Yoonjin Lee
Department of Mathematics, Simon Fraser University
yoonjinl@sfu.ca

Construction of Cubic Function Fields from Quadratic Infrastructure

Joint work with M. J. Jacobson, R. Scheidler, H. C. Williams at University of Calgary

Outline

- Motivation and goal
- Background
- CUFFQI work: Theoretical part
  - The Hass Theorem (function field version)
  - Cubic fields from quadratic ideals
- CUFFQI work: Algorithm

Motivation and goal

Motivation: The CUFFQI method was first proposed by Shanks for number fields in an unpublished manuscript from the 1970s.

Motivation and goal

Motivation: The CUFFQI method was first proposed by Shanks for number fields in an unpublished manuscript from the 1970s.

Goal: Finding an efficient method for generating all non-conjugate cubic function fields of a given squarefree discriminant, using the infrastructure of the dual real function field associated with the hyperelliptic field of the same discriminant.

Hyperelliptic function fields

$\mathbb{F}_q$ = the finite field of order q with q a power of an odd prime.

$k = \mathbb{F}_q(t)$ the rational function field with t transcendental over $\mathbb{F}_q$.

P_∞ = the prime at infinity (or the infinite place) of k defined by the negative degree valuation, $ord_\infty(g) = -$ deg (g) for $g \in K^*$.

Hyperelliptic function fields

$\mathbb{F}_q$ = the finite field of order q with q a power of an odd prime.

$k = \mathbb{F}_q(t)$ the rational function field with t transcendental over $\mathbb{F}_q$.

P_∞ = the prime at infinity (or the infinite place) of k defined by the negative degree valuation, $ord_\infty(g) = -$ deg (g) for $g \in K^*$.

A hyperelliptic function field is defined by

$$K = k(y)$$

where $y^2 = D(t)$ and $D \in \mathbb{F}_q[t]$ is a squarefree polynomial.

The genus of K is $g = \lfloor(\deg(D) - 1)/2\rfloor$,
and the discriminant of K/k is D.

Signature

M/k algebraic extension.

The maximal order $\mathcal{O}$ of M/k, i.e. the integral closure of $\mathbb{F}_q[t]$ in M/k, is a Dedekind domain.

So every place P of k splits in M uniquely, up to order of factors, as

$$(P) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}, \tag{1}$$

where $\mathfrak{p}_i$ is a place of M (a prime ideal in $\mathcal{O}$) of residue degree $f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_q] \in \mathbb{N}$ and ramification index $e_i \in \mathbb{N}$ with $\sum_{i=1}^{s} e_i f_i = n$.

Signature

M/k algebraic extension.

The maximal order $\mathcal{O}$ of M/k, i.e. the integral closure of $\mathbb{F}_q[t]$ in M/k, is a Dedekind domain.

So every place P of k splits in M uniquely, up to order of factors, as

$$(P) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_s^{e_s}, \tag{1}$$

where $\mathfrak{p}_i$ is a place of M (a prime ideal in $\mathcal{O}$) of residue degree $f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_q] \in \mathbb{N}$ and ramification index $e_i \in \mathbb{N}$ with $\sum_{i=1}^{s} e_i f_i = n$.

The P-signature of M/k is the $2s$-tuple $(e_1, f_1, e_2, f_2, \ldots, e_s, f_s)$ where the pairs (e_i, f_i), $1 \leq i \leq s$, are sorted in lexicographical order.

If P is the place at infinity of k, we refer to the P-signature as simply the signature (or the signature at infinity) of M/k.

Hyperelliptic function fields - imaginary or real

The extension K/k is said to be real

$$if \quad \deg(D) \text{ is even (so } \deg(D) = 2g+2) \text{ and}$$
$$\text{the leading coefficient } \operatorname{sgn}(D) \text{ of } D \text{ is a square in } \mathbb{F}_q,$$

and imaginary otherwise.

Hyperelliptic function fields - imaginary or real

The extension K/k is said to be real

$$if \quad \deg(D) \text{ is even (so } \deg(D) = 2g+2) \text{ and}$$
$$\text{the leading coefficient } \operatorname{sgn}(D) \text{ of } D \text{ is a square in } \mathbb{F}_q,$$

and imaginary otherwise.

More exactly,

$$\begin{aligned} (2,1) &\quad \text{if } \deg(D) \text{ is odd.} \\ (1,2) &\quad \text{if } \deg(D) \text{ is even and } \operatorname{sgn}(D) \text{ is a non-square,} \\ (1,1,1,1) &\quad \text{if } \deg(D) \text{ is even and } \operatorname{sgn}(D) \text{ is a square.} \end{aligned}$$

In the real case, if ϵ is any fundamental unit of K/k, then $R = |\deg(\epsilon)|$ is the regulator of K/k.

The Scholz theorem for function fields

The polynomials D and $D' = nD$ with $n \in \mathbb{F}_q^*$ any non-square $n \in \mathbb{F}_q$ are said to be dual discriminants.

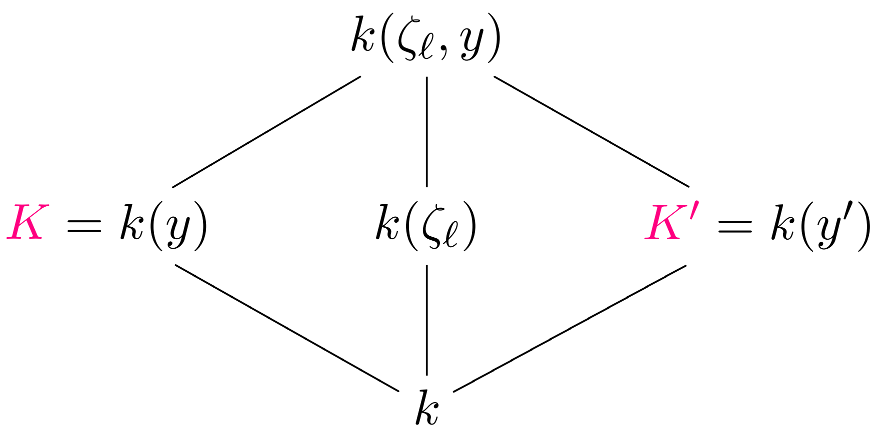
Corresponding extensions K/k and K'/k where $K' = k(y')$ and $(y')^2 = D'$ are dual hyperelliptic fields.

The Scholz theorem for function fields

The polynomials D and $D' = nD$ with $n \in \mathbb{F}_q^*$ any non-square $n \in \mathbb{F}_q$ are said to be dual discriminants.

