LINEAR CODES DEFINED FROM HIGHER-DIMENSIONAL VARIETIES

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Gary Lynn Salazar
B.S., Baylor University, 1994
August 2000

Acknowledgments

I attribute this accomplishment to the Lord who continues to grace us with uncountable blessings. I also want to thank those educators who have had a positive and valuable influence on me. In particular, an appreciation is expressed to Rose Volcik and Glover Laird for their willingness to sacrifice numerous hours and unceasing efforts to cultivate a skilled young scientist. Also, I am grateful to David Pennington for his instruction and encouragement in the field of chemistry. I wish to extend a special expression of gratitude to my advisor, Robert Lax, whose insight and advice have been indispensable.

I must also acknowledge my family which has remained a source of invaluable encouragement and inspiration. First, I want to thank my mom, Sheryl Salazar, who has always believed in me and has provided me with the confidence to pursue my dreams. I wish to extend thanks to my grandfathers, Cecil King and Juan Salazar, who have continually served as my role models. Also, I remain extensively appreciative of my fiancée, Jenny Potter, whose love and support helped me to withstand the difficulties I faced and inspired me to complete the task of obtaining a doctoral degree. Lastly, I wish to dedicate this dissertation to my late father, Manuel Salazar, who provided me with knowledge of the importance of family and social responsibility.

Table of Contents

Abstract

We establish an algebraic foundation to complement the improved geometric codes of Feng and Rao. Viewing linear codes as affine variety codes, we utilize the Feng-Rao minimum distance bound to construct codes with relatively large dimensions. We examine higher-dimensional affine hypersurfaces with properties similar to those of Hermitian curves. We determine a Gröbner basis for the ideal of the variety of rational points on certain affine Fermat varieties. This result is applied to determine parameters of codes defined from Fermat surfaces.

Introduction

Linear codes obtained by methods from algebraic geometry have gained significant notoriety since 1982, when Tsfasman, Vlăduţ, and Zink [10] determined the existence of a sequence of algebraic-geometric (or Goppa) codes that exceeded the Gilbert-Varshamov bound on the minimum distance. In 1995, G.-L. Feng and T.R.N. Rao [4] introduced the concept of improved geometric Goppa codes from plane curves. Absent of algebraic geometry, they were able to improve the current one-point Goppa codes from curves that have a single point at infinity.

The goal of this dissertation is to produce an algebraic foundation to complement these so-called "improved geometric codes." We shall also expand this notion to include affine varieties of arbitrary dimension.

In Chapter 1, we describe affine varieties and a formation of linear codes defined by them. We also develop and expand the fundamentals of improved geometric codes and the Feng-Rao bound on the minimum distance of a code. We conclude this chapter by examining codes from Type I curves, including Hermitian curves.

In Chapter 2, we review the theory of Gröbner bases and investigate its applications to higher-dimensional varieties. We determine a Gröbner basis for the ideal of the variety of rational points on certain affine Fermat varieties. This result is applied to determine parameters of codes defined from Fermat surfaces.

Generally, we will have restrictions on code length and minimum distance. We will require the Feng-Rao bound on the minimum distance to create codes with relatively large dimensions.

Chapter 1

The Feng-Rao Bound and Affine Variety Codes

1.1 Affine Variety Codes

Let $\mathbb{F}_q$ be the finite field with q elements. Let $S \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$. Let $\overline{\mathbb{F}}_q$ denote an algebraic closure of $\mathbb{F}_q$. The k-tuple $(a_1, \ldots, a_k) \in \overline{\mathbb{F}}_q^k$ is called a solution of S if $f(a_1, \ldots, a_k) = 0$ for all f in S. The affine variety in $\overline{\mathbb{F}}_q^k$ defined by S, denoted $V(S)$, is the set of all solutions of S. The elements $(a_1, \ldots, a_k)$ of $V(S)$ are known as the points of $V(S)$. Further, if each coordinate of a point of $V(S)$ lies in $\mathbb{F}_q$, then the point is called an $\mathbb{F}_q$-rational point of $V(S)$. Note that if I is the ideal of $\mathbb{F}_q[x_1, \ldots, x_k]$ generated by the set S, then $V(I) = V(S)$.

Definition 1.1. For I an ideal of $\mathbb{F}_q[x_1, \ldots, x_k]$, define

$$I_q := I + (x_1^q - x_1, \ldots, x_k^q - x_k).$$

Remark 1.2. The points of $V(I_q)$ are precisely the $\mathbb{F}_q$-rational points of $V(I)$.

Since the polynomials $x_i^q - x_i \in I_q$ for each i such that $1 \leq i \leq k$, we have that I_q is a zero-dimensional ideal. Moreover, by Seidenberg's Lemma 92 [9], I_q is in fact a radical ideal.

The ring $R = \mathbb{F}_q[x_1, \ldots, x_k]/I_q$ is called the coordinate ring of the variety $V(I_q)$. The elements of R are designated by $\bar{f}$, where $\bar{f}$ represents the equivalence class $f + I_q$, for each polynomial f. Let $\mathbb{A}^n = \mathbb{F}_q^n$ be affine n-space over $\mathbb{F}_q$, where n is the number of points of the affine variety $V(I_q)$. After ordering the points $P_1, \ldots, P_n$ of $V(I_q)$, define an evaluation map $\phi : R \mapsto \mathbb{A}^n$ by $\phi(\bar{f}) = (f(P_1), \ldots, f(P_n))$, where $\bar{f} = f + I_q$. The mapping ϕ is easily seen to be an isomorphism of $\mathbb{F}_q$-vector spaces.

Definition 1.3. A linear code of length n over $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$.

Let I be an ideal of $\mathbb{F}_q[x_1, \ldots, x_k]$ and $P_1, \ldots, P_n$ be all the points of $V(I_q)$. Let L be an $\mathbb{F}_q$-vector subspace of the coordinate ring R.

Definition 1.4. The affine variety codes, $C(I, L)$ and $C^{\perp}(I, L)$, are defined as follows:

$$C(I, L) = \phi(L)$$

$$C^{\perp}(I, L) = \phi(L)^{\perp}$$

where $\phi(L)$ is the image of L under the evaluation map ϕ, and $\phi(L)^{\perp}$ is the orthogonal complement of $\phi(L)$ with respect to the usual inner product on $\mathbb{A}^n$.

Remark 1.5. (i) Every $\mathbb{F}_q$-linear code can be represented as an affine variety code.

(ii) A different ordering of the points would yield an equivalent code, so a linear code with the same length, dimension, and minimum distance.

We define a weighted-degree lexicographic ordering on the (monic) monomials of $\mathbb{F}_q[x_1, \ldots, x_k]$. For each of the variables x_j, where $1 \leq j \leq k$, we can assign a positive integer, $wt(x_j)$. The weight of a monomial, $x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k}$, is defined as

$$wt(x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k}) = \sum_{j=1}^{k} i_j wt(x_j).$$

To define the total ordering $<_t$ on the monomials, apply the rule:

$$x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k} <_t x_1^{j_1} x_2^{j_2} \ldots x_k^{j_k} \text{ if}$$

(i) $wt(x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k}) < wt(x_1^{j_1} x_2^{j_2} \ldots x_k^{j_k})$ or

(ii) $wt(x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k}) = wt(x_1^{j_1} x_2^{j_2} \ldots x_k^{j_k})$ and there exists an l such that $i_m = j_m$ for $1 \leq m \leq l-1$ and $i_l < j_l$.

With this ordering we can further describe the elements of the coordinate ring R of the variety $V(I_q)$. Let T^k denote the set of (monic) monomials of $\mathbb{F}_q[x_1, \ldots, x_k]$, i.e. $T^k = \{x_1^{\alpha_1} \ldots x_k^{\alpha_k} | \alpha_i \in \mathbb{N} \text{ for } 1 \leq i \leq k\}$. To simplify notation, we will sometimes write x^{α} for $x_1^{\alpha_1} \ldots x_k^{\alpha_k}$ where $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{N}^k$. For every nonzero polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_k]$, we can express f as $f = c_1 x^{\beta_1} + c_2 x^{\beta_2} + \cdots + c_s x^{\beta_s}$ with $0 \neq c_i \in \mathbb{F}_q, x^{\beta_i} \in T^k$ and $x^{\beta_s} <_t \cdots <_t x^{\beta_2} <_t x^{\beta_1}$. Define the leading monomial of f, denoted $lm(f)$, by $lm(f) = x^{\beta_1}$. Also, define the leading term of f, denoted $lt(f)$, by $lt(f) = c_1 x^{\beta_1}$.

Definition 1.6. The *footprint* or Δ-*set* of an ideal $I \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$ is defined by $\Delta(I) := T^k \setminus \{lm(f) | f \in I, f \neq 0\}$.

Example 1.7. Let I be the principal ideal in $\mathbb{F}_4[x_1, x_2]$ generated by the polynomial $x_1^3 + x_2^2 + x_2$. This is known as the (affine) Hermitian curve over $\mathbb{F}_4$. Note that $I_q = \langle x_1^3 + x_2^2 + x_2, x_1^4 - x_1, x_2^4 - x_2 \rangle$. Let $wt(x_1) = 2$ and $wt(x_2) = 3$. An explanation of the motivation to choose these integers will follow later. Then we have $\Delta(I_q) = \{1, x_1, x_1^2, x_2, x_1x_2, x_1^2x_2, x_2^2, x_2^3\}$.

Definition 1.8. For an ideal $I \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$, we define the *H-sequence* as $H := \{h_i\}_{i=1}^{n'}$ the increasing sequence (under the ordering $<_t$) of the elements of $\Delta(I_q)$. With a slight abuse of notation, we will indicate that the monomial h_i appears in the H-sequence by the notation $h_i \in H$.

Remark 1.9. For $h_i \in H$, we claim that if a monomial m divides h_i, then $m \in H$. For if not, $m \notin H$ implies there exists a polynomial $f \in I_q$ such that $lm(f) = m$. Therefore, $(\frac{h_i}{m})f \in I_q$ and $lm((\frac{h_i}{m})f) = (\frac{h_i}{m})m = h_i$. Thus, $h_i \notin H$, which is a contradiction.

In Example 1.7, $H = \{1, x_1, x_2, x_1^2, x_1x_2, x_2^2, x_1^2x_2, x_2^3\}$. Note that the corresponding weights of each of the eight monomials are distinct.

Proposition 1.10. *The elements of the set* $\{\bar{h}_1, \ldots, \bar{h}_{n'}\}$ *form a basis for the coordinate ring* R. *Therefore,* $\dim \mathbb{F}_q[x_1, \ldots, x_k]/I_q = |\Delta(I_q)| = n$.

Proof. Since R is spanned by the set of equivalence classes of monomials that are not the leading monomial of any polynomial in I_q, it suffices to show that $\{\bar{h}_1, \ldots, \bar{h}_{n'}\}$ is a linearly independent set of elements of R. Suppose there exists $c_1, c_2, \ldots, c_{n'} \in \mathbb{F}_q$ not all zero such that $c_1\bar{h}_1 + c_2\bar{h}_2 + \cdots + c_{n'}\bar{h}_{n'} = \bar{0}$. Therefore, $f = c_1h_1 + c_2h_2 + \cdots + c_{n'}h_{n'} \in I_q$. Then $lm(f) = h_i$ for some i. However, $h_i \in \Delta(I_q)$ implies that $f \notin I_q$, which is a contradiction. It follows that $n = n'$. □

1.2 Improved Geometric Codes

We will next present several definitions that were first given by G.-L. Feng and T. R. N. Rao. [4]

Definition 1.11. Let $L(\underline{r})$ be the the linear subspace of R generated by the set $\{\bar{h}_1, \ldots, \bar{h}_r\}$. More generally, let $L(\underline{r}, v_1, \ldots, v_l)$ denote the subspace generated by $\{\bar{h}_1, \ldots, \bar{h}_r, \bar{h}_{v_1}, \ldots, \bar{h}_{v_l}\}$ where $r + 1 < v_1 < \cdots < v_l$ for some $l \geq 0$. Note that if $l = 0$ then $L(\underline{r}, v_1, \ldots, v_l) = L(\underline{r})$.

Definition 1.12. If $h_i = x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}$ and $h_j = x_1^{j_1}x_2^{j_2}\ldots x_k^{j_k}$ then put $h_{i,j} := x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_k^{\alpha_k}$ where for $l = 1, \ldots, k$,

$$\alpha_l = \begin{cases} i_l + j_l & \text{if } i_l + j_l < q \\ i_l + j_l - (q-1) & \text{otherwise.} \end{cases}$$

By this construction, $h_{i,j} \leq_t h_ih_j$. However, $h_{i,j}$ and h_ih_j are equal as functions; i.e. when viewed as mappings from $\mathbb{F}_q^k$ into $\mathbb{F}_q$, $h_{i,j}$ and h_ih_j are identical.

Definition 1.13. Let $h_r \in H$. A monomial h is said to be *consistent with* h_r if $\bar{h} \in L(\underline{r}) \setminus L(\underline{r-1})$ and $wt(h) = wt(h_r)$. If h is consistent with h_r, then we write $h \sim h_r$.

