Erdős-Ginzburg-Ziv problem and Convex Geometry

Zakharov Dmitriy

HSE, MIPT

Question

What is the minimal number $s = \mathfrak{s}(\mathbb{F}_p^d)$ such that among any s elements of $\mathbb{F}_p^d$ one can find p whose sum is $0 \pmod{p}$?

Question

What is the minimal number $s = \mathfrak{s}(\mathbb{F}_p^d)$ such that among any s elements of $\mathbb{F}_p^d$ one can find p whose sum is $0 \pmod p$?

Erdős-Ginzburg-Ziv, 1961

Among any $2p-1$ elements of $\mathbb{F}_p$ one can find p whose sum is $0 \pmod p$.

This is tight:

$$\underbrace{0, 0, \ldots, 0}_{p-1}, \underbrace{1, 1, \ldots, 1}_{p-1}$$

Question

What is the minimal number $s = \mathfrak{s}(\mathbb{F}_p^d)$ such that among any s elements of $\mathbb{F}_p^d$ one can find p whose sum is $0 \pmod p$?

Erdős-Ginzburg-Ziv, 1961

Among any $2p-1$ elements of $\mathbb{F}_p$ one can find p whose sum is $0 \pmod p$.

This is tight:

$$\underbrace{0, 0, \ldots, 0}_{p-1}, \underbrace{1, 1, \ldots, 1}_{p-1}$$

Reiher, 2007 (Kemnitz conjecture, 1983)

Among any $4p-3$ elements of $\mathbb{F}_p^2$ one can find p whose sum is $0 \pmod p$.

Also tight:

$$\underbrace{(0,0), (0,1), (1,0), (1,1)}_{p-1}$$

Question

What is the minimal number $s = \mathfrak{s}(\mathbb{F}_p^d)$ such that among any s elements of $\mathbb{F}_p^d$ one can find p whose sum is $0 \pmod p$?

We are interested in the case when $d = \mathrm{const}$ and p is large.

Question

What is the minimal number $s = \mathfrak{s}(\mathbb{F}_p^d)$ such that among any s elements of $\mathbb{F}_p^d$ one can find p whose sum is $0 \pmod p$?

We are interested in the case when $d = \mathrm{const}$ and p is large.
In this case, $\mathfrak{s}(\mathbb{F}_p^d)$ grows linearly in p:

- Lower bound: $\mathfrak{s}(\mathbb{F}_p^d) \geq 2^d(p-1)+1$.

Question

What is the minimal number $s = \mathfrak{s}(\mathbb{F}_p^d)$ such that among any s elements of $\mathbb{F}_p^d$ one can find p whose sum is $0 \pmod p$?

We are interested in the case when $d = \mathrm{const}$ and p is large.
In this case, $\mathfrak{s}(\mathbb{F}_p^d)$ grows linearly in p:

- Lower bound: $\mathfrak{s}(\mathbb{F}_p^d) \geq 2^d(p-1)+1$.
- Upper bound (Alon-Dubiner, 1995): $\mathfrak{s}(\mathbb{F}_p^d) \leq C_d p$ where $C_d = (Cd \log d)^d$.

Question

What is the minimal number $s = \mathfrak{s}(\mathbb{F}_p^d)$ such that among any s elements of $\mathbb{F}_p^d$ one can find p whose sum is $0 \pmod p$?

We are interested in the case when $d = \mathrm{const}$ and p is large.
In this case, $\mathfrak{s}(\mathbb{F}_p^d)$ grows linearly in p:

- Lower bound: $\mathfrak{s}(\mathbb{F}_p^d) \geq 2^d(p-1)+1$.
- Upper bound (Alon-Dubiner, 1995): $\mathfrak{s}(\mathbb{F}_p^d) \leq C_d p$ where $C_d = (Cd \log d)^d$.

In particular, for $d = 3$ we have:

$$9(p-1)+1 \leq \mathfrak{s}(\mathbb{F}_p^3) \leq 10000p,$$

Question

What is the minimal number $s = \mathfrak{s}(\mathbb{F}_p^d)$ such that among any s elements of $\mathbb{F}_p^d$ one can find p whose sum is $0 \pmod p$?

We are interested in the case when $d = \mathrm{const}$ and p is large.
In this case, $\mathfrak{s}(\mathbb{F}_p^d)$ grows linearly in p:

- Lower bound: $\mathfrak{s}(\mathbb{F}_p^d) \geq 2^d(p-1)+1$.
- Upper bound (Alon-Dubiner, 1995): $\mathfrak{s}(\mathbb{F}_p^d) \leq C_d p$ where $C_d = (Cd \log d)^d$.

