June 2007

Algebraic Geometric Codes on Anticanonical Surfaces

Jennifer A. Davis
University of Nebraska, Lincoln, jenniferdavis5@gmail.com

ALGEBRAIC GEOMETRIC CODES ON ANTICANONICAL SURFACES

by

Jennifer A. Davis

A DISSERTATION

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Doctor of Philosophy

Major: Mathematics

Under the Supervision of Professors Brian Harbourne and Judy Walker

Lincoln, Nebraska

June, 2007

ALGEBRAIC GEOMETRIC CODES ON ANTICANONICAL SURFACES

Jennifer A. Davis, Ph.D.

University of Nebraska, 2007

Advisors: Brian Harbourne and Judy Walker

Algebraic geometric codes (or AG codes) provide a way to correct errors that occur during the transmission of digital information. AG codes on curves have been studied extensively, but much less work has been done for AG codes on higher dimensional varieties. In particular, we seek good bounds for the minimum distance.

We study AG codes on anticanonical surfaces coming from blow-ups of $\mathbb{P}^2$ at points on a line and points on a conic. We can compute the dimension of such codes exactly due to known results. For certain families of these codes, we prove an exact result on the minimum distance. For other families, we obtain lower bounds on the minimum distance. We also investigate and obtain some results for codes on blow-ups of $\mathbb{P}^r$, where $r \geq 3$. We include tables of code parameters as well as Magma functions which can be used to generate the codes.

ACKNOWLEDGEMENTS

I would like to thank my advisors Brian Harbourne and Judy Walker. I thank Brain for countless hours spent explaining to me concepts in algebraic geometry and for his advice and support throughout my career at UNL. I thank Judy for providing helpful feedback on this dissertation; her suggestions helped make it understandable and interesting to a more general audience. I would like to thank the other members of my committee: Tom Marley, Mark Walker and Lance Perez. They are outstanding professors and taught me much of what I know about modern algebra and digital communications.

I am indebted to my fellow graduate students, whose mathematical camaraderie and friendship made the first few years of graduate school both manageable and enjoyable. I am particularly grateful to Suanne Au, Gargi Bhattacharyya, Kathy Bartley, Christina Eubanks-Turner, Heidi Feller, Mu-wan Huang, Joan Lubben, Livia Miller, Frank Moore, Dan Rezac and Erica Sanford. I thank Jon-Lark Kim, a former UNL postdoc, for introducing me to the field of coding theory. I am grateful to Mark Snavely, Aaron Trautwein and Erlan Wheeler, three excellent professors at Carthage College who introduced me to the intriguing field of discrete mathematics and encouraged me to consider graduate school.

The love and support of my family and friends have been empowering during the tough times in graduate school. I thank Steve and Vickie Everson, Lawrence Everson, Karissa Berg, Kristi Robertson, Anjela Tentis, Meredith White, Calvary Community Church and my friends in Monday night Bible study for their prayers and support. I am grateful to Lycan Davis, my best friend and fiancé, for being there through the ups and downs of writing a dissertation. Finally, I thank God for watching over me. I can always trust His plan, wherever it may lead. Jeremiah 29:11

Contents

Chapter 1

Introduction

Coding theory is the study of how to efficiently and reliably send information across a communications channel. A *linear code* C is a vector subspace of a finite dimensional vector space $\mathbb{F}^n$ over a finite field $\mathbb{F}$. If $k = \dim C$ and $q = |\mathbb{F}|$, we say C is a *q-ary* code of *length* n and *dimension* k. The *Hamming distance* between two codewords is the number of coordinate positions in which they differ. An important parameter of a linear code is the *minimum distance* d, which is equal to the smallest Hamming distance among all pairs of distinct codewords in the code. A linear code with minimum distance d can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ bit errors that occur during transmission; so the larger d is, the more errors the code can correct. In classical coding theory one seeks to find codes with large minimum distance d relative to the length and dimension of the code. Computing the parameter d is, in general, NP-hard [34].

In 1981, V.D. Goppa introduced algebraic geometric (AG) codes [8]. Goppa's codes were obtained by evaluating functions at points on algebraic curves. Some of these codes have very good parameters. In fact, in 1982, Tsfasman, Vlăduţ and Zink [33] demonstrated a family of curves yielding AG codes with minimum distance greater than that given by the well-known Varshamov-Gilbert Bound on a certain interval. The AG code construction is easily generalized to points on other algebraic varieties, although much less is known about such codes and the parameters k and d are often difficult to compute.

In [10], J. P. Hansen obtained some exact results and bounds on the dimension and minimum distance for AG codes on toric surfaces. Rational anticanonical surfaces preserve many of the nice properties of toric surfaces and are more general. In particular, a smooth projective toric surface is always a rational anticanonical surface but not vice versa. In this dissertation, we study AG codes on anticanonical surfaces coming from blow-ups of $\mathbb{P}^2$ at points on a line and points on a conic; we call these codes *anticanonical surface codes.*

Chapters 2 and 3 cover the necessary background material for understanding blow-ups of $\mathbb{P}^2$, anticanonical surfaces and the fundamentals of coding theory. In Chapter 4, we investigate various families of anticanonical surface codes. In Section 4.1, we compute the dimension and a lower bound on the minimum distance for codes whose corresponding divisor class is numerically effective. In Sections 4.2 and 4.3 we obtain an exact result for d for three families of codes. In Section 4.5, we obtain a lower bound on d in terms of the minimum distances of codes whose divisor classes sum to that of the original code. In Chapter 5, we obtain some results for codes on varieties of dimension greater than two; namely, on blow-ups of $\mathbb{P}^r$, where $r \geq 3$. In Appendix A, we give tables of code parameters for certain families of anticanonical surface codes. Appendix B contains Magma functions which can be used to generate the results in Appendix A.

Chapter 2

Algebraic Geometry Background

2.1 Basic Definitions and Theorems

We begin with some basic definitions. Our main source is [17]. Let k be an algebraically closed field. By *projective variety* we mean a closed, irreducible subset of $\mathbb{P}^n$. A *quasi-projective variety* is an open subset of a projective variety. Sometimes we use the notation $\mathbb{P}^n(k)$ to emphasize the field we are working over.

Definition 2.1.1. Let $Y \subset \mathbb{P}^n$ be a quasi-projective variety. A function $f : Y \to k$ is *regular at a point* $P \in Y$ if there is an open neighborhood U with $P \in U \subseteq Y$, and homogeneous polynomials $g, h \in S = k[x_0, ..., x_n]$, of the same degree, such that h is nowhere zero on U, and $f = g/h$ on U. For any subset V of Y, we say that f is *regular on* V if it is regular at every point of V.

Definition 2.1.2. The *function field* $k(Y)$ of Y is defined as follows: an element of $k(Y)$ is an equivalence class of pairs $\langle U, f\rangle$ where U is a nonempty open subset of Y and f is a regular function on U, and where we identify two pairs $\langle U, f\rangle$ and $\langle V, g\rangle$ if $f = g$ on $U \cap V$. The elements of $k(Y)$ are called *rational functions* on Y.

Definition 2.1.3. A *morphism* $\phi : X \to Y$ of quasi-projective varieties is a continuous map such that for every open set $V \subseteq Y$, and for every regular function $f : V \to k$, the function $f \circ \phi : \phi^{-1}(V) \to k$ is regular.

Next we define a rational map, which is more general than a rational function. In fact, a rational function is just a rational map to the field k.

Definition 2.1.4. A *rational map* $\phi : X \to Y$ is an equivalence class of pairs $\langle U, \phi_U \rangle$ where U is a nonempty open subset of X and ϕ_U is a morphism from U to Y, and where $\langle U, \phi_U \rangle$ and $\langle V, \phi_V \rangle$ are equivalent if ϕ_U and ϕ_V agree on $U \cap V$.

Definition 2.1.5. A *birational map* $\phi : X \to Y$ is a rational map which admits an inverse. If there is a birational map from X to Y, we say that X and Y are *birationally equivalent* or simply *birational*.

The following fact is Corollary I.4.5 in [17].

Proposition 2.1.6. *Let X and Y be quasi-projective varieties. Then X and Y are birational if and only if $k(X) \cong k(Y)$ as k-algebras.*

By *curve* we mean a smooth (see [17]), projective variety of dimension 1. Similarly, by *surface* we mean a smooth, projective variety of dimension 2. In this dissertation we will work with a blow-up of projective space at a finite set of points; the resulting projective variety is always smooth. A *rational surface* is a surface which is birational to $\mathbb{P}^2$.

2.2 Divisors and the Riemann-Roch Theorem

Throughout this section we work on a smooth projective variety X. For the development and definitions in this section, we refer to [2], [17] and [37].

Definition 2.2.1. Let $\mathrm{Div}(X)$ denote the free abelian group generated by all irreducible subvarieties of X of codimension 1. We define a *divisor* to be an element of $\mathrm{Div}(X)$; so we can write a divisor D as $D = \sum n_i D_i$, where the n_i are integers and the D_i are irreducible subvarieties of codimension 1. The *support* of the divisor $D = \sum n_i D_i$ is $\operatorname{supp} D = \{D_i | n_i \neq 0\}$. We say that $D = \sum n_i D_i$ is *effective* if $n_i \geq 0$ for all i, and in this case we write $D \geq 0$.

Definition 2.2.2. Let X be a smooth, projective, absolutely irreducible curve defined over the finite field $\mathbb{F}_q$. A *point of degree n* on X over $\mathbb{F}_q$ is a set $P = \{P_0, ..., P_{n-1}\}$ of n distinct points in $X(\mathbb{F}_{q^n})$ such that $P_i = \sigma^i_{q,n}(P_0)$ for $i = 1, ..., n-1$, where $\sigma_{q,n}$ is the Frobenius map. The Frobenius map acts on $X(\mathbb{F}_q)$, i.e., the $\mathbb{F}_q$-points of X, via $\sigma_{q,n}((a_0 : a_1 : a_2)) = (a_0^q : a_1^q : a_2^q)$.

Note that a point of degree n on a curve X is an irreducible (over $\mathbb{F}_q$) subvariety of dimension 0 (and hence of codimension 1). Thus a divisor on a curve is just a sum of points of arbitrary degree. If $D = \sum n_i D_i$ is an $\mathbb{F}_q$-divisor on a curve X, we say the *degree* of D is $\deg D = \sum n_i(\deg D_i)$. A divisor on a surface is a sum of curves. We now briefly recall the theory needed to define $\mathrm{Cl}(X)$ and $\mathrm{Pic}(X)$. For further details, see [17].

Definition 2.2.3. We say two divisors D and D' on X are *linearly equivalent* if $D - D'$ is a principal divisor, i.e., if $D - D' = \mathrm{div}(f)$, for some rational function f. The *divisor class group* of X, denoted $\mathrm{Cl}(X)$, is given by the group $\mathrm{Div}(X)$ modulo linear equivalence. We denote an element of $\mathrm{Cl}(X)$ by $[D]$, where $D \in \mathrm{Div}(X)$. The *Picard group* of X, denoted $\mathrm{Pic}(X)$, is the group of isomorphism classes of line bundles (or, equivalently, of invertible sheaves) on X.

Remark. The groups $\mathrm{Cl}(X)$ and $\mathrm{Pic}(X)$ can be quite complicated; but for the varieties we will work with, they are free abelian groups of finite rank. In Section 2.3 we give an explicit basis for $\mathrm{Pic}(X)$ when X is a blow-up of projective space at a finite set of points.

By Corollary II.6.16 of [17], there is a natural isomorphism between $\mathrm{Cl}(X)$ and $\mathrm{Pic}(X)$.

Definition 2.2.4. We say that a divisor class $[D] \in \mathrm{Cl}(X)$ is *effective* if it is the linear equivalence class of an effective divisor.

The definition of *anticanonical divisor* takes some development. We briefly recall the theory here. In Section 2.3, we give the class of the anticanonical divisor explicitly in terms of the basis for $\mathrm{Pic}(X)$ when X is a blow-up of $\mathbb{P}^2$ at a finite set of points. For a more detailed definition of canonical sheaf, see Section II.8 of [17]. Also, see [17] or [20] for details regarding the exterior algebra and nth exterior power.

Definition 2.2.5. Let X be an n-dimensional smooth variety over k. Let T_X^* be the cotangent bundle of X, i.e., the dual of the tangent bundle T_X. We define the *canonical line bundle* ω_X of X to be $\omega_X = \bigwedge^n T_X^*$, the nth exterior power of the cotangent bundle.

Definition 2.2.6. Any divisor K_X in the linear equivalence class corresponding to ω_X is called a *canonical divisor*. A divisor of the form $-K_X$ is called an *anticanonical divisor*. By abuse of notation, we often use $-K_X$ and $[-K_X]$ interchangeably, so we sometimes refer to $-K_X$ as *the* anticanonical divisor since the anticanonical divisor *class* is, in fact, unique.

Definition 2.2.7. An *anticanonical* variety is a variety which has an effective anticanonical divisor.

Definition 2.2.8. Let D be a divisor on a smooth variety X, where D and X are defined over a finite field $\mathbb{F}_q$. The *space of rational functions associated to D* is the vector subspace

$$L(D) := \{f \in \mathbb{F}_q(X) | \operatorname{div}(f) + D \geq 0\} \cup \{0\}$$

of the function field $\mathbb{F}_q(X)$.

A very useful theorem in algebraic geometry is the theorem of Riemann-Roch. We give two statements of the theorem here. The first is for a smooth, projective, absolutely irreducible curve and the second is for a smooth, projective, rational surface. See Sections IV.1 and V.1 of [17] for more details. We state the theorems here over a finite field $\mathbb{F}_q$. The dimension of $L(D)$ over the field $\mathbb{F}_q$ is equal to its dimension over the algebraic closure $\overline{\mathbb{F}_q}$, since tensoring by a field extension is exact and hence commutes with cohomology (see the proof of III.12.2 in [17] and the paragraph before Corollary 4.5 in [30]).

Recall that $H^0(X, \mathcal{O}_X(D))$ is the group of global sections of the line bundle $\mathcal{O}_X(D)$. We can also define groups $H^i(X, \mathcal{O}_X(D))$ for $i > 0$ in a standard cohomological way (see [17] for details). We let $h^i(X, \mathcal{O}_X(D))$ denote the dimension of $H^i(X, \mathcal{O}_X(D))$ for $i \geq 0$. For convenience, we write $h^i(X, D)$ for $h^i(X, \mathcal{O}_X(D))$.

Theorem 2.2.9 (Riemann-Roch for Smooth Curves)**.** *Let X be a smooth, projective, absolutely irreducible curve of genus g defined over a finite field $\mathbb{F}_q$ and let D be an $\mathbb{F}_q$-divisor on X. Then* $\dim L(D) - h^1(X, D) = \deg D + 1 - g$. *Furthermore, if* $\deg D > 2g - 2$, *then*

$$\dim L(D) = \deg D + 1 - g.$$

Theorem 2.2.10 (Riemann-Roch for Rational Surfaces)**.** *Let X be a smooth, projective, rational surface defined over the field $\mathbb{F}_q$ and let D be an $\mathbb{F}_q$-divisor on X. Then* $\dim L(D) - h^1(X, D) + h^2(X, D) = (D^2 - K_X \cdot D)/2 + 1$, *where K_X is the canonical* *divisor. Furthermore, if D is effective, then $h^2(X, D) = 0$ and so*

$$\dim L(D) - h^1(X, D) = (D^2 - K_X \cdot D)/2 + 1.$$

The "furthermore" clause of the previous theorem is Lemma 2(b) of [13].

2.3 Blowing-up of a Point and its Properties

Definition 2.3.1. Let $x_1, ..., x_n$ be affine coordinates of affine n-space, denoted $\mathbb{A}^n$. Let $y_1, ..., y_n$ be homogeneous coordinates of $\mathbb{P}^{n-1}$. Let $O = (0, ..., 0)$ be the origin in $\mathbb{A}^n$. Then the *blowing-up of* $\mathbb{A}^n$ *at the point* O is the closed subset X of $\mathbb{A}^n \times \mathbb{P}^{n-1}$ defined by the equations $\{x_i y_j = x_j y_i | i, j = 1, ..., n\}$. There is a natural morphism $\pi : X \to \mathbb{A}^n$, called the *blow-up morphism*, obtained by restricting the projection map $\mathbb{A}^n \times \mathbb{P}^{n-1} \to \mathbb{A}^n$ to X:

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[dr, "\pi"'] & \mathbb{A}^n \times \mathbb{P}^{n-1} \arrow[d] \\
 & \mathbb{A}^n
\end{tikzcd}$$

The blowing-up X of $\mathbb{A}^n$ at the point O has four important properties. For the proofs, see p. 28-29 of [17].

1. If $p \in \mathbb{A}^n$, $p \neq O$, then $\pi^{-1}(p)$ consists of a single point. In fact, π gives an isomorphism of $X - \pi^{-1}(O)$ onto $\mathbb{A}^n - O$.

2. $\pi^{-1}(O) \cong \mathbb{P}^{n-1}$

3. The points of $\pi^{-1}(O)$ are in 1-1 correspondence with the set of lines through O in $\mathbb{A}^n$.

4. X is irreducible.

We now define the blowing-up of a point on a closed subvariety of $\mathbb{A}^n$.

Definition 2.3.2. Let Y be a closed subvariety of $\mathbb{A}^n$ passing through O. Let $\pi : X \to \mathbb{A}^n$ be the morphism for the blowing-up of $\mathbb{A}^n$ at the point O. We define the *blowing-up of* Y *at the point* O to be $\widetilde{Y} = \overline{\pi^{-1}(Y - O)}$, i.e., $\widetilde{Y}$ is the closure of $\pi^{-1}(Y - O)$ in X. We denote also by $\pi : \widetilde{Y} \to Y$ the morphism obtained by restricting $\pi : X \to \mathbb{A}^n$ to $\widetilde{Y}$. To blow up at a point $p \in \mathbb{A}^n$ other than O, choose coordinates $x_1, ..., x_n$ on $\mathbb{A}^n$ such that p is the origin. We sometimes refer to $\widetilde{Y}$ as the *blow-up* of Y at the point p.

Let S be a smooth projective variety. Let $X_b \overset{\pi_b}{\to} X_{b-1} \overset{\pi_{b-1}}{\to} \cdots \overset{\pi_1}{\to} X_0 = S$ be a sequence of blow-ups $\pi_i : X_i \to X_{i-1}$ at points $p_i \in X_{i-1}$. By composition, we have morphisms $\Pi_{i,j} = \pi_i \cdots \pi_j : X_j \to X_{i-1}$ for $i < j$. Let $E_1, ..., E_b$ be the divisors $\Pi_{i,b}^{-1}(p_i)$ on X_b.

Definition 2.3.3. We say that the point p_j is *infinitely near* p_i if $p_j \in \Pi_{i,j}^{-1}(p_i)$.

By Exercise II.8.5(a) of [17], the groups $\text{Pic}(X)$ and $\text{Pic}(S) \oplus [E_1]\mathbb{Z} \oplus \cdots \oplus [E_b]\mathbb{Z}$ are isomorphic. Thus a basis for $\text{Pic}(X)$ is given by a basis for $\text{Pic}(S)$ together with the classes $[E_1], ..., [E_b]$ of the line bundles corresponding to $E_1, \ldots, E_b$.

Now let $\mathcal{B} = \{p_1, ..., p_b\} \subset \mathbb{P}^n$ and let $\pi : \mathbb{P}^n_{\mathcal{B}} \to \mathbb{P}^n$ be given by the sequential blowing up of the points of $\mathcal{B}$. By Proposition II.6.4(c) of [17], we know $\text{Pic}(\mathbb{P}^n) = [H]\mathbb{Z}$, where $[H]$ is the class of a general hyperplane in $\mathbb{P}^n$. If $n = 2$, we will use L, for line, instead of H. Thus, a basis for $\text{Pic}(\mathbb{P}^n_{\mathcal{B}})$ is given by $[H]$ together with the classes of the line bundles $[E_i]$ corresponding to $E_1, \ldots, E_b$.

If $n = 2$, we also have an intersection product on $\text{Pic}(\mathbb{P}^2_{\mathcal{B}})$ induced by the rules $[L] \cdot [L] = 1$, $[E_i] \cdot [E_i] = -1$, $[E_i] \cdot [L] = 0$ and $[E_i] \cdot [E_j] = 0$ for $i \neq j$. See Theorem V.1.1, Example V.1.4.1, Example V.1.4.2 and Proposition V.3.1 of [17] for details.

Definition 2.3.4. We say a divisor class $[D] \in \mathrm{Pic}(\mathbb{P}^2_{\mathcal{B}})$ is *numerically effective* if $[D] \cdot [G] \geq 0$ for every effective class $[G] \in \mathrm{Pic}(\mathbb{P}^2_{\mathcal{B}})$. We say that a divisor D is *numerically effective* whenever its class $[D]$ is numerically effective.

Remark. To each effective divisor D there is an associated numerically effective and effective divisor D' such that $D - D'$ is effective and $L(D) = L(D')$. The divisor D' is given by subtracting off all reduced, irreducible curves C that meet D negatively, since any such curve C is a component of every element of the linear system $|D|$ of effective divisors with class $[D]$.

We can determine the anticanonical divisor of a blow-up using Proposition V.3.3 of [17], which we now state:

Proposition 2.3.5. *If X and S are smooth projective surfaces and if $\pi : X \to S$ is the morphism obtained by blowing up a point of S, then $K_X = \pi^*(K_S) + E_p$, where $E_p = \pi^{-1}(p)$ and π^* is the natural map $\pi^* : \mathrm{Pic}(S) \to \mathrm{Pic}(X)$.*

By Example II.8.20.1 of [17], $[K] = [-3L]$ for $\mathbb{P}^2$. Then, by Proposition 2.3.5, we have that the class of the canonical divisor on $\mathbb{P}^2_{\mathcal{B}}$ is $[K] = [-3L + E_1 + \cdots + E_b]$. Note that $[-K] = [3L - E_1 - \cdots - E_b]$ is effective if and only if the points $p_1, ..., p_b$ lie on a curve of degree 3 or less in $\mathbb{P}^2$. Thus $\mathbb{P}^2_{\mathcal{B}}$ is anticanonical if and only if the points of $\mathcal{B}$ lie on a cubic curve.

By Proposition I.5.2 of [12], one can easily show that if $\mathcal{B}$ is contained in a single line in $\mathbb{P}^2$ then the divisor class $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ is numerically effective if and only if $m, m_1, ..., m_b \geq 0$ and $m \geq \sum_{i=1}^{b} m_i$. Similarly, by Proposition I.5.3 of [12], if the points of $\mathcal{B}$ are contained in two lines, say L_1 and L_2, in $\mathbb{P}^2$, then the divisor class $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ with $m_1 \geq m_2 \geq \cdots \geq m_b \geq 0$ is numerically effective if and only if the following conditions hold:

(i) $m - m_1 - m_2 \geq 0$

(ii) $m \geq \sum_{p_i \in L_1 \cap \mathcal{B}} m_i$ and

(iii) $m \geq \sum_{p_i \in L_2 \cap \mathcal{B}} m_i$.

By Lemma 3.1.1(b) of [15], if the points of $\mathcal{B}$ are contained in a conic (i.e., a curve of degree two) in $\mathbb{P}^2$ and if $[D]$ is numerically effective, then $[D]$ is effective and $h^1(X, D) = 0$. Hence, in this case, by Riemann-Roch for Rational Surfaces (Theorem 2.2.9), we have that

$$\dim L(D) = (D^2 - K_X \cdot D)/2 + 1.$$

One can then verify that if $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$, then

$$\dim L(D) = \binom{m+2}{2} - \sum_{i=1}^{b} \binom{m_i+1}{2}.$$

Remark. The results of [15] are for an algebraically closed field. In this dissertation, we will be working over a finite field $\mathbb{F}_q$. If the points of $\mathcal{B}$ have coordinates in $\mathbb{F}_q$ and if D is an $\mathbb{F}_q$-divisor, then when computing a basis for $L(D)$, whether over $\mathbb{F}_q$ or over the algebraic closure $\overline{\mathbb{F}_q}$, all of the computations will be over $\mathbb{F}_q$. Hence a basis of $L(D)$ over $\mathbb{F}_q$ is also a basis over $\overline{\mathbb{F}_q}$. Thus we can still use the results of [15] (see also the paragraph before Corollary 4.5 in [30]).

The next proposition holds by Corollary V.5.4 of [17].

Proposition 2.3.6. *Any birational morphism $X \to S$ of smooth surfaces factors as a sequence of blow-up morphisms $X = X_b \overset{\pi_b}{\to} X_{b-1} \overset{\pi_{b-1}}{\to} \cdots \overset{\pi_1}{\to} X_0 = S$, where X_i is a smooth surface for $i = 1, ..., b$.*

2.4 Fat Point Subschemes of Projective Space

In Section 2.3, we computed $\dim L(D)$ for a numerically effective divisor D when $\mathcal{B}$ is contained in a conic. In this section we recall a recursive formula (based on the results of [6] and [5]) to compute $\dim L(D)$ for certain divisors D on $\mathbb{P}^n_{\mathcal{B}}$ with $n \geq 2$. We will use this formula in Chapter 5 to compute the dimension of (or to find bounds on the dimension of) some codes on $\mathbb{P}^n_{\mathcal{B}}$. Throughout this section k is any field.

Definition 2.4.1. Let $f \neq 0$ be a homogeneous polynomial in $R = k[x_0, \ldots, x_n]$ and let $p \in \mathbb{P}^n(k)$. Let h be the image of the function f under the linear change of coordinates which moves p to the point $(0 : \cdots : 0 : 1)$. We say f has a *zero of multiplicity at least* t at the point p if $h(x_0, x_1, ..., x_{n-1}, 1)$ has no terms of degree less than t.

Given a set of points $\mathcal{B} = \{p_1, ..., p_b\} \subset \mathbb{P}^n(k)$ and positive integers $m_1, ..., m_b$, let Z denote the formal sum $m_1p_1 + \cdots + m_bp_b$, and let $I(Z)$ denote the ideal in $R = k[x_0, \ldots, x_n]$ generated by all homogeneous polynomials with a zero of multiplicity at least m_i at each $p_i \in \mathcal{B}$. It is convenient to allow the multiplicities m_i to be zero, but these do not affect the ideal since every polynomial vanishes with multiplicity at least 0 at every point. We refer to the set of points $\{p_i : m_i > 0\}$ as the *support* of Z. The ideal $I(Z)$ defines a closed 0-dimensional subscheme which topologically is just the set of points $p_1, \ldots, p_b$, but which is reduced if and only if $m_i = 1$ for each i. We use Z to denote this subscheme since the subscheme is completely determined by the points of $\mathcal{B}$ and the integers $m_1, ..., m_b$. A *fat point subscheme* is any subscheme defined in this way. (The word *fat* refers to the fact that the subscheme need not be reduced.)

Let $I(Z)_m$ denote the homogeneous component of $I(Z)$ of degree m. This is the k-vector space spanned by all homogeneous polynomials $F \in R$ of degree m in

$I(Z)$. This vector space is canonically isomorphic to $H^0(X, D)$, where $X = \mathbb{P}^n_{\mathcal{B}}$ is the sequential blowing-up of $\mathbb{P}^n$ at the points of $\mathcal{B}$ and $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$, where H is a hyperplane.

When $n = 2$, we can use the results in Section 2.3 to compute $\dim L(D) = h^0(X, D)$, at least when D is numerically effective and $\mathcal{B}$ is contained in a conic. We now recall an alternate approach (see [6] and [5]) for $\mathcal{B}$ contained in a hyperplane.

Given any homogeneous polynomial $F \in R$ of degree m, we can write $F = F_0 + x_nF_1 + \cdots + x_n^mF_m \in (k[x_0, ..., x_{n-1}])[x_n]$, where each F_i is homogeneous of degree $m - i$ and doesn't involve x_n, so that the coefficients F_i are uniquely determined. Now assume that the points of $\mathcal{B}$ all lie in the hyperplane defined by $x_n = 0$.

Claim 1: If $F = F_0 + x_nF_1 + \cdots + x_n^mF_m \in I(Z)_m$, then $F_0 \in I(Z)_m$.

Proof. We just need to show that F_0 vanishes with multiplicity at least m_i at each p_i. Since the nth coordinate of p_i is already 0 by the hypothesis that p_i is in the hyperplane $x_n = 0$, to check the multiplicity of F_0 at each p_i, we can do a linear change of coordinates that takes a given p_i to $(1 : 0 : \cdots : 0)$, and which involves only $x_0, \ldots, x_{n-1}$. This change of variables converts F to a polynomial G. Let F_j^* be the result of applying the same change of coordinates to F_j. Since our coordinate change did not involve x_n, we have $G_j = F_j^*$ for each j, where $G_1, ..., G_m$ give the canonical decomposition $G = G_0 + x_nG_1 + \cdots + x_n^mG_m$ of G as a polynomial in x_n with coefficients in $k[x_0, \ldots, x_{n-1}]$. Since F has multiplicity at least m_i at p_i, we know that no monomial term of $G(1, x_1, \ldots, x_n)$ has degree less than m_i. Thus each term of $G_0(1, x_1, \ldots, x_n)$, and hence of $F_0^*(1, x_1, \ldots, x_n)$, has degree at least m_i; so $F_0 \in I(Z)_m$, as claimed. □

Now let $Z^{(i)}$ denote the subscheme $(m_1 - i)_+p_1 + \cdots + (m_b - i)_+p_b$ where $(m_j - i)_+$ is the maximum of $m_j - i$ and 0, so that $Z^{(i)}$ is the result of reducing each multiplicity of Z by i but never making it less than 0.

