1.1 Finite Field

A finite field is a field with finite number of elements. The order of finite field is the number of elements in the field. The order is always a prime or power of prime. Finite field is also called Galois field. Finite field is important in number theory, algebraic geometry, Galois Theory, Cryptography and Coding theory. The finite field is classified as follows [1]

- The order or number of elements of field is of the form \( p^n \), where \( p \) is a prime number called the characteristic of the field and \( n \) is a positive integer.
- For every prime number \( p \) and positive integer \( n \), there exists a finite field with \( p^n \) elements.
- Any two finite fields with same number of elements are isomorphic.

Notation for the finite field is \( \mathbb{F}_p \). It can also be represented as \( \text{GF}(p^n) \) where GF stands for Galois field. The finite field \( \text{GF}(2) \) consists of elements 0 and 1.

1.1.1 Construction of finite fields

To construct \( \text{GF}(p^n) \), first we have to find an irreducible polynomial or minimal \( g \).
Definition 1.1 (Irreducible polynomial [2]): A polynomial \( g \in F[x] \) is said to be irreducible over a finite field \( F \) if \( g \) has a positive degree and \( g = b \cdot c \) with \( b, c \in F[x] \) implies that either \( b \) or \( c \) is a constant polynomial.

Definition 1.2 (Minimal Polynomial [2]): If \( \theta \in F \) is an algebraic field over \( k \), then the uniquely determined monic polynomial \( g \in k[x] \) generating a sub string \( \{ f \in k[x], f(\theta) = 0 \} \) of \( k[x] \) is called a minimal polynomial or irreducible polynomial of \( \theta \) over \( k \).

Properties of a Minimal polynomial include [2].

1. \( g \) is irreducible in \( k[x] \).
2. For \( f \in k[x], f(\theta) = 0 \), if and only if \( g \) divides \( f \).
3. \( g \) is monic polynomial in \( k[x] \) of least degree having \( \theta \) as a root.

The polynomial \( g \) is of degree \( n \) with coefficient in \( z_p \) (for any prime \( p \), \( z_p \) is the ring of integers) modulo \( p \) is field.

1.1.2 Properties of GF \((p^n)\) [3]

A Galois field will have following properties

i. It can be shown that for each positive integer \( n \), there exists an irreducible polynomial of degree \( n \) over GF \((p)\) for any \( p \).

ii. It can be shown that for each divisor \( m \) of \( n \), GF \((p^n)\) has a unique sub field of order \( p^m \) moreover these are the sub fields of GF \((p^n)\).

Theorem 1.1[3] Let \( \theta \in F \) be algebraic field of degree \( n \) over \( K \) and let \( g \) be the minimal polynomial of \( \theta \) over \( K \). Then

1. \( K(\theta) \) is isomorphic to \( K[x]/g \).
2. \( |K(\theta)|/|K| = n \) and \( \{1, \theta, \ldots, \theta^{n-1}\} \) is a basis of \( K(\theta) \) over \( K \).
3. Every \( \alpha \in K(\theta) \) is algebraic over \( K \) and its degree over \( K \) is a divisor of \( n \).

Theorem 1.2: (Existence of Finite Field [3]) For every prime \( p \) and every positive integer there exists a finite field with \( p^n \) elements.
Theorem 1.3[3]: For every finite field $F_q$ the multiplicative group $F_q^*$ of non-zero elements of $F_q$ is cyclic.

Definition 1.3: (Primitive element [3]) A generator of the cyclic group $F_q^*$ is called the primitive element of $F_q$.

Theorem 1.4[3]: Let $F_q$ be a finite field and $F_r$ be a finite extension field, then $F_r$ is a simple algebraic extension of $F_q$ and every primitive element of $F_r$ can serve as a defining element of $F_r$ over $F_q$.

Theorem 1.5[3]: If $F$ is an irreducible polynomial in $F_q[x]$ of degree $m$, then $F$ has a root $\alpha$ in $F_q^m$. Furthermore all roots of $F$ are simple and are given by the distinct $n$ elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ of $F_q^m$.

1.1.3 Finite field arithmetic

Arithmetic in finite field is different from standard integer arithmetic. There is limited number of elements in finite field and for all operations performed in the finite field, the result will be elements in the finite field. While each element in the finite field itself is not infinite, there are infinitely many different finite fields. Their number is necessarily of the form $p^n$, where $p$ is a prime number and $n$ is a positive integer. One can perform operations such as addition, multiplication, and subtraction using the usual operations on integers followed by modulo $p$.

