CONSTRUCTING AND TABULATING DIHEDRAL FUNCTION FIELDS

COLIN WEIR AND RENATE SCHEIDLER

ABSTRACT. We present algorithms for constructing and tabulating degree ℓ dihedral function fields over a finite field $\mathbb{F}_q$ of odd characteristic with q congruent to 1 modulo ℓ. 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 the main theorem, which gives an exact count for such fields. We then use this construction method in a tabulation algorithm to construct all cubic function fields over $\mathbb{F}_q$ up to a given discriminant bound, and provide tabulation data.

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 [DH71] and for quartics in [Bha05], to name just two. 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 [Coh02], and extensive tables of data are available at [Jon12].

Far less is known in the function field setting; only the asymptotic counts for cubic [DW88] and abelian [Wri89] extensions have been proved. However, there is a general programme described by Ellenberg and Venkatesh [VE10] 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 Roberts [Rob01] to conjecture the secondary term in the theorem of [DH71]. His conjecture was later proved independently in [Tho11] and [BST10]. In the function field setting, however, there is practically no experimental data to potentially identify a similar such gap. The only known algorithms to construct or tabulate function fields are those of [JLSW12], [RS08] and [RJS12], all of which pertain to only certain classes of cubic function fields.

This paper represents a next step toward function field tabulation. It first presents a method for constructing all degree ℓ extensions of $\mathbb{F}_q(x)$ with prescribed ramification whose Galois group is the dihedral group of order 2ℓ and $q \equiv 1 \bmod \ell$. We utilize a Kummer theoretic approach inspired by the methods of Cohen [Coh00]

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

[CDyDO02] for number fields. This construction method can be converted into a tabulation algorithm in the usual manner via iteration. However, we are able to utilize 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 non-trivial automorphisms on the rational numbers. Exploiting $\mathbb{F}_q(x)$-automorphisms reduces the number of constructions by a factor of order q^3 compared to the naive approach. We present our improved tabulation procedure along with numerical data obtained from an implementation in MAGMA [BCP97]. 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 bound.

2. Preliminaries

Let ℓ be an odd prime and $\mathbb{F}_q$ a finite field of characteristic different from 2 and ℓ. We denote by K the rational function field over $\mathbb{F}_q$. Throughout this paper, we denote a degree i extension of K as K_i, and make the common abuse of language by saying a function field K_i has Galois group G, when we are in fact referring to the Galois group of its Galois closure. We will also always assume an extension F of a function field K has absolute constant field $\mathbb{F}_q$.

Let $\mathbb{P}(F)$ denote the set of places of a function field F/K, and let $e(P'|P)$ and $f(P|'P)$ denote the ramification index and relative degree of a place $P' \in \mathbb{P}(F)$ lying over $P \in \mathbb{P}(K)$, respectively. The norm of a place $P' \in \mathbb{P}(F)$ is

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

and the co-norm of $P \in \mathbb{P}(K)$ is

$$\mathrm{Con}_{F/K}(P) := \sum_{P'|P} e(P'|P)P'.$$

Then $\mathrm{N}_{F/K}(\mathrm{Con}_{F/K}(P)) = [F:K]P$. These definitions extend additively to divisors. In another abuse of notation, we will also use $\mathrm{N}_{F/K}$ to denote the norm map on elements of F. This is reasonable by Proposition 7.8 in [Ros02]: the norm of a principal divisor (α) of F is the principal divisor $(N_{F/K}(\alpha))$ of K. Restricting to the cases where the characteristic is different from 2 and ℓ guarantees that there are no wildly ramified places. Thus, the different of F/K is

$$\mathrm{Diff}_{F/K} := \sum_{P \in \mathbb{P}(K)} \sum_{P'|P} (e(P'|P) - 1)P'.$$

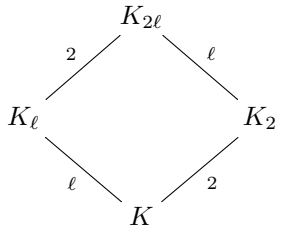
The discriminant divisor of F/K is defined as

$$\Delta_{F/K} := \mathrm{N}_{F/K}(\mathrm{Diff}_{F/K}) = \sum_{P \in \mathbb{P}(K)} \sum_{P'|P} (e(P'|P) - 1)f(P'|P)P.$$

When $K = \mathbb{F}_q(x)$, we drop K from the notation and simply write Δ_F. Note that the discriminant divisor is not the principal divisor of the discriminant as they differ at the infinite places. The discriminant divisor provides the ramification information at all places. Notice too that $\deg(\Delta_{F/K}) = \deg(\mathrm{Diff}_{F/K})$. Hence, one can replace $\mathrm{Diff}_{F/K}$ by $\Delta_{F/K}$ in the Hurwitz genus formula ([Sti00, Theorem 3.4.13]). For these reasons, we will henceforth describe the ramification of a function field in terms of its discriminant divisor.

Consider the diagram of function fields given in Figure 1. Here, the field $K_{2\ell}$ is the Galois closure of K_ℓ with Galois group $\mathcal{D}_\ell$, the dihedral group with 2ℓ elements.

FIGURE 1



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 conjugate subfields K_ℓ of $K_{2\ell}$. The field K_2 is called the *quadratic resolvent field* of K_ℓ. Let τ be a generator of $\mathrm{Gal}(K_2/K)$ and σ a generator of $\mathrm{Gal}(K_{2\ell}/K_2)$.

Our goal is to count the number of dihedral degree ℓ function fields with a given discriminant divisor and quadratic resolvent field. There is a one-to-one correspondence between non-conjugate 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 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 $\Delta_{K_\ell} = \Delta$.

3. Description of all degree ℓ dihedral fields

We count dihedral fields K_ℓ with fixed quadratic resolvent field K_2 by counting the cyclic degree ℓ extensions of K_2 as described above. As $q \equiv 1 \mod \ell$, all cyclic ℓ extensions are Kummer extensions. The next subsection describes Kummer extensions, and shows they are of the form $K_2(\sqrt[\ell]{\alpha})$ for some $\alpha \in K_2^\times \setminus (K_2^\times)^\ell$. We then give necessary and sufficient conditions on α such that $K_2(\sqrt[\ell]{\alpha})$ has Galois group $\mathcal{D}_\ell$. In the subsequent subsection, we decompose $K_2^\times/(K_2^\times)^\ell$ via virtual units to determine the elements α that correspond to non-isomorphic dihedral fields. With this information, we compute the discriminant divisor of $K_\ell \subset K_2(\sqrt[\ell]{\alpha})$ in terms of (α) and Δ_{K_2}. We conclude this section with a constructive proof of the main theorem; an exact count of the number of dihedral degree ℓ extensions of K with a given quadratic resolvent field K_2 and discriminant divisor.