Claim 2: We have $F = F_0 + x_n F_1 + \cdots + x_n^m F_m \in I(Z)_m$ if and only if $F_i \in I(Z^{(i)})_{m-i}$ for $0 \leq i \leq m$.

Proof. If $F_i \in I(Z^{(i)})_{m-i}$ for $0 \leq i \leq m$, then clearly $x_n^i F_i \in I(Z)_m$ for each i, hence $F \in I(Z)_m$. Conversely, say $F \in I(Z)_m$. Then $F_0 \in I(Z)_m$, but $Z^{(0)} = Z$, so $F_0 \in I(Z^{(0)})_m$. Also, $F - F_0 = x_n F_1 + \cdots + x_n^m F_m \in I(Z)_m$. Hence, dividing out a factor of x_n, we have $F_1 + \cdots + x_n^{m-1} F_m \in I(Z^{(1)})_{m-1}$. So now, as for F_0, we have $F_1 \in I(Z^{(1)})_{m-1}$. Continuing in this way gives $F_i \in I(Z^{(i)})_{m-i}$ for $0 \leq i \leq m$. □

Given any fat point subscheme $Z = m_1 p_1 + \cdots + m_b p_b \subset \mathbb{P}^n$ whose support lies in a hyperplane H, let Z' denote the fat point subscheme $Z \cap H$ regarded as a subscheme of $H = \mathbb{P}^{n-1}$; i.e., $Z' = m_1 p_1 + \cdots + m_b p_b \subset \mathbb{P}^{n-1}$. Then Claim 2 really just says:

Corollary 2.4.2. $I(Z)_m = \oplus_{0 \leq i \leq m} x_n^i I(Z^{(i)'})_{m-i}$

Thus computing $h^0(X, D)$ and finding a basis of $H^0(X, D)$ is equivalent to computing the dimension of and finding a vector space basis for $I(Z)_m$, which reduces to doing so for $I(Z^{(i)'})_{m-i}$ for each i. In the case where the points of $\mathcal{B}$ lie on a line in $\mathbb{P}^n$, finding a vector space basis for $I(Z^{(i)'})_{m-i}$ eventually reduces to the case of fat points in $\mathbb{P}^1$.

Suppose $Z = m_1 p_1 + \cdots + m_b p_b \subset \mathbb{P}^1$. Choose coordinates such that x_0 does not vanish at any point of $\mathcal{B}$. Then we can write $p_i = (1 : a_i)$ for $i = 1, ..., b$. Let $F = (x_1 - a_1 x_0)^{m_1} \cdots (x_1 - a_b x_0)^{m_r}$. If $m < m_1 + \cdots + m_b$, then $I(Z)_m = (0)$. If $m \geq m_1 + \cdots + m_b$, then a basis for $I(Z)_m$ is given by

$$\{F \cdot f : f \text{ is a monomial of degree } m - (m_1 + \cdots + m_b)\}.$$

Thus when the points of $\mathcal{B}$ lie on a line in $\mathbb{P}^n_{\mathcal{B}}$, we can easily compute $h^0(X, D)$.

2.5 Justification for Studying $\mathbb{P}^2_{\mathcal{B}}$

The purpose of this section is to show that studying $\mathbb{P}^2_{\mathcal{B}}$ is a reasonable thing to do for the initial research on anticanonical surface codes. Not every smooth, rational, anticanonical surface is obtained by blowing up points of $\mathbb{P}^2$. However, we will show in Proposition 2.5.2 that for any smooth, rational, anticanonical surface X there is a birational morphism $Y \to X$ where Y is anticanonical and has a birational morphism (not just a birational map) $Y \to \mathbb{P}^2$, i.e., Y is a sequential blowing-up of $\mathbb{P}^2$ at some set of points $\mathcal{B} = \{p_1, ..., p_b\}$. Thus, after blowing up some additional points of X (if necessary), any anticanonical surface X becomes an anticanonical surface which is a blow-up of $\mathbb{P}^2$.

A *Hirzebruch surface* is a $\mathbb{P}^1$-bundle over $\mathbb{P}^1$. A fiber F of the $\mathbb{P}^1$-bundle satisfies $F^2 = 0$. Each Hirzebruch surface has a section B with $B^2 = -n$ for a unique n with $n \geq 0$. Any two such Hirzebruch surfaces are isomorphic and denoted by H_n. By Lemma V.2.10 of [17], $[-K_{H_n}] = [2B+(n+2)F]$ and $[-K_{H_n}]\cdot[B] = 2-n$. In particular, $-K_{H_n}$ is effective and always has B as its component of least self-intersection (see Section V.2 of [17] for further details).

The surfaces $\mathbb{P}^2$, H_0, H_2, H_3,... are *relatively minimal models.* That is, every smooth, rational, projective surface X has a birational morphism either to H_n for some $n \neq 1$ or to $\mathbb{P}^2$. If X is either $\mathbb{P}^2$ or H_n for some $n \neq 1$, then any birational morphism from X to a smooth rational projective surface Y is an isomorphism. For more details, see [17].

We use a theorem of Castelnuovo to define the blowing-down of a curve C on a surface X (see Theorem V.5.7 of [17]).

Theorem 2.5.1 (Castelnuovo)**.** *If C is a curve on a smooth surface X with $C \cong \mathbb{P}^1$ and $C^2 = -1$, then there exists a morphism $\pi : X \to X_0$ to a smooth projective* *surface X_0, and a point $p \in X_0$, such that X is isomorphic via π to the blowing-up of X_0 at p, and C is the curve $\pi^{-1}(p)$. We call such a map π the* blowing-down *of C or, equivalently, the blowing-up of the point p.*

Blowing up a point $p \in H_n$ and then blowing down the proper transform $\pi^{-1}(F_p) - E_p$ of the fiber F_p through p is called an *elementary transformation.* An elementary transformation gives a birational transformation from H_n to H_m, where $m = n+1$ if $p \in B$ and where $m = n-1$ otherwise. By blowing-up p one obtains a surface Y and a birational morphism $Y \to H_n$. By Castelnuovo's Theorem (Theorem 2.5.1), F_p contracts to a smooth point. By blowing down $F_p \subset Y$ one obtains another birational morphism $Y \to X$ to some X. Thus both $\text{Pic}(X)$ and $\text{Pic}(H_n)$ are subgroups of $\text{Pic}(Y)$.

We know $\text{Pic}(H_n) = [B]\mathbb{Z} \oplus [F]\mathbb{Z}$ by Proposition V.2.3 of [17]. Then $\text{Pic}(Y) = [B]\mathbb{Z} \oplus [F]\mathbb{Z} \oplus [E_p]\mathbb{Z}$ by Proposition V.3.2 of [17] and the discussion in Section 2.3. Now we can determine $\text{Pic}(X)$ as a subgroup of $\text{Pic}(Y)$. If $p \in B$, $\text{Pic}(X)$ is spanned in $\text{Pic}(Y)$ by $[B - E_p]$ and $[F]$. If $p \notin B$, then $\text{Pic}(X)$ is spanned by $[B + F - E_p]$ and $[F]$. Using $[F]$ on X, one can verify that X is a ruled surface (i.e., a surface whose function field is of a product $\mathbb{P}^1 \times C$, where C is a curve). Also, using the basis for $\text{Pic}(X)$ described above, one can show that X has at most one irreducible subvariety of codimension 1 with negative self-intersection. The self-intersection of this negative curve determines the m for which $X = H_m$.

Proposition 2.5.2. *Let X be a smooth, rational surface. Then there is a birational morphism $Y \to X$ (hence Y is obtained by blowing-up points on X, possibly infinitely near) such that Y has a birational morphism $Y \to \mathbb{P}^2$. If X is anticanonical, then Y can also be chosen to be anticanonical.*

Proof. If there is a birational morphism $X \to \mathbb{P}^2$, take $Y = X$. If not, then let $X \to H_n$ be a birational morphism, which we know exists with $n \neq 1$ by Theorem V.5.8 of [17]. Let $[B], [F], [E_1], \ldots, [E_b]$ be the basis of $\mathrm{Pic}(X)$ corresponding to the morphism $X \to H_n$ (see Proposition 2.3.6 and the discussion in Section 2.3).

If $n = 0$ and $b > 0$, then X already has a birational morphism to $\mathbb{P}^2$ given by $\pi_2 \cdots \pi_b$, where π_i is defined as in Proposition 2.3.6. If $n = 0$ and $b = 0$, then $X = H_0$ and we can blow up any point of X to get Y. Then Y has a birational morphism to $\mathbb{P}^2$ given by $Y \to H_1 \to \mathbb{P}^2$ (see p.87 of [29] and Proposition 3 of [25]).

Now we can assume that $n > 1$. Pick a point p not on $B \cup E_1 \cup \cdots \cup E_b$. Let Y be the surface obtained by blowing-up p and let $E_p = \pi^{-1}(p)$ be the curve obtained by blowing-up p. The blow-up morphism gives us the birational morphism $Y \to X$. But now Y blows down to H_{n-1} by contracting $E_1, \ldots, E_b$ and $F - E_p$. (This is the same as blowing X down to H_n, then doing the elementary transformation given by blowing up p on H_n and then contracting $F - E_p$.) Thus by picking a point p which avoids a finite number of curves on X, we obtain $Y \to H_{n-1}$. We see that by picking points $p_1, \ldots, p_{n-1}$ avoiding a finite number of curves on X, blowing up all of the points p_i gives a birational morphism $Y \to X$, from which by iteration we get a birational morphism $Y \to H_1$. We can compose this with $H_1 \to \mathbb{P}^2$ to get the desired birational morphism $Y \to \mathbb{P}^2$.

To show that Y can be chosen to be anticanonical if X is, we just have to show that no effective anticanonical divisor on X is supported on $B \cup E_1 \cup \cdots \cup E_b$. Then we can choose our first point $p = p_1$ to avoid $B \cup E_1 \cup \cdots \cup E_b$ yet still be on the anticanonical divisor on X. Then $-K_{Y'} = \pi^*(-K_X) - E_p$ by Proposition 2.3.5, where Y' is obtained from X by blowing up p. Furthermore, $-K_{Y'}$ is effective since p is on $-K_X$, and so Y' is anticanonical. We choose $p_2, \ldots, p_b$ similarly so that the final Y is also anticanonical.

To see that no effective anticanonical divisor $-K_X$ on X is supported on $B \cup E_2 \cup \cdots \cup E_b$, recall that we have a birational morphism $X \rightarrow H_n$ for some n, so any effective anticanonical divisor on X contains the proper transform of some effective anticanonical divisor K_{H_n} on H_n. The only way the support of this proper transform could be contained in $B \cup E_1 \cup \cdots \cup E_b$ is if K_{H_n} were supported on B, which would mean that $-K_{H_n}$ is a multiple of B, which is never the case, since $[-K_{H_n}] = [2B + (n+2)F]$ by Lemma V.2.10 of [17]. This completes the proof. □

Remark. If our field k is the algebraic closure of some finite field $\mathbb{F}_q$ and X is defined over $\mathbb{F}_q$, then $Y \rightarrow X$ and $Y \rightarrow \mathbb{P}^2$ are defined over some finite extension of $\mathbb{F}_q$, if not over $\mathbb{F}_q$ itself.

2.6 Toric Varieties and Polytopes

We begin with the definitions of torus and toric variety given by Fulton in [7]. We give these definitions for context; we only need to know the lattice polygon corresponding to a (smooth, complete) toric surface to construct the corresponding code (see Sections 2.7 and 3.3).

Definition 2.6.1. Let k be a field. The *torus* T over k is the algebraic group $k^* \times \cdots \times k^*$.

Definition 2.6.2. A *toric variety* is a normal variety X (see [17] for a definition of normal) that contains the torus T as a dense open subset, together with an action $T \times X \rightarrow X$ of T on X that extends the natural action of T on itself.

In Definition 4.3 of [35], David Joyner gives a construction for a complete projective toric variety over a finite field $\mathbb{F}_q$, which depends only on a lattice polytope (i.e., the convex hull of a finite set of points in some lattice). Lisa Byrne [4] gives a nice exposition of this approach over the complex numbers, which we briefly recall here.

Given $\mathbf{t} = (t_1, ..., t_n) \in (\mathbb{C}^*)^n$ and $\mathbf{a} = (a_1, ..., a_n) \in \mathbb{Z}^n$, define $\mathbf{t}^{\mathbf{a}} = t_1^{a_1} t_2^{a_2} \cdots t_n^{a_n}$. Let P be a (convex) lattice polytope in $\mathbb{R}^n$ with $P \cap \mathbb{Z}^n = \{\mathbf{a}_0, ..., \mathbf{a}_m\}$, where $\mathbf{a}_i = (a_{i1}, ..., a_{in})$. Define $\phi_P : (\mathbb{C}^*)^n \to \mathbb{P}^m(\mathbb{C})$ by $\phi_P(\mathbf{t}) = [\mathbf{t}^{\mathbf{a}_0} : ... : \mathbf{t}^{\mathbf{a}_m}]$. The closure of the image of ϕ_P in $\mathbb{P}^m(\mathbb{C})$ is the *projective toric variety* X_P.

2.7 Correspondence between Polygons and Divisors

Toric surface codes are specified by Hansen [11] in terms of polygons. Our constructions of anticanonical surface codes are in terms of divisors. In order to compare the two, it is helpful to determine the divisor which arises from the polygon P. We outline the major steps in this process here and we refer the reader to Section 3 of [24] and Chapters 1 and 2 of [7] for more details.

Let $P \subset \mathbb{Z}^2$ be a convex polygon. Let $\mathbf{v}_0, ..., \mathbf{v}_{s+1}$ be the smallest integer vectors that are perpendicular to the sides of P and which point toward the interior of P. Label the vectors in a counterclockwise direction to obtain the ordered list $\{(a_i, b_i)\}_{i=0}^{s+1}$. In order to have a smooth toric surface, we need a list which satisfies the *determinant condition*:

$$\det \begin{pmatrix} a_{i-1} & a_i \\ b_{i-1} & b_i \end{pmatrix} = 1 \text{ for } i = 0, ..., s+1, \tag{2.1}$$

where we define $\begin{pmatrix} a_{-1} \\ b_{-1} \end{pmatrix} = \begin{pmatrix} a_{s+1} \\ b_{s+1} \end{pmatrix}$.

We force this condition to be satisfied by adding additional vectors to, or *refining*, the ordered list $\{(a_i, b_i)\}_{i=0}^{s+1}$. Suppose $\det \begin{pmatrix} a_{i-1} & a_i \\ b_{i-1} & b_i \end{pmatrix} = d > 1$ for some i. The number d is equal to the area of the parallelogram J determined by $\begin{pmatrix} a_{i-1} \\ b_{i-1} \end{pmatrix}$ and $\begin{pmatrix} a_i \\ b_i \end{pmatrix}$ (see

p. 26-29 of [16] for details). Since $d > 1$, there is an integer lattice point (a', b') in the interior of J (see Theorem 34 of [16]). Let $\mathbf{v}'$ be the shortest integer vector with the same direction as $\begin{pmatrix} a' \\ b' \end{pmatrix}$. Then $\mathbf{v}'$ subdivides J into two parallelograms of smaller area. We insert $\mathbf{v}'$ between $\begin{pmatrix} a_{i-1} \\ b_{i-1} \end{pmatrix}$ and $\begin{pmatrix} a_i \\ b_i \end{pmatrix}$ in our list of vectors and relabel to maintain the counterclockwise ordering. We continue this process of subdividing parallelograms and inserting new vectors into our ordered list until all parallelograms formed by consecutive vectors have area 1 (i.e., until the determinant condition is satisfied). In the end we have the ordered list: $\{(a_i, b_i)\}_{i=0}^{n+1}$, where $n \geq s$.

Following [7], one can generate a smooth toric surface X_P using the ordered list of vectors $\{(a_i, b_i)\}_{i=0}^{n+1}$. (The ordered list of vectors is the *fan*.) Then, as in Sections 3.1 and 3.2 of [24], we can find curves $C_0, ..., C_{n+1}$ such that each C_i is isomorphic to $\mathbb{P}^1$ and such that the Picard group $\mathrm{Pic}(X_P)$ of the toric surface X_P is freely generated by $C_1, ..., C_n$. (Note that we do not need to use the linear transformation in [24] which forces $\begin{pmatrix} a_0 \\ b_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, but then we do not know *a priori* which of the $n+2$ curves will generate the Picard group $\mathrm{Pic}(X_P)$.)

The canonical divisor is $K_{X_P} = -\sum_{i=0}^{n+1} C_i$. Hence the anticanonical divisor $-K_{X_P} = \sum_{i=0}^{n+1} C_i$ is effective and so the resulting surface is anticanonical. Thus we see that all smooth projective toric surfaces are anticanonical. There are anticanonical surfaces which are not toric, but we will not show this here.

The curves C_i form a cycle and their self-intersections are given by:

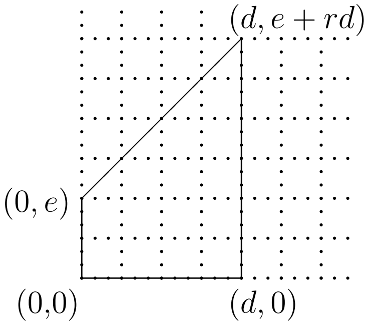
$$C_i \cdot C_j = \begin{cases} -(a_{i-1}b_{i+1} - a_{i+1}b_{i-1}) & \text{if } j = i; \\ 1 & \text{if } j = i \pm 1 \\ 0 & \text{otherwise,} \end{cases}$$

where we define $C_{-1} = C_{n+1}$ and $C_{n+2} = C_0$.

The divisor D_P corresponding to the polygon P is given by $D_P = \sum_{i=1}^{n} m_i C_i$, where m_i is the smallest integer such that $m_i + a_i x + b_i y \geq 0$ for all points $(x, y) \in P$. It follows that the intersection of the half planes defined by $m_i + a_i x + b_i y \geq 0$ is the polygon P. We give two examples for computing D_P and X_P.

Example 2.7.1. Let $P \subset \mathbb{Z}^2$ be the quadrilateral with vertices $(0, 0)$, $(d, 0)$, $(d, e+rd)$, and $(0, e)$, where d, e and r are positive integers (see Figure 2.7.1).

Figure 2.7.1: Quadrilateral with Vertices $(0, 0)$, $(d, 0)$, $(d, e + re)$ and $(0, e)$



Since the edge joining $(0, e)$ and $(d, e+rd)$ has slope r, the smallest integer vector perpendicular to this edge is $\begin{pmatrix} r \\ -1 \end{pmatrix}$. Listing all of the smallest integer vectors perpendicular to the edges of P in a counterclockwise fashion, we have: $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} -1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} r \\ -1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. These vectors already satisfy the determinant condition (2.1). The corresponding system of inequalities is:

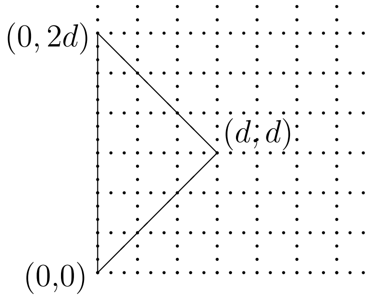
$$\begin{cases} m_0 + y \geq 0 \\ m_1 - x \geq 0 \\ m_2 + rx - y \geq 0 \\ m_3 + x \geq 0. \end{cases}$$

By minimizing each m_i over the points of P, we see that $m_0 = 0$, $m_1 = d$, $m_2 = e$ and $m_3 = 0$. Hence D_P has the form $D_P = 0C_1 + dC_1 + eC_2 + 0C_3 = dC_1 + eC_2$, where C_1 and C_2 can be found explicitly as curves on X_P using [24].

Using Fulton [7], we can determine the toric surface X_P corresponding to the polygon P using the list of vectors $\left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} r \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$ as the fan. In this case, however, it is easy to determine X_P from the self-intersections of the curves $C_0, ..., C_3$. Since $H_0, \mathbb{P}^2, H_2, H_3, ...$ are relatively minimal models, we know that X_P must be a blow-up of one of these surfaces. Since the rank of $\text{Pic}(X_P)$ is 2 (by Lemma 2 of [24]), we know that X_P must be equal to H_n for some $n \geq 2$ or $n = 0$. The self-intersections of $C_0, ..., C_3$ are r, 0, $-r$ and 0, respectively. Hence $X_P = H_r$ in this case.

Example 2.7.2. Let $P \subset \mathbb{Z}^2$ be the isosceles triangle with vertices $(0, 0)$, (d, d) and $(0, 2d)$, where d is a positive integer (see Figure 2.7.2).

Figure 2.7.2: Isosceles Triangle with Vertices $(0, 0)$, (d, d) and $(0, 2d)$



The smallest integer vectors perpendicular to the edges of P are $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} -1 \\ -1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. We add the vector $\frac{1}{2}\begin{pmatrix} -2 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$ as the second in this list so that

$$\det \begin{pmatrix} a_{i-1} & a_i \\ b_{i-1} & b_i \end{pmatrix} = 1 \text{ for } i = 0, ..., 3.$$

The corresponding system of inequalities is:

$$\begin{cases} m_0 - x + y \geq 0 \\ m_1 - x \geq 0 \\ m_2 - x - y \geq 0 \\ m_3 + x \geq 0. \end{cases}$$

By minimizing each m_i over the points of P, we see that $m_0 = 0$, $m_1 = d$, $m_2 = 2d$ and $m_3 = 0$. Hence D_P has the form $D_P = dC_1 + 2dC_2$, where we can find C_1 and C_2 explicitly as curves on X_P using [24]. Since the rank of $\mathrm{Pic}(X_P)$ is 2 and since the self-intersections of $C_0, ..., C_3$ are 0, -2, 0 and 2, respectively, we know the toric surface corresponding to P is H_2.

We have shown how to find the divisor D_P corresponding to a polygon P. In Section 3.4 of [24], Murray shows explicitly how to find the polygon P corresponding to a divisor D on a smooth toric surface S.

Chapter 3

Coding Theory Background

3.1 Basic Definitions and Theorems

Coding theory is the study of how to efficiently and reliably send information across a communications channel. We are not concerned with keeping messages secret but only with detecting and correcting errors that occur during transmission. When a message is sent through a channel, noise causes errors to occur in the message. For example, if messages are sent in binary, some of the bits may become “flipped” to the opposite value (a zero to a one or a one to a zero). Additional bits can be attached to each message so that the receiver can detect and correct the errors that occur. We wish to find efficient ways to attach additional information to messages so that the receiver can correct as many errors as possible. We now give the formal definition of a code.

Definition 3.1.1. A *linear code* C is a vector subspace of a finite dimensional vector space $\mathbb{F}^n$ over a finite field $\mathbb{F}$. The vectors in the code are called *codewords*. If $k = \dim C$ and $q = |\mathbb{F}|$, we say C is a *q-ary* code of *length* n and *dimension* k and we refer to C as an $[n, k]$ code. By *code*, we shall always mean a linear code.

Definition 3.1.2. The *Hamming distance* between two codewords is the number of coordinate positions in which they differ. The *minimum distance* d of a code C is equal to the smallest Hamming distance among all pairs of distinct codewords in C. If C is an $[n, k]$ code with minimum distance d, we often say C is an $[n, k, d]$ code.

As seen in the next Proposition, which is Theorem 2 of [26], the minimum distance tells us the error-correcting capability of a code.

Proposition 3.1.3. *Let d be the minimum distance of a code C. Then C can correct any $\left\lfloor \frac{d-1}{2} \right\rfloor$ or fewer errors.*

By Proposition 3.1.3, we see that the larger d is, the more errors the code can correct. In classical coding theory one seeks to find codes with large minimum distance d relative to the length and dimension of the code. The parameter d is, in general, difficult to compute for large codes.

Definition 3.1.4. The *Hamming weight* of a codeword $\mathbf{c}$ is the number of nonzero coordinates in $\mathbf{c}$. The *minimum weight* of a code C is the smallest weight of any nonzero codeword in C.

For a linear code, the minimum weight is equal to the minimum distance. This is due to the fact that the difference of two codewords is a codeword. We will use this fact frequently when computing the minimum distance.

A natural question is to ask how large the minimum distance d of an $[n, k]$ code C can be. A first result is the Singleton Bound (see Corollary 4 of [26]).

Proposition 3.1.5 (Singleton Bound)**.** *For an $[n, k, d]$ code C, we have*

$$d \leq n - k + 1.$$

A code whose parameters satisfy $d = n - k + 1$ is called a *Maximum Distance Separable code,* or simply an *MDS code.* Another "bound" on the code parameters is the Varshamov-Gilbert Bound. This bound helps us to determine whether a code with parameters $[n, k, d]$ exists over a given finite field $\mathbb{F}_q$ (see Corollary 3.3 of [27]).

Proposition 3.1.6 (Varshamov-Gilbert Bound)**.** *Given n, k and q, there exists a q-ary $[n, k]$ code with minimum distance d or more, provided that d satisfies the following inequality:*

$$(q-1)\binom{n-1}{1} + (q-1)^2\binom{n-1}{2} + \cdots + (q-1)^{d-2}\binom{n-1}{d-2} < q^{n-k} - 1. \qquad (3.1)$$

Remark. Note that the Varshamov-Gilbert Bound does *not* tell us that the parameters of a q-ary $[n, k, d]$ code *must* satisfy Inequality 3.1, but only that *if* the inequality is satisfied *then* such a code exists. The proof of the bound is constructive in a sense, but the procedure is not practical to carry out.

It turns out that in many situations we wish to use long codes, i.e., codes with large length. Therefore we are also interested in asymptotic bounds on the code parameters. Before we give an asymptotic bound, we need a definition.

Definition 3.1.7. Let C be an $[n, k, d]$ code. The *rate* of C is $R = k/n$. The *relative minimum distance* of C is $\delta = d/n$.

An infinite family of codes (with q fixed) is said to be *asymptotically good* if both the rate and relative minimum distance are bounded away from 0 as the length n approaches infinity. Proposition 3.1.8 shows asymptotically good families of codes exist (see Section 3 of [27] for details).

Proposition 3.1.8 (Asymptotic Varshamov-Gilbert Bound). *Let q be fixed. There exist infinite families of q-ary codes, called Varshamov-Gilbert codes, which satisfy*

$$1 - R \approx \varphi(\delta),$$

where $\varphi(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$ and where " $\approx$ " means asymptotic equality as $n \to \infty$.

For more than twenty years, it remained plausible the Asymptotic Varshamov-Gilbert Bound was the best possible [33]. In the next section we discuss AG codes, some of which beat the "bound" in Proposition 3.1.8 on a certain interval.

An important code construction in coding theory is that of concatenated codes. Concatenated codes perform well for correcting *burst errors*, i.e., errors that are clustered together. The development we use here is adapted from Section 5.5 of [18].

Definition 3.1.9. Let A be an $[n, k, d]$ code over $\mathbb{F}_q$. Let $Q = q^k$ and $\psi : \mathbb{F}_Q \to A$ be a bijective $\mathbb{F}_q$-linear map. Let B be an $[N, K, D]$ code over $\mathbb{F}_Q$. The *concatenation* of A and B is the code

$$C = \{(\psi(b_1), ..., \psi(b_N))|(b_1, ..., b_N) \in B\}.$$

The code C is called a *concatenated code* with *inner code A* and *outer code B*.

Theorem 3.1.10. *Let C be the concatenated code with inner code A and outer code B. Then C is a linear $[nN, kK]$ code over $\mathbb{F}_q$ whose minimum distance is at least dD.*

A common construction for concatenated codes is to use an MDS code as the outer code and to choose an inner code so that the resulting code is binary.

3.2 Algebraic Geometric Codes

Algebraic geometric (AG) codes on curves were first introduced by V.D. Goppa [8]. The AG code construction can easily be generalized for codes on other varieties, as described in Section 3.1.1 of [32].

Definition 3.2.1. Let X be a smooth, irreducible, projective variety defined over the finite field $\mathbb{F}_q$. Let D be an effective $\mathbb{F}_q$-divisor on X and let $\mathcal{P} = \{P_1, ..., P_n\}$ be a finite set of $\mathbb{F}_q$-points on X such that $\operatorname{supp} D \cap \mathcal{P} = \emptyset$. Let $ev_{\mathcal{P}} : L(D) \to \mathbb{F}_q^n$ be the evaluation map given by $ev_{\mathcal{P}}(f) = (f(P_1), ..., f(P_n))$. Then the *algebraic geometric code*, or *AG code*, over $\mathbb{F}_q$ associated to X, $\mathcal{P}$ and D is $C_q(X, \mathcal{P}, D) = ev_{\mathcal{P}}(L(D))$. When q is clear from context, we write $C(X, \mathcal{P}, D)$ for $C_q(X, \mathcal{P}, D)$.

It is not too difficult to compute the dimension of an AG code in the case where X is a smooth, projective, absolutely irreducible curve. One can also obtain a lower bound on the minimum distance of the code in this case. We give a proof of the results here, following that of Theorem 6.4 in [37].