E.g. $GF(5) \rightarrow 4 + 5 = 9$ is reduced to 4.

E.g. [3]: To represent the elements of $F_4$, let $F_4$ is regarded as a simple algebraic extension of $F_3$ of degree 2. This is obtained by conjunction of root of an irreducible quadratic polynomial over $F_3$ say $F(x) = x^2 + 1$ in $F_3[x]$. Thus $F(\alpha) = \alpha^2 + 1 = 0$ in $F_9$ and nine elements of $F_9$ is given by $\{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$. Here $a_0 + a_1\alpha$ form primitive element.
Chapter I

a. Addition and Subtraction

Addition and Subtraction of two finite fields are implemented in the intuitive way of adding and subtracting the coefficients and performing the modular reduction by subtracting or adding $p$ until the resulting coefficient is non-negative and less than $p$.

b. Multiplication

Multiplication is done in two stages: Multiply two polynomials, $A(x)$ and $B(x)$, using ordinary polynomial multiplication to form an intermediate product $c'(x)$ to produce the result $c(x)$.

c. Polynomial Exponentiation

Although raising a polynomial $A(x)$ to the $n^{th}$ power can be obtained by multiplying $A(x)$ $n$ times which is $O(n)$, this is very difficult for large $n$. Thus repeated squaring can be used, which can be obtained with complexity $O(\log n)$.

1.2 Coding Theory

Clauds Shannon ’s 1948 paper ‘A mathematical theory of communications’ give birth to twin disciplines Information theory and Coding theory. The basic goals of these disciplines are efficient and reliable communication in an uncooperative environment. To be efficient, the transfer of information must not require a prohibitive amount of time and effort. To be reliable, the received data stream must resemble the transmitted stream with narrow tolerances. [3]

1.2.1 General Communication System

Let us review the simplest communication scenario (The point – to-point communication).Shannon model of communication is as follows.
A source (emitting speech, audio, data etc) transmits via a noisy channel (e.g.: phone line, optical link, wireless storage medium) to a destination. But we are interested in a reliable transmission i.e. we would like to recreate the transmitted information with as little distortion as possible as transmitted. A more specific model of communication can be as follows

Message is passed through an encoder, which encodes the message. By encoding, k-tuple message is converted into a code word of n-tuple. This code word is passed through a channel. A channel is a discrete memory less channel. The channel is discrete because we shall only consider finite alphabets. It is memory less, in the sense, error in one symbol will not affect the reliability of the neighboring symbols. The decoder receives from the channel an n-tuple of symbols. Then the decoder decodes the information to get the transmitted image. Decoding involves the process of error detection and correction also.
The aim of coding is to provide secure transmission of message, in the sense that errors occurred during the transmission can be corrected. In the coding theory, basic thing is the creation of code words. The code word should be created in such a way that it is possible for

- Fast encoding of information.
- Easy transmission of encoded messages.
- Fast decoding of received messages.
- Correction of errors introduced in the channel.
- Maximum transfer of information per unit time.

### 1.2.2 Codes and Types of codes

A code $C$ over an alphabet $A$ is simply a subset of $A^n = A \times A \times \ldots \times A$ (n copies). Elements of a code are called code words and the length of the code is $n$, where $A$ is a finite field $\mathbb{F}_q$. The dimension of a linear code $C$ is defined as a vector space over $\mathbb{F}_q$.

Important parameters of code include

1. Information rate: It is the number that is designated to measure the proportion of each code word that is carrying the message and it is given by $k/n$ where $k$ is the dimension of code and $n$ is the length of the code.

2. Relative distance: It is the number of positions where two code words disagree.

Different types of codes include:

a. **Linear Code**

A code $C$ is a linear code, if $v + w$ is a word in $C$ so that $v$ and $w$ are in $C$. i.e. linear code is a code which is closed under addition of words.
For e.g.: \( c = \{000, 111\} \) is a linear code since
\[
\begin{align*}
000 + 000 & = 000 \\
111 + 111 & = 000 \\
111 + 000 & = 111 \\
000 + 111 & = 111
\end{align*}
\]

The distance of a linear code is equal to minimum weight of any non-zero code word. The parameter of a linear code can be defined as \((n, k, d)\) where \(n\) is the length of the code, \(k\) is the dimension of the code and \(d\) is the distance of the code.

If \( C \) is a linear code of length \( n \) and dimension \( k \), then any matrix whose rows form the basis for \( C \) is called generator matrix for \( C \). Generator matrix for a linear code must have \( k \) rows and \( n \) columns and rank \( K \).

