THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Constructing and tabulating dihedral function fields

Colin Weir, Renate Scheidler, and Everett W. Howe

msp

THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.557

Constructing and tabulating dihedral function fields

Colin Weir, Renate Scheidler, and Everett W. Howe

We present algorithms for constructing and tabulating degree-ℓ dihedral extensions of $\mathbb{F}_q(x)$, where $q \equiv 1 \bmod 2\ell$. We begin with a Kummer-theoretic algorithm for constructing these function fields with prescribed ramification and fixed quadratic resolvent field. This algorithm is based on the proof of our main theorem, which gives an exact count for such fields. We then use this construction method in a tabulation algorithm to construct all degree-ℓ dihedral extensions of $\mathbb{F}_q(x)$ up to a given discriminant bound, and we present tabulation data. We also give a formula for the number of degree-ℓ dihedral extensions of $\mathbb{F}_q(x)$ with discriminant divisor of degree $2(\ell-1)$, the minimum possible.

1. Introduction

Two important problems in algebraic and algorithmic number theory are the construction of global fields of a fixed discriminant or prescribed ramification — with its curve analogue of constructing Galois covers of fixed genus — and the tabulation of global fields with a certain Galois group up to some discriminant or genus bound. The latter problem goes hand in hand with asymptotic estimates for the number of such fields; for example, estimates for cubic number fields were first given in [11] and for quartics in [2]. There is a sizable body of literature on construction, tabulation, and asymptotic counts of number fields; a comprehensive survey of known results can be found in [6], and extensive tables of data are available at [19].

Far less is known in the function field setting; only the asymptotic counts for cubic [10] and abelian [39] extensions have been proved. However, there is a general program described by Ellenberg and Venkatesh [37] for formulating these asymptotic estimates for both number fields and function fields. In particular, they point out the "alarming gap between theory and experiment" in asymptotic predictions for number fields. In the case of cubic number fields, this inconsistency led

MSC2010: primary 11R58; secondary 11Y40.
Keywords: function field, Galois group, dihedral extension, construction, tabulation.

Roberts [23] to conjecture the secondary term in the theorem of Davenport and Heilbronn in [11]. His conjecture was later proved independently by Bhargava, Shankar, and Tsimerman [3] and by Taniguchi and Thorne [35]. In the function field setting, however, there is practically no experimental data to potentially identify a similar such gap. The only known algorithm for constructing all cubic function fields with a given squarefree discriminant is that of [18], although recently Pohst [22] showed how to construct all non-Galois cubic extensions of $\mathbb{F}_q(x)$ with a given discriminant, which also leads to such an algorithm. Tabulation methods for certain classes of cubic function fields can be found in [26] and [25].

This paper represents a next step toward function field tabulation. We present a method for constructing all degree-ℓ extensions of $\mathbb{F}_q(x)$ with prescribed ramification and with Galois group isomorphic to the dihedral group of order 2ℓ, in the case where $q \equiv 1 \bmod 2\ell$. We use a Kummer-theoretic approach inspired by the methods of Cohen [7; 8] for number fields. This construction method can be converted into a tabulation algorithm in the usual manner via iteration. However, we are able to use the automorphism group $\mathrm{PGL}(2,q)$ of $\mathbb{F}_q(x)$ to effect significant improvements. Note that this technique is unique to the function field setting, as there are no nontrivial automorphisms of the rational numbers. Exploiting $\mathbb{F}_q(x)$-automorphisms reduces the number of constructions by a factor of order q^3 compared to the naïve approach. We present our improved tabulation procedure along with numerical data obtained from an implementation in Magma [5]. It is important to note that in the special case $\ell = 3$, our algorithm generates complete tables of non-Galois cubic function fields over $\mathbb{F}_q(x)$ up to a given discriminant bound.

2. Preliminaries

Let ℓ be an odd prime and let $\mathbb{F}_q$ be a finite field of characteristic coprime to 2ℓ. We denote by K the rational function field over $\mathbb{F}_q$ and by K^{sep} a separable closure of K. In this paper, a *function field* will always mean a subfield L of K^{sep} that contains K as a subfield of finite index, and by the *Galois group* of L we mean the Galois group of its Galois closure over K.

Suppose F/E is a finite extension of functions fields. Let $\mathrm{Places}(F)$ denote the set of places of F, and let $e(P'|P)$ and $f(P'|P)$ denote the ramification index and relative degree of a place $P' \in \mathrm{Places}(F)$ lying over $P \in \mathrm{Places}(E)$, respectively. The *norm* of a place $P' \in \mathrm{Places}(F)$ is the divisor

$$\mathrm{N}_{F/E}(P') := f(P' \mid P)\, P,$$

and the *conorm* of $P \in \mathrm{Places}(E)$ is

$$\mathrm{Con}_{F/E}(P) := \sum_{P' \mid P} e(P' \mid P)\, P'.$$

Then $\mathrm{N}_{F/E}(\mathrm{Con}_{F/E}(P)) = [F : E]\,P$. These definitions extend additively to divisors. We will also use $\mathrm{N}_{F/E}$ to denote the norm map on elements of F. Proposition 7.8 in [24] shows that this is reasonable: The norm of a principal divisor (α) of F is the principal divisor $(\mathrm{N}_{F/E}(\alpha))$ of E. Restricting to the cases where the characteristic is different from 2 and ℓ guarantees that for the field extensions we will consider, there are no wildly ramified places. Thus, for the extensions F/E we will work with, the *different* is given by

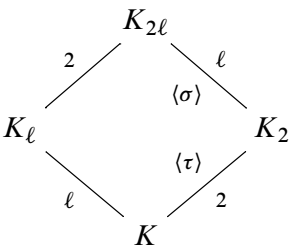
$$\mathrm{Diff}_{F/E} := \sum_{P \in \mathrm{Places}(E)} \sum_{P' \mid P} (e(P' \mid P) - 1)\, P'.$$

The *discriminant divisor* of F/E is defined as

$$\Delta_{F/E} := \mathrm{N}_{F/E}(\mathrm{Diff}_{F/E}) = \sum_{P \in \mathrm{Places}(E)} \sum_{P' \mid P} (e(P' \mid P) - 1) f(P' \mid P)\, P.$$

When $E = K$, we drop E from the notation and simply write Δ_F. Note that $\deg \Delta_{F/E} = \deg \mathrm{Diff}_{F/E}$, so one can replace $\mathrm{Diff}_{F/E}$ by $\Delta_{F/E}$ in the Hurwitz genus formula ([32, Theorem 3.4.13]). For these reasons, we will henceforth describe the ramification of a function field in terms of its discriminant divisor.

Let K_ℓ be a degree-ℓ function field with Galois group $\mathcal{D}_\ell$, the dihedral group with 2ℓ elements, and construct the dihedral extension $K_{2\ell}$ as the Galois closure of K_ℓ over K:



(1)

Here K_2 is the fixed field of the unique index-2 subgroup $\mathcal{C}_\ell$ of $\mathcal{D}_\ell$ and K_ℓ is the fixed field of an element of order 2 in $\mathcal{D}_\ell$. We note that there are ℓ such elements in $\mathcal{D}_\ell$, which give ℓ subfields of $K_{2\ell}$ conjugate to K_ℓ. The field K_2 is called the *quadratic resolvent field* of K_ℓ; we write $K_2 = \mathrm{QuadRes}\, K_\ell$. We let τ denote a generator of $\mathrm{Gal}(K_2/K)$ and σ a generator of $\mathrm{Gal}(K_{2\ell}/K_2)$.

3. Description of all degree-ℓ dihedral function fields

Our first goal is to count the number of ℓ-tuples of conjugate dihedral degree-ℓ function fields with a given discriminant divisor and quadratic resolvent field. There is a one-to-one correspondence between nonconjugate dihedral degree-ℓ function

fields K_ℓ and their Galois closures $K_{2\ell}$. Consequently, instead of counting degree-ℓ dihedral extensions, we count the number of dihedral Galois fields $K_{2\ell}$. We do so via construction: Given a quadratic function field K_2 and discriminant divisor Δ, we construct all degree-ℓ cyclic extensions $K_{2\ell}$ of K_2 such that $\mathrm{Gal}(K_{2\ell}/K) = \mathcal{D}_\ell$ and all conjugate index-2 subfields K_ℓ of $K_{2\ell}$ have discriminant divisor $\Delta_{K_\ell} = \Delta$.

Since $q \equiv 1 \bmod \ell$, all cyclic ℓ-extensions of K_2 are Kummer extensions — that is, extensions of the form $K_2(\sqrt[\ell]{\alpha})$ for some $\alpha \in K_2^\times \setminus (K_2^\times)^\ell$. In Section 3A we give necessary and sufficient conditions on α for $K_2(\sqrt[\ell]{\alpha})$ to be Galois over K with group $\mathcal{D}_\ell$. In Section 3B, we use virtual units to decompose $K_2^\times/(K_2^\times)^\ell$ in a way that allows us to determine the elements α that correspond to nonisomorphic dihedral function fields. With this information, in Section 3C we compute the discriminant divisor of $K_\ell \subset K_2(\sqrt[\ell]{\alpha})$ in terms of (α) and Δ_{K_2}. Next, in Section 3D we give a constructive proof of the main theorem: an exact count of the number of nonconjugate dihedral degree-ℓ extensions of K with a given quadratic resolvent field K_2 and discriminant divisor. We close in Section 3E by showing how to give explicit equations for the function fields we construct.

3A. *Kummer theory.* Let ℓ be a prime and let F be a field that contains the ℓ-th roots of unity. A *degree-ℓ Kummer extension* of F is an extension of the form $F(\theta)$, where θ^ℓ is an element of $F \setminus F^\ell$.

Theorem 3.1 (See [38, Theorem 5.8.5, Proposition 5.8.7, and Theorem 5.8.12]). *Let ℓ be a prime and let F be a field that contains the ℓ-th roots of unity.*

(1) *Let $F' = F(\theta)$ be a Kummer extension of F, with $\theta^\ell = \alpha \in F \setminus F^\ell$. Then the minimal polynomial of θ is $T^\ell - \alpha$, and F' is a degree-ℓ Galois extension of F.*

(2) *Every degree-ℓ Galois extension F' of F is a Kummer extension.*

(3) *Let $F' = F(\sqrt[\ell]{\alpha})$ and $F'' = F(\sqrt[\ell]{\beta})$ be two Kummer extensions of F. Then $F' \cong F''$ if and only if $\alpha = \beta^j \gamma^\ell$ for some $\gamma \in F^\times$ and some $j \in \mathbb{Z}$ with $1 \le j \le \ell - 1$.*

(4) *Suppose F is a function field. Let $F' = F(\sqrt[\ell]{\alpha})$ be a Kummer extension, let P be a place of F, and let P' be a place of F' lying over P. Then*

$$e(P' \mid P) = \frac{\ell}{\gcd(\ell, v_P(\alpha))},$$

where v_P is the additive valuation associated to P.

Note in particular that statement (3) gives a bijection between the Kummer extensions of F and the nontrivial cyclic subgroups of $F^\times/(F^\times)^\ell$.