Theorem 3.2.2. *Let X be a smooth, projective, absolutely irreducible curve of genus g, defined over the field $\mathbb{F}_q$. Let $\mathcal{P} \subset X(\mathbb{F}_q)$ be a set of n distinct $\mathbb{F}_q$-rational points on X, and let D be a divisor on X satisfying $2g - 2 < \deg D < n$ and $\mathcal{P} \cap \operatorname{supp} D = \emptyset$. Then the algebraic geometric code $C := C(X, \mathcal{P}, D)$ is linear of length n, dimension $k = \deg D + 1 - g$, and minimum distance d, where $d \geq n - \deg D$.*

Proof. The length of C is $|\mathcal{P}| = n$. Note that $\dim L(D) = \deg D + 1 - g$ by Riemann-Roch for Curves (Theorem 2.2.9) since $\deg D > 2g - 2$. The dimension of the code C is equal to $\dim L(D)$ if and only if the map $ev_{\mathcal{P}}$ is injective, i.e., if and only if the kernel of $ev_{\mathcal{P}}$ is trivial. Let $f \in \ker(ev_{\mathcal{P}})$; so $f(P_1) = \cdots = f(P_n) = 0$. Then each P_i has coefficient at least one in $\operatorname{div}(f)$. Since no P_i is in the support of D, we have that

$\mathrm{div}(f) + D - P_1 - \cdots - P_n \geq 0$ and so $f \in L(D - P_1 - \cdots - P_n)$. Since $\deg D < n$, the divisor $D - P_1 - \cdots - P_n$ has negative degree and so $L(D - P_1 - \cdots - P_n) = \{0\}$. Hence $f \equiv 0$ and so the kernel of $ev_{\mathcal{P}}$ is indeed trivial. This completes the proof that $k = \deg D + 1 - g$.

We have left to show that the minimum distance d of C is at least $n - \deg D$. Let $ev_{\mathcal{P}}(f) = (f(P_1), ..., f(P_n))$ be a codeword of nonzero weight d. Without loss of generality, suppose $f(P_{d+1}) = \cdots = f(P_n) = 0$. Then $\mathrm{div}(f) + D - P_{d+1} - \cdots - P_n$ is effective and thus has nonnegative degree. Hence $\deg D - (n - d) \geq 0$, i.e., $d \geq n - \deg D$. □

Remark. Finding exact results and good bounds for AG codes on varieties of higher dimension is much more complicated. Even the dimension of such a code is difficult to compute since $\dim L(D)$ is unknown in general.

One of the reasons that algebraic geometric codes are so exciting is that in 1982, Tsfasman, Vlăduţ and Zink demonstrated a family of curves yielding AG codes with minimum distance greater than that given by the Asymptotic Varshamov-Gilbert Bound (Proposition 3.1.8) on a certain interval [33].

3.3 Toric Surface Codes

In 1998, Johan P. Hansen introduced toric surface codes [10], which are algebraic geometric codes on toric surfaces. We recall the definition of toric code given in the paper by Little and Schenck [21].

Definition 3.3.1. Let $\mathbb{F}_q$ be a finite field with primitive element γ. Let $P \subset \mathbb{R}^2$ be an integral convex polygon such that P is contained the square $[0, q-2] \times [0, q-2] \subset \mathbb{R}^2$. For $0 \leq i, j \leq q-2$ let $P_{ij} = (\gamma^i, \gamma^j)$ in $\mathbb{F}_q^* \times \mathbb{F}_q^*$. For each $m = (m_1, m_2) \in P \cap \mathbb{Z}^2$, let

$$ev_m(P_{ij}) = (\gamma^i)^{m_1}(\gamma^j)^{m_2}.$$

The *toric code* $C_P(\mathbb{F}_q)$ over $\mathbb{F}_q$ associated to P is the code of length $(q-1)^2$ spanned by the vectors $\{(ev_m(P_{ij}))_{i=0,\ldots,q-2;j=0,\ldots,q-2} | m \in P \cap \mathbb{Z}^2\}$. When the field $\mathbb{F}_q$ is clear from context, for brevity we write C_P for $C_P(\mathbb{F}_q)$.

In [11], Hansen proved that the dimension of a toric code C_P is equal to the number of integral points in the polygon P. Using cohomology and intersection theory, Hansen obtained exact results on the minimum distance of C_P for certain polygons. In [19], David Joyner demonstrated an 8-ary $[49, 11, 28]$ toric code whose parameters were better than any other known code at the time. Joyner also presented a list decoding algorithm for toric codes.

In [21], Little and Schenck employed a new approach to obtain lower bounds on the minimum distance of toric codes. The *Minkowski sum* of two polygons Q and R is $Q + R = \{x + y : x \in Q, y \in R\}$. Using a Minkowski sum decomposition of a polygon $P = \sum_{i=1}^{\ell} P_i$, Little and Schenck were able to obtain a lower bound on the minimum distance of C_P in terms of the minimum distances of the codes C_{P_i} (see Theorem 1.2 of [21]). This approach can be applied to some polygons for which Hansen did not prove results on the minimum distance.

In this dissertation, we will work with algebraic geometric codes on anticanonical surfaces. Recall that every smooth toric surface is anticanonical, as shown in Section 2.7. Not every smooth, rational, anticanonical surface is a toric surface, however, since it need not be obtained from a convex polygon in the manner described in Section 2.7 for toric surfaces. We will obtain some exact results and lower bounds on the dimension and minimum distance of AG codes on anticanonical surfaces. In Section 4.5, we give a lower bound on the minimum distance of a code $C(\mathcal{B}, \mathcal{P}, D)$ in terms of the minimum distances of codes whose corresponding divisors sum to D. In this sense, our result is similar to Theorem 1.2 of Little and Schenck. Work has also been done on r-dimensional toric codes; see [28] and [22]. In Chapter 5, we investigate codes on $\mathbb{P}^r$.

Chapter 4

Anticanonical Surface Codes

In this chapter we begin a study of algebraic geometric codes associated to anticanonical surfaces X, which we call *anticanonical surface codes*. Recall by Proposition 2.5.2 and its subsequent remark that, after possibly increasing the field size and blowing up additional points, any smooth, projective, rational, anticanonical surface is isomorphic to a surface obtained by blowing up points of $\mathbb{P}^2$. Hence we will focus on anticanonical surfaces of the form $\mathbb{P}^2_{\mathcal{B}}$, where $\pi : \mathbb{P}^2_{\mathcal{B}} \to \mathbb{P}^2$ is the successive blowing-up of $\mathbb{P}^2$ at the points of $\mathcal{B}$, where $\mathcal{B} = \{p_1, ..., p_b\}$ is a set of $\mathbb{F}_q$-points in $\mathbb{P}^2$.

Let $L \subset \mathbb{P}^2_{\mathcal{B}}$ be the total transform of a general line on $\mathbb{P}^2$, i.e., let $L = \pi^{-1}(L^*)$, where L^* is a general line on $\mathbb{P}^2$. Let $E_1, ..., E_b$ be the blow-ups of $p_1, ..., p_b \in \mathcal{B}$, respectively. Since $[L], [E_1], ..., [E_b]$ form a basis for $\mathrm{Pic}(\mathbb{P}^2_{\mathcal{B}})$ (see Section 2.3), we can uniquely express the class $[D]$ of a divisor D on $\mathbb{P}^2_{\mathcal{B}}$ by $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$, for some $m, m_1, ..., m_b \in \mathbb{Z}$ (see Section 2.3 for details). Since $\dim L(D) = 0$ if $m < 0$ and since we have a canonical isomorphism $L(D) \cong L(D + m_iE_i)$ if $m_i < 0$, the divisors of interest to us will always have $m, m_1, ..., m_b \geq 0$.

Let x, y and z be projective coordinates on $\mathbb{P}^2$. We assume $\mathcal{B}$ is contained in the two lines defined by $xy = 0$. Since the points of $\mathcal{B}$ are contained in a conic, the resulting surface $\mathbb{P}^2_{\mathcal{B}}$ is anticanonical (see Section 2.3). Later we will work with a standard set of evaluation points (see Definition 4.1.6), but for now $\mathcal{P}$ is any set of points in $\mathbb{P}^2(\mathbb{F}_q)$ such that $\mathcal{B} \cap \mathcal{P} = \emptyset$. (Away from $\mathcal{B}$, the blow-up morphism $\pi : \mathbb{P}^2_{\mathcal{B}} \to \mathbb{P}^2$ establishes an isomorphism, and thus we can use projective coordinates on $\mathbb{P}^2$ to identify points of $\mathbb{P}^2_{\mathcal{B}}$ not in $\pi^{-1}(\mathcal{B})$.)

Let D be an effective divisor such that $\operatorname{supp} D \cap \mathcal{P} = \emptyset$. Recall that $L(D) = \{f \in \mathbb{F}_q(\mathbb{P}^2_{\mathcal{B}}) | \operatorname{div}(f) + D \geq 0\} \cup \{0\}$. By Proposition 2.1.6, this is equivalent to $\{f \in \mathbb{F}_q(\mathbb{P}^2) | \operatorname{div}(f) + D \geq 0\} \cup \{0\}$. Also recall from Definition 3.2.1 that the algebraic geometric code $C(\mathbb{P}^2_{\mathcal{B}}, \mathcal{P}, D)$ corresponding to $\mathbb{P}^2_{\mathcal{B}}$, $\mathcal{P}$ and D is the image of the evaluation map $ev_{\mathcal{P}} : L(D) \to \mathbb{F}_q^n$, where $n = |\mathcal{P}|$. We say $C(\mathbb{P}^2_{\mathcal{B}}, \mathcal{P}, D)$ is an *anticanonical surface code* since $\mathbb{P}^2_{\mathcal{B}}$ is an anticanonical surface. Finally, for brevity, we write $C(\mathcal{B}, \mathcal{P}, D)$ for $C(\mathbb{P}^2_{\mathcal{B}}, \mathcal{P}, D)$.

4.1 First Results

The purpose of the first few results in this section is to show that the parameters of an anticanonical surface code depend only on the divisor class $[D]$ of D and not on the specific divisor D. (This is also true for AG codes on the curve $\mathbb{P}^1$.)

Notation. Let $R = \mathbb{F}_q[x, y, z]$. Let R_m denote the vector space spanned by the set of homogeneous polynomials in R of degree m. For $f \in R_m$, let $Z(f)$ denote the set of zeros of f in $\mathbb{P}^2(\mathbb{F}_q)$. If $\frac{f}{h}$ is a rational function, i.e., if both f and h are elements of R_m with $h \neq 0$, then let $Z(\frac{f}{h}) = Z(f) \cap \operatorname{Dom}(\frac{f}{h})$, where $\operatorname{Dom}(\frac{f}{h})$ is the domain of $\frac{f}{h}$.

Definition 4.1.1. Let $0 \neq f \in R_m$ and let $p \in \mathbb{P}^2(\mathbb{F}_q)$. Let h be the image of the function f under the linear change of coordinates which moves p to the point $(0 : 0 : 1)$. We say f has a *zero of multiplicity at least* t at the point p if $h(x, y, 1)$ has no terms of degree less than t.

Example 4.1.2. Let $q = 9$ and γ be a primitive element of $\mathbb{F}_9$. Let $f = x^2 - y^2 \in R_2$ and $p = (\gamma : \gamma : 1) \in \mathbb{P}^2(\mathbb{F}_9)$. The linear change of coordinates which takes p to the point $(0 : 0 : 1)$ takes f to the function $h = (x - \gamma z)^2 - (y - \gamma z)^2 = x^2 - 2\gamma xz - y^2 + 2\gamma yz$. Since $h(x, y, 1)$ has no terms of degree 0, f has a zero of multiplicity at least one at p. (Since $h(x, y, 1)$ does have terms of degree one, we say that f has a zero of multiplicity exactly one at p.)

Definition 4.1.3. Let $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ be effective with $m, m_1, ..., m_b \geq 0$. Define

$$F\left([D]\right) = \{f \in R_m : \ f \text{ has a zero of multiplicity at least } m_i \text{ at each } p_i \in \mathcal{B}\}.$$

For any $h \in R_m$ with $Z(h) \cap \mathcal{P} = \emptyset$, define

$$L^h([D]) = \left\{ \frac{f}{h} : f \in F\left([D]\right) \right\}.$$

Let $ev_{\mathcal{P}}^h : L^h([D]) \to \mathbb{F}_q^n$ be the evaluation map on $L^h([D])$, where $n = |\mathcal{P}|$. We define the code $C^h(\mathcal{B}, \mathcal{P}, [D])$ to be the image of the evaluation map $ev_{\mathcal{P}}^h$. Note that $\dim L(D) = \dim L^h([D])$.

Our first proposition and the subsequent corollary show that the choice of denominator for the rational functions does not affect the code parameters.

Proposition 4.1.4. *Let $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ be effective with $m, m_1, ..., m_b \geq 0$. The parameters $[n, k, d]$ of $C^g(\mathcal{B}, \mathcal{P}, [D])$ and $C^h(\mathcal{B}, \mathcal{P}, [D])$ are the same for any $g, h \in R_m$ satisfying $Z(g) \cap \mathcal{P} = Z(h) \cap \mathcal{P} = \emptyset$.*

Proof. The length of each code is $|\mathcal{P}|$. Since $L^g([D])$ and $L^h([D])$ are finite dimensional vector spaces and since $ev_{\mathcal{P}}^g$ and $ev_{\mathcal{P}}^h$ are linear transformations, we have the following equalities:

$$\dim L^g([D]) = \dim ev^g_{\mathcal{P}}(L^g([D])) + \dim(\ker ev^g_{\mathcal{P}}) \text{ and} \tag{4.1}$$

$$\dim L^h([D]) = \dim ev^h_{\mathcal{P}}(L^h([D])) + \dim(\ker ev^h_{\mathcal{P}}). \tag{4.2}$$

Let $\phi : L^g([D]) \to L^h([D])$ be the map given by multiplication by $\frac{g}{h}$. Then ϕ is an isomorphism of vector spaces. Note that $Z(\frac{f}{g}) \cap \mathcal{P} = Z(\phi(\frac{f}{g})) \cap \mathcal{P} = Z(\frac{f}{h}) \cap \mathcal{P}$ since g and h are nonzero on $\mathcal{P}$. Hence $\ker ev^h_{\mathcal{P}} = \phi(\ker ev^g_{\mathcal{P}})$. Since ϕ is an isomorphism, we have $\dim(\ker ev^h_{\mathcal{P}}) = \dim(\ker ev^g_{\mathcal{P}})$ and $\dim L^g([D]) = \dim L^h([D])$. By equations 4.1 and 4.2, we have $\dim ev^h_{\mathcal{P}}(L^h([D])) = \dim ev^g_{\mathcal{P}}(L^g([D]))$, i.e., $\dim(C^h(\mathcal{B}, \mathcal{P}, [D])) = \dim(C^g(\mathcal{B}, \mathcal{P}, [D]))$.

Finally, since $Z(\frac{f}{g}) \cap \mathcal{P} = Z(\frac{f}{h}) \cap \mathcal{P}$ for all $f \in R_m$, we have

$$\begin{aligned} d_{C^g(\mathcal{B},\mathcal{P},[D])} &= (q-1)^2 - \max\left\{ \left| Z\left(\frac{f}{g}\right) \cap \mathcal{P} \right| : \frac{f}{g} \in L^g([D]), f \not\equiv 0 \text{ on } \mathcal{P} \right\} \\ &= (q-1)^2 - \max\left\{ \left| Z\left(\frac{f}{h}\right) \cap \mathcal{P} \right| : \frac{f}{h} \in L^h([D]), f \not\equiv 0 \text{ on } \mathcal{P} \right\} \\ &= d_{C^h(\mathcal{B},\mathcal{P},[D])}. \end{aligned}$$

□

Corollary 4.1.5. *Let D be an effective divisor such that* $\operatorname{supp} D \cap \mathcal{P} = \emptyset$ *and* $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ *with* $m, m_1, ..., m_b \geq 0$. *The parameters of the code* $C(\mathcal{B}, \mathcal{P}, D)$ *are the same as those of* $C^h(\mathcal{B}, \mathcal{P}, [D])$ *for any* $h \in R_m$ *with* $Z(h) \cap \mathcal{P} = \emptyset$.

Proof. We can write the functions of $L(D)$ with a fixed denominator $g \in R_m$ such that $Z(g) \cap \mathcal{P} = \emptyset$. The parameters of $C(\mathcal{B}, \mathcal{P}, D)$ are thus the same as those of $C^g(\mathcal{B}, \mathcal{P}, [D])$. By Proposition 4.1.4, the parameters of $C^g(\mathcal{B}, \mathcal{P}, [D])$ are the same as those of $C^h(\mathcal{B}, \mathcal{P}, [D])$ for any $h \in R_m$ such that $Z(h) \cap \mathcal{P} = \emptyset$. □

Remark. By Corollary 4.1.5, we see that the parameters of an anticanonical surface code depend only upon $\mathcal{B}$, $\mathcal{P}$ and $[D]$. Also, constructing $C^h(\mathcal{B}, \mathcal{P}, [D])$ is simpler than constructing $C(\mathcal{B}, \mathcal{P}, D)$ because we can find the functions in $F([D])$ by checking multiplicities at prescribed zeros. Finding the functions in $L(D)$ requires knowledge of the specific divisor $D \in \mathbb{P}^2_{\mathcal{B}}$. Thus, for the remainder of this chapter, we will study anticanonical surface codes of the form $C^h(\mathcal{B}, \mathcal{P}, [D])$, where $Z(h) \cap \mathcal{P} = \emptyset$.

To obtain exact results and good bounds on the dimension and minimum distance of anticanonical surface codes it is helpful to fix the set of evaluation points $\mathcal{P}$.

Definition 4.1.6. We define the *standard set of evaluation points*, or simply, the *standard set*, as follows:

$$\mathcal{P} = \{(a_0 : a_1 : a_2) \in \mathbb{P}^2(\mathbb{F}_q) : a_0 a_1 a_2 \neq 0\}.$$

Remark. Note that $|\mathcal{P}| = (q-1)^2$ if $\mathcal{P}$ is the standard set. If $h = z^m$ with $m \geq 0$, then $Z(h) \cap \mathcal{P} = \emptyset$. Also, since $\mathcal{B} \subset Z(xy)$, we have $\mathcal{B} \cap \mathcal{P} = \emptyset$.

To obtain results for the dimension and minimum distance of $C^h(\mathcal{B}, \mathcal{P}, [D])$, we need to bound the number of zeros in $\mathcal{P}$ of a function $f \in F([D])$. Serre [31] gives a bound for the number of zeros in $\mathbb{P}^r(\mathbb{F}_q)$ of any nonzero homogeneous polynomial. Since our functions $f \in F([D])$ have additional restrictions regarding multiplicities of certain zeros and since we wish to bound the zeros of f in the standard set $\mathcal{P} \subsetneq \mathbb{P}^2(\mathbb{F}_q)$, we adapt Serre's proof to obtain a (sharp) bound for $|Z(f) \cap \mathcal{P}|$. Later, we will make improvements on this bound in certain cases.

Lemma 4.1.7. *Let $\mathcal{P}$ be the standard set and $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ be effective with $m, m_1, ..., m_b \geq 0$, where $\mathcal{B} \subset Z(xy)$. Let $0 \neq f \in F([D])$. If $q \geq 2m - \sum_{i=1}^{b} m_i$, then $|Z(f) \cap \mathcal{P}| \leq m(q-1)$. Furthermore, if f is not a product of linear polynomials over $\mathbb{F}_q$, then $|Z(f) \cap \mathcal{P}| \leq m(q-1) - (q - 2m + \sum_{i=1}^{b} m_i)$.*

Proof. Let $S = Z(f) \cap \mathcal{P}$ and let $N = |S|$. Let $g_1, ..., g_\delta$ be the distinct linear factors of f over $\mathbb{F}_q$ and let $G_1, ..., G_\delta$ be the lines of $\mathbb{P}^2(\mathbb{F}_q)$ defined by $g_1, ..., g_\delta$. Let G be the point set given by the union of the $G_1, ..., G_\delta$. We have two cases.

Case 1. $S \subset G$

This is the case where f is a product of linear polynomials over $\mathbb{F}_q$. Since each G_i has no more than $q-1$ zeros in $\mathcal{P}$ and since $\delta \leq \deg(f) = m$, we have

$$N \leq \delta(q-1) \leq m(q-1).$$

Case 2. $S \not\subseteq G$

This is the case where f is not a product of linear polynomials. Let $P \in S \setminus G$. If L is a line of $\mathbb{P}^2(\mathbb{F}_q)$ passing through P, the restriction of f to L is not identically zero, by the choice of P. Since $deg(f|_L) = m$, we have $|Z(f) \cap L| \leq m$ for every line L through P. If a line L through P passes through two points, say p_i and p_j, of $\mathcal{B}$, then $|S \cap L| \leq m - m_i - m_j$ since $S = Z(f) \cap \mathcal{P}$ is disjoint from $\mathcal{B}$. If a line L through P passes through exactly one point, say p_ℓ, of $\mathcal{B}$, then $|S \cap L| \leq m - m_\ell$. Let t be the number of lines of $\mathbb{P}^2(\mathbb{F}_q)$ through P that pass through two points of $\mathcal{B}$. Reorder the m_i's (and corresponding p_i's) if necessary so that $\{m_1, m_2\}, \{m_3, m_4\}, ..., \{m_{2t-1}, m_{2t}\}$ correspond to pairs of points $\{p_i, p_{i+1}\} \subset \mathcal{B}$ such that the line through p_i and p_{i+1} also passes through P.

Now let A be the set of pairs (P', L') where $P' \in S \setminus \{P\}$ and L' is the line passing through P and P'. On the one hand, there are $N-1$ points $P' \in S \setminus \{P\}$ and exactly one line L' passing through P and P', so

$$|A| = N - 1. \tag{4.3}$$

On the other hand, there are $(q+1)$ lines L' passing through P. The number of points in $(S \setminus \{P\}) \cap L'$ is exactly one less than $|S \cap L'|$. We know t of the lines L' pass through two points of $\mathcal{B}$, $b-2t$ of the lines pass through exactly one point of $\mathcal{B}$ and the remaining $(q+1)-(b-t)$ lines pass through no points of $\mathcal{B}$. Hence

$$|A| \leq \sum_{i=1}^{t}(m-m_{2i-1}-m_{2i}-1)+\sum_{i=2t+1}^{b}(m-m_i-1)+((q+1)-(b-t))(m-1). \quad (4.4)$$

Note that since $P \in S \setminus G$, we know $m-m_{2i-1}-m_{2i}-1 \geq 0$ for $i=1,...,t$ and $m-m_i-1 \geq 0$ for $i=2t+1,...,b$. Combining Equations (4.3) and (4.4), we have that N is bounded above by

$$\sum_{i=1}^{t}(m-m_{2i-1}-m_{2i}-1)+\sum_{i=2t+1}^{b}(m-m_i-1)+((q+1)-(b-t))(m-1)+1,$$

which is equal to $m(q-1)-\left(q-2m+\sum_{i=1}^{b} m_i\right)$. This proves the "furthermore" part of the lemma. Since $q \geq 2m-\sum_{i=1}^{b} m_i$, we have that $N \leq m(q-1)$ in this case as well. □

We are now able to compute the dimension of the code $C^h(\mathcal{B}, \mathcal{P}, [D])$. Though the following proposition is stated for a numerically effective divisor class, recall that we can always reduce an effective divisor D to a numerically effective divisor D' such that $L(D)=L(D')$ (see the remark after Definition 2.3.4). Thus the parameters of the code $C(\mathcal{B}, \mathcal{P}, D)$ are the same as those of $C^h(\mathcal{B}, \mathcal{P}, [D'])$.

Proposition 4.1.8. *Let $[D]=[mL-m_1E_1-\cdots-m_bE_b]$ be numerically effective and let $\mathcal{P}$ be the standard set. Then for all $q \geq \max\{m+2,\ 2m-\sum_{i=1}^{b} m_i\}$, the* *dimension of* $C^h(\mathcal{B}, \mathcal{P}, [D])$ *(with* $h = z^m$*) is*

$$k = \dim L(D) = \binom{m+2}{2} - \sum_{i=1}^{b} \binom{m_i+1}{2}.$$

Proof. Recall that we have the evaluation map $ev_{\mathcal{P}}^h : L^h([D]) \to \mathbb{F}_q^n$, with $k = \dim ev_{\mathcal{P}}^h(L^h([D]))$ and

$$\dim L^h([D]) = \dim ev_{\mathcal{P}}^h(L^h([D])) + \dim(\ker ev_{\mathcal{P}}^h).$$

We now show that $\ker ev_{\mathcal{P}}^h = 0$. Let $\frac{f}{h} \not\equiv 0$ be in $L^h([D])$. By Lemma 4.1.7 and the fact that $m < q-1$, we have $|Z(\frac{f}{h}) \cap \mathcal{P}| = |Z(f) \cap \mathcal{P}| \leq m(q-1) < (q-1)^2$. Thus $\frac{f}{h}(p) \neq 0$ for some $p \in \mathcal{P}$ and so $\frac{f}{h} \notin \ker ev_{\mathcal{P}}^h$. Hence $\ker ev_{\mathcal{P}}^h = 0$ and so $\dim ev_{\mathcal{P}}^h(L^h([D])) = \dim L^h([D])$. Thus,

$$k = \dim L^h([D]) = \dim L(D) = \binom{m+2}{2} - \sum_{i=1}^{b} \binom{m_i+1}{2},$$

where the last equality holds since $[D]$ is numerically effective and the points of $\mathcal{B}$ lie on the conic defined by $xy = 0$ (see Section 2.3). □

Together, Lemma 4.1.7 and Proposition 4.1.8 give us the following theorem on the code parameters of an anticanonical surface code.

Theorem 4.1.9. *Let* $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ *be numerically effective and let* $\mathcal{P}$ *be the standard set. Then for all* $q \geq \max\{m+2,\ 2m - \sum_{i=1}^{b} m_i\}$, $C^h(\mathcal{B}, \mathcal{P}, [D])$ *(with* $h = z^m$*) is a*

$$\left[(q-1)^2, \binom{m+2}{2} - \sum_{i=1}^{b} \binom{m_i+1}{2}, d\right] \ \textit{code},$$

where $d \geq (q-1)^2 - m(q-1)$.

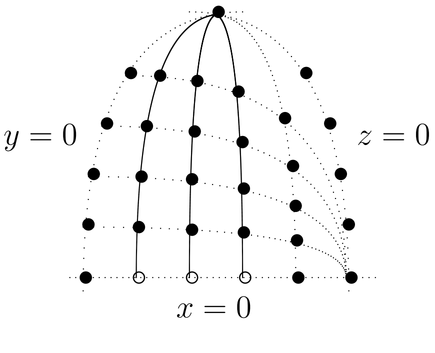
Proof. The dimension is given by Proposition 4.1.8. To compute the minimum distance d, note that the weight of a codeword $ev_{\mathcal{P}}(\frac{f}{h})$ is equal to $(q-1)^2$ minus the number of points of $\mathcal{P}$ at which $\frac{f}{h}$ vanishes. Hence by Lemma 4.1.7, we have

$$\begin{aligned} d &= (q-1)^2 - \max\left\{\left|Z\left(\frac{f}{h}\right)\cap\mathcal{P}\right| : \frac{f}{h}\in L^h([D]), \frac{f}{h}\neq 0\right\} \\ &= (q-1)^2 - \max\left\{|Z(f)\cap\mathcal{P}| : f\in F\left([D]\right), f\neq 0\right\} \\ &\geq (q-1)^2 - m(q-1). \end{aligned}$$

Note that since $q \geq m+2$, the bound is nontrivial, i.e., $d \geq (q-1)^2 - m(q-1) > 0$. □

Example 4.1.10. Let $[D] = [3L - E_1 - E_2 - E_3]$, so $m = 3$ and $m_i = 1$ for $i = 1, 2, 3$. Note that $q = 5$ satisfies the hypothesis of Theorem 4.1.9. Suppose $\mathcal{B} = \{(0:1:1), (0:2:1), (0:3:1)\}$. By Theorem 4.1.9, the dimension of the code is $k = \binom{5}{2} - 3 = 7$ and $d \geq 4^2 - 3\cdot 4 = 4$. Let $f = (y-z)(y-2z)(y-3z) \in F\left([D]\right)$. The zero set of f is shown below in Figure 4.1.1 with solid lines. (The curved lines in the figure are a convenient way of representing straight lines in $\mathbb{P}^2$.) The open circles are the points of $\mathcal{B}$ and the solid dots are the other points of $\mathbb{P}^2(\mathbb{F}_5)$.

Figure 4.1.1: Zero set of $f = (y-z)(y-2z)(y-3z)$



Since f has $3 \cdot 4 = 12$ zeros in $\mathcal{P}$, we see that the bound on d of Theorem 4.1.9 is sharp in this example, i.e., $C^h(\mathcal{B}, \mathcal{P}, [D])$ is a 5-ary $[16, 7, 4]$ code. The minimum distance of $C^h(\mathcal{B}, \mathcal{P}, [D])$ is 2 less than that guaranteed by the Varshamov-Gilbert

Bound (Proposition 3.1.6) and it is 3 less than that of the best known linear code with the same field size, length and dimension [9].