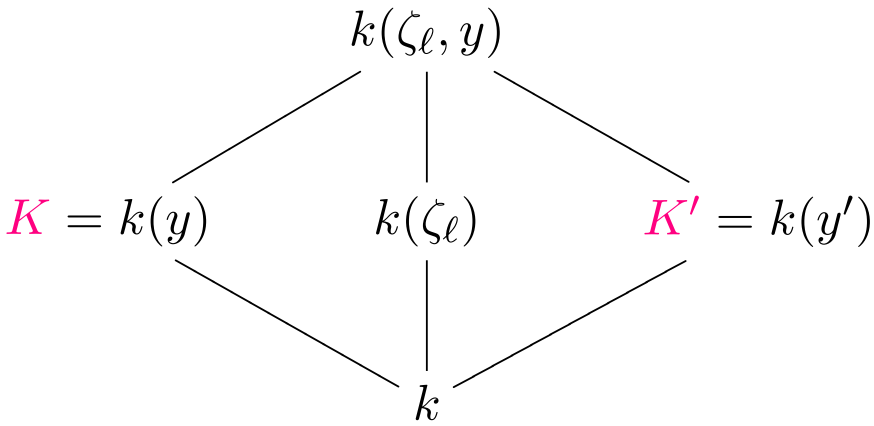
Corresponding extensions K/k and K'/k where $K' = k(y')$ and $(y')^2 = D'$ are dual hyperelliptic fields.

Let $L = KK' = K(\zeta_\ell, y)$, where ℓ is an odd prime dividing $q + 1$.



Note that K/k has signature $(1, 2)$ (inert) if and only if K'/k has signature $(1, 1, 1, 1)$ (splits completely).

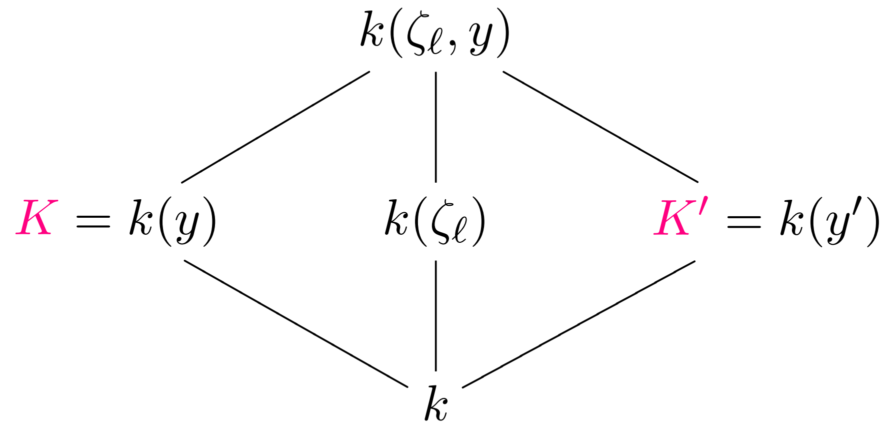
The Scholz theorem for function fields



$r = \ell$-rank of the ideal class group of K/k.

$r' = \ell$-rank of the ideal class group of K'/k.

The Scholz theorem for function fields

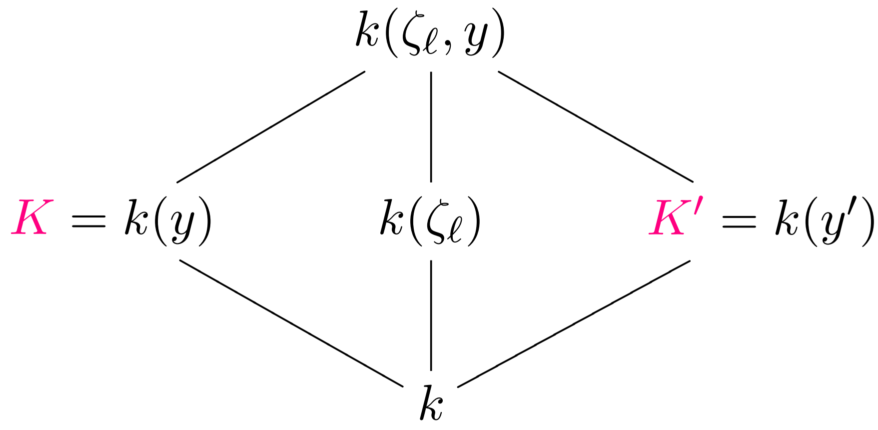


$r = \ell$-rank of the ideal class group of K/k.

$r' = \ell$-rank of the ideal class group of K'/k.

Then $\boxed{r_1 = r_2 \quad \text{or} \quad r_1 = r_2 + 1.}$

The Scholz theorem for function fields



$r = \ell$-rank of the ideal class group of K/k.

$r' = \ell$-rank of the ideal class group of K'/k.

Then $\boxed{r_1 = r_2 \quad \text{or} \quad r_1 = r_2 + 1.}$

• In the latter case, i.e. $r_1 = r_2 + 1$, the regulator R of K'/k is divisible by ℓ. Equivalently, if $\boxed{\ell \nmid R}$, then $r_1 = r_2$.

Linking a certain norm equation to ideal classes of order 1 or 3

Let $A, B, Q, D' \in \mathbb{F}_q[t]$ (q odd) be non-zero polynomials such that D' is squarefree and

$$\boxed{Q^3 = A^2 - B^2 D'.}$$

Linking a certain norm equation to ideal classes of order 1 or 3

Let $A, B, Q, D' \in \mathbb{F}_q[t]$ (q odd) be non-zero polynomials

such that D' is squarefree and

$$\boxed{Q^3 = A^2 - B^2 D'.}$$

Set $G = \gcd(A, Q)$ and assume that G divides D',

and $\boxed{\lambda = A + By'.}$

Assume $\boxed{\mathfrak{a} = (Q, \lambda/G)}$ is the ideal generated by Q and λ/G in the maximal order $\mathcal{O}'$ of the hyperelliptic function field K' of discriminant D'.

Linking a certain norm equation to ideal classes of order 1 or 3

Let $A, B, Q, D' \in \mathbb{F}_q[t]$ (q odd) be non-zero polynomials

such that D' is squarefree and

$$\boxed{Q^3 = A^2 - B^2 D'.}$$

Set $G = \gcd(A, Q)$ and assume that G divides D',

and

$$\boxed{\lambda = A + By'.}$$

Assume $\boxed{\mathfrak{a} = (Q, \lambda/G)}$ is the ideal generated by Q and λ/G in the maximal order $\mathcal{O}'$ of the hyperelliptic function field K' of discriminant D'.

Then $\mathfrak{a}$ satisfies the following properties:

- $\mathfrak{a} + \overline{\mathfrak{a}} = \mathfrak{g}$ where $\mathfrak{g}^2 = (G)$;
- $N(\mathfrak{a}) = \mathrm{sgn}(Q)^{-1} Q$;
- $\mathfrak{a}^3 = (\lambda)$;
- $\mathfrak{a}$ is primitive.

Cubic function fields

• Every cubic extension of k can be written in the form $L = k(z)$, where

$$\boxed{z^3 - 3Qz + 2A = 0}$$

with $Q, A \in \mathbb{F}_q[t]$.

• We may assume that L (and its defining polynomial $F(Z) = Z^3 - 3QZ + 2A$) are in standard form; that is, no non-constant polynomial $G \in \mathbb{F}_q[t]$ satisfies $v_G(Q) \geq 2$ and $v_G(A) \geq 3$.

