

Construction of all Cubic Function Fields of a Given Discriminant

Renate Scheidler



Centre for Information Security and Cryptography



joint work with:

Mike Jacobson & Hugh Williams, University of Calgary
Yoojin Lee, Ehwa Womans University, Seoul (South Korea)

Research supported in part by NSERC.

The Mathematical Interests of Peter Borwein — May 12, 2008

The Problem

Problem

Given $D(x) \in \mathbb{F}_q[x]$, find all cubic function fields of discriminant D .

For cubic number fields: Shanks, 1970's (unpublished), Fung (1990)

CUFFQI — Cubic Fields From Quadratic Infrastructure

For cubic function fields, we need restrictions on q and D :

- D is square-free
- $\deg(D)$ even
- q odd
- $q \equiv -1 \pmod{3}$



The Problem

Problem

Given $D(x) \in \mathbb{F}_q[x]$, find all cubic function fields of discriminant D .

For cubic number fields: Shanks, 1970's (unpublished), Fung (1990)

CUFFQI — Cubic Fields From Quadratic Infrastructure

For cubic function fields, we need restrictions on q and D :

- D is square-free
- $\deg(D)$ even
- q odd
- $q \equiv -1 \pmod{3}$



The Problem

Problem

Given $D(x) \in \mathbb{F}_q[x]$, find all cubic function fields of discriminant D .

For cubic number fields: Shanks, 1970's (unpublished), Fung (1990)

CUFFQI — Cubic Fields From Quadratic Infrastructure

For cubic function fields, we need restrictions on q and D :

- D is square-free
- $\deg(D)$ even
- q odd
- $q \equiv -1 \pmod{3}$



The Problem

Problem

Given $D(x) \in \mathbb{F}_q[x]$, find all cubic function fields of discriminant D .

For cubic number fields: Shanks, 1970's (unpublished), Fung (1990)

CUFFQI — Cubic Fields From Quadratic Infrastructure

For cubic function fields, we need restrictions on q and D :

- D is square-free
- $\deg(D)$ even
- q odd
- $q \equiv -1 \pmod{3}$



Hyperelliptic Function Fields

A square-free polynomial $D \in \mathbb{F}_q[x]$ is said to be

- **imaginary** if $\deg(D)$ is odd
- **unusual** if $\deg(D)$ is even and $\text{sgn}(D)$ is a non-square in \mathbb{F}_q
- **real** if $\deg(D)$ is even and $\text{sgn}(D)$ is a square in \mathbb{F}_q

Hyperelliptic function field:

$$K = \mathbb{F}_q(x, \sqrt{D})$$

Dual hyperelliptic function fields:

$$K = \mathbb{F}_q(x, \sqrt{D}) \text{ real}$$

$$K' = \mathbb{F}_q(x, \sqrt{D'}) \text{ unusual, where } D' = nD \text{ with } n \text{ a non-square in } \mathbb{F}_q$$

Hyperelliptic Function Fields

A square-free polynomial $D \in \mathbb{F}_q[x]$ is said to be

- **imaginary** if $\deg(D)$ is odd
- **unusual** if $\deg(D)$ is even and $\text{sgn}(D)$ is a non-square in \mathbb{F}_q
- **real** if $\deg(D)$ is even and $\text{sgn}(D)$ is a square in \mathbb{F}_q

Hyperelliptic function field:

$$K = \mathbb{F}_q(x, \sqrt{D})$$

Dual hyperelliptic function fields:

$$K = \mathbb{F}_q(x, \sqrt{D}) \text{ real}$$

$$K' = \mathbb{F}_q(x, \sqrt{D'}) \text{ unusual, where } D' = nD \text{ with } n \text{ a non-square in } \mathbb{F}_q$$

Hyperelliptic Function Fields

A square-free polynomial $D \in \mathbb{F}_q[x]$ is said to be

- **imaginary** if $\deg(D)$ is odd
- **unusual** if $\deg(D)$ is even and $\text{sgn}(D)$ is a non-square in \mathbb{F}_q
- **real** if $\deg(D)$ is even and $\text{sgn}(D)$ is a square in \mathbb{F}_q

Hyperelliptic function field:

$$K = \mathbb{F}_q(x, \sqrt{D})$$

Dual hyperelliptic function fields:

$$K = \mathbb{F}_q(x, \sqrt{D}) \text{ real}$$

$$K' = \mathbb{F}_q(x, \sqrt{D'}) \text{ unusual, where } D' = nD \text{ with } n \text{ a non-square in } \mathbb{F}_q$$

Hyperelliptic Function Fields

A square-free polynomial $D \in \mathbb{F}_q[x]$ is said to be

- **imaginary** if $\deg(D)$ is odd
- **unusual** if $\deg(D)$ is even and $\text{sgn}(D)$ is a non-square in \mathbb{F}_q
- **real** if $\deg(D)$ is even and $\text{sgn}(D)$ is a square in \mathbb{F}_q

Hyperelliptic function field:

$$K = \mathbb{F}_q(x, \sqrt{D})$$

Dual hyperelliptic function fields:

$$K = \mathbb{F}_q(x, \sqrt{D}) \text{ real}$$

$$K' = \mathbb{F}_q(x, \sqrt{D'}) \text{ unusual, where } D' = nD \text{ with } n \text{ a non-square in } \mathbb{F}_q$$

Cubic Function Fields

$F(Z) = Z^3 - 3QZ + 2A$ irreducible over $\mathbb{F}_q(x)$ ($A, Q \in \mathbb{F}_q[x]$)

Standard Form: no $G \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ satisfies $G^2 \mid Q$ and $G^3 \mid A$

Cubic function field: $L = \mathbb{F}_q(x, z)$ with $F(z) = 0$

$\Delta = \text{disc}(F) = 108(Q^3 - A^2) = (6B)^2 D$ with $D = \text{disc}(K)$

Set $\lambda = A + B\sqrt{D'} \in K'$ where $K' = \mathbb{F}_q(x, \sqrt{D'})$ with $D' = -3D$
 $\text{Tr}(\lambda) = 2A, N(\lambda) = Q^3$

$F(Z)$ in fact defines a triple of **conjugate** cubic fields $\{L, L', L''\}$, given by the three zeros $z, z', z'' = u^i \lambda^{1/3} + u^{-i} \bar{\lambda}^{1/3}$ of $F(Z)$ (u a primitive cube root of unity, $i = 0, 1, 2$).

$\{\lambda, \bar{\lambda}\}$ is a pair of **quadratic generators** of $\{L, L', L''\}$

Cubic Function Fields

$F(Z) = Z^3 - 3QZ + 2A$ irreducible over $\mathbb{F}_q(x)$ ($A, Q \in \mathbb{F}_q[x]$)

Standard Form: no $G \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ satisfies $G^2 \mid Q$ and $G^3 \mid A$

Cubic function field: $L = \mathbb{F}_q(x, z)$ with $F(z) = 0$

$\Delta = \text{disc}(F) = 108(Q^3 - A^2) = (6B)^2 D$ with $D = \text{disc}(K)$

Set $\lambda = A + B\sqrt{D'} \in K'$ where $K' = \mathbb{F}_q(x, \sqrt{D'})$ with $D' = -3D$
 $\text{Tr}(\lambda) = 2A, N(\lambda) = Q^3$

$F(Z)$ in fact defines a triple of **conjugate** cubic fields $\{L, L', L''\}$, given by the three zeros $z, z', z'' = u^i \lambda^{1/3} + u^{-i} \bar{\lambda}^{1/3}$ of $F(Z)$ (u a primitive cube root of unity, $i = 0, 1, 2$).

$\{\lambda, \bar{\lambda}\}$ is a pair of **quadratic generators** of $\{L, L', L''\}$

Cubic Function Fields

$F(Z) = Z^3 - 3QZ + 2A$ irreducible over $\mathbb{F}_q(x)$ ($A, Q \in \mathbb{F}_q[x]$)

Standard Form: no $G \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ satisfies $G^2 \mid Q$ and $G^3 \mid A$

Cubic function field: $L = \mathbb{F}_q(x, z)$ with $F(z) = 0$

$\Delta = \text{disc}(F) = 108(Q^3 - A^2) = (6B)^2 D$ with $D = \text{disc}(K)$

Set $\lambda = A + B\sqrt{D'} \in K'$ where $K' = \mathbb{F}_q(x, \sqrt{D'})$ with $D' = -3D$
 $\text{Tr}(\lambda) = 2A, N(\lambda) = Q^3$

$F(Z)$ in fact defines a triple of **conjugate** cubic fields $\{L, L', L''\}$, given by the three zeros $z, z', z'' = u^i \lambda^{1/3} + u^{-i} \bar{\lambda}^{1/3}$ of $F(Z)$ (u a primitive cube root of unity, $i = 0, 1, 2$).

$\{\lambda, \bar{\lambda}\}$ is a pair of **quadratic generators** of $\{L, L', L''\}$

Cubic Function Fields

$F(Z) = Z^3 - 3QZ + 2A$ irreducible over $\mathbb{F}_q(x)$ ($A, Q \in \mathbb{F}_q[x]$)

Standard Form: no $G \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ satisfies $G^2 \mid Q$ and $G^3 \mid A$

Cubic function field: $L = \mathbb{F}_q(x, z)$ with $F(z) = 0$

$\Delta = \text{disc}(F) = 108(Q^3 - A^2) = (6B)^2 D$ with $D = \text{disc}(K)$

Set $\lambda = A + B\sqrt{D'} \in K'$ where $K' = \mathbb{F}_q(x, \sqrt{D'})$ with $D' = -3D$
 $\text{Tr}(\lambda) = 2A, N(\lambda) = Q^3$

$F(Z)$ in fact defines a triple of **conjugate** cubic fields $\{L, L', L''\}$, given by the three zeros $z, z', z'' = u^i \lambda^{1/3} + u^{-i} \bar{\lambda}^{1/3}$ of $F(Z)$ (u a primitive cube root of unity, $i = 0, 1, 2$).