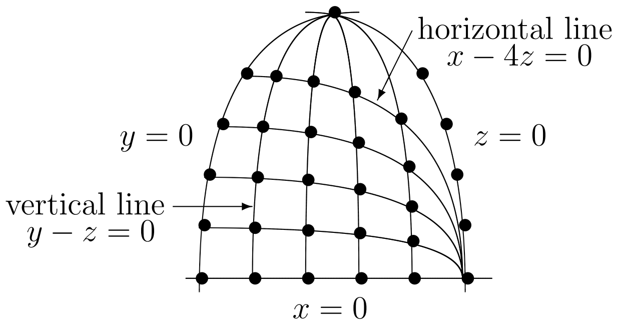
4.2 An Exact Result in a Special Case

In this section we restrict ourselves to the case where the points of $\mathcal{B}$ lie on the line defined by $x = 0$. In doing so, we obtain an exact result on the minimum distance when $[D] = [bL - E_1 - \cdots - E_b]$. (Note that $x^b \in F([D])$ and so $F([D]) \neq 0$.) In Example 4.5.5 of Section 4.5, we will see how this exact result can help us to find improved lower bounds on the minimum distance for other divisors and point sets $\mathcal{B}$.

A significant parameter throughout this and the following sections is the number c of coordinate vertices of $\mathbb{P}^2$ in $\mathcal{B}$. For example, if $(0 : 0 : 1)$ and $(0 : 1 : 0)$ are in $\mathcal{B}$, then $c = 2$. Note that we always have $c = 0$, 1 or 2 when the points of $\mathcal{B}$ are contained in the line $x = 0$. We will also frequently refer to the set $\mathcal{S} := Z(x) \setminus \{(0 : 0 : 1), (0 : 1 : 0)\}$. Table A.1 in Appendix A shows the parameters for a family of codes $C^h(\mathcal{B}, \mathcal{P}, [D])$ with $\mathcal{B} \subset Z(x)$, $\mathcal{P}$ the standard set, $[D] = [bL - E_1 - \cdots - E_b]$ and $c = 2$.

An important method of proof in this and the next section is to bound the number of zeros of a function $0 \neq f \in F([D])$ on "vertical" lines in $\mathbb{P}^2$, i.e., lines defined by polynomials in $\langle y, z\rangle \subset R_m$. Similarly, by a "horizontal" line, we mean a line defined by a polynomial in $\langle x, z\rangle \subset R_m$. Figure 4.2.1 shows all the vertical and horizontal lines in $\mathbb{P}^2(\mathbb{F}_5)$.

Figure 4.2.1: Horizontal and Vertical Lines in $\mathbb{P}^2(\mathbb{F}_5)$



We begin with a lemma which demonstrates the existence of a polynomial $f \in F([D])$ with $b(q-1) - c(b-c)$ zeros. This result will help us to obtain an upper bound on the minimum distance and to show that if f maximizes $|Z(f) \cap \mathcal{P}|$, then f must be a product of linear polynomials (Corollary 4.2.2).

Lemma 4.2.1. *Let $\mathcal{B} \subset Z(x)$, $[D] = [bL - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set and c be the number of coordinate vertices of $\mathbb{P}^2$ in $\mathcal{B}$. Then for all q and b such that $q - 1 \geq b > c$, there exists a function $f \in F([D])$ which is a product of linear polynomials and satisfies $|Z(f) \cap \mathcal{P}| = b(q-1) - c(b-c)$.*

Proof. If $c = 0$, let the factors of f be those corresponding to the vertical lines through the points of $\mathcal{B}$. Then $|Z(f) \cap \mathcal{P}| = b(q-1)$ since each line contains $q-1$ points in $\mathcal{P}$ and none of these lines intersect in $\mathcal{P}$.

If $c = 1$, let $b - 1$ of the factors of f correspond to the vertical lines through the points of $\mathcal{B} \cap \mathcal{S}$. If $(0 : 0 : 1) \in \mathcal{B}$, let the remaining factor of f be $(x - y)$. If $(0 : 1 : 0) \in \mathcal{B}$, let the remaining factor of f be $(x - z)$. Since the lines $x = y$ and $x = z$ pass through each of the $b - 1$ vertical lines exactly once in $\mathcal{P}$, in either case f has exactly $b(q-1) - (b-1)$ zeros in $\mathcal{P}$.

If $c = 2$, the function f is a little more complicated. Let $V_{\mathcal{B}}$ be the set of functions in R_1 (homogeneous linear polynomials in $\mathbb{F}_q[x, y, z]$) whose zero sets are vertical lines through points of $\mathcal{B} \cap \mathcal{S}$. Fix a factor $h = (y - \gamma^i z) \in V_{\mathcal{B}}$, where γ is a generator of the multiplicative group $\mathbb{F}_q^*$ and $i \in \{0, ..., q-2\}$. We know there exists such an h since $b > 2$ and $\mathcal{B} \subset Z(x)$. Let f be the function whose factors are those of $V_{\mathcal{B}}$ together with $(x-y)$ and $(x-\gamma^i z)$. Since $f(p) = 0$ for all $p \in \mathcal{B}$ we have that $f \in F([D])$.

Each factor of f has $(q-1)$ distinct zeros in $\mathcal{P}$. Three of its factors, $(x-y)$, $(x-\gamma^i z)$ and $h = (y-\gamma^i z)$, have one common zero, $(\gamma^i : \gamma^i : 1)$, in $\mathcal{P}$, so these three factors have $3(q-1)-2$ distinct zeros. The remaining $b-3$ factors of f are of the form $(y-\gamma^j z)$, $j \neq i$, and have no zeros in $\mathcal{P}$ in common with each other. Each has exactly two zeros, namely, $(\gamma^j : \gamma^j : 1)$ and $(\gamma^i : \gamma^j : 1)$, in common with the first three factors. Hence the number of distinct zeros of f in $\mathcal{P}$ is $3(q-1)-2+(b-3)(q-1)-2(b-3) = b(q-1)-2(b-2)$. □

Now we can say something interesting about a function $f \in F([D])$ which maximizes $|Z(f) \cap \mathcal{P}|$: we can say that f must be a product of linear polynomials.

Corollary 4.2.2. *Let $\mathcal{B} \subset Z(x)$, $\mathcal{P}$ be the standard set and c be the number of coordinate vertices of $\mathbb{P}^2$ in $\mathcal{B}$. Let $[D] = [bL - E_1 - \cdots - E_b]$. Let $0 \neq f \in F([D])$ such that $|Z(f) \cap \mathcal{P}|$ is as large as possible. If $q-1 \geq b > c$ and $q-b > c(b-c)$, then f is a product of linear polynomials, none of which is x, y or z.*

Proof. The fact that f is a product of linear polynomials follows from Lemma 4.1.7 and Lemma 4.2.1 since in this case,

$$\begin{aligned} m(q-1) - \left(q - 2m + \sum_{i=1}^{b} m_i\right) &= b(q-1) - \left(q - 2b + \sum_{i=1}^{b} 1\right) \\ &= b(q-1) - (q-b) \\ &< b(q-1) - c(b-c). \end{aligned}$$

Moreover, if a function $g \in F([D])$ contains x, y or z as a factor, then $|Z(g) \cap \mathcal{P}| \leq b(q-1) - (q-1) < b(q-1) - c(b-c)$. □

The next lemma will help us to obtain a lower bound on the minimum distance in the case where $c = 2$.

Lemma 4.2.3. *Suppose* $(0 : 0 : 1), (0 : 1 : 0) \in \mathcal{B} \subset Z(x)$ *and* $b > 2$. *Let* $[D] = [bL - E_1 - \cdots - E_b]$ *and* $\mathcal{P}$ *be the standard set. Let* $0 \neq f \in F([D])$. *Suppose* f *is a product of linear polynomials, none of which is* x, y *or* z, *and none of which give vertical lines through points of* $\mathcal{S} = Z(x) \setminus \{(0 : 0 : 1), (0 : 1 : 0)\}$. *Then* $|Z(f) \cap \mathcal{P}| \leq b(q-1) - 2(b-2)$.

Proof. Since f is a product of b linear factors, none of which is x, there is a one-to-one correspondence between the factors of f and the points of $\mathcal{B}$, i.e., for each point $p \in \mathcal{B}$, there is exactly one linear factor whose zero set includes p.

Let $l_1, ..., l_{b-2}$ be the linear factors of f whose zero sets $L_1, ..., L_{b-2}$ pass through the points of $\mathcal{B} \cap \mathcal{S}$. Let l' and l'' be the factors whose zero sets L' and L'' pass through $(0 : 0 : 1)$ and $(0 : 1 : 0)$, respectively.

We wish to bound $|Z(f) \cap \mathcal{P}| = \left| \left(L' \cup L'' \cup \bigcup_{i=1}^{b-2} L_i \right) \cap \mathcal{P} \right|$. Since no L_i is a vertical line and since every line in $\mathbb{P}^2(\mathbb{F}_q)$ passes through the three coordinate axes, we know $|L_i \cap \mathcal{P}| = q - 2$ for $i = 1, ..., b-2$. Hence, by the Principle of Inclusion and Exclusion, the number of zeros in $\mathcal{P} \cap \bigcup_{i=1}^{b-2} L_i$ is

$$(b-2)(q-2) - \sum_{I \subset \{1,...,b-2\}, |I| \geq 2} (-1)^{|I|} |L_I \cap \mathcal{P}|,$$

where $L_I = \bigcap_{i \in I} L_i$.

The lines L' and L'' each contain $q-1$ zeros in $\mathcal{P}$ since they pass through coordinate vertices of $\mathbb{P}^2$, and they have one zero in $\mathcal{P}$ in common. Hence the number of additional zeros coming from $(L' \cup L'') \cap \mathcal{P}$ is

$$(2(q-1)-1) - \sum_{i=1}^{b-2} |L_i \cap (L' \cup L'') \cap \mathcal{P}| + \sum_{I \subset \{1,\dots,b-2\}, |I| \geq 2} (-1)^{|I|} |L_I \cap (L' \cup L'') \cap \mathcal{P}|,$$

where $L_I = \bigcap_{i \in I} L_i$ as before.

Note that every L_i will pass through $(L' \cup L'')$ at one or more points of $\mathcal{P}$ with one possible exception: if the line L joining the point of $L' \cap Z(z)$ and the point of $L'' \cap Z(y)$ is one of the L_i's, then for this line alone, we will have $|L \cap (L' \cup L'') \cap \mathcal{P}| = 0$. Hence $\sum_{i=1}^{b-2} |L_i \cap (L' \cup L'') \cap \mathcal{P}| \geq b-3$.

Next note that $|L_I \cap (L' \cup L'') \cap \mathcal{P}| \leq |L_I \cap \mathcal{P}|$ for all $I \subset \{1, ..., b-2\}$. Using this fact, we have that the total number of zeros in $\left(L' \cup L'' \cup \bigcup_{i=1}^{b-2} L_i\right) \cap \mathcal{P}$ is no more than

$$(b-2)(q-2) + 2(q-1) - 1 - (b-3) = b(q-1) - 2(b-2).$$

□

We now show that any $0 \neq f \in F([D])$ must satisfy $|Z(f) \cap \mathcal{P}| \leq b(q-1) - c(b-c)$. Combining this with Lemma 4.2.1 allows us to obtain an exact result on the minimum distance for the divisor class $[D] = [bL - E_1 - \cdots - E_b]$ (see Theorem 4.2.5).

Lemma 4.2.4. *Let $\mathcal{B} \subset Z(x)$, $\mathcal{P}$ be the standard set, and c be the number of coordinate vertices of $\mathbb{P}^2$ in $\mathcal{B}$. Let $[D] = [bL - E_1 - \cdots - E_b]$. If $q-1 \geq b > c$ and $q - b > c(b-c)$, then*

$$\max\{|Z(f) \cap \mathcal{P}| : f \in F([D]), f \not\equiv 0\} = b(q-1) - c(b-c).$$

Proof. By Lemma 4.2.1, we have that $\max\{|Z(f) \cap \mathcal{P}| : f \in F([D]), f \not\equiv 0\} \geq b(q-1) - c(b-c)$. So we have left to show the other inequality.

Let $f \in F([D])$ such that $f \not\equiv 0$. By Corollary 4.2.2, since we wish to find an upper bound for $|Z(f) \cap \mathcal{P}|$, we may assume that f is a product of linear factors, none of which is x, y or z. Let V be the set of distinct linear factors of f whose zero sets are vertical lines through points of $\mathcal{S}$. Let $V_{\mathcal{B}} \subset V$ be the factors in V whose zero sets pass through a point of $\mathcal{B}$. Let $v = |V|$ and let $v_{\mathcal{B}} = |V_{\mathcal{B}}|$. Let $f' = \dfrac{f}{\prod_{g \in V} g^{m_g}}$, where m_g is the multiplicity of the factor g of f.

We wish to bound $|Z(f) \cap \mathcal{P}|$. We do this by summing the maximum number of zeros of f on each of the $q-1$ vertical lines through the points of $\mathcal{S}$. A vertical line ℓ through a point of $\mathcal{S}$ falls into one of the following three categories:

(1) ℓ is the zero set of a factor in V

(2) ℓ is not the zero set of a factor in V but ℓ passes through a point of $\mathcal{B}$

(3) ℓ is not the zero set of a factor in V but ℓ passes through a point of $\mathcal{S} \setminus \mathcal{B}$

There are v lines in case (1), each of which contains $q-1$ distinct zeros of f in $\mathcal{P}$. When considering cases (2) and (3), we need only bound the number of zeros of f' since all the zeros of $\prod_{g \in V} g^{m_g}$ have been counted. There are $(b-c) - v_{\mathcal{B}}$ lines in case (2). Since $deg(f') \leq deg(f) - v = b - v$ and since f' must pass through all the points of $\mathcal{B}$ which are not contained in lines of V, we know $Z(f') \cap \mathcal{P}$ has at most $b - v - 1$ points on a line in case (2). There are $(q-1) - v - ((b-c) - v_{\mathcal{B}})$ lines in case (3). Each of these lines contains at most $b - v$ zeros of f'. Thus, the maximum number of zeros of f in $\mathcal{P}$ is

$$\begin{aligned} N &\leq v(q-1) + ((b-c) - v_{\mathcal{B}})(b-v-1) + ((q-1) - v - ((b-c) - v_{\mathcal{B}}))(b-v) \\ &= v(q-1) + (q-1-v)(b-v) - (b-c) + v_{\mathcal{B}}. \qquad (4.5) \end{aligned}$$

We know $0 \leq v_{\mathcal{B}} \leq v \leq b = deg(f)$ and $0 \leq v_{\mathcal{B}} \leq b - c$. If $c = 1$ or $c = 2$, we cannot cover all the points of $\mathcal{B}$ with vertical lines through points of $\mathcal{S}$, so in these two cases we must have $v \leq b-1$. Furthermore, if $c = 2$ and $v = b-1$, then the only way for f to vanish at the remaining two points of $\mathcal{B}$ is for f to have x as a factor, which we assumed is not the case. Hence we have must have $0 \leq v_{\mathcal{B}} \leq v \leq b-c$ for $c = 0$, 1 and 2.

We see that the right-hand side of (4.5) is largest when $v_{\mathcal{B}}$ is as large as possible, so we rewrite it setting $v_{\mathcal{B}} = v$ to obtain

$$N \leq v(q-1) + (q-1-v)(b-v) - (b-c) + v.$$

This simplifies to

$$N \leq v^2 + (1-b)v + (b(q-1) - (b-c)). \tag{4.6}$$

The right-hand side of (4.6) achieves its maximum value at one of the endpoints $v = 0$ or $v = b-c$. If $v = b-c$ we obtain $b(q-1) - c(b-c)$ and if $v = 0$ we obtain $N \leq b(q-1) - (b-c)$. However, in the case where $v = 0$ and $c = 2$ we know by Lemma 4.2.3 that in fact $N \leq b(q-1) - 2(b-2)$. The right-hand side of (4.6) is equal to $b(q-1) - 2(b-2)$ when $c = 2$ and $v = 1$ (the next smallest value of v to consider). Thus, the maximum number of zeros of a function $f \in F([D])$ such that $f \neq 0$ is $b(q-1) - c(b-c)$. □

We now have an exact result on the minimum distance for $C^h(\mathcal{B}, \mathcal{P}, [D])$ when $[D] = [bL - E_1 - \cdots - E_b]$ and $\mathcal{B} \subset Z(x)$.

Theorem 4.2.5. *Let $\mathcal{B} \subset Z(x)$, $\mathcal{P}$ be the standard set and c be the number of coordinate vertices of $\mathbb{P}^2$ in $\mathcal{B}$. Let $[D] = [bL - E_1 - \cdots - E_b]$. If $q-1 > b > c$ and $q-b > c(b-c)$, then $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = z^m$) is a*

$$\left[(q-1)^2, \frac{b^2+b+2}{2}, (q-1)^2 - b(q-1) + c(b-c)\right] \textit{ code.}$$

Proof. By Proposition 4.1.8, the dimension of $C^h(\mathcal{B}, \mathcal{P}, [D])$ is equal to

$$\binom{b+2}{2} - \sum_{i=1}^{b} \binom{1+1}{2} = \frac{b^2+b+2}{2}.$$

The minimum distance is

$$\begin{aligned} d_{C^h(\mathcal{B},\mathcal{P},[D])} &= (q-1)^2 - \max\left\{ \left| Z\left(\frac{f}{h}\right) \cap \mathcal{P} \right| : \frac{f}{h} \in L^h([D]), \frac{f}{h} \not\equiv 0 \right\} \\ &= (q-1)^2 - \max\left\{ |Z(f) \cap \mathcal{P}| : f \in F\left([D]\right), f \not\equiv 0 \right\} \\ &= (q-1)^2 - b(q-1) + c(b-c), \end{aligned}$$

where the last line holds by Lemma 4.2.4.

□

Example 4.2.6. Let $\mathcal{B} = \{(0:0:1), (0:1:0), (0:1:1), (0:\gamma:1), (0:\gamma^2:1)\}$, where γ is a generator of the multiplicative group $\mathbb{F}_q^*$. Then $b = 5$ and $c = 2$. Note that $q = 16$ satisfies the hypotheses of Theorem 4.2.5. Hence the anticanonical surface code $C^h(\mathcal{B}, \mathcal{P}, [D])$ has length $15^2 = 225$, dimension $\frac{5^2+5+2}{2} = 16$ and minimum distance $15^2 - 5 \cdot 15 + 2(5-2) = 156$. The guaranteed minimum distance from the Varshamov-Gilbert Bound (Proposition 3.1.6) is 170.

4.3 Results for Blowing Up Points on Two Lines

In this section we consider the more general case where $\mathcal{B} \subset Z(xy)$. We consider two extreme cases: first, where the number of coordinate vertices in $\mathcal{B}$ is $c = 0$ and second, where $c = 3$. We will again obtain an exact result on the minimum distance for a specific divisor class, but we will also need the configuration of the points of $\mathcal{B}$ to meet certain criteria (see Theorems 4.3.1.8 and 4.3.2.8). For more general configurations, we obtain upper and lower bounds on the minimum distance (see Theorems 4.3.1.4 and 4.3.2.4).

Let $\mathcal{S} = Z(x) \setminus \{(0:1:0), (0:0:1)\}$ and let $\mathcal{R} = Z(y) \setminus \{(0:0:1), (1:0:0)\}$. Let $s = |\mathcal{S} \cap \mathcal{B}|$ and $r = |\mathcal{R} \cap \mathcal{B}|$. Without loss of generality, we assume $s \geq r$. We also need to assume $r \geq 1$ for the proofs in this section. This is a reasonable assumption for nontrivial two-line codes.

4.3.1 Two-Line Codes with $c = 0$

Here we assume that $c = 0$, $s \geq 2$ and $s \geq r \geq 1$. Note that $s \geq 2$ is a reasonable assumption: if $s = r = 1$ and $c = 0$ then the points of $\mathcal{B}$ lie on a single line.

Analogous to the previous section, we primarily work with $[D] = [sL - E_1 - \cdots - E_b]$, since s is the minimum value of m such that $[mL - E_1 - \cdots - E_b]$ is numerically effective (see Section 2.3 or Proposition I.5.3 of [12]). Table A.2 in Appendix A gives the parameters for a family of codes $C^h(\mathcal{B}, \mathcal{P}, [D])$ with $\mathcal{B} \subset Z(xy)$, $\mathcal{P}$ the standard set, $[D] = [sL - E_1 - \cdots - E_b]$ and $c = 0$.

Our first lemma will lead to an upper bound on the minimum distance and help us to show that any nonzero function which maximizes $|Z(f) \cap \mathcal{P}|$ must be a product of linear polynomials (Corollary 4.3.1.2).

Lemma 4.3.1.1. *Let $[D] = [sL - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 0$, $s \geq 2$ and $s \geq r \geq 1$. Then there exists a function $f \in F([D])$ which is a product of linear polynomials and satisfies $|Z(f) \cap \mathcal{P}| \geq s(q-1) - \left(sr - \binom{r}{2}\right)$. (Here we use the convention $\binom{r}{2} = 0$ if $r < 2$.)*

Proof. Let $s - r$ of the factors of f correspond to vertical lines through distinct points of $\mathcal{S} \cap \mathcal{B}$. These factors contribute $(s-r)(q-1)$ zeros to $|Z(f) \cap \mathcal{P}|$.

Let the remaining r factors of f correspond to lines connecting the remaining points of $\mathcal{S}$ to the points of $\mathcal{R} \cap \mathcal{B}$. (There will be one line for each pair of points.) These factors have $r(q-2)$ zeros but may intersect with the previous factors and with each other. The number of points of intersection (counted with appropriate multiplicities) is no more than $r(s-r) + \binom{r}{2} = r(s-r) + \frac{1}{2}r(r-1)$. Hence these r factors contribute at least $r(q-2) - r(s-r) - \frac{1}{2}r(r-1)$ zeros to $|Z(f) \cap \mathcal{P}|$. Adding the two quantities of zeros together and simplifying, we have that

$$\begin{aligned} |Z(f) \cap \mathcal{P}| &\geq (s-r)(q-1) + r(q-2) - r(s-r) - \frac{1}{2}r(r-1) \\ &= s(q-1) - \left(sr - \binom{r}{2}\right). \end{aligned}$$

□

Corollary 4.3.1.2. *Let $[D] = [sL - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 0$, $s \geq 2$ and $s \geq r \geq 1$. Suppose q satisfies $q - 2s + b > sr - \binom{r}{2}$. Then any function $f \in F([D])$ maximizing $|Z(f) \cap \mathcal{P}|$ is a product of linear polynomials.*

Proof. Since $s(q-1) - (q - 2s + b) < s(q-1) - \left(sr - \binom{r}{2}\right)$, by Lemma 4.1.7 and Lemma 4.3.1.1, we know that a function $f \in F([D])$ maximizing $|Z(f) \cap \mathcal{P}|$ must be a product of linear polynomials. □

The next lemma will lead to a lower bound on the minimum distance for an anticanonical surface code with $\mathcal{B} \subset Z(xy)$, $c = 0$ and $[D] = [sL - E_1 - \cdots - E_b]$.

Lemma 4.3.1.3. *Let $[D] = [sL - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 0$, $s \geq 2$ and $s \geq r \geq 1$. Suppose q satisfies $q - 2s + b > sr - \binom{r}{2}$. Then*

$$\max\{|Z(f) \cap \mathcal{P}| : f \in F([D]), f \not\equiv 0\} \leq s(q-1) - s.$$

Proof. The notation and method of proof are similar to that of Lemma 4.2.4. Let $f \in F([D])$ such that $f \not\equiv 0$. By Corollary 4.3.1.2, since we wish to find an upper bound for $|Z(f) \cap \mathcal{P}|$, we may assume that f is a product of linear polynomials over $\mathbb{F}_q$. Let V be the set of distinct linear factors of f whose zero sets are vertical lines through points of $\mathcal{S} := Z(x) \setminus \{(0:0:1),(0:1:0)\}$. Let $V_{\mathcal{B}} \subset V$ be the factors in V whose zero sets pass through a point of $\mathcal{B}$. Let $v = |V|$ and let $v_{\mathcal{B}} = |V_{\mathcal{B}}|$. Let $f' = \dfrac{f}{\prod_{g \in V} g^{m_g}}$, where m_g is the multiplicity of the factor g of f.

We wish to bound $|Z(f) \cap \mathcal{P}|$. We do this by summing the maximum number of zeros of f on each of the $(q-1)$ vertical lines through the points of $\mathcal{S}$. A vertical line ℓ through a point of $\mathcal{S}$ falls into one of the following three categories:

(1) ℓ is the zero set of a factor in V

(2) ℓ is not the zero set of a factor in V but ℓ passes through a point of $\mathcal{B}$

(3) ℓ is not the zero set of a factor in V but ℓ passes through a point of $\mathcal{S} \setminus \mathcal{B}$

There are v such lines in case (1), each of which contains $q-1$ distinct zeros of f in $\mathcal{P}$. When considering cases (2) and (3), we need only bound the number of zeros of f' since all the zeros of $\prod_{g \in V} g^{m_g}$ have been counted. There are $s - v_{\mathcal{B}}$ lines in case (2). Since $deg(f') \leq deg(f) - v = s - v$ and since f' must pass through all the points of $\mathcal{B}$ which are not contained in lines of V, we know $Z(f') \cap \mathcal{P}$ has at most $s - v - 1$ points on a line in case (2). There are $(q-1) - v - (s - v_{\mathcal{B}})$ lines in case (3). Each of these lines contains at most $s - v$ zeros of f'. Thus, the maximum number of zeros of f in $\mathcal{P}$ is

$$\begin{aligned} N &\leq v(q-1) + (s - v_{\mathcal{B}})(s - v - 1) + ((q-1) - v - (s - v_{\mathcal{B}}))(s - v) \\ &= v(q-1) + (q-1-v)(s-v) - s + v_{\mathcal{B}}. \end{aligned} \tag{4.7}$$

In order for f to vanish at the points of $\mathcal{R} \cap \mathcal{B}$ not all the factors of f can be in V. Since $deg(f) = s$, we must have $v \leq s - 1$. Hence $0 \leq v_{\mathcal{B}} \leq v \leq s - 1$.

We see that the right-hand side of (4.7) is largest when $v_{\mathcal{B}}$ is as large as possible, so we rewrite it setting $v_{\mathcal{B}} = v$ to obtain

$$N \leq v(q-1) + (q-1-v)(s-v) - s + v.$$

This simplifies to

$$N \leq v^2 + (1-s)v + (s(q-1) - s). \tag{4.8}$$

The right-hand side of (4.8) achieves its maximum value at one of the endpoints $v = 0$ or $v = s - 1$. If $v = 0$ or $v = s - 1$, we obtain $s(q-1) - s$. Thus, the maximum number of zeros of a function $0 \neq f \in F([D])$ is $s(q-1) - s$. □

Combining Lemmas 4.3.1.1 and 4.3.1.3 gives us the following theorem.

Theorem 4.3.1.4. *Let* $[D] = [sL - E_1 - \cdots - E_b]$, $\mathcal{P}$ *be the standard set,* $c = 0$, $s \geq 2$ *and* $s \geq r \geq 1$. *Suppose further that* $q - 2s + b > sr - \binom{r}{2}$ *and* $q \geq s + 2$. *Then* $C^h(\mathcal{B}, \mathcal{P}, [D])$ *(with* $h = z^m$*) is a*

$$\left[(q-1)^2, \binom{s+2}{2} - b, d\right] \text{ code, where}$$

$$(q-1)^2 - s(q-1) + s \leq d \leq (q-1)^2 - s(q-1) + \left(sr - \binom{r}{2}\right).$$

Proof. The dimension holds by Proposition 4.1.8. Noting that

$$d = (q-1)^2 - \max\{|Z(f) \cap \mathcal{P}| : f \in F([D]), f \not\equiv 0\},$$

the bounds on d hold by Lemmas 4.3.1.3 and 4.3.1.1. □

Remark. The upper bound in Theorem 4.3.1.4 is equal to the lower bound when $r = 1$, so in this case we have an exact result for the minimum distance. The upper bound is strictly greater than the lower bound when $r > 1$.

We now give two examples to show that it is possible to attain the upper bound in Theorem 4.3.1.4 as well as intermediate values for the minimum distance when $r > 1$.

Example 4.3.1.5. Let $q = 8$ and let γ be a generator for $\mathbb{F}_q^*$. Let

$$\mathcal{B} = \{(0 : 1 : 1), (0 : \gamma^2 : 1), (1 : 0 : 1), (\gamma : 0 : 1)\}.$$

Then $s = r = 2$ and $c = 0$. Note that q, c, s and r satisfy the hypotheses of Theorem 4.3.1.4 and so we have $n = 49$, $k = 2$ and $37 \leq d \leq 38$. A Magma [3] computation yields $d = 38$. The guaranteed minimum distance from the Varshamov-Gilbert Bound (Proposition 3.1.6) is 40. The best known linear code with the same q, length and dimension has $d = 43$ [9].

Example 4.3.1.6. Let $q = 9$ and let γ be a generator for $\mathbb{F}_q^*$. Let

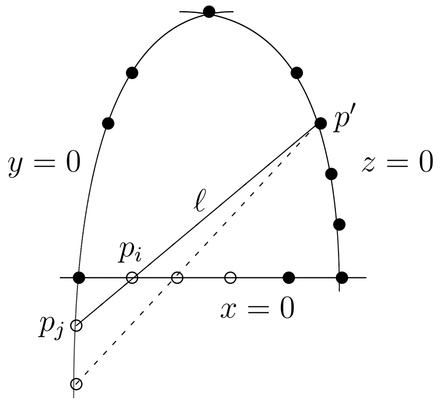
$$\mathcal{B} = \{(0 : 1 : 1), (0 : \gamma^2 : 1), (0 : \gamma^4 : 1)\} \cup \{(1 : 0 : 1), (\gamma : 0 : 1), (\gamma^3 : 0 : 1)\}.$$

Then $s = r = 3$ and $c = 0$. Note that q, c, s and r satisfy the hypotheses of Theorem 4.3.1.4 and so we have $n = 64$, $k = 4$ and $43 \leq d \leq 46$. A Magma [3] computation yields $d = 45$. The guaranteed minimum distance from the Varshamov-Gilbert Bound (Proposition 3.1.6) is 49. The best known linear code with the same q, length and dimension has $d = 54$ [9].

