DTU Library

Towers of Function Fields over Non-prime Finite Fields

Bassa, Alp; Beelen, Peter ; Garcia, Arnaldo; Stichtenoth, Henning

TOWERS OF FUNCTION FIELDS OVER
NON-PRIME FINITE FIELDS

ALP BASSA, PETER BEELEN, ARNALDO GARCIA, AND HENNING STICHTENOTH

ABSTRACT. Over all non-prime finite fields, we construct some recursive towers of function fields with many rational places. Thus we obtain a substantial improvement on all known lower bounds for Ihara's quantity $A(\ell)$, for $\ell = p^n$ with p prime and $n > 3$ odd. We relate the explicit equations to Drinfeld modular varieties.

2010 MATH. SUBJ. CLASS. 11G20, 11G09, 11R58.

KEY WORDS AND PHRASES. Curves with many points, towers of function fields, genus, rational places, Ihara's constant.

1. INTRODUCTION

Investigating the number of points on an algebraic curve over a finite field is a classical subject in Number Theory and Algebraic Geometry. The origins go back to Fermat, Euler and Gauss, among many others. The basic result is A. Weil's theorem, which is equivalent to the validity of Riemann's Hypothesis in this context. New impulses came from Goppa's construction of good codes from curves with many rational points, and also from applications to cryptography. For information, we refer to [9], [21].

One of the main open problems in this area of research is the determination of Ihara's quantity $A(\ell)$ for non-square finite fields; i.e., for cardinalities $\ell = p^n$ with p prime and n odd. This quantity controls the asymptotic behaviour of the number of $\mathbb{F}_\ell$-rational points (places) on algebraic curves (function fields) as the genus increases. This is the topic of our paper.

Let F be an algebraic function field of one variable over $\mathbb{F}_\ell$, with the field $\mathbb{F}_\ell$ being algebraically closed in F. We denote

$$N(F) = \text{number of } \mathbb{F}_\ell\text{-rational places of } F, \text{ and } g(F) = \text{genus of } F.$$

The Hasse–Weil upper bound states that

$$N(F) \leqslant 1 + \ell + 2\sqrt{\ell} \cdot g(F).$$

This upper bound was improved by Serre [23] who showed that the factor $2\sqrt{\ell}$ can be replaced above by its integer part $\lfloor 2\sqrt{\ell} \rfloor$.

Ihara [16] was the first to realize that the Hasse–Weil upper bound becomes weak when the genus $g(F)$ is large with respect to the size ℓ of the ground field $\mathbb{F}_\ell$. He introduced the quantity

$$A(\ell) = \limsup_{g(F) \to \infty} \frac{N(F)}{g(F)}, \tag{1}$$

where the limit is taken over all function fields $F/\mathbb{F}_\ell$ of genus $g(F) > 0$. By Hasse–Weil it holds that $A(\ell) \leqslant 2\sqrt{\ell}$, and Ihara showed that $A(\ell) < \sqrt{2\ell}$.

The best upper bound known is due to Drinfeld–Vlăduţ [2]. It states that

$$A(\ell) \leqslant \sqrt{\ell} - 1, \quad \text{for any prime power } \ell. \tag{2}$$

If ℓ is a square, the opposite inequality $A(\ell) \geqslant \sqrt{\ell} - 1$ had been shown earlier by Ihara using the theory of modular curves (see [15]). Hence

$$A(\ell) = \sqrt{\ell} - 1, \quad \text{when } \ell \text{ is a square.} \tag{3}$$

For all other cases when the cardinality ℓ is a non-square, the exact value of the quantity $A(\ell)$ is not known. Tsfasman–Vlăduţ–Zink [25] used Equation (3) to prove the existence of long linear codes with relative parameters above the Gilbert–Varshamov bound, for finite fields of square cardinality $\ell = q^2$ with $q \geqslant 7$. They also gave a proof of Equation (3) in the cases $\ell = p^2$ or $\ell = p^4$ with p a prime number.

To investigate $A(\ell)$ one introduces the notion of (infinite) towers of $\mathbb{F}_\ell$-function fields:

$$\mathcal{F} = (F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots \subseteq F_i \subseteq \ldots),$$

where all F_i are function fields over $\mathbb{F}_\ell$, with $\mathbb{F}_\ell$ algebraically closed in F_i, and $g(F_i) \to \infty$ as $i \to \infty$. Without loss of generality one can assume that all extensions F_{i+1}/F_i are separable. As follows from Hurwitz' genus formula, the limit below exists (see [6]) and it is called the limit of the tower $\mathcal{F}$:

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)}.$$

Clearly, the limit of any tower $\mathcal{F}$ over $\mathbb{F}_\ell$ provides a lower bound for $A(\ell)$; i.e.,

$$0 \leqslant \lambda(\mathcal{F}) \leqslant A(\ell), \quad \text{for any } \mathbb{F}_\ell\text{-tower } \mathcal{F}.$$

So one looks for towers with big limits in order to get good lower bounds for Ihara's quantity. Serre [23] used Hilbert classfield towers to show that for all prime powers ℓ,

$$A(\ell) > c \cdot \log_2(\ell), \quad \text{with an absolute constant } c > 0. \tag{4}$$

One can take $c = 1/96$, see [21, Theorem 5.2.9]. When $\ell = q^3$ is a cubic power, one has the lower bound

$$A(q^3) \geqslant \frac{2(q^2 - 1)}{q + 2}, \quad \text{for any prime power } q. \tag{5}$$

When $q = p$ is a prime number, this bound was obtained by Zink [26] using degenerations of modular surfaces. The proof of Equation (5) for general q was given by Bezerra, Garcia and Stichtenoth [1] using recursive towers of function fields; i.e., towers which are given in a recursive way by explicit polynomial equations. The concept of recursive towers turned out to be very fruitful for constructing towers with a large limit.