Lemma 1.14. *If $h <_t h_r$, then $\bar{h} \in L(\underline{r-1})$.*

Proof. Suppose $h <_t h_r$ and $\bar{h} \in L(\underline{s})$ for some $s \geq r$. Then $h + I_q = \sum_{i=1}^{s}(k_i h_i) + I_q$ for some $k_i \in \mathbb{F}_q$ for $1 \leq i \leq s$ with $k_s \neq 0$. Thus, $f = \sum_{i=1}^{s}(k_i h_i) - h \in I_q$ and $lm(f) = h_s$ since $k_s \neq 0$ and $h <_t h_r \leq_t h_s$. This is a contradiction since the monomial $h_s \in \Delta(I_q)$. □

Corollary 1.15. *If $h \sim h_r$, then $h_r \leq_t h$.*

Lemma 1.16. *If $\bar{h}_{i,j} \in L(\underline{r}) \setminus L(\underline{r-1})$ and $wt(h_i) + wt(h_j) = wt(h_r)$, then $h_i h_j = h_{i,j} \sim h_r$.*

Proof. In order to show that $h_{i,j} \sim h_r$, we only need to show that $wt(h_{i,j}) = wt(h_r)$. If $h_i h_j = h_{i,j}$ then the conclusion is satisfied. Assume $h_i h_j \neq h_{i,j}$. Then we have $wt(h_{i,j}) < wt(h_i) + wt(h_j) = wt(h_r)$. Hence, $h_{i,j} <_t h_r$. By Lemma 1.14, we have $\bar{h}_{i,j} \in L(\underline{r-1})$, which is a contradiction. □

Definition 1.17. Let $h_i, h_j \in H$ such that $wt(h_i) + wt(h_j) \leq wt(h_n)$ and $h_{i,j} \sim h_r$. If for each pair (u, v) such that $1 \leq u \leq i$, $1 \leq v \leq j$ and $(u, v) \neq (i, j)$ we have $\bar{h}_{u,v} \in L(\underline{r-1})$, then $h_{i,j}$ is called a *well-behaving term* (consistent with h_r).

Lemma 1.18. *Let h_i, h_j, and $h_r \in H$. If $h_i h_j = h_r$ then $h_{i,j}$ is a well-behaving term consistent with h_r.*

Proof. Suppose $h_i, h_j, h_r \in H$ such that $h_i h_j = h_r$. Then $h_r = h_i h_j = h_{i,j}$. Clearly, $h_{i,j} \sim h_r$. Let (u, v) be such that $1 \leq u \leq i$, $1 \leq v \leq j$ and $(u, v) \neq (i, j)$. Then $h_{u,v} \leq_t h_u h_v <_t h_i h_j = h_r$. Hence, $\bar{h}_{u,v} \in L(\underline{r-1})$. □

In Example 1.7, note that $h_{4,4} = x_1 = h_2$ although $h_4 h_4 = x_1^4$. Thus, $h_{4,4}$ is consistent with h_2. However, $h_{4,4}$ is not a well-behaving term since $\bar{h}_{1,2} \in L(\underline{2})$. On the other hand, since $x_1^3 + x_2^2 + x_2 \in I_q$, we have $h_{2,4} = x_1^3 \sim x_2^2 = h_6$. Therefore, $h_{2,4} \sim h_6$. Upon further inspection, $h_{2,4}$ is in fact a well-behaving term.

Definition 1.19. Define $\mathcal{N}_r := \{(i,j)|h_{i,j}$ is a well-behaving term consistent with $h_r\}$. Put $N_r := |\mathcal{N}_r|$.

In Example 1.7 $N_1 = 1, N_2 = 2, N_3 = 2, N_4 = 3, N_5 = 4, N_6 = 5, N_7 = 6, N_8 = 8$. Since $x_1^3 + x_2^2 + x_2 \in I_q$, we have $x_1^3 \sim x_2^2$ and $x_1^3 x_2 \sim x_2^3$. Hence, the monomials $h_{2,4}$ and $h_{4,2}$ as well as $h_{1,6}, h_{3,3}$, and $h_{6,1}$ are all consistent with h_6. Upon further inspection, they are all well-behaving terms also. Hence, $N_6 = 5$. Also, the monomials $h_{2,7}, h_{4,5}, h_{5,4}$, and $h_{7,2}$ as well as $h_{1,8}, h_{3,6}, h_{6,3}$, and $h_{8,1}$ are all consistent with h_8. Upon further inspection, they are all well-behaving terms also. Hence, $N_8 = 8$.

Lemma 1.20. *For $1 \leq r \leq n$, $\mathcal{N}_r$ is uniquely expressible as*

$$\mathcal{N}_r = \{(i_1, j_1), \ldots, (i_{N_r}, j_{N_r})\}$$

where $i_1 = j_{N_r} < i_2 = j_{N_r - 1} < \cdots < i_{N_r} = j_1$.

Proof. Let (i_α, j_α) and (i_β, j_β) be distinct elements of $\mathcal{N}_r$, where without loss of generality, we may assume $i_\alpha \leq i_\beta$. Assume $j_\alpha \leq j_\beta$. Then $i_\alpha \leq i_\beta$ and $j_\alpha \leq j_\beta$ with $(i_\alpha, j_\alpha) \neq (i_\beta, j_\beta)$ along with $h_{i_\alpha, j_\alpha} \sim h_r$ imply that h_{i_β, j_β} is not a well-behaving term. This is a contradiction. Thus, $j_\beta < j_\alpha$. Suppose $i_\alpha = i_\beta$, then $j_\beta < j_\alpha$ and $h_{i_\beta, j_\beta} \sim h_r$ imply h_{i_α, j_α} is not a well-behaving term. This is also a contradiction. Thus, for $1 \leq l \leq N_r$, each i_l is distinct. Also, since $h_{i,j} = h_{j,i}$ then $(i,j) \in \mathcal{N}_r$ implies that $(j,i) \in \mathcal{N}_r$. $\square$

Proposition 1.21. *For $h_r = x_1^{r_1} \ldots x_n^{r_n} \in H$, $N_r \geq \prod_{i=1}^n (r_i + 1)$.*

Proof. For each divisor d of h_r, we have $d \in H$ and $\frac{h_r}{d} \in H$ by Remark 1.9. There are $\prod_{i=1}^n (r_i + 1)$ such divisors. Thus each divisor yields a distinct pair (i,j) such that $h_i h_j = h_r$. By Lemma 1.18, each such $h_{i,j}$ is a well-behaving term consistent with h_r. $\square$

It is easy to see that N_r can be strictly greater than just the number of monomial divisors of h_r. Consider $h_6 = x_2^2$ from Example 1.7. The number of divisors of x_2^2 is 3 and $N_6 = 5$.

Definition 1.22. Let H_r denote the $r \times n$ matrix defined by $H_r := [h_i(P_j)]$, where $1 \leq i \leq r$ and $1 \leq j \leq n$. Note that H_r is a parity check matrix for the affine variety code $C^{\perp}(I, L(\underline{r}))$.

Definition 1.23. Consider the code $C^{\perp}(I, L)$ where $L = L(\underline{r}, v_1, \ldots, v_l)$. Define

$$H_r^* := \begin{pmatrix} & H_r & \\ h_{v_1}(P_1) & \cdots & h_{v_1}(P_n) \\ \vdots & \vdots & \vdots \\ h_{v_l}(P_1) & \cdots & h_{v_l}(P_n) \end{pmatrix}.$$

Note that H_r^* is a parity check matrix for $C^{\perp}(I, L)$ and if $l = 0$, then $H_r^* = H_r$.

We will now discuss the minimum distance of the codes with parity check matrix H_r^*. Let $h_i' := (h_i(P_1), \ldots, h_i(P_n))$ and $h_{i,j}' := (h_{i,j}(P_1), \ldots, h_{i,j}(P_n))$. For each $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, $1 \leq i \leq n$, and $1 \leq j \leq n$ define the following syndromes: $s_i(c) := h_i' c^T$ and $S_{i,j}(c) := h_{i,j}' c^T$. Note that if c is a codeword, then $s_i(c) = 0$ for $i = 1, 2, \ldots, r, v_1, v_2, \ldots, v_l$, and that $S_{i,j}(c) = 0$ if $\bar{h}_{i,j} \in L(\underline{r}, v_1, \ldots, v_l)$. Let $\mathcal{S}_c := [S_{i,j}(c)]$ be the $n \times n$ matrix of syndromes. Since $h_{i,j}$ and $h_i h_j$ are equal as functions, then $\mathcal{S}_c = H_n D(c) H_n^T$ where $D(c)$ is the diagonal $n \times n$ matrix with c on the diagonal,

$$D(c) = \begin{pmatrix} c_1 & 0 & \ldots & 0 \\ 0 & c_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & c_n \end{pmatrix}.$$

The square matrix H_n must have full rank. For if there existed $k_1, \ldots, k_r \in \mathbb{F}_q$ such that $\sum_{i=1}^{n}(k_i h'_i) = (0, \ldots, 0)$, then the function $f = \sum_{i=1}^{n}(k_i h_i)$ must vanish at each of the points $P_1, \ldots, P_n$. Hence, $f \in I(V(I_q)) = I_q$ since I_q is radical. However, $lm(f) \in H$ implies that $lm(f) \in \Delta(I_q)$, which is a contradiction. Since H_n and H_n^T both have full rank, then we have rank $\mathcal{S}_c =$ rank $D(c) = wt(c)$.

Proposition 1.24. *Suppose $c = (c_1, \ldots, c_n)$ is a codeword of the code with parity check matrix H_r^*. If $s_{r+1}(c) \neq 0$, then $wt(c) \geq N_{r+1}$.*

Proof. Since c is a codeword, then $s_i(c) = 0$ for $1 \leq i \leq r$. For each of the N_{r+1}-many $h_{i,j}$ which are well-behaving terms consistent with h_{r+1}, we have $S_{i,j}(c) \neq 0$. This follows since each $\bar{h}_{i,j} \in L(\underline{r+1}) \setminus L(\underline{r})$ implies $h_{i,j} + I_q = \sum_{i=1}^{r+1}(k_i h_i) + I_q$ for some $k_i \in \mathbb{F}_q$, $1 \leq i \leq r+1$ with $k_{r+1} \neq 0$. Thus, there exists a polynomial $f \in I_q$ such that $h_{i,j} = \sum_{i=1}^{r+1}(k_i h_i) + f$. Then,

$$h'_{i,j} = \sum_{i=1}^{r+1}(k_i h'_i) + (f(P_1), \ldots, f(P_n)).$$

Since $f \in I_q$, we have

$$S_{i,j}(c) = \sum_{i=1}^{r+1}(k_i h'_i c^T) + (0, \ldots, 0)c^T = \sum_{i=1}^{r+1}(k_i s_i(c)) = k_{r+1} s_{r+1}(c)$$

since $s_i(c) = 0$ for $1 \leq i \leq r$. Since $k_{r+1} \neq 0$ and $s_{r+1}(c) \neq 0$, we have $S_{i,j}(c) \neq 0$. However, $h_{i,j}$ a well-behaving term implies that for each pair (u, v) such that $1 \leq u \leq i$, $1 \leq v \leq j$ and $(u, v) \neq (i, j)$ we have $\bar{h}_{u,v} \in L(\underline{r})$. Thus $S_{u,v}(c) = 0$. Let $\mathcal{N}_{r+1} = \{(i_1, j_1), \ldots, (i_{N_{r+1}}, j_{N_{r+1}})\}$ where $i_1 = j_{N_{r+1}} < i_2 = j_{N_r} < \cdots < i_{N_{r+1}} = j_1$ as denoted in Lemma 1.20. For $1 \leq l \leq N_{r+1}$, the j_l-th row of the matrix $\mathcal{S}_c$ has zeros in the first $i_l - 1$ entries and the i_lth entry, namely $S_{i_l, j_l}(c)$, is nonzero. Since $i_1 < i_2 < \cdots < i_{N_{r+1}}$, then the set of rows $\{h'_{j_1}, \ldots, h'_{j_{N_{r+1}}}\}$ are linearly independent. Hence, rank $\mathcal{S}_c = wt(c) \geq N_{r+1}$. □

Theorem 1.25. *Suppose H_r^* is a parity check matrix of a nontrivial linear code. Let $\delta' := \min\{N_v | v \notin \{1, \ldots, r, v_1, \ldots, v_l\}\}$, then the code has minimum distance at least δ'. In this case, δ' is called the Feng-Rao bound for the minimum distance.*

Proof. Let c be a nonzero codeword. Let p be the smallest index such that $s_u(c) = 0$ for $1 \leq u \leq p$ and $s_{p+1}(c) \neq 0$. Let's show the existence of such a $p < n$. Assume $s_u(c) = 0$ for $1 \leq u \leq n$. Then $h'_u c^T = 0$ for $1 \leq u \leq n$. Therefore, $c \in C^{\perp}(I, L(\underline{n}))$. However, $C^{\perp}(I, L(\underline{n}))$ has dimension 0. Thus, $c = (0, \ldots, 0)$. This is a contradiction. Note that $p + 1 \notin \{1, \ldots, r, v_1, \ldots, v_l\}$ since c is a codeword. However, c is also a codeword for $C^{\perp}(I, L(\underline{p}))$. By Proposition 1.24, we know that $wt(c) \geq N_{p+1} \geq \delta'$. □

Suppose you desire a code of length n to have a designed minimum distance of δ. Simply construct an affine variety code $C^{\perp}(I, L)$ where $V(I_q)$ has n points and L is the linear subspace of the coordinate ring R spanned by $\{\bar{h}_i | h_i \in H, N_i < \delta\}$. Then L can be expressed in the form $L(\underline{r}, v_1, \ldots, v_l)$ where

(i) for $1 \leq v \leq r,$ we have $N_v < \delta$;

(ii) $N_{r+1} \geq \delta$;

(iii) for $r + 1 < v \leq n,$ if $N_v < \delta$ then $v \in \{v_1, \ldots, v_l\}$.

