Introduction To Algebraic Geometry Codes

Xing Chaoping

Department of Mathematics
National University of Singapore

0. Introduction

<u>Brief History</u>
<u>Algebraic Coding Theory</u>
<u>Algebraic Geometry Codes</u>
<u>Applications of Codes</u>

1. Goal of Coding Theory

Consider the following simple model of a communication system:

$$
\begin{array}{ccc}
\boxed{\text{message sent}} & & 10 \\
\downarrow & & \\
\boxed{\text{communication channel}} & \leftarrow & \text{noise} \\
\downarrow & & \\
\boxed{\text{message received}} & & 00
\end{array}
$$

The receiver may not realize that the message was corrupted. This communication fails.

We assume the followings for this model:

(a) message source consists of
$00, 10, 01, 11$;

(b) the probability that errors take place is at most $1/5$, i.e., at most one bit out of five bits will be corrupted when transmitted.

Let us consider the following encoding:
$00 \mapsto 00\mathit{000}, \quad 01 \mapsto 01\mathit{110}$
$10 \mapsto 10\mathit{111}, \quad 11 \mapsto 11\mathit{001}$
For example, when transmitting the message 10, we first encode it into 11011.

$$C := \{00000, 01110, 10111, 11001\}$$

is called a *code*.

This procedure can be described in the same model with **coding**:

$\boxed{\text{message sent}}$		10
$\downarrow$		
$\boxed{\text{Encoder}}$		10*111*
$\downarrow$		
$\boxed{\text{communication channel}}$	$\leftarrow$	noise
$\downarrow$		
$\boxed{\text{Decoder}}$		10011
$\downarrow$		
$\boxed{\text{decoded message}}$		10

Notice that in order to correct errors, we lose information transmission rate for this system.

<u>Goal of coding theory</u>

To construct codes such that they have

1. maximum information transmission per unit time, and
2. maximum error-correcting capability

However, as we will see later, the above two requirements are in general not compatible with each other.

2. Introduction to Codes

A – a finite set of q elements;
$A^n = \{(a_1, \ldots, a_n) : a_i \in A\}$– the affine space of dimension n over A.

Definition 2.1. A subset C of A^n is called a *code* of length n over A. The set A is called the *code alphabet*. We say that C is a q-ary (n, M)-code if the size of C is M.

For example, the code

$$C = \{00000, 01110, 10111, 11001\}$$

in the previous section is a binary $(5, 4)$-code.

The information rate of a q-ary (n, M)-code is defined by

$$R = \frac{\log_q M}{n}.$$

For two words $\mathbf{x}$ and $\mathbf{y}$ of A^n, the *Hamming distance* between $\mathbf{x}$ and $\mathbf{y}$ is defined to be the number of positions where $\mathbf{x}$ and $\mathbf{y}$ differ.
Example 2.2. Consider words

$$\mathbf{x} = (12201), \mathbf{y} = (01211).$$

Then $d(\mathbf{x}, \mathbf{y}) = 3$. $\square$

Definition 2.3. The *minimum distance* or *distance* $d(C)$ of a q-ary (n, M)-code C $(M \geq 2)$ is defined to be

$$d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \ \mathbf{x} \neq \mathbf{y} \in C\}.$$

An (n, M)-code with distance d is denoted by (n, M, d).

Example 2.4. For the code in Example 2.2, the distance is 3. It is a binary $(5, 4, 3)$-code. $\square$

Theorem 2.5. *A q-ary (n, M, d)-code can correct upto $\lfloor (d-1)/2 \rfloor$ errors and detect upto $d - 1$ errors.*

For instance, the code in Example 2.2 has distance 3. It can correct 1 error.

For a q-ary (n, M, d)-code, the error-correcting rate is defined by

$$\delta = \frac{d-1}{n}.$$

Goal: For a q-ary (n, M, d)-code, we want both $R = \log_q M/n$ and $\delta = (d-1)/n$ as large as possible.

Theorem 2.6. **(Singleton Bound)** Let R and δ be the information rate and error-correcting rate, respectively. Then

$$R + \delta \leq 1.$$

3. Linear Codes

$\mathbf{F}_q$ – the finite field with q elements.

Definition 3.1. A subspace C of the vector space $\mathbf{F}_q^n$ is called a linear code. The dimension of C as a linear space over $\mathbf{F}_q$ is called the *dimension* of the code C. A linear code of length n, dimension k and distance d is denoted by $[n, k, d]$.

