BOUNDS ON CODES FROM SMOOTH TORIC THREEFOLDS WITH RANK(PIC(X)) = 2

A Dissertation

by

JAMES LEE KIMBALL

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

August 2008

Major Subject: Mathematics

BOUNDS ON CODES FROM SMOOTH TORIC THREEFOLDS

WITH RANK(PIC(X)) = 2

A Dissertation

by

JAMES LEE KIMBALL

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Henry Schenck
Committee Members,	J. Maurice Rojas
	Peter Stiller
	Andreas Klappenecker
Head of Department	Albert Boggess

August 2008

Major Subject: Mathematics

ABSTRACT

Bounds on Codes from Smooth Toric Threefolds with Rank(Pic(X)) = 2.

(August 2008)

James Lee Kimball, B.S., Louisiana College;

M.S., Texas A&M University

Chair of Advisory Committee: Dr. Henry Schenck

In 1998, J. P. Hansen introduced the construction of an error-correcting code over a finite field $\mathbb{F}_q$ from a convex integral polytope in $\mathbb{R}^2$. Given a polytope $P \subset \mathbb{R}^2$, there is an associated toric variety X_P, and Hansen used the cohomology and intersection theory of divisors on X_P to determine explicit formulas for the dimension and minimum distance of the associated toric code C_P. We begin by reviewing the basics of algebraic coding theory and toric varieties and discuss how these areas intertwine with discrete geometry. Our first results characterize certain polygons that generate and do not generate maximum distance separable (MDS) codes and Almost-MDS codes. In 2006, Little and Schenck gave formulas for the minimum distance of certain toric codes corresponding to smooth toric surfaces with rank(Pic(X)) = 2 and rank(Pic(X)) = 3. Additionally, they gave upper and lower bounds on the minimum distance of an arbitrary toric code C_P by finding a subpolygon of P with a maximal, nontrivial Minkowski sum decomposition. Following this example, we give explicit formulas for the minimum distance of toric codes associated with two families of smooth toric threefolds with rank(Pic(X)) = 2, characterized by G. Ewald and A. Schmeinck in 1993. Lastly, we give explicit formulas for the dimension of a toric code generated from a Minkowski sum of a finite number of polytopes in $\mathbb{R}^2$ and $\mathbb{R}^3$ and a lower bound for the minimum distance.

ACKNOWLEDGMENTS

Before acknowledging the individuals who have greatly contributed to the completion of this work, I must first give thanks to God. For I firmly believe that it is by His will that these extraordinary people are a part of my life.

A special thanks to my wife Emily, whose unwavering support and encouragement provided me the fortitude to complete this task. I love you.

Special thanks also goes to Hal Schenck, without whom this accomplishment would not have been possible. As an advisor and mentor, his continued advice, encouragement, and unending patience were invaluable. He truly has a heart for mathematics and a heart for students.

I would like to thank the members of my advisory committee: Peter Stiller, J. Maurice Rojas, and Andreas Klappenecker. Their continued comments and suggestions were greatly appreciated. I am also very grateful to many of the professors in the Mathematics Department at Texas A&M. In particular, N. Sivakumar, Thomas Schlumprecht, J. M. Landsberg, Frank Sottile, Dante DeBlassie, Jon Pitts, and Kirby Smith. I would like to thank our Department Head, Al Boggess, and all the auxiliary staff for their help and support over many years. I am especially grateful to Monique Stewart and Sherry Floyd.

Thanks to all my fellow graduate students and colleagues for their help and friendship. To Terry McDonald and Stefan Tohăneanu for their friendship and for providing me with the template for this dissertation. To Jeb Belcher for his continued friendship.

A special thanks also goes to my parents, and my brother and sister for their continued love, support, and encouragement.

TABLE OF CONTENTS

CHAPTER Page

LIST OF FIGURES

LIST OF TABLES

CHAPTER I

INTRODUCTION TO CODING THEORY

A. Algebraic Error-Correcting Codes

Error-correcting codes play an important role in transmitting information reliably and efficiently across communication channels. By encoding our data or message in a way that allows the decoder to recognize and correct errors, we can greatly increase the accuracy of the received message. The development of "good" coding and decoding schemes is the goal of algebraic coding theory, and is studied by computer scientists, engineers, and mathematicians. One of the key ingredients of this research is determining the minimum distance between the codewords of a code.

The basic idea is to take a message, break it into pieces of fixed length, and encode these pieces by adding redundancy or extra structure. The majority of our notation and terminology follows Chapters 9 and 10 of [1]. Let $\mathbb{F}_q$ denote a finite field with q elements. The elements of this field will comprise the alphabet for our code. Each "word" of the message will have fixed length k, and the resulting encoded word will have fixed length n. Necessarily, we have $k < n$ to ensure our redundancy requirement. Thus our encoding process is a one-to-one function $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$, and the image $E(\mathbb{F}_q^k) = C$ is called the set of *codewords*. Similarly, the decoding process is a function $D : \mathbb{F}_q^n \to \mathbb{F}_q^k$, where $D \circ E$ is the identity on $\mathbb{F}_q^k$.

A *linear block code* is one whose set of codewords C forms a linear subspace of $\mathbb{F}_q^n$. We may, therefore, view our encoding function as a linear mapping between vector spaces whose image is the subspace C. The matrix representation of E with respect to the standard basis of $\mathbb{F}_q^k$ is called the *generator matrix* G of the code C. We write

---

This dissertation follows the style of SIAM Journal on Discrete Mathematics.

G as a $k \times n$ matrix, and we encode a word via multiplication on the left. (There are two conventions for the form of the generator matrix. Some texts write G as an $n \times k$ matrix, and the code it generates is called the dual code to C, denoted $C^{\perp}$. However, we lose no information by using the former convention.) As C is a proper subspace of $\mathbb{F}_q^n$, it is beneficial to have an idea of how much our codewords are "spread out," and for this we use the Hamming distance.

Definition I.1. Let $x, y \in \mathbb{F}_q^n$. Then the *Hamming distance* between x and y is

$$d(x, y) = |\{i, 1 \leq i \leq n : x_i \neq y_i\}|.$$

That is, $d(x, y)$ counts the number of terms in which x and y differ. The *minimum distance* of a code is the value $d = \min\{d(x, y) : x \neq y \in C\}$. We denote the minimum distance of a code C by $d(C)$.

Given a fixed n and k, we refer to a linear block code with minimum distance d as an $[n, k, d]$ code. Over the finite field $\mathbb{F}_q$, this code will have q^k distinct codewords. A "good" coding scheme is one for which the *information rate* k/n is not too small and for which the minimum distance d is large. This essentially means that our set of codewords is very "spread out" inside $\mathbb{F}_q^n$ and that we did not have to add an extraordinary amount of redundancy to obtain this beneficial property. However, one should not conclude that codes of small block length are better that those with long block length. Indeed, in 1948, Claude Shannon presented his Noisy Channel Coding Theorem, which stated the existence of codes with arbitrarily small probabilities of block error if the block length is large enough [20]. Similar results have also been shown for Low-Density-Parity-Check codes and the more recently discovered turbo codes.

Example I.1. A $[7,4,3]$ code with generator matrix G.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

One can quickly compute the 16 codewords of this code and observe that the minimum distance is 3.

Since $\mathbb{F}_q^n$ is a vector space, we can define the *weight* of the word x as $d(x,0)$, where 0 is the zero vector in $\mathbb{F}_q^n$. The weight of a word is just the number of nonzero entries. Thus, for linear block codes our goal is to find the minimum weight over all codewords of C. Two important results used in approximating this minimum distance are the *Singleton bound* and the *Gilbert-Varshamov bound*. The idea behind both results is to consider a code of block length n and minimum distance d and then find a code C of maximum size that satisfies these parameters. That is, we want to maximize k for a given q.

Proposition I.1. ***(Singleton Bound)*** *Let $C \subset \mathbb{F}_q^n$ be a linear code of maximum size with block length n and minimum distance d. Then $|C| \leq q^{n-d+1}$.*

To see the Singleton bound, simply remove any fixed set of $d-1$ entries from every codeword in C. Since the minimum distance of C is d, we still have a set containing q^k unique codewords. That is, $q^k \leq q^{n-d+1}$. So, we have an upper bound on the maximum number of codeswords in C. An alternate and commonly used version of the Singleton bound immediately follows. Namely, $d \leq n-k+1$. Since we, in general, like codes with large minimum distance, this last inequality provides a very pleasing upper bound. Codes that attain this upper bound are called *maximum distance separable* (MDS) and are used extensively in practice.

Proposition I.2. ***(Gilbert-Varshamov Bound)*** *Let $C \subset \mathbb{F}_q^n$ be a linear code of maximum size with block length n and minimum distance d, and let $b = |B_{d-1}(x)|$, the number of words in the ball $B_{d-1}(x)$ centered at an arbitrary codeword $x \in \mathbb{F}_q^n$. Then $b = \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i$ and $|C|$ satisfies $b \cdot |C| \geq q^n$.*

This follows from the observation that the union $\bigcup_{x \in C} B_{d-1}(x)$ must completely cover $\mathbb{F}_q^n$. If it did not, then we could increase the size of C and maintain the same minimum distance, contradicting maximality. This is also an alternate form of the Gilbert-Varshamov (GV) bound [23]. Precisely stated, the GV bound says that for a given q and $0 \leq \delta \leq \frac{q-1}{q}$, there exists an infinite sequence of linear $[n, k, d]$ codes with $\delta \equiv d/n$ and $R \equiv k/n$ such that

$$R \geq 1 - [\delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)] \text{ for all } n.$$

Improvements to the GV bound were elusive for many years, and some researchers believed it to be the best possible bound. In fact, the class of codes known as Goppa codes was known to only theoretically contain codes that met the GV bound. Then in 1982, Tsfasman, Vladut, and Zink proved the existence of algebraic-geometric codes that exceed the GV bound if q is sufficiently large [23]. This major contribution led to the Tsfasman-Vladut-Zink (TVZ) bound for linear codes, which is better than the GV bound when $q \geq 49$ [4]. The result of Tsfasman, Vladut, and Zink, and the very good parameters associated with algebraic-geometric codes provides motivation for investigating toric codes.

Before describing algebraic-geometric codes and toric codes, we define Reed-Solomon (RS) codes. We do this because Reed-Solomon codes appear as a subclass of algebraic-geometric and toric codes, and it is helpful to understand their properties. Reed-Solomon codes are extensively used in industry and have very nice properties, such as being MDS. It is also possible to generate RS codes of a predefined minimum distance. Since there are many ways to describe Reed-Solomon codes, we will use the definition from [1] because it leads us to the observation that Reed-Solomon codes are 1-dimensional toric codes.

Definition I.2. Given a finite field $\mathbb{F}_q$, let $\alpha \in \mathbb{F}_q$ be a primitive element and $n = q-1$. Fix $k-1 < n$, and let $L_{k-1} = \{\sum_{i=0}^{k-1} a_i t^i : a_i \in \mathbb{F}_q\}$, the set of polynomials of degree at most $k-1$ over $\mathbb{F}_q$. Then the *Reed-Solomon* code is the set of codewords

$$C = \{(f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \in \mathbb{F}_q^n : f \in L_{k-1}\}.$$

A convenient way to construct a generator matrix for a Reed-Solomon code of dimension k is to take a basis $\{1, t, \ldots, t^{k-1}\}$ of L_{k-1} and then evaluate each basis element over the set of points $\mathbb{F}_q^*$. This creates k vectors of length n that generate the Reed-Solomon code. Thus, our generator matrix looks like

$$G = \begin{array}{c} \\ 1 \\ t \\ \vdots \\ t^{k-1} \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \alpha & \ldots & \alpha^{q-2} \end{array} \\ \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \alpha & \ldots & \alpha^{q-2} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{k-1} & \ldots & \alpha^{(q-2)(k-1)} \end{pmatrix} \end{array}$$

To see that Reed-Solomon codes are linear codes, observe that the above generator matrix is a submatrix of a Vandermonde matrix. So, our linear map is injective and our code is a vector subspace of $\mathbb{F}_q^n$. This generator matrix also highlights the fact that Reed-Solomon codes are closed under cyclic permutations. Codes of this nature are called *cyclic codes*. That Reed-Solomon codes are MDS follows from the fact that the polynomial $f = (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_{k-1})$, with all $\alpha_i \in \mathbb{F}_q^*$ distinct, is an element of L_{k-1} that has exactly $k-1$ zeros. Thus, the corresponding codeword will have exactly $n - k + 1$ nonzero entries. It is this connection between codewords and zero sets of polynomials that leads us to Goppa codes, also known as algebraic-geometric codes.

Goppa presented his construction of algebraic-geometric codes in [7] in 1981, and there has since been many variations. The idea is to choose a non-singular projective curve X of genus g defined over a finite field $\mathbb{F}_q$ with distinct $\mathbb{F}_q$-rational points $P_1, P_2, \ldots, P_m$. Set $D = P_1 + \ldots + P_m$, a divisor on X, and choose a divisor E with support disjoint from D. (We will formally define divisors in Chapter II). There is a finite dimensional $\mathbb{F}_q$-vector space of rational functions associated with E, denoted $L(E)$. The algebraic-geometric code associated with E will have dimension $\dim(L(E))$ and is the image of the evaluation map

$$\begin{aligned} ev : L(E) &\longrightarrow \mathbb{F}_q^m \\ f &\longmapsto (f(P_1), \ldots, f(P_m)) \end{aligned}$$

While this construction seems to introduce unnecessary complexity, the Riemann-Roch Theorem makes the determination of the code parameters very accessible. Notice that the points P_i do not all necessarily lie in $(\mathbb{F}_q^*)^2$. So, this construction is not identical to the previous one. However, we can still generate a Reed-Solomon code.

