Ann. Sci. Math. Québec **36**, No 2, (2012), 325–348

PRIME DECOMPOSITION AND CLASS NUMBER FACTORS FOR CERTAIN FUNCTION FIELDS

TOBIAS BEMBOM, RENATE SCHEIDLER AND QINGQUAN WU

RÉSUMÉ. Le but de cet article est double. En premier lieu, nous donnons une caractérisation explicite de la décomposition de n'importe quelle place d'un corps de fonctions quartique contenant un sous-corps quadratique. Notre approche est générale et peut (potentiellement) être étendue pour déterminer les décompositions dans tout corps de fonctions. En second lieu, nous obtenons des résultats sur les facteurs premiers des nombres de classes de certaines familles infinies d'extensions de corps de fonctions. Les deux résultats peuvent être utilisés pour accélérer le calcul du nombre de classes des extensions de corps de fonctions considérées.

ABSTRACT. The contribution of this paper is two-fold. Firstly, we provide an explicit characterization of the decomposition of any place in a quartic function field with quadratic subfields. Our approach is general and can be potentially extended to determine decompositions in any function field. Secondly, we provide results on prime factors of class numbers of certain infinite families of function field extensions. Both results can be used to speed up the computation of the class number for the function field extensions under consideration.

1. Introduction and motivation

Computing the class number of a global field is a central problem in number theory, and a large amount of literature has been devoted to this subject. Recently, a general method for determining the class number of an arbitrary function field was presented in [13]. This algorithm consists of two stages. In the first stage, an approximation E of the class number h and an error bound U are computed such that $|h - E| \leq U$. The approximation E is generated via the truncated Euler product representation of the zeta function of the function field. In order to obtain this representation, the prime decompositions of a large number of irreducible polynomials in the function field need to be determined. In the second stage of the class number algorithm of [13], the interval $[E - U, E + U]$ is searched using a baby step giant step or Pollard kangaroo method. This stage can be improved significantly if the class number is known to belong to a particular congruence class. In essence, if $h \pmod m$ is known, then the search can be sped up by a factor of m. The method of [13] had previously been applied to quadratic [15] and purely cubic [12, 7] function fields with considerable success and motivates the work in this article, most of which can also be found in [5].

Reçu le 19 octobre 2012 et, sous forme définitive, le 1 mars 2013.

We provide an explicit characterization of the decomposition of any rational place in a quartic function field with a quadratic subfield. This decomposition can be easily and efficiently determined from a suitable minimal polynomial of the quartic extension, including the cases that cannot be resolved by Kummer's Theorem. In contrast to previous approaches, our method can potentially be generalized to arbitrary function fields. It does not make use of properties that are specific to extensions of this degree only, such as root formulas. In contrast, the signature characterizations for cubic fields given in [14], [9] and [8] for example make use of Cardano's formulas. Moreover, unlike the techniques just cited as well as that of [19], we do not need to resort to P-adic expansions. Our technique has two main surprisingly simple ingredients. Firstly, where possible, we apply suitable variable transformations to the initial minimal polynomial of the extension to reduce potentially problematic cases that cannot be resolved by Kummer's Theorem to simpler scenarios that are covered by this theorem. Secondly, instead of viewing the function field $\mathcal{F}$ as an algebraic extension $\mathbb{F}_q(x)(y)$ of $\mathbb{F}_q(x)$, where x is transcendental over $\mathbb{F}_q$, as is generally done, we view it as an extension of $\mathbb{F}_q(y)$. This allows for a simpler classification of possible prime decompositions. The degree of the extension $\mathcal{F}/\mathbb{F}_q(y)$ is the degree of the pole divisor of y which will play an important role in our work. By applying suitable variable transformations that do not change the decomposition of any rational place, we can determine this degree explicitly.

Our second contribution is a collection of results on factors of class numbers for certain function field extensions that need not be defined by non-singular curves. Rather than having to resort to genus theory, these results can be obtained by considering the zero divisors of certain well-chosen elements in the function field and explicitly constructing appropriate divisor classes.

This paper is organized as follows. We introduce the necessary notation and properties of function fields in Section 2, thereby laying the ground work for our later results. We briefly revisit prime decomposition in a cubic extension in Section 3. The decomposition of the infinite place of $\mathbb{F}_q(x)$ and every finite place of $\mathbb{F}_q(x)$ in a quartic extension with an intermediate quadratic subfield are presented in Sections 4 and 5, respectively. Section 6 contains divisibility results for divisor class numbers of certain infinite families of function fields. We conclude with some open problems in Section 7.

2. Function fields — notation and preliminaries

2.1. Notation

For a general introduction to algebraic function fields, we refer to [16] or [11]. Throughout this paper, let $\mathbb{F}_q$ be a finite field of order q and x be a fixed transcendental element over $\mathbb{F}_q$. For any non-zero polynomial $Q \in \mathbb{F}_q[x]$, we denote by $\deg(Q)$ its degree and by $\mathrm{sgn}(Q)$ the leading coefficient of Q. Throughout the paper, $\mathcal{F}$ will denote an algebraic function field over $\mathbb{F}_q$ such that $\mathcal{F}/\mathbb{F}_q(x)$ is separable.

Denote the set of places of $\mathcal{F}$ by $\mathbb{P}_{\mathcal{F}}$. For each $\mathfrak{P} \in \mathbb{P}_{\mathcal{F}}$, we let $v_{\mathfrak{P}}$ denote its normalized discrete valuation and $\mathcal{O}_{\mathfrak{P}}$ its valuation ring. Write $\mathfrak{P} \mid P$ if $\mathfrak{P}$ lies above $P \in \mathbb{P}_{\mathbb{F}_q(x)}$. The infinite place P_∞ of $\mathbb{F}_q(x)$ has uniformizer $1/x$ and the finite places

in $\mathbb{F}_q(x)$ can be one-to-one identified with the (non-constant) monic irreducible polynomials in $\mathbb{F}_q[x]$ which are respective uniformizers for these places; we will use the same notation (usually P) for both a finite place of $\mathbb{F}_q(x)$ and its corresponding monic irreducible polynomial in $\mathbb{F}_q[x]$. The infinite places of $\mathcal{F}$ are the places $\mathfrak{P} \mid P_\infty$, and the finite places of $\mathcal{F}$ satisfy $\mathfrak{P} \mid P$ for some finite place P of $\mathbb{F}_q(x)$.

For any $P \in \mathbb{P}_{\mathbb{F}_q(x)}$ and $\mathfrak{P} \in \mathbb{P}_\mathcal{F}$ lying above P, the ramification index and relative degree of $\mathfrak{P} \mid P$ are denoted by $e(\mathfrak{P}|P)$ and $f(\mathfrak{P}|P)$, respectively. For brevity, we also write $e_\mathfrak{P}$ and $f_\mathfrak{P}$ if P is fixed. The tuple of pairs $(e(\mathfrak{P}|P), f(\mathfrak{P}|P))$, usually sorted in lexicographical order, is the *P-signature* of $\mathcal{F}/\mathbb{F}_q(x)$. The P_∞-signature is usually just called the signature of $\mathcal{F}/\mathbb{F}_q(x)$.

For most places $P \in \mathbb{P}_{\mathbb{F}_q(x)}$, Kummer's Theorem (see Theorem 3.3.7 of [16]) can be used to completely determine the P-signature of $\mathcal{F}/\mathbb{F}_q(x)$. Suppose $\mathcal{F} = \mathbb{F}_q(x, y)$ with y integral over $\mathcal{O}_P$. Let $F(T) \in \mathcal{O}_P[T]$ be the minimal polynomial of y and $\gamma(T) \in \mathbb{F}_{q^{\deg(P)}}[T]$ be any monic irreducible factor of F modulo P. If $\gamma(y) \in \mathfrak{P}$, *i.e.*, $v_\mathfrak{P}(\gamma(y)) > 0$ for some $\mathfrak{P} \in \mathbb{P}_\mathcal{F}$ lying above P, then γ is said to *belong to* $\mathfrak{P}$. Kummer's Theorem asserts that every such $\gamma(T)$ belongs to at least one place $\mathfrak{P} \mid P$, and $f(\mathfrak{P}|P) \geq \deg(\gamma)$. Moreover, if the powers $1, y, \ldots, y^{n-1}$ of y form an $\mathcal{O}_P$-basis of $\mathcal{O}_\mathfrak{P}$, then the number of irreducible factors of $F \pmod P$ is equal to the number of places $\mathfrak{P} \mid P$, $f(\mathfrak{P}|P) = \deg(\gamma)$ if γ belongs to $\mathfrak{P}$, and $e(\mathfrak{P}|P)$ is the exact power of γ that divides $F \pmod P$.

Throughout this paper, we will assume that $\mathcal{F} = \mathbb{F}_q(x, y)$, where the minimal polynomial of y over $\mathbb{F}_q(x)$ is

$$F(x, T) = T^k + A_{k-1}(x)T^{k-1} + \cdots + A_1(x)T + A_0(x) \in \mathbb{F}_q(x)[T]. \tag{2.1}$$

Most of the time, we will additionally assume that $A_i \in \mathbb{F}_q[x]$, for $0 \leq i \leq k-1$; so $F(x, T) \in \mathbb{F}_q[x, T]$. If this is the case, then for any finite place $P \in \mathbb{P}_{\mathbb{F}_q(x)}$, F is said to be in *standard form at P* if $v_P(A_i) < k - i$ for some $i \in \{0, \ldots, k-1\}$. Standard form at any P can easily be obtained: if $v_P(A_i) \geq k - i$ for $0 \leq i \leq k-1$, then we can simply divide $F(x, T)$ by P^k and replace y by y/P to achieve standard form at P.

2.2. A helpful identity

Our main goal in this section is to establish the highly useful identity

$$\sum_{\mathfrak{P}|P} v_\mathfrak{P}(y) f(\mathfrak{P}|P) = v_P(A_0)$$

for all places $P \in \mathfrak{P}_{\mathbb{F}_q(x)}$, with $A_0 = F(x, 0)$ and $F(x, T) \in \mathbb{F}_q[x, T]$ given by (2.1). First, some auxiliary results that will lead up to this identity.

Lemma 2.1. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$ be a function field with $F(x, y) = 0$ and let $F(x, T) \in \mathbb{F}_q[x, T]$ as in* (2.1). *Then $0 \leq v_\mathfrak{P}(y) \leq e(\mathfrak{P}|P) \max_i\{v_P(A_i)\}$ for every finite place P of $\mathbb{F}_q(x)$ and every place $\mathfrak{P} \mid P$ of $\mathcal{F}$.*

Proof. Let $\mathfrak{P}$ be any finite place of $\mathcal{F}$, and let P be the unique finite place of $\mathbb{F}_q(x)$ such that $\mathfrak{P} \mid P$. Obviously, $v_\mathfrak{P}(A_i) \geq 0$ for $1 \leq i \leq k-1$. Hence y is integral over $\mathcal{O}_\mathfrak{P}$. Since $\mathcal{O}_\mathfrak{P}$ is integrally closed in $\mathcal{F}$ by Proposition 3.2.5 (b) of [16], we know that $y \in \mathcal{O}_\mathfrak{P}$; hence $v_\mathfrak{P}(y) \geq 0$.

