Report on Algebraic Geometry Codes

Soham Chatterjee
sohamc@cmi.ac.in
BMC202175

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

Course: Algorithmic Coding Theory
Instructor: Amit Kumar Sinhababu

Chennai Mathematical Institute

2023

Abstract

We, Soham Chatterjee, Bsc 2nd Year, Math and Computer Science and Shree Ganesh S J, Msc 2nd Year, Computer Science students of Chennai Mathematical Institute have created this report for the presentation on the introduction of Algebraic Geometric Codes to Prof. Amit Kumar Sinhababu for the course Algorithmic Coding Theory. We mainly followed the survey [BHHW98]. We also followed the course on Algebraic Geometric Codes by Gil Cohen, [Coh22]. He followed the book [Sti08]. Initial works on Algebraic Geometric Codes were done by V. D. Goppa that is why these codes are also called *Goppa Codes*. Goppa submitted his seminal paper [Gop77] i June 1975. Goppa also published more papers on this topic, [Gop81], [Gop84]. Later he published a book on Goppa Codes, [Gop88]. There are 2 more books [TV91] and [TVN07] on Algebraic Geometric Codes.

Contents

CHAPTER 1

Preliminaries

1.1 Introduction

This field of coding theory is studied since the publication of Goppa's paper describing them [Gop77], [Gop81], [Gop84]. These codes attracted interest in the coding theory community because they have the ability to surpass the Gilbert–Varshamov bound; at the time this was discovered, the Gilbert–Varshamov bound had not been broken in the 30 years since its discovery. This was demonstrated by Tfasman, Vlăduţ, and Zink in the same year as the code construction was published, in their paper [TVZ82]. To describe the construction of the codes we first need to set up the mathematics. We will define some objects like divisors, differentials which we need to define the code and also state some theorems. Then we will dive right into the construction and some bounds of the code.

1.2 Mathematics

1.2.1 Divisors

Definition 1.2.1 (Divisor)**.** *A divisor is a formal sum $\mathcal{D} = \sum_{P \in X} n_p P$ with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finite number of points P.*

The support of a divisor is the set of all points with nonzero coefficient. A divisor $\mathcal{D}$ is called *effective* if all coefficients n_P are nonnegative (We denote it by $\mathcal{D} \succcurlyeq 0$) The degree $\deg(\mathcal{D}) := \sum_{P \in X} n_P$.

Definition 1.2.2 (Principal Divisor)**.** *If f is a rational function on $\mathcal{X}$ not identically 0 the we define the divisor of f to be*

$$(f) = \sum_{P \in X} v_P(f) P$$

Divisor of a rational function is called a principal divisor.

Two divisors $\mathcal{D}, \mathcal{D}'$ are linearly equivalent if and only if $\mathcal{D} - \mathcal{D}'$ is a principal divisor

1.2.2 Reimann-Roch Spaces

Definition 1.2.3 (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 $l(0) = 1$*

1.2.3 Differentials

Definition 1.2.4 (Derivation)**.** *Let $\mathcal{V}$ be a vector space over $\mathbb{F}(\mathcal{X})$. An $\mathbb{F}$-linear map $D : \mathbb{F}(\mathcal{X}) \to \mathcal{V}$ is called a derivation if it satisfies the product rule*

$$D(fg) = fD(g) + gD(f)$$

The set of all derivations $D : \mathbb{F}(\mathcal{X}) \to \mathcal{V}$ will be denoted by $Der(\mathcal{X}.\mathcal{V})$. $Der(\mathcal{X}, \mathcal{V})$ forms a vector space over $\mathbb{F}(\mathcal{X})$. We denote $Der(\mathcal{X}, \mathcal{V})$ by $Der(\mathcal{X})$ if $\mathcal{V} = \mathbb{F}(\mathcal{X})$.

Theorem 1.2.3. *Let t be a local parameter at a point P. Then there exists a unique derivation $D_t : \mathbb{F}(\mathcal{X}) \to \mathbb{F}(\mathcal{X})$ such that $D_t(t) = 1$ and $\dim_{\mathbb{F}(\mathcal{X})}(Der(\mathcal{X})) = 1$ and D_t is a basis element for every local parameter t*

Definition 1.2.5 (Differential)**.** *A rational differential form or differential on $\mathcal{X}$ is an $\mathbb{F}9\mathcal{X})$-linear map from $Der(\mathcal{X})$ to $\mathbb{F}(\mathcal{X})$. The set of all rational differential forms $\mathcal{X}$ is denoted by $\Omega(\mathcal{X})$.*

Again $\Omega(\mathcal{X})$ forms a vector space over $\mathbb{F}(\mathcal{X})$. The differential $df : Der(\mathcal{X}) \to \mathbb{F}(\mathcal{X})$ is defined by $df(D) = D(f)$ for all $D \in Der(\mathcal{X})$. Then d is a derivation.

