Zeros of sparse polynomials over finite fields

IAG Seminar, Magdeburg 2021

Ivan Soprunov*

(with Kyle Meyer and Jenya Soprunova)

*Cleveland State University

October 19, 2021

$\mathbb{F}_q$-zeros of irreducible polynomials

Let $\mathbb{F}_q$ finite field of q elements. Consider an absolutely irreducible polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree d.

Problem: Estimate $\mathsf{N}_f = |\{p \in \mathbb{P}^n(\mathbb{F}_q) : f(p) = 0\}|$,
the number of $\mathbb{F}_q$-zeros of f in projective space.

$\mathbb{F}_q$-zeros of irreducible polynomials

Let $\mathbb{F}_q$ finite field of q elements. Consider an absolutely irreducible polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree d.

Problem: Estimate $\mathrm{N}_f = |\{p \in \mathbb{P}^n(\mathbb{F}_q) : f(p) = 0\}|$, the number of $\mathbb{F}_q$-zeros of f in projective space.

For $f \in \mathbb{F}_q[x, y]$, we have
Hasse-Weil (1949):

$$|\mathrm{N}_f - (q+1)| \leq g q^{\frac{1}{2}}, \text{ where } g \text{ is the genus}$$

For irreducible projective varieties X of dimension n and degree d
Lang-Weil Bound (1954):

$$|\mathrm{N}_X - \frac{q^{n+1}-1}{q-1}| \leq (d-1)(d-2)q^{n-\frac{1}{2}} + Cq^{n-1}.$$

Maximum number of $\mathbb{F}_q$-zeros for families of polynomials

Let $\mathcal{L} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a finite subset.

Problem 1: Estimate $\mathrm{N}_{\mathcal{L}} = \max\{\mathrm{N}_f : 0 \neq f \in \mathcal{L}\}$, the maximum number of $\mathbb{F}_q$-zeros of non-trivial f in $\mathcal{L}$.

Maximum number of $\mathbb{F}_q$-zeros for families of polynomials

Let $\mathcal{L} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a finite subset.

Problem 1: Estimate $\mathrm{N}_{\mathcal{L}} = \max\{\mathrm{N}_f : 0 \neq f \in \mathcal{L}\}$, the maximum number of $\mathbb{F}_q$-zeros of non-trivial f in $\mathcal{L}$.

Problem 2: Estimate $\mathrm{N}'_{\mathcal{L}}$, the maximum number of $\mathbb{F}_q$-zeros of f in $\mathcal{L}$ with the largest number of factors.

Maximum number of $\mathbb{F}_q$-zeros for families of polynomials

Let $\mathcal{L} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a finite subset.

Problem 1: Estimate $\mathrm{N}_{\mathcal{L}} = \max\{\mathrm{N}_f : 0 \neq f \in \mathcal{L}\}$, the maximum number of $\mathbb{F}_q$-zeros of non-trivial f in $\mathcal{L}$.

Problem 2: Estimate $\mathrm{N}'_{\mathcal{L}}$, the maximum number of $\mathbb{F}_q$-zeros of f in $\mathcal{L}$ with the largest number of factors.

Example: Let $\mathcal{L} = \mathcal{L}_d$, the set of all polynomials of degree at most d. Then $\mathrm{N}_{\mathcal{L}_d} = \mathrm{N}'_{\mathcal{L}_d}$ when $d \leq q$. Therefore,

$$\mathrm{N}_{\mathcal{L}_d} = dq^{n-1}.$$

Maximum number of $\mathbb{F}_q$-zeros for families of polynomials

Let $\mathcal{L} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a finite subset.

Problem 1: Estimate $\mathrm{N}_{\mathcal{L}} = \max\{\mathrm{N}_f : 0 \neq f \in \mathcal{L}\}$, the maximum number of $\mathbb{F}_q$-zeros of non-trivial f in $\mathcal{L}$.

Problem 2: Estimate $\mathrm{N}'_{\mathcal{L}}$, the maximum number of $\mathbb{F}_q$-zeros of f in $\mathcal{L}$ with the largest number of factors.