Now suppose we are given an odd prime ℓ and a prime power $q \equiv 1 \bmod 2\ell$, and let K be the rational function field over $\mathbb{F}_q$. We construct dihedral degree-ℓ

function fields over K with a given quadratic resolvent field K_2 by starting with the field K_2 and constructing, via Kummer's theorem, cyclic degree-ℓ extensions of K_2 that are Galois over K with Galois group $\mathcal{D}_\ell$. Our next proposition allows us to recognize when we have such an extension. Before stating the proposition, we note that the norm map from K_2 to K induces a norm map $K_2^\times/(K_2^\times)^\ell \to K^\times/(K^\times)^\ell$, and that the inclusion $K^\times \subset K_2^\times$ induces a conorm map $K^\times/(K^\times)^\ell \to K_2^\times/(K_2^\times)^\ell$.

Proposition 3.2. *Let K_2/K be a quadratic function field and let $K_2(\theta)$ be a Kummer extension of K_2, where $\theta^\ell = \alpha \in K_2^\times \setminus (K_2^\times)^\ell$. Let C be the cyclic subgroup of $K_2^\times/(K_2^\times)^\ell$ generated by the class of α. If C is contained in the image of the conorm map, then $K_2(\theta)$ is a cyclic Galois extension of K; if C is contained in the kernel of the norm map, then $K_2(\theta)$ is a Galois extension of K with group $\mathcal{D}_\ell$; and otherwise, $K_2(\theta)$ is not a Galois extension of K.*

Proof. Since K_2 is Galois over K, the group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts on $K_2^\times/(K_2^\times)^\ell$, and this action reflects the action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on the set of Kummer extensions of K_2 in K^{sep}. Thus, the field $L = K_2(\theta)$ is Galois over K if and only if $\omega(C) = C$ for all $\omega \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$, and this will be the case if and only if $\tau(C) = C$ for the nontrivial automorphism τ of K_2 over K.

Suppose $\tau(C) = C$, so that L/K is Galois. Since τ^2 is the identity on C, we have $\tau(\alpha) = \alpha^i \gamma^\ell$ for some $\gamma \in K_2$ and $i = \pm 1$. Let ω be an element of order 2 in $\mathrm{Gal}(L/K)$, so that ω is a lift of τ. If $i = 1$ then we have $(\omega(\theta)/\theta)^\ell = \gamma^\ell$, so $\omega(\theta) = \theta\gamma\zeta$ for some ℓ-th root of unity $\zeta \in K$; replacing γ with $\gamma\zeta$, we may assume that $\zeta = 1$ and $\omega(\theta) = \theta\gamma$. Then

$$\theta = \omega^2(\theta) = \omega(\theta)\cdot\omega(\gamma) = \theta\gamma\cdot\omega(\gamma)$$

so $1 = N_{K_2/K}(\gamma)$. By Hilbert 90, we have $\gamma = \varepsilon/\tau(\varepsilon)$ for some $\varepsilon \in K_2$. Since $\tau(\alpha) = \alpha\gamma^\ell$, we find that $\alpha\varepsilon^\ell$ is fixed by τ, so the image of α in $K_2^\times/(K_2^\times)^\ell$ lies in the image of the conorm. On the other hand, if $i = -1$ then $\gamma^\ell = N_{K_2/K}(\alpha) \in K$. Since $\gamma \in K_2$ and K_2 is a quadratic extension of K, we must have $\gamma \in K$. Thus the image of α in $K_2^\times/(K_2^\times)^\ell$ lies in the kernel of the norm. We see that if C is neither in the image of the conorm nor in the kernel of the norm, then $K_2(\theta)$ is not Galois over K; this is the final statement of the proposition.

If C is in the image of the conorm, then $\alpha = \beta\gamma^\ell$ for some $\beta \in K$ and $\gamma \in K_2$. Then $K_2(\theta)$ is the composition of the quadratic extension K_2/K with the Kummer extension $K(\sqrt[\ell]{\beta})/K$, so $K_2(\theta)$ is Galois over K with cyclic Galois group.

Finally, suppose C is killed by the norm map, so that $N_{K_2/K}(\alpha) = \gamma^\ell$ for some $\gamma \in K$. Then $\tau(\alpha) = \gamma^\ell/\alpha$, so $\tau(C) = C$, and L is Galois over K. If we again let ω be an element of order 2 in $\mathrm{Gal}(L/K)$, then $\omega(\theta) = \gamma\zeta/\theta$ for some ℓ-th root of unity $\zeta \in K$. If we let σ be a generator of $\mathrm{Gal}(L/K_2)$, we find that $\omega\sigma\omega = \sigma^{-1}$, so $\mathrm{Gal}(L/K) \cong \mathcal{D}_\ell$. □

Elements of K_2 whose norms are ℓ-th powers in K have divisors of a specific type, described below.

Proposition 3.3. *Let $\alpha \in K_2^\times$. If $\mathrm{N}_{K_2/K}(\alpha) = \gamma^\ell$ for some $\gamma \in K^\times$, then the principal divisor of α takes the form*

$$(\alpha) = \ell E' + \sum_{i=1}^{(\ell-1)/2} i(D_i' - D_{-i}'),$$

where E' is a divisor of K_2, the D_i' are squarefree effective divisors of K_2 with pairwise disjoint support, and where $\tau(D_i') = D_{-i}'$ for all i. Consequently, every place of K lying under a place in the support of some D_i' splits in K_2.

Proof. Let P' be a place in the support of the principal divisor (α), and set $n_P = v_P((\alpha))$. Then by the division algorithm we can uniquely write $n_P = q\ell + r$ for some $q, r \in \mathbb{Z}$ with $|r| \le (\ell-1)/2$. Repeating this for all places in the support of (α), we see that the divisor of α can be written uniquely as

$$(\alpha) = \ell E' + \sum_{i=1}^{(\ell-1)/2} i(D_i' - D_{-i}'),$$

where the D_i' are squarefree effective divisors with pairwise disjoint support. Applying the norm map $\mathrm{N}_{K_2/K}$ to (α), we obtain

$$\begin{aligned}(\mathrm{N}_{K_2/K}(\alpha)) &= (\alpha) + (\tau(\alpha)) \\ &= \ell(E' + \tau(E')) + \sum_{i=1}^{(\ell-1)/2} i(D_i' - D_{-i}' + \tau(D_i') - \tau(D_{-i}')).\end{aligned}$$

As $\mathrm{N}_{K_2/K}(\alpha) = \gamma^\ell$, we see that

$$i(D_i' - D_{-i}' + \tau(D_i') - \tau(D_{-i}')) = 0 \quad \text{for } 1 \le i \le (\ell-1)/2.$$

This shows that $D_i' = 0$ if and only if $D_{-i}' = 0$. If $D_i' \ne 0$, then D_i' and D_{-i}' are effective and have disjoint support, forcing $D_i' = \tau(D_{-i}')$. □

3B. ***Virtual unit decomposition.*** Theorem 3.1 states that elements of $K_2^\times$ that generate the same subgroup of $K_2^\times/(K_2^\times)^\ell$ produce the same Kummer extension. We wish to construct distinct dihedral function fields by constructing distinct Kummer extensions of K_2. To that end, we decompose the group $K_2^\times/(K_2^\times)^\ell$ using a function field definition of virtual units, as inspired by H. Cohen's work on number fields [7]. In particular, we show how to construct a basis for the kernel of the norm map $K_2^\times/(K_2^\times)^\ell \to K^\times/(K^\times)^\ell$.

We define the (ℓ-)*virtual units* of K_2 to be the elements of the set

$$V_\ell = \{\alpha \in K_2^\times : (\alpha) \in \ell \operatorname{Div}^0 K_2\}.$$

The map from V_ℓ to $\operatorname{Div}^0 K_2$ that sends α to $(\alpha)/\ell$ induces a map from V_ℓ to $(\operatorname{Pic}^0 K_2)[\ell]$, the ℓ-torsion of the degree-0 divisor class group of K_2; this leads to the exact sequence

$$1 \longrightarrow \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell \longrightarrow V_\ell/(K_2^\times)^\ell \longrightarrow (\operatorname{Pic}^0 K_2)[\ell] \longrightarrow 0.$$

We also have an exact sequence

$$1 \longrightarrow V_\ell/(K_2^\times)^\ell \longrightarrow K_2^\times/(K_2^\times)^\ell \longrightarrow K_2^\times/V_\ell \longrightarrow 1. \tag{2}$$

To better understand the final term of this sequence, we set

$$I_\ell = \operatorname{Prin} K_2/(\operatorname{Prin} K_2 \cap \ell \operatorname{Div}^0 K_2)$$

and define a map $\varphi\colon K_2^\times \to I_\ell$ by $\varphi(\alpha) = (\alpha) + \operatorname{Prin} K_2 \cap \ell \operatorname{Div}^0 K_2$. Then φ is surjective and $\ker\varphi = V_\ell$, so $K_2^\times/V_\ell \cong I_\ell$. All told, we obtain this diagram of exact sequences, which represents a virtual unit decomposition:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell & \longrightarrow & \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell & \longrightarrow & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & V_\ell/(K_2^\times)^\ell & \longrightarrow & K_2^\times/(K_2^\times)^\ell & \longrightarrow & K_2^\times/V_\ell & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\operatorname{Pic}^0 K_2)[\ell] & \longrightarrow & \operatorname{Prin} K_2/\ell \operatorname{Prin} K_2 & \longrightarrow & I_\ell & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{3}$$

The middle vertical sequence here shows that the divisor map from $K_2^\times/(K_2^\times)^\ell$ to $\operatorname{Prin} K_2/\ell \operatorname{Prin} K_2$ has kernel $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell$. However, by Proposition 3.2, Kummer extensions of K_2 that are Galois over K with group $\mathcal{D}_\ell$ correspond to nontrivial cyclic subgroups of the kernel of the norm map from $K_2^\times/(K_2^\times)^\ell$ to $K^\times/(K^\times)^\ell$. We now describe how the divisor map behaves on this kernel.

Let H be the group

$$H = \left\{\alpha \in K_2^\times : \mathrm{N}_{K_2/K}(\alpha) \in (K^\times)^\ell\right\}, \tag{4}$$

so that $H/(K_2^\times)^\ell$ is the kernel of the norm map from $K_2^\times/(K_2^\times)^\ell$ to $K^\times/(K^\times)^\ell$.

Proposition 3.4. *The map*

$$H/(K_2^\times)^\ell \longrightarrow \operatorname{Prin} K_2/\ell \operatorname{Prin} K_2$$

(*induced from the divisor map*) *is injective, and its image is the group*

$$J_\ell = \big\{(\beta) + \ell \operatorname{Prin} K_2 \in \operatorname{Prin} K_2/\ell \operatorname{Prin} K_2 : \mathrm{N}_{K_2/K}((\beta)) \in \ell \operatorname{Prin} K\big\}.$$

Proof. Let (H) be the group of divisors of elements in H. First we claim that the sequence

$$1 \longrightarrow (\mathbb{F}_q^\times)^\ell \longrightarrow H \longrightarrow (H) \longrightarrow 0$$

is exact. To see this, note that the map sending an element of H to its divisor is clearly surjective. The kernel of this map is the set $H \cap \mathbb{F}_q^\times$. Let $k \in \mathbb{F}_q^\times$ and suppose $\mathrm{N}_{K_2/K}(k) \in (K^\times)^\ell$. Then $\mathrm{N}_{K_2/K}(k) = k\tau(k) = k^2 \in (K^\times)^\ell$. As squaring is an isomorphism of $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell$, we have $k \in (\mathbb{F}_q^\times)^\ell$.