The next lemma will be used to obtain an upper bound on the minimum distance when the points of $\mathcal{B}$ satisfy certain criteria. This upper bound is equal to the lower bound on d from Theorem 4.3.1.4, as we will see in the proof of Theorem 4.3.1.8.

Lemma 4.3.1.7. *Let $[D] = [sL - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 0$, $s \geq 2$ and $q - 1 \geq s \geq r \geq 1$. Let p_i be a point of $\mathcal{S} \cap \mathcal{B}$ and let p_j be a point of $\mathcal{R} \cap \mathcal{B}$. Let ℓ be the line through p_i and p_j. Let p' be the point of intersection of ℓ and the line defined by $z = 0$. Suppose that the points of $\mathcal{B}$ are arranged so that all $r - 1$ of the lines joining p' with the points of $(\mathcal{R} \cap \mathcal{B}) \setminus \{p_j\}$ pass through distinct points of $(\mathcal{S} \cap \mathcal{B}) \setminus \{p_i\}$ (see Figure 4.3.1.1). Then there exists a function $f \in F([D])$ such that $|Z(f) \cap \mathcal{P}| = s(q-1) - s$.*

Figure 4.3.1.1: Meeting the conditions of Lemma 4.3.1.7 for $q = 5$



Proof. Let one of the factors of f correspond to the line ℓ through p_i and p_j. Let $r-1$ of the factors of f correspond to the lines through p' and the points of $(\mathcal{R} \cap \mathcal{B}) \setminus \{p_j\}$. Finally, let the remaining $s - r$ factors of f correspond to the lines through p' and the points of $\mathcal{S} \cap \mathcal{B}$ not yet covered by lines.

Each of the s lines has $q-2$ zeros and the only intersection point of the lines is p', which is not in the standard set $\mathcal{P}$. Hence $|Z(f) \cap \mathcal{P}| = s(q-2) = s(q-1) - s$. □

Remark. It is not too difficult to show that the point set

$$\mathcal{B} = \{(0:1:1), (0:\gamma:1), ..., (0:\gamma^{s-1}:1)\} \cup \{(1:0:1), (\gamma:0:1), ..., (\gamma^{r-1}:0:1)\}$$

satisfies the conditions of Lemma 4.3.1.7. If we let $p_i = (0:1:1)$ and $p_j = (1:0:1)$, then $p' = (1 : -1 : 0)$. The line ℓ_i through $(\gamma^i : 0 : 1)$ and p' also passes through $(0 : \gamma^i : 1)$ for $i = 1, ..., r-1$.

Theorem 4.3.1.8 states that when the points of $\mathcal{B}$ satisfy the conditions of Lemma 4.3.1.7, the lower bound of Theorem 4.3.1.4 is sharp. Thus we see that the arrangement of the points on $Z(xy)$ affects the minimum distance d and that our lower bound cannot be improved without additional restrictions on the distribution of the points of $\mathcal{B}$.

Theorem 4.3.1.8. *Let $[D] = [sL - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 0$, $s \geq 2$ and $s \geq r \geq 1$. Suppose the points of $\mathcal{B}$ are arranged to meet the conditions in Lemma 4.3.1.7. Suppose further that $q - 2s + b > sr - \binom{r}{2}$ and $q \geq s + 2$. Then $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = z^m$) is a*

$$\left[(q-1)^2, \binom{s+2}{2} - b, (q-1)^2 - s(q-1) + s\right] \text{ code.}$$

Proof. The lower bound on d in Theorem 4.3.1.4 is now exact since Lemma 4.3.1.7 demonstrates the existence of a function with $s(q-1) + s$ zeros in $\mathcal{P}$. □

Example 4.3.1.9. Let $q = 7$. Then 3 is a generator of $\mathbb{F}_7^*$. Let

$$\mathcal{B} = \{(0:1:1), (0:2:1), (0:3:1)\} \cup \{(1:0:1), (3:0:1)\}.$$

Then $s = 3$, $r = 2$ and $c = 0$. Note that q, c, s and r satisfy the hypotheses of both Lemma 4.3.1.7 and Theorem 4.3.1.8. One can check that the line through $(0 : 1 : 1)$ and $(1 : 0 : 1)$ is defined by $x + y - z = 0$ and passes through the point $p' = (1 : -1 : 0)$ in $Z(x)$. The line through p' and $(3 : 0 : 1)$ is defined by $x + y - 3z = 0$ and passes through $(0 : 3 : 1) \in \mathcal{S} \cap \mathcal{B}$. Hence the points of $\mathcal{B}$ satisfy the hypothesis of Lemma 4.3.1.7 and so by Theorem 4.3.1.8 we have $n = 36$, $k = 5$

and $d = 21$. The guaranteed minimum distance from the Varshamov-Gilbert Bound (Proposition 3.1.6) is 23.

4.3.2 Two-Line Codes with $c = 3$

Now we consider the case where $c = 3$, i.e., we assume that $(0:0:1)$, $(0:1:0)$, $(1:0:0) \in \mathcal{B}$. Here we only assume $s \geq r \geq 1$ (and not $s \geq 2$) since $s = r = 1$ does not imply that the points of $\mathcal{B}$ lie on a line when $c = 3$.

We work with the divisor class $[D] = [(s+2)L - E_1 - \cdots - E_b]$, since in this case $s+2$ is the minimum value of m such that $[mL - E_1 - \cdots - E_b]$ is numerically effective (see Section 2.3 or Proposition I.5.3 of [12]). Table A.3 in Appendix A shows the parameters for a family of codes $C^h(\mathcal{B}, \mathcal{P}, [D])$ with $\mathcal{B} \subset Z(xy)$, $\mathcal{P}$ the standard set, $[D] = [(s+2)L - E_1 - \cdots - E_b]$ and $c = 3$.

Our first lemma will lead to an upper bound on the minimum distance and help us to show that any nonzero function which maximizes $|Z(f) \cap \mathcal{P}|$ must be a product of linear polynomials (Corollary 4.3.2.2).

Lemma 4.3.2.1. *Let $[D] = [(s+2)L - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 3$ and $s \geq r \geq 1$. Then there exists a function $f \in F([D])$ which is a product of linear polynomials and satisfies $|Z(f) \cap \mathcal{P}| \geq (s+2)(q-1) - \left(s(r+1) - \binom{r-1}{2}\right)$. (Here we use the convention $\binom{r-1}{2} = 0$ if $r - 1 < 2$.)*

Proof. Let one of the factors of f correspond to the vertical line through a point $p_i \in \mathcal{S} \cap \mathcal{B}$. Let another factor of f correspond to the horizontal line through a point $p_j \in \mathcal{R} \cap \mathcal{B}$. Let a third factor of f correspond to the line through $(0:0:1)$ and the point where the first two factors of f intersect. Note that these three factors contribute exactly $3(q-1) - 2$ zeros to $|Z(f) \cap \mathcal{P}|$.

Let $s-r$ of the factors of f correspond to vertical lines through distinct points of $(\mathcal{S}\cap\mathcal{B})\setminus\{p_i\}$. These factors contribute $(s-r)(q-1)-2(s-r)$ new zeros to $|Z(f)\cap\mathcal{P}|$.

Let the remaining $r-1$ factors of f correspond to lines connecting the remaining points of $\mathcal{S}\cap\mathcal{B}$ to the points of $(\mathcal{R}\cap\mathcal{B})\setminus\{p_j\}$. (There will be one line for each pair of points.) These factors have $(r-1)(q-2)$ zeros but may intersect with the previous factors and with each other. The number of points of intersection (counted with appropriate multiplicities) is no more than $(r-1)(s-r+3)+\binom{r-1}{2}=(r-1)(s-r+3)+\frac{1}{2}(r-1)(r-2)$. Hence these $r-1$ factors contribute at least $(r-1)(q-2)-(r-1)(s-r+3)-\frac{1}{2}(r-1)(r-2)$ zeros to $|Z(f)\cap\mathcal{P}|$.

Adding the three quantities of zeros together and simplifying, we have that

$$\begin{aligned}|Z(f)\cap\mathcal{P}| &\geq (s+2)(q-1)-(2s+((s-r)+2)(r-1)+\frac{1}{2}(r-1)(r-2))\\ &= (s+2)(q-1)-\left(s(r+1)-\binom{r-1}{2}\right).\end{aligned}$$

□

Corollary 4.3.2.2. *Let $[D]=[(s+2)L-E_1-\cdots-E_b]$, $\mathcal{P}$ be the standard set, $c=3$ and $s\geq r\geq 1$. Suppose q satisfies $q-2(s+2)+b>s(r+1)-\binom{r-1}{2}$. Then any function $f\in F([D])$ maximizing $|Z(f)\cap\mathcal{P}|$ is a product of linear polynomials.*

Proof. Since $(s+2)(q-1)-(q-2(s+2)+b)<(s+2)(q-1)-\left(s(r+1)-\binom{r-1}{2}\right)$, by Lemma 4.1.7 and Lemma 4.3.2.1, we know that a function $f\in F([D])$ maximizing $|Z(f)\cap\mathcal{P}|$ must be a product of linear polynomials. □

The next lemma will lead to a lower bound on the minimum distance for an anticanonical surface code $C^h(\mathcal{B},\mathcal{P},[D])$ with $\mathcal{B}\subset Z(xy)$, $c=3$ and $[D]=[(s+2)L-E_1-\cdots-E_b]$.

Lemma 4.3.2.3. *Let $[D] = [(s+2)L - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 3$ and $s \geq r \geq 1$. Suppose q satisfies $q - 2(s+2) + b > s(r+1) - \binom{r-1}{2}$ and $q - 1 \geq 2s$. Then*

$$\max\{|Z(f) \cap \mathcal{P}| : f \in F\left([D]\right), f \not\equiv 0\} \leq (s+2)(q-1) - 2s.$$

Proof. The notation and method of proof are similar to that of Lemma 4.2.4. Let $f \in F\left([D]\right)$ such that $f \not\equiv 0$. By Corollary 4.3.2.2, since we wish to find an upper bound for $|Z(f) \cap \mathcal{P}|$, we may assume that f is a product of linear polynomials over $\mathbb{F}_q$. Let V be the set of distinct linear factors of f whose zero sets are vertical lines through points of $\mathcal{S} := Z(x) \setminus \{(0:0:1),(0:1:0)\}$. Let $V_{\mathcal{B}} \subset V$ be the factors in V whose zero sets pass through a point of $\mathcal{B}$. Let $v = |V|$ and let $v_{\mathcal{B}} = |V_{\mathcal{B}}|$. Let $f' = \dfrac{f}{\prod_{g \in V} g^{m_g}}$, where m_g is the multiplicity of the factor g of f.

We wish to bound $|Z(f) \cap \mathcal{P}|$. We do this by summing the maximum number of zeros of f on each of the $(q-1)$ vertical lines through the points of $\mathcal{S}$. A vertical line ℓ through a point of $\mathcal{S}$ falls into one of the following three categories:

(1) ℓ is the zero set of a factor in V

(2) ℓ is not the zero set of a factor in V but ℓ passes through a point of $\mathcal{B}$

(3) ℓ is not the zero set of a factor in V but ℓ passes through a point of $\mathcal{S} \setminus \mathcal{B}$

There are v such lines in case (1), each of which contains $q-1$ distinct zeros of f in $\mathcal{P}$. When considering cases (2) and (3), we need only bound the number of zeros of f' since all the zeros of $\prod_{g \in V} g^{m_g}$ have been counted. There are $s - v_{\mathcal{B}}$ lines in case (2). Since $deg(f') \leq deg(f) - v = (s+2) - v$ and since f' must pass through all the points of $\mathcal{B}$ which are not contained in lines of V, we know $Z(f') \cap \mathcal{P}$ has at most $(s+2) - v - 1$ points on a line in case (2). There are $(q-1) - v - (s - v_{\mathcal{B}})$ lines in case (3). Each of these lines contains at most $(s+2) - v$ zeros of f'. Thus, the maximum number of zeros of f in $\mathcal{P}$ is

$$\begin{aligned} N &\leq v(q-1)+(s-v_{\mathcal{B}})((s+2)-v-1)+((q-1)-v-(s-v_{\mathcal{B}}))((s+2)-v) \\ &= v(q-1)+(q-1-v)(s+2-v)-s+v_{\mathcal{B}}. \end{aligned} \tag{4.9}$$

We need at least two lines not in V in order for our function f to vanish at $(0:0:1)$, $(0:1:0)$ and the points of $\mathcal{R}\cap\mathcal{B}$. Since $deg(f)=s+2$, we must have $v\leq s$. In order for f to vanish at $(1:0:0)$, we need at least one factor of f to correspond to a vertical line. If y or z is a factor of f, then

$$|Z(f)\cap\mathcal{P}|\leq(s+2)(q-1)-(q-1)\leq(s+2)(q-1)-2s.$$

Hence we may assume that neither y nor z is a factor of f and so we have $v\geq 1$ and $0\leq v_{\mathcal{B}}\leq v\leq s$.

We see that the right-hand side of (4.9) is largest when $v_{\mathcal{B}}$ is as large as possible, so we rewrite it setting $v_{\mathcal{B}}=v$ to obtain

$$N\leq v(q-1)+(q-1-v)(s+2-v)-s+v.$$

This simplifies to

$$N\leq v^2-(s+1)v+((s+2)(q-1)-s). \tag{4.10}$$

The right-hand side of (4.10) achieves its maximum value at one of the endpoints $v=1$ or $v=s$. If $v=s$ or $v=1$, we obtain $(s+2)(q-1)-2s$. Thus, the maximum number of zeros of a function $0\neq f\in F([D])$ is $(s+2)(q-1)-2s$. □

Combining Lemmas 4.3.2.1 and 4.3.2.3 gives us the following theorem.

Theorem 4.3.2.4. *Let $[D] = [(s+2)L - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 3$, $s \geq r \geq 1$ and $q - 1 \geq 2s$. Suppose further that $q - 2(s+2) + b > s(r+1) - \binom{r-1}{2}$ and $q \geq s + 4$. Then $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = z^m$) is a*

$$\left[(q-1)^2, \binom{s+4}{2} - b, d\right] \text{ code, where}$$

$$(q-1)^2 - (s+2)(q-1) + 2s \leq d \leq (q-1)^2 - (s+2)(q-1) + s(r+1) - \binom{r-1}{2}.$$

Proof. The dimension holds by Proposition 4.1.8. Noting that

$$d = (q-1)^2 - \max\{|Z(f) \cap \mathcal{P}| : f \in F\left([D]\right), f \not\equiv 0\},$$

the bounds on d hold by Lemmas 4.3.2.3 and 4.3.2.1. □

Remark. The upper bound in Theorem 4.3.2.4 is equal to the lower bound when $r = 1$, so in this case we have an exact result for the minimum distance. The upper bound is strictly greater than the lower bound when $r > 1$.

We now give two examples to show that it is possible to attain the upper bound in Theorem 4.3.2.4 as well as intermediate values for the minimum distance when $r > 1$.

Example 4.3.2.5. Let $q = 9$ and let γ be a generator for $\mathbb{F}_q^*$. Let

$$\mathcal{B} = \{(0:0:1), (0:1:0), (1:0:0), (0:1:1), (0:\gamma:1), (1:0:1), (\gamma:0:1)\}.$$

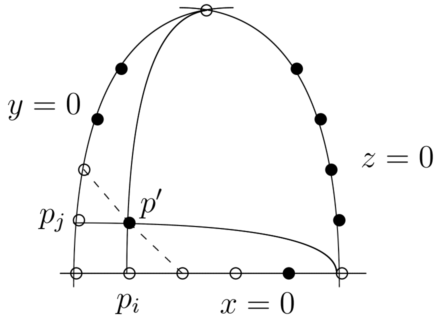
Then $s = r = 2$ and $c = 3$. Note that q, c, s and r satisfy the hypotheses of Theorem 4.3.2.4 and so we have $n = 64$, $k = 8$ and $36 \leq d \leq 38$. A Magma [3] computation yields $d = 38$. The guaranteed minimum distance from the Varshamov-Gilbert Bound (Proposition 3.1.6) is 42.

Example 4.3.2.6. Let $q = 8$ and let γ be a generator for $\mathbb{F}_q^*$. Let $\mathcal{B} = \{(0:0:1),(0:1:0),(1:0:0)\} \cup \{(0:1:1),(0:\gamma:1),(0:\gamma^2:1)\} \cup \{(1:0:1),(\gamma:0:1),(\gamma^2:0:1)\}$. Then $s = r = 3$ and $c = 3$. Note that q, c, s and r satisfy the hypotheses of Theorem 4.3.2.4 and so we have $n = 49$, $k = 12$ and $20 \leq d \leq 27$. A Magma [3] computation yields $d = 22$. It is interesting to note that the best known minimum distance of a code with the same q, length and dimension is 27 [9]. The guaranteed minimum distance from the Varshamov-Gilbert Bound (Proposition 3.1.6) is 25.

The next lemma will be used to obtain an upper bound on the minimum distance when the points of $\mathcal{B}$ satisfy certain criteria. This upper bound is equal to the lower bound on d from Theorem 4.3.2.4, as we will see in the proof of Theorem 4.3.2.8.

Lemma 4.3.2.7. *Let $[D] = [(s+2)L - E_1 - \cdots - E_b]$, $\mathcal{P}$ be the standard set, $c = 3$ and $q - 1 \geq s \geq r \geq 1$. Let p_i be a point of $\mathcal{S} \cap \mathcal{B}$ and let p_j be a point of $\mathcal{R} \cap \mathcal{B}$. Let $p' \in \mathcal{P}$ be the point of intersection of the vertical line through p_i and the horizontal line through p_j. Suppose that the points of $\mathcal{B}$ are arranged so that all $r - 1$ of the lines joining p' with the points of $(\mathcal{R} \cap \mathcal{B}) \setminus \{p_j\}$ pass through distinct points of $(\mathcal{S} \cap \mathcal{B}) \setminus \{p_i\}$ (see Figure 4.3.2.1). Then there exists a function $f \in F([D])$ such that $|Z(f) \cap \mathcal{P}| = (s+2)(q-1) - 2s$.*

Figure 4.3.2.1: Meeting the conditions of Lemma 4.3.2.7 for $q = 5$



Proof. Let two of the factors of f correspond to the vertical line through p_i and the horizontal line through p_j. Let a third factor of f correspond to the line through $(0:0:1)$ and p'. These three factors give $3(q-1)-2$ distinct zeros of $|Z(f)\cap\mathcal{P}|$.

Let $r-1$ of the factors of f correspond to the lines joining the points of $(\mathcal{R}\cap\mathcal{B})\backslash\{p_j\}$ with p'. Each of these factors has $(q-2)$ zeros in $\mathcal{P}$ and intersects the previous factors in exactly one point: p'. Hence these $r-1$ factors yield $(r-1)(q-2)-(r-1)$ new zeros.

Let the remaining $s-r$ factors of f correspond to lines joining p' with points of $\mathcal{S}\cap\mathcal{B}$ not already covered by the lines through p' and the points of $\mathcal{R}\cap\mathcal{B}$. These factors yield $(s-r)(q-2)-(s-r)$ new zeros.

Adding these three quantities of zeros together, we have that

$$|Z(f)\cap\mathcal{P}| = (s+2)(q-1)-2s.$$

$\square$

Theorem 4.3.2.8 states that when the points of $\mathcal{B}$ satisfy the conditions of Lemma 4.3.2.7, the lower bound of Theorem 4.3.2.4 is sharp. Thus we see also for $c=3$ that the arrangement of the points on $Z(xy)$ affects the minimum distance d and that our lower bound cannot be improved without additional restrictions on the distribution of the points of $\mathcal{B}$.

Theorem 4.3.2.8. *Let $[D]=[(s+2)L-E_1-\cdots-E_b]$, $\mathcal{P}$ be the standard set, $c=3$, $s\geq r\geq 1$ and $q-1\geq 2s$. Suppose the points of $\mathcal{B}$ are arranged to meet the conditions in Lemma 4.3.2.7. Suppose further that $q-2(s+2)+b > s(r+1)-\binom{r-1}{2}$ and $q\geq s+4$. Then $C^h(\mathcal{B},\mathcal{P},[D])$ (with $h=z^m$) is a*

$$\left[(q-1)^2, \binom{s+4}{2}-b, (q-1)^2-(s+2)(q-1)+2s\right] \textit{ code.}$$

Proof. The lower bound on d in Theorem 4.3.2.4 is now exact since Lemma 4.3.2.7 demonstrates the existence of a function with $(s+2)(q-1)+2s$ zeros in $\mathcal{P}$. $\square$

We conclude with a proposition which gives an upper bound on the minimum distance for the divisor class $[D] = [bL - E_1 - \cdots - E_b]$ when $c = 3$. (Note that $m = b = s + r + 3$ instead of $m = s + 2$.) We use this bound to show that some of our examples in the next section have the best minimum distance possible. Table A.4 in Appendix A shows the parameters for a family of codes $C^h(\mathcal{B}, \mathcal{P}, [D])$ with $\mathcal{B} \subset Z(xy)$, $\mathcal{P}$ the standard set, $[D] = [bL - E_1 - \cdots - E_b]$ and $c = 3$.

Proposition 4.3.2.9. *Let* $[D] = [bL - E_1 - \cdots - E_b]$*,* $\mathcal{P}$ *be the standard set,* $c = 3$ *and* $s \geq r \geq 1$*. Let* q *be such that* $q - 1 \geq s + 2$*, and let* γ *be a generator of the multiplicative group* $\mathbb{F}_q^*$*. Let* $\mathcal{B} = \{(0 : 0 : 1), (0 : 1 : 0), (0 : 0 : 1)\} \cup \{(0 : \gamma^0 : 1), ..., (0 : \gamma^{s-1} : 1)\} \cup \{(\gamma^0 : 0 : 1), ..., (\gamma^{r-1} : 0 : 1)\}$*. Then the minimum distance of* $C^h(\mathcal{B}, \mathcal{P}, [D])$ *satisfies* $d \leq (q-1)^2 - b(q-1) + (s+2)(r+1)$*.*

Proof. It suffices to show that there exists a function $f \in F([D])$ with $b(q-1)-(s+2)(r+1)$ zeros in $\mathcal{P}$. Let $s+2$ of the factors of f be $(x-\gamma^0 z)$,...,$(x-\gamma^{s+1} z)$. Let r of the factors of f be $(y - \gamma^0 z)$,...,$(y - \gamma^{r-1} z)$. Let $x - y$ be the final factor of f. Note that f has $(s+2)+r+1 = b$ factors.

Now each of the factors of f has $q-1$ zeros. The $s+2$ vertical lines have $(s+2)r$ zeros in common with the r horizontal lines and $s+2$ zeros in common with the line defined by $x - y = 0$. Since all of the common zeros are accounted for, we know that f has $b(q-1) - (s+2)r - (s+2) = b(q-1) - (s+2)(r+1)$ zeros. Finally, since f vanishes at all the points of $\mathcal{B}$, we have $f \in F([D])$. $\square$

4.3.3 Comparison of Two-Line Codes with $c = 0$ and $c = 3$

We are now ready to make some comparison between the parameters of two-line codes with $c = 0$ and two-line codes with $c = 3$. We will see that the range for the minimum distance in Theorem 4.3.1.4 almost always includes the range in Theorem 4.3.2.4 when the dimensions of the codes are the same, so we cannot tell from these theorems which type of code has better parameters in general. When Theorems 4.3.1.8 and 4.3.2.8 can be applied, we will see that the minimum distance is better when $c = 3$. We conclude with an example where it is advantageous to choose $c = 0$.

If we apply Theorem 4.3.2.4 to the divisor class $[D] = [(s+2)L - E_1 - \cdots - E_b]$ with $c = 3$, we obtain a code C with dimension $\binom{s+4}{2} - b$ and minimum distance d satisfying both $d \geq (q-1)^2 - (s+2)(q-1) + 2s$ and $d \leq (q-1)^2 - (s+2)(q-1) + s(r+1) - \binom{r-1}{2}$.

Applying Theorem 4.3.1.4 to the divisor class $[D'] = [s'L - E_1 - \cdots - E_{b'}]$ with $c = 0$, $s' = s + 2$ and $r' = r + 1$, we obtain a code C' with dimension $\binom{s+4}{2} - b$ and minimum distance d' satisfying both $d' \geq (q-1)^2 - (s+2)(q-1) + (s+2)$ and $d' \leq (q-1)^2 - (s+2)(q-1) + (s+2)(r+1) - \binom{r+1}{2}$.

The dimension of C' is the same as that of C. The lower bound on d' is less than or equal to the lower bound on d for $s \geq 2$. One can show that the upper bound on d' is exactly 3 greater than the upper bound on d (for $r \geq 1$). Hence the range for d' given by Theorem 4.3.1.4 includes the range for d given by Theorem 4.3.2.4 whenever $s \geq 2$.

Let $\mathcal{B}$ and $\mathcal{B}'$ satisfy the conditions of Theorem 4.3.2.8 and 4.3.1.8, respectively. Then the lower bounds on the minimum distance from Theorems 4.3.2.4 and 4.3.1.4 are sharp, so in this case it is advantageous to choose $c = 3$ for $s > 2$.

We conclude with an example which demonstrates two codes, C and C', with $c = 3$ and $c = 0$, respectively, such that $s > 2$ but the parameters of C' are better than those of C.

Example 4.3.3.1. Let $q = 7$ and let γ be a generator of the multiplicative group $\mathbb{F}_7^*$. We first construct a code with $c = 3$. Let

$$\mathcal{B} = \{(0:0:1), (0:1:0), (1:0:0), (0:1:1), (1:0:1)\}$$

and $[D] = [3L - E_1 - \cdots - E_5]$. A Magma [3] computation shows that $C := C^h(\mathcal{B}, \mathcal{P}, [D])$ is a $[36, 5, 20]$ code. To construct a comparable code with $c = 0$, we let

$$\mathcal{B}' = \{(0:1:1), (0:\gamma^3:1), (0:\gamma^4:1), (1:0:1)\}, (\gamma:0:1)\}$$

and $[D'] = [3L - E_1 - \cdots - E_5]$. A Magma [3] computation shows that the resulting code $C' := C^h(\mathcal{B}', \mathcal{P}, [D'])$ has parameters $[36, 5, 22]$.

For further examples where choosing $c = 0$ appears to be advantageous, we refer the reader to Tables A.2 and A.3.

4.4 Comparison of One-Line and Two-Line Codes

The purpose of this section is to investigate whether it is advantageous to have $\mathcal{B} \subset Z(xy)$ instead of just $\mathcal{B} \subset Z(x)$. It turns out that for the families of codes for which we have exact results, the one-line codes have better parameters. However, by looking at some other examples of two-line codes, we see that there are situations in which two-line codes have better parameters.

If we apply Theorem 4.2.5 to the divisor class $[D] = [bL - E_1 - \cdots - E_b]$ with $c = 2$, we obtain a one-line code C with dimension $\binom{b+2}{2} - b$ and minimum distance $(q-1)^2 - b(q-1) + 2(b-2)$. Applying Theorem 4.3.2.8 to the divisor class $[D'] = [(s+2)L - E_1 - \cdots - E_{b'}]$ with $c = 3$, we obtain a two-line code C' with minimum distance $(q-1)^2 - (s+2)(q-1) + 2s$ and dimension $\binom{s+4}{2} - b'$, where $b' = s + r + 3$.

To compare the two codes, choose s so that $s = b - 2$. Then C' has minimum distance $(q-1)^2 - b(q-1) + 2(b-2)$ and dimension $\binom{b+2}{2} - b - r - 1$. Note that the minimum distance of C is the same as that of C' and the dimension of C is greater than that of C'. Hence C, the one-line code, has better parameters.

We now give two examples of pairs of codes for which the two-line code has better parameters.

Example 4.4.1. Let $q = 7$ and let γ be a generator of the multiplicative group $\mathbb{F}_7^*$. First, we construct our one-line code $C^h(\mathcal{B}, \mathcal{P}, [D])$. Let

$$\mathcal{B} = \{(0:0:1), (0:1:0), (0:1:1), (0:\gamma:1), (0:\gamma^2:1), (0:\gamma^3:1)\}$$

and $[D] = [6L - E_1 - \cdots - E_6]$. A Magma [3] computation shows that $C^h(\mathcal{B}, \mathcal{P}, [D])$ is a $[36, 22, 6]$ code. To construct a comparable two-line code, we let

$$\mathcal{B}' = \{(0:0:1), (0:1:0), (0:0:1), (0:1:1), (0:\gamma:1), (1:0:1)\}.$$

Note that $|\mathcal{S} \cap \mathcal{B}| = 2$ and $|\mathcal{R} \cap \mathcal{B}| = 1$ in this case. Let $[D'] = [6L - E_1 - \cdots - E_6]$. A Magma [3] computation shows that the resulting code $C'(\mathcal{B}', \mathcal{P}, [D'])$ has parameters $[36, 22, 8]$. It is interesting to note that 8 is precisely the guaranteed minimum distance from the Varshamov-Gilbert Bound (Proposition 3.1.6).