Theorem 1.6[3] Generator Matrix: A matrix \( G \) is generator matrix for some linear code \( C \) if and only if rank \( G \) is equals to number of rows of \( G \).

Let \( C \) be a linear code of length \( n \) and dimension \( k \), if \( G \) is a generator for \( C \) and \( u \) is a word of length \( k \) written as a row vector then
\[
V = uG \quad \text{(1.1)}
\]

is a word in \( C \).

There is another matrix associated with a code and closely connected with a generator matrix. This matrix is called a parity check matrix and this matrix plays an important role in decoding of code, which is used for the purpose of error correction and detection.

A matrix \( H \) is called a parity check matrix for a linear code if the columns of \( H \) form a basis for the dual code \( C^\perp \). If \( C \) has a length \( n \) and
dimension $k$, then any parity check matrix of $C$ must have $n$ rows and $n-k$ columns and rank $n-k$.

Theorem 1.7[3]: A matrix $H$ is a parity check matrix for some linear code $C$ if and only if the columns of $H$ are linearly independent.

Theorem 1.8[3]: If $H$ is a parity check matrix for a linear code $C$ of length $n$ then $C$ consists precisely of all code words $V$ in $K$ such that

$$ VH = 0 \quad (1.2) $$

These results can be used for error detection and correction.

Theorem 1.9[3] Matrix $G$ and $H$ are generating and parity check matrices, respectively for some linear code if and only if

1. The rows of $G$ are linearly independent.
2. The columns of $H$ are linearly independent.
3. Number of rows of $G$ plus the number of columns of $H$ equals the number of columns of $G$, which is equal to number of rows of $H$.
4. $GH = 0$.

b. Hamming Code

A code of length $n = 2^r-1$, $r \geq 2$ having parity check matrix $H$ whose rows consists of all non-zero vectors of length $r$ is called a hamming code of length $2^r-1$. Parity check matrix $H$ for a hamming code $C$ contains all $r$ rows of weight $r$ and $r$ columns of $H$ are linear independent. Thus hamming code has dimension $2^r - 1 - r$ and contains $2^{2r-1-r}$ code words. Hamming codes are perfect error correcting codes.
c. Reed-Muller codes

This is another important class of codes, which includes the extended Hamming code. The r-th order Reed-Muller code of length $2^m$ is denoted by $RM(r, m), 0 \leq r \leq m$. We present a recursive definition of these codes

1. $R(0, m) = \{0, 0, 0, 1, 1, 1, 1, ...\}$
2. $RM(m, m) = K^{2^m}$
3. $RM(r, m) = \{(x, x + y) | x \in RM(r, m-1), y \in RM(r-1, m-1)\}; 0 < r < m$

Generator matrix of $RM(r, m)$ is defined by

$$G(r, m) = \begin{pmatrix} G(r, m-1) & G(r, m-1) \\ 0 & G(r-1, m-1) \end{pmatrix}$$

Theorem 1.10 [3]: The r-th order Reed-Muller code $RM(r, m)$ defined above have the following properties

1. Length $n = 2^m$
2. Distance $d = 2^{m-r}$
3. Dimension $k = \sum r^m(i)$
4. $RM(r-1, m)$ is contained in $RM(r, m)$
5. Dual code $RM(m-1-r, m)$, $r < m$

d. BCH codes

An Important class of multiple-error correcting code is the class of Bose Chaudhari-Hocquingham codes or BCH codes. They are important because of two reasons. Firstly they admit easy decoding scheme and secondly the class of BCH code is quite extensive.
e. Reed-Solomon code

Reed Solomon code is a linear systematic block code based on finite field theory. The basic building block of Reed-Solomon codes is a symbol composed of $m$ binary bits, where $m$ can be any natural numbers greater than or equal to 2. For a given length $m$, the length of all the Reed-Solomon codes composed of $m$ bit symbols is $2^m-1$. Reed-Solomon code is a special case of BCH code. An efficient algorithm for BCH code was discovered in 1968. We can apply same thing to reed-Solomon code also. An alternate definition of Reed-Solomon code is as follows

**Definition 1.4 [3]:** Given a finite field $F$ of size $q$, let $n = q-1$ and let $\alpha$ be a primitive $n$th root of unity in $F$. Also, let $1 \leq K \leq n$ then, the Reed-Solomon code for these parameters has a code word $(f_0, f_1, \ldots, f_{n-1})$. If and only if $\alpha, \alpha^1, \alpha^2, \ldots, \alpha^{n-k}$ are root of polynomial $p(x) = f_0 + f_1 x + \ldots + f_{n-1} x^{n-1}$.

