Algebraic Geometric Codes

Soham Chatterjee
sohamc@cmi.ac.in
BMC202175

Shree Ganesh S J
shreeganesh@cmi.ac.in
MCS202219

2023

Contents

CHAPTER 1

Mathematics

1.1 Divisors

1.2 Reimann-Roch Spaces

Definition 1.2.1 (Reimann-Roch Spaces). *For any divisor $\mathcal{D} \in \tilde{\mathfrak{D}}$*

$$\mathcal{L}(\mathcal{D}) = \{f \in \mathbb{F}(\mathcal{X})^* \mid (f) + \mathcal{D} \succcurlyeq 0\} \cup \{0\}$$

The dimension of $\mathcal{L}(\mathcal{D})$ over $\mathbb{F}$ is denoted by $l(\mathcal{D})$

Theorem 1.2.1. *(i) If $\deg(\mathcal{D}) < 0$ then $l(\mathcal{D}) = 0$*

(ii) $l(\mathcal{D}) \leq 1 + \deg(\mathcal{D})$

Theorem 1.2.2. $\mathcal{L}(0) = \mathbb{F}$. *Hence $l(0) = 1$*

1.3 Differentials

1.4 Reimann-Roch Theorem

Theorem 1.4.1 (Reimann-Roch Theorem). *$\mathcal{D}$ is a divisor on a smooth projective curve with genus g. Then for any canonical divisor W*

$$l(\mathcal{D}) - l(W - \mathcal{D}) = \deg(\mathcal{D}) - (g - 1)$$

Corollary 1.4.2. *For any canonical divisor W,* $\deg(W) = 2g - 2$

Proof: Take $\mathcal{D} = W$. Then $l(W - \mathcal{D}) = l(0) = 1$ by Theorem 1.2.2. So we have

$$l(W) - 1 = \deg(W) - (g - 1)$$

By definition $l(W) = g$. Hence we have $g - 1 = \deg(W) - (g - 1) \iff \deg(W) = 2g - 2$. ∎

With the help of this corollary we can finally focus on the divisors which we will actually use to define codes. The following corollary gives the dimension of the Reimann-Roch Spaces of divisors with degree more than $2g - 2$.

Corollary 1.4.3. *Let $\mathcal{D}$ be a divisor on a smooth projective curve of genus g and let* $\deg(\mathcal{D}) > 2g-2$. *Then*

$$l(\mathcal{D}) = \deg(D) - (g-1)$$

Proof: We have $\deg(W-\mathcal{D}) = \deg(W) - \deg(\mathcal{D})$. Now by Corollary 1.4.2 $\deg(W-\mathcal{D}) < 0$. So $l(W-\mathcal{D}) = 0$ by Theorem 1.2.1 part (ii). So We have $l(D) = \deg(D) - (g-1)$. ■

1.5 Index of speciality

Definition 1.5.1 (Index of speciality)**.** *Let $\mathcal{D}$ be a divisor on a curve $\mathcal{X}$. We define*

$$\Omega(\mathcal{D}) = \{\omega \in \Omega(\mathcal{X}) \mid (w) - D \succcurlyeq 0\}$$

and we denote the dimension of $\Omega(\mathcal{D})$ over $\mathbb{F}$ by $\delta(\mathcal{D})$ called the index of speciality of $\mathcal{D}$.

Theorem 1.5.1. $\delta(\mathcal{D}) = l(W-\mathcal{D})$

Proof: If $W = (\omega)$. Define the linear map $\varphi : \mathcal{L}(W-\mathcal{D}) \to \Omega(\mathcal{D})$ by $\varphi(f) = f\omega$.

$$f \in \mathcal{L}(W-\mathcal{D}) \implies (f) + W - \mathcal{D} \succcurlyeq 0 \iff (f) + (\omega) - \mathcal{D} \succcurlyeq \iff (f\omega) - \mathcal{D} \succcurlyeq 0 \iff f \in \Omega(\mathcal{D})$$

Hence φ is an isomorphism. Therefore $\delta(\mathcal{D}) = l(W-\mathcal{D})$ ■

CHAPTER 2

Codes from Algebraic Curves

We have now came to define the Algebraic Geometric Codes.

2.1 Preliminaries

First we will define the system where we will define the codes.

