Toric Surface Codes and the Periodicity of Polytopes

Amelia Gibbs, Eliza Hogan, Jenna Plute, and Nicholas Toloczko
Advised by Dr. Jabbusch

The University of Michigan-Dearborn

August 14, 2024

Contents

Preliminaries

What is a code?

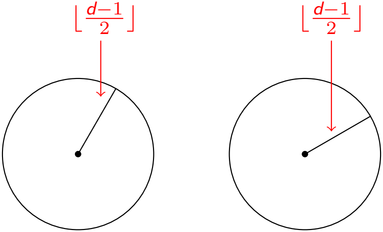
1. Let $\mathbb{F}_q$ be a finite field, with $q = p^l$ elements. A code C over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n = \mathbb{F}_q \times \ldots \times \mathbb{F}_q$.
2. Elements of a code are called **codewords**, and the **length** of the code is **n**, where $C \subset \mathbb{F}_q^n$.
3. C is a **linear code** if it is a vector subspace of $\mathbb{F}_q^n$, and the dimension of the code is $k := \dim_{\mathbb{F}_q} C$. The dimension of the code tells us how much information each codeword contains.

What is a code?

1. For $\mathrm{x} = (x_1, \ldots, x_n), \mathrm{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, **Hamming distance** from x to y is
$$d(\mathrm{x}, \mathrm{y}) := \#\{i \,|\, x_i \neq y_i\}$$
The **Hamming weight** of x is $wt(\mathrm{x}) = d(\mathrm{x}, (0, 0, \cdots, 0))$, or simply the number of non-zero entries in a codeword.
2. The **minimum distance** of C is
$$d_{\min} = \min\{d(\mathrm{x}, \mathrm{y}) \,|\, \mathrm{x}, \mathrm{y} \in C \text{ and } \mathrm{x} \neq \mathrm{y}\}$$
If C is a linear code,
$$d_{\min} = \min\{wt(\mathrm{x}) | \mathrm{x} \in C \text{ and } \mathrm{x} \neq (0, 0, \ldots, 0)\}.$$

Minimum Distance

The minimum distance of a code tells you how many errors a code can detect/correct. Linear codes can detect up to $d-1$ errors and correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.



Toric Codes

Hansen (1997): Consider codes given by **toric varieties**:

$$\{\text{toric variety of dim } m\} \leftrightarrow \{\text{an integral convex polytope } P \subset \mathbb{R}^m\}$$

Given an integral convex polytope $P \subset \mathbb{R}^m$:

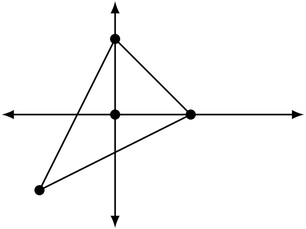
$$L_P = \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{x}^\beta \mid \beta \in P \cap \mathbb{Z}^m\}$$

and define the evaluation map

$$\begin{array}{rcl} ev : L_P & \rightarrow & \mathbb{F}_q^{(q-1)^m} \\ f & \mapsto & (f(\gamma) \mid \gamma \in (\mathbb{F}_q^*)^m) \end{array}$$

The image of the evaluation map gives the **toric code** $C_P(\mathbb{F}_q)$. The matrix corresponding to this evaluation map gives the generator matrix for C_P.

Example: Consider the polytope $P \subset \mathbb{R}^2$ with the $k = 4$ lattice points $(0,0), (1,0), (0,1)$ and $(-1,-1)$



$$L_P = \mathrm{Span}_{\mathbb{F}_q}\{x^0y^0, x^1y^0, x^0y^1, x^{-1}y^{-1}\}$$
$$= \mathrm{Span}_{\mathbb{F}_q}\{1, x, y, x^{-1}y^{-1}\}$$

