Toric codes and Minkowski length of polytopes

CIMPA 2018 Zacatecas

Ivan Soprunov

Cleveland State University

July 3, 2018

What are toric codes? (reminder and setup)

• Let
$$\mathbb{T} = (\mathbb{F}_q^*)^r = \{p_1, \dots, p_n\}$$
, the algebraic torus.

► Let P be a lattice polytope in R^r. It defines a finite dimensional space of Laurent polynomials:

$$\mathcal{L}_{P} = \operatorname{span}_{\mathbb{F}_{a}} \{ t^{a} \mid a \in P \cap \mathbb{Z}^{r} \}, \text{ where } t^{a} = t_{1}^{a_{1}} \cdots t_{r}^{a_{r}}.$$

Evaluation Map:

$$\operatorname{ev}_{\mathbb{T}}: \mathcal{L}_P \to \mathbb{F}_q^n \quad f \mapsto (f(p_1), \ldots, f(p_n)).$$

Toric Code: $C_P = ev_{\mathbb{T}}(\mathcal{L}_P)$.

What are toric codes? (reminder and setup)

• Let
$$\mathbb{T} = (\mathbb{F}_q^*)^r = \{p_1, \dots, p_n\}$$
, the algebraic torus.

Let P be a lattice polytope in ℝ^r. It defines a finite dimensional space of Laurent polynomials:

$$\mathcal{L}_{P} = \operatorname{span}_{\mathbb{F}_{a}} \{ t^{a} \mid a \in P \cap \mathbb{Z}^{r} \}, \text{ where } t^{a} = t_{1}^{a_{1}} \cdots t_{r}^{a_{r}}.$$

Evaluation Map:

$$\operatorname{ev}_{\mathbb{T}}: \mathcal{L}_P \to \mathbb{F}_q^n \quad f \mapsto (f(p_1), \ldots, f(p_n)).$$

Toric Code: $C_P = ev_{\mathbb{T}}(\mathcal{L}_P)$.

Example:

Let
$$\mathbb{F}_q = \mathbb{F}_4$$
 and $r = 2$. Then $|\mathbb{T}| = |(\mathbb{F}_q^*)^2| = 9$.
 $\mathcal{L}_P = \{\lambda_1 t_1 + \lambda_2 t_2 + \lambda_3 t_1 t_2 + \lambda_4 t_1^2 t_2^2 \mid \lambda_i \in \mathbb{F}_4\}.$
In fact, \mathcal{C}_P is a $[9, 4, 3]_4$ -code.

Ivan Soprunov, Cleveland State University

D. Ruano (2007): The evaluation map $ev_{\mathbb{T}} : \mathcal{L}_P \to \mathbb{F}_q^n$ is injective *iff* points in $P \cap \mathbb{Z}^r$ are distinct in $(\mathbb{Z}/(q-1)\mathbb{Z})^r$.

In this case C_P has parameters:

 $n = (q-1)^r$ (length) $k = |P \cap \mathbb{Z}^r|$ (dimension) d = ? (min distance)

D. Ruano (2007): The evaluation map $ev_{\mathbb{T}} : \mathcal{L}_P \to \mathbb{F}_q^n$ is injective *iff* points in $P \cap \mathbb{Z}^r$ are distinct in $(\mathbb{Z}/(q-1)\mathbb{Z})^r$.

In this case C_P has parameters:

 $n = (q-1)^r$ (length) $k = |P \cap \mathbb{Z}^r|$ (dimension) d = ? (min distance)

Serre (1989) If $P = \ell \triangle_r$, where \triangle_r is the standard simplex then

 $d = (q-1)^{r-1}(q-1-\ell).$

D. Ruano (2007): The evaluation map $ev_{\mathbb{T}} : \mathcal{L}_P \to \mathbb{F}_q^n$ is injective *iff* points in $P \cap \mathbb{Z}^r$ are distinct in $(\mathbb{Z}/(q-1)\mathbb{Z})^r$.

In this case C_P has parameters: $n = (q-1)^r$ (length) $k = |P \cap \mathbb{Z}^r|$ (dimension) d = ? (min distance)

Serre (1989) If $P = \ell \triangle_r$, where \triangle_r is the standard simplex then

$$d = (q-1)^{r-1}(q-1-\ell).$$

Little, Schwarz (2007) If $P = [0, \ell_1] \times \cdots \times [0, \ell_r]$ then

$$d=(q-1-\ell_1)\cdots(q-1-\ell_r).$$

D. Ruano (2007): The evaluation map $ev_{\mathbb{T}} : \mathcal{L}_P \to \mathbb{F}_q^n$ is injective *iff* points in $P \cap \mathbb{Z}^r$ are distinct in $(\mathbb{Z}/(q-1)\mathbb{Z})^r$.