3.1. Kummer Theory.

Let K_2 be a quadratic field with $q \equiv 1 \mod 2\ell$. Hence, all cyclic degree ℓ extensions of K_2 are Kummer extensions, which are completely described by the following theorem (see [VS06, Theorem 5.8.5 and Proposition 5.8.7]).

Theorem 3.1. *Let F be an algebraic function field containing a primitive ℓ-th root of unity, with $\ell > 1$ and ℓ relatively prime to the characteristic of F. Let $\alpha \in F^\times \setminus (F^\times)^\ell$. Define the Kummer extension $F' = F(\theta)$ with $\theta^\ell = \alpha$. Then the following hold.*

1. *The polynomial $T^\ell - \alpha$ is the minimal polynomial of θ. The extension F'/F has degree $[F' : F] = \ell$ and its Galois group is $\mathcal{C}_\ell$.*

(2) *Let $P \in \mathbb{P}(F)$ and $P' \in \mathbb{P}(F')$ lie over P. Then*

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

(3) *Every cyclic extension $F'|F$ of degree ℓ is a Kummer extension.*
(4) *Let $F' = F(\sqrt[\ell]{\alpha})$ and $F'' = F(\sqrt[\ell]{\beta})$. Then $F' = F''$ if and only if $\alpha = \beta^j \gamma^\ell$ for some $\gamma \in F^\times$ and $j \in \mathbb{Z}$, $1 \leq j \leq \ell - 1$.*

We construct dihedral degree ℓ fields with a given quadratic resolvent field K_2 by starting with the quadratic field K_2 and constructing, via Kummer's theorem, cyclic degree ℓ extensions of K_2 that are Galois with Galois group D_ℓ. It remains to classify the degree ℓ Kummer extensions of K_2 that are dihedral extensions of K.

Proposition 3.2. *Let K_2/K be a quadratic field and $K_2(\theta)$ an extension of K_2 where $\theta^\ell = \alpha \in K_2^\times$. Then $K_2(\theta)/K$ is Galois with $Gal(K_2(\theta)/K) = \mathcal{D}_\ell$ if and only if $\alpha \notin K$, $\alpha \notin (K_2^\times)^\ell$, and $N_{K_2/K}(\alpha) = \gamma^\ell$ for some $\gamma \in K$.*

Proof. By abuse of notation, let τ denote any lift of the non-trivial Galois automorphism of K_2/K to $K_2(\theta)/K$. Suppose that $\mathrm{Gal}(K_2(\theta)/K) = \mathcal{D}_\ell$. Then $K_2(\theta)/K_2$ is a nontrivial Kummer extension and hence $\alpha \notin (K_2^\times)^\ell$. By Theorem 3.1, $K_2(\theta)/K$ is Galois, so $\tau(\theta) \in K_2(\theta)$ and $\tau(\theta)^\ell = \tau(\alpha)$.

Suppose towards a contradiction that $\alpha \in K$, i.e. that $\tau(\alpha) = \alpha$. Let $\zeta \in K$ be a primitive ℓ-th root of unity and σ a generator of $\mathrm{Gal}(K_2(\theta)/K_2)$. Then

$$\tau(\theta)^\ell = \tau(\alpha) = \alpha = \theta^\ell,$$

and thus $\tau(\theta) = \zeta^i \theta$ for some i. However, as $\sigma(\theta) = \zeta^j \theta$ for some j, it follows that τ and σ commute; a contradiction. Furthermore, as $\alpha \in K_2$,

$$\mathrm{N}_{K_2/K}(\alpha) = \alpha\tau(\alpha) = (\theta\tau(\theta))^\ell.$$

Conversely, suppose that $\alpha \notin K$ and $\mathrm{N}_{K_2/K}(\alpha) = \gamma^\ell$ for some $\gamma \in K$. Then $\theta\gamma^{-1} \in K_2(\theta)$. Moreover,

$$(\theta\gamma^{-1})^\ell = \alpha \mathrm{N}_{K_2/K}(\alpha)^{-1} = \tau(\alpha).$$

As $\alpha \notin (K_2^\times)^\ell$, $K_2(\theta)/K_2$ is a degree ℓ Kummer extension. By Theorem 3.1, the minimal polynomial of θ over K_2 is $T^\ell - \alpha$ and by applying τ we have the minimal polynomial of $\tau(\theta)$, $T^\ell - \tau(\alpha)$. Therefore, $K_2(\theta)$ is the splitting field of $(T^\ell - \alpha)(T^\ell - \tau(\alpha)) \in K[T]$ and is Galois over K with Galois group $\mathcal{D}_\ell$. □

Elements in K_2 whose norm is an ℓ-th power in K have specific types of divisors, described below.

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

$$(\alpha) = \ell D'_\ell + \sum_{i=1}^{(\ell-1)/2} i(D'_i - \tau(D'_i)),$$

where $D'_i, i = 1, 2, \ldots, (\ell-1)/2$ are square-free effective divisors of K_2 with pairwise disjoint support. Consequently, each D'_i is only supported at places of K_2 which are split over K.

Proof. Let $P' \in \mathrm{supp}((\alpha))$ 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 $|r| \leq (\ell-1)/2$. Repeating this for all places $P' \in \mathrm{supp}((\alpha))$, we see that the divisor of α can be written uniquely as

$$(\alpha) = \ell D'_\ell + \sum_{i=1}^{(\ell-1)/2} i(D'_i - D'_{-i}),$$

where for all $i \in \mathbb{Z}$, $|i| \leq (\ell-1)/2$, all the D'_i are square-free effective divisors with disjoint support. Applying the norm map $N_{K_2/K}$ to (α) we obtain

$$(N_{K_2/K}(\alpha)) = (\tau(\alpha)) + (\alpha) = \ell D'_l + \sum_{i=1}^{(\ell-1)/2} i(D'_i - D'_{-i} + \tau(D'_i) - \tau(D'_{-i})).$$

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

$$D'_i - D'_{-i} + \tau(D'_i) - \tau(D'_{-i}) = 0 \text{ for all } 1 \leq i \leq (\ell-1)/2.$$

For $1 \leq i \leq (\ell-1)/2$, D'_i and D'_{-i} are effective. Moreover, as D'_i and D'_{-i} have disjoint support, it follows that $D'_i = \tau(D'_{-i})$. Therefore, the divisor of α is as claimed. □

3.2. **Virtual Unit Decomposition.** Kummer's Theorem 3.1 states that elements of K_2 in the same coset of $K_2^\times/(K_2^\times)^\ell$ produce the same Kummer extension. We wish to construct distinct dihedral 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 [Coh00]. In particular, we establish a one-to-one correspondence between cosets of certain groups of divisors and cosets $\alpha(K_2^\times)^\ell$, where $\mathrm{N}_{K_2/K}(\alpha) \in (K^\times)^\ell$.