It follows from the exact sequence above that the divisor map

$$H/(K_2^\times)^\ell \longrightarrow \operatorname{Prin} K_2/\ell \operatorname{Prin} K_2$$

is injective. Its image is certainly contained in J_ℓ. To complete the proof, we must show that every element of J_ℓ lies in the image of $H/(K_2^\times)^\ell$.

Let $(\beta) + \ell \operatorname{Prin} K_2$ be an element of J_ℓ, where $\beta \in K_2^\times$ satisfies $\mathrm{N}_{K_2/K}((\beta)) \in \ell \operatorname{Prin} K$, say $\mathrm{N}_{K_2/K}((\beta)) = \ell(\gamma)$ for some $\gamma \in K^\times$. Then $\mathrm{N}_{K_2/K}(\beta) = c\gamma^\ell$ for some $c \in \mathbb{F}_q^\times$. If we let $d = c^{(\ell-1)/2}$, then $\mathrm{N}_{K_2/K}(d\beta) = (c\gamma)^\ell$, so $d\beta$ is an element of H whose image in $\operatorname{Prin} K_2/\ell \operatorname{Prin} K_2$ is $(\beta) + \ell \operatorname{Prin} K_2$. □

Proposition 3.5. *The image of* $(\operatorname{Pic}^0 K_2)[\ell]$ *in* $\operatorname{Prin} K_2/\ell \operatorname{Prin} K_2$ *is contained in* J_ℓ.

Proof. Suppose $D' \in \operatorname{Div}^0 K_2$ represents an element of $(\operatorname{Pic}^0 K_2)[\ell]$, so that $\ell D'$ is a principal divisor, say equal to (α) for some $\alpha \in K_2^\times$. Then the divisor of $\mathrm{N}_{K_2/K}(\alpha)$ is also an ℓ-multiple of a principal divisor. □

Let U_ℓ be the image of $H/(K_2^\times)^\ell$ in I_ℓ, so that

$$U_\ell = \{(\alpha) + \operatorname{Prin} K_2 \cap \ell \operatorname{Div}^0 K_2 : \alpha \in H\}.$$

Corollary 3.6. *The bottom row of Diagram* (3) *gives rise to an exact sequence*

$$0 \longrightarrow (\operatorname{Pic}^0 K_2)[\ell] \longrightarrow H/(K_2^\times)^\ell \longrightarrow U_\ell \longrightarrow 0,$$

which splits (*noncanonically*).

Proof. The sequence is obtained from combining the exact sequence

$$0 \longrightarrow (\mathrm{Pic}^0\, K_2)[\ell] \longrightarrow J_\ell \longrightarrow U_\ell \longrightarrow 0$$

of subgroups of the bottom row of Diagram (3) with the isomorphism $H/(K_2^\times)^\ell \cong J_\ell$. The sequence splits because all of the groups are ℓ-torsion. □

This corollary, together with Proposition 3.2, gives us the following theorem:

Theorem 3.7. *There is a one-to-one correspondence between Kummer extensions $K_{2\ell}/K_2$ such that $K_{2\ell}$ is Galois over K with group $\mathcal{D}_\ell$ and the set of nontrivial cyclic subgroups of $(\mathrm{Pic}^0\, K_2)[\ell] \times U_\ell$.*

3C. *The discriminant divisors of $\mathcal{D}_\ell$ extensions.* Now that we have established the correspondence of Theorem 3.7 for $\mathcal{D}_\ell$ Kummer extensions $K_{2\ell} = K_2(\sqrt[\ell]{\alpha})$ of K_2, it remains to compute the discriminant divisor of $K_\ell \subset K_2(\sqrt[\ell]{\alpha})$. In particular, we compute the discriminant divisor Δ_{K_ℓ} of K_ℓ in terms of (α) and Δ_{K_2}. We begin by describing the discriminant divisor $\Delta_{K_{2\ell}/K_2}$. Our description is simplified by the introduction of the following terminology.

Suppose α is an element of the group H defined by (4). Let $D'_1, \ldots, D'_{(\ell-1)/2}$ be the divisors arising from the representation of (α) as described in Proposition 3.3. We define the *ramification divisor* of α to be the divisor

$$D'_1 + \tau(D'_1) + \cdots + D'_{(\ell-1)/2} + \tau(D'_{(\ell-1)/2})$$

of K_2, and the *reduced ramification divisor* of α to be the divisor

$$\mathrm{N}_{K_2/K}(D'_1 + \cdots + D'_{(\ell-1)/2})$$

of K. Note that the ramification divisor is the conorm of the reduced ramification divisor.

Lemma 3.8. *Let K_2 be a quadratic function field over K. Suppose that $K_{2\ell} = K_2(\sqrt[\ell]{\alpha})$ is a Kummer extension of K_2 such that $K_{2\ell}/K$ is Galois with Galois group $\mathcal{D}_\ell$. Then*

$$\Delta_{K_{2\ell}/K_2} = (\ell - 1)D',$$

where D' is the ramification divisor of α.

Proof. By Theorem 3.1, for all places P' in the support $\mathrm{Supp}\, D'$ of the divisor D', there is a unique place P'' of $K_{2\ell}$ lying over P' such that $e(P'' \mid P') = \ell$. Furthermore, all other places of K_2 are unramified in $K_{2\ell}$. □

We now compute the degree of the discriminant divisor Δ_{K_ℓ}, which will in turn allow us to compute Δ_{K_ℓ} itself. To that end, we examine the characters of $\mathcal{D}_\ell$. For subgroups G of $\mathcal{D}_\ell$, let $\Psi(G)$ denote the induced character of $\mathcal{D}_\ell$ obtained from the trivial character of G (see [27, Chapter 3]). The fields K, K_2, K_ℓ and

$K_{2\ell}$ of Diagram (1) are the fixed fields of the four subgroups $\mathcal{D}_\ell$, $\mathcal{C}_\ell$, $\mathcal{C}_2$, and 1, respectively. The induced characters of these groups are linearly dependent and satisfy the relation

$$\Psi(1) + 2\Psi(\mathcal{D}_\ell) = 2\Psi(\mathcal{C}_2) + \Psi(\mathcal{C}_\ell).$$

Since the Artin L function of an induced character $\Psi(G)$ is the ζ function of the fixed field of G (see [16, Chapter 8]), we obtain

$$\zeta_{K_{2\ell}}(s)\zeta_K^2(s) = \zeta_{K_\ell}^2(s)\zeta_{K_2}(s).$$

From the functional equation of the ζ function, we have

$$\deg \Delta_{K_{2\ell}} + 2\deg \Delta_K = 2\deg \Delta_{K_\ell} + \deg \Delta_{K_2},$$

and since $\Delta_K = 0$ we find

$$\deg \Delta_{K_{2\ell}} = 2\deg \Delta_{K_\ell} + \deg \Delta_{K_2}. \tag{5}$$

By [32, Corollary 3.4.12(a)] we have $\mathrm{Diff}_{K_{2\ell}} = \mathrm{Con}_{K_{2\ell}/K_2}(\mathrm{Diff}_{K_2}) + \mathrm{Diff}_{K_{2\ell}/K_2}$. Applying norms yields

$$\Delta_{K_{2\ell}} = [K_{2\ell} : K_2]\Delta_{K_2} + \mathrm{N}_{K_2/K}(\Delta_{K_{2\ell}/K_2}).$$

By Lemma 3.8, we obtain

$$\Delta_{K_{2\ell}/K_2} = (\ell - 1)D',$$

where D' is the ramification divisor of any α that defines $K_{2\ell}$ as a Kummer extension of K_2. Let M be the reduced ramification divisor of α. Then

$$\mathrm{N}_{K_2/K}(\Delta_{K_{2\ell}/K_2}) = 2(\ell - 1)M,$$

and (5) can be rewritten as

$$\ell \deg \Delta_{K_2} + 2(\ell - 1)\deg M = 2\deg \Delta_{K_\ell} + \deg \Delta_{K_2}.$$

Thus,

$$\deg \Delta_{K_\ell} = \frac{\ell - 1}{2}\deg \Delta_{K_2} + (\ell - 1)\deg M.$$

Using this information we can now compute the discriminant divisor of K_ℓ.

Theorem 3.9. *With notation as above, we have* $\Delta_{K_\ell} = \frac{\ell-1}{2}\Delta_{K_2} + (\ell - 1)M$.

Proof. Let $E = \frac{\ell-1}{2}\Delta_{K_2} + (\ell - 1)M$. First note that the only places of K ramified in K_ℓ are those lying over places in the support of M and Δ_{K_2} as $K_{2\ell}/K_2/K$ is only ramified at these places. Moreover, for all places $P \in \mathrm{Supp}\, M$ and all $P'' \in \mathrm{Places}(K_{2\ell})$ lying over P, we have $e(P'' \mid P) = \ell$. Similarly, for all places $P \in \mathrm{Supp}\, \Delta_{K_2}$ and all $P'' \in \mathrm{Places}(K_{2\ell})$ lying over P, we have $e(P'' \mid P) = 2$.

As $[K_{2\ell} : K_\ell] = 2 \nmid \ell$, all places $P' \in \text{Places}(K_\ell)$ lying over M must have $e(P' \mid P) = \ell$. Also, for all $P' \in \text{Places}(K_\ell)$ lying over Δ_{K_2}, $e(P' \mid P) \leq 2$. Applying the identity

$$\sum_{P' \mid P} e(P' \mid P) f(P' \mid P) = \ell$$

to any place $P \in \text{Supp}\, \Delta_{K_2}$ allows at most $(\ell - 1)/2$ places $P' \mid P$ to be ramified. Thus, Δ_{K_ℓ} divides E. Since both divisors have the same degree, they must be equal. □

We note that the above proof in fact gives the complete decomposition of the ramified places of K_ℓ / K.

3D. ***The number of $\mathcal{D}_\ell$ function fields.*** We now prove the main result, Theorem 3.10, which provides the number of nonconjugate degree-ℓ dihedral extensions K_ℓ of K with fixed discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2. We use the correspondence of Theorem 3.7 and the discriminant divisor result of Theorem 3.9. First, we introduce some more notation.

