhat technical to state).

Interestingly, in this multi-colored generalization the bound is almost tight (there is a lower bound $\sqrt{p}^n$ for even n).

Let $p \geq 5$ be a fixed prime and n large.

Theorem (S., 2021)

If $A \subseteq \mathbb{F}_p^n$ does not contain p distinct elements summing to zero, then $|A| \leq C_p \cdot (2\sqrt{p})^n$ for some constant C_p only depending on p.

The proof combines the slice rank polynomial method with combinatorial ideas (in order to overcome the problem of the tensor not being diagonal).

The same proof gives a "multi-colored" generalization (which is somewhat technical to state).

Interestingly, in this multi-colored generalization the bound is almost tight (there is a lower bound $\sqrt{p}^n$ for even n).

This is similar to the situation for the Cap-Set Problem, where the bound is known to be tight for the "multi-colored" generalization.

Let $p \geq 5$ be a fixed prime and n large.

Theorem (S., 2021)

If $A \subseteq \mathbb{F}_p^n$ does not contain p distinct elements summing to zero, then $|A| \leq C_p \cdot (2\sqrt{p})^n$ for some constant C_p only depending on p.

The proof combines the slice rank polynomial method with combinatorial ideas (in order to overcome the problem of the tensor not being diagonal).

The same proof gives a "multi-colored" generalization (which is somewhat technical to state).

Interestingly, in this multi-colored generalization the bound is almost tight (there is a lower bound $\sqrt{p}^n$ for even n).

This is similar to the situation for the Cap-Set Problem, where the bound is known to be tight for the "multi-colored" generalization.

One barrier to improving the result above or the bound for the Cap-Set Problem is that one needs an approach which does not generalize to the "multi-colored" setting.

Overcoming this barrier, in joint work with Zakharov, improved the bound as follows.

Theorem (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has a bound $|A| \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$ for any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero.

Overcoming this barrier, in joint work with Zakharov, improved the bound as follows.

Theorem (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has a bound $|A| \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$ for any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero.

The proof combines the slice rank polynomial method with combinatorial and probabilistic arguments, as well as a higher uniformity version of the Balog–Szemerédi–Gowers Theorem due to Borenstein–Croot (2011).

Overcoming this barrier, in joint work with Zakharov, improved the bound as follows.

Theorem (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has a bound $|A| \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$ for any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero.

The proof combines the slice rank polynomial method with combinatorial and probabilistic arguments, as well as a higher uniformity version of the Balog–Szemerédi–Gowers Theorem due to Borenstein–Croot (2011).

Corollary (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has $\mathfrak{s}(\mathbb{F}_p^n) \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$.

Overcoming this barrier, in joint work with Zakharov, improved the bound as follows.

Theorem (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has a bound $|A| \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$ for any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero.

The proof combines the slice rank polynomial method with combinatorial and probabilistic arguments, as well as a higher uniformity version of the Balog–Szemerédi–Gowers Theorem due to Borenstein–Croot (2011).

Corollary (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has $\mathfrak{s}(\mathbb{F}_p^n) \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$.

In particular, $\mathfrak{s}(\mathbb{F}_p^n) \leq D_p \cdot (C \cdot p^{0.01})^n$ for some absolute constant C.

A similar bound holds when replacing 0.01 by any fixed $\varepsilon > 0$.

Corollary (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has $\mathfrak{s}(\mathbb{F}_p^n) \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$.

Corollary (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has $\mathfrak{s}(\mathbb{F}_p^n) \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$.

The best lower bound for $\mathfrak{s}(\mathbb{F}_p^n)$ for fixed p and large n is roughly 2.1398^n (Edel, 2008).

Corollary (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has $\mathfrak{s}(\mathbb{F}_p^n) \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$.

The best lower bound for $\mathfrak{s}(\mathbb{F}_p^n)$ for fixed p and large n is roughly 2.1398^n (Edel, 2008).

Thus, there is still a significant gap between the upper and lower bounds. In particular, the following question is open.

Open problem

Is there a bound of the form $\mathfrak{s}(\mathbb{F}_p^n) \leq C_p \cdot c^n$ for some absolute constant c?

Corollary (S., Zakharov, 2023+)

For every fixed $\varepsilon > 0$, for all primes p and all n, one has $\mathfrak{s}(\mathbb{F}_p^n) \leq D_{\varepsilon,p} \cdot (C_\varepsilon p^\varepsilon)^n$.

The best lower bound for $\mathfrak{s}(\mathbb{F}_p^n)$ for fixed p and large n is roughly 2.1398^n (Edel, 2008).

Thus, there is still a significant gap between the upper and lower bounds. In particular, the following question is open.

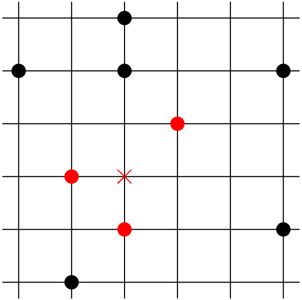
Open problem

Is there a bound of the form $\mathfrak{s}(\mathbb{F}_p^n) \leq C_p \cdot c^n$ for some absolute constant c?

In the opposite parameter regime, where n is fixed and p is large with respect to n, Zakharov (2020+) proved $\mathfrak{s}(\mathbb{F}_p^n) \leq p \cdot 4^n$.

However, his methods do not apply for fixed p and large n.

Thank you very much for your attention!



Combinatorial Theory

- Mathematician-run journal, owned by its editorial board
- Diamond Open Access: no fees for authors or readers
- Established in 2020, by the editorial board who resigned from Elsevier-owned JCTA

Combinatorial Theory

- Mathematician-run journal, owned by its editorial board
- Diamond Open Access: no fees for authors or readers
- Established in 2020, by the editorial board who resigned from Elsevier-owned JCTA
- The first volume published in 2021 with 19 papers
- Publisher: eScholarship (University of California Library System)
- Funded by MathOA and LYRASIS via The Combinatorics Consortium
- Indexed in MathSciNet and Zentralblatt (Scopus and Web of Science in progress)

Combinatorial Theory

- Mathematician-run journal, owned by its editorial board
- Diamond Open Access: no fees for authors or readers
- Established in 2020, by the editorial board who resigned from Elsevier-owned JCTA
- The first volume published in 2021 with 19 papers
- Publisher: eScholarship (University of California Library System)
- Funded by MathOA and LYRASIS via The Combinatorics Consortium
- Indexed in MathSciNet and Zentralblatt (Scopus and Web of Science in progress)
- Scope: Additive, Algebraic, Analytic, Enumerative, Extremal, Geometric, Topological, and Probabilistic Combinatorics, as well as theoretical aspects of their applications to other areas of mathematics and the sciences