In this case C_P has parameters: $n = (q-1)^r$ (length) $k = |P \cap \mathbb{Z}^r|$ (dimension) d = ? (min distance)

Serre (1989) If $P = \ell \triangle_r$, where \triangle_r is the standard simplex then

$$d = (q-1)^{r-1}(q-1-\ell).$$

Little, Schwarz (2007) If $P = [0, \ell_1] \times \cdots \times [0, \ell_r]$ then

$$d=(q-1-\ell_1)\cdots(q-1-\ell_r).$$

J. Soprunova, — (2010) For any lattice polytopes P, Q

$$d(\mathcal{C}_{P\times Q})=d(\mathcal{C}_P)d(\mathcal{C}_Q).$$

$$d(\mathcal{C}_{\ell Pyr(Q)}) = (q-1)d(\mathcal{C}_{\ell Q}), ext{ for any } \ell = 1,2,3,\dots$$

$$d(\mathcal{C}_P)=n-N_q(P),$$

where

$$N_q(P) = \max_{0 \neq f \in \mathcal{L}_P} |Z(f)|$$
 and $Z(f) = \{p \in \mathbb{T} \mid f(p) = 0\},$

the zero set of f in \mathbb{T} .

1

$$d(\mathcal{C}_P)=n-N_q(P),$$

where

$$N_q(P) = \max_{0 \neq f \in \mathcal{L}_P} |Z(f)|$$
 and $Z(f) = \{p \in \mathbb{T} \mid f(p) = 0\},$

the zero set of f in \mathbb{T} .

Serre (1989): For $q > \ell$, among all polynomials of degree ℓ , the polynomials that factor the most have the most zeroes in \mathbb{T} .

$$d(\mathcal{C}_P)=n-N_q(P),$$

where

$$N_q(P) = \max_{0
eq f \in \mathcal{L}_P} |Z(f)|$$
 and $Z(f) = \{p \in \mathbb{T} \mid f(p) = 0\},$

the zero set of f in \mathbb{T} .

Serre (1989): For $q > \ell$, among all polynomials of degree ℓ , the polynomials that factor the most have the most zeroes in \mathbb{T} .

Thus we should take f to be the product of linear factors, so

$$N_q(\ell \triangle_r) = \max_{0 \neq f \in \mathcal{L}_{\ell \triangle_r}} |Z(f)| = \ell(q-1)^{r-1},$$

attained at $f(t_1, \ldots, t_r) = (t_1 - \alpha_1) \cdots (t_1 - \alpha_\ell)$ for distinct $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q^*$.

$$d(\mathcal{C}_P)=n-N_q(P),$$

where

$$N_q(P) = \max_{0
eq f \in \mathcal{L}_P} |Z(f)|$$
 and $Z(f) = \{p \in \mathbb{T} \mid f(p) = 0\},$

the zero set of f in \mathbb{T} .

Serre (1989): For $q > \ell$, among all polynomials of degree ℓ , the polynomials that factor the most have the most zeroes in \mathbb{T} .

Thus we should take f to be the product of linear factors, so

$$N_q(\ell \triangle_r) = \max_{0 \neq f \in \mathcal{L}_{\ell \triangle_r}} |Z(f)| = \ell(q-1)^{r-1},$$

attained at $f(t_1, \ldots, t_r) = (t_1 - \alpha_1) \cdots (t_1 - \alpha_\ell)$ for distinct $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q^*$.

Similar principle holds in general for large q.

Little-Schenck (2006) (r = 2); J. Whitney (2010) (r = 3)

Theorem

Let P be a lattice polytope in \mathbb{R}^r and $q > \alpha(P)$ (large enough). For any $f, g \in \mathcal{L}_P$ consider factorizations into absolutely irreducible factors:

 $f = f_1 \cdots f_s$ and $g = g_1 \cdots g_t$,

and assume the g_i are distinct. Then s < t implies |Z(f)| < |Z(g)|.

Little-Schenck (2006) (r = 2); J. Whitney (2010) (r = 3)

Theorem

Let P be a lattice polytope in \mathbb{R}^r and $q > \alpha(P)$ (large enough). For any $f, g \in \mathcal{L}_P$ consider factorizations into absolutely irreducible factors:

 $f = f_1 \cdots f_s$ and $g = g_1 \cdots g_t$,

and assume the g_i are distinct. Then s < t implies |Z(f)| < |Z(g)|.

