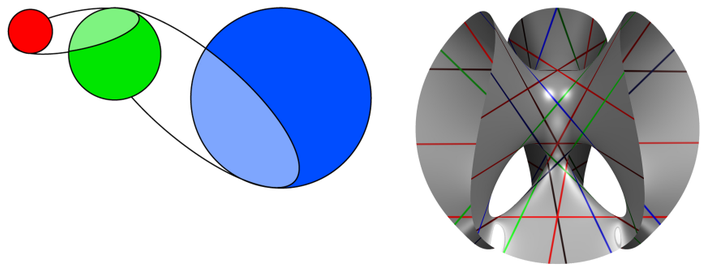
Young Women in Algebraic Geometry



Algebraic Geometric Codes on a Quotient of the Ree Curve

Shabieh Farwa

(Joint work with Gul Khatab)

COMSATS Institute of Information Technology

A Quotient of the Ree Curve

Definition 1: The function field of the Ree curve $C'/\mathbb{F}_q$ (where $q = 3q_0^2$, with $q_0 = 3^s$, $s \geq 1$) is given by $\mathbb{F}_q(C') = \mathbb{F}_q(x, y_1, y_2)$, with

$$y_1^q - y_1 = x^{q_0}(x^q - x) \quad (1)$$
$$y_2^q - y_2 = x^{q_0}(y_1^q - y_1). \quad (2)$$

The genus of C' is $g = \frac{3}{2}q_0(q-1)(q+q_0+1)$, and it has $1+q^3$ $\mathbb{F}_q$-rational points, including one point at infinity.

Let X be the non-singular model of the function field of the affine curve defined by (1). It is a quotient of $C'/\mathbb{F}_q$, via the map $\pi : C' \to X$ such that

$$(x, y_1, y_2) \mapsto (x, y_1).$$

For the sake of simplicity we will replace y_1 by y, so (the function field of) X is defined by the equation

$$y^q - y = x^{q_0}(x^q - x).$$

We state some important facts developed about the curve X in [4, 5].

Proposition 1: $X/\mathbb{F}_q$ is irreducible with a single point at infinity (i.e. in the complement of the affine curve), denoted by P_∞. The rational functions on $X/\mathbb{F}_q$, defined by

$$1,\ x,\ y,\ u = x^{3q_0+1} - y^{3q_0}, \text{and } v = x^2y^{3q_0} - u^{3q_0}$$

are regular on $X \setminus \{P_\infty\}$. At P_∞, the pole orders of these functions are

$$-\text{ord}_\infty(1) = 0,\ -\text{ord}_\infty(x) = q,\ -\text{ord}_\infty(y) = q + q_0,$$
$$-\text{ord}_\infty(u) = q + 3q_0,\ -\text{ord}_\infty(v) = 2q + 3q_0 + 1.$$

The element $\frac{xu}{v}$ is a uniformizer at P_∞.

Proposition 2: The curve X has genus $g = \frac{3}{2}q_0(q-1)$ with $1+q^2$ $\mathbb{F}_q$-rational points. The divisor of the differential dx, known as the canonical divisor K_X is given by

$$\text{div}(dx) = (2g-2)P_\infty$$

.
See [5] for proof.

Zeta Function and Holomorphic Differentials on X

The Zeta function of the Ree curve C' is given by

$$Z(C', T) = \frac{(1+3q_0T+qT^2)^{q_0(q^2-1)}(1+qT^2)^{\frac{q_0(q-1)(q+3q_0+1)}{2}}}{(1-T)(1-qT)}$$

Being quotient of the Ree curve, X then has Zeta function.

$$Z(X, T) = \frac{(1+3q_0T+qT^2)^{q_0(q-1)}(1+qT^2)^{\frac{q_0}{2}(q-1)}}{(1-T)(1-qT)}$$

Proposition 3: The curve $X : y^q - y = x^{q_0}(x^q - x)/\mathbb{F}_{q^r}$, (where $q = 3q_0^2$, with $q_0 = 3^s$, $s \geq 1$) is maximal if and only if $r \equiv 6 (\text{mod} 12)$

Space of Holomorphic Differentials on X

Define a set I of indices $(a, b, c, d) \in \mathbb{Z}^4$ by the following conditions:

1. $a, b, c, d \geq 0$.
2. $a + b + c + 2d \leq 3q_0 - 1$.
3. If $a + b + c + 2d = 3q_0 - 2$ then $0 \leq c \leq 2q_0 - 2$. Writing $c = 2q_0 - 2 - i$, where $0 \leq i \leq 2q_0 - 2$, either (i) $b + 3d < 2 + 3i$ and $d \leq \frac{q_0+i}{2}$ or (ii) $b + 3d = 2 + 3i$ and $0 \leq d \leq q_0 - 2$.
4. If $a + b + c + 2d = 3q_0 - 1$ then $0 \leq c \leq q_0 - 2$. Writing $c = q_0 - 2 - j$, $b + 3d \leq 2 + 3j$.

Proposition 4: The differential $x^a y^b u^c v^d\, dx$ is holomorphic if and only if $(a, b, c, d) \in I$.

