

Tabulation of Cubic Function Fields with Imaginary and Unusual Hessian

Pieter Rozenhart and Renate Scheidler

Department of Mathematics and Statistics, University of Calgary,
2500 University Drive NW, Calgary, Alberta, Canada, T2N 1N4
{pieter,rscheidl}@math.ucalgary.ca

Abstract. We give a general method for tabulating all cubic function fields over $\mathbb{F}_q(t)$ whose discriminant D has odd degree, or even degree such that the leading coefficient of $-3D$ is a non-square in \mathbb{F}_q^* , up to a given bound on $|D| = q^{\deg(D)}$. The main theoretical ingredient is a generalization of a theorem of Davenport and Heilbronn to cubic function fields. We present numerical data for cubic function fields over \mathbb{F}_5 and over \mathbb{F}_7 with $\deg(D) \leq 7$ and $\deg(D)$ odd in both cases.

1 Introduction

In 1997, Belabas [2] presented an algorithm for tabulating all non-isomorphic cubic number fields of discriminant D with $|D| \leq X$ for any $X > 0$. The results make use of the reduction theory for binary cubic forms with integral coefficients. A theorem of Davenport and Heilbronn [8] states that there is a discriminant-preserving bijection between \mathbb{Q} -isomorphism classes of cubic number fields of discriminant D and a certain explicitly characterizable set \mathcal{U} of equivalence classes of primitive irreducible integral binary cubic forms of the same discriminant D . Using this one-to-one correspondence, one can enumerate all cubic number fields of discriminant D with $|D| \leq X$ by computing the unique reduced representative $f(x, y)$ of every equivalence class in \mathcal{U} of discriminant D with $|D| \leq X$. The corresponding field is then obtained by simply adjoining a root of the irreducible cubic $f(x, 1)$ to \mathbb{Q} . Belabas' algorithm is essentially linear in X , and performs quite well in practice.

In this paper, we give an extension of the above approach to function fields. That is, we present a method for tabulating all cubic function fields over a fixed finite field up to a given upper bound on the degree of the discriminant, using the theory for binary cubic forms with coefficients in $\mathbb{F}_q[t]$, where \mathbb{F}_q is a finite field with $\text{char}(\mathbb{F}_q) \neq 2, 3$. While some of the ideas of [2] translate essentially directly from number fields to function fields, there are in fact a number of obstructions to a straightforward adaptation of Belabas' algorithm [2] to the function field setting. Firstly, there is a very simple connection between the signatures of cubic and quadratic number fields of the same discriminant D , which are simply characterized as real or complex/imaginary according to whether $D > 0$ or $D < 0$. In cubic function fields, this connection is far more complicated and in some

cases no longer exists, due to the increased level of flexibility in how the place at infinity of $\mathbb{F}_q(t)$ splits in the cubic extension. Secondly, the case of unusual quadratic function fields, where the place at infinity is inert, has no number field analogue. Thirdly, the extensions of the degree map on $\mathbb{F}_q(t)$ to any function field are non-Archimedean valuations, i.e. satisfy the strong triangle inequality $|a + b| \leq \max\{|a|, |b|\}$, whereas the absolute value on any number field is Archimedean, satisfying the ordinary triangle inequality $|a + b| \leq |a| + |b|$. This results in somewhat different bounds on the coefficients of the binary cubic forms that the function field version of the tabulation algorithm uses for its search.

Our main tool is the function field analogue of the Davenport-Heilbronn theorem [8] mentioned above (see [10, 13]). We also make use of the association of any binary cubic form f of discriminant D over $\mathbb{F}_q[t]$ to its Hessian H_f which is a binary quadratic form over $\mathbb{F}_q[t]$ of discriminant $-3D$. Under certain conditions, this association can be exploited to develop a reduction theory for binary cubic forms over $\mathbb{F}_q[t]$ that is analogous to the reduction theory for integral binary cubic forms. Suppose that $\deg(D)$ is odd, i.e. H_f is an imaginary binary quadratic form, or that $\deg(D)$ is even and the leading coefficient of $-3D$ is a non-square in \mathbb{F}_q^* , i.e. H_f is an unusual binary quadratic form. We will establish that under these conditions, the equivalence class of f contains a unique reduced form, i.e. a binary cubic form that satisfies certain normalization conditions and has an associated Hessian that is a reduced binary quadratic form. Thus, equivalence classes of binary cubic forms can be efficiently identified via their unique representatives. This result no longer holds when H_f is a real binary quadratic form, i.e. $\deg(D)$ is even and the leading coefficient of $-3D$ is a square in \mathbb{F}_q^* . In this case, the equivalence class of f contains many — in fact, generally exponentially many — reduced forms, and a different reduction theory needs to be developed. This is the subject of future research.