Remark 3.2. For an q-ary $[n, k, d]$-linear code C

1. The information rate is k/n since $|C| = q^k$.

2. The Singleton bound for C is

$$k + d \leq n + 1.$$

The Hamming weight $wt(\mathbf{u})$ of a vector $\mathbf{u}$ of $\mathbf{F}_q^n$ is defined to be the number of non-zero positions.

Example 3.3. Consider vectors

$$\mathbf{x} = (12201), \mathbf{y} = (01211), \mathbf{u} = (00021) \in \mathbf{F}_3^5.$$

Then

$$wt(\mathbf{x}) = wt(\mathbf{y}) = 4 \quad \text{and} \quad wt(\mathbf{u}) = 2.$$

□

Lemma 3.4. *Let C be a linear code over $\mathbf{F}_q$ of length n, then*

$$\begin{aligned} d(C) &= \min\{d(\mathbf{x}, \mathbf{y}) | \mathbf{x} \neq \mathbf{y} \in C\} \\ &= \min\{wt(\mathbf{z}) | \mathbf{z} \in C \setminus \{\mathbf{0}\}\}. \end{aligned}$$

4 Algebraic Geometry Codes

Example 4.1. (Reed-Solomon) For $1 \leq k \leq n \leq q$, consider a subset $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $\mathbf{F}_q$ and construct a linear code in the following way:

$$C = \{(f(\alpha_1), \ldots, f(\alpha_n)) : f \in \mathbf{F}_q[x], \deg(f) \leq k - 1\}.$$

The linear code C constructed as above has parameters $[n, k, d]$ with $d = n + 1 - k$, i.e., $k + d = n + 1$. Thus, it achieves the Singleton bound. □

Example 4.2. Consider the elliptic curve over $\mathbf{F}_3$ defined by

$$y^2 = x^3 - x + 1.$$

It has 7 points $\infty, P_1, ..., P_6$ which are

$$\{\infty, (0, \pm 1), (1, \pm 1), (-1, \pm 1)\}.$$

Let V be the space of all functions of "degree" ≤ 3. Then

$$V = span\{1, x, y\}/\mathbf{F}_3.$$

Define the code

$$C = \{(f(P_1), \ldots, f(P_6)) | f \in V\}.$$

Then, C is a ternary $[6, 3, 3]$ linear code. □

Geometric interpretation of the polynomial codes

Recall terminology from Niederreiter's notes, such as, places, residue class fields, divisor, Riemann-Roch spaces, etc.

Correspondence between curves and function fields:

curves $\mathcal{X}$: $f(x, y) = 0 \Leftrightarrow$ function filed $\mathbf{F}_q(\mathcal{X}) = \mathbf{F}_q(x, y)$
points on $\mathcal{X}/\mathbf{F}_q \Leftrightarrow$ places of degree one of $\mathbf{F}_q(\mathcal{X})$
genus of $\mathcal{X}$=genus of $\mathbf{F}_q(\mathcal{X}) = (\deg(f) - 1)(\deg(f) - 2)/2$.

Let ∞ be the place of $\mathbf{F}_q(x)$ corresponding to the degree (see Section 5 of [Nied]). Then a function $f(x)$ is a polynomial of degree $\leq k - 1$ if and only if

$$\nu_\infty(f) \geq -(k-1), \text{ and } \nu_P(f) \geq 0$$

for all other places P, i.e.,

$$\mathrm{div}(f) + (k-1)\infty \geq 0.$$

This is equivalent to that $f(x)$ is in the Riemann-Roch space $\mathcal{L}((k-1)\infty)$. Hence

$$\mathcal{L}((k-1)\infty) = \{f \in \mathbf{F}_q[x] : \deg(f) \leq k-1\},$$

and the Reed-Solomon codes can be expressed in the following way:

$$C = \{(f(\alpha_1), \ldots, f(\alpha_n)) : f \in \mathcal{L}((k-1)\infty)\}.$$

Geometric interpretation of the elliptic codes

For the curves

$$y^2 = x^3 - x + 1$$

over $\mathbf{F}_3$, we have $\nu_\infty(x) = -2$ and $\nu_\infty(y) = -3$. Thus,

$$V = span\{1, x, y\} \subseteq \mathcal{L}(3\infty).$$

By the Riemann-Roch theorem, we have in fact

$$V = span\{1, x, y\} = \mathcal{L}(3\infty).$$

The code in Example 4.2 can be rewritten:

$$C = \{(f(P_1), \ldots, f(P_6)) : f \in \mathcal{L}(3\infty)\}.$$

Let $\mathcal{X}/\mathbf{F}_q$ be a curve over $\mathbf{F}_q$. Let $\infty, P_1, ..., P_n$ be $n+1$ points. For an integer $m < n$, we consider the map

$$\theta : \mathcal{L}(m\infty) \to \mathbf{F}_q^n, \quad f \mapsto (f(P_1), \ldots, f(P_n)).$$