Example: Let $\mathcal{L} = \mathcal{L}_d$, the set of all polynomials of degree at most d. Then $\mathrm{N}_{\mathcal{L}_d} = \mathrm{N}'_{\mathcal{L}_d}$ when $d \leq q$. Therefore,

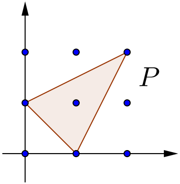
$$\mathrm{N}_{\mathcal{L}_d} = dq^{n-1}.$$

Observe: We have $\mathrm{N}_{\mathcal{L}} = \mathrm{N}'_{\mathcal{L}}$ for large enough q.
Reason: If $f = f_1 \cdots f_k$ factorization into irreducible factors then $\mathrm{N}_f = kq^{n-1} + o(q^{n-1})$ (from Lang-Weil Bound)

$\mathbb{F}_q$-zeros of sparse polynomials

We are interested in $\mathcal{L}_P \subset \mathbb{F}_q[x_1, \dots, x_n]$ defined by a lattice polytope $P \subset \mathbb{R}^n$. It defines a space of sparse polynomials

$$\mathcal{L}_P = \mathrm{span}_{\mathbb{F}_q}\{x^a : a \in P \cap \mathbb{Z}^n\}, \text{ where } x^a = x_1^{a_1} \cdots x_n^{a_n}.$$



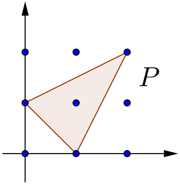
Example 1: Here $\mathcal{L}_P \subset \mathbb{F}_q[x_1, x_2]$,

$$\begin{aligned}\mathcal{L}_P &= \mathrm{span}_{\mathbb{F}_q}\{x_1, x_2, x_1x_2, x_1^2x_2^2\} \\ &= \{\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_1 x_2 + \lambda_4 x_1^2 x_2^2 : \lambda_i \in \mathbb{F}_q\}.\end{aligned}$$

$\mathbb{F}_q$-zeros of sparse polynomials

We are interested in $\mathcal{L}_P \subset \mathbb{F}_q[x_1, \ldots, x_n]$ defined by a lattice polytope $P \subset \mathbb{R}^n$. It defines a space of sparse polynomials

$$\mathcal{L}_P = \operatorname{span}_{\mathbb{F}_q}\{x^a : a \in P \cap \mathbb{Z}^n\}, \text{ where } x^a = x_1^{a_1} \cdots x_n^{a_n}.$$



Example 1: Here $\mathcal{L}_P \subset \mathbb{F}_q[x_1, x_2]$,

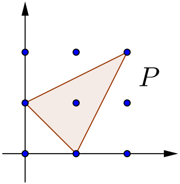
$$\begin{aligned}\mathcal{L}_P &= \operatorname{span}_{\mathbb{F}_q}\{x_1, x_2, x_1x_2, x_1^2x_2^2\} \\ &= \{\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_1 x_2 + \lambda_4 x_1^2 x_2^2 : \lambda_i \in \mathbb{F}_q\}.\end{aligned}$$

Example 2: When $P = d\Delta_n = \operatorname{conv}\{0, de_1, \ldots, de_n\}$ we get $\mathcal{L}_{d\Delta_n} = \mathcal{L}_d$, the set of polynomials of degree at most d.

$\mathbb{F}_q$-zeros of sparse polynomials

We are interested in $\mathcal{L}_P \subset \mathbb{F}_q[x_1, \dots, x_n]$ defined by a lattice polytope $P \subset \mathbb{R}^n$. It defines a space of sparse polynomials

$$\mathcal{L}_P = \mathrm{span}_{\mathbb{F}_q}\{x^a : a \in P \cap \mathbb{Z}^n\}, \text{ where } x^a = x_1^{a_1} \cdots x_n^{a_n}.$$



Example 1: Here $\mathcal{L}_P \subset \mathbb{F}_q[x_1, x_2]$,

$$\begin{aligned}\mathcal{L}_P &= \mathrm{span}_{\mathbb{F}_q}\{x_1, x_2, x_1x_2, x_1^2x_2^2\} \\ &= \{\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_1 x_2 + \lambda_4 x_1^2 x_2^2 : \lambda_i \in \mathbb{F}_q\}.\end{aligned}$$

From now on $\mathrm{N}_f = |\{p \in (\mathbb{F}_q^*)^n : f(p) = 0\}|$

Goal: Estimate $\mathrm{N}_{\mathcal{L}_P} = \max\{\mathrm{N}_f : 0 \neq f \in \mathcal{L}_P\}$ in terms of q and geometric invariants of P.

Motivation from Coding Theory

A linear code is a linear subspace

$$\mathcal{C} \subseteq \mathbb{F}_q^N$$

Parameters

- N is the length of $\mathcal{C}$
- $k = \dim_{\mathbb{F}_q} \mathcal{C}$ is the dimension of $\mathcal{C}$
- $\delta = \min\{\mathrm{weight}(c) : 0 \neq c \in \mathcal{C}\}$ is the minimum distance of $\mathcal{C}$ where weight(c) is the number of non-zero entries of c.

We call $\mathcal{C}$ a $[N, k, \delta]_q$-code.