In particular, for $d = 3$ we have:

$$9(p-1)+1 \leq \mathfrak{s}(\mathbb{F}_p^3) \leq 10000p,$$

Z., 2020

For fixed d and $p > p_0(d)$ we have $\mathfrak{s}(\mathbb{F}_p^d) \leq 4^d p$.
For $d = 3$ we have $\mathfrak{s}(\mathbb{F}_p^3) \sim 9p$.

Lower bound

Weak EGZ constant

Let $\mathfrak{w}(\mathbb{F}_p^d)$ be the maximal cardinality of a set $S \subset \mathbb{F}_p^d$ such that the multiset $(p-1) \cdot S$ does not contain p elements with zero sum.

By definition, $\mathfrak{s}(\mathbb{F}_p^d) \geq \mathfrak{w}(\mathbb{F}_p^d)(p-1)+1$. For example, $S = \{0,1\}^d$ gives $\mathfrak{w}(\mathbb{F}_p^d) \geq 2^d$.

Lower bound

Weak EGZ constant

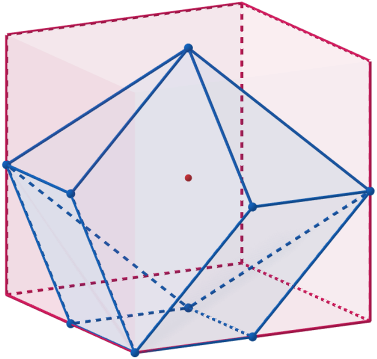
Let $\mathfrak{w}(\mathbb{F}_p^d)$ be the maximal cardinality of a set $S \subset \mathbb{F}_p^d$ such that the multiset $(p-1) \cdot S$ does not contain p elements with zero sum.

By definition, $\mathfrak{s}(\mathbb{F}_p^d) \geq \mathfrak{w}(\mathbb{F}_p^d)(p-1)+1$. For example, $S = \{0,1\}^d$ gives $\mathfrak{w}(\mathbb{F}_p^d) \geq 2^d$.

Claim

We have $\mathfrak{w}(\mathbb{F}_p^3) \geq 9$ for $p > 2$. More generally, $\mathfrak{w}(\mathbb{F}_p^d) \geq 9^{[d/3]}$.

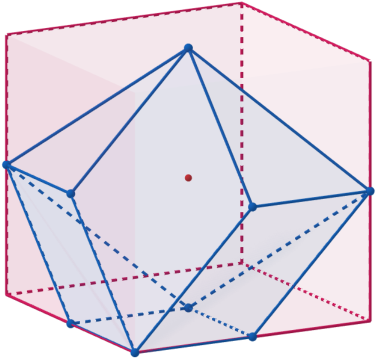
$\mathfrak{w}(\mathbb{F}_p^3) \geq 9$ and Elsholtz's construction



This is a polytope in $\mathbb{R}^3$ with coordinates of vertices:

$$S = \{(0,0,2),\\ (1,0,1),(1,-1,1),(0,1,1),(-1,1,1),\\ (0,0,0),(1,0,0),(0,1,0),(1,1,0)\}$$

$\mathfrak{w}(\mathbb{F}_p^3) \geq 9$ and Elsholtz's construction



This is a polytope in $\mathbb{R}^3$ with coordinates of vertices:

$$S = \{(0,0,2), (1,0,1), (1,-1,1), (0,1,1), (-1,1,1), (0,0,0), (1,0,0), (0,1,0), (1,1,0)\}$$

This polytope is *hollow* in the following sense: for any face Γ let Λ_Γ be the minimal lattice containing vertices of Γ, then $\Lambda_\Gamma \cap \operatorname{int}\Gamma = \emptyset$.

Claim

Let $P \subset \mathbb{Q}^d$ be a *hollow* polytope, that is $\Lambda_\Gamma \cap \operatorname{int} \Gamma = \emptyset$ for any face Γ of P. Then for almost all primes p the constant $\mathfrak{w}(\mathbb{F}_p^d)$ is at least the number of vertices of P.

Claim

Let $P \subset \mathbb{Q}^d$ be a *hollow* polytope, that is $\Lambda_\Gamma \cap \operatorname{int} \Gamma = \emptyset$ for any face Γ of P. Then for almost all primes p the constant $\mathfrak{w}(\mathbb{F}_p^d)$ is at least the number of vertices of P.