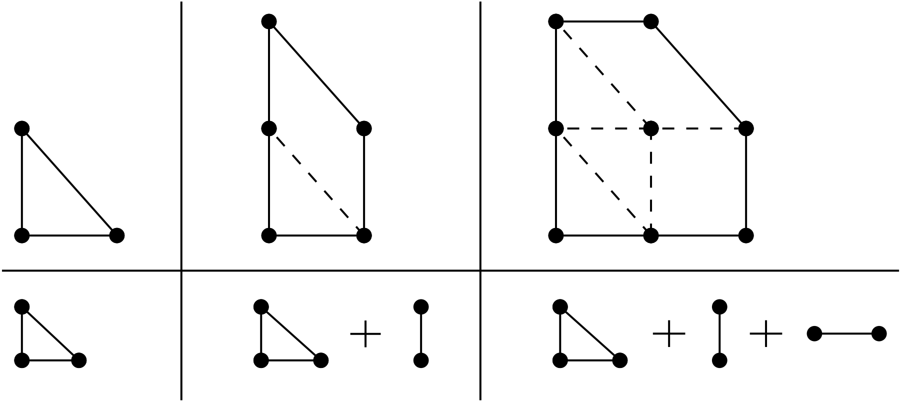
Given $P \subset \mathbb{R}^m$, we know the length and dimension of P's corresponding code.

- The length of $C_P(\mathbb{F}_q)$ is $n = (q-1)^m$
- The dimension of $C_P(\mathbb{F}_q)$ is $k =$ the number of lattice points in P
- The minimum distance of C_P, denoted $d(C_P)$, is exactly $(q-1)^m - \max_{0 \neq f \in L_P} |Z(f)|$ where $Z(f)$ is the set of all $(\mathbb{F}_q^\times)^m$-zeros of f.

Minkowski Sum

Let P and Q be convex polytopes in $\mathbb{R}^m$. Their **Minkowski sum** is

$$P + Q := \{p + q \in \mathbb{R}^m | \; p \in P, q \in Q\}$$



Minkowski Length

The (full) **Minkowski length** $L = L(P)$ of a lattice polytope P is the largest number of primitive segments (line segments with lattice points only on each end) whose Minkowski sum is in P.

Equivalently, $L(P)$ is the largest number of non-trivial lattice polytopes whose Minkowski sum is in P. Such a polytope is called a **maximal decomposition** in P.

The Connection to Minimum Distance

In [1], Soprunov and Soprunova proved the following, relating the Minkowski length of polytopes to the minimum distance of the codes generated by them:

The Connection to Minimum Distance

In [1], Soprunov and Soprunova proved the following, relating the Minkowski length of polytopes to the minimum distance of the codes generated by them:

Proposition

$|Z(f)| \leqslant L(q-1) + \lfloor 2\sqrt{q} \rfloor - 1$ where f is the polynomial with the largest number of irreducible factors.

Thus, if we can determine with certainty $L(P)$, then we have a direct bound on $d(C_p)$ because $d(C_p) = (q-1)^2 - max_{f \in L_P}|Z(f)|$.

A Stronger Connection to Toric Surface Codes

A Stronger Connection to Toric Surface Codes

Proposition

Suppose that $P \subset \mathbb{R}^2$ does not contain an exceptional triangle in any maximal decomposition. Let $0 \neq g \in L_P$ be a polynomial with maximum number of zeros and $g = g_1 \dots g_r$ be its factorization into irreducible polynomials. Then, when q is sufficiently large, we have that $r = L(P)$.

A Stronger Connection to Toric Surface Codes

Proposition

Suppose that $P \subset \mathbb{R}^2$ does not contain an exceptional triangle in any maximal decomposition. Let $0 \neq g \in L_P$ be a polynomial with maximum number of zeros and $g = g_1 \ldots g_r$ be its factorization into irreducible polynomials. Then, when q is sufficiently large, we have that $r = L(P)$.