An $\mathbb{F}_\ell$-tower $\mathcal{F} = (F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots)$ is recursively defined by $f(X, Y) \in \mathbb{F}_\ell[X, Y]$ when

(i) $F_1 = \mathbb{F}_\ell(x_1)$ is the rational function field, and
(ii) $F_{i+1} = F_i(x_{i+1})$ with $f(x_i, x_{i+1}) = 0$, for all $i \geqslant 1$.

For instance, when $\ell = q^2$ is a square, the polynomial (see [6])

$$f(X, Y) = (1 + X^{q-1})(Y^q + Y) - X^q \in \mathbb{F}_{q^2}[X, Y]$$

defines a recursive tower over $\mathbb{F}_{q^2}$ whose limit $\lambda(\mathcal{F}) = q - 1$ attains the Drinfeld–Vlăduţ bound.

When $\ell = q^3$ is a cubic power one can choose the polynomial (see [1])

$$f(X, Y) = Y^q(X^q + X - 1) - X(1 - Y) \in \mathbb{F}_{q^3}[X, Y] \tag{6}$$

to obtain a recursive tower over $\mathbb{F}_{q^3}$ with limit $\lambda(\mathcal{F}) \geqslant 2(q^2 - 1)/(q + 2)$; this is the proof of Equation (5) above. The case $q = 2$ of Equation (6) is due to van der Geer–van der Vlugt [11].

In the particular case of a prime field, no explicit or modular tower with positive limit is known; only variations of Serre's classfield tower method have been successful in this case, see [3], [21].

All known lower bounds for $A(p^n)$, with a prime number p and an odd exponent $n > 3$, are rather weak, see [18], [21]. For example, one has for q odd and $n \geqslant 3$ prime (see [19])

$$A(q^n) \geqslant \frac{4q + 4}{\left\lfloor \frac{3 + \lfloor 2\sqrt{2q+2} \rfloor}{n-2} \right\rfloor + \lfloor 2\sqrt{2q+3} \rfloor}. \tag{7}$$

The main contribution of this paper is a new lower bound on $A(p^n)$ that gives a substantial improvement over all known lower bounds, for any prime p and any odd $n > 3$. For large n and small p, this new bound is rather close to the Drinfeld–Vlăduţ upper bound for $A(p^n)$. Moreover, it is obtained through a recursive tower with an explicit polynomial $f(X, Y) \in \mathbb{F}_p[X, Y]$.

Our lower bound is:

Theorem 1.1. *Let p be a prime number and $n = 2m + 1 \geqslant 3$ an odd integer. Then*

$$A(p^n) \geqslant \frac{2(p^{m+1} - 1)}{p + 1 + \epsilon} \quad \text{with } \epsilon = \frac{p - 1}{p^m - 1}.$$

In particular $A(p^{2m+1}) > p^m - 1$, which shows that a conjecture by Manin [10], [20] is false for all odd integers $n = 2m + 1 \geqslant 3$.

The bound of Drinfeld–Vlăduţ can be written as

$$A(p^{2m+1}) \leqslant p^m \cdot \sqrt{p} - 1.$$

Fixing the prime number p, we get

$$\frac{\text{our lower bound}}{\text{Drinfeld–Vlăduţ bound}} \to \frac{2\sqrt{p}}{p+1}, \quad \text{as } m \to \infty.$$

For $p = 2$ we have $2\sqrt{p}/(p+1) \approx 0.9428\ldots$, hence our lower bound is only around 6% below the Drinfeld–Vlăduţ upper bound, for large odd-degree extensions of the binary field $\mathbb{F}_2$.

Now we give the defining equations for the several recursive towers $\mathcal{F}$ that we consider in this paper. Let $\mathbb{F}_\ell$ be a non-prime field and write $\ell = q^n$ with $n \geqslant 2$. Here the integer n can be even or odd. For every partition of n in relatively prime parts,

$$n = j + k \quad \text{with } j \geqslant 1, k \geqslant 1 \quad \text{and} \quad \gcd(j, k) = 1, \tag{8}$$

we consider the recursive tower $\mathcal{F}$ over $\mathbb{F}_\ell$ that is given by the equation

$$\mathrm{Tr}_j\left(\frac{Y}{X^{q^k}}\right) + \mathrm{Tr}_k\left(\frac{Y^{q^j}}{X}\right) = 1, \tag{9}$$

where

$$\mathrm{Tr}_a(T) := T + T^q + T^{q^2} + \cdots + T^{q^{a-1}} \quad \text{for any } a \in \mathbb{N}.$$

Theorem 1.2. *Equation* (9) *defines a recursive tower* $\mathcal{F}$ *over* $\mathbb{F}_\ell$ *whose limit satisfies*

$$\lambda(\mathcal{F}) \geqslant 2\left(\frac{1}{q^j - 1} + \frac{1}{q^k - 1}\right)^{-1};$$

i.e., the harmonic mean of $q^j - 1$ *and* $q^k - 1$ *is a lower bound for* $\lambda(\mathcal{F})$.

