Tabulation of cubic function fields with imaginary and unusual Hessian

8th Algorithmic Number Theory Symposium

Pieter Rozenhart and Renate Scheidler

University of Calgary

Sunday, May 18th, 2008

The problem at hand

In 1997, Belabas presented an algorithm for tabulating all non-isomorphic cubic number fields of discriminant D with $|D| \leq X$ for any $X > 0$.

We give an extension of this approach to function fields.

Specifically, we wish to tabulate cubic extensions of discriminant D of the rational function field $\mathbb{F}_q(t)$, where $q = 5, 7$ and $|D| < X$ for any $X > 0$.

Talk Outline

- The main tool and some preliminaries: A version of the Davenport-Heilbronn Theorem (DH) for algebraic function fields.
- Using this, we can tabulate cubic function fields by tabulating equivalence classes of binary cubic forms belonging to a certain set $\mathcal{U}$.
- To this end, we adapt the reduction theory for integral binary cubic forms to binary cubic forms with coefficients in $\mathbb{F}_q[t]$.
- Tabulation algorithm and numerical results.
- Open problems.

Note: A completely generalized version of DH has been proved by Taniguchi (2006).

Talk Outline

- The main tool and some preliminaries: A version of the Davenport-Heilbronn Theorem (DH) for algebraic function fields.
- Using this, we can tabulate cubic function fields by tabulating equivalence classes of binary cubic forms belonging to a certain set $\mathcal{U}$.
- To this end, we adapt the reduction theory for integral binary cubic forms to binary cubic forms with coefficients in $\mathbb{F}_q[t]$.
- Tabulation algorithm and numerical results.
- Open problems.

Note: A completely generalized version of DH has been proved by Taniguchi (2006).

Talk Outline

- The main tool and some preliminaries: A version of the Davenport-Heilbronn Theorem (DH) for algebraic function fields.
- Using this, we can tabulate cubic function fields by tabulating equivalence classes of binary cubic forms belonging to a certain set $\mathcal{U}$.
- To this end, we adapt the reduction theory for integral binary cubic forms to binary cubic forms with coefficients in $\mathbb{F}_q[t]$.
- Tabulation algorithm and numerical results.
- Open problems.

Note: A completely generalized version of DH has been proved by Taniguchi (2006).

Talk Outline

- The main tool and some preliminaries: A version of the Davenport-Heilbronn Theorem (DH) for algebraic function fields.
- Using this, we can tabulate cubic function fields by tabulating equivalence classes of binary cubic forms belonging to a certain set $\mathcal{U}$.
- To this end, we adapt the reduction theory for integral binary cubic forms to binary cubic forms with coefficients in $\mathbb{F}_q[t]$.
- Tabulation algorithm and numerical results.
- Open problems.

Note: A completely generalized version of DH has been proved by Taniguchi (2006).

Talk Outline

- The main tool and some preliminaries: A version of the Davenport-Heilbronn Theorem (DH) for algebraic function fields.
- Using this, we can tabulate cubic function fields by tabulating equivalence classes of binary cubic forms belonging to a certain set $\mathcal{U}$.
- To this end, we adapt the reduction theory for integral binary cubic forms to binary cubic forms with coefficients in $\mathbb{F}_q[t]$.
- Tabulation algorithm and numerical results.
- Open problems.

Note: A completely generalized version of DH has been proved by Taniguchi (2006).

Talk Outline

- The main tool and some preliminaries: A version of the Davenport-Heilbronn Theorem (DH) for algebraic function fields.
- Using this, we can tabulate cubic function fields by tabulating equivalence classes of binary cubic forms belonging to a certain set $\mathcal{U}$.
- To this end, we adapt the reduction theory for integral binary cubic forms to binary cubic forms with coefficients in $\mathbb{F}_q[t]$.
- Tabulation algorithm and numerical results.
- Open problems.

Note: A completely generalized version of DH has been proved by Taniguchi (2006).

Some Preliminaries

- Let $\mathbb{F}_q$ be a finite field of characteristic at least 5, and set $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$.
- Denote by $\mathbb{F}_q[t]$ and $\mathbb{F}_q(t)$ the ring of polynomials and the field of rational functions in the variable t over $\mathbb{F}_q$, respectively.
- For any non-zero $H \in \mathbb{F}_q[t]$ of degree $n = \deg(H)$, we let $|H| = q^n = q^{\deg(H)}$, and denote by $\operatorname{sgn}(H)$ the leading coefficient of H. For $H = 0$, we set $|H| = 0$.

The lynchpin of this whole operation...

Here's something straightforward:

We can obtain a cubic function field from an irreducible binary cubic form f with coefficients in $\mathbb{F}_q[t]$ in the obvious way; we adjoin any root θ of $f(x, 1)$ to $\mathbb{F}_q(t)$. This yields a cubic function field $K = \mathbb{F}_q(t, \theta)$. In other words, K is a degree three extension of $\mathbb{F}_q(t)$.

Can we go the other way? That is, can we obtain a binary cubic form from a cubic function field?

Note: By "cubic function field", we mean a degree three extension of the rational function field $\mathbb{F}_q(t)$.

...The Davenport Heilbronn Theorem

Theorem

Let q be a prime power with $\gcd(q, 6) = 1$. Then there exists a discriminant-preserving bijection between $\mathbb{F}_q(t)$-isomorphism classes of cubic function fields and equivalence classes of binary cubic forms with coefficients in $\mathbb{F}_q[t]$ belonging to a certain set $\mathcal{U}$.

Note: We assume that binary forms $f(x, y)$ are primitive, and that $f(x, 1)$ is irreducible over $\mathbb{F}_q[t]$.

Why is this useful?

This theorem has a very nice algorithmic translation:

- As we shall see, the reduction theory for cubic forms gives us a canonical representative in each equivalence class of primitive irreducible cubic forms.
- If a form f is "reduced", any reduced form equivalent to f is equal to f. So we essentially have uniqueness of "reduced" forms.
- Hence, to a given field, we can associate a unique binary cubic form.
- Reduced forms have "small" coefficients.

Why is this useful?

This theorem has a very nice algorithmic translation:

- As we shall see, the reduction theory for cubic forms gives us a canonical representative in each equivalence class of primitive irreducible cubic forms.
- If a form f is "reduced", any reduced form equivalent to f is equal to f. So we essentially have uniqueness of "reduced" forms.
- Hence, to a given field, we can associate a unique binary cubic form.
- Reduced forms have "small" coefficients.

Why is this useful?

This theorem has a very nice algorithmic translation:

- As we shall see, the reduction theory for cubic forms gives us a canonical representative in each equivalence class of primitive irreducible cubic forms.
- If a form f is "reduced", any reduced form equivalent to f is equal to f. So we essentially have uniqueness of "reduced" forms.
- Hence, to a given field, we can associate a unique binary cubic form.
- Reduced forms have "small" coefficients.

Why is this useful?

This theorem has a very nice algorithmic translation:

- As we shall see, the reduction theory for cubic forms gives us a canonical representative in each equivalence class of primitive irreducible cubic forms.
- If a form f is "reduced", any reduced form equivalent to f is equal to f. So we essentially have uniqueness of "reduced" forms.
- Hence, to a given field, we can associate a unique binary cubic form.
- Reduced forms have "small" coefficients.

Reduction of binary quadratic forms (E. Artin)

A *binary quadratic form over* $\mathbb{F}_q[t]$ is a homogeneous quadratic polynomial in two variables with coefficients in $\mathbb{F}_q[t]$.

We abbreviate binary quadratic forms $f(x, y) = Px^2 + Qxy + Ry^2$ by $f = (P, Q, R)$.

The *discriminant* D of a binary quadratic form $f = (P, Q, R)$ is given by $D(f) = D = Q^2 - 4PR$.

The binary quadratic form f is said to be:

imaginary if $\deg(D)$ is odd,

unusual if $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a non-square in $\mathbb{F}_q^*$,

real if $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a square in $\mathbb{F}_q^*$.

Reduction of binary quadratic forms (E. Artin)

A *binary quadratic form over* $\mathbb{F}_q[t]$ is a homogeneous quadratic polynomial in two variables with coefficients in $\mathbb{F}_q[t]$.

We abbreviate binary quadratic forms $f(x, y) = Px^2 + Qxy + Ry^2$ by $f = (P, Q, R)$.

The *discriminant* D of a binary quadratic form $f = (P, Q, R)$ is given by $D(f) = D = Q^2 - 4PR$.

The binary quadratic form f is said to be:

imaginary if $\deg(D)$ is odd,

unusual if $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a non-square in $\mathbb{F}_q^*$,

real if $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a square in $\mathbb{F}_q^*$.

Binary quadratic forms cont'd

Two binary quadratic (or cubic) forms F and G over $\mathbb{F}_q[t]$ are said to be equivalent if

$$\mu F(\alpha x + \beta y, \gamma x + \delta y) = G(x, y)$$

for some $\mu \in \mathbb{F}_q^*$ and $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q[t]$ with $\alpha\delta - \beta\gamma \in \mathbb{F}_q^*$.

That is $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{F}_q[t])$.

Up to associates, equivalent binary forms have the same discriminant.

Now we need a canonical representative for each equivalence class.

Reduced imaginary quadratic forms

We restrict our attention to imaginary and unusual quadratic forms.

An imaginary binary quadratic form $H = (P, Q, R)$ of discriminant $D = D(H)$ is said to be reduced if:

1. $|Q| < |P| \leq |D|^{1/2}$,
2. $\mathrm{sgn}(P) = 1$,
3. $Q = 0$ or $\mathrm{sgn}(Q)$ belongs to a certain finite set $S \subset \mathbb{F}_q^*$.

Note: The last two conditions here ensures that our reduced imaginary forms are "unique".

Reduced unusual quadratic forms

The situation is only slightly more complicated for unusual forms.

An unusual binary quadratic form $H = (P, Q, R)$ of discriminant $D = D(H)$ is said to be reduced if:

1. $|Q| < |P| \leq |D|^{1/2}$,
2. $\operatorname{sgn}(P) = 1$,
3. $Q = 0$ or $\operatorname{sgn}(Q)$ belongs to a certain finite set $S \subset \mathbb{F}_q^*$.
4. If $|P| = |D|^{1/2}$, then P is lexicographically minimal in the set $\{\tilde{P} \mid \tilde{H} = (\tilde{P}, \tilde{Q}, \tilde{R})$ is a reduced form equivalent to $H\}$.

Note: It is possible to obtain $|P| = |D|^{1/2}$, as D has even degree.

Reduced unusual quadratic forms

The situation is only slightly more complicated for unusual forms.

An unusual binary quadratic form $H = (P, Q, R)$ of discriminant $D = D(H)$ is said to be reduced if:

1. $|Q| < |P| \leq |D|^{1/2}$,
2. $\mathrm{sgn}(P) = 1$,
3. $Q = 0$ or $\mathrm{sgn}(Q)$ belongs to a certain finite set $S \subset \mathbb{F}_q^*$.
4. If $|P| = |D|^{1/2}$, then P is lexicographically minimal in the set $\{\tilde{P} \mid \tilde{H} = (\tilde{P}, \tilde{Q}, \tilde{R})$ is a reduced form equivalent to $H\}$.

Note: It is possible to obtain $|P| = |D|^{1/2}$, as D has even degree.

Summary of results that carry over from integral quadratic forms

We readily obtain the following:

1. The number of reduced quadratic forms for each fixed imaginary or unusual discriminant D is finite.
2. Every binary quadratic form with imaginary or unusual D is equivalent to a reduced imaginary or unusual binary quadratic form.
3. Any two equivalent reduced imaginary or unusual quadratic forms must be equal, provided we adopt certain conditions. Hence, every equivalence class of imaginary or unusual binary quadratic forms has a unique reduced representative.

Reduction of Binary Cubic Forms

A binary cubic form over $\mathbb{F}_q[t]$ is a homogeneous cubic polynomial in two variables with coefficients in $\mathbb{F}_q[t]$.

We abbreviate the binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ as (a, b, c, d).

The *discriminant*, D, of a binary cubic form $f = (a, b, c, d)$ is given by the formula $D = 18abcd + b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2$.

Binary Cubic Forms cont'd

The basic idea is to associate a binary quadratic form to each cubic form, and then essentially say that a cubic form is reduced whenever its associated quadratic form is also reduced.

Which quadratic form is appropriate for this purpose? The Hessian.

The Hessian of the cubic form f, denoted by $H_f(x, y)$, is given by the formula

$$H_f(x,y) = -\frac{1}{4}\begin{vmatrix} \frac{\partial^2 f}{\partial x \partial x} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y \partial y} \end{vmatrix} = Px^2 + Qxy + Ry^2,$$

where $P = b^2 - 3ac$, $Q = bc - 9ad$ and $R = c^2 - 3bd$.

The Hessian has a couple of nice properties.

Binary Cubic Forms cont'd

The basic idea is to associate a binary quadratic form to each cubic form, and then essentially say that a cubic form is reduced whenever its associated quadratic form is also reduced.

Which quadratic form is appropriate for this purpose? The Hessian.

The Hessian of the cubic form f, denoted by $H_f(x, y)$, is given by the formula

$$H_f(x,y) = -\frac{1}{4}\begin{vmatrix} \frac{\partial^2 f}{\partial x \partial x} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y \partial y} \end{vmatrix} = Px^2 + Qxy + Ry^2,$$

where $P = b^2 - 3ac$, $Q = bc - 9ad$ and $R = c^2 - 3bd$.

The Hessian has a couple of nice properties.

Hessian Properties

Let $f = (a, b, c, d)$ be a binary cubic form over $\mathbb{F}_q[t]$ and denote by $H_f = (P, Q, R)$ its Hessian. Then the following identities hold:

1. $D(H_f) = -3 \cdot D(f)$, where $D(f)$ denotes the discriminant of the cubic form f.
2. Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{F}_q[t])$. Let g be the form obtained by transforming f with M. That is, $g = f \circ M = f(\alpha x + \beta y, \gamma x + \delta y)$. Then $H_g = H_{f \circ M} = (\det M)^2 \cdot H_f \circ M$.

Note: A binary cubic form f over $\mathbb{F}_q[t]$ is said to be imaginary, unusual, or real according to whether its Hessian H_f is an imaginary, unusual, or real binary quadratic form.

How is this useful?

The properties of the Hessian allow for the following:

From the first property, if f has odd degree discriminant D, then $H(f)$ is an imaginary quadratic form. If f has even degree discriminant D, we can still use the Hessian provided $\mathrm{sgn}(-3D)$ is not a square in $\mathbb{F}_q^*$.

From the second property, we can reduce f using essentially the same transformation of variables used to reduce H_f.

Hence, we say an imaginary or unusual cubic form f is *reduced* if its Hessian H_f is reduced, along with some extra normalization conditions.

How is this useful?

The properties of the Hessian allow for the following:

From the first property, if f has odd degree discriminant D, then $H(f)$ is an imaginary quadratic form. If f has even degree discriminant D, we can still use the Hessian provided $\mathrm{sgn}(-3D)$ is not a square in $\mathbb{F}_q^*$.

From the second property, we can reduce f using essentially the same transformation of variables used to reduce H_f.

Hence, we say an imaginary or unusual cubic form f is *reduced* if its Hessian H_f is reduced, along with some extra normalization conditions.

The upshot for cubic forms

We once again obtain the following:

1. Every binary cubic form with imaginary or unusual Hessian is equivalent to a reduced cubic form with imaginary or unusual Hessian respectively.
2. Any two equivalent reduced imaginary or unusual cubic forms must be equal. Hence, every equivalence class of imaginary or unusual binary cubic forms with discriminant D has a unique reduced representative.

Finiteness results

We can bound the size of the coefficients of reduced binary cubic forms.

Theorem

Let $f = (a, b, c, d)$ be a reduced imaginary or unusual binary cubic form over $\mathbb{F}_q[t]$ of discriminant D. Then

$$|a|, |b| \leq |D|^{1/4}, \quad |c| \leq |D|^{1/2}/|a|, \quad |d| \leq \max\{|bc|/|a|, |b|^2/|a|q, |c|/q\}.$$

From this theorem, we deduce that there are only finitely many imaginary and unusual reduced binary cubic forms over $\mathbb{F}_q[t]$ of discriminant D.

Back to DH Theorem

Recall:

Theorem

Let q be a prime power with $\gcd(q, 6) = 1$. Then there exists a discriminant-preserving bijection between $\mathbb{F}_q(t)$-isomorphism classes of cubic function fields and classes of binary cubic forms over $\mathbb{F}_q[t]$ belonging to a certain set $\mathcal{U}$.

We need to describe $\mathcal{U}$, and be able to test whether any given binary cubic form lies in the set $\mathcal{U}$.

The set $\mathcal{U}$

First, let $[f]$ denote the equivalence class of any primitive binary cubic form f over $\mathbb{F}_q[t]$.
Fix any irreducible polynomial $p \in \mathbb{F}_q[t]$.

Let $\mathcal{U}_p$ be the set of equivalence classes $[f]$ of binary cubic forms over $\mathbb{F}_q[t]$ such that

- either $p^2 \nmid D(f)$, or
- $f(x,y) \equiv \lambda(\delta x - \gamma y)^3 \pmod{p}$ for some $\lambda \in \mathbb{F}_q[t]/(p)^*$, $\gamma, \delta \in \mathbb{F}_q[t]/(p)$, $x, y \in \mathbb{F}_q[t]/(p)$ not both zero, and in addition, $f(\gamma, \delta) \not\equiv 0 \pmod{p^2}$.

Finally, let $\mathcal{U} = \bigcap_p \mathcal{U}_p$.

The set $\mathcal{U}$

First, let $[f]$ denote the equivalence class of any primitive binary cubic form f over $\mathbb{F}_q[t]$.
Fix any irreducible polynomial $p \in \mathbb{F}_q[t]$.

Let $\mathcal{U}_p$ be the set of equivalence classes $[f]$ of binary cubic forms over $\mathbb{F}_q[t]$ such that

- either $p^2 \nmid D(f)$, or
- $f(x,y) \equiv \lambda(\delta x - \gamma y)^3 \pmod{p}$ for some $\lambda \in \mathbb{F}_q[t]/(p)^*$, $\gamma, \delta \in \mathbb{F}_q[t]/(p)$, $x, y \in \mathbb{F}_q[t]/(p)$ not both zero, and in addition, $f(\gamma, \delta) \not\equiv 0 \pmod{p^2}$.

Finally, let $\mathcal{U} = \bigcap_p \mathcal{U}_p$.

Testing see whether $[f]$ lies in $\mathcal{U}$

Algorithm

Input: A binary cubic form $f = (a, b, c, d)$ *over* $\mathbb{F}_q[t]$.
Output: `true` *if* $[f] \in \mathcal{U}$, `false` *otherwise.*
Algorithm:

1. *If* f *is not primitive, i.e.* $\gcd(a, b, c, d) \neq 1$, *return* `false`.
2. *Put* $P := b^2 - 3ac$, $Q := bc - 9ad$, $R := c^2 - 3bd$, $H_f := (P, Q, R)$, $\ell_H := \gcd(P, Q, R)$, $D := Q^2 - 4PR$ *(so that* $D = -3\,\mathrm{disc}(f)$*).*
3. *If* ℓ_H *is not squarefree, return* `false`.
4. *Put* $s := D/(\ell_H)^2$. *If* $\gcd(s, \ell_H) \neq 1$, *return* `false`
5. *If* s *is squarefree, return* `true`. *Otherwise return* `false`.