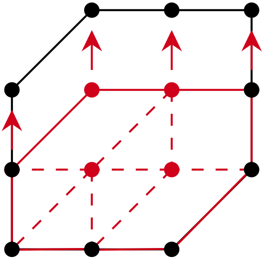
Take-away: To compute the maximum number of zeros in L_P (equivalently $d(C_P)$), we only need to look at the polynomials corresponding to maximal decompositions in P.

The Mapping Lemma

$f: \partial Z \cap \mathbb{Z}^2 \to \partial P \cap \mathbb{Z}^2 \Rightarrow \#\partial P \geqslant \#\partial Z$

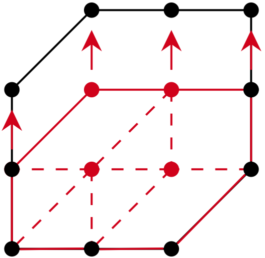
The Mapping Lemma

$f : \partial Z \cap \mathbb{Z}^2 \to \partial P \cap \mathbb{Z}^2 \Rightarrow \#\partial P \geqslant \#\partial Z$



The Mapping Lemma

$f \colon \partial Z \cap \mathbb{Z}^2 \to \partial P \cap \mathbb{Z}^2 \Rightarrow \#\partial P \geqslant \#\partial Z$



Proposition

Let $P \subset \mathbb{R}^2$ be an integral convex polytope which is lattice equivalent to

$$Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2].$$

Then, $L(P) = m + n + \ell$.

Periodicity of Polytopes

Scaling a Polytope

One important transformation is the t-**dilation of a polytope** P

$$tP := \{tp : p \in P\}.$$

While this transformation is easily defined, the effect it has on the Minkowski length of P is not so easily described.

Scaling a Polytope

One important transformation is the t-**dilation of a polytope** P

$$tP := \{tp : p \in P\}.$$

While this transformation is easily defined, the effect it has on the Minkowski length of P is not so easily described. We can, however, always say that

$$L(tP) \geq tL(P).$$

But, when do we have equality $(=)$ or strict inequality $(>)$?

Period-1 Polytopes

We know that

$$Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$$

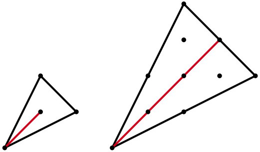
has Minkowski length $m + n + \ell$ so $L(tQ) = tm + tn + t\ell = tL(Q)$.

Period-1 Polytopes

We know that

$$Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$$

has Minkowski length $m + n + \ell$ so $L(tQ) = tm + tn + t\ell = tL(Q)$. But this isn't the case for the exceptional triangle.



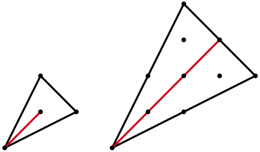
$L(T) = 1$ $\quad$ $L(2T) = 3$

Period-1 Polytopes

We know that

$$Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$$

has Minkowski length $m + n + \ell$ so $L(tQ) = tm + tn + t\ell = tL(Q)$. But this isn't the case for the exceptional triangle.



$L(T) = 1$ $\quad$ $L(2T) = 3$

Definition

Let $P \subset \mathbb{R}^m$ be a convex integral polytope. We say that P is a **period-1** polytope iff $L(tP) = tL(P)$ for all $t \geq 0$. If there is some t such that $L(tP) > tL(P)$ then we say that P has **period strictly greater than 1**. Equivalently defined in [2].

Period-1 Polytopes and The Exceptional Triangle

It is known that the exceptional triangle can appear as a summand in a maximal decomposition [1]. But, can this happen for a period-1 polytope?

Period-1 Polytopes and The Exceptional Triangle

It is known that the exceptional triangle can appear as a summand in a maximal decomposition [1]. But, can this happen for a period-1 polytope? If $T_0 + Q_2 + \cdots + Q_L = Q \subseteq P$ is a maximal decomposition then

$$L(tP) \geq L(tQ) \geq L(tT_0) + t(L-1) > tL = tL(P)$$

as $L(tT_0) > t$ when $t > 1$.