The very special case $n = 2$ and $k = j = 1$ of Equation (9) gives a recursive representation of the first explicit tower attaining the Drinfeld–Vlăduţ bound, see [5]. This particular case was our inspiration to consider Equation (9).

For a fixed finite field $\mathbb{F}_\ell$ with non-prime ℓ, Theorem 1.2 may give several towers over $\mathbb{F}_\ell$ with distinct limits; this comes from two sources: the chosen representation $\ell = q^n$ with $n \geqslant 2$ (i.e., the choice of q), and the chosen partition $n = j + k$. For a cardinality ℓ that is neither a prime nor a square, the best lower bound comes from

representing ℓ as $\ell = p^n$ (i.e., choose $q = p$);
writing $n \geqslant 3$ as $n = 2m + 1$, choose the partition with $j = m$ and $k = m + 1$.

The lower bound in Theorem 1.2 in this case reads as

$$\lambda(\mathcal{F}) \geqslant 2\left(\frac{1}{p^m - 1} + \frac{1}{p^{m+1} - 1}\right)^{-1} = \frac{2(p^{m+1} - 1)}{p + 1 + \epsilon}, \quad \text{with } \epsilon = \frac{p - 1}{p^m - 1}.$$

This is the tower that proves Theorem 1.1, our main result.

Furthermore, we show that the curves in the tower are related to one-dimensional varieties parametrizing certain $\mathbb{F}_q[T]$-Drinfeld modules of characteristic $T - 1$ and rank $n \geqslant 2$ together with some additional varying structure.

This paper is organized as follows. In Section 2 we investigate the 'basic function field' of the tower $\mathcal{F}$. This is defined as $F = \mathbb{F}_\ell(x, y)$, where x, y satisfy Equation (9). In particular, the ramification structure of the extensions $F/\mathbb{F}_\ell(x)$ and $F/\mathbb{F}_\ell(y)$ is discussed in detail. Section 3 is the core of our paper. Here we study

the tower $\mathcal{F} = (F_1 \subseteq F_2 \subseteq \cdots)$ and prove Theorem 1.2. The principal difficulty is to show that the genus $g(F_i)$ grows 'rather slowly' as $i \to \infty$. Finally, in Section 4 we show that our tower $\mathcal{F}$ occurs quite naturally when studying Drinfeld modules of rank n, thus providing a modular motivation of the tower.

We hope that this paper will lead to further developments in the theories of explicit towers and of modular towers, and their relations.

2. The Basic Function Field

First we introduce some notation.

p is a prime number, q is a power of p, and $\ell = q^n$ with $n \geqslant 2$,
$\mathbb{F}_\ell$ is the finite field of cardinality ℓ, and $\overline{\mathbb{F}}_\ell$ is the algebraic closure of $\mathbb{F}_\ell$.
For simplicity we also denote $K = \mathbb{F}_\ell$ or $\overline{\mathbb{F}}_\ell$.
For an integer $a \geqslant 1$, we set $\mathrm{Tr}_a(T) := T + T^q + \cdots + T^{q^{a-1}} \in K[T]$.

Remark 2.1. (i) Let $a, b \geqslant 1$. Then $(\mathrm{Tr}_a \circ \mathrm{Tr}_b)(T) = (\mathrm{Tr}_b \circ \mathrm{Tr}_a)(T)$.

(ii) Let $\Omega \supseteq \mathbb{F}_q$ be a field. The evaluation map $\mathrm{Tr}_a \colon \Omega \to \Omega$ is $\mathbb{F}_q$-linear; its kernel is contained in the subfield $\mathbb{F}_{q^a} \cap \Omega \subseteq \Omega$.

(iii) Let $a, b \geqslant 1$ and $\gcd(a, b) = 1$. Then $K(s) = K(\mathrm{Tr}_a(s), \mathrm{Tr}_b(s))$ for any $s \in \Omega$.