With this definition, it is immediately seen that a Reed-Solomon code is a polynomial code. Let $g(x)$ be a generator polynomial, which is minimal, roots $\alpha, \alpha^2, \alpha^3 \ldots \alpha^{n-k}$ and the code words are exactly the polynomials that are divisible by $g(x)$.

Let $p(x) = V_0 + V_1 x + V_2 x^2 + \ldots + V_{n-1} x^{n-1}$ and $q(x) = f_0(x) + f_1(x) + \ldots + f_{n-1}(x^{n-1})$, using these facts we have

- $(f_0, f_1, \ldots, f_n)$ is a code word of the Reed-Solomon code
- iff $p(x)$ is of degree $< k$.
- iff $V_i = 0$ for $i = k, \ldots, n-1$.
- iff $q(\alpha^i) = 0$ for $i = 1, \ldots, n-k$.

We can say in Reed – Solomon code data encoded is visualized as a polynomial. The code relies on a theorem from algebra that states that any $k$ distinct point uniquely determines a polynomial of degree at most $k-1$. 
Next code that is important and used in our algorithm is algebraic geometric code. Algebraic geometric code is code based on Algebraic Curves. Here in our system we are making use of Elliptic curves. The detail of the code is given in section 1.4.

1.2.3 Bounds on Codes

Quality of codes is determined by two variants. They are transmission rate and relative distance. The transmission rate is given by $R = \frac{k}{n}$ and relative distance given by $\delta = \frac{d}{n}$, where $n$ is the length of the code, $k$ is the dimension and $d$ is the minimum distance. The main aim of coding theory is to generate codes that optimize these parameters [4, 5, 6]. Quality of code can be defined using bounds on codes.

a) Singleton bound

Let $C$ be a code over a finite field with dimension $k$, minimum distance $d$ and length $n$ then $d \leq n-k+1$. Any code having parameters, which meet singleton bond, is maximum separable code.

Definition 1.5[4] : Let $q$ be a prime power and let $n$, $d$ be positive integers with $d \leq n$, then the quantity $A_q(n, d)$ is defined as maximum value of $M$, such that there is a code over $F_q$ of length $n$ with $M$ code words and minimum distance $d$. By singleton bound, we will have $A_q(n, d) \leq q^{n-d+1}$.

b) Plotkin bound

Here we will set $\theta = 1-1/q$, then $A_q(n, d) = 0$ if $d < \theta n$ and $A_q(n, d) \leq d/d- \theta n$, if $d > \theta n$.

If we have a code that satisfied that the above condition, then we will say it is having Plotkin bound [4].
c) Gilbert – Vaishnamov bound

Here \( A_q(n, d) \leq q^n / v_q(n, d-1) \)

d) Asymptotic bounds

Since we are looking for codes, which have large dimension and large minimum distance with respect to \( n \), it makes sense to normalize these parameters by dividing by \( n \). Let \( C \) be a code over \( F_q \) of length \( n \) with \( q^k \) code words and minimum distance \( d \). As specified, \( R \) and \( \delta \) determines quality of code. Both \( R \) and \( \delta \) should be between 0 and 1 and \( C \) is a good code if both \( R \) and \( \delta \) is close to 1. Let \( q \) be a prime power and \( \delta \in R \) with \( 0 \leq \delta \leq 1 \) then

\[
a_q(\delta) = \frac{\log q(A_q(n, d))}{n}.
\]

We will see asymptotic version of Plotkin and Gilbert Varshnamov bounds. These bounds, give bounds on the value of \( a_q(\delta) \).

Asymptotic Plotkin bound [3, 4] is as follows

With \( \theta = 1 - 1/q \) we have \( a_q(\delta) = 1 - \delta / \theta \), if \( 0 \leq \delta \leq \theta \)

\[
a_q(\delta) = 0, \text{ if } 0 < \delta \leq 1.
\]

In order to define Gilbert Varshnomov bound we have to specify Hilbert entropy on set \( \theta = 1 - 1/q \) and define a function \( H_q(x) \) on an interval \( 0 \leq x \leq 0 \) by \( x = 0 \).

\[
H_q(x) = \begin{cases} 
0 & \text{if } x = 0 \\
\log q(q-1)-x \log q(x)-(1-x) & \text{if } 0 \leq x \leq q
\end{cases}
\]

The function \( H_q(x) \) is called Hilbert entropy function.
Asymptotic Gilbert – Varshamov bound [4] can be defined as follows find any \( \delta \) with \( 0 \leq \delta \leq q \), we have \( a_q(\delta) \geq 1 - H_q(\delta) \). The Fig 1.3 is a graph for Plotkin bound and Gilbert Varshamov bound.