Theorem 1.2.4. $\dim_{\mathbb{F}(\mathcal{X})}(\Omega(\mathcal{X})) = 1$ *and dt is a basis for every point P with local parameter t.*

For every point P and local parameter t_P a differential ω on $\mathcal{X}$ can be represented in a unique way as $\omega = f_P dt_P$ where f_P is a rational function. The order or valuation of ω at P is defined by $v_P(\omega) = v_P(f_P)$. A differential form ω is called *regular* if it has no poles. The regular differentials on $\mathcal{X}$ form an $\mathbb{F}[\mathcal{X}]$-module which we denote by $\Omega[\mathcal{X}]$

Definition 1.2.6 (Canonical Divisor)**.** *Let ω be a differential then the divisor (ω) is defined by*

$$(\omega) = \sum_{P \in \mathcal{X}} v_P(\omega) P$$

Divisors of differentials are called canonical divisor.

If ω' be another nonzero differential then $\omega' = f\omega$ for some rational function f. Hence canonical divisors form one equivalence class. Let W denote the divisor of the differential ω. Hence $\mathcal{L}(W) \equiv \Omega[\mathcal{X}]$

Definition 1.2.7 (Genus of a Curve)**.** *Let $\mathcal{X}$ be a smooth projective curve over $\mathbb{F}$. The the genus g of $\mathcal{X}$ is defined by $l(W)$.*

Theorem 1.2.5. *Let $\mathcal{X}$ is nonsingular projective curve of degree m in $\mathbb{P}^2$. Then*

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

1.2.4 Reimann-Roch Theorem

Theorem 1.2.6 (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 1.2.7. *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 1.2.8. *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 1.2.7 $\deg(W - \mathcal{D}) < 0$. So $l(W - \mathcal{D}) = 0$ by Theorem 1.2.1 part (ii). So We have $l(D) = \deg(D) - (g - 1)$. ■

1.2.5 Index of speciality

Definition 1.2.8 (Index of Specialty)**.** *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 specialty of $\mathcal{D}$.

Theorem 1.2.9. $\delta(\mathcal{D}) = l(W - \mathcal{D})$

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 Setting up the System

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 1.2.8, $l(\mathcal{G}) = a + b + 1$ 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 $L = \{\alpha_1, \dots, \alpha_n\}$ be a set of n distinct elements of $\mathbb{F}_{q^m}$. Let g be a polynomial 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*

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

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

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

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 $P_1, \dots, P_n$ 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 useful to have both classes when treating decoding methods. These use parity check, so one needs a generator matrix for the dual codes.

CHAPTER 3

Asymptotically Good Sequences of Codes and Curves

3.1 Introduction to Good Codes

Following the distance and dimension of both the Geometric Reed Solomon Codes and Geometric Goppa Codes we have the following theorem

Theorem 3.1.1. *For any algebraic geometry code with dimension k and distance d on a curve of genus g with n points that are defined over $\mathbb{F}_q$ satisfy*

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

This bound feels almost like Singleton Bound but with the genus of the curve involved. First we define what Asymptotically Good code is

Definition 3.1.1 (Asymptotically Good Codes). *A sequence of codes $\{C_m \mid m \in \mathbb{N}\}$ with parameters $[n_m, k_m, d_m]$ over a fixed finite fields $\mathbb{F})q$ is called asymptotically good if n_m tends to infinity, $\frac{d_m}{n_m}$ tends to a nonzero constant δ and $\frac{k_m}{n_m}$ tends to a nonzero constant R for $m \to \infty$.*

By Gilbert-Vershamov bound there exists asymptotically good sequences of codes attaining the bound $R \geq 1 - H_q(\delta)$.

In order to construct asymptotically good codes we therefore need curves with low genus and many $\mathbb{F}_q$-rational points.

