Algebraic Geometric Coding Theory

ZHUO JIA DAI

zhuojia.dai@gmail.com

Original Supervisor: Dr David R. Kohel

This is a modified version of the thesis submitted in fulfillment of the requirements for the degree of
Bachelor of Science (Advanced Mathematics) Honours
completed at the
School of Mathematics and Statistics, University of Sydney, Australia

26 November 2006

Acknowledgements

Firstly, I would like to thank my supervisor, Dr David R. Kohel whose many helpful comments and patient guidance made this thesis possible.

Secondly, I would like to thank David Gruenwald for volunteering his time to proofread this thesis. Almost all of his recommendations were taken on board. This thesis is the better for it.

To a less extent, my thanks go to the IT school of University of Sydney for making this excellent thesis template available for general use.

CONTENTS

CHAPTER 1

Introduction

1.1 About this thesis

The original version of this thesis was written in 2006 when the author was studying at the University of Sydney (USYD). This thesis has since been slightly modified, but it remains an atrocious piece of junk. In my opinion, this is one of the worst honours thesis to have come out of the mathematics department at USYD. The inconsistency in the description of a "function field" in chapter 2 and 4 is a good illustration of the poor quality of this thesis.

1.2 What is Coding Theory?

The study of coding theory, or more descriptively - error-correcting codes, is primarily concerned with dealing with errors introduced by noise when transmitting data over communication channels. In this thesis, we consider a class of codes known as block-codes where data is encoded as a block of digits of uniform length.

Computer scientists have devised a number of strategies to deal with errors introduced by noise. The simplest of which is a technique called parity-check, where a single 0 or 1 is added to end of the data block so that the block has an even number of 1's. If the data is contaminated at only one place during transmission, then the received block of data will have an odd number of 1's. This tells the receiver that the data has been affected by noise, so that retransmission may be requested.

The parity check technique may not be practical in many situations. For example in satellite communication, retransmission is prohibitively expensive and time-consuming. Often, a better strategy is to encode the data in a way that allows the receiver to detect and correct the errors! A very intuitive strategy is repetition. It is implemented simply by sending each digit n times. Suppose the sender sends 00000 but 00101 was received instead. The receiver notes that there are more 0's than 1's. Therefore the block 00101 is decoded as 00000. Effectively, two errors were corrected. This strategy of encoding is called a "repetition code".

However, the repetition code sacrifices a lot of bandwidth for error correcting ability. Indeed, in the repetition scheme above, every five bits of data sent represent only one bit of real information. In this thesis we will introduce a class of very powerful codes called Algebraic Geometric codes that offer a high degree of flexibility in choosing the trade-offs between bandwidth costs and error correting abilities.

1.3 Why Algebraic Geometry?

Although the general theory of linear codes is well established, a number of computational problems central to coding theory, such as decoding and the determination of minimum distances, are known to be NP-Complete, see $([12], 98)$. There is no known "efficient" algorithm for solving any of the NP-Complete problems. In fact, the first person to discover a deterministic polynomial-time algorithm for any of the NP-Complete problems attracts a cash prize of US$1,000,000 from the "Clay Mathematics Institute".

The above discussion suggests that finding an efficient decoding algorithm for linear codes is close to being impssible. Hence, our best chance is to focus on linear codes with special properties that lend themselves to efficient decoding. We will show that the Riemann-Roch theorem from the theory of algebraic curves provides the desired special linear codes! Also worth noting is that it is theoretically possible to construct a sequence of algebraic geometric codes with parameters that better than the asymtoptic Gilbert-Varshamov Bound (GV-Bound), see $([9], 82)$. Prior to that discovery, it was widely believed that the GV-Bound was unattainable.

1.4 A Quick Tour

The next two chapters, **2. Algebraic Curves** and **3. Function Fields**, develop the key definitions and theorems regarding algebraic curves and their associated function fields leading to the explicit construction of some Riemann-Roch spaces. The chapter **4. Algebraic Geometric Codes** uses the explicitly constructed Riemann-Roch spaces to develop practical Algebraic Geometric codes. The decoding problem for these codes are discussed (and partially solved) in the chapter **5. Basic Decoding Algorithm**. The highlight of this thesis comes in the final chapter, **6. Majority Voting Algorithm**, where capabilities of the various Algebraic Geometric codes are exploited to the full by a clever algorithm named Majority Voting Scheme. This algorithm solves the decoding problem in polynomial time.

1.5 Assumed Knowledge

It is assumed that the reader is familiar with materials covered in a typical first course in Algebraic Curves, in particular the all important Riemann-Roch Theorem will be stated but not proved. Also, variously concepts from Commutative Algebra such as localisation and local rings are assumed knowleddge. Some basic results in linear algebra are also assumed.

Some familarity with coding theory is assumed. However, a brief introduction to coding theory is presented in Appendix A for completeness.

1.6 Notations

Throughout, we denote the finite field of order q as $\mathbb{F}_q$. Let $\mathbb{F}$ be a field, we denote by $\mathbb{F}[x_1, x_2, ..., x_n]$ the ring of polynomials in the indeterminate $x_1, x_2, ..., x_n$ with coefficients in $\mathbb{F}$. The notation $A = B$ means A is equal to B, while $A := B$ means A is by definition equal to B.

CHAPTER 2

Algebraic Curves

In this chapter, we cover the basic theory of algebraic curves. Some of the materials presented here are covered by a typical first undergraduate course in the subject, so the presentation will be kept brief.

This chapter assumes some commutative algebra.

2.1 Affine Curves

Some of the definitions below closely follow $([12], 98)$.

DEFINITION 2.1.1. (Affine Space, Algebraic Set, Affine Variety)
Let $\mathbb{K}$ be an algebraically closed field. The n-dimensional affine space, denoted $\mathbb{A}^n$, is the space of n-tuples of $\mathbb{K}$. An element of $\mathbb{A}^n$ is called a point. An ideal $I \subsetneq \mathbb{K}[x_1, x_2, \cdots, x_n]$ corresponds to an algebraic set defined as

$$V(I) := \{(a_1, a_2, \cdots, a_n) \in \mathbb{A}^n \mid F(a_1, a_2, \cdots, a_n) = 0 \text{ for all } F \in I\}$$

If $I \subsetneq \mathbb{K}[x_1, x_2, \cdots, x_n]$ is a prime ideal, the algebraic set $V(I)$ is called an affine variety.

DEFINITION 2.1.2. (Transcedence degree)
Let L and K be fields such that $K \subseteq L$. The transcendence degree of L over K is defined as the maximum number of algebraically independent elements of L over K.

DEFINITION 2.1.3. (Coordinte ring, Function field, Degree of Variety)
Let $\mathcal{X} = V(I)$ where I is as above. The integral domain $\mathbb{K}[\mathcal{X}] := \mathbb{K}[x_1, x_2, \cdots, x_n]/I$ is called the coordinate ring of the affine variety $\mathcal{X}$. The function field, denoted by $\mathbb{K}(\mathcal{X})$, is the field of fractions of $\mathbb{K}[\mathcal{X}]$.

REMARK 2.1.4.
Since I is prime, $\mathbb{K}[\mathcal{X}]$ is an integral domain, and so $\mathbb{K}(\mathcal{X})$ is indeed a field.

DEFINITION 2.1.5. (Dimension, Algebraic Curve)
The dimension of the variety $\mathcal{X}$ is the transcendence degree of $\mathbb{K}(\mathcal{X})$ over $\mathbb{K}$. An algebraic curve is a variety of dimension 1.

2.2 Plane Curves

From here on we will focus our attention on plane curves, i.e. curves defined by the indetermintes x and y in the affine case and X, Y and Z in the projective case. We will show that planes curves satisfying certain properties are indeed algebraic curves.

Throughout, assume $\mathbb{F}$ is a finite field, so $\mathbb{F}$ is not algebraically closed. Let $\mathbb{K} = \bar{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$, and let $\mathbb{A}^n$ be the n-dimensional affine space of $\mathbb{K}$.

DEFINITION 2.2.1. (Point, Affine Plane Curve)
Let $f \in \mathbb{F}[x, y]$. An affine plane curve C, defined by f over $\mathbb{F}$, denoted $C : f = 0$ is the set of zeroes of f in $\mathbb{A}^n$ i.e. n-tuples $P = (p_1, p_2, ..., p_n) \in \mathbb{A}^n$ such that

$$f(p_1, p_2, ..., p_n) = 0$$

If P is a such a n-tuple then P is called a point on the curve, and we write $P \in C$.

REMARK 2.2.2.
Notice that our definition of a plane curve is specific to a field $\mathbb{F}$ which may not be algebraically closed.

DEFINITION 2.2.3. (Degree, Rational Points)
Let $\tilde{\mathbb{F}}$ be a finite field extension of $\mathbb{F}$ of minimal degree such that $Q \in \tilde{\mathbb{F}}^n$ is a point on the curve, then the degree of Q is defined to be $[\tilde{\mathbb{F}} : \mathbb{F}]$. A point of degree 1 is called a rational point. Points of higher degree are not rational.

EXAMPLE 2.2.4.
Consider the plane affine curve $C : y - x^2$ defined over $\mathbb{F}_2$. The points $(0, 0)$ and $(1, 1)$ are the only rational points while (w, w^2) and $(w^2, 1)$ where $\mathbb{F}_4 := \mathbb{F}[w]$ and $w^2 + w + 1$ are points of degree 2 and therefore not rational.

DEFINITION 2.2.5. (Irreducible Polynomial, Irreducible Curve)
Let f be as above. We say f is irreducible over $\mathbb{F}$ if $f = gh$ where $g, h \in \mathbb{F}[x, y]$ then $g \in \mathbb{F}$ or $h \in \mathbb{F}$. Otherwise we say f is reducible. If an affine plane curve C, is defined by an irreducible polynomial f then we say C is irreducible over $\mathbb{F}$. Otherwise C is reducible.

If f is irreducible over $\mathbb{F}$, it does not guarantee that f cannot be expressed as the product of polynomials with coeffecients in an extension field of $\mathbb{F}$. For example Let $\mathbb{F} = \mathbb{R}$ then $f = x^2 + y^2$ is irreducible over $\mathbb{F}$, but $f = (x + iy)(x - iy)$, hence $\mathbb{F}$ is reducible over $\mathbb{C}$. Being reducible over a finite field of $\mathbb{F}$ implies that $(f) := \{\ fg \mid g \in \mathbb{K}[x, y]\ \}$ is not prime in $\mathbb{K}[x, y]$ and so in that case $C : f = 0$ is not an algebraic curve. This motivates the following definition.

DEFINITION 2.2.6. (Absolutely irreducible Curve)
A polynomial $f \in \mathbb{F}[x_1, x_2, ..., x_n]$ is absolutely irreducible if f is irreducible over any finite field

extension of $\mathbb{F}$. If C is defined by an absolutely irreducible polynomial $f \in \mathbb{F}[x, y]$ then C is an absolutely irreducible affine plane curve.

LEMMA 2.2.7.
Let $f \in \mathbb{F}[x, y]$ be an absolutely irreducible polynomial. The ideal

$$(f) := \{\ fg \mid g \in \mathbb{K}[x, y]\ \} \subsetneq \mathbb{K}[x, y]$$

generated by f is prime. Furthermore, $C : f = 0$ is an algebraic curve.

PROOF
Since f is absolutely irreducible, f is irreducible over $\mathbb{K}$. Clearly, (f) must be prime since $\mathbb{K}[x, y]$ is an unique factorization domain. Consider x as a transcendental element over $\mathbb{K}$. Since y is algebraically related to x via f, x must be the only transcendental element in the function field $\mathbb{K}(C)$. Therefore by definition, $C : f = 0$ is an algebraic curve. □

REMARK 2.2.8.
We mainly deal with finite fields and any field $\mathbb{F}$ is a unique factorization domain (UFD), and so is $\mathbb{F}[x_1]$. In fact, if R is a UFD then so is $R[x]$. Therefore $\mathbb{F}[x_1, x_2, \cdots, x_n]$ are UFDs for all n. See Theorem 4.5 p223, $([11], 96)$.

LEMMA 2.2.9. (Eisenstein's criterion)
Let R be an unique factorization domain (UFD), and let $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. Suppose there exists an irreducible element $p \in R$ such that

$$\begin{aligned} a)&\quad p \text{ divides } a_i \text{ for all } i \neq n \\ b)&\quad p \text{ does not divide } a_n \\ c)&\quad p^2 \text{ does not divide } a_0 \end{aligned}$$

then f is irreducible.

PROOF
Suppose f satisfies properties a), b) and c), and

$$f = (\sum_{i=0}^{s} b_i x^i)(\sum_{i=0}^{t} c_i x^i)$$

where $s > 0$ and $t > 0$. We have $a_0 = b_0 c_0$ and by property a) and c), p divides one of b_0 and c_0, but not both. Suppose p divides c_0 but not b_0. By our assumption p does not divide $a_n = \sum_{i=0}^{n} b_i c_{n-i}$, so p cannot divide all the c_i's. Let $k > 0$ be the smallest value such that p does not divide c_k. We have $a_k = \sum_{i=0}^{k} b_i c_{k-i}$, which is divisible by p by property b), but p does not divide b_0 nor c_k. This is a contradiction. Therefore either $s = 0$ or $t = 0$. □

REMARK 2.2.10.
In Example 2.4.3, it is shown that the Hermitian Curves are absolutely irreducible.

From this point onwards we simply assume all our curves are absolutely irreducible; and they are.

2.3 Projective Plane Curves

DEFINITION 2.3.1. (Projective Space)
A projective space of dimension n, denoted $\mathbb{P}^n$, is the set

$$\mathbb{P}^n = (\mathbb{A}^n \setminus \{0\})/\equiv$$

where

$$(p_1, p_2, ..., p_{n+1}) \equiv \lambda(p_1, p_2, ..., p_{n+1}) \qquad \forall \lambda \in \mathbb{K}^*$$

Let $[p_1 : p_2 : .. : p_{n+1}]$ denote the equivalence class containing the element $(p_1, p_2, .., p_{n+1})$. We have

$$\mathbb{P}^n := \{\ [p_1 : p_2 : .. : p_{n+1}] \mid (p_1, p_2, .., p_{n+1}) \in \mathbb{A}^n \setminus \{0\}\}$$

where $\{0\}$ is the set $\{(0, 0, \cdots, 0)\}$

REMARK 2.3.2.
The fact that $\equiv$ is an equivalence relation is elementary to check. Note that $[0 : 0 : \cdots : 0]$ is not a point in the projective space.

DEFINITION 2.3.3. (Homogeneous Polynomial)
A polynomial $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$ is called homogeneous if every term of f is of equal degree. If f is not homogeneous, let x_{n+1} be an additional indeterminate distinct from the x_i's for $i \leq n$. Let d be the degree of f, we produce $\tilde{f}$ by multiplying each term of f by x_{n+1} raised to an appropriate power so that each term of $\tilde{f}$ has degree d; this process is called the homogenization of f.

NOTATION
We write non-homogeneous polynomials using lower-case letters x, y as the indeterminates while a homogeneous polynomial uses capital letters X, Y and Z.

EXAMPLE 2.3.4.
Let $f = x^3y + y^3 + x$ then $\tilde{f} = X^3Y + Y^3Z + XZ^3$.

DEFINITION 2.3.5. (Projective Variety)
Consider a prime ideal $I \subsetneq \mathbb{K}[x_1, x_2, \cdots, x_{n+1}]$ consisting of homogeneous polynomials. A projective variety is defined as the set of points in $\mathbb{P}^n$ that vanishes at every $F \in I$.

DEFINITION 2.3.6. (Projective Closure, Plane Projective Curve)
Let $f \in \mathbb{F}[x, y]$ be absolutely irreducible. The projective closure $\tilde{C}$, of $C : f = 0$ is the projective variety $V(\tilde{f})$. A plane projective curve is defined as the projective closure of an affine absolutely irreducible plane curve $C : f(x, y) = 0$.

DEFINITION 2.3.7. (Coordinate Ring, Function Field)
Let C be a projective curve. The coordinate ring is defined as $\mathbb{K}[C] := \mathbb{K}[X, Y, Z]/I$. The function field of C, denoted $\mathbb{K}(C)$ is defined as the subring of the quotient field of $\mathbb{K}[C]$ where every element is of the form F/G where F and G have the same degree.

REMARK 2.3.8.
The requirement that every element of $\mathbb{K}(C)$ must be of the form F/G where F and G have the same degree ensures that different representations of a point in $\mathbb{P}^2$ do not get evaluated to different values under the same function.

DEFINITION 2.3.9. (Point at infinity)
Let C be a plane projective curve. We call a point in the form of $[p_1 : p_2 : 0] \in C$ a point at infinity.

REMARK 2.3.10.
One may think of the projective curve $\tilde{C} : \tilde{f} = 0$ as the affine curve $C : f = 0$ with some added points at infinity.

2.4 Some Examples of Curves

EXAMPLE 2.4.1. (Parabola)
Let $f = y - x^2$. The affine plane curve $C : f = 0$ consists of the points (i, i^2) for $i \in \mathbb{K}$. The projective closure of C is $\tilde{C} : YZ - X^2$, it has points $[i : i^2 : 1]$ and one point at infinity $[0 : 1 : 0]$. Over $\mathbb{F}_2$, the only rational points are $[0 : 1 : 0], [1 : 1 : 1]$ and $[0 : 0 : 1]$

EXAMPLE 2.4.2. (Cusp)
Let $f = y^2 - x^3$. The projective closure has only one point at infinity $[0 : 1 : 0]$.

EXAMPLE 2.4.3. (Hermitian Curve)
The curve $C : f = x^{q+1} + y^{q+1} + 1 = 0$ over $\mathbb{F}_{q^2}$ is called the q-Hermitian Curve. The projective closure is defined by $\tilde{f} = X^{q+1} + Y^{q+1} + Z^{q+1}$. It has $q + 1$ points at infinity. Indeed, let $Z = 0, Y = 1$, we get $X^{q+1} + 1 = 0$ which has $q+1$ roots. Let $w_1, w_2, \cdots, w_{q+1}$ be the roots, then clearly $[w_i : 1 : 0] \in \tilde{C}$.

HERMITIAN CURVES ARE ABSOLUTELY IRREDUCIBLE
As an example we show that the affine Hermitian Curve is absolutely irreducible. Consider the defining polynomial $f = a_0 + a_{q+1}y^{q+1}$ as an element of $\bar{\mathbb{F}}[x][y]$, where $a_0 = 1 + x^{q+1}$, $a_{q+1} = 1$ and $a_i = 0$

for $i \neq 0, q+1$. Choose $x+1$ as the irreducible element. If $\mathbb{F}$ is of characteristic 2 then

$$x^{q+1}+1 = x^{q+1}-1 = (x-1)(\sum_{i=0}^{q} x^i)$$

and so $x+1$ divides a_0 but not a_{q+1}, and since $\sum_{i=0}^{q} 1^i = q+1 = 1 \neq 0$, we can clearly see that $(x+1)^2$ does not divide a_0. So f must be absolutely irreducible since it cannot be factored over $\bar{\mathbb{F}}$ by the Eisenstein's criterion. If $\mathbb{F}$ is not of characteristic 2 then $q+1 = 2r$ for some r since q is odd. So $x^{q+1}+1 = x^{2r}+1 = (x^r+1)(x^r-1) = (x^r+1)(x-1)(\sum_{i=0}^{r-1} x^i)$, so $x-1$ divides a_0 but not a_{q+1}, and $(x-1)^2$ clearly does not divide a_0, so f is absolutely irreducible.

THE RATIONAL POINTS ON HERMITIAN CURVE

Consider the projective closure of the q-Hermitian Curve defined by $\tilde{f} = X^{q+1} + Y^{q+1} + Z^{q+1}$. Setting $Z = 0, Y = 1$, we have $X^{q+1} + 1 = 0$, and there are $q+1$ roots. These roots must lie in $\mathbb{F}_{q^2}$ since $X^{(q+1)(q-1)} = (-1)^{q-1} = 1$ for any q any prime power, i.e. $X^{q^2-1} = 1$ which confirms that the roots must lie in $\mathbb{F}_{q^2}$. Setting $Z = 1$, we have $X^{q+1} + Y^{q+1} + 1 = 0$. There $q+1$ values for Y such that $Y^{q+1} + 1 = 0$, so there are $q+1$ points of the form $[0 : a : 1]$ lying on the curve. Now if $b = Y^{q+1} + 1 \neq 0$, then $X^{q+1} + b$ have $q+1$ distinct roots. The number of possible Y's that satisfy the above must be $q^2 - q - 1$ since out of the q^2 elements of $\mathbb{F}_{q^2}$, $q+1$ satisfy $Y^{q+1} + 1 = 0$.
So the number of rational points on a q-Hermitian Curve is

$$(q+1) + (q+1) + (q^2-q-1)(q+1) = (q+1) + (q^2-q)(q+1) = q^3 + 1$$

In summary, if q is a prime power, there are q^3+1 rational points on the q-Hermitian Curve over $\mathbb{F}_{q^2}$

EXAMPLE 2.4.4. (Hermitian Curve Form 2)

We will see that curves with only one point at infinity are more convenient to deal with. We transform the Hermitian Curve defined by $f = x^{q+1} + y^{q+1} + 1$ over $\mathbb{F}_{q^2}$ into a curve with only one point at infinity by the following substitutions as described in $([10], 88)$:

$$\begin{aligned} u &= b/(x-by) \\ v &= ux - a \end{aligned}$$

where $b^{q+1} = -1 = a^q + a$ and $P = [1 : b : 0] \in \tilde{C}$. The only place where u is undefined is when $x = by$. In that case we have

$$b^{q+1}y^{q+1} + y^{q+1} + 1 = 1 \neq 0$$

so u is defined everywhere on the curve. The above substitution gives

$$\begin{aligned} x &= (v+a)/u \\ y &= x/b - 1/u \\ y &= (v+a)/bu - 1/u \end{aligned}$$

which yields

$$u^{q+1} - v^q - v = 0$$

Therefore, we can use $f = x^{q+1} - y^q - y$ as an alternative formulation of the q-Hermitian Curve. As mentioned, there is only one point at infinity in this representation of the curve. Using a similar argument as in the previous example we see that there are also $q^3 + 1$ rational points on $\tilde{C}$ over $\mathbb{F}_{q^2}$

EXAMPLE 2.4.5. (Klein Quartic)
In many papers the Klein Quartic is discussed. It is defined by $f = X^3Y + Y^3 + X$ over $\mathbb{F}_8$.