For brevity, set $A_k = 1$. Applying the triangle inequality to $F(x,y) = 0$, we see that there must exist indices i, j, with $0 \le i < j \le k$ and $v_{\mathfrak{P}}(A_j y^j) = v_{\mathfrak{P}}(A_i y^i)$. Thus,

$$\begin{aligned} v_{\mathfrak{P}}(y) &= \frac{v_{\mathfrak{P}}(A_j) - v_{\mathfrak{P}}(A_i)}{j-i} \\ &\le v_{\mathfrak{P}}(A_j) \\ &= e(\mathfrak{P}|P) v_P(A_j) \\ &\le e(\mathfrak{P}|P) \max_{1 \le i \le k-1} \{v_P(A_i)\}. \end{aligned}$$

□

Lemma 2.2. *Let $\mathcal{F} = \mathbb{F}_q(x,y)$ be a function field with $F(x,y) = 0$ and let $F(x,T) \in \mathbb{F}_q(x)[T]$ as in* (2.1). *If $\min v_{P_\infty}(A_i) = v_{P_\infty}(A_0) \le 0$, then $v_{\mathfrak{P}}(y) \le 0$ for every infinite place $\mathfrak{P}$ of $\mathcal{F}$.*

Proof. Let $\mathfrak{P}$ be any infinite place of $\mathcal{F}$. Then $v_{\mathfrak{P}}(A_0) = \min_i\{v_{\mathfrak{P}}(A_i)\} \le 0$. If $v_{\mathfrak{P}}(y) > 0$, then $v_{\mathfrak{P}}(A_0) < v_{\mathfrak{P}}(y^n)$ and $v_{\mathfrak{P}}(A_0) < v_{\mathfrak{P}}(A_i y^i)$ for $1 \le i \le k-1$, which contradicts the strict triangle inequality applied to $F(x,y) = 0$. □

Lemma 2.3. *Let $F(x,T) \in \mathbb{F}_q[x,T]$ be given by* (2.1). *Then $F(T,y)$ is irreducible over $\mathbb{F}_q(y)$.*

Proof. Let $F(T,y) = f(T,y)g(T,y)$ with $f, g \in \mathbb{F}_q[y][T]$. Since $F(T,y)$ is irreducible over $\mathbb{F}_q(T)$, either $f(T,y)$ or $g(T,y)$ must be constant with respect to y; say $g(T,y) \in \mathbb{F}_q[T]$. Since $F(T,y)$ is monic in y, $g(T,y)$ is also constant with respect to T, so $g \in \mathbb{F}_q^*$. It follows that $F(y,T)$ is irreducible over $\mathbb{F}_q[y]$, and hence over $\mathbb{F}_q(y)$. □

Every divisor D of $\mathcal{F}$ can be written as $D = D_+ - D_-$, where

$$D_+ = \sum_{v_{\mathfrak{P}}(D) > 0} v_{\mathfrak{P}}(D)\mathfrak{P}, \qquad D_- = -\sum_{v_{\mathfrak{P}}(D) < 0} v_{\mathfrak{P}}(D)\mathfrak{P},$$

and the sums run over all the places $\mathfrak{P}$ of $\mathcal{F}$ with $v_{\mathfrak{P}}(D) \ne 0$. If $\operatorname{div}(z)$ denotes the principal divisor of $z \in \mathcal{F}^*$, then

$$\deg(\operatorname{div}(z)_+) = \deg(\operatorname{div}(z)_-) = [\mathcal{F} : \mathbb{F}_q(z)] \tag{2.2}$$

by Theorem 1.4.11 of [16].

Corollary 2.4. *Let $\mathcal{F} = \mathbb{F}_q(x,y)$ be a function field with $F(x,y) = 0$ and let $F(x,T) \in \mathbb{F}_q[x,T]$ as in* (2.1). *Then* $\deg(\operatorname{div}(y)_-) = \max_i\{\deg(A_i)\}$.

Proof. By Lemma 2.3, $F(T,y) \in \mathbb{F}_q[T,y]$ is irreducible over $\mathbb{F}_q(y)$. Consequently, by (2.2), $\deg(\operatorname{div}(y)_-) = [\mathcal{F} : \mathbb{F}_q(y)]$ is the degree in T of $F(T,y)$ which is equal to $\max_i\{\deg(A_i)\}$. □

Corollary 2.5. *Let $\mathcal{F} = \mathbb{F}_q(x,y)$ be a function field with $F(x,y) = 0$ and let $F(x,T) \in \mathbb{F}_q[x,T]$ as in* (2.1). *If $\deg(A_0) = \max_i\{\deg(A_i)\}$, then*

$$-\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(y) f(\mathfrak{P}|P_\infty) = \deg(\operatorname{div}(y)_-) = \deg(A_0).$$

Proof. The first equality of the claim follows from Lemmata 2.1 and 2.2, and the second one from Corollary 2.4. □

We are now ready to present the main result of this section.

Theorem 2.6. *Let $\mathcal{F} = \mathbb{F}_q(x,y)$ be a function field with $F(x,y) = 0$ and let $F(x,T) \in \mathbb{F}_q[x,T]$ be as in* (2.1)*. Then $\sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(y) f(\mathfrak{P}|P) = v_P(A_0)$ for every place $P \in \mathbb{F}_q(x)$.*

Proof. For brevity, set $A_k = 1$ and $n_i = \deg(A_i)$, for $0 \le i \le k$. We first prove the theorem for the infinite place P_∞ of $\mathbb{F}_q(x)$. Let $n \in \mathbb{N}$, with $n \ge \max_i\{n_i\}$. Then $n \ge (n_i - n_0)/i$, for $1 \le i \le k$, and it now follows easily that

$$\max_{0\le i\le k}\{n_i + (k-i)n\} = n_0 + kn. \tag{2.3}$$

For any finite degree 1 place Q of $\mathbb{F}_q(x)$, the minimal polynomial of yQ^n over $\mathbb{F}_q(x)$ is

$$T^k + \sum_{i=0}^{k-1} A_i(x) Q(x)^{(k-i)n} T^i \in \mathbb{F}_q[x,T].$$

By Corollary 2.5 and (2.3), we see that

$$\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(yQ^n) f(\mathfrak{P}|P_\infty) = -\deg(\operatorname{div}(y)_-) = -(n_0 + kn). \tag{2.4}$$

Since $\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(Q^n) f(\mathfrak{P}|P_\infty) = nk\, v_{P_\infty}(Q) = -nk$, we obtain

$$\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(y) f(\mathfrak{P}|P_\infty) = -n_0 = v_{P_\infty}(A_0).$$

So the result of Theorem 2.6 holds for the infinite place P_∞ of $\mathbb{F}_q(x)$.

Next, we prove the claim for any finite place of $\mathbb{F}_q(x)$. So let $P \in \mathbb{P}_{\mathbb{F}_q(x)}$ be such a place. For brevity, set $n_P = \deg(P)$, $l = v_P(A_0)$ and $m = \max_i\{v_P(A_i)\}$. We need to show that $\sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(y) f(\mathfrak{P}|P) = l$.

Let $n \in \mathbb{N}$, with $n \ge mn_P + \max_i\{n_i\}$. Then

$$n \ge mn_P + (n_i - n_0)/i \ge (n_i - n_0)/i$$

for $0 \le i \le k$, and it now follows easily that (2.3) holds and

$$\max_{0\le i\le k}\{n_i + (k-i)n + (i-k)mn_P\} = n_0 + kn - kmn_P. \tag{2.5}$$

Let $Q \ne P$ be any finite place of degree 1, and set $z = yQ^n/P^m \in \mathcal{F}$. Then

$$v_{\mathfrak{P}}(z) = v_{\mathfrak{P}}(y/P^m) = v_{\mathfrak{P}}(y) - e(\mathfrak{P}|P)m$$

for all places $\mathfrak{P} \mid P$ of $\mathcal{F}$, so

$$\sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(y) f(\mathfrak{P}|P) = \sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(z) f(\mathfrak{P}|P) + km. \tag{2.6}$$

To establish the claim of the theorem for P, we therefore need to prove that

$$\sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(z) f(\mathfrak{P}|P) = l - km.$$

To that end, we determine the support of $\mathrm{div}(z)_-$.

The minimal polynomial of z over $\mathbb{F}_q(x)$ is

$$T^k + \sum_{i=0}^{k-1} A_i(x)Q(x)^{(k-i)n}P(x)^{(i-k)m}T^i \in \mathbb{F}_q(x)[T].$$

By (2.5), we have $\min_i\{v_{P_\infty}(A_iQ^{(k-i)n}P^{(i-k)m})\} = -n_0 - kn + kmn_P \leq -n_k = 0$. Thus, by Lemma 2.2, $v_{\mathfrak{P}}(z) \leq 0$ for all the infinite places $\mathfrak{P}$ of $\mathcal{F}$.

For every finite place $\mathfrak{P} \in \mathbb{P}_{\mathcal{F}}$ with $\mathfrak{P} \nmid P$, we have

$$v_{\mathfrak{P}}(z) = v_{\mathfrak{P}}(yQ^n) \geq v_{\mathfrak{P}}(y) \geq 0$$

by Lemma 2.1. Finally, for every finite place $\mathfrak{P}$ of $\mathcal{F}$ lying above P, we have

$$v_{\mathfrak{P}}(z) = v_{\mathfrak{P}}(y) - e(\mathfrak{P}|P)m \leq 0,$$

again by Lemma 2.1. It follows that $\mathrm{div}(z)_-$ is only supported at places $\mathfrak{P}$ of $\mathcal{F}$ with $\mathfrak{P} \mid P$ or $\mathfrak{P} \mid P_\infty$. Hence

$$-\deg(\mathrm{div}(z)_-) = n_P \sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(z)f(\mathfrak{P}|P) + \sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(z)f(\mathfrak{P}|P_\infty).$$

Now $v_{\mathfrak{P}}(z) = v_{\mathfrak{P}}(yQ^n) + e(\mathfrak{P}|P_\infty)mn_P$ for any $\mathfrak{P}|P_\infty$. So by (2.4),

$$\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(z)f(\mathfrak{P}|P_\infty) = -n_0 - kn + kmn_P.$$

It follows that

$$n_P \sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(z)f(\mathfrak{P}|P) = -\deg(\mathrm{div}(z)_-) + n_0 + kn - kmn_P. \tag{2.7}$$

It remains to determine $\deg(\mathrm{div}(z)_-) = [\mathcal{F} : \mathbb{F}_q(z)]$. We proceed similarly to the proofs of Corollary 2.4 and Lemma 2.3. Set

$$\begin{aligned} G(z,T) &= z^kP(T)^{km-l} + \sum_{i=0}^{k-1} z^i \frac{A_i(T)}{P(T)^l} Q(T)^{(k-i)n}P(T)^{im} \\ &= F(T,y)Q(T)^{nk}/P(T)^l. \end{aligned}$$

Note that $G(z,T) \in \mathbb{F}_q[z,T]$ since $l \leq km$ and $v_P(A_i) \geq l$ for $0 \leq i \leq k-1$. Furthermore, $G(z,x) = 0$. We claim that $G(z,T)$ is irreducible over $\mathbb{F}_q(z)$. Note that $G(z,T)$ is irreducible over $\mathbb{F}_q(T)$, since $F(T,y)$ is irreducible over $\mathbb{F}_q(T)$. Suppose that $G(z,T) = g(z,T)h(z,T)$, with $g,h \in \mathbb{F}_q[z][T]$. Then either $g(z,T)$ or $h(z,T)$ is constant with respect to z; say $g \in \mathbb{F}_q[T]$. Then

$$g \mid G(0,T) = A_0Q^{kn}P^{-l} = Q^{nk}A_0/P^{v_P(A_0)},$$

which implies that $P \nmid g$. Besides this, g divides the leading coefficient of $G(z,T)$, which is P^{km-l}. Since $l \leq m < km$, g is also a constant with respect to T, so $g \in \mathbb{F}_q^*$. It follows that $G(z,T)$ is irreducible over $\mathbb{F}_q[z]$, and hence over $\mathbb{F}_q(z)$.