Consider the following exact sequence:

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

where

$$V_\ell = \{\alpha \in K_2^\times : (\alpha) = \ell D' \text{ for some } D' \in \ Div(K_2)\}.$$

The elements of V_ℓ are called the (ℓ-)*virtual units* of the field K_2. Define the set V'_ℓ as

$$V'_\ell = \{D' \in \mathrm{Div}(K_2) : \ell D' \in \mathrm{Prin}(K_2)\}.$$

The map $\phi : V_\ell \to V'_\ell$, where $\phi(\alpha) = D'$, yields the exact sequence

$$1 \longrightarrow \mathbb{F}_q^\times/\mathbb{F}_q^{\times\ell} \longrightarrow V_\ell/(K_2^\times)^\ell \longrightarrow V'_\ell/\ell\,\mathrm{Prin}(K_2) \longrightarrow 1.$$

Now consider the natural map $\psi : V'_\ell \to \mathrm{Pic}^0(K_2)[\ell]$, where

$$\mathrm{Pic}^0(K_2)[\ell] \cong \mathrm{Pic}^0(K_2)/\ell\,\mathrm{Pic}^0(K_2)$$

is the ℓ-torsion of the degree 0 divisor class group of K_2. Then $\ker(\psi) = \ell\,\mathrm{Prin}(K_2)$, and thus (3.2) implies

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

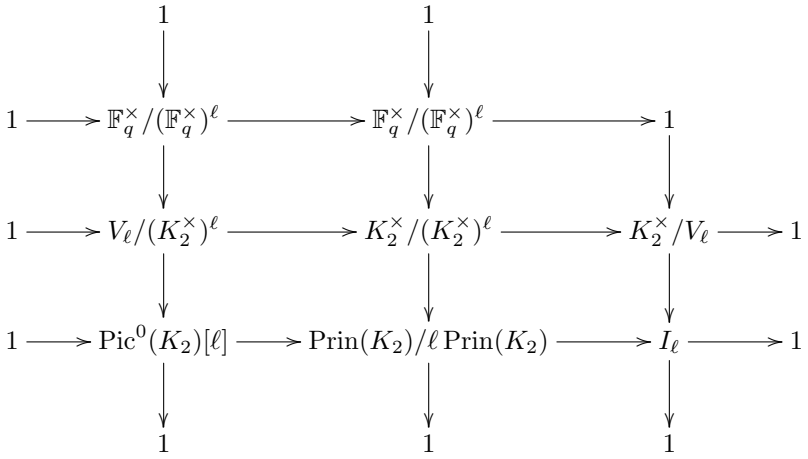
Returning to the sequence in (1), consider the group

$$I_\ell := \left\{D' + \ell\,\mathrm{Div}(K_2) \in \mathrm{Div}(K_2)/\ell\,\mathrm{Div}(K_2) : [D'] \in \ell\,\mathrm{Pic}^0(K_2)\right\},$$

where $[D']$ denotes the divisor class of D'. We define the map $\varphi : K_2^\times \to I_\ell$ such that $\varphi(\alpha) := (\alpha) + \ell\,\mathrm{Div}(K_2)$. Then φ is surjective by definition of I_ℓ, since for all

$D' + \ell \operatorname{Div}(K_2)$ there exists an element $\alpha \in K_2^\times$ such that $(\alpha) = D' - \ell E'$ for some $E' \in \operatorname{Div}(K_2)$. Hence, $\varphi(\alpha) = D' + \ell \operatorname{Div}(K_2)$. Moreover, $\ker(\varphi) = V_\ell$. Therefore, $K_2^\times / V_\ell \cong I_\ell$. This yields the diagram of exact sequences depicted in Figure 2.

FIGURE 2. Virtual Unit Decomposition



Using the sequences in Figure 2, we see that cosets $\alpha(K_2^\times)^\ell$ correspond to cosets of $\operatorname{Prin}(K_2)/\ell \operatorname{Prin}(K_2)$ up to a choice of constant in $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\ell$. However, by Proposition 3.2, Kummer extensions $K_2(\sqrt[\ell]{\alpha})$ of K_2 such that $\operatorname{Gal}(K_2(\sqrt[\ell]{\alpha})/K) \cong \mathcal{D}_\ell$ correspond to cosets $\alpha(K_2^\times)^\ell$ such that $\mathrm{N}_{K_2/K}(\alpha) \in (K^\times)^\ell$. We now describe the correspondence between cosets of this type and their divisors.

Proposition 3.4. *Let H be the group*

$$H = \left\{\alpha \in K_2^\times : N_{K_2/K}(\alpha) \in (K^\times)^\ell\right\},$$

and let (H) be the group of divisors of elements in H. Then

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

is an exact sequence.

Proof. 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 $N_{K_2/K}(k) \in (K^\times)^\ell$. 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 $k \in (\mathbb{F}_q^\times)^\ell$. □

The following two corollaries follow directly from Propositions 3.3 and 3.4, and Figure 2.

Corollary 3.5. *For every coset $(\beta)+\ell\, Prin(K_2)$ such that $N_{K_2/K}((\beta)) \in \ell\, Prin(K)$, there is a unique lift $\alpha(K_2^\times)^\ell$ such that $(\alpha) = (\beta)$ and $N_{K_2/K}(\alpha) \in (K^\times)^\ell$.*

Corollary 3.6. *Let U be the set*

$$U = \left\{ B \in I_\ell : B = \sum_{i=1}^{(\ell-1)/2} i(D_i' - \tau(D_i')) + \ell\, Div(K_2) \right\}$$

where D_i', $i = 1, 2, \ldots, (\ell-1)/2$ are square-free effective divisors with disjoint support. Let S the set of pairs (A, B) with $A \in Pic^0(K_2)[\ell]$ and $B \in U$. Then there is a one-to-one correspondence between the cosets $\alpha(K_2^\times)^\ell$ such that $N_{K_2/K}(\alpha) \in (K^\times)^\ell$ and the set S.

By Theorem 3.1, $K_2(\sqrt[\ell]{\alpha}) = K_2(\sqrt[\ell]{\alpha^j})$ for all $j \in \mathbb{Z}$ with $0 < j < \ell$. Thus, to construct distinct Kummer extensions, we define an equivalence relation $\sim$ on the set S by

$(A, B) \sim (A', B')$ if and only if $A = jA'$ and $B = jB'$ for some $j \in \mathbb{Z}$, $0 < j < \ell$.