For the case when I defines a plane curve that has one point at infinity, these codes are the so-called "improved" geometric Goppa codes of Feng and Rao [4]. They are constructed by starting with the usual geometric Goppa code where $L = L(1, 2, \ldots, v_l)$ which has the same minimum distance bound δ. The above construction deletes certain generators of $L(1, 2, \ldots, v_l)$ while maintaining the same minimum distance bound. When generators are deleted, the dimension of L is decreased, which in turn increases the dimension of the code $C^{\perp}(I, L)$, thereby forming an "improved" code. Note that δ' as defined in Theorem 1.25 is also a lower bound on the minimum distance of the constructed code. Note that $\delta \leq \delta'$. Therefore, in order to obtain a tighter lower bound, we may assume $\delta = N_v$ for some v.

Thus, the minimum distance of the code $C^{\perp}(I, L)$, where $L = L(\underline{r}, v_1, \ldots, v_l)$, is bounded below by some N_v. Recall, N_v depends on the number of $h_{i,j} \sim h_v$ (i.e., $wt(h_{i,j}) = wt(h_v)$ and $\bar{h}_{i,j} \in L(\underline{v}) \setminus L(\underline{v-1})$). Hence, in order to increase the bound on the minimum distance, we must increase the number of such $h_{i,j}$. To accomplish this it is beneficial to assign the weights of each of the variables such that each generator polynomial of I has at least two monomials of equal weight. In Example 1.7, by assigning $wt(x_1) = 2$ and $wt(x_2) = 3$, we obtain $wt(x_1^3) = wt(x_2^2)$ for the lone generator polynomial $x_1^3 + x_2^2 + x_2$.

Definition 1.26. Define $\mathcal{P}_r := \{(i,j) | wt(h_i) + wt(h_j) = wt(h_r)\}$.

Theorem 1.27. *Let $V(I_q)$ be an affine variety, where I is an ideal in $\mathbb{F}_q[x_1, \ldots, x_n]$. Let H be the monomial sequence obtained from $\Delta(I_q)$. Then $\mathcal{N}_r \subseteq \mathcal{P}_r$.*

Proof. Let $(i,j) \in \mathcal{N}_r$. Suppose $h_i = x_1^{i_1} \ldots x_n^{i_n}$ and $h_j = x_1^{j_1} \ldots x_n^{j_n} \in H$. We know $i_l \leq q-1$ and $j_l \leq q-1$ for $1 \leq l \leq n$. Consider the monomials $h_u = x_1^{u_1} \ldots x_n^{u_n}$ and $h_v = x_1^{v_1} \ldots x_n^{v_n}$ where for $1 \leq l \leq n$:

$$u_l = \begin{cases} i_l + j_l - (q-1) & \text{if } i_l + j_l \geq q \\ i_l & \text{otherwise} \end{cases}$$

and

$$v_l = \begin{cases} 0 & \text{if } i_l + j_l \geq q \\ j_l & \text{otherwise.} \end{cases}$$

Note that $u_l \leq i_l$ and $v_l \leq j_l$ for $1 \leq l \leq n$. Therefore, h_i is a multiple of h_u and h_j is a multiple of h_v. Thus $h_u, h_v \in H$. Assume there exists an l such that $i_l + j_l \geq q$.

Then, $h_u \leq_t h_i$ and $h_v <_t h_j$. This implies that $u \leq i$, $v < j$ and $(u,v) \neq (i,j)$. However, by construction $h_{u,v} = h_{i,j} \sim h_r$, so that $\bar{h}_{u,v} \in L(\underline{r}) \setminus L(\underline{r-1})$. Thus, $h_{i,j}$ is not a well-behaving term, which is a contradiction. Therefore, $i_l + j_l < q$ for $1 \leq l \leq n$, and so $h_i h_j = h_{i,j}$. Hence $wt(h_i) + wt(h_j) = wt(h_{i,j}) = wt(h_r)$, since $h_{i,j} \sim h_r$, which implies that $(i,j) \in \mathcal{P}_r$. □

Therefore a necessary condition for $h_{i,j}$ to be a well-behaving term consistent with h_r is that it must satisfy: $wt(h_i) + wt(h_j) = wt(h_r)$.

Corollary 1.28. *If $(i,j) \in \mathcal{N}_r$, then $h_{i,j} = h_i h_j$.*

Example 1.29. Let I be the principal ideal in $\mathbb{F}_8[x_1, x_2]$ generated by the polynomial $x_1^3 + x_1 x_2^3 + x_2$. This is known as the affine Klein quartic curve over $\mathbb{F}_8$. The variety $V(I_q)$ contains 22 points. Let $wt(x_1) = 3$ and $wt(x_2) = 2$. Then we have

$$\Delta(I_q) = \{x_1^\alpha x_2^\beta | 0 \leq \alpha \leq 2, 0 \leq \beta \leq 7, \text{ and if } \alpha > 0, \text{then } \beta < 7\}.$$

Thus, the H-sequence is

$$\{1, x_2, x_1, x_2^2, x_1 x_2, x_2^3, x_1^2, x_1 x_2^2, \ldots, x_1^2 x_2^6\}.$$

Note that

$$\mathcal{P}_6 = \mathcal{P}_7 = \{(1,7), (1,6), (2,4), (3,3), (4,2), (6,1), (7,1)\}.$$

However, $\mathcal{N}_6 = \{(1,6), (2,4), (4,2), (6,1)\}$ and $\mathcal{N}_7 = \{(1,7), (3,3), (7,1)\}$. Hence, $\mathcal{N}_6 \neq \mathcal{P}_6$ and $\mathcal{N}_7 \neq \mathcal{P}_7$.

Whenever $wt(h_i) = wt(h_j)$, we have $\mathcal{P}_i = \mathcal{P}_j$. However, since $\mathcal{N}_i$ and $\mathcal{N}_j$ are disjoint, we know that $\mathcal{N}_i \neq \mathcal{P}_i$ and/or $\mathcal{N}_j \neq \mathcal{P}_j$. In the next section we will discuss a class of codes in which $\mathcal{N}_r = \mathcal{P}_r$ for each r.

Remark 1.30. Kirfel and Pellikaan [7] defined a minimum distance bound which they originally called the Feng-Rao bound, but which was later renamed the order bound [5]. This bound is related to the sets $\mathcal{P}_r$ defined above. The Feng-Rao bound is tighter than the order bound to the true minimum distance. However, for Type I curves, it follows from Theorem 1.35 that these bounds are identical.

1.3 Type I Curves

Definition 1.31. If $wt(h_i) < wt(h_{i+1})$ for $1 \leq i \leq n-1$, then the H-sequence is said to *contain distinct weights.*

Lemma 1.32. *If the H-sequence contains distinct weights, then*

$$\mathcal{N}_r = \{(i,j) | h_{i,j} \sim h_r\}.$$

Proof. We need to show that if $h_{i,j} \sim h_r$ then $h_{i,j}$ is a well-behaving term. For any $u \leq i$ and $v \leq j$ with $(u,v) \neq (i,j)$, we have that

$$wt(h_{u,v}) \leq wt(h_u) + wt(h_v) < wt(h_i) + wt(h_j) = wt(h_r).$$

Hence, $\bar{h}_{u,v} \in L(\underline{r-1})$. □

Definition 1.33. The affine plane curves over $\mathbb{F}_q$ defined by the principal ideal $I = \langle x_1^a + x_2^b + f(x_1,x_2)\rangle \subseteq \mathbb{F}_q[x_1,x_2]$ where $\gcd(a,b) = 1$ and $\deg f < \min\{a,b\}$ are the so-called *Type I curves* of Feng and Rao. We may assume that $a < q$ and $b < q$.

Given a Type I curve, we set $wt(x_1) = b$ and $wt(x_2) = a$ so that $wt(x_1^a) = wt(x_2^b)$. Let $H = \{h_i\}_{i=1}^n$ be the corresponding sequence of the elements of $\Delta(I_q)$.

Proposition 1.34. *For Type I curves, H contains distinct weights.*

Proof. Since $x_1^a + x_2^b + f(x_1,x_2) \in I_q$, its leading monomial, $x_1^a \notin \Delta(I_q)$. Thus, any multiple of x_1^a is not in $\Delta(I_q)$. Suppose there exists two monomials of H, $h_i = x_1^{i_1}x_2^{i_2}$ and $h_j = x_1^{j_1}x_2^{j_2}$ where $i_1 < a$ and $j_1 < a$ such that $wt(h_i) = wt(h_j)$. Then $i_1 b + i_2 a = wt(h_i) = wt(h_j) = j_1 b + j_2 a$ implies that $a(i_2 - j_2) = b(j_1 - i_1)$.

However, $|j_1 - i_1| < a$ and $\gcd(a, b) = 1$ imply that $i_1 = j_1$ and $i_2 = j_2$. Thus, $h_i = h_j$. Hence, H contains distinct weights. □

Theorem 1.35. *For Type I curves, $\mathcal{P}_r = \mathcal{N}_r$ for $1 \leq r \leq n$.*

Proof. By Lemma 1.32 and Proposition 1.34, we know that $\mathcal{N}_r = \{(i, j) | h_{i,j} \sim h_r\}$. By Theorem 1.27, it suffices to show that $(i, j) \in \mathcal{P}_r$ implies that $h_{i,j} \sim h_r$. Suppose $h_i = x_1^{i_1} x_2^{i_2}$, $h_j = x_1^{j_1} x_2^{j_2}$, and $h_r = x_1^{r_1} x_2^{r_2}$ are members of H such that $wt(h_i) + wt(h_j) = wt(h_r)$. Since i_1, j_1, and r_1 are each less than a, then either $h_r = h_i h_j$ or $h_r = h_i h_j x_1^{-a} x_2^{b} = x_1^{i_1+j_1-a} x_2^{i_2+j_2+b}$. If $h_r = h_i h_j$, then by Lemma 1.18, the conclusion is satisfied. We may assume that $h_r \neq h_i h_j$. Then, $i_1 + j_1 = r_1 + a$ and $i_2 + j_2 + b = r_2$. Therefore,

$$h_i h_j = x_1^{r_1+a} x_2^{r_2-b} = x_1^{r_1} x_2^{r_2-b}(g - x_2^b - f) = x_1^{r_1} x_2^{r_2-b} g - h_r - x_1^{r_1} x_2^{r_2-b} f$$

where $g = x_1^a + x_2^b + f(x_1, x_2)$, the defining polynomial for the ideal I. Now, $x_1^{r_1} x_2^{r_2-b} g \in I_q$ and $wt(h_r) > wt(x_1^{r_1} x_2^{r_2-b} lm(f))$. Therefore, $\bar{h}_i \bar{h}_j \in L(\underline{r}) \setminus L(\underline{r-1})$. To apply Lemma 1.16, we want $\bar{h}_{i,j} \in L(\underline{r}) \setminus L(\underline{r-1})$. Assume that $h_{i,j} \neq h_i h_j$. Since $r_2 - b < q$, we have $r_1 + a \geq q$. Thus, $h_i h_j - h_{i,j} = p(x_1, x_2)(x_1^q - x_1)$ for some polynomial $p(x_1, x_2)$. Since $x_1^q - x_1 \in I_q$, we have $\bar{h}_{i,j} = \bar{h}_i \bar{h}_j$. Hence, $\bar{h}_{i,j} \in L(\underline{r}) \setminus L(\underline{r-1})$ and by Lemma 1.16, $h_{i,j} \sim h_r$. □.

Definition 1.36. A special class of Type I curves are the *Hermitian curves.* They are curves in which $I = \langle x_1^q + x_2^{q+1} + x_1 \rangle \subseteq \mathbb{F}_{q^2}[x_1, x_2]$. The variety $V(I_{q^2})$ has q^3 rational points.

Remark 1.37. In Definition 1.36, we could have also included ideals of the form $I^* = \langle x_2^q + x_1^{q+1} + x_2 \rangle$. Their footprints, $\Delta(I_{q^2})$ and $\Delta(I^*_{q^2})$ are not equal. However, for their respective monomial sequences, $H = \{h_i\}_{i=1}^{q^3}$ and $H^* = \{h_i^*\}_{i=1}^{q^3}$, we do have the property that $wt(h_i) = wt(h_i^*)$ for $1 \leq i \leq n = q^3$. Since $\mathcal{P}_r = \mathcal{N}_r$

for $1 \leq r \leq n$, the codes $C^{\perp}(I, L)$ and $C^{\perp}(I^*, L)$ where $L = L(\underline{r}, v_1, \ldots, v_l)$ have the exact same minimum distance bound. Since the length, dimension, and minimum distance bounds are equal, we can simply examine the case as stated in the definition.