Example I.2. [6, Exercise 4.2] Given affine coordinates X, Y, and Z, consider the projective curve $Y = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_{11}$. Then $D = (0 : 0 : 1) + (1 : 0 : 1) + (2 : 0 : 1) + \ldots + (9 : 0 : 1)$ is a divisor on our curve and $E = 7(1 : 0 : 0)$ is a divisor with support disjoint from D. So our code has block length 10. A consequence of the Riemann-Roch Theorem is $\dim(L(E)) = \deg(E) - g + 1$ when $\deg(E) > 2g - 2$. Since the genus g of our curve is 0, the dimension of $L(E)$ is 8. It can be shown that $d \geq n - k + 1 - g$, provided $\deg(E) < n$. Thus, $d \geq 3$ and, by the Singleton Bound,

$d \leq 10 - 8 + 1 = 3$. So, we have a $[10, 8, 3]$ Reed-Solomon Code.

B. Codes from Integral Convex Polytopes

In 1998, J. P. Hansen introduced the notion of constructing error-correcting codes from integral convex polygons associated with certain toric surfaces [9]. These codes not only use the cohomology and intersection theory of surfaces to determine parameters, but also the geometry of integral convex polygons. In this section, we present the code construction and postpone the connection with toric surfaces until Chapter III. Begin by fixing an integral convex polytope $P \subset \mathbb{R}^m$, $m \geq 1$, and a finite field $\mathbb{F}_q$ such that, up to translation, P is properly contained in $[0, q-1]^m$. By evaluating monomials with integer exponents from $P \cap \mathbb{Z}^m$ at every point of $(\mathbb{F}_q^*)^m$, we obtain $\#(P \cap \mathbb{Z}^m)$ linearly independent vectors of length $n = (q-1)^m$ that generate the corresponding toric code.

Definition I.3. Let $P \subset \mathbb{R}^m$, be an integral convex polytope with $P \subset [0, q-1]^m$, and let $\mathbb{F}_q$ be a finite field. Let $\chi^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$ denote monomials with exponents $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in (P \cap \mathbb{Z}^m)$. Then form the codewords

$$\{ (\, \chi^{\mathbf{a}}(\xi_1), \chi^{\mathbf{a}}(\xi_2), \ldots, \chi^{\mathbf{a}}(\xi_n)\,) : \mathbf{a} \in (P \cap \mathbb{Z}^2) \;\text{ and }\; \xi_i \in (\mathbb{F}_q^*)^m \;\},$$

where $n = (q-1)^m$. This set of codewords is linearly independent and generates a linear block code of block length n and dimension $\#(P \cap \mathbb{Z}^m)$. We denote this code as C_P.

Example I.3. Let $\alpha \in \mathbb{F}_4$ be a primitive element. Then the integral convex polygon in Figure 1 corresponds to the generator matrix G. The monomials associated with the lattice points are $\{1, xy, x^2y, xy^2\}$ and evaluating these over all points in $(\mathbb{F}_4^*)^2$ yields the rows of G. This is a [9,4,3] linear code.

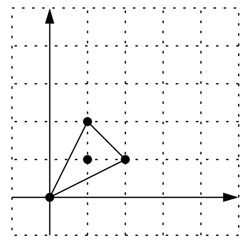


Fig. 1. Integral convex polygon.

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & 1 & \alpha^2 & 1 & \alpha \\ 1 & \alpha & \alpha^2 & \alpha^2 & 1 & \alpha & \alpha & \alpha^2 & 1 \\ 1 & \alpha^2 & \alpha & \alpha & 1 & \alpha^2 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

One easily sees that Reed-Solomon codes of dimension k are toric codes defined by integral line segments with k lattice points. Codes defined by 2-dimensional polytopes are called toric surface codes because of the connection between convex integral polygons and toric surfaces.

CHAPTER II

INTRODUCTION TO TORIC VARIETIES

A. Toric Varieties from Polyhedral Cones

Toric varieties are very rich and interesting objects that highlight links between discrete geometry and algebraic geometry. The notation here follows that of Fulton [5]. Although our setting is primarily a finite field with q elements, we will introduce these varieties over the field $\mathbb{C}$ and later restrict to the finite field $\mathbb{F}_q$. The word "toric" refers to the *m-dimensional algebraic torus.*

Definition II.1. The set of points $(\mathbb{C}^*)^m := (\mathbb{C} \setminus \{\mathbf{0}\})^m$ is called the *complex m-dimensional algebraic torus.* If $\mathbb{F}$ is any field, then $(\mathbb{F}^*)^m$ is just the *m-dimensional algebraic torus.* We will refer to this set as, simply, the algebraic torus.

Definition II.2. A *toric variety* is a normal variety X that contains the algebraic torus $(\mathbb{C}^*)^m$ as a Zariski open subset, and for which the action of $(\mathbb{C}^*)^m$ on itself extends to an action on X.

Begin with an integer lattice $N \simeq \mathbb{Z}^m$, for some $m \geq 1$. A *strongly convex polyhedral cone* σ inside the vector space $N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R}$ is a cone which has its apex at the origin, is generated by a finite number of vectors in the lattice, and does not contain a line through the origin. We will hereafter simply refer to these as *cones.* The dimension of a cone σ, denoted $\dim(\sigma)$, is the dimension of the linear space spanned by σ. A *face* τ of σ is the intersection of σ with any supporting hyperplane and can be of dimension zero through $\dim(\sigma) - 1$. Faces of codimension 1 are called *facets.* A cone σ is called a *simplex cone* if its defining vectors are linearly independent. If every proper face of σ is a simplex cone, then σ is called *simplicial.* We generally denote the facets of a cone by τ_i. We denote the vector in N defined by the first integral point of τ_i by $v(\tau_i)$, or just v_i when the context is clear.

Example II.1. Consider the 3-dimensional cone σ in Figure 2. Then $\dim(\sigma) = 3$. The origin is a zero dimensional face, and the one dimensional faces are τ_1, τ_2, τ_3, and τ_4. The facets are the subspaces determined by $\langle\tau_1, \tau_2\rangle$, $\langle\tau_2, \tau_3\rangle$, $\langle\tau_3, \tau_4\rangle$, and $\langle\tau_4, \tau_1\rangle$.

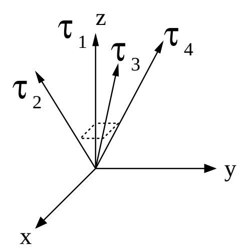


Fig. 2. Three dimensional polyhedral cone.

Let $M = \mathrm{Hom}(N, \mathbb{Z})$ be the dual lattice of N with dual pairing $\langle\ ,\ \rangle : M \times N \to \mathbb{Z}$ defined by $\langle u, v\rangle \mapsto u(v)$. Similarly, we have the vector space $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$ dual to $N_{\mathbb{R}}$ with dual pairing $\langle\ ,\ \rangle : M_{\mathbb{R}} \times N_{\mathbb{R}} \to \mathbb{Z}$ defined by $\langle u, v\rangle \mapsto u(v)$. Thus, given a cone σ, we define its dual cone as $\sigma^\vee = \{u \in M_{\mathbb{R}} : \langle u, v\rangle \geq 0,\ \forall\ v \in \sigma\}$. Inside the dual lattice, this defines a finitely generated commutative semigroup

$$S_\sigma = \sigma^\vee \cap M = \{u \in M : \langle u, v\rangle \geq 0, \forall\ \ v \in \sigma\}.$$

This semigroup has an associated $\mathbb{C}$-algebra, denote $\mathbb{C}[S_\sigma]$, that is also finitely generated and commutative, with generators denoted by χ^u. Thus, it is convenient to consider the elements of this $\mathbb{C}$-algebra as Laurent polynomials in $\mathbb{C}[S_\sigma]$. Setting $U_\sigma = \mathrm{Spec}(\mathbb{C}[S_\sigma])$, we obtain the affine toric variety corresponding to σ. For the following examples, $\mathbf{e}_1, \ldots, \mathbf{e}_m$ represent the basis vectors for $N_{\mathbb{R}}$, and $\mathbf{e}_1^*, \ldots, \mathbf{e}_m^*$ represent the basis vectors for $M_{\mathbb{R}}$. Thus, we may represent the generators of $\mathbb{C}[M_{\mathbb{R}}]$ by $\chi^{\alpha_1\mathbf{e}_1^*+\cdots+\alpha_m\mathbf{e}_m^*} = x_1^{\alpha_1}\cdots x_m^{\alpha_m}$.

Example II.2. Let $m = 2$ and consider the cone σ generated by $\mathbf{e}_2$ and $2\mathbf{e}_1 - \mathbf{e}_2$ and its dual $\sigma^\vee$ in Figure 3.

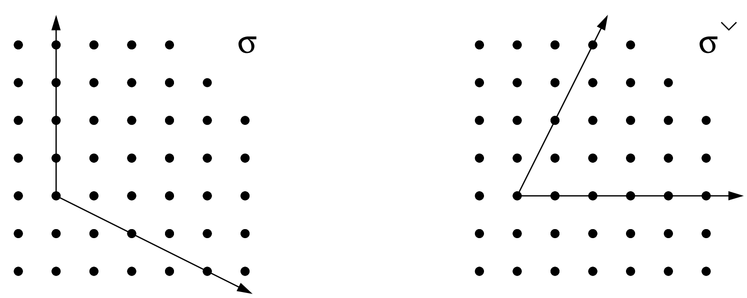


Fig. 3. Polyhedral cone and dual cone corresponding to the quadric cone.

The generators for the dual cone semigroup are $\mathbf{e}_1^*$, $\mathbf{e}_1^* + \mathbf{e}_2^*$, and $\mathbf{e}_1^* + 2\mathbf{e}_2^*$. Thus, $\mathbb{C}[S_\sigma] = \mathbb{C}[x_1, x_1x_2, x_1x_2^2] = \mathbb{C}[X,Y,Z]/\langle Y^2 - XZ\rangle$, and the affine toric variety U_σ is the quadric cone.

Since each face of a cone is also a cone, it is important note the relation between the corresponding semigroups, $\mathbb{C}$-algebras, and affine varieties. If τ is a face of σ, then $S_\sigma \subset S_\tau$, and $\mathbb{C}[S_\sigma]$ is a subalgebra of $\mathbb{C}[S_\tau]$. Consequently, U_τ embeds into U_σ as a principal open subset [5, p. 18]. In particular, every toric variety contains the algebraic torus $(\mathbb{C}^*)^m$ as an open subset since the origin $\{0\}$ corresponds to

$$U_{\{0\}} = \mathrm{Spec}(\mathbb{C}[x_1, x_1^{-1}, \ldots, x_m, x_m^{-1}])$$

This property leads us to the construction of a toric variety from a *fan.* A *fan* Δ is a collection of cones in $N_{\mathbb{R}}$ such that every face of a cone in Δ is also a cone and the intersection to two cones in Δ is a face common to both. Thus, we obtain the toric variety associated with a fan Δ, denoted X_Δ, by gluing together the affine toric varieties U_σ for each m-dimensional cone σ of Δ. If the union of all cones σ in a fan generate the entire space $N_{\mathbb{R}}$, then we call the fan (and its associated toric variety) *complete*.

Example II.3. Let $m = 2$ and consider the fan and dual cones in Figure 4.

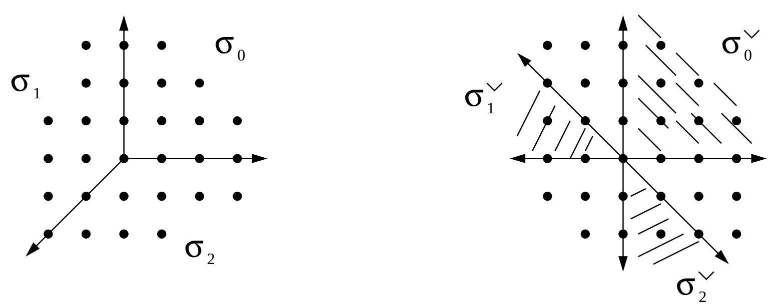


Fig. 4. Fan and dual cones corresponding to $\mathbb{P}^2$.

$$U_{\sigma_0} = \mathrm{Spec}(\mathbb{C}[x, y]), \quad U_{\sigma_1} = \mathrm{Spec}(\mathbb{C}[x^{-1}, x^{-1}y]), \quad U_{\sigma_2} = \mathrm{Spec}(\mathbb{C}[y^{-1}, xy^{-1}]).$$

Each of these affine varieties is isomorphic to $\mathbb{C}^2$ and gluing them together in the usual way yields the projective plane $\mathbb{P}^2$.

Notice that Example II.2 is singular and that Example II.3 is smooth. In general, we can use the following proposition to determine whether a given cone generates a singular or nonsingular affine toric variety.

Proposition II.1. *[5, p. 29] An affine toric variety U_σ is nonsingular (or smooth) if and only if σ is generated by part of a basis for the lattice N.*

A cone with the above property is often called *regular*. By this, we see that Example II.2 is singular since the vector $\mathbf{e}_1$ is not in the span of the facets of σ. Thus, a toric variety defined by a fan Δ is nonsingular if every cone $\sigma \in \Delta$ is generated by a subset of a basis for N. However, toric varieties with singularities are not completely troublesome. If we have a singular toric variety defined by Δ, then we may resolve the singularity by considering a *refinement* of Δ. A fan Δ' is a refinement of Δ if every cone of Δ is a union of cones in Δ'. So, given a singular U_σ, we refine σ by adding vectors that are not contained in the span of the facets of σ. This will subdivide σ into a finite number of cones whose interiors are generated by their facets. More importantly, the morphism between the associated toric varieties is birational and proper [5, p. 45].

B. Divisors on Toric Varieties

In general, we can define a divisor on a variety in more than one way, depending on the nature of our variety. However, for complete, nonsingular toric varieties, these notions will coincide in a very nice way. For a more thorough treatment on divisors, see [12, Section II.6] and [21, Section III.1].

Definition II.3. Let X be a variety and $V_1, \ldots, V_r$ be irreducible closed subvarieties of codimension one; ie. *prime divisors.* Then a finite formal sum of the form $D = \sum_{i=1}^{r} a_i V_i$ with $a_i \in \mathbb{Z}$ is called a *(Weil) divisor.* If $a_i \geq 0$ for $i = 1, \ldots, r$, then D is called *effective* and denoted by $D \geq 0$.

Given a nonzero rational function f on a normal variety X, we have the notion of the divisor of f, denoted $\mathrm{div}(f)$. Namely,

$$\mathrm{div}(f) = \sum_{i=1}^{r} v_{V_i}(f) V_i,$$

where the V_i are prime divisors of X and $v_{V_i}(f)$ is the order of vanishing of f over V_i. For $v_{V_i}(f) > 0$ (or $v_{V_i}(f) < 0$), we say f has a *zero* (or *pole*) along V_i. Thus, for

$\mathrm{div}(f) = \sum a_i V_i$, we can write

$$\mathrm{div}_0(f) = \sum_{a_i > 0} a_i V_i \qquad \text{and} \qquad \mathrm{div}_\infty(f) = \sum_{a_i < 0} a_i V_i,$$

for the *divisors of zeros* and *divisors of poles* of f, respectively. Divisors of the form $D = \mathrm{div}(f)$ are called *principal divisors* and, under addition, form a group, denoted $\mathrm{Div}_P(X)$. Two divisors D and D' are called *linearly equivalent* if $D - D'$ is principal. Given an open cover and a compatible system of functions on X, we can, additionally, define a *Cartier divisor*.

Definition II.4. For a variety X, a *Cartier divisor* is given by an open cover $\{U_i\}$ of X and a corresponding system of nonzero rational functions $\{f_i\}$, such that (1) the f_i are not identically zero and (2) f_i/f_j and f_j/f_i are regular on $U_i \cap U_j$. This is also called a *locally principal divisor*.

Essentially, a divisor D is a Cartier divisor if at every point $x \in X$, there exists a Zariski open subset $U \subset X$ such that $x \in U$ and D is principal on U [2, p. 264]. The Cartier divisors also form a group under addition, denoted $\mathrm{Div}_C X$, and it follows from the definitions that $\mathrm{Div}_P(X)$ is a subgroup of $\mathrm{Div}_C(X)$. The quotient group $\mathrm{Div}_C(X) \setminus \mathrm{Div}_P(X)$ is called the *Picard group* and is denoted $\mathrm{Pic}(X)$.

Since toric varieties come equipped with an action by the algebraic torus, we are interested in divisors that are unchanged by this mapping. Such objects are called *T-invariant*. From [5], we learn that T-invariant, irreducible, codimension one subvarieties of X_Δ correspond directly with the 1-dimensional rays $\tau_1, \tau_2, \ldots, \tau_r \subset \Delta(1)$ with a given ordering. The corresponding divisors are defined as the *orbit closures* $D_i = V(\tau_i)$ [5, Section 3.1]. Thus, T-invariant Weil divisors are of the form $\sum a_i D_i$, $a_i \in \mathbb{Z}$. We also learn that a T-invariant Cartier divisor on an affine open set U_σ has the form $\mathrm{div}(\chi^u)$ for some unique $u \in M$. If our defining fan Δ is regular (equivalently, X_Δ is smooth), then a T-invariant Weil divisor D is also a T-invariant Cartier divisor and $\mathrm{Pic}(X) \simeq \mathbb{Z}^{r-m}$ [5, p. 65]. We denote the group of T-invariant Cartier divisors as $\mathrm{Div}_C^T(X)$.

Now we make the connection between divisors and sheaves. Roughly speaking, a sheaf allows us to systematically keep track of and "glue together" algebraic objects related to the open subsets of a topological space. Given a topological space X, a *presheaf* $\mathcal{F}$ is a collection of open subsets $U \subseteq X$, algebraic objects $\mathcal{F}(U)$ (vector spaces, Abelian groups, rings, etc.), and mappings $U \to \mathcal{F}(U)$, such that for every inclusion $U \subseteq V$ of open sets, there is a morphism $\rho_{VU} : \mathcal{F}(V) \to \mathcal{F}(U)$. These morphisms must also satisfy (i) $\mathcal{F}(\varnothing) = 0$, (ii) $\rho_{UU} = id_{\mathcal{F}(U)}$, and (iii) if $U \subseteq V \subseteq W$ as open sets, then $\rho_{WV} = \rho_{VU} \circ \rho_{WV}$.

Definition II.5. Let $\mathcal{F}$ be a presheaf on a X. Then $\mathcal{F}$ is a *sheaf* on X if it satisfies the following for any open set $U \subseteq X$ with $\{V_i\}$ an open cover of U:

1. if $s \in \mathcal{F}(U)$ and $s|_{V_i} = 0$ for all i, then $s = 0$ in $\mathcal{F}(U)$;
2. if $s_i \in \mathcal{F}(V_i)$ and $s_j \in \mathcal{F}(V_j)$ and $s_i|_{V_i \cap V_j} = s_j|_{V_i \cap V_j}$, then there exists $s \in \mathcal{F}(V_i \cup V_j)$ such that $s|_{V_i} = s_i$ and $s|_{V_j} = s_j$.

As the definition of a Cartier divisor implies, we are concerned with the rational functions on the open sets of our toric variety. For every open subset U on a toric variety X_Δ, denote the ring of regular functions on U as $\mathcal{O}(U)$. Taken over all open subsets, we can form a *sheaf of rational functions* of X_Δ, denoted $\mathcal{O}_{X_\Delta}$. When the variety we are working over is clear, we will denote this sheaf simply as $\mathcal{O}$. Since we can assign an $\mathcal{O}$-module of rational functions to the affine pieces of X_Δ, toric varieties come equipped with a sheaf of $\mathcal{O}_{X_\Delta}$-modules.

Additionally, each Cartier divisor D on X_Δ determines a sheaf by

$$\mathcal{O}_{X_\Delta}(D)(U) = \{f \in K(X_\Delta) \mid \operatorname{div}(f) + D \geq 0 \text{ on } U \subseteq X_\Delta \},$$

where $K(X_\Delta)$ denotes the quotient field of X_Δ. We denote this sheaf by $\mathcal{O}(D)$. For each open subset $U \subset X_\Delta$, it can be shown that $\mathcal{O}(D)(U)$ is isomorphic to $\mathcal{O}_{X_\Delta}(U)$ [2, p. 268]. That is, $\mathcal{O}(D)$ is *invertible* and, hence, also called a line bundle.

Definition II.6. Let $U \subset X_\Delta$ be an open subset, and let $\mathcal{O}_{X_\Delta}$ be a sheaf of $\mathcal{O}$-modules on X_Δ. Then $f \in \mathcal{O}(U)$ is called a *section* of $\mathcal{O}_{X_\Delta}$. If $f \in \mathcal{O}_{X_\Delta}$, then f is called a *global section*.

We are particularly interest in when $\mathcal{O}(D)$ is generated by its global sections. That is, there exists global sections of $\mathcal{O}(D)$ such that at every point of X at least one is nonzero. In [5, Section 3.4], Fulton shows that $\mathcal{O}(D)$ is generated by global sections when a particular piecewise linear function defined on the support of Δ is convex. However, this condition is satisfied when our toric variety is defined from a polytope. While we do this construction formally in the next section, we can still state the following lemma.

Lemma II.1. *[5, p. 66] Let $D = \sum a_i D_i$ be a T-invariant Cartier divisor on X_Δ, and let v_i denote the primitive element of the cone $\tau_i \in \Delta(1)$ associated with D_i. Define a rational convex polyhedron by*

$$P_D = \{u \in M_\mathbb{R} \mid \ < u, v_i > \geq -a_i \ \textit{for all } \ i \}.$$

Then the global sections of $\mathcal{O}(D)$ are linear combinations of χ^u as u varies over $P_D \cap M$. If the cones in Δ span $N_\mathbb{R}$ as a cone, then the space of global sections is finite dimensional. That is, P_D is a rational convex polytope.

Given a T-invariant Cartier divisor D on X_Δ, we will hereafter denote the space of global sections by the zeroth cohomology group $\mathrm{H}^0(X_\Delta, \mathcal{O}(D))$. This is because we can define a Čech cohomology on an open cover of X_Δ such that the elements of H^0 are the globally defined sections [18, p. 130].

C. Toric Varieties from Polytopes

Recall that the toric codes we wish to study are generated by m-dimensional polytopes. As Lemma II.1 suggests, these polytopes contain all the necessary information to describe the toric varieties described above. Formally, a *rational convex polytope* P in $M_\mathbb{R}$ is the convex hull of a finite set of points in M. (Anytime we refer to a polytope in this or subsequent sections, it is understood that the polytope is integral and convex.) If H is any supporting hyperplane of P, then we call $F = P \cap H$ a *face* of P. Similar to cones, if P is m-dimensional, then faces of dimension $m-1$ are called *facets*. In addition to being the convex hull of a finite set of points, we may also describe P as the intersection of a finite number of halfspaces in $M_\mathbb{R}$. Namely, for each facet F of P, there exists a primitive inward normal vector $v_F \in N$ and an integer d_F such that

$$P = \bigcap_{\text{F a facet of } P} \{u \in M : \langle u, v_F \rangle \geq -d_F\}.$$

The one dimensional cones τ_F generated by the vectors v_F join together at the origin of N to create the fan associated with P, denoted Δ_P. Thus, there is a toric variety X_{Δ_P}, denoted X_P, associated to P that is complete when P is nontrivial.

Example II.4. Let P be the rectangle defined by $conv\{(0,0),(2,0),(0,3),(2,3)\}$. Then the facets of P are the four edges, the primitive inward normals are $v_1 = \mathbf{e}_1,\ v_2 = \mathbf{e}_2,\ v_3 = -\mathbf{e}_1,\ v_4 = -\mathbf{e}_2$, and the integers are $d_1 = 0,\ d_2 = 0,\ d_3 = 2,\ d_4 = 3$. Thus,

$$P = \{(x,y) \in \mathbb{R}^2 \mid x \geq 0,\ y \geq 0,\ x \leq 2,\ y \leq 3\}.$$

The τ_i generated by the v_i join together to form the fan corresponding to the complete and nonsingular toric variety $\mathbb{P}^1 \times \mathbb{P}^1$.

Notice that the polytope P corresponding to the above toric variety is not unique. We could have also used the rectangle $conv\{(0,0),(17,0),(0,1),(17,1)\}$; however, the d_i would change accordingly. Recall from the previous section that the facets of our defining fan Δ correspond to T-invariant divisors on the toric variety X_Δ. Specifically, we defined the divisors D_i as the orbit closures $V(\tau_i)$ of the 1-dimensional cones τ_i. Thus, given a polytope P with inward normals $v_1, \ldots, v_s$ and integers $d_1, \ldots, d_s$, we have a complete fan Δ_P defining a toric variety X_P and a divisor $D_P = d_1 D_1 + \cdots + d_s D_s$ on X_P corresponding to P. So, the divisor corresponding to the polygon in Example II.4 is $2D_3 + 3D_4$. It is not difficult to see that increasing or decreasing a particular d_i will translate the associated hyperplane away from or toward the origin.

Example II.5. Consider the polytopes $P_1 = conv\{(0,0),(1,0),(0,1)\}$ and $P_a = conv\{(0,0),(a,0),(0,a)\}$, $a \geq 1$. The inward normals for both P_1 and P_a generate one dimensional cones that define the fan of Example II.3. That is, $X_{P_1} = X_{P_a} = \mathbb{P}^2$. However, letting the divisors D_1, D_2, and D_3 correspond to the rays generated by $\mathbf{e}_1$, $\mathbf{e}_2$, and $-\mathbf{e}_1 - \mathbf{e}_2$, respectively, we have that $D_{P_1} = D_3$ and $D_{P_2} = aD_3$.

Returning to the issue of when a line bundle is generated by global sections, we now have the necessary convex function. That is, given a nontrivial polytope P, we have a complete toric variety X_P and a T-invariant Cartier divisor D_P such that the function

$$\psi_D(v) = \min_{u \in P} \langle u, v \rangle = \min_{u \in P \cap M} \langle u, v \rangle = \min \langle u_i, v \rangle,$$

where the u_i are the vertices of P, is convex [5, p. 72]. Thus, $\mathcal{O}(D_P)$ is generated by global sections and $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ is finite dimensional with generators $\{\chi^u | u \in$

$P \cap M\}$.

While Δ_P will be complete when P is nontrivial, the corresponding toric variety X_P may be singular. However, we may remove singularities by refining Δ_P as described in the previous section to obtain Δ'_P . Consequently, we obtain a divisor D_P that lies on a complete and nonsingular toric variety.

Example II.6. Take the polytope $T_d = conv\{(0,0),(d,d),(0,2d)\}$, and the associated refined fan Δ'_{T_d} in Figure 5.

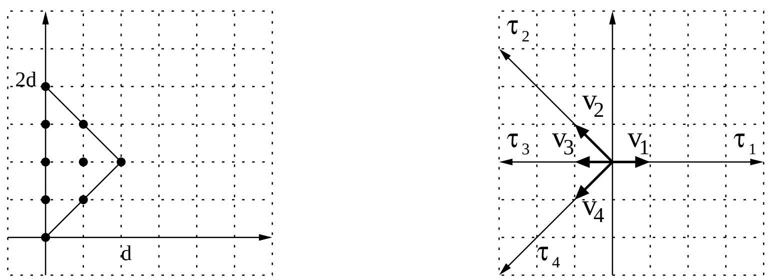


Fig. 5. Polygon T_d and corresponding refined normal fan Δ'_{T_d}.

The 1-dimensional cones τ_1, τ_2, and τ_4 correspond to the inward normals of T_d. Although these define a complete fan, we must add τ_3 to make it nonsingular. Thus, $D_{T_d} = dD_3 + 2dD_4$.

Finally, we are able to state the key to our construction of toric codes from rational convex polytopes.

Lemma II.2. *[16, Lemma 2.1] Let X_P be the toric variety associated to a rational convex polytope P , and let $\mathcal{O}(D_P)$ be the line bundle on X_P associated with D_P, the divisor corresponding to P. Then the set $H^0(X_P, \mathcal{O}(D_P))$ of global sections of $\mathcal{O}(D_P)$ is a finite dimensional vector space with $\{\chi^u : u \in P \cap M\}$ as a basis.*

Using this, we can define a set of codewords C_P of block length $n = (q-1)^m$ as the image of the evaluation map

$$ev : \mathrm{H}^0(X_P, \mathcal{O}(D_P)) \to (\mathbb{F}_q)^n$$
$$f \mapsto (\ f(\xi_1)\ , \ldots ,\ f(\xi_n)\ ), \quad \xi_i \in (\mathbb{F}_q^*)^m$$

The set of codewords generated by $\{\chi^u : u \in P \cap M\}$ forms a basis for the code C_P provided the evaluation map ev is injective. The criteria for injectivity is to require that, up to translation, P be properly contained in $[0, q-1]^m$ [16, Lemma 3.2].

D. Intersection Numbers and Mixed Volume

The interpretation of the codewords of a toric code C_P as the evaluation of sections of a line bundle leads us to a brief discussion of intersection numbers of divisors. In general, if we are given a finite number of hypersurfaces that intersect at a finite number of points, we would like to count these points with multiplicity. For curves on a surface, the notion of an intersection number is the natural one; however, the proof is nontrivial and follows from a "moving lemma" and Bertini's Theorem. Simply stated, given curves C and D on a surface X, their intersection number $C.D$ is

$$C.D = \sum_{p \in C \cap D} (C.D)_p,$$

where $(C.D)_p$ is the intersection multiplicity at the point p.

For a complete, nonsingular m-dimensional toric variety X_Δ, the intersection number of the divisors relates very nicely to the defining fan Δ. Before giving the definition, we make the following observations. Let X_Δ be a complete, nonsingular m-dimensional toric variety. Let $\tau_1, \tau_1, \ldots, \tau_m \in \Delta(1)$ be one dimensional cones of Δ with corresponding divisors $D_1, D_2, \ldots, D_m$. If the span $\sigma = \tau_1 + \cdots + \tau_m$ is an

m-dimensional cone of Δ, then the D_i correspond to the closures of the coordinate hyperplanes of the subvariety defined by $\sigma^\vee$. Thus, their intersection number is 1. If $\dim(\sigma)$ is less than m, the D_i have empty intersection, and their intersection number is 0 [2, p. 290]. For complete smooth toric surfaces, this translates into $D_i.D_j$ equalling 1 or 0 when $i \neq j$ and τ_i and τ_j are adjacent or not adjacent, respectively. When $i = j$, there is a convenient formula for calculating this self-intersection [2, p. 291].

Definition II.7. [2, p. 291] Let X_Δ be a complete, nonsingular m-dimensional toric variety. Then *intersection number* is a mapping

$$\mathrm{Div}_C^T \times \cdots \times \mathrm{Div}_C^T \ \rightarrow\ \mathbb{Z}$$

$$D_1.D_2.\cdots.D_m \mapsto a$$

such that the following are satisfied:

1. $(D_1.\cdots.D_m) = (D_{\pi(1)}.\cdots.D_{\pi(m)})$ for any permutation π of $1, \ldots, m$.
2. $(D_1 + D_1'.D_2.\cdots.D_m) = (D_1.\cdots.D_m) + (D_1'.\cdots.D_m)$.
3. $(D_1.\cdots.D_m) = (D_1'.\cdots.D_m)$, if D_1 and D_1' are linearly equivalent.
4. For $\tau_1, \ldots, \tau_m \in \Delta(1)$,

$$(D_{\tau_1}.\cdots.D_{\tau_m}) = \begin{cases} 1 & \text{if } \tau_1 + \ldots + \tau_m \in \Delta(n) \\ 0 & \text{if } \tau_1 + \ldots + \tau_m \notin \Delta(n) \end{cases}$$

When our toric variety X_P is generated from a polytope P, we have an additional connection between the intersection number of the global sections of T-invariant divisors and the geometry of P. Recall from Lemma II.1 that T-invariant Cartier divisors on X_P will correspond to bounded integral convex polytopes. Then we may interpret the intersection number of divisors as the mixed volume of their associated polytopes (with some dimension considerations).

Definition II.8. Let P and Q be polytopes in $\mathbb{R}^n$. The Minkowski sum of P and Q is

$$P + Q = \{x + y : x \in P \text{ and } y \in Q\}.$$

Example II.7. The Minkowski sum of $P = conv\{(1,0),(0,1),(2,2)\}$ and $Q = conv\{(0,0),(0,2),(2,2)\}$; see Figure 6.

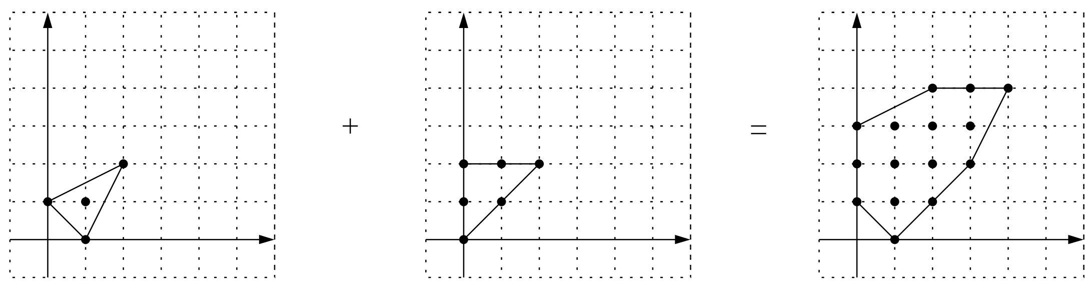


Fig. 6. Minkowski sum of polygons.

Notice that the inward normal fan Δ_{P+Q} is a refinement of both Δ_P and Δ_Q. So, there are divisors D_P, D_Q, and D_{P+Q} on X_{P+Q} that correspond to P, Q, and $P+Q$, respectively. Let $\mathcal{O}(D_P)$, $\mathcal{O}(D_P)$, and $\mathcal{O}(D_{P+Q})$ be line bundles corresponding to P, Q, and $P+Q$, respectively. In [5, p. 69], we learn in an exercise that, since $\mathcal{O}(D_P)$ and $\mathcal{O}(D_Q)$ are generated by global sections, the divisor $D_P + D_Q$ corresponds exactly to the Minkowski sum $P+Q$. That is, $D_P + D_Q = D_{P+Q}$. Consequently, we obtain the equality

$$H^0(X_{P+Q}, \mathcal{O}(D_P)) \otimes H^0(X_{P+Q}, \mathcal{O}(D_Q)) = H^0(X_{P+Q}, \mathcal{O}(D_P + D_Q)).$$

So, given sections $s_1 \in H^0(X_{P+Q}, \mathcal{O}(D_P))$ and $s_2 \in H^0(X_{P+Q}, \mathcal{O}(D_Q))$, we have that

$$s_1 s_2 \in H^0(X_{P+Q}, \mathcal{O}(D_P)) \otimes H^0(X_{P+Q}, \mathcal{O}(D_Q)) = H^0(X_{P+Q}, \mathcal{O}(D_P + D_Q)).$$

Thus, knowing the zero sets of sections in $H^0(X_{P+Q}, \mathcal{O}(D_P))$ and $H^0(X_{P+Q}, \mathcal{O}(D_Q))$ means we know the zero sets of *certain* sections in $H^0(X_{P+Q}, \mathcal{O}(D_P + D_Q))$. (Remember $H^0(X_{P+Q}, \mathcal{O}(D_P + D_Q))$ will also contain sections that are not of the form $s_1 s_2$.)

Suppose we have polytopes $P_1, \ldots, P_m$ and integers $k_1, \ldots, k_m \in \mathbb{Z}$. By a theorem of Minkowski, we know that the m-dimensional volume of the Minkowski sum $k_1 P_1 + \cdots + k_m P_m$ is a homogeneous polynomial of degree m in the variables $k_1, \ldots, k_m$. We denote this polynomial by $\mathrm{Vol}_m(k_1 P_1 + \cdots + k_m P_m)$.

Definition II.9. The *mixed volume* of the polytopes $P_1, \ldots, P_m$ is the coefficient of the $k_1 \cdot k_2 \cdot \ldots \cdot k_m$ term in the polynomial $\mathrm{Vol}_m(k_1 P_1 + \cdots + k_m P_m)$. We denote this value by $MV_m(P_1, P_2, \ldots, P_m)$.

Using the above correlation between divisors and polytopes, we have the following proposition, whose details are given in [5, Section 5.4].

Proposition II.2. *Let Δ be the refined normal m-dimensional fan of the Minkowski sum $P_1 + P_2 + \cdots + P_m$. Let X be the corresponding smooth toric variety with divisors D_i corresponding to P_i. Then*

1. *$Vol_m(P_1 + \cdots + P_m) = \frac{1}{m!}(D_1 + \cdots + D_m)^m$, and*
2. *$MV_m(P_1, \ldots, P_m) = \frac{1}{m!}(D_1.D_2.\cdots.D_m)$.*

We may also express the mixed volume of m polytopes by the alternating sum

$$m! MV_m(P_1, \ldots, P_m) = \sum_{i=1}^{m} (-1)^{m-j} \sum_{1 \le i_1 < \cdots < i_j \le m} \mathrm{Vol}_m(P_{i_1} + \cdots + P_{i_j}).$$

CHAPTER III

TORIC ERROR-CORRECTING CODES

A. Toric Surface Codes

J. P. Hansen introduced the connection between toric surfaces and error-correcting codes in 1998 [9]. Since that time, these codes and their m-dimensional counterparts have been studied in [10, 11, 13, 14, 15, 16, 17] and many others. In this section, we present the results from the works that developed much of the interest in toric codes and motivated the analysis of the toric threefolds in Chapter IV.

As stated in Chapter I, constructing an error-correcting code via an evaluation map over a finite set of points was known since Goppa. In [9], Hansen used the connection between convex bodies and toric varieties to construct the error-correcting codes, as well as formulae for their dimension and minimum distance, for the following three families of convex polygons:

1. $T_d = conv\{(0,0),(d,d),(0,2d)\}$
2. $P_d = conv\{(0,0),(0,d),(d,0)\}$
3. $\square_{d,e} = conv\{(0,0),(d,0),(0,e),(d,e)\}, e \leq d$

We will briefly explain Hansen's method for the polygon P_d and its associated toric variety $X = X_{P_d}$. First, we consider the $\mathbb{F}_q$-rational points of the algebraic torus $(\mathbb{F}_q^*)^2$ as $q-1$ "lines" of points defined by $C_{\alpha_i} = Z(\{x_1 - \alpha_i\})$, for all $\alpha_i \in \mathbb{F}_q^*$. Suppose $H^0(X, \mathcal{O}_X(D_{P_d}))$ contains a nonzero section f that is zero in exactly a lines of the torus. Since the divisors of zeros $\mathrm{div}_0(x_1 - \alpha)$ and $\mathrm{div}_0(x_1)$ are linearly equivalent, we also have that $\mathrm{div}(f) + (D_{P_d} - a\mathrm{div}_0(x_1)) \geq 0$; ie. $f \in H^0(X, \mathcal{O}_X(D_{P_d} - a\mathrm{div}_0(x_1)))$. Then by Lemma II.2, we must have $a \leq d$. As for the number of zeros of f on the remaining $q-1-a$ lines of the torus, this number is bounded above by the intersection number $(D_{P_d} - a\mathrm{div}_0(x_1)) \cdot (\mathrm{div}_0(x_1)) = d - a$ [11]. Therefore, the $\mathbb{F}_q$-rational zeros are bounded above by

$$a(q-1) + ((q-1)-a)(d-a) \leq d(q-1).$$

Provided $P_d \subset \Box_{q-1}$, the evaluation map ev from Chapter II is injective, and the minimum distance is $d(C_{P_d}) = (q-1)^2 - d(q-1)$.

D. Ruano used these same arguments in [16] for polytopes of dimension $m \geq 2$. To do this, he noted that all of the $\mathbb{F}_q$-rational points of $(\mathbb{F}_q^*)^m$ lie on the $(q-1)^{m-1}$ lines defined by

$$C_{\xi_1,\ldots,\xi_{m-1}} = Z(\{\chi^{u_i} - \xi_i \mid i = 1,\ldots,m-1\}), \quad \text{for all } \xi_i \in \mathbb{F}_q^*,$$

where $Z(\cdot)$ denotes the common zero set and $u_i = \mathbf{e}_i$. Thus, given a nonzero section $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$ that is zero along exactly a of these lines, we can bound the zeros of f along the other $(q-1)^{m-1} - a$ lines by the intersection number $D_P.C_{\xi_1,\ldots,\xi_{m-1}}$. Since all of these lines are linearly equivalent, the number of zeros of f over $(\mathbb{F}_q^*)^m$ is bounded by

$$a(q-1) + ((q-1)^{m-1} - a)(D_P.C),$$

where C is any of the lines $C_{\xi_1,\ldots,\xi_{m-1}}$. Thus, we obtain a lower bound on the minimum distance of C_P.

In [10], J. P. Hansen considered the polygon $Q = conv\{(0,0),(d,0),(o,e),(d,e+rd)\}$, with $d, e < q-1$ and r a positive integer, and used the above technique to prove $d(C_Q) = \min\{(q-1-d)(q-1-e),(q-1)(q-1-(e+rd))\}$. Polygons of this form are associated with *Hirzebruch surfaces*, denoted $\mathcal{H}_r$, and, up to isomorphism, account for all smooth toric surfaces that satisfy $\mathrm{rank}(\mathrm{Pic}(\mathcal{H}_r)) = 2$. Thus, it was possible to calculate the dimension and minimum distance for a large class of toric surface codes. In this paper, Hansen also refers to extensive computations done by D. Joyner in [13] and their help in modifying a preliminary version of [10].

D. Joyner calculated the minimum distance of an extensive list of toric codes in [13] using both the MAGMA and GAP programs. However, rather than beginning with a particular polygon of arbitrary size, such as T_d, P_d, or $\Box_{d,e}$, he considered divisors on a particular refined normal fan. In this way, Joyner was able to calculate the parameters for polygons of, potentially, different size and shape in a very systematic fashion. More importantly, he described a $[49, 11, 28]$ code whose minimum distance was larger that any other known code at the time for that particular block length and dimension. This code is given below.

Example III.1. [13, Example 3.2] Consider the toric surface code generated from the polytope $P = conv\{(0,0), (1,5), (5,1)\}$ over $\mathbb{F}_8$. The dimension is $k = \#P = 11$, and the inward pointing normals are $v_1 = 5\mathbf{e}_1 - \mathbf{e}_2$, $v_2 = -\mathbf{e}_1 + 5\mathbf{e}_2$, and $v_3 = -\mathbf{e}_1 - \mathbf{e}_2$. This code has parameters $[49, 11, 28]$, which was better than the previous $[49, 11, 27]$.

The results of [14] and [15] provide some very helpful tools for the analysis of the toric threefold codes described in Chapter IV. In [15], Little and Schwarz begin with the observation that certain submatrices of a $k \times n$ generator matrix G for a toric code C are "examples of a multivariate generalization of the familiar univariate Vandermonde matrices" [15]. They use this to prove the following results for the minimum distance of toric codes defined by m-dimensional rectangles and simplices.

Theorem III.1. *Let $P_{k_1,k_2,\ldots,k_m}$ denote the $k_1 \times k_2 \times \cdots k_m$ rectangular polytope, and suppose $P_{k_1,k_2,\ldots,k_m} \subset [0, q-1]^m$ for some prime power q. Then the minimum distance* *of the m-dimensional toric code* $C_{P_{k_1,k_2,\ldots,k_m}}$ *is*

$$d(C_{P_{k_1,k_2,\ldots,k_m}}) = \prod_{i=1}^{m}((q-1)-k_i).$$

Theorem III.2. *Let* $P_{\ell_1,\ell_2,\ldots,\ell_m}$ *denote the general simplex conv*$\{\mathbf{0}, \ell_1\mathbf{e}_1, \ldots, \ell_m\mathbf{e}_m\}$, *with* $\ell_i \geq 1$, *and suppose* $P_{\ell_1,\ell_2,\ldots,\ell_m} \subset [0, q-1]^m$ *for some prime power* q. *If* $\ell = \max_i\{\ell_i\}$, *then the minimum distance of the m-dimensional toric code* $C_{P_{\ell_1,\ell_2,\ldots,\ell_m}}$ *is*

$$d(C_{P_{\ell_1,\ell_2,\ldots,\ell_m}}) = (q-1)^m - \ell(q-1)^{m-1}.$$

Additionally, Little and Schwarz prove a very useful connection between lattice equivalent polytopes and monomial equivalent toric codes. Two polytopes P and Q are said to be *lattice equivalent* if there exists a unimodular integer affine transformation T such that $T(P) = Q$. Two toric codes C_1 and C_2 are said to be *monomial equivalent* if their exists an invertible $n \times n$ diagonal matrix M and an $n \times n$ permutation matrix N, such that the corresponding generator matrices G_1 and G_2 satisfy $G_2 = G_1MN$. Consequently, monomial equivalent codes will have the same dimension and the same minimum distance. From [15, Theorem 3.3], we have that if two polytopes P_1 and P_2 are lattice equivalent, then the two toric codes C_{P_1} and C_{P_2} are monomially equivalent.

In [14], Little and Schenck take a polygon P and find a subpolygon with a maximal Minkowski sum decomposition to find sections of $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ with the most zeros. As we know, these correspond to minimum weight codeswords. Recall from Section D of Chapter II that the Minkowski sum of polygons P and Q has an associated refined normal fan Δ_{P+Q} and complete smooth toric variety X_{P+Q}. Consequently, the global sections of the divisors D_P and D_Q are related by

$$H^0(X_{P+Q}, \mathcal{O}(D_P)) \otimes H^0(X_{P+Q}, \mathcal{O}(D_P)) = H^0(X_{P+Q}, \mathcal{O}(D_P + D_P)).$$

Using the above notions in reverse, Little and Schenck noticed that the irreducible factors of a section in $H^0(X_P, \mathcal{O}(D_P))$ correspond to subpolygons whose Minkowski sum is contained in P. Thus, they obtained a nice upper bound for the minimum distance of the corresponding toric code in terms of the these subpolygons [14, Proposition 2.3]. The following is a generalization of Proposition 2.3 to toric codes corresponding to polytopes $P \subset \mathbb{R}^m$.

Proposition III.1. *Let $\sum_{i=1}^{k} P_i \subseteq P$, with $P \subset \mathbb{R}^m$, and let X_P be the toric variety corresponding to P. Let m_i be the maximum number of zeros in $(\mathbb{F}_q^*)^m$ of a section of the line bundle on X_P corresponding to P_i, and assume there exits sections s_i with sets of m_i zeros that are pairwise disjoint in $(\mathbb{F}_q^*)^m$. Then*

$$d(C_P) \leq \sum_{i=1}^{k} d(C_{P_i}) - (k-1)(q-1)^m.$$

Proof. For each P_i, the minimum distance of the corresponding toric code is $d(C_{P_i}) = (q-1)^m - m_i$. As stated above, the product $s = s_1 s_2 \ldots s_k$ is a section of the line bundle corresponding to $\sum_{i=1}^{k} P_i \subseteq P$. Since the sets of m_i zeros are pairwise disjoint, the section s has exactly $m_1 + m_2 + \ldots + m_k$ zeros in $(\mathbb{F}_q^*)^n$. Thus, there is a code word of C_P with weight

$$w = (q-1)^m - (m_1 + m_2 + \ldots + m_k) = \sum_{i=1}^{k} d(C_{P_i}) - (k-1)(q-1)^m,$$

which shows

$$d(C_P) \leq \sum_{i=1}^{k} d(C_{P_i}) - (k-1)(q-1)^m.$$

□

For cases where sections with maximum zeros have overlapping zero sets, we can extend this result by using the inclusion-exclusion principle.

The key ingredient for the main result of [14] comes from [14, Proposition 5.2]. In it, Little and Schenck prove that for a line bundle $\mathcal{O}(D_P)$ on a smooth toric surface X_P, the sections with the most zeros over $(\mathbb{F}_q^*)^2$ will be the ones with the most irreducible factors as long as q is sufficiently large. They specifically showed sufficiency when $q \geq (4I(P)+3)^2$, where $I(P)$ is the number of interior lattice points of P. This result allows for an lower bound on the minimum distance of the toric surface code C_P by finding a maximal Minkowski sum decomposition within P.

Theorem III.3. *Let $\mathbb{F}_q$ be a finite field and let $P \subset \mathbb{R}^2$ be an integral convex polygon strictly contained in $\square_{q-1}$. Assume that $q \geq (4I(P)+3)^2$, where $I(P)$ is the number of interior lattice points of P. Let ℓ be the largest positive integer such that there is some $P' \subseteq P$ that decomposes as a Minkowski sum $P' = P_1 + P_2 + \cdots + P_\ell$ with nontrivial P_i. Then there exists some $P' \subseteq P$ of this form such that*

$$d(C_P) \geq \sum_{i=1}^{\ell} d(C_{P_i}) - (\ell - 1)(q-1)^2.$$

B. MDS Polygons

As we mentioned in Chapter I, Reed-Solomon codes are MDS. That is, given an integral line segment with one endpoint at the origin and length $k-1$, there is an associated Reed-Solomon code with minimum distance $d = (q-1) - k + 1$, provided $k < q-1$. The natural question that follows is whether there exists specific polygons in $\mathbb{R}^2$ that also generate maximum distance separable codes. Little and Schwarz posed a variation of this question in [15].

A linear code is MDS when $d = n - k + 1$, or, equivalently, when the maximum number of zeros, m, of any codeword equals $k-1$. For toric codes, this becomes $m = \#(P) - 1$, where $\#(P)$ is the number of lattice points in the polytope P. Thus, this becomes an exercise in algebra when we know the number of lattice points and the minimum distance for a particular polytope.

Example III.2. Fix q and consider the toric code $C_{\square_a}$ generated by the square $\square_a = conv\{(0,0),(0,a),(a,0),(a,a)\}$, with $a < q-1$. By Theorem III.1, we know the maximum number of zeros in any codeword is $2a(q-1)-a^2$. Since the number of lattice points in $\square_a$ is $(a+1)^2$, we have

$$2a(q-1)-a^2 = (a+1)^2 - 1$$
$$q-2 = a.$$

So, for fixed q, the square polygon $\square_{q-2}$ is MDS. (Notice that we could have fixed our square and let q vary to obtain the same result.) It is important to note that while these toric codes are MDS, the minimum distance in not very good. Indeed,

$$\begin{aligned} d &= n-k+1 \\ &= (q-1)^2-(a+1)^2+1 \\ &= (q-1)^2-((q-2)+1)^2+1 \\ &= 1. \end{aligned}$$

The fact that $d=1$ means that we completely cover $(\mathbb{F}_q)^2$. But this makes sense because the corresponding generator matrix is a full rank $(q-1)^2 \times (q-1)^2$ matrix. For rectangles of the form $\square_{a,b} = conv\{(0,0),(a,0),(0,b),(a,b)\}$, with $0 < b < a < q-1$, the analysis is similar, but more tedious.

Proposition III.2. *For the rectangle $\square_{a,b} = conv\{(0,0),(a,0),(0,b),(a,b)\}$, with $0 < b < a < q-1$, the toric surface code $C_{\square_{a,b}}$ is not maximum distance separable.*

Proof. We know q must satisfy $q \geq a+2$. When $q = a+2$, we have

$$d(C_{\square_{a,b}}) = (q-1-a)(q-1-b) = (1)(a-b+1).$$

and

$$\begin{aligned} n-k+1 &= (q-1)^2-(a+1)(b+1)+1 \\ &= (a+1)^2-(a+1)(b+1)+1 \\ &= a^2-ab+a-b+1. \end{aligned}$$

Equality above only occurs for $a=0$ or $a=b$, which are not allowed. Thus we always have $d(C_{\square_{a,b}}) < n-k+1$, and $C_{\square_{a,b}}$ is not MDS.

Suppose we increase q to q_1. Direct computation shows that $d(C_{\square_{a,b}})$ will increase by a factor of $q_1^2-q^2-2(q_1-q)-(a+b)(q_1-q)$ while $n-k+1$ increases by $q_1^2-q^2-2(q_1-q)$. So, our inequality remains strict as q increases, and $C_{\square_{a,b}}$ cannot become MDS. $\square$

We do one more example with a polygon from Hansen [9].

Example III.3. Fix q and consider the triangle $P_a = conv\{(0,0),(0,a),(a,0)\}$, with $a<q-1$. By Theorem III.2, $d(C_{P_a}) = (q-1)^2-a(q-1)$, and $\#P_a = \frac{1}{2}(a+1)(a+2)$. Thus,

$$\begin{aligned} 2a(q-1) &= (a^2+3a+2)-2 \\ 2aq &= a^2+5a \\ 2q-5 &= a \end{aligned}$$

While this seems convenient, it eliminates most triangles from being MDS. When $a=1$ and $q=3$, we obtain a $[4,3,2]$ MDS code. However, when $a=3$, we must have $q=4$, which violates our requirement. In fact, by graphing the equations $q=\frac{1}{2}(a+5)$ and $q \geq a+2$, one sees that there is only a very small feasible region that includes the point $(a,q)=(1,3)$. Similar to Proposition III.2, we have the following result for a large class of subcodes contained in C_{P_a}.

Proposition III.3. *For the triangle* $P = conv\{(0,0),(a,0),(b,c)\}$*, with* $b + c \leq a$*, in Figure 7, the toric surface code* C_P *is not maximum distance separable.*

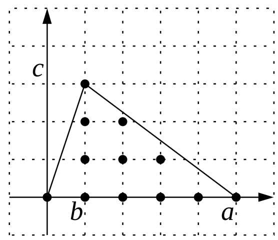


Fig. 7. Subpolygons of the triangle P_a.

Proof. First note that $d(C_{P_a}) = d(C_P)$ by [14, Proposition 3.2]. Since $\#P \leq \#P_a$, we may conclude that P is not MDS when $q > 3$. Indeed, when $q > 3$ we must have $d(C_{\triangle_a}) < n - k + 1$ and our previous statements imply that d will remain the same while $n - k + 1$ will, at least, not decrease. □

The above results seem to indicate that MDS toric surface codes only come from squares with side length equal to $q - 1$. However, direct computation and some examples from [13] show that this is not the case. Consider the polygon in Figure 8, and let $a = 2$. Setting $q = 4$ and using the GAP program, we see that this corresponds to a [9,8,2] toric code that is MDS. We would like to extend this result for all values of a, but first we need the following proposition.

Proposition III.4. *Let* $P = conv\{(0,0),(a,0),(0,a),(a,a-1),(a-1,a)\}$*, the square* $\square_a$ *with one corner lattice point removed. If* q *is sufficiently large, then*

$$d(C_P) = (q-1)^2 - (2a-1)(q-1) + a(a-1).$$

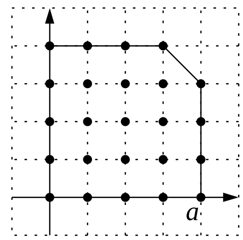


Fig. 8. Polygon $\square_a$ with one corner lattice point removed.

Proof. Since $\square_{a,a-1} \subset P$, $C_{\square_{a,a-1}}$ is a subcode of C_P and $d(C_{\square_{a,a-1}}) \geq d(C_P)$. Thus,

$$d(C_P) \leq (q-1-a)(q-1-(a-1)) = (q-1)^2 - (2a-1)(q-1) + a(a-1).$$

We see that $\square_{a,a-1}$ is also a subpolygon of C_P with a maximal number of Minkowski summands. Note that we can also take the decomposition $\square_{a-1} + P_1 = P$, but this has the same number of summands. A section of $H^0(X_P, \mathcal{O}(D_P))$ with a maximum number of zeros will be of the form $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_a)(y-\beta_1)\ldots(y-\beta_{a-1})$, with $\alpha_i \in \mathbb{F}_q^*$ distinct and $\beta_i \in \mathbb{F}_q^*$ distinct. If we take q sufficiently large and account for overlapping zeros, Theorem III.3 yields

$$\begin{aligned} d(C_P) &\geq \sum_{i=1}^{2a-1} [(q-1)^2 - (q-1)] + a(a-1) - (2a-1-1)(q-1)^2 \\ &= (q-1)^2 - (2a-1)(q-1) + a(a-1). \end{aligned}$$

$\square$

Now we use the process of Example III.3 to see that C_P is MDS exactly when

$$\begin{aligned} (2a-1)(q-1) - a(a-1) &= (a+1)^2 - 1 - 1 \\ (2a-1)(q-1) &= 2a^2 + a - 1 \\ (2a-1)(q-1) &= (2a-1)(a+1) \\ q &= a+2 \end{aligned}$$

So, if we did not require q to be sufficiently large, then the polygons of Figure 8 would correspond to MDS codes with minimum distance $d = (a+1)^2 - [(a+1)^2 - 1] + 1 = 2$.

CHAPTER IV

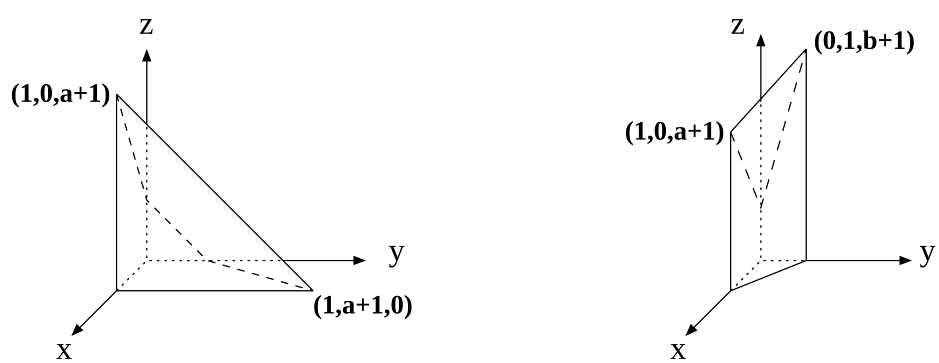
CODES FROM SMOOTH TORIC THREEFOLDS WITH RANK(PIC(X)) = 2

A. Minimum Distance of Codes

There are two families of polytopes corresponding to smooth toric threefolds with rank(Pic(X)) = 2 [3]. We begin with the simplest members, those with no interior lattice points; see Figure 9.

$$P_1(a) = conv\{\mathbf{0}, \mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3}, \mathbf{e_1} + (\mathrm{a}+1)\mathbf{e_3}, \mathbf{e_1} + (\mathrm{a}+1)\mathbf{e_2}\}$$

$$P_2(a,b) = conv\{\mathbf{0}, \mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3}, \mathbf{e_1} + (\mathrm{a}+1)\mathbf{e_3}, \mathbf{e_2} + (\mathrm{b}+1)\mathbf{e_3}\}$$



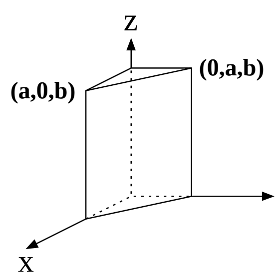
(a) Polytope $P_1(a)$. (b) Polytope $P_2(a,b)$.

Fig. 9. Polytopes with no interior lattice points corresponding to the two families of smooth toric threefolds with rank(Pic(X))=2.

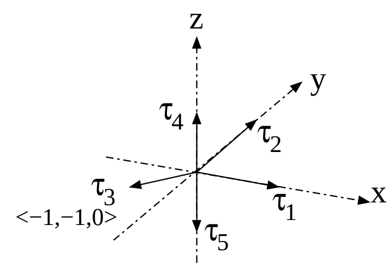
In this section, we prove formulas for the minimum distance of the toric codes $C_{P_1(a)}$ and $C_{P_2(a,b)}$ followed by tables of minimum distance values for different values of a and b. Recall that an integer affine transformation of a polytope creates a monomially equivalent toric code. Thus, it is helpful to consider unimodular integer affine transformations of $P_1(a)$ and $P_2(a,b)$. For both polytopes, there are specific cases when particular integer values for a and b yield subpolytopes of a simplex. Thus, we use Theorem III.2 for these cases. The remaining cases yield polytopes with a Minkowski sum decomposition, and we apply Proposition III.1 and the following lemma.

Lemma IV.1. *Let P_a be the triangle in Chapter III and $Q = conv\{(0,0,0),(0,0,b)\}$. Fix a prime power q such that $P_a + Q \subset [0, q-1]^3$. Then*

$$d(C_{P_a+Q}) = (q-1)^3 - (a+b)(q-1)^2 + ab(q-1).$$



(a) Polytope $P_a + Q$.



(b) Fan Δ_{P_a+Q}.

Fig. 10. Polytope $P_a + conv\{(0,0,0),(0,0,b)\}$ and corresponding normal fan.

Proof. The proof uses arguments similar to those in [16, Section 4]. The normal fan corresponding to $P_a + Q$ has one dimensional rays $\tau_1, \ldots, \tau_5$ with corresponding primitive vectors $v_1 = \mathbf{e}_1$, $v_2 = \mathbf{e}_2$, $v_3 = -\mathbf{e}_1 - \mathbf{e}_2$, $v_4 = \mathbf{e}_3$, and $v_5 = -\mathbf{e}_3$; see Figure 10. Since Δ_{P_a+Q} is regular, the divisor corresponding to P_a+Q is $D_{P_a+Q} = aD_3+bD_5$, where $D_i = V(\tau_i)$, as usual.

Recall that the $\mathbb{F}_q$-rational points of $(\mathbb{F}_q^*)^3$ lie on $(q-1)^2$ lines defined by the zero set $C_{\xi_1,\xi_2} = Z(\{\chi^{\mathbf{e}_1} - \xi_1, \chi^{\mathbf{e}_2} - \xi_2\})$. Let $f \in \mathrm{H}^0(X_{P_a+Q}, \mathcal{O}(D_{P_a+Q}))$ be a nonzero section with a maximum number of zeros over $(\mathbb{F}_q^*)^3$. From Chapter III, we know this number is bounded above by

$$c(q-1)+((q-1)^2-c)(D_{P_a+Q}.C),$$

where C is any line defined above and c is the maximum number of zeros of a section defined by a projection of P_a+Q onto the xy-plane. Thus, $c \leq a(q-1)$ by Theorem III.2.

Next, we compute $\mathrm{div}_0(\chi^{u_1}) = D_1$ and $\mathrm{div}_0(\chi^{u_2}) = D_2$, and the intersection number

$$D_{P_a+Q}.C = (aD_3+bD_5).D_1.D_2 = b.$$

This easily follows from Definition II.7 or by calculating mixed volumes as in [16]. So, the maximum number of zeros of our section f is bounded above by

$$a(q-1)(q-1-b)+b(q-1)^2 = (a+b)(q-1)^2 - ab(q-1),$$

and $d(C_{P_a+Q}) \geq (q-1)^3-(a+b)(q-1)^2+ab(q-1)$. Since P_a+Q contains the square $\square_{a,b}$ in the xz-plane, we know

$$d(C_{P_a+Q}) \leq d(C_{\square a,b}) = (q-1-a)(q-1-b)(q-1),$$

and we have equality. $\square$

Theorem IV.1. *Let $a \in \mathbb{Z}_{\geq 0}$ and q be a prime power such that $q-1 > a+1$, and consider $P_1(a)$ defined above. Then the minimum distance of the toric code $C_{P_1(a)}$ over the finite field $\mathbb{F}_q$ is*

$$d(C_{P_1(a)}) = \begin{cases} (q-1)^3-2(q-1)^2+(q-1) & \textit{if } a=0 \\ (q-1)^3-(a+1)(q-1)^2 & \textit{if } a>0 \end{cases}$$

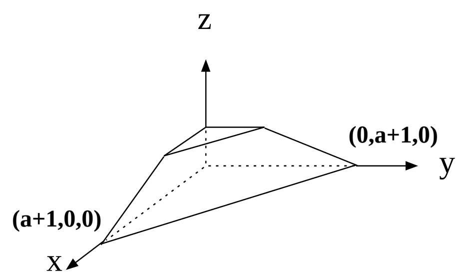


Fig. 11. Polytope $\hat{P}_1(a)$.

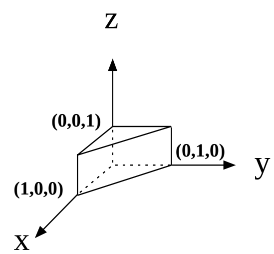


Fig. 12. Polytope $\hat{P}_1(0)$.

Proof. We first perform a translation and a rotation of $P_1(a)$ to obtain Figure 11.

The case with $a = 0$ corresponds to Figure 12. So, this is a direct consequence of Lemma IV.1.

When $a > 0$, we see that Figure 11 is contained in the tetrahedron $P_{a+1,a+1,2} = conv\{\mathbf{0}, (a+1)\mathbf{e}_1, (a+1)\mathbf{e}_2, 2\mathbf{e}_3\}$. Thus, $C_{\hat{P}_1(a)}$ is a subcode of $C_{P_{a+1,a+1,2}}$. Combining this with Theorem III.2 yields

$$\begin{aligned} d(C_{P_1(a)}) &\geq d(C_{P_{a+1,a+1,2}}) \\ &= (q-1)^3 - (a+1)(q-1)^2 \end{aligned}$$

But $C_{P_1(a)}$ contains codewords of weight $(q-1)^3 - (a+1)(q-1)^2$ obtained from irreducible sections in $\mathcal{O}(D_{P_1(a)})$ of the form $x(y-\alpha_1)\ldots(y-\alpha_{a+1})$, with $\alpha_i \in \mathbb{F}_q^*$ distinct. Therefore, $d(C_{P_1(a)}) = (q-1)^3 - (a+1)(q-1)^2$.

□

Theorem IV.2. *Let $a, b \in \mathbb{Z}_{\geq 0}$ and q be a prime power such that $q - 1 > \max\{a+1, b+1\}$, and consider $P_2(a,b)$ defined above. Then the minimum distance of the toric code $C_{P_2(a,b)}$ over the finite field $\mathbb{F}_q$ is*

$$d(C_{P_2(a,b)}) = \begin{cases} (q-1)^3 - 2(q-1)^2 + (q-1) & \textit{if } a = b = 0 \\ (q-1)^3 - (b+2)(q-1)^2 + (b+1)(q-1) & \textit{if } a = b > 0 \\ (q-1)^3 - (b+1)(q-1)^2 & \textit{if w.l.o.g. } b > a \end{cases}$$

Proof. First, we apply a unimodular integer affine transformation to obtain $\hat{P}_2(a,b)$, as this makes calculations easier and the visualization more natural; see Figure 13. The transformation is a combination of a rotation in the xy-plane by $\frac{\pi}{2}$, a shear of the x coordinate by a factor of -1, and a translation by $[1,0,0]$.

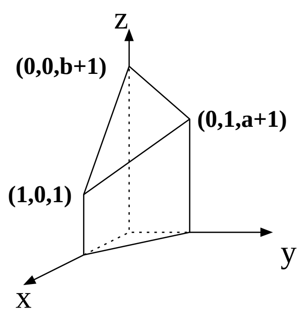


Fig. 13. Polytope $\hat{P}_2(a,b)$.

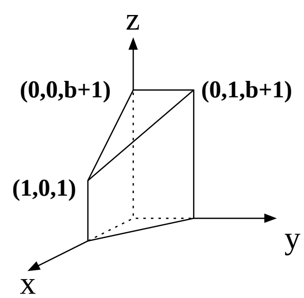


Fig. 14. Polytope $\hat{P}_2(b,b)$.

For the case with $a = b = 0$, we obtain $\hat{P}_1(0)$. So the conclusion follows from Lemma IV.1.

When $a = b > 0$, we obtain Figure 14. As we have seen many times before, $\hat{P}_2(b,b)$ is contained in the polytope $P = conv\{(0,0,0),(1,0,0),(0,1,0),(0,0,b+1),(1,0,b+1),(0,1,b+1)\}$ and its corresponding toric code contains codewords that attain the maximum number of zeros of codewords from C_P. Thus, the result follows from Lemma IV.1.

For the last case, we see from Figure 13 that $\hat{P}_2(a,b) \subset P_{2,b+1,b+1}$ and $d(C_{P_2(a,b)}) = (q-1)^3 - (b+1)(q-1)^2$ using the usual subcode arguments.

$\square$

Table 1 and Table 2 show minimum distance values for the toric codes $C_{P_1(a)}$ and $C_{P_2(a,b)}$, respectively. The dimensions of these codes come from the formulas $\#P_1(a) = \frac{a^2+5a+12}{2}$ and $\#P_2(a,b) = a+b+6$ found in [19]. The rightmost column of both tables gives the upper and lower bound from [8] for unknown minimum distance values of linear q-ary codes with the same block length n and dimension k. So, codes with minimum distance values within this range would be new codes.

Table 1. Codes corresponding to $P_1(a)$.

a	q	n	k	$d(C_{P_1(a)})$	unknown d range [8]
0	3	8	6	2	$2 < d < 2$
0	4	27	6	12	$16 < d < 16$
0	5	64	6	36	$45 < d \leq 48$
0	7	216	6	150	no bounds
1	4	27	9	9	$13 < d \leq 14$
1	5	64	9	32	$40 < d \leq 45$
1	7	216	9	144	no bounds
1	8	343	9	245	no bounds
2	5	64	13	16	$35 < d \leq 41$
2	7	216	13	108	no bounds
2	8	343	13	196	no bounds
3	7	216	18	72	no bounds
3	8	343	18	147	no bounds

So far, we have only looked at polytopes containing no interior lattice points. In order to state the minimum distance of all smooth toric threefolds with rank(Pic(X)) = 2, we need to understand all associated polytopes. Consider the fans $\Delta_{\hat{P}_1(a)}$ and $\Delta_{\hat{P}_2(a,b)}$ associated with $\hat{P}_1(a)$ and $\hat{P}_2(a,b)$, respectively; see Figures 15 and 16. Since we know both varieties are smooth, a general divisor on each will look like $d_1D_1 + \cdots + d_5D_5$ with $D_i = V(\tau_i)$ and $d_i \in \mathbb{Z}$. Using the fact that both $X_{\Delta_{\hat{P}_1(a)}}$ and $X_{\Delta_{\hat{P}_2(a,b)}}$ satisfy $\text{rank}(\text{Pic}(X_{\Delta_{\hat{P}_1(a)}})) = \text{rank}(\text{Pic}(X_{\Delta_{\hat{P}_2(a,b)}})) = 2$, we can find all associated polytopes by finding the generators of the associated Picard groups.

Recall that the Picard group of a variety X is defined as $\text{Pic}(X) = \text{Div}_C(X) \setminus$

Table 2. Codes corresponding to $P_2(a,b)$.

a	b	q	n	k	$d(C_{P_2(a,b)})$	unknown d range [8]
0	1	4	27	7	9	$15 < d \leq 16$
0	1	5	64	7	32	$44 < d \leq 47$
0	1	7	216	7	144	no bounds
1	1	4	27	8	6	$14 < d \leq 15$
1	1	5	64	8	24	$41 < d \leq 46$
1	1	7	216	8	120	no bounds
0	2	5	64	8	16	$41 < d \leq 46$
0	2	7	216	8	108	no bounds
0	2	8	343	8	196	no bounds
1	2	5	64	9	16	$40 < d \leq 45$
1	2	7	216	9	108	no bounds
1	2	8	343	9	196	no bounds

$\mathrm{Div}_P(X)$ and that two divisors are linearly equivalent if their difference is principal. For $X_{\Delta_{\hat{P}_1(a)}}$, we know $D_1, \ldots, D_5$ are generators for Div_C^T. For the group of principal divisors, we must calculate $\mathrm{div}(\chi^{\mathbf{e}_i}) = \sum_j < \mathbf{e}_i, v_j > D_j$, where v_j is the primitive element of τ_j. These calculations yield $\mathrm{div}(\chi^{\mathbf{e}_1}) = D_1 - D_5$, $\mathrm{div}(\chi^{\mathbf{e}_2}) = D_2 - D_5$, and $\mathrm{div}(\chi^{\mathbf{e}_3}) = D_3 - D_4 - aD_5$. Thus, linear combinations of the form $d_4 D_4 + d_5 D_5$ with $d_4, d_5 \in \mathbb{Z}$ and $a \in \mathbb{Z}_{\geq 0}$ will generate all divisors on $X_{\Delta_{\hat{P}_1(a)}}$. Similar calculations for $X_{\Delta_{\hat{P}_2(a,b)}}$ show that linear combinations of the form $d_3 D_3 + d_5 D_5$ generated all divisors on this variety. In Tables 3 and 4, we set d_3, d_4, and d_5 so that we only generate 3-dimensional polytopes. We also omit d_i values that generate code parameters listed in Table 1 or Table 2.

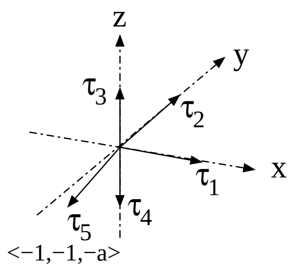


Fig. 15. Fan $\Delta_{\hat{P}_1(a)}$.

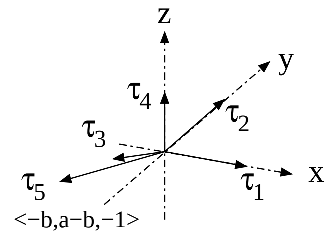


Fig. 16. Fan $\Delta_{\hat{P}_2(a,b)}$.

Table 3. Codes corresponding to divisors on $X_{\Delta_{\hat{P}_1(a)}}$.

a	d_4	d_5	q	n	k	$d(C_P)$	unknown d range [8]
0	2	2	4	27	18	3	$6 < d \leq 7$
0	2	2	5	64	18	16	$28 < d \leq 37$
0	2	2	7	216	18	96	no bounds
1	2	2	4	27	10	9	$12 < d \leq 13$
1	2	2	5	64	10	32	$38 < d \leq 44$
1	2	2	7	216	10	144	no bounds
1	1	3	5	64	16	16	$30 < d \leq 39$
1	2	3	5	64	19	16	$28 < d \leq 37$
1	3	3	5	64	20	16	$27 < d \leq 36$
2	2	4	7	216	22	72	no bounds

Table 4. Codes corresponding to divisors on $X_{\Delta_{\hat{P}_2(a,b)}}$.

a	b	d_3	d_5	q	n	k	$d(C_P)$	unknown d range [8]
1	1	1	1	3	8	5	2	$3 < d < 3$
1	1	1	1	4	27	5	12	$17 < d < 17$
1	1	1	1	5	64	5	36	$48 < d \leq 49$
1	1	1	2	4	27	8	6	$14 < d \leq 15$
1	1	1	2	5	64	8	24	$41 < d \leq 46$
1	2	1	1	4	27	6	9	$16 < d < 16$
1	2	1	2	7	216	12	72	no bounds

B. Code Parameters and Minkowski Sums of Polytopes

In this section, we consider the parameters of toric codes whose underlying polytope is a Minkowski sum. Specifically, we want to express the dimension and minimum distance in terms of the summands. For the dimension calculations, we need the notion of a *Chern class* and a *Todd class*.

Definition IV.1. Let X_Δ be the m-dimensional toric variety defined by the fan Δ, and let $U_1, U_2, \ldots, U_s$ be the variables of the Chow ring of X_Δ. Then the *pth Chern class* of X_Δ is

$$c_p := \sum_{i_1 < i_2 < \cdots < i_p} U_{i_1} \cdots U_{i_p}, \qquad \{i_1, \ldots, i_p\} \subset \{1, \ldots, s\}.$$

By convention, we set $c_0 = 1$.

The variables of the Chow ring uniquely correspond to the 1-dimensional cones $\tau_1, \tau_2, \ldots, \tau_s \in \Delta(1)$ and the corresponding T-invariant Weil divisors $D_1, \ldots, D_s$. More importantly, we have the following correspondence between the product of these variables and intersection numbers [2, p. 325],

$$U_{i_1} \cdots U_{i_p} \quad \longleftrightarrow \quad D_{i_1}. \cdots .D_{i_p}.$$

So, for example, $c_1(X_\Delta)$ corresponds to the anticanonical divisor $-K = D_1 + \cdots + D_s$.

The *pth Todd class* of X_Δ is formally defined as the term of order p in a particular formal Taylor expansion involving the Chern roots. However, for our purposes, we simply state the following initial terms of the series:

$$Td_0 = 1, \quad Td_1 = \frac{1}{2}c_1, \quad Td_2 = \frac{1}{12}(c_1^2 + c_2), \quad Td_3 = \frac{1}{24}c_1c_2.$$

Now we are ready to state the Hirzebruch-Riemann-Roch Theorem (HRR) [2, p.

325].

Theorem IV.3. *Let X_Δ be a smooth, projective toric variety of dimension n and let D be the Cartier divisor on X_Δ corresponding to the convex polytope P. Then*

$$\chi(X_\Delta, \mathcal{O}(D)) = \#(P) = \sum_{j=0}^{n} \frac{1}{j!} \quad D^j.\, Td_{n-j}.$$

So, in dimension $m = 2$, we have

$$\chi(X_\Delta, \mathcal{O}(D)) = Td_2 + D.Td_1 + \frac{1}{2}D^2,$$

and in dimension $m = 3$, we have

$$\chi(X_\Delta, \mathcal{O}(D)) = Td_3 + D.Td_2 + \frac{1}{2}D^2.Td_1 + \frac{1}{3!}D^3.$$

Theorem IV.4. *Let P_1 and P_2 be convex lattice polygons, and let $\Delta = \Delta_{P_1+P_2}$ be the refined normal fan associated with the Minkowski sum $P_1 + P_2$. Let $X = X_\Delta$ be the corresponding smooth toric variety with divisors D_1 and D_2 corresponding to P_1 and P_2, respectively. Then*

$$\#(P_1 + P_2) = \#(P_1) + \#(P_2) + 2MV(P_1, P_2) - 1.$$

Proof. From Fulton, the divisor corresponding to $P_1 + P_2$ is $D_1 + D_2$, since $\mathcal{O}(D_1)$ and $\mathcal{O}(D_2)$ are both globally generated. So, by HRR, the number of lattice points in $P_1 + P_2$ equals

$$\begin{aligned}\chi(X, \mathcal{O}(D_1 + D_2)) &= Td_2 + (D_1 + D_2).Td_1 + \frac{1}{2}(D_1 + D_2)^2 \\ &= Td_2 + D_1.Td_1 + D_2.Td_1 + \frac{1}{2}D_1^2 + \frac{1}{2}D_1^2 + D_1.D_2.\end{aligned}$$

To simplify Td_2, we notice that when $D = 0$ for surfaces

$$\chi(X, \mathcal{O}_X) = Td_2.$$

A calculation in [5, p. 75] shows that $\chi(X, \mathcal{O}_X) = 1$ when X is complete and $\mathcal{O}(D)$ is generated by global sections. Thus, we have

$$\begin{aligned}
\chi(X, \mathcal{O}(D_1 + D_2)) &= 1 + D_1.Td_1 + D_2.Td_1 + \frac{1}{2}D_1^2 + \frac{1}{2}D_1^2 + D_1.D_2 \\
&= \chi(X, \mathcal{O}(D_1)) + \chi(X, \mathcal{O}(D_2)) - 1 + 2MV(P_1, P_2) \\
&= \#(P_1) + \#(P_2) + 2MV(P_1, P_2) - 1.
\end{aligned}$$

□

Example IV.1. Recall Example II.7, the Minkowski sum of the polygons $P = conv\{(1,0),(0,1),(2,2)\}$ and $Q = conv\{(0,0),(0,2),(2,2)\}$. Using Theorem IV.2, we have

$$\begin{aligned}
\#(P + Q) &= \#(P) + \#(Q) + 2MV(P, Q) - 1 \\
&= 4 + 6 + 6 - 1 \\
&= 15,
\end{aligned}$$

which we can verify manually.

Corollary IV.1. *Let P_i $i = 1, \ldots, n$ be convex lattice polygons with Minkowski sum $P = \sum_i P_i$, and let $\Delta = \Delta_P$ be the associated refined normal fan. Let $X = X_\Delta$ be the corresponding smooth toric variety with divisors E_i corresponding to P_i. Then*

$$\#(P) = \sum_i^n \#(P_i) + \sum_{i<j} 2MV(P_i, P_j) - (n - 1).$$

Proof. From the above proof it is easy to see that the $(\sum_i D_i).Td_1$ term distributes and

$$\frac{1}{2}(\sum_i D_i)^2 = \frac{1}{2}\sum_i (D_i)^2 + \sum_{i<j} D_i.D_j.$$

Thus, after accounting for the $n-1$ missing ones, we obtain our result. $\square$

Theorem IV.5. *Let P_1 and P_2 be convex lattice polytopes in $\mathbb{R}^3$, and let $\Delta = \Delta_{P_1+P_2}$ be the refined normal fan associated with the Minkowski sum $P_1 + P_2$. Let $X = X_\Delta$ be the corresponding smooth toric variety with divisors D_1 and D_2 corresponding to P_1 and P_2, respectively. Lastly, let Q be the 3-dimensional polytope corresponding to the anticanonical divisor $-K$. Then*

$$\#(P_1+P_2) = \#(P_1)+\#(P_2)+3!MV(P_1,P_2,Q)+Vol_3(P_1+P_2)-Vol_3(P_1)-Vol_3(P_2)-1$$

Proof.

$$\begin{aligned}\chi(X,\mathcal{O}(D_1+D_2)) &= Td_3 + (D_1+D_2).Td_2 + \frac{1}{2}(D_1+D_2)^2.Td_1 + \frac{1}{3!}(D_1+D_2)^3 \\ &= \chi(X,\mathcal{O}(D_1)) + \chi(X,\mathcal{O}(D_2)) - 1 + D_1.D_2.Td_1 \cdots \\ &\quad \cdots + \frac{1}{3!}(3D_1^2.E_2 + 3D_1.D_2^2) \\ &= \#(P_1) + \#(P_2) + 3!MV(P_1,P_2,Q) + Vol_3(P_1+P_2) \cdots \\ &\quad \cdots - Vol_3(P_1) - Vol_3(P_2) - 1.\end{aligned}$$

First, note that $Td_3 = 1$ by the same reasoning as Theorem IV.4. The last line follows from the Steiner decomposition,

$$Vol_n(P_1+P_2) = \sum_{i=0}^{n} \binom{n}{i} MV(P_1,i;P_2,n-i),$$

where $MV(P_1,i;P_2,n-i)$ represents the mixed volume of i copies of P_1 and $n-i$ copies of P_2 and from the fact that $MV_n(P,\ldots,P) = \mathrm{Vol}_n(P)$. $\square$

We now move to the question of finding formulas for the minimum distance of toric codes arising from the Minkowski sum of polytopes. First, we have the following generalization of Lemma IV.1.

Theorem IV.6. *Let* $Q = conv\{(0,0,0),(0,0,b)\}$*, and let* P *be an integral convex polytope in* $\mathbb{R}^2$*. Fix a prime power* q *such that* $P+Q \subset [0,q-1]^3$*, and let* $d(C_P)$ *be the minimum distance of the toric surface code* C_P *over* $\mathbb{F}_q^2$*. Then*

$$d(C_{P+Q}) = d(C_P)(q-1-b).$$

Proof. The proof is similar to that of Lemma IV.1. Set $X = X_{P+Q}$, and let $f \in \mathrm{H}^0(X, \mathcal{O}(D_{P+Q}))$ be a section with a maximum number of zeros over $(\mathbb{F}_q^*)^3$. As before, the maximum number of zeros of f is bounded above by

$$c(q-1) + ((q-1)^2 - c)(D_{P+Q}.C),$$

where $C = Z(\{\chi^{u_1}, \chi^{u_2}\})$ and c is the maximum number of zeros of a section defined by a projection of $P+Q$. Since this projection is just P, we must have $c \leq (q-1)^2 - d(C_P)$. Now, label the one dimensional cones τ_i, $i = 1, \ldots, r$ of the refined normal fan Δ_{P+Q} such that $D_r = V(\tau_r)$, where τ_r is generated by the vector $-\mathbf{e}_3$.

Then we can compute the intersection number

$$\begin{aligned} D_{P+Q}.C &= (D_P + D_Q).C \\ &= D_P.C + bD_r.C \\ &= b. \end{aligned}$$

We see that $D_P.C = 0$ because their associated polygons lie in the same plane and, thus, have zero 3-volume. To see that $D_r.C = 1$, we notice that this is the nontrivial intersection of a hyperplane and a line. So, the maximum number of zeros of f is bounded above by

$$\begin{aligned} c(q-1) + ((q-1)^2 - c)(D_{P+Q}.C) &= c((q-1) - D_{P+Q}.C) + D_{P+Q}.C(q-1)^2 \\ &\leq ((q-1)^2 - d(C_P))((q-1) - b) + b(q-1)^2 \\ &= (q-1)^3 - d(C_P)(q-1-b). \end{aligned}$$

Therefore, $d(C_{P+Q}) \geq d(C_P)(q-1-b)$.

To obtain the reverse inequality, take $g \in \mathrm{H}^0(X, \mathcal{O}(D_P))$ to be a section with a maximum number of zeros, m, in $\mathbb{F}_q^2$. Then there exists a section in $\mathrm{H}^0(X, \mathcal{O}(D_{P+Q}))$ of the form

$$g(z-\alpha_1)\cdots(z-\alpha_b), \quad \text{with distinct } \alpha_i \in \mathbb{F}_q^*.$$

This section has $m(q-1) + b(q-1)^2 - bm$ zeros in $\mathbb{F}_q^3$. Since $m = (q-1)^2 - d(C_P)$, we have

$$\begin{aligned} d(C_{P+Q}) &\leq (q-1)^3 - [m(q-1) + b(q-1)^2 - bm] \\ &= (q-1)^3 - m(q-1-b) - b(q-1)^2 \\ &= (q-1)^3 - ((q-1)^2 - d(C_P))(q-1-b) - b(q-1)^2 \\ &= d(C_P)(q-1-b). \end{aligned}$$

□

Lastly, we give an upper bound for a toric surface code whose corresponding polygon is the Minkowski sum of two polygons. This follows immediately from the fact that our line bundles are generated by global sections.

Proposition IV.1. *Let P and Q be convex polygons and consider the toric surface code C_{P+Q} generated by their Minkowski sum $P+Q$ over $\mathbb{F}_q^2$. Then*

$$d(C_{P+Q}) \leq d(C_P) + d(C_Q) - (q-1)^2 + 2!MV(P_1, P_2),$$

where P_1 is the polygon corresponding to a section $s_1 \in H^0(X, \mathcal{O}(D_P))$ with a maximum number of zeros in the algebraic torus, and P_2 is similar for D_Q.

Proof. Let $\Delta = \Delta_{P+Q}$ be the refined normal fan of $P + Q$, and $X = X_\Delta$ the corresponding toric surface. Let D_P, D_Q, and D_{P+Q} be divisors on X corresponding to P, Q, and $P + Q$, respectively. Let $s_1 \in \mathrm{H}^0(X, \mathcal{O}(D_P))$, $s_2 \in \mathrm{H}^0(X, \mathcal{O}(D_Q))$, and $s_3 \in \mathrm{H}^0(X, \mathcal{O}(D_{P+Q}))$ be sections with the maximum number of zeros m_1, m_2, and m_3, respectively. Let D_1 and D_2 be divisors on X corresponding to s_1 and s_2, respectively. By Proposition II.2, the intersection of s_1 and s_2 inside the algebraic torus is less than or equal to $D_1.D_2 = 2!MV_2(P_{D_1}, P_{D_2})$, where P_{D_i} is the polygon corresponding to D_i. Since $s_1 s_2 \in \mathrm{H}^0(X, D_P + D_Q)$, we have

$$\begin{aligned} m_3 &\geq m_1 + m_2 - 2!MV_2(P_1, P_2) \\ (q-1)^2 - m_3 &\leq (q-1)^2 - m_1 + (q-1)^2 - m_2 - (q-1)^2 + 2!MV(P_1, P_2) \\ d(C_{P+Q}) &\leq d(C_P) + d(C_Q) - (q-1)^2 + 2!MV(P_1, P_2) \end{aligned}$$

$\square$

Direct computation shows that this bound is very good for certain polytopes. Specifically, when the Minkowski sum $P + Q$ does not contain a maximal decomposition that is larger than the sum of maximal decompositions contained in P and Q. However, this will not guarantee equality because the maximum number of zeros of a section will depend on the field $\mathbb{F}_q$.

Example IV.2. Consider the toric code over $\mathbb{F}_5$ and $\mathbb{F}_7$ generated from the Minkowski sum in Figure 17. Let $P = conv\{(0,0), (2,0), (1,1)\}$ and $Q = \square_1$. Over $\mathbb{F}_5$,

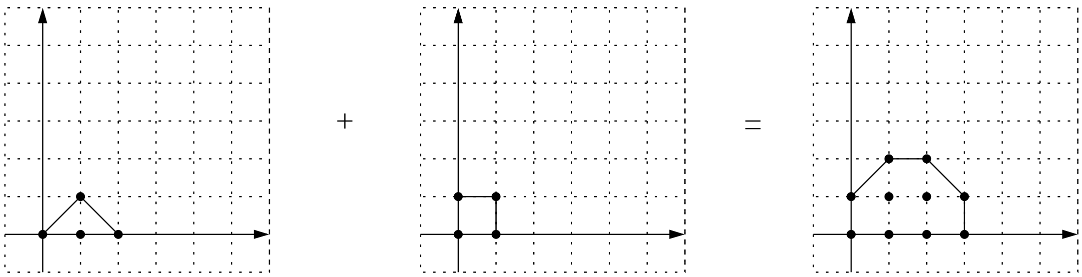


Fig. 17. Minkowski sum that gives equality in Proposition IV.1.

we know $d(C_P) = 8$ and $d(C_Q) = 9$, and the polygons associated with sections in $\mathcal{O}(D_P)$ and $\mathcal{O}(D_Q)$ having the maximum number of zeros are $P_1 = conv\{(0,0),(2,0)\}$ and Q, respectively. Then $2MV_2(P_1, Q) = 2$ and, by Proposition IV.1, $d(C_{P+Q}) \leq 8 + 9 - 16 + 2 = 3$. Using the GAP program, we know this minimum distance value to be exact. Similarly, over $\mathbb{F}_7$ we have $d(C_P) = 24$ and $d(C_Q) = 25$ and $d(C_{P+Q}) \leq 24 + 25 - 36 + 2 = 15$, which is also exact according to the GAP program.

Example IV.3. Consider the toric code over generated from the Minkowski sum in Figure 18. Let $P = conv\{(1,0),(0,1),(2,2)\}$ and $Q = conv\{(0,0),(1,0),(1,1)\}$.

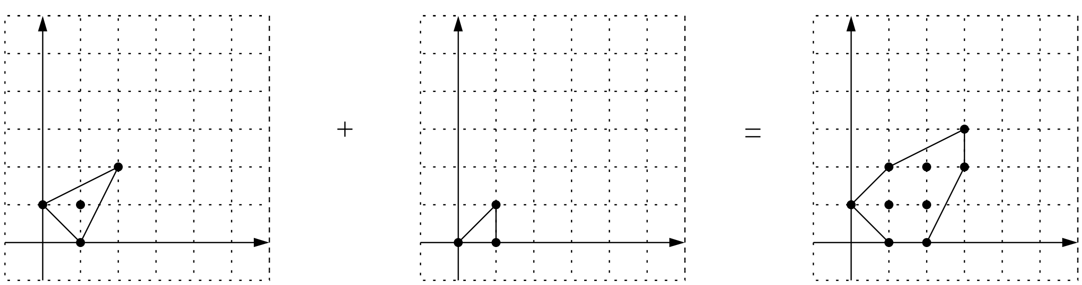


Fig. 18. Minkowski sum that does not give equality in Proposition IV.1.

Over $\mathbb{F}_{11}$, we know $d(C_P) = 85$ and $d(C_Q) = 90$. Since polygons corresponding to sections with maximum zeros are subpolygons of either P or Q, respectively, we can use $2MV_2(P,Q) = 3$ as upper bound for the mixed volume calculation. Thus,

$$d(C_{P+Q}) \leq 85 + 90 - 100 + 3 = 78.$$

However, Soprunov and Soprunova show in [22] that $d(C_{P+Q}) = (q-1)^2 - 3(q-1) + 2$ for $q \geq 11$. Thus, $d(C_{P+Q}) = 72$.

CHAPTER V

SUMMARY AND CONCLUSIONS

We gave explicit formulas for the minimum distance of toric codes arising from smooth toric threefolds with $\mathrm{rank}(\mathrm{Pic}(X)) = 2$. All such threefolds arise from one of two families of 3-dimensional polytopes. For the families of polytopes with no interior lattice points, we chose specific polytopes and calculated the dimension and minimum distance of the corresponding toric codes. We then calculated the code parameters for families of polytopes that do contain interior lattice points. Based on our tables of values, these codes do not appear to be "better" than other known codes. That is, they do not yield higher minimum distance values for specific block length and dimension. However, based on their long block length and relatively small dimension, it would be beneficial to find constructive ways to restrict the zero set over which the codes are evaluated. This will effectively shorten the block length.

Lastly, we gave an explicit formula for the minimum distance of a toric code whose corresponding polytope is the Minkowski sum of an arbitrary polygon P in the xy-plane of $\mathbb{R}^3$ and an integral line segment in the direction of the z-axis. Of particular interest is the fact that this formula relies solely on $d(C_P)$ and the characteristic of the field. We also gave a simple upper bound on the minimum distance of a toric code whose corresponding polytope is the Minkowski sum of two arbitrary polytopes P and Q. We suspect this bound to be very close to the actual minimum distance, but not exact, when we place certain restrictions on P and Q.

REFERENCES

[1] D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics, 185, Springer, New York, 2005.

[2] G. Ewald, *Combinatorial Convexity and Algebraic Geometry*, Graduate Texts in Mathematics, 168, Springer-Verlag, New York, 1996.

[3] G. Ewald and A. Schmeinck, *Representation of the Hirzebruch-Kleinschmidt varieties by quadrics*, Beiträge Algebra Geom., 34 (1993), pp. 151-156.

[4] G. L. Feng and T. R. N. Rao, *Reflections on the "Decoding of algebraic-geometric codes up to the designed minimum distance,"* IEEE IT Newsletter, 45 (1), 1995.

[5] W. Fulton, *Introduction to Toric Varieties*, Princeton University Press, Princeton, NJ, 1993.

[6] M. Giulietti, *Notes on algebraic-geometric codes*, available online at http://www.math.kth.se/math/forskningsrapporter/Giulietti.pdf (2008).

[7] V. D. Goppa, *Codes on algebraic curves*, Sov. Math. Dokl. 24 (1981), pp. 170-172.

[8] M. Grassl, *Bounds on the minimum distance of linear codes*, available online at http://www.codetables.de. Accessed on 5 June 2008.

[9] J. Hansen, *Toric surfaces and error-correcting codes*, in Coding theory, Cryptogrphy, and Related Areas (Guanajuato, 1998), Springer, Berlin, 2000, pp. 132-142.

[10] J. Hansen, *Toric varieties, Hirzebruch surfaces and error-correcting codes*, Appl. Algebra Engrg. Comm. Comput., 13 (2002), pp. 289-300.

[11] S. H. Hansen, *Error-correcting codes from higher-dimensional varieties*, Finite Fields Appl., 7 (2001), pp. 530-552.

[12] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[13] D. Joyner, *Toric codes over finite fields*, Appl. Algebra Engrg. Comm. Comput., 15 (2004), pp. 63-79.

[14] J. Little and H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math., 20 (2006), pp. 999-1014.

[15] J. Little and R. Schwarz, *On toric codes and multivariate Vandermonde matrices*, Appl. Algebra in Engrg. Comm. Comput., 18 (2007), pp. 349-367.

[16] D. Ruano, *On the parameters of r-dimensional toric codes*, Finite Fields Appl., 13 (2007), pp. 962-976.

[17] D. Ruano, *On the structure of generalized toric codes*, preprint, 2006 (arXiv:cs.IT/0611010v1).

[18] H. Schenck, *Computational Algebraic Geometry*, London Mathematical Society student texts, 58, Cambridge University Press, Cambridge, UK, 2003.

[19] H. Schenck, *Lattice polygons and Green's theorem*, Proceedings of the American Mathematical Society, 132 (2004), pp. 3509-3512.

[20] C. E. Shannon, *A mathematical theory of communication*, Bell System Technical Journal, 27 (1948), pp. 379-423.

[21] I. Shafarevich, *Basic Algebraic Geometry 1: Varieties in Projective Space*, Springer-Verlag, Berlin, 1977.

[22] I. Soprunov and J. Soprunova, *Toric surface codes and Minkowski length of polygons*, preprint, 2008 (arXiv:0802.2088v1).

[23] M. A. Tsfasman, S. G. Vlădut, and T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr., 109 (1982), pp. 21-28.

VITA

James L. Kimball attended Louisiana College from June 1996 to May 2000 and received a Bachelor of Science in mathematics. From June 2000 to July 2002, he was the area manager for Acadiana Computer Systems, Inc. in Alexandria, Louisiana. He entered graduate school at Texas A&M University in August 2002 to study mathematics. In May 2004, he received his Master of Science in mathematics from Texas A&M University and immediately began work on his doctorate in mathematics. He completed his Ph.D. in mathematics at Texas A&M University under the supervision of his advisor Hal Schenck in August 2008.

James may be reached at J. Kimball, Department of Mathematics, Mailstop 3368, Texas A&M University, College Station, TX 77843-3368.