Introduction to Algebraic Geometric Codes

Introduction

Initial ideas that led to algebraic geometric codes (AG codes) came from V. Goppa (early 1980s)

I will give a brief overview of AG codes, a review of basic notions on algebraic curves necessary to describe Goppa's construction of codes

Motivations

- Show codes that exceed the Gilbert-Varshamov bound
- Show that codes can be constructed from different mathematical objects

Reed-Solomon code

AG codes are a natural generalization of Reed-Solomon codes

$\mathbb{F}_q^\times := \{\alpha_1, \ldots, \alpha_{q-1}\}$; $L_k := \{f \in \mathbb{F}_q[x]/\deg f \leq k-1\} \cup \{0\}$

The Reed-Solomon code is
$RS(k,q) := \{(f(\alpha_1), \ldots, f(\alpha_{q-1})) \in \mathbb{F}_q^{q-1}/f \in L_k\}$

$RS(k,q)$ is an $[q-1, k, n-k+1]_q$-code. (an MDS code!)

Since $1, x, \ldots, x^{k-1}$ forms a basis of L_k, the generator matrix for $RS(k,q)$ is:

$$G = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{q-1} \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_{q-1}^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_{q-1}^{k-1} \end{bmatrix}.$$

Generalized Reed-Solomon code

For $1 \leq k \leq n \leq q$, let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct elements of $\mathbb{F}_q$

Let $v_1, v_2, \ldots, v_n$ be non-zero elements of $\mathbb{F}_q$

The code

$$GRS(k, q) := \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) \in \mathbb{F}_q^n / f \in L_k\}$$

is the **Generalized Reed-Solomon code**.

If $\forall i,\ v_i = 1$, we have the Reed-Solomon code.

The Generalized Reed-Solomon code is also an MDS code.

K : field

$f(x, y) \in K[x, y]$

The **affine curve** defined by f over K is

$$\chi_f := \{(a, b) \in K^2 / f(a, b) = 0\}.$$

We usually look at roots of f lying in the algebraic closure of K. In particular, if $K = \mathbb{F}_q$, we look at points (a, b) over $\mathbb{F}_{q^m}$ for some m, with $f(a, b) = 0$

Let K be a field. The **projective plane** $\mathbb{P}^2(K)$ is

$$\mathbb{P}^2(K) := (K^3 \backslash 0)/\sim$$

where $(X_0, Y_0, Z_0) \sim (X_1, Y_1, Z_1)$ iff $\exists \alpha \in K^\times$ such that $X_1 = \alpha X_0,\ Y_1 = \alpha Y_0,\ Z_1 = \alpha Z_0$.

If χ_f is the affine curve defined by f of degree $= d$, the **projective closure** of χ_f is $\widehat{\chi_f} := \{(a : b : c) \in \mathbb{P}^2(\bar{K}) / F(a, b, c) = 0\}$ where $F(X, Y, Z) := Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ is the homogenization of f.

Example: The affine curve defined by $y^2 - x^2(x+1)$ is associated with the projective curve: $Y^2Z - X^3 - X^2Z$. The projective curve defined by $X^5 + Y^5 - Z^5$ is associated with the affine curve with equation $x^5 + y^5 = 1$

An affine (resp. projective) curve is **irreducible** is $f(x, y)$ (resp. $F(X, Y, Z)$) cannot be written as the product of two non-constant polynomials.

A point $P(a : b : c)$ on an irreducible projective curve χ defined by $F(X, Y, Z)$ is **singular** if all the partial derivatives F_X, F_Y, F_Z vanish at P. Otherwise P is **simple**.The curve χ is **non-singular** or **smooth** is all its points are simple.

Example: Let χ be the curve defined by $F(X, Y, Z) = X^5 + Y^5 + Z^5$ over a field K. If $char\ K \neq 5$ then χ is non-singular. Otherwise, every point on χ is singular.

Example. Let *char* $K = 2$, and χ be defined by

$$F(X, Y, Z) = X^3Y + Y^3Z + Z^3X.$$

χ is non-singular. (Klein quartic)

Example. (Hermitian curve) Let q be a prime power and $K = \mathbb{F}_{q^2}$, The curve χ defined by

$$F(X, Y, Z) = Y^qZ + YZ^q - X^{q+1}$$

is non-singular. (Exercise: show that the number of points in $\chi(\mathbb{F}_{q^2})$ is $q^3 + 1$).

Bezout's Theorem. If $f, g \in K[x, y]$ are polynomials with degrees d_f, d_g with no non-constant common factors, then the affine curves χ_f and χ_g intersect in at most $d_f\ d_g$ points. The projective curves $\widehat{\chi_f}$ and $\widehat{\chi_g}$ intersect in exactly $d_f d_g$ points of $\mathbb{P}^2(\bar{K})$ where we consider multiplicity.

If $\widehat{\chi_f}$ is a non-singular projective curve defined by $f \in K[x, y]$ of degree d, the **genus** of χ_f (or $\widehat{\chi_f}$) is

$$g := (d-1)(d-2)/2$$

rational points

Let C be a projective curve defined by $F(X, Y, Z)$ over a field K. If $K \subseteq L$, a field, an L-**rational point on** C is a point $(a : b : c) \in \mathbb{P}^2(L)$ such that $F(a, b, c) = 0$. The set of L-rational points is denoted as $C(L)$. The set $C(K)$ are simply **rational points**.