Cubic function fields

• Every cubic extension of k can be written in the form $L = k(z)$, where

$$\boxed{z^3 - 3Qz + 2A = 0}$$

with $Q, A \in \mathbb{F}_q[t]$.

• We may assume that L (and its defining polynomial $F(Z) = Z^3 - 3QZ + 2A$) are in standard form; that is, no non-constant polynomial $G \in \mathbb{F}_q[t]$ satisfies $v_G(Q) \geq 2$ and $v_G(A) \geq 3$.

• The discriminant of $F(Z)$ is $\Delta = 4(3Q)^3 - 27(2A)^2 = 108(Q^3 - A^2)$.

• It is easy to compute the discriminant D of L/k from Δ using the following theorem:

Cubic function fields

• Every cubic extension of k can be written in the form $L = k(z)$, where

$$\boxed{z^3 - 3Qz + 2A = 0}$$

with $Q, A \in \mathbb{F}_q[t]$.

• We may assume that L (and its defining polynomial $F(Z) = Z^3 - 3QZ + 2A$) are in standard form; that is, no non-constant polynomial $G \in \mathbb{F}_q[t]$ satisfies $v_G(Q) \geq 2$ and $v_G(A) \geq 3$.

• The discriminant of $F(Z)$ is $\Delta = 4(3Q)^3 - 27(2A)^2 = 108(Q^3 - A^2)$.

• It is easy to compute the discriminant D of L/k from Δ using the following theorem:

Assume $\mathbb{F}_q$ has characteristic at least 5, and let P be any irreducible divisor of Δ. Then

- $v_P(D) = 2$ if and only if $v_P(Q) \geq v_P(A) \geq 1$;
- $v_P(D) = 1$ if and only if $v_P(\Delta)$ is odd;
- $v_P(D) = 0$ otherwise.

Cubic function fields - signature

- The signature of L/k at infinity is

$$(1,1,1,1,1,1),(1,1,1,2),(1,3),(1,1,2,1), \text{ or } (3,1).$$

Cubic function fields - signature

• The signature of L/k at infinity is

$$(1,1,1,1,1,1),(1,1,1,2),(1,3),(1,1,2,1), \text{ or } (3,1).$$

• We have an explicit signature characterization for cubic extensions (Renate, Lee) only depending on degree and sgn conditions of A, Q, Δ.

Cubic function fields - signature

• The signature of L/k at infinity is

$$(1,1,1,1,1,1), (1,1,1,2), (1,3), (1,1,2,1), \text{ or } (3,1).$$

• We have an explicit signature characterization for cubic extensions (Renate, Lee) only depending on degree and sgn conditions of A, Q, Δ.

• If z, z', z'' are the three zeros of $F(Z) = Z^3 - 3QZ + 2A$,
then $L = k(z)$, $L' = k(z')$, $L'' = k(z'')$ are conjugate fields;
obviously, they all have the same discriminant D.

Cubic function fields - signature

• The signature of L/k at infinity is

$$(1,1,1,1,1,1),(1,1,1,2),(1,3),(1,1,2,1), \text{ or } (3,1).$$

• We have an explicit signature characterization for cubic extensions (Renate, Lee) only depending on degree and sgn conditions of A, Q, Δ.

• If z, z', z'' are the three zeros of $F(Z) = Z^3 - 3QZ + 2A$,
then $L = k(z)$, $L' = k(z')$, $L'' = k(z'')$ are conjugate fields;
obviously, they all have the same discriminant D.

• The extension L/k is Galois if and only if D (and hence Δ) is a square in $\mathbb{F}_q[t]$, and $\mathrm{Gal}(L/k) = \mathbb{Z}/3\mathbb{Z}$.

Cubic function fields - signature

- The signature of L/k at infinity is

$$(1,1,1,1,1,1),(1,1,1,2),(1,3),(1,1,2,1), \text{ or } (3,1).$$

- We have an explicit signature characterization for cubic extensions (Renate, Lee) only depending on degree and sgn conditions of A, Q, Δ.

- If z, z', z'' are the three zeros of $F(Z) = Z^3 - 3QZ + 2A$, then $L = k(z)$, $L' = k(z')$, $L'' = k(z'')$ are conjugate fields; obviously, they all have the same discriminant D.

- The extension L/k is Galois if and only if D (and hence Δ) is a square in $\mathbb{F}_q[t]$, and $\mathrm{Gal}(L/k) = \mathbb{Z}/3\mathbb{Z}$.

- If L/k is not Galois, then the Galois closure of L/k is $N = KK'K'' = K(y)$ where $y^2 =$ the squarefree part of D. Then $[N : k] = 6$, and the Galois group of N/k is $\mathcal{S}_3$ (=the symmetric group on 3 letters).

Connections between cubic and hyperelliptic Function Fields

A very deep connection between cubic and quadratic extensions was first observed by Hasse for number fields.

Connections between cubic and hyperelliptic Function Fields

A very deep connection between cubic and quadratic extensions was first observed by Hasse for number fields.

Hasse's Theorem: function field version

Let K/k be a hyperelliptic extension of squarefree discriminant D and characteristic at least 5, and let r be the 3-rank of the ideal class group of K/k.

If K/k is inert at P_∞ (signature $(1, 2)$),

Connections between cubic and hyperelliptic Function Fields

A very deep connection between cubic and quadratic extensions was first observed by Hasse for number fields.

Hasse's Theorem: function field version

Let K/k be a hyperelliptic extension of squarefree discriminant D and characteristic at least 5, and let r be the 3-rank of the ideal class group of K/k.

If K/k is inert at P_∞ (signature $(1, 2)$),

then the number of distinct unordered triples of conjugate cubic fields $\{L, L', L''\}$ over k of discriminant D of unit rank 1 is

$$(3^r - 1)/2.$$

Connections between cubic and hyperelliptic Function Fields

A very deep connection between cubic and quadratic extensions was first observed by Hasse for number fields.

Hasse's Theorem: function field version

Let K/k be a hyperelliptic extension of squarefree discriminant D and characteristic at least 5, and let r be the 3-rank of the ideal class group of K/k.

If K/k is inert at P_∞ (signature $(1, 2)$),

then the number of distinct unordered triples of conjugate cubic fields $\{L, L', L''\}$ over k of discriminant D of unit rank 1 is

$$(3^r - 1)/2.$$

If K/k is splits completely at P_∞ (signature $(1, 1, 1, 1)$),

Connections between cubic and hyperelliptic Function Fields

A very deep connection between cubic and quadratic extensions was first observed by Hasse for number fields.

Hasse's Theorem: function field version

Let K/k be a hyperelliptic extension of squarefree discriminant D and characteristic at least 5, and let r be the 3-rank of the ideal class group of K/k.

If K/k is inert at P_∞ (signature $(1, 2)$),

then the number of distinct unordered triples of conjugate cubic fields $\{L, L', L''\}$ over k of discriminant D of unit rank 1 is

$$(3^r - 1)/2.$$

If K/k is splits completely at P_∞ (signature $(1, 1, 1, 1)$),

then the number of distinct unordered triples of conjugate cubic fields $\{L, L', L''\}$ over k of discriminant D of unit rank 2 is

$$(3^r - 1)/2.$$

Hasse's Theorem: Idea Sketch

- Let H be the maximal unramified abelian extension of K (in K_s) with exponent 3 in which P_∞ splits completely.