$\{\lambda, \bar{\lambda}\}$ is a pair of **quadratic generators** of $\{L, L', L''\}$

Cubic Function Fields

$F(Z) = Z^3 - 3QZ + 2A$ irreducible over $\mathbb{F}_q(x)$ ($A, Q \in \mathbb{F}_q[x]$)

Standard Form: no $G \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ satisfies $G^2 \mid Q$ and $G^3 \mid A$

Cubic function field: $L = \mathbb{F}_q(x, z)$ with $F(z) = 0$

$\Delta = \text{disc}(F) = 108(Q^3 - A^2) = (6B)^2 D$ with $D = \text{disc}(K)$

Set $\lambda = A + B\sqrt{D'} \in K'$ where $K' = \mathbb{F}_q(x, \sqrt{D'})$ with $D' = -3D$
 $\text{Tr}(\lambda) = 2A, N(\lambda) = Q^3$

$F(Z)$ in fact defines a triple of **conjugate** cubic fields $\{L, L', L''\}$, given by the three zeros $z, z', z'' = u^i \lambda^{1/3} + u^{-i} \bar{\lambda}^{1/3}$ of $F(Z)$ (u a primitive cube root of unity, $i = 0, 1, 2$).

$\{\lambda, \bar{\lambda}\}$ is a pair of **quadratic generators** of $\{L, L', L''\}$

Cubic Function Fields

$F(Z) = Z^3 - 3QZ + 2A$ irreducible over $\mathbb{F}_q(x)$ ($A, Q \in \mathbb{F}_q[x]$)

Standard Form: no $G \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ satisfies $G^2 \mid Q$ and $G^3 \mid A$

Cubic function field: $L = \mathbb{F}_q(x, z)$ with $F(z) = 0$

$\Delta = \text{disc}(F) = 108(Q^3 - A^2) = (6B)^2 D$ with $D = \text{disc}(K)$

Set $\lambda = A + B\sqrt{D'} \in K'$ where $K' = \mathbb{F}_q(x, \sqrt{D'})$ with $D' = -3D$
 $\text{Tr}(\lambda) = 2A, N(\lambda) = Q^3$

$F(Z)$ in fact defines a triple of **conjugate** cubic fields $\{L, L', L''\}$, given by the three zeros $z, z', z'' = u^i \lambda^{1/3} + u^{-i} \bar{\lambda}^{1/3}$ of $F(Z)$ (u a primitive cube root of unity, $i = 0, 1, 2$).

$\{\lambda, \bar{\lambda}\}$ is a pair of **quadratic generators** of $\{L, L', L''\}$

Cubic Function Fields

$F(Z) = Z^3 - 3QZ + 2A$ irreducible over $\mathbb{F}_q(x)$ ($A, Q \in \mathbb{F}_q[x]$)

Standard Form: no $G \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ satisfies $G^2 \mid Q$ and $G^3 \mid A$

Cubic function field: $L = \mathbb{F}_q(x, z)$ with $F(z) = 0$

$\Delta = \text{disc}(F) = 108(Q^3 - A^2) = (6B)^2 D$ with $D = \text{disc}(K)$

Set $\lambda = A + B\sqrt{D'} \in K'$ where $K' = \mathbb{F}_q(x, \sqrt{D'})$ with $D' = -3D$
 $\text{Tr}(\lambda) = 2A, N(\lambda) = Q^3$

$F(Z)$ in fact defines a triple of **conjugate** cubic fields $\{L, L', L''\}$, given by the three zeros $z, z', z'' = u^i \lambda^{1/3} + u^{-i} \bar{\lambda}^{1/3}$ of $F(Z)$ (u a primitive cube root of unity, $i = 0, 1, 2$).

$\{\lambda, \bar{\lambda}\}$ is a pair of **quadratic generators** of $\{L, L', L''\}$

Properties of Quadratic Generators

Theorem

The principal ideal (λ) of K' is the cube of a primitive ideal of K' .

Theorem

Let $\lambda \in K'$. Then $\{\lambda, \bar{\lambda}\}$ is a pair of quadratic generators if and only if $\lambda \neq \bar{\lambda}$, λ is not a cube in K' , and λ is the cube of a primitive ideal in K' .

Theorem

$\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields if and only if λ_1/λ_2 or $\lambda_1/\bar{\lambda}_2$ is a cube in K' .

Corollary

If $\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields, with $(\lambda_1) = \mathfrak{a}_1^3$ and $(\lambda_2) = \mathfrak{a}_2^3$, then $\{[\mathfrak{a}_1], [\bar{\mathfrak{a}}_1]\} = \{[\mathfrak{a}_2], [\bar{\mathfrak{a}}_2]\}$.

Properties of Quadratic Generators

Theorem

The principal ideal (λ) of K' is the cube of a primitive ideal of K' .

Theorem

Let $\lambda \in K'$. Then $\{\lambda, \bar{\lambda}\}$ is a pair of quadratic generators if and only if $\lambda \neq \bar{\lambda}$, λ is not a cube in K' , and λ is the cube of a primitive ideal in K' .

Theorem

$\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields if and only if λ_1/λ_2 or $\lambda_1/\bar{\lambda}_2$ is a cube in K' .

Corollary

If $\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields, with $(\lambda_1) = \mathfrak{a}_1^3$ and $(\lambda_2) = \mathfrak{a}_2^3$, then $\{[\mathfrak{a}_1], [\bar{\mathfrak{a}}_1]\} = \{[\mathfrak{a}_2], [\bar{\mathfrak{a}}_2]\}$.

Properties of Quadratic Generators

Theorem

The principal ideal (λ) of K' is the cube of a primitive ideal of K' .

Theorem

Let $\lambda \in K'$. Then $\{\lambda, \bar{\lambda}\}$ is a pair of quadratic generators if and only if $\lambda \neq \bar{\lambda}$, λ is not a cube in K' , and λ is the cube of a primitive ideal in K' .

Theorem

$\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields if and only if λ_1/λ_2 or $\lambda_1/\bar{\lambda}_2$ is a cube in K' .

Corollary

If $\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields, with $(\lambda_1) = \mathfrak{a}_1^3$ and $(\lambda_2) = \mathfrak{a}_2^3$, then $\{[\mathfrak{a}_1], [\bar{\mathfrak{a}}_1]\} = \{[\mathfrak{a}_2], [\bar{\mathfrak{a}}_2]\}$.

Properties of Quadratic Generators

Theorem

The principal ideal (λ) of K' is the cube of a primitive ideal of K' .

Theorem

Let $\lambda \in K'$. Then $\{\lambda, \bar{\lambda}\}$ is a pair of quadratic generators if and only if $\lambda \neq \bar{\lambda}$, λ is not a cube in K' , and λ is the cube of a primitive ideal in K' .

Theorem

$\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields if and only if λ_1/λ_2 or $\lambda_1/\bar{\lambda}_2$ is a cube in K' .

Corollary

If $\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields, with $(\lambda_1) = \mathfrak{a}_1^3$ and $(\lambda_2) = \mathfrak{a}_2^3$, then $\{[\mathfrak{a}_1], [\bar{\mathfrak{a}}_1]\} = \{[\mathfrak{a}_2], [\bar{\mathfrak{a}}_2]\}$.

Properties of Quadratic Generators

Theorem

The principal ideal (λ) of K' is the cube of a primitive ideal of K' .

Theorem

Let $\lambda \in K'$. Then $\{\lambda, \bar{\lambda}\}$ is a pair of quadratic generators if and only if $\lambda \neq \bar{\lambda}$, λ is not a cube in K' , and λ is the cube of a primitive ideal in K' .

Theorem

$\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields if and only if λ_1/λ_2 or $\lambda_1/\bar{\lambda}_2$ is a cube in K' .

Corollary

If $\{\lambda_1, \bar{\lambda}_1\}$ and $\{\lambda_2, \bar{\lambda}_2\}$ define the same triple of conjugate cubic function fields, with $(\lambda_1) = \mathfrak{a}_1^3$ and $(\lambda_2) = \mathfrak{a}_2^3$, then $\{[\mathfrak{a}_1], [\bar{\mathfrak{a}}_1]\} = \{[\mathfrak{a}_2], [\bar{\mathfrak{a}}_2]\}$.

Approach

$$\mathcal{L} = \{ \{L, L', L''\} \mid L \text{ a cubic function field of discriminant } D \}$$

$$\mathcal{I} = \{ \{[\mathfrak{a}], [\bar{\mathfrak{a}}]\} \mid \mathfrak{a} \text{ is an ideal of } K' \text{ with } \mathfrak{a}^3 \text{ principal} \}$$

Define a map $\Phi : \mathcal{L} \longrightarrow \mathcal{I}$ via

$$\{L, L', L''\} \mapsto \{[\mathfrak{a}], [\bar{\mathfrak{a}}]\} \text{ such that } \mathfrak{a}^3 = (\lambda) \text{ where } \{\lambda, \bar{\lambda}\} \text{ is a pair of quadratic generator of } \{L, L', L''\}$$

Theorem

If D is real (i.e. D' unusual), then

- Φ is a bijection onto $\mathcal{I} \setminus \{\text{principal class pair}\}$

If D is unusual (i.e. D' real), then

- Φ is one-to-one onto the principal class pair
- Φ is three-to-one onto $\mathcal{I} \setminus \{\text{principal class pair}\}$

Approach

$$\mathcal{L} = \{ \{L, L', L''\} \mid L \text{ a cubic function field of discriminant } D \}$$

$$\mathcal{I} = \{ \{[\mathfrak{a}], [\bar{\mathfrak{a}}]\} \mid \mathfrak{a} \text{ is an ideal of } K' \text{ with } \mathfrak{a}^3 \text{ principal} \}$$

Define a map $\Phi : \mathcal{L} \longrightarrow \mathcal{I}$ via

$$\{L, L', L''\} \mapsto \{[\mathfrak{a}], [\bar{\mathfrak{a}}]\} \text{ such that } \mathfrak{a}^3 = (\lambda) \text{ where } \{\lambda, \bar{\lambda}\} \text{ is a pair of quadratic generator of } \{L, L', L''\}$$