Let $M \in \text{Div}(K)$ be a squarefree effective divisor. Set $N = \#\,\text{Supp}\, M$, and suppose that every place $P_i \in \text{Supp}\, M$, $1 \leq i \leq N$, splits in K_2 as $P_i = P_i' + \tau(P_i')$ with $P_i' \neq \tau(P_i')$. We then define a set $\mathcal{Q}_\ell(M)$ of formal sums by

$$\mathcal{Q}_\ell(M) := \left\{ \sum_{i=1}^{N} n_i (P_i' - \tau(P_i')) : n_i \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}.$$

We can view $\mathcal{Q}_\ell(M)$ as a subset of the group

$$\overline{\mathcal{Q}}_\ell(M) = \sum_{i=1}^{N} (\mathbb{Z}/\ell\mathbb{Z})(P_i' - \tau(P_i'));$$

note that the natural map $\text{Div}^0 K_2 \to \text{Pic}^0 K_2$ reduces to a homomorphism

$$\rho\colon \overline{\mathcal{Q}}_\ell(M) \longrightarrow \text{Pic}^0 K_2 / \ell\, \text{Pic}^0 K_2.$$

We set

$$T_\ell(M) := \{E' \in \mathcal{Q}_\ell(M) : \rho(E') = 0\}. \tag{6}$$

Theorem 3.10. *Let K_2 be a quadratic function field over $K = \mathbb{F}_q(x)$ with discriminant divisor Δ_{K_2}, with $q \equiv 1 \bmod 2\ell$. Let r denote the ℓ-rank of $\text{Pic}^0 K_2$, and let M be a divisor of K that is either zero or a sum of distinct places of K supported away from Δ_{K_2}. Let $\Delta = \frac{\ell-1}{2}\Delta_{K_2} + (\ell - 1)M$.*

(1) *If $M = 0$, then the number of nonconjugate dihedral degree-ℓ function fields K_ℓ / K with discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2 is $(\ell^r - 1)/(\ell - 1)$.*

(2) *If $M \neq 0$ and some $P \in \operatorname{Supp} M$ is inert in K_2/K, then there are no dihedral degree-ℓ function fields K_ℓ/K with discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2.*

(3) *Suppose $M \neq 0$ and that all $P_i \in \operatorname{Supp} M$ split in K_2 as $P_i = P_i' + \tau(P_i')$ with $P_i' \neq \tau(P_i')$. Then the number of nonconjugate dihedral degree-ℓ function fields with discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2 is $\#T_\ell(M)\ell^r/(\ell-1)$, where $T_\ell(M)$ is defined by (6).*

Proof. Let $U_{\ell,M}$ denote the subset of U_ℓ consisting of those classes

$$(\alpha) + \operatorname{Prin} K_2 \cap \ell \operatorname{Div}^0 K_2$$

such that the reduced ramification divisor of α is equal to M. Note that $U_{\ell,M}$ is closed under multiplication by nonzero elements of $\mathbb{Z}/\ell\mathbb{Z}$.

Using the correspondence of Theorem 3.7, the conjugacy classes of dihedral degree-ℓ function fields with discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2 are in one-to-one correspondence with the number of nontrivial cyclic subgroups of $(\operatorname{Pic}^0 K_2)[\ell] \times U_\ell$ that can be generated by elements (A, B) with $B \in U_{\ell,M}$.

If $M = 0$, then $U_{\ell,M}$ consists of the identity, so $B = 0$ and A can be any nonzero class in $(\operatorname{Pic}^0 K_2)[\ell]$. There are $\ell^r - 1$ such pairs, and they generate $(\ell^r-1)/(\ell-1)$ different cyclic subgroups.

If $M \neq 0$, then $\#U_{\ell,M} = \#T_\ell(M)$. This is because an element α of H gives rise to an element of $U_{\ell,M}$ if and only if its divisor is of the form E' (up to multiples of ℓ) for some E' in $T_\ell(M)$. Thus, there are $\#T_\ell(M)\ell^r$ pairs (A, B) in $(\operatorname{Pic}^0 K_2)[\ell]\times U_\ell$ with $B \in U_{\ell,M}$, and there are $\#T_\ell(M)\ell^r/(\ell-1)$ cyclic subgroups generated by such pairs. □

3E. *Defining equations.* In this section, we will write down explicit defining equations for $\mathcal{D}_\ell$ extensions of K constructed as above.

Definition 3.11. Given an integer $n > 0$ and an element γ of K, let $C_{n,\gamma}$ be the polynomial

$$C_{n,\gamma}(X) = \sum_{r=0}^{\lfloor n/2 \rfloor} (-\gamma)^r \frac{n}{n-r} \binom{n-r}{r} X^{n-2r}$$

in $K[X]$. (Note that the coefficient $\frac{n}{n-r}\binom{n-r}{r}$ is in fact an integer, so the definition makes sense in positive characteristic; see [30, Sequence A082985].)

The polynomials $C_{n,\gamma}$ are scaled versions of the Chebyshev polynomials of the first kind, and it follows that if u and v are elements of a field extension L of K that satisfy $uv = \gamma$, then

$$C_{n,\gamma}(u + v) = u^n + v^n.$$

Proposition 3.12. *Let ℓ be an odd prime, let $q \equiv 1 \bmod 2\ell$ be a prime power, and let K_2 be a quadratic extension of $K = \mathbb{F}_q(x)$. Let α be an element of $K_2 \setminus K_2^\ell$ such that $\mathrm{N}_{K_2/K}(\alpha) = \gamma^\ell$ for some $\gamma \in K$, and let $K_{2\ell}$ be the Kummer extension $K_2(\sqrt[\ell]{\alpha})$, so that $K_{2\ell}/K$ is Galois with group $\mathcal{D}_\ell$. Then the roots in $K_{2\ell}$ of the polynomial*

$$C_{\ell,\gamma}(X) - \mathrm{Tr}_{K_2/K}(\alpha)$$

are generators for the index-2 subfields of $K_{2\ell}/K$.

Proof. Let θ be a root of $z^\ell - \alpha$, let σ be a generator of $\mathrm{Gal}(K_{2\ell}/K_2)$, and let τ be an element of $\mathrm{Gal}(K_{2\ell}/K)$ that restricts to the nontrivial element of $\mathrm{Gal}(K_2/K)$. Then $\tau(\theta)$ and γ/θ are both roots of $z^\ell - \tau(\alpha)$, so $\tau'(\theta) = \gamma/\theta$ for some $\tau' = \sigma^i\tau$. Thus, $\theta + \gamma/\theta$ lies in the fixed field of τ' (but does not lie in K, for otherwise θ would lie in a quadratic extension of K).

It follows that

$$C_{\ell,\gamma}(\theta + \gamma/\theta) = \theta^\ell + (\gamma/\theta)^\ell = \alpha + \tau(\alpha) = \mathrm{Tr}_{K_2/K}(\alpha),$$

so one of the roots of $C_{\ell,\gamma}(X) - \mathrm{Tr}_{K_2/K}(\alpha)$ generates an index-2 subfield of $K_{2\ell}/K$. Since all of these index-2 subfields are conjugate to one another, the other roots of the polynomial generate the other fields. □

4. Algorithms and data

4A. ***Construction algorithm.*** The correspondence of Theorem 3.7 can be made explicit, and the proof of Theorem 3.10 is constructive; this leads naturally to Algorithm 4.1 below. This algorithm takes as input a quadratic function field K_2 and an effective squarefree divisor M of K, and outputs all nonconjugate degree-ℓ dihedral function fields with discriminant divisor $\frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M$ and quadratic resolvent field K_2. Note that K_2 may be the unique degree-2 constant field extension of K, in which case $\Delta_{K_2} = 0$.

Algorithm 4.1 (Constructing all $\mathcal{D}_\ell$ function fields with a given quadratic resolvent and given ramification divisor).

Input: A quadratic extension K_2 of K, an odd prime ℓ, and a squarefree effective divisor M of K with support disjoint from that of Δ_{K_2}.

Output: A set L of defining equations for all the dihedral extensions K_ℓ of K with $\Delta_{K_\ell} = \frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M$ and with QuadRes $K_\ell = K_2$.

1. Compute fundamental information:
   (a) Compute a basis $\{[B_1], \ldots, [B_r]\}$ of $(\mathrm{Pic}^0 K_2)[\ell]$ and an element ζ of $\mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times\ell}$.
   (b) Set $N \leftarrow \varnothing$; eventually, N will contain the pairs of places of K_2 lying over the support of M.

(c) For $P \in \operatorname{Supp} M$:
   i. Ensure $P = P_0' + P_1'$ in $\operatorname{Div} K_2$; upon failure, return the empty set.
   ii. $N \leftarrow N \cup \{(P_0', P_1')\}$.

(d) Use N to compute the set $\mathcal{Q}_\ell(M)$.

2. Compute functions in H representing elements of $\mathcal{Q}_\ell(M)$ that map into U_ℓ:
   (a) Set $T \leftarrow \varnothing$; eventually, T will contain lifts to H of all elements of $\mathcal{Q}_\ell(M)$ (up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$) that can be lifted to H.
   (b) For $E' \in \mathcal{Q}_\ell(M)$ up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ such that $\rho(E') = 0$:
      i. Find $\beta \in K_2^\times$ such that $(\beta) \equiv E' \bmod \ell$.
      ii. Repeat $\beta \leftarrow \zeta\beta$ until $\mathrm{N}_{K_2/K}(\beta) \in (K^\times)^\ell$.
      iii. $T \leftarrow T \cup \{\beta\}$.

3. Compute virtual units in H:
   (a) Set $V \leftarrow \varnothing$; eventually V will contain elements of $H \cap V_\ell$ whose images in $V_\ell/(K_2^\times)^\ell$ form a basis for that group.
   (b) For $[B_i]$ in the basis of $(\operatorname{Pic}^0 K_2)[\ell]$ computed in step 1(a):
      i. Find $\eta_i \in K_2$ such that $(\eta_i) = \ell B_i$.
      ii. Repeat $\eta_i \leftarrow \zeta\eta_i$ until $\mathrm{N}_{K_2/K}(\eta_i) \in (K^\times)^\ell$.
      iii. $V \leftarrow V \cup \{\eta_i\}$.

4. Create defining equations:
   (a) Set $L \leftarrow \varnothing$.
   (b) If $M = 0$ then for all nonzero $(z_i) \in (\mathbb{Z}/\ell\mathbb{Z})^r$ up to the action of $(\mathbb{Z}/\ell\mathbb{Z})^\times$:
      i. Compute $\alpha := \prod_{i=1}^r \eta_i^{z_i}$ and $\gamma \in K$ with $\gamma^\ell = \mathrm{N}_{K_2/K}(\alpha)$.
      ii. Let $C(X) \leftarrow C_{\ell,\gamma}(X) - \mathrm{Tr}_{K_2/K}(\alpha)$, as in Proposition 3.12.
      iii. $L \leftarrow L \cup \{C(X)\}$.
   (c) If $M \neq 0$ then for all $\beta \in T$ and for all $(z_i) \in (\mathbb{Z}/\ell\mathbb{Z})^{\#V}$:
      i. Compute $\alpha := \beta \prod_{\gamma_i \in V} \eta_i^{z_i}$ and $\gamma \in K$ with $\gamma^\ell = \mathrm{N}_{K_2/K}(\alpha)$.
      ii. Let $C(X) \leftarrow C_{\ell,\gamma}(X) - \mathrm{Tr}_{K_2/K}(\alpha)$, as in Proposition 3.12.
      iii. $L \leftarrow L \cup \{C(X)\}$.
   (d) Return L.

Algorithm 4.1 is precisely the construction in the proof of Theorem 3.10, and thus computes all elements α such that $K_2(\sqrt[\ell]{\alpha})$ is a Galois dihedral function field. Notice that the repeat loops in steps 2(b)(ii) and 3(b)(ii) will halt, as by Proposition 3.4, there is a unique $\beta \in K_2^\times$ with $(\beta) = B' - \tau(B') - \ell E'$ and $\beta \in H$; similarly for η.

Remarks 4.2. There are several ways to perform Algorithm 4.1 more efficiently.