Then H/K is Galois, and let $Cl(K)(3) := Cl(K)/Cl(K)^3$.

Hasse's Theorem: Idea Sketch

• Let H be the maximal unramified abelian extension of K (in K_s) with exponent 3 in which P_∞ splits completely.

Then H/K is Galois, and let $Cl(K)(3) := Cl(K)/Cl(K)^3$.

• From Class field Theory,

$$\mathcal{G} = \mathrm{Gal}(H/K) \simeq Cl(K)(3)$$

by the Artin symbol $(\ ,H/K)$. They are isomorphic as $\mathbb{F}_3[G]$-modules.

Hasse's Theorem: Idea Sketch

• Let H be the maximal unramified abelian extension of K (in K_s) with exponent 3 in which P_∞ splits completely.

Then H/K is Galois, and let $Cl(K)(3) := Cl(K)/Cl(K)^3$.

• From Class field Theory,

$$\mathcal{G} = \mathrm{Gal}(H/K) \simeq Cl(K)(3)$$

by the Artin symbol $(\ , H/K)$. They are isomorphic as $\mathbb{F}_3[G]$-modules.

• Since the 3-rank of $Cl(K)$ is r, $\mathcal{G}$ has exactly $\frac{3^r-1}{3-1}$ distinct subgroups of index 3.

< > ⋘ ⋙ i ? P

Hasse's Theorem: Idea Sketch

• Let H be the maximal unramified abelian extension of K (in K_s) with exponent 3 in which P_∞ splits completely.

Then H/K is Galois, and let $Cl(K)(3) := Cl(K)/Cl(K)^3$.

• From Class field Theory,

$$\mathcal{G} = \mathrm{Gal}(H/K) \simeq Cl(K)(3)$$

by the Artin symbol $(\ , H/K)$. They are isomorphic as $\mathbb{F}_3[G]$-modules.

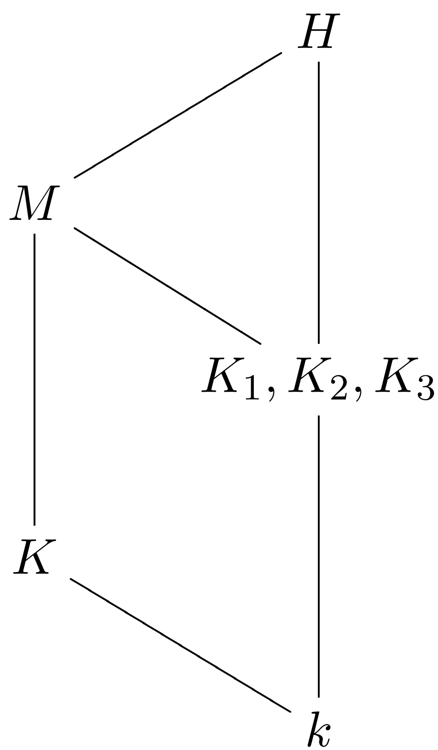
• Since the 3-rank of $Cl(K)$ is r, $\mathcal{G}$ has exactly $\frac{3^r-1}{3-1}$ distinct subgroups of index 3.

• Let N be a subgroup of $\mathcal{G}$ of index 3.

Then the corresponding fixed field M of N is a Galois extension of k containing K with $\mathrm{Gal}(M/k) \simeq S_3$.

Hasse's Theorem: Idea Sketch - cont'd

• There are three elements of order 2 in S_3, which are all conjugate. The fixed fields K_1, K_2, K_3 of the elements of order 2 in $\mathrm{Gal}(M/k)$ are all isomorphic cubic extensions of k.



• We can show that K_1, K_2, K_3 have the same discriminants as that of K up to constant factors in ${\mathbb{F}_q}^*$.

Cubic fields from quadratic ideals

- Henceforth, $q \equiv -1 \pmod 3$ (so, -3 is a non-square in $\mathbb{F}_q$).

- Fix a squarefree polynomial $D \in \mathbb{F}_q[t]$ of even degree
whose leading coefficient is a nonsquare.

- $D' := D/(-3)$.

Cubic fields from quadratic ideals

• Henceforth, $q \equiv -1 \pmod 3$ (so, -3 is a non-square in $\mathbb{F}_q$).

• Fix a squarefree polynomial $D \in \mathbb{F}_q[t]$ of even degree
whose leading coefficient is a nonsquare.

• $D' := D/(-3)$.

• Then $K = k(y)$ with $y^2 = D$
is an imaginary hyperelliptic function field of signature $(1, 2)$.

• $K' = k(y')$ with $(y')^2 = D'$
is the dual real hyperelliptic function field.

• $\mathcal{O}' :=$ the maximal order of K'.
For any ideal $\mathfrak{a} \in \mathcal{O}'$, the ideal class of $\mathfrak{a}$ is denoted by $[\mathfrak{a}]$.
Finally, if L/k is a cubic extension, we denote by L' and L'' the conjugate fields of L.

Cubic fields from quadratic ideals

Our goal: Generating every element in $\mathcal{L}$.

Cubic fields from quadratic ideals

Our goal: Generating every element in $\mathcal{L}$.

- We consider the following sets:

$$\mathcal{L} = \{\ \{L, L', L''\} \mid [L:k] = 3,\ L/k \text{ has discriminant } D\ \},$$

$$\mathcal{I} = \{\ \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} \mid\ \mathfrak{a} \text{ is a primitive ideal in } \mathcal{O}' \text{ and } [\mathfrak{a}]^3 = [\mathcal{O}']\ \}.$$

Cubic fields from quadratic ideals

Our goal: Generating every element in $\mathcal{L}$.

- We consider the following sets:

$$\mathcal{L} = \{\ \{L, L', L''\} \mid [L:k] = 3,\ L/k \text{ has discriminant } D\ \},$$

$$\mathcal{I} = \{\ \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} \mid\ \mathfrak{a} \text{ is a primitive ideal in } \mathcal{O}' \text{ and } [\mathfrak{a}]^3 = [\mathcal{O}']\ \}.$$

- Define a surjection $\Phi : \mathcal{L} \to \mathcal{I}$.

- Then we prove that for any $s = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} \in \mathcal{I}$,

  the pre-image $\Phi^{-1}(s)$ of s under Φ contains

  three distinct triples in $\mathcal{L}$ if $\mathfrak{a}$ is a non-principal ideal,

  and one such triple if $\mathfrak{a}$ is principal.

The map Φ from $\mathcal{L}$ to $\mathcal{I}$

Let $F(Z) = Z^3 - 3QZ + 2A$ with $Q, A \in \mathbb{F}_q[t]$ be a defining polynomial of L/k in standard form.