![Plotkin and GV Bound](image)

1.3. Elliptic curves

1.3.1 Introduction

Elliptic curves are becoming more and important, not only as cryptographic applications but as important in mathematical theory. Elliptic curve originated from early mathematicians trying to find rational solutions to the cubic equations. Curves can be defined over affine plane, by adding points at infinity to affine plane to produce a projective plane and projective plane can be defined as follows

1. Affine Coordinates: Co-ordinates of the form \( f(x, y) = 0 \) where \( f \) is a non-zero polynomial.
2. Projective coordinates [8]: coordinates of the form \( f(x, y, z) = 0 \) where \( f \) is a non-zero polynomial of some degree \( d \) and projective rational solutions are \((x, y, z)\) and \((\lambda x, \lambda y, \lambda z)\) for \( \lambda = 0 \). We can define elliptic curve over a finite field \( \mathbb{F}_p \) as follows

Definition 1.5 \([7]\) \( E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \) \quad (1.3)

Where \( a_1, a_2 \ldots a_6 \in \mathbb{F}_p \) and \( \Delta \neq 0 \), \( \Delta \) is the discriminant of \( E \) and is defined as follows

1. \( \Delta = d_2^3 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \)

2. \( d_2 = a_1^2 + 4a_2 \)

3. \( d_4 = 2a_4 + 4a_2 \)

4. \( d_6 = a_3^2 + 4a_6 \)

5. \( d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \)

Let \( L \) be the extension field of \( \mathbb{F}_q \) then the set of rational points on \( E \) is

\[ E(L) = \{(x, y) \in L \times L: y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0\} \cup \{\infty\} \quad (1.4) \]

Where \( \infty \) is point at infinity and certain properties of the curve are as follows.

1) Equation \((1.3)\) is a Weierstrass equation.

2) Condition \( \Delta \neq 0 \) ensures that the elliptic curve is smooth, that is, there are no points at which curve have one or more tangent lines. The point \( \infty \) is the only point on the line at infinity that satisfies the projective form of Weierstrass equation.
3) The $L$-rational function points on $E$ are the points $(x, y)$ that satisfy the equation of the curve and whose coordinates $x$ and $y$ belong to $L$.

The point at infinity is considered as $L$ rational point for all extension fields of $L$ on $F_p$. We can transform the elliptic curve Equation (1.3) to

$$y^2 = x^3 + ax + b \quad (1.5)$$

where $a$ and $b \in F_p$, $F_p$ is finite field of size $p$. Such a curve is said to be super singular and has discriminant $\Delta = -a^3$. In this thesis we will be using elliptic curve of equation (1.5). Consider an elliptic curve $y^2 = x^3 + 6x + 5$ over field $F_8$.

The curve can be represented as follows as in Fig 1.5.

![Elliptic curve point representation](image)

**Fig 1.4 Elliptic curve point represent representation $E_3(6,5)$**

This is the representation of curve along with points using algorithm in MATLAB as specified in Appendix-A-II

### 1.3.2 Properties

Properties of an elliptic curve $y^2 = x^3 + ax + b$ [7] are

1. Identity: $P + \infty = \infty + P$ for all $P \in E (F_p)$. 

2. Negatives: If $P(x, y) \in E(F_p)$ then $(x, y) + (x, -y) = \infty$. The point $(x, -y)$ is denoted as $-p$ and is called negative of $P$.

### 1.3.3 Arithmetic of Elliptic curves

Arithmetic of elliptic curve includes all operations which can be done on points on a curve

**i. Point addition**

Let $P(x_1, y_1) \in E(F_p)$ and $Q(x_2, y_2) \in E(F_p)$ where $P \neq Q$, then $P + Q = (x_3, y_3)$ where

$$x_3 = \frac{(y_2 - y_1)(x_2 - x_1)^2 - x_1 - x_2}{1}$$(1.6)

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_3 - x_1) - y_1$$ (1.7)

Addition [7, 8] can be done by chord and tangent rule. The sum $R$ of two points $P$ and $Q$ is as follows. Draw a line through $P_1$ and $P_2$, this line intersect at $3^{rd}$ point. Then $P_3$ is the reflection of this point about the x-axis.