Theorem

If D is real (i.e. D' unusual), then

- Φ is a bijection onto $\mathcal{I} \setminus \{\text{principal class pair}\}$

If D is unusual (i.e. D' real), then

- Φ is one-to-one onto the principal class pair
- Φ is three-to-one onto $\mathcal{I} \setminus \{\text{principal class pair}\}$

Approach

$$\mathcal{L} = \{ \{L, L', L''\} \mid L \text{ a cubic function field of discriminant } D \}$$

$$\mathcal{I} = \{ \{[\mathfrak{a}], [\bar{\mathfrak{a}}]\} \mid \mathfrak{a} \text{ is an ideal of } K' \text{ with } \mathfrak{a}^3 \text{ principal} \}$$

Define a map $\Phi : \mathcal{L} \longrightarrow \mathcal{I}$ via

$$\{L, L', L''\} \mapsto \{[\mathfrak{a}], [\bar{\mathfrak{a}}]\} \text{ such that } \mathfrak{a}^3 = (\lambda) \text{ where } \{\lambda, \bar{\lambda}\} \text{ is a pair of quadratic generator of } \{L, L', L''\}$$

Theorem

If D is real (i.e. D' unusual), then

- Φ is a bijection onto $\mathcal{I} \setminus \{\text{principal class pair}\}$

If D is unusual (i.e. D' real), then

- Φ is one-to-one onto the principal class pair
- Φ is three-to-one onto $\mathcal{I} \setminus \{\text{principal class pair}\}$

Approach

$$\mathcal{L} = \{ \{L, L', L''\} \mid L \text{ a cubic function field of discriminant } D \}$$

$$\mathcal{I} = \{ \{[\mathfrak{a}], [\bar{\mathfrak{a}}]\} \mid \mathfrak{a} \text{ is an ideal of } K' \text{ with } \mathfrak{a}^3 \text{ principal} \}$$

Define a map $\Phi : \mathcal{L} \longrightarrow \mathcal{I}$ via

$$\{L, L', L''\} \mapsto \{[\mathfrak{a}], [\bar{\mathfrak{a}}]\} \text{ such that } \mathfrak{a}^3 = (\lambda) \text{ where } \{\lambda, \bar{\lambda}\} \text{ is a pair of quadratic generator of } \{L, L', L''\}$$

Theorem

If D is real (i.e. D' unusual), then

- Φ is a bijection onto $\mathcal{I} \setminus \{\text{principal class pair}\}$

If D is unusual (i.e. D' real), then

- Φ is one-to-one onto the principal class pair
- Φ is three-to-one onto $\mathcal{I} \setminus \{\text{principal class pair}\}$

More on Hyperelliptic Function Fields

$$K = \mathbb{F}_q(x, \sqrt{D}) \quad (q \text{ odd, } D \text{ squarefree})$$

The **genus** of K is $g = \left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor$

A primitive ideal \mathfrak{a} of K is

- **reduced** if $\deg(N(\mathfrak{a})) \leq g$
- **almost reduced** if $\deg(N(\mathfrak{a})) = g + 1$



Theorem

Every ideal class of K contains

- *a unique reduced ideal if D is imaginary,*
- *either a unique reduced ideal or $q + 1$ almost reduced ideals if D is unusual,*
- *finitely, but usually exponentially many reduced ideals if D is real.*

More on Hyperelliptic Function Fields

$$K = \mathbb{F}_q(x, \sqrt{D}) \quad (q \text{ odd, } D \text{ squarefree})$$

The **genus** of K is $g = \left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor$

A primitive ideal \mathfrak{a} of K is

- **reduced** if $\deg(N(\mathfrak{a})) \leq g$
- **almost reduced** if $\deg(N(\mathfrak{a})) = g + 1$



Theorem

Every ideal class of K contains

- *a unique reduced ideal if D is imaginary,*
- *either a unique reduced ideal or $q + 1$ almost reduced ideals if D is unusual,*
- *finitely, but usually exponentially many reduced ideals if D is real.*

More on Hyperelliptic Function Fields

$$K = \mathbb{F}_q(x, \sqrt{D}) \quad (q \text{ odd, } D \text{ squarefree})$$

The **genus** of K is $g = \left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor$

A primitive ideal \mathfrak{a} of K is

- **reduced** if $\deg(N(\mathfrak{a})) \leq g$
- **almost reduced** if $\deg(N(\mathfrak{a})) = g + 1$



Theorem

Every ideal class of K contains

- *a unique reduced ideal if D is imaginary,*
- *either a unique reduced ideal or $q + 1$ almost reduced ideals if D is unusual,*
- *finitely, but usually exponentially many reduced ideals if D is real.*

More on Hyperelliptic Function Fields

$$K = \mathbb{F}_q(x, \sqrt{D}) \quad (q \text{ odd, } D \text{ squarefree})$$

The **genus** of K is $g = \left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor$

A primitive ideal \mathfrak{a} of K is

- **reduced** if $\deg(N(\mathfrak{a})) \leq g$
- **almost reduced** if $\deg(N(\mathfrak{a})) = g + 1$



Theorem

Every ideal class of K contains

- *a unique reduced ideal if D is imaginary,*
- *either a unique reduced ideal or $q + 1$ almost reduced ideals if D is unusual,*
- *finitely, but usually exponentially many reduced ideals if D is real.*

More on Hyperelliptic Function Fields

$$K = \mathbb{F}_q(x, \sqrt{D}) \quad (q \text{ odd, } D \text{ squarefree})$$

The **genus** of K is $g = \left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor$

A primitive ideal \mathfrak{a} of K is

- **reduced** if $\deg(N(\mathfrak{a})) \leq g$
- **almost reduced** if $\deg(N(\mathfrak{a})) = g + 1$



Theorem

Every ideal class of K contains

- *a unique reduced ideal if D is imaginary,*
- *either a unique reduced ideal or $q + 1$ almost reduced ideals if D is unusual,*
- *finitely, but usually exponentially many reduced ideals if D is real.*

Roadmap – D real

A reduced or almost reduced ideal \mathfrak{a} of K' , $[\mathfrak{a}]$ has order 3



$$\lambda = A + B\sqrt{D'} \text{ with } \mathfrak{a}^3 = (\lambda), \quad N(\lambda) = Q^3 = (\text{sgn}(Q) N(\mathfrak{a}))^3$$



$$L = \mathbb{F}_q(x, z) \text{ with } z^3 - 3Qz + 2A = 0$$



A reduced or almost reduced ideal \mathfrak{a} of K' , $[\mathfrak{a}]$ has order 3

$$\lambda = A + B\sqrt{D'} \text{ with } \mathfrak{a}^3 = (\lambda), \quad N(\lambda) = Q^3 = (\text{sgn}(Q) N(\mathfrak{a}))^3$$

$$L = \mathbb{F}_q(x, z) \text{ with } z^3 - 3Qz + 2A = 0$$



A reduced or almost reduced ideal \mathfrak{a} of K' , $[\mathfrak{a}]$ has order 3

$$\lambda = A + B\sqrt{D'} \text{ with } \mathfrak{a}^3 = (\lambda), \quad N(\lambda) = Q^3 = (\text{sgn}(Q) N(\mathfrak{a}))^3$$

$$L = \mathbb{F}_q(x, z) \text{ with } z^3 - 3Qz + 2A = 0$$



A reduced or almost reduced ideal \mathfrak{a} of K' , $[\mathfrak{a}]$ has order 3

$$\lambda = A + B\sqrt{D'} \text{ with } \mathfrak{a}^3 = (\lambda), \quad N(\lambda) = Q^3 = (\text{sgn}(Q) N(\mathfrak{a}))^3$$

$$L = \mathbb{F}_q(x, z) \text{ with } z^3 - 3Qz + 2A = 0$$



Computing \mathcal{L} for D Real

Precomputation: The 3-torsion part of the ideal class group of $K' = \mathbb{F}_q(x, \sqrt{-3D})$

Input: Reduced or almost reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

For $i = 1$ to l do

- 1 Compute \mathfrak{a}_i with $(S)\mathfrak{a}_i = \tau_i^3$, $S \in \mathbb{F}_q[x]$
- 2 Compute a generator λ_i of \mathfrak{a}_i
- 3 Set $2A_i = \text{Tr}(\lambda_i)$ and $Q_i = aN(\tau_i)$ with $a^3 = \text{sgn}(N(\lambda_i))$
- 4 Output $F_i(Z) = Z^3 - 3Q_iZ + 2A_i$

Computing \mathcal{L} for D Real

Precomputation: The 3-torsion part of the ideal class group of $K' = \mathbb{F}_q(x, \sqrt{-3D})$

Input: Reduced or almost reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

For $i = 1$ to l do

- ① Compute α_i with $(S)\alpha_i = \tau_i^3$, $S \in \mathbb{F}_q[x]$
- ② Compute a generator λ_i of α_i
- ③ Set $2A_i = \text{Tr}(\lambda_i)$ and $Q_i = aN(\tau_i)$ with $a^3 = \text{sgn}(N(\lambda_i))$
- ④ Output $F_i(Z) = Z^3 - 3Q_iZ + 2A_i$

Computing \mathcal{L} for D Real

Precomputation: The 3-torsion part of the ideal class group of $K' = \mathbb{F}_q(x, \sqrt{-3D})$

Input: Reduced or almost reduced representatives $\mathfrak{r}_1, \mathfrak{r}_2, \dots, \mathfrak{r}_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

For $i = 1$ to l do

- 1 Compute \mathfrak{a}_i with $(S)\mathfrak{a}_i = \mathfrak{r}_i^3$, $S \in \mathbb{F}_q[x]$
- 2 Compute a generator λ_i of \mathfrak{a}_i
- 3 Set $2A_i = \text{Tr}(\lambda_i)$ and $Q_i = aN(\mathfrak{r}_i)$ with $a^3 = \text{sgn}(N(\lambda_i))$
- 4 Output $F_i(Z) = Z^3 - 3Q_iZ + 2A_i$