Period-1 Polytopes and The Exceptional Triangle

It is known that the exceptional triangle can appear as a summand in a maximal decomposition [1]. But, can this happen for a period-1 polytope? If $T_0 + Q_2 + \cdots + Q_L = Q \subseteq P$ is a maximal decomposition then

$$L(tP) \geq L(tQ) \geq L(tT_0) + t(L-1) > tL = tL(P)$$

as $L(tT_0) > t$ when $t > 1$.

Proposition

If P is a period-1 polytope then the exceptional triangle doesn't appear in any maximal decomposition.

Periodicity and Subpolytopes

Let $P, Q \subset \mathbb{R}^m$ be integral polytopes.

Proposition

If $P \subseteq Q$ with $L(P) = L(Q)$ and Q has period 1, then P also has period 1.

Periodicity and Subpolytopes

Let $P, Q \subset \mathbb{R}^m$ be integral polytopes.

Proposition

If $P \subseteq Q$ with $L(P) = L(Q)$ and Q has period 1, then P also has period 1.

Proposition

If $P \subseteq Q$ with $L(P) = L(Q)$ and P has period strictly greater than 1, then Q also has period strictly greater than 1.

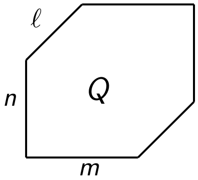
A Minimum Distance Formula

Minimum Distance of Smallest Maximal Decompositions

It is known [1] that all smallest maximal decompositions are lattice equivalent to $Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$.

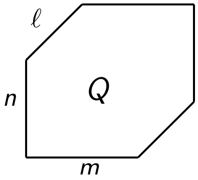
Minimum Distance of Smallest Maximal Decompositions

It is known [1] that all smallest maximal decompositions are lattice equivalent to $Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$.



Minimum Distance of Smallest Maximal Decompositions

It is known [1] that all smallest maximal decompositions are lattice equivalent to $Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$.

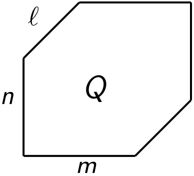


Lemma

The only maximal decomposition in Q is Q itself.

Minimum Distance of Smallest Maximal Decompositions

It is known [1] that all smallest maximal decompositions are lattice equivalent to $Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$.



Lemma

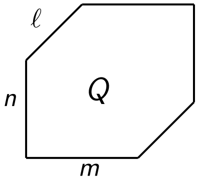
The only maximal decomposition in Q is Q itself.

Thus, the polynomial in L_Q which has the maximum number of zeros takes the form

$$\prod_{i=1}^{m}(x - a_i)\prod_{i=1}^{n}(y - b_i)\prod_{i=1}^{\ell}(xy - c_i).$$

Minimum Distance of Smallest Maximal Decompositions

It is known [1] that all smallest maximal decompositions are lattice equivalent to $Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$.



Theorem

The minimum distance of the toric code associate to Q is

$$d(C_Q) = \begin{cases} (q-1)^2 - L(Q)(q-1) + mn, & \text{when } \ell = 0 \\ (q-1)^2 - L(Q)(q-1) + \ell(m+n) & \text{when } \ell > 0 \end{cases}.$$

Acknowledgements

This research was completed at the REU Site: Mathematical Analysis and Applications at the University of Michigan-Dearborn. We would like to thank the National Science Foundation (DMS-1950102 and DMS-2243808), the National Security Agency (H98230-24), the College of Arts, Sciences, and Letters, and the Department of Mathematics and Statistics for their support.

References

[1] Ivan Soprunov and Jenya Soprunova. Toric surface codes and Minkowski length of polygons. *SIAM J. Discrete Math.*, 23(1):384–400, 2008/09.

[2] Ivan Soprunov and Jenya Soprunova. Eventual quasi-linearity of the Minkowski length. *European J. Combin.*, 58:107–117, 2016.