(1) The generators $[B_1], \ldots, [B_r]$ of $(\mathrm{Pic}^0 K_2)[\ell]$ in step 1(a) can be computed from a set of generators $[A_1], \ldots, [A_h]$ of $\mathrm{Pic}^0 K_2$ chosen so that the order m_i of $[A_i]$ is equal to the i-th invariant factor of the group $\mathrm{Pic}^0 K_2$. Using the $[A_i]$, it is also easy to check whether an element E' of $\mathcal{Q}_\ell(M)$ is in the kernel of the map ρ, and, if so, to obtain an element $\beta \in K_2^\times$ such that $(\beta) \equiv E' \bmod \ell$, as is required in step 2(b)(i). We do this as follows: Suppose D' is a lift of E' to the degree-0 divisor group of K_2. Write $[D'] = d_1[A_1] + \cdots + d_h[A_h]$. Then E' is in the kernel of ρ if and only if ℓ divides d_i whenever m_i is divisible by ℓ. If this is the case, set $e_i = d_i/\ell$ when $\ell \,|\, m_i$ and $e_i \equiv d_i \ell^{-1} \bmod m_i$ when $\ell \nmid m_i$. Then $D' - \ell(e_1 A_1 + \cdots e_h A_h)$ is principal, and we can compute $\beta \in K_2^\times$ with this divisor; this is the desired β.

(2) When K_2 has positive genus, it is the function field of an elliptic or hyperelliptic curve $y^2 = f(x)$. One could potentially take advantage of faster arithmetic available for the Jacobians of hyperelliptic curves, instead of the slower generic arithmetic in $\mathrm{Pic}^0 K_2$.

Algorithm 4.3 takes as input a pair of effective squarefree divisors D and M of K with disjoint support and uses Algorithm 4.1 to generate all nonconjugate degree-ℓ dihedral function fields K_ℓ with discriminant divisor $\frac{\ell-1}{2} D + (\ell - 1)M$. It takes advantage of the following observation: In order for any degree-ℓ dihedral function fields K_ℓ to exist, D must be the discriminant divisor of a quadratic function field — that is, effective, squarefree, and of even degree. Moreover, all the places in the support of M must be split over the quadratic resolvent field of K_ℓ, which has discriminant divisor D. If $D = 0$, then this field is the unique quadratic constant field extension of K. If D is nonzero, then there are exactly two quadratic function function fields K_2 and K_2' of discriminant divisor D; they are in fact twists of one another. Any place $P \notin \mathrm{Supp}\, D$ splits in K_2 if and only if it is inert in K_2', and vice versa. Thus, if M is nonzero, only one of K_2 and K_2' needs to be considered in the construction of K_ℓ.

Algorithm 4.3 (Constructing all $\mathcal{D}_\ell$ function fields from divisors).

Input: An odd prime ℓ and squarefree effective divisors D and M of K with disjoint support.

Output: A set L of defining equations for all the degree-ℓ dihedral extensions K_ℓ of K with $\Delta_{K_2} = D$ and $\Delta_{K_\ell} = \frac{\ell-1}{2} D + (\ell - 1)M$.

1. If $\deg D$ is even, construct a quadratic field K_2 with discriminant divisor D; otherwise, return "D IS NOT A QUADRATIC DISCRIMINANT DIVISOR".
2. If $D = 0$, get L from Algorithm 4.1 with input K_2, ℓ, M, return L, and stop.
3. Construct the quadratic twist K_2' of K_2.

4. If $M = 0$ then:
   (a) Get L_1 from Algorithm 4.1 with input K_2, ℓ, M.
   (b) Get L_2 from Algorithm 4.1 with input K_2', ℓ, M.
   (c) Return $L_1 \cup L_2$, and stop.
5. Pick $P \in \operatorname{Supp} M$.
6. If $P = P_0' + P_1'$ in $\operatorname{Div} K_2$ then set $K_2'' \leftarrow K_2$; otherwise, set $K_2'' \leftarrow K_2'$.
7. Get L from Algorithm 4.1 with input K_2'', ℓ, M, return L, and stop.

All finite places P of K correspond to irreducible polynomials $f_P(x) \in \mathbb{F}_q[x]$. Therefore, in step 1 we can easily construct $K_2 = K(y)$ as follows: If $D = 0$, then y is simply the square root of a nonsquare in $\mathbb{F}_q$. If $D \neq 0$, then K_2 is the function field of the curve

$$y^2 = \prod_{\substack{P \in \operatorname{Supp} D \\ P \text{ finite}}} f_P(x).$$

4B. ***Tabulation algorithm.*** Algorithm 4.1 constructs all degree-ℓ dihedral function fields with a given discriminant divisor and quadratic resolvent field; by iterating this algorithm, we obtain a procedure for tabulating all degree-ℓ dihedral function fields whose discriminant divisor has degree at most some fixed input bound $B \geq 0$. However, in this context, we can use the automorphism group of K to significantly reduce the number of quadratic function fields that need to be considered.

Recall that $\operatorname{Aut} K = \operatorname{Aut} \mathbb{F}_q(x)$ is isomorphic to $\mathrm{PGL}(2, q)$, the group of fractional linear transformations of x over $\mathbb{F}_q$. The group $\operatorname{Aut} K$ also acts on the set of extension fields of K, and for every $\phi \in \operatorname{Aut} K$ we have $\phi(\Delta_{K_i}) = \Delta_{\phi(K_i)}$. Therefore, instead of applying Algorithm 4.1 to all suitable K_2 and M, we only need to consider a representative from each orbit of $\operatorname{Aut} K$ acting on the set of suitable quadratic function fields K_2. Moreover, for each such field K_2 we need only consider representatives of the action of the stabilizer $\operatorname{Stab} K_2 \subseteq \mathrm{PGL}(2, q)$ on the set of suitable M.

These ideas are captured below in three algorithms. We start with Algorithm 4.4, which, given an integer B, finds orbit representatives for the set of quadratic function fields whose discriminant divisors are of degree at most $2B/(\ell - 1)$.

Recall that every quadratic function field K_2 can be expressed as $K(y)$, where y^2 is equal to either a nonsquare in $\mathbb{F}_q$ or a squarefree polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $2g + 1$ or $2g + 2$, where g is the genus of K_2. In the former case, K_2 is fixed under $\mathrm{PGL}(2, q)$. In the latter case, the action of $\phi \in \mathrm{PGL}(2, q)$ on K_2 does not necessarily preserve the degree of $f(x)$, but $\phi(K_2)$ has the same genus as K_2; in fact, the discriminant divisors of K_2 and $\phi(K_2)$ have the same degree, namely $2g + 2$.

In the following algorithm, we will let $P(q, \ell, B, h)$ denote the set of nonconstant squarefree polynomials $f \in \mathbb{F}_q[x]$ whose degrees satisfy

$$\lceil \deg(f)/2 \rceil \leq \lfloor 2B/(\ell - 1) \rfloor$$

and whose leading coefficient is either 1 or a fixed nonsquare $h \in \mathbb{F}_q$.

Algorithm 4.4 (Constructing a list of $\mathrm{PGL}(2, q)$-orbit representatives for quadratic function fields of bounded discriminant).

Input: A nonnegative integer B, an odd prime ℓ, and a prime power $q \equiv 1 \bmod 2\ell$.

Output: A set R'_B of pairs (f, S) such that each f is a squarefree element of $\mathbb{F}_q[x]$ such that $K_2 := K[y]/(y^2 - f)$ has discriminant divisor of degree at most $2B/(\ell - 1)$, each S is the $\mathrm{PGL}(2, q)$-stabilizer of the class of f in $K^\times/(K^\times)^2$, and such that every quadratic extension K_2 of K with $\deg \Delta_{K_2} \leq 2B/(\ell - 1)$ has exactly one $\mathrm{PGL}(2, q)$-orbit representative in the collection of fields defined by the f.

1. Compute a primitive element h of $\mathbb{F}_q$.
2. Initialize $R'_B \leftarrow \{(h, \mathrm{PGL}(2, q))\}$.
3. Set $L(f) \leftarrow 0$ for all $f \in P(q, \ell, B, h)$.
4. For all $f \in P(q, \ell, B, h)$:
   (a) If $L(f) = 0$ then
      i. $S \leftarrow \varnothing$.
      ii. For all $\phi = \frac{ax+b}{cx+d} \in \mathrm{PGL}(2, q)$:
         - $f_1(x) \leftarrow (cx + d)^{2\lceil (\deg f)/2 \rceil} f(\phi(x))$.
         - If the leading coefficient m of f_1 is a square, replace f_1 with f_1/m; otherwise, replace f_1 with hf_1/m.
         - $L(f_1) \leftarrow 1$.
         - If $f_1 = f$, then $S \leftarrow S \cup \{\phi\}$.
      iii. $R'_B \leftarrow R'_B \cup \{(f, S)\}$.
5. Return R'_B.

Next we have Algorithm 4.5, which constructs minimal polynomials for all dihedral function fields with discriminant divisors $\frac{\ell-1}{2}\Delta_{K_2} + (\ell - 1)M$ for representatives K_2 and M obtained from Algorithm 4.4.

Algorithm 4.5 (Tabulating $\mathrm{PGL}(2, q)$-orbit representatives of dihedral function fields with bounded discriminant).

Input: A nonnegative integer B, an odd prime ℓ, a prime power $q \equiv 1 \bmod 2\ell$, and the set R'_B computed by Algorithm 4.4 on input B, ℓ, q.

Output: A set R_B of triples (L_2, Δ, S') such that each Δ is an effective divisor of K of degree at most B, the group S' is the $\mathrm{PGL}(2,q)$-stabilizer of Δ, the set L_2 consists of equations defining $\mathcal{D}_\ell$ extensions of K with discriminant divisor Δ, and such that every $\mathcal{D}_\ell$ extension of K with discriminant divisor of degree at most B has a unique $\mathrm{PGL}(2,q)$-orbit representative in the collection of fields defined by the elements of the L_2.

1. Initialize $R_B \leftarrow \varnothing$.
2. For $(f, S) \in R'_B$:
   (a) Construct $K_2 = K(x)[y]/(y^2 - f)$ and compute Δ_{K_2}.
   (b) Compute $B' = \lfloor B/(\ell-1) - (\deg \Delta_{K_2})/2 \rfloor$.
   (c) Initialize $\mathcal{M} \leftarrow \varnothing$; eventually, $\mathcal{M}$ will contain all effective squarefree divisors of K with support disjoint from Δ_{K_2} and degree at most B'.
   (d) Compute lists
   $$L_j = \{P \in \mathrm{Places}(K) \setminus \mathrm{Supp}\, \Delta_{K_2} : \deg P = j\}$$
   for $1 \le j \le B'$.
   (e) For i from 0 to B' and for every partition $\mathbf{n} = [n_1, .., n_r]$ of i:
      i. Generate the set $W_{\mathbf{n}} = \{\sum_{k=1}^{r} P_k : P_k \in L_{n_k}\}$.
      ii. $\mathcal{M} \leftarrow \mathcal{M} \cup W_{\mathbf{n}}$.
   (f) Compute the set $\mathcal{M}_S$ of all pairs (M, S') where each $M \in \mathcal{M}$ is a unique orbit representative of S acting on $\mathcal{M}$ and S' is the stabilizer of M in S.
   (g) For $(M, S') \in \mathcal{M}_S$:
      i. Get L_2 from Algorithm 4.1 on input (K_2, ℓ, M).
      ii. Compute $\Delta = \frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M$.
      iii. $R_B \leftarrow R_B \cup \{(L_2, \Delta, S')\}$.
3. Return R_B.

Finally, Algorithm 4.6 reapplies Aut K to each of the constructed minimal polynomials to obtain the full list of degree-ℓ dihedral function fields whose discriminant divisor has degree bounded by B.

Algorithm 4.6 (Tabulating the full list of dihedral function fields with bounded discriminant).

Input: A nonnegative integer B, an odd prime ℓ, a prime power $q \equiv 1 \bmod 2\ell$, and the set R_B computed by Algorithm 4.5 on input B, ℓ, q.