Computing \mathcal{L} for D Real

Precomputation: The 3-torsion part of the ideal class group of $K' = \mathbb{F}_q(x, \sqrt{-3D})$

Input: Reduced or almost reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

For $i = 1$ to l do

- 1 Compute α_i with $(S)\alpha_i = \tau_i^3$, $S \in \mathbb{F}_q[x]$
- 2 Compute a generator λ_i of α_i
- 3 Set $2A_i = \text{Tr}(\lambda_i)$ and $Q_i = aN(\tau_i)$ with $a^3 = \text{sgn}(N(\lambda_i))$
- 4 Output $F_i(Z) = Z^3 - 3Q_iZ + 2A_i$

Computing \mathcal{L} for D Real

Precomputation: The 3-torsion part of the ideal class group of $K' = \mathbb{F}_q(x, \sqrt{-3D})$

Input: Reduced or almost reduced representatives $\mathfrak{r}_1, \mathfrak{r}_2, \dots, \mathfrak{r}_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

For $i = 1$ to l do

- 1 Compute \mathfrak{a}_i with $(S)\mathfrak{a}_i = \mathfrak{r}_i^3$, $S \in \mathbb{F}_q[x]$
- 2 Compute a generator λ_i of \mathfrak{a}_i
- 3 Set $2A_i = \text{Tr}(\lambda_i)$ and $Q_i = aN(\mathfrak{r}_i)$ with $a^3 = \text{sgn}(N(\lambda_i))$
- 4 Output $F_i(Z) = Z^3 - 3Q_iZ + 2A_i$

Roadmap – D unusual

Let

- \mathcal{O}' be the maximal order of K'
- ϵ the fundamental unit of K' , $N(\epsilon) = e^3 \in \mathbb{F}_q^*$
- $R = \deg(\epsilon)$ the regulator of K'

For the principal class:

\mathcal{O}' reduced

\updownarrow

ϵ

\updownarrow

$$F(Z) = Z^3 - 3e + \text{Tr}(\epsilon)$$

For classes of order 3:

α reduced, $\alpha^3 = (\lambda)$

$\swarrow \quad \downarrow \quad \searrow$

$$\lambda_0 = \lambda$$

$$\lambda_1 = \epsilon\lambda$$

$$\lambda_2 = \epsilon^2\lambda$$

\updownarrow

\updownarrow

\updownarrow

$$F_0(Z)$$

$$F_1(Z)$$

$$F_2(Z)$$

Problem: the constant coefficient of the minimal polynomial is BIG!

Roadmap – D unusual

Let

- \mathcal{O}' be the maximal order of K'
- ϵ the fundamental unit of K' , $N(\epsilon) = e^3 \in \mathbb{F}_q^*$
- $R = \deg(\epsilon)$ the regulator of K'

For the principal class:

\mathcal{O}' reduced

\updownarrow

ϵ

\updownarrow

$$F(Z) = Z^3 - 3e + \text{Tr}(\epsilon)$$

For classes of order 3:

α reduced, $\alpha^3 = (\lambda)$

$\swarrow \quad \downarrow \quad \searrow$

$$\lambda_0 = \lambda$$

$$\lambda_1 = \epsilon\lambda$$

$$\lambda_2 = \epsilon^2\lambda$$

\updownarrow

$$F_0(Z)$$

\updownarrow

$$F_1(Z)$$

\updownarrow

$$F_2(Z)$$

Problem: the constant coefficient of the minimal polynomial is BIG!

Roadmap – D unusual

Let

- \mathcal{O}' be the maximal order of K'
- ϵ the fundamental unit of K' , $N(\epsilon) = e^3 \in \mathbb{F}_q^*$
- $R = \deg(\epsilon)$ the regulator of K'

For the principal class:

\mathcal{O}' reduced

\updownarrow

ϵ

\updownarrow

$$F(Z) = Z^3 - 3e + \text{Tr}(\epsilon)$$

For classes of order 3:

α reduced, $\alpha^3 = (\lambda)$

$\swarrow \quad \downarrow \quad \searrow$

$$\lambda_0 = \lambda$$

$$\lambda_1 = \epsilon\lambda$$

$$\lambda_2 = \epsilon^2\lambda$$

\updownarrow

\updownarrow

\updownarrow

$$F_0(Z)$$

$$F_1(Z)$$

$$F_2(Z)$$

Problem: the constant coefficient of the minimal polynomial is BIG!

Roadmap – D unusual

Let

- \mathcal{O}' be the maximal order of K'
- ϵ the fundamental unit of K' , $N(\epsilon) = e^3 \in \mathbb{F}_q^*$
- $R = \deg(\epsilon)$ the regulator of K'

For the principal class:

\mathcal{O}' reduced

\updownarrow

ϵ

\updownarrow

$$F(Z) = Z^3 - 3e + \text{Tr}(\epsilon)$$

For classes of order 3:

\mathfrak{a} reduced, $\mathfrak{a}^3 = (\lambda)$

$\swarrow \quad \downarrow \quad \searrow$

$$\lambda_0 = \lambda$$

$$\lambda_1 = \epsilon\lambda$$

$$\lambda_2 = \epsilon^2\lambda$$

\updownarrow

$$F_0(Z)$$

\updownarrow

$$F_1(Z)$$

\updownarrow

$$F_2(Z)$$

Problem: the constant coefficient of the minimal polynomial is BIG!

Roadmap – D unusual

Let

- \mathcal{O}' be the maximal order of K'
- ϵ the fundamental unit of K' , $N(\epsilon) = e^3 \in \mathbb{F}_q^*$
- $R = \deg(\epsilon)$ the regulator of K'

For the principal class:

\mathcal{O}' reduced

\updownarrow

ϵ

\updownarrow

$$F(Z) = Z^3 - 3e + \text{Tr}(\epsilon)$$

For classes of order 3:

\mathfrak{a} reduced, $\mathfrak{a}^3 = (\lambda)$

$\swarrow \quad \downarrow \quad \searrow$

$$\lambda_0 = \lambda$$

$$\lambda_1 = \epsilon\lambda$$

$$\lambda_2 = \epsilon^2\lambda$$

\updownarrow

\updownarrow

\updownarrow

$$F_0(Z)$$

$$F_1(Z)$$

$$F_2(Z)$$

Problem: the constant coefficient of the minimal polynomial is BIG!

Infrastructures

Let D' be real. Every reduced ideal \mathfrak{a} of K' has the form

$$\mathfrak{a} = \mathbb{F}_q[x]Q \oplus \mathbb{F}_q[x](P + \sqrt{D'}) = (Q, P), \quad N(\mathfrak{a}) = Q \mid D' - P^2$$

The **infrastructure** of \mathfrak{a} is the set of all reduced ideals in the class of \mathfrak{a} :

$$\mathcal{R}_{\mathfrak{a}} = \{ \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots, \mathfrak{a}_m \}$$

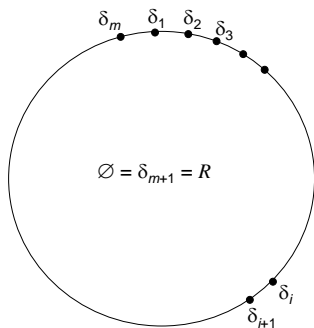
$$\mathfrak{a}_1 = \mathfrak{a}, \quad \mathfrak{a}_i = (Q_i, P_i) \text{ with}$$

$$q_{i-1} = \left\lfloor \frac{P_{i-1} + \lfloor \sqrt{D'} \rfloor}{Q_{i-1}} \right\rfloor$$

$$P_i = Q_{i-1} - q_{i-1}P_{i-1}$$

$$Q_i = \frac{D' - P_i^2}{Q_{i-1}}$$

$$\text{Distance: } \delta_i = \delta(\mathfrak{a}_i, \mathfrak{a}_0) = \sum_{j=0}^{i-1} \deg(q_j)$$



Infrastructures

Let D' be real. Every reduced ideal \mathfrak{a} of K' has the form

$$\mathfrak{a} = \mathbb{F}_q[x] Q \oplus \mathbb{F}_q[x] (P + \sqrt{D'}) = (Q, P), \quad N(\mathfrak{a}) = Q \mid D' - P^2$$

The **infrastructure** of \mathfrak{a} is the set of all reduced ideals in the class of \mathfrak{a} :

$$\mathcal{R}_{\mathfrak{a}} = \{ \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots, \mathfrak{a}_m \}$$

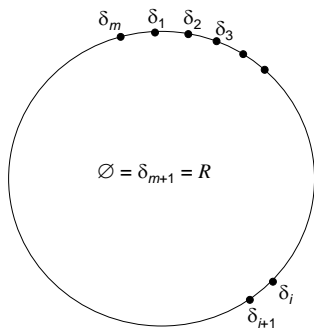
$$\mathfrak{a}_1 = \mathfrak{a}, \quad \mathfrak{a}_j = (Q_j, P_j) \text{ with}$$

$$q_{i-1} = \left\lfloor \frac{P_{i-1} + \lfloor \sqrt{D'} \rfloor}{Q_{i-1}} \right\rfloor$$

$$P_i = Q_{i-1} - q_{i-1} P_{i-1}$$

$$Q_i = \frac{D' - P_i^2}{Q_{i-1}}$$

$$\text{Distance: } \delta_i = \delta(\mathfrak{a}_i, \mathfrak{a}_0) = \sum_{j=0}^{i-1} \deg(q_j)$$



Infrastructures

Let D' be real. Every reduced ideal \mathfrak{a} of K' has the form

$$\mathfrak{a} = \mathbb{F}_q[x] Q \oplus \mathbb{F}_q[x] (P + \sqrt{D'}) = (Q, P), \quad N(\mathfrak{a}) = Q \mid D' - P^2$$

The **infrastructure** of \mathfrak{a} is the set of all reduced ideals in the class of \mathfrak{a} :

$$\mathcal{R}_{\mathfrak{a}} = \{ \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots, \mathfrak{a}_m \}$$

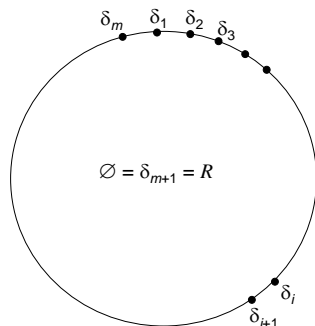
$$\mathfrak{a}_1 = \mathfrak{a}, \quad \mathfrak{a}_j = (Q_j, P_j) \text{ with}$$

$$q_{i-1} = \left\lfloor \frac{P_{i-1} + \lfloor \sqrt{D'} \rfloor}{Q_{i-1}} \right\rfloor$$

$$P_i = Q_{i-1} - q_{i-1} P_{i-1}$$

$$Q_i = \frac{D' - P_i^2}{Q_{i-1}}$$

$$\text{Distance: } \delta_i = \delta(\mathfrak{a}_i, \mathfrak{a}_0) = \sum_{j=0}^{i-1} \deg(q_j)$$



Infrastructures

Let D' be real. Every reduced ideal \mathfrak{a} of K' has the form

$$\mathfrak{a} = \mathbb{F}_q[x] Q \oplus \mathbb{F}_q[x] (P + \sqrt{D'}) = (Q, P), \quad N(\mathfrak{a}) = Q \mid D' - P^2$$

The **infrastructure** of \mathfrak{a} is the set of all reduced ideals in the class of \mathfrak{a} :

$$\mathcal{R}_{\mathfrak{a}} = \{ \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots, \mathfrak{a}_m \}$$

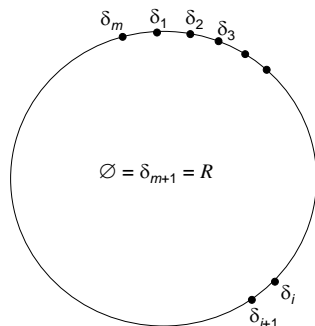
$$\mathfrak{a}_1 = \mathfrak{a}, \quad \mathfrak{a}_i = (Q_i, P_i) \text{ with}$$

$$q_{i-1} = \left\lfloor \frac{P_{i-1} + \lfloor \sqrt{D'} \rfloor}{Q_{i-1}} \right\rfloor$$

$$P_i = Q_{i-1} - q_{i-1} P_{i-1}$$

$$Q_i = \frac{D' - P_i^2}{Q_{i-1}}$$

$$\text{Distance: } \delta_i = \delta(\mathfrak{a}_i, \mathfrak{a}_0) = \sum_{j=0}^{i-1} \deg(q_j)$$



Infrastructures

Let D' be real. Every reduced ideal \mathfrak{a} of K' has the form

$$\mathfrak{a} = \mathbb{F}_q[x] Q \oplus \mathbb{F}_q[x] (P + \sqrt{D'}) = (Q, P), \quad N(\mathfrak{a}) = Q \mid D' - P^2$$

The **infrastructure** of \mathfrak{a} is the set of all reduced ideals in the class of \mathfrak{a} :

$$\mathcal{R}_{\mathfrak{a}} = \{ \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots, \mathfrak{a}_m \}$$

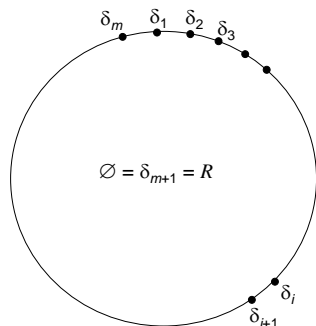
$$\mathfrak{a}_1 = \mathfrak{a}, \quad \mathfrak{a}_i = (Q_i, P_i) \text{ with}$$

$$q_{i-1} = \left\lfloor \frac{P_{i-1} + \lfloor \sqrt{D'} \rfloor}{Q_{i-1}} \right\rfloor$$

$$P_i = Q_{i-1} - q_{i-1} P_{i-1}$$

$$Q_i = \frac{D' - P_i^2}{Q_{i-1}}$$

$$\text{Distance: } \delta_i = \delta(\mathfrak{a}_i, \mathfrak{a}_0) = \sum_{j=0}^{i-1} \deg(q_j)$$



Small Quadratic Generators

An element $\lambda \in K'$ is **small** if $\deg(\lambda), \deg(\bar{\lambda}) \leq 3g + 1$

For the principal ideal class:

$$\lambda = \alpha^3 \epsilon^{-1} \quad \text{where } \mathfrak{a} = (\alpha) \quad \text{with } \delta(\mathfrak{a}, \mathcal{O}) \approx R/3$$

For ideal classes $[\mathfrak{t}]$ of order 3:

$$\lambda_0 = \alpha_0^3 \rho \epsilon^{-1} \quad \text{where } \mathfrak{a}_0 = (\alpha_0)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_0, \mathfrak{t}) \approx (R - \deg(\rho))/3$$

$$\lambda_1 = \alpha_1^3 \rho \epsilon^{-2} \quad \text{where } \mathfrak{a}_1 = (\alpha_1)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_1, \mathfrak{t}) \approx (2R - \deg(\rho))/3$$

$$\lambda_2 = \alpha_2^3 \rho \epsilon^{-3} \quad \text{where } \mathfrak{a}_2 = (\alpha_2)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_2, \mathfrak{t}) \approx (3R - \deg(\rho))/3$$

where ρ is a generator of \mathfrak{t}^3

Infrastructure ideal arithmetic is heavily used here.

Small Quadratic Generators

An element $\lambda \in K'$ is **small** if $\deg(\lambda), \deg(\bar{\lambda}) \leq 3g + 1$

For the principal ideal class:

$$\lambda = \alpha^3 \epsilon^{-1} \quad \text{where } \mathfrak{a} = (\alpha) \quad \text{with } \delta(\mathfrak{a}, \mathcal{O}) \approx R/3$$

For ideal classes $[\mathfrak{t}]$ of order 3:

$$\lambda_0 = \alpha_0^3 \rho \epsilon^{-1} \quad \text{where } \mathfrak{a}_0 = (\alpha_0)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_0, \mathfrak{t}) \approx (R - \deg(\rho))/3$$

$$\lambda_1 = \alpha_1^3 \rho \epsilon^{-2} \quad \text{where } \mathfrak{a}_1 = (\alpha_1)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_1, \mathfrak{t}) \approx (2R - \deg(\rho))/3$$

$$\lambda_2 = \alpha_2^3 \rho \epsilon^{-3} \quad \text{where } \mathfrak{a}_2 = (\alpha_2)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_2, \mathfrak{t}) \approx (3R - \deg(\rho))/3$$

where ρ is a generator of \mathfrak{t}^3

Infrastructure ideal arithmetic is heavily used here.

Small Quadratic Generators

An element $\lambda \in K'$ is **small** if $\deg(\lambda), \deg(\bar{\lambda}) \leq 3g + 1$

For the principal ideal class:

$$\lambda = \alpha^3 \epsilon^{-1} \quad \text{where } \mathfrak{a} = (\alpha) \quad \text{with } \delta(\mathfrak{a}, \mathcal{O}) \approx R/3$$

For ideal classes $[\mathfrak{t}]$ of order 3:

$$\lambda_0 = \alpha_0^3 \rho \epsilon^{-1} \quad \text{where } \mathfrak{a}_0 = (\alpha_0)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_0, \mathfrak{t}) \approx (R - \deg(\rho))/3$$

$$\lambda_1 = \alpha_1^3 \rho \epsilon^{-2} \quad \text{where } \mathfrak{a}_1 = (\alpha_1)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_1, \mathfrak{t}) \approx (2R - \deg(\rho))/3$$

$$\lambda_2 = \alpha_2^3 \rho \epsilon^{-3} \quad \text{where } \mathfrak{a}_2 = (\alpha_2)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_2, \mathfrak{t}) \approx (3R - \deg(\rho))/3$$

where ρ is a generator of \mathfrak{t}^3

Infrastructure ideal arithmetic is heavily used here.

Small Quadratic Generators

An element $\lambda \in K'$ is **small** if $\deg(\lambda), \deg(\bar{\lambda}) \leq 3g + 1$

For the principal ideal class:

$$\lambda = \alpha^3 \epsilon^{-1} \quad \text{where } \mathfrak{a} = (\alpha) \quad \text{with } \delta(\mathfrak{a}, \mathcal{O}) \approx R/3$$

For ideal classes $[\mathfrak{t}]$ of order 3:

$$\lambda_0 = \alpha_0^3 \rho \epsilon^{-1} \quad \text{where } \mathfrak{a}_0 = (\alpha_0)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_0, \mathfrak{t}) \approx (R - \deg(\rho))/3$$

$$\lambda_1 = \alpha_1^3 \rho \epsilon^{-2} \quad \text{where } \mathfrak{a}_1 = (\alpha_1)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_1, \mathfrak{t}) \approx (2R - \deg(\rho))/3$$

$$\lambda_2 = \alpha_2^3 \rho \epsilon^{-3} \quad \text{where } \mathfrak{a}_2 = (\alpha_2)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_2, \mathfrak{t}) \approx (3R - \deg(\rho))/3$$

where ρ is a generator of \mathfrak{t}^3

Infrastructure ideal arithmetic is heavily used here.

Small Quadratic Generators

An element $\lambda \in K'$ is **small** if $\deg(\lambda), \deg(\bar{\lambda}) \leq 3g + 1$

For the principal ideal class:

$$\lambda = \alpha^3 \epsilon^{-1} \quad \text{where } \mathfrak{a} = (\alpha) \quad \text{with } \delta(\mathfrak{a}, \mathcal{O}) \approx R/3$$

For ideal classes $[\mathfrak{t}]$ of order 3:

$$\lambda_0 = \alpha_0^3 \rho \epsilon^{-1} \quad \text{where } \mathfrak{a}_0 = (\alpha_0)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_0, \mathfrak{t}) \approx (R - \deg(\rho))/3$$

$$\lambda_1 = \alpha_1^3 \rho \epsilon^{-2} \quad \text{where } \mathfrak{a}_1 = (\alpha_1)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_1, \mathfrak{t}) \approx (2R - \deg(\rho))/3$$

$$\lambda_2 = \alpha_2^3 \rho \epsilon^{-3} \quad \text{where } \mathfrak{a}_2 = (\alpha_2)\mathfrak{t} \quad \text{with } \delta(\mathfrak{a}_2, \mathfrak{t}) \approx (3R - \deg(\rho))/3$$

where ρ is a generator of \mathfrak{t}^3

Infrastructure ideal arithmetic is heavily used here.

Computing \mathcal{L} for D Unusual

Precomputation: Regulator R , 3-torsion of ideal class group of K'

Input: R and reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

1. Compute the principal ideal \mathfrak{a} from above
2. Compute the small generator λ of \mathfrak{a}^3
3. Set $2A = \text{Tr}(\lambda)$ and $Q = aN(\mathfrak{a})$ with $a^3 = \text{sgn}(N(\lambda))$
4. Output $F(Z) = Z^3 - 3QZ + 2A$
5. For $i = 1$ to l do
 - For $j = 0$ to 2 do
 - 5.1. Compute the ideal \mathfrak{a}_{ij} from above
 - 5.2. Compute the small generator λ_{ij} of \mathfrak{a}_{ij}^3
 - 5.3. Compute A_{ij} and Q_{ij} analogous to step 3
 - 5.4. Output $F_{ij}(Z) = Z^3 - 3Q_{ij}Z + 2A_{ij}$

Computing \mathcal{L} for D Unusual

Precomputation: Regulator R , 3-torsion of ideal class group of K'

Input: R and reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

1. Compute the principal ideal \mathfrak{a} from above
2. Compute the small generator λ of \mathfrak{a}^3
3. Set $2A = \text{Tr}(\lambda)$ and $Q = aN(\mathfrak{a})$ with $a^3 = \text{sgn}(N(\lambda))$
4. Output $F(Z) = Z^3 - 3QZ + 2A$
5. For $i = 1$ to l do
 - For $j = 0$ to 2 do
 - 5.1. Compute the ideal \mathfrak{a}_{ij} from above
 - 5.2. Compute the small generator λ_{ij} of \mathfrak{a}_{ij}^3
 - 5.3. Compute A_{ij} and Q_{ij} analogous to step 3
 - 5.4. Output $F_{ij}(Z) = Z^3 - 3Q_{ij}Z + 2A_{ij}$

Computing \mathcal{L} for D Unusual

Precomputation: Regulator R , 3-torsion of ideal class group of K'

Input: R and reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

1. Compute the principal ideal \mathfrak{a} from above
2. Compute the small generator λ of \mathfrak{a}^3
3. Set $2A = \text{Tr}(\lambda)$ and $Q = aN(\mathfrak{a})$ with $a^3 = \text{sgn}(N(\lambda))$
4. Output $F(Z) = Z^3 - 3QZ + 2A$
5. For $i = 1$ to l do
 - For $j = 0$ to 2 do
 - 5.1. Compute the ideal \mathfrak{a}_{ij} from above
 - 5.2. Compute the small generator λ_{ij} of \mathfrak{a}_{ij}^3
 - 5.3. Compute A_{ij} and Q_{ij} analogous to step 3
 - 5.4. Output $F_{ij}(Z) = Z^3 - 3Q_{ij}Z + 2A_{ij}$

Computing \mathcal{L} for D Unusual

Precomputation: Regulator R , 3-torsion of ideal class group of K'

Input: R and reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

1. Compute the principal ideal \mathfrak{a} from above
2. Compute the small generator λ of \mathfrak{a}^3
3. Set $2A = \text{Tr}(\lambda)$ and $Q = aN(\mathfrak{a})$ with $a^3 = \text{sgn}(N(\lambda))$
4. Output $F(Z) = Z^3 - 3QZ + 2A$
5. For $i = 1$ to l do
 - For $j = 0$ to 2 do
 - 5.1. Compute the ideal \mathfrak{a}_{ij} from above
 - 5.2. Compute the small generator λ_{ij} of \mathfrak{a}_{ij}^3
 - 5.3. Compute A_{ij} and Q_{ij} analogous to step 3
 - 5.4. Output $F_{ij}(Z) = Z^3 - 3Q_{ij}Z + 2A_{ij}$

Computing \mathcal{L} for D Unusual

Precomputation: Regulator R , 3-torsion of ideal class group of K'

Input: R and reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

1. Compute the principal ideal \mathfrak{a} from above
2. Compute the small generator λ of \mathfrak{a}^3
3. Set $2A = \text{Tr}(\lambda)$ and $Q = aN(\mathfrak{a})$ with $a^3 = \text{sgn}(N(\lambda))$
4. Output $F(Z) = Z^3 - 3QZ + 2A$
5. For $i = 1$ to l do
 - For $j = 0$ to 2 do
 - 5.1. Compute the ideal \mathfrak{a}_{ij} from above
 - 5.2. Compute the small generator λ_{ij} of \mathfrak{a}_{ij}^3
 - 5.3. Compute A_{ij} and Q_{ij} analogous to step 3
 - 5.4. Output $F_{ij}(Z) = Z^3 - 3Q_{ij}Z + 2A_{ij}$

Computing \mathcal{L} for D Unusual

Precomputation: Regulator R , 3-torsion of ideal class group of K'

Input: R and reduced representatives $\tau_1, \tau_2, \dots, \tau_l$ of all the ideal classes of K' of order 3

Output: Minimal polynomials for all conjugate triples of cubic function fields of discriminant D

Algorithm

1. Compute the principal ideal \mathfrak{a} from above
2. Compute the small generator λ of \mathfrak{a}^3
3. Set $2A = \text{Tr}(\lambda)$ and $Q = aN(\mathfrak{a})$ with $a^3 = \text{sgn}(N(\lambda))$
4. Output $F(Z) = Z^3 - 3QZ + 2A$
5. For $i = 1$ to l do
 - For $j = 0$ to 2 do
 - 5.1. Compute the ideal \mathfrak{a}_{ij} from above
 - 5.2. Compute the small generator λ_{ij} of \mathfrak{a}_{ij}^3
 - 5.3. Compute A_{ij} and Q_{ij} analogous to step 3
 - 5.4. Output $F_{ij}(Z) = Z^3 - 3Q_{ij}Z + 2A_{ij}$

Counting Cubic Function Fields

Set $\mathcal{I}^* = \mathcal{I} \setminus \{\text{principal class pair}\}$, the set of conjugate pairs of ideal classes of K' order 3.

$$|\mathcal{I}^*| = \frac{3^{r'} - 1}{2} \quad \text{where } r' \text{ is the 3-rank of the ideal class group of } K'$$

Recall: D real: $|\mathcal{L}| = |\mathcal{I}^*|$
 D unusual: $|\mathcal{L}| = 3|\mathcal{I}^*| + 1$



Theorem

If D is real, then there are $(3^{r'} - 1)/2$ triples of conjugate cubic fields of discriminant D .

If D is unusual, then there are $(3^{r'+1} - 1)/2$ triples of conjugate cubic fields of discriminant D .

Counting Cubic Function Fields

Set $\mathcal{I}^* = \mathcal{I} \setminus \{\text{principal class pair}\}$, the set of conjugate pairs of ideal classes of K' order 3.

$$|\mathcal{I}^*| = \frac{3^{r'} - 1}{2} \quad \text{where } r' \text{ is the 3-rank of the ideal class group of } K'$$

Recall: D real: $|\mathcal{L}| = |\mathcal{I}^*|$
 D unusual: $|\mathcal{L}| = 3|\mathcal{I}^*| + 1$



Theorem

If D is real, then there are $(3^{r'} - 1)/2$ triples of conjugate cubic fields of discriminant D .

If D is unusual, then there are $(3^{r'+1} - 1)/2$ triples of conjugate cubic fields of discriminant D .

Counting Cubic Function Fields

Set $\mathcal{I}^* = \mathcal{I} \setminus \{\text{principal class pair}\}$, the set of conjugate pairs of ideal classes of K' order 3.

$$|\mathcal{I}^*| = \frac{3^{r'} - 1}{2} \quad \text{where } r' \text{ is the 3-rank of the ideal class group of } K'$$

Recall: D real: $|\mathcal{L}| = |\mathcal{I}^*|$
 D unusual: $|\mathcal{L}| = 3|\mathcal{I}^*| + 1$



Theorem

If D is real, then there are $(3^{r'} - 1)/2$ triples of conjugate cubic fields of discriminant D .

If D is unusual, then there are $(3^{r'+1} - 1)/2$ triples of conjugate cubic fields of discriminant D .

Counting Cubic Function Fields

Set $\mathcal{I}^* = \mathcal{I} \setminus \{\text{principal class pair}\}$, the set of conjugate pairs of ideal classes of K' order 3.

$$|\mathcal{I}^*| = \frac{3^{r'} - 1}{2} \quad \text{where } r' \text{ is the 3-rank of the ideal class group of } K'$$

Recall: D real: $|\mathcal{L}| = |\mathcal{I}^*|$
 D unusual: $|\mathcal{L}| = 3|\mathcal{I}^*| + 1$



Theorem

If D is real, then there are $(3^{r'} - 1)/2$ triples of conjugate cubic fields of discriminant D .

If D is unusual, then there are $(3^{r'+1} - 1)/2$ triples of conjugate cubic fields of discriminant D .

More on Cubic Function Fields

Lemma

Let $q \equiv -1 \pmod{3}$ and $L/\mathbb{F}_q(x)$ a cubic function field of discriminant D . Then we have for the place ∞ of infinity of $\mathbb{F}_q(x)$:

- D is imaginary if and only if $(\infty) = \mathfrak{p}q^2$ in L ;
- D is unusual if and only if $(\infty) = \mathfrak{p}q$ or $(\infty) = \mathfrak{p}^3$ in L ;
- D is real if and only if $(\infty) = \mathfrak{p}q\mathfrak{r}$ or $(\infty) = \mathfrak{p}$ in L .