For Hermitian curves,

$$\Delta(I_{q^2}) = \{x_1^{\alpha_1} x_2^{\alpha_2} | 0 \leq \alpha_1 \leq q-1 \text{ and } 0 \leq \alpha_2 \leq q^2 - 1\}.$$

For $h_r = x_1^{r_1} x_2^{r_2} \in H$ we can compute N_r. Since the x_1 exponent of any monomial in the H-sequence is bounded above by $q-1$, we have

$$\begin{aligned} \mathcal{N}_r = \mathcal{P}_r &= \{(i,j) | wt(h_i) + wt(h_j) = wt(h_r)\} \\ &= \{(i,j) | h_i h_j = h_r \text{ or } h_i h_j = x_1^{r_1+q} x_2^{r_2-q-1}\}. \end{aligned}$$

Thus,

$$\begin{aligned} N_r = |\mathcal{N}_r| &= |\{\text{monomial divisors of either } h_r \text{ or } x_1^{r_1+q} x_2^{r_2-q-1}\}| \\ &= \begin{cases} (r_1+1)(r_2+1) & \text{if } r_2 \leq q \\ (r_1+1)(r_2+1) + (q - r_1 - 1)(r_2 - q) & \text{otherwise.} \end{cases} \end{aligned}$$

Example 1.38. Consider the Hermitian curve over $\mathbb{F}_9$ defined by the principal ideal $I = \langle x_1^3 + x_2^4 + x_1 \rangle \subseteq \mathbb{F}_9[x_1, x_2]$. We set $wt(x_1) = 4$ and $wt(x_2) = 3$. Also, $\Delta(I_9) = \{x_1^{\alpha_1} x_2^{\alpha_2} | 0 \leq \alpha_1 \leq 2 \text{ and } 0 \leq \alpha_2 \leq 8\}$. Therefore, the H-sequence is

$$\{1, x_2, x_1, x_2^2, x_1 x_2, x_1^2, x_2^3, \ldots, x_1^2 x_2^8\}.$$

Then, $N_1 = 1, N_2 = 2, N_3 = 2, N_4 = 3, N_5 = 4, N_6 = 3, N_7 = 4$. Also, for $r \geq 8$ we have $N_r \geq 6$. Hence, the affine variety code $C^{\perp}(I, L(\underline{7}))$ over $\mathbb{F}_9$ has length 27, dimension 20, and minimum distance at least 6.

Chapter 2
Codes on Fermat Surfaces

2.1 Gröbner Bases

In this section we will introduce some Gröbner basis theory necessary for the subsequent sections of this chapter. We shall mostly follow the notation and terminology of Adams and Loustaunau [1]. Fix a monomial ordering.

Definition 2.1. Let f and g be two nonzero polynomials in $\mathbb{F}_q[x_1, \ldots, x_k]$. We say that f *reduces to* r *modulo* g (or *by* g) *in one step*, denoted by

$$f \xrightarrow{g} r,$$

if and only if $lm(g)$ divides a nonzero term X that appears in f and

$$r = f - \frac{X}{lt(g)} g.$$

Note that we have subtracted from the polynomial f the entire term X and have replaced it with strictly smaller terms under our ordering. For the case when $X = lt(f)$, we are applying the division algorithm to f by dividing by g and receiving r as our remainder.

Definition 2.2. Let f, r and $f_1, \ldots, f_l$ be polynomials in $\mathbb{F}_q[x_1, \ldots, x_k]$ with $f_i \neq 0$ for $1 \leq i \leq l$ and let $F = \{f_1, \ldots, f_l\}$. We say that f *reduces to* r *modulo* F, denoted by

$$f \xrightarrow{F}_+ r,$$

if and only if there exist a sequence of indices $i_1, i_2, \ldots, i_s \in \{1, \ldots, l\}$ and a sequence of polynomials $r_1, \ldots, r_{s-1} \in \mathbb{F}_q[x_1, \ldots, x_k]$ such that

$$f \xrightarrow{f_{i_1}} r_1 \xrightarrow{f_{i_2}} r_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{s-1}}} r_{s-1} \xrightarrow{f_{i_s}} r.$$

Definition 2.3. A polynomial r is called *reduced* with respect to a set of nonzero polynomials $F = \{f_1, \ldots, f_l\}$ if either $r = 0$ or no monomial that appears in r is divisible by some $lm(f_i)$ where $1 \leq i \leq l$.

Definition 2.4. A set of nonzero polynomials $G = \{g_1, \ldots, g_l\}$ contained in an ideal I is called a *Gröbner basis* for I if and only if for each nonzero polynomial $f \in I$ there exists some i, where $1 \leq i \leq l$, such that $lm(g_i)$ divides $lm(f)$.

Theorem 2.5. *Let I be a nonzero ideal of $\mathbb{F}_q[x_1, \ldots, x_k]$. The following statements are equivalent for a set of nonzero polynomials $G = \{g_1, \ldots, g_l\} \subseteq I$.*

(i) *G is a Gröbner basis for I.*

(ii) *$f \in I$ if and only if $f \xrightarrow{G}_+ 0$.*

(iii) *$\Delta(I) = \{x_1^{\alpha_1} \ldots x_k^{\alpha_k} | \text{For each } i, 1 \leq i \leq l, \text{we have } lm(g_i) \nmid x_1^{\alpha_1} \ldots x_k^{\alpha_k}\}$.*

Proof. (i) $\Rightarrow$ (ii) Let f be a polynomial. Then there exists an r such that $f \xrightarrow{G}_+ r$, where r is reduced with respect to G. Thus, $f - r \in \langle G \rangle \subseteq I$. Hence, $f \in I$ if and only if $r \in I$. Clearly, if $r = 0$ (i.e. $f \xrightarrow{G}_+ 0$) then $f \in I$. Conversely, suppose $f \in I$. Then $r \in I$ and by (i), there exists $g_i \in G$ such that $lm(g_i) | lm(r)$. However, since r is reduced with respect to G, we must have $r = 0$.

(ii) $\Rightarrow$ (iii) Put

$$A = \{x_1^{\alpha_1} \ldots x_k^{\alpha_k} | \text{For each } i, 1 \leq i \leq l, \text{we have } lm(g_i) \nmid x_1^{\alpha_1} \ldots x_k^{\alpha_k}\}.$$

Since $\{g_1, \ldots, g_l\} \subseteq I$, we have $\Delta(I) \subseteq A$. Suppose $x_1^{\alpha_1} \ldots x_k^{\alpha_k} \notin \Delta(I)$. Then, there exists a polynomial $f \in I$ such that $lm(f) = x_1^{\alpha_1} \ldots x_k^{\alpha_k}$. By (ii), f reduces to 0 modulo G. Therefore, there exists $g_i \in G$ such that $lm(g_i) | x_1^{\alpha_1} \ldots x_k^{\alpha_k}$. Hence, $x_1^{\alpha_1} \ldots x_k^{\alpha_k} \notin A$.

(iii) $\Rightarrow$ (i) Suppose $f \in I$. Then we have $lm(f) \notin \Delta(I)$. By (iii), there exists $g_i \in G$ such that $lm(g_i) | lm(f)$. □

Lemma 2.6. *Let $G = \{g_1, \ldots, g_l\}$ be a Gröbner basis for $I \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$. Then for all $f \in \mathbb{F}_q[x_1, \ldots, x_k]$ the reduction of f with respect to G is unique.*

Proof. Suppose $f \xrightarrow{G}_+ r_1$ and $f \xrightarrow{G}_+ r_2$ with r_1 and r_2 reduced with respect to G. Note that $f - r_1 \in I$ and $f - r_2 \in I$. Therefore, $r_1 - r_2 \in I$. Since $r_1 - r_2$ is reduced with respect to G, we must have $r_1 - r_2 = 0$. □

Remark 2.7. Let I be an ideal in $\mathbb{F}_q[x_1, \ldots, x_k]$. Let G be a Gröbner basis for I_q. Let f be a polynomial in $\mathbb{F}_q[x_1, \ldots, x_k]$. Suppose $f \notin I_q$ and let $c_1 x^{\beta_1} + \cdots + c_s x^{\beta_s}$ (where $x^{\beta_s} <_t \cdots <_t x^{\beta_1}$) be the unique reduction of f with respect to G. Then $x^{\beta_1}, \ldots, x^{\beta_s}$ are in $\Delta(I_q)$. Suppose $x^{\beta_1} = h_r$, the r-th element in the H-sequence (cf. Definition 1.8). Then, $\bar{f} \in L(\underline{r}) \setminus L(\underline{r-1})$.

Indeed, since $f + I_q = c_1 x^{\beta_1} + \cdots + c_s x^{\beta_s} + I_q$, we have $f \in L(\underline{r})$. Assume $f \in L(\underline{r-1})$. Then $f + I_q = \sum_{i=1}^{r-1} k_i h_i + I_q$ where $k_i \in \mathbb{F}_q$ for $1 \leq i \leq r-1$. Thus,

$$c_1 x^{\beta_1} + I_q = \sum_{i=1}^{r-1} k_i h_i - (c_2 x^{\beta_2} + \cdots + c_s x^{\beta_s}) + I_q$$

implies that $h_r \in L(\underline{r-1})$, which is a contradiction.

Corollary 2.8. *Let $h_i, h_j \in H$ and suppose $h_{i,j} \notin I_q$. Reduce $h_{i,j}$ with respect to a Gröbner basis G for I_q. Let h_r be the leading monomial of the reduction. Then $h_{i,j} \sim h_r$ if and only if $wt(h_{i,j}) = wt(h_r)$.*

Note that Remark 2.7 implies that $h_{i,j}$ can only be consistent with the leading monomial of its reduction with respect to the Gröbner basis G. Also, there is a discrepancy for the case when $h_{i,j} \in I_q$. In this case the reduction of $h_{i,j}$ with respect to G is 0. Clearly, $h_{i,j}$ cannot be consistent with any h_r. However, when we examine the Fermat surfaces in Section 2.4, this case will not play a role.

Definition 2.9. Let f and g be nonzero polynomials in $\mathbb{F}_q[x_1, \ldots, x_k]$. Put $L = \operatorname{lcm}(lm(f), lm(g))$. The *$S$-polynomial of f and g*, denoted by $S(f,g)$, is defined as

$$S(f,g) = \frac{L}{lt(f)}f - \frac{L}{lt(g)}g.$$

These S-polynomials play a vital role in the computation of a Gröbner basis. More specifically, we are interested in the reduction of S-polynomials of any two polynomials in the Gröbner basis as demonstrated by Buchberger's Criterion [1].

Theorem 2.10. (Buchberger's Criterion) *Let $G = \{g_1, \ldots, g_l\}$ be a set of nonzero polynomials in $\mathbb{F}_q[x_1, \ldots, x_k]$. Then G is a Gröbner basis for the ideal $I = \langle g_1, \ldots, g_l \rangle$ if and only if for all $i \neq j$, we have $S(g_i, g_j) \xrightarrow{G}_{+} 0$.*

Proof. See [1]. □

From this Criterion we have a procedure, known as Buchberger's Algorithm, for computing a Gröbner basis. We can begin with the initial generators of our ideal I, say $f_1, \ldots, f_l$, and determine the S-polynomial of any two generators. Then reduce the S-polynomial with respect to the set of generators. If the reduction is nonzero, then add it to your set of generators for I.

Repeat the process of computing reductions of S-polynomials of pairs of generators from this "growing" set of generators. Eventually, after adding enough reductions to your generator set all S-polynomials of pairs of generators will reduce to zero with respect to the final set of generators (cf. [1]). This set will be a Gröbner basis for the ideal I. The algorithm is shown below.

As an easy consequence of Definition 2.4, we have

Lemma 2.11. *Suppose $G = \{g_1, \ldots, g_l\}$ is a Gröbner basis for the ideal I. If $lm(g_2)$ divides $lm(g_1)$, then $\{g_2, \ldots, g_l\}$ is also a Gröbner basis for I.*

Proof. See [1]. □

Buchberger's Algorithm

INPUT: $F = \{f_1, \ldots, f_l\} \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$ with $f_i \neq 0$ for $1 \leq i \leq l$

OUTPUT: $G = \{g_1, \ldots, g_s\}$, a Gröbner basis for $\langle f_1, \ldots, f_l \rangle$

INITIALIZATION: $G := F, \mathcal{G} := \{\{f_i, f_j\} | f_i \neq f_j \in G\}$

WHILE $\mathcal{G} \neq \emptyset$ DO

  Choose any $\{f, g\} \in \mathcal{G}$

  $\mathcal{G} := \mathcal{G} \setminus \{\{f, g\}\}$

  $S(f, g) \xrightarrow{G} r$, where r is reduced with respect to G.

  IF $r \neq 0$ THEN

    $\mathcal{G} := \mathcal{G} \cup \{\{u, r\}|$ for all $u \in G\}$.

    $G := G \cup \{r\}$

Definition 2.12. A Gröbner basis $G = \{g_1, \ldots, g_l\}$ is called a *reduced* Gröbner basis if, for all i, $lm(g_i) = lt(g_i)$ and g is reduced with respect to $G \setminus \{g_i\}$, i.e. no term that appears in g_i is divisible by $lm(g_j)$ for some $j \neq i$.

