JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Daniel KELIHER

Enumerating D_4 quartics and a Galois group bias over function fields

Tome 34, n° 2 (2022), p. 371-391.

https://doi.org/10.5802/jtnb.1206

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **34** (2022), 371–391

Enumerating D_4 quartics and a Galois group bias over function fields

par Daniel KELIHER

Résumé. Nous donnons une formule asymptotique pour le nombre d'extensions quartiques du type D_4 et de discriminant donné d'un corps de fonctions en démontrant un résultat analogue à celui de Cohen, Diaz y Diaz et Olivier pour les corps de nombres mais avec un meilleur terme d'erreur. Nous étudions aussi la densité relative des extensions quartiques des types D_4 et S_4 d'un corps de fonctions. Nous montrons que sous des hypothèses faibles, le nombre d'extensions quartiques du type D_4 peut largement dépasser le nombre d'extensions quartiques du type S_4.

Abstract. We give an asymptotic formula for the number of D_4 quartic extensions of a function field with discriminant equal to some bound, essentially reproducing the analogous result over number fields due Cohen, Diaz y Diaz, and Olivier, but with a stronger error term. We also study the relative density of D_4 and S_4 quartic extensions of a function field and show that with mild conditions, the number of D_4 quartic extensions can far exceed the number of S_4 quartic extensions.

1. Introduction

If F is a number field, the number of D_4 and S_4 quartic extensions of F with bounded discriminant is understood by work of Cohen, Diaz y Diaz, and Olivier [2], and of Bhargava, Shankar and Wang [1], respectively. In recent work, Friedrichsen and the author [3] study the relative sizes of these quantities and prove that 100% of quadratic number fields have arbitrarily many more D_4 quartic than S_4 quartic extensions.

In this note we seek to recover the results of [3] but over function fields. The result of Bhargava, Shankar, and Wang counting S_4 quartic extensions still applies in the function field setting. For counting D_4 extensions, the work of Cohen, Diaz y Diaz, and Olivier, while expected to generalize, has hitherto been stated only for number fields.

Manuscrit reçu le 30 septembre 2020, accepté le 1er avril 2022.
Mathematics Subject Classification. 11R45, 11R11, 11R16, 11R58.
Mots-clefs. Field counting, function fields, Galois theory, polynomials.

As such, our first task is to enumerate D_4 quartic extensions of function fields. Throughout, let F be a function field with constants $\mathbb{F}_q$ of characteristic not 2, and let $N_d^F(G;q^{2n})$ be the number of degree d extensions of F with Galois closure G over F and discriminant equal to q^{2n}.[1]

Theorem 1.1. *Let F be a function field with constants $\mathbb{F}_q$ of characteristic not 2 and $q \geq 5$. Then,*

$$N_4^F(D_4;q^{2n}) = q^{2n}\log q \sum_{\substack{K \\ [K:F]=2}} \frac{\operatorname*{Res}_{s=1}\zeta_K(s)}{D_K^2\zeta_F(2)} + O(n4^n q^{n+1}) \tag{1.1}$$

where D_K is the absolute discriminant of K, and $\zeta_K(s)$ is the Dedekind zeta function of K.

The main tool in proving Theorem 1.1 is an effective count of quadratic extensions of function fields.

Theorem 1.2. *Let F be a function field of genus g_F with constants $\mathbb{F}_q$. Then,*

$$N_2^F(S_2;q^{2n}) = \frac{2q^{2n}\log q}{\zeta_F(2)} \operatorname*{Res}_{s=1}\zeta_F(s) + O\left(A^{g_F} q^{\frac{n}{2}+\frac{2g_F+1}{4}}\right) \tag{1.2}$$

where A and the implied constants are absolute.

For number fields, the expected error term for $N_2^F(S_2,X)$ is $O(X^{1/4+\varepsilon})$, essentially mirroring the conjectured error term to obtain when enumerating the number of square-free integers up to some bound [6], though this is not known even assuming the Riemann Hypothesis. As $q \to \infty$, we are seeing this error term reflected on the funcion field side in Theorem 1.2. Likewise, Theorem 1.1 has an error term analagous to $O(X^{1/2+\epsilon})$, which one might expect to be the best possible for enumerating D_4 quartic extensions over a number field, though again this is not known.

Finally, note that in the function field setting we are counting extensions with discriminant equal to some bound, namely even powers of q, as in Theorems 1.1 and 1.2. In the number field setting, one instead usually counts up to some bound for the discriminant. If we did that here, all of the mass of our counting function would be concentrated at even powers of q and we'd fail to get asymptotics. Further, the asymptotic we obtain by counting discriminant equal to even powers of q tend to mirror the analogous results over number fields.

Theorem 1.1 together with the $n = 4$ case of [1, Theorem 1.b] together imply that $N_4^F(D_4;q^{2n})$ and $N_4^F(S_4;q^{2n})$ have the same order of magnitude. It's natural then to compare their relative sizes.

[1] If F is a function field of genus g, its absolute discriminant is $D_F = q^{2g-2}$.

Theorem 1.3. *For any genus g function field F with constants $\mathbb{F}_q$,*

$$\lim_{n\to\infty} \frac{N_4^F(D_4; q^{2n})}{N_4^F(S_4; q^{2n})} \gg \#Cl_F[2] \left(1 - \frac{1}{\sqrt{q}}\right)^{4g-2} \tag{1.3}$$

By specializing to hyperelliptic extensions F of $\mathbb{F}_q(t)$, we can make an analagous statement for a positive proportion of all such F.

Theorem 1.4. *For any $g \geq 2$ and q a power of an odd prime, the proportion of genus g hyperelliptic extensions F of the rational function field $\mathbb{F}_q(t)$ such that*

$$\lim_{n\to\infty} \frac{N_4^F(D_4; q^{2n})}{N_4^F(S_4; q^{2n})} \gg g^{\frac{1}{2}\log 2} \left(1 - \frac{1}{\sqrt{q}}\right)^{4g-2}$$

is at least $1 - O(\frac{1}{\log g})$.

Observe that as $q \to \infty$ the lower bound from Theorem 1.4 aproaches $g^{\frac{1}{2}\log 2}$. Thus, Theorem 1.4 implies, as $q \to \infty$ and for g sufficiently large, an arbitrarily large proportion of genus g hyperelliptic extensions of $\mathbb{F}_q(t)$ have arbitrarily many more D_4 quartic than S_4 quartic extensions.

Later, in Theorem 4.1, we extend Theorem 1.3 in a different direction than Theorem 1.4 by giving conditions under which one can artificially inflate the number D_4 relative to the number of S_4 by base changing the function field under consideration to one with a larger field of constants.

Throughout, function fields will be taken to have constants $\mathbb{F}_q$ where 2 does not divide q. In our setting, these function fields correspond to smooth projective and geometrically connected curves over $\mathbb{F}_q$.

In Section 2 we prove Theorem 1.2. In Section 3 we collect more results from field counting and prove Theorem 1.1. The main idea is to count quadratic-on-quadratic extensions of a ground field using the estimates obtained in Section 2. In Section 4 we turn to the study of the ratio $N_4^F(D_4; X)/N_4^F(S_4; X)$ and prove Theorem 1.3. Finally, in Section 5, we study the statistics of the number of irreducible factors of polynomials over $\mathbb{F}_q$ in order to prove Theorem 1.4.