- Our alphabet will be $\mathbb{F}_q$
- We will consider the functions $f \in \mathbb{F}_q[X_1, \ldots, X_n]$. Sometimes we will write $\overline{\mathrm{X}}$ to denote $(X_1, \ldots, X_n)$. n depends on the context
- If the affine curve $\mathcal{X}$ over $\mathbb{F}_q$ is defined by a prime ideal I in $\mathbb{F}_q[\overline{\mathrm{X}}]$ then its coordinate ring $\mathbb{F}_q[\mathcal{X}] = \mathbb{F}_q[\overline{\mathrm{X}}]/I$ and its function field $\mathbb{F}_q(\mathcal{X})$ is the quotient field of $\mathbb{F}_q[\mathcal{X}]$.
- It is always assumed that the curve is *absolutely irreducible*, i.e. the defining ideal is also prime in $\mathbb{F}[\overline{\mathrm{X}}]$ where $\mathbb{F} := \overline{\mathbb{F}_q}$ i.e. $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_q$.

Similar adaptations are made for projective curves.

Observation. *For any $F \in \mathbb{F}_q[\overline{\mathrm{X}}]$, $F(x_1, \ldots, x_n)^q = F(x_1^q, \ldots, x_n^q)$. So if $(x_1, \ldots, x_n)$ is a zero of F and F is defined over $\mathbb{F}_q$ then $(x_1^q, \ldots, x_n^q)$ is also a zero of F.*

We can extend the *Frobenius Map*, $Fr : x \mapsto x^q$ coordinate-wise to points in affine and projective space by $Fr(x_1, \ldots, x_n) = (x_1^q, \ldots, x_n^q)$. If $\mathcal{X}$ is a curve defined over $\mathbb{F}_q$ and P is a point of $\mathcal{X}$, then $Fr(P)$ is also a point of $\mathcal{X}$.

Definition 2.1.1 (Rational Divisor)**.** *A divisor $\mathcal{D}$ on $\mathcal{X}$ is called rational if the coefficients of P and $Fr(P)$ is $\mathcal{D}$ are the same for any point P of $\mathcal{X}$.*

Remark: Now on the space $\mathcal{L}(\mathcal{D})$ will only be considered for rational divisors and as before but with the restriction of the rational functions to $\mathbb{F}_q(\mathcal{X})$

Let $\mathcal{W}$ be an absolutely irreducible nonsingular projective curve over $\mathbb{F}_q$. We will define two kinds of algebraic geometry codes from $\mathcal{X}$, *Geometric Reed Solomon Codes* and *Geometric Goppa Codes*. Let $P_1, \ldots, P_n$ are rational points

on $\mathcal{X}$ and $\mathcal{D}$ be the divisor $\mathcal{D} = P_1 + \cdots + P_n$. Furthermore $\mathcal{G}$ is some other divisor that has support disjoint from $\mathcal{D}$.
Remark: We will make more restrictions on $\mathcal{G}$, $\deg(\mathcal{G}) > 2g - 2$

2.2 Geometric Reed Solomon Codes

With the setting as above we define

Definition 2.2.1 (Geometric Reed Solomon Codes)**.** *The linear code $C(\mathcal{D}, \mathcal{G})$ of length n over $\mathbb{F}_q$ is the image of the linear map $\alpha : \mathcal{L}(\mathcal{G}) \to \mathbb{F}_q^n$ defined by $\alpha(f) = (f(P_1), \ldots, f(P_n))$*

Theorem 2.2.1. *The code $C(\mathcal{D}, \mathcal{G})$ has dimension*

$$k = \deg(\mathcal{G}) - (g - 1)$$

and distance

$$d \geq n - \deg(\mathcal{G})$$

Corollary 2.2.2. $k + d \geq n - (g - 1)$

Proof: $k + n \geq \deg(\mathcal{G}) - (g - 1) + n - \deg(\mathcal{G}) = n - (g - 1)$ ■