Theorem (Hasse)

Let $r = 3\text{-rank}(K)$. Then there are $(3^r - 1)/2$ triples of conjugate cubic fields of discriminant D that have at least two places at infinity.

Theorem (Scholz)

Let D be unusual (so D' real), $r = 3\text{-rank}(K)$, $r' = 3\text{-rank}(K')$. Then either $r = r'$ (non-escalatory)
or $r = r' + 1$ (escalatory).

More on Cubic Function Fields

Lemma

Let $q \equiv -1 \pmod{3}$ and $L/\mathbb{F}_q(x)$ a cubic function field of discriminant D . Then we have for the place ∞ of infinity of $\mathbb{F}_q(x)$:

- D is imaginary if and only if $(\infty) = \mathfrak{p}q^2$ in L ;
- D is unusual if and only if $(\infty) = \mathfrak{p}q$ or $(\infty) = \mathfrak{p}^3$ in L ;
- D is real if and only if $(\infty) = \mathfrak{p}q\mathfrak{r}$ or $(\infty) = \mathfrak{p}$ in L .

Theorem (Hasse)

Let $r = 3\text{-rank}(K)$. Then there are $(3^r - 1)/2$ triples of conjugate cubic fields of discriminant D that have at least two places at infinity.

Theorem (Scholz)

Let D be unusual (so D' real), $r = 3\text{-rank}(K)$, $r' = 3\text{-rank}(K')$. Then either $r = r'$ (non-escalatory) or $r = r' + 1$ (escalatory).

More on Cubic Function Fields

Lemma

Let $q \equiv -1 \pmod{3}$ and $L/\mathbb{F}_q(x)$ a cubic function field of discriminant D . Then we have for the place ∞ of infinity of $\mathbb{F}_q(x)$:

- D is imaginary if and only if $(\infty) = \mathfrak{p}q^2$ in L ;
- D is unusual if and only if $(\infty) = \mathfrak{p}q$ or $(\infty) = \mathfrak{p}^3$ in L ;
- D is real if and only if $(\infty) = \mathfrak{p}q\mathfrak{r}$ or $(\infty) = \mathfrak{p}$ in L .

Theorem (Hasse)

Let $r = 3\text{-rank}(K)$. Then there are $(3^r - 1)/2$ triples of conjugate cubic fields of discriminant D that have at least two places at infinity.

Theorem (Scholz)

Let D be unusual (so D' real), $r = 3\text{-rank}(K)$, $r' = 3\text{-rank}(K')$. Then either $r = r'$ (non-escalatory) or $r = r' + 1$ (escalatory).

More on Cubic Function Fields

Lemma

Let $q \equiv -1 \pmod{3}$ and $L/\mathbb{F}_q(x)$ a cubic function field of discriminant D . Then we have for the place ∞ of infinity of $\mathbb{F}_q(x)$:

- D is imaginary if and only if $(\infty) = \mathfrak{p}q^2$ in L ;
- D is unusual if and only if $(\infty) = \mathfrak{p}q$ or $(\infty) = \mathfrak{p}^3$ in L ;
- D is real if and only if $(\infty) = \mathfrak{p}q\mathfrak{r}$ or $(\infty) = \mathfrak{p}$ in L .

Theorem (Hasse)

Let $r = 3\text{-rank}(K)$. Then there are $(3^r - 1)/2$ triples of conjugate cubic fields of discriminant D that have at least two places at infinity.

Theorem (Scholz)

Let D be unusual (so D' real), $r = 3\text{-rank}(K)$, $r' = 3\text{-rank}(K')$. Then either $r = r'$ (**non-escalatory**)
or $r = r' + 1$ (**escalatory**).

Counting Cubic Fields by Signature

Theorem

Let $q \equiv -1 \pmod{3}$, $\deg(D)$ even, $r = 3\text{-rank}(K)$, $r' = 3\text{-rank}(K')$.

Suppose that D is unusual.

- In the escalatory case ($r = r' + 1$), all $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q$.*
- In the non-escalatory case ($r = r'$), $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q$, the other 3^r such triples have $(\infty) = \mathfrak{p}^3$.*

Suppose that D is real.

- In the escalatory case ($r = r' - 1$), $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q\mathfrak{r}$, the other 3^r such triples have $(\infty) = \mathfrak{p}$.*
- In the non-escalatory case ($r = r'$), all $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q\mathfrak{r}$.*

Counting Cubic Fields by Signature

Theorem

Let $q \equiv -1 \pmod{3}$, $\deg(D)$ even, $r = 3\text{-rank}(K)$, $r' = 3\text{-rank}(K')$.

Suppose that D is unusual.

- In the escalatory case ($r = r' + 1$), all $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q$.
- In the non-escalatory case ($r = r'$), $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q$, the other 3^r such triples have $(\infty) = \mathfrak{p}^3$.

Suppose that D is real.

- In the escalatory case ($r = r' - 1$), $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q\mathfrak{r}$, the other 3^r such triples have $(\infty) = \mathfrak{p}$.
- In the non-escalatory case ($r = r'$), all $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q\mathfrak{r}$.

Counting Cubic Fields by Signature

Theorem

Let $q \equiv -1 \pmod{3}$, $\deg(D)$ even, $r = 3\text{-rank}(K)$, $r' = 3\text{-rank}(K')$.

Suppose that D is unusual.

- In the escalatory case ($r = r' + 1$), all $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q$.
- In the non-escalatory case ($r = r'$), $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q$, the other 3^r such triples have $(\infty) = \mathfrak{p}^3$.

Suppose that D is real.

- In the escalatory case ($r = r' - 1$), $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q\mathfrak{r}$, the other 3^r such triples have $(\infty) = \mathfrak{p}$.
- In the non-escalatory case ($r = r'$), all $(3^r - 1)/2$ triples of cubic function fields of discriminant D have $(\infty) = \mathfrak{p}q\mathfrak{r}$.

Example – Escalatory, D Unusual

$$q = 11, \quad D = 7x^{10} + x^7 + 3x^6 + 2x^5 + 7x^4 + 8x^3 + 4x^2 + 2x \quad (\text{unusual})$$

$$r = 3, \quad r' = 2 \text{ (escalatory)} \Rightarrow (3^3 - 1)/2 = 13 \text{ fields, all with } (\infty) = pq$$

$$F(Z) = Z^3 - 3QZ + 2A \text{ with}$$

#	$3Q$	$2A$
1	$5x^3 + 10x + 4$	$4x^6 + x^5 + x^3 + 9x^2 + 6x + 4$
2	$10x^4 + 9x^3 + x^2 + 5x + 9$	$10x^6 + 8x^5 + 5x^3 + 5x^2 + 5x + 3$
3	$6x^4 + 4x^3 + 10x + 4$	$5x^6 + 4x^5 + 3x^4 + 5x^3 + 3x^2 + x + 7$
4	$9x^4 + 4x^3 + 6x^2 + 5x + 1$	$x^6 + 4x^5 + 8x^4 + 9x^3 + 4x^2 + 7x + 5$
5	$4x^4 + 7x^3 + 10x^2 + 5x + 4$	$6x^6 + 6x^5 + 4x^4 + 4x^3 + 8x^2 + 10x + 4$
6	$9x^3 + 4x^2 + 8x + 9$	$x^6 + 3x^5 + 3x^3 + 6x + 3$
7	$x^4 + 3x^3 + 9x + 3$	$x^6 + 2x^5 + 2x^4 + 3x^3 + 6x^2 + 3x + 2$
8	$x^4 + 8x^3 + 6x^2 + 3x + 1$	$x^6 + 9x^5 + 7x^4 + 4x^3 + 6x^2 + 3x + 6$
9	$7x^4 + 4x^3 + 9x^2 + 6x$	$9x^6 + 10x^5 + 10x^4 + 9x^3 + 6x^2$
10	$6x^4 + 4x^3 + 5x^2 + 9x + 4$	$5x^6 + 10x^4 + 2x^3 + 5x^2 + 8x + 7$
11	$3x^4 + 5x^3 + 4x^2 + 6x + 9$	$8x^6 + 10x^5 + 4x^4 + 4x^3 + 8x^2 + 2x + 3$
12	$5x^4 + 6x^2 + 8x + 9$	$2x^6 + 10x^5 + 3x^4 + x^3 + x^2 + 10x + 3$
13	$4x^4 + 3x^3 + 5x^2 + 10x + 9$	$8x^6 + 5x^4 + 3x^3 + 9x^2 + x + 3$