2. Enumerating Quadratic Extensions

Throughout, let F be the function field of a smooth projective and geometrically connected curve of genus g_F over $\mathbb{F}_q$. We denote by $\mathrm{Cl}(F)$ the class group of F, and by $\mathrm{Cl}_F[2]$ those elements of the class group with order dividing 2. The goal of this section is to prove an estimate for the number of quadratic extensions of F with discriminant equal to q^{2n}.

Our first goal is to prove Theorem 1.2. To begin, we'll focus on the Dirichlet series

$$\phi_{F,2}(s) := \sum_{\substack{K \\ [K:F]=2}} \frac{1}{D_{K/F}^s} \tag{2.1}$$

where the sum ranges over quadratic extensions K over F; $D_{K/F}$ is the norm of the relative discriminant ideal. Its coefficients will determine the quantity $N_2^F(S_2, q^{2n})$ of interest. We first obtain the following characterization of $\phi_{F,2}(s)$:

Lemma 2.1. *If $\phi_{F,2}(s)$ is as above, then,*

$$\phi_{F,2}(s) = \frac{2}{\zeta_F(2s)} \sum_{\chi \in \widehat{\mathrm{Cl}(F)[2]}} L(s, \chi)$$

where the sum ranges over the group characters of $\mathrm{Cl}(F)[2]$.

Proof. Let $\mathcal{O}_F$ be the integral closure of $\mathbb{F}_q[x]$ in F. Then we can write any quadratic extension K/F as $F(\sqrt{\alpha})$ for some non-square $\alpha \in \mathcal{O}_F$. Write $\alpha\mathcal{O}_F = \mathfrak{a}\mathfrak{b}^2$ with $\mathfrak{a}$ square free, this determines the discriminant, $D_{K/F} = |\mathfrak{a}|$. Further, if for some $\alpha' \in F$ we had $F(\sqrt{\alpha}) \simeq F(\sqrt{\alpha'})$ and $\alpha'\mathcal{O}_F = \mathfrak{a}\mathfrak{b}'^2$ then $\mathfrak{b}$ and $\mathfrak{b}'$ belong to the same ideal class in $\mathrm{Cl}(F)$.

Indeed, we may think of any quadratic extension K/F as determined by a choice of $\mathfrak{a}$ (giving the discriminant), a choice of class $[\mathfrak{b}] \in \mathrm{Cl}(F)$ and a unit u (cf. [2, Lemma 3.3]).

Note that if $u \neq u'$ are two non-square units, then $F(\sqrt{\alpha}) \ncong F(\sqrt{u\alpha})$, but $F(\sqrt{u\alpha}) \cong F(\sqrt{u'\alpha})$ since u and u' differ by a square as the unit group of a finite field is cyclic. This establishes a bijection between quadratic extensions K over F and triples of the form $(\mathfrak{a}, [\mathfrak{b}], u)$ where $\mathfrak{a}$ is a square-free ideal of $\mathcal{O}_F$, $[\mathfrak{b}]$ is a class of ideal in $\mathrm{Cl}(F)$ such that $\mathfrak{a}\mathfrak{b}^2 = \alpha\mathcal{O}_F$ and $u \in \mathcal{O}_F^\times/\mathcal{O}_F^{\times 2}$. Now, by orthogonality, the number of quadratic extensions K over F with discriminant $\mathfrak{a}$ is

$$2 \sum_{\chi \in \widehat{\mathrm{Cl}(F)[2]}} \chi(\mathfrak{a}).$$

Observing that

$$N_2^F(S_2; q^n) = 2 \sum_{\substack{\mathfrak{a} \\ |\mathfrak{a}|=q^n}} \sum_{\chi \in \widehat{\mathrm{Cl}(F)[2]}} \chi(\mathfrak{a}),$$

where the sum is over square-free ideals $\mathfrak{a}$ of $\mathcal{O}_F$, we then have

$$\begin{aligned}(2.2)\quad \phi_{F,2}(s) &= \sum_{n=1}^{\infty} \sum_{\substack{K \\ [K:F]=2 \\ D_{K/F}=q^n}} q^{-ns} = \sum_{n=1}^{\infty} N_2^F(S_2, q^n) q^{-ns} \\ &= 2\sum_{n=1}^{\infty} \sum_{\substack{\mathfrak{a} \\ |\mathfrak{a}|=q^n}} \sum_{\chi \in \widehat{\mathrm{Cl}(F)[2]}} \chi(\mathfrak{a})|\mathfrak{a}|^{-s} = 2\sum_{\mathfrak{a}} \sum_{\chi \in \widehat{\mathrm{Cl}(F)[2]}} \chi(\mathfrak{a})|\mathfrak{a}|^{-s} \\ &= 2 \sum_{\chi \in \widehat{\mathrm{Cl}(F)[2]}} \frac{L(s,\chi)}{L(2s,\chi^2)} = \frac{2}{\zeta_F(2s)} \sum_{\chi \in \widehat{\mathrm{Cl}(F)[2]}} L(s,\chi)\end{aligned}$$

as needed. □

This is reminiscent of the expression for the Dirichlet series obtained in [2, Theorem 1.3], but the computations are significantly simpler in the function field setting. In particular, 2 does not divide the characteristic of F.

Before proceeding to the proof of Theorem 1.2, we state some additional supporting lemmas needed for the proof and in further sections. A detailed discussion of the following two lemmas can be found, for example, in Rosen's book [7].

Making the change of variables $u = q^{-s}$, the zeta function of F is given by

$$(2.3)\qquad \zeta_F(s) := Z_F(u) = \frac{L_F(u)}{(1-u)(1-qu)} \text{ with } L_F(u) \in \mathbb{Z}[u].$$

Over $\mathbb{C}$, $L_F(u)$ factors as

$$(2.4)\qquad L_F(u) = \prod_{i=1}^{2g_F} (1 - \pi_i u)$$

where g_F is the genus of the function field F. We mainly will use the fact that the Riemann Hypothesis for Function Fields implies that the inverse roots of $L_F(u)$ have absolute value $\sqrt{q}$. We will make frequent use of the fact that $\zeta_F(s)$ and related L-functions may be written as rational functions.

We also need an estimate for the 2-part of the class group of K, $\#\,\mathrm{Cl}_F[2]$. See [7, Proposition 5.11].

Lemma 2.2. *With the notation all as before,*

$$\#\,\mathrm{Cl}_F[2] \leq \#\,\mathrm{Cl}_F \leq (1+\sqrt{q})^{2g_F}.$$

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Beginning with (2.2) and making the convenient change of variables $u := q^{-s}$ we have

$$\phi_{F,2}(s) = \sum_{n=1}^{\infty} N_2^F(S_2, q^n)u^s.$$

Write $\mathcal{L}_\chi(u)$ for the L-function $L(s,\chi)$ after the change of varibles to $u = q^{-s}$. By applying Cauchy's integral formula to the expression for $\phi_{F,2}(s)$ of Lemma 2.1, we have

$$N_2^F(S_2; q^{2n}) = \frac{1}{\pi i} \sum_{\chi \in \widehat{\mathrm{Cl}(F)[2]}} \oint_\gamma \frac{\mathcal{L}_\chi(u)}{Z_F(u^2)u^{2n+1}} \mathrm{d}u \tag{2.5}$$

where γ is a circle of sufficiently small radius $\varepsilon > 0$ centered at $u = 0$. We compute a_n by expanding the radius of γ and computing residues of the integrand. The integrand has poles at the poles of $\mathcal{L}_\chi(u)$ and at the zeros of denominator.