Output: A set L_B of defining equations for all the dihedral extensions K_ℓ of K with $\deg \Delta_{K_\ell} \le B$.

1. Initialize $L_B \leftarrow \varnothing$.

2. For $(L, \Delta, S') \in R_B$:
   (a) For all distinct representatives ϕ of cosets in $\mathrm{PGL}(2,q)/S'$ and for all $C(X) \in L$, set $L_B \leftarrow L_B \cup \{(\phi(C(X)), \phi(\Delta))\}$.
3. Return L_B.

4C. ***Numerical results.*** We implemented our algorithms in Magma [5]. In Table 1, we provide data for all odd primes ℓ, prime powers $q \equiv 1 \bmod 2\ell$, and multiples $B > \ell-1$ of $\ell-1$ such that $q^{2B/(\ell-1)+1} < 2^{29}$. The column headed $K_2/\sim$ gives the number of quadratic function fields generated by Algorithm 4.4. The number of function fields constructed by Algorithm 4.5 is given in the column headed $K_\ell/\sim$, and the total number of nonconjugate dihedral degree-ℓ function fields whose discriminant divisor has degree at most B is listed in the column headed K_ℓ. The running times of Algorithms 4.4, 4.5, and 4.6 are listed in the next three columns. For each ℓ, q and B, we also computed the value $R = (q^3-q)T_5/(T_4+T_5+T_6)$, where T_i denotes the running time of Algorithm 4.i for $i = 4, 5, 6$. The quantity R estimates the improvement factor obtained by our tabulation method relative to simply iterating Algorithm 4.1 over all possible quadratic function fields without using the $\mathrm{PGL}(2,q)$ action.

Notice that the improvement factor R is highly varied. For fixed ℓ and B, R tends to decrease as q increases although the improvement still remains significant. Why this decrease occurs is unclear; it may be due to the fact that R is not a sufficiently refined estimate for the actual running time improvement. Overall, the running time of Algorithm 4.1 is dominated by the construction of the set $\mathcal{Q}_\ell(M)$ and obtaining functions for the principal divisors in steps 2(b)(i) and 3(b)(i). Data suggests that as B grows, finding the generators of these principal divisors will tend to dominate the running time. Using Jacobian arithmetic as opposed to divisor arithmetic as suggested in part (2) of Remarks 4.2 improved the performance of our tabulation only very marginally, even for larger parameters.

The entries of columns 4 and 5 of Table 1 differ by a factor that is very close to $\ell-1$; in other words, for the data we collected, it looks like the number of quadratic extensions of K with discriminant degree at most $2B/(\ell-1)$ is about $\ell-1$ times as large as the number of $\mathcal{D}_\ell$ extensions of K with discriminant degree at most B. When $B = 2(\ell-1)$ this is explained by the results of the following section, but we do not know whether it is true in general.

5. A formula for the case $B = 2(\ell-1)$

In this section we give an explicit formula for the number of $\mathcal{D}_\ell$ extensions whose discriminant divisor has degree $2(\ell-1)$.

First we note that there are no $\mathcal{D}_\ell$ extensions with discriminant of degree smaller than $2(\ell-1)$. To see this, suppose K_ℓ is a $\mathcal{D}_\ell$ extension of K with Galois closure

						Running time (seconds)			
ℓ	q	B	$K_2/\sim$	$K_\ell/\sim$	K_ℓ	Alg. 4.4	Alg. 4.5	Alg. 4.6	R
3	7	4	33	17	2,373	0.9	1.1	0.8	132.0
		6	782	472	117,285	25.8	35.2	47.1	109.4
		8	35,010	18,149	5,763,093	1,321.5	2,416.9	2,505.1	130.1
	13	4	61	33	28,470	13.7	3.2	9.5	264.7
		6	4,650	2,564	4,824,534	1,379.5	286.1	1,870.2	176.7
	19	4	81	41	130,131	82.8	7.6	44.5	385.4
	25	4	109	57	390,300	726.8	17.6	149.1	307.3
	31	4	129	65	923,025	821.0	31.7	357.2	779.7
	37	4	157	81	1,873,458	1,983.1	56.5	731.7	1,031.9
	43	4	177	89	3,417,855	4,040.5	100.2	1,341.9	1,452.3
	49	4	205	105	5,763,576	20,544.4	189.6	2,376.5	964.8
5	11	8	45	9	6,655	6.1	1.4	2.7	181.2
		12	2,858	949	1,058,695	461.5	102.9	463.5	132.1
	31	8	109	33	446,865	821.0	29.2	191.0	834.6
	41	8	169	45	1,378,420	3,178.2	80.5	602.0	1,436.2
7	29	12	121	19	219,646	546.8	22.6	94.8	828.9
	43	12	177	29	1,086,911	4,000.5	95.2	567.8	1,622.2
11	23	20	93	8	48,829	192.7	10.1	23.8	541.3
13	53	24	217	21	1,340,794	10,935.6	235.8	742.8	2,945.5
23	47	44	189	11	519,961	5,951.6	184.2	364.9	2,940.5

Table 1. Function field counts for all ℓ and $q \equiv 1 \bmod 2\ell$ with $q^{\frac{2B}{\ell-1}+1} < 2^{29}$, for $B \geq 2(\ell-1)$. For each ℓ, q, and B given in the first three columns, we list in column 4 the number of $\mathrm{PGL}(2,q)$-equivalence classes of quadratic extension of $K = \mathbb{F}_q(x)$ whose discriminants have degree at most $2B/(\ell-1)$. In column 5, we list the number of $\mathrm{PGL}(2,q)$-equivalence classes of $\mathcal{D}_\ell$ extensions of K whose discriminants have degree at most B, and in column 6 we list the total number of such extensions. In the next three columns we give the running times of the algorithms that computed these quantities, and in the final column we give an estimate of the improvement in running time obtained by using the $\mathrm{PGL}(2,q)$ action in our computations. (Computations were carried out on one core of a 2GHz Intel Xeon X7550, with 64GB of available RAM.)

$K_{2\ell}$ and quadratic resolvent K_2. Theorem 3.9 gives $\Delta_{K_\ell} = \frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M$, where M is as in Section 3C. Quadratic extensions have discriminants of even degree, so $\deg \Delta_{K_\ell}$ is divisible by $\ell-1$. If $\deg \Delta_{K_\ell}$ were zero, K_ℓ/K would be a constant field extension, and would not have Galois group $\mathcal{D}_\ell$. If $\deg \Delta_{K_\ell}$ were $\ell-1$, then either K_2 would have genus 0 and $\deg M = 0$, or K_2/K would be a constant field extension and $\deg M = 1$. In the first case, $K_{2\ell}/K_2$ would be unramified and hence a constant field extension, so K_ℓ/K would also be a constant

field extension, a contradiction. In the second case, M would be a single place of degree 1; since every place in M must split in K_2, and since the places of K that split in a quadratic constant field extension are the places of even degree, we again have a contradiction. On the other hand, there do exist $\mathcal{D}_\ell$ extensions with discriminant divisor of degree $2(\ell-1)$, as the following theorem shows.

Theorem 5.1. *Let ℓ be an odd prime and let q be a prime power with $q \equiv 1 \bmod 2\ell$. For every nonnegative even integer d, let N_d be the number of $\mathcal{D}_\ell$ extensions of K whose discriminant divisors have degree $2(\ell-1)$ and whose quadratic resolvents have discriminant divisors of degree d. Let X be the modular curve $X_1(\ell)$. Then*

$$\frac{N_d}{q^3-q} = \begin{cases} \dfrac{1}{2q+2} & \text{if } d=0, \\ 1 & \text{if } d=2, \\ -2+\dfrac{2\#X(\mathbb{F}_q)}{\ell-1} & \text{if } d=4, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 5.2. For $\ell = 3$, 5, and 7, the modular curve $X_1(\ell)$ has genus 0, so for these values of ℓ the formula for N_4 simplifies to

$$\frac{N_4}{q^3-q} = \frac{2(q-\ell+2)}{\ell-1}.$$

Equations for $X_1(\ell)$ for larger values of ℓ are known. For example, Sutherland [33] gives equations for all $\ell \le 47$; as of this writing, Sutherland's online tables [34] extend the results of [33] up to $\ell = 181$.

Proof of Theorem 5.1. Theorem 3.9 shows that if K_ℓ is a $\mathcal{D}_\ell$ extension of K with quadratic resolvent K_2, and if $\deg \Delta_{K_\ell} = 2(\ell-1)$, then $\deg \Delta_{K_2}$ is 0, 2, or 4.

Let us count the number of $\mathcal{D}_\ell$ extensions K_ℓ such that $\deg \Delta_{K_2} = 0$; that is, such that K_2 is the unique quadratic extension of K obtained by extending the constant field from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$. In this case, we must have $\deg M = 2$. We know that every place in M splits in K_2, and since the places of K that split in K_2 are precisely the places of even degree, M must consist of a single degree-2 place P.

If $\alpha \in K_2$ gives rise to a $\mathcal{D}_\ell$ extension of K, its divisor is of the shape given in Proposition 3.3, where exactly one of the D'_i with $i > 0$ is nonzero (and consists of a place of K_2 lying over P). Replacing α by a power if necessary, we may assume that D'_1 and D'_{-1} are the only nonzero D'_i, and we can choose which of the two places above P appears in D'_1 and which in D'_{-1}. Since K_2 has genus 0, we can modify α by an ℓ-th power so that the divisor E' from the proposition is 0. If we let x be a generator of K, so that $K_2 \cong \mathbb{F}_{q^2}(x)$, then $\alpha = b(x-c)/(x-c^q)$ for

some $b \in \mathbb{F}_{q^2}$ and $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and we see that $N_{K_2/K}(\alpha) = b^{q+1}$. Since this norm is supposed to be an ℓ-th power, b itself must be an ℓ-th power, so we may replace α by α/b. We find that for every degree-2 place P of K, we obtain exactly one $\mathcal{D}_\ell$ extension of K_2, so $N_0 = (q^2 - q)/2$. This leads to the formula for N_0 in the statement of the theorem.

Now let us count the number of $\mathcal{D}_\ell$ extensions K_ℓ such that $\deg \Delta_{K_2} = 2$; that is, such that K_2 is a genus-0 extension K_2 with constant field $\mathbb{F}_q$. Such extensions are obtained by adjoining to K a square root of a polynomial f that is either linear or quadratic with nonzero discriminant; the polynomial is determined by the extension, if we require that its leading coefficient be either 1 or a fixed nonsquare element of $\mathbb{F}_q$. These extensions are of two different types: The ramification points of the cover can either be rational over $\mathbb{F}_q$, or not. There are $q^2 + q$ extensions of the first type, and $q^2 - q$ of the second.

Since $\deg \Delta_{K_2} = 2$, we must have $\deg M = 1$, so M consists of a degree-1 place of K that splits in K_2. The number of such places is equal to half of the number of degree-1 places of K_2 that are not ramified in K_2/K; this is equal to $(q-1)/2$ for extensions with rational ramification, and $(q+1)/2$ for extensions without rational ramification.