The image of θ is a linear code of length n. It is called a *algebraic geometry code*, denoted by $C(P_1, \ldots, P_n; m\infty)$.

Theorem 4.3. *Let $\mathcal{X}/\mathbf{F}_q$ be a curve of genus g. Then the code $C(P_1, \ldots, P_n; m)$ constructed above is a q-ary $[n, k, d]$-linear code with*

$$k \geq m - g + 1, \quad d \geq n - m.$$

Remark 5.4. From the above theorem, we find that for an algebraic geometry code based on a curve of genus g, we have

$$n+1-g \leq k+d \leq n+1.$$

Example 4.5. Look at the curve

$$\mathcal{X}: \quad y^r + y = x^{r+1}$$

over $\mathbf{F}_q$ with $q = r^2$.

For each $x = \alpha \in \mathbf{F}_q$, we get r solutions for

$$y^r + y = \alpha^{r+1}.$$

Thus, total number of points is $r^3 + 1$.

The genus of $\mathcal{X}$ is $r(r-1)/2$. Hence for any

$$r(r-1) - 1 = 2g - 1 \leq m < n = r^3,$$

the code $C(P_1, ..., P_n; m\infty)$ is a q-ary $[r^3, m-g+1, r^3-m]$-linear code.

For example, if $q = 4 = r^2$, we get $[8, m, 8-m]$-linear codes over $\mathbf{F}_4$ for any $1 \leq m \leq 8$.
□

5. The Fundamental Coding Problem

In coding theory, people are interested in performance of long codes. In other words, we like to find the ratio

$$\limsup_{n\to\infty} \frac{k}{n} \quad \text{and} \quad \limsup_{n\to\infty} \frac{d-1}{n}$$

for q-ary $[n, k, d]$-linear codes.

Definition 5.1. The q-ary linear code domain U_q^{lin} is the set of ordered pairs $(\delta, R) \in \mathbf{R}^2$ for which there exists an infinite sequence $C_1, C_2, \ldots$ of linear codes over $\mathbf{F}_q$ with $n(C_i) \to \infty$ and

$$R = \lim_{i\to\infty} \frac{k(C_i)}{n(C_i)}, \quad \delta = \lim_{i\to\infty} \frac{d(C_i)-1}{n(C_i)}.$$

Proposition 5.2. *There exists a continuous function* $\alpha_q^{\mathrm{lin}}(\delta), \delta \in [0,1]$, *such that*

$$U_q^{\mathrm{lin}} = \{(\delta, R) \in \mathbf{R}^2 : 0 \leq R \leq \alpha_q^{\mathrm{lin}}(\delta), 0 \leq \delta \leq 1\}.$$

Moreover, $\alpha_q^{\mathrm{lin}}(0) = 1, \alpha_q^{\mathrm{lin}}(\delta) = 0$ *for* $\delta \in [(q-1)/q, 1]$*, and* $\alpha_q^{\mathrm{lin}}(\delta)$ *decreases on the interval* $[0, (q-1)/q]$.

For $0 < \delta < 1$ define the q-ary entropy function

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta),$$

where $\log_q$ is the logarithm to the base q, and put

$$R_{GV}(q, \delta) = 1 - H_q(\delta).$$

Then the Gilbert-Varshamov bound says that

$$\alpha_q^{\mathrm{lin}}(\delta) \geq R_{GV}(q, \delta) \quad \text{for all } \delta \in (0, \frac{q-1}{q}). \tag{1}$$

For any prime power q and any integer $g \geq 0$ put

$$N_q(g) = \max N(\mathcal{X}/\mathbf{F}_q),$$

where the maximum is extended over all curves $\mathcal{X}/\mathbf{F}_q$ with $g(\mathcal{X}) = g$.