CHAPTER 3

Function Fields

3.1 Function Fields

We shall study the function fields associated with an algebraic curve in detail. Recall that our definition of a plane curve is specific to a field $\mathbb{F}$ where $\mathbb{F}$ may not be algebraically closed, see Definition 2.2.1.

In this chapter, important and well known theorems with long proofs such as the Riemann-Roch theorem will be stated without proof. The main aim of this chapter is to develop enough theory to facilitate some very explicit contructions of Riemann-Roch spaces.

Previously we denoted the coordinate ring and function field as $\mathbb{K}[C]$ and $\mathbb{K}(C)$ where $\mathbb{K}$ is algebraically closed. In this chapter, we give slightly different definitions that are field specific.

DEFINITION 3.1.1.
The coordinate ring $\mathbb{F}[C]$ of $C : f = 0$ over $\mathbb{F}$ is defined as

$$\mathbb{F}[C] := \mathbb{F}[x, y]/(f)$$

The function field of C, denoted $\mathbb{F}(C)$, is the field of fractions of $\mathbb{F}[C]$. If $g + (f) = h + (f)$, we write $g \equiv h$ or as an abuse of notation $g = h$.

DEFINITION 3.1.2. (Equivalence of Rational Functions)
Given a curve $C : f = 0$, two elements g and h of $\mathbb{F}(C)$, are equivalent if g can be transformed into h using only the relation $f = 0$. If g and h are equivalent, we write $g \equiv h$. As an abuse of notation, sometimes the equal sign is used instead of the equivalence sign.

EXAMPLE 3.1.3.
In the function field of the curve $C : y - x^2 = 0$, the function $y/x \equiv x^2/x = x$.

REMARK 3.1.4.
The above definition applies to both affine and projective plane curves.

DEFINITION 3.1.5. (Local Ring, Maximal Ideal)
Let $f \in \mathbb{F}(C)$. A point $P \in C$ is said to be defined on f if $f \equiv g/h$ where $h(P) \neq 0$ for some

$g, h \in \mathbb{F}[C]$. Reciprocally, such an f is said to be defined at P. The local ring of P denoted $\mathbb{F}[C]_P$, is the ring of functions in $\mathbb{F}(C)$ that are defined at P.

REMARK 3.1.6.
The concept of a local ring of a curve C corresponds exactly to the notion of localizing the coordinate ring at $M_P =: \{f \in \mathbb{F}[C]_P \mid f(P) = 0\}$ i.e. $\mathbb{F}[C]_P = \mathbb{F}[C]_{M_P} := S^{-1}\mathbb{F}[C]$ where $S = \mathbb{F}[C] \setminus M_P$.

DEFINITION 3.1.7. (Non-singular Points, Non-singular Curve)
A point is non-singular if for all $f \in \mathbb{F}(C)$ either $f \in \mathbb{F}[C]_P$ or $1/f \in \mathbb{F}[C]_P$. An affine curve C is non-singular if all the points on C are non-singular.

REMARK 3.1.8.
We will show that the definition of non-singularity given above agrees with other canonical defintions such as the one involving the partial derivatives. The above definition followed $([4], 98)$.

LEMMA 3.1.9.
If we define $f(P)$ to be $a(P)/b(P)$ where $f \equiv a/b$ and $b(P) \neq 0$, then the value of $f(P)$ for $f \in \mathbb{F}[C]_P$ is independent of the presentation of f given that the presentation is defined at P.

PROOF
Suppose $f \equiv a/b \equiv c/d$ where $b(P) \neq 0$ and $d(P) \neq 0$ then $ad \equiv bc \in \mathbb{F}[C]$. If we consider ad and bc as elements of $\mathbb{F}[X, Y, Z]$, then the equivalence above implies that

$$ad = bc + gf$$

for some $g \in \mathbb{F}[X, Y, Z]$. Evaluating at P, we get

$$a(P)d(P) = b(P)c(P) + g(P)f(P)$$

but since $P \in C$, we have $f(P) = 0$ and therefore

$$a(P)d(P) = b(P)c(P)$$

as required. □

LEMMA 3.1.10.
If P is non-singular then $\mathbb{F}[C]_P$ is a local ring with

$$M_P := \{f \in \mathbb{F}[C]_P \mid f(P) = 0\}$$

as the unique maximal ideal.

PROOF
By definition, $\mathbb{F}[C]_P$ is a local ring. Consider the homomorphism

$$\varphi : \mathbb{F}[C]_P \to \mathbb{F}; \quad f \to f(P)$$

which is clearly onto, and M_P is the kernel of φ. By the first isomorphism theorem,

$$\mathbb{F}[C]_P/M_P \cong \mathbb{F}$$

is a field, and thus M_P must be maximal.

Let $f = a/b \in \mathbb{F}[C]_P$ where $b(P) \neq 0$. Supppose $f \notin M_P$. We have $a(P)/b(P) \neq 0$ i.e. $a(P) \neq 0$ and therefore $b(P)/a(P)$ is defined; further, $b/a \notin M_P$ since $b(P) \neq 0$. It is immediate that f is a unit with inverse $b/a \in \mathbb{F}[C]_P$.

Now suppose $f = a/b \in M_P$, then $a(P) = 0$. If $a/b \equiv c/d$ and $d/c \in \mathbb{F}[C]_P$ where $c(P) \neq 0$, then we have

$$0 = a(P)d(P) \equiv b(P)c(P)$$

but $b(P) \neq 0 \Rightarrow c(P) = 0$ which is a contradiction. Therefore $a/b \notin \mathbb{F}[C]_P^*$. We have established that

$$\mathbb{F}[C]_P^* = \mathbb{F}[C]_P \setminus M_P$$

and therefore M_P must be all the non-units. Since every proper ideal is contained in the set of non-units, M_P must be the unique maximal ideal. □

REMARK 3.1.11.
All fields are Noetherian since a field has only two ideals. So $\mathbb{F}$ is Noetherian, which implies that $\mathbb{F}[x_1, x_2, \cdots, x_n]$ is Noetherian by repeated applications of the Hilbert's Basis Theorem. Since there is an obvious onto-homomorphism from $\mathbb{F}[x_1, x_2, \cdots, x_n]$ to $\mathbb{F}[C]$, we see that $\mathbb{F}[C]$ is also Noetherian. Clearly, M_P is a prime ideal since C is defined by an irreducible polynomial. So $\mathbb{F}[C]_P$ is also Noetherian. See $([6], 69)$.

3.2 Discrete Valuation

DEFINITION 3.2.1. (Discrete Valuation Ring (DVR))
A valuation ring of an irreducible curve C is a ring R satisfying

1) $\mathbb{F} \subsetneq R \subsetneq \mathbb{F}(C)$

2) For any $\varphi \in \mathbb{F}(C)$, either $\varphi \in R$ or $1/\varphi \in R$

A discrete valuation ring is a local valuation ring R where the maximal ideal m is principal, together with a valuation function

$$v : R \to \mathbb{N} \cup \{\infty\}$$

such that for all $x, y \in R$, the following are satisfied

$$\begin{aligned} &1) \qquad v(xy) = v(x) + v(y) \\ &2) \qquad v(x) + v(y) \geq \min\{v(x),\ v(y)\} \\ &3) \qquad v(x) = 1 \text{ for some } x \in R \\ &4) \qquad v(0) = \infty \end{aligned}$$

REMARK 3.2.2.
By the above definition, we see that if C is a non-singular curve then every local ring is a valuation ring. In fact, the non-singularity of C implies that every $\mathbb{F}[C]_P$ is a DVR.

DEFINITION 3.2.3. (Uniformizing Parameter)
Suppose $\mathbb{F}[C]_P$ is a DVR. An element $t \in M_P$ is called an uniformizing parameter at P, if every element $z \in \mathbb{F}(C)$ is expressible as $z = ut^n$ for some $u \in \mathbb{F}[C]_P^*$ and $n \in \mathbb{Z}$.

The following lemma closely follows $([5], 69)$ pg 46.

LEMMA 3.2.4.
Suppose the maximal ideal M_P of $\mathbb{F}[C]_P$ is principal. Then there exists $t \in M_P$ such that every non-zero element of $\mathbb{F}[C]_P$ may be uniquely written as ut^n for some $u \in \mathbb{F}[C]_P^*$ and $n \in \mathbb{N}$. Furthermore, $\mathbb{F}[C]_P$ is a DVR with a valuation $v_P(z) = n$ if $z = ut^n$, such that the choice of the uniformizing parameter t does not affect the value of the valuation.

PROOF
By assumption M_P is principal, so we can write $M_P = t\mathbb{F}[C]_P$ for some $t \in M_P$. Suppose $ut^n = vt^m$, where u and v are units and $n \geq m$, then $ut^{n-m} = v$ is a unit. But $t \in M_P$ is not a unit, hence $n = m$, which implies $u = v$. Let $z \in \mathbb{F}[C]_P$. If z is a unit in $\mathbb{F}[C]_P$ then we are done. So suppose $z \in M_P$. We have $z = z_1 t$ for some $z_1 \in \mathbb{F}[C]_P$ since by assumption M_P is principal. If z_1 is a unit we are done, so assume $z_1 = z_2 t$. Continuing in this way, we obtain an infinite sequence $z_1, z_2, \cdots$ where $z_i = z_{i+1}t$. But by Remark 3.1.11, $\mathbb{F}[C]_P$ is Noetherian, therefore the chain

$$(z_1) \subseteq (z_2) \subseteq (z_3) \cdots$$

must have a maximal element. Therefore $(z_n) = (z_{n+1})$ for some n i.e. $vz_n = z_{n+1}$ for some $v \in F[C]_P$, and so $vtz_{n+1} = z_{n+1}$ which yields $vt = 1$. This is a contradiction since we chose t to be a non-unit in $\mathbb{F}[C]_P$. Therefore z_i must have been a unit for some i. Clearly if $z = ut^n$ and we define $v_P(z) = n$, then v_P is a valuation rendering $\mathbb{F}[C]_P$ a DVR.

Suppose s also satisfies $M_P = s\mathbb{F}[C]_P$ then we must have $s = wt$ for some $w \in \mathbb{F}[C]_P^*$. If $z = ut^n = xs^m$ for some $x \in \mathbb{F}[C]_P^*$, then $ut^n = xw^m t^m$. Clearly, we must have $m = n$ since xw^m is a unit. Hence the valuation yields the same value regardless of which uniformizing parameter is chosen. □

There is an obvious extension of the valuation to $\mathbb{F}(C)$.

DEFINITION 3.2.5. (Order, Poles, Zeroes)
Let C be a non-singular affine curve and $P \in C$. Let $f \in \mathbb{F}(C)$, and define the order function at P to be

$$\begin{aligned} \mathrm{ord}_P(f) &:= v_P(f) \quad \text{if } f \in \mathbb{F}[C]_P \\ &:= -v_P(f) \quad \text{if } 1/f \in \mathbb{F}[C]_P \end{aligned}$$

If $\mathrm{ord}_P(f) > 0$ then P is called a zero of order $\mathrm{ord}_P(f)$ of f. On the other hand, if $\mathrm{ord}_P(f) < 0$, then P is called a pole of order $-\mathrm{ord}_P(f)$ of f.

REMARK 3.2.6.
Clearly, $\mathrm{ord}_P(f) > 0$ if and only if $f(P) = 0$, and $\mathrm{ord}_P(f) < 0$ if and only if $f^{-1}(P) = 0$.

LEMMA 3.2.7.
Let $C : f(x, y) = 0$ be an affine curve and let $P = (a, b) \in C$, then $M_P = (x - a, y - b)$.

PROOF
Assume without loss of generality that $P = (0, 0)$, since we can shift the curve C so that P is situated at the origin by letting $P \equiv P' \in C' : f(x' + a, y' + b)$. If $g \in M_P$, then it must be without a constant term since we require $g(P) = 0$, and so $g \equiv xh + yi$ for some $h, i \in \mathbb{F}(C)$. □

REMARK 3.2.8.
It can be noted that Hilbert's Nullstellensatz can also be applied to show that $M_P = (x - a, y - b)$ if $P = (a, b)$ is non-singular. See $([12], 98)$.

THEOREM 3.2.9.
Let $C : f(x, y) = 0$ and let $P = (a, b) \in C$. If $(y - b)/(x - a) \in \mathbb{F}[C]_P$, then $x - a$ is a uniformizing parameter at P and P is non-singular.

PROOF
Assume $P = (0, 0)$. By assumption $y/x \in \mathbb{F}[C]_P$, so we can write

$$\frac{y}{x} = \frac{g}{h} \in \mathbb{F}[C]_P$$

where $g, h \in \mathbb{F}[C]$ and $h(P) \neq 0$. Let

$$n = \max\{i \mid g = x^i g' \text{ where } g' \in \mathbb{F}[C]_P\}$$

and

$$m = \max\{i \mid g = x^n y^i g'' \text{ where } g'' \in \mathbb{F}[C]_P\}$$

so we can write $yh = x^{n+1}y^m g''$. If $m \geq 1$, then we have $y(h - x^{n+1}y^{m-1}g'') = 0$. Assume that $y \neq 0$ (since that defines a trivial curve where $\mathbb{F}[C]$ is the ring of polynomials in x and so x is clearly the uniformizing parameter). We must have $h - x^{n+1}y^{m-1}g'' = 0$, and in particular $h(P) = 0$ which is a contradiction. Therefore $y = x^{n+1}g''/h$. If g'' is a unit in $\mathbb{F}[C]_P$ then we have expressed y in the form of ux^k for some $u \in \mathbb{F}_P^*$, and so x is a uniformizing parameter.

So suppose $g'' \in M_P$. By Lemma 3.2.7, $M_P = \langle x, y \rangle$, so $g'' = xp(x,y) + yq(x,y)$ for some $p(x,y), q(x,y) \in \mathbb{F}[C]$. By our construction of g'', we must have $p(x,y)/y, q(x,y)/x \notin \mathbb{F}[C]_P$, or the maximality of either n or m is contradicted. Rearranging, we obtain

$$\begin{aligned} yh &= x^{n+1}(xp(x,y) + yq(x,y)) \\ y(h - x^{n+1}q(x,y)) &= x^{n+2}p(x,y) \\ y &= x^{n+2}\frac{p(x,y)}{(h - x^{n+1}q(x,y))} \end{aligned}$$

which contradicts the maximality of n and so $g'' \notin M_P$. This shows that x is a uniformizing parameter.

Consider an arbitrary element $g(x,y)/h(x,y) \in \mathbb{F}(C)$, where $g, h \in \mathbb{F}[C] \subseteq \mathbb{F}[C]_P$. Write

$$g(x,y) = x^n g'(x,y) \text{ and } h(x,y) = x^m h'(x,y)$$

where n and m are maximal such that $g', h' \in \mathbb{F}[C]_P$. If $n \geq m$, then $g/h \in \mathbb{F}[C]_P$, otherwise $h/g \in \mathbb{F}[C]_P$. Therefore by definition, P is non-singular, since g/h was arbitrary. □

COROLLARY 3.2.10.
A point P on a curve C is non-singular if and only if $\mathbb{F}[C]_P$ is a DVR. Furthermore, a curve is non-singular if and only if $\mathbb{F}[C]_P$ is a DVR for all $P \in C$.

PROOF
Assume $P = (0,0)$. If P is non-singular then by definition $y/x \in \mathbb{F}[C]_P$ or $x/y \in \mathbb{F}[C]_P$. By the theorem, either x or y is the uniformizing parameter at P. This implies that M_P is principal. Therefore by definiton $\mathbb{F}[C]_P$ is a DVR. Hence we can conclude that a curve is non-singular if and only if P is non-singular for all $P \in C$ if and only if every local ring $\mathbb{F}[C]_P$ if DVR. □

DEFINITION 3.2.11. (Differentiation)
Suppose $f = \sum a_{i,j}x^i y^j \in \mathbb{F}[x,y]$, define $f_x = \sum a_{i,j} i x^{i-1} y^j$, and $f_y = \sum a_{i,j} x^i j y^{j-1}$.

THEOREM 3.2.12.
Let $C : f(x,y) = 0$ be an affine curve and let $P = (a,b) \in C$. We have

$$f_y(P) \neq 0 \text{ if and only if } (y-b)/(x-a) \in \mathbb{F}[C]_P$$

PROOF
Assume P = (0,0). Since $P \in C$, we have $f(P) = 0$, so we can write

$$f(x, y) = cx + dy + x^2 f_1(x) + y^2 f_2(y) + xyf_3(x, y) \tag{3.1}$$

for some $c, d \in \mathbb{F}$ and $f_1, f_2, f_3 \in \mathbb{F}[x, y]$. Clearly $c = f_x(P)$ and $d = f_y(P)$. By assumption $d \neq 0$, rearranging we get

$$y(b + yf_2(y) + xf_3(x, y)) = f(x, y) - x(a - xf_1(x))$$

so we have

$$y/x = \frac{-(a - xf_1(x))}{(b + yf_2(y) + xf_3(x, y))} \in \mathbb{F}(C)$$

since $f \equiv 0$. Clearly, y/x is defined at P since $b \neq 0$.

Conversely, suppose $y/x = g/h \in \mathbb{F}[C]_P$, then we have

$$yh(x, y) = xg(x, y) + k(x, y)f(x, y) \in \mathbb{F}[x, y]$$

for some $k \in \mathbb{F}[x, y]$ where $h(x, y) = c' + h'(x, y)$ for some non-zero $c' \in \mathbb{F}$ and $h' \in \mathbb{F}[x, y]$ since $h(P) \neq 0$. Therefore the left hand side must contain a $c'y$ term. This term must appear in $k(x, y)f(x, y)$ on the right hand side since every term of $xg(x, y)$ must have x as a factor. By comparing with (3.1), we see that $c'y = k(P)dy$ which implies $d = f_y(P) \neq 0$ since $c' \neq 0$. □

COROLLARY 3.2.13.
Let C, P and f be as in the theorem. Then $f_y(P) \neq 0$ implies that $x - a$ is an uniformizing parameter at P, and $f_x(P) \neq 0$ implies that $y - b$ is an uniformizing parameter at P. Furthermore, P is singular if and only if $f_x(P) = 0 = f_y(P)$.

PROOF
If $f_y(P) \neq 0$ then $(y - b)/(x - a) \in \mathbb{F}[C]_P$ which implies that $x - a$ is an uniforming parameter. Assume $P = (0, 0)$. By the theorem, $f_y(P) \neq 0$ if and only if $y/x \in F[C]_P$. The contrapositive gives $f_y(P) = 0$ if and only if $y/x \notin F[C]_P$. Similarly, $f_x(P) = 0$ if and only if $x/y \notin F[C]_P$. Therefore, $f_x(P) = 0 = f_y(P)$ if and only if $y/x, x/y \notin F[C]_P$. By definition, P is singular. □

3.2.1 Some Explicit Determination of Singularities and Valuations

EXAMPLE 1 (PARABOLA)
Consider the irreducible affine plane curve $C : f = y - x^2 = 0$. Differentiating with respect to y give

$$\frac{\partial f}{\partial y} = 1 \neq 0$$

so this curve is non-singular by Corollary 3.2.13. Let $P = (0, 0)$ then x is the uniformizing parameter in $\mathbb{F}[C]_P$ and $v_P(x) = 1$. Therefore $v_P(x^m) = mv_P(x) = m$. Let $Q = (1, 1)$, then $x-1$ is a uniformizing

parameter in $\mathbb{F}[C]_Q$, and $0 = f = y - 1 + 1 - x^2 = y - 1 + (1 - x)(1 + x)$, from this we can deduce that, $y - 1 = -(1 - x)(1 + x) = (x - 1)(x + 1)$. When working over a field of characteristic two $v_Q(y - 1) = 2$, otherwise $v_Q(y - 1) = 1$.

EXAMPLE 2 ($f = y^2 - x^3$)
Differentiating with repsect to y then x and equating the derivatives to zero,

$$\frac{\partial f}{\partial y} = 2y = \frac{\partial f}{\partial x} = 3x^2 = 0$$

We see that any singular point must satisfy $x = 0 = y$, and so $P = (0, 0)$ is the only singular point. Let $Q = (1, -1)$, then $y + 1$ is a uniformizing parameter over fields of characteristic 2, while $x - 1$ is not as $f_y(Q) = 0$.