Idea for r = 2: If Y is an irreducible projective curve over $\overline{\mathbb{F}}_q$ then

Hasse-Weil Bound $q+1-2g\sqrt{q} \leq |Y(\mathbb{F}_q)| \leq q+1+2g\sqrt{q}$

where g is the genus of Y. On one hand,

$$|Z(f)| \leq \sum_{i=1}^{s} |Z(f_i)| \leq sq + ext{lower order terms}$$

Little-Schenck (2006) (r = 2); J. Whitney (2010) (r = 3)

Theorem

Let P be a lattice polytope in \mathbb{R}^r and $q > \alpha(P)$ (large enough). For any $f, g \in \mathcal{L}_P$ consider factorizations into absolutely irreducible factors:

$$f = f_1 \cdots f_s$$
 and $g = g_1 \cdots g_t$,

and assume the g_i are distinct. Then s < t implies |Z(f)| < |Z(g)|.

Idea for r = 2: If Y is an irreducible projective curve over $\overline{\mathbb{F}}_q$ then

Hasse-Weil Bound $q+1-2g\sqrt{q} \leq |Y(\mathbb{F}_q)| \leq q+1+2g\sqrt{q}$

where g is the genus of Y. On the other hand,

$$tq+ ext{lower order terms} \leq \sum_{i=1}^t |Z(g_i)| - \sum_{i < j} |Z(g_i) \cap Z(g_j)| \leq |Z(g)|$$

Little-Schenck (2006) (r = 2); J. Whitney (2010) (r = 3)

Theorem

Let P be a lattice polytope in \mathbb{R}^r and $q > \alpha(P)$ (large enough). For any $f, g \in \mathcal{L}_P$ consider factorizations into absolutely irreducible factors:

$$f = f_1 \cdots f_s$$
 and $g = g_1 \cdots g_t$,

and assume the g_i are distinct. Then s < t implies |Z(f)| < |Z(g)|.

Main Questions:

- 1. What is the largest number of factors $f \in \mathcal{L}_P$ may have?
- 2. What do the irreducible factors in this case look like?
- 3. Can we bound the number of \mathbb{F}_q -zeros of irreducible factors?

In fact, the first two questions are about the geometry of P.

- 1. The largest number of factors $f \in \mathcal{L}_P$ may have is the Minkowski length of P.
- 2. The irreducible factors of such *f* have Newton polytopes that are strongly indecomposable.
- The third question is more algebraic.
 - 3. Bound the maximum number of \mathbb{F}_q -zeros $N_q(P)$ where P is strongly indecomposable.

Once we know that we can bound the minimum distance of \mathcal{C}_P

Newton polytopes and Minkowski Sum

Let f be a Laurent polynomial $f \in \mathbb{F}_q[t_1, \ldots, t_r]$. Let P(f) be its Newton Polytope: $P(f) = \text{ conv.hull } \{ \text{ exponents of } f \} \subset \mathbb{R}^r$ Note: Newton polytope generalizes the notion of degree:

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

Newton polytopes and Minkowski Sum

Let f be a Laurent polynomial $f \in \mathbb{F}_q[t_1, \ldots, t_r]$. Let P(f) be its Newton Polytope: $P(f) = \text{ conv.hull} \{ \text{ exponents of } f \} \subset \mathbb{R}^r$ Note: Newton polytope generalizes the notion of degree:

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

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



Let *P* be a lattice polytope in \mathbb{R}^r .

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

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

Polytopes with L(P) = 1 are called strongly indecomposable.

Let *P* be a lattice polytope in \mathbb{R}^r .

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

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

Polytopes with L(P) = 1 are called strongly indecomposable. Example



Let P be a lattice polytope in \mathbb{R}^r .

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

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

Polytopes with L(P) = 1 are called strongly indecomposable. Example

•
$$L(P) = 3$$



Let P be a lattice polytope in \mathbb{R}^r .

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

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

Polytopes with L(P) = 1 are called strongly indecomposable.

Example

- ► *L*(*P*) = 3
- Every primitive segment (i.e. with exactly two lattice points) is strongly indecomposable.



Minkowski length L(P): Connection

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

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

Polytopes with L(P) = 1 are called strongly indecomposable.

Claim: L(P) equals the largest number of factors of f in \mathcal{L}_P .

Minkowski length L(P): Connection

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

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

Polytopes with L(P) = 1 are called strongly indecomposable.