We also define the following asymptotic quantity

$$A(q) := \lim_{g \to \infty} \sup \frac{N_q(g)}{g}.$$

(see Section 9 of [Nied]).

Theorem 5.3. *For any prime power* q*, one has*

$$\alpha_q^{\mathrm{lin}}(\delta) \geq 1 - \delta - \frac{1}{A(q)} \quad \textit{for all } \delta \in [0, 1]. \tag{2}$$

Define the linear function

$$R_G(q, \delta) = 1 - \frac{1}{A(q)} - \delta$$

for any prime power q. Then Theorem 5.3 says that $\alpha_q^{\mathrm{lin}}(\delta) \geq R_G(q, \delta)$.

Proposition 5.4. (see Chapter 5 of [N-X])

1. *If* q *is a square, then*
$$A(q) = \sqrt{q} - 1.$$

2. *If* q *is a cube, then*
$$A(q) \geq \frac{\sqrt{q^{1/3}} + 1}{\lfloor 2\sqrt{2q^{1/3} + 2} \rfloor + 2}.$$

Theorem 5.5.

1. *If* $q \geq 49$ *is a square, then there exists an open interval* $(\delta_1, \delta_2) \subseteq (0,1)$ *such that*
$$R_G(\delta) > R_{GV}(\delta) \quad \textit{for any } \delta \in (\delta_1, \delta_2)\ .$$
2. *If* $q > 15552$ *is a cube, then there exists an open interval* $(\delta_1, \delta_2) \subseteq (0,1)$ *such that*
$$R_G(\delta) > R_{GV}(\delta) \quad \textit{for any } \delta \in (\delta_1, \delta_2)\ .$$

6. New Codes from Algebraic Geometry Codes

Construction 1

Rational points are not sufficient for curve of a given genus. We will make use of points over $\mathbf{F}_{q^2}$.

First we fix some notations for this section.

$\mathcal{X}/\mathbf{F}_{q^2}$ – an algebraic curve;
$g := g(\mathcal{X})$ – the genus of $\mathcal{X}/\mathbf{F}_{q^2}$;
$\mathbf{F}_{q^2}(\mathcal{X})$ – the function field of $\mathcal{X}/\mathbf{F}_{q^2}$;

We choose $n+1$ points $\infty, P_1, ..., P_n$ over $\mathbf{F}_{q^2}$.

For $m \geq g$, we have
$$\dim_{\mathbf{F}_{q^2}}(\mathcal{L}(m\infty)) \geq m+1-g \geq 1$$
by the Riemann-Roch theorem. Therefore, we can find $m+1-g$ non-gaps $0 = v_1 < v_2 < \cdots < v_{m+1-g} \leq m$ of ∞, i.e, there exist $m+1-g$ functions $f_1, f_2, .., f_{m+1-g}$ of $\mathcal{L}(m\infty)$ such that
$$\nu_\infty(f_i) = -v_i \tag{3}$$
for all $1 \leq i \leq m+1-g$, where ν_∞ denotes the normalized discrete valuation of ∞. Since v_i are strictly increasing, we obtain
$$v_i \leq v_{m+1-g} - ((m+1-g)-i) \leq m - (m+1-g-i) = g+i-1. \tag{4}$$

Put
$$e_{ij} = f_i^q f_j + f_i f_j^q$$
for all $1 \leq i < j \leq m+1-g$, and
$$e_{ii} = f_i^{q+1}$$
for all $1 \leq i \leq m+1-g$.

Choose an element γ of $\mathbf{F}_{q^2} - \mathbf{F}_q$ and put

$$e'_{ij} = \gamma^q f_i^q f_j + \gamma f_i f_j^q$$

for all $1 \le i < j \le m+1-g$.

Lemma 6.1. For any $\mathbf{F}_{q^2}$-rational point $P \ne \infty$ of $\mathcal{X}/\mathbf{F}_{q^2}$, both $e_{ij}(P)$ and $e'_{ij}(P)$ are elements of $\mathbf{F}_q$ for all i, j.

Let U_m be the $\mathbf{F}_q$-linear span of the set

$$\{e_{ij} | 1 \le i \le j \le m+1-g\} \cup \{e'_{ij} | 1 \le i < j \le m+1-g\}.$$

Lemma 6.2. *The dimension of the* $\mathbf{F}_q$*-linear space* U_m *is equal to* $(m+1-g)^2$ *if* $m < q$.