Proof. Item (ii) is clear and the proof of (i) is straightforward. Item (iii) follows by induction from the equation

$$\mathrm{Tr}_c(T) = \mathrm{Tr}_r(T) + (\mathrm{Tr}_d(T))^{q^r},$$

which holds whenever $c = d + r > d$. $\qquad\qquad\square$

We also fix a partition of n into relatively prime integers; i.e., we write

$$n = j + k, \quad \text{with integers } j, k \geqslant 1 \text{ and } \gcd(j, k) = 1. \tag{10}$$

Without loss of generality we can assume that

$$p \text{ does not divide } j. \tag{11}$$

In this section we study the function field $F = K(x, y)$, where x, y satisfy the equation

$$\mathrm{Tr}_j\left(\frac{y}{x^{q^k}}\right) + \mathrm{Tr}_k\left(\frac{y^{q^j}}{x}\right) = 1. \tag{12}$$

This 'basic function field' F is the first step in the tower $\mathcal{F}$ that will be considered in Section 3. We abbreviate

$$R := \frac{y}{x^{q^k}}, \quad S := \frac{y^{q^j}}{x} \quad \text{and} \quad \alpha := j^{-1} \in \mathbb{F}_p. \tag{13}$$

Proposition 2.2. There exists a unique element $u \in F$ such that

$$R = \mathrm{Tr}_k(u) + \alpha \quad \text{and} \quad S = -\mathrm{Tr}_j(u). \tag{14}$$

Moreover it holds that $K(u) = K(R, S)$ and $F = K(x, y) = K(x, u) = K(u, y)$.

Proof. Let $\Omega \supseteq F$ be an algebraically closed field. Choose $u_0 \in \Omega$ such that $\mathrm{Tr}_k(u_0) = R - \alpha$. Set

$$\mathcal{M} := \{\mu \in \Omega \colon \mathrm{Tr}_k(\mu) = 0\} \quad \text{and} \quad u_\mu := u_0 + \mu, \quad \text{for } \mu \in \mathcal{M}.$$

Then $\mathrm{Tr}_k(u_\mu) = R - \alpha$ for all $\mu \in \mathcal{M}$, and by Equation (12)

$$\begin{aligned} 1 &= \mathrm{Tr}_j(R) + \mathrm{Tr}_k(S) = \mathrm{Tr}_j(\mathrm{Tr}_k(u_\mu) + \alpha) + \mathrm{Tr}_k(S) \\ &= \mathrm{Tr}_k(\mathrm{Tr}_j(u_\mu)) + j\alpha + \mathrm{Tr}_k(S) = \mathrm{Tr}_k(S + \mathrm{Tr}_j(u_\mu)) + 1. \end{aligned}$$

Hence $S + \mathrm{Tr}_j(u_\mu) \in \mathcal{M}$. The map $\mu \mapsto S + \mathrm{Tr}_j(u_\mu)$ from $\mathcal{M}$ to itself is injective. To see this, assume that $S + \mathrm{Tr}_j(u_0 + \mu) = S + \mathrm{Tr}_j(u_0 + \mu')$ with $\mu, \mu' \in \mathcal{M}$. Then $\mathrm{Tr}_j(\mu - \mu') = 0 = \mathrm{Tr}_k(\mu - \mu')$, hence $\mu - \mu' \in \mathbb{F}_{q^j} \cap \mathbb{F}_{q^k} = \mathbb{F}_q$ and $0 = \mathrm{Tr}_j(\mu - \mu') = j(\mu - \mu')$. As j is relatively prime to p, it follows that $\mu = \mu'$.

Since $\mathcal{M}$ is a finite set and $0 \in \mathcal{M}$, there exists some $\mu_0 \in \mathcal{M}$ such that $S + \mathrm{Tr}_j(u_{\mu_0}) = 0$, and then the element $u := u_{\mu_0}$ satisfies Equation (14). From item (iii) of Remark 2.1, we conclude that $K(u) = K(R, S) \subseteq F$. In particular, the element u belongs to F.

To prove uniqueness, assume that $\tilde{u} \in \Omega$ is another element which satisfies Equation (14). Then $\mathrm{Tr}_k(\tilde{u}) = \mathrm{Tr}_k(u)$ and $\mathrm{Tr}_j(\tilde{u}) = \mathrm{Tr}_j(u)$; hence $\tilde{u} - u \in \mathbb{F}_{q^k} \cap \mathbb{F}_{q^j} = \mathbb{F}_q$ and $0 = \mathrm{Tr}_j(\tilde{u} - u) = j(\tilde{u} - u)$. This implies $\tilde{u} = u$.

The inclusion $K(x, u) \subseteq K(x, y)$ is clear. Conversely, we have $y = Rx^{q^k} \in K(x, u)$ by Equation (14), hence $K(x, y) \subseteq K(x, u)$. The equality $K(x, y) = K(u, y)$ is shown similarly. $\square$

Proposition 2.3. The extension $F/K(u)$ is a cyclic extension of degree $[F : K(u)] = q^n - 1$. The elements x and y are Kummer generators for $F/K(u)$, and they satisfy the equations

$$x^{q^n - 1} = \frac{-\mathrm{Tr}_j(u)}{(\mathrm{Tr}_k(u) + \alpha)^{q^j}} \quad \text{and} \quad y^{q^n - 1} = \frac{-(\mathrm{Tr}_j(u))^{q^k}}{\mathrm{Tr}_k(u) + \alpha}.$$

The field K is the full constant field of F; i.e., K is algebraically closed in F.

