Toric Surface Codes and Periodicity of Polytopes

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

The University of Michigan-Dearborn

July 11, 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

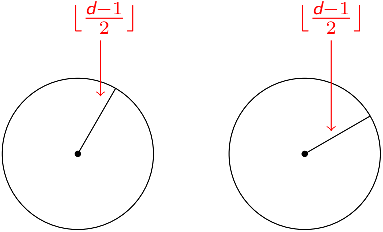
$$d_{\min} = \min\{d(\mathrm{x}, \mathrm{y}) \,|\, \mathrm{x}, \mathrm{y} \in C \text{ and } \mathrm{x} \neq \mathrm{y}\}$$

   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 $\lfloor \frac{d-1}{2} \rfloor$ 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 $P \subset \mathbb{R}^m$:

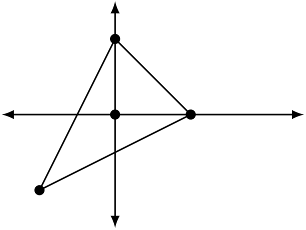
$$L_P = \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{x}^\beta \mid \beta \in P \cap \mathbb{Z}^m\}$$

and define the evaluation map

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

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 $(-1,-1)$



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

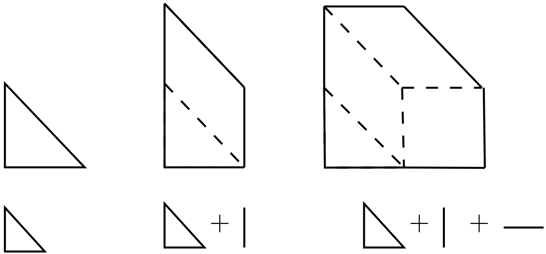
Given $P \subset \mathbb{R}^m$, we know the length and dimension of P's corresponding code.

- 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. We call the largest of these decompositions the **maximal decomposition** in P.

In [3], Soprunov and Soprunova [2009], proved bounds relating Minkowski length of polytopes to the minimum distance of the codes generated by them.

Periodicity of Polytopes

Scaling a Polytope

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

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

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

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

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

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 [4].

Period-1 Polytopes

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 [4].

So, what do period-1 polytopes look like?

Period-1 Polytopes

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 [4].

So, what do period-1 polytopes look like?

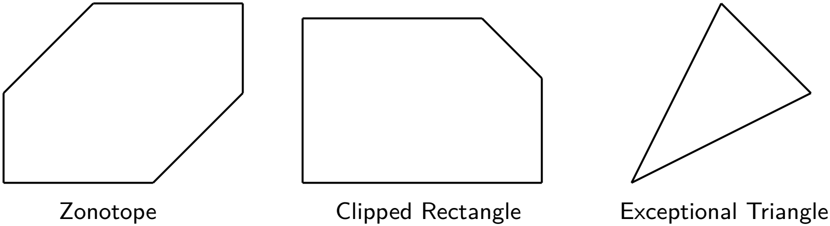


Figure: Two (2) Examples and a Non-Example

How Do We Know When a Polytope is Period-1?

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

How Do We Know When a Polytope is Period-1?

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.

How Do We Know When a Polytope is Period-1?

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.

How Do We Know When a Polytope is Period-1?

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.

Corollary (Period-1 Polytopes are Nice)

If $P \subset \mathbb{R}^2$ and P has period 1, then the exceptional triangle cannot be a summand in any of its maximal decompositions.

Connection to Toric Surface Codes

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 $q > \mathrm{Area}(P)$, we have that $r = L(P)$.

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 $q > \mathrm{Area}(P)$, 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.

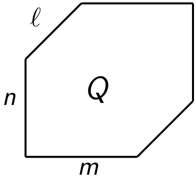
Minimum Distance of Representative Period-1 Polytopes

Minimum Distance of Smallest Maximal Decompositions

It is known [3, Proposition 3.1] that all smallest maximal decompositions are lattice equivalent to $Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$.

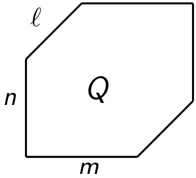
Minimum Distance of Smallest Maximal Decompositions

It is known [3, Proposition 3.1] 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 [3, Proposition 3.1] that all smallest maximal decompositions are lattice equivalent to $Q = m[0, \vec{e}_1] + n[0, \vec{e}_2] + \ell[0, \vec{e}_1 + \vec{e}_2]$.

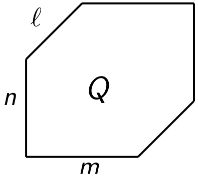


Lemma

The only maximal decomposition in Q is Q itself.