Our tabulation procedure proceeds analogously to the number field scenario. The function field analogue of the Davenport-Heilbronn theorem states that there is again a discriminant-preserving bijection between $\mathbb{F}_q(t)$ -isomorphism classes of cubic function fields of discriminant $D \in \mathbb{F}_q[t]$ and a certain set \mathcal{U} of primitive irreducible binary cubic forms over $\mathbb{F}_q[t]$ of discriminant D . Hence, in order to list all $\mathbb{F}_q(t)$ -isomorphism classes of cubic function fields up to an upper bound X on $|D|$, it suffices to enumerate the unique reduced representatives of all equivalence classes of binary cubic forms of discriminant D for all $D \in \mathbb{F}_q[t]$ with $|D| = q^{\deg(D)} \leq X$. Bounds on the coefficients of such a reduced form show that there are only finitely many candidates for any reduced form of a fixed discriminant. These bounds can then be employed in nested loops to test whether each form found lies in \mathcal{U} . As mentioned earlier, the coefficient bounds obtained for function fields are different from those used by Belabas for number fields, due to the fact that the degree valuation is non-Archimedean.

This paper is organized as follows. After a brief overview of binary quadratic and cubic forms over $\mathbb{F}_q[t]$ in Section 2, the reduction theory for imaginary and unusual binary cubic forms is developed in Sections 3 and 4, respectively. We present the Davenport-Heilbronn theorem for function fields and an explicit

characterization of the set \mathcal{U} in Section 6. Bounds on the coefficients of a reduced binary cubic form are derived in Section 5. Finally, we present the tabulation algorithm as well as numerical results in Section 7.

2 Binary Quadratic and Cubic Forms over $\mathbb{F}_q[t]$

For a general introduction to algebraic function fields, we refer the reader to Rosen [9] or Stichtenoth [12]. Let \mathbb{F}_q be a finite field of characteristic at least 5, and set $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. 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 $\text{sgn}(H)$ the leading coefficient of H . For $H = 0$, we set $|H| = 0$. This absolute value extends in the obvious way to $\mathbb{F}_q(t)$. Note that in contrast to the absolute value on the rationals, the absolute value on $\mathbb{F}_q(t)$ is non-Archimedean.

Any non-zero $r \in \mathbb{F}_q(t)$ can be written as $r = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 + a_{-1} t^{-1} + \cdots$ with $n \in \mathbb{Z}$ and $a_i \in \mathbb{F}_q$ for $i \leq n$. We set $\lfloor r \rfloor = a_n t^n + \cdots + a_1 t + a_0$ to be the polynomial part of r ; note that $\lfloor r \rfloor = 0$ if $n < 0$. We also set $\lfloor 0 \rfloor = 0$. The function $\lfloor r \rfloor$ is analogous to the floor function for integers.

We give a brief overview of binary quadratic and cubic forms with coefficients in $\mathbb{F}_q[t]$; their reduction theory will be developed in Sections 3 and 4 respectively. Much of this material is completely analogous to the theory for binary cubic forms over the integers.

A *binary quadratic form over $\mathbb{F}_q[t]$* is a homogeneous quadratic polynomial in two variables with coefficients in $\mathbb{F}_q[t]$. If $H(x, y) = Px^2 + Qxy + Ry^2$ is a binary quadratic form over $\mathbb{F}_q[t]$, then we write $H = (P, Q, R)$ for brevity. The *discriminant* of H is the polynomial $\text{disc}(H) = Q^2 - 4PR \in \mathbb{F}_q[t]$. H is said to be *imaginary* if $\deg(\text{disc}(H))$ is odd, *unusual* if $\deg(\text{disc}(H))$ is even and $\text{sgn}(\text{disc}(H))$ is a non-square in \mathbb{F}_q^* , and *real* if $\deg(\text{disc}(H))$ is even and $\text{sgn}(\text{disc}(H))$ is a square in \mathbb{F}_q^* .

A *binary cubic form over $\mathbb{F}_q[t]$* is a homogeneous cubic polynomial in two variables with coefficients in $\mathbb{F}_q[t]$. If $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ is a binary cubic form over $\mathbb{F}_q[t]$, then we write $f = (a, b, c, d)$ for brevity. The *discriminant* of $f = (a, b, c, d)$ is the polynomial

$$\text{disc}(f) = 18abcd + b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 \in \mathbb{F}_q[t] .$$

For the remainder of this paper, we assume that all binary cubic forms $f = (a, b, c, d)$ are *primitive*, i.e. $\gcd(a, b, c, d) = 1$.

Definition 2.1. *Let F be a binary quadratic or cubic form over $\mathbb{F}_q[t]$. If*

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

is a 2×2 matrix with entries in $\mathbb{F}_q[t]$, then the action of M on F is defined by $F \circ M = f(\alpha x + \beta y, \gamma x + \delta y)$.

We obtain an equivalence relation from this action by restricting to matrices $M \in GL_2(\mathbb{F}_q[t])$, the group of 2×2 matrices over $\mathbb{F}_q[t]$ whose determinant lies in \mathbb{F}_q^* . That is, 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 $\alpha\delta - \beta\gamma \in \mathbb{F}_q^*$. Up to associates, equivalent binary forms have the same discriminant. Furthermore, the action of the group $GL_2(\mathbb{F}_q[t])$ on binary forms over $\mathbb{F}_q[t]$ preserves irreducibility over $\mathbb{F}_q(t)$.