Proof. By Equation (13),

$$Sx = y^{q^j} = (Rx^{q^k})^{q^j} = R^{q^j} x^{q^n}.$$

Hence, using Equation (14), we obtain

$$x^{q^n - 1} = \frac{S}{R^{q^j}} = \frac{-\mathrm{Tr}_j(u)}{(\mathrm{Tr}_k(u) + \alpha)^{q^j}}.$$

The equation for $y^{q^n - 1}$ is proved in the same way. The element

$$\frac{-\mathrm{Tr}_j(u)}{(\mathrm{Tr}_k(u) + \alpha)^{q^j}} \in K(u)$$

has a simple zero at $u = 0$; this place is therefore totally ramified in $F = K(x, u)$ over $K(u)$, with ramification index $e = q^n - 1$. Hence $[F : K(u)] = q^n - 1$, and K is algebraically closed in F. As the field K contains all $(q^n - 1)$-th roots of unity, the extension $F/K(u)$ is cyclic. $\square$

Corollary 2.4. *Set $w := -x^{q^n-1}$ and $z := -y^{q^n-1}$. Then one has a diagram of subfields of F as in Figure 1. The extensions $K(x)/K(w)$, $K(y)/K(z)$ and $F/K(u)$ are all cyclic of degree $q^n - 1$; the extensions $F/K(x)$, $F/K(y)$, $K(u)/K(w)$ and $K(u)/K(z)$ are all of degree q^{n-1}.*

Proof. This follows directly from Proposition 2.3, since

$$w = -x^{q^n-1} = \frac{\mathrm{Tr}_j(u)}{(\mathrm{Tr}_k(u) + \alpha)^{q^j}} \quad \text{and} \quad z = -y^{q^n-1} = \frac{(\mathrm{Tr}_j(u))^{q^k}}{\mathrm{Tr}_k(u) + \alpha}. \tag{15}$$
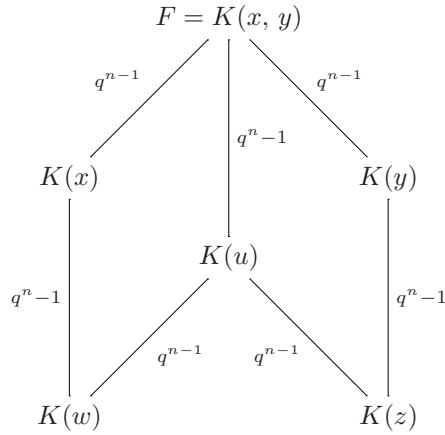□

FIGURE 1. Subextensions of F and their degrees

Our next goal is to describe ramification and splitting of places in the various field extensions in Figure 1. Denote by $\mathbb{F}_\ell^\times$ the multiplicative group of $\mathbb{F}_\ell$. We need some more notation:

(i) Let E be a function field over K and $0 \neq t \in E$. Then the divisors

$$\mathrm{div}(t), \ \mathrm{div}_0(t) \text{ and } \mathrm{div}_\infty(t)$$

are the principal divisor, zero divisor and pole divisor of t in E. Similarly, the divisor of a nonzero differential ω of E is denoted by $\mathrm{div}(\omega)$.

(ii) Let $K(t)$ be a rational function field over K. Then the places

$$[t = \infty] \quad \text{and} \quad [t = \beta]$$

are the pole of t and the zero of $t - \beta$ in $K(t)$, for any $\beta \in K$.

(iii) Let E/H be a finite separable extension of function fields over K. Let P be a place of H and P' a place of E lying above P. Then $e(P'|P)$ is the ramification index, and $d(P'|P)$ is the different exponent of P' over P.

Proposition 2.5. *For all $\beta \in \mathbb{F}_\ell^\times$, the place $[x = \beta]$ splits completely in F; i.e., there are q^{n-1} distinct places of F above $[x = \beta]$, all of degree one. For all places P of F above $[x = \beta]$, the restriction of P to $K(y)$ is a place $[y = \beta']$ with some $\beta' \in \mathbb{F}_\ell^\times$.*

Proof. Upon multiplication by $x^{q^{k-1}}$, Equation (12) is the minimal polynomial of y over $K(x)$. Substituting $x = \beta$ into this equation we obtain

$$\mathrm{Tr}_n\left(\frac{y}{\beta^{q^k}}\right) = 1,$$

which has q^{n-1} simple roots, all belonging to $\mathbb{F}_\ell^\times$. $\square$

Next we describe ramification in subextensions of F. As ramification indices and different exponents do not change under separable constant field extensions, we will assume until the end of Section 2 that $K = \overline{\mathbb{F}}_\ell$. Hence all places of F will have degree one. Recall that $\alpha \in \mathbb{F}_p$ and $j\alpha = 1$. The following sets will be important:

$$\Gamma := \{\gamma \in K \colon \mathrm{Tr}_j(\gamma) = 0\} \tag{16}$$

and

$$\Delta := \{\delta \in K \colon \mathrm{Tr}_k(\delta) + \alpha = 0\}. \tag{17}$$

Clearly $\#\Gamma = q^{j-1}$, $\#\Delta = q^{k-1}$ and $\Gamma \cap \Delta = \varnothing$.