As in the case where K_2 was a constant field extension, the Kummer extension $K_{2\ell}/K_2$ is completely determined by the divisor M. Thus, the number of K_ℓ whose quadratic resolvents are genus-0 extensions of K with rational ramification is equal to

$$(q^2 + q) \cdot \frac{q-1}{2} = \frac{q^3 - q}{2},$$

while the number whose quadratic resolvents are genus-0 extensions of K without rational ramification is equal to

$$(q^2 - q) \cdot \frac{q+1}{2} = \frac{q^3 - q}{2}.$$

We thus see that $N_2 = q^3 - q$.

Finally, we count the number of $\mathcal{D}_\ell$ extensions K_ℓ such that $\Delta_{K_2} = 4$; that is, such that K_2 is a genus-1 extension of K. In this case, the degree of M is 0, so that $K_{2\ell}$ is an unramified degree-ℓ Galois extension of K_2.

Let E be an elliptic curve over $\mathbb{F}_q$ and let K_2 be its function field. Let $\mathrm{Aut}\, E$ (respectively, $\mathrm{Aut}'\, E$) denote the automorphism group of E in the category of elliptic curves (respectively, in the category of curves). Then

$$\mathrm{Aut}'\, E \cong E(\mathbb{F}_q) \rtimes \mathrm{Aut}\, E,$$

where the subgroup $E(\mathbb{F}_q)$ acts on E by translation [29, Proposition X.5.1].

Up to twists, the unramified degree-ℓ Galois extensions of K_2 (with constant field $\mathbb{F}_q$) are in bijection with the index-ℓ subgroups of $E(\mathbb{F}_q)$ (see [28, §VI.6]); by duality, the number of such families of twists is equal to the number of order-ℓ subgroups of $E(\mathbb{F}_q)$, which is equal to

$$\frac{\#E[\ell](\mathbb{F}_q)-1}{\ell-1}.$$

Exactly one twist $z^\ell = f$ in each family has the property that $N_{K_2/K}(f) \in (K^\times)^\ell$. Thus,

$$N_4 = \sum_{E/\mathbb{F}_q} \frac{\#E[\ell](\mathbb{F}_q)-1}{\ell-1} \cdot \#\{\text{degree-2 maps } E \to \mathbb{P}^1 \text{ up to isomorphism}\}; \quad (7)$$

here we say that two degree-2 maps $\pi_1, \pi_2 \colon E \to \mathbb{P}^1$ are isomorphic if there is an $\alpha \in \mathrm{Aut}' E$ such that $\pi_2 = \pi_1 \alpha$.

Given an $E/\mathbb{F}_q$, we will count the number of isomorphism classes of degree-2 maps $E \to \mathbb{P}^1$ in two steps. First, we count the number of $(\mathrm{Aut}' E)$-orbits of index-2 genus-0 subfields of the function field K_2 of E. Then, for each orbit, we fix an orbit representative L and we count the number of isomorphism classes of degree-2 maps $E \to \mathbb{P}^1$ that send the function field K of $\mathbb{P}^1$ to L.

Every index-2 genus-0 subfield of K_2 is the fixed field of an involution in $\mathrm{Aut}' E$ that induces -1 on the Jacobian of E. The involutions that induce -1 on the Jacobian are the maps i_Q, for $Q \in E(\mathbb{F}_q)$, defined by $i_Q(P) = Q - P$. The fixed fields of two such involutions i_{Q_1} and i_{Q_2} lie in the same $(\mathrm{Aut}' E)$-orbit if and only if i_{Q_1} and i_{Q_2} are conjugate in $\mathrm{Aut}' E$; this translates into the condition that $Q_2 - \alpha(Q_1) \in 2E(\mathbb{F}_q)$ for some $\alpha \in \mathrm{Aut}\, E$. Thus, the $(\mathrm{Aut}' E)$-orbits of index-2 genus-0 subfields L are in bijection with the orbits of $E(\mathbb{F}_q)/2E(\mathbb{F}_q)$ under the action of $\mathrm{Aut}\, E$.

Let L be an index-2 genus-0 subfield of K_2, corresponding to an involution i_Q. Let $\mathcal{S}_L$ denote the set of isomorphism classes of degree-2 maps $E \to \mathbb{P}^1$ that send the function field K of $\mathbb{P}^1$ to the subfield L of K_2, and let π be one such map. The group $\mathrm{PGL}(2,q)$ acts transitively on $\mathcal{S}_L$, so to compute $\#\mathcal{S}_L$ it suffices to compute the stabilizer of π. Tracing through the definitions, we see that $\phi \in \mathrm{PGL}(2,q)$ stabilizes π if and only if there is an automorphism α of E (as a curve) such that $\phi\pi = \pi\alpha$. Furthermore, every automorphism α of E whose induced automorphism of K_2 sends L to itself gives rise to a ϕ that stabilizes the isomorphism class of π; also, two such automorphisms $\alpha_1 \neq \alpha_2$ will give rise to distinct ϕ, unless $\alpha_1^{-1}\alpha_2 = i_Q$. We find that we have

$$\begin{aligned}\#\{\phi \in \mathrm{PGL}(2,q) : \phi \text{ stabilizes } \pi\} &= (1/2)\#\{\alpha \in \mathrm{Aut}' E : \alpha \text{ stabilizes } L\} \\ &= (1/2)\#\{\alpha \in \mathrm{Aut}' E : \alpha \text{ commutes with } i_Q\}.\end{aligned}$$

We check that an element $(P, a) \in E(\mathbb{F}_q) \rtimes \operatorname{Aut} E \cong \operatorname{Aut}' E$ commutes with i_Q if and only if $2P = Q - a(Q)$. This shows that for every element of $\operatorname{Aut} E$ that fixes the image of Q in $E(\mathbb{F}_q)/2E(\mathbb{F}_q)$, there are $\#E(\mathbb{F}_q)[2]$ choices for P that give an element of $\operatorname{Aut} E'$ that commutes with i_Q. In other words, if we let O be the $(\operatorname{Aut} E)$-orbit of Q in $E(\mathbb{F}_q)/2E(\mathbb{F}_q)$, then

$$\#\{\alpha \in \operatorname{Aut}' E : \alpha \text{ commutes with } i_Q\} = \#E(\mathbb{F}_q)[2] \frac{\#\operatorname{Aut} E}{\#O}.$$

Putting this all together, we obtain

$$\begin{aligned}\frac{\#\mathcal{S}_L}{\#\operatorname{PGL}(2,q)} &= \frac{1}{\#\{\phi \in \operatorname{PGL}(2,q) : \phi \text{ stabilizes } \pi\}} \\ &= \frac{2}{\#\{\alpha \in \operatorname{Aut}' E : \alpha \text{ commutes with } i_Q\}} \\ &= \frac{2}{\#\operatorname{Aut} E} \frac{\#O}{\#E(\mathbb{F}_q)[2]}.\end{aligned}$$

The total number of degree-2 maps $E \to \mathbb{P}^1$ (up to isomorphism) is equal to the sum $\sum_L \mathcal{S}_L$, where L ranges over a set of representatives for the $(\operatorname{Aut} E')$-orbits of index-2 genus-0 subfields of K_2. Summing over these L is the same as summing over the $(\operatorname{Aut} E)$-orbits O of $E(\mathbb{F}_q)/2E(\mathbb{F}_q)$. Thus,

$$\begin{aligned}\frac{\#\{\text{degree-2 maps } E \to \mathbb{P}^1\}/\cong}{\#\operatorname{PGL}(2,q)} &= \frac{2}{\#\operatorname{Aut} E} \frac{1}{\#E(\mathbb{F}_q)[2]} \sum_{\text{orbits } O} \#O \\ &= \frac{2}{\#\operatorname{Aut} E} \frac{1}{\#E(\mathbb{F}_q)[2]} \#(E(\mathbb{F}_q)/2E(\mathbb{F}_q)) \\ &= \frac{2}{\#\operatorname{Aut} E}.\end{aligned}$$

Combining this with (7) gives

$$\begin{aligned}\frac{N_4}{\#\operatorname{PGL}(2,q)} &= \sum_{E/\mathbb{F}_q} \frac{\#E[\ell](\mathbb{F}_q) - 1}{\ell - 1} \frac{2}{\#\operatorname{Aut} E} \\ &= \frac{2}{\ell - 1} \sum_{E/\mathbb{F}_q} \sum_{P \in E[\ell](\mathbb{F}_q) \setminus \{O\}} \frac{1}{\#\operatorname{Aut} E} \\ &= \frac{2}{\ell - 1} \sum_{(E,P)/\cong} \frac{1}{\#\operatorname{Aut}(E, P)}. \qquad (8)\end{aligned}$$

Let us explain the notation in the final line. The sum is over isomorphism classes of pairs (E, P), where E is an elliptic curve over $\mathbb{F}_q$ and P is a nonzero ℓ-torsion point in $E(\mathbb{F}_q)$; two such pairs (E_1, P_1) and (E_2, P_2) are isomorphic to one another

when there is an isomorphism $E_1 \to E_2$ that takes P_1 to P_2. The automorphism group of a pair (E, P) consists of the automorphisms of E (as an elliptic curve) that fix P.

From [17, Proposition 3.3 on p. 240 and Proposition 2.3 on p. 233], we find that

$$\sum_{(E,P)/\cong} \frac{1}{\#\operatorname{Aut}(E, P)} = \#X(\mathbb{F}_q) - c,$$

where X is the modular curve $X_1(\ell)$ and c is the number of $\mathbb{F}_q$-rational cusps on X. Since $\mathbb{F}_q$ contains the ℓ-th roots of unity, all of the $\ell - 1$ geometric cusps of X are defined over $\mathbb{F}_q$ [31, Theorem 1.3.1, p. 12], so we have $c = \ell - 1$. Combining this with (8) gives the formula for N_4 stated in the theorem. □

6. Conclusions and future work

It is interesting that the number of degree-ℓ dihedral function fields with a given quadratic resolvent K_2 and discriminant divisor $\Delta = \frac{\ell-1}{2}\Delta_{K_2} + (\ell - 1)M$ behaves quite differently depending on whether or not M is trivial. We see from Theorem 3.10 that when $M = 0$, the number of such fields with a given resolvent field K_2 depends exclusively on the ℓ-rank r of $\operatorname{Pic}^0 K_2$. The probability that the divisor class group of K_2 has a certain ℓ-Sylow subgroup is the focus of various heuristics of Cohen-Lenstra type. These are discussed further in [1], [14], [15], and [21], and directly relate to the number of $\mathcal{D}_\ell$ function fields with $M = 0$.

When $M \neq 0$, the number of degree-ℓ dihedral function fields with given quadratic resolvent field K_2 depends additionally on the cardinality of the set $T_\ell(M)$ defined in Section 3D. The natural map $\operatorname{Div}^0 K_2 \to \operatorname{Pic}^0 K_2/\ell \operatorname{Pic}^0 K_2$ is surjective, and when $\#\operatorname{Supp} M$ is greater than r it is reasonable to expect that the map ρ from Section 3D is also surjective, so that a random element of $\overline{\mathcal{Q}}_\ell(M)$ will lie in the kernel of ρ with probability

$$\frac{1}{\#(\operatorname{Pic}^0 K_2/\ell \operatorname{Pic}^0 K_2)} = \frac{1}{\ell^r}.$$

Now, an element of $\mathcal{Q}_\ell(M)$ lies in $T_\ell(M)$ if and only if it is in the kernel of ρ, so we expect $T_\ell(M)$ to contain about $\#\mathcal{Q}_\ell(M)/\ell^r = (\ell-1)^{\#\operatorname{Supp} M}/\ell^r$ elements. From Theorem 3.10, the number of nonconjugate degree-ℓ dihedral function fields with quadratic resolvent K_2 and with discriminant divisor $\Delta = \frac{\ell-1}{2}D + (\ell-1)M$ is $\#T_\ell(M)\ell^r/(\ell-1)$, which we expect to be approximately $(\ell-1)^{\#\operatorname{Supp} M - 1}$. Note that this is independent of r. When $\#\operatorname{Supp} M$ is sufficiently large, our data seems to support this heuristic.