Definition 3.1.2. *Let $N_q(g)$ be the maximal number of $\mathbb{F}_q$-rational points on an absolutely irreducible nonsingular projective curve over $\mathbb{F}_q$ of genus g. Let*

$$A(q) := \limsup_{g \to \infty} \frac{N_q(g_)}{g}$$

3.2 Some Bounds

We know that to find good codes we must find long codes. To use the methods from algebraic geometry it is necessary to find rational points on a given curve. The number of these is a bound on the length of the codes. A central problem in algebraic geometry is finding for the number of rational points on a variety. So we mention the *Hasse-Weil Bound*

Theorem 3.2.1 (Hasse-Weil Bound, [Has36]). *Let $\mathcal{X}$ be a curve of genus g over $\mathbb{F}_q$. If $N_q(\mathcal{X})$ denotes the number of rational points on $\mathcal{X}$ then*

$$|N_q(\mathcal{X}) - (q+1)| \leq g2\sqrt{q}$$

Which was latter improved by Serre in [Wei48], known as *Weil-Serre Bound*

Theorem 3.2.2 (Weil-Serre Bound, [Wei48]). *Let $\mathcal{X}$ be a curve of genus g over $\mathbb{F}_q$. If $N_q(\mathcal{X})$ denotes the number of rational points on $\mathcal{X}$ then*

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

From this Bound by dividing both side by the genus (provided the genus is not 0) and taking the limit we obtain

$$A(q) \leq 2\lfloor q\rfloor$$

.This has been improved to the *Drinfeld-Vlăduţ*

Theorem 3.2.3 (Drinfeld-Vlăduţ Bound, [VD83]).

$$A(q) \leq \sqrt{q} - 1$$

Equality holds if q is a square.

And Ihara in [Iha82] has shown that

Theorem 3.2.4 ([Iha82]).

$$A(q) \geq \sqrt{q} - 1$$

when q is a square

The equality is proved by studying the number of rational points of *modular curves* over finite fields. Applying this to the algebraic geometric codes we finally get the *Tsfasman-Vlăduţ-Zink (TVZ) Bound*

Theorem 3.2.5 (Tsfasman-Vlăduţ-Zink (TVZ) Bound, [TVZ82]). *Let q be a square. Then for every R there exists an asymptotically good sequences of codes such that their rate tends to R and relative distance δ and*

$$R + \delta \geq 1 - \frac{1}{\sqrt{q} - 1}$$

This means that TVZ bound is better than the GV bound when q is a square and $q \geq 49$ in a certain range of δ.

3.3 Asymptotically Good Curves

First if $\mathcal{X}$ is absolutely irreducible then it is called a curve. Now we define what asymptotically good curve is.

Definition 3.3.1 (Asymptotically Good Curves). *A sequence of curves $\{\mathcal{X}_m \mid m \in \mathbb{N}\}$ is called asymptotically good if $g(\mathcal{X}_m)$ tends to infinity and the following limit exists*

$$\lim_{m\to\infty} \frac{N_q(\mathcal{X}_m)}{g(\mathcal{X}_m)} > 0$$

where $g(\mathcal{X})$ is the genus of $\mathcal{X}$.

In the following we discuss an asymptotically good curve family.

Let $F \in \mathbb{F}_q[X, Y]$. Let $d = \deg_Y(F)$. Assume that there exists a subset S of $\mathbb{F}_q$ such that for any $x \in S$ there exists exactly d distinct $y_1, \ldots, y_d \in S$ such that $F(x, y_i) = 0$ for all $i \in [d]$. Now consider the algebraic set $\mathcal{X}_m$ in $\mathbb{A}^m$ defined by the equations

$$F(X_i, X_{i+1}) = 0 \quad \text{for } i \in [m-1]$$

We can easily get a lower bound on the number of rational points for $\mathcal{X}_m$. X_1 has $|S|$ many choices and after words for all X_i, $2 \leq i \leq m$ has d choices. So number of rational points is at least $|S| \cdot d^{m-1}$.