Bonus fact: Any form lying in $\mathcal{U}$ is irreducible.

The Algorithm

Algorithm

Input: A prime power q not divisible by 2 or 3, and a positive integer X.
Output: Minimal polynomials for all $\mathbb{F}_q(t)$-isomorphism classes of cubic function fields of imaginary or unusual discriminant D and $|D| \leq X$.
Algorithm:

$\mathtt{for}\ |a| \leq X^{1/4}$
  $\mathtt{for}\ |b| \leq X^{1/4}$
    $\mathtt{for}\ |c| \leq X^{1/2}/|a|$
      $\mathtt{for}\ |d| \leq \max\{|bc|/|a|, |b|^2/|a|q, |c|/q\}$
        $\mathtt{Set}\ f := (a, b, c, d)\mathtt{;}$
        $\mathtt{compute}\ D = \mathrm{disc}(f)\mathtt{;}$
        $\mathtt{if}\ |D| \leq X\ \mathtt{AND}\ [f] \in \mathcal{U}\ \mathtt{AND}\ f\ \mathtt{is\ reduced}$
        $\mathtt{then\ output}\ f(x, 1).$

The Algorithm's complexity

Using the bounds of the previously specified algorithm, it follows that $O(X^{5/4})$ forms need to be checked.

This differs from Belabas' algorithm for cubic number fields.

Note: Despite this, there are some advantages to this algorithm in the function field setting.

- Like Belabas' algorithm, no need for an irreducibility check, no need to factor the discriminant and no need to keep all forms found so far in memory.
- In addition, as we are in the function field setting, testing whether or not some $z(t) \in \mathbb{F}_q[t]$ is squarefree is much easier (gcd computation).

Numerical Results

We implemented a tabulation algorithm for imaginary discriminants using the C++ programming language coupled with the number theory library NTL.

The lists of imaginary cubic function fields over $\mathbb{F}_5$ up to discriminant degree 9 and $\mathbb{F}_7$ up to discriminant degree 7 were computed on a Pentium 4 machine running Linux with 1 GB of RAM.

Degree bound X	# of fields	Elapsed time
3	50	0.06 seconds
5	2050	53.09 sec
7	33290	24 min 21.36 sec
9	1689710	13 days, 1 hour, 31 min 0.78 sec

Table: Cubic Function Fields over $\mathbb{F}_5$ with imaginary Hessian

Numerical Results cont'd

Degree bound X	# of fields	Elapsed time
3	147	0.52 seconds
5	12495	29 min 53.22 sec
7	365421	1 day, 3 hours, 45 min 58.78 sec

Table: Cubic Function Fields over $\mathbb{F}_7$ with imaginary Hessian

Computations for unusual function fields are a work in progress.

Open Problems

Some open problems:

- What if the Hessian of $f = (a, b, c, d)$ is a real form? There doesn't seem to be a way to deal with this at the moment.
- Look at applying asymptotic results to this specific setting to improve complexity results.
- Adapt algorithm to find large 3-ranks of quadratic function fields (work in progress).

Open Problems

Some open problems:

- What if the Hessian of $f = (a, b, c, d)$ is a real form? There doesn't seem to be a way to deal with this at the moment.
- Look at applying asymptotic results to this specific setting to improve complexity results.
- Adapt algorithm to find large 3-ranks of quadratic function fields (work in progress).

Open Problems

Some open problems:

- What if the Hessian of $f = (a, b, c, d)$ is a real form? There doesn't seem to be a way to deal with this at the moment.
- Look at applying asymptotic results to this specific setting to improve complexity results.
- Adapt algorithm to find large 3-ranks of quadratic function fields (work in progress).