---

Figure: 1.5 Elliptic curve point addition
An example for elliptic curve addition is as follows. The curve equation is $y^2 = x^3 + ax + b$ with $a = -4$, $b = 4$. To add two points, draw a line through them and reflect the third point, where this line intersects the curve, in the x-axis.

![Elliptic curve addition example](image)

**Fig 1.6[8]** (Elliptic curve addition example)

The result of addition of points $A (-2, -2)$ and $B (1, 1)$ is $C (2, -2)$.

**ii. Point doubling**

Elliptic curve doubling occurs when $P = Q$. Doubling a point is a process of computing $P + P$, $P \in E$. Let $m$ be the slope of the curve,

If $y_1 \neq 0$ then $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$. Here we take slope as $(3x_1^2 + a)/2y_1$.

If $y_1 = 0$ then $P_1 + P_2 = \infty$. Also we can say $P + \infty = P$ for all points $P$ on $E$.

![Elliptic curve doubling](image)

**Figure 1.7 [8]**. Elliptic curve doubling
iii. Scalar multiplication

Scalar multiplication is a process of multiplying a scalar value with a point on curve. Let \( P \) be a point on curve, \( kP \), that means scalar multiplication of an integer \( k \) with a point \( P \). That is \( P + P + P + \ldots + P \) (\( k \) times). It is done by doubling and adding method. This property of elliptic curve is used in this thesis for implementation of cryptographic algorithm. Elliptic curve used in cryptography contains only finite number of points. The figure below shows scalar multiplication on elliptic curves.

iv. Point Subtraction

Point subtraction consists of point addition and point negation or point inverse. It is represented as \( P - Q \). This can be evaluated by point addition of the point \( P \) and inverse \( Q (\neg Q) \). i.e. \( R = P + (\neg Q) \).
1.4. Algebraic Geometric Codes

Algebraic Geometric codes are codes defined over curves. Algebraic geometric code is defined by V.D Goppa [5, 9, 10]. The curve used in algebraic geometric code is defined over a finite field $F_q$, here we can make use of affine and projective variety of curve whose dimension is one. This curve is absolutely irreducible and non-singular, equations of curve should be polynomials with coefficients of $F_q$.

The key aim of algebraic geometric code is to replace polynomial over a finite field by more general constructions. Goppa used language of algebraic curves to introduce codes. So we can call it as Algebraic Geometric codes. Before going into function and construction of algebraic geometric codes we will discuss certain factors used for describing the code. They include

1.4.1 Divisors

A divisor[6] $D$ on a curve $X$ is a formal sum of form $D = \sum n_P P$ where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but a finite number of points $P$ on $X$. Divisors are often thought to be the key stone to understand how Algebraic Geometry is formed and its relationship to curve. To describe it more clearly, let $C$ be a non-singular projective curve in $P_k$. The projective plane is over an algebraically closed field $K$. For each line $L$ in $P_k^2$, we consider $L \cap C$, which is a finite set of points on $C$. If $C$ is a curve of degree $d$ and if we counts points with proper multiplicity then $L \cap C$ will contains exactly $d$ points. So we can write $L \cap C = \sum n_P P$ where $P \in C$ are the points, $n_i$ the multiplicity and this formal sum is a divisor on $C$. As $L$ varies, we obtain a family of divisors on $C$ parameterized by the set of all lines in $P^2$, which is a dual projective space $(P_k^2)\ast$. We refer to this set of divisors as a linear system of divisors on $C$. If $P$ is a point of $C$, the set of divisors in the linear system contains $P$. They correspond to the lines $L \in (P_k^2)\ast$ passing through $P$ and this set of lines determines $P$ uniquely as a point in $P_k^2$. 
Another important thing in the construction of Algebraic Geometric code is order function. The order is a generalization of the degree of a function as well as its zeroes. There are two candidates, the x-order and the y-order. Usually they are the same; however care must be taken to ensure their accuracy.

Definition 1.6[6]: Let $X: f(x, y) = 0$ be a curve and $P (x=a, y=β)$ be a point on curve $X$ with $α$ and $β ∈ F$. Let $g (x, y) ∈ F [X]$, then the largest power $n$ for which there exists polynomials $g^0 ∈ F [X]$ and $h^0 (x, y) ∈ F [x, y]$ with $h^0 (0, 0) \neq 0$ such that

$$g = ((x- α) g^0 (x- α)/h^0 (x- α, y- β)) \mod f$$

is called the x-order of $g$ at $P$ and denoted by $\text{ord}_p (g)$. The x-order can be defined using the notation $V_{p,x} (g/h)$ and is $V_{p,x} (g) - V_{p,x} (h)$ and y order is defined analogously.