Motivation from Coding Theory

A linear code is a linear subspace

$$\mathcal{C} \subseteq \mathbb{F}_q^N$$

Parameters

- N is the length of $\mathcal{C}$
- $k = \dim_{\mathbb{F}_q} \mathcal{C}$ is the dimension of $\mathcal{C}$
- $\delta = \min\{\text{weight}(c) : 0 \neq c \in \mathcal{C}\}$ is the minimum distance of $\mathcal{C}$ where $\text{weight}(c)$ is the number of non-zero entries of c.

We call $\mathcal{C}$ a $[N, k, \delta]_q$-code.

Basic Problem
Given N and k, construct $\mathcal{C}$ with the largest possible δ.

Toric Codes

Generalize Reed-Solomon and Reed-Muller codes

As before, let P be a lattice polytope in $\mathbb{R}^n$ and $\mathcal{L}_P$ the corresponding space of sparse polynomials.

Enumerate the points of $(\mathbb{F}_q^*)^n = \{p_1, \dots, p_N\}$.

Evaluation Map:

$$\mathrm{ev} : \mathcal{L}_P \to \mathbb{F}_q^N \quad f \mapsto (f(p_1), \dots, f(p_N))$$

Toric Code: $\mathcal{C}_P = \mathrm{ev}(\mathcal{L}_P) \subseteq \mathbb{F}_q^N$

Toric Codes

Generalize Reed-Solomon and Reed-Muller codes

As before, let P be a lattice polytope in $\mathbb{R}^n$ and $\mathcal{L}_P$ the corresponding space of sparse polynomials.

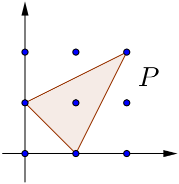
Enumerate the points of $(\mathbb{F}_q^*)^n = \{p_1, \dots, p_N\}$.

Evaluation Map:

$$\mathrm{ev} : \mathcal{L}_P \to \mathbb{F}_q^N \quad f \mapsto (f(p_1), \dots, f(p_N))$$

Toric Code: $\mathcal{C}_P = \mathrm{ev}(\mathcal{L}_P) \subseteq \mathbb{F}_q^N$

Example:



Let $\mathbb{F}_q = \mathbb{F}_4$ and $n = 2$. Then $|(\mathbb{F}_q^*)^2| = 9$.

$$\mathcal{L}_P = \mathrm{span}_{\mathbb{F}_q}\{x_1, x_2, x_1x_2, x_1^2x_2^2\}.$$

In fact, $\mathcal{C}_P$ is a $[9, 4, 3]_4$-code.

Toric Codes

Generalize Reed-Solomon and Reed-Muller codes

As before, let P be a lattice polytope in $\mathbb{R}^n$ and $\mathcal{L}_P$ the corresponding space of sparse polynomials.

Enumerate the points of $(\mathbb{F}_q^*)^n = \{p_1, \ldots, p_N\}$.

Evaluation Map:

$$\mathrm{ev} : \mathcal{L}_P \to \mathbb{F}_q^N \quad f \mapsto (f(p_1), \ldots, f(p_N))$$

Toric Code: $\mathcal{C}_P = \mathrm{ev}(\mathcal{L}_P) \subseteq \mathbb{F}_q^N$

Some champion (generalized) toric codes:

$[49, \ 8, 34]_8$ A. Carbonara, J. Murillo, A. Ortiz (2010)
$[49, 12, 28]_8$ J. Little (2011)
$[36, 19, 12]_7$ G. Brown, A. Kasprzyk (2012)
$[49, 13, 27]_8$, $[49, 19, 21]_8$ G. Brown and A. Kasprzyk, — (2013)

Toric Codes

Generalize Reed-Solomon and Reed-Muller codes

As before, let P be a lattice polytope in $\mathbb{R}^n$ and $\mathcal{L}_P$ the corresponding space of sparse polynomials.

Enumerate the points of $(\mathbb{F}_q^*)^n = \{p_1, \dots, p_N\}$.

Evaluation Map:

$$\mathrm{ev} : \mathcal{L}_P \to \mathbb{F}_q^N \quad f \mapsto (f(p_1), \dots, f(p_N))$$

Toric Code: $\mathcal{C}_P = \mathrm{ev}(\mathcal{L}_P) \subseteq \mathbb{F}_q^N$

Parameters:

- $N = (q-1)^n$
- $k = |P \cap \mathbb{Z}^n|$ iff points in $P \cap \mathbb{Z}^n$ are distinct in $(\mathbb{Z}/(q-1)\mathbb{Z})^n$
- $\delta = (q-1)^n - \mathrm{N}_{\mathcal{L}_P}$

Explicit formulas exist for a large class of polytopes (Little-Schwarz, Soprunova,—)

Toric Codes

Generalize Reed-Solomon and Reed-Muller codes

As before, let P be a lattice polytope in $\mathbb{R}^n$ and $\mathcal{L}_P$ the corresponding space of sparse polynomials.