• Note that $Q \neq 0$ since L/k has squarefree discriminant, and $A \neq 0$ since F is irreducible over k. Then we have $L = k(z)$ where

$$\boxed{z^3 - 3Qz + 2A = 0.}$$

The map Φ from $\mathcal{L}$ to $\mathcal{I}$

Let $F(Z) = Z^3 - 3QZ + 2A$ with $Q, A \in \mathbb{F}_q[t]$ be a defining polynomial of L/k in standard form.

• Note that $Q \neq 0$ since L/k has squarefree discriminant, and $A \neq 0$ since F is irreducible over k. Then we have $L = k(z)$ where

$$\boxed{\mathrm{z}^3 - 3Qz + 2A = 0.}$$

• If Δ is the discriminant of $F(Z)$, then $\Delta = 108(Q^3 - A^2)$. Let I be the index of z, so $\Delta = I^2 D$ and set $B = I/6$. Then $\Delta = (6B)^2(-3D') = -108B^2D'$ and hence

$$\boxed{\mathrm{A}^2 - B^2 D' = Q^3.}$$

The map Φ from $\mathcal{L}$ to $\mathcal{I}$

Let $F(Z) = Z^3 - 3QZ + 2A$ with $Q, A \in \mathbb{F}_q[t]$ be a defining polynomial of L/k in standard form.

• Note that $Q \neq 0$ since L/k has squarefree discriminant, and $A \neq 0$ since F is irreducible over k. Then we have $L = k(z)$ where

$$\boxed{\mathsf{z}^3 - 3Qz + 2A = 0.}$$

• If Δ is the discriminant of $F(Z)$, then $\Delta = 108(Q^3 - A^2)$. Let I be the index of z, so $\Delta = I^2 D$ and set $B = I/6$. Then $\Delta = (6B)^2(-3D') = -108B^2D'$ and hence

$$\boxed{\mathsf{A}^2 - B^2D' = Q^3.}$$

The unordered pair $\{\lambda, \overline{\lambda}\}$ where $\lambda = A + By' \in \mathcal{O}'$ is called a pair of *quadratic generators* of $\{L, L', L''\}$.

• Pairs of quadratic generators $\Longleftrightarrow$ $\boxed{\mathsf{z}^3 - 3Qz + 2A = 0.}$ (one-to-one correspondence):

$$\boxed{\{\lambda, \overline{\lambda}\} = \text{quadratic generators of } \{L, L', L''\}} \Longleftrightarrow \boxed{Tr(\lambda) = 2A,\ N(\lambda) = Q^3.}$$

The map Φ from $\mathcal{L}$ to $\mathcal{I}$ -continued

- Let $\lambda \in \mathcal{O}'$.

$$\boxed{\{\lambda, \overline{\lambda}\} \text{ is a pair of quadratic generators of a triple } \{L, L', L''\} \in \mathcal{L}.}$$

$$\Updownarrow$$

$$\boxed{\lambda \neq \overline{\lambda},\ \lambda \text{ is not a cube in } \mathcal{O}', \text{ and } (\lambda) \text{ is the cube of a primitive ideal in } \mathcal{O}'.}$$

The map Φ from $\mathcal{L}$ to $\mathcal{I}$ -continued

- Let $\lambda \in \mathcal{O}'$.

$\{\lambda, \overline{\lambda}\}$ is a pair of quadratic generators of a triple $\{L, L', L''\} \in \mathcal{L}$.

$$\Updownarrow$$

$\lambda \neq \overline{\lambda}$, λ is not a cube in $\mathcal{O}'$, and (λ) is the cube of a primitive ideal in $\mathcal{O}'$.

We now investigate under what circumstances different pairs of quadratic generators correspond to the same triple of fields in $\mathcal{L}$:

- For $i = 1, 2$, let $\{\lambda_i, \overline{\lambda}_i\}$ be a pair of quadratic generators of a triple $\{L_i, L_i', L_i''\} \in \mathcal{L}$. Then $(L_1, L_1', L_1'') = (L_2, L_2', L_2'')$ if and only if there exists a non-zero element $\beta \in K'$ such that

$$\frac{\lambda_1}{\overline{\lambda}_1}\left(\frac{\beta}{\overline{\beta}}\right)^3 \in \left\{\frac{\lambda_2}{\overline{\lambda}_2}, \frac{\overline{\lambda}_2}{\lambda_2}\right\}.$$

The map Φ from $\mathcal{L}$ to $\mathcal{I}$ -continued

• **Cor.** For $i = 1, 2$, let $\{\lambda_i, \overline{\lambda}_i\}$ be two pairs of quadratic generators of a triple $\{L, L', L''\} \in \mathcal{L}$, and let $\mathfrak{a}_i$ be the primitive ideal in $\mathcal{O}'$ such that $(\lambda_i) = \mathfrak{a}_i^3$.

Then $\mathfrak{a}_1$ is equivalent to $\mathfrak{a}_2$ or $\overline{\mathfrak{a}}_2$.

The map Φ from $\mathcal{L}$ to $\mathcal{I}$ -continued

• **Cor.** For $i = 1, 2$, let $\{\lambda_i, \overline{\lambda}_i\}$ be two pairs of quadratic generators of a triple $\{L, L', L''\} \in \mathcal{L}$, and let $\mathfrak{a}_i$ be the primitive ideal in $\mathcal{O}'$ such that $(\lambda_i) = \mathfrak{a}_i^3$.

Then $\mathfrak{a}_1$ is equivalent to $\mathfrak{a}_2$ or $\overline{\mathfrak{a}}_2$.

• The map $\Phi : \mathcal{L} \to \mathcal{I}$:

$\{L, L, L''\}$ = each unordered triple of conjugate cubic fields of discriminant D

$\downarrow$

$s := \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ = the unordered pair of ideal classes such that $(\lambda) = \mathfrak{a}^3$ for some pair $\{\lambda, \overline{\lambda}\}$ of quadratic generators of $\{L, L, L''\}$.

The map Φ from $\mathcal{L}$ to $\mathcal{I}$ -continued

• **Cor.** For $i = 1, 2$, let $\{\lambda_i, \overline{\lambda}_i\}$ be two pairs of quadratic generators of a triple $\{L, L', L''\} \in \mathcal{L}$, and let $\mathfrak{a}_i$ be the primitive ideal in $\mathcal{O}'$ such that $(\lambda_i) = \mathfrak{a}_i^3$.

Then $\mathfrak{a}_1$ is equivalent to $\mathfrak{a}_2$ or $\overline{\mathfrak{a}}_2$.

• The map $\Phi : \mathcal{L} \to \mathcal{I}$:

$\{L, L, L''\}$ = each unordered triple of conjugate cubic fields of discriminant D

$\downarrow$

$s := \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ = the unordered pair of ideal classes such that $(\lambda) = \mathfrak{a}^3$ for some pair $\{\lambda, \overline{\lambda}\}$ of quadratic generators of $\{L, L, L''\}$.

• The map Φ is well-defined and surjective.

Pre-Images under Φ

Goal: Prove that pre-images of pairs of non-principal conjugate ideal classes under the map Φ have cardinality 3,

and the pre-image of the pair $\{[\mathcal{O}'], [\bar{\mathcal{O}}']\}$ under Φ contains one triple in $\mathcal{L}$.