Example: Let C be defined by $X^2 + Y^2 = Z^2$. Then $(3 : 4 : 5) = (3/5 : 4/5 : 1)$ is a $\mathbb{Q}$-rational point on C. The points $(3 : 2i : \sqrt{5})$ and $(3 : -2i : \sqrt{5})$ are $\mathbb{C}$-rational points on C.

Frobenius automorphism, degree of points

The **Frobenius automorphism** is the map $\sigma_{q,n} : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ defined by $\alpha \longmapsto \alpha^q$.

If C is a projective curve over $\mathbb{F}_q$, the action of $\sigma_{q,n}$ on $C(\mathbb{F}_{q^n})$ is $\sigma_{q,n}((a : b : c :)) := (a^q : b^q : c^q)$. Action on affine curves is similarly defined.

Let C be a non-singular projective curve. A **point of degree** n **on** C **over** $\mathbb{F}_q$ is a set $P = \{P_0, P_1, \ldots, P_{n-1}\}$ of n distinct points such that $P_i = \sigma^i_{q,n}(P_0)$ for $i = 1, 2, \ldots, n-1$.

intersection divisors, divisors on curves

By Bezout's Theorem, two curves C_1, C_2 over $\mathbb{F}_q$ defined by polynomials of degrees d_1, d_2 will intersect in $d_1 d_2$ points. These $d_1 d_2$ points can be grouped into points of varying degrees, the sum of degrees is $d_1 d_2$. i.e. $C_1 \cap C_2 = P_1 + P_2 + \ldots + P_l$ with $d_1 d_2 = \deg\ P_1 + \deg\ P_2 + \ldots \deg\ P_l$. The **intersection divisor** of C_1 and C_2 is $C_1 \cap C_2$.

Let C be a curve over $\mathbb{F}_q$. A **divisor** D on C over $\mathbb{F}_q$ is a sum of the form $\Sigma n_P P$ where $n_P \in \mathbb{Z}$ and each P is a point (of arbitrary degree) on C. The **degree** of the divisor D is deg $D := \Sigma n_p \deg\ P$. The **support** of the divisor D is supp $D := \{P \mid n_P \neq 0\}$.

If $n_P \geq 0\ \forall P$, D is called an **effective divisor**, and we write $D \geq 0$.

Let the C be a projective curve over $\mathbb{F}_q$ defined by $F(X, Y, Z)$. A **rational function on** C is a ratio $g(X, Y, X)/h(X, Y, Z)$ of two homogeneous polynomials $g,\ h \in \mathbb{F}_q[X, Y, Z]$ of the same degree. We define the equivalence relation $\sim$ on rational functions: $g_0/h_0 \sim g_1/h_1$ if and only if $g_0 h_1 - g_1 h_0$ is in the principal ideal $< F >$ generated by F in $\mathbb{F}_q[X, Y, Z]$. The **field** $\mathbb{F}_q(C)$ **of rational functions on** C is the set

$$(\{g/h \mid g, h \in \mathbb{F}_q[X, Y, Z], \text{h}omogeneous\ of\ same\ degree\} \cup \{0\})/\sim$$

Let C be a curve over $\mathbb{F}_q$ and let $f = g/h$ be a rational function on C. The **divisor of** f is defined as $\text{div}(f) := \sum P - \sum Q$, where $\sum P$ is the intersection divisor $C \cap C_g$ and $\sum Q$ is the intersection divisor $C \cap C_h$;

Let C be a non-singular projective curve over $\mathbb{F}_q$ and D a divisor on C. The **space of rational functions associated to** D is

$$L(D) := \{f \in \mathbb{F}_q(C) \mid \text{div}\,(f) + D \geq 0\} \cup \{0\}.$$

Riemann-Roch Theorem. If χ be a non-singular projective curve over $\mathbb{F}_q$, with genus $= g$, and D, a divisor on χ, then the dimension $L(D)$ as a vector space over $\mathbb{F}_q$ is $\geq \deg\, D + 1 - g$. If $\deg\, D > 2g - 2$ then $\dim\, L(D) = \deg\, D + 1 - g$.

AG codes

Let $\mathbb{F}_q^\times = \{\alpha_1, \dots, \alpha_{q-1}\}$ and consider the projective line $\mathbb{P}^1(\mathbb{F}_q) = \{(a:1) \mid a \in \mathbb{F}_q\} \cup \{(1:0)\}$. Set $P_i := (\alpha_i : 1)$ and $D := (k-1)P_\infty$ where $P_\infty = (1:0)$.

The space $L(D)$ of rational functions associated to D is L_k.

$RS(k,q) = \{(f(P_1), \dots, f(P_{q-1})) \mid f \in L(D)\}$

Goppa's generalization: Let χ be a projective non-singular plane curve over F_q, and D a divisor on χ. Let $P = (P_1, P_2, \dots, P_n)$ be a set of n distinct $\mathbb{F}$-rational points on the curve. The **algebraic geometric code associated to χ, P and D is**

$$C(\chi, P, D) := \{(f(P_1), \dots, f(P_n)) \mid f \in L(D)\} \subset \mathbb{F}_q^n.$$

Parameters of $C(\chi, P, D)$:
length$=n$
dimension C is dim $L(D)$

Theorem. Let χ be a non-singular projective curve over $\mathbb{F}_q$, with genus g. Let P be a set of n distinct $\mathbb{F}_q$-rational points on χ, and let D be a divisor on χ such that $2g-2 < \deg D < n$. Then $C(\chi, P, D)$ is a linear code of length n, dimension $=$ $\deg D + 1 - g$ and minimum distance d where $d \geq n - \deg D$.