Minimum Distance of Smallest Maximal Decompositions

It is known [3, Proposition 3.1] 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.

Theorem

The minimum distance of the toric code associate to Q is

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

Little and Schwarz's Method

- In [2], Little and Schwarz use Vandermonde matrices to determine the minimum distance of simplices and boxes

  Let $P \cap \mathbb{Z}^2 = \{(a_i, b_i) : 1 \leqslant i \leqslant \#P\}$, and $S = \{(x_1, y_1), (x_2, y_2), \ldots, (x_{\#P}, y_{\#P})\}$, with $|S| = \#P$, then we have:

$$V(P;S) = \begin{pmatrix} x_1^{a_1} y_1^{b_1} & x_2^{a_1} y_2^{b_1} & x_3^{a_1} y_3^{b_1} & \cdots & x_{\#P}^{a_1} y_{\#P}^{b_1} \\ x_1^{a_2} y_1^{b_2} & x_2^{a_2} y_2^{b_2} & x_3^{a_2} y_3^{b_2} & \cdots & x_{\#P}^{a_2} y_{\#P}^{b_2} \\ x_1^{a_3} y_1^{b_3} & x_2^{a_3} y_2^{b_3} & x_3^{a_3} y_3^{b_3} & \cdots & x_{\#P}^{a_3} y_{\#P}^{b_3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{a_{\#P}} y_1^{b_{\#P}} & x_2^{a_{\#P}} y_2^{b_{\#P}} & x_3^{a_{\#P}} y_3^{b_{\#P}} & \cdots & x_{\#P}^{a_{\#P}} y_{\#P}^{b_{\#P}} \end{pmatrix}$$

Little and Schwarz's Method

[2, Proposition 1]

Let d be a positive integer and assume that in every set $T \subset (\mathbb{F}_q^*)^m$ with $|T| = (q-1)^m - d + 1$ there exists some $S \subset T$ with $|S| = \#(P)$ such that $\det V(P;S) \neq 0$. Then the minimum distance satisfies $d(C_P) \geqslant d$.

Little and Schwarz's Method

[2, Proposition 1]

Let d be a positive integer and assume that in every set $T \subset (\mathbb{F}_q^*)^m$ with $|T| = (q-1)^m - d + 1$ there exists some $S \subset T$ with $|S| = \#(P)$ such that $\det V(P;S) \neq 0$. Then the minimum distance satisfies $d(C_P) \geqslant d$.

- To get $d(C_p) \leqslant d$, we can find a polynomial with an appropriate amount of zeroes (which can be difficult).

Little and Schwarz's Method

[2, Proposition 1]

Let d be a positive integer and assume that in every set $T \subset (\mathbb{F}_q^*)^m$ with $|T| = (q-1)^m - d + 1$ there exists some $S \subset T$ with $|S| = \#(P)$ such that $\det V(P;S) \neq 0$. Then the minimum distance satisfies $d(C_P) \geqslant d$.

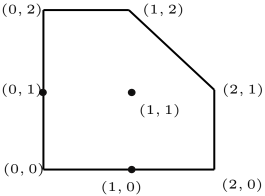
- To get $d(C_p) \leqslant d$, we can find a polynomial with an appropriate amount of zeroes (which can be difficult).

Can we replicate Little and Schwarz's methods for different, but still "simple" polytopes in $\mathbb{R}^2$?

Example

Let $P \subset \mathbb{R}^2$ be an integral, convex, period-1 polytope with 8 lattice points:
$P = \ell[0, \vec{e}_1] + \ell[0, \vec{e}_2] + \ell\Delta$ with $\ell = 1$

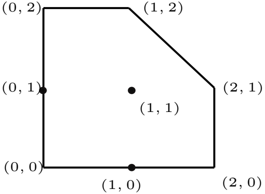
P :



Example

Let $P \subset \mathbb{R}^2$ be an integral, convex, period-1 polytope with 8 lattice points:
$P = \ell[0, \vec{e}_1] + \ell[0, \vec{e}_2] + \ell\Delta$ with $\ell = 1$

P :



Using the methods of Little and Schwarz, we showed that the following bounds hold for $q > 2\ell + 1$:

$$d(C_P) \leqslant (q-1)^2 - 3(q-1) + 2 \text{ , and } d(C_P) \geqslant (q-1)^2 - 3(q-1) + 2$$

Example

1. Consider the rectangle $R := \mathrm{conv}\{(0,0),(2,0),(0,1),(2,1)\} \subset P$. From [2, Theorem 3], the minimum distance of this rectangle is $d(C_R) = (q-1)^2 - 3(q-1) + 2$. Thus, $d(C_P) \leqslant (q-1)^2 - 3(q-1) + 2$.