It follows from (2.2) and (2.5) that

$$\begin{aligned}\deg(\mathrm{div}(z)_-) &= [\mathcal{F} : \mathbb{F}_q(z)] \\ &= \max_{0\le i\le k}\{\deg(A_i Q^{(k-i)n} P^{im-l})\} \\ &= \max_{0\le i\le k}\{n_i + (k-i)n + (im-l)n_P\} \\ &= n_0 + kn - ln_P,\end{aligned}$$

and thus from (2.7),

$$\sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(z) f(\mathfrak{P}|P) = l - km.$$

Finally, the assertion of the theorem follows for P by (2.6). □

3. Interlude: some problematic prime decompositions in cubic extensions

Simple variable transformations to a new field extension generator, as used in the proof of Theorem 2.6, can be a surprisingly powerful tool for finding prime decompositions that are not completely resolved by Kummer's Theorem. Here, we illustrate very briefly the effectiveness of this technique using the well-known example of cubic extensions. Certain P-signatures which were previously treated at a consirable level of complexity can be settled in a few lines with this method.

Explicit descriptions of prime decompositions in cubic function fields were provided in [14], [9], [8], [19] and [4]. As mentioned earlier, the first three sources considered only the case where $\mathbb{F}_q$ has characteristic at least 5 and needed to resort to Puiseux series expansions and Cardano's formulas in order to settle the cases that are unresolved by Kummer's Theorem. The case of characteristic 3 was discussed in [4], while in [19] any characteristic were considered, but again by using P-adic completions. We show here that for any cubic extension of $\mathbb{F}_q(x)$ of characteristic at least 5, and any place P of $\mathbb{F}_q(x)$, it is always possible — and straightforward — to find a suitable minimal polynomial for which Kummer's Theorem determines the P-signature.

Every cubic extension of $\mathbb{F}_q(x)$ can be written in the form $\mathcal{F} = \mathbb{F}_q(x, y)$, where the minimal polynomial of y over $\mathbb{F}_q(x)$ is of the form

$$F(x, T) = T^3 - A(x)T + B(x) \in \mathbb{F}_q[x, T], \tag{3.1}$$

with discriminant $D = 4A^3 - 27B^2 \in \mathbb{F}_q[x]$. The cases for which the signature at infinity of $\mathcal{F}/\mathbb{F}_q(x, y)$ cannot be simply obtained through Kummer's Theorem (applied to P_∞) occur exactly when $2\deg(B) = 3\deg(A)$ and $4\,\mathrm{sgn}(A)^3 = 27\,\mathrm{sgn}(B)^2$, so that $\deg(D) < 3\deg(A) = 2\deg(B)$.

Proposition 3.1. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$ be a cubic function field with $F(x, y) = 0$ and $F(x, T)$ as in* (3.1)*. Set $D = 4A^3 - 27B^2$ and assume that $2\deg(B) = 3\deg(A)$ and $4\,\mathrm{sgn}(A)^3 = 27\,\mathrm{sgn}(B)^2$. Then $\mathcal{F}/\mathbb{F}_q(x)$ has signature*

(a) $(1, 1; 1, 1; 1, 1)$, *if $\deg(D)$ is even and $\mathrm{sgn}(D)$ is a square in $\mathbb{F}_q$;*

(b) $(1,1;1,2)$, *if* $\deg(D)$ *is even and* $\operatorname{sgn}(D)$ *is not a square in* $\mathbb{F}_q$*;*

(c) $(1,1;2,1)$, *if* $\deg(D)$ *is odd.*

Proof. The idea is to find a suitable generator of $\mathcal{F}/\mathbb{F}_q(x)$ so that D is a common factor of the coefficients of the minimal polynomial.

Set $y_1 = 2Ay$, $y_2 = y_1 - 3B$, $y_3 = y_2/B$, $y_4 = y_3^{-1}$, $y_5 = y_4 + 1/3$, and $y_6 = 3Dy_5/A$. Note that replacing y by any y_i does not change the field $\mathcal{F}$ or the signature of $\mathcal{F}/\mathbb{F}_q(x)$. For $1 \le i \le 6$, let F_i be the minimal polynomial of y_i. Then it is straightforward to verify that

$$\begin{cases} F_1(T) = T^3 - 4A^3T + 8A^3B, \\ F_2(T) = T^3 + 9BT^2 - DT - DB, \\ F_3(T) = T^3 + 9T^2 - (D/B^2)T - D/B^2, \\ F_4(T) = T^3 + T^2 - (9B^2/D)\,T - B^2/D, \\ F_5(T) = T^3 - (9B^2/D + 1/3)T + (2B^2/D + 2/27) \\ \qquad\quad = T^3 - (4A^3/3D)T + 8A^3/27D, \\ F_6(T) = T^3 - 12ADT + 8D^2. \end{cases}$$

Since $3\deg(A) > \deg(D)$, we see that $3\deg(12AD) > 2\deg(8D^2)$. So this is one of the scenarios where Kummer's Theorem provides the P_∞-signature. □

For any finite place P of $\mathbb{F}_q(x)$, the problematic P-signatures correspond precisely to the scenario when $P \nmid AB$ and $P \mid D$. We can obtain these P-signatures by applying Kummer's Theorem to the minimal polynomial $F_6(T)$ as given in the proof of Proposition 3.1, converted to standard form at P.

4. Infinite prime decomposition in quartic fields with a quadratic subfield

We now turn our attention to quartic fields $\mathcal{F}/\mathbb{F}_q(x)$ of odd characteristic that contain at least one quadratic subfield. First, we determine the (P_∞-)signature of such an extension. Our method will make use of Corollary 2.5, combined with suitable changes of the generator of $\mathcal{F}/\mathbb{F}_q(x)$ and Kummer's Theorem.

Let $\mathcal{F}$ be an algebraic function field over $\mathbb{F}_q$ of odd characteristic such that $\mathcal{F}/\mathbb{F}_q(x)$ has degree 4 and contains at least one intermediate quadratic field. Then $\mathcal{F}/\mathbb{F}_q(x)$ is separable and simple. By Proposition 3.1 of [17], we can always obtain $\mathcal{F} = \mathbb{F}_q(x,y)$ with

$$F(x,y) = y^4 - A(x)y^2 + B(x) = 0, \tag{4.1}$$

where $A(x), B(x) \in \mathbb{F}_q[x]$. The required variable transformation does not change the P-signature of $\mathcal{F}/\mathbb{F}_q(x)$ for any place P. Note that the discriminant of $T^2 - AT + B$

is $D = A^2 - 4B$. For brevity, set

$$n_2 = \deg(A) \quad \text{and} \quad n_0 = \deg(B), \quad \text{with } n_2 < n_0. \tag{4.2}$$

This inequality can easily be achieved if we replace y by yx^m, $A(x)$ by $A(x)x^{2m}$ and $B(x)$ by $B(x)x^{4m}$ for sufficiently large $m \in \mathbb{Z}_+$. From Corollary 2.5, we obtain

$$-\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(y) f_{\mathfrak{P}} = \deg(\operatorname{div}(y)_-) = n_0. \tag{4.3}$$

By (4.1),

$$4v_{\mathfrak{P}}(y) \geq \min(L), \quad \text{where } L = \{-e_{\mathfrak{P}} n_2 + 2v_{\mathfrak{P}}(y), -e_{\mathfrak{P}} n_0\} \tag{4.4}$$

for any infinite place $\mathfrak{P}$ of $\mathcal{F}$, with $e_{\mathfrak{P}} = e(\mathfrak{P}|P_\infty)$. This leads to the following three cases:

Case (i). If $\min(L) = -e_{\mathfrak{P}} n_2 + 2v_{\mathfrak{P}}(y)$ is the strict minimum of L, then

$$4v_{\mathfrak{P}}(y) = -e_{\mathfrak{P}} n_2 + 2v_{\mathfrak{P}}(y),$$

i.e., $v_{\mathfrak{P}}(y) = -e_{\mathfrak{P}} n_2/2$. It follows that $n_0 < 2n_2$.

Case (ii). If $\min(L) = -e_{\mathfrak{P}} n_0$ is the strict minimum of L, then similarly

$$v_{\mathfrak{P}}(y) = -e_{\mathfrak{P}} n_0/4,$$

and hence $n_0 > 2n_2$.

Case (iii). If $\min(L) = -e_{\mathfrak{P}} n_2 + 2v_{\mathfrak{P}}(y) = -e_{\mathfrak{P}} n_0$, *i.e.*,

$$v_{\mathfrak{P}}(y) = -e_{\mathfrak{P}}(n_0 - n_2)/2,$$

then similarly $n_0 \leq 2n_2$.

Considering these three cases separately is helpful to determine the signature of $\mathcal{F}/\mathbb{F}_q(x)$. Note that since $\mathbb{F}_q$ has odd characteristic, polynomials of the form $T^2 - a$ and $T^4 + b$ cannot have multiple roots.

Theorem 4.1. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$ be of characteristic at least 3, with $F(x, y) = 0$ as in* (4.1). *Let n_2, n_0 be as in* (4.2), $a = \operatorname{sgn}(A)$, $b = \operatorname{sgn}(B)$, $D = A^2 - 4B$, $d = \operatorname{sgn}(D)$, *and $n_D = \deg(D)$. Then $\mathcal{F}/\mathbb{F}_q(x)$ has signature*

(a) $(1, 1; 1, 1; 1, 1; 1, 1)$, *if*

$$\begin{cases} n_0 < 2n_2,\ 2 \mid n_0,\ 2 \mid n_2, \text{ and both } a \text{ and } b \text{ are squares in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ 2 \mid n_2, \text{ and } T^4 - aT^2 + b \text{ has four distinct roots in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ 2 \mid n_2,\ a^2 = 4b,\ 2 \mid n_D, \text{ and both } a/2 \text{ and } d \text{ are squares in } \mathbb{F}_q, \text{ or} \\ 2n_2 < n_0,\ 4 \mid n_0, \text{ and } T^4 + b \text{ has four distinct roots in } \mathbb{F}_q; \end{cases}$$

(b) $(1, 1; 1, 1; 1, 2)$, *if*

$$\begin{cases} n_0 < 2n_2,\ 2 \mid n_0,\ 2 \mid n_2, \text{ and } b \text{ is not a square in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ 2 \mid n_2, \text{ and } T^4 - aT^2 + b \text{ has exactly two distinct roots in } \mathbb{F}_q, \text{ or} \\ 2n_2 < n_0,\ 4 \mid n_0, \text{ and } T^4 + b \text{ has exactly two distinct roots in } \mathbb{F}_q; \end{cases}$$

(c) $(1,1;1,1;2,1)$, *if*

$$\begin{cases} n_0 < 2n_2,\ 2 \nmid n_0,\ 2 \nmid n_2, \text{ and } ab \text{ is a square in } \mathbb{F}_q, \text{ or} \\ n_0 < 2n_2,\ 2 \nmid n_0,\ 2 \mid n_2, \text{ and } a \text{ is a square in } \mathbb{F}_q; \end{cases}$$

(d) $(1,2;1,2)$, *if*

$$\begin{cases} n_0 < 2n_2,\ 2 \mid n_0,\ 2 \mid n_2,\ a \text{ is not a square in } \mathbb{F}_q, \text{ and } b \text{ is a square in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ 2 \mid n_2, \text{ and } T^4 - aT^2 + b \text{ factors into a product of two distinct irreducible quadratic polynomials in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ 2 \mid n_2,\ a^2 = 4b,\ 2 \mid n_D, \text{ and at least one of } a/2 \text{ and } d \text{ is not a square in } \mathbb{F}_q, \text{ or} \\ 2n_2 < n_0,\ 4 \mid n_0, \text{ and } T^4 + b \text{ factors into a product of two irreducible quadratic polynomials in } \mathbb{F}_q; \end{cases}$$