Enumerate the points of $(\mathbb{F}_q^*)^n = \{p_1, \dots, p_N\}$.

Evaluation Map:

$$\text{ev} : \mathcal{L}_P \to \mathbb{F}_q^N \quad f \mapsto (f(p_1), \dots, f(p_N))$$

Toric Code: $\mathcal{C}_P = \text{ev}(\mathcal{L}_P) \subseteq \mathbb{F}_q^N$

Parameters:

- $N = (q-1)^n$
- $k = |P \cap \mathbb{Z}^n|$ iff points in $P \cap \mathbb{Z}^n$ are distinct in $(\mathbb{Z}/(q-1)\mathbb{Z})^n$
- $\delta = (q-1)^n - \mathrm{N}_{\mathcal{L}_P} \leftarrow$ what we need

Explicit formulas exist for a large class of polytopes (Little-Schwarz, Soprunova,—)

Estimating $N_{\mathcal{L}_P}$

Fix $\mathbb{F}_q$ and a lattice polytope P in $[0, q-2]^n$.
How to estimate the number of $\mathbb{F}_q$-zeros of $f \in \mathcal{L}_P$ that factor the most?

Main Steps:

1. Find the largest number L of factors $f \in \mathcal{L}_P$ may have.
2. Describe what irreducible factors may look like in this case.
3. Estimate the number of $\mathbb{F}_q$-zeros of such irreducible factors.
4. Estimate the number of $\mathbb{F}_q$-zeros of $f \in \mathcal{L}_P$ with L factors.

Newton polytopes and Minkowski Sum

Let f be a Laurent polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$.

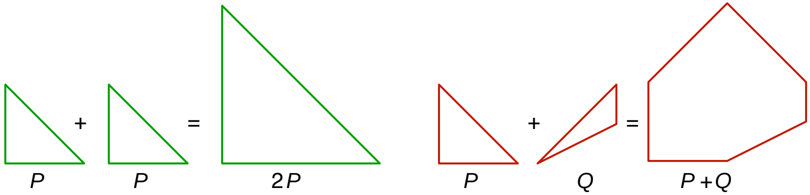
Newton Polytope: $P(f) = \text{conv}\{\text{exponents of } f\} \subset \mathbb{R}^n$

Note: Newton polytope generalizes the notion of degree:

$$P(fg) = P(f) + P(g)$$

The Minkowski sum of polytopes P, Q in $\mathbb{R}^n$ is

$$P + Q = \{p + q \in \mathbb{R}^n : p \in P,\ q \in Q\}.$$



Minkowski length $L(P)$

Definition: The largest number of lattice polytopes of positive dimension whose Minkowski sum is contained in P is called the Minkowski length:

$$L(P) = \max\{L \in \mathbb{N} : Q = Q_1 + \cdots + Q_L \subseteq P, \dim Q_i > 0\}.$$

Note: $L(P)$ is the largest number of factors of f in $\mathcal{L}_P = \{f : P(f) \subseteq P\}$

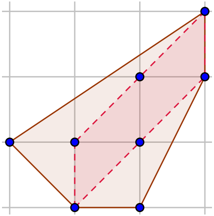
Minkowski length $L(P)$

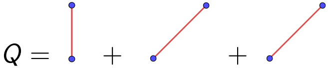
Definition: The largest number of lattice polytopes of positive dimension whose Minkowski sum is contained in P is called the Minkowski length:

$$L(P) = \max\{L \in \mathbb{N} : Q = Q_1 + \cdots + Q_L \subseteq P, \dim Q_i > 0\}.$$

Note: $L(P)$ is the largest number of factors of f in $\mathcal{L}_P = \{f : P(f) \subseteq P\}$

Example: $L(P) = 3$





a maximal decomposition in P

Minkowski length $L(P)$

Definition: The largest number of lattice polytopes of positive dimension whose Minkowski sum is contained in P is called the Minkowski length:

$$L(P) = \max\{L \in \mathbb{N} : Q = Q_1 + \cdots + Q_L \subseteq P, \dim Q_i > 0\}.$$

Note: $L(P)$ is the largest number of factors of f in $\mathcal{L}_P = \{f : P(f) \subseteq P\}$

Some Properties:

- Monotonicity: $L(Q) \leq L(P)$ if $Q \subseteq P$,
- Superadditivity: $L(P) + L(Q) \leq L(P + Q)$,
- Invariance: $L(P)$ is $\mathrm{AGL}(n, \mathbb{Z})$-invariant.
- $L(P)$ can be computed in polynomial time in size of P for $n = 2, 3$ (Soprunova et al, 2009, 2012)

Solving the problem for $n = 2$

Example: Consider $f = 1 - x^a y^b$, where $\gcd(a, b) = 1$. What is N_f?