Pre-Images under Φ

Goal: Prove that pre-images of pairs of non-principal conjugate ideal classes under the map Φ have cardinality 3,

and the pre-image of the pair $\{[\mathcal{O}'], [\bar{\mathcal{O}}']\}$ under Φ contains one triple in $\mathcal{L}$.

• Let $s \in \mathcal{I}$, $s \neq \{[\mathcal{O}'], [\bar{\mathcal{O}}']\}$, and let $\{L_1, L_1', L_1''\}, \{L_2, L_2', L_2''\} \in \Phi^{-1}(s)$. For $i = 1, 2$, let $\{\lambda_i, \overline{\lambda}_i\}$ be a pair of quadratic generators of L_i, L_i', L_i''. Then $\{L_1, L_1', L_1''\} = \{L_2, L_2', L_2''\}$ if and only if $\lambda_1 = \alpha^3 \lambda_2$ or $\lambda_1 = \alpha^3 \overline{\lambda}_2$ for some non-zero $\alpha \in K'$.

Pre-Images under Φ

Goal: Prove that pre-images of pairs of non-principal conjugate ideal classes under the map Φ have cardinality 3,

and the pre-image of the pair $\{[\mathcal{O}'], [\bar{\mathcal{O}}']\}$ under Φ contains one triple in $\mathcal{L}$.

• Let $s \in \mathcal{I}$, $s \neq \{[\mathcal{O}'], [\bar{\mathcal{O}}']\}$, and let $\{L_1, L_1', L_1''\}, \{L_2, L_2', L_2''\} \in \Phi^{-1}(s)$. For $i = 1, 2$, let $\{\lambda_i, \overline{\lambda}_i\}$ be a pair of quadratic generators of L_i, L_i', L_i''. Then $\{L_1, L_1', L_1''\} = \{L_2, L_2', L_2''\}$ if and only if $\lambda_1 = \alpha^3\lambda_2$ or $\lambda_1 = \alpha^3\overline{\lambda}_2$ for some non-zero $\alpha \in K'$.

• Lemma. Let $s \in \mathcal{I}$, $\mathfrak{a}$ any primitive ideal such that $s = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$, and λ a generator of $\mathfrak{a}^3$ such that $\lambda \neq \overline{\lambda}$ and λ not a cube in $\mathcal{O}'$. Then any pair of quadratic generators of any triple of fields in $\Phi^{-1}(s)$ is of the form $\{\mu, \overline{\mu}\}$ where $\mu = e^j\alpha^3\beta$ with $j \in \{0, 1, 2\}$, $\alpha \in K'$ non-zero, and $\beta \in \{\lambda, \overline{\lambda}\}$.

Pre-Images under Φ

Goal: Prove that pre-images of pairs of non-principal conjugate ideal classes under the map Φ have cardinality 3,

and the pre-image of the pair $\{[\mathcal{O}'], [\bar{\mathcal{O}}']\}$ under Φ contains one triple in $\mathcal{L}$.

- Let $s \in \mathcal{I}$, $s \neq \{[\mathcal{O}'], [\bar{\mathcal{O}}']\}$, and let $\{L_1, L_1', L_1''\}, \{L_2, L_2', L_2''\} \in \Phi^{-1}(s)$. For $i = 1, 2$, let $\{\lambda_i, \overline{\lambda}_i\}$ be a pair of quadratic generators of L_i, L_i', L_i''. Then $\{L_1, L_1', L_1''\} = \{L_2, L_2', L_2''\}$ if and only if $\lambda_1 = \alpha^3 \lambda_2$ or $\lambda_1 = \alpha^3 \overline{\lambda}_2$ for some non-zero $\alpha \in K'$.

- Lemma. Let $s \in \mathcal{I}$, $\mathfrak{a}$ any primitive ideal such that $s = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$, and λ a generator of $\mathfrak{a}^3$ such that $\lambda \neq \overline{\lambda}$ and λ not a cube in $\mathcal{O}'$. Then any pair of quadratic generators of any triple of fields in $\Phi^{-1}(s)$ is of the form $\{\mu, \overline{\mu}\}$ where $\mu = e^j \alpha^3 \beta$ with $j \in \{0, 1, 2\}$, $\alpha \in K'$ non-zero, and $\beta \in \{\lambda, \overline{\lambda}\}$.

- Let $s \in \mathcal{I}$. If $s = \{[\mathcal{O}'], [\bar{\mathcal{O}}']\}$, then $\Phi^{-1}(s)$ contains exactly one triple of fields in $\mathcal{L}$. If s is a pair of ideal classes of order 3, then $\Phi^{-1}(s)$ contains exactly three distinct triples of fields in $\mathcal{L}$.

< > ≪ ≫ i ? P

The Count

• If $r' :=$ the 3-rank of the ideal class group of K'/k,

then since $[\mathfrak{a}]$ and $[\overline{\mathfrak{a}}]$ are distinct ideal classes of order 3,

the number of unordered pairs $s = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ of conjugate ideal classes of order 3 is

$$\boxed{(3^{r'} - 1)/2.}$$

The Count

• If $r' :=$ the 3-rank of the ideal class group of K'/k,

then since $[\mathfrak{a}]$ and $[\overline{\mathfrak{a}}]$ are distinct ideal classes of order 3,

the number of unordered pairs $s = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ of conjugate ideal classes of order 3 is

$$\boxed{(3^{r'} - 1)/2.}$$

• These pairs correspond to $3(3^{r'} - 1)/2$ pre-images under Φ in $\mathcal{L}$,

and the pair $s = ([\mathcal{O}'], [\mathcal{O}'])$ yields one more pre-image under Φ,

for a total of $3(3^{r'} - 1)/2 + 1 = \boxed{(3^{r'+1} - 1)/2}$ distinct triples of fields in $\mathcal{L}$.

The Count - cont'd

- If K is an escalatory field, i.e. $r = r' + 1$,

then the $(3^{r'+1} - 1)/2$ distinct triples of fields in the pre-image $\Phi^{-1}(\mathcal{I})$ are exactly the $(3^r - 1)/2$ fields in $\mathcal{L}$.

The Count - cont'd

• If K is an escalatory field, i.e. $r = r' + 1$,

then the $(3^{r'+1} - 1)/2$ distinct triples of fields in the pre-image $\Phi^{-1}(\mathcal{I})$ are exactly the $(3^r - 1)/2$ fields in $\mathcal{L}$.

• If K is non-escalatory, i.e. $r = r'$,

then 3^r fields in $\mathcal{L}$ are covered multiple times by the pre-images of Φ

(since $(3^{r+1} - 1)/2 - (3^r - 1)/2 = 3^r$), and one would need a way to eliminate these duplicates.

The Count - cont'd

• If K is an escalatory field, i.e. $r = r' + 1$,

then the $(3^{r'+1} - 1)/2$ distinct triples of fields in the pre-image $\Phi^{-1}(\mathcal{I})$ are exactly the $(3^r - 1)/2$ fields in $\mathcal{L}$.