EXAMPLE 3 (HERMITIAN CURVE)
Consider the Hermitian Curve $C : f = x^5 + y^5 + 1$ defined over $\mathbb{F}_{16}$. It is non-singular, since

$$\frac{\partial f(x, y)}{\partial x} = 5x^4 = 5y^4 = \frac{\partial f(x, y)}{\partial y} = 0$$

is true if and only if $x = y = 0$, but $f(0, 0) \neq 0$. Let $Q = (0, 1)$, then x is a uniformizing parameter at Q. Consider $y + 1 = x^5/(1 + y + y^2 + y^3 + y^4)$. Clearly $1/(1 + y + y^2 + y^3 + y^4)$ is a unit in $\mathbb{F}[C]_P$, and so $v_Q(y + 1) = 5$.

3.3 Divisors and Riemann Roch Spaces

In this section, we shift our focus to non-singular plane projective curves.

DEFINITION 3.3.1. (Non-singular Plane Projective Curve)
Let $C : f(X, Y, Z) = 0$ be a plane projective curve. A point $P \in C$ is singular if

$$\frac{\partial f}{\partial X}(P) = \frac{\partial f}{\partial Y}(P) = \frac{\partial f}{\partial Z}(P) = 0$$

A plane projective curve is non-singular if all the $P \in C$ are non-singular.

REMARK 3.3.2.
It can also be shown that the projective curve C is non-singular if and only if the affine plane curves defined by $f(x, y, 1)$, $f(x_y, 1, z_y)$ and $f(1, y_x, z_x)$ are non-singular.

REMARK 3.3.3.
The above remark was made in view of the fact that a projective curve may be viewed as the union of three patches of affine curves. The three patches correspond to the affine curves given by setting $Z = 1$, $Y = 1$ and $X = 1$ in f. This approach reduces the problem of determining the valuation of non-singular points to the affine case where the theory was sufficiently developed in the last section. It

is an easy consequence that if C is non-singular then the three affine patches must also be non-singular, see $([12], 98)$.

DEFINITION 3.3.4. (Order)
Let $C : f = 0$ be a plane projective curve. Without loss of generality, let $P = [a : b : 1] \in C$ be non-singular. Let $g \in \mathbb{F}(C)$, define

$$\mathrm{ord}_P(g) := \mathrm{ord}_{(a,b)}(g(x, y, 1))$$

where $\mathrm{ord}_{(a,b)}$ is the order function defined on the point $(a, b) \in C' : f(x, y, 1) = 0$

REMARK 3.3.5.
Since $g = h/h'$ and $\deg h = \deg h'$, we have $g(X, Y, Z) = g(X/Z, Y/Z, 1)$. So if we define $x = X/Z$ and $y = Y/Z$ then $g(x, y, 1) = g(X, Y, Z)$. Therefore a uniformizing parameter in $C' : f(x, y, 1)$ with respect to the local ring $\mathbb{F}(C')_{(a,b)}$ is a uniformizing parameter in $\mathbb{F}[C]_P$. We saw that if s and t are both uniformizing parameters then $s = tu$ for some unit u in $\mathbb{F}[C]_P$, so the value of $\mathrm{ord}_P(g)$ does not depend on which variable we set to 1.

EXAMPLE 3.3.6.
Consider the curve $C : YZ - X^2 = 0$ defined over $\mathbb{F}_2$. Consider $P = [1 : 1 : 1] \in C$. Setting $Z = 1$, we have

$$\mathrm{ord}_P((X - Z)/Z) = \mathrm{ord}_{(1,1)}(X - 1) = 1$$

and setting $X = 1$ gives

$$\mathrm{ord}_{(1,1)}((1 - Z)/Z) = \mathrm{ord}_{(1,1)}(1 - Z) - \mathrm{ord}_{(1,1)}(Z) = 1 - 0 = 1$$

We simplify our presentation a little by considering only rational points. It can be noted that any point on a curve can be regarded as a rational point if we enlarge the field on which the curve is defined to an appropriate degree.

DEFINITION 3.3.7. (Rational Divisor, Effective divisor, Degree, Support)
The set of divisors of C is the free abelian additive group generated by the set of rational points $P \in C$. If $D = \sum_{P \in C} D_P P$ for $D_P \in \mathbb{Z}$ is divisor such that $D_P \geq 0$ for all rational points $P \in C$, then D is called effective. The degree of a divisor is $d(D) := \sum_{P \in C} D_P$. The support of D is

$$\mathrm{supp}(D) := \{P \mid D_P \neq 0\}$$

REMARK 3.3.8.
By definition of a free group, if $D = \sum_{P \in C} D_P P$ for $D_P \in \mathbb{Z}$ then only a finite number of the D_P's are non-zero.

DEFINITION 3.3.9. (Riemann-Roch space)
Let $D = \sum_{P \in C} D_P P$ be a divisor. The Riemann-Roch space of D, denoted $L(D)$, is the vector space

$$L(D) := \{f \in \mathbb{F}(C) \mid \mathrm{ord}_P(f) + D_P \geq 0 \quad \text{for all } P \in C\}$$

The dimension of $L(D)$ is denoted $l(D)$.

REMARK 3.3.10.
Recall that $\mathrm{ord}_P(0) = v_P(0) = \infty$ for all $P \in C$ and therefore $0 \in L(D)$ for all D. Clearly, if D is not effective then $L(D) = \{0\}$ which gives $l(D) = 0$.

Recall the Riemann-Roch theorem stated below without proof. For a complete proof of theorem, see $([4], 98)$ p125-p140.

THEOREM 3.3.11.
Let C be a non-singular projective curve. There is an integer $g \geq 0$ called the genus of C, such that for any divisor D the $\mathbb{F}$-vector space $L(D)$ is finite dimensional, and

$$l(D) - l(K_C - D) = d(D) + 1 - g$$

for some divisor K_C known as the canonical divisor of C.

COROLLARY 3.3.12.
The canonical divisor satisfies $d(K_C) = 2g - 2$ and $l(K_C) = g$.

PROOF
Firstly, $L(0P) = L(0)$ the vector space whose members do not have a pole or zero, clearly $L(0)$ must be the constants, so $l(0P) = 1$. Setting $D = 0$, we get

$$l(0) - l(K_C) = 1 - g$$

which yields $l(K_C) = g$. Setting $D = K_C$, we get

$$\begin{aligned} l(K_C) - l(K_C - K_C) &= d(K_C) + 1 - g \\ l(K_C) - 1 &= d(K_C) + 1 - g \\ l(K_C) &= d(K_C) + 2 - g \end{aligned}$$

which yields $d(K_C) = 2g - 2$. □

REMARK 3.3.13.
If $d(D) \geq 2g - 1$, then $K_C - D$ is not effective and so $l(K_C - D) = 0$. Hence, we can deduce that

$$l(D) = d(D) + 1 - g$$

if $d(D) \geq 2g - 1$.

COROLLARY 3.3.14.
Let C be a non-singular curve defined over $\mathbb{F}$. Let $P \in C$ be a rational point. We have

$$l(D) \leq l(D + P) \leq l(D) + 1$$

for any divisor D.

PROOF
Omitted see $([4], 98)$ p44. □

THEOREM 3.3.15. (Degree theorem)
Let C be a non-singular projective curve. Let $f \in \mathbb{F}(C)$, then $\mathrm{ord}_P(f) \neq 0$ for only a finite number of $P \in C$. Moreover,

$$\sum_{P \in C} \mathrm{ord}_P(f) = 0$$

PROOF
Omitted. See $([4], 98)$ p119. □

DEFINITION 3.3.16. (Principal Divisor)
Let $f \in \mathbb{F}(C)$ be non-zero. The principal divisor of f denoted (f), is defined to be

$$(f) := \sum_{P \in C} \mathrm{ord}_P(f) P$$

REMARK 3.3.17.
The definition of Riemann-Roch spaces can be restated using principal divisors. We have

$$L(D) = \{f \in \mathbb{F}(C) \mid (f) + D \geq 0\}$$

REMARK 3.3.18.
By the degree theorem, $d((f)) = 0$.

As mentioned in $([4], 98)$, the exact value of $l(D)$ is difficult to calculate, so the following theorem is useful.

THEOREM 3.3.19. (Plucker)
If $C : f = 0$ is a non-singular irreducible plane projective curve then the genus g of C is given by the formula

$$g = \frac{(d-1)(d-2)}{2}$$

where $d = \deg(f)$

PROOF
Omitted. See $([4], 98)$ p171. □

REMARK 3.3.20.
We will see that the Riemann-Roch theorem allows us to estimate the various parameters of algebraic geometric codes, and that is why we study the theorem.

3.4 Some Explicit Constructions of Riemann-Roch Spaces

EXAMPLE 1 (PARABOLA)
Consider the non-singular plane projective curve $C : f = YZ - X^2 = 0$. There is only one point $Q = [0 : 1 : 0]$ at infinity. Consider the order of $Z/X \in \mathbb{F}[C]$ at Q. Let $x_y = X/Y$ and $z_y = Z/Y$, we get $f(x_y, 1, z_y) = z_y - x_y^2$, and

$$\frac{\partial f}{\partial z_y} = 1 \neq 0$$

so x_y is the uniformizing parameter of $\mathbb{F}[C]_P$ for all $P \in C$. We have $z_y/x_y = x_y^2/x_y = x_y$. So $\mathrm{ord}_Q(z_y/x_y) = \mathrm{ord}_Q(Z/X) = 1 \Rightarrow \mathrm{ord}_Q(X/Z) = -1$. The only poles of X/Z must have $Z = 0$, but Q is the only point with $Z = 0$, therefore $L(mQ)$ has basis $\{1, x, x^2, \cdots, x^m\}$, where $x = X/Z$.

EXAMPLE 2 (HERMITIAN CURVE FORM 2)
Consider $C : f = X^5 + Y^4Z + YZ^4$ over $\mathbb{F}_{16}$. It is non-singular, since equating the partial derivatives gives

$$5X^4 = 4Y^3Z + Z^4 = Y^4 + Z^3Y$$

which simplifies to

$$X^4 = Z^4 = Y^4 + Z^3Y$$

Any singular point must satisfy $X = 0 = Z = Y$. So there is no singular point. Let $Q = [0 : 1 : 0]$ be the sole point at infinity. Let $x_y = X/Y$ and $z_y = Z/Y$, and consider the plane affine curve defined by $f(x_y, 1, z_y)$. Differentiating shows that x_y is a uniformization parameter, so $\mathrm{ord}_Q(x_y) = 1$. We have

$$\begin{aligned} x_y^5 + z_y^4 + z_y &= 0 \\ z_y^4 + z_y &= x_y^5 \\ z_y(z_y^3 + 1) &= x_y^5 \\ z_y &= \frac{x_y^5}{(z_y^3 + 1)} \end{aligned}$$

We see that $1/(z_y^3 + 1)(0, 0) = 1$ i.e. $1/(z_y^3 + 1) \in \mathbb{F}[C]_P^*$. Therefore

$$\mathrm{ord}_Q(z_y) = \mathrm{ord}_Q(\frac{x_y^5}{(z_y^3 + 1)}) = 5\mathrm{ord}_Q(x_y) = 5$$

We can deduce

$$\mathrm{ord}_Q(Y/Z) = \mathrm{ord}_Q(1/z_y) = -5$$

and similarly

$$\mathrm{ord}_Q(X/Z) = \mathrm{ord}_Q(x_y/z_y) = \mathrm{ord}_Q(x_y) - \mathrm{ord}_Q(z_y) = 1 - 5 = -4$$

By Plucker's formula, the curve has genus $g = 6$ and so $L(11Q) = 11+1-6 = 6$. Since both $x := X/Z$ and $y := Y/Z$ can only have poles at Q. Clearly we must have $L(11Q) = \langle 1, x, y, x^2, xy, y^2\rangle$.

EXAMPLE 3 (GENERAL HERMITIAN CURVE)
More generally, for a q-Hermitian Curve, we have $\mathrm{ord}_Q(x) = -q$ and $\mathrm{ord}_Q(y) = -(q+1)$ where Q is the point at infinity and $x = X/Z$ and $y = Y/Z$.

REMARK 3.4.1.
In fact, it is well known that $L(mQ)$ for any $m \in \mathbb{N}$ can be written as a polynomial in x and y. Let g be the genus of the q-Hermitian Curve. It has been shown that every natural number larger than $2g-2$ can be expressed as $qa + (q+1)b$ for some $a, b \in \mathbb{N}$. This is due to the fact that $[q, q+1]$ is so called a telescopic sequence. See $([13], 95)$.

EXAMPLE 3.1 (HERMITIAN CURVE)
Consider the Hermitian Curve $C : f = X^5 + Y^5 + Z^5$ defined over $\mathbb{F}_{16}$. It is non-singular. Let $Q = [0 : 1 : 1]$. Consider $g := f(x, y, 1) = x^5 + y^5 + 1$. We have $\frac{\partial g}{\partial y}(0, 1) = 5y^4(0, 1) = 5 \neq 0$, and so x is a uniformizing parameter at Q. It can be shown that

$$\mathrm{ord}_Q \frac{x^i y^j}{(y+1)^{i+j}} = -(4i + 5j)$$

and

$$L(11Q) = \langle 1, x/(y+1), y/(y+1), x^2/(y+1)^2, xy/(y+1)^2, y^2/(y+1)^2\rangle$$

REMARK 3.4.2.
It can seen that the second form of the Hermitian Curve is more convenient to use since $L(mQ)$ where Q is the point at infinity, can be constructed using monomials in x, y instead of the more complicated functions as shown above,

EXAMPLE 4 (KLEIN QUARTIC)
The point $Q = [0 : 0 : 1]$ lies on the Klein quartic over $\mathbb{F}_4$. It can be shown that $\mathrm{ord}_Q(y^i/x^j) = 3j - i$ and that $L(mQ)$ for any m can constructed using only those elements.

CHAPTER 4

Algebraic Geometric Codes

4.1 Introduction

The class of codes now known as Algebraic Geometric Codes (AG-codes) was first described by Goppa in $([16], 81)$. For that reason, AG-codes are also known as Goppa codes. Goppa's insight was that a code can be constructed by evaluating functions belonging to a Riemann-Roch space on a set of rational points.

Recall that $L(D)$ is a $\mathbb{F}$-vector space for any rational divisor D on a curve defined over $\mathbb{F}$. Recall also that a linear code is simply a vector subspace of $\mathbb{F}^n$ for some positive integer n. But $L(D)$ is a vector space of functions, so it is not immediately a code. In this chapter, we show how the linear property of the Riemann-Roch spaces can be exploited to construct linear codes. Furthermore, the Riemann-Roch theorem is used to determine the ranks and (designed) minimum distances of these codes. This highlights the importance of the Riemann-Roch theorem to the theory of AG-codes, since the problem of determining the minimum distances for linear codes is NP-Complete.

4.2 Function Codes

DEFINITION 4.2.1. (Function Code)
Let C be a non-singular projective curve. Let P_i for $i = 1, 2, ...n$ be n distinct rational points on C. Let

$$B = P_1 + P_2 + \cdots + P_n$$

and let D be a divisor with support disjoint from the support of B, i.e.

$$\text{supp}(D) \cap \{P_i \mid i = 1, 2, \ldots n\} = \varnothing$$

The function code of B and D, denoted $C_L(B, D)$, is the image of the following evaluation map

$$ev : L(D) \to \mathbb{F}^n; \qquad f \longmapsto (f(P_1), f(P_2), \ldots, f(P_n))$$

that is

$$C_L(B, D) = \{(f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in L(D)\}$$

REMARK 4.2.2.
The requirement that the support of D is disjoint from the support of B is necessary and practical. Suppose $\mathrm{supp}(D') \cap \mathrm{supp}(B) = \emptyset$ and $m \in \mathbb{N} \setminus \{0\}$. If $D = D' + mP_i$, then a function in $L(D)$ may have a pole at P_i, then $f(P_i)$ is not defined. On the hand if $D = D' - mP_i$ then any function in $L(D)$ will evaluate to zero at P_i. So every codeword in $C_L(B, D)$ has a zero at position i, so we can delete that position and not affect the code's minimum distance at all! Therefore $\mathrm{supp}(D) \cap \mathrm{supp}(B) = \varnothing$ is a sensible requirement.

REMARK 4.2.3.
The code $C_L(B, D)$ is clearly linear since $L(D)$ is a vector space.

LEMMA 4.2.4.
The function code $C_L(B, D)$ is a linear code of length $n = d(B)$, rank $m = l(D) - l(D - B)$ and minimum distance $d \geq n - d(D)$

PROOF
Clearly, since the points of B are rational, the length of the code n is the same as the degree of B. We can prove $m = l(D) - l(D - B)$ via a simple application of the first isomorphism theorem for vector spaces. We know that $C_L(B, D) = \mathrm{im}(ev)$, so

$$m := \dim C_L(B, D) = \dim \mathrm{im}(ev) = \dim L(D) - \dim \ker(ev)$$

By definition $l(D) := \dim L(D)$, so it remains to find $\dim \ker(ev)$. It is clear that $f \in \ker(ev)$ if and only if $f(P_i) = 0$ for $i = 1, 2, \ldots, n$, therefore $\mathrm{ord}_{P_i}(f) \geq 1$. So $(f) - \sum_{i=1}^{n} P_i \geq 0$. Since $f \in L(D)$ and f has a zero at each of the P_i's, we can deduce that $f \in L(D - \sum P_i) = L(D - B)$. Hence $\ker(ev) = L(D - B)$, and so $\dim \ker(ev) = l(D - B)$.

Suppose $(f(P_1), f(P_2), \ldots, f(P_n))$ is a codeword of minimum weight in $C_L(B, D)$, i.e. $f(P_i) \neq 0$ for exactly d distinct values of i, then there exists $n - d$ distinct values $\{i_1, i_2, \ldots, i_{n-d}\}$ such that $f(P_{i_j}) = 0$ for $j = 1, 2, \ldots, n - d$. By a similar argument as above $f \in L(D - \sum_{j=1}^{n-d} P_{i_j})$. Therefore

$$(f) + D - \sum_{j=1}^{n-d} P_{i_j} \geq 0$$

taking degrees of both sides we obtain

$$d(D) - (n - d) \geq 0$$

since $\deg((f)) = 0$, which yields $d \geq n - d(D)$ as required. □

4.3 Residue codes

DEFINITION 4.3.1. (Residue Code)
Let B and D be as before. The residue code $C_\Omega(B, D)$, is the dual code of the function code $C_L(B, D)$. We have

$$C_\Omega(B, D) := \{ (f_1, f_2, \ldots, f_n) \in \mathbb{F}^n \mid \sum_{i=1}^{n} f_i \varphi(P_i) = 0 \text{ for all } \varphi \in L(D)\}$$

REMARK 4.3.2.
Since we did not develop the theory of differentials necessary for an proper account of the construction of $C_\Omega(B, D)$, we resort to the above definition. It can be noted that the canonical construction of $C_\Omega(B, D)$ does not play a part in the description of the theory covered in this thesis. For an account of a more canonical construction of $C_\Omega(B, D)$ we refer the reader to ([4], 98) p138 and ([8], 99) p245.

LEMMA 4.3.3.
The residue code $C_\Omega(B, D)$ is a linear code of length $n = d(B)$, rank $m = n - l(D) + l(D - B)$ and minimum distance $d \geq d(D) - (2g - 2)$ where g is the genus of C.

PROOF
As before $n = d(B)$ is clear. Since $C_\Omega(B, D)$ is the dual of $C_L(B, D)$, we have

$$\dim C_\Omega(B, D) + \dim C_L(B, D) = n \tag{4.1}$$

By Lemma 4.2.4, $\dim C_L(B, D) = l(D) - l(D - B)$. Using (4.1) and we obtain the required result.

For the minimum distance, it is clear that if $d(D) \leq 2g - 2$ then the lemma does not improve upon the obvious bound $d \geq 0$. So assume $d(D) > 2g - 2$. For a contradiction, suppose $d < d(D) - (2g - 2)$. Let $c = (c_1, c_2, \ldots, c_n) \in C_\Omega(B, D)$ be a word of minimum weight. Consider of indices of c where $c_i \neq 0$. We denote it

$$C_0 := \{i \mid c_i \neq 0\}$$

Clearly, $|C_0| = d$, so we have

$$|C_0| = d(\sum_{i \in C_0} P_i) < d(D) - (2g - 2)$$

which yields

$$d(D - \sum_{i \in C_0} P_i) > 2g - 2$$

By Riemann-Roch we have

$$l(D - \sum_{i \in C_0} P_i) = d(D) - d + 1 - g$$

Let $j \in C_0$, then we have

$$l(D - \sum_{i \in C_0} P_i + P_j) = d(D) - (d-1) + 1 - g > l(D - \sum_{i \in C_0} P_i)$$

So there exists $\varphi \in L(D - \sum_{i \in C_0} P_i + P_j)$ but $\varphi \notin L(D - \sum_{i \in C_0} P_i)$. Since $P_i \in \mathrm{supp}(B)$ and $P_i \notin \mathrm{supp}(D)$, we must have $\mathrm{ord}_{P_i}(\varphi) \geq 1$ for $i \neq j$, implying that $\varphi(P_i) = 0$ for $i \neq j$. Similarly since $\mathrm{ord}_{P_j}(\varphi) < 0$, we must have $\varphi(P_j) \neq 0$. By $D - \sum_{i \in c_0} P_i \leq D$, we have $\varphi \in L(D)$, and by the definition of $C_\Omega(B, D)$ we have

$$c_1\varphi(P_1) + c_2\varphi(P_2) + \cdots + c_n\varphi(P_n) = 0$$

If $i \in C_0$ then $\varphi(P_i) = 0$ and if $i \notin C_0$ then $c_i = 0$, so the above equation reduces to $c_j\varphi(P_j) = 0$. But $j \in C_0$ which implies $c_j \neq 0$, and this is a contradiction, since $\varphi(P_j) \neq 0$. Therefore we must have $d \geq d(D) - (2g-2)$ if $d(D) > 2g - 2$. □

COROLLARY 4.3.4.
Suppose $d(D) > 2g - 2$. The residue code $C_\Omega(B, D)$ has rank $m = n - d(D) + g - 1 + l(D - B)$.