(e) $(1,2;2,1)$, *if*

$$\begin{cases} n_0 < 2n_2,\ 2 \nmid n_0,\ 2 \nmid n_2, \text{ and } ab \text{ is not a square in } \mathbb{F}_q, \text{ or} \\ n_0 < 2n_2,\ 2 \nmid n_0,\ 2 \mid n_2, \text{ and } a \text{ is not a square in } \mathbb{F}_q; \end{cases}$$

(f) $(1,4)$, *if*

$$\begin{cases} n_0 = 2n_2,\ 2 \mid n_2, \text{ and } T^4 - aT^2 + b \text{ is irreducible in } \mathbb{F}_q, \text{ or} \\ 2n_2 < n_0, \text{ and } T^4 + b \text{ is irreducible in } \mathbb{F}_q; \end{cases}$$

(g) $(2,1;2,1)$, *if*

$$\begin{cases} n_0 < 2n_2,\ 2 \mid n_0 \text{ and } 2 \nmid n_2, \text{ or} \\ n_0 = 2n_2,\ 2 \nmid n_2,\ a^2 \neq 4b, \text{ and } a^2 - 4b \text{ is a square in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ 2 \nmid n_2,\ a^2 = 4b,\ 2 \mid n_D, \text{ and } d \text{ is a square in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ a^2 = 4b,\ 2 \nmid n_D, \text{ and } a/2 \text{ is a square in } \mathbb{F}_q, \text{ or} \\ 2n_2 < n_0,\ n_0 \equiv 2 \pmod 4, \text{ and } -b \text{ is a square in } \mathbb{F}_q; \end{cases}$$

(h) $(2,2)$, *if*

$$\begin{cases} n_0 = 2n_2,\ 2 \nmid n_2,\ a^2 \neq 4b, \text{ and } a^2 - 4b \text{ is not a square in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ 2 \nmid n_2,\ a^2 = 4b,\ 2 \mid n_D, \text{ and } d \text{ is not a square in } \mathbb{F}_q, \text{ or} \\ n_0 = 2n_2,\ a^2 = 4b,\ 2 \nmid n_D, \text{ and } a/2 \text{ is not a square in } \mathbb{F}_q, \text{ or} \\ 2n_2 < n_0,\ n_0 \equiv 2 \pmod 4, \text{ and } -b \text{ is not a square in } \mathbb{F}_q; \end{cases}$$

(i) $(4,1)$, *if* $2n_2 < n_0$, *and* $2 \nmid n_0$.

Proof. Henceforth, $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3$ refer to infinite places of $\mathcal{F}$ that satisfy cases (i), (ii), (iii) above, respectively.

Case 1. Assume that $n_0 < 2n_2$. Then, clearly, only cases (i) and (iii) may occur. We claim that both cases must occur. Otherwise, first assume that (i) is the only possible case. Then every infinite place $\mathfrak{P}$ of $\mathcal{F}$ satisfies $v_{\mathfrak{P}}(y) = -e_{\mathfrak{P}} n_2/2$, which implies $n_0 = 2n_2$ by (4.3), a contradiction. Likewise, (iii) cannot be the only possible case.

We now distinguish according to the parities of n_0 and n_2.

Case 1.1. Assume that both n_0 and n_2 are odd. It follows that $e_{\mathfrak{P}_1}$ is even. Since there are at least two infinite places in $\mathcal{F}$, it follows that $e_{\mathfrak{P}_1} = 2$. The minimal polynomial of $z = Bx^{-(n_0+n_2)/2}y^{-1}$ reduces to $T^2(T^2-ab)$ modulo P_∞. It is straightforward to verify that $v_{\mathfrak{P}_1}(z) = 2n_2 - n_0 > 0$, hence $v_{\mathfrak{P}_1}(z^2 - ab) = 0$ by strict triangle inequality. This implies that any irreducible factor $\gamma(T)$ of $T^2 - ab \pmod{P_\infty}$ belongs to a place $\mathfrak{P}_3$. By Kummer's Theorem, if ab is a square in $\mathbb{F}_q$, then there are two places $\mathfrak{P}_3$ above P_∞, implying signature $(1, 1; 1, 1; 2, 1)$, whereas if ab is a non-square in $\mathbb{F}_q$, then there is one inert place $\mathfrak{P}_3$, implying signature $(1, 2; 2, 1)$.

Case 1.2. Assume that n_0 is even and n_2 is odd. By the equalities

$$v_{\mathfrak{P}_1}(y) = -e_{\mathfrak{P}_1} n_2/2 \quad \text{and} \quad v_{\mathfrak{P}_3}(y) = -e_{\mathfrak{P}_3}(n_0 - n_2)/2,$$

both $e_{\mathfrak{P}_1}$ and $e_{\mathfrak{P}_3}$ are even, which implies signature (2,1;2,1).

Case 1.3. Assume that n_0 is odd and n_2 is even. Then $e_{\mathfrak{P}_3}$ is even, and as in Case 1.1, we see that $e_{\mathfrak{P}_3} = 2$. The minimal polynomial of $z = x^{-n_2/2}\, y$ modulo P_∞ is $T^2(T^2 - a)$. It is easy to verify that $v_{\mathfrak{P}_3}(z) = 2n_2 - n_0 > 0$, which implies that $v_{\mathfrak{P}_3}(z^2 - a) = 0$. Thus, any irreducible factor $\gamma(T)$ of $T^2 - a$ belongs to a place $\mathfrak{P}_1$. Again by Kummer's Theorem, if a is a square in $\mathbb{F}_q$, then there are two places $\mathfrak{P}_1$ above P_∞, which implies signature $(1, 1; 1, 1; 2, 1)$, whereas if a is a non-square in $\mathbb{F}_q$, then there is one inert place $\mathfrak{P}_1$, which implies signature $(1, 2; 2, 1)$.

Case 1.4. Assume that both n_0 and n_2 are even. The reductions modulo P_∞ of the minimal polynomials of $x^{-n_2/2}\, y$ and $Bx^{-(n_0+n_2)/2}y^{-1}$ are

$$T^2(T^2 - a) \quad \text{and} \quad T^2(T^2 - ab),$$

respectively. Similar to Cases 1.1 and 1.3, any irreducible factor of $T^2 - ab$ belongs to $\mathfrak{P}_3$ and any irreducible factor of $T^2 - a$ belongs to $\mathfrak{P}_1$. Thus, the factorizations of $T^2 - a$ and $T^2 - ab$ over $\mathbb{F}_q$ will again determine the signature uniquely.

Case 2. Assume that $n_0 > 2n_2$. Then case (ii) is the only possibility. Thus any infinite place $\mathfrak{P}_2$ in $\mathcal{F}$ satisfies $v_{\mathfrak{P}_2}(y) = -e_{\mathfrak{P}_2} n_0/4$.

Case 2.1. If n_0 is odd, then $\mathcal{F}$ must have signature (4,1).

Case 2.2 If $n_0 \equiv 2 \pmod 4$, there exists at least one place $\mathfrak{P}_2$ with $e_{\mathfrak{P}_2}$ even. Then the minimal polynomial of $x^{-n_0/2}y^2$ modulo P_∞ is $T^2 + b$, hence P_∞ is unramified in the quadratic extension $\mathbb{F}_q(x, y^2)/\mathbb{F}_q(x)$. Thus the factorization of $T^2 + b$ over $\mathbb{F}_q$ will determine the signature uniquely.

Case 2.3. Assume that $4 \mid n_0$. Then the minimal polynomial of $x^{-n_0/4}y$ modulo P_∞ is $T^4 + b$, which has no multiple roots. Hence Kummer's Theorem yields the signature.

Case 3. Assume that $n_0 = 2n_2$ and $a^2 \neq 4b$. Then only case (iii) is possible, hence any infinite place $\mathfrak{P}_3$ in $\mathcal{F}$ satisfies $v_{\mathfrak{P}_3}(y) = -e_{\mathfrak{P}_3}(n_0 - n_2)/2 = -e_{\mathfrak{P}_3} n_2/2$.

Case 3.1. Assume that n_2 is odd. Then $e_{\mathfrak{P}_3}$ is even. The reduction modulo P_∞ of the minimal polynomial of $y^2 - A/2$ is $T^2 - a^2/4 + b$ which has distinct roots. Hence P_∞ is unramified in the quadratic extension $\mathbb{F}_q(x, y^2)/\mathbb{F}_q(x)$. Together with the fact that $e_{\mathfrak{P}_3}$ is even, our result follows.

Case 3.2. Assume that n_2 is even. The reduction modulo P_∞ of the minimal polynomial of $x^{-n_2/2}y$ is $T^4 - aT^2 + b$, which has distinct roots. Kummer's Theorem again yields the signature.

Case 4. Finally, assume that $n_0 = 2n_2$ and $a^2 = 4b$. Then $n_D < n_0 = 2n_2$. Again, only case (iii) is possible, and as in Case 3, any infinite place $\mathfrak{P}_3$ in $\mathcal{F}$ satisfies $v_{\mathfrak{P}_3}(y) = -e_{\mathfrak{P}_3} n_2/2$.

Let $M = \mathbb{F}_q(x)(y^2) = \mathbb{F}_q(\sqrt{D})$, and consider the quadratic extension $\mathcal{F}/M$ defined by the equation $T^2 = (A + \sqrt{D})/2$. Let $\mathfrak{p}_M$ be any infinite place of M. Since $n_D < 2n_2$, we have

$$v_{\mathfrak{p}_M}(A) = -e(\mathfrak{p}_M|P_\infty)n_2 < -e(\mathfrak{p}_M|P_\infty)n_D/2 = -v_{\mathfrak{p}_M}(D)/2 = -v_{\mathfrak{p}_M}(\sqrt{D}),$$

which implies that $v_{\mathfrak{p}_M}(A + \sqrt{D}) = v_{\mathfrak{p}_M}(A) = -e(\mathfrak{p}_M|P_\infty)n_2$. By Proposition 3.7.3 of [16], $\mathfrak{p}_M$ is ramified in the quadratic extension $\mathcal{F}/M$ if $e(\mathfrak{p}_M|P_\infty)n_2$ is odd and unramified in $\mathcal{F}/M$ if $e(\mathfrak{p}_M|P_\infty)n_2$ is even. Equivalently, by the same proposition, $\mathfrak{p}_M$ is ramified in $\mathcal{F}/M$ if and only if n_2 is odd and n_D is even. Combined with the fact that P_∞ is ramified in $M/\mathbb{F}_q(x)$ if and only if n_D is odd, we infer that P_∞ is unramified in $\mathcal{F}/\mathbb{F}_q(x)$ if and only if both n_2 and n_D are even, and P_∞ has ramification index 2 otherwise.

Case 4.1. Assume that both n_2 and n_D are odd, so $e_{\mathfrak{P}_3} = 2$. Note that a uniformizer for $\mathfrak{p}_M$ is $t = \sqrt{D}\, x^m$ for $m = -(1 + n_D)/2$. Changing the field generator of $\mathcal{F}/M$ from y to $z = yt^{n_2}$ does not change the signature. The minimal polynomial of z over M is

$$T^2 = (A + \sqrt{D})t^{2n_2}/2 = (A + \sqrt{D})D^{n_2}x^{2mn_2}/2,$$

which reduces to $T^2 - a/2$ modulo $\mathfrak{p}_M$. If $a/2$ is a square in $\mathbb{F}_q$, then $\mathcal{F}$ has at least two infinite places, whereas if $a/2$ is a non-square in $\mathbb{F}_q$, then $\mathcal{F}$ has one infinite place. Combined with the fact that $e_{\mathfrak{P}_3} = 2$, our result follows.