We then obtain the following theorem:

Theorem 3.7. *There is a one-to-one correspondence between Kummer extensions $K_{2\ell}/K_2$ such that $Gal(K_{2\ell}/K_2) \cong \mathcal{D}_\ell$ and the set of non-trivial equivalence classes of S, denoted $S/\sim$.*

3.3. **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 $\Delta_{K_{2\ell}/K_2}$.

Lemma 3.8. *Let K_2 be a quadratic 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*

$$\Delta_{K_{2\ell}/K_2} = (\ell - 1) \sum_{i=1}^{(\ell-1)/2} D_i' + \tau(D_i'),$$

where the D_i' arise from the representation of (α) as described in Proposition 3.3.

Proof. By Theorem 3.1, for all places $P' \in \mathrm{supp}(D_i')$ where $1 \le i \le (\ell-1)/2$, there is a unique place P'' of $K_{2\ell}$ lying over P' such that $e(P''|P') = \ell$. Furthermore, all other places of K_2 are unramified in $K_{2\ell}/K_2$. □

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 [Ser77, Ch. 3]). The fields K, K_2, K_ℓ and $K_{2\ell}$ of Figure 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 [Gos98, Ch. 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

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

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

By Corollary 3.4.12 (a) of [Sti00], $\mathrm{Diff}_{K_{2\ell}} = \mathrm{Con}_{K_{2\ell}/K_2}(\mathrm{Diff}_{K_2}) + \mathrm{Diff}_{K_{2\ell}/K_2}$. 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

$$\Delta_{K_{2\ell}/K_2} = (\ell-1)\sum_{i=1}^{(\ell-1)/2} D_i' + \tau(D_i').$$

Define the divisor M as

$$M := \sum_{i=1}^{(\ell-1)/2)} \sum_{P\in\mathrm{supp}(D_i)} P.$$

Then $\mathrm{N}_{K_2/K}(\Delta_{K_{2\ell}/K_2}) = 2(\ell-1)M$, and equation (2) 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 ramification divisor of K_ℓ.

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

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 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 $P'' \in \mathbb{P}(K_{2\ell})$ lying over P, $e(P''|P) = \ell$. Similarly, for all places $P \in \mathrm{supp}(\Delta_{K_2})$ and all $P'' \in \mathbb{P}(K_{2\ell})$ lying over P, $e(P''|P) = 2$.

As $[K_{2\ell} : K_\ell] = 2 \nmid \ell$, all places $P' \in \mathbb{P}(K_\ell)$ lying over M must have $e(P'|P) = \ell$. Also, for all $P' \in \mathbb{P}(K_\ell)$ lying over Δ_{K_2}, $e(P'|P) \le 2$. Applying

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

to any place $P \in \mathrm{supp}(\Delta_{K_2})$ allows at most $(\ell-1)/2$ places $P'|P$ 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.

3.4. **The Number of $\mathcal{D}_\ell$ Function Fields.** We now prove the main result, Theorem 3.10, providing the number of non-conjugate 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 between dihedral degree ℓ extensions and certain divisor classes, and the discriminant divisor result of Theorem 3.9. First, we require some more notation.

Let $M \in \mathrm{Div}(K)$ be a square-free effective divisor such that every place P in $\mathrm{supp}(M)$ splits in K_2 as $P_0' + P_1'$. We then define

$$\mathcal{P}_\ell(M) := \left\{ \sum_{P\in\mathrm{supp}(M)} n_i P_j' : n_i \in \mathbb{Z},\, 0 < n_i \le (\ell-1)/2,\, j \in \{0,1\} \right\}.$$

Let $N = \#\,\mathrm{supp}(M)$. Then

$$\#\mathcal{P}_\ell(M) = \left(\frac{\ell-1}{2}\right)^N 2^N = (\ell-1)^N.$$

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 odd and $q \equiv 1 \bmod \ell$. Let r denote the ℓ-rank of $Pic^0(K_2)$ and M a sum of distinct places of K, i.e. $M = \sum_i P_i$ with $P_i \neq P_j$, supported away from D. Let $\Delta = \frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M$.*

(1) *If $M = 0$, then there are exactly $(\ell^r - 1)/(\ell - 1)$ non-conjugate dihedral degree ℓ fields with discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2.*
(2) *If $M \neq 0$, then consider the set*

$$T_\ell = \{E' \in \mathcal{P}_\ell(M) : E' - \tau(E') \in \ell\, Pic^0(K_2)\}.$$

If all $P \in supp(M)$ split in K_2 as $P = P_0' + P_1'$, then there are exactly $\ell^r(\#T_\ell)/(\ell-1)$ non-conjugate dihedral degree ℓ fields with discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2. Otherwise, there are no degree ℓ dihedral fields with discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2.

Proof. For ease of notation, set $T_\ell = \{0\}$ if $M = 0$. Using the correspondence of Theorem 3.7, the number of non-conjugate dihedral degree ℓ fields with discriminant divisor $\Delta_{K_\ell} = \Delta$ and quadratic resolvent field K_2 is the number of non-trivial equivalence classes of pairs (A, B), with A a class of $\mathrm{Pic}^0(K_2)[\ell]$ and $B = \{E' + \ell\,\mathrm{Div}(K_2) : E \in T_\ell\} \subset I_\ell$.

In case (1), B is only the trivial coset. There are $\ell^r - 1$ non-trivial elements of A, so there are $(\ell^r-1)/(\ell-1)$ non-trivial equivalence classes, and thus $(\ell^r-1)/(\ell-1)$ distinct fields.

In case (2), as $\#\,\mathrm{Pic}^0(K_2)[\ell] = \ell^r$, there are $\ell^r(\#T_\ell)$ nontrivial pairs (A, B), and therefore $\ell^r(\#T_\ell)/(\ell-1)$ non-trivial equivalence classes. Thus, this is also the number of distinct fields as specified above. □

4. Algorithms and Data

4.1. **Construction Algorithm.** The correspondence of Theorem 3.7 is explicit, and the proof of Theorem 3.10 is constructive, which naturally leads to Algorithm 1. This algorithm which takes as input a quadratic function field K_2 and an effective square-free divisor M of K and outputs all non-conjugate degree ℓ dihedral fields with discriminant divisor $\frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M$.

Note that there are exactly two quadratic fields with a fixed discriminant divisor; they are in fact twists of each other. This leads to Algorithm 2, which on input a pair of effective square-free divisors D and M of K utilizes Algorithm 1 to generate all non-conjugate degree ℓ dihedral fields with discriminant divisor $\frac{\ell-1}{2}D + (\ell-1)M$.