Let $F$ be a field. A discrete valuation $V$ on $F$ is a function $f$ to $Z$. It has the following properties

- $V (a, b) = V (a) + V (b)$
- $V (a + b) ≥ \min \{V (a), V (b)\}$
- $V (a) = 1$ for at least one $a$.

It is some times convenient to put $V (0) = ∞$, which preserves the axioms even when $a=0$ or $b=0$.

Proposition 1.1[8]: If $V$ is a discrete valuation then

$$V (1) = 0 \text{ and if } V (a) < V (b) \text{ then } V (a + b) = V (a).$$

Assume further $X$ is projective and $f ∈ K (X)^*$ then the following is equivalent

$$\text{Ord}_y (f) ≥ 0 \text{ for all } y$$

$$\text{Ord}_y (f) = 0 \text{ for all } y, f ∈ K^*.$$
The properties of $\text{ord}_y$ shown above allow us to define the divisor of a function. Let $X$ be a variety and $f \in K(X)$ be a rational function (section 1.4.2) on $X$, then divisor of $f$ is

$$\text{Div}(f) = \sum_y \text{ord}_y(f) y \in \text{Div}(X).$$

A divisor is said to be principal if it is the divisor of a function. Two divisors $D$ and $D'$ are linearly equivalent ($D \sim D'$), if the difference is a principal divisor. We can use notation $(f)$ for the divisor of $f$. The divisor at poles and zeroes denoted by $(f)_0$ and $(f)_\infty$, respectively.

$$(f)_0 = \sum_{\text{ord}_y(f) > 0} \text{ord}_y(f)y.$$

$$(f)_\infty = \sum_{\text{ord}_y(f) < 0} \text{ord}_y(f)y.$$

Thus we can say that divisor of a function is the difference between poles and zeroes.

1.4.2 Rational Functions

Let $X$ is a curve defined by a field $F$. On the points of $X$, any two polynomials that differ by multiples of $F$ have same value. So when we compare it with the curve they will be the same.

Definition 1.7 [6]: Rational function $R$ as the ratio $f = (x, y, z)/B(x, y, z)$ of two homogeneous polynomials of the same degree up to factorization modulo $F(x, y, z)$.

A rational function $f$ is defined at a point $P$, if there exists a representation $f = A/B$ such that $B(P) \neq 0$.

Another important thing we have to discuss before the construction and definition of algebraic geometric code is the space associated with the divisor. The space associated with the divisor can be called as linear space.
Chapter 1

Let \( D = \sum n_P P \), be a divisor and there are set of all functions satisfying \( V_p(f) \geq -n_P \) at every point \( P \), together with the zero function is called space associated to \( D \) and is denoted by \( L(D) \). For an effective divisor \( D \), \( L(D) \) consists of rational functions and all its poles lie in the \( \text{Supp} \, (D) \) and the multiplicity of each of them is not greater than \( n_P \). We can describe it with the help of a Lemma and a proof.

Lemma [1.1] Let \( D \in D \), then

1. If \( D' \) is linearly equivalent to \( D \), then \( L(D) \) is isomorphic to \( L(D') \) (as a vector space over \( K \))

2. If \( \text{deg}(D) < 0 \) then \( L(D) = \{0\} \)

3. \( L(0) = K \).

Proof: (1) As \( D \) and \( D' \) are equivalent there exists \( z \in K(X) \) such that \( D = D' + (z) \). Define a mapping \( \Phi : L(D) \rightarrow K(X) \), \( x \mapsto xz \). Clearly \( \Phi \) is \( k \)-linear and its image is contained in \( L(D') \): \( V_p(xz) = V_p(x) - V_p(y) \geq -n_p + V_p(z) = -n_p \) for every \( P \in X \). Moreover \( \Phi \) is bijective as \( \psi : L(D') \rightarrow L(D), x \mapsto xz^{-1} \) is an inverse of \( \Phi \).

(2) Assume that there exists \( x \in L(D) \), \( x \neq 0 \), then \( D' = D + (x) \) is effective and linearly equivalent to \( D \). Hence, \( 0 \leq \text{deg}(D') = \text{deg}(D) \), which is a contradiction.