We construct a code as follows:

$$C_m = \{(f(P_1), f(P_2), ..., f(P_n)) | f \in U_m\}.$$

This code is defined over $\mathbf{F}_q$ by Lemma 3.1 and it is clear that C_m is a linear code of length n.

In fact, U_m is a subspace of $\mathcal{L}(m(q+1)\infty)$. Hence,

$$C_m \subseteq C(P_1, P_2, ..., P_n; m(q+1)\infty).$$

Theorem 6.3. *Let* $\mathcal{X}/\mathbf{F}_{q^2}$ *be an algebraic curve of genus* g *with* $n+1$ *rational points* $\infty, P_1, ..., P_n$. *Suppose* $g \le m < \min\{q, n/(q+1)\}$. *Then* C_m *is an* $[n, (m+1-g)^2, d]$ *linear code over* $\mathbf{F}_q$ *with*

$$d \ge n - m(q+1).$$

Example 6.4. Let $q = 8$. Consider the elliptic curve

$$y^2 + y = x^3$$

over $\mathbf{F}_{64}$. Then it has 81 points over $\mathbf{F}_{64}$ and the genus is 1. Thus, for any $1 \le m \le 7$ we have a q-ary $[80, m^2, d \ge 80 - 9m]$-linear codes. In particular, we obtain the following new codes:

$$[80, 36, 26], \quad [80, 49, 17].$$

Corollary 6.5. *If* $1 \le m < q$, *then there exist*
(1) *a* q*-ary* $[q^2, (m+1)^2, d \ge q^2 - m(q+1)]$ *linear code, and*
(2) *a* q*-ary* $[q^2+2q, m^2, d \ge q^2+2q-m(q+1)]$ *linear code.*

Construction 2

This construction is only for the reader who is quite familar with function fields.

The ingredients for this construction case are as follows.

$F = F/\mathbf{F}_q$ — algebraic function field with full constant field $\mathbf{F}_q$.
g — the genus of $F/\mathbf{F}_q$.
$P_1, P_2, ..., P_s$ — s distinct places of F.
$k_i = \deg(P_i)$ — degree of P_i for $1 \le i \le s$.
G — divisor of F with $\mathrm{Supp}(G) \cap \{P_1, P_2, ..., P_s\} = \emptyset$.
C_i — q-ary linear code of parameters $[n_i, k_i = \deg(P_i), d_i]$ with $k_i \ge d_i$ for $1 \le i \le s$.
π_i — fixed $\mathbf{F}_q$-linear isomorphism mapping the residue class field of P_i onto C_i for $1 \le i \le s$.

Then by concatenation we define the q-ary linear code

$$C := \{(\pi_1(f(P_1)), \pi_2(f(P_2)), ..., \pi_s(f(P_s)))|f \in \mathcal{L}(G)\},$$

where $\mathcal{L}(G)$ is the usual Riemann-Roch space

$$\mathcal{L}(G) = \{f \in F^*|\mathrm{div}(f) + G \ge 0\} \cup \{0\}$$

and $\mathrm{div}(f)$ is the principal divisor of $f \in F^*$.

Theorem 6.6. *With the notations above, suppose that $g \le \deg(G) < \sum_{i=1}^{s} k_i$. Then the code C defined above is a q-ary $[n, k, d]$ linear code with*

$$n = \sum_{i=1}^{s} n_i; \quad k \ge \deg(G) - g + 1; \quad d \ge \sum_{i=1}^{s} d_i - \deg(G).$$

Example 6.7. Consider the elliptic function field $F = \mathbf{F}_4(x, y)$ defined by

$$y^2 + y = x^3 + x.$$

Then F has 5 rational places, and hence its L-polynomial is equal to

$$4T^2 + 1.$$

It follows that there are 10 places of degree 2 and 20 places of degree 3. Since there exist linear codes over $\mathbf{F}_4$ with the following parameters

$$[1, 1, 1]; \quad [3, 2, 2]; \quad [5, 3, 3],$$

we can choose all of these places and get the codes with parameters

$$[135, k, d \ge 85 - k]$$

for any $1 \leq k \leq 84$ from Theorem 6.6. In particular, we obtain two new codes

$$[135, 29, d \geq 56], \quad [135, 30, d \geq 55]$$

Reference

- [Nied] H. Niederreiter, *Algebraic Function Fields over Finite Fields*, lecture notes, IMS 2001.
- [N-X] H. Niederreiter and C. P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications,* Cambridge University Press, 2001.