Let K_2 and K_2' be the two fields with discriminant divisor D. Then, as K_2 and K_2' are twists of each other, a place $P \notin \mathrm{supp}(D)$ splits in K_2 if and only if it is inert in K_2' and vice versa. In order for any degree ℓ dihedral fields K_ℓ to exist, all the places in the support of M must be split over the quadratic resolvent field of K_ℓ. Thus, if M is non-zero, only one of K_2 and K_2' needs to be considered.

Algorithm 1 is precisely the construction in the proof of Theorem 3.10 and thus gives all elements α such that $K_2(\sqrt[\ell]{\alpha})$ is a Galois dihedral function field. The equivalence relation $\sim$ in step 7 is that of Theorem 3.7 but restricted to only one set. Notice that the REPEAT loops in steps 13 and 18 will halt, as by Proposition 3.4, there is a unique $\beta \in K_2$ such $(\beta) = B' - \tau(B') - \ell E'$ and $\mathrm{N}(\beta) \in (K^\times)^\ell$; similarly

Algorithm 1 Constructing $\mathcal{D}_\ell$ Fields From Their Quadratic Resolvent

1: INPUT: (K_2, ℓ, M)
2: OUTPUT: $L_2 = \left\{K_\ell : \Delta_{K_\ell} = \frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M, \texttt{QuadRes}(K_\ell) = K_2\right\}$
3: set $E = \{\}, L_2 = \{\}, L = \{\}$, $T_2 = \{\}$, $V = \{\}$
4: for $P \in \texttt{supp}(M)$ do
5: ensure $P = P_0' + P_1'$ in $\texttt{Div}(K_2)$, return E on failure
6: $L = L \cup \{(P_0', P_1')\}$
7: compute a basis $\{A_1, \ldots, A_r\}$ of $\texttt{Pic}^0(K_2)$, an ℓ-th root of unity $\zeta \in \mathbb{F}_q$, $\mathcal{P}_\ell(M)$ from L, and $T_1 = \{B' - \tau(B') : B' \in \mathcal{P}_\ell(M)\}$, and $T_1/\sim$
8: [Compute function of divisors in $T_\ell \subset I_\ell$]
9: for $B' - \tau(B') \in T_1/\sim$ do
10: if $B' - \tau(B') \in \ell\,\texttt{Pic}^0(K_2)$ then
11: compute E' such that $B' - \tau(B') \equiv \ell E'$
12: find $\beta \in K_2$ such that $(\beta) = B' - \tau(B') - \ell E'$.
13: repeat $\beta = \zeta\beta$ until $\texttt{N}(\beta) \in (K^\times)^\ell$
14: $T_2 = T_2 \cup \{\beta\}$
15: [Compute Virtual Units]
16: for i from 1 to r do
17: find $\gamma_i \in K_2$ such that $(\gamma_i) = \ell A_i$
18: repeat $\gamma_i = \zeta\gamma_i$ until $\texttt{N}(\gamma_i) \in (K^\times)^\ell$
19: $V = V \cup \{\gamma_i\}$
20: [Create the defining equations]
21: if $M = 0$ then
22: set $T_2 = \{\gamma_1\}$ and remove γ_1 from V
23: for $\beta \in T_2$ do
24: for $[z_i] \in (\mathbb{Z}/\ell\mathbb{Z})^{\#V}$ do
25: compute $\alpha := \beta \prod_{\gamma \in V} \alpha^{z_i}$
26: compute the resultant $R(X) = \mathrm{Res}_Y(Y^\ell - \alpha, (X-Y)^\ell - \tau(\alpha))$
27: factor $R(X)$ and let $C(X)$ be a factor of degree ℓ.
28: $L_2 = L_2 \cup \{C(X)\}$
29: return E

for γ. It remains to show that steps 25-27 indeed find a defining equation for a degree ℓ subfield of $K_2(\sqrt[\ell]{\alpha})$.

Let $\theta \in K_{2\ell}$ be such that $\theta^\ell = \alpha$ of step 25 and let $\theta_i = \zeta^i\theta$, where $\zeta \in \mathbb{F}_q$ is an ℓ-th root of unity. The roots of $R(X)$ are all of the form $\theta_i + \tau(\theta_j)$, for all $0 \le i, j, \le \ell - 1$ where τ denotes a lift to $K_{2\ell}$ of the non trivial Galois automorphism of K_2/K. Let σ be a generator of $\mathrm{Gal}(K_2(\theta)/K_2)$. Then consider the ℓ polynomials

$$Q_j = \prod_{k=0}^{\ell-1} (X - \sigma^i(\theta_j + \tau(\theta_j)))$$

for $0 \le j < \ell$. Notice that Q_j is clearly stable under σ. Moreover, as $\tau\sigma\tau = \sigma^{-1}$, Q_j is stable under τ as well. Consequently $Q_j \in K[X]$.

We claim that Q_j is the minimal polynomial of $\theta_j + \tau(\theta_j)$ which is an element of some index 2 subfield of $K_2(\theta)$. As $\theta_j + \tau(\theta_j)$ is invariant under τ, it lies in its fixed field. However, as it is not invariant under σ, it does not lie in K. Thus, as ℓ is prime, $\theta_j + \tau(\theta_j) \in K_\ell$ for some $K_2(\theta)/K_\ell/K$ with $[K_2(\theta) : K_\ell] = 2$. Hence,

$\theta_j + \tau(\theta_j)$ has a degree ℓ monic irreducible minimal polynomial $m_j \in K[X]$. As $\theta_j + \tau(\theta_j)$ is a root of Q_j, m_j divides Q_j. However, Q_j is also a monic polynomial of degree ℓ, and therefore $m_j = Q_j$. So there are ℓ possible choices of irreducible factors of $R(X)$, each one corresponding to a conjugate subfield of $K_2(\sqrt[\ell]{\alpha})$.

Remarks 4.1. There are several ways to perform Algorithm 1 more efficiently.

(1) For any value of ℓ one can compute the minimal polynomial of the fixed field of $K_2(\sqrt[\ell]{\alpha})$ by τ directly by symbolically expanding Q_1. For example, when $\ell = 3$, K_3 has equation $X^3 - 3\sqrt[3]{\mathrm{N}_{K_2/K}(\alpha)}\,X - \mathrm{Tr}_{K_2/K}(\alpha)$. This avoids having to compute and factor a resolvent polynomial.