3. Clearly \( K \) is contained in \( L(0) \). On the other hand, each element in \( L(0) \) has no poles, therefore it is a constant.

1.4.3 Riemann–Roch Theorem.

It is one of the famous theorems in algebraic geometry. It deals with computation of \( l(D) \), the dimension of vector space \( L(D) \). Let \( X \) be a curve defined over a projective field and let \( d \) be the degree of \( X \), \( g \) the genus of curve \( =(d-1)(d-2)/2 \). A canonical divisor \( w \) is also defined such that \( \text{deg}(w) = 2g-2 \) and \( l(w) = g \).
Theorem 1.11 [5] Given a divisor $D$, $l(D) = \deg(D) + 1 - g + l(w-D)$, where $w$ is any canonical divisor.

By making use of all the above discussed concepts of algebraic geometry we can define an algebraic geometric code by V.D Goppa as follows,

Let $X$ be a curve, $P$ be a set of points on the curve, $D$ be the divisor then the Algebraic Geometric code associated to $(X, P, D)$ is

$$C(X, P, D) := \{(f(p_1), f(p_2), \ldots, f(p_n)) \mid f \in \mathcal{L}(D)\} \subset F_q^n$$

In other words, the algebraic geometric code $C(X, P, D)$ is the image of the evaluation map

$$E: \mathcal{L}(D) \rightarrow F_q^n$$

$$f \mapsto (f(p_1), f(p_2), \ldots, f(p_n))$$

1.4.4 Construction of Algebraic Geometric Code

By making use of the definition described above we can construct a Goppa code as follows. Let $X$ be a curve, $P$ be a set of $n$ points on the curve $\{P_1, P_2, \ldots, P_n\}$ and divisor $D = P_1 - P_2 - \ldots - P_n$. Let $\mathcal{L}(D)$ denote vector space for the curve $X$, length of the vector space $l(D)$ as per Riemann Roch theorem is $l(D) = n + g - 1$. Let $g = 1$, genus of an elliptic curve is one (in this thesis we are concentrating only on elliptic curve). For an elliptic curve $d = 3$, and genus $g$ is given by $((d-1)(d-2))/2$. So $g$ here is 1. Then $l(D) = n = \#P$ (number of points on the curve). A code is represented by $(n, k, d)$ from where $n$ is the number of elements, $k$ is the dimension and $d$ is the distance.

The dimension $K$ is $\deg D + 1 - g$ and minimum distance $d > n - \deg D$ (Thus we are mapping $(X, P, D)$ to $(n, k, d)$ curve). Let $C = (X, P, D)$ be an algebraic geometric code and let $f_1, f_2, \ldots, f_k$ be a basis for the vector space $\mathcal{L}(D)$ over finite field $F_q$ under the conditions above dim $C = K$ and geometric matrix is defined as
An example for an Algebraic Geometric code over Hermition curve is as follows. Let our curve be $F=V(x^3+y^2z+yz^2)$ over the field $\mathbb{F}_4$. As this curve is smooth we can find genus of a curve by using Plucker's formula as $g=(3-1)(3-2)/2=1$. This curve contains 9 points.

\[\begin{array}{c}
\begin{aligned}
f_1(P_1) & \ldots & f_1(P_6) \\
. & \\
f_k(P_1) & \ldots & f_k(P_6)
\end{aligned}
\end{array}\]

Let $D$ be the divisor of the sum of eight affine points, that is

\[D = P_1 + \ldots + P_8.\]

Let the code be $C_L(D, 4Q)$. The 4 dimensional space $L(4Q)$ is spanned by the following basis functions. The numbers in parentheses indicate the order of the pole at point $Q$.

\[\Phi_1 = 1(0) \quad \Phi_2 = x/z(2) \quad \Phi_3 = y/z(3) \quad \Phi_4 = x^2/z^2(4)\]

with this information we can already give a generator matrix for the code $C_L(D, 4Q)$ by evaluating $\Phi_1, \ldots, \Phi_4$ at points $P_1, \ldots, P_8$. 

\[Q=(0:1:0)\]

\[P_1=(0:0:1) \quad P_2=(0:1:1) \quad P_3=(1:1:1)\]

\[P_4=(1:1:1) \quad P_5=(a:a:1) \quad P_6=(a:a^2:1)\]

\[P_7=(a^2:a:1) \quad P_8=(a^2:a^2:1)\]
\[ G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha \end{pmatrix} \]

1.5 References