Example 3.3.1. *Let $q = 4$. Let $F = XY^2 + Y + X^2$. The F is an example with $d = 2$ and $S = \mathbb{F}_4^*$. Therefore this gives a curve with $3 \cdot 2^{m-1}$ points with nonzero coordinates in $\mathbb{F}_4$ and in fact it gives a sequence of curves that is asymptotically good.*

In general let $q = r^2$. Consider $F = Z^{r-1}Y^r + Y = X^r$. Then we get an example with $a = r$ and $S = \mathbb{F}_q^*$. The equation $F = 0$ has the property that for every given nonzero element $x \in \mathbb{F}_q$ there are exactly r nonzero solutions in $\mathbb{F}_q$ of the equation $F(x, Y) = 0$ in Y. To see this first multiply the equation with X to get $XF = X^r y^r + XY - X^{r+1}$. Then replace $z = XY$ and we get

$$G = Z^r + Z - X^{r+1}$$

This defines an hermitian curve $U^{r+1} + V^{r+1} + 1 = 0$ whose homogeneous version is $U^{r+1} + V^{r+1} + W^{r+1} = 0$, which is a Fermat curve. Therefore the corresponding sequence of curves $\mathcal{X}_m$ satisfies

$$N_q(\mathcal{X}) \geq (q-1)r^{m-1}$$

The genus of the curve $\mathcal{X}_m$ is computed by induction by applying formula of *Hurwitz-Zeuthen*, [Har77] to the covering $\pi_m : \mathcal{X}_m \to \mathcal{X}_{m-1}$ where $\pi_m(x_1, \ldots, x_m) = (x_1, \ldots, x_{m-1})$. It is easier to view this in terms of function fields. Let $\mathcal{F}_m$ be the function field of $\mathcal{X}_m$. Then $\mathcal{F}_1 = \mathbb{F}_q(z_1)$ and $\mathcal{F}_m$ is obtained from $\mathcal{F}_{m-1}$ by adjoining a new element z_m that satisfies the equation

$$z_m^r + z_m = x_{m-1}^{r+1}$$

where $x_{m-1} = \frac{z_{m-1}}{x_{m-2}} \in \mathcal{F}_{m-1}$ for $m \geq 2$ and $x_1 = z_1$, $x_0 = 1$.

Theorem 3.3.2. *The genus g_m of the curve $\mathcal{X}_m$ or equivalently of the function field $\mathcal{F}_m$ is equal to*

$$g_m = \begin{cases} r^m + r^{m-1} - r^{\frac{m+1}{2}} - 2r^{\frac{m-1}{2}} + 1 & \text{when } m \text{ is odd} \\ r^m + r^{m-1} - \frac{1}{2}r^{\frac{m+2}{2}} - \frac{3}{2}r^{\frac{m}{2}} - r^{\frac{m-2}{2}} + 1 & \text{when } m \text{ is even} \end{cases}$$

Thus the Drinfeld-Vlăduţ Bound is attained.

CHAPTER 4

Bibliography

[BHHW98] Ian Blake, Chris Heegard, Tom Høholdt, and Victor Wei. Algebraic-geometry codes. *Information Theory, IEEE Transactions on*, 44:2596 – 2618, 11 1998.

[Coh22] Gil Cohen. Algebraic geometric codes: https://www.gilcohen.org/2022-ag-codes, 2022.

[Gop77] V. D. Goppa. Codes associated with divisors. *Probl. Peredachi Inf.*, 13:33–39, 1977.

[Gop81] V. D. Goppa. Codes on algebraic curves. 1981.

[Gop84] V. D. Goppa. Codes and information. *Russian Mathematical Surveys*, 39:87–141, 1984.

[Gop88] V. D. Goppa. Geometry and codes. 1988.

[Har77] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Has36] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper iii. die struktur des meromorphismenrings. die riemannsche vermutung. *Journal für die reine und angewandte Mathematik*, 1936(175):193–208, 1936.

[Iha82] Yasutaka Ihara. Some remarks on the number of rational points of algebratic curves over finite fields. *Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics*, 28:721–724, 1982.

[Sti08] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer Publishing Company, Incorporated, 2nd edition, 2008.

[TV91] Michael A. Tsfasman and Serge G. Vladut. Algebraic-geometric codes. 1991.

[TVN07] Michael Tsfasman, Serge Vlăduţ, and Dmitrii Nogin. *Algebraic geometric codes. Basic notions.* 01 2007.

[TVZ82] M. A. Tsfasman, S. G. Vlădutx, and Th. Zink. Modular curves, shimura curves, and goppa codes, better than varshamov-gilbert bound. *Mathematische Nachrichten*, 109(1):21–28, 1982.

[VD83] Serge Vlăduţ and V. Drinfel'd. Number of points of an algebraic curve. *Functional Analysis and Its Applications - FUNCT ANAL APPL-ENGL TR*, 17:53–54, 01 1983.

[Wei48] André Weil. Sur les courbes algébriques et les variétés qui sén déduisent. *Actualités scientifiques et industrielles 1041*, page 85, 1948.