Solving the problem for $n = 2$

Example: Consider $f = 1 - x^a y^b$, where $\gcd(a, b) = 1$. What is N_f?

Change of variables: $x = u^r v^{-b}$, $y = u^s v^a$,
for some $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

This is an automorphism of $(\mathbb{F}_q^*)^2$ and, hence, does not change N_f.

Solving the problem for $n = 2$

Example: Consider $f = 1 - x^a y^b$, where $\gcd(a, b) = 1$. What is N_f?

Change of variables: $x = u^r v^{-b}$, $y = u^s v^a$,
for some $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

This is an automorphism of $(\mathbb{F}_q^*)^2$ and, hence, does not change N_f.

Then $f = 1 - x^a y^b = 1 - (u^r v^{-b})^a (u^s v^a)^b = 1 - u$
We have $\mathrm{N}_f = q - 1$.

Solving the problem for $n = 2$

Example: Consider $f = 1 - x^a y^b$, where $\gcd(a, b) = 1$. What is N_f?

Change of variables: $x = u^r v^{-b}$, $y = u^s v^a$,
for some $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

This is an automorphism of $(\mathbb{F}_q^*)^2$ and, hence, does not change N_f.

Then $f = 1 - x^a y^b = 1 - (u^r v^{-b})^a (u^s v^a)^b = 1 - u$
We have $\mathrm{N}_f = q - 1$.

Geometrically, $\begin{pmatrix} r & s \\ -b & a \end{pmatrix} \in \mathrm{AGL}(2, \mathbb{Z})$ brings $P(f)$ to $[0, e_1]$.

Solving the problem for $n = 2$

Let $L = L(P)$ and consider $f = f_1 \cdots f_L$ in $\mathcal{L}_P$.

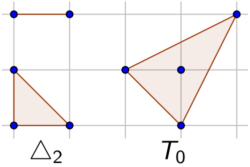
Observe: Each f_i has $P(f_i)$ of Minkowski length one.

Solving the problem for $n = 2$

Let $L = L(P)$ and consider $f = f_1 \cdots f_L$ in $\mathcal{L}_P$.

Observe: Each f_i has $P(f_i)$ of Minkowski length one.

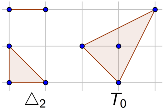
Theorem: (Soprunova, —, 2009)
Minkowski length one polytopes in $\mathbb{R}^2$ up to $\mathrm{AGL}(n, \mathbb{Z})$-equivalence are



Proposition: (Soprunova, —, 2009) At *most one* of the f_i has $P(f_i) \simeq T_0$.

Solving the problem for $n = 2$

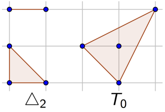
Proposition (Soprunova, —, 2009)



- if $P(f_i) =$ primitive segment then $\mathrm{N}_{f_i} = q - 1$
- if $P(f_i) = \triangle_2$ then $\mathrm{N}_{f_i} = q - 2$
- if $P(f_i) = T_0$ then $\mathrm{N}_{f_i} \leq q - 1 + 2\sqrt{q} - 1$ (from Hasse-Weil)

Solving the problem for $n = 2$

Proposition (Soprunova, —, 2009)



- if $P(f_i) =$ primitive segment then $\mathrm{N}_{f_i} = q - 1$
- if $P(f_i) = \triangle_2$ then $\mathrm{N}_{f_i} = q - 2$
- if $P(f_i) = T_0$ then $\mathrm{N}_{f_i} \le q - 1 + 2\sqrt{q} - 1$ (from Hasse-Weil)

Theorem (Soprunova, —, 2009) Let P be lattice polygon in $\mathbb{R}^2$, and $q > \alpha(P)$. Then

$$\mathrm{N}_{\mathcal{L}_P} \le L(P)(q-1) + 2\sqrt{q} - 1$$

(Remove $2\sqrt{q} - 1$ term if no T_0 appears in a maximal decomposition.)

Now we enter dimension $n = 3$ ...

Polytopes of Minkowski length one in $\mathbb{R}^3$

Let $L(P) = 1$. Observe:

- P has at most $2^3 = 8$ lattice points
- Every edge of P (in fact, every segment in P) is primitive
- Every face of P is a triangle (either $\simeq \triangle_2$ or $\simeq T_0$)

Polytopes of Minkowski length one in $\mathbb{R}^3$

Let $L(P) = 1$. Observe:

- P has at most $2^3 = 8$ lattice points
- Every edge of P (in fact, every segment in P) is primitive
- Every face of P is a triangle (either $\simeq \triangle_2$ or $\simeq T_0$)

Theorem (Whitney, 2010; Blanco-Santos, 2016)
Let $P \subset \mathbb{R}^3$ have $L(P) = 1$. Then P belongs to

- one of the infinite families of width one polytopes:
  - hollow and clean tetrahedra (empty tetrahedra) White (1964)
  - hollow clean and non-clean 5- and 6-vertex polytopes, OR
- one of 108 classes of non-hollow polytopes.