Case 4.2. Assume that n_2 is odd and n_D is even, so again $e_{\mathfrak{P}_3} = 2$. The reduction modulo P_∞ of the minimal polynomial of $x^{-n_D/2}(y^2 - A/2)$ over $\mathbb{F}_q(x)$ is $T^2 - d/4$, which has distinct roots. Thus, P_∞ is unramified in the quadratic extension $M/\mathbb{F}_q(x)$. If d is a square in $\mathbb{F}_1$, then $\mathcal{F}$ has at least two infinite places, whereas if d is a non-square in $\mathbb{F}_q$, then $\mathcal{F}$ has one infinite place. Combined with the fact that $e_{\mathfrak{P}_3} = 2$, our result follows.

Case 4.3. Assume that n_2 is even and n_D is odd, so once again $e_{\mathfrak{P}_3} = 2$. The reduction modulo P_∞ of the minimal polynomial of $x^{-n_2/2}y$ over $\mathbb{F}_q(x)$ is

$$T^4 - aT^2 + b = (T^2 - a/2)^2.$$

If $a/2$ is a square in $\mathbb{F}_q$, then $\mathcal{F}$ has at least two infinite places, whereas if $a/2$ is a non-square in $\mathbb{F}_q$, then $\mathcal{F}$ has one infinite place. Combined with the fact that $e_{\mathfrak{P}_3} = 2$, our result follows.

Case 4.4. Assume that both n_2 and n_D are even, so P_∞ is unramified in $\mathcal{F}/\mathbb{F}_q(x)$. If d is a square in $\mathbb{F}_q$, then P_∞ splits completely in $M/\mathbb{F}_q(x)$, whereas if d is a non-square in $\mathbb{F}_q$, then P_∞ is inert in $M/\mathbb{F}_q(x)$. Clearly, changing the field generator of $\mathcal{F}/M$ from y to $z = yx^{-n_2/2}$ does not change the signature. The minimal polynomial of z over $\mathbb{F}_q(x)$ is $T^2-(A+\sqrt{D})/2x^{n_2}$, which reduces to $T^2-a/2$ modulo $\mathfrak{p}_M$. If $a/2$ is a square in $\mathbb{F}_q$, then $\mathfrak{p}_M$ splits completely in $\mathcal{F}/M$, whereas if $a/2$ is a non-square in $\mathcal{F}/M$, then $\mathfrak{p}_M$ is inert in $\mathcal{F}$. Our result now follows. □

It should be mentioned that the P-adic completion method, *i.e.*, determining the smallest field of Puiseux series containing each root of (4.1), could also be used to prove Theorem 4.1 if the proper machinery is introduced. More specifically, one can apply Lemma 4.1 of [14] and Theorem 3.1 of [8] to provide an alternative proof.

5. Finite prime decomposition in quartic fields with a quadratic subfield

In this section, we determine for every finite place of $\mathbb{F}_q(x)$ the P-signature of a quartic extension $\mathcal{F}/\mathbb{F}_q(x)$ with at least one intermediate quadratic field. So fix any finite place $P \in \mathbb{P}_{\mathbb{F}_q(x)}$ and assume without loss of generality that the minimal polynomial of y over $\mathbb{F}_q(x)$, as given in (4.1), has standard form at P. This assumption simplifies the description of the different signatures compared to Theorem 4.1. For brevity, set

$$m_2 = v_P(A), \quad m_0 = v_P(B) \quad \text{and} \quad m_D = v_P(D), \tag{5.1}$$

where we recall that $D = A^2 - 4B$. Similar to Lemma 2.3, we have the following result.

Proposition 5.1. *Let $\mathcal{F} = \mathbb{F}_q(x,y)$ with $F(x,y) = 0$ as given in* (4.1)*, P be a finite place of $\mathbb{F}_q(x)$ of degree $n_P = \deg(P)$, m_0, m_2 as in* (5.1)*, and $z = y/P$. Assume that $m_0 \geq 3$ and $m_2 = 1$. Then*

$$G(z,T) = z^4P(T) - z^2A(T)/P(T) + B(T)/P(T)^3$$

is irreducible over $\mathbb{F}_q(z)$, $G(z,x) = 0$, and

$$\deg(\mathrm{div}(z)_-) = \max\{n_P, n_2 - n_P, n_0 - 3n_P\}.$$

Proof. Observe that $G(z,T) \in \mathbb{F}_q[z,T]$ as $m_2 = 1$ and $m_0 \geq 3$ by assumption. The rest of the proof is very analogous to those of Lemma 2.3 and Corollary 2.4. □

If in (4.4), we replace $-n_i$ by m_i as given in (5.1), and set

$$L = \{e_{\mathfrak{P}}m_2 + 2v_{\mathfrak{P}}(y), e_{\mathfrak{P}}m_0\}$$

for any place $\mathfrak{P} \mid P$ of $\mathcal{F}$, then Theorem 2.6 leads to three cases that are analogous to those derived from (4.3) and (4.4) as follows:

Case (iv). If $\min(L) = e_{\mathfrak{P}}\, m_2 + 2v_{\mathfrak{P}}(y)$ is the strict minimum of L, then

$$v_{\mathfrak{P}}(y) = e_{\mathfrak{P}}\, m_2/2 \quad \text{and} \quad 2m_2 < m_0.$$

Case (v). If $\min(L) = e_{\mathfrak{P}}\, m_0$ is the strict minimum of L, then

$$v_{\mathfrak{P}}(y) = e_{\mathfrak{P}}\, m_0/4 \quad \text{and} \quad 2m_2 > m_0.$$

Case (vi). If $\min(L) = e_{\mathfrak{P}}\, m_2 + 2v_{\mathfrak{P}}(y) = e_{\mathfrak{P}}\, m_0$, then

$$v_{\mathfrak{P}}(y) = e_{\mathfrak{P}}(m_0 - m_2)/2 \quad \text{and} \quad 2m_2 \le m_0.$$

As before, for $j = 4, 5, 6$, let $\mathfrak{P}_j \mid P$ denote the places of $\mathcal{F}$ that satisfy cases (iv), (v), (vi) above, respectively. The following preliminary result will be useful.

Lemma 5.2. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$ with $F(x, y) = 0$ as given in* (4.1)*, P be a finite place of $\mathbb{F}_q(x)$ of degree $n_P = \deg(P)$, and m_0, m_2 as in* (5.1)*.*

(a) *If $m_0 \ge 3$ and $m_2 = 1$, then there is a place $\mathfrak{P}_4 \mid P$ in $\mathcal{F}$ with $e_{\mathfrak{P}_4} = 2$.*

(b) *If $m_0 < 2m_2$ and $2 \nmid m_0$, then there is a place $\mathfrak{P}_5 \mid P$ in $\mathcal{F}$ with $e_{\mathfrak{P}_5} = 4$.*

Proof. (a) If necessary, we replace y by $Q^k y$ for some sufficiently large integer k and some monic irreducible polynomial $Q \in \mathbb{F}_q[x]$ that divides neither A nor B. This leaves the P-signature of $\mathcal{F}/\mathbb{F}_q(x)$ as well as m_0, m_2 unchanged, but changes n_2 to $n_2 + 2k\deg(Q)$ and n_0 to $n_0 + 4k\deg(Q)$. If we choose k sufficiently large k, then Proposition 5.1 implies that

$$\deg(\operatorname{div}(y/P)_-) = n_0 - 3n_P. \tag{5.2}$$

Cases (i)-(iii) just before Theorem 4.1 imply that

$$v_{\mathfrak{P}}(y) \in \{-e_{\mathfrak{P}} n_2/2, -e_{\mathfrak{P}} n_0/4, -e_{\mathfrak{P}}(n_0 - n_2)/2\}$$

for any infinite place $\mathfrak{P}$ of $\mathcal{F}$. Thus,

$$v_{\mathfrak{P}}(y/P) \in \{-e_{\mathfrak{P}} n_2/2 + e_{\mathfrak{P}} n_P, -e_{\mathfrak{P}} n_0/4 + e_{\mathfrak{P}} n_P, -e_{\mathfrak{P}}(n_0 - n_2)/2 + e_{\mathfrak{P}} n_P\}.$$

If we choose k sufficiently large, then we can assume that $v_{\mathfrak{P}}(y/P) \le 0$ for any infinite place $\mathfrak{P} \mid P_\infty$.

We claim that in addition to possibly some infinite places of $\mathcal{F}$, the support of $\operatorname{div}(y/P)_-$ only contains divisors $\mathfrak{P}_4$. By assumption, only cases (iv) and (vi) can occur. For any $\mathfrak{P}_6 \mid P$, we have

$$v_{\mathfrak{P}_6}(y) = e_{\mathfrak{P}_6}(m_0 - m_2)/2 \ge e_{\mathfrak{P}_6}(3 - 1)/2 = e_{\mathfrak{P}_6},$$

so $v_{\mathfrak{P}_6}(y/P) \ge 0$. For any $\mathfrak{P}_4 \mid P$, we have $v_{\mathfrak{P}_4}(y) = e_{\mathfrak{P}_4}/2$, so

$$v_{\mathfrak{P}_4}(y/P) = -e_{\mathfrak{P}_4}/2 < 0.$$

Thus, (5.2) implies that

$$n_0 - 3n_P = -\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(y/P) f(\mathfrak{P}|P_\infty) - n_P \sum_{\mathfrak{P}_4|P} v_{\mathfrak{P}_4}(y/P) f(\mathfrak{P}_4|P). \tag{5.3}$$

By (4.3),

$$\begin{aligned} -\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(y/P) f(\mathfrak{P}|P_\infty) &= -\sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(y) f(\mathfrak{P}|P_\infty) + \sum_{\mathfrak{P}|P_\infty} v_{\mathfrak{P}}(P) f(\mathfrak{P}|P_\infty) \\ &= n_0 - 4n_P. \end{aligned}$$

From (5.3) and the fact that $v_{\mathfrak{P}_4}(y/P) = -e_{\mathfrak{P}_4}/2$, it follows that

$$1 = -\sum_{\mathfrak{P}_4|P} v_{\mathfrak{P}_4}(y/P) f(\mathfrak{P}_4|P) = \frac{1}{2} \sum_{\mathfrak{P}_4|P} e(\mathfrak{P}_4|P) f(\mathfrak{P}_4|P),$$

so $\sum_{\mathfrak{P}_4} e_{\mathfrak{P}_4} f_{\mathfrak{P}_4} = 2$. Note also that $e_{\mathfrak{P}_4} = 2v_{\mathfrak{P}_4}(y)$ is even. Since $\sum_{\mathfrak{P}|P} e_{\mathfrak{P}} f_{\mathfrak{P}} = 4$, this forces $e_{\mathfrak{P}_4} = 2$ for some $\mathfrak{P}_4 \mid P$.

(b) Since $m_0 < 2m_2$, only case (v) can occur, *i.e.*, $v_{\mathfrak{P}_5}(y) = e_{\mathfrak{P}_5} m_0/4$ for every place $\mathfrak{P}_5|P$. Since m_0 is odd, $e_{\mathfrak{P}_5} = 4$. □

It is now possible to provide the P-signature of $\mathcal{F}/\mathbb{F}_q(x)$ for any finite place P in $\mathbb{P}_{\mathbb{F}_q(x)}$.