(2) As we have a basis for $\mathrm{Pic}^0(K_2)$, we can easily check if an element D' is in $\mathrm{Pic}^0(K_2)[\ell]$ by writing it in terms of the basis elements, and obtain E' such that $\ell[E'] = [D']$ as required in line 11. Suppose

$$[D'] = \bigoplus_{i=1}^{r} d_i A_i.$$

If the order of A_i is divisible by ℓ, then check that $\ell \mid d_i$, as otherwise D' is not an ℓ-scalar multiple. If this is the case, set $e_i = d_i/\ell$. If the order of A_i is not divisible by ℓ, then compute $\ell^{-1} \mod \mathrm{ord}(A_i)$ and set $e_i = \ell^{-1} d_i$. Then return E' such that $\ell[E'] = [D']$, where

$$E' = \bigoplus_{i=1}^{r} e_i A_i.$$

(3) As K_2 is a quadratic field, it corresponds to a hyperelliptic curve $y^2 = f(x)$. One can often take advantage of faster arithmetic available for the Jacobians of hyperelliptic curves, denoted $\mathrm{Jac}(K_2)$, instead of the slower generic arithmetic in $\mathrm{Pic}^0(K_2)$. For example, in MAGMA, such packages are available as long as the infinite place of K is not inert K_2. This faster arithmetic utilizes the Mumford representation for $\mathrm{Div}^0(K_2)$. One should compute $\mathrm{Jac}(K_2)$ using Mumford representations instead of $\mathrm{Pic}^0(K_2)$ and map all calculations to and from $\mathrm{Jac}(K_2)$.

Mapping the divisors in $T_1/\sim$ of step 10 and 11 into $\mathrm{Jac}(K_2)$ can be done quite efficiently as we know the support of all $t \in T_1$. For example, if the infinite place P_∞ of K is ramified in K_2, say $P_\infty = 2P'_\infty$, then we can rewrite t as

$$t = \sum_{P' \in \mathrm{supp}(t)} n_{P'}(P' - \deg(P')P'_\infty)$$

In our algorithm t is supported away from P'_∞; thus, all $P' \in \mathrm{supp}(t)$ are finite. Finding the Mumford representation $J_{P'}$ of $P' - \deg(P')P'_\infty$ is quite simple, and so we can use the fast arithmetic of $\mathrm{Jac}(K_2)$ to compute $\sum_{P' \in \mathrm{supp}(t)} n_{P'} J_{P'}$ efficiently.

(4) The coefficients of $R(X)$ and $C(X)$ can easily become very large if Algorithm 1 is run as stated. To avoid this, after line 25, given the element α one may wish to look for an element α' such that $K_2(\sqrt[\ell]{\alpha}) = K_2(\sqrt[\ell]{\alpha'})$. The element α' viewed as an element of $K(x)[y]$ should be chosen such that it has integral coefficients of small degree. One can search for such an element by considering various powers of α and factoring out common ℓ-th powers from the coefficients.

Algorithm 2 Constructing All $\mathcal{D}_l$ Fields from Divisors

```
1: INPUT: ℓ and square-free effective divisors D and M
2: OUTPUT: L_2 = {K_ℓ : Δ_{K_ℓ} = ((ℓ−1)/2) Δ_{K_2} + (ℓ−1)M}
3: if deg(D) is even then
4:      construct K_2, K_2' with discriminant divisor D
5: else
6:      return "NOT A QUADRATIC DISCRIMINANT DIVISOR"
7: if M ≠ 0 then
8:      pick P ∈ supp(M)
9:      if P = P_0' + P_1' in Div(K_2) then
10:          set K_2'' = K_2
11:     else
12:          set K_2'' = K_2'
13:     get L from Algorithm 1 with input K_2'', ℓ, M
14: else
15:     get L_1 from Algorithm 1 with input K_2, ℓ, M
16:     get L_2 from Algorithm 1 with input K_2', ℓ, M
17:     set L = L_1 ∪ L_2.
18: return  L
```

Note that in Algorithm 2, all finite places P of K correspond to irreducible polynomials $f_P(x) \in \mathbb{F}_q[x]$. Therefore, in step 4, we can easily construct K_2 as the function field of the hyperelliptic curve

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

4.2. **Tabulation Algorithm.** Algorithm 1 for constructing all degree ℓ dihedral fields with a given discriminant divisor and quadratic resolvent field can easily be adapted, via iteration, to a procedure for tabulating all such extensions whose discriminant divisor has degree below a fixed input bound $B > 0$. However, in this context, we can utilize the automorphism group of K to significantly reduce the number of quadratic fields that need to be considered.

Recall that $\mathrm{Aut}(K) = \mathrm{Aut}(\mathbb{F}_q(x)) \cong \mathrm{PGL}(2, q)$, the group of fractional linear transformations of x. Given any $\phi \in \mathrm{Aut}(K)$, ϕ lifts to a map on $K_{2\ell}$, and hence to all its subfields. Consequently, ϕ also lifts to a map on the corresponding divisor groups. Moreover, $\phi(\Delta_{K_i}) = \Delta_{\phi(K_i)}$. Therefore, instead of applying Algorithm 1 to all suitable K_2 and M, we only need to consider a representative from each orbit of $\mathrm{Aut}(K)$ acting on the set of suitable quadratic fields K_2. Moreover, for each field K_2 we need only consider representatives of the action of the stabilizer $\mathrm{Stab}(K_2) \subset \mathrm{PGL}(2, q)$ on the set of suitable M.

This is captured below in three algorithms. The first (Algorithm 3) finds orbit representatives for the set of suitable quadratic fields. The second (Algorithm 4) constructs minimal polynomials for all dihedral fields with ramification divisors $\frac{\ell-1}{2}\Delta_{K_2}+(\ell-1)M$ for representatives K_2 and M. The third (Algorithm 5) reapplies $\mathrm{Aut}(K)$ to each of the constructed minimal polynomials to obtain the full list of degree ℓ dihedral fields whose discriminant divisor has degree bounded by B.

Recall that every quadratic field K_2 can be expressed as $K(y)$ where $y^2 = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ square-free and $\deg(f)$ is either $2g + 1$ or $2g + 2$, where g is

the genus of K_2. 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, or equivalently, the discriminant divisors of K_2 and $\phi(K_2)$ have the same degree, namely $2g+2$. We further note that $\deg(\Delta_{K_2}) = 2\lceil \deg(f)/2 \rceil$.