Claim: L(P) equals the largest number of factors of f in \mathcal{L}_P .

Indeed, let $f \in \mathcal{L}_P$ be a polytope with the largest number of factors

$$f = f_1 \cdots f_L.$$

Then $P(f) = P(f_1) + \cdots + P(f_L) \subseteq P$. Hence $L \leq L(P)$. Conversely, let $Q = Q_1 + \cdots + Q_{L(P)} \subseteq P$ be a maximal decomposition. Choose any g_i with $P(g_i) = Q_i$. Then the polynomial $g = g_1 \cdots g_{L(P)}$ is in \mathcal{L}_P and, hence, $L(P) \leq L$.

Minkowski length L(P): Properties

Simple Properties:

- Invariance: L(P) is AGL (r, \mathbb{Z}) -invariant,
- Monotonicity: $L(Q) \leq L(P)$ if $Q \subseteq P$,
- Superadditivity: $L(P) + L(Q) \le L(P + Q)$,

Note: $AGL(r, \mathbb{Z})$ -equivalent polytopes produce equivalent codes!

Minkowski length L(P): Properties

Simple Properties:

- ▶ Invariance: *L*(*P*) is AGL(*r*, ℤ)-invariant,
- Monotonicity: $L(Q) \leq L(P)$ if $Q \subseteq P$,
- Superadditivity: $L(P) + L(Q) \le L(P+Q)$,

Note: $AGL(r, \mathbb{Z})$ -equivalent polytopes produce equivalent codes!

Some examples:

- $L(\ell \triangle_r) = \ell$ for the simplex \triangle_r and any $\ell \in \mathbb{N}$.
- For $P = [0, \ell_1] \times \cdots \times [0, \ell_r]$ we have $L(P) = \ell_1 + \cdots + \ell_r$.
- $L(P \times Q) = L(P) + L(Q)$

How to compute L(P)?

Let L = L(P). The maximal decompositions $Q_1 + \cdots + Q_L \subseteq P$ form a *poset* with respect to inclusion (up to a lattice translation). Minimal elements are smallest maximal decompositions.

How to compute L(P)?

Let L = L(P). The maximal decompositions $Q_1 + \cdots + Q_L \subseteq P$ form a *poset* with respect to inclusion (up to a lattice translation). Minimal elements are smallest maximal decompositions.

Proposition

Every smallest maximal decomposition is a sum of primitive segments with at most $2^r - 1$ distinct direction vectors.

How to compute L(P)?

Let L = L(P). The maximal decompositions $Q_1 + \cdots + Q_L \subseteq P$ form a *poset* with respect to inclusion (up to a lattice translation). Minimal elements are smallest maximal decompositions.

Proposition

Every smallest maximal decomposition is a sum of primitive segments with at most $2^r - 1$ distinct direction vectors.

Reason: The direction vectors v_1, \ldots, v_k are non-zero mod $(2\mathbb{Z})^r$. If $k \ge 2^r$ then $v_i + v_j = 2v$ for some i < j.



This produced a simple algorithm for computing L(P) for r = 2, 3.

Strongly indecomposable lattice polytopes

Claim: If L(P) = 1 then $|P \cap \mathbb{Z}^r| \leq 2^r$.

Strongly indecomposable lattice polytopes

Claim: If L(P) = 1 then $|P \cap \mathbb{Z}^r| \leq 2^r$.

Reason: If $|P \cap \mathbb{Z}^r| > 2^r$ then there are two points $p, q \in P \cap \mathbb{Z}^r$ congruent mod $(2\mathbb{Z})^r$. Then the segment $[p, q] \in P$ is not primitive (contains an interior lattice point) so L(P) > 1.

Strongly indecomposable lattice polytopes

Claim: If L(P) = 1 then $|P \cap \mathbb{Z}^r| \leq 2^r$.

Reason: If $|P \cap \mathbb{Z}^r| > 2^r$ then there are two points $p, q \in P \cap \mathbb{Z}^r$ congruent mod $(2\mathbb{Z})^r$. Then the segment $[p, q] \in P$ is not *primitive* (contains an interior lattice point) so L(P) > 1.

Strongly indecomposable lattice polytopes in \mathbb{R}^2

primitive lattice segments two classes of triangles



A bound for toric surface codes



Note By observation and Hasse-Weil

• if P(f) = primitive segment then |Z(f)| = q - 1

• if
$$P(f) = \triangle_2$$
 then $|Z(f)| = q - 2$

• if $P(f) = T_0$ then $|Z(f)| \le q - 1 + 2\sqrt{q} - 1$

Moreover: Every maximal decomposition contains at most one T_0 .