Observe that if χ in the sum of (2.5) is the trivial character, then $\mathcal{L}_\chi(u) = Z_F(u)$ and we get a pole at $u = \frac{1}{q}$. In other cases, $\mathcal{L}_\chi(u)$ doesn't contribute a pole, and so we will focus on the trivial χ case. The rest will follow in a similar fashion. Note, the zeros of $Z_F(u^2)$ occur, by the Weil's work on the Riemann Hypothesis for function fields, only for values of u where $|u| = q^{-\frac{1}{4}}$.

Let γ' be a circle centered at $u = 0$ with radius R satisfying $q^{-1} < R < q^{-\frac{1}{4}}$. In shifting the contour from γ to γ', this constraint forces us to pick up the residue of the integrand at $u = \frac{1}{q}$ but not any of the residues contributed from the zeros of $Z_F(u^2)$. For any such R we have

$$\frac{1}{\pi i}\oint_\gamma \frac{Z_F(u)}{Z_F(u^2)u^{2n+1}}\mathrm{d}u = \frac{1}{\pi i}\oint_{\gamma'} \frac{Z_F(u)}{Z_F(u^2)u^{2n+1}}\mathrm{d}u - 2\operatorname*{Res}_{u=\frac{1}{q}} \frac{Z_F(u)}{Z_F(u^2)u^{2n+1}}. \tag{2.6}$$

One verifies, using the change of variables $u = q^{-s}$, that

$$\operatorname*{Res}_{u=\frac{1}{q}} \frac{Z_F(u)}{Z_F(u^2)u^{2n+1}} = -\frac{q^{2n}\log q}{\zeta_F(2)} \operatorname*{Res}_{s=1} \zeta_F(s).$$

This shows the right side of (2.6) yields

$$N_2^F(S_2; q^{2n}) = \frac{2q^{2n}\log q}{\zeta_F(s)} \operatorname*{Res}_{s=1}\zeta_F(s) + \frac{1}{\pi i}\oint_{\gamma'} \frac{Z_F(u)}{Z_F(u^2)u^{2n+1}}\mathrm{d}u. \tag{2.7}$$

Using the factorization of $Z_F(u)$ as a rational function [7, Theorem 5.6], bound the integral above by bounding the integrand. Set

$$E := \left|\frac{Z_F(u)}{Z_F(u^2)u^{2n+1}}\right| = \left|\frac{(1-u^2)(1-qu^2)\prod_{i=1}^{2g_F}(1-\alpha_i u)}{(1-u)(1-qu)\prod_{i=1}^{2g_F}(1-\alpha_i u^2)u^{2n+1}}\right| \tag{2.8}$$

where $|\alpha_i| = \sqrt{q}$.

To complete our understanding of (2.7), we will bound E in the cases $R = q^{-\frac{1}{2}}$ and $R = q^{-\frac{1}{4}-\varepsilon}$ for some small $\varepsilon > 0$. In both cases we bound the size of $Z_F(u)/Z_F(u^2)$ when $|u| = R$. In bounding the numerator from above and denominator from below, we simply suppose each term is as large or small as possible, i.e. bounds following from taking $\alpha_i = \pm\sqrt{q}$ and $u = \pm R$.

First, setting $R = q^{-\frac{1}{2}}$, one finds

$$E \leq 2\left(\frac{2}{1-\frac{1}{\sqrt{q}}}\right)^{2g_F}\left(\frac{1+\frac{1}{\sqrt{q}}}{\sqrt{q}-1}\right)q^n. \tag{2.9}$$

Second, setting $R = q^{-\frac{1}{4}-\varepsilon}$, one finds,

$$E \leq \left(\frac{(1+q^{\frac{1}{4}-\varepsilon})^{2g_F}(1+q^{-\frac{1}{4}-\varepsilon})(1+q^{\frac{3}{4}-\varepsilon})}{(1-q^{-\varepsilon})^{2g_F}(q^{\frac{3}{4}-\varepsilon}-1)}\right)q^{\frac{2n-1+\varepsilon}{4}}. \tag{2.10}$$

Repeating these computations for nontrivial χ which contributed to the remaining terms in (2.5) suffices to prove the lemma. We then multiply each E by $2\pi R$, the length of the circle of integration, to get an error term. After doing so and substituting $2n$ for n, (2.9) and (2.10) yield, respectively,

(2.11)

$$N_2^F(S_2;q^{2n}) = \frac{2q^{2n}\log q}{\zeta_F(2)}\operatorname*{Res}_{s=1}\zeta_F(s) + O\left(2\left(\frac{2}{1-\frac{1}{\sqrt{q}}}\right)^{2g_F}\left(1+\frac{1}{\sqrt{q}}\right)q^n\right)$$

and, for any $\varepsilon > 0$,

$$N_2^F(S_2;q^{2n}) = \frac{2q^{2n}\log q}{\zeta_F(2)}\operatorname*{Res}_{s=1}\zeta_F(s) + O\left(\left(\frac{(1+q^{\frac{1}{4}-\varepsilon})^{2g_F}(1+q^{-\frac{1}{2}-\varepsilon})(1+q^{\frac{3}{4}-\varepsilon})}{(1-q^{-\varepsilon})^{2g_F}}\right)q^{\frac{n+\varepsilon}{2}}\right). \tag{2.12}$$

Note that each of the two formulas in (2.11) and (2.12) may have utility in their own right. We now make a choice of $\varepsilon > 0$ in (2.12) that gives the statment of the theorem and a formula which is amenable to computation.

Set $\varepsilon = 1/\log q$. Then the error term in (2.12) becomes

$$O\left(A^{g_F}q^{\frac{n}{2}+\frac{2g_F+1}{4}}\right)$$

where $A = (1-1/e)^{-2}$. The implied constant can be computed from (2.10) and is absolute. □

Remark 2.3. After fixing q (and possibly some $\varepsilon > 0$) in the proof above, the computations for E for all χ in the proof of Theorem 1.2 can be converted into explicit bounds on the error in the formulae of Theorem 1.2.

We conclude the section with a uniform upper bound on the number of quadratic extensions of F. Though it isn't a strong as the preceding theorem, it will simplify some computations later.

Lemma 2.4. *Fix a function field F with constants $\mathbb{F}_q$. For any $n \geq 0$,*

$$N_2^F(S_2; q^{2n}) \ll \#\operatorname{Cl}_F[2] B^{2g_F} q^{2n+1}$$

where $B = \left(\frac{1+e^{-1}q^{-1/2}}{1-e^{-2}q^{-3/2}}\right)^2$.

Proof. We will mimic the method used in the proof of Theorem 1.2 and use the same notation. Starting with (2.5), bound the integrand but now with $R = 1/eq$. This has the effect of avoiding the pole at $u = 1/q$ contributed by the integrand when χ is the trivial character.