Algorithm 3 List K_2 Orbit Representatives Under $\mathrm{PGL}(2,q)$ Action

INPUT B, ℓ, q
OUTPUT: $R = \{(f, \mathtt{Stab}_{\mathtt{PGL}(2,q)}(f))\}$, the list of orbit representatives and their stabilizers
compute a primitive element $g \in \mathbb{F}_q$
set $L(f) = 0$ for all $f \in \mathbb{F}_q[x]$
for $h(x) \in \mathbb{F}_q[x]$ such that $2\lceil \deg(f)/2 \rceil \leq \left\lfloor \frac{2B}{\ell-1} \right\rfloor$ do
    if $L(f) = 0$ then
        for $\phi = \frac{ax+b}{cx+d} \in \mathtt{PGL}(2,q)$ do
            $f'(x) = (cx+d)^{2\lceil \deg(f)/2 \rceil} \phi(f(x))$
            for i from 1 to $(q-1)/2$ do
                $f' = h^2 f'$
                $L(f') = 1$
                if $f' = f$ then
                    $S = S \cup \{\phi\}$
        $R = R \cup \{(f, S)\}$
        $S = \emptyset$
return R

Algorithm 4 Tabulate Dihedral Fields under $\mathrm{PGL}(2,q)$ with $\deg(\Delta_{K_\ell}) \leq B$

INPUT: B, ℓ, q
OUTPUT: $L = \{(\{K_\ell\}, \Delta_{K_\ell}, \mathtt{Stab}_{\mathtt{PGL}(2,q)}(\Delta_{K_\ell})) : \mathtt{QuadRes}(K_\ell) = K_2 \in R\}$
get $R = \{(f, S)\}$ from Algorithm 3
for $(f, S) \in R$ do
    set $M_{K_2} := \{\}$, $K_2 = K(x)[y]/\langle y^2 - f \rangle$ and compute Δ_{K_2}
    compute $B_M = \lfloor B/(\ell-1) - \deg(f)/2 \rfloor$
    compute lists $L_j = \{P \in K : \deg(P) = j\}$ for $j \leq B_M$
    for i from 0 to B_M do
        for every partition $p = [n_1, .., n_r]$ of i do
            generate $M_p = \{\sum_{k=1}^{r} P_k : P_k \in L_k\}$
            $M_f = M_f \cup M_p$
    compute $M/S = \{(E/S(E), \mathtt{Stab}_S(E)) : E \in M_f\}$
    for $(M, \mathtt{Stab}_S(M)) \in M/S$ do
        get L_{K_2} from Algorithm 1 on (K_2, ℓ, M)
        $L = L \cup \{(L_{K_2}, \frac{\ell-1}{2}\Delta_{K_2} + (\ell-1)M, \mathtt{Stab}_S(M))\}$
return L

4.3. **Numerical Results.** Our algorithm was implemented in MAGMA [BCP97]. In Table 1, we provide tabulation data for the case of all even bounds $B > 4$ and odd primes ℓ and odd prime powers $q \equiv 1 \mod \ell$ such that $q^{2B/(\ell-1)+1} < 2^{29}$.

Algorithm 5 Reapply $\mathrm{PGL}(2,q)$ to the Dihedral Fields

INPUT: $R_2 = \{(\{K_\ell\}, \Delta_{K_\ell}, \mathtt{Stab}_{\mathtt{PGL}(2,q)}(\Delta_{K_\ell}))\}$ from Algorithm 4
OUTPUT: $L = \{(K_\ell, \Delta_{K_\ell}) : \deg(\Delta_{K_\ell}) \leq B\}$
set $L = \{\}$
for $(\{K_\ell\}, \Delta, S) \in R_2$ do
    for $\phi \in \mathtt{PGL}(2,q)/S$ do
        for $F \in \{K_\ell\}$ do
            $L = L \cup \{(\phi(F), \phi(\Delta))\}$
return L

TABLE 1. Field counts for all q, ℓ with $q^{\frac{2B}{\ell-1}+1} < 2^{29}$ for $B \geq 4$

ℓ	q	B	$K_2/\sim$	$K_\ell/\sim$	K_ℓ	T_1	T_2	T_3	R
3	7	4	30	16	2,352	2.73	0.33	1.27	25.6
		6	749	471	117,264	87.9	9.31	47.34	21.6
		8	34,228	18,138	5,762,064	4,861.1	653.92	2,254.2	28.2
	13	4	58	32	28,392	47.7	0.58	15.35	19.9
		6	4,589	2,563	4,824,456	5510.2	66.89	1869.0	19.6
	19	4	78	40	129,960	273.2	0.74	70.4	14.69
	25	4	106	56	390,000	1,203.4	1.38	233.5	14.96
	31	4	126	64	922,560	2,851.4	1.56	507.7	13.81
	37	4	154	78	1,822,176	7,076.5	1.60	955.6	10.8
	43	4	174	86	3,337,488	14,119.2	1.70	1893.4	8.43
	49	4	202	102	5,644,800	32,406.2	2.41	6,743.1	7.24
5	11	8	42	8	6,660	20.2	0.45	3.30	46.38
		12	2813	948	1,058,640	1774.2	47.1	514.49	26.6
	31	8	126	32	446,400	2851.8	1.71	272.0	16.28
	41	8	166	42	1,308,720	11269.6	2.10	802.1	11.9
7	29	12	118	18	219,240	2114.4	1.72	126.47	18.68
	43	12	174	26	1,006,544	14119.2	2.34	644.0	12.59
11	23	20	90	7	48,576	659.9	1.94	28.2	34.1
13	53	24	214	18	1,190,592	41962.8	10.4	1147.2	35.89
23	47	44	186	8	415,104	31542.1	12.2	419.0	39.5

The column entitled $K_2/\sim$ represents the number of quadratic fields generated by Algorithm 3. The number of cubic fields constructed by Algorithm 4 is under the column $K_\ell/\sim$, and the total number of non-Galois fields whose discriminant divisor has degree at most B is under column K_ℓ. The running time in seconds of Algorithms 3, 4, and 5 are listed under T_1, T_2, and T_3, respectively. For each q and B, we also computed $R = (q^3 - q)T_2/(T_1 + T_2 + T_3)$, which estimates the approximate improvement factor obtained by our tabulation method relative to simply iterating Algorithm 1 over all possible quadratic fields.

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 run time improvement. Overall, the run time of Algorithm 1 is dominated by the construction of the set $\mathcal{P}_\ell(M)$ and

obtaining functions for the principal divisors in steps 12 and 17. Data suggests that as B grows, finding the generators of these principal divisors will tend to dominate the run time.

The entries of columns 4 and 5 of Table 1 differ by a factor that is very close to $\ell - 1$. This seems to suggest that the size of the moduli space of Galois D_ℓ curves under $\mathrm{PGL}(2, q)$ is approximately $1/(\ell - 1)$ times the size of the corresponding space for hyperelliptic curves. We also notice that the total number of D_ℓ fields for a fixed B and q is always divisible by $q^3 - q$, the order of $\mathrm{PGL}(2, q)$, despite the existence of non-trivial stabilizers.

5. Conclusions and Future Work

It is interesting that the number of degree ℓ dihedral function fields with a given discriminant divisor $\Delta = \frac{\ell-1}{2}D + (\ell - 1)M$ 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 K_2. The probability that the divisor class group of K_2 has a certain ℓ-Sylow subgroup is the focus of various Cohen-Lenstra type heuristics. These are discussed further in [FW89], [Ach06], [Mal08], and [Gar12], and directly relate to the number of D_l fields with square-free discriminant divisor.