As in the case of integral binary cubic forms, any binary cubic form $f = (a, b, c, d)$ over $\mathbb{F}_q[t]$ is closely associated with its *Hessian*

$$H_f(x, y) = -\frac{1}{4} \begin{vmatrix} \frac{\partial^2 f}{\partial x \partial x} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y \partial y} \end{vmatrix} = (P, Q, R) ,$$

where $P = b^2 - 3ac$, $Q = bc - 9ad$, and $R = c^2 - 3bd$. Note that H_f is a binary quadratic form over $\mathbb{F}_q[t]$. The Hessian has a number of useful properties, which are easily verified by direct computation:

Proposition 2.1. *Let $f = (a, b, c, d)$ be a binary cubic form over $\mathbb{F}_q[t]$ with Hessian $H_f = (P, Q, R)$. Then the following are satisfied.*

1. $H_{f \circ M} = (\det M)^2 (H_f \circ M)$ for any $M \in GL_2(\mathbb{F}_q[t])$.
2. $\text{disc}(H_f) = -3 \text{disc}(f)$.

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. By Proposition 2.1, f is imaginary if $\text{disc}(f)$ has odd degree, unusual if $\text{disc}(f)$ has even degree and $-3 \text{sgn}(\text{disc}(f))$ is a non-square in \mathbb{F}_q^* , and real if $\text{disc}(f)$ has even degree and $-3 \text{sgn}(\text{disc}(f))$ is a square in \mathbb{F}_q^* .

For the tabulation of cubic function fields, it will be important to represent equivalence classes of binary cubic forms over $\mathbb{F}_q[t]$ via a unique and efficiently identifiable representative. This can be accomplished via reduction. As in the case of integral forms, reduction of cubic forms is accomplished via reduction of their associated binary quadratic forms. Specifically, in the imaginary and unusual cases, a binary cubic form over $\mathbb{F}_q[t]$ is declared to be reduced essentially if its associated Hessian is reduced and certain normalization conditions are satisfied.

3 Reduction Theory of Imaginary Binary Cubic Forms

We begin with an overview of the reduction theory for imaginary binary quadratic forms over $\mathbb{F}_q[t]$ which can be found in Artin [1]. We then use this theory to develop a reduction theory for imaginary binary cubic forms via their associated Hessians. This theory is quite similar to its counterpart for integral binary forms.

In the case of unusual binary cubic forms, we will proceed in an analogous fashion to the approach for imaginary forms; this is done in Section 4.

An imaginary binary quadratic form $H = (P, Q, R)$ of discriminant $D = \text{disc}(H)$ is said to be *reduced* if $|Q| < |P| \leq |D|^{1/2}$, $\text{sgn}(P) = 1$, and either $Q = 0$ or $\text{sgn}(Q) \in S$, where $S \subset \mathbb{F}_q$ is a set such that if $a \in S$, then $-a \notin S$ and $|S| = (q - 1)/2$. Such a set can always be found. One such choice is as follows: order the non-zero elements of \mathbb{F}_q lexicographically and let S consist of the first $(q - 1)/2$ elements. If $q = p$ is a prime, this is simply the set $\{1, 2, \dots, (p - 1)/2\}$. Note that since $\deg(D)$ is odd, the exponent in $\sqrt{|D|} = q^{\deg(D)/2}$ is a half integer, so the second inequality is in fact equivalent to the strict inequality $|P| < \sqrt{|D|}$. Note also that in contrast to integral binary quadratic forms, the only matrices $M \in GL_2(\mathbb{F}_q[t])$ whose action on H leaves H unchanged are the identity matrix, its negative and $\pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ when $Q = 0$ (see [1]).

The algorithm for reducing a binary quadratic form over $\mathbb{F}_q[t]$ is almost the same as for integral imaginary binary quadratic forms. If $H = (P, Q, R)$ with $|Q| \geq |P|$, then compute $s = \lfloor -Q/2P \rfloor$ and apply the matrix

$$T = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_q[t])$$

to H to obtain a new form $H_1(x, y) = H(x + sy, y) = (P_1, Q_1, R_1)$ equivalent to H . Now the inequality $|Q_1| < |P_1|$ is satisfied. If $|P_1| > |D|^{1/2}$, then apply the matrix

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{F}_q[t])$$

to H_1 to obtain the equivalent form $H_2(x, y) = H_1(-y, x) = (P_2, Q_2, R_2)$ with $(P_2, Q_2, R_2) = (R_1, -Q_1, P_1)$. If as a result of this last transformation, the condition $|Q_2| < |P_2|$ is not satisfied, then we repeat this procedure from the beginning with $H = H_2 = (P_2, Q_2, R_2)$. Since P_i, Q_i, R_i are polynomials in $\mathbb{F}_q[t]$, the process must eventually terminate after a finite number of steps, as we reduce the degree of P_i at each step.

Now suppose $H_j = (P_j, Q_j, R_j)$ satisfies $|Q_j| < |P_j| \leq \sqrt{|D|}$ for some j . To obtain the condition $\text{sgn}(P_j) = 1$, we apply

$$N = \begin{pmatrix} 1 & 0 \\ 0 & \nu \end{pmatrix} \in GL_2(\mathbb{F}_q[t])$$

to H_j , where $\nu \in \mathbb{F}_q^*$ is chosen appropriately. It follows from the above reduction procedure that every imaginary binary quadratic form over $\mathbb{F}_q[t]$ is equivalent to a unique reduced quadratic form, see [1].