Proof. Suppose that $\Lambda_P = \mathbb{Z}^d$ and let S be the set of vertices of P reduced modulo p. Suppose that $(p-1) \cdot S$ has a zero-sum sequence. This means that for some integer coefficients α_s, $s \in S$ we have:

$$\sum_{s \in S} \alpha_s = p, \quad \sum_{s \in S} \alpha_s s \equiv 0 \pmod{p},$$

Claim

Let $P \subset \mathbb{Q}^d$ be a *hollow* polytope, that is $\Lambda_\Gamma \cap \operatorname{int} \Gamma = \emptyset$ for any face Γ of P. Then for almost all primes p the constant $\mathfrak{w}(\mathbb{F}_p^d)$ is at least the number of vertices of P.

Proof. Suppose that $\Lambda_P = \mathbb{Z}^d$ and let S be the set of vertices of P reduced modulo p. Suppose that $(p-1) \cdot S$ has a zero-sum sequence. This means that for some integer coefficients α_s, $s \in S$ we have:

$$\sum_{s \in S} \alpha_s = p, \quad \sum_{s \in S} \alpha_s s \equiv 0 \pmod{p},$$

Let $q = \frac{1}{p} \sum_{s \in S} \alpha_s s$ and let Γ be the minimal face of P containing q. By assumption, $q \in \mathbb{Z}^d$ and we want to show that $q \in \Lambda_\Gamma$.

Claim

Let $P \subset \mathbb{Q}^d$ be a *hollow* polytope, that is $\Lambda_\Gamma \cap \operatorname{int} \Gamma = \emptyset$ for any face Γ of P. Then for almost all primes p the constant $\mathfrak{w}(\mathbb{F}_p^d)$ is at least the number of vertices of P.

Proof. Suppose that $\Lambda_P = \mathbb{Z}^d$ and let S be the set of vertices of P reduced modulo p. Suppose that $(p-1) \cdot S$ has a zero-sum sequence. This means that for some integer coefficients α_s, $s \in S$ we have:

$$\sum_{s \in S} \alpha_s = p, \quad \sum_{s \in S} \alpha_s s \equiv 0 \pmod{p},$$

Let $q = \frac{1}{p} \sum_{s \in S} \alpha_s s$ and let Γ be the minimal face of P containing q. By assumption, $q \in \mathbb{Z}^d$ and we want to show that $q \in \Lambda_\Gamma$.Let $\Theta = \mathbb{Z}^d \cap \operatorname{aff} \Gamma$ and consider the quotient Θ / Λ_Γ (figure).

Claim

Let $P \subset \mathbb{Q}^d$ be a *hollow* polytope, that is $\Lambda_\Gamma \cap \operatorname{int} \Gamma = \emptyset$ for any face Γ of P. Then for almost all primes p the constant $\mathfrak{w}(\mathbb{F}_p^d)$ is at least the number of vertices of P.

Proof. Suppose that $\Lambda_P = \mathbb{Z}^d$ and let S be the set of vertices of P reduced modulo p. Suppose that $(p-1)\cdot S$ has a zero-sum sequence. This means that for some integer coefficients α_s, $s \in S$ we have:

$$\sum_{s\in S} \alpha_s = p, \quad \sum_{s\in S} \alpha_s s \equiv 0 \pmod{p},$$

Let $q = \frac{1}{p}\sum_{s\in S} \alpha_s s$ and let Γ be the minimal face of P containing q. By assumption, $q \in \mathbb{Z}^d$ and we want to show that $q \in \Lambda_\Gamma$.Let $\Theta = \mathbb{Z}^d \cap \operatorname{aff} \Gamma$ and consider the quotient Θ/Λ_Γ (figure).
In Θ/Λ_Γ we have $p \cdot [q] \equiv 0$, but Θ/Λ_Γ does not have p-torsion for almost all primes p. So $[q] \equiv 0$ in Θ/Λ_Γ and $q \in \Lambda_\Gamma$.

We showed that $\mathfrak{w}(\mathbb{F}_p^d) \geq 9^{[d/3]}$.

Claim

We have $\mathfrak{w}(\mathbb{F}_p^d) \leq 4^d$.

We showed that $\mathfrak{w}(\mathbb{F}_p^d) \geq 9^{[d/3]}$.

Claim

We have $\mathfrak{w}(\mathbb{F}_p^d) \leq 4^d$.

Sketch. Let S be the set from definition of $\mathfrak{w}$. Consider a polynomial in $d \times p$ variables $(x_{i,j})$:

$$F(x_1, \ldots, x_p) = \prod_{j=1}^{d} \left(1 - (x_{1,j} + \ldots + x_{p,j})^{p-1}\right)$$

We showed that $\mathfrak{w}(\mathbb{F}_p^d) \geq 9^{[d/3]}$.