• If K is non-escalatory, i.e. $r = r'$,

then 3^r fields in $\mathcal{L}$ are covered multiple times by the pre-images of Φ

(since $(3^{r+1} - 1)/2 - (3^r - 1)/2 = 3^r$), and one would need a way to eliminate these duplicates.

• We can determine the signatures of triples of fields in $\mathcal{L}$ constructed as above:

Every triple of fields in $\mathcal{L}$ has signature, i.e. $(1, 1, 1, 2)$ or i.e. $(3, 1)$.

We can eliminate the latter case by adding $3 \nmid \deg(A)$ (and $\mathrm{sgn}(A)$ is a cube in $\mathbb{F}_q$).

The CUFFQI Algorithm

Goal: Giving efficient algorithms for constructing for each $s \in \mathcal{I}$ defining polynomials for all triples of fields in the pre-image $\Phi^{-1}(s)$.

< > ⋘ ⋙ i ? P

The CUFFQI Algorithm

Goal: Giving efficient algorithms for constructing for each $s \in \mathcal{I}$ defining polynomials for all triples of fields in the pre-image $\Phi^{-1}(s)$.

• We define a small generator of a principal ideal in $\mathcal{O}'$

to be a generator λ such that $\deg(\lambda) \leq 3g+1$ and $\deg(\overline{\lambda}) \leq 3g+1$.

The CUFFQI Algorithm

Goal: Giving efficient algorithms for constructing for each $s \in \mathcal{I}$ defining polynomials for all triples of fields in the pre-image $\Phi^{-1}(s)$.

- We define a small generator of a principal ideal in $\mathcal{O}'$

to be a generator λ such that $\deg(\lambda) \leq 3g+1$ and $\deg(\overline{\lambda}) \leq 3g+1$.

If $\lambda = A + By'$ is a small generator,

then $\deg(A) \leq 3g+1$ and $\deg(B) \leq 3g+1-\deg(y') = 2g$,

so λ can be represented by at most $(3g+2)+(2g+1) = 5g+3$ elements in $\mathbb{F}_q$.

The CUFFQI Algorithm

Idea:

For each pair $s = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$,

our goal is to compute generators of ideals equivalent to $\mathfrak{a}$ or $\overline{\mathfrak{a}}$

that produce the three triples of fields if $\mathfrak{a}$ is non-principal,

or the one triple of fields if $\mathfrak{a}$ is principal, in $\Phi^{-1}(s)$,

and we wish to do this computationally efficiently.

The CUFFQI Algorithm

Idea:

For each pair $s = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$,

our goal is to compute generators of ideals equivalent to $\mathfrak{a}$ or $\overline{\mathfrak{a}}$

that produce the three triples of fields if $\mathfrak{a}$ is non-principal,

or the one triple of fields if $\mathfrak{a}$ is principal, in $\Phi^{-1}(s)$,

and we wish to do this computationally efficiently.

- If $[\mathfrak{a}]$ is non-principal, we will generate three distinct reduced ideals equivalent to $\mathfrak{a}$ such that each of these ideals has a small generator, and each such generator produces a different triple of fields in $\mathcal{L}$.

- If $\mathfrak{a}$ is principal, we find a reduced ideal equivalent to $\mathfrak{a}$ with a small generator and use this to produce the unique triple of fields in $\Phi^{-1}(s)$.

Infrastructure - Giant step and Baby step

- An ideal in $\mathcal{O}$ is *primitive* if it is not contained in any principal ideal of the form (S) with $S \in \mathbb{F}_q[t]$.
- An *reduced* ideal in $\mathcal{O}$ is a primitive ideal $\mathfrak{a}$ in $\mathcal{O}$ with $\deg(N(\mathfrak{a})) \leq g$.

Infrastructure - Giant step and Baby step

- An ideal in $\mathcal{O}$ is *primitive* if it is not contained in any principal ideal of the form (S) with $S \in \mathbb{F}_q[t]$.
- An *reduced* ideal in $\mathcal{O}$ is a primitive ideal $\mathfrak{a}$ in $\mathcal{O}$ with $\deg(N(\mathfrak{a})) \leq g$.

- The number r of reduced ideals in each ideal class is finite; for fields of signature $(2,1)$, we have $r = 1$, for signature $(1,2)$, $r \leq 1$, and for real hyperelliptic fields, $r \approx R$ and r varies with each ideal class.

Infrastructure - Giant step and Baby step

• An ideal in $\mathcal{O}$ is *primitive* if it is not contained in any principal ideal of the form (S) with $S \in \mathbb{F}_q[t]$.

• An *reduced* ideal in $\mathcal{O}$ is a primitive ideal $\mathfrak{a}$ in $\mathcal{O}$ with $\deg(N(\mathfrak{a})) \leq g$.

• The number r of reduced ideals in each ideal class is finite; for fields of signature $(2,1)$, we have $r = 1$, for signature $(1,2)$, $r \leq 1$, and for real hyperelliptic fields, $r \approx R$ and r varies with each ideal class.

• Stein showed Shanks' infrastructure idea for a real number field also applies to the set of reduced principal ideals in a real quadratic function field.

The set of reduced ideals can be found by the Baby Step - Giant step.

Conclusion and Future Work

Conclusion

• We have an efficient method for generating non-conjugate cubic function fields of a given squarefree discriminant with unit rank 1, using the infrastructure of the dual real function field associated with the hyperelliptic field of the same discriminant.

Conclusion and Future Work

Conclusion

• We have an efficient method for generating non-conjugate cubic function fields of a given squarefree discriminant with unit rank 1, using the infrastructure of the dual real function field associated with the hyperelliptic field of the same discriminant.

• There are several explicit constructions of hyperelliptic function fields whose Jacobian or ideal class group has large l-rank, with particular emphasis on the case $l = 3$.

So, we certainly have lots of examples of hyperelliptic function fields of high 3-ranks.

Conclusion and Future Work

Conclusion

• We have an efficient method for generating non-conjugate cubic function fields of a given squarefree discriminant with unit rank 1, using the infrastructure of the dual real function field associated with the hyperelliptic field of the same discriminant.

• There are several explicit constructions of hyperelliptic function fields whose Jacobian or ideal class group has large l-rank, with particular emphasis on the case $l = 3$.

So, we certainly have lots of examples of hyperelliptic function fields of high 3-ranks.

Future Work

• Implementation is being done.

Conclusion and Future Work

Conclusion

- We have an efficient method for generating non-conjugate cubic function fields of a given squarefree discriminant with unit rank 1, using the infrastructure of the dual real function field associated with the hyperelliptic field of the same discriminant.

- There are several explicit constructions of hyperelliptic function fields whose Jacobian or ideal class group has large l-rank, with particular emphasis on the case $l = 3$.

So, we certainly have lots of examples of hyperelliptic function fields of high 3-ranks.

Future Work

- Implementation is being done.

- Construction of cubic function fields of unit rank 2 with a given discriminant.

Conclusion and Future Work

Conclusion

• We have an efficient method for generating non-conjugate cubic function fields of a given squarefree discriminant with unit rank 1, using the infrastructure of the dual real function field associated with the hyperelliptic field of the same discriminant.