Now let $f = (a, b, c, d)$ be an imaginary binary cubic form over $\mathbb{F}_q[t]$ of discriminant $D = \text{disc}(f)$ with (imaginary) Hessian $H_f = (P, Q, R)$. Then f is said to be *reduced* if H_f is reduced, $\text{sgn}(a) = 1$ and if $Q = 0$, then $\text{sgn}(d) \in S$, where $S \subset \mathbb{F}_q$ as described above. Equivalently, by Proposition 2.1, f is reduced if

$$|Q| < |P| \leq |D|^{1/2}, \quad \text{sgn}(P) = 1, \quad \text{sgn}(a) = 1, \quad \text{sgn}(Q) \in S \text{ or } \text{sgn}(d) \in S,$$

depending on whether or not $Q = 0$. Analogous to [2], one can deduce that any two equivalent reduced imaginary forms are equal, so equivalence classes of such forms can be efficiently identified by their unique reduced representative.

Theorem 3.1.

1. Every equivalence class of imaginary binary cubic forms over $\mathbb{F}_q[t]$ has a unique reduced representative.
2. Every imaginary binary cubic form over $\mathbb{F}_q[t]$ is equivalent to a unique reduced binary cubic form.

4 Reduction Theory of Unusual Binary Cubic Forms

As in the previous section, we first outline reduction for unusual binary quadratic forms over $\mathbb{F}_q[t]$ and then apply this theory to unusual binary cubic forms over $\mathbb{F}_q[t]$. Both the reduction theory and the algorithm for the unusual case are almost identical to that of imaginary forms, with one crucial difference: the analogous definition of reducedness does not lead to a unique reduced representative in each equivalence class, but instead to $q+1$ equivalent reduced forms. To achieve uniqueness, a distinguished representative among these $q+1$ equivalent forms will need to be identified.

Again, the reduction theory for unusual binary quadratic forms over $\mathbb{F}_q[t]$ goes back to Artin [1]. An unusual binary quadratic form $H = (P, Q, R)$ of discriminant $D = \text{disc}(H)$ is said to be *reduced* if $|Q| < |P| \leq \sqrt{|D|}$ and $\text{sgn}(P) = 1$. At first glance, this definition looks exactly like the definition of a reduced imaginary binary quadratic form. However, the crucial difference is that here, the exponent in $\sqrt{|D|} = q^{\deg(D)/2}$ is an integer, whereas in the imaginary scenario, it was a half integer. So here, equality $|P| = \sqrt{|D|}$ can in fact be achieved. The algorithm for reducing an unusual binary quadratic form is the same as for imaginary binary quadratic forms, so every unusual binary quadratic form is equivalent to a reduced form.

Unusual reduced binary quadratic forms $H = (P, Q, R)$ with $|P| < \sqrt{|D|}$ behave exactly like reduced imaginary binary quadratic forms. However, if $H = (P, Q, R)$ is an unusual reduced binary quadratic form with $|P| = \sqrt{|D|}$, then so is $H_\alpha = (P_\alpha, Q_\alpha, R_\alpha)$ for all $\alpha \in \mathbb{F}_q$, where

$$H_\alpha = H \circ \left(\frac{1}{\mu_\alpha} \begin{pmatrix} \alpha & \text{sgn}(D) \\ 4 & \alpha \end{pmatrix} \right) = H \left(\frac{\alpha}{\mu_\alpha} x + \frac{\text{sgn}(D)}{\mu_\alpha} y, \frac{4}{\mu_\alpha} x + \frac{\alpha}{\mu_\alpha} y \right),$$

with $\alpha \in \mathbb{F}_q$ and $\mu_\alpha = \alpha^2 - 4 \text{sgn}(D)$. Note that $\mu_\alpha \neq 0$ for all $\alpha \in \mathbb{F}_q$, since $\text{sgn}(D)$ is a non-square in \mathbb{F}_q^* . Hence, we have a family of $q+1$ equivalent reduced unusual binary quadratic forms when $|P| = \sqrt{|D|}$. These $q+1$ forms can be sorted according to lexicographical order in $\mathbb{F}_q[t]$ of their x^2 -coefficients. To identify a unique representative in the class of H , one selects the form $H' = (P', Q', R') \in \{H, H_\alpha\}_{\alpha \in \mathbb{F}_q}$ so that P' is minimal in terms of lexicographical order in $\mathbb{F}_q[t]$ amongst $\{P, P_\alpha\}_{\alpha \in \mathbb{F}_q}$. We call the form H' *distinguished*. Thus,

to find such a representative, it is necessary to execute the reduction algorithm described in Section 3 and then computing the q forms H_α , $\alpha \in \mathbb{F}_q$. This is slower than reduction for imaginary binary quadratic forms, especially for large values of q .