2.2 Higher-Dimensional Varieties

We now direct our attention to codes defined over higher-dimensional varieties of the form $V(I_q)$ where $I_q \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$ for some $k \geq 3$. In this section we will consider principal ideals $I = \langle g \rangle$ with the following properties:

(i) $g(x_1, \ldots, x_k) = x_1^d + f(x_2, \ldots, x_k)$

(ii) $lm(g) = x_1^d$

(iii) $d|(q-1)$

Define $n := (q-1)/d$. Following Buchberger's Algorithm, we will construct a Gröbner basis for the ideal $I_q = \langle g, f_1, \ldots, f_k \rangle$ where $f_i := x_i^q - x_i$ for $1 \leq i \leq k$.

Consider the S-polynomials. We have separated all possible S-polynomials into 12 various types.

(1)
$$\begin{aligned} S(g, f_1) &= \frac{x_1^q}{x_1^d} g - \frac{x_1^q}{x_1^q} f_1 = x_1^{q-d} g - f_1 = x_1^q + x_1^{q-d} f(x_2, \ldots, x_k) - x_1^q + x_1 \\ &= x_1^{q-d} f(x_2, \ldots, x_k) + x_1 \end{aligned}$$

which can be reduced successively by g an additional $n-1$ times to obtain

$$S(g, f_1) \xrightarrow{g}_+ x_1((-1)^{n+1}[f(x_2, \ldots, x_k)]^n + 1).$$

This can be further reduced, if necessary, by some of the f_i. If there exists an exponent $e_i \geq q$ of x_i in the expansion of $[f(x_2, \ldots, x_k)]^n$, then reduce the previous reduction by f_i. In essence, such a reduction replaces x_i^q with x_i whenever possible.

(2)
$$\begin{aligned} \text{For } i \geq 2,\ S(g, f_i) &= \frac{x_1^d x_i^q}{x_1^d} g - \frac{x_1^d x_i^q}{x_i^q} f_i = x_i^q g - x_1^d f_i \\ &= x_1^d x_i^q + x_i^q f - x_1^d x_i^q + x_1^d x_i = x_i^q f + x_1^d x_i, \end{aligned}$$

which can be reduced by both f_i and g.

$$S(g, f_i) \xrightarrow{f_i} x_i^q f + x_1^d x_i - f(f_i) = x_1^d x_i + x_i f \xrightarrow{g} x_1^d x_i + x_i f - x_i g = x_i f - x_i f = 0.$$

(3)
$$\begin{aligned} S(f_i, f_j) &= \frac{x_i^q x_j^q}{x_i^q} f_i - \frac{x_i^q x_j^q}{x_j^q} f_j = x_j^q f_i - x_i^q f_j \\ &= x_i^q x_j^q - x_i x_j^q - x_i^q x_j^q + x_i^q x_j = x_i^q x_j - x_i x_j^q, \end{aligned}$$

which can be reduced by both f_i and f_j.

$$S(f_i, f_j) \xrightarrow{f_i} x_i^q x_j - x_i x_j^q - x_j f_i = x_i x_j - x_i x_j^q \xrightarrow{f_j} x_i x_j - x_i x_j^q + x_i f_j = x_i x_j - x_i x_j = 0.$$

Note that through (1), (2), and (3), we have examined all the S-polynomials determined by the pairs of the $k+1$ initial generators of I_q. At this point, we now have $G = \{g, f_1, \ldots, f_k, S^*(g, f_1)\}$ where $S^*(g, f_1)$ is the reduction of $S(g, f_1)$ by $G \setminus \{S^*(g, f_1)\}$ discussed in (1).

Let h_α denote an arbitrary polynomial in the variables $x_2, \ldots, x_k$ such that $x_1 h_\alpha \in G$. Let h_β denote an arbitrary polynomial in the variables $x_2, \ldots, x_k$ such that $h_\beta \in G$. We may assume that $lm(h_\alpha) = lt(h_\alpha)$ and $lm(h_\beta) = lt(h_\beta)$. These polynomials are defined to be "in progress," of course. Right now, we have one of type h_α, namely $S^*(g, f_1)$, and $k-1$ of type $h_\beta \in G$. We now must consider the following S-polynomials.

$$\begin{aligned} S(g, x_1 h_\alpha) &= \frac{x_1^d lt(h_\alpha)}{x_1^d} g - \frac{x_1^d lt(h_\alpha)}{x_1 lt(h_\alpha)} x_1 h_\alpha = lt(h_\alpha) g - x_1^d h_\alpha \\ &= x_1^d lt(h_\alpha) + lt(h_\alpha) f - x_1^d h_\alpha = lt(h_\alpha) f - x_1^d [h_\alpha - lt(h_\alpha)], \end{aligned} \tag{4}$$

which can be reduced by g.

$$\begin{aligned} S(g, x_1 h_\alpha) &\xrightarrow{g} lt(h_\alpha) f - x_1^d [h_\alpha - lt(h_\alpha)] + g[h_\alpha - lt(h_\alpha)] \\ &= lt(h_\alpha) f + f[h_\alpha - lt(h_\alpha)] = f h_\alpha. \end{aligned}$$

$$\begin{aligned} S(f_1, x_1 h_\alpha) &= \frac{x_1^q lt(h_\alpha)}{x_1^q} f_1 - \frac{x_1^q lt(h_\alpha)}{x_1 lt(h_\alpha)} x_1 h_\alpha = lt(h_\alpha) f_1 - x_1^q h_\alpha \\ &= x_1^q lt(h_\alpha) - x_1 lt(h_\alpha) - x_1^q h_\alpha = -x_1 lt(h_\alpha) - x_1^q [h_\alpha - lt(h_\alpha)], \end{aligned} \tag{5}$$

which can be reduced by both f_1 and $x_1 h_\alpha$.

$$\begin{aligned} S(f_1, x_1 h_\alpha) &\xrightarrow{f_1} - x_1 lt(h_\alpha) - x_1^q [h_\alpha - lt(h_\alpha)] + f_1 [h_\alpha - lt(h_\alpha)] \\ &= \; - x_1 lt(h_\alpha) - x_1 [h_\alpha - lt(h_\alpha)] = -x_1 h_\alpha \xrightarrow{x_1 h_\alpha} -x_1 h_\alpha + x_1 h_\alpha = 0. \end{aligned}$$

(6) For $i \geq 2$, $S(f_i, x_1 h_\alpha) = \dfrac{lcm(x_i^q, x_1 lt(h_\alpha))}{x_i^q} f_i - \dfrac{lcm(x_i^q, x_1 lt(h_\alpha))}{x_1 lt(h_\alpha)} x_1 h_\alpha = x_1 h'$

where h' is a polynomial in the variables $x_2, \ldots, x_k$. If $x_1 h'$ is reducible by G, then the reduction must be of the form x_1 times a polynomial independent of x_1 (i.e., a polynomial in $F_q[x_2, \ldots, x_k]$).

$$S(g,h_\beta) = \frac{x_1^d lt(h_\beta)}{x_1^d} g - \frac{x_1^d lt(h_\beta)}{lt(h_\beta)} h_\beta = lt(h_\beta)g - x_1^d h_\beta \tag{7}$$

$$= x_1^d lt(h_\beta) + lt(h_\beta)f - x_1^d h_\beta = lt(h_\beta)f - x_1^d[h_\beta - lt(h_\beta)],$$

which can be reduced by both g and h_β.

$$S(g,h_\beta) \xrightarrow{g} lt(h_\beta)f - x_1^d[h_\beta - lt(h_\beta)] + g[h_\beta - lt(h_\beta)] = lt(h_\beta)f + f[h_\beta - lt(h_\beta)]$$

$$= fh_\beta \xrightarrow{h_\beta} fh_\beta - fh_\beta = 0.$$

$$S(f_1,h_\beta) = \frac{x_1^q lt(h_\beta)}{x_1^q} f_1 - \frac{x_1^q lt(h_\beta)}{lt(h_\beta)} h_\beta = lt(h_\beta)f_1 - x_1^q h_\beta \tag{8}$$

$$= x_1^q lt(h_\beta) - x_1 lt(h_\beta) - x_1^q(h_\beta) = -x_1 lt(h_\beta) - x_1^q[h_\beta - lt(h_\beta)],$$

which can be reduced by both f_1 and h_β.

$$S(f_1,h_\beta) \xrightarrow{f_1} -x_1 lt(h_\beta) - x_1^q[h_\beta - lt(h_\beta)] + f_1[h_\beta - lt(h_\beta)]$$

$$= -x_1 lt(h_\beta) - x_1[h_\beta - lt(h_\beta)] = -x_1 h_\beta \xrightarrow{h_\beta} -x_1 h_\beta + x_1 h_\beta = 0.$$

$$\text{For } i \geq 2,\ S(f_i,h_\beta) = \frac{lcm(x_i^q, lt(h_\beta))}{x_i^q} f_i - \frac{lcm(x_i^q, lt(h_\beta))}{lt(h_\beta)} h_\beta = h_\gamma \tag{9}$$

where h_γ is a polynomial in the variables $x_2, \ldots, x_k$. If this is reducible by G, then the reduction must be independent of x_1.

$$S(x_1 h_\alpha, h_\beta) = \frac{x_1 lcm(lt(h_\alpha), lt(h_\beta))}{x_1 lt(h_\alpha)} x_1 h_\alpha - \frac{x_1 lcm(lt(h_\alpha), lt(h_\beta))}{lt(h_\beta)} h_\beta = x_1 h_\delta \tag{10}$$

where h_δ is a polynomial in the variables $x_2, \ldots, x_k$. If $x_1 h_\delta$ is reducible by G, then the reduction must be of the form x_1 times a polynomial independent of x_1.

Finally, let h_{α_1} and h_{α_2} denote any two polynomials in the variables $x_2, \ldots, x_k$ such that $x_1 h_{\alpha_1}, x_1 h_{\alpha_2} \in G$. Similarly, let h_{β_1} and h_{β_2} denote any two polynomials in the variables $x_2, \ldots, x_k$ such that $h_{\beta_1}, h_{\beta_2} \in G$.

(11)

$$S(x_1h_{\alpha_1}, x_1h_{\alpha_2}) = \frac{lcm(lt(h_{\alpha_1}), lt(h_{\alpha_2}))}{lt(h_{\alpha_1})}x_1h_{\alpha_1} - \frac{lcm(lt(h_{\alpha_1}), lt(h_{\alpha_2}))}{lt(h_{\alpha_2})}x_1h_{\alpha_2} = x_1h_\epsilon$$

where h_ϵ is a polynomial in the variables $x_2, \ldots, x_k$. If x_1h_ϵ is reducible by G, then the reduction must be of the form x_1 times a polynomial independent of x_1.

$$(12) \qquad S(h_{\beta_1}, h_{\beta_2}) = \frac{lcm(lt(h_{\beta_1}), lt(h_{\beta_2}))}{lt(h_{\beta_1})}h_{\beta_1} - \frac{lcm(lt(h_{\beta_1}), lt(h_{\beta_2}))}{lt(h_{\beta_2})}h_{\beta_2} = h_\zeta$$

where h_ζ is a polynomial in the variables $x_2, \ldots, x_k$. If this is reducible by G, then the reduction must be independent of x_1.

Since the code length of $C^\perp(I, L)$ is equal to the the number of rational points of $V(I_q)$, we need to work with varieties with many rational points to obtain long codes. Observe that in Buchberger's Algorithm, each time an S-polynomial fails to reduce to zero, we append a new polynomial to G. When this occurs, we are informed that any multiple of the leading monomial of the polynomial does not appear in $\Delta(I_q)$. Hence, in order to make $|\Delta(I_q)|$ relatively large, we would like a large number of these S-polynomials to reduce to zero.

Consider the "first" S-polynomial represented in (4); namely, $S(g, S^*(g, f_1))$. When does this reduce to zero? Note that $S(g, S^*(g, f_1))$ reduces to zero if and only if

$$f((-1)^{n+1}f^n + 1) = (-1)^{n+1}f^{n+1} + f \xrightarrow{F}_+ 0.$$

Lemma 2.13. *Suppose n is a divisor of $q-1$ that satisfies $n+1 = (\mathrm{char}\ \mathbb{F}_q)^m$ for some integer m. Then there exists a subfield of $\mathbb{F}_q$ with $n+1$ elements.*

Proof. Suppose there exist positive integers d and n such that $dn = q-1$ and $n+1 = (\mathrm{char}\ \mathbb{F}_q)^m$ for some integer m. Express $q = (\mathrm{char}\ \mathbb{F}_q)^t$ where t is a positive integer. Then $d = (q-1)/n$ implies that

$$d = \frac{(\text{char } \mathbb{F}_q)^t - 1}{(\text{char } \mathbb{F}_q)^m - 1}.$$

Since d is an integer, it follows that $m|t$. Therefore, there exists a subfield of $\mathbb{F}_q$ with $n+1$ elements [6]. □

Let $\mathbb{F}_{n+1}$ denote that subfield. Suppose $f = c_1 m_1 + \cdots + c_s m_s$ where $c_i \in \mathbb{F}_q$ and $m_i \in T^k$ for $1 \leq i \leq s$. Note that

$$(-1)^{n+1} = \begin{cases} -1 & \text{if char } \mathbb{F}_q \neq 2 \\ 1 & \text{if char } \mathbb{F}_q = 2. \end{cases}$$

So we always have $(-1)^{n+1} = -1$ in $\mathbb{F}_q$. Therefore,

$$\begin{aligned} (-1)^{n+1} f^{n+1} + f = -f^{n+1} + f &= -(c_1 m_1 + \cdots + c_s m_s)^{n+1} + (c_1 m_1 + \cdots + c_s m_s) \\ &= -((c_1 m_1)^{n+1} + \cdots + (c_s m_s)^{n+1}) + c_1 m_1 + \cdots + c_s m_s \\ &= (c_1 m_1) - (c_1 m_1)^{n+1} + \cdots + (c_s m_s) - (c_s m_s)^{n+1}. \end{aligned}$$

When does this reduce to zero by F? To answer this question, we will use the following concept.