Proposition 2.6. Ramification in $F/K(u)$ is as follows:
  (i) The places $[u = \gamma]$ with $\gamma \in \Gamma$ and $[u = \delta]$ with $\delta \in \Delta$ are totally ramified in $F/K(u)$. We denote by P_γ (resp. Q_δ) the unique place of F lying above $[u = \gamma]$ (resp. above $[u = \delta]$).
  (ii) There are exactly $q - 1$ places of F above $[u = \infty]$; we denote them by $V_1, \ldots, V_{q-1}$. Their ramification indices are $e(V_i|[u = \infty]) = (q^n - 1)/(q - 1)$.
  (iii) All other places of $K(u)$ are unramified in F.

Proof. Follows from Hasse's theory of Kummer extensions, see [24, Proposition 3.7.3]. $\square$

Corollary 2.7. *The genus of F is*

$$g(F) = \frac{1}{2}\big((q^n - 2)(q^{j-1} + q^{k-1} - 2) + (q^n - q)\big).$$

*Proof.* Apply Hurwitz' genus formula [24, Theorem 3.4.13] to the extension $F/K(u)$. Observe that all ramifications in this extension are tame. $\square$

The next proposition will play an essential role in Section 3. For abbreviation we set

$$N_r := \frac{q^r - 1}{q - 1}, \quad \text{for every integer } r \geqslant 1. \tag{18}$$

Proposition 2.8. Ramification indices and different exponents of the places P_γ, Q_δ and V_i in the various subextensions of F are as shown in Figures 2, 3 and 4. All other places in these subextensions are unramified.

Proof. We work out the behaviour of the places V_i in Figure 4; the other cases are done in a similar way. So we consider a place $V = V_i$ of F lying above the place $[u = \infty]$. It follows from Equation (15) that V is a zero of x and w, and a pole of y and z. Hence the restrictions of V to the subfields $K(x)$, $K(w)$, $K(y)$ and $K(z)$ are the places $[x = 0]$, $[w = 0]$, $[y = \infty]$ and $[z = \infty]$.

$$P_\gamma$$
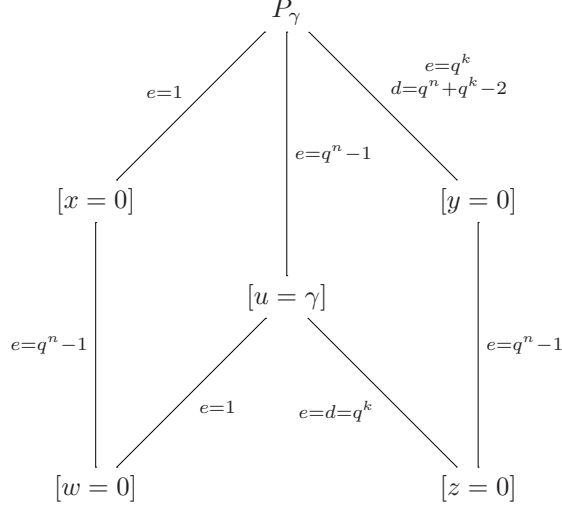
Figure 2. Ramification and different exponents for P_γ, $\gamma \in \Gamma$

$$Q_\delta$$
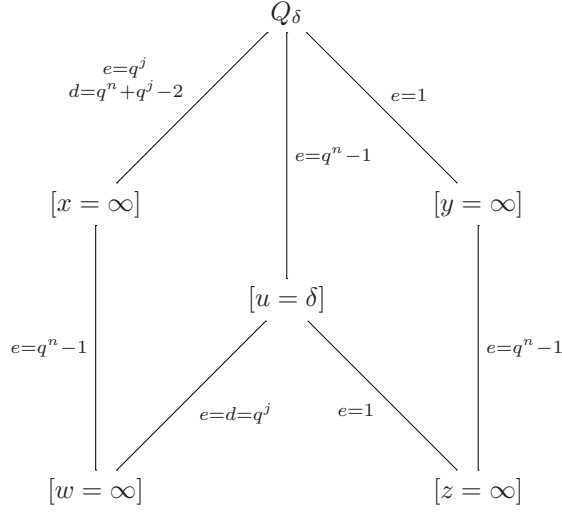
Figure 3. Ramification and different exponents for Q_δ, $\delta \in \Delta$

Next we investigate ramification of $[u = \infty]$ over $[w = 0]$. From Equation (15), the zero and pole divisor of w in $K(u)$ are as follows:

$$\mathrm{div}_0(w) = \sum_{\gamma \in \Gamma} [u = \gamma] + (q^{n-1} - q^{j-1})\,[u = \infty] \tag{19}$$