In the case when $\ell = 3$, our algorithm tabulates all non-Galois cubic function fields up to a given degree bound on the discriminant divisor. Galois cubics are

		Number of cubic extensions				
q	B	Non-Galois	Galois	Total	$q^{B-2}(q^2+q+1)$	Ratio
7	4	2,373	85	2,458	2,793	1.136
	6	117,285	1,093	118,378	136,857	1.156
	8	5,763,093	4,117	5,767,210	6,705,993	1.163
13	4	28,470	274	28,744	30,927	1.076
	6	4,824,534	6,826	4,831,360	5,226,663	1.082
19	4	130,131	571	130,702	137,541	1.052
25	4	390,300	976	391,276	406,875	1.040
31	4	923,025	1,489	924,514	954,273	1.032
37	4	1,873,458	2,110	1,875,568	1,926,183	1.027
43	4	3,417,855	2,839	3,420,694	3,500,157	1.023
49	4	5,763,576	3,676	5,767,252	5,884,851	1.020

Table 2. Cubic function field counts compared to asymptotics, for $q \equiv 1 \bmod 3$ and $B \geq 4$ with $q^{B+1} < 2^{29}$. For the q and B given in the first two columns, we list the number of cubic extensions of $\mathbb{F}_q(x)$ with discriminant divisor of degree at most B, subdivided into the counts of non-Galois and Galois extensions. The sixth column gives an estimate for the total number derived from the asymptotic formula (9), and the seventh column gives the ratio between the estimate and the actual number from column 5.

easy to count, so we can find the total number of cubic extensions of K whose discriminant divisors have degree at most some fixed bound. On the other hand, using a result of Datskovsky and Wright [10, Theorem I.1] we can compute an asymptotic formula for the number of cubic extensions:

$$\lim_{\substack{B\to\infty \\ B \text{ even}}} q^{-B} \sum_{\substack{K_3/K \\ \deg \Delta_{K_3} \leq B}} 1 = \frac{q^3}{(q^2-1)(q-1)\zeta_K(3)} = \frac{q^2+q+1}{q^2}. \tag{9}$$

(Note that the term $2\log q$ in [10, Theorem I.1] should be simply $\log q$.) In Table 2 we compare this asymptotic expression to actual computations. For each q and B listed in the first two columns, the entry in column 5 gives the total number of cubic extensions of $\mathbb{F}_q(x)$ with discriminant divisor of degree at most B, broken down into the number of non-Galois extensions (column 3) and Galois extensions (column 4). Column 6 gives the estimate from (9), and column 7 gives the ratio of the estimate to the actual values.

Note that for $B = 4$ we have explicit formulas for the number of cubic extensions:

By Theorem 5.1, the number of non-Galois extensions is

$$(q^3 - q)\left(\frac{1}{2q+2} + 1 + (q-1)\right) = q^4 - \frac{q^2+q}{2},$$

and it is not hard to show that the number of Galois extensions is $(3q^2+3q+2)/2$, so the total number of cubic extension is q^4+q^2+q+1. It follows that for $B = 4$ the ratio in column 7 is equal to

$$1 + \frac{q^3 - q - 1}{q^4 + q^2 + q + 1}.$$

As in the number field setting, the leading term of the asymptotic expression overestimates the actual number of cubic function fields, which leads us to believe that the secondary term has a negative coefficient. An explicit computation of this secondary term is currently underway by Yongqiang Zhao (private communication, 2012).

One obstacle to generating larger amounts of data is the memory intensive nature of Algorithm 4.4 as written. One could obtain most of the results by instead looking for orbit representatives of $\mathrm{PGL}(2, q)$ acting on elliptic and hyperelliptic curves of genus g by iterating over these curves and computing their invariants. One would then only need to store a representative for each set of invariants. This would largely remove the storage requirements of the algorithm; however, it would also be a slower process as additional time must be spent computing these invariants.

For primes $\ell > 3$, no asymptotic estimates on counts of degree-ℓ function fields are known; it may be possible to obtain such estimates by generalizing the work of [9] or adapting the program of [37] to the case $q \equiv 1 \bmod \ell$ by using results in [13], [15], and [21]. It would be very interesting to see if the "gaps" for the number field setting referred to in Section 1 occur here as well. This is research in progress by the first two authors and several others.

We close by noting that our work is readily extendable to the problem of finding $\mathcal{D}_\ell$ extensions of function fields K other than $\mathbb{F}_q(x)$. This should be reasonably straightforward if one restricts to cases where $(\mathrm{Pic}^0 K)[\ell]$ is trivial. Work is also in progress to extend our algorithms to the cases when $q \not\equiv 1 \bmod \ell$. As in [8], one can construct cyclic function fields by adjoining the ℓ-th roots of unity to K, applying Kummer theory to the extension field, and finally taking a fixed field by the Frobenius automorphism of $\mathbb{F}_{q^{\ell-1}}/\mathbb{F}_q$. We expect that one can combine this technique with the work above to construct $\mathcal{D}_\ell$ function fields with $q \not\equiv 1 \bmod \ell$.

Acknowledgments

The first author is supported by NSERC and AITF of Canada. The second author is supported in part by NSERC of Canada.

References

[1] Jeffrey D. Achter, *The distribution of class groups of function fields*, J. Pure Appl. Algebra **204** (2006), no. 2, 316–333. MR 2006h:11132

[2] Manjul Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063. MR 2006m:11163

[3] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math. **193** (2013), no. 2, 439–499. MR 3090184

[4] Rajendra Bhatia, Arup Pal, G. Rangarajan, V. Srinivas, and M. Vanninathan (eds.), *Proceedings of the International Congress of Mathematicians (Hyderabad, 2010)*, vol. 2, New Delhi, Hindustan Book Agency, 2010. MR 2012d:00009

[5] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[6] H. Cohen, *Constructing and counting number fields*, in Li [20], 2002, pp. 129–138. http://www.mathunion.org/ICM/ICM2002.2/Main/icm2002.2.0129.0138.ocr.pdf MR 2003m:11186

[7] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, no. 193, Springer, New York, 2000. MR 2000k:11144

[8] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. Reine Angew. Math. **550** (2002), 169–209. MR 2004a:11115

[9] Henri Cohen and Anna Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478. MR 2012b:11168

[10] Boris Datskovsky and David J. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. **386** (1988), 116–138. MR 90b:11112

[11] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields, II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420. MR 58 #10816

[12] Jean-Marie De Koninck and Claude Levesque (eds.), *Théorie des nombres*: *Proceedings of the International Conference held at the Université Laval*, *Quebec*, *July* 5–18, 1987, Berlin, de Gruyter, 1989. MR 90f:11002

[13] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, 2009. arXiv 0912.0325v2 [math.NT]

[14] Eduardo Friedman and Lawrence C. Washington, *On the distribution of divisor class groups of curves over a finite field*, in De Koninck and Levesque [12], 1989, pp. 227–239. MR 91e:11138

[15] Derek Garton, *Random matrices and Cohen-Lenstra statistics for global fields with roots of unity*, Ph.D. thesis, University of Wisconsin — Madison, 2012. http://digital.library.wisc.edu/1711.dl/VB2JDB7JUO4RZ8N

[16] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 35, Springer, Berlin, 1996. MR 97i:11062

[17] Everett W. Howe, *On the group orders of elliptic curves over finite fields*, Compositio Math. **85** (1993), no. 2, 229–247. MR 94a:11089

[18] M. J. Jacobson, Jr., Y. Lee, R. Scheidler, and H. C. Williams, *Construction of all cubic function fields of a given square-free discriminant*, preprint, 2012.

[19] J. Jones, *Number fields* (searchable database), 2012. http://hobbes.la.asu.edu/NFDB

[20] Tatsien Li (ed.), *Proceedings of the International Congress of Mathematicians (Beijing, 2002)*, vol. 2, Beijing, Higher Education Press, 2002. MR 2003i:00010a

[21] Gunter Malle, *On the distribution of class groups of number fields*, Experiment. Math. **19** (2010), no. 4, 465–474. MR 2011m:11224

[22] Michael E. Pohst, *On computing non-Galois cubic global function fields of prescribed discriminant in characteristic > 3*, Publ. Math. Debrecen **79** (2011), no. 3-4, 611–621. MR 2907993

[23] David P. Roberts, *Density of cubic field discriminants*, Math. Comp. **70** (2001), no. 236, 1699–1705. MR 2002e:11142

[24] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, no. 210, Springer, New York, 2002. MR 2003d:11171

[25] Pieter Rozenhart, Michael Jacobson, and Renate Scheidler, *Tabulation of cubic function fields via polynomial binary cubic forms*, Math. Comp. **81** (2012), no. 280, 2335–2359. MR 2945159

[26] Pieter Rozenhart and Renate Scheidler, *Tabulation of cubic function fields with imaginary and unusual Hessian*, in van der Poorten and Stein [36], 2008, pp. 357–370. MR 2009m:11213

[27] Jean-Pierre Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, no. 42, Springer, New York, 1977. MR 56 #8675

[28] ———, *Algebraic groups and class fields*, Graduate Texts in Mathematics, no. 117, Springer, New York, 1988. MR 88i:14041

[29] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer, New York, 1986. MR 87g:11070

[30] Neil J. A. Sloane, *The on-line encyclopedia of integer sequences*, 2012. http://oeis.org

[31] Glenn Stevens, *Arithmetic on modular curves*, Progress in Mathematics, no. 20, Birkhäuser, Boston, 1982. MR 87b:11050

[32] Henning Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer, Berlin, 1993. MR 94k:14016

[33] Andrew V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147. MR 2012m:11079

[34] ———, *Defining equations for $X_1(N)$*, 2012. http://math.mit.edu/∼drew/X1_altcurves.html

[35] Takashi Taniguchi and Frank Thorne, *Secondary terms in counting functions for cubic fields*, 2011. arXiv 1102.2914v1 [math.NT]

[36] Alfred J. van der Poorten and Andreas Stein (eds.), *Algorithmic number theory: Proceedings of the 8th International Symposium (ANTS-VIII) held in Banff, AB, May 17–22, 2008*, Lecture Notes in Computer Science, no. 5011, Berlin, Springer, 2008. MR 2009h:11002

[37] Akshay Venkatesh and Jordan S. Ellenberg, *Statistics of number fields and function fields*, in Bhatia et al. [4], 2010, pp. 383–402. http://www.mathunion.org/ICM/ICM2010.2/Main/icm2010.2.0383.0402.pdf MR 2012h:11160

[38] Gabriel Daniel Villa Salvador, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications, Birkhäuser, Boston, 2006. MR 2007i:11002

[39] David J. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), no. 1, 17–50. MR 90b:11115

COLIN WEIR: colin_weir@sfu.ca
Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, BC V5A 1S6, Canada

RENATE SCHEIDLER: rscheidl@ucalgary.ca
Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada

EVERETT W. HOWE: however@alumni.caltech.edu
Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1969, United States

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS