On the size of subsets of $\mathbb{F}_p^n$ without p distinct elements summing to zero

Lisa Sauermann

Stanford University

September 2, 2019

Introduction

Let $p \geq 3$ be a prime.

Problem

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

Introduction

Let $p \geq 3$ be a prime.

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 is the famous cap-set problem asking for the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression.

Indeed, for $x, y, z \in \mathbb{F}_3^n$, we have $x + y + z = 0$ if and only if x, y, z form a three-term arithmetic progression.

Introduction

Let $p \geq 3$ be a prime.

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 is the famous cap-set problem asking for the maximum size of a subset of $\mathbb{F}_3^n$ without a three-term arithmetic progression.

Indeed, for $x, y, z \in \mathbb{F}_3^n$, we have $x + y + z = 0$ if and only if x, y, z form a three-term arithmetic progression.

We will consider the case $p \geq 5$ in this talk.

Erdős-Ginzburg-Ziv constants

Let m and n be positive integers.

Problem

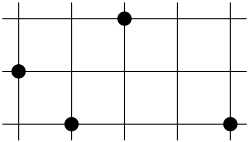
What is the minimum integer s such that among any s points in the integer lattice $\mathbb{Z}^n$ there are m points whose centroid is also a lattice point in $\mathbb{Z}^n$?

Erdős-Ginzburg-Ziv constants

Let m and n be positive integers.

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 $\mathbb{Z}^n$?

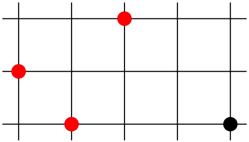


Erdős-Ginzburg-Ziv constants

Let m and n be positive integers.

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 $\mathbb{Z}^n$?

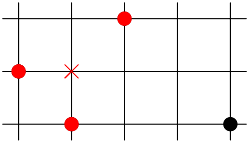


Erdős-Ginzburg-Ziv constants

Let m and n be positive integers.

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 $\mathbb{Z}^n$?

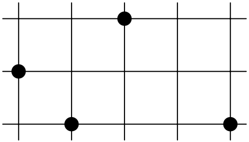


Erdős-Ginzburg-Ziv constants

Let m and n be positive integers.

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 $\mathbb{Z}^n$?



Equivalent problem

What is the is the minimum s such that every sequence of s (not necessarily distinct) elements of $\mathbb{Z}_m^n$ has a zero-sum subsequence of length m?

This number s is the Erdős-Ginzburg-Ziv constant $\mathfrak{s}(\mathbb{Z}_m^n)$ of $\mathbb{Z}_m^n$.

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the smallest s such that every sequence of s (not necessarily distinct) elements of $\mathbb{Z}_m^n$ has a zero-sum subsequence of length m.

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the smallest s such that every sequence of s (not necessarily distinct) elements of $\mathbb{Z}_m^n$ has a zero-sum subsequence of length m.

The study of Erdős-Ginzburg-Ziv constants was initiated by a result of Erdős, Ginzburg and Ziv from 1961 which essentially states that $\mathfrak{s}(\mathbb{Z}_m) = 2m - 1$.

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the smallest s such that every sequence of s (not necessarily distinct) elements of $\mathbb{Z}_m^n$ has a zero-sum subsequence of length m.

The study of Erdős-Ginzburg-Ziv constants was initiated by a result of Erdős, Ginzburg and Ziv from 1961 which essentially states that $\mathfrak{s}(\mathbb{Z}_m) = 2m - 1$.

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

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the smallest s such that every sequence of s (not necessarily distinct) elements of $\mathbb{Z}_m^n$ has a zero-sum subsequence of length m.

The study of Erdős-Ginzburg-Ziv constants was initiated by a result of Erdős, Ginzburg and Ziv from 1961 which essentially states that $\mathfrak{s}(\mathbb{Z}_m) = 2m - 1$.

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

Alon and Dubiner proved that $\mathfrak{s}(\mathbb{Z}_m^n) \leq (cn \log n)^n m$ for some constant c. Thus, when n is fixed, $\mathfrak{s}(\mathbb{Z}_m^n)$ grows linearly with m.

Definition

$\mathfrak{s}(\mathbb{Z}_m^n)$ is the smallest s such that every sequence of s (not necessarily distinct) elements of $\mathbb{Z}_m^n$ has a zero-sum subsequence of length m.

The study of Erdős-Ginzburg-Ziv constants was initiated by a result of Erdős, Ginzburg and Ziv from 1961 which essentially states that $\mathfrak{s}(\mathbb{Z}_m) = 2m - 1$.

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

Alon and Dubiner proved that $\mathfrak{s}(\mathbb{Z}_m^n) \leq (cn \log n)^n m$ for some constant c. Thus, when n is fixed, $\mathfrak{s}(\mathbb{Z}_m^n)$ grows linearly with m.

They posed the problem of finding good upper bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ for fixed m and large n.

Alon and Dubiner posed the problem of finding good upper bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ for fixed m and large n.

Alon and Dubiner posed the problem of finding good upper bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ for fixed m and large n.

The special case of finding upper bounds for $\mathfrak{s}(\mathbb{F}_p^n)$ for a fixed prime $p \geq 3$ and large n has received particular attention.

In fact, one can deduce bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ from bounds for $\mathfrak{s}(\mathbb{F}_p^n)$ for the prime factors p of m.

Alon and Dubiner posed the problem of finding good upper bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ for fixed m and large n.

The special case of finding upper bounds for $\mathfrak{s}(\mathbb{F}_p^n)$ for a fixed prime $p \geq 3$ and large n has received particular attention.

In fact, one can deduce bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ from bounds for $\mathfrak{s}(\mathbb{F}_p^n)$ for the prime factors p of m.

For a fixed prime $p \geq 3$ and large n, bounding $\mathfrak{s}(\mathbb{F}_p^n)$ is essentially equivalent to bounding the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero.

Alon and Dubiner posed the problem of finding good upper bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ for fixed m and large n.

The special case of finding upper bounds for $\mathfrak{s}(\mathbb{F}_p^n)$ for a fixed prime $p \geq 3$ and large n has received particular attention.

In fact, one can deduce bounds for $\mathfrak{s}(\mathbb{Z}_m^n)$ from bounds for $\mathfrak{s}(\mathbb{F}_p^n)$ for the prime factors p of m.

For a fixed prime $p \geq 3$ and large n, bounding $\mathfrak{s}(\mathbb{F}_p^n)$ is essentially equivalent to bounding the maximum size of a subset of $\mathbb{F}_p^n$ without p distinct elements summing to zero.

Problem

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

Background and Main Result

Let $p \geq 3$ be prime.

Problem

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

Background and Main Result

Let $p \geq 3$ be prime.

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.

Background and Main Result

Let $p \geq 3$ be prime.

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.

Background and Main Result

Let $p \geq 3$ be prime.

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.

Background and Main Result

Let $p \geq 3$ be prime.

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 an easy consequence of Tao's slice rank formulation of the Croot-Lev-Pach polynomial method.
However, this argument fails for the top problem.

Problem

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

Problem

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

Naslund introduced a variant of Tao's slice rank and used it to show $|A| \le (2^p - p - 2) \cdot \Gamma_p^n$.

Here, $\Gamma_p < p$ is the constant in the work of Ellenberg and Gijswijt on progression-free subsets of $\mathbb{F}_p^n$. It satisfies $0.8414p \le \Gamma_p \le 0.9184p$.

Problem

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

Naslund introduced a variant of Tao's slice rank and used it to show $|A| \leq (2^p - p - 2) \cdot \Gamma_p^n$.

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

Theorem (Ellenberg, Gijswijt, 2017)

Any subset of $\mathbb{F}_p^n$ without a three-term arithmetic progression has size at most Γ_p^n.

Ellenberg and Gijswijt's proof uses the Croot-Lev-Pach polynomial method.

Problem

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

Naslund introduced a variant of Tao's slice rank and used it to show $|A| \leq (2^p - p - 2) \cdot \Gamma_p^n$.

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

Theorem (Ellenberg, Gijswijt, 2017)

Any subset of $\mathbb{F}_p^n$ without a three-term arithmetic progression has size at most Γ_p^n.

Ellenberg and Gijswijt's proof uses the Croot-Lev-Pach polynomial method.

In joint work with Jacob Fox, we combined the result of Ellenberg and Gijswijt with a probabilistic subspace sampling argument to prove the bound $|A| \leq 3 \cdot \Gamma_p^n$ for the problem above.

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

Here,

$$\gamma_p = \min_{0<t<1} \frac{1 + t + \cdots + t^{p-1}}{t^{(p-1)/p}} < 4,$$

and C_p is a constant just depending on the prime p. One can take $C_p = 2p^2 \cdot P(p)$, where $P(p)$ denotes the number of partitions of p. Then C_p is exponential in $\sqrt{p}$.

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

Here,

$$\gamma_p = \min_{0<t<1} \frac{1 + t + \cdots + t^{p-1}}{t^{(p-1)/p}} < 4,$$

and C_p is a constant just depending on the prime p. One can take $C_p = 2p^2 \cdot P(p)$, where $P(p)$ denotes the number of partitions of p. Then C_p is exponential in $\sqrt{p}$.

For fixed $p \geq 5$ and large n, this significantly improves the previous bound $\mathfrak{s}(\mathbb{F}_p^n) \leq 3 \cdot \Gamma_p^n$. ($\Gamma_p$ is between $0.8414p$ and $0.9184p$)

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

Here,

$$\gamma_p = \min_{0<t<1} \frac{1+t+\cdots+t^{p-1}}{t^{(p-1)/p}} < 4,$$

and C_p is a constant just depending on the prime p. One can take $C_p = 2p^2 \cdot P(p)$, where $P(p)$ denotes the number of partitions of p. Then C_p is exponential in $\sqrt{p}$.

For fixed $p \geq 5$ and large n, this significantly improves the previous bound $\mathfrak{s}(\mathbb{F}_p^n) \leq 3 \cdot \Gamma_p^n$. ($\Gamma_p$ is between $0.8414p$ and $0.9184p$)

For large n and p, this bound is of the form $p^{(1/2-o(1))n}$, whereas all previous bounds were of the form $p^{(1-o(1))n}$.

Proof Overview

Our proof uses the multi-colored sum-free Theorem, which is a consequence of Tao's slice rank formulation of the Croot-Lev-Pach polynomial method.

Multi-colored sum-free Theorem

Let p be a prime, and let $(x_{1,i}, x_{2,i}, \dots, x_{p,i})_{i=1}^{m}$ be a collection of p-tuples in $\mathbb{F}_p^n \times \dots \times \mathbb{F}_p^n$ such that

$$x_{1,i_1} + x_{2,i_2} + \dots + x_{p,i_p} = 0 \quad \Leftrightarrow \quad i_1 = i_2 = \dots = i_p.$$

Then $m \le \gamma_p^n$.

Proof Overview

Our proof uses the multi-colored sum-free Theorem, which is a consequence of Tao's slice rank formulation of the Croot-Lev-Pach polynomial method.

Multi-colored sum-free Theorem

Let p be a prime, and let $(x_{1,i}, x_{2,i}, \dots, x_{p,i})_{i=1}^{m}$ be a collection of p-tuples in $\mathbb{F}_p^n \times \dots \times \mathbb{F}_p^n$ such that

$$x_{1,i_1} + x_{2,i_2} + \dots + x_{p,i_p} = 0 \quad \Leftrightarrow \quad i_1 = i_2 = \dots = i_p.$$

Then $m \leq \gamma_p^n$.

The constant γ_p is best-possible here (by joint work with László Miklós Lovász).

Proof Overview

Our proof uses the multi-colored sum-free Theorem, which is a consequence of Tao's slice rank formulation of the Croot-Lev-Pach polynomial method.

Multi-colored sum-free Theorem

Let p be a prime, and let $(x_{1,i}, x_{2,i}, \dots, x_{p,i})_{i=1}^{m}$ be a collection of p-tuples in $\mathbb{F}_p^n \times \cdots \times \mathbb{F}_p^n$ such that

$$x_{1,i_1} + x_{2,i_2} + \cdots + x_{p,i_p} = 0 \quad \Leftrightarrow \quad i_1 = i_2 = \cdots = i_p.$$

Then $m \leq \gamma_p^n$.

The constant γ_p is best-possible here (by joint work with László Miklós Lovász).

However, the multi-colored sum-free Theorem cannot be directly applied in our situation.

Proof Overview

Our proof uses the multi-colored sum-free Theorem, which is a consequence of Tao's slice rank formulation of the Croot-Lev-Pach polynomial method.

Multi-colored sum-free Theorem

Let p be a prime, and let $(x_{1,i}, x_{2,i}, \dots, x_{p,i})_{i=1}^{m}$ be a collection of p-tuples in $\mathbb{F}_p^n \times \dots \times \mathbb{F}_p^n$ such that

$$x_{1,i_1} + x_{2,i_2} + \dots + x_{p,i_p} = 0 \quad \Leftrightarrow \quad i_1 = i_2 = \dots = i_p.$$

Then $m \leq \gamma_p^n$.

The constant γ_p is best-possible here (by joint work with László Miklós Lovász).

However, the multi-colored sum-free Theorem cannot be directly applied in our situation.

We use new combinatorial ideas in order to be able to apply this theorem.

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n.$$

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

Let us say a p-tuple $(x_1, \dots, x_p) \in \mathbb{F}_p^n \times \dots \times \mathbb{F}_p^n$ is a *cycle* if $x_1 + \dots + x_p = 0$.

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

Let us say a p-tuple $(x_1, \dots, x_p) \in \mathbb{F}_p^n \times \cdots \times \mathbb{F}_p^n$ is a *cycle* if $x_1 + \cdots + x_p = 0$.

Call two cycles $(x_1, \dots, x_p), (x_1', \dots, x_p') \in \mathbb{F}_p^n \times \cdots \times \mathbb{F}_p^n$ disjoint if no element of $\mathbb{F}_p^n$ appears in both of them.

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

Let us say a p-tuple $(x_1, \ldots, x_p) \in \mathbb{F}_p^n \times \cdots \times \mathbb{F}_p^n$ is a *cycle* if $x_1 + \cdots + x_p = 0$.

Call two cycles $(x_1, \ldots, x_p), (x_1', \ldots, x_p') \in \mathbb{F}_p^n \times \cdots \times \mathbb{F}_p^n$ disjoint if no element of $\mathbb{F}_p^n$ appears in both of them.

Let $A \subseteq \mathbb{F}_p^n$ be as above. Then each cycle $(x_1, \ldots, x_p) \in A \times \cdots \times A$ contains some element of $\mathbb{F}_p^n$ at least twice.

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n.$$

Let us say a p-tuple $(x_1, \dots, x_p) \in \mathbb{F}_p^n \times \dots \times \mathbb{F}_p^n$ is a *cycle* if $x_1 + \dots + x_p = 0$.

Call two cycles $(x_1, \dots, x_p), (x_1', \dots, x_p') \in \mathbb{F}_p^n \times \dots \times \mathbb{F}_p^n$ disjoint if no element of $\mathbb{F}_p^n$ appears in both of them.

Let $A \subseteq \mathbb{F}_p^n$ be as above. Then each cycle $(x_1, \dots, x_p) \in A \times \dots \times A$ contains some element of $\mathbb{F}_p^n$ at least twice.

For a given cycle in $A \times \dots \times A$, we obtain a pattern of how many different elements of $\mathbb{F}_p^n$ occur in this cycle and with which multiplicities the different elements occur.

Each cycle $(x_1, \dots, x_p) \in A \times \cdots \times A$ contains some element of $\mathbb{F}_p^n$ at least twice.

We categorize the cycles $(x_1, \dots, x_p) \in A \times \cdots \times A$ by their multiplicity pattern.

Each cycle $(x_1, \dots, x_p) \in A \times \dots \times A$ contains some element of $\mathbb{F}_p^n$ at least twice.

We categorize the cycles $(x_1, \dots, x_p) \in A \times \dots \times A$ by their multiplicity pattern.

We go through all the possible multiplicity patterns (in a suitable order).

For each multiplicity pattern we can either find a large collection of disjoint cycles, or we can delete a small number of elements of A to destroy all cycles with this multiplicity pattern.

Each cycle $(x_1, \dots, x_p) \in A \times \cdots \times A$ contains some element of $\mathbb{F}_p^n$ at least twice.

We categorize the cycles $(x_1, \dots, x_p) \in A \times \cdots \times A$ by their multiplicity pattern.

We go through all the possible multiplicity patterns (in a suitable order).

For each multiplicity pattern we can either find a large collection of disjoint cycles, or we can delete a small number of elements of A to destroy all cycles with this multiplicity pattern.

This way, we construct subsets $Y_1, \dots, Y_p \subseteq \mathbb{F}_p^n$ such that:

- Each cycle $(x_1, \dots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.
- There is a collection of at least $|A|/(p \cdot P(p))$ disjoint cycles in $Y_1 \times \cdots \times Y_p$.

We constructed subsets $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ such that:

- Each cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.
- There is a collection $\mathcal{M}$ of at least $|A|/(p \cdot P(p))$ disjoint cycles in $Y_1 \times \cdots \times Y_p$.

We constructed subsets $Y_1, \dots, Y_p \subseteq \mathbb{F}_p^n$ such that:

- Each cycle $(x_1, \dots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.
- There is a collection $\mathcal{M}$ of at least $|A|/(p \cdot P(p))$ disjoint cycles in $Y_1 \times \cdots \times Y_p$.

Now, the following proposition finishes the proof of the theorem.

Proposition

Suppose that $Y_1, \dots, Y_p \subseteq \mathbb{F}_p^n$ are subsets such that every cycle $(x_1, \dots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.

Furthermore, suppose that $\mathcal{M}$ is a collection of disjoint cycles in $Y_1 \times \cdots \times Y_p$. Then $|\mathcal{M}| \leq 2p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n$.

We constructed subsets $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ such that:

- Each cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.
- There is a collection $\mathcal{M}$ of at least $|A|/(p \cdot P(p))$ disjoint cycles in $Y_1 \times \cdots \times Y_p$.

Now, the following proposition finishes the proof of the theorem.

Proposition

Suppose that $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ are subsets such that every cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.

Furthermore, suppose that $\mathcal{M}$ is a collection of disjoint cycles in $Y_1 \times \cdots \times Y_p$. Then $|\mathcal{M}| \leq 2p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n$.

Indeed, the proposition implies

$$|A|/(p \cdot P(p)) \leq |\mathcal{M}| \leq 2p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n,$$

and therefore $|A| \leq 2p^2 \cdot P(p) \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n = C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n$.

Let $Y_1, \dots, Y_p \subseteq \mathbb{F}_p^n$ be such that every cycle $(x_1, \dots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.

Let $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ be such that every cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.

Key observation

Let $3 \leq j \leq p$. Consider cycles $(x_1, \ldots, x_p), (x_1', \ldots, x_p') \in Y_1 \times \cdots \times Y_p$. If $(x_1, x_j) \neq (x_1', x_j')$, then $x_1 + x_j \neq x_1' + x_j'$.

Let $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ be such that every cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.

Key observation

Let $3 \leq j \leq p$. Consider cycles $(x_1, \ldots, x_p), (x_1', \ldots, x_p') \in Y_1 \times \cdots \times Y_p$. If $(x_1, x_j) \neq (x_1', x_j')$, then $x_1 + x_j \neq x_1' + x_j'$.

Proof: Assume that $j = 3$. Suppose that $(x_1, x_3) \neq (x_1', x_3')$, but $x_1 + x_3 = x_1' + x_3'$.

Let $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ be such that every cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.

Key observation

Let $3 \le j \le p$. Consider cycles $(x_1, \ldots, x_p), (x_1', \ldots, x_p') \in Y_1 \times \cdots \times Y_p$. If $(x_1, x_j) \neq (x_1', x_j')$, then $x_1 + x_j \neq x_1' + x_j'$.

Proof: Assume that $j = 3$. Suppose that $(x_1, x_3) \neq (x_1', x_3')$, but $x_1 + x_3 = x_1' + x_3'$.

Then $x_1' \neq x_1$ and $x_1 = x_2$, so $x_1' \neq x_2$.

Let $Y_1, \dots, Y_p \subseteq \mathbb{F}_p^n$ be such that every cycle $(x_1, \dots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.

Key observation

Let $3 \le j \le p$. Consider cycles $(x_1, \dots, x_p), (x_1', \dots, x_p') \in Y_1 \times \cdots \times Y_p$. If $(x_1, x_j) \neq (x_1', x_j')$, then $x_1 + x_j \neq x_1' + x_j'$.

Proof: Assume that $j = 3$. Suppose that $(x_1, x_3) \neq (x_1', x_3')$, but $x_1 + x_3 = x_1' + x_3'$.

Then $x_1' \neq x_1$ and $x_1 = x_2$, so $x_1' \neq x_2$.

Hence the cycle $(x_1', x_2, x_3', x_4 \dots, x_p) \in Y_1 \times \cdots \times Y_p$ contradicts the assumptions on $Y_1, \dots, Y_p$. $\square$

Let $Y_1, \dots, Y_p \subseteq \mathbb{F}_p^n$ be such that every cycle $(x_1, \dots, x_p) \in Y_1 \times \dots \times Y_p$ satisfies $x_1 = x_2$.

Key observation

Let $3 \leq j \leq p$. Consider cycles $(x_1, \dots, x_p), (x_1', \dots, x_p') \in Y_1 \times \dots \times Y_p$. If $(x_1, x_j) \neq (x_1', x_j')$, then $x_1 + x_j \neq x_1' + x_j'$.

Proof: Assume that $j = 3$. Suppose that $(x_1, x_3) \neq (x_1', x_3')$, but $x_1 + x_3 = x_1' + x_3'$.

Then $x_1' \neq x_1$ and $x_1 = x_2$, so $x_1' \neq x_2$.

Hence the cycle $(x_1', x_2, x_3', x_4 \dots, x_p) \in Y_1 \times \dots \times Y_p$ contradicts the assumptions on $Y_1, \dots, Y_p$. □

So for every $j = 3, \dots, p$, there are at most p^n different pairs in $Y_1 \times Y_j$ occurring as (x_1, x_j) for some cycle $(x_1, \dots, x_p) \in Y_1 \times \dots \times Y_p$.

Proposition

Suppose that $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ are subsets such that every cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.
Furthermore, suppose that $\mathcal{M}$ is a collection of disjoint cycles in $Y_1 \times \cdots \times Y_p$. Then $|\mathcal{M}| \leq 2p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n$.

Proposition

Suppose that $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ are subsets such that every cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.
Furthermore, suppose that $\mathcal{M}$ is a collection of disjoint cycles in $Y_1 \times \cdots \times Y_p$. Then $|\mathcal{M}| \leq 2p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n$.

For every $j = 3, \ldots, p$, there are at most p^n different pairs in $Y_1 \times Y_j$ occurring as (x_1, x_j) for some cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$.

Proposition

Suppose that $Y_1, \ldots, Y_p \subseteq \mathbb{F}_p^n$ are subsets such that every cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$ satisfies $x_1 = x_2$.
Furthermore, suppose that $\mathcal{M}$ is a collection of disjoint cycles in $Y_1 \times \cdots \times Y_p$. Then $|\mathcal{M}| \leq 2p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n$.

For every $j = 3, \ldots, p$, there are at most p^n different pairs in $Y_1 \times Y_j$ occurring as (x_1, x_j) for some cycle $(x_1, \ldots, x_p) \in Y_1 \times \cdots \times Y_p$.

By a greedy procedure we can now choose a sufficiently large subcollection of $\mathcal{M}$ satisfying the assumptions in the multi-colored sum-free theorem.

Multi-colored sum-free Theorem

Let p prime, $k \geq 3$ and let $(x_{1,i}, x_{2,i}, \ldots, x_{p,i})_{i=1}^m$ be a collection of p-tuples in $\mathbb{F}_p^n \times \cdots \times \mathbb{F}_p^n$ such that

$$x_{1,i_1} + x_{2,i_2} + \cdots + x_{p,i_k} = 0 \quad \Leftrightarrow \quad i_1 = i_2 = \cdots = i_p.$$

Then $m \leq (\gamma_p)^n$.