and

$$\mathrm{div}_\infty(w) = q^j \sum_{\delta \in \Delta} [u = \delta]. \tag{20}$$
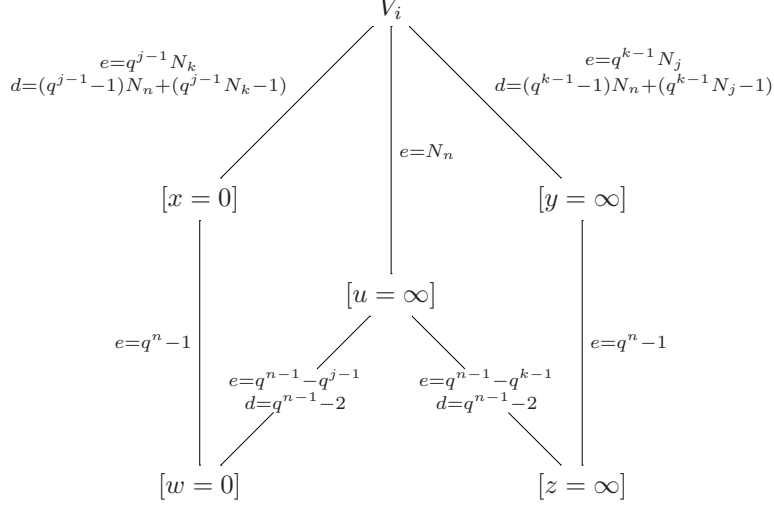
FIGURE 4. Ramification and different exponents for V_i, $1 \leqslant i \leqslant q$

Equation (19) shows that $e([u = \infty]|[w = 0]) = q^{n-1} - q^{j-1} = q^{j-1}(q^k - 1)$. The divisor of the differential dw in $K(u)$ is

$$\operatorname{div}(dw) = -2\operatorname{div}_\infty(w) + \operatorname{Diff}(K(u)/K(w)), \tag{21}$$

where $\operatorname{Diff}(K(u)/K(w))$ is the different of the extension $K(u)/K(w)$, see [24, p. 178, Equation (4.37)]. Differentiating the equation

$$\operatorname{Tr}_j(u) = (\operatorname{Tr}_k(u) + \alpha)^{q^j} \cdot w$$

gives

$$du = (\operatorname{Tr}_k(u) + \alpha)^{q^j} \cdot dw$$

and hence

$$\begin{aligned}
\operatorname{div}(dw) &= \operatorname{div}(du) - q^j \cdot \operatorname{div}(\operatorname{Tr}_k(u) + \alpha) \\
&= -2\,[u = \infty] - q^j \sum_{\delta \in \Delta} [u = \delta] + q^j \cdot q^{k-1}\,[u = \infty] \\
&= (q^{n-1} - 2)\,[u = \infty] - q^j \sum_{\delta \in \Delta} [u = \delta]. \tag{22}
\end{aligned}$$

We substitute (22) and (20) into Equation (21) and obtain

$$\operatorname{Diff}(K(u)/K(w)) = (q^{n-1} - 2)\,[u = \infty] + q^j \sum_{\delta \in \Delta} [u = \delta],$$

hence the different exponent of the place $[u = \infty]$ over $[w = 0]$ is

$$d([u = \infty]|[w = 0]) = q^{n-1} - 2.$$

The place extensions $V|[u = \infty]$ and $[x = 0]|[w = 0]$ are tamely ramified, with ramification indices given by $e(V|[u = \infty]) = N_n$ and $e([x = 0]|[w = 0]) = q^n - 1$.

We see easily that

$$e(V|[x=0]) = q^{j-1}N_k,$$

and transitivity of different exponents gives (see [24, Corollary 3.4.12])

$$d(V|[x=0]) = (q^{j-1}-1)N_n + (q^{j-1}N_k - 1).$$

We have thus proved the left hand side of Figure 4. The proof of the right hand side is analogous. $\qquad\square$

We will also need the following lemma.

Lemma 2.9. We have $K(u) = K(z, w)$.

Proof. The field $L := K(z, w)$ is clearly contained in $K(u)$ (see Figure 1). As $F = L(x, y)$ and $x^{q^n-1}, y^{q^n-1} \in L$, it follows that $[F : L]$ divides $(q^n - 1)^2$, and therefore $[K(u) : L]$ is relatively prime to p. But $[K(u) : L]$ divides the degree $[K(u) : K(w)] = q^{n-1}$, hence $[K(u) : L] = 1$. $\qquad\square$

For the convenience of the reader, we state Abhyankar's lemma and Hensel's lemma; they will be used frequently in Section 3.

Proposition 2.10 (Abhyankar's lemma, [24, Theorem 3.9.1])**.** Let H be a field with a discrete valuation $\nu\colon H \to \mathbb{Z} \cup \{\infty\}$ having a perfect residue class field. Let H'/H be a finite separable field extension of H and suppose that $H' = H_1 \cdot H_2$ is the composite of two intermediate fields $H \subseteq H_1, H_2 \subseteq H'$. Let ν' be an extension of ν to H' and ν_i the restriction of ν' to H_i, for $i = 1, 2$. Assume that at least one of the extensions $\nu_1|\nu$ or $\nu_2|\nu$ is tame (i.e., the ramification index $e(\nu_i|\nu)$ is relatively prime to the characteristic of the residue class field of ν). Then one has $e(\nu'|\nu) = \mathrm{lcm}\{e(\nu_1|\nu), e(\nu_2|\nu)\}$, where lcm means the least common multiple.