Now let $f = (a, b, c, d)$ be an unusual binary cubic form over $\mathbb{F}_q[t]$ of discriminant $D = \text{disc}(f)$ with (unusual) Hessian $H_f = (P, Q, R)$. Then f is said to be *reduced* if H_f is reduced, H_f is distinguished if $|P| = \sqrt{|D|}$, $\text{sgn}(a) = 1$ and either $Q = 0$ or $\text{sgn}(Q) \in S$, where $S \subset \mathbb{F}_q$ is a set such that if $a \in S$, then $-a \notin S$ and $|S| = (q-1)/2$. Equivalently, by Proposition 2.1, f is reduced if

$|Q| < |P| \leq |D|^{1/2}$, $\text{sgn}(P) = 1$, $\text{sgn}(a) = 1$, $\text{sgn}(Q) \in S$ or if $Q = 0$ then $\text{sgn}(d) \in S$, where S is as described above,
if $|P| = \sqrt{|D|}$, then P is lexicographically minimal in the set $\{\tilde{P} \mid \tilde{H} = (\tilde{P}, \tilde{Q}, \tilde{R}) \text{ is a reduced form equivalent to } H\}$.

Analogous to the imaginary case, we again obtain

Theorem 4.1.

1. Every equivalence class of unusual binary cubic forms over $\mathbb{F}_q[t]$ has a unique reduced representative.
2. Every unusual binary cubic form over $\mathbb{F}_q[t]$ is equivalent to a unique reduced binary cubic form.

5 Bounds on Reduced Binary Cubic Forms

For our tabulation algorithm, we will need to search over all candidates for reduced imaginary or unusual binary cubic forms $f = (a, b, c, d)$ of discriminant D where $|D|$ is bounded above by some given bound X . It then remains to test via Algorithm 6.4 whether such a reduced form lies in the Davenport-Heilbronn set \mathcal{U} defined in Section 6 below. If this is the case, then the reduced form corresponds to a triple of $\mathbb{F}_q(t)$ -isomorphic cubic function fields.

In order to establish that this set of candidates for reduced forms of discriminant D of absolute value at most X is in fact finite, and to ensure that the search procedure is as efficient as possible, we develop good bounds on the absolute values of the coefficients a, b, c, d of an imaginary or unusual reduced binary cubic form in terms of the absolute value of D . The following inequality appears in Cremona [5] and is easily verified by straightforward computation.

Lemma 5.1. $f = (a, b, c, d)$ be a binary cubic form over $\mathbb{F}_q[t]$ of discriminant D and Hessian $H_f = (P, Q, R)$, where we recall that $P = b^2 - 3ac$. Set $U = 2b^3 + 27a^2d - 9abc$. Then $4P^3 = U^2 + 27a^2D$.

The above identity can be used to establish degree bounds on the coefficients of an imaginary or unusual reduced binary cubic form over $\mathbb{F}_q[t]$ in terms of the degree of its discriminant.

Proposition 5.2. *Let $f = (a, b, c, d)$ be an imaginary or unusual binary cubic form over $\mathbb{F}_q[t]$ of discriminant D , and set $P = b^2 - 3ac$ and $U = 2b^3 + 27a^2d - 9abc$. Then $|U|^2 \leq |P|^3$.*

Proof. By Lemma 5.1, we have

$$4P^3 = U^2 + 27a^2D = U^2 - (-3D)(9a)^2 . \quad (5.1)$$

Now $|P|^3 < |U|^2$ if and only if the leading terms of the polynomials U^2 and $(-3D)(9a)^2$ in the right hand side of (5.1) cancel, which is the case if and only if $\deg(U^2) = \deg((-3D)(9a)^2)$ and $\text{sgn}(U^2) = \text{sgn}((-3D)(9a)^2)$. The first of these two equalities implies that $\deg(D)$ is even, and the second one forces $\text{sgn}(-3D)$ to be a square in \mathbb{F}_q^* , which would imply that H_f is a real binary quadratic form, a contradiction.

We can now derive our desired degree bounds for imaginary or unusual reduced binary cubic forms.

Corollary 5.3. *Let $f = (a, b, c, d)$ be a reduced imaginary or unusual binary cubic form over $\mathbb{F}_q[t]$ of discriminant D . Then*

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

Proof. Let $H_f = (P, Q, R)$ be the Hessian of f . Then $P = b^2 - 3ac$ and $|Q| < |P| \leq \sqrt{|D|}$. Set $U = 2b^3 + 27a^2d - 9abc$. Then $4P^3 = U^2 + 27a^2D$ by Lemma 5.1, and $|U|^2 \leq |P|^3$ by Proposition 5.2. It follows that

$$|a^2D| = |4P^3 - U^2| \leq \max\{|P|^3, |U|^2\} \leq |P|^3 \leq |D|^{3/2} ,$$

and hence $|a| \leq |D|^{1/4}$.

A straightforward computation shows that $U = 2bP - 3aQ$. Hence,

$$|bP| = |U + 3aQ| \leq \max\{|U|, |aQ|\} \leq \max\{|P|^{3/2}, |a||P|\} ,$$

so $|b| \leq \max\{|P|^{1/2}, |a|\} \leq |D|^{1/4}$.