PROOF
By Riemann-Roch, $l(D) = d(D) + 1 - g$ if $d(D) > 2g - 2$. Substitute into the equation in the above lemma. □

DEFINITION 4.3.5. (Designed Minimum Distance, Minimum distance)
The designed minimum distance of $C_\Omega(B, D)$ is defined to be $d^* := d(D) - (2g - 2)$. We sometimes denote d^* as $d^*(C_\Omega(B, D))$ to emphasise that the code is $C_\Omega(B, D)$. Define $t^* := \lfloor \frac{d^*-1}{2} \rfloor$. Let $d(C_\Omega(B, D))$ denote the true minimum distance of $C_\Omega(B, D)$.

REMARK 4.3.6.
The designed minimum distance is only useful if $d(D) > 2g - 2$.

4.4 Examples of AG-codes

Recall that the generator matrix or parity check matrix uniquely determines a linear code. We shall construct the parity check matrices for some residue codes. Note that $C_\Omega(B, D)$ is the dual code of $C_L(B, D)$ and so the generator matrix of $C_L(B, D)$ is the parity check matrix of $C_\Omega(B, D)$.

EXAMPLE 4.4.1. (Parabola)
Consider $C : f = YZ - X^2 = 0$ over $\mathbb{F}_7$. This curve is non-singular with genus 0 and its rational points are $P_i = [i : i^2 : 1]$ for $i = 0, 1, \cdots, 6$ and $Q = [0 : 1 : 0]$. Let $x = X/Z$ and recall that $L(mQ)$ is the vector space spanned by x^i for $i = 0, 1, 2, \cdots, m$. Let

$$B = P_0 + P_1 + \cdots + P_6$$

then the parity check matrix for $C_\Omega(B, mQ)$ is

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ x(P_0) & x(P_1) & x(P_2) & \cdots & x(P_6) \\ x^2(P_0) & x^2(P_1) & x^2(P_2) & \cdots & x^2(P_6) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x^m(P_0) & x^m(P_1) & x^m(P_2) & \cdots & x^m(P_6) \end{pmatrix}$$

which evaluates to

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & 6 \\ 0 & 1 & 2^2 & \cdots & 6^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 2^m & \cdots & 6^m \end{pmatrix}$$

Of course the value of m cannot be too large. Since by Corollary 4.3.4, the rank of $C_\Omega(B, D)$ is $d(B) - m + 0 - 1 + l(mQ - B) = 6 - m$. We have $d^*(C_\Omega(B, mQ)) = m - (2g - 2) = m + 2$. Consider $m = 3$, this code has $d^* = 5$ and so it can correct (at least) 2 errors.

EXAMPLE 4.4.2.

Consider the 2-Hermitian Curve form 2 defined by $f = X^3 + Y^2Z + YZ^2$. It is non-singular with genus 1. It has 9 rational points and one point at infinity, $Q = [0 : 1 : 0]$. Consider $C_\Omega(B, aQ)$ where B is the sum of all the rational points except Q. The code has designed minimum distance $d^* = a - (2g - 2) = a$. So letting $a = 5$ will allow the correction of 2 errors. The codes has rank $8 - a + 1 - 1 = 8 - a = 3$ if $a = 5$. We have $L(5Q) = \langle 1, x, y, x^2, xy \rangle$. Define $\mathbb{F}_4 := \mathbb{F}_2[w]$ where $w^2 + w + 1 = 0$. Let

$$P_1 = [0 : 0 : 1] \quad P_2 = [0 : 1 : 1] \quad P_3 = [1 : w : 1] \quad P_4 = [1 : w^2 : 1]$$

$$P_5 = [w : w : 1] \quad P_6 = [w : w^2 : 1] \quad P_7 = [w^2 : w : 1] \quad P_8 = [w^2 : w^2 : 1]$$

The code $C_\Omega(B, 5Q)$ has parity check matrix.

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x(P_1) & x(P_2) & \cdots & x(P_8) \\ y(P_1) & y(P_2) & \cdots & y(P_8) \\ x^2(P_1) & x^2(P_2) & \cdots & x^2(P_8) \\ xy(P_1) & xy(P_2) & \cdots & xy(P_8) \end{pmatrix}$$

which evaluates to

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & w & w & w^2 & w^2 \\ 0 & 1 & w & w^2 & w & w^2 & w & w^2 \\ 0 & 0 & 1 & 1 & w^2 & w^2 & w & w \\ 0 & 0 & w & w^2 & w^2 & 1 & 1 & w \end{pmatrix}$$

4.5 The Number of Rational Points on an Algebraic Curve

We state without proof a bound on the number of rational points on a curve in relation to the genus.

THEOREM 4.5.1. (Serre's Bound)
Let C be a non-singular projective curve defined over $\mathbb{F}_q$. Let N be the number of rational points in C, then

$$|N - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor$$

where g is the genus of C.

REMARK 4.5.2.
It can easily be verified that the Hermitian curves and the Klein Quartic all attain the upper bound. Hence, they are known as maximal curves. We saw that the number of rational points on a curve determines the maximum length of the Algebraic Geometrice codes it can define. Therefore it is more efficient to use maximal curves.

CHAPTER 5

Basic Decoding Algorithm

5.1 Introduction

5.1.1 Preliminaries

Ever since the discovery of the AG codes, researchers have tried to design practical algorithms for the decoding problem. Skorobogatov and Vladut's 1990 paper $([14], 90)$ introduced the notion of an error-locator and utilized it to design the first practical decoding algorithm. An error-locator, to be defined more precisely below, is a function that narrows down the possible locations of the errors. Once an error-locator has been found, the error word can be determined precisely in polynomial time by solving a linear system. This procedure is known as the SV-Algorithm. Unfortunately, sometimes an error-locator may be impossible to compute using the method covered in this chapter. Therefore, the algorithm can only correct up $t^* - g/2$ errors, where $t^* = \lfloor \frac{d^*-1}{2} \rfloor$ and d^* is the designed minimum distance. However, in $([2], 93)$ Feng and Rao developed an algorithm that corrected the serious defect for One-Point codes. Their algorithm was soon generalised by Duursma in $([15], 93)$. In this chapter we will present the SV-algorithm in such a way that it paves the way for a complete description of the more advanced algorithm with mimimal modification.

Assumptions
Throughout, let C be a non-singular projective curve of genus g. Let $B := \sum_{i=1}^{n} P_i$ where $P_i \in C$ are distinct rational points. We also let D be an arbitrary divisor with $\mathrm{supp}(D) \cap \mathrm{supp}(B) = \varnothing$ and $d(D) = 2g + 2t^* - 1$ for some $t^* \in \mathbb{N}$ so $d^*(C_\Omega(B, D)) = 2t^* + 1$.

5.2 Error Locators

DEFINITION 5.2.1. (Vector Syndrome, Syndrome)
Let $\varphi, \phi \in L(D)$. Define the vector syndrome of φ and any vector $r = (r_1, r_2, \ldots, r_n) \in \mathbb{F}^n$ to be

$$(\varphi \times r)_B := (\varphi(P_1)r_1, \varphi(P_2)r_2, \ldots, \varphi(P_n)r_n)$$

A syndrome is defined to be

$$(\varphi \cdot r)_B := \varphi(P_1)r_1 + \varphi(P_2)r_2 + \ldots + \varphi(P_n)r_n$$

When there is no confusion as to the composition of B, we simply drop the subscript to make the notation nicer.

REMARK 5.2.2.
The definition of $C_\Omega(B, D)$ can be restated using syndromes. We have

$$C_\Omega(B, D) = \{c \in C \mid \varphi \cdot c = 0 \quad \text{for all } \varphi \in L(D)\ \}$$

Clearly the syndromes are bilinear. For example

$$(\varphi + \phi) \cdot (c + e) = \varphi \cdot c + \varphi \cdot e + \phi \cdot c + \phi \cdot e$$

LEMMA 5.2.3. (Syndrome lemma)
Let $r = c + e$ where $c \in C_\Omega(B, D)$ and $e \in \mathbb{F}^n$, then $\varphi \cdot r = \varphi \cdot e$ for all $\varphi \in L(D)$.

PROOF
We have $\varphi \cdot r = \varphi \cdot c + \varphi \cdot e = 0 + \varphi \cdot e = \varphi \cdot e$ □

DEFINITION 5.2.4. (Error Location, Error Locator)
Suppose $e = (e_1, e_2, \ldots, e_n) \in \mathbb{F}^n$. If $e_i \neq 0$ then P_i is called an error location for e. A non-zero function $\varphi \in \mathbb{F}(C)$ is an error locator for e if $\varphi(P_i) = 0$ for all error locations P_i of e.

REMARK 5.2.5.
Notice that we did *not* require $\varphi(P_i) = 0$ only if P_i is an error location.

LEMMA 5.2.6.
If a function $\theta \in \mathbb{F}(C)$ is an error locator of e then $\theta \cdot e = 0$.

PROOF
If θ is an error locator of $e = (e_1, e_2, \cdots, e_n)$ then $e_i \neq 0$ implies $\theta(P_i) = 0$, clearly $\theta \cdot e = 0$ in this case. □

5.2.1 Existence of Error Locator

Before we discuss how to use an error locator to compute e, we first show that one exists. We assume that we know the genus of C and we are able to compute a basis of $L(D)$. Although in practice, the genus of a curve and a basis of $L(D)$ can be extremely difficult to compute.

LEMMA 5.2.7.
Let $e \in \mathbb{F}^n$ with $wt(e) \leq t$ for some $0 \neq t \in \mathbb{N}$. Let A be an arbitrary divisor with support disjoint from the support of B. Suppose $l(A) > t$, then there exists an error locator in $L(A)$ for e.

PROOF
Let $P_e := \{P_i \mid e_i \neq 0\}$ i.e. P_e is the set of error locations of e. Let $\{\phi_i \mid i = 1, 2, \ldots, l(A)\}$ be a basis of $L(A)$. Then

$$\theta = \sum_{j=1}^{l(A)} \alpha_j \phi_j \quad \in L(A)$$

is an error locator if and only if $\theta(P_i) = 0$ for all $P_i \in P_e$. Then finding an error locator θ is equivalent to solving the linear system

$$\theta(P_i) = \sum_{j=1}^{l(A)} \alpha_j \phi_j(P_i) = 0 \quad \text{for } P_i \in P_e$$

we have $l(A)$ unknowns and at most t ($\geq wt(e)$) equations, where $l(A) > t$ by assumption. Therefore there must be a non-zero solution. and that solution corresponds to an error locator. □

THEOREM 5.2.8.
Let A and E be divisors with support disjoint from the support of B, such that

$$d(C_\Omega(B, E)) > d(A) \tag{5.1}$$

Suppose also that $\{\phi_i \mid i = 1, 2, \ldots, l(E)\}$ is a basis for $L(E)$. Let $\theta \in L(A)$ and let

$$I_\theta := \{e \in \mathbb{F}^n \mid \theta \text{ is an error locator of } e\ \}$$

then

$$\begin{aligned} f_\theta : \quad I_\theta &\longrightarrow \{\ (\phi_1 \cdot e,\ \phi_2 \cdot e,\ \cdots,\ \phi_{l(E)} \cdot e) \mid e \in I_\theta\} \\ e &\longmapsto (\phi_1 \cdot e,\ \phi_2 \cdot e,\ \cdots,\ \phi_{l(E)} \cdot e) \end{aligned}$$

is a bijection.

PROOF
The surjective property is clear from the definition. Suppose $e, e' \in I_\theta$ and that $f_\theta(e) = f_\theta(e')$. We have $f_\theta(e) - f_\theta(e') = 0$, i.e. $\phi_i \cdot (e - e') = 0$ for $i = 1, 2, \cdots, l(E)$. But the ϕ_i's form a basis of $L(E)$. Therefore $\phi \cdot (e - e') = 0$ for all $\phi \in L(E)$ and so by definition $(e - e') \in C_\Omega(B, E)$.

If $e - e' \neq 0$ then $wt(e - e') \geq d(C_\Omega(B, E)) > d(A)$ by (5.1). But this cannot be the case since $\theta \in L(A)$ is an error locator for e and e'. Indeed, let $P_\theta = \{P_i \mid \theta(P_i) = 0\ \}$, then we have

$$\theta \in L(A - \sum_{P \in P_\theta} P)$$

therefore

$$L(A - \sum_{P \in P_\theta} P) \neq \varnothing \Rightarrow d(A - \sum_{P \in P_\theta} P) \geq 0$$

from which we can deduce

$$d(A) \geq d(\sum_{P \in P_\theta} P) = |P_\theta| \geq wt(e - e')$$

Hence $wt(e-e') > d(A)$ must be incorrect, therefore $e - e' = 0$ since 0 is the only codeword of weight less than $d(A)$ by definition of minimum distance. This shows that f_θ is injective. □

REMARK 5.2.9.

The task now is to decipher the above theorem and use it to help decode received codewords. The theorem states that if e and e' are both error words with the same error locator $\theta \in L(A)$, then they can be distinguished using some Riemann-Roch space $L(E)$ with $d(C_\Omega(B, E)) > d(A)$. We have

$$e' \neq e \text{ if and only if } \phi \cdot e \neq \phi \cdot e' \text{ for some } \phi \in L(E)$$

Therefore, if we assume that $(\phi_1 \cdot e,\ \phi_2 \cdot e,\ \cdots,\ \phi_{l(E)} \cdot e)$ is known, then it is at least theorectical possible to find e by computing f_θ^{-1}, since we have

$$e = f_\theta^{-1}(\phi_1 \cdot e,\ \phi_2 \cdot e,\ \cdots,\ \phi_{l(E)} \cdot e) \tag{5.2}$$

We will show that solving (5.2) is equivalent to solving a linear system in the following corollary.

COROLLARY 5.2.10.

Let A and E be as in the theorem. Let $e = (e_1, e_2, \cdots, e_n)$ be a vector with error locator $\theta \in L(A)$. Define

$$P_\theta := \{P_i \mid \theta(P_i) = 0\}$$

then we have

$$\phi_i \cdot e = \sum_{P_j \in P_\theta} \phi_i(P_j) e_j$$

for $i = 1, 2, \cdots, l(E)$. Suppose $E \leq D$ then the e_i's are the only unknowns and e is the unique solution of the above linear system.

PROOF

We have

$$\begin{aligned} \phi_i \cdot e &:= \sum_{i=1}^{n} \phi_i(P_j) e_j \\ &= \sum_{P_j \in P_\theta}^{n} \phi_i(P_j) e_j \quad \text{since } e_j = 0 \text{ if } P_j \notin P_\theta \end{aligned}$$

If $E \leq D$ then $L(E) \subseteq L(D)$, which gives $\phi_i \cdot r = \phi_i \cdot e$ by Lemma 5.2.3. So the e_i's are the only unknowns. As in Theorem 5.2.8, the solution is unique. □

REMARK 5.2.11.
Although the above corollary allows us to calculate the error vector given an error locator, we still have not discussed how to find an error locator yet. In fact the SV-Algorithm's biggest weakness is that it is not guaranteed that an error locator can be found for all e with $wt(e) \leq t^*$ given $d^*(C_\Omega(B, D)) = 2t^* + 1$.

5.3 Finding an Error Locator

LEMMA 5.3.1.
Let $e = (e_1, e_2, \cdots, e_n) \in \mathbb{F}^n$ with $wt(e) \leq s$ and let A be a divisor with $\text{supp}(A) \cap \text{supp}(B) = \emptyset$. Then a non-zero $\phi \in L(A)$ is an error locator of e if and only if $\phi \times e = 0$.

PROOF
By definition we have

$$\phi \times e := (\phi(P_1)e_1, \phi(P_2)e_2, \cdots, \phi(P_n)e_n)$$

If ϕ is an error locator of e, then $\phi(P_i) = 0$ if $e_i \neq 0$. In that case, clearly $\phi \times e = 0$. If $\phi \times e = 0$, i.e. $\phi(P_i)e_i = 0$ for all i. Then $e_i \neq 0$ implies $\phi(P_i) = 0$ since we are working over a field. Therefore by definition, ϕ is an error locator of e. □

LEMMA 5.3.2.
Let $e \in \mathbb{F}^n$ with $wt(e) \leq s$ and let Y be a divisor with $\text{supp}(Y) \cap \text{supp}(B) = \emptyset$. If $d(C_\Omega(B, Y)) > s$, then θ is an error locator of e if and only if $\theta\chi \cdot e = 0$ for all $\chi \in L(Y)$.

PROOF
This proof is similar to Theorem 5.2.8. Suppose θ is an error locator of e, then clearly the vector syndrome $\theta \times e = 0$ and so

$$\theta\chi \cdot e = \chi \cdot (\theta \times e) = \chi \cdot 0 = 0$$

Conversely, suppose that $\theta\chi \cdot e = \chi \cdot (\theta \times e) = 0$ for all $\chi \in L(Y)$. We can deduce that $wt(\theta \times e) \leq s$ since $wt(e) \leq s$. Now $\theta\chi \cdot e = \chi \cdot (\theta \times e) = 0$ for all $\chi \in L(Y)$ then by definition $\theta \times e \in C_\Omega(B, Y)$. But $C_\Omega(B, Y)$ has minimum distance greater than s. Therefore $\theta \times e = 0$, and so ϕ is an error locator as required. □

From the above lemma we can derive the following practical result.

COROLLARY 5.3.3.
Let A be an arbitrary divisor with $\text{supp}(A) \cap \text{supp}(B) = \varnothing$ and $l(A) = s + 1$ with basis φ_i for $i = 1, 2, \cdots, s + 1$ and let $e \in \mathbb{F}^n$ with $wt(e) \leq s$. Let Y be as in the lemma and assume that

$\chi_i \in L(Y)$ for $i = 1, 2, \cdots, l(Y)$ form a basis of $L(Y)$. Let α_i for $i = 1, 2, \cdots, s+1$, not all zero, satisfy,

$$\sum_{i=1}^{s+1} \alpha_i \varphi_i \chi_j \cdot e = 0 \quad \text{for } j = 1, 2, \cdots, l(Y)$$

that is if the α_i's satisfy

$$\begin{pmatrix} \chi_1\varphi_1 \cdot e & \chi_1\varphi_2 \cdot e & \cdots & \chi_1\varphi_{s+1} \cdot e \\ \chi_2\varphi_1 \cdot e & \chi_2\varphi_2 \cdot e & \cdots & \chi_2\varphi_{s+1} \cdot e \\ \vdots & \vdots & \ddots & \vdots \\ \chi_{l(Y)}\varphi_1 \cdot e & \chi_{l(Y)}\varphi_2 \cdot e & \cdots & \chi_{l(Y)}\varphi_{s+1} \cdot e \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{s+1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{5.3}$$

then

$$\theta = \alpha_1\varphi_1 + \alpha_2\varphi_2 + \cdots + \alpha_{s+1}\varphi_{s+1}$$

is an error locator of e.

REMARK 5.3.4.
Since an error locator exists in $L(A)$ if $l(A) > s$, clearly we can also choose $l(A)$ to be bigger than $s+1$, but there is no need.

PROOF
If $\theta = \sum_{i=1}^{s+1} \alpha_i\varphi_i \in L(A)$ satisfies the above condition for α_i's in $\mathbb{F}$, then we have

$$\begin{aligned} 0 &= \sum_{i=1}^{s+1} \alpha_i \varphi_i \chi_j \cdot e \quad \text{for } j = 1, 2, \cdots, l(Y) \\ &= (\sum_{i=1}^{s+1} \alpha_i \varphi_i)\chi_j \cdot e \\ &= \theta\chi_j \cdot e \quad \text{for } j = 1, 2, \cdots, l(Y) \end{aligned}$$

but the χ_j's form a basis for $L(Y)$, so $\theta\chi \cdot e = 0$ for all $\chi \in L(Y)$ since the one dimensional syndrome is (bi)linear. Hence by the theorem, θ is an error locator. □

Unfortunately, our good fortune in terms of decoding success ends here. It is an easy consequence that if we choose s to be big enough, then not all the required syndromes $\varphi_i\chi_j \cdot e$ are computable via Lemma 5.2.3. If the syndromes are not always computable, then we can not solve (5.3). Therefore we may not be able to compute error locators for all error words of weight less than t^* given $d^*(C_\Omega(B, D)) = 2t^* + 1$. We shall investigate what is the biggest value of s such that all errors of of weight less than s are correctable.

Firstly we have $l(A) \geq d(A) + 1 - g$ by Riemann-Roch. To guarantee that $l(A) \geq s + 1$, we require

$$d(A) \geq s + g \tag{5.4}$$

On the other hand we want

$$d^*(C_\Omega(B, Y)) = d(Y) - (2g - 2) \geq s + 1$$

Therefore, we must have

$$d(Y) \geq s + 2g - 1 \tag{5.5}$$

Combining condition (5.4) and (5.5) we see that

$$d(A) + d(Y) \geq 2s + 3g - 1$$

so the minimum value for $d(A + Y)$ is $2s + 3g - 1$. But $d(D) = 2g + 2t^* - 1$ by assumption. If we want all the syndromes to be computable, we need $A + Y \leq D$. For that to happen we must necessarily have $d(A + Y) \leq d(D)$, so

$$2s + 3g - 1 \leq 2t^* + 2g - 1 \quad \Rightarrow \quad s \leq t^* - g/2$$

In fact we can assume $s \leq \lfloor t^* - g/2 \rfloor$ since s is a natural number. So our decoding algorithm is not perfect, since we can only correct up to $t^* - g/2$ errors, when in theory we should be able to correct at least t^*.