Theorem 5.3. *Let q be an odd prime power, $\mathcal{F} = \mathbb{F}_q(x, y)$ with $F(x, y) = 0$ as given in* (4.1)*, and $D = A^2 - 4B$. Let P be a finite place of $\mathbb{F}_q(x)$ of degree $n_P = \deg(P)$ such that* (4.1) *has standard form at P, and let m_0, m_2, m_D be as in* (5.1)*. Then $\mathcal{F}/\mathbb{F}_q(x)$ has P-signature*

(a) $(1, 1; 1, 1; 1, 1; 1, 1)$, *if*

$$\begin{cases} 0 = m_0, \text{ and } T^4 - AT^2 + B \text{ has four distinct roots modulo } P, \text{ or} \\ 0 = m_0 = m_2 < m_d,\ 2 \mid m_d, \text{ and both } A/2 \text{ and } D/P^{m_d} \text{ are squares modulo } P, \text{ or} \\ 0 = m_2 < m_0,\ 2 \mid m_0, \text{ and both } A \text{ and } B/P^{m_0} \text{ are squares modulo } P; \end{cases}$$

(b) $(1, 1; 1, 1; 1, 2)$, *if*

$$\begin{cases} 0 = m_0, \text{ and } T^4 - AT^2 + B \text{ has exactly two distinct roots modulo } P, \text{ or} \\ 0 = m_2 < m_0,\ 2 \mid m_0, \text{ and } B/P^{m_0} \text{ is not a square modulo } P; \end{cases}$$

(c) $(1, 1; 1, 1; 2, 1)$, *if*

$$\begin{cases} 0 = m_2 < m_0,\ 2 \nmid m_0, \text{ and } A \text{ is a square modulo } P, \text{ or} \\ 1 = m_2,\ 2 < m_0,\ 2 \nmid m_0, \text{ and } AB/P^{m_0+1} \text{ is a square modulo } P; \end{cases}$$

(d) $(1, 2; 1, 2)$, *if*

$$\begin{cases} 0 = m_0, \text{ and } T^4 - AT^2 + B \text{ factors into a product of two irreducible quadratic polynomials modulo } P, \text{ or} \\ 0 = m_0 = m_2 < m_d,\ 2 \mid m_d, \text{ and at least one of } A \text{ and } D/P^{m_d} \text{ is not a square modulo } P, \text{ or} \\ 0 = m_2 < m_0,\ 2 \mid m_0, A \text{ is not a square modulo } P, \text{ and } B/P^{m_0} \text{ is a square modulo } P; \end{cases}$$

(e) $(1, 2; 2, 1)$, *if*

$$\begin{cases} 0 = m_2 < m_0,\ 2 \nmid m_0, \text{ and } A \text{ is not a square modulo } P, \text{ or} \\ 1 = m_2,\ 2 < m_0,\ 2 \nmid m_0, \text{ and } AB/P^{m_0+1} \text{ is not a square modulo } P; \end{cases}$$

(f) $(1,4)$ *if* $0 = m_0$, *and* $T^4 - AT^2 + B$ *is irreducible modulo* P;

(g) $(2,1;2,1)$, *if*

$$\begin{cases} 1 = m_2,\ 2 < m_0,\ 2 \mid m_0, \text{ or} \\ 2 = m_0 < 2m_2, \text{ and } -B/P^2 \text{ is a square modulo } P, \text{ or} \\ 2 = m_0 = 2m_2 < m_d,\ 2 \mid m_d, \text{ and } D/P^{m_d} \text{ is a square modulo } P, \text{ or} \\ 2 = m_0 = 2m_2 = m_d, \text{ and } D/P^2 \text{ is a square modulo } P, \text{ or} \\ m_0 = 2m_2 < m_d,\ 2 \nmid m_d, \text{ and } A/2P^{m_2} \text{ is a square modulo } P; \end{cases}$$

(h) $(2,2)$, *if*

$$\begin{cases} 2 = m_0 < 2m_2, \text{ and } -B/P^2 \text{ is not a square modulo } P, \text{ or} \\ 2 = m_0 = 2m_2 < m_d,\ 2 \mid m_d, \text{ and } D/P^{m_d} \text{ is not a square modulo } P, \text{ or} \\ 2 = m_0 = 2m_2 = m_d, \text{ and } D/P^2 \text{ is not a square modulo } P, \text{ or} \\ m_0 = 2m_2 < m_d,\ 2 \nmid m_d, \text{ and } A/2P^{m_2} \text{ is not a square modulo } P; \end{cases}$$

(i) $(4,1)$ *if* $m_0 < 2m_2$, *and* $2 \nmid m_0$.

Proof. As mentioned before, the assumption that $F(x,T)$ has standard form at P introduces some simplification over Theorem 4.1. The proof of Theorem 5.3 is analogous to that of Theorem 4.1 and employs Lemma 5.2. In essence, one replaces $-n_i$ by m_i for $i = 0, 2$, $\operatorname{sgn}(G)$ by $G/P^{v_P(G)}$ for $G \in \{A, B, D\}$, and factorizations over $\mathbb{F}_q$ by factorizations modulo P; similarly for roots, squares and non-squares. □

6. Factors of class numbers

The results of Theorems 4.1 and 5.3 can be used to compute an approximation to the class number h of a quartic function field with an intermediate quadratic field as required by the algorithm of [13]. This was explicitly described in Section 3.4 of [5]. As mentioned earlier, the search phase of this method can essentially be sped up by a factor of $m \in \mathbb{N}$ if $h \pmod m$ is known. This section presents several divisibility results for class numbers.

We begin with a brief overview of what is known. A lower bound on the number of 2-factors dividing the class number of a hyperelliptic function field was first determined in [1], with a stronger result provided in [18]. The case of function fields of Picard curves was investigated in [3]. All these results assume that the defining curve is non-singular at all finite points. This assumption can in fact be computationally detrimental, as a singular representation might support much more efficient arithmetic than the non-singular model. For example, any cyclic cubic function field over $\mathbb{F}_q$ with $q \equiv 1 \pmod 3$ is a Kummer extension and can hence be represented in the form $\mathcal{F} = \mathbb{F}_q(x,y)$, where $y^3 = A(x) \in \mathbb{F}_q[x]$. If A is not square-free, then the curve $y^3 = A(x)$ is singular. However, this representation of $\mathcal{F}/\mathbb{F}_q(x)$ allows for much faster

divisor arithmetic than the non-singular cubic model, which is advantageous in many applications, including class number computation.

Genus theory for function fields was used to establish ℓ-ranks of class groups of Kummer extensions in [2] and [10]. In this section, we provide results on factors of the class numbers of certain types of function field extensions. Unlike the case of hyperelliptic and Picard curves, we do not require a non-singular model. Moreover, unlike [2] and [10], we include radical extensions that need not be cyclic, and we do not need to resort to genus theory; instead, we explicitly construct appropriate divisor classes.

Henceforth, let $\mathcal{C}$ denote the degree 0 divisor class group of a function field $\mathcal{F}/\mathbb{F}_q$, h be its order (*i.e.*, the class number of $\mathcal{F}$), and $\mathcal{P}$ be the subgroup of $\mathcal{C}$ of principal divisors. We begin with a useful auxiliary lemma.

Lemma 6.1. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$, with $y^\ell = A \in \mathbb{F}_q[x]$, be a radical function field of prime degree ℓ so that ℓ divides neither $\deg(A)$ nor the characteristic of $\mathcal{F}$. Let $\tilde{A}$ denote the square-free kernel of A. Then $\deg(\mathrm{div}(z)_+) > \deg(\tilde{A})/2$ for every $z \in \mathcal{F} \setminus \mathbb{F}_q(x)$.*

Proof. By Proposition 6.3.1 of [16], the genus of $\mathcal{F}$ is

$$g = \frac{(\ell - 1)(\deg(\tilde{A}) - 1)}{2}.$$

Let $z \in \mathcal{F} \setminus \mathbb{F}_q(x)$. Then z is a generator of $\mathcal{F}/\mathbb{F}_q(x)$ as $[\mathcal{F} : \mathbb{F}_q(x)] = \ell$ is prime. Now Riemann's Inequality (Corollary 3.11.4 of [16]) implies

$$[\mathcal{F} : \mathbb{F}_q(z)] \geq \frac{g}{[\mathcal{F} : \mathbb{F}_q(x)] - 1} + 1 = \frac{g}{\ell - 1} + 1.$$

Combined with the genus formula, we obtain

$$\deg(\mathrm{div}(z)_+) = [\mathcal{F} : \mathbb{F}_q(z)] \geq \frac{\deg(\tilde{A}) + 1}{2} > \frac{\deg(\tilde{A})}{2}. \qquad \square$$

Our first result shows that for radical function fields of prime degree, the extension degree always divides the class number. We note that when $\ell \mid q - 1$, *i.e.*, in the case of Kummer extensions, this is a simple consequence of Corollary 3.14 of [2].

Theorem 6.2. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$, with $y^\ell = A \in \mathbb{F}_q[x]$, be a radical function field of prime degree ℓ such that A factors into $r \geq 2$ distinct powers of irreducible polynomials. Assume that ℓ divides neither $\deg(A)$ nor the characteristic of $\mathcal{F}$. Then $\ell \mid h$.*

Proof. Let $A = \mathrm{sgn}(A) \prod_{i=1}^r P_i^{e_i}$ be the factorization of A into powers of irreducible polynomials. If $\tilde{A}$ again denotes the square-free kernel of A, then $\tilde{A} = \prod_{i=1}^r P_i$. By Proposition 6.3.1 of [16], the ramified places of $\mathbb{F}_q(x)$ are exactly $P_1, \ldots, P_r, P_\infty$ and they are all totally ramified.

For $1 \leq i \leq r$, let $\mathfrak{P}_i$ be the unique place of $\mathcal{F}$ lying above P_i, and $\mathfrak{P}_\infty$ be the unique infinite place of $\mathcal{F}$. Then $\deg(\mathfrak{P}_i) = \deg(P_i)$ for $1 \leq i \leq r$, and $\deg(\mathfrak{P}_\infty) = 1$. The principal divisor of each P_i in $\mathcal{F}$ is $\mathrm{div}(P_i) = \ell D_i$, where $D_i = \mathfrak{P}_i - \deg(P_i)\mathfrak{P}_\infty$. It suffices to show that $D_i \notin \mathcal{P}$ for some $1 \leq i \leq r$.

By way of contradiction, suppose that for every i with $1 \le i \le r$, $D_i = \operatorname{div}(z_i)$ for some $z_i \in \mathcal{F}^*$. Then $z_i \notin \mathbb{F}_q(x)$, as otherwise

$$1 = v_{\mathfrak{P}_i}(z_i) = e(\mathfrak{P}_i|P_i)v_{P_i}(z_i) = \ell\, v_{P_i}(z_i) \in \ell\,\mathbb{Z},$$

a contradiction. Thus, $z_i \in \mathcal{F} \setminus \mathbb{F}_q(x)$. By Lemma 6.1, we have

$$\deg(P_i) = \deg(\operatorname{div}(z_i)_+) > \deg(\tilde{A})/2$$

for $1 \le i \le r$. But then

$$\deg(\tilde{A}) = \sum_{i=1}^{r} \deg(P_i) > r\deg(\tilde{A})/2 \ge \deg(\tilde{A}),$$

a contradiction. □

As an application of Theorem 6.2, we obtain the following result.

Corollary 6.3. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$ be an algebraic function field given by*

$$ax^k + by^l = c,$$

where k, l, and the characteristic of $\mathcal{F}$ are pairwise distinct primes, and a, b, c are in $\mathbb{F}_q \setminus \{0\}$. Assume that neither $ax^k - c$ nor $by^l - c$ is irreducible over $\mathbb{F}_q$. Then kl divides the class number of $\mathcal{F}$.