Example

1. Consider the rectangle $R := \mathrm{conv}\{(0,0),(2,0),(0,1),(2,1)\} \subset P$. From [2, Theorem 3], the minimum distance of this rectangle is $d(C_R) = (q-1)^2 - 3(q-1) + 2$. Thus, $d(C_P) \leqslant (q-1)^2 - 3(q-1) + 2$.

2. Using the pigeonhole principle, we showed that for all $T \subset (\mathbb{F}_q^*)^2$ with $|T| = (q-1)^2 - d + 1$ where $d = (q-1)^2 - 3(q-1) + 2$ we can choose an $S \subset T$, with $S = \{(x_1, y_1), \ldots, (x_8, y_8)\}$, such that $x_1 = x_2 = x_3, x_4 = x_5 = x_6$, and $x_7 = x_8$.

Vandermonde Matrix

Thus, the Vandermonde matrix corresponding to P is given below:

$$V(P;S) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ x_1 & x_1 & x_1 & x_4 & x_4 & x_4 & x_7 & x_7 \\ x_1^2 & x_1^2 & x_1^2 & x_4^2 & x_4^2 & x_4^2 & x_7^2 & x_7^2 \\ y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 & y_8 \\ y_1^2 & y_2^2 & y_3^2 & y_4^2 & y_5^2 & y_6^2 & y_7^2 & y_8^2 \\ x_1y_1 & x_1y_2 & x_1y_3 & x_4y_4 & x_4y_5 & x_4y_6 & x_7y_7 & x_7y_8 \\ x_1^2y_1 & x_1^2y_2 & x_1^2y_3 & x_4^2y_4 & x_4^2y_5 & x_4^2y_6 & x_7^2y_7 & x_7^2y_8 \\ x_1y_1^2 & x_1y_2^2 & x_1y_3^2 & x_4y_4^2 & x_4y_5^2 & x_4y_6^2 & x_7y_7^2 & x_7y_8^2 \end{pmatrix}$$

Vandermonde Matrix

At the cost of changing the sign of the determinant, we can perform column operations on $V(P;S)$ to obtain the following:

$$V(P;S) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ x_1 & x_4 & x_7 & 0 & 0 & 0 & 0 & 0 \\ x_1^2 & x_4^2 & x_7^2 & 0 & 0 & 0 & 0 & 0 \\ y_1 & y_4 & y_7 & y_1 - y_2 & y_1 - y_3 & y_4 - y_5 & y_4 - y_6 & y_7 - y_8 \\ y_1^2 & y_4^2 & y_7^2 & y_1^2 - y_2^2 & y_1^2 - y_3^2 & y_4^2 - y_5^2 & y_4^2 - y_6^2 & y_7^2 - y_8^2 \\ x_1y_1 & x_4y_4 & x_7y_7 & x_1y_1 - x_1y_2 & x_1y_1 - x_1y_3 & x_4y_4 - x_4y_5 & x_7y_4 - x_2y_6 & x_3y_7 - x_7y_8 \\ x_1^2y_1 & x_4^2y_4 & x_7^2y_7 & x_1^2y_1 - x_1^2y_2 & x_1^2y_1 - x_1^2y_3 & x_4^2y_4 - x_4^2y_5 & x_4^2y_4 - x_4^2y_6 & x_7^2y_7 - x_7^2y_8 \\ x_1y_1^2 & x_4y_4^2 & x_4y_7^2 & x_1y_1^2 - x_1y_2^2 & x_1y_1^2 - x_1y_3^2 & x_4y_4^2 - x_4y_5^2 & x_4y_4^2 - x_4y_6^2 & x_7y_7^2 - x_7y_8^2 \end{pmatrix}$$