Claim

We have $\mathfrak{w}(\mathbb{F}_p^d) \leq 4^d$.

Sketch. Let S be the set from definition of $\mathfrak{w}$. Consider a polynomial in $d \times p$ variables $(x_{i,j})$:

$$F(x_1, \ldots, x_p) = \prod_{j=1}^{d} \left(1 - (x_{1,j} + \ldots + x_{p,j})^{p-1}\right)$$

Clearly $F(x_1, \ldots, x_p)$ is an indicator function of the event that $x_1 + \ldots + x_p = 0$. So in restriction on the set $S \times \ldots \times S$ we have $F|_{S \times \ldots \times S} = \delta_{x_1 = x_2 = \ldots = x_p}$. So the "rank" of F is at least $|S|$. But expanding the product in definition of F shows that the "rank" of F is at most 4^d.

"Thin" case

Any multiset $S \subset [K]^d \subset \mathbb{F}_p^d$ of size at least $4^d p$ contains p distinct elements with zero sum. (Here we assume $p \gg_{d,K} 1$).

“Thin" case

Any multiset $S \subset [K]^d \subset \mathbb{F}_p^d$ of size at least $4^d p$ contains p distinct elements with zero sum. (Here we assume $p \gg_{d,K} 1$).

A point q is called θ-central point of P if every half-space H^+ containing q contains at least θ-fraction of vertices of P.

"Thin" case

Any multiset $S \subset [K]^d \subset \mathbb{F}_p^d$ of size at least $4^d p$ contains p distinct elements with zero sum. (Here we assume $p \gg_{d,K} 1$).

A point q is called θ-central point of P if every half-space H^+ containing q contains at least θ-fraction of vertices of P.

Central Point Theorem

Any set of points $S \subset \mathbb{R}^d$ has a $\frac{1}{d+1}$-central point.

"Thin" case

Any multiset $S \subset [K]^d \subset \mathbb{F}_p^d$ of size at least $4^d p$ contains p distinct elements with zero sum. (Here we assume $p \gg_{d,K} 1$).

A point q is called θ-central point of P if every half-space H^+ containing q contains at least θ-fraction of vertices of P.

Central Point Theorem

Any set of points $S \subset \mathbb{R}^d$ has a $\frac{1}{d+1}$-central point.

Doignon's Central Point Theorem, 1973

Every set of points in $\mathbb{Z}^d$ has a 2^{-d}-central point $q \in \mathbb{Z}^d$.

"Thin" case

Any multiset $S \subset [K]^d \subset \mathbb{F}_p^d$ of size at least $4^d p$ contains p distinct elements with zero sum. (Here we assume $p \gg_{d,K} 1$).

A point q is called θ-central point of P if every half-space H^+ containing q contains at least θ-fraction of vertices of P.

Central Point Theorem

Any set of points $S \subset \mathbb{R}^d$ has a $\frac{1}{d+1}$-central point.

Doignon's Central Point Theorem, 1973

Every set of points in $\mathbb{Z}^d$ has a 2^{-d}-central point $q \in \mathbb{Z}^d$.

For a polytope P we say that a point q is an integer point of P if $q \in \Lambda_\Gamma \cap \operatorname{int} \Gamma$ for some face Γ.

Integer Central Point Theorem

Any polytope $P \subset \mathbb{Q}^d$ has a 4^{-d}-central integer point q.

A K-slab in $\mathbb{F}_p^d$ is the set of points $x \in \mathbb{F}_p^d$ such that $\xi(x) \in [a, a+K]$ for some $a \in \mathbb{F}_p$ and a linear function ξ.

A K-slab in $\mathbb{F}_p^d$ is the set of points $x \in \mathbb{F}_p^d$ such that $\xi(x) \in [a, a+K]$ for some $a \in \mathbb{F}_p$ and a linear function ξ.

"Thick" case

Let $S \subset \mathbb{F}_p^d$ be a set such that $|X \cap H| \leq (1-\varepsilon)|S|$ for any K-slab H. Suppose that $|S| > (1+\varepsilon)p$, $K \gg_{d,\varepsilon} 1$. Then S contains a zero-sum sequence.

A K-slab in $\mathbb{F}_p^d$ is the set of points $x \in \mathbb{F}_p^d$ such that $\xi(x) \in [a, a+K]$ for some $a \in \mathbb{F}_p$ and a linear function ξ.

"Thick" case

Let $S \subset \mathbb{F}_p^d$ be a set such that $|X \cap H| \leq (1-\varepsilon)|S|$ for any K-slab H. Suppose that $|S| > (1+\varepsilon)p$, $K \gg_{d,\varepsilon} 1$. Then S contains a zero-sum sequence.