Example – Escalatory, D Unusual

$$q = 11, \quad D = 7x^{10} + x^7 + 3x^6 + 2x^5 + 7x^4 + 8x^3 + 4x^2 + 2x \quad (\text{unusual})$$

$$r = 3, \quad r' = 2 \quad (\text{escalatory}) \Rightarrow (3^3 - 1)/2 = 13 \text{ fields, all with } (\infty) = pq$$

$$F(Z) = Z^3 - 3QZ + 2A \text{ with}$$

#	$3Q$	$2A$
1	$5x^3 + 10x + 4$	$4x^6 + x^5 + x^3 + 9x^2 + 6x + 4$
2	$10x^4 + 9x^3 + x^2 + 5x + 9$	$10x^6 + 8x^5 + 5x^3 + 5x^2 + 5x + 3$
3	$6x^4 + 4x^3 + 10x + 4$	$5x^6 + 4x^5 + 3x^4 + 5x^3 + 3x^2 + x + 7$
4	$9x^4 + 4x^3 + 6x^2 + 5x + 1$	$x^6 + 4x^5 + 8x^4 + 9x^3 + 4x^2 + 7x + 5$
5	$4x^4 + 7x^3 + 10x^2 + 5x + 4$	$6x^6 + 6x^5 + 4x^4 + 4x^3 + 8x^2 + 10x + 4$
6	$9x^3 + 4x^2 + 8x + 9$	$x^6 + 3x^5 + 3x^3 + 6x + 3$
7	$x^4 + 3x^3 + 9x + 3$	$x^6 + 2x^5 + 2x^4 + 3x^3 + 6x^2 + 3x + 2$
8	$x^4 + 8x^3 + 6x^2 + 3x + 1$	$x^6 + 9x^5 + 7x^4 + 4x^3 + 6x^2 + 3x + 6$
9	$7x^4 + 4x^3 + 9x^2 + 6x$	$9x^6 + 10x^5 + 10x^4 + 9x^3 + 6x^2$
10	$6x^4 + 4x^3 + 5x^2 + 9x + 4$	$5x^6 + 10x^4 + 2x^3 + 5x^2 + 8x + 7$
11	$3x^4 + 5x^3 + 4x^2 + 6x + 9$	$8x^6 + 10x^5 + 4x^4 + 4x^3 + 8x^2 + 2x + 3$
12	$5x^4 + 6x^2 + 8x + 9$	$2x^6 + 10x^5 + 3x^4 + x^3 + x^2 + 10x + 3$
13	$4x^4 + 3x^3 + 5x^2 + 10x + 9$	$8x^6 + 5x^4 + 3x^3 + 9x^2 + x + 3$

Example – Escalatory, D Unusual

$q = 11$, $D = 7x^{10} + x^7 + 3x^6 + 2x^5 + 7x^4 + 8x^3 + 4x^2 + 2x$ (unusual)

$r = 3$, $r' = 2$ (escalatory) $\Rightarrow (3^3 - 1)/2 = 13$ fields, all with $(\infty) = pq$

$F(Z) = Z^3 - 3QZ + 2A$ with

#	$3Q$	$2A$
1	$5x^3 + 10x + 4$	$4x^6 + x^5 + x^3 + 9x^2 + 6x + 4$
2	$10x^4 + 9x^3 + x^2 + 5x + 9$	$10x^6 + 8x^5 + 5x^3 + 5x^2 + 5x + 3$
3	$6x^4 + 4x^3 + 10x + 4$	$5x^6 + 4x^5 + 3x^4 + 5x^3 + 3x^2 + x + 7$
4	$9x^4 + 4x^3 + 6x^2 + 5x + 1$	$x^6 + 4x^5 + 8x^4 + 9x^3 + 4x^2 + 7x + 5$
5	$4x^4 + 7x^3 + 10x^2 + 5x + 4$	$6x^6 + 6x^5 + 4x^4 + 4x^3 + 8x^2 + 10x + 4$
6	$9x^3 + 4x^2 + 8x + 9$	$x^6 + 3x^5 + 3x^3 + 6x + 3$
7	$x^4 + 3x^3 + 9x + 3$	$x^6 + 2x^5 + 2x^4 + 3x^3 + 6x^2 + 3x + 2$
8	$x^4 + 8x^3 + 6x^2 + 3x + 1$	$x^6 + 9x^5 + 7x^4 + 4x^3 + 6x^2 + 3x + 6$
9	$7x^4 + 4x^3 + 9x^2 + 6x$	$9x^6 + 10x^5 + 10x^4 + 9x^3 + 6x^2$
10	$6x^4 + 4x^3 + 5x^2 + 9x + 4$	$5x^6 + 10x^4 + 2x^3 + 5x^2 + 8x + 7$
11	$3x^4 + 5x^3 + 4x^2 + 6x + 9$	$8x^6 + 10x^5 + 4x^4 + 4x^3 + 8x^2 + 2x + 3$
12	$5x^4 + 6x^2 + 8x + 9$	$2x^6 + 10x^5 + 3x^4 + x^3 + x^2 + 10x + 3$
13	$4x^4 + 3x^3 + 5x^2 + 10x + 9$	$8x^6 + 5x^4 + 3x^3 + 9x^2 + x + 3$

Example – Non-Escalatory, D Unusual

$$q = 11, \quad D = 2x^8 + x^6 + 5x^4 + 6x^2 + 7 \quad (\text{unusual})$$

$$r = r' = 2 \text{ (non-escalatory)} \Rightarrow \begin{cases} (3^2 - 1)/2 = 4 & \text{fields with } (\infty) = pq \\ 3^2 = 9 & \text{fields with } (\infty) = p^3 \end{cases}$$

$$F(Z) = Z^3 - 3QZ + 2A \text{ with}$$

#	$3Q$	$2A$
1	$9x^2 + 6$	$x^6 + 7x^4 + 6x^2$
2	$7x^3 + 7x + 8$	$6x^6 + 7x^5 + 8x^4 + 5x^3 + 4x^2 + 4$
3	$9x^3 + 3x^2 + 8x + 1$	$2x^6 + 6x^5 + 6x^4 + x^3 + 5x + 5$
4	$9x^3 + 2x^2 + 8x + 4$	$4x^6 + 6x^5 + 4x^3 + 3x^2 + x + 5$
5	$4x^3 + 4x^2 + 6x + 2$	$10x^5 + 4x^4 + 8x^3 + 10x$
6	$5x^2 + 8x + 5$	$2x^5 + 6x^3 + 2x + 10$
7	$10x^3 + 5x^2 + 5x + 1$	$8x^5 + 6x^4 + 6x^3 + 9x^2 + x + 6$
8	$5x^2 + 3x + 5$	$9x^5 + 5x^3 + 9x + 10$
9	$x^3 + 5x^2 + 6x + 1$	$8x^5 + 5x^4 + 6x^3 + 2x^2 + x + 5$
10	$7x^3 + 4x^2 + 5x + 2$	$10x^5 + 7x^4 + 8x^3 + 10x$
11	$5x^2 + 1$	$10x^4 + 2x^2 + 1$
12	$3x^2 + 4$	$10x^4 + 6x^2 + 6$
13	$3x^2$	$10x^4 + 6x^2 + 3$

Example – Non-Escalatory, D Unusual

$$q = 11, \quad D = 2x^8 + x^6 + 5x^4 + 6x^2 + 7 \quad (\text{unusual})$$

$$r = r' = 2 \quad (\text{non-escalatory}) \Rightarrow \begin{cases} (3^2 - 1)/2 = 4 & \text{fields with } (\infty) = pq \\ 3^2 = 9 & \text{fields with } (\infty) = p^3 \end{cases}$$

$$F(Z) = Z^3 - 3QZ + 2A \quad \text{with}$$

#	$3Q$	$2A$
1	$9x^2 + 6$	$x^6 + 7x^4 + 6x^2$
2	$7x^3 + 7x + 8$	$6x^6 + 7x^5 + 8x^4 + 5x^3 + 4x^2 + 4$
3	$9x^3 + 3x^2 + 8x + 1$	$2x^6 + 6x^5 + 6x^4 + x^3 + 5x + 5$
4	$9x^3 + 2x^2 + 8x + 4$	$4x^6 + 6x^5 + 4x^3 + 3x^2 + x + 5$
5	$4x^3 + 4x^2 + 6x + 2$	$10x^5 + 4x^4 + 8x^3 + 10x$
6	$5x^2 + 8x + 5$	$2x^5 + 6x^3 + 2x + 10$
7	$10x^3 + 5x^2 + 5x + 1$	$8x^5 + 6x^4 + 6x^3 + 9x^2 + x + 6$
8	$5x^2 + 3x + 5$	$9x^5 + 5x^3 + 9x + 10$
9	$x^3 + 5x^2 + 6x + 1$	$8x^5 + 5x^4 + 6x^3 + 2x^2 + x + 5$
10	$7x^3 + 4x^2 + 5x + 2$	$10x^5 + 7x^4 + 8x^3 + 10x$
11	$5x^2 + 1$	$10x^4 + 2x^2 + 1$
12	$3x^2 + 4$	$10x^4 + 6x^2 + 6$
13	$3x^2$	$10x^4 + 6x^2 + 3$

Example – Non-Escalatory, D Unusual

$$q = 11, \quad D = 2x^8 + x^6 + 5x^4 + 6x^2 + 7 \quad (\text{unusual})$$

$$r = r' = 2 \quad (\text{non-escalatory}) \Rightarrow \begin{cases} (3^2 - 1)/2 = 4 & \text{fields with } (\infty) = p^4 \\ 3^2 = 9 & \text{fields with } (\infty) = p^3 \end{cases}$$

$$F(Z) = Z^3 - 3QZ + 2A \quad \text{with}$$

#	$3Q$	$2A$
1	$9x^2 + 6$	$x^6 + 7x^4 + 6x^2$
2	$7x^3 + 7x + 8$	$6x^6 + 7x^5 + 8x^4 + 5x^3 + 4x^2 + 4$
3	$9x^3 + 3x^2 + 8x + 1$	$2x^6 + 6x^5 + 6x^4 + x^3 + 5x + 5$
4	$9x^3 + 2x^2 + 8x + 4$	$4x^6 + 6x^5 + 4x^3 + 3x^2 + x + 5$
5	$4x^3 + 4x^2 + 6x + 2$	$10x^5 + 4x^4 + 8x^3 + 10x$
6	$5x^2 + 8x + 5$	$2x^5 + 6x^3 + 2x + 10$
7	$10x^3 + 5x^2 + 5x + 1$	$8x^5 + 6x^4 + 6x^3 + 9x^2 + x + 6$
8	$5x^2 + 3x + 5$	$9x^5 + 5x^3 + 9x + 10$
9	$x^3 + 5x^2 + 6x + 1$	$8x^5 + 5x^4 + 6x^3 + 2x^2 + x + 5$
10	$7x^3 + 4x^2 + 5x + 2$	$10x^5 + 7x^4 + 8x^3 + 10x$
11	$5x^2 + 1$	$10x^4 + 2x^2 + 1$
12	$3x^2 + 4$	$10x^4 + 6x^2 + 6$
13	$3x^2$	$10x^4 + 6x^2 + 3$