Vandermonde Matrix

At the cost of changing the sign of the determinant, we can perform column operations on $V(P;S)$ to obtain the following:

$$V(P;S) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ x_1 & x_4 & x_7 & 0 & 0 & 0 & 0 & 0 \\ x_1^2 & x_4^2 & x_7^2 & 0 & 0 & 0 & 0 & 0 \\ y_1 & y_4 & y_7 & y_1 - y_2 & y_1 - y_3 & y_4 - y_5 & y_4 - y_6 & y_7 - y_8 \\ y_1^2 & y_4^2 & y_7^2 & y_1^2 - y_2^2 & y_1^2 - y_3^2 & y_4^2 - y_5^2 & y_4^2 - y_6^2 & y_7^2 - y_8^2 \\ x_1y_1 & x_4y_4 & x_7y_7 & x_1y_1 - x_1y_2 & x_1y_1 - x_1y_3 & x_4y_4 - x_4y_5 & x_7y_4 - x_2y_6 & x_3y_7 - x_7y_8 \\ x_1^2y_1 & x_4^2y_4 & x_7^2y_7 & x_1^2y_1 - x_1^2y_2 & x_1^2y_1 - x_1^2y_3 & x_4^2y_4 - x_4^2y_5 & x_4^2y_4 - x_4^2y_6 & x_7^2y_7 - x_7^2y_8 \\ x_1y_1^2 & x_4y_4^2 & x_4y_7^2 & x_1y_1^2 - x_1y_2^2 & x_1y_1^2 - x_1y_3^2 & x_4y_4^2 - x_4y_5^2 & x_4y_4^2 - x_4y_6^2 & x_7y_7^2 - x_7y_8^2 \end{pmatrix}$$

After performing column operations, we get a lower block triangular matrix with blocks A, B, C, D whose determinant is equal to $det(A)det(D)$

Vandermonde Matrix

The lower right block, D, is a 5×5 matrix. Each column of D has a common factor $y_i - y_j$ that can be taken out at the cost of the determinant changing by some nonzero scalar.

$$D := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ x_1 & x_1 & x_2 & x_2 & x_3 \\ x_1^2 & x_1^2 & x_2^2 & x_2^2 & x_3^2 \\ y_1 + y_2 & y_1 + y_3 & y_4 + y_5 & y_4 + y_6 & y_7 + y_8 \\ x_1(y_1 + y_2) & x_1(y_1 + y_3) & x_2(y_4 + y_5) & x_2(y_4 + y_6) & x_3(y_7 + y_8) \end{pmatrix}$$

Vandermonde Matrix

This process can be repeated once more until we are left with D_2, a 2×2 standard univariate Vandermonde matrix, for which we know the determinant to be non-zero.

Vandermonde Matrix

This process can be repeated once more until we are left with D_2, a 2×2 standard univariate Vandermonde matrix, for which we know the determinant to be non-zero.

Thus, applying [2, Proposition 1], we know that $d(C_P) \geqslant d$. Finally, $d(C_P) = (q-1)^2 - 3(q-1) + 2$.

Vandermonde Matrix

This process can be repeated once more until we are left with D_2, a 2×2 standard univariate Vandermonde matrix, for which we know the determinant to be non-zero.

Thus, applying [2, Proposition 1], we know that $d(C_P) \geqslant d$. Finally, $d(C_P) = (q-1)^2 - 3(q-1) + 2$.

Using this same method, we proved that for $\ell = 2$, $d(C_P) = (q-3)(q-5)$, for $q > 5$. Similarly, for $\ell = 3$, $d(C_P) = (q-4)(q-7)$, for $q > 7$

Next Steps

1. Extend the Little and Schwarz method to prove a minimum distance formula for $P = \ell[0, e_1] + \ell[0, e_2] + \ell\Delta$ for any $\ell \in \mathbb{Z}^+$

Next Steps

1. Extend the Little and Schwarz method to prove a minimum distance formula for $P = \ell[0, e_1] + \ell[0, e_2] + \ell\Delta$ for any $\ell \in \mathbb{Z}^+$
2. Prove minimum distance formulas for "nice" polytopes which can be maximal decompositions, a classification of which already exists [3, 1]

Next Steps

1. Extend the Little and Schwarz method to prove a minimum distance formula for $P = \ell[0, e_1] + \ell[0, e_2] + \ell\Delta$ for any $\ell \in \mathbb{Z}^+$
2. Prove minimum distance formulas for “nice” polytopes which can be maximal decompositions, a classification of which already exists [3, 1]
3. Use these formulas to create a polynomial time algorithm for computing a minimum distance formula of a polytope not containing the exceptional triangle in any maximal decomposition

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] Olivia Beckwith, Matthew Grimm, Jenya Soprunova, and Bradley Weaver. Minkowski length of 3d lattice polytopes. *Discrete & Computational Geometry*, Jun 2012.

[2] John Little and Ryan Schwarz. On toric codes and multivariate Vandermonde matrices. *Appl. Algebra Engrg. Comm. Comput.*, 18(4):349–367, 2007.

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

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