To obtain the upper bound for c , we observe that $3ac = b^2 - P$, so

$$|ac| \leq \max\{|b|^2, |P|\} \leq |D|^{1/2} ,$$

and hence $|c| \leq |D|^{1/2}/|a|$. Finally, $Q = bc - 9ad$, $P = b^2 - 3ac$, and $|Q| \leq |P|/q$ imply

$$\begin{aligned} |d| &= |bc - Q|/|a| \leq \max\{|bc/a|, |Q|/|a|\} \leq \max\{|bc/a|, |P|/|a|q\} \\ &= \max\{|bc/a|, |b^2 - 3ac|/|a|q\} \leq \max\{|bc|/|a|, |b|^2/|a|q, |c|/q\} . \end{aligned}$$

This concludes the proof.

The bounds for a and b are essentially of the same order of magnitude as the corresponding bounds for integral imaginary binary cubic forms. However, the bounds for c and d are different.

Corollary 5.4. *For any fixed discriminant D in $\mathbb{F}_q[t]$, there are only finitely many imaginary and unusual reduced binary cubic forms over $\mathbb{F}_q[t]$ of discriminant D .*

6 The Davenport-Heilbronn Theorem

Recall that the Davenport-Heilbronn theorem [8] states that there is a discriminant-preserving bijection from a certain set \mathcal{U} of equivalence classes of integral binary cubic forms of discriminant D to the set of \mathbb{Q} -isomorphism classes of cubic fields of the same discriminant D . Therefore, if one can compute the unique reduced representative f of any class of forms in \mathcal{U} of discriminant D with $|D| < X$, then this leads to a list of minimal polynomials $f(x, 1)$ for all cubic fields of discriminant D with $|D| \leq X$.

The situation for cubic function fields is completely analogous. We now describe the Davenport-Heilbronn set \mathcal{U} for function fields, state the function field version of the Davenport-Heilbronn theorem, and provide a fast algorithm for testing membership in \mathcal{U} that is in fact more efficient than its counterpart for integral forms.

For brevity, we let $[f]$ denote the equivalence class of any primitive binary cubic form f over $\mathbb{F}_q[t]$. Fix any irreducible polynomial $p \in \mathbb{F}_q[t]$. We define \mathcal{V}_p to be the set of all equivalence classes $[f]$ of binary cubic forms such that $p^2 \nmid \text{disc}(f)$. In other words, if $\text{disc}(f) = i^2 \Delta$ where Δ is squarefree, then $f \in \mathcal{V}_p$ if and only if $p \nmid i$. Hence, $f \in \bigcap_p \mathcal{V}_p$ if and only if $\text{disc}(f)$ is squarefree.

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

- either $[f] \in \mathcal{V}_p$, 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, $f(\gamma, \delta) \not\equiv 0 \pmod{p^2}$.

For brevity, we summarize the condition $f(x, y) \equiv \lambda(\delta x - \gamma y)^3 \pmod{p(t)}$ for some $\gamma, \delta \in \mathbb{F}_q[t]/(p)$ and $\lambda \in \mathbb{F}_q[t]/(p)^*$ with the notation $(f, p) = (1^3)$ as was done in [7, 8].

Finally, we set $\mathcal{U} = \bigcap_p \mathcal{U}_p$; this is the set under consideration in the Davenport-Heilbronn theorem for function fields. The version given below appears in [10]. A more general version of this theorem for Dedekind domains appears in Taniguchi [13].

Theorem 6.1. *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 \mathcal{U} .*

In order to convert Theorem 6.1 into an algorithm, we require a fast method for testing membership in the set \mathcal{U} . This is aided by the following efficiently testable conditions:

Proposition 6.2. *Let $f = (a, b, c, d)$ be a binary cubic form over $\mathbb{F}_q[t]$ with Hessian $H_f = (P, Q, R)$. Let $p \in \mathbb{F}_q[t]$ be irreducible. Then the following hold:*

1. $(f, p) = (1^3)$ if and only if $p \mid \gcd(P, Q, R)$.
2. If $(f, p) = (1^3)$ then $f \in \mathcal{U}_p$ if and only if $p^3 \nmid \text{disc}(f)$.

In addition, classes in \mathcal{U} contain only irreducible forms; this result can be found for integral cubic forms in [4] and is completely analogous for forms over $\mathbb{F}_q[t]$. In other words, by Theorem 6.1, if $[f] \in \mathcal{U}$, then $f(x, 1)$ is the minimal polynomial of a cubic function field over $\mathbb{F}_q(t)$. This useful fact eliminates the necessity for a potentially costly irreducibility test when testing membership in \mathcal{U} .

Theorem 6.3. *Any binary cubic form whose equivalence class belongs to \mathcal{U} is irreducible.*

Using Proposition 6.2, we can now formulate an algorithm for testing membership in \mathcal{U} . This algorithm will be used in our tabulation routines for cubic function fields.

Algorithm 6.4.

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, 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 $D = -3 \operatorname{disc}(f)$).
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**.