Proof. $\mathbb{F}_q(y)$ is an intermediate field of $\mathcal{F}/\mathbb{F}_q$ with $[\mathcal{F} : \mathbb{F}_q(y)] = k$, and $\mathbb{F}_q(x)$ is an intermediate field of $\mathcal{F}/\mathbb{F}_q$ with $[\mathcal{F} : \mathbb{F}_q(x)] = l$. The claim now follows immediately from Theorem 6.2. □

Theorem 6.2 reveals nothing about higher powers of ℓ dividing h. However, we can strengthen this result in the case $\ell = 3$ as follows.

Theorem 6.4. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$ be a purely cubic extension of $\mathbb{F}_q(x)$, where $y^3 = A(x) \in \mathbb{F}_q[x]$ factors into r distinct powers of irreducible polynomials. Assume that 3 divides neither $\deg(A)$ nor the characteristic of $\mathbb{F}_q$. Then $\mathcal{C}$ has 3-rank at least $\lceil r/2 \rceil$, so $3^{\lceil r/2 \rceil} \mid h$, where $\lceil\ \rceil$ is the ceiling function.*

Proof. Assume that $r \ge 2$, otherwise there is nothing to prove. Define $\tilde{A}$, P_i, $\mathfrak{P}_i$, P_∞, $\mathfrak{P}_\infty$ and D_i analogous to the proof of Theorem 6.2. Let l be the 3-rank of $\mathcal{C}$. Our goal is to show that the number of independent divisor classes represented by the D_i is at least $\lceil r/2 \rceil$.

Note that $D_i, -D_i \notin \mathcal{P}$, while $3D_i \in \mathcal{P}$, for $1 \le i \le r$. So the set

$$S = \left\{ D = \sum_{i=1}^{r} k_i D_i \in \mathcal{P} \;\middle|\; k_i \in \{0, \pm 1\},\ k_i \ne 0 \text{ for some } i \right\}$$

is a generating system of the subgroup of $\mathcal{P}$ generated by the divisor classes of the D_i. Let

$$m = \min_{D \in S} \# \left\{ i \;\middle|\; k_i \ne 0 \text{ for } D = \sum_{i=1}^{r} k_i D_i \in S \right\}$$

be the minimum of the number of non-zero coefficients k_i for all elements in S, *i.e.*, the minimum non-zero ternary Hamming weight of S. Then $1 \le m \le r$ and $l \ge m - 1$.

Let $D = \sum_{i=1}^{n} k_i D_i \in S$. Reordering the D_i, we may assume that $k_i = 1$ for $1 \leq i \leq t$, and $k_i = -1$ for $t+1 \leq i \leq m$ for some suitable t. Let

$$D' = \sum_{i=1}^{t} \mathfrak{P}_i \quad \text{and} \quad D'' = \sum_{i=t+1}^{m} \mathfrak{P}_i.$$

Then $D = D' - D'' - (\deg(D') - \deg(D''))\mathfrak{P}_\infty$. Replacing D by $-D$ if necessary, we may assume that $\deg(D') \geq \deg(D'')$, so $D_+ = D'$.

Write $D = \operatorname{div}(z)$ with $z \in \mathcal{F}^*$. Then $z \notin \mathbb{F}_q(x)$, as otherwise

$$1 = v_{\mathfrak{P}_1}(z) = 3v_{P_1}(z) \in 3\mathbb{Z},$$

a contradiction. Hence,

$$\deg(D_+) = \sum_{i=1}^{t} \deg(P_i) > \deg(\tilde{A})/2 \tag{6.1}$$

by Lemma 6.1.

We claim that the $r-t$ divisor classes represented by $D_{t+1}, \ldots, D_r$ are independent in $\mathcal{C}$. To that end, suppose by way of contradiction that there exist $k_i \in \mathbb{Z}$, not all zero, such that $E = \sum_{i=t+1}^{r} k_i D_i$ is principal. Without loss of generality, we may assume that $k_i \in \{0, \pm 1\}$ for $t+1 \leq i \leq r$, so $E \in S$. As before, we reorder $D_{t+1}, \ldots, D_r$ so that $k_i = 1$ for $t+1 \leq i \leq s$, $k_i \in \{0, -1\}$ for $s+1 \leq i \leq r$ for some suitable s, and $E_+ = \sum_{i=t+1}^{s} \mathfrak{P}_i$ is non-zero. Thus, E is the divisor of an element in $\mathcal{F} \setminus \mathbb{F}_q(x)$, which by Lemma 6.1 implies that

$$\deg(E_+) = \sum_{i=t+1}^{s} \deg(P_i) > \deg(\tilde{A})/2. \tag{6.2}$$

Now (6.1) and (6.2) together yield

$$\deg(\tilde{A}) = \sum_{i=1}^{r} \deg(P_i) \geq \sum_{i=1}^{s} \deg(P_i) = \sum_{i=1}^{t} \deg(P_i) + \sum_{i=t+1}^{s} \deg(P_i) > \deg(\tilde{A}),$$

a contradiction. It follows that $l \geq r - t$. Thus,

$$l \geq \max\{r-t, m-1\} \geq \max\{m-1, r-m\} \geq \lfloor r/2 \rfloor, \tag{6.3}$$

where $\lfloor\ \rfloor$ is the floor function. This proves our result for even r, and for those odd r for which any of the inequalities in (6.3) is strict for some t.

We prove that the remaining case leads to a contradiction. To that end, assume equality throughout (6.3) for any t, and r odd. Then it is easy to infer that

$$l = r - t = m - 1 = \lfloor r/2 \rfloor = (r-1)/2,$$

so

$$l + 1 = m = t = (r+1)/2,$$

and any $D \in S$ that is a linear combination of exactly m among $D_1, \ldots D_r$ must be the sum of these m divisors D_i (since our ordering forces the first $t = m$ divisors D_i in the linear combination to have coefficient $k_i = 1$).

Without loss of generality, assume that $A(x)$ is cube-free, so $v_P(A) \not\equiv 0 \pmod 3$ for any $P \in \{P_1, \ldots, P_r, P_\infty\}$. For every place $\mathfrak{P} \mid P$, we have

$$3v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(y^3) = v_{\mathfrak{P}}(A) = e(\mathfrak{P}|P)v_P(A).$$

Since $e(\mathfrak{P}|P) = 3$ for $P \in \{P_1, \ldots, P_r, P_\infty\}$, this implies $v_{\mathfrak{P}}(y) = v_P(A)$ for all $P \in \mathbb{P}_{\mathbb{F}_q(x)}$ and $\mathfrak{P} \mid P$. It follows that $\operatorname{div}(y) = \sum_{i=1}^r v_{P_i}(A)D_i$. Subtracting suitable multiples of $3D_i$ from $\operatorname{div}(y)$, for $1 \le i \le r$, yields a principal divisor

$$\operatorname{div}(u) = \sum_{i=1}^r a_i D_i, \quad \text{with } a_i = \pm 1 \text{ for } 1 \le i \le r.$$

Among the r coefficients a_i, there are at least $(r+1)/2 = m$ identical ones. By replacing u by u^{-1} and reordering the D_i if necessary, we may thus assume that $a_i = 1$ for $1 \le i \le m$. So

$$\operatorname{div}(u) = \sum_{i=1}^m D_i + \sum_{i=m+1}^r a_i D_i, \quad \text{with } a_i = \pm 1 \text{ for } \ m+1 \le i \le r.$$

Since $l = (r-1)/2$, the $m = (r+1)/2$ divisors $D_1, \ldots, D_m$ represent dependent divisor classes in $\mathcal{C}$, so there exist $k_1, \ldots, k_m \in \{\pm 1\}$ and $w \in \mathcal{F}^*$ such that $\sum_{i=1}^m k_i D_i = \operatorname{div}(w)$. Since this divisor belongs to S and is a linear combination of exactly m of the D_i, we must have $k_i = 1$, for $1 \le i \le m$. Hence

$$\operatorname{div}(w) = \sum_{i=1}^m D_i \quad \text{and} \quad \operatorname{div}(u/w) = \sum_{i=m+1}^r a_i D_i.$$

Now

$$\begin{aligned} \deg(\operatorname{div}(u/w)_+) &= \max\left\{ \sum_{a_i=1,\, m+1\le i\le r} \deg(P_i), \sum_{a_i=-1,\, m+1\le i\le r} \deg(P_i) \right\} \\ &\le \sum_{i=m+1}^r \deg(P_i). \end{aligned} \tag{6.4}$$

Note that $v_{\mathfrak{P}_1}(w) = 1$ and $v_{\mathfrak{P}_r}(u/w) = a_r = \pm 1$. Since neither of these values is divisible by 3, it follows that w and u/w belong to $\mathcal{F} \setminus \mathbb{F}_q(x)$. By Lemma 6.1, we obtain

$$\deg(\operatorname{div}(w)_+) > \deg(\tilde{A})/2 \quad \text{and} \quad \deg(\operatorname{div}(u/w)_+) > \deg(\tilde{A})/2. \tag{6.5}$$

Then (6.4) and (6.5) together imply

$$\begin{aligned} \deg(\tilde{A}) &= \sum_{i=1}^r \deg(P_i) \\ &= \sum_{i=1}^m \deg(P_i) + \sum_{i=m+1}^r \deg(P_i) \\ &\ge \deg(\operatorname{div}(w)_+) + \deg(\operatorname{div}(u/w)_+) > \deg(\tilde{A}), \end{aligned}$$

a contradiction. □

If A is square-free, a stronger result than Theorem 6.4 holds.

Corollary 6.5. *With the notation as in Theorem 6.4, if A is square-free, then $\mathcal{C}$ has 3-rank at least $r-1$; so $3^{r-1} \mid h$.*

Proof. Let z be defined as in the proof of Theorem 6.4. Then

$$\operatorname{div}(y/z) = \operatorname{div}(y) - \operatorname{div}(z) = \sum_{i=1}^{r} D_i - \left(\sum_{i=1}^{t} D_i - \sum_{i=t+1}^{m} D_i \right) = 2 \sum_{i=t+1}^{r} D_i.$$

The proof of Theorem 6.4 established that the divisor classes of $D_{t+1}, \ldots, D_r$ are independent, so this sum must vanish. Since $t \leq m \leq r$, this forces $t = m = r$. By (6.3), $\mathcal{C}$ has 3-rank at least $m - 1 = r - 1$. □

We point out that for Kummer extensions, this result is a direct consequence of Lemma 5 (2) of [10]. The quadratic analogue to Corollary 6.5 was first stated in [1] and generalized in [18], while its origin (for quadratic number fields) goes back to Gauss's genus theory in his *Disquisitiones Arithmeticae*. For Picard curves, Corollary 6.5 was proved in [3], along with other divisibility results for the class numbers of such curves. Genus theory establishes that the ideal class group of any cyclic extension of $\mathbb{Q}$ of prime degree ℓ has ℓ-rank at least $r-1$, where r is the number of ramified primes; Gerth asserted in [6] that this bound is met for most such extensions.

The following proposition provides a necessary condition for a prime to divide the class number of a function field.