Definition 2.14. [8] A polynomial $f \in \mathbb{F}_q[x_2, \ldots, x_k]$ is called an $(\mathbb{F}_q^{k-1}, \mathbb{F}_{n+1})$-*polynomial* if the image of f when restricted to $\mathbb{F}_q^{k-1}$ is contained in $\mathbb{F}_{n+1}$.

In fact, given this condition, we will show next that all S-polynomials that are independent of x_1 will reduce to zero. This leaves us with a Gröbner basis of the form

$$\{x_1(g_1), \ldots, x_1(g_s), g, f_2, \ldots, f_k\}$$

for the ideal I_q.

Theorem 2.15. *Let* $g(x_1, \ldots, x_k) := x_1^d + f(x_2, \ldots, x_k) \in \mathbb{F}_q[x_1, \ldots, x_k]$, *where* $d|(q-1)$, $n := \frac{q-1}{d}$, $n+1 = (\text{char } \mathbb{F}_q)^m$ *for some positive integer* m, f *is an*

$(\mathbb{F}_q^{k-1}, \mathbb{F}_{n+1})$-polynomial, and $lt(g) = x_1^d$. Put $I = \langle g \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$ and let $J = \langle f^n - 1 \rangle \subseteq \mathbb{F}_q[x_2, \ldots, x_k]$. If $\{g_1, \ldots, g_s, f_2, \ldots, f_k\}$ is a Gröbner basis for J_q, where $f_i := x_i^q - x_i$ for $2 \leq i \leq k$, then $\{x_1(g_1), \ldots, x_1(g_s), g, f_2, \ldots, f_k\}$ is a Gröbner basis for I_q.

Proof. Put $I' := \langle x_1(g_1), \ldots, x_1(g_s), g, f_2, \ldots, f_k \rangle$. We need to show $I' \subseteq I_q$. It suffices to show that $x_1(g_i) \in I_q$ for all i such that $1 \leq i \leq s$. Since $g_i \in J_q$, then $g_i = \sum_{j=2}^k p_j f_j + p_1[f^n - 1]$ for some $p_1, p_2, \ldots, p_k \in \mathbb{F}_q[x_2, \ldots, x_k]$. Therefore, $x_1(g_i) = \sum_{j=2}^k x_1 p_j f_j + p_1 x_1[f^n - 1]$. Since $f_j \in I_q$ for $2 \leq j \leq k$, we have that $\sum_{j=2}^k x_1 p_j f_j$ is in I_q. Also, $x_1[f^n - 1]$ is the negative of the reduction of $S(g, f_1)$ represented in (1). Hence, $x_1(g_i) \in I_q$. Thus, $I' \subseteq I_q$.

Put $K := \langle f \rangle \subseteq \mathbb{F}_q[x_2, \ldots, x_k]$. Since I_q, J_q, and K_q are radical ideals, put

$a :=$ number of points of $V(I_q) = |\Delta(I_q)|$,

$b :=$ number of points of $V(J_q) = |\Delta(J_q)|$,

$c :=$ number of points of $V(K_q) = |\Delta(K_q)|$.

Notice that

$$b = |\{(c_2, \ldots, c_k) \in \mathbb{F}_q^{k-1} | f(c_2, \ldots, c_k) \in \mathbb{F}_{n+1} \setminus \{0\}\}|$$

and

$$c = |\{(c_2, \ldots, c_k) \in \mathbb{F}_q^{k-1} | f(c_2, \ldots, c_k) = 0\}|.$$

For $c_1 \in \mathbb{F}_q$ we have that $c_1^d \in \mathbb{F}_{n+1}$ since $(c_1^d)^{n+1} = (c_1)^{q-1+d} = c_1^d$. For each nonzero element $y \in \mathbb{F}_{n+1}$ there exists d-many choices for $c_1 \in \mathbb{F}_q$ such that $c_1^d = y$. Therefore, from the defining polynomial $g(x_1, \ldots, x_k)$, we have $a = db + c$. Note that $\Delta(I') \subseteq \{x_1^{\alpha_1} \ldots x_k^{\alpha_k} | 0 \leq \alpha_1 < d$, $0 \leq \alpha_i < q$ for $2 \leq i \leq k$, and either $\alpha_1 = 0$ or $x_2^{\alpha_2} \ldots x_k^{\alpha_k} \in \Delta(J_q)\}$. Therefore,

$$|\Delta(I')| \leq q^{k-1} + (d-1)|\Delta(J_q)| = q^{k-1} + (d-1)b.$$

Since $I' \subseteq I_q$, then $\Delta(I_q) \subseteq \Delta(I')$. Thus, $a = |\Delta(I_q)| \leq |\Delta(I')|$.

Assume that $|\Delta(I_q)| < |\Delta(I')|$. Hence,

$$a = db + c < q^{k-1} + (d-1)b,$$

which implies that $b + c < q^{k-1}$. However,

$$\begin{aligned} b + c &= |\{(c_2, \ldots, c_k) \in \mathbb{F}_q^{k-1} | f(c_2, \ldots, c_k) \in \mathbb{F}_{n+1} \setminus \{0\}\}| \\ &\quad + |\{(c_2, \ldots, c_k) \in \mathbb{F}_q^{k-1} | f(c_2, \ldots, c_k) = 0\}| \\ &= |\{(c_2, \ldots, c_k) \in \mathbb{F}_q^{k-1} | f(c_2, \ldots, c_k) \in \mathbb{F}_{n+1}\}| = q^{k-1} \end{aligned}$$

since f is an $(\mathbb{F}_q^{k-1}, \mathbb{F}_{n+1})$-polynomial, which is a contradiction. Therefore, we have $|\Delta(I_q)| = |\Delta(I')|$. Thus, $\Delta(I_q) = \Delta(I') = \{x_1^{\alpha_1} \ldots x_k^{\alpha_k} | 0 \leq \alpha_1 < d,\ 0 \leq \alpha_i < q$ for $2 \leq i \leq k$, and either $\alpha_1 = 0$ or $x_2^{\alpha_2} \ldots x_k^{\alpha_k} \in \Delta(J_q)\}$. By Theorem 2.5, we have that $\{x_1(g_1), \ldots, x_1(g_s), g, f_2, \ldots, f_k\}$ is a Gröbner basis for I_q. $\square$

2.3 Fermat Varieties

Specifically, consider the Fermat varieties defined by the ideal

$$I = \langle x_1^d + x_2^d + \cdots + x_k^d + b \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$$

where $nd = q - 1$, $n + 1 = (\text{char } \mathbb{F}_q)^m$ for some positive integer m, and $b \in \mathbb{F}_{n+1}$, which is a subfield of $\mathbb{F}_q$ by Lemma 2.13. The following table displays all varieties of this type for $q \leq 729 = 3^6$. Note that this includes all affine Hermitian varieties. This is the case when $q = (d-1)^2$.

We now wish to determine the exact number of solutions in $\mathbb{F}_q^k$ for the equation $x_1^d + x_2^d + \cdots + x_k^d + b = 0$ satisfying the above conditions. This has been done previously by [11] and [12]. However, the argument is usually done using character sums. We will provide a simpler explanation.

Fermat Varieties Table

q	d	n	q	d	n	q	d	n
4	3	1	64	63	1	289	18	16
8	7	1	81	10	8	343	57	6
9	4	2	81	40	2	361	20	18
16	5	3	121	12	10	512	73	7
16	15	1	125	31	4	512	511	1
25	6	4	128	127	1	529	24	22
27	13	2	169	14	12	625	26	24
32	31	1	243	121	2	625	156	4
49	8	6	256	17	15	729	28	26
64	9	7	256	85	3	729	91	8
64	21	3	256	255	1	729	364	2

Note that $c^d \in \mathbb{F}_{n+1}$ for all $c \in \mathbb{F}_q$ since $(c^d)^{n+1} = (c)^{q-1+d} = c^d$. Therefore, $x_1^d + x_2^d + \cdots + x_k^d + b$ is an $(\mathbb{F}_q^{k-1}, \mathbb{F}_{n+1})$-polynomial. Put $y_j := x_j^d$ for $1 \leq j \leq k$. Consider the solutions in $\mathbb{F}_{n+1}^k$ to the equation $y_1 + \cdots + y_k + b = 0$. Assume that exactly i of the y_j are nonzero. For $1 \leq i \leq k$, define $z_{i,b}$ to be the number of ways to choose i elements $a_1, \ldots, a_i \in \mathbb{F}_{n+1} \setminus \{0\}$ such that $a_1 + \cdots + a_i + b = 0$. For $i = 0$, we set

$$z_{0,b} = \begin{cases} 1 & \text{if } b = 0 \\ 0 & \text{otherwise.} \end{cases}$$

For each nonzero $y_j \in \mathbb{F}_{n+1}$ there exists d-many $x_j \in \mathbb{F}_q$ such that $x_j^d = y_j$. Of course, if $y_j = 0$ then $x_j = 0$. Thus, the number of solutions to $x_1^d + \cdots + x_k^d + b = 0$ in which there are exactly i nonzero x_j is $\binom{k}{i} z_{i,b} d^i$. Hence, the number of solutions over $\mathbb{F}_q^k$ to $x_1^d + x_2^d + \cdots + x_k^d + b = 0$ is $\sum_{i=0}^{k} \binom{k}{i} z_{i,b} d^i$. Now, we will examine the two cases of $z_{i,b}$ more explicitly beginning with a recursive formula.

Lemma 2.16. [3] *For $i \geq 2$, $z_{i,b} = n^{i-1} - z_{i-1,b}$.*

Proof. There are n^{i-1} ways to choose elements $a_1, \ldots, a_{i-1}$ from $\mathbb{F}_{n+1} \setminus \{0\}$. Exactly $z_{i-1,b}$ of these choices have the property that $a_1 + \cdots + a_{i-1} + b = 0$. However, for each of these $z_{i-1,b}$ choices there does not exist a nonzero a_i such that $a_1 + \cdots + a_i + b = 0$. On the other hand, if $a_1 + \cdots + a_{i-1} + b \neq 0$, then there exists a unique nonzero a_i such that $a_1 + \cdots + a_i + b = 0$. □

Proposition 2.17. (i) *The number of solutions in $\mathbb{F}_q^k$ to $x_1^d + x_2^d + \cdots + x_k^d = 0$ is*

$$\frac{q^k + n(1-d)^k}{n+1}.$$

(ii) *The number of solutions over $\mathbb{F}_q^k$ to $x_1^d + x_2^d + \cdots + x_k^d + b = 0$ when $b \neq 0$ is*

$$\frac{q^k - (1-d)^k}{n+1}.$$

Proof. (i) $b = 0$. Note that $z_{0,0} = 1$ and $z_{1,0} = 0$. Therefore, by expansion of the recursive formula, we obtain that for $i \geq 2$,

$$z_{i,0} = n^{i-1} - n^{i-2} + \cdots + (-1)^i n = \sum_{l=0}^{i-2} (-1)^l n^{i-1-l}.$$

Note that $z_{i,0}$ is also expressed as a geometric series, so

$$z_{i,0} = \frac{(-1)^i n[1 - (-n)^{i-1}]}{1+n} = \frac{n^i + (-1)^i n}{n+1}$$

for $i \geq 0$. Hence, the number of solutions is

$$\begin{aligned}
\sum_{i=0}^{k} \binom{k}{i} d^i \frac{n^i + (-1)^i n}{n+1} &= \frac{1}{n+1} \sum_{i=0}^{k} \binom{k}{i} (dn)^i + \frac{n}{n+1} \sum_{i=0}^{k} \binom{k}{i} (-d)^i \\
&= \frac{1}{n+1} \sum_{i=0}^{k} \binom{k}{i} (q-1)^i + \frac{n}{n+1} \sum_{i=0}^{k} \binom{k}{i} (-d)^i \\
&= \frac{1}{n+1}(q^k) + \frac{n}{n+1}(1-d)^k = \frac{q^k + n(1-d)^k}{n+1}.
\end{aligned}$$

(ii) $b \neq 0$. Note that $z_{0,b} = 0$ and $z_{1,b} = 1$. Therefore, by expansion of the recursive formula, we obtain that for $i \geq 1$,

$$z_{i,b} = n^{i-1} - n^{i-2} + \cdots + (-1)^i n + (-1)^{i+1} = \sum_{l=0}^{i-1} (-1)^l n^{i-1-l}.$$

Note that $z_{i,b}$ is expressed as a geometric series, so

$$z_{i,b} = \frac{(-1)^{i+1}[1-(-n)^i]}{1+n} = \frac{n^i + (-1)^{i+1}}{n+1}$$

for $i \geq 0$. Hence, the number of solutions is

$$\begin{aligned}
\sum_{i=0}^{k} \binom{k}{i} d^i \frac{n^i + (-1)^{i+1}}{n+1} &= \frac{1}{n+1} \sum_{i=0}^{k} \binom{k}{i} (dn)^i + \frac{1}{n+1} \sum_{i=0}^{k} \binom{k}{i} (-1)^{i+1} d^i \\
&= \frac{1}{n+1} \sum_{i=0}^{k} \binom{k}{i} (q-1)^i - \frac{1}{n+1} \sum_{i=0}^{k} \binom{k}{i} (-d)^i \\
&= \frac{1}{n+1}(q^k) - \frac{1}{n+1}(1-d)^k = \frac{q^k - (1-d)^k}{n+1}. \square
\end{aligned}$$

Throughout the rest of this chapter, we will choose to assign the variables equal weight. Thus we may assume $wt(x_1) = wt(x_2) = \cdots = wt(x_k) = 1$. Note that our monomial ordering is then simply the degree lexicographic ordering.