Proposition 5: Define $J = \{(a, b, c, d) \in I \mid 0 \leq b \leq 2 \text{ and } 0 \leq c, d \leq q_0 - 1\}$. Then

$$\{x^a y^b u^c v^d\, dx \mid (a, b, c, d) \in J\}$$

is a basis for $H^0(X, \Omega^1)$.

Remark 1: According to the Riemann-Roch Theorem, for the canonical divisor K_C on the smooth projective curve C,

$$l(K_C) = l(H^0(C, \Omega^1)) = g$$

One can easily verify that the above propositions produce exactly g differentials $f\,dx$, where $f = x^a y^b u^c v^d : (a, b, c, d) \in J$.

Algebraic Geometric Codes

Linear Codes

Definition 2: A linear code $\mathfrak{C}(n, k, d)$ over a finite field F is a subspace of F^n. The elements of $\mathfrak{C}$ are called codewords.
n: length of code.
k: dimension of code as a subspace.
d: minimum distance defined as

$$d(\mathfrak{C}) := min\{d(x, y) | x, y \in \mathfrak{C}\ and\ x \neq y\} = min\{wt(x) | 0 \neq x \in \mathfrak{C}\}.$$

Remark 2: $\mathfrak{C}(n, k, d)$ can detect $d-1$ and correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

Remark 3: For an efficient code, we need large d (to correct more errors) and large k (to transmit long messages).

For each linear code $\mathfrak{C}(n, k, d)$ we define the generating matrix $G(\mathfrak{C})$ by the help of k- basis vectors for $\mathfrak{C}$, i.e. if $r_i = (r_{i1}, r_{i2}.....r_{in})$ form basis for $\mathfrak{C}$, where $1 \leq i \leq k$, then the generating matrix is given by

$$G(\mathfrak{C}) = \begin{bmatrix} r_{11} & r_{12} & . & . & . & r_{1n} \\ r_{21} & r_{22} & . & . & . & r_{2n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ r_{k1} & r_{k2} & . & . & . & r_{kn} \end{bmatrix}$$

Algebraic Geometric Codes

Algebraic geometric codes (commonly known as Goppa codes) are linear codes constructed with the help of algebraic curves over the finite field with many rational points (i.e. maximal curves).
Let C be a smooth curve over $\mathbb{F}_q$. Let $D = P_1 + P_2 + ...P_n$ be a divisor $\epsilon\ Div(C)$, where $P_{i's}(1 \leq i \leq n)$ are $\mathbb{F}_{q-}$ rational points on C.
Let G be another divisor on C, such that $Supp(G)$ is disjoint from $\{P_{i's}\}$.
Let $f_i's \epsilon\ L(G)$ form a basis for $L(G)$. We can evaluate each of $f_i's$ at the rational points $P_i's(1 \leq i \leq n)$, thus we can define a map $\varphi : L(G) \to \mathbb{F}_q^n$ by

$$\varphi(f_i) = (f_i(P_1), f_i(P_2), ...f_i(P_n))$$

The Image of φ produces Goppa codes on C.

Algebraic Geometric Codes on X

On $X : y^q - y = x^{q_0}(x^q - x)$, if we take $D = P_1 + P_2 + ...P_{q^2}$ and $G = (2g-2)P_\infty$. Then by Remark 1, $f_i's \epsilon\ L(G) = L(K_X)$. These $f_i's$ (where $1 \leq i \leq g$), when evaluated at P_j's (where $1 \leq j \leq q^2$) produce the generating matrix for Goppa codes as follows

$$G(\mathfrak{C}) = \begin{bmatrix} f_1(P_1) & f_1(P_2) & . & . & . & f_1(P_{q^2}) \\ f_2(P_1) & f_2(P_2) & . & . & . & f_2(P_{q^2}) \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ f_g(P_1) & f_g(P_2) & . & . & . & f_g(P_{q^2}) \end{bmatrix}$$

In particular, for $s = 1$, $g = 117$ i.e. 117 rational functions serve as a basis and hence form 117 rows of our generating matrix (i.e. $k = 117$). On the other hand, in case of $s = 1$, number of rational points involved in the divisor D are $q^2 = 729$ and they form $n = 729$ columns of the generating matrix. With these parameters $d \leq n - (2g-2) = 497$, this produces a code $\mathfrak{C}$ which may correct up to 248 errors.

References

1. V. D. Goppa. *Geometry and Codes*. Kluwer Academic Publishers, Dordrecht, (1988).
2. J. P. Hansen and H. Stichtenoth. Group codes on certain algebraic curves with many rational points. *Appl. Algebra Engrg. Comm. Comput.*, 1,(1990): 67-77.
3. J. P. Hansen, Deligne-Lusztig varieties and group codes, in *Coding theory and algebraic geometry (Luminy, 1991)*, Lect. Notes Math. 1518, 63-81, Springer- Verlag, 1992.
4. S. Farwa, *Exact holomorphic differentials on certain algebraic curves*. Ph. D. thesis, University of Sheffeld, June (2012).
5. N. Dummigan, S. Farwa, Exact holomorphic differentials on a quotient of the Ree curve, *Journal of Algebra*, 400,(2014): 249-272.

2015 COMSATS Institute of Information Technology, Wah Campus, Paksitan
drsfarwa@gmail.com