This result is essentially due to Alon-Dubiner. By induction, it implies the bound $\mathfrak{s}(\mathbb{F}_p^d) \leq C_d p$.
Proof idea. The condition on K-slabs implies that a certain graph assosiated to S has a large spectral gap. Using expanding properties of this graph one can show that **every** element of $\mathbb{F}_p^d$ can be expressed as a sum of p distinct elements of X.

General case

We established the following special cases of EGZ problem:

"Thin" case

Any multiset $S \subset [K]^d \subset \mathbb{F}_p^d$ of size at least $4^d p$ contains a zero-sum sequence.

"Thick" case

If a multiset $S \subset \mathbb{F}_p^d$ is not concentrated on any K-slab then S contains a zero-sum sequence.

The proof of the bound $\mathfrak{s}(\mathbb{F}_p^d) \leq 4^d p$ is based on these two approaches.

Final remarks

- Our main result states that $\mathfrak{s}(\mathbb{F}_p^d) \sim \mathfrak{w}(\mathbb{F}_p^d)p$ as $p \to \infty$.
- Let $L(d)$ be the maximal number of vertices in a hollow polytope in $\mathbb{Q}^d$. As we have seen, $\mathfrak{w}(\mathbb{F}_p^d) \geq L(d)$ for almost all primes p. Is it true that $\mathfrak{w}(\mathbb{F}_p^d) = L(d)$ for almost all primes p?

Final remarks

- Our main result states that $\mathfrak{s}(\mathbb{F}_p^d) \sim \mathfrak{w}(\mathbb{F}_p^d)p$ as $p \to \infty$.
- Let $L(d)$ be the maximal number of vertices in a hollow polytope in $\mathbb{Q}^d$. As we have seen, $\mathfrak{w}(\mathbb{F}_p^d) \geq L(d)$ for almost all primes p. Is it true that $\mathfrak{w}(\mathbb{F}_p^d) = L(d)$ for almost all primes p?
- Do we have stability for EGZ problem?
- If we do, can we deduce an *exact* result from it? Say, $\mathfrak{s}(\mathbb{F}_p^3) = 9(p-1)+1$ for large p.

Final remarks

- Our main result states that $\mathfrak{s}(\mathbb{F}_p^d) \sim \mathfrak{w}(\mathbb{F}_p^d)p$ as $p \to \infty$.
- Let $L(d)$ be the maximal number of vertices in a hollow polytope in $\mathbb{Q}^d$. As we have seen, $\mathfrak{w}(\mathbb{F}_p^d) \geq L(d)$ for almost all primes p. Is it true that $\mathfrak{w}(\mathbb{F}_p^d) = L(d)$ for almost all primes p?
- Do we have stability for EGZ problem?
- If we do, can we deduce an *exact* result from it? Say, $\mathfrak{s}(\mathbb{F}_p^3) = 9(p-1)+1$ for large p.
- Is it true that $\mathfrak{s}(\mathbb{F}_p^d) < C^d p$ for *all* primes p? The best known bounds for p fixed and d large are
    - $\mathfrak{s}(\mathbb{F}_3^d) \leq 2.756^d$ (Ellenberg-Gijswijt, 2017, Annals)
    - $\mathfrak{s}(\mathbb{F}_p^d) \leq C_p(2\sqrt{p})^d$ (Sauermann, 2019)

Final remarks

- Our main result states that $\mathfrak{s}(\mathbb{F}_p^d) \sim \mathfrak{w}(\mathbb{F}_p^d)p$ as $p \to \infty$.
- Let $L(d)$ be the maximal number of vertices in a hollow polytope in $\mathbb{Q}^d$. As we have seen, $\mathfrak{w}(\mathbb{F}_p^d) \geq L(d)$ for almost all primes p. Is it true that $\mathfrak{w}(\mathbb{F}_p^d) = L(d)$ for almost all primes p?
- Do we have stability for EGZ problem?
- If we do, can we deduce an *exact* result from it? Say, $\mathfrak{s}(\mathbb{F}_p^3) = 9(p-1)+1$ for large p.
- Is it true that $\mathfrak{s}(\mathbb{F}_p^d) < C^d p$ for *all* primes p? The best known bounds for p fixed and d large are
  - $\mathfrak{s}(\mathbb{F}_3^d) \leq 2.756^d$ (Ellenberg-Gijswijt, 2017, Annals)
  - $\mathfrak{s}(\mathbb{F}_p^d) \leq C_p(2\sqrt{p})^d$ (Sauermann, 2019)
- We know that $2.1^d \leq L(d) \leq 4^d$. What is the right exponent?