Polytopes of Minkowski length one in $\mathbb{R}^3$

Let $L(P) = 1$. Observe:

– P has at most $2^3 = 8$ lattice points
– Every edge of P (in fact, every segment in P) is primitive
– Every face of P is a triangle (either $\simeq \triangle_2$ or $\simeq T_0$)

Theorem (Whitney, 2010; Blanco-Santos, 2016)
Let $P \subset \mathbb{R}^3$ have $L(P) = 1$. Then P belongs to

- one of the infinite families of width one polytopes:
  - hollow and clean tetrahedra (empty tetrahedra) White (1964)
  - hollow clean and non-clean 5- and 6-vertex polytopes, OR
- one of 108 classes of non-hollow polytopes.

Remark: Lattice polytopes $P \subset \mathbb{R}^3$ with $L(P) = 1$ were defined independently by Reznick (2002), as dps polytopes.

$\mathbb{F}_q$-zeros of irreducible factors, $n = 3$

Example:
Consider $f = 1 - x + z - x^a y^b z$, where $\gcd(a, b) = 1$. Bound on N_f?
Here $P(f) = \mathrm{conv}\{0, e_1, e_3, ae_1 + be_2 + e_3\}$ an empty tetrahedron.

$\mathbb{F}_q$-zeros of irreducible factors, $n = 3$

Example:
Consider $f = 1 - x + z - x^a y^b z$, where $\gcd(a, b) = 1$. Bound on N_f?
Here $P(f) = \mathrm{conv}\{0, e_1, e_3, ae_1 + be_2 + e_3\}$ an empty tetrahedron.

We have $f = (1 - x) + (1 - x^a y^b)z$

two cases	upper bound on # of zeros
$x = 1$, $y^b = 1$, any $z \in \mathbb{F}_q^*$	$b(q-1)$
$x \neq 1$, $x^a y^b \neq 1$, z unique	$(q-1)^2 - 2(q-1) + b$, by incl/excl

$\mathbb{F}_q$-zeros of irreducible factors, $n = 3$

Example:
Consider $f = 1 - x + z - x^a y^b z$, where $\gcd(a, b) = 1$. Bound on N_f?
Here $P(f) = \mathrm{conv}\{0, e_1, e_3, ae_1 + be_2 + e_3\}$ an empty tetrahedron.

We have $f = (1 - x) + (1 - x^a y^b)z$

two cases	upper bound on # of zeros
$x = 1$, $y^b = 1$, any $z \in \mathbb{F}_q^*$	$b(q-1)$
$x \neq 1$, $x^a y^b \neq 1$, z unique	$(q-1)^2 - 2(q-1) + b$, by incl/excl

Total: $\mathrm{N}_f \le (q-1)^2 + (b-2)q + 2$

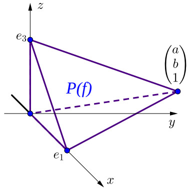
$\mathbb{F}_q$-zeros of irreducible factors, $n = 3$

Example:
Consider $f = 1 - x + z - x^a y^b z$, where $\gcd(a, b) = 1$. Bound on N_f?
Here $P(f) = \mathrm{conv}\{0, e_1, e_3, ae_1 + be_2 + e_3\}$ an empty tetrahedron.

We have $f = (1 - x) + (1 - x^a y^b)z$

two cases	upper bound on # of zeros
$x = 1,\ y^b = 1$, any $z \in \mathbb{F}_q^*$	$b(q-1)$
$x \neq 1,\ x^a y^b \neq 1$, z unique	$(q-1)^2 - 2(q-1) + b$, by incl/excl

Total: $\mathrm{N}_f \leq (q-1)^2 + \underset{\substack{\uparrow \\ \mathrm{Vol}(P(f))}}{(b-2)}q + 2$



$\mathbb{F}_q$-zeros of irreducible factors, $n = 3$

Theorem (Meyer, Soprunova, — 2021) Let $\operatorname{char} \mathbb{F}_q > 41$, $f \in \mathbb{F}_q[x, y, z]$ with $L(P(f)) = 1$ and $\dim P(f) = 3$. Then

$$\mathrm{N}_f \leq (q-1)^2 + (\mathrm{Vol}(P) - 2)q + 2.$$

$\mathbb{F}_q$-zeros of irreducible factors, $n = 3$

Theorem (Meyer, Soprunova, — 2021) Let $\operatorname{char} \mathbb{F}_q > 41$, $f \in \mathbb{F}_q[x, y, z]$ with $L(P(f)) = 1$ and $\dim P(f) = 3$. Then

$$\mathrm{N}_f \leq (q-1)^2 + (\mathrm{Vol}(P) - 2)q + 2.$$

- For the 108 $\mathrm{AGL}(3, \mathbb{Z})$-classes it follows from J. Whitney's work
- For the lattice width 1 polytopes we use mixed volumes and the BKK bound