Fortunately, in turns out that some of the required unknown entries may be obtained via a so called "majority voting" process. We will cover an advanced algorithm pioneered by Feng and Rao in $([2], 93)$ to decode up to the designed minimum distance and sometimes beyond! For now we shall give some worked examples of the SV-Algorithm.

5.4 Examples of SV decoding

EXAMPLE 5.4.1. (Parabola)
Consider the code $C_\Omega(B, 3Q)$ over $\mathbb{F}_7$ as in Example $4.4.1$, where the curve is $C : YZ - X^2 = 0$. This code can correct 2 errors. We use the following codeword c, error word e and received word r

$$c = (1, 1, 1, 1, 1, 1, 1)$$
$$e = (0, 2, 0, 5, 0, 0, 0)$$
$$r = (1, 3, 1, 6, 1, 1, 1)$$

where c is the codeword sent and e the errorword and r the received word. If we assume the role of the receiver, we know only the vector r. By our prediction, we can correct upto $t^* - 0/2 = t^* = 2$ errors. Let $\varphi_i = x^i$ and let $h_{i,j} = \varphi_i\varphi_j \cdot e$. By Corollary $5.3.3$ we need to compute the following to obtain an

error locator

$$\begin{pmatrix} h_{0,0} & h_{0,1} & h_{0,2} \\ h_{1,0} & h_{1,1} & h_{1,2} \end{pmatrix}$$

Here $h_{i,j} = \varphi_{i+j} \cdot e$ and all the above entries are computable. Solving for

$$\begin{pmatrix} 0 & 3 & 5 \\ 3 & 5 & 4 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

We get $(\alpha_1, \alpha_2, \alpha_3) = (3, 3, 1)$. So $\phi = 3 + 3x + x^2$ is error locator. We see that $\phi = (x-1)(x-3)$ which implies that only P_1 and P_3 are zeroes of ϕ. Therefore the errors must be confined to those two locations. Since $L(3Q)$ contains an error locator and

$$d(C_\Omega(B, 2Q)) \geq d^*(C_\Omega(B, 2Q)) = 4 > d(3Q)$$

hence by Corollary 5.2.10, we can solve the following to obtain the error vector

$$\begin{pmatrix} 1 & 1 \\ 1 & 3 \\ 1 & 3^2 \end{pmatrix} \begin{pmatrix} e_2 \\ e_4 \end{pmatrix} = \begin{pmatrix} 1 \cdot e \\ x \cdot e \\ x^2 \cdot e \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 5 \end{pmatrix}$$

We get $e_2 = 2$ and $e_4 = 5$ which gives us the error vector as $e = (0, 2, 0, 5, 0, 0, 0)$ as given.

EXAMPLE 5.4.2. (Hermitian Curve)
Consider the 2-Hermitian Curve form 2. Recall that the code $C_\Omega(B, 5Q)$ has $d^* = 5$, and $\mathbb{F}_4 = \mathbb{F}_2[w]$ where $w^2 + w + 1 = 0$, see Example 4.4.2. We use the following codeword c, error word e and recieved word r

$$c = (1, 1, 1, 1, 1, 1, 1, 1)$$
$$e = (0, 0, w, 0, 0, 0, 0, 0)$$
$$r = (1, 1, w^2, 1, 1, 1, 1, 1)$$

Take $\varphi_0 = 1$, $\varphi_2 = x$, $\varphi_3 = y$, $\varphi_4 = x^2$, and $\varphi_5 = xy$ as a basis for $L(5Q)$. Let $h_{i,j} = \varphi_i \varphi_j \cdot e$. Assume we only know r, we have

$$h_{0,0} = w \quad h_{0,2} = w \quad h_{0,3} = w^2 \quad h_{0,4} = w \quad h_{0,5} = w^2$$

and note that $h_{i,j} = \varphi_{i+j} \cdot e$ if $i + j \leq 5$. We have the syndrome matrix

$$\begin{pmatrix} w & w & w^2 \\ w & w & w^2 \\ w^2 & w^2 & h_{3,3} \end{pmatrix}$$

where $h_{3,3} = \varphi_3 \varphi_3 \cdot 3 = y^2 \cdot e$ cannot be computed using the Syndrome Lemma 5.2.3. If $h_{3,3}$ is known, then we would be able to find an error locator for any error word with 2 or fewer errors. But since $h_{3,3}$

is unknown, Corollary 5.3.3 only guarantees that one error can be corrected. We drop the third column and the third row and try to solve

$$\begin{pmatrix} w & w \\ w & w \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

clearly $\alpha_1 = 1$ and $\alpha_2 = 1$ is a solution. So $\phi = 1 + x$ is an error locator, and $P_3 = [1 : w : 1]$ and $P_4 = [1 : w : 1]$ are the only possible zeroes. We can deduce that $e = (e_1, e_2, \cdots, e_8)$ must have $e_j = 0$ except possibly e_3 or e_4. Our error locator is contained in $L(2Q)$, and since

$$d(C_\Omega(B, 3Q)) \geq d^*(C_\Omega(B, 3Q)) = 3 > d(2Q)$$

We see that we need to solve

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \\ w & w^2 \end{pmatrix} \begin{pmatrix} e_3 \\ e_4 \end{pmatrix} = \begin{pmatrix} 1 \cdot e \\ x \cdot e \\ y \cdot e \end{pmatrix} = \begin{pmatrix} w \\ w \\ w^2 \end{pmatrix}$$

which yields $e_3 = w$ and $e_4 = 0$ as given.

In the next chapter we will show how to obtain unknown syndromes such as $h_{3,3}$ above so that we can correct errors up to the designed minimum distance and (sometimes) beyond!

CHAPTER 6

Majority Voting Algorithm

6.1 Introduction

From the last chapter we saw that the SV-Algorithm can only correct up to $t^* - g/2$ errors, where theoretically at least t^* errors are correctable. The breakthrough can be found in $([2], 93)$ where Feng and Rao utilized a Majority Voting Scheme (MVS) to obtain the unknown syndromes for a One-Point codes via a "voting process". During the revision phase of the paper Duursma derived a generalization of Feng-Rao's MVS to arbitrary divisors. In this chapter, we will treat the One-Point codes first and define the Feng-Rao minimum distance which is better than designed minimum distance in many cases. From there we present Duursma's extension.

Assumptions
Throughout, let C be a non-singular projective curve. Let $B := \sum_{i=1}^{n} P_i$ where $P_i \in C$ are distinct rational points. We also let D be an arbitrary divisor with $\mathrm{supp}(D) \cap \mathrm{supp}(B) = \emptyset$.

6.2 Majority Voting Scheme for One-Point Codes

We will consider One-Point codes and the decoding algorithm (MVS) that allows us to decode upto half the designed minimum distance and sometimes beyond! In the last chapter, the difficulty we had was that not all the syndromes can be computed. So our main aim is to compute the syndromes by other means. We start by developing some theory of Weierstrass points, crucial to the theoretical underpinning of the MVS.

Throughout, let $D = mQ$ where $m = 2g + 2t^* - 1$, therefore $d^*(C_\Omega(B, D)) = 2t^* + 1$ implying that at least t^* errors may be corrected.

6.2.1 Basic Weierstrass Points theory

Let $P \in C$ be a rational point. We would like to study the values of m where $l(mP) = l((m-1)P)$. These values are related to an improved estimate of the minimum distance named after Feng and Rao proposed in $([3], 95)$. We will derived these results using the Riemann-Roch theorem.

DEFINITION 6.2.1. (Gap, Non-Gap)
Let $P \in C$. For any $m \in \mathbb{N}$, if $l(mP) = l((m-1)P)$ then m is called a gap. Otherwise m is a non-gap. We denote the set of gaps of P by $G(P)$.

LEMMA 6.2.2.
The set $\mathbb{N} \setminus G(P)$ for any $P \in C$ is a semigroup with respect to addition.

PROOF
Suppose $m, n \in \mathbb{N} \setminus G(P)$, then there exists $\varphi \in L(mP)$ and $\phi \in L(nP)$ where $\mathrm{ord}_P(\varphi) = m$ and $\mathrm{ord}_P(\phi) = n$. The product $\varphi\phi \in L((m+n)P)$ but does not lie in $L((m+n-1)P)$, so $m+n \in \mathbb{N}\setminus G(P)$. The associativity of the non-gaps is clear. □

LEMMA 6.2.3.
The gaps $G(P)$, is a subset of $\{1, 2, \cdots, 2g-1\}$. Moreover there are exactly g gaps.

PROOF
Clearly, $l(-kP) = 0$ for k positive. So $0 \notin G(P)$. Now we establish that $n \in G(P)$ implies $n \leq 2g$ via a proof by contradiction. Suppose $n > 2g$ (so $n - 1 > 2g - 1$), by Riemman-Roch we have

$$l(nP) = n + 1 - g \neq n - g = l((n-1)P)$$

therefore we have $G(P) \subseteq \{1, 2, \cdots, 2g-1\}$. Also by Riemann Roch we have

$$l((2g-1)P) = 2g - 1 + 1 - g = g$$

which helps us to derive the following inequilities

$$1 = l(0P) \leq l(P) \leq l(2P) \leq \cdots \leq l((2g-1)P) = g$$

Together with the fact that $0 \leq l(D+P) - l(D) \leq 1$ for any divisor D, we see that there must be exactly $g-1$ values of m for which $l((m-1)P) + 1 = l(mP)$ for m between 1 and $2g-1$. Hence there are $(2g-1) - (g-1) = g$ gaps. □

REMARK 6.2.4.
A Weierstrass Point is a point where $G(P) \neq \{1, 2, \cdots, g\}$. There are only a finite number of Weierstrass points on any curve.

6.2.2 Preliminaries

DEFINITION 6.2.5.
A One-Point code is a residue code $C_\Omega(B, D)$ where $D = sP$ for some $s \in \mathbb{N}$ and $P \in C$.

Let X_i for $i \in \mathbb{N}$ be a sequence of divisors such that $l(X_i) = i$ and $X_i = jP$ for some $j \in \mathbb{N} \setminus G(P)$. As an immediate consequence we see that $X_i \leq X_{i+1}$ for all i, $D = X_{t^*+2g}$, and $\mathrm{ord}_P(\varphi_i) = -d(X_i)$.

Throughout we assume that

$$L(X_i) = \langle \varphi_j \mid j = 1, 2, \cdots, i \rangle$$

As in the last chapter, an error locator exists in $L(X_{t^*+1})$ and we see that

$$\begin{aligned} & l(X_{t^*+g}) = t^* + g = d(X_{t^*+g}) + 1 - g; \text{ by Riemann-Roch} \\ \Rightarrow \quad & d(X_{t^*+g}) = t^* + 2g - 1 \\ \Rightarrow \quad & d^*(C_\Omega(B, X_{t+g})) = t^* + 1 \end{aligned}$$

We know that X_{t^*+g} can be used in conjunction with X_{t^*+1} to find any error word e of weight less than or equal to t^*, provided we can compute the following matrix of syndromes

$$S := \begin{pmatrix} \varphi_1\varphi_1 \cdot e & \varphi_1\varphi_2 \cdot e & \cdots & \varphi_1\varphi_{t+1} \cdot e \\ \varphi_2\varphi_1 \cdot e & \varphi_2\varphi_2 \cdot e & \cdots & \varphi_2\varphi_{t+1} \cdot e \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{t^*+g}\varphi_1 \cdot e & \varphi_{t^*+g}\varphi_2 \cdot e & \cdots & \varphi_{t^*+g}\varphi_{t^*+1} \cdot e \end{pmatrix}$$

But we will see that it is more beneficial to consider a larger $s \times s$ matrix where $s = \max(t^*+1, t^*+g)$. Therefore, from here on we will consider

$$S := \begin{pmatrix} \varphi_1\varphi_1 \cdot e & \varphi_1\varphi_2 \cdot e & \cdots & \varphi_1\varphi_s \cdot e \\ \varphi_2\varphi_1 \cdot e & \varphi_2\varphi_2 \cdot e & \cdots & \varphi_2\varphi_s \cdot e \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_s\varphi_1 \cdot e & \varphi_s\varphi_2 \cdot e & \cdots & \varphi_s\varphi_s \cdot e \end{pmatrix};\ s = \max(t^*+1, t^*+g)$$

REMARK 6.2.6.
In many texts, S is assumed to be a $(t^* + g) \times (t^* + g)$ syndrome matrix instead. This is a minor oversight, since if $g = 0$ then we should consider the $(t^* + 1) \times (t^* + 1)$ syndrome matrix to ensure that an error locator can be found.

REMARK 6.2.7.
By the theory we have developed in the last chapter, we see that X_{t^*+g} can be replaced by X_{t+k}, provided k satisfiies $d(C_\Omega(B, X_{t+k})) \geq t + 1$ and $t = \lfloor \frac{\bar{d}-1}{2} \rfloor$ for some the minimum distance estimate $\bar{d}$.

Notation
Suppose M be a matrix. Then $M_{\leq u,\leq v}$ denotes the submatrix of M consisting of the intersection of the first u rows and v columns.

For convenience we define $\Phi(i,j) := d(X_i) + d(X_j)$, and $d_{ij} := l(\Phi(i,j)P)$

6.2.3 Rank Matrices, Pivots and Non-Pivots

In this section, we aim to discuss the main insights of the Majority Voting Scheme informally in order to build an intuition about why the method works. In particular, we will introduce an original novel approach via rank matrices.

DEFINITION 6.2.8. (Rank Matrix)
Let M be a matrix with entries coming from $\mathbb{F}$. Define R_M, the rank matrix of M to be the matrix where the (i,j)th entry is the rank of the submatrix $M_{\leq i,\leq j}$. We adopt the convention that $R_M = (r_{i,j})$ and define $r_{0,i} = 0 = r_{i,0}$ for all i and j. Note that R_M has the same shape as M, and the $r_{0,j}$'s and $r_{i,0}$'s are not entries of R_M.

REMARK 6.2.9.
We will see that the rank matrix helps us to visualise the majority voting scheme, providing an interesting insight into the problem.

DEFINITION 6.2.10. (Totally Rank Equivalent)
We call M and M' totally rank equivalent (TRE) if $R_M = R_{M'}$, and we write $M \equiv_R M'$.

REMARK 6.2.11.
The relation $\equiv_R$, is indeed an equivalence relation. More interesting however, is that $R_M \equiv_R M$. As a consequence, the theory of rank matrices allows us to study a large class of matrices simultaneously.

LEMMA 6.2.12.
Let R_M be the rank matrix of M and let $R_M = (r_{i,j})$. We have

$$\text{a)} \quad r_{i,j} \leq r_{i+1,j} \leq r_{i,j} + 1$$
$$\text{b)} \quad r_{i,j} \leq r_{i,j+1} \leq r_{i,j} + 1$$
$$\text{c)} \quad r_{i,j} \leq r_{i+1,j+1} \leq r_{i,j} + 2$$

PROOF
Consider the submatrices $M_{\leq i,\leq j}$ and $M_{\leq i+1,\leq j}$. The latter is the former with an added row. The $(i+1)$th row of $M_{\leq i+1,\leq j}$ is either a linear combination of the other rows, in which case $r_{i,j} = r_{i+1,j}$ by definition, or it is linearly independent of the other rows and we have $r_{i,j} + 1 = r_{i+1,j}$. For part b) consider $M^T_{\leq i,\leq j}$ and $M^T_{\leq i,\leq j+1}$ and apply a). For c), apply a) and then b). □

Consider a $m \times n$ matrix M of rank r. By Lemma 6.2.12, the $r_{i,j}$'s increase at most by one for successive values of i and j, and additionally $r_{m,n} = r$. Hence we can conclude that there are at most $2r$ positions of i, j where $r_{i,j} < r_{i+1,j}$ or $r_{i,j} < r_{i,j+1}$. Assume without loss of generality that $r \leq m \leq n$. The ratio of the entries that are larger than entries on the previous row of column is at most $\frac{2r}{mn} \leq \frac{2m}{mn} = \frac{2}{n}$. For n large, this ratio is small. This insight motivates the following definition.

DEFINITION 6.2.13. (Pivot, Non-Pivot)
Let M be a matrix with rank matrix $R_M = (r_{i,j})$, and recall $r_{0,j} = 0 = r_{i,0}$ for all i and j. A pivot of M is a position (i, j) where

$$r_{i,j} \neq r_{i-1,j-1} = r_{i-1,j} = r_{i,j-1}$$

If (i, j) is not a pivot then it is called a non-pivot.

LEMMA 6.2.14.
Let M be a matrix, r be the rank of M and $R_M = (r_{i,j})$, then

a) If (i, j) is a pivot then $(i', j)$and (i, j') are non-pivots for all $i' > i$ and $j' > j$

b) The number of pivots of $M$is equal to the rank of M

PROOF
Suppose (i, j) is a pivot so we have $r_{i,j-1} + 1 = r_{i,j}$. Now $r_{i+1,j}$ cannot be a pivot since $r_{i,j-1} \neq r_{i,j}$. If $r_{i+1,j-1} = r_{i+1,j-1} + 1$ then $r_{i+1,j} = r_{i+1,j} + 1$ since if the first $(i + 1)$th row restricted to the $j - 1$ columns is linearly indepedent of the previous row then adding another column will not change the linear independence. In this way we see that $(i + 2, j)$ can not be a pivot either since $r_{i+1,j} \neq r_{i+1,j-1}$. Continuing in this way, we see that (i', j) can not be pivots for all $i' > i$ if (i, j) is. An identical argument can be applied to show that (i, j') are not pivots for all $j' > j$.

If (i, j) is a pivot then $r_{i,j} > r_{i-1,j-1}$, but $r \geq r_{i,j}$, so the number of pivots is less than r. But by part a) the pivots are on different rows, and each row that contains a pivot is linearly independent of the previous rows. So the number of pivots must equal to the number of linearly independent rows, which is the rank. □

6.2.4 Application to Decoding

Recall that we defined $S = (s_{i,j})$ where $s_{i,j} := \varphi_i \varphi_j \cdot e$. Also, recall that we need to be able to compute all the values of S to ensure that an error locator can be found for all error vector e with $wt(e) \leq t^*$. Unfortunately, if $d(X_i) + d(X_j) > 2t^* + 2g - 1$, then there is no easy way of computing $s_{i,j}$.

By the discussion in the previous section, the ratio of pivots to non-pivots of S is at most $1/\max n, m$ for a $m \times n$ matrix S. Suppose $s_{i,j}$ is unknown, then we should "guess" that it is a non-pivot, since that is more likely.

It turns out that if (i, j) is a non-pivot satisfying the following relations

$$r_{i,j} = r_{i-1,j-1} = r_{i-1,j} = r_{i,j-1}$$

then we can produce a guess value for $s_{i,j}$. There is no known way of producing a good guess value for $s_{i,j}$ if (i, j) does not satisfy the above. This motivates the following definition and theorem.

DEFINITION 6.2.15. (Good non-pivot, Bad non-pivots)
A non-pivot (i, j) is good if

$$r_{i,j} = r_{i-1,j-1} = r_{i-1,j} = r_{i,j-1}$$

Other non-pivots are referred to as bad.

THEOREM 6.2.16.
Let S be a matrix over $\mathbb{F}$. Let s_k denote the kth row of $S_{i,j-1}$ and let $R_S = (r_{i,j})$. Suppose (i, j) satisfies

$$r_{i-1,j-1} = r_{i-1,j} = r_{i,j-1}$$

then it is either a good non-pivot or a pivot, and

$$s_i = \sum_{k=1}^{i-1} \alpha_k s_k \tag{6.1}$$

for some $\alpha_i \in \mathbb{F}$. Furthermore, if $s_{i,j}$ is a good non-pivot then

$$s_{i,j} = \sum_{k=1}^{i-1} \alpha_k s_{k,j}$$

PROOF
Clearly, (i, j) is either a pivot or a good non-pivot by definitions 6.2.13 and 6.2.15. Since we have $r_{i-1,j-1} = r_{i,j-1}$, this tells us that there exists a linear row relation in $S_{i,j-1}$, such that the ith row of $S_{i,j-1}$ is expressible as a linear combination of the other rows. Suppose we have a linear relation as in (6.1). Apply the following row operations

$$r_i \leftarrow r_i - \sum_{k=1}^{i-1} \alpha_k r_k$$

to $S_{i,j}$ to obtain $S'_{i,j}$. We have

$$S'_{i,j} = \begin{pmatrix} s_{1,1} & s_{1,2} & \cdots & \cdots & s_{1,j} \\ s_{2,1} & s_{2,2} & \cdots & \cdots & s_{2,j} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & x \end{pmatrix}$$

where the value x must satisfy the following (by the row operations we applied),

$$x = s_{i,j} - \sum_{k=1}^{i-1} \alpha_k s_{k,j} \tag{6.2}$$

We also have $r_{i-1,j} = r_{i-1,j-1}$, i.e. the jth column of $S_{i-1,j}$ is expressible as a linear combination of the other columns, therefore we can apply column operations of the form

$$c_j \leftarrow c_j - \sum_{k=1}^{j-1} \beta_k c_k$$

to $S'_{i,j}$ and obtain $S''_{i,j}$ such that

$$S''_{i,j} = \begin{pmatrix} s_{1,1} & s_{1,2} & \cdots & \cdots & 0 \\ s_{2,1} & s_{2,2} & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & 0 & x \end{pmatrix}$$

We note that the ith row of $S''_{i,j}$ is the same as $S'_{i,j}$ since the column operations had the effect of only adding zeroes to x. Note also that the row and column operations applied to $S_{i,j}$ and $S'_{i,j}$ do not affect the submatrix $S_{i-1,j-1}$. Furthermore, applying row and column operations do not affect the rank.