Generally, it is difficult to describe the H-sequence for Fermat varieties of dimension k. However, we can obtain a description of N_r under certain circumstances. In the next section we will show that the hypothesis in the following theorem is valid in the case of Fermat surfaces.

Theorem 2.18. *Let $V(I_q)$ be an affine variety defined by $I \subseteq \mathbb{F}_q[x_1, \ldots, x_k]$ where $k \geq 3$. Suppose that $wt(x_i) = wt(x_j)$ for $1 \leq i, j \leq k$. For each $h_i, h_j, h_r \in H$, if $h_{i,j} = x_1^{p_1} x_2^{p_2} \ldots x_k^{p_k} \sim h_r = x_1^{r_1} x_2^{r_2} \ldots x_k^{r_k}$ implies that $p_n \leq r_n$ for $3 \leq n \leq k$, then $N_r = \prod_{n=1}^{k} (r_n + 1)$.*

Proof. By Proposition 1.21, we know that $N_r \geq \prod_{n=1}^{k}(r_n+1)$. Assume equality does not hold. Then there exist elements $h_i = x_1^{i_1} \ldots x_k^{i_k}, h_j = x_1^{j_1} \ldots x_k^{j_k} \in H$ such that

$h_i h_j = h_{i,j}$ is a well-behaving term consistent with h_r but $h_i h_j \neq h_r$. By Lemma 1.20, we may assume that h_i and h_j are non-divisors of h_r. This implies that there exist α and β such that $i_\alpha > r_\alpha$ and $j_\beta > r_\beta$. Since $i_n + j_n \leq r_n$ for $3 \leq n \leq k$ (by our hypothesis) and $h_r <_t h_i h_j$ (by Corollary 1.15), we have $\alpha, \beta \in \{1, 2\}$ and $i_1 + j_1 \geq r_1$.

We will show that $h_{i,j}$ cannot be well-behaving. We will find $h_u = x_1^{u_1} \ldots x_k^{u_k}$ and $h_v = x_1^{v_1} \ldots x_k^{v_k}$ such that $h_u <_t h_i$, $h_v <_t h_j$, and $h_u h_v = h_r$.

Put $u_1 := \min\{i_1, r_1\}$. For $2 \leq n \leq k$ put

$$u_n := \min\{r_n, \sum_{l=1}^{k} i_l - \sum_{l=1}^{n-1} u_l\}.$$

Put $v_n := r_n - u_n$ for $1 \leq n \leq k$. Now, since $wt(h_i) + wt(h_j) = wt(h_r)$, we have that

$$\sum_{n=1}^{k} i_n + \sum_{n=1}^{k} j_n = \sum_{n=1}^{k} r_n.$$

Clearly, $\sum_{n=1}^{k} u_n \leq \sum_{n=1}^{k} i_n$.

Assume $\sum_{n=1}^{k} u_n < \sum_{n=1}^{k} i_n$. Then, for all n such that $2 \leq n \leq k$,

$$u_n = r_n < \sum_{l=1}^{k} i_l - \sum_{l=1}^{n-1} u_l$$

(otherwise, $\sum_{l=1}^{k} i_l = \sum_{l=1}^{n} u_l \leq \sum_{l=1}^{k} u_l$, which is a contradiction). Furthermore, $u_1 = i_1 < r_1$ (otherwise, $\sum_{n=1}^{k} u_n = \sum_{n=1}^{k} r_n < \sum_{n=1}^{k} i_n$, which is a contradiction). Therefore,

$$i_1 + \sum_{n=2}^{k} r_n = \sum_{n=1}^{k} u_n < \sum_{n=1}^{k} i_n = \sum_{n=1}^{k} r_n - \sum_{n=1}^{k} j_n$$

which implies that $i_1 + j_1 \leq i_1 + \sum_{n=1}^{k} j_n < r_1$, which is a contradiction. Thus, $\sum_{n=1}^{k} u_n = \sum_{n=1}^{k} i_n$.

By construction,

$$\sum_{n=1}^{k} v_n = \sum_{n=1}^{k} r_n - \sum_{n=1}^{k} u_n = \sum_{n=1}^{k} r_n - \sum_{n=1}^{k} i_n = \sum_{n=1}^{k} j_n.$$

Let $h_u = x_1^{u_1} \dots x_k^{u_k}$ and $h_v = x_1^{v_1} \dots x_k^{v_k}$. So, $wt(h_u) = wt(h_i)$ and $wt(h_v) = wt(h_j)$. Note that $h_u h_v = h_r$. Therefore, $h_u, h_v \in H$ by Remark 1.9. We claim that $h_u <_t h_i$ and $h_v <_t h_j$.

Suppose $u_1 = r_1 < i_1$. Then we have $h_u <_t h_i$. Also, $u_1 = r_1$ implies that $v_1 = r_1 - u_1 = 0$. Hence, if $j_1 > 0$ then $h_v <_t h_j$. If $j_1 = 0$, then since $h_j \nmid h_r$, we have $r_2 < j_2$. This implies that $v_2 < j_2$ and $h_v <_t h_j$.

Suppose $u_1 = i_1 \leq r_1$. Since $h_i \nmid h_r$, we have $r_2 < i_2$. Thus, $u_2 < i_2$ and $h_u <_t h_i$. Also, $u_1 = i_1$ and $i_1 + j_1 \geq r_1$ imply that $v_1 \leq j_1$. If $i_1 + j_1 > r_1$, then $v_1 < j_1$ and so $h_v <_t h_j$. If $i_1 + j_1 = r_1$, then since $h_j \nmid h_r$, we have $r_2 < j_2$. This implies that $v_2 < j_2$ and $h_v <_t h_j$.

Thus, in each of the cases we have $h_{u,v} = h_r$ with $h_u <_t h_i$ and $h_v <_t h_j$. Hence, $h_{i,j}$ is not a well-behaving term, which is a contradiction. □

2.4 Fermat Surfaces

Theorem 2.19. *Consider the affine variety $V(I_q)$ defined by a Fermat surface where $I = \langle x_1^d + x_2^d + x_3^d + b \rangle \subseteq \mathbb{F}_q[x_1, x_2, x_3]$ and d satisfies $1 < d < q$. The set of leading terms of the reduced Gröbner basis for I_q is $\{x_1^d, x_2^q, x_3^q, x_1 x_2^{q-1}, x_1 x_2^{q-d} x_3^d\}$ if and only if $d | (q-1)$, $n+1 = (\text{char } \mathbb{F}_q)^m$ for some integer m where $n := (q-1)/d$, and $b \in \mathbb{F}_{n+1} \setminus \{0\}$.*

Proof. ($\Longleftarrow$) We apply Buchberger's Algorithm and carefully examine two of the S-polynomials. First,

$$S(g, f_1) \xrightarrow{g} x_1((-1)^{n+1} f^n + 1) = x_1(-f^n + 1) = x_1(-(x_2^d + x_3^d + b)^n + 1),$$

whose leading term is $-x_1 x_2^{q-1}$. Second,

$$S(f_2, S^*(g, f_1)) = x_1 x_2^q - x_1 x_2 + x_1 x_2(-(x_2^d + x_3^d + b)^n + 1),$$

which has leading term $-x_1x_2^{d(n-1)+1}x_3^d = -x_1x_2^{q-d}x_3^d$ since the term $x_1x_2^q$ is canceled. Currently in the algorithm we have $G =$

$$\{x_1^d + x_2^d + x_3^d + b, x_2^q - x_2, x_3^q - x_3, x_1((x_2^d + x_3^d + b)^n - 1), x_1x_2(x_2^d + x_3^d + b)^n - x_1x_2^q\}.$$

The set of leading monomials of G is

$$\{x_1^d, x_2^q, x_3^q, x_1x_2^{q-1}, x_1x_2^{q-d}x_3^d\}.$$

All other S-polynomials must reduce to zero since the set of leading monomials implies that $\Delta(I_q) \subseteq A \cup B \cup C$, where

$$\begin{aligned}
A &= \{x_2^\beta x_3^\gamma | 0 \leq \beta < q, 0 \leq \gamma < q\} \\
B &= \{x_1^\alpha x_2^\beta x_3^\gamma | 1 \leq \alpha < d, 0 \leq \beta < q-d, 0 \leq \gamma < q\} \\
C &= \{x_1^\alpha x_2^\beta x_3^\gamma | 1 \leq \alpha < d, q-d \leq \beta < q-1, 0 \leq \gamma < d\}.
\end{aligned}$$

Thus,

$$\begin{aligned}
|\Delta(I_q)| &\leq q^2 + (d-1)(q-d)q + (d-1)(d-1)d \\
&= q^2 + (d-1)q^2 - dq(d-1) + d(d-1)^2 = dq^2 + dq(1-d) + d(1-d)^2 \\
&= d(q^2 + q(1-d) + (1-d)^2) = d\frac{q^3 - (1-d)^3}{q-(1-d)} = \frac{q^3-(1-d)^3}{\frac{q-1+d}{d}} \\
&= \frac{q^3-(1-d)^3}{\frac{q-1}{d}+1} = \frac{q^3-(1-d)^3}{n+1},
\end{aligned}$$

which is the actual number of points of $V(I_q)$ by Proposition 2.17.

($\Longrightarrow$) Assume $d \nmid (q-1)$. Express $(q-1) = nd + r$ where $n \geq 1$ and $1 \leq r \leq d-1$. Suppose $r \neq d-1$. Then in the ring $\mathbb{F}_q[x_1, x_2, x_3]/I_q$ we have

$$x_1 + I_q = x_1^q + I_q = x_1^{r+1}(x_1^d)^n + I_q = x_1^{r+1}(-1)^n(x_2^d + x_3^d + b)^n + I_q.$$

Thus, the polynomial $f = x_1^{r+1}(-1)^n(x_2^d + x_3^d + b)^n - x_1 \in I_q$ and $lm(f) = x_1^{r+1}x_2^{dn}$. However, since $r+1 < d$ and $dn < q-1$, we know that $x_1^{r+1}x_2^{dn}$ is not a multiple of any of the leading terms of the Gröbner basis, which is a contradiction. Suppose $r = d-1$, then $q = (n+1)d$. Note that $n+1 > 1$ implies that $n+1 = (\text{char } \mathbb{F}_q)^m$ for some $m > 0$. Therefore,

$$\begin{aligned} x_1 + I_q = x_1^q + I_q = (x_1^d)^{n+1} + I_q &= (-1)^{n+1}(x_2^d + x_3^d + b)^{n+1} + I_q \\ &= (-1)^{n+1}(x_2^{d(n+1)} + x_3^{d(n+1)} + b^{n+1}) + I_q = (-1)^{n+1}(x_2^q + x_3^q + b^{n+1}) + I_q \\ &= (-1)^{n+1}(x_2 + x_3 + b^{n+1}) + I_q. \end{aligned}$$

Thus, the polynomial $f = x_1 - (-1)^{n+1}(x_2 + x_3 + b^{n+1}) \in I_q$ and $lm(f) = x_1$. However, x_1 is not a multiple of any of the leading terms of the Gröbner basis, which is a contradiction. Hence, $d|(q-1)$.