Proposition 6.6. *Let $\mathcal{F} = \mathbb{F}_q(x, y)$ be a function field and ℓ be a prime. If $\ell \mid h$, then there exists $z \in \mathcal{F}$, integral over $\mathbb{F}_q[x]$, such that the norm $N_{\mathbb{F}_q(x)}^{\mathcal{F}}(z)$ is an ℓ-th power in $\mathbb{F}_q[x]$ up to a constant factor in $\mathbb{F}_q^*$, but z is not an ℓ-th power in $\mathcal{F}$.*

Proof. Suppose $\ell \mid h$. Then there exists a non-principal degree 0 divisor D such that $\ell D \in \mathcal{P}$. By adding multiples $k\mathfrak{P} \in \mathcal{P}$ to D if necessary for every place $\mathfrak{P}$ of $\mathcal{F}$ in the support of D, we may assume that D_+ is supported at finite places of $\mathcal{F}$, and D_- is supported at infinite places of $\mathcal{F}$ only. It follows that $\ell D = \operatorname{div}(z)$, for some $z \in \mathcal{F}$ that is integral over $\mathbb{F}_q[x]$. Since $D \notin \mathcal{P}$, z is not an ℓ-th power in $\mathcal{F}$ up to constants in $\mathbb{F}_q^*$.

Let

$$F(x, T) = T^k + \sum_{i=0}^{k-1} A_i T^i$$

be the minimal polynomial of z, with $A_i \in \mathbb{F}_q[x]$, for $0 \leq i \leq n-1$. Applying Theorem 2.6 to $\mathcal{G} = \mathbb{F}_q(x, z)$, we see that $\sum_{\mathfrak{P}|P} v_{\mathfrak{P}}(z) f(\mathfrak{P}|P) = v_P(A_0)$ for every place P of $\mathbb{F}_q(x)$. Since $\operatorname{div}(z) = \ell D$, $\ell \mid v_{\mathfrak{P}}(z)$ for every place $\mathfrak{P}$ of $\mathcal{F}$. It follows that $\ell \mid v_P(A_0)$ for every place P of $\mathbb{F}_q(x)$, hence A_0 is an ℓ-th power in $\mathbb{F}_q[x]$ up to a constant factor. Thus,

$$N_{\mathbb{F}_q(x)}^{\mathcal{F}}(z) = N_{\mathbb{F}_q(x)}^{\mathcal{G}}(z)^{[\mathcal{F}:\mathcal{G}]} = \pm A_0^{[\mathcal{F}:\mathcal{G}]}$$

is an ℓ-th power in $\mathbb{F}_q[x]$ up to a constant factor. □

The following result provides a partial converse of the above proposition.

Proposition 6.7. *Let ℓ be a prime and $\mathcal{F} = \mathbb{F}_q(x,y)$ be a function field with $F(x,y) = 0$ and $F(x,T) \in \mathbb{F}_q(x)[T]$ as in* (2.1)*. Assume that the following conditions are satisfied:*

(1) *A_0 is an ℓ-th power in $\mathbb{F}_q[x]$ up to a constant in $\mathbb{F}_q^*$;*

(2) *$\ell \mid v_{\mathfrak{P}}(y)$ for every infinite place $\mathfrak{P}$ of $\mathcal{F}$;*

(3) *y is not an ℓ-th power in $\mathcal{F}$;*

(4) $\gcd(A_0, A_1) = 1$.

Then $\ell \mid h$.

Proof. We first claim that $\ell \mid v_{\mathfrak{P}}(y)$ for all places $\mathfrak{P}$ of $\mathcal{F}$. By property (2), this is true if $\mathfrak{P}$ is infinite. Let $\mathfrak{P}$ be a place in $\mathcal{F}$ lying above any finite place P of $\mathbb{F}_q(x)$. Then $v_{\mathfrak{P}}(y) \geq 0$ by Lemma 2.1. If $v_{\mathfrak{P}}(y) = 0$, there is nothing to prove, so suppose that $v_{\mathfrak{P}}(y) > 0$. Since $F(x,y) = 0$, we have

$$A_0 = -y(A_1 + \beta y), \quad \text{with } \beta = y^{k-2} + \sum_{i=0}^{k-3} A_{i+2} y^i.$$

Note that $v_{\mathfrak{P}}(\beta) \geq 0$ by triangle inequality, so

$$v_{\mathfrak{P}}(A_1 + y\beta) \geq 0 \quad \text{and hence} \quad v_P(A_0) \geq v_{\mathfrak{P}}(y) > 0.$$

Property (4) now forces $v_P(A_1) = 0$ and hence $v_{\mathfrak{P}}(A_1 + y\beta) = 0$ by the strict triangle inequality. Therefore $v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(A_0)$ is a multiple of ℓ as A_0 is an ℓ-th power.

It now follows that $\operatorname{div}(y) = \ell D$ for some degree 0 divisor D. By property (3), $D \notin \mathcal{P}$. So the divisor class of D has order ℓ in $\mathcal{C}$. □

Given a prime ℓ and a random function field $\mathcal{F}$, it is unlikely that ℓ divides the class number h of $\mathcal{F}$. However, suppose one generates a random polynomial $F(x,T)$ in $\mathbb{F}_q[x,T]$ that is monic in T, irreducible over $\mathbb{F}_q(x)$, and satisfies properties (1) and (4) above. Let y be a root of $F(x,T)$ and $\mathcal{F} = \mathbb{F}_q(x,y)$. Note that if $\mathcal{F}$ is cubic or quartic with at least one quadratic intermediate field, and y as given in (3.1) or (4.1), for example, then it is easy to determine $v_{\mathfrak{P}}(y)$ as shown in Section 4, and thus verify property (2). Moreover, if $\mathcal{F}$ has only one infinite place $\mathfrak{P}$, then ℓ always divides $v_{\mathfrak{P}}(y)$; this follows immediately from Theorem 2.6. In general, y is expected to satisfy property (3), so it is likely that $\ell \mid h$. This could be taken advantage of during the search phase when computing the class number h of $\mathcal{F}$ using the technique of [13].

7. Conclusion and further work

While this paper deals predominantly with particular families of function fields, such as cubic, quartic and radical extensions of a rational function field, the underlying techniques are general and have the potential for broader utilization.

Our method for determining P-signatures as applied to quartic fields with at least one quadratic subfield in Sections 4 and 5 apply in principle to any function field. Recall

that this technique distinguished between different cases that characterize the possible values $v_{\mathfrak{P}}(y)$ of a generator y at any place $\mathfrak{P}$ of the function field. In practice, the method works best for extensions defined by minimal polynomials with few non-zero coefficients. For such extensions, the number of cases to be considered is manageable. The most promising candidates are trinomials and other sparse irreducible polynomials.

It would also be interesting to see if analogues of Theorem 6.4 and Corollary 6.5 extend to radical extensions of higher degree. The ideas that lead to these two results as well as those used in the proofs of Lemma 6.1 and Theorem 6.2 can potentially be applied to other function fields. For example, suppose that the infinite place P_∞ and some finite place P of $\mathbb{F}_q(x)$ of a degree k extension of $\mathbb{F}_q(x)$ have respective signatures $(e, k/e)$ and $(e_\infty, k/e_\infty)$ with $e \mid e_\infty \deg(P)$. If $D = \mathfrak{P} - (e_\infty \deg(P)/e)\mathfrak{P}_\infty$, where $\mathfrak{P} \mid P$ and $\mathfrak{P}_\infty \mid P_\infty$, then $\deg(D) = 0$ and eD is principal. If D is non-principal, then a non-trivial divisor of the class number is found. The same idea can be extended to other degree zero divisors supported at suitable places only. If in addition, several such divisors can be shown to represent independent divisor classes whose respective orders have a common prime factor ℓ, then the number of these classes is a lower bound on the ℓ-rank of the class group of the field.

The extendability of our results to other function fields represents the subject of future research and work in progress.

Acknowledgments

This work represents a significant portion of the first author's thesis [5], co-supervised by Andreas Stein and by the third author who subsequently strengthened and improved on some of the results (in particular Theorem 6.4). Mr. Bembom wishes to thank Professor Stein for bringing this topic to his attention and for many useful discussions. All three authors are indebted to an anonymous referee for carefully reading their manuscript and providing helpful feedback which led to improvements in the overall quality of this paper. The second and third authors were supported by NSERC of Canada and by a University Research Grant of Texas A & M University, respectively.

REFERENCES

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen I, II*, Math. Z. **19** (1924), 153–246.

[2] S. Bae and J. K. Koo, *Genus theory for function fields*, J. Austral. Math. Soc. Ser. A **60** (1996), no. 3, 301–310.

[3] M. Bauer, E. Teske and A. Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), no. 252, 1983–2005.

[4] M. Bauer and J. Webster, *Computations in cubic function fields of characteristic three*, preprint, 2011.

[5] T. Bembom, *Arithmetic problems in cubic and quartic function fields*, Diplomarbeit. Carl von Ossietzky Universität Oldenburg (Germany), 2009.

[6] F. Gerth III, *Sufficiency of genus theory for certain number fields*, Exposition. Math. **1** (1983), no. 4, 357–359.

[7] E. Landquist, *Infrastructure, arithmetic, and class number computations in purely cubic function fields of characteristic at least 5*, Thesis (Ph.D.), University of Illinois at Urbana-Champaign (2009), 194 pp.

[8] E. Landquist, P. Rozenhart, R. Scheidler, J. Webster, and Q. Wu, *An explicit treatment of cubic function fields with applications*, Canad. J. Math. **62** (2010), no. 4, 787–807.

[9] Y. Lee, *The unit rank classification of a cubic function field by its discriminant*, Manuscripta Math. **116** (2005), no. 2, 173–181.

[10] G. Peng, *The genus fields of Kummer function fields*, J. Number Theory **98** (2003), no. 2, 221–227.

[11] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, **210**, Springer-Verlag, New York, 2002, xii+358 pp.

[12] R. Scheidler and A. Stein, *Class number approximation in cubic function fields*, Contrib. Discrete Math. **2** (2007), no. 2, 107–132 (electronic).

[13] R. Scheidler and A. Stein, *Approximating Euler products and class number computation in algebraic function fields*, Rocky Mountain J. Math. **40** (2010), no. 5, 1689–1727.

[14] R. Scheidler, *Algorithmic aspects of cubic function fields*, in Algorithmic number theory, 395–410, Lecture Notes in Comput. Sci., **3076**, Springer, Berlin, 2004.

[15] A. Stein and H. C. Williams, *Some methods for evaluating the regulator of a real quadratic function field*, Experiment. Math. **8** (1999), no. 2, 119–133.

[16] H. Stichtenoth, *Algebraic function fields and codes*, Second edition, Graduate Texts in Mathematics, **254**, Springer-Verlag, Berlin, 2009, xiv+355 pp.

[17] Q. Wu and R. Scheidler, *An explicit treatment of biquadratic function fields*, Contrib. Discrete Math. **2** (2007), no. 1, 43–60 (electronic).

[18] X. K. Zhang, *Ambiguous classes and 2-rank of class group of quadratic function field*, J. China Univ. Sci. Tech. **17** (1987), no. 4, 425–431.

[19] Y. Zhao, W. Li and X. Zhang, *Effective determination of prime decompositions of cubic function fields*, Int. J. Number Theory **6** (2010), no. 2, 437–448.

T. BEMBOM, MATH. INSTITUT, GEORG-AUGUST U. GÖTTINGEN, BUNSENSTRASSE 3-5, D-37073 GÖTTINGEN, GERMANY
TBembom@gmx.de

R. SCHEIDLER, DEPT. OF MATH. & STAT., U. OF CALGARY, 2500 UNIVERSITY DRIVE NW, CALGARY, AB T3N 1N4, CANADA
rscheidl@ucalgary.ca

Q. WU, DEPT. OF ENGINEERING, MATH. AND PHYSICS, TEXAS A&M INTERNATIONAL U., 5201 UNIVERSITY BOULEVARD, LAREDO, TX 78041, USA
qingquan.wu@tamiu.edu