$\mathbb{F}_q$-zeros of irreducible factors, $n = 3$

Theorem (Meyer, Soprunova, — 2021) Let $\operatorname{char}\mathbb{F}_q > 41$, $f \in \mathbb{F}_q[x, y, z]$ with $L(P(f)) = 1$ and $\dim P(f) = 3$. Then

$$\mathrm{N}_f \leq (q-1)^2 + (\mathrm{Vol}(P) - 2)q + 2.$$

- For the 108 $\mathrm{AGL}(3, \mathbb{Z})$-classes it follows from J. Whitney's work
- For the lattice width 1 polytopes we use mixed volumes and the BKK bound

Remark: If $P(f) \simeq T_0 \subset \mathbb{R}^3$ we get a worse bound

$$\mathrm{N}_f \leq (q-1)(q + 2\sqrt{q} - 2) \sim q^2 + cq^{3/2} + O(q)$$

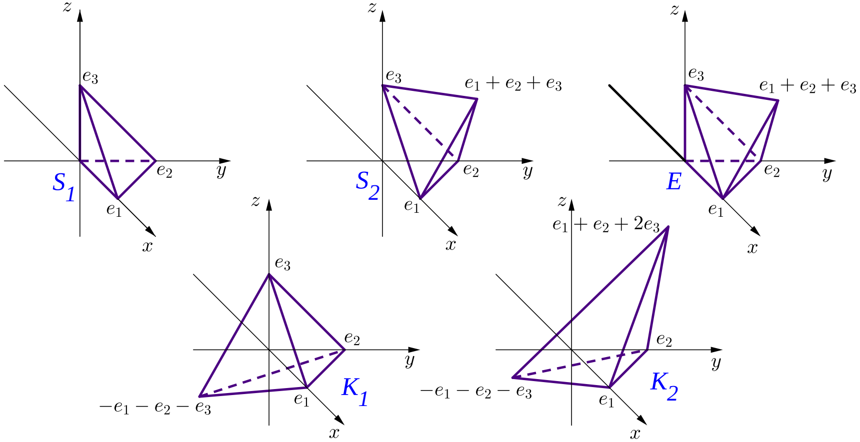
Classifying maximal decompositions in $\mathbb{R}^3$

Let $Q_1 + \cdots + Q_L \subset P$ be a maximal decomposition with $L(P) = L > 1$ and $\dim Q_i = 3$. Note $L(Q_i + Q_i) = 2$, $L(Q_i + Q_j + Q_k) = 3$, etc.

Classifying maximal decompositions in $\mathbb{R}^3$

Let $Q_1 + \cdots + Q_L \subset P$ be a maximal decomposition with $L(P) = L > 1$ and $\dim Q_i = 3$. Note $L(Q_i + Q_i) = 2$, $L(Q_i + Q_j + Q_k) = 3$, etc.

Theorem (Meyer, Soprunova, —, 2021) Each $Q_i \simeq$



Classifying maximal decompositions in $\mathbb{R}^3$

Pairs: Suppose $L(Q_1) = L(Q_2) = 1$, $L(Q_1 + Q_2) = 2$. Then

$(\lvert Q_1 \cap \mathbb{Z}^3\rvert, \lvert Q_2 \cap \mathbb{Z}^3\rvert)$	$(Q_1, Q_2) \simeq$
(4,4)	(T_0, Q), where $Q \simeq T_0$ or S_2 $Q_1 \simeq S_1$ or S_2 and $Q_2 \simeq S_1$ or S_2
(5,4)	(K_1, S_1), (E, S_2) (K_2, S), where $S \simeq S_1$
(5,5)	(K_1, K_1)
$(\geq 6, \geq 3)$	impossible

Classifying maximal decompositions in $\mathbb{R}^3$

Pairs: Suppose $L(Q_1) = L(Q_2) = 1$, $L(Q_1 + Q_2) = 2$. Then

$(\lvert Q_1 \cap \mathbb{Z}^3 \rvert, \lvert Q_2 \cap \mathbb{Z}^3 \rvert)$	$(Q_1, Q_2) \simeq$
(4,4)	(T_0, Q), where $Q \simeq T_0$ or S_2 $Q_1 \simeq S_1$ or S_2 and $Q_2 \simeq S_1$ or S_2
(5,4)	(K_1, S_1), (E, S_2) (K_2, S), where $S \simeq S_1$
(5,5)	(K_1, K_1)
$(\geq 6, \geq 3)$	impossible

k-tuples with $k \geq 3$: Suppose $L(Q_1) = \cdots = L(Q_k) = 1$, $L(Q_1 + \cdots + Q_k) = k$. Then $(Q_1, \ldots, Q_k) \simeq (S_1, \ldots, S_1)$, or $(S_2, \ldots, S_2)$, or $(E, S_2, \ldots S_2)$, or $(S_1, S, \ldots, S)$, where $S \simeq S_2$.