Assume $n+1 = st$ where $s =$(char $\mathbb{F}_q)^k$ for some $k \geq 0$ and (char $\mathbb{F}_q) \nmid t$ with t an integer greater than 1. In the ring $\mathbb{F}_q[x_1, x_2, x_3]/I_q$ we have that

$$\begin{aligned} x_1^d + I_q = x_1^{q-1+d} + I_q = x_1^{nd+d} + I_q = (x_1^d)^{n+1} + I_q &= (-1)^{n+1}(x_2^d + x_3^d + b)^{n+1} + I_q \\ &= (-1)^{n+1}((x_2^d + x_3^d + b)^{n+1} + (x_2^d - x_2^{q-1+d}) + (x_3^d - x_3^{q-1+d})) + I_q \\ &= (-1)^{n+1}((x_2^d + x_3^d + b)^{st} + x_2^d - x_2^{q-1+d} + x_3^d - x_3^{q-1+d}) + I_q \\ &= (-1)^{n+1}((x_2^{ds} + x_3^{ds} + b^s)^t + x_2^d - x_2^{q-1+d} + x_3^d - x_3^{q-1+d}) + I_q \end{aligned}$$

Thus, the polynomial

$$f = (-1)^{n+1}((x_2^{ds} + x_3^{ds} + b^s)^t + x_2^d - x_2^{q-1+d} + x_3^d - x_3^{q-1+d}) - x_1^d \in I_q.$$

Since

$$dst = d(n+1) = dn + d = q - 1 + d,$$

we have that $x_2^{dst} - x_2^{q-1+d} = 0$ and $lm(f) = x_2^{ds(t-1)}x_3^{ds}$ and its coefficient is $(-1)^{n+1}t$. Note that

$$ds(t-1) = d(st - s) = d(n+1-s) \leq dn = q - 1$$

and $(-1)^{n+1}t \neq 0$ over $\mathbb{F}_q$. Thus, $x_2^{ds(t-1)}x_3^{ds}$ is not a multiple of any of the leading terms of the Gröbner basis, which is a contradiction. Hence $n+1 = (\text{char } \mathbb{F}_q)^m$ for some integer m.

From the proof of ($\Longleftarrow$) we know that the leading terms imply that

$$|\Delta(I_q)| = \frac{q^3 - (1-d)^3}{n+1}.$$

Therefore, by Proposition 2.17, $b \neq 0$. □

Corollary 2.20. *Let $V(I_q)$ be the affine variety defined by a Fermat surface where $I = \langle x_1^d + x_2^d + x_3^d + b\rangle \subseteq \mathbb{F}_q[x_1, x_2, x_3]$ where $d|(q-1)$, $n+1 = (\text{char } \mathbb{F}_q)^m$ for some integer m where $n := (q-1)/d$, and $b \in \mathbb{F}_{n+1} \setminus \{0\}$. A Gröbner basis for I_q is $\{x_1^d + x_2^d + x_3^d + b, x_2^q - x_2, x_3^q - x_3, x_1((x_2^d + x_3^d + b)^n - 1), x_1x_2(x_2^d + x_3^d + b)^n - x_1x_2^q\}$.*

Corollary 2.21. (i) *For each polynomial g_i of the Gröbner basis G in Corollary 2.20, if $x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}$ is a monomial that appears in g_i such that $wt(x^\alpha) = wt(lm(g_i))$, where $lm(g_i) = x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}$, then $\beta_1 \geq \alpha_1$ and $\beta_1 + \beta_2 \geq \alpha_1 + \alpha_2$.*

(ii) *Suppose f reduces to r modulo G. Also, suppose $lm(f) = x_1^{\beta_1}x_2^{\beta_2}x_3^{\beta_3}$ and $lm(r) = x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}$. If $wt(lm(f)) = wt(lm(r))$ then $\beta_1 \geq \alpha_1$ and $\beta_1 + \beta_2 \geq \alpha_1 + \alpha_2$.*

Proof. This follows by inspection of the polynomials in the Gröbner basis in Corollary 2.20. □

For the remainder of this chapter we will assume that $V(I_q)$ satisfies the conditions stated in Corollary 2.20. We will now show that for each $h_r \in H$, its corresponding N_r is easy to determine.

Lemma 2.22. *For $h_i = x_1^{i_1}x_2^{i_2}x_3^{i_3}$, $h_j = x_1^{j_1}x_2^{j_2}x_3^{j_3}$, and $h_r = x_1^{r_1}x_2^{r_2}x_3^{r_3} \in H$, if $h_{i,j} = x_1^{p_1}x_2^{p_2}x_3^{p_3}$ is consistent with h_r, then $p_3 \leq r_3$.*

Proof. First we will show that for Fermat surfaces $h_{i,j} \notin I_q$. Indeed, if $h_{i,j} = x_1^{p_1}x_2^{p_2}x_3^{p_3} \in I_q$, then $x_1^q x_2^q x_3^q \in I_q$. It follows that $x_1x_2x_3 \in I_q$. However, there does not exist a Gröbner basis polynomial whose leading term divides $x_1x_2x_3$, which is a contradiction. Now, by Remark 2.7, we have that h_r is the leading monomial of the reduction of $h_{i,j}$ with respect to the Gröbner basis. Also, $h_{i,j} \sim h_r$ implies that $wt(h_{i,j}) = wt(h_r)$. Therefore, Corollary 2.21 implies that $p_1 + p_2 \geq r_1 + r_2$. However, since $h_{i,j}$ and h_r have the same total degree, we have $p_3 \leq r_3$. □

Proposition 2.23. *For the Fermat surfaces of this section, we have that* $N_r = \prod_{i=1}^{3}(r_i + 1)$, *the number of monomial divisors of* h_r.

Proof. This follows from Lemma 2.22 and Theorem 2.18. □

Not only are we interested in the actual value of N_r, but in order to determine the dimensions of our codes we need to know how many times that value occurs. Put

$$S_t = |\{h_r \in H | N_r \leq t\}|.$$

The footprint of the ideal I_q can be expressed as $\Delta(I_q) = U \setminus (V \cup W)$ where

$$\begin{aligned} U &= \{x_1^\alpha x_2^\beta x_3^\gamma | 0 \leq \alpha < d, 0 \leq \beta < q, 0 \leq \gamma < q\}, \\ V &= \{x_1^\alpha x_2^{q-1} x_3^\gamma | 1 \leq \alpha < d, 0 \leq \gamma < q\}, \\ W &= \{x_1^\alpha x_2^\beta x_3^\gamma | 1 \leq \alpha < d, q - d \leq \beta \leq q - 2, d \leq \gamma < q\}. \end{aligned}$$

Since N_r is simply the number of monomial divisors of h_r, we know from $\Delta(I_q)$ that $S_t = |U_t| - |V_t| - |W_t|$ where

$$\begin{aligned} U_t &= \{(\alpha, \beta, \gamma) | \alpha\beta\gamma \leq t, 1 \leq \alpha \leq d, 1 \leq \beta \leq q, 1 \leq \gamma \leq q\} \\ V_t &= \{(\alpha, \gamma) | \alpha q \gamma \leq t, 2 \leq \alpha \leq d, 1 \leq \gamma \leq q\} \\ W_t &= \{(\alpha, \beta, \gamma) | \alpha\beta\gamma \leq t, 2 \leq \alpha \leq d, q - d < \beta < q, d < \gamma \leq q\}. \end{aligned}$$

However, if we restrict

$$t < 2(q - d + 1)(d + 1),$$

then $C_t = \varnothing$. Hence,

$$S_t = |U_t| - |V_t|.$$

If we fix the value of the product $\beta\gamma$, call it x, then $|\{\alpha|(\alpha, \beta, \gamma) \in U_t\}| = \min\{d, \lfloor t/x \rfloor\}$. Hence,

$$|U_t| = \sum_{x=1}^{t} f_t(x) g(x)$$

where

$$f_t(x) = \min\{d, \lfloor t/x \rfloor\}$$

and

$$g(x) = |\{(\beta, \gamma)|\beta\gamma = x, 1 \leq \beta \leq q, 1 \leq \gamma \leq q\}|.$$

If we fix the value of the product $\alpha\gamma$, call it y, then

$$|V_t| = \sum_{y=2}^{\lfloor t/q \rfloor} h(y)$$

where

$$h(y) = |\{(\alpha, \gamma)|\alpha\gamma = y, 2 \leq \alpha \leq d, 1 \leq \gamma \leq q\}|.$$

Thus, for $t < 2(q - d + 1)(d + 1)$ we have

$$S_t = \sum_{x=1}^{t} f_t(x) g(x) - \sum_{y=2}^{\lfloor t/q \rfloor} h(y).$$

For affine variety codes $C^{\perp}(I, L)$ of length $\frac{q^3-(1-d)^3}{n+1}$ where $I = \langle x_1^d + x_2^d + x_3^d + b \rangle \subseteq \mathbb{F}_q[x_1, x_2, x_3]$, if we want a minimum distance lower bound of δ, then we put $L = \mathrm{span}\{\bar{h}_r | N_r < \delta\}$. Hence, L has dimension $S_{\delta-1}$. Thus, our code has dimension

$$\frac{q^3 - (1 - d)^3}{n + 1} - S_{\delta-1}.$$

Example 2.24. Suppose you desire a code over $\mathbb{F}_4$ to have length 36 and minimum distance at least 6. Consider the affine variety code $C^{\perp}(I, L)$ where the ideal $I =$

$\langle x_1^3 + x_2^3 + x_3^3 + 1\rangle \subseteq \mathbb{F}_4[x_1, x_2, x_3]$, put $L = \text{span}\{\bar{h}_r | N_r < 6\}$. We need to calculate $S_5 = \sum_{x=1}^{5} f_5(x)g(x)$ with $f_5(x) = \min\{3, \lfloor 5/x \rfloor\}$ and

$$g(x) = |\{(\beta, \gamma)|\beta\gamma = x, 1 \le \beta \le 4, 1 \le \gamma \le 4\}|.$$

Thus,

$$S_5 = 3g(1) + 2g(2) + g(3) + g(4) + g(5) = 3 + 4 + 2 + 3 + 0 = 12.$$

Hence, $C^{\perp}(I, L)$ is a $[36, 24, \ge 6]$-code over $\mathbb{F}_4$, i.e. a code of length 36, dimension 24, and minimum distance at least 6. The actual minimum distance is 6 since the columns of the parity check matrix H_r^* corresponding to the points $P_1 = (1, \alpha^2, \alpha^2), P_2 = (1, 1, \alpha^2), P_3 = (\alpha, 1, 1), P_4 = (\alpha, \alpha, 1), P_5 = (\alpha^2, \alpha, \alpha)$, and $P_6 = (\alpha^2, \alpha^2, \alpha)$, where α is a generator of the multiplicative group of $\mathbb{F}_4$, are linearly dependent.

Example 2.25. Suppose you wish to obtain a code over $\mathbb{F}_9$ with length 252 and minimum distance at least 12. Consider the affine variety code $C^{\perp}(I, L)$ where $I = \langle x_1^4 + x_2^4 + x_3^4 + 1\rangle \subseteq \mathbb{F}_9[x_1, x_2, x_3]$, put $L = \text{span}\{\bar{h}_r | N_r < 12\}$. Now, $S_{11} = \sum_{x=1}^{11} f_{11}(x)g(x)$ with $f_{11}(x) = \min\{4, \lfloor 11/x \rfloor\}$ and

$$g(x) = |\{(\beta, \gamma)|\beta\gamma = x, 1 \le \beta \le 9, 1 \le \gamma \le 9\}|.$$

Therefore,

$$\begin{aligned} S_{11} &= 4g(1) + 4g(2) + 3g(3) + 2g(4) + 2g(5) + \sum_{x=6}^{11} g(x) \\ &= 4 + 8 + 6 + 6 + 4 + 4 + 2 + 4 + 3 + 2 + 0 = 43. \end{aligned}$$

Thus, our code is a $[252, 209, \ge 12]$, $\mathbb{F}_9$-linear code.

References

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, 1994.

[2] D. Cox, J. Little, and D. O'Shea: *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag, New York, 1992.

[3] J. Fitzgerald, *Applications of Gröbner Bases to Linear Codes*, Doctoral dissertation, Louisiana State University, 1996.

[4] G.-L. Feng and T. R. N. Rao, "Improved Geometric Goppa Codes, Part I: Basic Theory", *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1678-1693, Nov. 1995.

[5] T. Høholdt, J. H. van Lint, and R. Pellikaan, "Algebraic Geometry Codes," in *Handbook of Coding Theory*, V. Pless, W. C. Huffman and R. A. Brualdi, Eds., pp. 871-961 (vol. 1), Elsevier, Amsterdam, 1998.

[6] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[7] C. Kirfel and R. Pellikaan, "The Minimum Distance of Codes in an Array Coming from Telescopic Semigroups," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1720-1732, Nov. 1995.

[8] L. Rédei, *Lacunary Polynomials over Finite Fields*, North-Holland, Amsterdam, 1973.

[9] A. Seidenberg, "Constructions in Algebra," *Transactions of the American Mathematical Society*, 197, pp. 273-313, 1974.

[10] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, "Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound," *Math. Nachrichten*, 109, pp. 21-28, 1982.

[11] A. Weil, "Numbers of Solutions of Equations in Finite Fields," *Bulletin of the American Mathematical Society*, 55, pp. 497 - 508, 1949.

[12] J. Wolfmann, "The Number of Solutions of Certain Diagonal Equations Over Finite Fields," *J. Number Theory*, vol. 42, no. 3, pp. 247-257, 1992.

Vita

Gary Salazar was born on April 15, 1972 in Waco, Texas. He finished his undergraduate studies in mathematics and chemistry at Baylor University in May, 1994. After a year of graduate studies at Baylor University, Gary decided to pursue a doctorate in mathematics specializing in the field of coding theory at Louisiana State University. He is currently a candidate for the doctoral degree in mathematics which will be awarded in August, 2000.