Proposition 6.5. *Algorithm 6.4 is correct.*

Proof. Step 1 is correct, as \mathcal{U} only contains classes of primitive forms by definition. If $p^2 \mid \ell_H$, then $p^4 \mid D$. If $p \mid \ell_H$ and $p \mid s$, then $p^3 \mid D$. In both cases, it follows that $p^3 \mid \operatorname{disc}(f)$, so $[f] \notin \mathcal{U}_p$, and hence $[f] \notin \mathcal{U}$, by part 2 of Proposition 6.2. This proves the correctness of steps 3 and 4.

Assume now that f passes steps 1-4, so $p^2 \nmid \ell_H$ and $p \mid \gcd(s, \ell_H)$ for some irreducible polynomial $p \in \mathbb{F}_q[t]$. Then s is not squarefree if and only if there exists an irreducible polynomial $z \in \mathbb{F}_q[t]$ with $z^2 \mid s$ and hence $z \nmid \ell_H$. By part 1 of Proposition 6.2, this rules out $(f, z) = (1^3)$. On the other hand, we also have $z^2 \mid \operatorname{disc}(f)$, so $f \notin \mathcal{V}_z$, and hence $f \notin \mathcal{U}_z$, by steps 3 and 4 above. Thus, s is squarefree if and only if $[f] \in \mathcal{U}_p$ for all p , or equivalently, $[f] \in \mathcal{U}$, proving the validity of step 5.

Note that steps 3 and 5 of Algorithm 6.4 require tests for whether a polynomial $F \in \mathbb{F}_q[t]$ is squarefree. This can be accomplished very efficiently with a simple gcd computation, namely by checking whether $\gcd(F, F') = 1$, where F' denotes the formal derivative of F with respect to t . This is in contrast to the integral case, where squarefree testing of integers is generally difficult; in fact, squarefree factorization of integers is just as difficult as complete factorization. Hence, the membership test for \mathcal{U} is more efficient than its counterpart for integral forms.

7 Tabulation Algorithm and Numerical Results

We now describe the tabulation algorithms for cubic function fields corresponding to imaginary and unusual reduced binary cubic forms over $\mathbb{F}_q[t]$; that is, cubic extensions of $\mathbb{F}_q(t)$ of discriminant D where $\deg(D)$ is odd, or $\deg(D)$ is even and $\text{sgn}(-3D)$ is a non-square in \mathbb{F}_q^* , respectively.

The idea of both algorithms is as follows. Input a prime power q coprime to 6 and a bound $X \in \mathbb{N}$. The first algorithm outputs minimal polynomials for all $\mathbb{F}_q(t)$ -isomorphism classes of cubic extension of $\mathbb{F}_q(t)$ of discriminant D such that $\deg(D)$ is odd and $|D| \leq X$. For the second algorithm, the output is analogous, except that all the discriminants D satisfy $\deg(D)$ even, $\text{sgn}(-3D)$ is a non-square in \mathbb{F}_q^* , and again $|D| \leq X$. Both algorithms search through all coefficient 4-tuples (a, b, c, d) that satisfy the degree bounds of Corollary 5.3 with $|D|$ replaced by X such that the form $f = (a, b, c, d)$ satisfies the following conditions:

1. f is reduced;
2. f is imaginary, respectively, unusual;
3. f belongs to an equivalence class in \mathcal{U} ;
4. f has a discriminant D whose degree is bounded above by X .

If f passes all these tests, the algorithm outputs $f(x, 1)$ which by Theorem 6.1 is the minimal polynomial of a triple of $\mathbb{F}_q(t)$ -isomorphic cubic function fields of discriminant D .

Algorithm 7.1.

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 discriminant D with $\deg(D)$ odd and $|D| \leq X$.

Algorithm:

```

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

```

Each loop of the form “for $|f| \leq M$ ” runs through all polynomials $f \in \mathbb{F}_q[t]$ with $\deg(f) = 0, 1, \dots, \log_q(M)$. The algorithm for unusual forms (Algorithm 7.2) is completely analogous, except that the test of whether or not f is reduced in Algorithm 7.2 is more involved. Recall that if $H_f = (P, Q, R)$ is the Hessian of f and $|P| = \sqrt{|D|}$, then this test requires the computation and sorting of $q + 1$ reduced binary quadratic forms equivalent to H_f . This makes Algorithm 7.2 a good deal slower than Algorithm 7.1.

Algorithm 7.2.

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 discriminant D with $\deg(D)$ is even, $\text{sgn}(-3D)$ is a non-square in \mathbb{F}_q^* , and $|D| \leq X$.

Algorithm:

```

for  $|a| \leq X^{1/4}$ 
  for  $|b| \leq X^{1/4}$ 
    for  $|c| \leq X^{1/2}/|a|$ 
      for  $|d| \leq \max\{|bc|/|a|, |b|^2/|a|q, |c|/q\}$ 
        Set  $f := (a, b, c, d)$ ;
        compute  $D = \text{disc}(f)$ ;
        if  $\deg(D)$  is even AND  $\text{sgn}(-3D)$  is not a square in  $\mathbb{F}_q$  AND
            $|D| \leq X$  AND  $[f] \in \mathcal{U}$  AND  $f$  is reduced
          then output  $f(x, 1)$ .