Now if (i,j) is a pivot then $x \neq 0$ since in that case $r_{i,j} > r_{i-1,j-1}$. On the other hand, if (i,j) is a good non-pivot then $x = 0$ since we require $r_{i,j} = r_{i-1,j-1}$.

By (6.2), we have

$$s_{i,j} = \sum_{k=1}^{j-1} \alpha_k s_{i,k}$$

as required. □

Based on the above theorem, we have a way of making an educated "guess" for the value of $s_{i,j}$ when (i,j) satisfies $r_{i-1,j-1} = r_{i-1,j} = r_{i,j-1}$, by assuming that (i,j) is a good non-pivot. Note that if (i,j) is a pivot then it also satisfies $r_{i-1,j-1} = r_{i-1,j} = r_{i,j-1}$. In fact if $s_{i,j}$ is unknown then there is no straightforward way of determining whether (i,j) is a pivot or a good non-pivot. We summarise the discussion in the following corollary.

COROLLARY 6.2.17.
Suppose $s_{i,j}$ satisfies

$$r_{i-1,j-1} = r_{i-1,j} = r_{i,j-1}$$

and

$$s_i = \sum_{k=1}^{i-1} \alpha_k s_k$$

where s_k is the kth row of $S_{i,j-1}$ and $\alpha_k \in \mathbb{F}$ for all k, then

$$s_{i,j} = \sum_{k=1}^{i-1} \alpha_k s_{k,j}$$

if and only if (i, j) is a good non-pivot.

PROOF

As in the proof of theorem, if (i, j) is good pivot then $s_{i,j} = \sum_{k=1}^{i-1} \alpha_k s_{k,j}$. On the other hand, if (i, j) is a pivot then the value of x must be non zero, and

$$s_{i,j} = \sum_{k=1}^{i-1} \alpha_k s_{k,j} + x$$

instead. □

REMARK 6.2.18.

The corollary tells us that any row relation involving s_i allows us to uniquely determine the value of $s_{i,j}$, if (i, j) is a good non-pivot. The theorem makes use of all the properties of a good non-pivot, and there is no obvious extension to guessing the value of $s_{i,j}$ if it is a bad non-pivot. Also, if we produce a guess value for $s_{i,j}$ assuming that it's a good non-pivot, then our guess will be wrong if it is indeed a pivot.

LEMMA 6.2.19.

Let M be a matrix and let $r_{i,j}$ be the (i, j)th entry of R_M. The position (i, j) is a bad non-pivot if and only if there exists (i', j) or (i, j') such that (i', j) or (i, j') is a pivot for some $i' < i$ or $j' < j$.

PROOF

Suppose (i', j) is a pivot for some $i' < i$. By Lemma 6.2.14, (i, j) must be a non-pivot. Further, by definition of a pivot we must have $(i', j - 1) < (i', j)$, so $(i, j - 1) < (i, j)$ and therefore it cannot be a good non-pivot. The case (i, j') being a pivot for some $j' < j$ is entirely analogous.

Conversely, suppose (i, j) is bad non-pivot then we can classify them into one of the four different types listed below

$$\text{Type 1} \quad \begin{pmatrix} r_{i-1,j-1} & r_{i-1,j} \\ r_{i,j-1} & r_{i,j} \end{pmatrix} = \begin{pmatrix} k-1 & k \\ k & k \end{pmatrix}$$

$$\text{Type 2} \quad \begin{pmatrix} r_{i-1,j-1} & r_{i-1,j} \\ r_{i,j-1} & r_{i,j} \end{pmatrix} = \begin{pmatrix} k-2 & k-1 \\ k-1 & k \end{pmatrix}$$

$$\text{Type 3} \quad \begin{pmatrix} r_{i-1,j-1} & r_{i-1,j} \\ r_{i,j-1} & r_{i,j} \end{pmatrix} = \begin{pmatrix} k-1 & k \\ k-1 & k \end{pmatrix}$$

$$\text{Type 4} \quad \begin{pmatrix} r_{i-1,j-1} & r_{i-1,j} \\ r_{i,j-1} & r_{i,j} \end{pmatrix} = \begin{pmatrix} k-1 & k-1 \\ k & k \end{pmatrix}$$

For type 1, we must have $r_{i-2,j-1} = k-1$ or $k-2$ since the rank values on the same column and successive rows must only differ by at most one by Lemma 6.2.12. If $r_{i-2,j-1} = k-1$, then by applying Lemma 6.2.12 again, either (1) $r_{i-1,j} = k$ in which case

$$\begin{pmatrix} r_{i-2,j-1} & r_{i-2,j} \\ r_{i-1,j-1} & r_{i-1,j} \\ r_{i,j-1} & r_{i,j} \end{pmatrix} = \begin{pmatrix} k-1 & k \\ k-1 & k \\ k & k \end{pmatrix}$$

which reduces to type 3; or (2) $r_{i-1,j} = k$ yielding

$$\begin{pmatrix} r_{i-2,j-1} & r_{i-2,j} \\ r_{i-1,j-1} & r_{i-1,j} \\ r_{i,j-1} & r_{i,j} \end{pmatrix} = \begin{pmatrix} k-1 & k-1 \\ k-1 & k \\ k & k \end{pmatrix}$$

in which case we can easily see that $(i-1, j)$ is a pivot.

If $r_{i-2,j-1} = k-2$ then $r_{i-2,j}$ must equal $k-1$, because the only other alternative $r_{i-2,j} = k$ violates Lemma 6.2.12; so we have

$$\begin{pmatrix} r_{i-2,j-1} & r_{i-2,j} \\ r_{i-1,j-1} & r_{i-1,j} \\ r_{i,j-1} & r_{i,j} \end{pmatrix} = \begin{pmatrix} k-2 & k-1 \\ k-1 & k \\ k & k \end{pmatrix}$$

Clearly this reduces to type 2.

Now to type 2, again, either $r_{i-2,j-1} = k-1$ and (1) $r_{i-2,j} = k-1$ or (2) $r_{i-2,j} = k-2$; or (3) $r_{i-2,j-1} = k-2$ and $r_{i-2,j} = k-1$. Following a similar argument set out in proving type 1, we see that case (1) reduces to type 3, case (2) gives that $(i-1, j)$ is a pivot, and case (3) gives

$$\begin{pmatrix} r_{i-2,j-1} & r_{i-2,j} \\ r_{i-1,j-1} & r_{i-1,j} \\ r_{i,j-1} & r_{i,j} \end{pmatrix} = \begin{pmatrix} k-3 & k-2 \\ k-2 & k-1 \\ k-1 & k \end{pmatrix}$$

which reduces back to type 2. But we see that a type 2 sometimes can not be reduced back to a type 2 since $r_{i,j} \geq 0$ by definition, so if we apply our analysis to the type 2 problem above, we see that eventually it must reduce to case (1) or (2). This proves type 2.

It remains to show that type 3 satisfies the theorem and note that type 4 can be solved by considering its transpose as type 3. Again we have 3 cases: (1) $r_{i-2,j-1} = k-1$ and $r_{i-2,j} = k$ or (2) $r_{i-2,j-1} = k-1$ and $r_{i-2,j} = k-1$; or (3) $r_{i-2,j-1} = k-2$ and $r_{i-2,j} = k-1$. Case (1) reduces to type 3, but this reduction can not always happen since $r_0, j-1 = 0$ by definition, so as we traverse $i, i-1, \cdots, 0$, we see that $r_{i-a,j-1} > r_{r-a+1,j-1}$ or $r_{i-a,j} > r_{r-a+1,j}$ for some $a \in \mathbb{N}$ which in effect reduces case (1) to (2) or (3). Case (2) shows that $r_{i-1,j}$ is a pivot. Case (3) reduces back to type 2, but note that this reduction is accompanied by a reduction in the value of the rank. A type 2 is sometimes reduced back to type 3, but since the reduction from type 3 to type 2 lowers the rank value, this reduction pattern can not continue forever, so case (3) either gets resolved by the prove for type ! 2 or it is reduced to case (1) or (2). □

To gain some more insight into the intuition behind the MVS we prove the following lemma.

LEMMA 6.2.20.
Let r be the rank of S then $r \leq wt(e)$.

PROOF
Recall, $s = \max(t^* + g, t^* + 1)$. We express S as the following product of matrices

$$S := \begin{pmatrix} \varphi_1(P_1) & \varphi_1(P_2) & \cdots & \varphi_1(P_n) \\ \varphi_2(P_1) & \varphi_2(P_2) & \cdots & \varphi_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_s(P_1) & \varphi_s(P_2) & \cdots & \varphi_s(P_n) \end{pmatrix} \begin{pmatrix} e_1 & 0 & \cdots & 0 \\ 0 & e_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e_n \end{pmatrix} \begin{pmatrix} \varphi_1(P_1) & \varphi_2(P_1) & \cdots & \varphi_s(P_1) \\ \varphi_1(P_2) & \varphi_2(P_2) & \cdots & \varphi_s(P_2) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(P_n) & \varphi_2(P_n) & \cdots & \varphi_s(P_n) \end{pmatrix}$$

where we assume $e = (e_1, e_2, \cdots, e_n)$. Clearly, the rank of S is at most equal to the rank of the middle diagonal matrix, which is $wt(e)$. □

We have been arguing the case that we can produce a guess for some $s_{i,j}$ by assuming (i, j) is a good non-pivot and our guesses are more likely to be correct. The next lemma shows that a lot of our seemingly different guesses are actually guesses about the same thing. Therefore, if the majority of them are correct then we can discover the unknown values of $s_{i,j}$ via a voting process!

Recall that $\Phi(i, j) := d(X_i) + d(X_j)$ and $d_{ij} := l(\Phi(i, j)P)$ where $l(X_i) = i$.

LEMMA 6.2.21.
Suppose the $s_{i,j}$'s are known for all (i,j) such that $\Phi(i,j) < s$, for some $s \in \mathbb{N}$, then knowing any one $s_{i,j}$ with $\Phi(i,j) = s$ determines all other $s_{k,l}$'s with $\Phi(k,l) = s$.

PROOF
Suppose we know the value of $s_{i,j}$ with $\Phi(i,j) = s$, then we have

$$s_{i,j} = \alpha_1\varphi_1 \cdot e + \alpha_2\varphi_2 \cdot e + \cdots + \alpha_{d_{ij}}\varphi_{di,j} \cdot e$$

If $\Phi(i',j') = s$, then similarly we have

$$s_{i',j'} = \alpha_1\varphi_1 \cdot e + \alpha_2\varphi_2 \cdot e + \cdots + \alpha_{d_{i'j'}}\varphi_{d_{i',j'}} \cdot e$$

By assumption, we know the value of $s_{i,j}$, and φ_k's are known for $k < \Phi(i,j)$. So from $s_{i,j}$ we can derive the value for $\varphi_{d_{i,j}} = \varphi_s = \varphi_{d_{i',j'}}$, which in turn determines $s_{i',j'}$. □

6.2.5 Majority Voting

In this section we will prove a number of technical results that confirm our intuition and show how we can make use of those results to design a reasonably fast decoding algorithm we call MVS. We begin with a definition.

Definition (Candidate, Non-candiate)
Let $S = (s_{i,j})$ be as before and let $R_M = (r_{i,j})$. Suppose $s_{u,v}$ is an unknown syndrome but all $s_{i,j}$ for $i \leq u$ and $j \leq v$, except $(i,j) = (u,v)$, are known. We call $s_{i,j}$ a candidate if (i,j) is either a good non-pivot or pivot. Otherwise, $s_{i,j}$ is called a non-candidate. If (i,j) is a good non-pivot, then it is a correct or true candidate, otherwise it is called incorrect or false.

REMARK 6.2.22.
Consistent with previous discussions, a candidate is one for which we can produce a guess value for, and our guess will be false if the position of the candidate is actually a pivot, hence the above definition.

We can now describe the MVS that completely determines the syndrome matrix S defined earlier. Firstly, we give a description of the MVS algorithm.

Recall that $\Phi(i,j) := d(X_i) + d(X_j)$ and $d_{i,j} := l(\Phi(i,j)P)$, and

$$L(X_i) = \langle \varphi_1, \varphi_2, \cdots, \varphi_i \rangle$$

and suppose that

$$s_{i,j} = \sum_{k=1}^{d_{i,j}} \beta_{i,k}\varphi_k \cdot e$$

where the values of the scalars $\beta_{i,k}$'s are known.

Assume the code we use is $C_\Omega(B, X_s)$ for some $s \in \mathbb{N} \setminus G(P)$.

The Basic MVS Algorithm

Initialise $d \leftarrow d(X_{s+1})$.

(1): Locate all candidates, $s_{i,j}$ with $\Phi(i,j) = d$. For each candidate $s_{i,j}$, find a linear row relation in the form of

$$s_i = \sum_{k=1}^{i-1} \alpha_{i,k} s_k$$

where s_l is the lth row of $S_{i,j-1}$ and $\alpha_{i,k}$'s are scalars.

Let $s'_{i,j} \leftarrow \sum_{k=1}^{i-1} \alpha_{i,k} s_{k,j}$, then let

$$g_{i,j} = \frac{1}{\alpha_{i,d_{i,j}}}(s'_{i,j} - \sum_{k=1}^{d_{i,j}-1} \alpha_{i,k} s_{k,j})$$

Once all the possible $g_{i,j}$'s are computed, let g be the value that most of the $g_{i,j}$'s take. Let

$$s_{i,j} \leftarrow \sum_{k=1}^{d_{i,j}-1} \beta_{i,k}\varphi_k \cdot e + g$$

If a row/column relation is found in S then we can use that relation to compute an error-locator, and hence the error word, and so we halt the algorithm in that case. Otherwise, if not all the $s_{i,j}$ are known then increment d by 1 and go back to step (1).

EXAMPLE 1

Consider the 2-Hermitian Curve, see Example 4.4.2. For $Q = [0 : 1 : 0]$ We have $L(5Q) = \langle 1, x, y, x^2, xy \rangle$, where $\mathbb{F}_4 := \mathbb{F}_2[w]$ and $w^2 + w + 1 = 0$. Let

$$P_1 = [0:0:1] \quad P_2 = [0:1:1] \quad P_3 = [1:w:1] \quad P_4 = [1:w^2:1]$$

$$P_5 = [w:w:1] \quad P_6 = [w:w^2:1] \quad P_7 = [w^2:w:1] \quad P_8 = [w^2:w^2:1]$$

The code $C_\Omega(B, 5Q)$ can correct 2 errors and it has parity check matrix.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & w & w & w^2 & w^2 \\ 0 & 1 & w & w^2 & w & w^2 & w & w^2 \\ 0 & 0 & 1 & 1 & w^2 & w^2 & w & w \\ 0 & 0 & w & w^2 & w^2 & 1 & 1 & w \end{pmatrix}$$

For this example we let

$$e = (1, 0, w, 0, 0, 0, 0)$$

and $\phi_0 = 1$, $\phi_2 = x$, $\phi_3 = y$, $\phi_4 = x^2$, $\phi_5 = xy$. Since the genus is 1, we need to compute the 3×3 matrix

$$S = \begin{pmatrix} \phi_0\phi_0 \cdot e & \phi_0\phi_2 \cdot e & \phi_0\phi_3 \cdot e \\ \phi_2\phi_0 \cdot e & \phi_2\phi_2 \cdot e & \phi_2\phi_3 \cdot e \\ \phi_3\phi_0 \cdot e & \phi_3\phi_2 \cdot e & \phi_3\phi_3 \cdot e \end{pmatrix} = \begin{pmatrix} 1 \cdot e & x \cdot e & y \cdot e \\ x \cdot e & x^2 \cdot e & xy \cdot e \\ y \cdot e & xy \cdot e & y^2 \cdot e \end{pmatrix} = \begin{pmatrix} w^2 & w & w^2 \\ w & w & 0 \\ w^2 & 0 & y^2 \cdot e \end{pmatrix}$$

and

$$R_S = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & r_{3,3} \end{pmatrix}$$

clearly $(3, 3)$ is a candidate. The third row of $S_{3,2}$ can be expressed as the sum of $w^2 r_1 + w^2 r_2$ where r_1 and r_2 are the first and second row of $S_{3,2}$, so we guess $S_{3,3}$ to be $w^2 w^2 + w^2 0 = w^4 = w$. It can be confirmed that $y^2 \cdot e = w$.

REMARK 6.2.23.
For larger scale examples, see $([3], 95)$ or Appendix B.

6.2.6 Feng-Rao Minimum Distance

We now prove a theorem that validates the MVS, where the main skeleton of the proof was sketched in $([3], 95)$. We start with some definitions.

DEFINITION 6.2.24.
Define $d_i := d(X_i)$. We let the set of pairs N_r be defined by

$$N_r = \{(d_i, d_j) \in \mathbb{N}^2 \mid d_i + d_j = d_{r+1})\}$$

where $l(X_i) = i$ and $d_i \in \mathbb{N} \setminus G(P)$.

DEFINITION 6.2.25. (Feng-Rao Minimum Distance)
Let n_r denote the cardinality of N_r. The Feng-Rao minimum distance d_{FR} of the One-Point code $C_\Omega(B, X_s)$ is defined to be

$$d_{FR} = \min\{n_r \mid r \geq s\}$$

LEMMA 6.2.26.
For a code $C_\Omega(B, X_s)$. We have $d_{FR} \geq d^*$, and they are equal if $d(X_s) \geq 4g - 2$, where g is the genus of C.

PROOF
Consider n_r for some $r \geq s$. If $d(X_s) \leq 2g - 2$, then $d^* = d(X_s) - (2g - 2) \leq 0$ which is clearly less

than n_r. So assume $d(X_s) \geq 2g-1$. Let $d_i := d(X_i)$ and define the sets N, I and J by

$$\begin{aligned} N &:= \{(i, d_{r+1}-i) \mid i = 0, 1, \cdots, d_{r+1}\} \\ I &:= \{(i, d_{r+1}-i) \in N \mid i \in \mathbb{N} \setminus G(P)\} \\ J &:= \{(d_{r+1}-j, j) \in N \mid j \in \mathbb{N} \setminus G(P)\} \end{aligned}$$

then we have $N_r = I \cap J$, and by the Inclusion-Exclusion Principle

$$|I \cap J| = |I| + |J| - |I \cup J| \tag{6.3}$$

For the values between $0, 1, 2, \cdots, d_{r+1}$ there are g non-gaps from $0, 1, \cdots, 2g-1$ since $l((2g-1)P) = g$ for any rational point $P \in C$. The $d_{r+1} - 2g + 1$ values between $2g$ and d_{r+1} are all non-gaps, so $|I| = g + d_{r+1} - 2g + 1 = d_{r+1} - g + 1$. Note that $|J| = |I|$ and $I \cup J \subseteq N$ and so $|I \cup J| \leq d_{r+1} + 1$. Substitute into (6.3), we get

$$\begin{aligned} n_r = |I \cap J| &= d_{r+1} - g + 1 + d_{r+1} - g + 1 - |I \cup J| \\ &\geq 2d_{r+1} - 2g + 2 - (d_{r+1} + 1) \quad (*) \\ &= d_{r+1} - 2g + 1 \\ &= d_r - 2g + 2; \quad \text{since } d_r \geq 2g-1 \text{ and so } d_{r+1} = d_r + 1 \\ &\geq d_s - (2g-2) =: d^*; \quad \text{by assumption } d_r \geq d_s \end{aligned}$$

Therefore $d_{FR} := \min\{n_r \mid r \geq s\} \geq d^*$. Now if $d_s \geq 4g-2 \Rightarrow d_{r+1} \geq 4g-1$, then $I \cup J = N$ since if $i \notin \mathbb{N}(P)$ then $d_{r+1} - i \geq 4g - 1 - (2g-1) = 2g$ is a non-gap, so $(i,j) \in N$ implies either $(i,j) \in I$ or $(i,j) \in J$. So $(*)$ is an equality and hence $d_{FR} := \min\{n_r \mid r \geq s\} = n_s = d^*$. □

THEOREM 6.2.27.
Consider the code $C_\Omega(B, X_s)$. Let $d_i := d(X_i)$. Suppose the $s_{i,j}$'s are known for all (i,j)'s with $d_i + d_j \leq d_r$. Additionally, suppose $wt(e) \leq (n_r - 1)/2$. Then the set N_r has more good non-pivots then pivots.