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 $T_\ell = \{E' \in \mathcal{P}_\ell(M) \mid E' - \tau(E') \in \ell \operatorname{Pic}^0(K_2)\}$. One can show that every divisor class of K_2 contains an element whose norm is an ℓ-th power in $K^\times$. The natural homomorphism from divisor classes whose norm is an ℓ-th power to $\operatorname{Pic}^0(K_2)/\ell \operatorname{Pic}^0(K_2)$ is surjective, so a randomly chosen element is in the kernel of this map with probability $(\#(\operatorname{Pic}^0(K_2)/\ell \operatorname{Pic}^0(K_2)))^{-1} = \ell^{-r}$. Thus, assuming that the set $T'_\ell = \{E' - \tau(E') : E' \in \mathcal{P}_\ell(M)\}$ has the same distribution, the expected number of degree ℓ dihedral fields with the given discriminant divisor $\Delta = \frac{\ell-1}{2}D + (\ell - 1)M$ is $\#T'_\ell/(\ell - 1)$, which is independent of r. When $\deg(M)$ 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 discriminant bound. As the number of Galois cubics is negligible by comparison, it is reasonable to compare the number of non-Galois cubics to the asymptotic estimate of [DW88]:

$$\lim_{B\to\infty} q^{-B} \sum_{\substack{K_3/K \\ \deg \Delta_{K_3} = q^B}} 1 = \frac{q}{(q-1)\zeta(3)}.$$

This comparison is shown in Table 2. The above asymptotic estimate is given for all computed values of q and B in column 4. Column 5 provides the ratio of the asymptotic estimate over the actual number of non-Galois cubic function fields. As in the number field setting, the leading term of the asymptotic overestimates the number of cubic fields. Thus, similar to the number field setting, this leads us to believe that the secondary term has a negative coefficient. An explicit computation of the secondary terms is currently underway by Yongqiang Zhao [Zha].

We also include, in the last column of Table 2, the number of cubic fields divided by the order of $\mathrm{PGL}(2, q)$. As mentioned, in all cases $q^3 - q$ divides the number of D_ℓ fields. Taking the quotient, we see that the number of non-Galois cubic fields

TABLE 2. Cubic field counts compared to asymptotics for all q with $q^{B+1} < 2^{29}$, $B \geq 4$

q	B	$\#K_3$	$q^{B+1}/((q-1)\zeta(3))$	Ratio	$\#K_3/(q^3-q)$
7	4	2,352	2,736	1.163	7
	6	117,264	134,064	1.143	349
	8	5,762,064	6,569,136	1.140	17149
13	4	28,392	30,744	1.083	13
	6	4,824,456	5,195,735	1.077	2209
19	4	129,960	137,160	1.055	19
25	4	390,000	406,224	1.042	25
31	4	922,560	953,280	1.033	31
37	4	1,822,176	1,924,776	1.056	36
43	4	3,337,488	3,498,264	1.048	42
49	4	5,644,800	5,882,400	1.042	48

whose discriminant divisor is degree at most 4, is either $q(q^3-q)$ or $(q-1)(q^3-q)$ for the cases we computed. We are unsure why is this is the case. Perhaps additional data and further analysis will shed more light on these patterns.

For larger primes ℓ, no asymptotic estimates are known; it may be possible to obtain such estimates by generalizing the work of [CM11] or adapting the programme of [VE10] to the case $q \equiv 1 \bmod \ell$ by utilizing results [EVW], [Mal08] and [Gar12]. 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 authors and several others.

We also note that our work is readily extendable to relative extensions where $\mathbb{F}_q(x)$ is replaced by a higher degree function field K. This should be relatively 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 [CDyDO02], one can construct cyclic fields by adjoining the ℓ-th roots of unity to K, then apply Kummer theory to the extension field, and finally take 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 D_ℓ fields when $q \not\equiv 1 \bmod \ell$.

REFERENCES

[Ach06] J. D. Achter, *The distribution of class groups of function fields*, J. Pure Appl. Algebra **204** (2006), no. 2, 316–333.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[Bha05] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.

[BST10] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport-Heilbronn theorem and second order terms*, arXiv:1005.0672v2 [math.NT].

[CDyDO02] H. Cohen, F. Diaz y Diaz, and M. Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. Reine Angew. Math. **550** (2002), 169–209.

[CM11] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478.

[Coh00] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.

[Coh02] ———, *Constructing and counting number fields*, Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002) (Beijing), Higher Ed. Press, 2002, pp. 129–138.

[DH71] 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.

[DW88] B. Datskovsky and D.J. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. **386** (1988), 116–138.

[EVW] J. Ellenberg, A. Venkatesh, and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, arxiv.org/abs/0912.0325v2[math.NT].

[FW89] E. Friedman and L.C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239.

[Gar12] D. Garton, *Random matrices and the Cohen-Lenstra statistics for global fields with roots of unity*, Ph.D. thesis, University of Wisconsin Madison, 2012, in progress.

[Gos98] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, Berlin, 1998.

[JLSW12] M.J. Jacobson, Y. Lee, R. Scheidler, and H.C. Williams, *Construction of all cubic function fields of a given square-free discriminant*, Preprint, 2012.

[Jon12] J. Jones, *Number field data base*, 2012, http://hobbes.la.asu.edu/NFDB.

[Mal08] G. Malle, *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), no. 10, 2823–2835.

[RJS12] P. Rozenhart, M.J. Jacobson, and R. Scheidler, *Tabulation of cubic function fields via polynomial binary cubic forms*, To appear in Mathematics of Computation, 2012.

[Rob01] D.P. Roberts, *Density of cubic field discriminants*, Math. Comp. **70** (2001), no. 236, 1699–1705 (electronic).

[Ros02] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[RS08] P. Rozenhart and R. Scheidler, *Tabulation of cubic function fields with imaginary and unusual Hessian*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 357–370.

[Ser77] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Sti00] H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, Berlin, 2000.

[Tho11] F. Thorne, *Secondary terms in counting functions for cubic fields*, arXiv:1102.2914v1 [math.NT].

[VE10] A. Venkatesh and J.S. Ellenberg, *Statistics of number fields and function fields*, Proceedings of the International Congress of Mathematicians. Volume II (New Delhi), Hindustan Book Agency, 2010, pp. 383–402.

[VS06] G.D. Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Mathematics: Theory & Applications, Birkhäuser Boston Inc., Boston, MA, 2006.

[Wri89] D.J. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), no. 1, 17–50.

[Zha] Y. Zhao, *Private correspondence*.

Department of Mathematics & Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4

E-mail address: {cjweir,rscheidl}@ucalgary.ca