```

The algorithms presented here have some of the same advantages as Belabas' algorithm [2]. In particular, there is no need to check for irreducibility of binary cubic forms lying in \mathcal{U} , no need to factor the discriminant, and no need to keep all fields found so far in memory. Our algorithm has the additional advantage that there is no overhead computation needed for using a sieve to compute numbers that are not squarefree, since by the remarks following Algorithm 6.4, we need only perform a gcd computation of a polynomial and its formal derivative. There is an additional bottleneck for Algorithm 7.2, namely the computation of additional Hessians and subsequently finding the smallest one in terms of lexicographical ordering in $\mathbb{F}_q[t]$.

The following tables present the results of our computations for cubic function fields with imaginary Hessian for $q = 5, 7$ for various degrees. In the interests of space, we only include our computational results on imaginary forms. We implemented the tabulation algorithm using the C++ programming language coupled with the number theory library NTL [11]. The lists of cubic function fields were computed on a 3 GHz 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

Table 1. Cubic Function Fields over \mathbb{F}_5 with imaginary Hessian

In [2], Belabas derived essentially the same bounds on the coefficients a and b as ours, i.e. $O(X^{1/4})$. However, his bounds on c and d are different and were obtained using analytic methods that do not seem to have an obvious analogue

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 2. Cubic Function Fields over \mathbb{F}_7 with imaginary Hessian

in function fields. Using the bounds of Corollary 5.3, it is possible to show that $O(X^{5/4})$ forms need to be checked. Belabas obtained a quasi-linear complexity for his algorithm for tabulating cubic number fields, using the fact that the number of reduced binary cubic forms of discriminant up to $|X|$ is $O(|X|)$, see Theorem 3.7 of [4]. For function fields, we have no such asymptotic available, but we conjecture an analogous complexity of $O(X)$; this is a subject of future research.

8 Conclusions and Future Work

This paper presented a method for computing all cubic function fields with imaginary and unusual Hessian. We computed all cubic function fields with imaginary Hessian up to $|D| \leq q^7$ for $q = 5, 7$.

An immediate question is how to obtain a more exact complexity analysis of Algorithms 7.1 and 7.2; in particular whether the bound of $O(X^{5/4})$ on the number of forms searched can be improved to $O(|X|^{1+\epsilon})$, as in the case of Belabas' algorithm. In addition, a method for finding a distinguished representative in each class of reduced unusual cubic forms that is more efficient than brute force exhaustive search would significantly improve the performance of Algorithm 7.2.

We intend to extend our computations to function fields whose associated binary cubic form is unusual, and to larger values of q and $\deg(D)$. We also hope to derive an algorithm analogous to Algorithms 7.1 and 7.2 for cubic function fields where the associated binary cubic form is real. It is unclear how to develop a reduction theory for binary cubic forms with real Hessian that guarantees a unique reduced cubic form in each equivalence class. Achieving this goal via the Hessian of the cubic form is impossible, since this Hessian is a real binary quadratic form. It well-known that the number of real reduced binary quadratic forms in each equivalence class of discriminant D is of order $\sqrt{|D|}$, i.e. exponential in the size of the discriminant.

In addition, we plan to apply our methods to the task of finding quadratic function fields with large 3-rank, in a similar way to Belabas' method [3] for number fields.

Finally, recall that a cubic function field can have 5 different signatures at infinity, whereas a cubic number field can only have 2 (three real roots or one real root and two non-real complex roots, according to whether the discriminant is positive or negative). For some of the possible signatures of a cubic function field of a given discriminant, it is unclear how they relate to the signature of the

quadratic function field of the same discriminant. For cubic fields that are not totally ramified at infinity, it is possible to establish the connection between the cubic and the quadratic signature through the Hilbert class field. If the place at infinity is totally ramified, the situation is unclear. It would also be interesting to analyze density results like those of [6] according to the signature of a cubic function field or of the underlying quadratic field. Such density results are the subject of future investigation.

References

1. E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen I, *Math. Zeitschrift* **19** (1924), 153-206.
2. K. Belabas, A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997), no. 219, 1213-1237.
3. K. Belabas, On quadratic fields with large 3-rank, *Math. Comp.* **73** (2004), no. 248, 2061-2074.
4. H. Cohen, *Advanced Topics in Computational Number Theory*, Springer-Verlag, New York, 2000.
5. J.E. Cremona, Reduction of binary cubic and quartic forms, *LMS J. Comput. Math.* **2** (1999), 62-92.
6. B. Datskovsky and D.J. Wright, Density of discriminants of cubic extensions, *J. reine angew. Math.* **386** (1988), 116-138.
7. H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields I, *Bull. London Math. Soc.* **1** (1969), 345-348.
8. H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Royal Soc. London A* **322** (1971), 405-420.
9. M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York, 2002.
10. P. Rozenhart, *Fast Tabulation of Cubic Function Fields*, Ph.D. Thesis, University of Calgary, in progress.
11. V. Shoup, *NTL: A Library for Doing Number Theory*, Software, 2001, see <http://www.shoup.net/ntl>.
12. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, New York, 1993.
13. T. Taniguchi, "Distributions of discriminants of cubic algebras", Preprint, Available from <http://arxiv.org/abs/math.NT/0606109> (2006).