Example 2.2.3. *Let $\mathcal{X}$ be the projective line over $\mathbb{F}_{q^m}$. Hence genus $g = 0$. Let $n = q^m - 1$. Define $P_0 = (0 : 1)$, $P_\infty = (1 : 0)$. Let β be the primitive nth root of unity. Define $P_i = (\beta^i : 1)$ for all $i \in [n]$. Define $\mathcal{D} = \sum_{i=1}^{n} P_i$ and $\mathcal{G} = aP_0 + bP_\infty$ where $a, b \geq 0$ are non-negative integers. By Corollary 1.4.3, $l(\mathcal{G}) = a + b + 1$ and the functions $\left(\frac{x}{y}\right)^i$ for $-a \leq i \leq b$ forms a basis of $\mathcal{L}(\mathcal{G})$. Consider the code $C(\mathcal{D}, \mathcal{G})$. A generator matrix for this code has rows $(\beta^i, \beta^{2i}, \ldots, \beta^{ni})$ with $-a \leq i \leq b$. IT follows that $C(\mathcal{D}, \mathcal{G})$ is a Reed-Solomon Code.*

2.3 Geometric Goppa Codes

We now come to the second class of algebraic geometry codes.

Definition 2.3.1. *The linear code $C^*(\mathcal{D}, \mathcal{G})$ of length n over $\mathbb{F}_q$ is the image of the linear map $\alpha^* : \Omega(\mathcal{G} - \mathcal{D}) \to \mathbb{F}_q^n$ defined by*

$$\alpha^*(\omega) = (\mathrm{Res}_{P_1}(\eta), \ldots, \mathrm{Res}_{P_n}(\eta))$$

Theorem 2.3.1. *The code $C^*(\mathcal{D}, \mathcal{G})$ has dimension*

$$k^* = n - \deg(\mathcal{G}) + (g - 1)$$

and distance

$$d^* \geq \deg(\mathcal{G}) - 2(g - 1)$$

Corollary 2.3.2. $k^* + d^* \geq n - (g - 1)$

Proof: $k^* + d^* \geq n - \deg(\mathcal{G}) + (g - 1) + \deg(\mathcal{G}) - 2(g - 1) = n - (g - 1)$ ■

Example 2.3.3. *Let $L = \{\alpha_1, \ldots, \alpha_n\}$ be a set of n distinct elements of $\mathbb{F}_{q^m}$. Let g be a polynomail in $\mathbb{F}_{q^m}[X]$ which is not zero at α_i for all $i \in [n]$. The Classical Goppa Code $\Gamma(L, g)$ is defined by*

$$\Gamma(L, g) = \left\{ \bar{c} \in \mathbb{F}_q^n \mid \sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{g} \right\}$$

Let $P_i = (\alpha_i : 1)$, $Q = (1 : 0)$ and $\mathcal{D} = P_1 + \cdots + P_n$. If we take for E the divisor of zeros of g on the projective line, then

$$\Gamma(L, g) = C^*(\mathcal{D}, E - Q)$$

and

$$\bar{c} \in \Gamma(L, g) \iff \sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} dX \in \Omega(E - Q - \mathcal{D})$$

It is a well-known fact that the parity check matrix of the Goppa Code $\Gamma(L, g)$ is equal to the following generator matrix of a generalized RS code

$$\begin{bmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \ddots & \vdots \\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} g(\alpha_n)^{-1} \end{bmatrix}$$

where r is the degree of the Goppa polynomial g.

2.4 Relation between the 2 Codes

Theorem 2.4.1. *The codes $C(\mathcal{D}, \mathcal{G})$ and $C^*(\mathcal{D}, \mathcal{G})$ are dual codes.*

Theorem 2.4.2. *Let $\mathcal{X}$ be a curve defined over $\mathbb{F}_q$. Let $P_1, \ldots, P_n$ be n rational points on $\mathcal{X}$. Let $\mathcal{D} = P_1 + \cdots + P_n$. Then there exists a differential form ω with simple poles at the P_i such that $\mathrm{Res}_{P_i}(\omega) = 1$ for all $i \in [n]$. Furthermore*

$$C^*(\mathcal{D}, \mathcal{G}) = C(\mathcal{D}, W + \mathcal{D} - \mathcal{G})$$

So one can do without differentials and the codes $C^*(\mathcal{D}, \mathcal{G})$. However it is usefull to have both classes when treating decoding methods. These use parity check, so one needs a generator matrix for the dual codes.

Theorem 2.4.3. *For any algebraic geometry code with dimension k and distance k on a curve of genus g with n points that are defined over $\mathbb{F}_q$ satisfy*

$$k + d \geq n - (g - 1) \iff R + \delta \geq 1 - \frac{g - 1}{n}$$

CHAPTER 3

Assymptotically Good Sequences of Codes and Curves

CHAPTER 4

Bibliography