When χ is the trivial character and $R = 1/eq$,

$$E \ll B^{g_F} q^{2n+1}$$

where

$$B = \left(\frac{1 + e^{-1}q^{-1/2}}{1 - e^{-2}q^{-3/2}}\right)^2.$$

The same bound, albeit with different implied constants, is obtained for the remaining $\#\operatorname{Cl}_F[2] - 1$ nontrival characters, χ, appearing in (2.5). Whence,

$$N_2^F(S_2; q^{2n}) \ll \#\operatorname{Cl}_F[2] B^{2g_F} q^{2n+1}. \qquad \square$$

3. Enumerating D_4 Extensions

We are now ready to enumerate D_4 quartic extensions of a function field F, i.e. to prove Theorem 1.1. We'll first state some lemmas which, when taken with the results of Section 2, will suffice to prove the theorem.

Lemma 3.1 ([2, Corollary 2.3])**.** *Fix a global field F. We have the formal equality:*

$$\sum_{\substack{K \\ [K:F]=2}} \sum_{\substack{L \\ [L:K]=2 \\ D_{L/F} \leq X}} 1 = 2N_4^F(D_4; X) + N_4^F(C_4; X) + 3N_4^F(V_4; X) \tag{3.1}$$

The proof of this fact is the same as in [2] and relies only on the Galois correspondence and the structure of quartic extensions obtained as quadratic-on-quadratic extensions of F. Since we can only have discriminants which are even powers of q, we'll take $X = q^{2n}$.

The idea is to use (3.1) to understand $N_4^F(D_4; X)$. Now we state some lemmas that will control the last two terms of (3.1). Then the remainder of the section will be devoted to understanding the lefthand side of (3.1).

Lemma 3.2. *If F is a global field, then as $n \to \infty$,*

$$N_4^F(C_4; q^{2n}) = O\left(q^n\right)$$

and

$$N_4^F(V_4; q^{2n}) = O\left(q^n \log(q^{2n})^2\right).$$

Proof. Both of these estimates follow from [8, Theorem 1] and applications of Tauberian theorems. □

Remark 3.3. An immediate consequence of Lemmas 3.1 and 3.2 is that

$$N_4^F(D_4; q^{2n}) = \frac{1}{2} \sum_{\substack{K \\ [K:F]=2}} \sum_{\substack{L \\ [L:K]=2 \\ D_L = q^{2n}}} 1 + O\left(q^n \log(q^{2n})^2\right). \tag{3.2}$$

Indeed, analyzing the sum above will constitute the main idea of the proof.

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. Let D_F be the discriminant of F and let $D_{L/F}$ be the norm of the relative discriminant ideal of L/F. We have the relation that $D_F D_{L/F}^2 = D_L$ [4, Theorem A].

We are trying to compute the sum (3.2) in Remark 3.3.

$$N_4^F(D_4; q^{2n}) = \frac{1}{2} \sum_{\substack{K \\ [K:F]=2}} \sum_{\substack{L \\ [L:K]=2 \\ D_L = q^{2n}}} 1 + O\left(q^n \log(q^{2n})^2\right) \tag{3.3}$$

where the sum counts quadratic-on-quadratic extensions of F of discrimiant q^{2n} and the error term comes from those biquadratic extensions with Galois group C_4 or V_4.

To control the sum above, we introduce an auxiliary parameter j, which will start at -1 and then run over integers up to $n/2$, and rewrite (3.3) as:

$$\sum_{j \le n/2} \sum_{\substack{K \\ [K:F]=2 \\ D_K = q^{2j}}} \sum_{\substack{L \\ [L:K]=2 \\ D_{L/K} = q^{2n-4j}}} 1 = \sum_{j \le n/2} \sum_{\substack{K \\ [K:F]=2 \\ D_K = q^{2j}}} N_2^K(q^{2n-4j}). \tag{3.4}$$

Note that the parameter j controls the discriminant (and also the genus) of the intermediate field K. In particular, the genus of each intermediate field K is $g_K = j + 1$.

First apply the first estimate for $N_2^K(S_2; q^{2n-4j})$ as it appears in (2.11):

$$\sum_{j\le n/2}\sum_{\substack{K\\[K:F]=2\\D_K=q^{2j}}} N_2^K(S_2;q^{2n-4j}) = \sum_{j\le n/2}\sum_{\substack{K\\[K:F]=2\\D_K=q^{2j}}}\left[\frac{2q^{2n-4j}\log q}{\zeta_F(2)}\operatorname*{Res}_{s=1}\zeta_K(s) + O\left(2\left(\frac{2}{1-\frac{1}{\sqrt{q}}}\right)^{2g_K}\left(1+\frac{1}{\sqrt{q}}\right)q^{n-2j}\right)\right] \tag{3.5}$$

The main term of the above is

$$2q^{2n}\log q\sum_{j\le n/2}\sum_{\substack{K\\[K:F]=2\\D_K=q^{2j}}}\frac{\operatorname*{Res}_{s=1}\zeta_K(s)}{q^{4j}\zeta_F(2)}. \tag{3.6}$$

We can compare the sum above to the same, but untruncated, series where j runs over all the integers, to find:

$$2q^{2n}\log q\sum_{j\le n/2}\sum_{\substack{K\\[K:F]=2\\D_K=q^{2j}}}\frac{\operatorname*{Res}_{s=1}\zeta_K(s)}{q^{4j}\zeta_K(2)} = 2q^{2n}\log q\sum_{j=0}^{\infty}\sum_{\substack{K\\[K:F]=2\\D_K=q^{2j}}}\frac{\operatorname*{Res}_{s=1}\zeta_K(s)}{q^{4j}\zeta_K(2)}+O(1). \tag{3.7}$$

The above can be seen by estimating the infinite series with a geometric series using upper and lower bounds on $\operatorname*{Res}_{s=1}\zeta_K(s)$ and $\zeta_K(2)$. We'll see the error term of (3.7) is subsumed by the error term from (3.5).

Now we compute the error term in (3.5). For ease of notation, set $c_q := \frac{2}{1-q^{-\frac{1}{2}}}$.

Using Lemma 2.4, the error term can be seen to be of size

$$q^n \sum_{j\le n/2} \sum_{\substack{K \\ [K:F]=2 \\ D_K=q^{2j}}} 2c_q^{2j+2}\left(1+\frac{1}{\sqrt{q}}\right) q^{-2j}$$

$$= q^n \sum_{j\le n/2} N_2^F(S_2, q^{2j}) 2c_q^{2j+2}\left(1+\frac{1}{\sqrt{q}}\right) q^{-2j}$$

$$\ll q^{n+1} c_q^2 h_2(F) B^{g_F}\left(1+\frac{1}{\sqrt{q}}\right) \sum_{j\le n/2} c_q^{2j}$$

$$\ll q^{n+1} h_2(F) B^{g_F} n c_q^n.$$

This gives an error term $O\left(nc_q^n q^{n+1}\right)$ which dominates the error term in (3.3). Notice $c_q < 5$ for any choice of q, and $c_q < 4$ when $q \ge 5$. We have thus proved (1.1) of Theorem 1.1. Further, note that if $q \le 3$, the main term is not distinguishable from the error term we have just calculated. □

Remark 3.4. Using (1.2) of Theorem 1.2 in the proof above does not yield a better error term.

This essentially recovers the asymtotic given by Cohen, Diaz y Diaz, and Olivier in [2] in the function field setting. The easier analysis granted to us by the Weil Conjectures lets us improve on the number field version, yielding more than just an asymptotic. If we take $n \to \infty$ in Theorem 1.1, this connection is made visibly clear by the following formulae.

Corollary 3.5. With the same notation as above,

$$\lim_{n\to\infty} \frac{N_4^F(D_4; q^{2n})}{q^{2n}} = \frac{\log q}{2} \sum_{j=-1}^{\infty} \sum_{\substack{K \\ [K:F]=2 \\ D_K=q^{2j}}} \frac{\operatorname{Res}_{s=1}\zeta_K(s)}{q^{4j}\zeta_F(2)}$$

$$= \frac{\log q}{2} \sum_{\substack{K \\ [K:F]=2}} \frac{\operatorname{Res}_{s=1}\zeta_K(s)}{D_K^2\zeta_F(2)}.$$

4. Enumerating the D_4-S_4 disparity

We'll turn now to considering the ratio $N_4^F(D_4; q^{2n})/N_4^F(S_4; q^{2n})$. In [3], this quantity is studied in the case that F is a number field. Of interest is the case when F has more D_4 than S_4 quartic extensions. One of the main results of [3] is that this ratio may be skewed arbitrarily much in favor of the D_4 quantity. To obtain the analagous result for function fields, i.e.

Theorem 1.4, we'll first address ourselves to the proof of Theorem 1.3 to give a lower bound for $N_4^F(D_4;q^{2n})/N_4^F(S_4;q^{2n})$.

Proof of Theorem 1.3. First, we underestimate $N_4^F(q^{2n};D_4)$ by restricting the sum in Theorem 1.1 to be over only those K which are unramified over F. Given such an extension K, the different divisor $\mathrm{Diff}(L/K)=\sum_{\mathfrak{P}} c_{\mathfrak{P}}\mathfrak{P}$ is 0, i.e. $c_{\mathfrak{P}}=0$ for all primes $\mathfrak{P}$ of K. So Riemann–Hurwitz tells us $g_K = 2g_F-1$. Note also that class field theory tells us that there are $\#\,\mathrm{Cl}_F[2]-1$ such extensions K.

Further, in restricting ourselves to unramified extension, the q^{4j} term appearing in Theorem 1.1 can be rewrriten as $q^{4(2g_F-2)}$ via $j=g_k-1=2g_F-2$. Our underestimate for $N_4^F(D_4;q^{2n})$ is

$$\begin{aligned}(4.1)\quad \lim_{n\to\infty}\frac{N_4^F(D_4;q^{2n})}{q^{2n}} &\gg \log q \sum_{\substack{K\\ [K:F]=2\\ \text{unram.}}} \frac{\operatorname*{Res}_{s=1}\zeta_K(s)}{q^{4(2g_F-2)}\zeta_F(2)}\\ &= \log q \sum_{\substack{K\\ [K:F]=2\\ \text{unram.}}} \frac{L(1,\chi_{K/F})\operatorname*{Res}_{s=1}\zeta_F(s)}{q^{4(2g_F-2)}\zeta_F(2)}\\ &\geq \log q\ \#\,\mathrm{Cl}_F[2]\left(1-\frac{1}{\sqrt{q}}\right)^{2(2g_F-1)}\frac{\operatorname*{Res}_{s=1}\zeta_F(s)}{q^{4(2g_F-2)}\zeta_F(2)}.\end{aligned}$$

Note that this is not such a terrible truncation of the sum in Theorem 1.1: Estimate each residue of $\zeta_K(s)$ at 1, then factoring these estimates outside the sum leaves a rapidly convergent series, to which the main contributions are made by small j terms, including the unramified extensions.

We'll now estimate $N_4^F(S_4;q^{2n})$. The degree 4 case of [1, Theorem 1.b] gives the number of S_4 quartic extensions of F with relative descriminant equal to some power of q. Using the relation $D_{L/F}D_F^4=D_L$ [4, Theorem A], we can find the number of S_4 quartic extensions L over F with absolute discriminant q^{2n} by counting the number of S_4 quartic extensions L over F with relative discriminant of norm $D_{L/F}=q^{2n}/D_F^4=q^{2n}/q^{4(g_F-2)}$. Whence,

$$(4.2)\qquad \lim_{n\to\infty}\frac{N_4^F(S_4;q^{2n})}{q^{2n}} \ll_F q^{-4(2g_F-2)}\log q\operatorname*{Res}_{s=1}\zeta_F(s).$$

Taking the ratio of (4.1) and (4.2) gives us the desired result. □

The contribution from $\mathrm{Cl}_F[2]$ in Theorem 1.3 is not necessarily easily computed. We can base change our field F over $\mathbb{F}_q$ to have some larger field of constants $\mathbb{F}_{q^m}$ to get a more explicit bound on the right of (1.3) of Theorem 1.3. In doing so, we can understand fully the contribution of $\mathrm{Cl}_F[2]$.

Theorem 4.1. *Let F be the function field of a curve $C/\mathbb{F}_q$ of genus g. There exists a constant m such that if we base change C to be over $\mathbb{F}_{q^m}$ and let F' be the corresponding function field, then*

$$\lim_{n\to\infty} \frac{N_4^{F'}(q^{2n}; D_4)}{N_4^{F'}(q^{2n}; S_4)} \gg 2^{2g}\left(1 - \frac{1}{\sqrt{q^m}}\right)^{4g-2}.$$

Proof. Let J_F be the Jacobian of F. There is a natural map $J_F \hookrightarrow \mathrm{Cl}_F$ and so also an injective map on the two-torsion: $J_F[2] \hookrightarrow Cl_F[2]$. In particular we can use $\#J_F[2]$ as a (possibly crude) proxy for $\#\,\mathrm{Cl}_F[2]$. Consider the multiplication by 2 endomorphism, [2], on the $\overline{\mathbb{F}}_q$ points of J_F,

$$J_F(\overline{\mathbb{F}}_q) \xrightarrow{[2]} J_F(\overline{\mathbb{F}}_q).$$

This is a surjective, degree 2^{2g} map. The two torsion of $J_F(\overline{\mathbb{F}}_q)$ is given by $\ker([2])$. We're looking at J_F over $\overline{\mathbb{F}}_q$ and we're concerned only with an extension of the field of constants to a larger finite field, but we have the relation $J_F(\overline{\mathbb{F}}_q)^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)} = J_F(\mathbb{F}_q)$.

Notice that the 2^{2g} points in $J_F(\overline{\mathbb{F}}_q)[2]$ are partitioned into Galois orbits under the action of $\widehat{\mathbb{Z}} \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. So there is some positive integer m such that all of $J_F(\overline{\mathbb{F}}_q)[2]$ is stable under the action of $m\widehat{\mathbb{Z}} < \widehat{\mathbb{Z}}$. These are exactly the points of $J_F(\mathbb{F}_{q^m})[2]$.

Let F' be the base extension of F having constants $\mathbb{F}_{q^m}$. This is a constant extension of function fields and so the genus of F' is also g [7, Chapter 8], thus passing from the lower bound given by Theorem 1.3 to the lower bound under consideration only requires is to make the substitution of 2^{2g} for $\#\,\mathrm{Cl}_{F'}[2]$ since we have just demonstrated that $2^{2g} \leq \#\,\mathrm{Cl}_{F'}[2]$. □

Observe then that we need only pick a high enough genus curve with suitably large q in order to skew the D_4-S_4 ratio arbitrarily high in favor of the number of D_4 extensions.

5. Typical Behavior of Quadratic Function Fields

Throughout this section, let P_n be the set of degree n square-free polynomials with coefficients in $\mathbb{F}_q$ and let $\pi(d)$ be the number of irreducible degree d polynomials over $\mathbb{F}_q$. Recall $\#P_n = q^n - q^{n-1}$.

Indeed, for everything that follows, all polynomials will be taken to have coefficients in $\mathbb{F}_q$. In light of Theorem 1.3, our interest is in understanding hyperelliptic curves $y^2 = f(x)$ over $\mathbb{F}_q$ which have many two torsion elements in the class groups of their corresponding function fields. Such elements correspond to factors of $f(x)$, and so we will settle for understanding what the typical number of irreducible factors is for a "random" $f(x)$. Many results of a similar flavor, particularly regarding mean and variance, due to Knopfmacher and Knopfmacher can be found in [5].

In the following two propositions $T = T(n)$ will be a function of $n \in \mathbb{N}$ such that both $T(n) \to \infty$ and $n - T(n) \to \infty$ as $n \to \infty$ We will make a convenient choice of T later.

Our primary tool for understanding the typical number of irreducible factors is the following theorem due to Chebyshev, stated here in the context of a finite sets:

Theorem 5.1 (Chebyshev's Inequality)**.** *Let X be a finite set and $f\colon X \to \mathbb{C}$. Then if ϕ has mean and variance given respectively by*

$$\mu := \frac{1}{\#X}\sum_{x\in X}\phi(x) \text{ and } \sigma^2 := \frac{1}{\#X}\sum_{x\in X}(\phi(x)-\mu)^2,$$

then for any k,

$$\#\{x \in X \mid |\phi(x) - \mu| \geq k\sigma\} \leq \frac{\#X}{k^2}.$$

For our considerations the X of Theorem 5.1 will be P_n, and the ϕ will be the function counting the number of irreducible divisors of all $f \in P_n$ with degree bounded by T. As such, let $\omega_T(f)$ be the number of irreducible divisors of f with degree bounded by T.

Proposition 5.2 ("Expected Number" of Factors)**.** The expected number of irreducible factors with degree bounded by T of polynomials in P_n is

$$\mu := \frac{1}{\#P_n}\sum_{f\in P_n}\omega_T(f) = \sum_{d\leq T}\frac{\pi(d)}{q^d+1} + O\left(q^{2T-n+1}\right).$$

Proof. The mean number of irreducible factors with degree bounded by T of polynomials ranging over P_n is given by

$$\mu := \frac{1}{\#P_n}\sum_{f\in P_n}\sum_{\substack{p \text{ irred.}\\ p\mid f\\ \deg p\leq T}} 1 = \frac{1}{\#P_n}\sum_{d\leq T}\sum_{\substack{p \text{ irred.}\\ \deg p = d}}\sum_{\substack{f\in P_n\\ p\mid f}} 1 \tag{5.1}$$

First, for a fixed d and irreducible p of degree d, we aim to understand the innermost sum of (5.1), i.e. $\sum_{\substack{f\in P_n\\ p\mid f}} 1$. This sum is counting the number of polynomials $f \in P_n$ which can be written as $f = gp$ for some $g \in P_{n-d}$. Since f is square-free, we have $p \nmid g$. Now set

$$N_1 := \#\{f \in P_n \mid f = pg, g \in P_{n-d}, p \nmid g\}.$$

Computing N_1 is the same as understanding the number of g with the given condition. So similarly, set

$$N_2 := \#\{g \in P_{n-d} \mid g = ph, h \in P_{n-2d}, p \nmid h\}$$

and observe

$$N_1 = \#P_{n-d} - N_2.$$

One can inductively continue this procedure, if

$$N_s = \#\{t \in P_{n-(s-1)d} \mid t = pu, u \in P_{n-sd}, p \nmid u\}$$

then $N_s = \#P_{n-sd} - N_{s+1}$. The definition of N_s is only sensical for $s+1$ up to $\lfloor \frac{n}{d} \rfloor$. One then finds that

$$N_1 = \left(\sum_{k=1}^{\lfloor \frac{n}{d} \rfloor - 1} (-1)^{k+1} \#P_{n-kd} \right) \pm N_{\lfloor \frac{n}{d} \rfloor}. \tag{5.2}$$

We can bound $N_{\lfloor \frac{n}{d} \rfloor}$ trivially by $P_{n-\lfloor \frac{n}{d} \rfloor d}$. We have $n - \lfloor \frac{n}{d} \rfloor d \leq d$ so, at worst $N_{\lfloor \frac{n}{d} \rfloor} = O(q^d)$. When we compute the mean and divide through by $\#P_n$, this error will be negligible.

Beginning from (5.2), we find

$$\begin{aligned}
N_1 &= \left(\sum_{k=1}^{\lfloor \frac{n}{d} \rfloor - 1} (-1)^{k+1} \#P_{n-kd} \right) + O(q^d) \\
&= \left(\sum_{k=1}^{\lfloor \frac{n}{d} \rfloor - 1} (-1)^{k+1} (q^{n-kd} - q^{n-kd-1}) \right) + O(q^d) \\
&= (q^n - q^{n-1}) \left(\sum_{k=1}^{\lfloor \frac{n}{d} \rfloor - 1} (-1)^{k+1} q^{-kd} \right) + O(q^d) \\
&= (q^n - q^{n-1}) \left(\frac{1}{q^d + 1} + O(q^{-n-1}) \right) + O(q^d) \\
&= (q^n - q^{n-1}) \frac{1}{q^d + 1} + O(q^d)
\end{aligned}$$

Substituting this last expression into (5.1) yields,

$$\begin{aligned}
\mu = \frac{1}{\#P_n} \sum_{d \leq T} \sum_{\substack{p \text{ irred.} \\ \deg p = d}} \sum_{\substack{f \in P_n \\ p \mid f}} 1 &= \sum_{d \leq T} \sum_{\substack{p \text{ irred.} \\ \deg p = d}} \left(\frac{1}{q^d + 1} + O(q^{d-n+1}) \right) \\
&= \sum_{d \leq T} \pi(d) \left(\frac{1}{q^d + 1} + O(q^{d-n+1}) \right).
\end{aligned}$$

Finally, using the prime number theorem for irreducible polynomials over $\mathbb{F}_q$, the above becomes

$$\sum_{d \leq T} \frac{\pi(d)}{q^d + 1} + O\left(q^{2T-n+1} \right)$$

as desired. □

Proposition 5.3 (The "variance" in the number of irreducible factors)**.** The variance in the number of irreducible factors with degree bounded by T of polynomials in P_n is

$$\begin{aligned}\sigma^2 &\coloneqq \frac{1}{\#P_n}\sum_{f\in P_n}(\omega_T(f)-\mu)^2\\ &= \sum_d \pi(d)\frac{1}{q^d+1}\left(1-\frac{1}{q^d+1}\right)+O\left(q^{2(T-n+1)}\right).\end{aligned}$$

Proof. For a random variable X, the variance is given by $\mathbb{E}[X^2]-\mathbb{E}[X]^2$. One easily verifies the following analogue of that identity:

$$\sigma^2 = \frac{1}{\#P_n}\sum_{f\in P_n}\left(\sum_{\substack{p \text{ irred.}\\ p|f\\ \deg p\le T}} 1\right)^2 - \left(\frac{1}{\#P_n}\sum_{f\in P_n}\sum_{\substack{p \text{ irred.}\\ p|f\\ \deg p\le T}} 1\right)^2. \tag{5.3}$$

We'll compute the first term in the difference in (5.3):

$$\begin{aligned}\frac{1}{\#P_n}\sum_{f\in P_n}\left(\sum_{\substack{p \text{ irred.}\\ p|f\\ \deg p\le T}} 1\right)^2 &= \frac{1}{\#P_n}\sum_{f\in P_n}\sum_{\substack{p,p' \text{ irred.}\\ p,p'|f\\ \deg p,\ \deg p'\le T}} 1\\ &= \frac{1}{\#P_n}\sum_{d,d'\le T}\sum_{\substack{p,p' \text{ irred.}\\ \deg p=d\\ \deg p'=d'}}\sum_{\substack{f\in P_n\\ p,p'|f}} 1.\end{aligned} \tag{5.4}$$

Let $N_n^{p_1,\dots,p_r}$ be size of the set of all polynomials $f\in P_n$ such that $p_1|f,\dots,p_r|f$. Note, for fixed irreducible polynomials p and p' of degrees d and d', respectively. Set $N_n^{p_1,\dots,p_r}=\#P_n^{p_1,\dots,p_r}$, then we have $N_n^{p,p'}=\sum_{\substack{f\in P_n\\ p,p'|f}}1$, which is the innermost sum on the right size of (5.4). We have then that

$$N_n^{p,p'} = N_{n-d'}^{p} - N_{n-d'}^{p,p'}$$

Proceeding in the same was as the proof of Proposition 5.2, we get

$$N_n^{p,p'} = \sum_{k=1}^{\lfloor \frac{n}{d'}\rfloor}(-1)^{k+1}N_{n-kd'}^{p}+O(q^d).$$

Proposition 5.2 give us the size of the $P^p_{n-kd'}$, so

$$N_n^{p,p'} = \sum_{k=1}^{\lfloor \frac{n}{d'} \rfloor} (-1)^{k+1} \#P_{n-kd'} \frac{1}{q^d+1} + O(q^d).$$

Letting $n \to \infty$ we evaluate the geometric series and find

$$N_n^{p,p'} = (q^n - q^{n-1}) \frac{1}{q^d+1} \frac{1}{q^{d'}+1} + O(q^d). \tag{5.5}$$

Substituting (5.5) back into (5.4) and rewriting, we get

$$\begin{aligned} \frac{1}{\#P_n} \sum_{d,d' \le T} \sum_{\substack{p,p' \text{ irred.} \\ \deg p = d \\ \deg p' = d'}} \sum_{\substack{f \in P_n \\ p,p' | f}} 1 \\ = \sum_{d,d' \le T} \sum_{\substack{p,p' \text{ irred.} \\ \deg p = d \\ \deg p' = d'}} \frac{1}{q^d+1} \frac{1}{q^{d'}+1} + O(q^{d-n+1}). \end{aligned} \tag{5.6}$$

We'll break the sum in (5.6) up into three cases depending on if $d = d'$ or not as follows:

$$\begin{aligned} \sum_{d \neq d' \le T} \sum_{\substack{p,p' \text{ irred.} \\ \deg p = d \\ \deg p' = d'}} \frac{1}{q^d+1} \frac{1}{q^{d'}+1} + \sum_{d = d' \le T} \sum_{\substack{p \neq p' \text{ irred.} \\ \deg p = d \\ \deg p' = d'}} \frac{1}{q^d+1} \frac{1}{q^{d'}+1} \\ + \sum_{d = d' \le T} \sum_{\substack{p = p' \text{ irred.} \\ \deg p = d}} \frac{1}{q^d+1} + O(q^{d-n+1}). \end{aligned} \tag{5.7}$$

Notice in the above equation, the summands have no dependence on the irreducible polynomials p or p' and so we these terms may be pulled out and counted as $\pi(d)$ or $\pi(d')$. Then, evaluating each of the three expressions, (5.7) is equal to

$$\begin{aligned} \sum_{d \neq d' \le T} \pi(d)\pi(d') \frac{1}{q^d+1} \frac{1}{q^{d'}+1} + \sum_{d = d' \le T} \Big(\pi(d)^2 - \pi(d) \Big) \left(\frac{1}{q^d+1} \right)^2 \\ + \sum_{d = d' \le T} \pi(d) \frac{1}{q^d+1} + O(q^{T-n+1}). \end{aligned} \tag{5.8}$$

We'll now address the second term of (5.3). We have, using Proposition 5.2, that

$$\begin{aligned}
\mu^2 &= \left(\frac{1}{\#P_n} \sum_{f \in P_n} \sum_{\substack{p \text{ irred.} \\ p|f \\ \deg p \leq T}} 1 \right)^2 \\
&= \left(\sum_{d \leq T} \pi(d) \frac{1}{q^d + 1} + O(q^{T-n+1}) \right)^2 \\
&= \sum_{d,d' \leq T} \pi(d)\pi(d') \frac{1}{q^d+1} \frac{1}{q^{d'}+1} + O\left(q^{2(T-n+1)}\right) \\
&= \sum_{d=d' \leq T} \pi(d)^2 \left(\frac{1}{q^d+1} \right)^2 + \sum_{d \neq d' \leq T} \pi(d)\pi(d') \frac{1}{q^d+1} \frac{1}{q^{d'}+1} \\
&\qquad + O\left(q^{2(T-n+1)}\right) \qquad (5.9)
\end{aligned}$$

Finally, taking the difference of (5.8) and (5.9) to get σ^2 as in (5.3), we obtain

$$\sigma^2 = \sum_d \pi(d) \frac{1}{q^d+1} \left(1 - \frac{1}{q^d+1} \right) + O\left(q^{2(T-n+1)}\right)$$

as desired. □

Corollary 5.4. With the notation as above, and as $n \to \infty$, we have

$$\mu \sim \log T$$

and

$$\sigma^2 \sim \log T.$$

Proof. Starting with the conclusion of Proposition 5.2, we have as $n \to \infty$ that

$$\mu \sim \sum_{d \leq T} \pi(d) \frac{1}{q^d+1}. \qquad (5.10)$$

It is known, see e.g. [7], that

$$\pi(d) = \frac{q^d}{d} + O\left(\frac{q^{d/2}}{d} \right) \qquad (5.11)$$

From (5.10) and (5.11) one obtains

$$\sum_{d\le T}\pi(d)\frac{1}{q^d+1}=\sum_{d<T}\left(\frac{q^d}{d(q^d+1)}+O(q^{-d/2})\right)$$

$$=\sum_{d<T}\frac{q^d}{d(q^d+1)}+O\left(q^{-1/2}\right) \tag{5.12}$$

Now we compute the sum on the right side of (5.12),

$$\sum_{d<T}\frac{q^d}{d(q^d+1)}=\sum_{d<T}\frac{1}{d}-\sum_{d<T}\frac{1}{d}\left(\frac{1}{q^d+1}\right)$$

$$=\log T+O(1/T)-\sum_{d<T}\frac{1}{d}\left(\frac{1}{q^d+1}\right)$$

$$=\log T+O\left(\frac{1}{T}\right) \tag{5.13}$$

Where the final equality comes by integrating the last sum by parts and trivially bounding the integrand by $1/q^t$. The result follows. The analysis for σ^2 is essentially the same. □

Theorem 5.5. *As $n\to\infty$, all but a proportion of $\frac{1}{\log\frac{n}{2}}$ square-free polynomials $f\in P_n\subset\mathbb{F}_q[x]$ are such that f has at least $\log\frac{n}{2}+O\left(\sqrt{\log\frac{n}{2}}\right)$ irreducible factors.*

Proof. Set $k=\sqrt{\log\frac{n}{2}}$. Now apply Theorem 5.1 with $X=P_n$, $\phi=\omega_T$, and with μ and σ^2 given by Corollary 5.4 setting $T=\frac{n}{2}$. One finds,

$$\frac{\#\{f\in P_n\mid\ |\omega_{\frac{n}{2}}(f)-\log\frac{n}{2}|\ge\log\frac{n}{2}\}}{\#P_n}\le\frac{1}{\log\frac{n}{2}}.$$

Consequently,

$$\lim_{n\to\infty}\frac{\#\{f\in P_n\mid\ |\omega_{\frac{n}{2}}(f)-\log\frac{n}{2}|\le\log\frac{n}{2}\}}{q^n-q^{n-1}}\ge\lim_{n\to\infty}1-\frac{1}{\log\frac{n}{2}}=1.\qquad\square$$

Proof of Theorem 1.4. We apply Theorem 5.1 with $X=P_d$, $\phi=\omega_T$, $T=\frac{d}{2}$, and $k=\alpha\sqrt{\log\frac{d}{2}}$ where $\alpha=\beta+O\left(\frac{1}{d\sqrt{\log\frac{d}{2}}}\right)$.

For the parameter α, we'll make a choice of β and a choice of error term in the course of the proof. We essentially mimic the proof of Theorem 5.5 and then apply Theorem 1.3.

With μ and σ as above, an immediate consequence of Theorem 5.1 is that for a random $f(x)\in P_d$,

$$\omega_{d/2}(f)\ge\mu-k\sigma \tag{5.14}$$

with probability at least $1 - \frac{1}{k^2}$. If (5.14) holds, Corollary 5.4 implies

$$\omega_{d/2}(f) \geq (1-\alpha)\log\frac{d}{2} + O\left(\frac{\sqrt{\log\frac{d}{2}}}{d}\right). \tag{5.15}$$

Pick α as follows: pick the error term which is the negative of the implicit error appearing in (5.15) and pick any $0 < \beta < 1$. Note that the error terms we're countering with this choice, coming from Corollary 5.4, depend only on d, not on $f(x)$.

For convenience, pick $\beta = 1/2$. We have then that a proportion of least $1 - \frac{1}{k^2}$ of $f(x) \in P_d$ have at least $\beta \log\frac{n}{2}$ irreducible factors.

Let F be the quadratic extensions of $\mathbb{F}_q(x)$ corresponding to a hyperelliptic curve $y^2 = f(x)$ where $f(x) \in P_d \subset \mathbb{F}_q[x]$. Note $d = \deg f(x) = 2g+1$ or $2g+2$ where g is the genus of F. The discussion above shows that as $f(x)$ ranges through P_d, a proportion of $1 - \frac{1}{k^2} = 1 - O\left(\frac{1}{\log g}\right)$ of the associated F, are such that $\mathrm{Cl}_F[2] = 2^{\omega(f)} > 2^{\beta \log g}$ where $\omega(f)$ is the number of irreducible factors of $f(x)$.

So, for a proportion of $1 - O\left(\frac{1}{\log g}\right)$ hyperelliptic genus g extensions $F/\mathbb{F}_q(x)$, we have

$$\begin{aligned}
\lim_{n\to\infty}\frac{N_4^F(q^{2n};D_4)}{N_4^F(q^{2n};S_4)} &\gg \#\mathrm{Cl_F}[2]\left(1-\frac{1}{\sqrt{\mathrm{q}}}\right)^{4\mathrm{g}-2} \\
&= 2^{\omega_T(f)}\left(1-\frac{1}{\sqrt{q}}\right)^{4g-2} \\
&\geq 2^{\beta\log g}\left(1-\frac{1}{\sqrt{q}}\right)^{4g-2} \\
&= g^{\beta\log 2}\left(1-\frac{1}{\sqrt{q}}\right)^{4g-2},
\end{aligned}$$

proving the theorem. □

For completeness, note that in the proof above any choice $0 < \beta < 1$ will do. One can thus slightly improve the exponent of g stated in Theorem 1.4.

Finally, note that taking $q \to \infty$ and large g in Theorem 1.4 is essentially an extremal version of [3, Corollary 1.2] but for function fields rather than number fields. It is plausible that the L-function techniques used in the number field version could be ported over to the function field setting in order to ease the condition on q.

Acknowledgements. Many thanks to Robert Lemke Oliver, Shamil Asgarli, Matt Friedrichsen, and George McNinch for helpful conversations and

suggestions. Thanks also to Ofir Gorodetsky and an anonymous referee for a careful reading of an earlier draft.

References

[1] M. Bhargava, A. Shankar & X. Wang, "Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces", https://arxiv.org/abs/1512.03035, 2015.

[2] H. Cohen, F. Diaz y Diaz & M. Olivier, "Enumerating Quartic Dihedral Extensions of $\mathbb{Q}$", *Mathematica* **133** (2002), no. 1, p. 65-93.

[3] M. Friedrichsen & D. Keliher, "Comparing the density of D_4 and S_4 quartic extensions of number fields", *Proc. Am. Math. Soc.* **149** (2021), no. 6, p. 2357-2369.

[4] M. Jarden & G. Prasad, "Appendix: The discriminant quotient formula for global fields", *Publ. Math., Inst. Hautes Étud. Sci.* **69** (1989), p. 115-117.

[5] A. Knopfmacher & J. Knopfmacher, "Counting irreducible factors of polynomials over a finite field", *Discrete Math.* **112** (1993), no. 1-3, p. 103-118.

[6] F. Pappalardi, "A survey on k-freeness", in *Number theory*, Ramanujan Mathematical Society Lecture Notes Series, vol. 1, Ramanujan Mathematical Society, 2005, p. 71-88.

[7] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, vol. 210, Springer, 2002.

[8] D. J. Wright, "Distribution of Discriminants of Abelian Extensions", *Proc. Lond. Math. Soc.* **3** (1989), no. 58, p. 17-50.

Daniel Keliher
Tufts University
177 College Ave.
Medford, MA, USA
E-mail: daniel.keliher@tufts.edu
URL: https://www.danielkeliher.com