Example 4.4.2. Let $q = 8$ and let γ be a generator of the multiplicative group $\mathbb{F}_8^*$. Again, we first construct our one-line code C. Let

$$\mathcal{B} = \{(0:0:1), (0:1:0), (0:1:1), (0:\gamma:1), (0:\gamma^2:1), (0:\gamma^3:1)\}$$

and $[D] = [6L - E_1 - \cdots - E_6]$. A Magma [3] computation shows that $C := C^h(\mathcal{B}, \mathcal{P}, [D])$ is a $[49, 22, 14]$ code.

Now let $\mathcal{B}' = \{(0:0:1), (0:1:0), (0:0:1), (0:1:1), (0:\gamma:1), (1:0:1)\}$ and $[D'] = [6L - E_1 - \cdots - E_6]$. A Magma [3] computation shows that the resulting code $C' := C^h(\mathcal{B}', \mathcal{P}, [D'])$ has parameters $[49, 22, 15]$. In this case, 16 is the guaranteed minimum distance from the Varshamov-Gilbert Bound (Proposition 3.1.6).

In both examples we saw that the two-line code had better parameters than the one-line code. One might wonder why we didn't consider larger values of q or b. The reason is that the minimum distance takes an increasingly long time to compute.

In both examples, the value of q for the one-line code was too small to apply our main Theorem (4.2.5) from Section 4.2. It is interesting to note that in both examples the minimum distance of the two-line code attained the upper bound given in Proposition 4.3.2.9. More work needs to be done to determine if and when there exist entire families of two-line codes with better parameters than one-line codes.

Remark. This section is similar, at least in spirit, to the work of Gretchen Matthews in [23]. Matthews compares one-point and two-point AG codes on Hermitian curves. She shows that some two-point codes on the curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$ have better parameters than any one-point code of the same dimension on the same curve.

4.5 Induced Bound

In this section we consider an effective divisor class $[D]$ which is a sum $[D] = \sum_{k=1}^{\ell}[D_k]$ of effective divisor classes $[D_k]$. Let d denote the minimum distance of $C^h(\mathcal{B}, \mathcal{P}, [D])$ and let d_k denote the minimum distance of $C^{h_k}(\mathcal{B}, \mathcal{P}, [D_k])$ for $k = 1, ..., \ell$. When $\mathcal{B} \subset Z(x)$, we obtain a bound for d in terms of $d_1, ..., d_\ell$ (see Theorem 4.5.4). In this way, we obtain improvements on the lower bound in Theorem 4.1.9 for divisor classes other than those already studied. We begin with some notation and a lemma.

Let $\mathcal{B} = \{p_1, ..., p_b\} \subset Z(x)$. Let $\mathcal{S} := Z(x) \setminus \{(0:1:0),(0:0:1)\}$ and $s = |\mathcal{S} \cap \mathcal{B}|$. Let c be the number of coordinate vertices of $\mathbb{P}^2$ in $\mathcal{B}$. So $b = s + c$.

Our first lemma will help us to show that any nonzero polynomial $f \in F([D])$ which maximizes $|Z(f) \cap \mathcal{P}|$ is a product of linear polynomials (Corollary 4.5.2). Although the lemma can also easily be applied to obtain an upper bound on the minimum distance, we do not state this result explicitly here. Instead we apply its corollary to obtain a lower bound on the minimum distance (Theorem 4.5.4).

Notation. In the proof of Lemma 4.5.1 and the results that follow, we will use the notation

$$\widetilde{m_i} = \begin{cases} m_i - 1 & \text{if } p_i \in \mathcal{B} \cap \mathcal{S} \text{ and} \\ m_i & \text{if } p_i \in \mathcal{B} \setminus \mathcal{S}. \end{cases}$$

Lemma 4.5.1. *Let $\mathcal{B} \subset Z(x)$ and let $\mathcal{P}$ be the standard set. Let $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ with $m \geq \sum_{i=1}^{b} m_i$ and $m_i \geq 1$ for each $i = 1, ..., b$. Let $s = |\mathcal{S} \cap \mathcal{B}|$. Suppose q satisfies the following two conditions:*
(i) $q - 1 \geq s + m - \sum_{i=1}^{b} m_i$
(ii) $q - 1 \geq m_i$ for $i = 1, ..., b$
Then there exists a function $f \in F([D])$, which is a product of linear polynomials, and satisfies

$$|Z(f) \cap \mathcal{P}| \geq m(q-1) - \left((m+1)\left(\sum_{i=1}^{b} \widetilde{m_i}\right) - \frac{1}{2}\left(\sum_{i=1}^{b} \widetilde{m_i}\right)^2 - \frac{1}{2}\left(\sum_{i=1}^{b} \widetilde{m_i}^2\right)\right).$$

Proof. We define our nonzero function $f \in F([D])$ as follows. Let s of the factors of f be those corresponding to the vertical lines through the points of $\mathcal{S} \cap \mathcal{B}$. Let $m - \sum_{i=1}^{b} m_i$ of the factors correspond to vertical lines through distinct points of $\mathcal{S} \setminus \mathcal{B}$. This is possible provided that q satisfies (i). These $s + m - \sum_{i=1}^{b} m_i$ factors yield $(s + m - \sum_{i=1}^{b} m_i)(q-1)$ zeros in $\mathcal{P}$.

For each point $p_i \in \mathcal{B} \setminus \mathcal{S}$, choose m_i distinct, nonvertical, nonhorizontal lines through p_i. For each point $p_i \in \mathcal{B} \cap \mathcal{S}$, choose $m_i - 1$ distinct nonvertical, nonhorizontal lines through p_i. These choices are possible if q satisfies (ii). Then we have $\sum_{i=1}^{b} m_i - s$ nonvertical lines with at least $q-2$ zeros each. The maximum number of intersection points of the nonvertical lines with the $s + m - \sum_{i=1}^{b} m_i$ vertical lines is $(s+m-\sum_{i=1}^{b} m_i)(\sum_{i=1}^{b} m_i - s)$. The maximum number of intersection points of the nonvertical lines with each other in $\mathcal{P}$ is

$$\binom{\sum_{i=1}^{b} m_i - s}{2} - \sum_{i=1}^{b} \binom{\widetilde{m_i}}{2}.$$

We subtract off $\displaystyle\sum_{i=1}^{b} \binom{\widetilde{m_i}}{2}$ because distinct lines through a point of $\mathcal{B}$ cannot intersect in $\mathcal{P}$. The total number of new zeros on the nonvertical lines is at least

$$\left(\sum_{i=1}^{b} m_i - s\right)(q-2) - \left(s + m - \sum_{i=1}^{b} m_i\right)\left(\sum_{i=1}^{b} m_i - s\right) - \binom{\sum_{i=1}^{b} m_i - s}{2} + \sum_{i=1}^{b} \binom{\widetilde{m_i}}{2}.$$

Adding to this the number of zeros on the vertical lines and then doing some simplification, we see that

$$|Z(f) \cap \mathcal{P}| \geq m(q-1) - \left((m+1)\left(\sum_{i=1}^{b} \widetilde{m_i}\right) - \frac{1}{2}\left(\sum_{i=1}^{b} \widetilde{m_i}\right)^2 - \frac{1}{2}\left(\sum_{i=1}^{b} \widetilde{m_i}^2\right)\right).$$

□

Notation. For future reference we define

$$g([D]) := (m+1)\left(\sum_{i=1}^{b} \widetilde{m_i}\right) - \frac{1}{2}\left(\sum_{i=1}^{b} \widetilde{m_i}\right)^2 - \frac{1}{2}\left(\sum_{i=1}^{b} \widetilde{m_i}^2\right),$$

where $\mathcal{B} = \{p_1, ..., p_b\}$ and $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$.

Corollary 4.5.2. *Let $\mathcal{B} \subset Z(x)$ and let $\mathcal{P}$ be the standard set. Let $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ with $m \geq \sum_{i=1}^{b} m_i$ and $m_i \geq 1$ for $i = 1, ..., b$. Suppose q satisfies conditions (i) and (ii) of Lemma 4.5.1 and in addition:*
(iii) $q - 2m + \sum_{i=1}^{b} m_i > g([D])$.
Then a function $f \in F([D])$ maximizing $|Z(f) \cap \mathcal{P}|$ is a product of distinct linear polynomials, none of which is equal to x, y or z.

Proof. Since $m(q-1) - (q - 2m + \sum_{i=1}^{b} m_i) < m(q-1) - (g([D]))$, by Lemma 4.1.7 and Lemma 4.5.1, we know that a function $f \in F([D])$ maximizing $|Z(f) \cap \mathcal{P}|$ must be a product of linear polynomials. Moreover, if a function $g \in F([D])$ is a product of linear polynomials and has x, y or z as a factor, then $|Z(g) \cap \mathcal{P}| \leq m(q-1) - (q-1)$. Similarly, if a function $g \in F([D])$ is a product of linear polynomials and has a repeated factor, then by the proof of Lemma 4.1.7, we have $|Z(g) \cap \mathcal{P}| \leq m(q-1) - (q-1)$. Since $m \geq \sum_{i=1}^{b} m_i$, in either case we have

$$q - 1 \geq q - m \geq q - m - \left(m - \sum_{i=1}^{b} m_i\right) = q - 2m + \sum_{i=1}^{b} m_i > g([D]).$$

Hence, such polynomials g have fewer zeros than a polynomial of the form described in Lemma 4.5.1. □

The next lemma is the most significant in this section. It will help us relate d to d_1,...,d_ℓ (Theorem 4.5.4). The thrust of the proof is in the claim that if $0 \neq f \in F([D])$ maximizes $|Z(f) \cap \mathcal{P}|$, then f can be written as a product $f = \prod_{k=1}^{\ell} g_k$ such that $g_k \in F([D_k])$ for $k = 1, ..., \ell$. This claim does not always hold in the case where $\mathcal{B} \subset Z(xy)$ (see Example 4.5.6), so the proof of Lemma 4.5.3 does not easily generalize.

Lemma 4.5.3. *Let $\mathcal{B} \subset Z(x)$ and let $\mathcal{P}$ be the standard set. Let $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ with $m \geq \sum_{i=1}^{b} m_i$ and $m_i \geq 1$ for each $i = 1, ..., b$. Let*

$\{[D_k]\}_{k=1}^{\ell}$ be numerically effective divisor classes, i.e., $[D_k] = [m^{(k)}L - m_1^{(k)}E_1 - \cdots - m_b^{(k)}E_b]$ with $m^{(k)} \geq \sum_{i=1}^{b} m_i^{(k)}$ and $m^{(k)}, m_1^{(k)}, ..., m_b^{(k)} \geq 0$ for $k = 1, ..., \ell$. Suppose $[D] = \sum_{k=1}^{\ell}[D_k]$. Suppose q satisfies (i) and (ii) of Lemma 4.5.1 and condition (iii) of Corollary 4.5.2. Then

$$\max\{|Z(f) \cap \mathcal{P}| : f \in F\left([D]\right)\} \leq \sum_{k=1}^{\ell} \max\{|Z(f_k) \cap \mathcal{P}| : f_k \in F\left([D_k]\right)\}.$$

Proof. First, we prove a claim.

Claim: Let $[D], [D_1], ..., [D_\ell]$ be as above. Let $f \in F\left([D_1 + \cdots + D_\ell]\right)$ be a product of distinct linear polynomials, none of which is equal to x, y or z. Then we can write f as a product $f = \prod_{k=1}^{\ell} g_k$ such that $g_k \in F\left([D_k]\right)$ for $k = 1, ..., \ell$.

We induct on ℓ to prove the claim. If $\ell = 1$ we obtain the result by setting $g_1 = f$. Now let $f \in F\left([D_1 + \cdots + D_\ell]\right)$ be a product of distinct linear polynomials, none of which is equal to x, y or z. The zero set of a linear factor of f contains either no points of $\mathcal{B}$ or exactly one point of $\mathcal{B}$.

Since f has a zero of multiplicity at least m_i at each point $p_i \in \mathcal{B}$, we can find (disjoint) sets $\mathscr{F}_{p_1}, ..., \mathscr{F}_{p_b}$ of linear factors of f such that $|\mathscr{F}_{p_i}| = m_{p_i}$ for each $i = 1, ..., b$ and such that $g(p_i) = 0$ for all $g \in \mathscr{F}_{p_i}$. Let $\mathscr{F}$ denote the set of linear factors of f which are not in any of the sets $\mathscr{F}_{p_i}$. Note that the choice of the $\mathscr{F}_{p_i}$ is not unique since there may be elements g of $\mathscr{F}$ which satisfy $g(p_i) = 0$ for some $i = 1, ..., b$.

Choose subsets $\mathscr{G}_{p_1} \subset \mathscr{F}_{p_1}, \mathscr{G}_{p_2} \subset \mathscr{F}_{p_2}$, ..., and $\mathscr{G}_{p_b} \subset \mathscr{F}_{p_b}$ such that $|\mathscr{G}_{p_i}| = m_i^{(\ell)}$ for $i = 1, ..., b$. Choose a subset $\mathscr{G} \subset \mathscr{F}$ of size $m^{(\ell)} - \sum_{i=1}^{b} m_i^{(\ell)}$. Let g_ℓ denote the product of all the factors in $\mathscr{G}_{p_1}, ..., \mathscr{G}_{p_b}$ together with the factors in $\mathscr{G}$. Then $g_\ell \in F\left([D_\ell]\right)$. Also, $h = f/g_\ell \in F\left([D_1 + \cdots + D_{\ell-1}]\right)$ is a product of distinct linear polynomials, none of which is x, y or z. By the induction hypothesis, we can write h as a product

$h = \prod_{k=1}^{\ell-1} g_k$ such that $g_k \in F([D_k])$ for $k = 1, ..., \ell - 1$. Since $f = \prod_{k=1}^{\ell} g_k$, this completes the proof of the claim.

Now let $f' \in F([D])$ be such that $|Z(f) \cap \mathcal{P}|$ is maximized. By Corollary 4.5.2, f' is a product of distinct linear polynomials, none of which is x, y or z. By the claim, we can write $f' = \prod_{k=1}^{\ell} g_k$ such that $g_k \in F([D_k])$ for $k = 1, ..., \ell$. Then $|Z(f') \cap \mathcal{P}| = |Z(\prod_{k=1}^{\ell} g_k) \cap \mathcal{P}| \leq \sum_{k=1}^{\ell} |Z(g_k) \cap \mathcal{P}|$ since the g_k's may have some zeros in common. Since $\sum_{k=1}^{\ell} |Z(g_k) \cap \mathcal{P}| \leq \sum_{k=1}^{\ell} \max\{|Z(f_k) \cap \mathcal{P}| : f_k \in F([D_k])\}$, this proves the result. □

We can now state our main theorem and obtain a bound on d in terms of d_1,...,d_ℓ. This result is analogous to Theorem 1.2 in the paper by Little and Schenck [21] in the sense that we use the decomposition of a divisor class $[D]$ into a sum of other divisor classes to induce a bound on d.

Theorem 4.5.4. *Let $\mathcal{B} \subset Z(x)$ and let $\mathcal{P}$ be the standard set. Let $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ with $m \geq \sum_{i=1}^{b} m_i$ and $m_i \geq 1$ for each $i = 1, ..., b$. Let $\{[D_k]\}_{k=1}^{\ell}$ be such that $[D_k] = [m^{(k)}L - m_1^{(k)}E_1 - \cdots - m_b^{(k)}E_b]$ with $m^{(k)} \geq \sum_{i=1}^{b} m_i^{(k)}$ and $m^{(k)}, m_1^{(k)}, ..., m_b^{(k)} \geq 0$ for $k = 1, ..., \ell$. Let d_k denote the minimum distance of $C^{h_k}(\mathcal{B}, \mathcal{P}, [D_k])$, where $h_k = z^{m^{(k)}}$, for $k = 1, ..., \ell$. Suppose $[D] = \sum_{k=1}^{\ell}[D_k]$. Suppose q satisfies conditions (i) and (ii) of Lemma 4.5.1 and condition (iii) of Corollary 4.5.2. Suppose further that $q \geq m + 2$. Then $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = z^m$) is a*

$$\left[(q-1)^2, \binom{m+2}{2} - \sum_{i=1}^{b} \binom{m_i+1}{2}, d\right] \text{ code, where}$$

$$d \geq \sum_{k=1}^{\ell} d_k - (\ell - 1)(q-1)^2. \tag{4.11}$$

Proof. Note that the class $[D]$ is numerically effective by Section 2.3 since $m \geq \sum_{i=1}^{b} m_i$ and $m_i \geq 1$ for each $i = 1, ..., b$. Thus the dimension of $C^h(\mathcal{B}, \mathcal{P}, [D])$ is $\binom{m+2}{2} - \sum_{i=1}^{b} \binom{m_i+1}{2}$ by Proposition 4.1.8. To see the inequality regarding d, note that d is equal to

$$\begin{aligned}
& (q-1)^2 - \max\{|Z(f) \cap \mathcal{P}| : f \in F([D]), f \not\equiv 0\} \\
\geq \; & (q-1)^2 - \sum_{k=1}^{\ell} \max\{|Z(f_k) \cap \mathcal{P}| : f_k \in F([D_k]), f_k \not\equiv 0\} \\
= \; & \sum_{k=1}^{\ell} \big((q-1)^2 - \max\{|Z(f_k) \cap \mathcal{P}| : f_k \in F([D_k]), f_k \not\equiv 0\}\big) - (\ell-1)(q-1)^2 \\
= \; & \sum_{k=1}^{\ell} d_k - (\ell-1)(q-1)^2.
\end{aligned}$$

□

We can use Theorems 4.1.9, 4.2.5, and 4.5.4 in combination to obtain an induced bound on d, where $[D]$ is a divisor class not studied in Section 4.2 or Section 4.3. The next example demonstrates how to combine these theorems.

Example 4.5.5. Suppose $\mathcal{B} = \{p_1, p_2, p_3\} \subset Z(x)$, where p_2 and p_3 are coordinate vertices. Let $[D] = [5L - E_1 - 2E_2 - E_3]$, $[D_1] = [3L - E_1 - E_2 - E_3]$ and $[D_2] = [2L - 0E_1 - E_2 - 0E_3]$. Note that $[D] = [D_1] + [D_2]$. Let $q = 19$. By checking the hypotheses, one sees that $q = 19$ is sufficiently large so that the hypotheses of Theorems 4.1.9, 4.2.5 and 4.5.4 are satisfied for D_2, D_1 and D, respectively. By Theorem 4.1.9, we have $d_2 \geq 18^2 - 2 \cdot 18 = 288$. By Theorem 4.2.5, we know $d_1 = 18^2 - 3 \cdot 18 + 2(3-2) = 272$. Finally, by Theorem 4.5.4, we have $d \geq d_1 + d_2 - 18^2 \geq 236$. Note that if we had used Theorem 4.1.9 directly to compute d, we would have obtained $d \geq 18^2 - 5 \cdot 18 = 234$.

The following example shows that the claim in the proof of Lemma 4.5.3 does not always hold in the case where $\mathcal{B} \subset Z(xy)$ and $\mathcal{B} \not\subseteq Z(x)$. However, the conclusion of

Lemma 4.5.3 still holds with the decomposition in this example. Therefore, it may be possible to prove an analogous result to Lemma 4.5.3 for the case $\mathcal{B} \subset Z(xy)$ but this will require further work.

Example 4.5.6. Let $q \geq 4$ and let γ be a generator of $\mathbb{F}_q^*$. (We choose $q \geq 4$ so that 1, γ and γ^{-1} are all distinct.) Let $\mathcal{B} = \{p_1, p_2, p_3, p_4\}$, where $p_1 = (0 : 1 : 1)$, $p_2 = (1 : 0 : 1)$, $p_3 = (\gamma : 0 : 1)$ and $p_4 = (0 : \gamma : 1)$. Let $[D] = [2L - E_1 - E_2 - E_3 - E_4]$. Let $[D_1] = [L - E_1 - 0E_2 - E_3 - 0E_4]$ and let $[D_2] = [L - 0E_1 - E_2 - 0E_3 - E_4]$. Note that $[D], [D_1]$ and $[D_2]$ satisfy the conditions of Lemma 4.5.3.

There exists a line L_{12} through p_1 and p_2 which is defined by $x + y - z = 0$. There exists a line L_{34} through p_3 and p_4 which is defined by $x + y - \gamma z = 0$. The polynomial $f' = (x + y - z)(x + y - \gamma z)$ is in $F([D])$ but f' cannot be factored so that $f' = g_1 \cdot g_2$ with $g_1 \in F([D_1])$ and $g_2 \in F([D_2])$. This shows that the claim in the proof of Lemma 4.5.3 does not hold in this case.

However, one can show that, for sufficiently large q, a polynomial in $F([D])$ which maximizes $|Z(f) \cap \mathcal{P}|$ must be a product of two lines, each of which passes through two points of $\mathcal{B}$. Hence $2(q - 2)$ is the maximum number of zeros in $\mathcal{P}$ of a function in $F([D])$, i.e., $\max\{|Z(f) \cap \mathcal{P}| : f \in F([D])\} = 2(q - 2)$. Furthermore, since polynomials in $F([D_1])$ and $F([D_2])$ have degree one and do not pass through any coordinate vertices of $\mathbb{P}^2$, we have $\max\{|Z(f) \cap \mathcal{P}| : f_1 \in F([D_1])\} = q - 2$ and $\max\{|Z(f) \cap \mathcal{P}| : f_2 \in F([D_2])\} = q - 2$. Hence

$$\max\{|Z(f) \cap \mathcal{P}| : f \in F([D])\} = \sum_{k=1}^{2} \max\{|Z(f) \cap \mathcal{P}| : f_k \in F([D_k])\},$$

which satisfies the conclusion of Lemma 4.5.3.

4.6 An Asymptotically Good Family of Codes (with q Increasing)

Let $\mathcal{B} \subset Z(x)$ and $\mathcal{P}$ be the standard set. Let q be a power of 2 such that $q \geq \max\{4, 2b\}$. Let $[D] = [\frac{1}{2}qL - E_1 - \cdots - E_b]$, i.e., $m = \frac{1}{2}q$ and $m_i = 1$ for $i = 1, ..., b$. Note that $[D]$ is numerically effective since $\frac{1}{2}q \geq b$ (see Section 2.3 or Proposition I.5.2 of [12]). Also, note that $q \geq \frac{1}{2}q + 2 = m + 2$ and $q \geq q - b = 2m - \sum_{i=1}^{b} m_i$. Thus by Theorem 4.1.9, the dimension of $C^h(\mathcal{B}, \mathcal{P}, [D])$ is $k = \binom{\frac{1}{2}q+2}{2} - b$ and the minimum distance is at least $(q-1)^2 - \frac{1}{2}q(q-1)$. We let our family of codes be indexed by $\ell = 2, 3, 4, ...$, where $q = 2^\ell$. This family has rate $k/n = (\frac{1}{8}q^2 + \frac{3}{4}q + 1 - b)/(q-1)^2$, which approaches $\frac{1}{8}$ as $\ell \to \infty$. Similarly, the relative minimum distance d/n is at least $((q-1)^2 - \frac{1}{2}q(q-1))/(q-1)^2$, which approaches $\frac{1}{2}$ as $\ell \to \infty$.

Hence, we have found an infinite family of codes for which both the rate and relative minimum distance are bounded away from zero as $n = (q-1)^2$ approaches infinity. The problem is that q must increase in order to obtain larger codes, and this increases the complexity of encoding.

It may be possible to employ the concatenated code construction (see Definition 3.1.9 and the subsequent theorem) to obtain an infinite family of codes with q fixed, using our codes as the outer codes and a family of binary codes as the inner codes. The family of inner codes would need to have dimension ℓ (where $q = 2^\ell$ as described above). They would also need to have sufficiently large minimum distance d' relative to their length n' so that $d \cdot d'/(n \cdot n') \to \epsilon > 0$ as $\ell \to \infty$. Such a result is still being investigated.

Chapter 5

Codes on $\mathbb{P}^r_{\mathcal{B}}$

Our goal is to generalize the construction in Chapter 4 to $\mathbb{P}^r$, where r is the dimension of the projective space in which we are working. That is, we blow up a set of points $\mathcal{B} \subset \mathbb{P}^r(\mathbb{F}_q)$ and try to find bounds and exact results on the parameters of the AG code $C(\mathbb{P}^r_{\mathcal{B}}, \mathcal{P}, D)$. In order to compute the dimension of these codes, we restrict ourselves to the case where the points of $\mathcal{B}$ lie on two intersecting lines in a hyperplane of $\mathbb{P}^r$. The resulting surfaces $\mathbb{P}^r_{\mathcal{B}}$ are anticanonical, but we will not use this fact when obtaining results on the parameters k and d since no analog of the results of [12], [14] or [15] is known for higher dimensions. We will need to change our set of evaluation points (see Definition 5.1.5) so that we can obtain a result analogous to Lemma 4.1.7, which will lead to a lower bound on the minimum distance.

Definition 5.0.1. Let $x_0, ..., x_r$ be projective coordinates on $\mathbb{P}^r$. Define $\mathcal{T}_2 := Z(x_2)$ and $\mathcal{T}_r := Z(x_0x_1) \cap (\bigcap_{i=3}^r Z(x_i))$ for $r \geq 3$.

We will assume that $\mathcal{B} \subset \mathcal{T}_r$, so the points of $\mathcal{B}$ lie on two (or fewer) lines in the hyperplane defined by $x_r = 0$. Let $\mathcal{P}$ be a set of points in $\mathbb{P}^r(\mathbb{F}_q)$ such that $\mathcal{B} \cap \mathcal{P} = \emptyset$. Later we will work with a specific $\mathcal{P}$ (see Definition 5.1.5). Let D be an effective divisor such that $\operatorname{supp} D \cap \mathcal{P} = \emptyset$. Then the algebraic geometric code $C(\mathbb{P}^r_{\mathcal{B}}, \mathcal{P}, D)$

associated to $\mathbb{P}^r_{\mathcal{B}}$, $\mathcal{P}$ and D is the image of the evaluation map $ev_{\mathcal{P}} : L(D) \to \mathbb{F}_q^n$, where $n = |\mathcal{P}|$. For brevity, we write $C(\mathcal{B}, \mathcal{P}, D)$ for $C(\mathbb{P}^r_{\mathcal{B}}, \mathcal{P}, D)$.

We begin this chapter with results which parallel those at the beginning of Chapter 4, in order to show that the parameters of a code on $\mathbb{P}^r_{\mathcal{B}}$ do not depend on the divisor but only on the divisor class.

5.1 First Results

In this section, we show that the parameters of $C(\mathcal{B}, \mathcal{P}, D)$ depend only on the divisor class $[D]$ of D and not on the specific divisor D.

Let $H \subset \mathbb{P}^r_{\mathcal{B}}$ be the total transform of a general hyperplane on $\mathbb{P}^r$. Let $E_1, ..., E_b$ be the blow-ups of $p_1, ..., p_b \in \mathcal{B}$, respectively. Since $[H], [E_1], ..., [E_b]$ form a basis for $\text{Pic}(\mathbb{P}^r_{\mathcal{B}})$, we can uniquely express the class $[D]$ of a divisor D on $\mathbb{P}^2_{\mathcal{B}}$ by $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$, for some $m, m_1, ..., m_b \in \mathbb{Z}$ (see Section 2.3 for details). As in the previous chapter, we work with the case where $m, m_1, ..., m_b \geq 0$.

Notation. Let $R = \mathbb{F}_q[x_0, ..., x_r]$. Let R_m denote the vector space spanned by the set of homogeneous polynomials in R of degree m. For $f \in R_m$, let $Z(f)$ denote the set of zeros of f in $\mathbb{P}^r(\mathbb{F}_q)$. If $\frac{f}{h}$ is a rational function, i.e., if both f and h are elements of R_m, then let $Z(\frac{f}{h}) = Z(f) \cap \text{Dom}(\frac{f}{h})$, where $\text{Dom}(\frac{f}{h})$ is the domain of $\frac{f}{h}$.

Definition 5.1.1. Let $0 \neq f \in R_m$ and let $p \in \mathbb{P}^r(\mathbb{F}_q)$. Let h be the image of the function f under the linear change of coordinates which takes p to the point $(0 : \cdots : 0 : 1)$. We say f has a *zero of multiplicity at least* t at the point p if $h(x_0, x_1, ..., x_{r-1}, 1)$ has no terms of degree less than t.

Definition 5.1.2. Let $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ be effective with $m, m_1, ..., m_b \geq 0$. Define

$$F([D]) = \{f \in R_m : \text{ } f \text{ has a zero of multiplicity at least } m_i \text{ at each } p_i \in \mathcal{B}\}.$$

For any $h \in R_m$ with $Z(h) \cap \mathcal{P} = \emptyset$, define

$$L^h([D]) = \left\{ \frac{f}{h} : f \in F([D]) \right\}.$$

Let $ev_{\mathcal{P}}^h : L^h([D]) \to \mathbb{F}_q^n$ be the evaluation map on $L^h([D])$, where $n = |\mathcal{P}|$. Define the corresponding code to be $C^h(\mathcal{B}, \mathcal{P}, [D]) = ev_{\mathcal{P}}^h(L^h([D]))$.

The next proposition and corollary show that the choice of denominator for the rational functions does not affect the resulting code parameters.

Proposition 5.1.3. *Let $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ be effective with $m, m_1, ..., m_b \geq 0$. The parameters $[n, k, d]$ of $C^g(\mathcal{B}, \mathcal{P}, [D])$ and $C^h(\mathcal{B}, \mathcal{P}, [D])$ are the same for any $g, h \in R_m$ satisfying $Z(g) \cap \mathcal{P} = Z(h) \cap \mathcal{P} = \emptyset$.*

Proof. The length of each code is $|\mathcal{P}|$. The proof that the two codes have the same dimension and minimum distance is the same as that of Proposition 4.1.4. □

Corollary 5.1.4. *Let D be an effective divisor such that* $\operatorname{supp} D \cap \mathcal{P} = \emptyset$ *and $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ with $m, m_1, ..., m_b \geq 0$. The parameters of the code $C(\mathcal{B}, \mathcal{P}, D)$ are the same as those of $C^h(\mathcal{B}, \mathcal{P}, [D])$ for any $h \in R_m$ with $Z(h) \cap \mathcal{P} = \emptyset$.*

Proof. The proof is the same as that of Corollary 4.1.5 except that we apply Proposition 5.1.3 in place of Proposition 4.1.4. □

Remark. By Corollary 5.1.4, the parameters of $C(\mathcal{B}, \mathcal{P}, D)$ depend only upon $\mathcal{B}$, $\mathcal{P}$ and $[D]$. As in Chapter 4, constructing $C^h(\mathcal{B}, \mathcal{P}, [D])$ is simpler than constructing

$C(\mathcal{B}, \mathcal{P}, D)$ because we can find the functions in $F([D])$ by checking multiplicities at prescribed zeros. Finding the functions in $L(D)$ requires knowledge of the specific divisor $D \in \mathbb{P}^r_{\mathcal{B}}$. Thus, for the remainder of this chapter, we will study codes of the form $C^h(\mathcal{B}, \mathcal{P}, [D])$.

We now fix the set of evaluation points $\mathcal{P}$ in order to obtain more precise results on the dimension and minimum distance.

Definition 5.1.5. For any $r \geq 1$, we define the *regular set of evaluation points*, or simply, the *regular set*, as follows:

$$\mathcal{P} = \{(a_0 : \cdots : a_r) \in \mathbb{P}^r(\mathbb{F}_q) : a_r \neq 0\}.$$

Remark. Note that $|\mathcal{P}| = q^r$ if $\mathcal{P}$ is the regular set. If $h = x_r^m$ with $m \geq 0$, then $Z(h) \cap \mathcal{P} = \emptyset$. Also, since $\mathcal{B} \subset \mathcal{T}_r \subset Z(x_r)$ for $r \geq 2$, we have $\mathcal{B} \cap \mathcal{P} = \emptyset$.

Table A.5 in Appendix A gives the parameters for a family of codes on $\mathbb{P}^3_{\mathcal{B}}$ with $\mathcal{B} \subset Z(x_0 x_1) \cap Z(x_3)$, $\mathcal{P}$ the regular set, $[D] = [bH - E_1 - \cdots - E_b]$ and $c = 2$, where c is the number of coordinate vertices of $\mathbb{P}^3$ in $\mathcal{B}$.

5.2 Bounds on k and d

Our first result is analogous to that in the paper by Serre [31] and will lead to a lower bound on the minimum distance. The difference between this result and that of Serre is that we bound the number of zeros of a polynomial $f \in R_m$ in the regular set $\mathcal{P}$ instead of in the entire space $\mathbb{P}^r(\mathbb{F}_q)$.

Lemma 5.2.1. *Let $r \geq 1$, let $\mathcal{P}$ be the regular set and let $0 \neq f \in R_m$. If $q \geq m$, then $|Z(f) \cap \mathcal{P}| \leq mq^{r-1}$.*

Proof. Let $S = Z(f) \cap \mathcal{P}$ and let $N = |S|$. We prove the result by induction on r. If $r = 1$, we know $|Z(f) \cap \mathcal{P}| \leq m$. So we may assume $r \geq 2$.

Let $n_i = |\mathbb{P}^i(\mathbb{F}_q)| = q^i + q^{i-1} + \cdots + 1$ for $i = 0, ..., r$. Let $g_1, ..., g_\delta$ be the distinct linear factors of f over $\mathbb{F}_q$ and let $G_1, ..., G_\delta$ be the hyperplanes of $\mathbb{P}^r(\mathbb{F}_q)$ defined by the g_i. Let G be the point set given by the union of the G_i. We have two cases.

$Case$ 1: $S \subset G$

In this case, each G_i has n_{r-1} points in $\mathbb{P}^r(\mathbb{F}_q)$, and at least n_{r-2} of these points lie on the hyperplane $x_r = 0$. Hence $|G_i \cap \mathcal{P}| \leq n_{r-1} - n_{r-2} = q^{r-1}$ for $i = 1, ..., \delta$. Thus,

$$N \leq \delta q^{r-1} \leq m q^{r-1}$$

since the degree of f is m.

$Case$ 2: $S \not\subseteq G$

Let $P \in S \setminus G$. If H is a hyperplane of $\mathbb{P}^r(\mathbb{F}_q)$ passing through P, the restriction of f to H is not identically zero, by the choice of P. Since $deg(f|_H) = m$, by the induction hypothesis, we have $|S \cap H| \leq m q^{r-2}$.

Now let A be the set of pairs (P', H') where $P' \in S \setminus \{P\}$ and H' is a hyperplane passing through P and P'. On the one hand, there are $N - 1$ points $P' \in S \setminus \{P\}$ and exactly n_{r-2} hyperplanes H' (defined over $\mathbb{F}_q$) that pass through P and P', so

$$|A| = (N - 1) n_{r-2}. \tag{5.1}$$

On the other hand, there are n_{r-1} hyperplanes H' passing through P. The number of points in $(S \setminus \{P\}) \cap H'$ is exactly one less than $|S \cap H'|$. Hence

$$|A| \leq n_{r-1}(m q^{r-2} - 1). \tag{5.2}$$

Combining Equations 5.1 and 5.2, we have

$$(N-1)n_{r-2} \quad \leq \quad n_{r-1}(mq^{r-2}-1). \tag{5.3}$$

Substituting $n_{r-1} = qn_{r-2} + 1$ into (5.3) and rearranging terms, we have

$$\begin{aligned} Nn_{r-2} &\leq (qn_{r-2}+1)(mq^{r-2}-1) + n_{r-2} \\ &= mq^{r-1}n_{r-2} - (q^{r-1} - mq^{r-2}). \end{aligned}$$

Thus, we have

$$\begin{aligned} N &\leq mq^{r-1} - (q^{r-1} - mq^{r-2})/n_{r-2} \\ &\leq mq^{r-1}, \end{aligned}$$

where the last line holds since $q \geq m$. □

We now prove some lemmas which will help us compute the dimension of the codes for various divisor classes.

Lemma 5.2.2. *Let $r \geq 2$ and let $\mathcal{B} \subset \mathcal{T}_r$. Let D be an effective divisor such that $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ with $m, m_1, ..., m_b \geq 0$. Then* $\dim L(D) \leq \binom{m+r}{r}$.

Proof. The number of monomials of degree m in R is $\binom{m+r}{r}$. This is the dimension of the space of functions $L(D')$, where $[D'] = [mH]$. By imposing the conditions

$$\{f \text{ has a zero of multiplicity at least } m_i \text{ at each } p_i \in \mathcal{B}\},$$

we can only decrease the dimension. □

Lemma 5.2.3. *Let $r \geq 2$ and let $\mathcal{B} \subset \mathcal{T}_r$. Let D be an effective divisor such that $[D] = [mH - E_1 - \cdots - E_b]$ with $m \geq b$. Then* $\dim L(D) = \binom{m+r}{r} - b$.

Proof. We give two proofs. The first is for the algebraic geometer and the second is for the more general reader.

Proof 1: The condition $m \geq b$ guarantees that none of the points of $\mathcal{B}$ is a base point of the linear system of hyperplanes in $\mathbb{P}^r$ of degree m which pass through the rest of the points of $\mathcal{B}$. Thus the points of $\mathcal{B}$ impose independent conditions. Since $\dim R_m = \binom{m+r}{r}$ we subtract b from this to obtain the result.

Proof 2: We prove the result using induction on r. If $r = 2$, then $\dim L(D) = \binom{m+2}{2} - b$ by Section 2.3. So suppose $r \geq 3$. Let Z be the subscheme defined by $p_1 + \cdots + p_b$ (see Section 2.4). Recall that $L(D)$ is canonically isomorphic to $I(Z)_m$, the vector space spanned by all homogeneous polynomials of degree m in $R = \mathbb{F}_q\,[x_0, ..., x_r]$. Let $W = Z(x_r)$. Then by Corollary 2.4.2, we have that

$$\dim I(Z)_m \;=\; \sum_{\ell=0}^{m} \dim I(Z^{(\ell)'})_{m-\ell},$$

where $Z^{(\ell)'}$ is the subscheme $((1-\ell)_+ p_1 + \cdots + (1-\ell)_+ p_b) \cap W_{\mathcal{B}}$ regarded as a subscheme of $W_{\mathcal{B}} = \mathbb{P}^{r-1}_{\mathcal{B}}$. Here $(1-\ell)_+$ is the maximum of $1-\ell$ and 0, so when $\ell = 0$ we have $I(Z^{(\ell)'})_{m-\ell} = F\left([mH' - E_1' - \cdots - E_b']\right)$, where H' is the proper transform of H restricted to $W_{\mathcal{B}}$ and E_i' is the proper transform of E_i restricted to $W_{\mathcal{B}}$. When $\ell = 1, ..., m$, we have $I(Z^{(\ell)'})_{m-\ell} = F\left([mH' - 0E_1' - \cdots - 0E_b']\right) = F\left([mH']\right)$.

Since $D|_{W_{\mathcal{B}} = \mathbb{P}^{r-1}_{\mathcal{B}}}$ is effective, by the induction hypothesis, we have $\dim I(Z^{(0)'})_m = \dim F\left([mH' - E_1' - \cdots - E_b']\right) = \begin{pmatrix} m+r-1 \\ r-1 \end{pmatrix} - b$. For $\ell = 1, ..., m$, it is clear that $\dim I(Z^{(\ell)'})_{m-\ell} = \dim F\left([(m-\ell)H']\right) = \begin{pmatrix} m-\ell+r-1 \\ r-1 \end{pmatrix}$ since there are no conditions imposed by $p_1, ..., p_b$. Hence we have:

$$\sum_{\ell=0}^{m} \dim I(Z^{(\ell)'})_{m-\ell} = \binom{m+r-1}{r-1} - b + \sum_{\ell=1}^{m} \binom{m-\ell+r-1}{r-1}.$$

Using the combinatorial equality $\binom{n-1}{k-1} = \binom{n}{k} - \binom{n-1}{k}$ for integers n and k, and noting the telescoping series, we continue the chain of equalities:

$$\begin{aligned} &= \binom{m+r-1}{r-1} - b + \sum_{\ell=1}^{m} \left(\binom{m-\ell+r}{r} - \binom{m-\ell+r-1}{r} \right) \\ &= \binom{m+r-1}{r-1} - b + \binom{m-1+r}{r} \\ &= \binom{m+r}{r} - b. \end{aligned}$$

□

Remark. The condition $m \geq b$ implies that $[D]$ is effective. For each $i = 1, ..., b$, let H_i be a hyperplane in $\mathbb{P}^r$ through p_i that does not pass through any p_j with $j \neq i$. Let $H_{b+1}, ..., H_m$ be hyperplanes in $\mathbb{P}^r$ that do not pass through any of the points of $\mathcal{B}$. Let H'_i be the proper transform in $\mathbb{P}^r_{\mathcal{B}}$ of H_i for $i = 1, ..., m$. Then $D' = \sum_{i=1}^{m} H'_i$ is clearly effective and satisfies $[D'] = [mH - E_1 - \cdots - E_b] = [D]$. Hence $[D]$ is an effective divisor class.

Lemma 5.2.4. *Let $r = 3$ and $\mathcal{B} \subset Z(x_0x_1) \cap Z(x_3) = \mathcal{T}_3$. Let D be a divisor on $\mathbb{P}^3_{\mathcal{B}}$ such that the restriction of $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ to the proper transform of the plane $W := Z(x_3)$ containing $\mathcal{T}_3$ is numerically effective. Then*

$$\dim L(D) = \sum_{\ell=0}^{m} \left(\binom{m-\ell+2}{2} - \sum_{i=1}^{b} \binom{m_i-\ell+1}{2} \right).$$

Proof. Let Z be the subscheme defined by $m_1p_1 + \cdots + m_bp_b$ (see Section 2.4). Recall that $L(D)$ is canonically isomorphic to $I(Z)_m$, the vector space spanned by all homogeneous polynomials of degree m in $R = \mathbb{F}_q\,[x_0, ..., x_3]$. Then by Corollary 2.4.2, we have that

$$\dim I(Z)_m \;=\; \sum_{\ell=0}^{m} \dim I(Z^{(\ell)'})_{m-\ell},$$

where $Z^{(\ell)'}$ is the subscheme $((m_1 - \ell)_+ p_1 + \cdots + (m_b - \ell)_+ p_b) \cap W_{\mathcal{B}}$ regarded as a subscheme of $W_{\mathcal{B}}$. (Here $(m_j - \ell)_+$ is the maximum of $m_j - \ell$ and 0.) Thus $I(Z^{(\ell)'})_{m-\ell} = F\left([(m-\ell)H' - (m_1 - \ell)_+ E_1' - \cdots - (m_b - \ell)_+ E_b']\right)$, where H' is the proper transform of H restricted to $W_{\mathcal{B}}$ and E_i' is the proper transform of E_i restricted to $W_{\mathcal{B}}$.

We assumed that $[D|_{W_{\mathcal{B}}}] = [mH' - m_1E_1' - \cdots - m_bE_b']$ is numerically effective, so by Section 2.3 (after possibly reordering the m_i's), we have $m - m_1 - m_2 \geq 0$, $m \geq \displaystyle\sum_{p_i \in Z(x_0) \cap \mathcal{B}} m_i$ and $m \geq \displaystyle\sum_{p_i \in Z(x_1) \cap \mathcal{B}} m_i$. Then we have:

(i) $(m - \ell) - (m_1 - \ell)_+ - (m_2 - \ell)_+ \geq 0$,
(ii) $m - \ell \geq \displaystyle\sum_{p_i \in Z(x_0) \cap \mathcal{B}} (m_i - \ell)_+$ and
(iii) $m \geq \displaystyle\sum_{p_i \in Z(x_1) \cap \mathcal{B}} (m_i - \ell)_+$ for $\ell = 0, ..., m$.

So $[(m-\ell)H' - (m_1 - \ell)_+ E_1' - \cdots - (m_b - \ell)_+ E_b']$ is also numerically effective. Hence

$$\begin{aligned} \dim I(Z^{(\ell)'})_{m-\ell} &= \dim F\left([(m-\ell)H' - (m_1 - \ell)_+ E_1' - \cdots - (m_b - \ell)_+ E_b']\right) \\ &= \binom{m-\ell+2}{2} - \sum_{i=0}^{b} \binom{m_i - \ell + 1}{2}, \end{aligned}$$

where the last line holds by Section 2.3. Finally, we have

$$\sum_{\ell=0}^{m} \dim I(Z^{(\ell)'})_{m-\ell} \;=\; \sum_{\ell=0}^{m} \left(\binom{m-\ell+2}{2} - \sum_{i=0}^{b} \binom{m_i-\ell+1}{2} \right),$$

where we use the convention $\binom{m_i-\ell+1}{2} = 0$ whenever $m_i - \ell < 0$. □

We now prove three propositions which give the dimension (or a bound on the dimension) for codes coming from various divisor classes.

Proposition 5.2.5. *Let $r \geq 2$, $\mathcal{B} \subset \mathcal{T}_r$ and $\mathcal{P}$ be the regular set. Let $[D] = [mL - m_1E_1 - \cdots - m_bE_b]$ be effective with $m, m_1, ..., m_b \geq 0$. Then for all q, the dimension of $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = x_r^m$) is less than or equal to $\dim L(D)$. In particular, we have*

$$k \leq \binom{m+r}{r}.$$

Proof. Recall that we have the evaluation map $ev_{\mathcal{P}}^h : L^h([D]) \to \mathbb{F}_q^n$, with $k = \dim ev_{\mathcal{P}}^h(L^h([D]))$ and

$$\dim L^h([D]) = \dim ev_{\mathcal{P}}^h(L^h([D])) + \dim(\ker ev_{\mathcal{P}}^h).$$

Hence

$$\dim ev_{\mathcal{P}}^h(L^h([D])) \leq \dim L^h([D]) = \dim L(D) \leq \binom{m+r}{r},$$

where the last inequality holds by Lemma 5.2.2. □

Proposition 5.2.6. *Let $r \geq 2$, $\mathcal{B} \subset \mathcal{T}_r$ and $\mathcal{P}$ be the regular set. Let $[D] = [mH - E_1 - \cdots - E_b]$ with $m \geq b$. Then for all $q > m$, the dimension of $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = x_r^m$) is equal to $\dim L(D)$. In particular, we have*

$$k = \binom{m+r}{r} - b.$$

Proof. The proof is similar to that of Proposition 4.1.8. Recall that we have the evaluation map $ev^h_{\mathcal{P}} : L^h([D]) \to \mathbb{F}_q^n$, with $k = \dim ev^h_{\mathcal{P}}(L^h([D]))$ and

$$\dim L^h([D]) = \dim ev^h_{\mathcal{P}}(L^h([D])) + \dim(\ker ev^h_{\mathcal{P}}).$$

We now show that $\ker ev^h_{\mathcal{P}} = 0$. Let $\frac{f}{h} \not\equiv 0$ be in $L^h([D])$. By Lemma 5.2.1, since $q > m$, we have $|Z(\frac{f}{h}) \cap \mathcal{P}| = |Z(f) \cap \mathcal{P}| \leq mq^{r-1} < q^r$. Thus $\frac{f}{h}(p) \neq 0$ for some $p \in \mathcal{P}$ and so $\frac{f}{h} \notin \ker ev^h_{\mathcal{P}}$. Hence $\ker ev^h_{\mathcal{P}} = 0$ and so $\dim ev^h_{\mathcal{P}}(L^h([D])) = \dim L^h([D])$. Thus,

$$k = \dim L^h([D]) = \dim L(D) = \binom{m+r}{r} - b,$$

where the last equality holds by Lemma 5.2.3. □

Proposition 5.2.7. *Let $r = 3$, $\mathcal{B} \subset Z(x_0x_1) \cap Z(x_3) = \mathcal{T}_3$ and $\mathcal{P}$ be the regular set. Let $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ be such that the restriction of $[D]$ to the proper transform of the plane containing $\mathcal{T}_3$ is numerically effective. Then for all $q > m$, the dimension of $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = x_3^m$) is equal to $\dim L(D)$. In particular, we have*

$$k = \dim L(D) = \sum_{\ell=0}^{m} \left(\binom{m-\ell+2}{2} - \sum_{i=1}^{b} \binom{m_i - \ell + 1}{2} \right).$$

Proof. The proof is the same as that of Proposition 5.2.6 except that we apply Lemma 5.2.4. □

We can now state three theorems (corresponding to the previous three propositions) which give bounds or exact results on the code parameters $[n, k, d]$ for the various divisor classes. All of these theorems employ the bound in Lemma 5.2.1.

Theorem 5.2.8. *Let $r \geq 2$, $\mathcal{B} \subset \mathcal{T}_r$ and $\mathcal{P}$ be the regular set. Let $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ be effective with $m, m_1, ..., m_b \geq 0$. Then for all $q > m$, $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = x_r^m$) is a $[q^r, k, d]$ code, where $k \leq \binom{m+r}{r}$ and $d \geq q^r - mq^{r-1}$.*

Proof. The proof is similar to that of Theorem 4.1.9. The upper bound on the dimension is given by Proposition 5.2.5. To compute the minimum distance d, note that the weight of a codeword $ev_{\mathcal{P}}(\frac{f}{h})$ is equal to q^r minus the number of number of points of $\mathcal{P}$ at which $\frac{f}{h}$ vanishes. Hence by Lemma 5.2.1, we have

$$\begin{aligned} d &= q^r - \max\left\{\left|Z\left(\frac{f}{h}\right)\cap\mathcal{P}\right| : \frac{f}{h}\in L^h([D]),\ \frac{f}{h}\not\equiv 0\right\} \\ &= q^r - \max\left\{|Z(f)\cap\mathcal{P}| : f\in F\left([D]\right),\ f\not\equiv 0\right\} \\ &\geq q^r - mq^{r-1}. \end{aligned}$$

□

Theorem 5.2.9. *Let $r \geq 2$, $\mathcal{B} \subset \mathcal{T}_r$ and $\mathcal{P}$ be the regular set. Let $[D] = [mH - E_1 - \cdots - E_b]$ with $m \geq b$. Then for all $q > m$, $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = x_r^m$) is a $[q^r, k, d]$ code, where $k = \binom{m+r}{r} - b$ and $d \geq q^r - mq^{r-1}$.*

Proof. The dimension is given by Proposition 5.2.6. We use the argument in the proof of Theorem 5.2.8 to obtain the lower bound on the minimum distance. □

Theorem 5.2.10. *Let $r = 3$, $\mathcal{B} \subset Z(x_0x_1) \cap Z(x_3) = \mathcal{T}_3$ and $\mathcal{P}$ be the regular set. Let $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ be such that the restriction of $[D]$ to the proper transform of the plane containing $\mathcal{T}_3$ is numerically effective. Then for all $q > m$, $C^h(\mathcal{B}, \mathcal{P}, [D])$ (with $h = x_3^m$) is a $[q^3, k, d]$ code where $d \geq q^3 - mq^2$ and*

$$k = \sum_{\ell=0}^{m}\left(\binom{m-\ell+2}{2} - \sum_{i=1}^{b}\binom{m_i-\ell+1}{2}\right).$$

Proof. The dimension is given by Proposition 5.2.7. We use the argument in the proof of Theorem 5.2.8 to obtain the lower bound on the minimum distance. □

5.3 Asymptotic Results

The construction in Definition 5.0.1 yields infinite families of codes with q fixed. (We obtain such a family by fixing q and a divisor class $[D]$ and then letting $r \to \infty$.) We will see that the relative minimum distance d/n is bounded away from 0 as $n \to \infty$, but that the rate k/n approaches 0 as $n \to \infty$.

By Proposition 5.2.5, we know that for $r \geq 2$ the dimension of $C^h(\mathcal{B}, \mathcal{P}, [D])$ for any divisor class $[D] = [mH - m_1E_1 - \cdots - m_bE_b]$ with $m, m_1, ..., m_b \geq 0$ is at most $\binom{m+r}{r}$. Let q be fixed. Then

$$\begin{aligned} k/n &\leq \frac{\binom{m+r}{r}}{q^r} = \left(\frac{m+r}{qr}\right)\left(\frac{m+r-1}{q(r-1)}\right)\cdots\left(\frac{m+1}{q}\right) \\ &= \prod_{i=1}^{r} \frac{m+i}{qi}. \end{aligned}$$

Now $\lim_{r\to\infty} \prod_{i=1}^{r} \frac{m+i}{qi} = 0$ since $\frac{m+r}{qr} \to 1/q < 1$ as $r \to \infty$. Hence an infinite family of codes with a fixed divisor class $[D]$ and field size will have a rate which approaches 0 as the dimension r of projective space approaches infinity.

On the other hand, by Theorem 5.2.8 we have that $d/n \geq \frac{q^r - mq^{r-1}}{q^r} = 1 - m/q$. Hence an infinite family of codes will always have relative minimum distance bounded away from zero, provided that $q > m$.

This leads us to believe that there is potential for asymptotically good codes with a similar construction to that in Definition 5.0.1, but we would need to use a larger space of functions than $L(D)$ or we would need to evaluate at a smaller point set than the regular set $\mathcal{P} = \{(a_0 : \cdots : a_r) \in \mathbb{P}^r(\mathbb{F}_q) : a_r \neq 0\}$.

5.4 Comparison of Codes on $\mathbb{P}^r_{\mathcal{B}}$

Even though the rate or relative minimum distance of a family of codes may approach 0, it is possible that many good codes exist if the convergence is slow. We investigate this possibility in this section for the construction in Definition 5.0.1. Table 5.1 shows the upper bound on the rate k/n from Theorem 5.2.8 for various values of q and $r \geq 2$. We use $m = q - 1$ to obtain as large a rate as possible, while maintaining the lower bound on the minimum distance from Theorem 5.2.8.

Table 5.1: Upper bounds for rates of codes on $\mathbb{P}^r_{\mathcal{B}}$, where $\mathcal{B} \subset \mathcal{T}_r$

r	$q=2$	$q=3$	$q=4$	$q=5$	$q=7$	$q=8$	$q=9$	$q=11$	$q=13$	$q=16$
2	.75	.67	.63	.60	.57	.56	.56	.55	.54	.53
3	.50	.37	.32	.28	.24	.23	.23	.21	.21	.20
4	.31	.19	.14	.11	.09	.08	.08	.07	.06	.06
5	.19	.09	.05	.04	.03	.02	.02	.02	.02	.01
6	.11	.04	.02	.01	.01	.01	.01	.00	.00	.00
7	.06	.02	.01	.00	.00	.00	.00	.00	.00	.00

We see that the convergence of k/n to zero as $r \to \infty$ is quite fast, so one is most likely to use a code with, say, $r \leq 3$. Results on the minimum distance for $r = 3$ are still being investigated (see, for example, Table A.5). To get families of codes with higher rates, one could decrease the size of the set of evaluation points $\mathcal{P}$, as mentioned at the end of Section 5.3.

Appendix A

Code Tables

A.1 One-Line Codes with $[D] = [bL - E_1 - \cdots - E_b]$ and $c = 2$

Table A.1 shows the parameters for a family of one-line codes with $\mathcal{P}$ the standard set, $[D] = [bL - E_1 - \cdots - E_b]$ and

$$\mathcal{B} = \{(0:0:1), (0:1:0)\} \cup \{(0:1:1), (0:\gamma:1), ..., (0:\gamma^{b-3}:1)\},$$

where γ is a primitive element of the finite field $\mathbb{F}_q$. (Note that $c = 2$.) The Magma function in Section B.2 can be used to generate the codes $C^h(\mathcal{B}, \mathcal{P}, [D])$. The results in Table A.1 were either obtained using Magma [3] (for small q) or using Theorem 4.2.5 of Section 4.2. An entry is marked "n/a" if q is too small for the points of $\mathcal{B}$ to be distinct. An entry is marked with a "-" if q is too large to easily compute the minimum distance using Magma [3] and too small to apply Theorem 4.2.5. Note that we start with $q = 3$ since anticanonical surface codes over $\mathbb{F}_2$ have length one and are therefore trivial.

Table A.1: Parameters k, d of one-line codes with $[D] = [bL - E_1 - \cdots - E_b]$ and $c = 2$

	$q = 3$	$q = 4$	$q = 5$	$q = 7$	$q = 8$	$q = 9$	$q = 11$	$q = 13$	$q = 16$
b	$n = 4$	$n = 9$	$n = 16$	$n = 36$	$n = 49$	$n = 64$	$n = 100$	$n = 144$	$n = 224$
2	4,1	4,4	4,9	4,25	4,36	4,49	4,81	4,121	4,196
3	4,1	7,2	7,6	7,20	7,30	7,42	7,72	7,110	7,182
4	4,1	9,1	11,4	11,16	11,25	11,36	11,64	11,100	11,169
5	n/a	9,1	14,2	16,12	16,20	16,30	16,-	16,90	16,156
6	n/a	n/a	15,2	22,6	22,14	22,-	22,-	22,-	22,143
7	n/a	n/a	n/a	27,4	29,7	29,-	29,-	29,-	29,-
8	n/a	n/a	n/a	30,4	35,5	37,-	37,-	37,-	37,-
9	n/a	n/a	n/a	n/a	39,5	44,-	46,-	46,-	46,-

A.2 Two-Line Codes with $[D] = [sL - E_1 - \cdots - E_b]$ and $c = 0$

Table A.2 shows the parameters for a family of two-line codes with $\mathcal{P}$ the standard set, $[D] = [(s+2)L - E_1 - \cdots - E_b]$ and $\mathcal{B} = \{(0:1:1), (0:\gamma^2:1), ..., (0:\gamma^{2(s-1)}:1)\} \cup \{(1:0:1), (\gamma:0:1), ..., (\gamma^{r-1}:0:1)\}$, where γ is a primitive element of the finite field $\mathbb{F}_q$. (Note that $c = 0$.) The Magma function in Section B.3 can be used to generate the codes $C^h(\mathcal{B}, \mathcal{P}, [D])$. An entry in Table A.2 is marked "n/a" if q is too small for the points of $\mathcal{B}$ to be distinct. (We need $q - 1 \geq 2s - 1$ if q is odd and $q - 1 \geq s$ if q is even.) An entry is marked with a "-" if q is too large to easily compute the minimum distance using Magma [3].

Table A.2: Parameters k, d of two-line codes with $[D] = [sL - E_1 - \cdots - E_b]$ and $c = 0$

			$q = 3$	$q = 4$	$q = 5$	$q = 7$	$q = 8$	$q = 9$	$q = 11$
b	s	r	$n = 4$	$n = 9$	$n = 16$	$n = 36$	$n = 49$	$n = 64$	$n = 100$
2	1	1	1,3	1,7	1,13	1,31	1,43	1,57	1,91
2	2	0	n/a	4,3	4,8	4,24	4,35	4,48	4,80
3	2	1	n/a	3,5	3,10	3,26	3,37	3,50	3,82
3	3	0	n/a	6,3	n/a	7,18	7,28	7,40	7,70
4	2	2	n/a	2,5	2,11	2,27	2,38	2,51	2,83
4	3	1	n/a	6,3	n/a	6,21	6,31	6,43	6,73
4	4	0	n/a	n/a	n/a	n/a	11,21	11,32	11,60
5	3	2	n/a	5,3	n/a	5,22	5,32	5,44	5,75
5	4	1	n/a	n/a	n/a	n/a	10,25	10,36	10,64
5	5	0	n/a	n/a	n/a	n/a	16,14	n/a	16,-
6	3	3	n/a	4,3	n/a	4,23	4,33	4,45	4,75
6	4	2	n/a	n/a	n/a	n/a	9,25	9,38	9,66
6	5	1	n/a	n/a	n/a	n/a	15,19	n/a	15,-
6	6	0	n/a	n/a	n/a	n/a	22,7	n/a	n/a
7	4	3	n/a	n/a	n/a	n/a	8,27	8,39	8,66
7	5	2	n/a	n/a	n/a	n/a	14,19	n/a	14,-
7	6	1	n/a	n/a	n/a	n/a	21,13	n/a	n/a
7	7	0	n/a	n/a	n/a	n/a	28,-	n/a	n/a
8	4	4	n/a	n/a	n/a	n/a	7,28	7,40	7,68
8	5	3	n/a	n/a	n/a	n/a	13,19	n/a	13,-
8	6	2	n/a	n/a	n/a	n/a	20,13	n/a	n/a
8	7	1	n/a	n/a	n/a	n/a	28,-	n/a	n/a
8	8	0	n/a	n/a	n/a	n/a	n/a	n/a	n/a
9	5	4	n/a	n/a	n/a	n/a	12,19	n/a	12,-
9	6	3	n/a	n/a	n/a	n/a	19,13	n/a	n/a
9	7	2	n/a	n/a	n/a	n/a	27,-	n/a	n/a
9	8	1	n/a	n/a	n/a	n/a	n/a	n/a	n/a
9	9	0	n/a	n/a	n/a	n/a	n/a	n/a	n/a

A.3 Two-Line Codes with $[D] = [(s+2)L - E_1 - \cdots - E_b]$ and $c = 3$

Table A.3 shows the parameters for a family of two-line codes with $\mathcal{P}$ the standard set, $[D] = [(s+2)L - E_1 - \cdots - E_b]$ and $\mathcal{B} = \{(0:0:1),(0:1:0),(1:0:0)\} \cup \{(0:1:1),(0:\gamma:1),...,(0:\gamma^{s-1}:1)\} \cup \{(1:0:1),(\gamma:0:1),...,(\gamma^{r-1}:0:1)\}$, where γ is a primitive element of the finite field $\mathbb{F}_q$. (Note that $c = 3$.) The Magma function in Section B.4 can be used to generate these codes. An entry in Table A.3 is marked "n/a" if q is too small for the points of $\mathcal{B}$ to be distinct. An entry is marked with a "-" if q is too large to easily compute the minimum distance using Magma [3].

Table A.3: Parameters k, d of two-line codes with $[D] = [(s+2)L - E_1 - \cdots - E_b]$ and $c = 3$

			$q=3$	$q=4$	$q=5$	$q=7$	$q=8$	$q=9$	$q=11$
b	s	r	$n=4$	$n=9$	$n=16$	$n=36$	$n=49$	$n=64$	$n=100$
3	0	0	3,2	3,6	3,12	3,30	3,42	3,56	3,90
4	1	0	4,1	6,2	6,6	6,20	6,30	6,42	6,72
5	1	1	4,1	5,2	5,6	5,20	5,30	5,42	5,72
5	2	0	4,1	9,1	10,4	10,16	10,25	10,36	10,64
6	2	1	4,1	9,1	9,4	9,16	9,25	9,36	9,64
6	3	0	n/a	9,1	14,2	15,12	15,20	15,30	15,-
7	2	2	4,1	8,1	8,4	8,16	8,26	8,38	8,64
7	3	1	n/a	9,1	14,2	14,12	14,20	14,30	14,-
7	4	0	n/a	n/a	15,2	21,6	21,14	21,-	21,-
8	3	2	n/a	9,1	13,2	13,12	13,20	13,30	13,-
8	4	1	n/a	n/a	15,2	20,8	20,15	20,-	20,-
8	5	0	n/a	n/a	n/a	27,4	28,7	28,-	28,-
9	3	3	n/a	8,2	12,2	12,12	12,22	12,30	12,-
9	4	2	n/a	n/a	15,2	19,8	19,15	19,-	19,-
9	5	1	n/a	n/a	n/a	27,4	27,-	27,-	27,-
9	6	0	n/a	n/a	n/a	30,4	35,-	36,-	36,-

A.4 Two-Line Codes with $[D] = [bL - E_1 - \cdots - E_b]$ and $c = 3$

Table A.4 shows the parameters for a family of two-line codes with $\mathcal{P}$ the standard set, $[D] = [bL - E_1 - \cdots - E_b]$ and $\mathcal{B} = \{(0:0:1),(0:1:0),(1:0:0)\} \cup \{(0:1:1),(0:\gamma:1),...,(0:\gamma^{s-1}:1)\} \cup \{(1:0:1),(\gamma:0:1),...,(\gamma^{r-1}:0:1)\}$, where γ is a primitive element of the finite field $\mathbb{F}_q$. (Note that $c = 3$.) The Magma function in Section B.4 can be used to generate these codes. An entry in Table A.4 is marked "n/a" if q is too small for the points of $\mathcal{B}$ to be distinct. An entry is marked with a "-" if q is too large to easily compute the minimum distance using Magma [3].

Table A.4: Parameters k, d of two-line codes with $[D] = [bL - E_1 - \cdots - E_b]$ and $c = 3$

			$q = 3$	$q = 4$	$q = 5$	$q = 7$	$q = 8$	$q = 9$	$q = 11$
b	s	r	$n = 4$	$n = 9$	$n = 16$	$n = 36$	$n = 49$	$n = 64$	$n = 100$
3	0	0	4,1	7,2	7,6	7,20	7,30	7,42	7,72
4	1	0	4,1	9,1	11,4	11,16	11,24	11,36	11,-
5	1	1	4,1	9,1	15,2	16,12	16,20	16,30	16,-
5	2	0	4,1	9,1	15,2	16,12	16,20	16,-	16,-
6	2	1	4,1	9,1	16,1	22,8	22,15	22,-	22,-
6	3	0	n/a	9,1	16,1	22,6	22,-	22,-	22,-
7	2	2	4,1	9,1	16,1	29,4	29,-	29,-	29,-
7	3	1	n/a	9,1	16,1	29,4	29,-	29,-	29,-
7	4	0	n/a	n/a	16,1	28,4	29,7	29,-	29,-
8	3	2	n/a	9,1	16,1	33,3	37,5	37,-	37,-
8	4	1	n/a	n/a	16,1	32,3	37,5	37,-	37,-
8	5	0	n/a	n/a	n/a	31,3	36,5	37,-	37,-
9	3	3	n/a	9,1	16,1	35,2	42,4	46,-	46,-
9	4	2	n/a	n/a	16,1	35,2	42,4	46,-	46,-
9	5	1	n/a	n/a	n/a	34,2	41,4	46,-	46,-
9	6	0	n/a	n/a	n/a	33,3	40,4	45,6	46,-

A.5 One-Line Codes on $\mathbb{P}^3_{\mathcal{B}}$ with $[D] = [bH - E_1 - \cdots - E_b]$ and $c = 2$

Table A.5 shows the parameters for a family of one-line codes on $\mathbb{P}^3$ with $\mathcal{P}$ the regular set, $[D] = [bH - E_1 - \cdots - E_b]$ and

$$\mathcal{B} = \{(0:0:1:0), (0:1:0:0)\} \cup \{(0:1:1:0), ..., (0:\gamma^{b-3}:1:0)\},$$

where γ is a primitive element of the finite field $\mathbb{F}_q$. (Note that $c = 2$.) The Magma function in Section B.5 can be used to generate these codes. An entry in Table A.5 is marked "n/a" if q is too small for the points of $\mathcal{B}$ to be distinct. An entry is marked with a "-" if q is too large to easily compute the minimum distance using Magma [3].

Table A.5: Parameters k, d of one-line codes on $\mathbb{P}^3_{\mathcal{B}}$ with $[D] = [bH - E_1 - \cdots - E_b]$ and $c = 2$

	$q = 2$	$q = 3$	$q = 4$	$q = 5$	$q = 7$	$q = 8$	$q = 9$	$q = 11$
b	$n = 8$	$n = 27$	$n = 64$	$n = 125$	$n = 343$	$n = 512$	$n = 729$	$n = 1331$
2	7,2	8,9	8,32	8,75	8,245	8,384	8,567	8,-
3	8,1	16,6	17,16	17,50	17,-	17,-	17,-	17,-
4	n/a	22,3	30,12	31,25	31,-	31,-	31,-	31,-
5	n/a	n/a	42,8	50,-	51,-	51,-	51,-	51,-
6	n/a	n/a	n/a	69,-	78,-	78,-	78,-	78,-
7	n/a	n/a	n/a	n/a	112,-	113,-	113,-	113,-
8	n/a	n/a	n/a	n/a	148,-	156,-	157,-	157,-
9	n/a	n/a	n/a	n/a	n/a	202,-	210,-	211,-

Appendix B

Magma Functions for Computing Codes

B.1 Using the Magma Functions

We first give an example of how to use the Magma function *ChBPD1L* defined in Section B.2 to compute the parameters of an anticanonical surface code. Use of the other Magma functions (*ChBPD2Lnoc*, *ChBPD2L* and *ChBPD1LP3*) is similar. In each function the parameter q is a prime power corresponding to the size of the finite field $\mathbb{F}_q$.

Example B.1.1. Let $q = 9$ and γ be a generator of the multiplicative group $\mathbb{F}_q^*$. Let $\mathcal{B} = \{(0 : 0 : 1), (0 : 1 : 0), (0 : 1 : 1)\}$, $[D] = [3L - E_1 - E_2 - E_3]$ and $\mathcal{P}$ be the standard set. Then $C^h(\mathcal{B}, \mathcal{P}, [D])$ is a one-line code with $c = 2$. Note that $\mathcal{B}$ is the same as that defined in the Magma code of Section B.2 for $b = 3$. Our inputs to the function are $q = 9$, $m = 3$ and $b = 3$. A sample Magma session follows, where the user input immediately follows the ">". We assume the text in Section B.2 has been saved in a file named *ChBPD1L_file* in the MAGMA directory.

```
> load "ChBPD1L_file";

Loading "ChBPD1L_file"

> C:=ChBPD1L(9,3,3);

> Length(C);

64

> Dimension(C);

7

> MinimumDistance(C);

42
```

Thus C is a 9-ary [64,7,42] code. This matches the result in Table A.1.

B.2 One-Line Code with $[D] = [mL - E_1 - \cdots - E_b]$ and $c = 2$

```
//Filename: ChBPD1L_file

//This program defines the function ChBPD1L(q,m,b) which returns

//the anticanonical surface code C=C^h(B,P,[D]) over F_q where:

//B={(0:0:1),(0:1:0)} U {(0:1:1),...,(0:g^(b-3):1)},

//P is the standard set,

//[D]=[mL-E_1-...-E_b] and

//h=z^m.

////////////////////////////////////////////////////////////////////

ChBPD1L:=function(q,m,b)

//We define the finite field F_q and a primitive element g of F_q.

F_q:=GF(q);

g:=PrimitiveElement(F_q);
```

```
//We define the points of B as a matrix, where each row contains the
//coordinates of a single point.
if b eq 1 then
B:=Matrix(F_q,1,3,[1,0,0]);
else
B:=ZeroMatrix(F_q,b,3);
B[1]:=Vector(F_q,3,[0,0,1]);
B[2]:=Vector(F_q,3,[0,1,0]);
for i in [1..b-2] do
B[i+2]:=Vector(F_q,3,[0,g^(i-1),1]);
end for;
end if;
//We now define the polynomial ring R:=F_q[x,y,z].
R<x,y,z>:=PolynomialRing(F_q,3);
//Next we define the vector R_m of monomials in R of degree m.
//Note that these generate all the homogeneous polynomials
//in R of degree m.
R_m:=[];
index:=0;
for j in [0..m] do
for k in [0..(m-j)] do
index:=index+1;
R_m[index]:=x^j*y^k*z^(m-j-k);
end for;
end for;
R_mLength:=#R_m;
```

```
R_m:=Vector(R,R_mLength,R_m);
//We now define the matrix M whose entries are the values of the
//monomials in R_m at the points of B.
M:=ZeroMatrix(F_q,R_mLength,b);
for i in [1..R_mLength] do
for j in [1..b] do
M[i,j]:=Evaluate(R_m[i],[B[j,1],B[j,2],B[j,3]]);
end for;
end for;
//Next we find a basis for the nullspace of M.
//This gives us a basis for the functions in F([D]).
N:=NullspaceMatrix(M);
//Now we define the vector whose entries are a basis for the
//polynomials in F([D]).
FD:=[];
index:=0;
for j in [1..NumberOfRows(N)] do
poly:=0;
index:=index+1;
for k in [1..R_mLength] do
poly:=poly+N[j,k]*R_m[k];
end for;
FD[index]:=poly;
end for;
k:=#FD;
FD:=Vector(R,k,FD);
```

```
//We are now ready to compute the matrix G whose rows are the
//vectors ev_P(f) for f in FD. The linear span of these vectors
//is our code.
G:=ZeroMatrix(F_q,k,(q-1)^2);
for t in [1..k] do
for i in [0..(q-2)] do
for j in [0..(q-2)] do
G[t,(q-1)*i+j+1]:=Evaluate(FD[t],[g^i,g^j,1])/
Evaluate(z^m,[g^i,g^j,1]);
end for;
end for;
end for;
//Finally, we construct the code C^h(B,P,[D]), which is the
//linear subspace of F_q^n spanned by the rows of the matrix G.
C:=LinearCode(G);
return C;
end function;
```

B.3 Two-Line Code with $[D] = [mL - E_1 - \cdots - E_b]$ and $c = 0$

```
//Filename: ChBPD2Lnoc_file
//This program defines the function ChBPD2Lnoc(q,m,s,r) which returns
//the anticanonical surface code C=C^h(B,P,[D]) over F_q where:
//B={(0:1:1),(0:g^2:1),...,(0:g^(2*(s-1)):1)} U
//{(1:0:1),(g:0:1),...,(g^(r-1):0:1)},
//P is the standard set,
//[D]=[mL-E_1-...-E_b] and
//h=z^m.
////////////////////////////////////////////////////////////////////
ChBPD2Lnoc:=function(q,m,s,r)
//We define the finite field F_q and a primitive element g of F_q.
F_q:=GF(q);
g:=PrimitiveElement(F_q);
//We have the following equality for b since c=0.
b:=s+r;
//We define the points of B as a matrix, where each row contains the
//coordinates of a single point.
B:=ZeroMatrix(F_q,b,3);
for i in [1..s] do
B[i]:=Vector(F_q,3,[0,g^(2*(i-1)),1]);
end for;
for j in [1..r] do
B[s+j]:=Vector(F_q,3,[g^(j-1),0,1]);
end for;
//We now define the polynomial ring R:=F_q[x,y,z].
R<x,y,z>:=PolynomialRing(F_q,3);
//Next we define the vector R_m of monomials in R of degree m.
//Note that these generate all the homogeneous polynomials in R
//of degree m.
R_m:=[];
index:=0;
```

```
for j in [0..m] do
for k in [0..(m-j)] do
index:=index+1;
R_m[index]:=x^j*y^k*z^(m-j-k);
end for;
end for;
R_mLength:=#R_m;
R_m:=Vector(R,R_mLength,R_m);
//We now define the matrix M whose entries are the values of the
//monomials in R_m at the points of B.
M:=ZeroMatrix(F_q,R_mLength,b);
for i in [1..R_mLength] do
for j in [1..b] do
M[i,j]:=Evaluate(R_m[i],[B[j,1],B[j,2],B[j,3]]);
end for;
end for;
//Next we find a basis for the nullspace of M.
//This gives us a basis for the functions in F([D]).
N:=NullspaceMatrix(M);
//Now we define the vector whose entries are a basis for the
//polynomials in F([D]).
FD:=[];
index:=0;
for j in [1..NumberOfRows(N)] do
poly:=0;
index:=index+1;
```

```
for k in [1..R_mLength] do
poly:=poly+N[j,k]*R_m[k];
end for;
FD[index]:=poly;
end for;
k:=#FD;
FD:=Vector(R,k,FD);
//We are now ready to compute the matrix G whose rows are the
//vectors ev_P(f) for f in FD. The linear span of these vectors
//is our code.
G:=ZeroMatrix(F_q,k,(q-1)^2);
for t in [1..k] do
for i in [0..(q-2)] do
for j in [0..(q-2)] do
G[t,(q-1)*i+j+1]:=Evaluate(FD[t],[g^i,g^j,1])/
Evaluate(z^m,[g^i,g^j,1]);
end for;
end for;
end for;
//Finally, we construct the code C^h(B,P,[D]), which is the
//linear subspace of F_q^n spanned by the rows of the matrix G.
C:=LinearCode(G);
return C;
end function;
```

B.4 Two-Line Code with $[D] = [mL - E_1 - \cdots - E_b]$ and $c = 3$

```
//Filename: ChBPD2L_file
//This program defines the function ChBPD2L(q,m,s,r) which returns
//the anticanonical surface code C=C^h(B,P,[D]) over F_q where:
//B={(0:0:1),(0:1:0),(1:0:0)} U {(0:1:1),...,(0:g^(s-1):1)} U
//{(1:0:1),...,(g^(r-1):0:1)},
//P is the standard set,
//[D]=[mL-E_1-...-E_b] and
//h=z^m.
////////////////////////////////////////////////////////////////////
ChBPD2L:=function(q,m,s,r)
//We define the finite field F_q and a primitive element g of F_q.
F_q:=GF(q);
g:=PrimitiveElement(F_q);
//We have the following equality for b since c=3.
b:=s+r+3;
//We define the points of B as a matrix, where each row contains the
//coordinates of a single point.
B:=ZeroMatrix(F_q,b,3);
B[1]:=Vector(F_q,3,[0,0,1]);
B[2]:=Vector(F_q,3,[0,1,0]);
B[3]:=Vector(F_q,3,[1,0,0]);
for i in [1..s] do
B[i+3]:=Vector(F_q,3,[0,g^(i-1),1]);
```

```
end for;
for j in [1..r] do
B[s+j+3]:=Vector(F_q,3,[g^(j-1),0,1]);
end for;
//We now define the polynomial ring R:=F_q[x,y,z].
R<x,y,z>:=PolynomialRing(F_q,3);
//Next we define the vector R_m of monomials in R of degree m.
//Note that these generate all the homogeneous polynomials
//in R of degree m.
R_m:=[];
index:=0;
for j in [0..m] do
for k in [0..(m-j)] do
index:=index+1;
R_m[index]:=x^j*y^k*z^(m-j-k);
end for;
end for;
R_mLength:=#R_m;
R_m:=Vector(R,R_mLength,R_m);
//We now define the matrix M whose entries are the values of the
//monomials in R_m at the points of B.
M:=ZeroMatrix(F_q,R_mLength,b);
for i in [1..R_mLength] do
for j in [1..b] do
M[i,j]:=Evaluate(R_m[i],[B[j,1],B[j,2],B[j,3]]);
end for;
end for;
//Next we find a basis for the nullspace of M.
//This gives us a basis for the functions in F([D]).
N:=NullspaceMatrix(M);
//Now we define the vector whose entries are a basis for the
//polynomials in F([D]).
FD:=[];
index:=0;
for j in [1..NumberOfRows(N)] do
poly:=0;
index:=index+1;
for k in [1..R_mLength] do
poly:=poly+N[j,k]*R_m[k];
end for;
FD[index]:=poly;
end for;
k:=#FD;
FD:=Vector(R,k,FD);
//We are now ready to compute the matrix G whose rows are the
//vectors ev_P(f) for f in FD. The linear span of these vectors
//is our code.
G:=ZeroMatrix(F_q,k,(q-1)^2);
for t in [1..k] do
for i in [0..(q-2)] do
for j in [0..(q-2)] do
G[t,(q-1)*i+j+1]:=Evaluate(FD[t],[g^i,g^j,1])/
```

```
Evaluate(z^m,[g^i,g^j,1]);
end for;
end for;
end for;
//Finally, we construct the code C^h(B,P,[D]), which is the
//linear subspace of F_q^n spanned by the rows of the matrix G.
C:=LinearCode(G);
return C;
end function;
```

B.5 One-Line Code on $\mathbb{P}^3_{\mathcal{B}}$ with $[D] = [mH - E_1 - \cdots - E_b]$ and $c = 2$

```
//Filename: ChBPD1LP3_file
//This program defines the function ChBPD1LP3(q,m,b) which returns
//the anticanonical surface code C=C^h(B,P,[D]) over F_q where:
//B={(0:0:1:0),(0:1:0:0)} U {(0:1:1:0),...,(0:g^(b-3):1:0)},
//P is the regular set in P^3,
//[D]=[mH-E_1-...-E_b] and
//h=x_3^m.
/////////////////////////////////////////////////////////////////////
ChBPD1LP3:=function(q,m,b)
//We define the finite field F_q and a primitive element g of F_q.
F_q:=GF(q);
g:=PrimitiveElement(F_q);
//We define the points of B as a matrix, where each row contains the
```

```
//coordinates of a single point.
if b eq 1 then
B:=Matrix(F_q,1,4,[1,0,0,0]);
else
B:=ZeroMatrix(F_q,b,4);
B[1]:=Vector(F_q,4,[0,0,1,0]);
B[2]:=Vector(F_q,4,[0,1,0,0]);
for i in [1..(b-2)] do
B[i+2]:=Vector(F_q,4,[0,g^(i-1),1,0]);
end for;
end if;
//We now define the polynomial ring R:=F_q[x_0,x_1,x_2,x_3].
R<x_0,x_1,x_2,x_3>:=PolynomialRing(F_q,4);
//Next we define the vector R_m of monomials in R of degree m.
//Note that these generate all the homogeneous polynomials
//in R of degree m.
R_m:=[];
index:=0;
for j in [0..m] do
for k in [0..(m-j)] do
for l in [0..(m-j-k)] do
index:=index+1;
//
R_m[index]:=x_0^j*x_1^k*x_2^l*x_3^(m-j-k-l);
end for;
end for;
end for;

R_mLength:=#R_m;

R_m:=Vector(R,R_mLength,R_m);

//We now define the matrix M whose entries are the values of the

//monomials in R_m at the points of B.

M:=ZeroMatrix(F_q,R_mLength,b);

for i in [1..R_mLength] do

for j in [1..b] do

M[i,j]:=Evaluate(R_m[i],[B[j,1],B[j,2],B[j,3],B[j,4]]);

end for;

end for;

//Next we find a basis for the nullspace of M.

//This gives us a basis for the functions in F([D]).

N:=NullspaceMatrix(M);

//Now we define the vector FD whose entries are a basis for the

//polynomials in F([D]).

FD:=[];

index:=0;

for j in [1..NumberOfRows(N)] do

poly:=0;

index:=index+1;

for k in [1..R_mLength] do

poly:=poly+N[j,k]*R_m[k];

end for;

FD[index]:=poly;

end for;
```

```
k:=#FD;

FD:=Vector(R,k,FD);

//We are now ready to compute the matrix G whose rows are the

//vectors ev_P(f) for f in FD. The linear span of these vectors

//is our code.

G:=ZeroMatrix(F_q,k,q^3);

//

for t in [1..k] do

for i in [0..(q-1)] do

for j in [0..(q-1)] do

for l in [0..(q-1)] do

G[t,q^2*i+q*j+l+1]:=Evaluate(FD[t],

[Ceiling(i/q)*g^i,Ceiling(j/q)*g^j,Ceiling(l/q)*g^l,1])/

Evaluate(x_3^m,[Ceiling(i/q)*g^i,Ceiling(j/q)*g^j,Ceiling(l/q)*g^l,1]);

end for;

end for;

end for;

end for;

//Finally, we construct the code C^h(B,P,[D]), which is the

//linear subspace of F_q^n spanned by the rows of the matrix G.

C:=LinearCode(G);

return C;

end function;
```

Bibliography

[1] Arnaud Beauville, *Complex algebraic surfaces*, London Mathematical Society Lecture Note Series, vol. 68, Cambridge University Press, Cambridge, 1983, Translated from the French by R. Barlow, N. I. Shepherd-Barron and M. Reid.

[2] Enrico Bombieri and Dale Husemoller, *Classification and embeddings of surfaces*, Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974), Amer. Math. Soc., Providence, R.I., 1975, pp. 329–420.

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[4] Lisa Byrne, *Polytopes, Toric Varieties, and Ideals*, preprint, http://www.mtholyoke.edu/ jsidman/byrnePaper.pdf.

[5] Giuliana Fatabbi, Brian Harbourne, and Anna Lorenzini, *Resolutions of ideals of fat points with support in a hyperplane*, Proc. Amer. Math. Soc. **134** (2006), no. 12, 3475–3483 (electronic).

[6] Simona Franceschini and Anna Lorenzini, *Fat points of $\mathbb{P}^n$ whose support is contained in a linear proper subspace*, J. Pure Appl. Algebra **160** (2001), no. 2-3, 169–182.

[7] William Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies, vol. 131, Princeton University Press, Princeton, NJ, 1993, , The William H. Roever Lectures in Geometry.

[8] V. D. Goppa, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR **259** (1981), no. 6, 1289–1290.

[9] Markus Grassl, *Code Tables: Bounds on the parameters of various types of codes*, http://www.codetables.de/.

[10] Johan P. Hansen, *Toric surfaces and error-correcting codes*, Coding theory, cryptography and related areas (Guanajuato, 1998), Springer, Berlin, 2000, pp. 132–142.

[11] ______, *Toric varieties Hirzebruch surfaces and error-correcting codes*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 4, 289–300.

[12] Brian Harbourne, *The geometry of rational surfaces and Hilbert functions of points in the plane*, Proceedings of the 1984 Vancouver conference in algebraic geometry (Providence, RI), CMS Conf. Proc., vol. 6, Amer. Math. Soc., 1986, pp. 95–111.

[13] ______, *Rational surfaces with $K^2 > 0$*, Proc. Amer. Math. Soc. **124** (1996), no. 3, 727–733.

[14] ______, *Anticanonical rational surfaces*, Trans. Amer. Math. Soc. **349** (1997), no. 3, 1191–1208.

[15] ______, *Free resolutions of fat point ideals on $\mathbf{P}^2$*, J. Pure Appl. Algebra **125** (1998), no. 1-3, 213–234.

[16] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fourth ed., Oxford, at the Clarendon Press, 1960.

[17] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[18] W. Cary Huffman and Vera Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[19] David Joyner, *Toric codes over finite fields*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 63–79.

[20] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

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

[22] John Little and Ryan Schwarz, *On m-dimensional toric codes*, preprint, arXiv:cs.IT/0506102.

[23] Gretchen L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Des. Codes Cryptogr. **22** (2001), no. 2, 107–121.

[24] Glenn Murray, *The Gaussian map for smooth toric surfaces*, Math. Z. **227** (1998), no. 2, 187–210.

[25] Masayoshi Nagata, *On rational surfaces I. Irreducible curves of arithmetic genus* 0 *or* 1, Mem. Coll. Sci. Univ. Kyoto Ser. A Math. **32** (1960), 351–370.

[26] Vera Pless, *Introduction to the theory of error-correcting codes*, third ed., Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication.

[27] Vera S. Pless, W. Cary Huffman, and Richard A. Brualdi, *An introduction to algebraic codes*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 3–139.

[28] Diego Ruano, *On the Parameters of r-dimensional Toric Codes*, preprint, arXiv:math.AG/0512285.

[29] I. R. Šafarevič, B. G. Averbuh, Ju. R. Vaĭnberg, A. B. Žižčenko, Ju. I. Manin, B. G. Moĭšezon, G. N. Tjurina, and A. N. Tjurin, *Algebraic surfaces*, Trudy Mat. Inst. Steklov. **75** (1965), 1–215.

[30] Henry K. Schenck, *Linear systems on a special rational surface*, Math. Res. Lett. **11** (2004), no. 5-6, 697–713.

[31] Jean-Pierre Serre, *Lettre à M. Tsfasman*, Astérisque (1991), no. 198-200, 11, 351–353 (1992), Journées Arithmétiques, 1989 (Luminy, 1989).

[32] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Mathematics and its Applications (Soviet Series), vol. 58, Kluwer Academic Publishers Group, Dordrecht, 1991, Translated from the Russian by the authors.

[33] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.

[34] Alexander Vardy, *The intractability of computing the minimum distance of a code*, IEEE Trans. Inform. Theory **43** (1997), no. 6, 1757–1766.

[35] Helena Verrill and David Joyner, *Notes on toric varieties*, preprint, arXiv:math.AG/0208065.

[36] José Felipe Voloch and Marcos Zarzar, *Algebraic Geometric Codes on Surfaces*, preprint, www.ma.utexas.edu/users/zarzar/papers.

[37] Judy L. Walker, *Codes and curves*, Student Mathematical Library, vol. 7, American Mathematical Society, Providence, RI, 2000, IAS/Park City Mathematical Subseries.