Concluding remarks

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero, satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

Concluding remarks

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero, satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

The best known lower bounds are due to Edel. They are of the form $\Omega(c^n)$ for some absolute constant $c \approx 2.1398$.

Concluding remarks

Theorem (S., 2019+)

Let $p \geq 5$ be a fixed prime. Then any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero, satisfies

$$|A| \leq C_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p \cdot (2\sqrt{p})^n .$$

The best known lower bounds are due to Edel. They are of the form $\Omega(c^n)$ for some absolute constant $c \approx 2.1398$.

Thus, there is still a big gap between the upper and lower bound. In particular, the following problem is open.

Open problem

Is there an absolute constant C such that any subset $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero has size at most C^n?

The proof of our main result also gives a multi-colored generalization:

Theorem

Let $p \geq 5$ be a fixed prime. Consider a collection of p-tuples $(x_{1,i}, x_{2,i}, \dots, x_{p,i})_{i=1}^{L}$ of elements of $\mathbb{F}_p^n$ such that for each $j = 1, \dots, p$ all the elements $x_{j,i}$ for $i \in \{1, \dots, L\}$ are distinct. Assume that for $i = 1, \dots, L$, we have

$$x_{1,i} + x_{2,i} + \dots + x_{p,i} = 0,$$

and that there are no distinct indices $i_1, \dots, i_p \in \{1, \dots, L\}$ with

$$x_{1,i_1} + x_{2,i_2} + \dots + x_{p,i_p} = 0.$$

Then $L \leq C_p' \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p' \cdot \left(2\sqrt{p}\right)^n$.

The proof of our main result also gives a multi-colored generalization:

Theorem

Let $p \geq 5$ be a fixed prime. Consider a collection of p-tuples $(x_{1,i}, x_{2,i}, \ldots, x_{p,i})_{i=1}^{L}$ of elements of $\mathbb{F}_p^n$ such that for each $j = 1, \ldots, p$ all the elements $x_{j,i}$ for $i \in \{1, \ldots, L\}$ are distinct. Assume that for $i = 1, \ldots, L$, we have

$$x_{1,i} + x_{2,i} + \cdots + x_{p,i} = 0,$$

and that there are no distinct indices $i_1, \ldots, i_p \in \{1, \ldots, L\}$ with

$$x_{1,i_1} + x_{2,i_2} + \cdots + x_{p,i_p} = 0.$$

Then $L \leq C_p' \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C_p' \cdot \left(2\sqrt{p}\right)^n$.

This implies our bound on the size of subsets $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero by considering the collection of p-tuples $(x, \ldots, x)$ for all $x \in A$.

The proof of our main result also gives a multi-colored generalization:

Theorem

Let $p \geq 5$ be a fixed prime. Consider a collection of p-tuples $(x_{1,i}, x_{2,i}, \dots, x_{p,i})_{i=1}^{L}$ of elements of $\mathbb{F}_p^n$ such that for each $j = 1, \dots, p$ all the elements $x_{j,i}$ for $i \in \{1, \dots, L\}$ are distinct. Assume that for $i = 1, \dots, L$, we have

$$x_{1,i} + x_{2,i} + \cdots + x_{p,i} = 0,$$

and that there are no distinct indices $i_1, \dots, i_p \in \{1, \dots, L\}$ with

$$x_{1,i_1} + x_{2,i_2} + \cdots + x_{p,i_p} = 0.$$

Then $L \leq C'_p \cdot \left(\sqrt{\gamma_p \cdot p}\right)^n < C'_p \cdot \left(2\sqrt{p}\right)^n$.

This implies our bound on the size of subsets $A \subseteq \mathbb{F}_p^n$ without p distinct elements summing to zero by considering the collection of p-tuples $(x, \dots, x)$ for all $x \in A$.

Interestingly, in this multi-colored version, the bound is close to optimal. For all even n, there are examples with $L = \sqrt{p}^n$.

Thank you very much for your attention!