Main Result for $n = 3$

Theorem (Meyer, Soprunova, —, 2021) Let $\mathrm{char}\,(\mathbb{F}_q) > 41$, $P \subset [0, q-2]^3$, and $L = L(P)$. Consider $f \in \mathcal{L}_P$ with the largest number of absolutely irreducible factors. Let k be the number of such factors with 4 or more monomials. Then

1. if $k = 0$ then $\mathrm{N}_f \le L(q-1)^2$;
2. if $k = 1$ then
   (a) $\mathrm{N}_f \le L(q-1)^2 + (q-1)(2\sqrt{q}-1)$, if f has a factor with Newton polytope equivalent to T_0,
   (b) $\mathrm{N}_f \le L(q-1)^2 + (\mathrm{Vol}(P) - 3L + 1)q + 2$, otherwise;
3. if $k = 2$ then $\mathrm{N}_f \le L(q-1)^2 + 2(q-1)(2\sqrt{q}-1)$;
4. if $k \ge 3$ then $\mathrm{N}_f \le L(q-1)^2 + 2k + 1 \le L(q-1)^2 + 2L + 1$.

Main Result for $n = 3$

Theorem (Meyer, Soprunova, —, 2021) Let $\mathrm{char}\,(\mathbb{F}_q) > 41$, $P \subset [0, q-2]^3$, and $L = L(P)$. Consider $f \in \mathcal{L}_P$ with the largest number of absolutely irreducible factors. Let k be the number of such factors with 4 or more monomials. Then

1. if $k = 0$ then $\mathrm{N}_f \leq L(q-1)^2$;
2. if $k = 1$ then
   (a) $\mathrm{N}_f \leq L(q-1)^2 + (q-1)(2\sqrt{q}-1)$, if f has a factor with Newton polytope equivalent to T_0,
   (b) $\mathrm{N}_f \leq L(q-1)^2 + (\mathrm{Vol}(P) - 3L + 1)q + 2$, otherwise;
3. if $k = 2$ then $\mathrm{N}_f \leq L(q-1)^2 + 2(q-1)(2\sqrt{q}-1)$;
4. if $k \geq 3$ then $\mathrm{N}_f \leq L(q-1)^2 + 2k + 1 \leq L(q-1)^2 + 2L + 1$.

Main Result for $n = 3$

Theorem (Meyer, Soprunova, —, 2021) Let $\mathrm{char}(\mathbb{F}_q) > 41$, $P \subset [0, q-2]^3$, and $L = L(P)$. Then for q large enough we have

$$\mathrm{N}_{\mathcal{L}_P} \leq L(q-1)^2 + 2(q-1)(2\sqrt{q} - 1).$$

Remark: Compare to $\mathrm{N}_{\mathcal{L}_P} \leq L(q-1) + 2\sqrt{q} - 1$ for $n = 2$.

Some references

- I. Soprunov, J. Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math. 23, Issue 1, (2009) pp. 384-400
- Josh Whitney, *A bound on the minimum distance of three dimensional toric codes* Ph.D. Thesis, UC Irvine 2010
- O. Beckwith, M. Grimm, J. Soprunova, B. Weaver, *Minkowski length of 3D lattice polytopes*, Discrete and Computational Geometry 48, Issue 4 (2012), 1137-1158.
- K. Meyer, I. Soprunov, J. Soprunova, *On the number of* $\mathbb{F}_q$*-zeros of families of sparse trivariate polynomials*, arXiv:2105.10071, MATLAB code: `github.com/isoprou/minkowski-length`

Some references

- I. Soprunov, J. Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math. 23, Issue 1, (2009) pp. 384-400
- Josh Whitney, *A bound on the minimum distance of three dimensional toric codes* Ph.D. Thesis, UC Irvine 2010
- O. Beckwith, M. Grimm, J. Soprunova, B. Weaver, *Minkowski length of 3D lattice polytopes*, Discrete and Computational Geometry 48, Issue 4 (2012), 1137-1158.
- K. Meyer, I. Soprunov, J. Soprunova, *On the number of $\mathbb{F}_q$-zeros of families of sparse trivariate polynomials*, arXiv:2105.10071, MATLAB code: `github.com/isoprou/minkowski-length`

Thank you!