• There are several explicit constructions of hyperelliptic function fields whose Jacobian or ideal class group has large l-rank, with particular emphasis on the case $l = 3$.

So, we certainly have lots of examples of hyperelliptic function fields of high 3-ranks.

Future Work

• Implementation is being done.

• Construction of cubic function fields of unit rank 2 with a given discriminant.

• Construction of cubic function fields of unit rank 0 with a given discriminant.

References

• M. L. Bauer, M. J. Jacobson, Jr., Y. Lee and R. Scheidler, Construction of Hyperelliptic Function Fields of High Three-Rank. Submitted to *Math. Comp.*

• G. W.-W. Fung, *Computational Problems in Complex Cubic Fields*. Doctoral Dissertation, University of Manitoba, 1990.

• H. Hasse, *Arithmetische Theorie der kubischen Einheiten*. *Math. Zeitschrift* **31** (1930), 565-582.

• Y. Lee, The Scholz theorem in function fields. To appear in J. Number Theory.

• P. Llorente & E. Nart, Effective determination of the decomposition of the rational primes in a cuvic field. *Proc.. Math. Soc.* **87** (1983), 579-585.

• M. Rosen, The Hilbert class field in function fields. *Exposition. Math.* **5** (1987), 365–378.

References

• R. Scheidler, Algorithmic aspects of cubic function fields. In *Proc. Sixth Algorithmic Number Theory Symposium ANTS-VI*, *Lecture Notes Comput. Sci.* **3976**, Springer, Berlin 2004, 395-410.

• D. Shanks, *Determining all cubic fields having a given fundamental discriminant*. Unpublished manuscript.

• A. Stein and E. Teske, The parallelized Pollard kangaroo method in real quadratic function fields. *Math. Comp.* **71** (2002), 793–814

• R. Scheidler, A. Stein and H. C. Williams, Key exchange in real quadratic congruence function fields. *Designs, Codes Crypt.* **7** (1996) 153-174.

The CUFFQI Algorithm

We define a small generator of a principal ideal in $\mathcal{O}'$ to be a generator λ such that $\deg(\lambda) \leq 3g+1$ and $\deg(\overline{\lambda}) \leq 3g+1$. If $\lambda = A + By'$ is a small generator, then $\deg(A) \leq 3g+1$ and $\deg(B) \leq 3g+1-\deg(y') = 2g$, so λ can be represented by at most $(3g+2)+(2g+1) = 5g+3$ elements in $\mathbb{F}_q$.

The following algorithm is for computing for each pair $s = \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ three reduced ideals equivalent to $\mathfrak{a}$ (one such ideal if $\mathfrak{a}$ is principal) that possess small generators.

In the non-principal case, these generators and their conjugates form pairs of quadratic generators for the three distinct triples of fields in $\Phi^{-1}(s)$, while for the principal class, the small generator and its conjugate forms a pair of quadratic generators of the unique triple of fields in $\Phi^{-1}(s)$.

The CUFFQI Algorithm

Theorem 1. Let $\mathfrak{a}$ be the reduced principal ideal closest to $N = \lceil R/3 + g/2 \rfloor$ with respect to $\mathcal{O}'$. Then $\mathfrak{a}^3$ has a small generator $\lambda = \alpha^3 \epsilon^{-1}$ where α is the minimal non-negative generator of $\mathfrak{a}$. Furthermore, if $R \geq 3g + 2$, then $\mathfrak{a} \neq \mathcal{O}'$.

Theorem 2. Let $\mathfrak{r}$ be any reduced ideal whose class has order 3. Let $\mathfrak{c}$ be a reduced principal ideal equivalent to $\mathfrak{r}^3$, θ a relative generator of $\mathfrak{c}$ with respect to $\mathfrak{r}^3$, and write $\deg(\theta) - \delta(\mathfrak{c}, \mathcal{O}') = nR + r$ with $-3(g+1)/2 \leq r < R - 3(g+1)/2$. For $i = 0, 1, 2$, set $N_i = \lceil (r + iR)/3 + g/2 \rfloor$, and define $\mathfrak{a}_i$ to be the reduced ideal closest to N_i with respect to $\mathfrak{r}$.

Then $\mathfrak{a}_i^3$ has a small generator $\lambda_i = \alpha_i^3 \epsilon^{n-i} \gamma / \theta$, where α_i is the minimal non-negative relative generator of $\mathfrak{a}_i$ with respect to $\mathfrak{r}$, and γ is the minimal non-negative generator of $\mathfrak{c}$.

The CUFFQI Algorithm

Input:

- an odd prime power q with $q \equiv -1 \pmod 3$;
- a polynomial $D \in \mathbb{F}_q[t]$ of even degree whose leading coefficient is a non-square in $\mathbb{F}_q$;
- the regulator R of the hyperelliptic function field K' of discriminant $D' = D/(-3)$;
- the fundamental unit ϵ of K'/k (in the case where $R \leq 3g$ only);
- the 3-rank r' of the ideal class group of K'/k;
- a set of pairwise non-equivalent reduced ideals $\{\mathfrak{r}_1, \mathfrak{r}_2, \ldots, \mathfrak{r}_l\}$ with $l = (3^{r'} - 1)/2$ such that each $\mathfrak{r}_i$ is a representative of some ideal class of order 3 or its conjugate class.

Output: Defining polynomials for $(3^{r'+1} - 1)/2$ distinct triples of conjugate cubic fields of discriminant D.

The CUFFQI Algorithm

Algorithm:

1. Compute the ideal $\mathfrak{a}$ of Theorem 1 and for each $\mathfrak{r} = \mathfrak{r}_i$, compute the three ideals $\mathfrak{a}_{i0}, \mathfrak{a}_{i1}, \mathfrak{a}_{i2}$ of Theorem 2.

2. If $R \leq 3g + 1$, then

   a) if $\mathfrak{a} = \mathcal{O}'$, set $\lambda = \epsilon$, else compute a small generator λ of $\mathfrak{a}^3$ as described in Theorem 1;

   b) for each i, compute small generators $\lambda_{i0}, \lambda_{i1}, \lambda_{i2}$ of $\mathfrak{a}_{i0}, \mathfrak{a}_{i1}, \mathfrak{a}_{i2}$, respectively, as described in Theorem 2;

   else compute a small generator λ of $\mathfrak{a}^3$, and for each i small generators $\lambda_{i0}, \lambda_{i1}, \lambda_{i2}$ of $\mathfrak{a}_{i0}, \mathfrak{a}_{i1}, \mathfrak{a}_{i2}$, respectively, as described in Algorithm **??**.

3. Set $F(Z) = Z^3 - 3N(\lambda)^{1/3}Z + Tr(\lambda)$, and for $1 \leq i \leq l$ and $0 \leq j \leq 2$, set $F_{ij}(Z) = Z^3 - 3N(\lambda_{ij})^{1/3} + Tr(\lambda_{ij})$.

4. Output F and $\{F_{i0}, F_{i1}, F_{i2}\}$ for $1 \leq i \leq l$.