A bound for toric surface codes



Note By observation and Hasse-Weil

• if P(f) = primitive segment then |Z(f)| = q - 1

• if
$$P(f) = \triangle_2$$
 then $|Z(f)| = q - 2$

• if $P(f) = T_0$ then $|Z(f)| \le q - 1 + 2\sqrt{q} - 1$

Moreover: Every maximal decomposition contains at most one T_0 . Theorem (J. Soprunova, —, 2008) Let P be lattice polygon in \mathbb{R}^2 , and $q > \alpha(P)$. Then

$$d(\mathcal{C}_P) \geq (q-1)(q-1-L(P)) - (2\sqrt{q}-1)$$

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

Let L(P) = 1. First observations:

- 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 a \triangle_2 or a T_0).
- -P can have arbitrarily large volume.

Let L(P) = 1. First observations:

- 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 a \triangle_2 or a T_0).
- P can have arbitrarily large volume.

Theorem (Whitney, 2010; Santos-Blanco, 2016) Let L(P) = 1, dim P = 3. Then

```
▶ P may have 4, 5, or 6 vertices.
```

Let L(P) = 1. First observations:

- 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 a \triangle_2 or a T_0).
- P can have arbitrarily large volume.

Theorem (Whitney, 2010; Santos-Blanco, 2016)

Let L(P) = 1, dim P = 3. Then

- P may have 4, 5, or 6 vertices.
- There are infinite families of such P:
 - hollow and clean tetrahedra
 - hollow clean and non-clean double pyramids
 - hollow clean and non-clean 6 vertex polytopes

Let L(P) = 1. First observations:

- 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 a \triangle_2 or a T_0).
- P can have arbitrarily large volume.

Theorem (Whitney, 2010; Santos-Blanco, 2016)

Let L(P) = 1, dim P = 3. Then

- P may have 4, 5, or 6 vertices.
- There are infinite families of such P:
 - hollow and clean tetrahedra
 - hollow clean and non-clean double pyramids
 - hollow clean and non-clean 6 vertex polytopes
- There are 38 + 56 + 13 = 107 classes of non-hollow P.

What do maximal decompositions look like?

A lot has been understood recently by Beckwith, Grimm, Meyer, Soprunova, Weaver. In particular,

Theorem

- Any maximal decomposition contains at most one polytope with more than 5 lattice points. If it does then the other summands are primitive segments.
- Any maximal decomposition contains at most two distinct polytopes with 4 or 5 lattice points.

A bound for toric 3-fold codes?

What about bounds on $N_q(P)$ for strongly indecomposable P?

Theorem (Whitney, 2010) If P belongs to a finite family then for q > 41

$$N_q(P) \le 1 + F(P)/2 + (6 \operatorname{Vol}(P) - F(P)/2 - 2)q + q^2$$

If P belongs to an infinite family then there are bounds involving parameters of the family.

No simple bound for $d(\mathcal{C}_{\mathcal{P}})$ yet, but we are hopeful!

References

- O. Beckwith, M. Grimm, J. Soprunova, B. Weaver, *Minkowski length of 3D lattice polytopes*, Discrete and Computational Geometry 48, Issue 4 (2012), 1137-1158.



J. Hansen, Toric varieties Hirzebruch surfaces and error-correcting codes, Appl. Algebra Engrg. Comm. Comput. 13 (2002), pp. 289300



J. Little, H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), no. 4, 999–1014 (electronic).



- J. Little, R. Schwarz, *On toric codes and multivariate Vandermonde matrices*, Appl. Algebra Engrg. Comm. Comput. 18 (4) (2007), pp. 349–367.
- Diego Ruano, On the parameters of r-dimensional toric codes, Finite Fields and Their Applications 13 (2007), pp. 962–976.



J.-P. Serre, Lettre a M. Tsfasman, Astérisque 198-199-200 (1991), pp. 351-353.



I. Soprunov, J. Soprunova, Toric surface codes and Minkowski length of polygons, SIAM J. Discrete Math. 23, Issue 1, (2009) pp. 384-400



- I. Soprunov, J. Soprunova, *Bringing Toric Codes to the next dimension*, SIAM J. Discrete Math. 24, Issue 2, (2010) pp. 655-665
- Josh Whitney, A bound on the minimum distance of three dimensional toric codes Ph.D. Thesis, 2010