PROOF
This proof is based on the proof sketched in $([13], 95)$. Let K be the number of known pivots in S, let F be the number of pivots in the set N_r, and let T the number of good non-pivots in N_r. We must have $K + F$ less than the total number of pivots, and so

$$K + F \leq \text{rank}S \leq wt(e) \tag{6.4}$$

If (i,j) is a pivot then (i', j) and (i, j') for $i' > i$ and $j' > j$ are all bad non-pivots, so the set N_r consists of at most $2K$ bad non-pivots. Note that any element $(d_i, d_j) \in N_r$ fit into three categories: (i,j) is a

pivot, a good non-pivot, or a bad non-pivot. Therefore

$$n_r \leq T + F + 2K$$

which implies

$$wt(e) \leq (n_r - 1)/2 \leq (T + F)/2 + K - 1/2$$

Combine with (6.4) yields $F < T$ as required. □

COROLLARY 6.2.28.
For a code $C_\Omega(B, X_s)$, the MVS can correct all error word e satisfying

$$wt(e) \leq \frac{(d_{FR} - 1)}{2}$$

PROOF
Initially, all the sydnromes $s_{i,j}$ for $d_{i,j} \leq d_s$ are known. By the theorem, the syndromes $s_{i,j}$ with $d_i + d_j = d_{s+1}$ can be obtained via the MVS since $(n_r - 1)/2 \geq (d_{FR} - 1)/2 \geq wt(e)$. Now we can obtain the syndromes that satisfy $d_i + d_j = d_{s+2}$. Clearly this process may be repeated until all the required syndromes are obtained. □

REMARK 6.2.29.
It may be noted that not all the syndromes that we claim to be computable are situated in the matrix S which is a $(t^* + g) \times (t^* + g)$ matrix if $g \geq 1$. For example, s_{k,t^*+g+1} is not an element of S for any k. But if s_{k,t^*+g+1} is a candidate, then s_{k,t^*+g+1} must have been a good non-pivot. Which means that the kth row of $S_{\leq k,\leq t^*+g}$ is expressible as a linear row relation of the previous rows, in which case the MVS would have halted. So if the algorithm needs to compute s_{k,t^*+g+1}, then s_{k,t^*+g+1} must be a non-candidate. Hence it does not contribute a vote, and so it can be ignored.

REMARK 6.2.30.
We see that d_{FR} is a better measure of the minimum distance than d^*. Therefore we can consider a smaller syndrome matrix S of shape $s' \times s'$ where $s' = \max(t + g, t + 1)$ and $t = (d_{FR} - 1)/2$.

The following example demonstrates the superiority of the Feng-Rao minimum distance to the designed minimum distance. We consider the code $C_\Omega(B, D)$ where C is the 4-Hermitian codes form 2. Recall that $\mathrm{ord}_Q(x) = -4$ and $\mathrm{ord}_Q(y) = -5$ for $Q = [0 : 1 : 0]$. The non-gaps are

$$0, 4, 5, 8, 9, 10, 12, 13, 14, 15, \cdots$$

Let $d_r := d(X_r)$, where $X_r = d_r P$ and $L(X_r) = r$. Recall that $g = 6$ and so $4g - 2 = 22$ and $2g - 2 = 10$. We have

d_r	5	8	9	10	12	13	14	15	16	17	18	19	20	21	22
d_{r+1}	8	9	10	12	13	14	15	16	17	18	19	20	21	22	23
n_r	3	4	3	4	6	6	4	5	8	9	8	9	10	12	12
d_{FR}	3	3	3	4	4	4	4	5	8	8	8	9	10	12	12
d^*	$-$	$-$	$-$	0	2	3	4	5	6	7	8	9	10	11	12

The $-$ symbol denotes a minimum distance that cannot be estimated with d^*. Clearly, d_{FR} is superior to d^* in many cases. The difference is very pronounced in a class of codes defined over the Suzuki curves. See Example 8.4 $([3], 95)$.

6.3 The General Algorithm

6.3.1 Definitions and Preliminaries

The general MVS is very similar to the One-Point code MVS. Throughout, assume we are considering a code $C_\Omega(B, D)$, and by a curve we mean a non-singular projective curve.

DEFINITION 6.3.1. (μ-Order)
Let C a curve, let $P \in C$ and let X be a divisor. Define

$$\begin{aligned} \mu_{X,P}(\phi) &:= \min\{m \mid \phi \in L(X - d(X)P + mP)\}; \quad \text{if defined} \\ &:= \infty; \quad \text{otherwise} \end{aligned}$$

REMARK 6.3.2.
The μ-order provides an indexing of functions similar to that of the indexing via order at P in the MVS for One-Point codes. Note that if $X = d_s P$ for some $d_s \in \mathbb{N} \setminus G(P)$ then $\mu_{X,P}(\varphi_i) = -\mathrm{ord}_P(\varphi_i)$.

DEFINITION 6.3.3. (Gaps, Non-Gaps)
Let C be a curve. Let X be a divisor and let $P \in C$. Define the gaps of X at P by

$$G_X(P) := \{m \mid l(X - d(X) + mP) = l(X - d(X) + (m-1)P)\}$$

The elements of $\mathbb{N} \setminus G_X(P)$ are called the non-gaps of X at P. Any element $a \in G_X(P)$ is called a X-gap, similarly any element $b \in \mathbb{N} \setminus G_X(P)$ is called a X-non-gap.

REMARK 6.3.4.
The above definitions are generalisations of the Weierstrass Points gaps and non-gaps. It can be seen that if we set $X = 0$, then the definitions above agrees with the definitions of gaps and non-gaps in the One-Point code case. By almost exactly the same proof as Lemma 6.2.3, we see that there are exactly g

gaps between 1 and $2g-1$. Indeed, clearly $d(X-d(X)P+(2g-1)P) = 2g-1$ which by the Riemann-Roch theorem implies that $l(X - d(X)P + (2g-1)P) = g$. Since $l(E) \leq l(E+P) \leq l(E)+1$ for any divisor E, there must be $g-1$ X-gap between 1 and $2g-1$ from which our claim follows.

DEFINITION 6.3.5. (Duursma sequence)
The Duursma sequence of X with respect to P is the sequence of divisors X_i where $l(X_i) = i$ and $X_i = X - d(X)P + mP$ for some $m \in \mathbb{N} \setminus G_X(P)$.

We prove some properties of the Duursma sequence.

LEMMA 6.3.6.
Let (X_i) be the Duursma sequence of a divisor X with respect to P.
1) If $\phi \in L(X_{i+1}) \setminus L(X_i)$ then $\mu_{X,P}(\phi) = d(X_i)$.
2) If $X = 0$ then for any $\phi \in L(X_i)$, we have

$$\mu_{X,P}(\phi) = -\mathrm{ord}_P(\phi)$$

3) If $d(X_i) \leq d(X)$ then $X_i \leq X$

PROOF
Let $X_i = X-d(X)P+mP$ and $X_{i+1} = X-d(X)P+nP$ where clearly $d(X_i) = m$ and $d(X_{i+1}) = n$. Let $\phi \in L(X_{i+1}) \setminus L(X_i)$, then $\mu_{X,P}(\phi) > m$ or else $\phi \in L(X_i)$. Clearly $\mu_{X,P}(\phi) = d(X_i)$ by definition.

If $X = d_s P$ for some $d_s \in \mathbb{N} \setminus G(P)$, then

$$\mu_{X,P}(\phi) := \min\{k \mid \phi \in L(X - d(X)P + kP)\} = \min\{k \mid \phi \in L(kP)\} = -\mathrm{ord}_P(\phi)$$

If $d(X_i) \leq d(X)$ then we must have $d(X_i) = m \leq d(X)$ where $X_i = X - d(X)P + mP$ for some $m \in \mathbb{N} \setminus G_X(P)$. Clear $X \geq X + (m - d(X))P = X_i$. $\square$

DEFINITION 6.3.7.
Let C be a curve. Let X and Y be divisors, let $P \in C$, and let (X_i) and (Y_i) be the Duursma sequence of X and Y, respectively, with respect to P. Additionally, let (W_i) be the Duursma sequence of $X+Y$ with respect to P. Define

$$N^P_{X,Y,r} := \{(d(X_i), d(Y_j)) \mid d(X_i) + d(Y_j) = d(W_{r+1})\}$$

LEMMA 6.3.8.
If $\mu_{X,P}(\varphi) = a < \infty$ and $\mu_{Y,P}(\phi) = b < \infty$ then $\mu_{X+Y,P}(\varphi\phi) = a + b$.

PROOF
Clearly $\varphi\phi \in L(X+Y-(d(X)+d(Y))P+(a+b)P)$ and so $\mu_{X+Y,P}(\varphi\phi) \leq a+b$. We can see that

$$\mathrm{ord}_P(\varphi) = d(X) - X_P - a$$

where X_P is the coefficient of P in the divisor X, since $\varphi \in L(X - d(X)P + a)$ where a is minimal. Similarly

$$\mathrm{ord}_P(\phi) = d(Y) - Y_P - b$$

where Y_P is the coefficient of P in the divisor X. Lastly

$$\mathrm{ord}_P(\varphi\phi) = d(X+Y) - (X+Y)_P - \mu_{X+Y,P}(\varphi\phi)$$

The three equations above are related by $\mathrm{ord}_P(\varphi\phi) = \mathrm{ord}_P(\varphi) + \mathrm{ord}_P(\phi)$ which gives

$$d(X+Y) - (X+Y)_P - \mu_{X+Y,P}(\varphi\phi) = d(X) - X_P - a + \mathrm{ord}_P(\phi) + d(Y) - Y_P - b$$

rearrange and we get the result required. □

6.3.2 The General MVS

Given a code $C_\Omega(B, D)$, we aim to adapt the MVS algorithm developed for One-Point codes to help decode received words. Here D is generally not assumed to be of the form $d_s P$ for some $P \in C$ and $d_s \in \mathbb{N}$.

Let $L(D) = \langle \varphi_{d_i} \mid d_i = d(D_i) \rangle$ where $P \notin \mathrm{supp}(B)$. Let (D_i) be the Duursma sequence of D with respect to P. Note that Lemma 6.3.6 gives $D_i \leq D$ if $d(D_i) \leq d(D)$ and so every function in $L(D)$ have a μ-order of D with respect to P.

Let $s = \max\{t+1, t+g\}$ where g is the genus of C and $t = \lfloor \frac{\bar{d}-1}{2} \rfloor$ where $\bar{d}$ is some estimate of minimum distance such as the generalised minimum distance defined below. Let (Y_i) be the Duursma's sequence for the zero divisor with respect to P. Let $y_i := d(Y_i)$ and let $L(Y_i) = \langle \phi_{y_j} \mid j \leq i \rangle$, we consider the syndrome matrix

$$S := \begin{pmatrix} \varphi_{d_1}\phi_{y_1} \cdot e & \varphi_{d_1}\phi_{y_2} \cdot e & \cdots & \varphi_{d_1}\phi_{y_s} \cdot e \\ \varphi_{d_2}\phi_{y_1} \cdot e & \varphi_{d_2}\phi_{y_2} \cdot e & \cdots & \varphi_{d_2}\phi_{y_s} \cdot e \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{d_s}\phi_{y_1} \cdot e & \varphi_{d_s}\phi_{y_2} \cdot e & \cdots & \varphi_{d_s}\phi_{y_s} \cdot e \end{pmatrix}$$

As before, if we know enough of the syndromes to find a linear row or column relation, then we can find an error locator and hence the error.

By Lemma 6.3.8, we see that

$$\mu_{D+0,P}(\varphi_i\phi_j) = \mu_{D,P}(\varphi_i\phi_j) = i + j$$

and so $i+j = i'+j' = k$ is the minimum value such that

$$\varphi_i\phi_j, \varphi_{i'}\phi_{j'} \in L(D - d(D)P + kP)$$

therefore if we try to produce a guess for the positions (d_i, d_j) and $(d_{i'}, d_{j'})$, then they are guesses about the same thing. Hence the MVS we developed in the previous section can be applied with minimal modification.

Using the definitions above we see that the theory we developed for One-Point codes is naturally extended to solving the problem for a general residue code $C_\Omega(B, D)$. Note that $l(D_{t+1}) = t+1$ and $l(Y_{t+1}) = t+1$ and so error locators can be found in $L(D_{t+1})$ or $L(Y_{t+1})$. So the natural extension is to look for linear row relations in S as well as linear column relations. Note that the μ-order provided a way to index the functions similar to that found in the One-Point code MVS, and this is important for the definition of the generalised Feng-Rao Minimum distance given below. Also worthing noting is that our choice of the ϕ_i's and φ_j's ensured that as many syndromes are computable as possible.

REMARK 6.3.9.
In the One-Point code case, we have $(D_i) = (Y_i)$. Therefore the syndrome matrix S given above would have been symmetric and hence looking for row relations is the same as looking for column relations.

DEFINITION 6.3.10. (Generalised Feng-Rao minimum distance)
Consider a code $C_\Omega(B, D)$. Let (D_i) be the Duursma sequence of D with respect to $P \notin \mathrm{supp}(B)$, and let $n_r := |N^P_{D,0,r}|$ assuming $D = D_{l(D)}$. The generalised Feng-Rao minimum distance with respect to P is defined to be

$$d^P_{FR} := \min\{n_r \mid r \geq l(D)\}$$

REMARK 6.3.11.
The requirement that $P \notin \mathrm{supp}(B)$ ensures that the syndromes $s_{i,j} = \varphi_i\phi_j \cdot e$ are defined for all i and j.

The validity of the MVS in the general setting is verifiable by essentially the same proofs as in the One-Point code case.

LEMMA 6.3.12.
For a code $C_\Omega(B, D)$, where we assume $D = D_{l(D)}$. We have $d^P_{FR} \geq d^*$, and they are equal if $d(D) \geq 4g - 2$ where g is the genus of C and $P \notin \mathrm{supp}(B)$.

PROOF
The case where $d(D) \leq 2g - 2$ is clear, see Lemma 6.2.26. So assume $d(D) \geq 2g - 1$. Let $d_i = d(D_i)$

and $y_i = d(Y_i)$ where (D_i) and (Y_i) are as defined above. We define the sets N, I, and J by

$$\begin{aligned} N &:= \{(i, d_{r+1} - i) \mid i = 0, 1, \cdots, d_{r+1}\} \\ I &:= \{(d_i, d_{r+1} - d_i) \in N\} \\ J &:= \{(d_{r+1} - y_j, y_j) \in N\} \end{aligned}$$

We have $N_r = I \cap J$. There are g D-non-gaps from 0 to $2g-1$. The $d_{r+1} - 2g + 1$ values between $2g$ and d_{r+1} are all D-non-gaps, so

$$|I| = g + d_{r+1} - 2g + 1 = d_{r+1} - g + 1$$

Similarly, $|J| = |I|$. Note that $I \cup J \subseteq N$ and so $|I \cup J| \leq d_{r+1} + 1$. By the Inclusion-Exclusion Principle we get

$$\begin{aligned} n_r = |I \cap J| &= d_{r+1} - g + 1 + d_{r+1} - g + 1 - |I \cup J| \\ &\geq 2d_{r+1} - 2g + 2 - (d_{r+1} + 1) \quad (*) \\ &\geq d_s - (2g-2) =: d^*; \quad \text{by assumption } d_r \geq d_s \end{aligned}$$

The rest of the proof is entirely identical to Lemma 6.2.26. □

LEMMA 6.3.13.
Let $N_r = N^P_{D,0,r}$ and let $n_r = |N_r|$. For the code $C_\Omega(B, D)$, where we assume $D = D_{l(D)}$, and d_i, y_i,(D_i) and (Y_i) are as defined above. Suppose $wt(e) \leq (n_r - 1)/2$. Suppose the s_{d_i,y_j}'s are known for all (d_i, y_j) such that $d_i + d_j \leq d_r$. The set N_r has more good non-pivots then pivots.

PROOF
This proof is very similar to Theorem 6.2.27. Let K be the number of known pivots in S, let F be the number of pivots in the N_r, and T the number of good non-pivots in N_r. We have as before

$$K + F \leq \text{rank} S \leq wt(e) \tag{6.5}$$

Also N_r must have no more than $2K$ bad non-pivots. Note that any element $(d_i, y_j) \in N_r$ must satisfy one of the following: (i, j) is a pivot, a good non-pivot, or a bad non-pivot, and so

$$n_r \leq T + F + 2K$$

which with (6.5) yields $F < T$ as required. □

The general MVS is essentially the same as the One-Point code MVS. It proceeds by computing all syndromes computable by the Syndrome Lemma. Then it produces guess values for all the candidates. The syndrome table is updated using the values of the correct candidates. Continue this process until a row or column relation is found. Recall that a column/row relation determines an error locator, and the error locator uniquely determines the error word e.

The correctness of the general MVS is guaranteed by the above lemma. The lemma shows that if e satisfies $wt(e) \leq (d^P_{FR} - 1)/2$, then the correct candidates outnumber the incorrect candidates at every stage of the MVS. Hence we have solved the decoding problem for Algebraic Geometric codes!

References

[1] O. Pretzel 1992 "Error-Correcting Codes and Finite Fields" Oxford. Clarendon Press

[2] G.L. Feng T.R.N. Rao 1993. "Decoding Algebraic-Geometric Codes up to the Designed Minimum Distance" In *IEEE Transactions on Information Theory*, Vol39, No. 1, pages 37–45

[3] T. Hoholdt R. Pellikaan 1995. "On the decoding of algebraic-geometric codes" In *IEEE Transactions on Information Theory*, IT-41, pages 1589–1614

[4] O. Pretzel 1998. "Codes and Algebraic Curves" New York. Oxford University Press, Inc.

[5] W. Fulton 1969. "Algebraic Curves - An Introduction to Algebraic Geometry" pages 35–74, New York. W.A. Benjamin, Inc.

[6] M.F. Atiyah I.G. Macdonald 1969. "Introduction to Commutative Algebra" pages 80–84, Reading, MA. Addison-Wesley Publishing Company

[7] H. Stichtenoth 1991. "Algebraic Function Fields and Codes" pages 1–2, New York, Springe-Verlag

[8] S. Stepanov 1999. "Codes on Algebraic Curves" New York, Kluwer Academic/Plenum Publishers

[9] M. A. Tsfaman. S.G. Vladut. T. Zink 1982. "Modular curves, Shmura curves and Goppa codes beter than the Varshamov-Gilbert bound." Math. Nachr, 109, 21-28

[10] H. Stichtenoth 1988. "A note on Hermitian codes over $GF(q^2)$" In *IEEE Trans. Inform. Theory 34*, pages 1345–1349.

[11] P. Morandi 1996. "Fields and Galois Theory" New York, Springer.

[12] V.S. Pless and W.C. Huffman 1998. "Handbook of Coding Theory Volume 1" Amsterdam, The Nethelands, Elsevier Science B.V.

[13] C. Kirfel and R. Pellikaan 1995. "The minimum distance of codes in an array coming from telescopic semigroups" In *IEEE Trans. Inform. Theory*, IT-41, pages 1720-1732.

[14] S.G. Vladut A.N. Skorobogatov 1990. "On the decoding of algebraic-geometric codes" In *IEEE Trans. Inform. Theory*, 36, pages 1051-1960.

[15] I. M. Duursma 1993. "Majority coset decoding" In *IEEE Trans. Inform. Theory*, 39, pages 1067-1070.

[16] V. D. Goppa 1981. "Codes on algebraic curves" In *Dokl. Akad. Nauk. SSSR*, 259, pages 1289-1290.

APPENDIX A

Basic Coding Theory

A.1 Block Codes

DEFINITION A.1.1. (Block Code, Codeword)
Let $\mathbb{F}$ be a field. A block code C, of length n over $\mathbb{F}$ is a subset of $\mathbb{F}^n$. As we will only be dealing with block codes in this essay, we will simply refer to C as just a code. Any element of C is called a codeword.

Throughout, assume that a block code C is defined over a field $\mathbb{F}$.

One of the most important parameters of a code is its minimum distance, which is defined in terms of the Hamming distance. It measures how many errors can be corrected by the Majority Logic Decoding (MLD) method, to be defined later.

DEFINITION A.1.2. (Weight, Hamming Distance, Minimum Distance)
Let c be a codeword. The weight of c denoted $wt(c)$ is defined to be the number of components of c not equal to zero. The Hamming distance (or just distance) between $x, y \in C$ is $d(x, y) := wt(x - y)$. The distance between a codeword and a code is defined to be

$$d(x, C) := \min \{d(x,\ c) \mid c \in C\}$$

The minimum distance of a code C is

$$d(C) := \min\{d(x, y)|x, y \in C\}$$

Examples: $wt(0101) = 2$ and $d(010, 000) = 1$ and $d(010, 101) = 3$.

LEMMA A.1.3.
The Hamming distance defined by $d(x, y) := wt(x - y)$ is a metric.

PROOF
1) $d(x, y) \geq 0$ is clear.
2) $d(x, y) = wt(x - y) = wt(-(y - x)) = wt(y - x) = d(y, x)$; since multiplying by -1 does not

change the weight
3) This proof follows ([1], 92). Let $x = (x_1, x_2, \cdots, x_n)$, $y = (y_1, y_2, \cdots, y_n)$ and $z = (z_1, z_2, \cdots, z_n)$. Let $D_{x,z} = \{i \mid x_i \neq z_i\}$, then clearly $D_{x,z} = S \cup T$ where $S = \{i \mid x_i \neq z_i, x_i = y_i\}$ and $T = \{i \mid x_i \neq z_i, x_i \neq y_i\}$. It follows that

$$|T| \leq d(x, y)$$

and since $i \in S$, then $y_i = x_i \neq z_i$. Therefore

$$|S| \leq d(y, z)$$

which yields

$$d(x, z) = |D_{x,z}| = |S| + |T| \leq d(x, y) + d(y, z)$$

as required. □

DEFINITION A.1.4. (Closest Point Set)
Let C be a code and let $x \in C$. Define $P_C(x) := \{\, c \in C \mid d(x, c) = d(x, C)\}$.

REMARK A.1.5.
In this thesis, $\mathbb{F}$ is always finite, certainly $P_C(x)$ must not be empty.

DEFINITION A.1.6. (Majority Logic Decoding)
The Majority Logic Decoding (MLD) scheme is the process where the received word $c + e$ is decoded as $P_C(c + e)$.

The following lemma is important in that it describes when the closest point set is a singleton set. It illustrates the importance of the minimum distance.

LEMMA A.1.7.
Let C be a code and let $d(C) = 2t + 1$ or $d(C) = 2t + 2$ for some $t \in \mathbb{N}$. If $wt(e) \leq t$, then $P_C(c + e)$ = {c}.

PROOF
Let $f = c+e$, then we have $d(f, c) = wt(e) \leq t$. Suppose $c' \in C$ and $c' \neq c$ such that $d(c', f) \leq wt(e)$, then $2t + 1 = d(C) \leq d(c', c) \leq d(c', f) + d(f, c) \leq 2wt(e) \leq 2t$ which is a contradiction. Therefore c is the closest to f. The case $d(C) = 2t + 2$ uses exactly the same proof. □

Notation
For convenience, when there is no chance of confusion we think of $P_C(c + e)$ as an element, not a set.

REMARK A.1.8.
The above lemma says that if the receiver receives $c + e$ and $wt(e) \leq t$, then by computing $P_C(c + e)$ the original message can be recovered. Computing the closest point set while assuming $wt(e) \leq t$ is

referred to as the decoding problem. A large portion of this thesis is devoted to the decoding problem for Algebraic Geometric codes.

A.2 Linear Codes

Large block codes that lack some internal structure can be difficult to define and decode. It is even difficult to determine whether a vector is a codeword or not. This motivates the development of linear codes.

DEFINITION A.2.1. (Linear Code, Rank)
Let $\mathbb{F}$ be a field. A linear code C, of length n is a three-tuple (U, G, H) where U is a vector-subspace of $\mathbb{F}^n$ and $G : \mathbb{F}^{\dim U} \to \mathbb{F}^n$ is a linear operator such that $\mathrm{im}G = U$, and $H : \mathbb{F}^n \to \mathbb{F}^{n-\dim U}$ such that $\ker H = U$. The rank of C is the dimension of U.

DEFINITION A.2.2. (Generator Matrix)
The linear operator G in matrix form is called the generator matrix.

REMARK A.2.3.
Note that G or H uniquely determines U.

Notation
We abuse notation a little by referring to the vector space U as C. When there is no chance of a confusion, C refers to the associated subspace U. Also the linear operators G and H are almost always expressed explicitly as matrices.

A code is useless if it can not convey information. So it is important to understand how we represent information using a linear code. Let C be a linear code and let m be the rank of C. Fix a basis of C, say, $c_1, c_2, ..., c_m$. We can represent a m-digit information block, $(d_1, d_2, ..., d_m)$, as the vector $d_1c_1 + d_2c_2 + ... + d_mc_m$. So every vector in C represents m-bits of information.

In coding theory, we take $\mathbb{F}$ to be a finite field of size q, say. So a linear code C of rank m have q^m distinct vectors. If each vector represent a different symbol, then C can be thought of as an alphabet of size q^m .

Notation
Let $\mathbb{F} = \mathbb{F}_q$. We call a linear code of length n, rank k and minimum distance d a q-ary $[n, k, d]$ code. This is standard notation.

DEFINITION A.2.4. (Dual)
Let C be a q-ary $[n, k, d]$ code. Define an inner product

$$\langle x, y \rangle := \sum_{i=1}^{n} x_i y_i$$

, where $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$. We say x is orthogonal to y if $\langle x, y \rangle = 0$. We define the dual of C to be the set

$$C^{\perp} := \{x \in \mathbb{F}^n \mid \langle x, c \rangle = 0 \, \forall \, c \in C\}$$

REMARK A.2.5.
1. The space $C^{\perp}$ is the orthogonal complement to C.
2. It can easily be shown that $C^{\perp}$ is a subspace of $\mathbb{F}^n$ and therefore is also a linear code.
3. The dimension of $C^{\perp}$ is $n - k$ since we have $\mathbb{F}^n = C \oplus C^{\perp}$ by an elementary result in functional analysis.
4. We also have $(C^{\perp})^{\perp} = C$

DEFINITION A.2.6. (Parity Check Matrix)
Let $C^{\perp}$ have basis $c'_1, c'_2, ..., c'_{n-k}$, and assume c'_i is a row vector for all i between 1 and $n - k$, then the matrix

$$H = \begin{pmatrix} c'_1 \\ c'_2 \\ \vdots \\ c'_{n-k} \end{pmatrix}$$

is called the parity check matrix of C.

LEMMA A.2.7.
Let H be as above, then $Hc^T = 0$ if and only if $c \in C$.

PROOF
Clearly, if $c \in C$ then $\langle c, c'_i \rangle = 0$ for all i. By definition of H, we have

$$Hc^T = \begin{pmatrix} \langle c'_1, c \rangle \\ \langle c'_2, c \rangle \\ \vdots \\ \langle c'_{n-m}, c \rangle \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Conversely, suppose $Hc^T = 0$, i.e. $\langle c'_i, c \rangle = 0$ for all i between 1 and $n - k$. Since the inner proudct is linear, any linear combination of the c'_i's is also orthogonal to c, i.e. every element of $C^{\perp}$ is orthogonal to c, by definition $c \in (C^{\perp})^{\perp} = C$. $\square$

REMARK A.2.8.
Note that the parity check matrix H is the generator matrix for $C^{\perp}$.

REMARK A.2.9.
The matrix H allows us to decide whether a vector c is a codeword or not, but this does not tell us how to compute $P_C(c+e)$. Some texts do not require the rows of H to be linearly indepedent.

LEMMA A.2.10.
Let C be a code of length n. Then $\dim C + \dim C^{\perp} = n$

PROOF
Consider the parity check matrix H as a linear operator, then we have $\dim \mathrm{im} H + \dim \ker H = n$. But $\dim \ker H = \dim C = k$ and we have $\dim \mathrm{im} H = \mathrm{rank} H = \dim C^{\perp} = n - k$. $\square$

APPENDIX B

A Large Scale MVS Example

Consider the code $C_\Omega(B, 19Q)$ where $C : X^5 + Y^4Z + YZ^4 = 0$ is the 4-Hermitian Curve form 2, and $Q = [0 : 1 : 0]$. Let $B = P_1 + P_2 + \cdots + P_{16}$, where

$$\begin{array}{cccc} P_1 = [1 : w : 1]; & P_2 = [1 : w^2 : 1]; & P_3 = [1 : w^4 : 1]; & P_4 = [1 : w^8 : 1]; \\ P_5 = [w^3 : w : 1]; & P_6 = [w^3 : w^2 : 1]; & P_7 = [w^3 : w^4 : 1]; & P_8 = [w^3 : w^8 : 1]; \\ P_9 = [w^6 : w : 1]; & P_{10} = [w^6 : w^2 : 1]; & P_{11} = [w^6 : w^4 : 1]; & P_{12} = [w^6 : w^8 : 1]; \\ P_{13} = [w^9 : w : 1]; & P_{14} = [w^9 : w^2 : 1]; & P_{15} = [w^9 : w^4 : 1]; & P_{16} = [w^9 : w^8 : 1]; \end{array}$$

We recall $\mathbb{F}[16] := \mathbb{F}[2][w]$ where $w^4 + w + 1 = 0$. Also recall that

$$L(19Q) = \langle 1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, x^4, x^3y, x^2y^2, xy^3 \rangle$$

By the example following Remark 6.3.24. we have $d_{FR}(C_\Omega(B, 19Q)) = 9$. Therefore $t = 4$ errors can be corrected. We consider the $t + g = 10$ by 10 syndrome matrix S.

Assume we know only $c + e$ for some $c \in C_\Omega(B, 19Q)$. Consider the case where

$$e = (0, 1, w, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, w, w^2)$$

For convenience, we index the functions by their order at P, and write $\varphi_{4i+5j} = x^i y^j$ for $4i + 5j \leq 19$ noting that the representation is unique. Also, let $h_{i,j} := \varphi_i \varphi_j \cdot e$ and the (i, j)th position of S refers to

the position that $h_{i,j}$ is located, instead of the position situated in the ith row and jth column. We have

$$S := \begin{pmatrix} w^8 & w^9 & w^4 & w^5 & w^3 & w^7 & w^{10} & w^9 & w^{11} & w \\ w^9 & w^5 & w^3 & w^{10} & w^9 & w^{11} & w^{13} & w^{13} & w^9 & w^6 \\ w^4 & w^3 & w^7 & w^9 & w^{11} & w & w^{13} & w^9 & w^6 & h_{5,15} \\ w^5 & w^{10} & w^9 & w^{13} & w^{13} & w^9 & h_{8,12} & h_{8,13} & h_{8,14} & h_{8,15} \\ w^3 & w^9 & w^{11} & w^{13} & w^9 & w^6 & h_{9,12} & h_{9,13} & h_{9,14} & h_{9,15} \\ w^7 & w^{11} & w & w^9 & w^{61} & h_{10,10} & h_{10,12} & h_{10,13} & h_{10,14} & h_{10,15} \\ w^{10} & w^{13} & w^{13} & h_{12,8} & h_{12,9} & h_{12,10} & h_{12,12} & h_{12,13} & h_{12,14} & h_{12,15} \\ w^9 & w^13 & w^9 & h_{13,8} & h_{13,9} & h_{13,10} & h_{13,12} & h_{13,13} & h_{13,14} & h_{13,15} \\ w^{11} & w^9 & w^6 & h_{14,8} & h_{14,9} & h_{14,10} & h_{14,12} & h_{14,13} & h_{14,14} & h_{14,15} \\ w & w^6 & h_{15,5} & h_{15,8} & h_{15,9} & h_{15,10} & h_{15,12} & h_{15,13} & h_{15,14} & h_{15,15} \end{pmatrix}$$

where the values not computable by the Syndrome Lemma are shown as $h_{i,j}$'s. Let $R_S = (r_{i,j})$. We compute the $r_{i,j}$'s where we can and we have

$$R_S := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & r_{5,15} \\ 1 & 2 & 3 & 3 & 3 & 3 & r_{8,12} & r_{8,13} & r_{8,14} & r_{8,15} \\ 1 & 2 & 3 & 3 & 4 & 4 & r_{9,12} & r_{9,13} & r_{9,14} & r_{9,15} \\ 1 & 2 & 3 & 3 & 4 & r_{10,10} & r_{10,12} & r_{10,13} & r_{10,14} & r_{10,15} \\ 1 & 2 & 3 & r_{12,8} & r_{12,9} & r_{12,10} & r_{12,12} & r_{12,13} & r_{12,14} & r_{12,15} \\ 1 & 2 & 3 & r_{13,8} & r_{13,9} & r_{13,10} & r_{13,12} & r_{13,13} & r_{13,14} & r_{13,15} \\ 1 & 2 & 3 & r_{14,8} & r_{14,9} & r_{14,10} & r_{14,12} & r_{14,13} & r_{14,14} & r_{14,15} \\ 1 & 2 & r_{15,5} & r_{15,8} & r_{15,9} & r_{15,10} & r_{15,12} & r_{15,13} & r_{15,14} & r_{15,15} \end{pmatrix}$$

Although we do not yet know the values of $h_{5,15}$ or $h_{15,5}$, we can deduce that $r_{5,15} = 3 = r_{15,5}$. We see that $(8, 12), (10, 10), (12, 8)$ are the only candidates. Since the matrix is symmetric, $(8, 12)$ and $(12, 8)$ must produce the same vote, and since there are a total of only three votes, they must be correct candidates. We find an linear row relation in $S_{\leq 8,\leq 10}$, by solving for the α_i's in the following linear system

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} \begin{pmatrix} w^8 & w^9 & w^4 & w^5 & w^3 & w^7 \\ w^9 & w^5 & w^3 & w^{10} & w^9 & w^{11} \\ w^4 & w^3 & w^7 & w^9 & w^{11} & w \end{pmatrix} = \begin{pmatrix} w^5 & w^{10} & w^9 & w^{13} & w^{13} & w^9 \end{pmatrix}$$

One solution is $(\alpha_1, \alpha_2, \alpha_3) = (w^9, w^7, 0)$. Therefore, we have

$$h_{8,12} = w^9 w^{10} + w^7 w^{13} = w^{19} + w^{20} = w^4 + w^5 = w^8$$

We have $h_{8,12} = x^5 \cdot e = h_{12,8}$, and recall that the values of $h_{5,15}$, $h_{15,5}$ and $h_{10,10}$ can be calculated using $h_{8,12}$. Indeed,

$$h_{5,15} = h_{15,5} = h_{10,10} = y^4 \cdot e = (x^5 + y) \cdot e = h_{8,12} + h_{0,5} = w^8 + w^4 = w^5$$

Updating the syndrome matrix and the rank matrix gives

$$S = \begin{pmatrix} w^8 & w^9 & w^4 & w^5 & w^3 & w^7 & w^{10} & w^9 & w^{11} & w \\ w^9 & w^5 & w^3 & w^{10} & w^9 & w^{11} & w^{13} & w^{13} & w^9 & w^6 \\ w^4 & w^3 & w^7 & w^9 & w^{11} & w & w^{13} & w^9 & w^6 & w^5 \\ w^5 & w^{10} & w^9 & w^{13} & w^{13} & w^9 & w^8 & h_{8,13} & h_{8,14} & h_{8,15} \\ w^3 & w^9 & w^{11} & w^{13} & w^9 & w^6 & h_{9,12} & h_{9,13} & h_{9,14} & h_{9,15} \\ w^7 & w^{11} & w & w^9 & w^{61} & w^5 & h_{10,12} & h_{10,13} & h_{10,14} & h_{10,15} \\ w^{10} & w^{13} & w^{13} & h_{12,8} & h_{12,9} & h_{12,10} & h_{12,12} & h_{12,13} & h_{12,14} & h_{12,15} \\ w^9 & w^13 & w^9 & h_{13,8} & h_{13,9} & h_{13,10} & h_{13,12} & h_{13,13} & h_{13,14} & h_{13,15} \\ w^{11} & w^9 & w^6 & h_{14,8} & h_{14,9} & h_{14,10} & h_{14,12} & h_{14,13} & h_{14,14} & h_{14,15} \\ w & w^6 & w^8 & h_{15,8} & h_{15,9} & h_{15,10} & h_{15,12} & h_{15,13} & h_{15,14} & h_{15,15} \end{pmatrix}$$

and

$$R_S = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 3 & 3 & 3 & 3 & r_{8,13} & r_{8,14} & r_{8,15} \\ 1 & 2 & 3 & 3 & 4 & 4 & r_{9,12} & r_{9,13} & r_{9,14} & r_{9,15} \\ 1 & 2 & 3 & 3 & 4 & 4 & r_{10,12} & r_{10,13} & r_{10,14} & r_{10,15} \\ 1 & 2 & 3 & 3 & r_{12,9} & r_{12,10} & r_{12,12} & r_{12,13} & r_{12,14} & r_{12,15} \\ 1 & 2 & 3 & r_{13,8} & r_{13,9} & r_{13,10} & r_{13,12} & r_{13,13} & r_{13,14} & r_{13,15} \\ 1 & 2 & 3 & r_{14,8} & r_{14,9} & r_{14,10} & r_{14,12} & r_{14,13} & r_{14,14} & r_{14,15} \\ 1 & 2 & 3 & r_{15,8} & r_{15,9} & r_{15,10} & r_{15,12} & r_{15,13} & r_{15,14} & r_{15,15} \end{pmatrix}$$

From R_S we can see that $(8, 13)$ and $(13, 8)$ are the candidates and so they are both true candidates, since they produce the same vote and the number of correct votes is in the majority. Again by looking for row relations, we get

$$h_{8,13} = w^9 h_{0,13} + w^7 h_{4,13} = w^3 + w^5 = w^{11}$$

and

$$h_{9,12} = (xy \times x^3) \cdot e = (x^2 \times x^2 y) \cdot e = h_{8,13} = w^{11}$$

We update the table

$$S = \begin{pmatrix} w^8 & w^9 & w^4 & w^5 & w^3 & w^7 & w^{10} & w^9 & w^{11} & w \\ w^9 & w^5 & w^3 & w^{10} & w^9 & w^{11} & w^{13} & w^{13} & w^9 & w^6 \\ w^4 & w^3 & w^7 & w^9 & w^{11} & w & w^{13} & w^9 & w^6 & w^5 \\ w^5 & w^{10} & w^9 & w^{13} & w^{13} & w^9 & w^8 & w^{11} & h_{8,14} & h_{8,15} \\ w^3 & w^9 & w^{11} & w^{13} & w^9 & w^6 & w^{11} & h_{9,13} & h_{9,14} & h_{9,15} \\ w^7 & w^{11} & w & w^9 & w^{61} & w^5 & h_{10,12} & h_{10,13} & h_{10,14} & h_{10,15} \\ w^{10} & w^{13} & w^{13} & w^8 & w^11 & h_{12,10} & h_{12,12} & h_{12,13} & h_{12,14} & h_{12,15} \\ w^9 & w^13 & w^9 & w^11 & h_{13,9} & h_{13,10} & h_{13,12} & h_{13,13} & h_{13,14} & h_{13,15} \\ w^{11} & w^9 & w^6 & h_{14,8} & h_{14,9} & h_{14,10} & h_{14,12} & h_{14,13} & h_{14,14} & h_{14,15} \\ w & w^6 & w^5 & h_{15,8} & h_{15,9} & h_{15,10} & h_{15,12} & h_{15,13} & h_{15,14} & h_{15,15} \end{pmatrix}$$

Continuing in this way, we get all the required syndromes

$$S = \begin{pmatrix} w^8 & w^9 & w^4 & w^5 & w^3 & w^7 & w^{10} & w^9 & w^{11} & w \\ w^9 & w^5 & w^3 & w^{10} & w^9 & w^{11} & w^{13} & w^{13} & w^9 & w^6 \\ w^4 & w^3 & w^7 & w^9 & w^{11} & w & w^{13} & w^9 & w^6 & w^5 \\ w^5 & w^{10} & w^9 & w^{13} & w^{13} & w^9 & w^8 & w^{11} & w^2 & w^9 \\ w^3 & w^9 & w^{11} & w^{13} & w^9 & w^6 & w^{11} & w^2 & w^9 & h_{9,15} \\ w^7 & w^{11} & w & w^9 & w^{61} & w^5 & w^2 & w^9 & h_{10,14} & h_{10,15} \\ w^{10} & w^{13} & w^{13} & w^8 & w^11 & w^2 & h_{12,12} & h_{12,13} & h_{12,14} & h_{12,15} \\ w^9 & w^13 & w^9 & w^11 & w^2 & w^9 & h_{13,12} & h_{13,13} & h_{13,14} & h_{13,15} \\ w^{11} & w^9 & w^6 & w^2 & w^9 & h_{14,10} & h_{14,12} & h_{14,13} & h_{14,14} & h_{14,15} \\ w & w^6 & w^5 & w^9 & h_{15,9} & h_{15,10} & h_{15,12} & h_{15,13} & h_{15,14} & h_{15,15} \end{pmatrix}$$

Let c_i be the ith column of S. We see that

$$w^9 c_1 + w^7 c_2 + c_4 = 0$$

From which we can deduce that

$$\phi = w^9 + w^7 x + x^2 = (x+1)(x+w^9)$$

is an error locator of e. The zeroes of ϕ are $P_1, P_2, P_3, P_4, P_{13}, P_{14}, P_{15}$ and P_{16}. We see that $\phi \in L(8Q)$, and

$$d(C_\Omega(B, 19Q)) \geq d_{FR}(C_\Omega(B, 19Q)) = 9 > d(8Q)$$

Therefore by Corollary 5.2.10 the errorword is the unique solution to the following linear system

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & w^9 & w^9 & w^9 & w^9 \\ w & w^2 & w^4 & w^8 & w & w^2 & w^4 & w^8 \\ 1 & 1 & 1 & 1 & w^3 & w^3 & w^3 & w^3 \\ w & w^2 & w^4 & w^8 & w^{10} & w^{11} & w^{13} & w^2 \\ w^2 & w^4 & w^8 & w & w^2 & w^4 & w^8 & w \\ 1 & 1 & 1 & 1 & w^{12} & w^{12} & w^{12} & w^{12} \\ w & w^2 & w^4 & w^8 & w^4 & w^5 & w^7 & w^{11} \\ w^2 & w^4 & w^8 & w & w^{11} & w^{13} & w^2 & w^{10} \\ w^3 & w^6 & w^{12} & w^9 & w^3 & w^6 & w^{12} & w^9 \\ 1 & 1 & 1 & 1 & w^6 & w^6 & w^6 & w^6 \\ w & w^2 & w^4 & w^8 & w^{13} & w^{14} & w & w^5 \\ w^2 & w^4 & w^8 & w & w^5 & w^7 & w^{11} & w^4 \\ w^3 & w^6 & w^{12} & w^9 & w^{12} & 1 & w^6 & w^3 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_{13} \\ e_{14} \\ e_{15} \\ e_{16} \end{pmatrix} = \begin{pmatrix} w^8 \\ w^9 \\ w^4 \\ w^5 \\ w^3 \\ w^7 \\ w^{10} \\ w^9 \\ w^{11} \\ w \\ w^{13} \\ w^{13} \\ w^9 \\ w^6 \end{pmatrix}$$

which has the unique solution $e_2 = 1$, $e_3 = w$, $e_{15} = w$, $e_{16} = w^2$ and $e_i = 0$ for i not equal to $2, 3, 15$ or 16 as given.