Proposition 2.11 (Hensel's lemma, [17, p. 230])**.** Let H be a field which is complete with respect to a discrete valuation $\nu\colon H \to \mathbb{Z} \cup \{\infty\}$. Let $\mathcal{O}$ be the valuation ring of ν and $\mathfrak{m}$ its maximal ideal. Denote by $H^* = \mathcal{O}/\mathfrak{m}$ the residue class field of ν and by $a \mapsto a^*$ the canonical homomorpism of $\mathcal{O}$ onto H^*. Suppose that the polynomial $\varphi(T) \in \mathcal{O}[T]$ has the following property: its reduction $\varphi^*(T) \in H^*[T]$ factorizes as $\varphi^*(T) = \eta_1(T) \cdot \eta_2(T)$ with

$$\eta_1(T),\ \eta_2(T) \in H^*[T],\ \ \gcd(\eta_1(T), \eta_2(T)) = 1,\ \text{ and }\ \eta_1(T) \text{ is monic.}$$

Then there are polynomials $\varphi_1(T), \varphi_2(T) \in \mathcal{O}[T]$ such that $\varphi(T) = \varphi_1(T) \cdot \varphi_2(T)$ with

$$\varphi_1(T) \text{ is monic, } \deg \varphi_1(T) = \deg \eta_1(T),\ \ \varphi_1^*(T) = \eta_1(T)\ \text{ and }\ \varphi_2^*(T) = \eta_2(T).$$

3. The Tower

We keep all notation as before. In this section we consider a sequence of function fields,

$$\mathcal{F} = (F_1 \subseteq F_2 \subseteq F_3 \subseteq \dots),$$

where $F_1 = K(x_1)$ is the rational function field, and for all $i \geqslant 1$, $F_{i+1} = F_i(x_{i+1})$ with

$$\mathrm{Tr}_j\left(\frac{x_{i+1}}{x_i^{q^k}}\right) + \mathrm{Tr}_k\left(\frac{x_{i+1}^{q^j}}{x_i}\right) = 1. \tag{23}$$

A convenient way to investigate such a sequence is to consider the corresponding 'pyramid' of field extensions as shown in Figure 5. Note that the fields $K(x_i, x_{i+1})$ are isomorphic to the 'basic function field' $F = K(x, y)$ that was studied in Section 2.

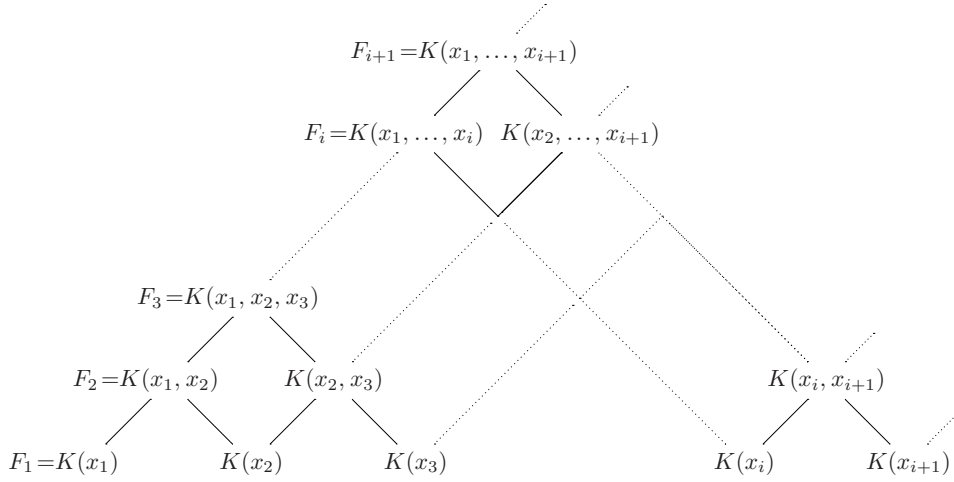

FIGURE 5. The pyramid corresponding to $\mathcal{F}$

Proposition 3.1. The sequence $\mathcal{F}$ is a tower of function fields over K; i.e., for all $i \geqslant 1$ the following hold:

(i) K is the full constant field of F_i,
(ii) F_{i+1}/F_i is a separable extension of degree $[F_{i+1} : F_i] > 1$,
(iii) $g(F_i) \to \infty$ as $i \to \infty$.

Proof. Equation (23) is a separable equation for x_{i+1} over F_i, hence F_{i+1}/F_i is separable. Let P be a place of F_{i+1} which lies above the place $[x_1 = \infty]$ of F_1. From Figure 3 we have ramification indices and different exponents in the pyramid as shown in Figure 6.

As the ramification index of P over F_i is $e = q^j > 1$, it follows that $F_i \subsetneqq F_{i+1}$. Let $\beta \in \mathbb{F}_\ell^\times$. We show by induction that the rational place $[x_1 = \beta]$ splits completely in F_i/F_1, for all $i \geqslant 2$. For $i = 2$ this holds by Proposition 2.5. Assume that the claim holds for F_i, and let P_i be a place of F_i lying above $[x_1 = \beta]$. Again by Proposition 2.5, the restriction of P_i to $K(x_i)$ is of the form $[x_i = \beta']$ with some $\beta' \in \mathbb{F}_\ell^\times$, and the place $[x_i = \beta']$ splits completely in $K(x_i, x_{i+1})/K(x_i)$. Hence P_i splits completely in F_{i+1}/F_i, see [24, Proposition 3.9.6].
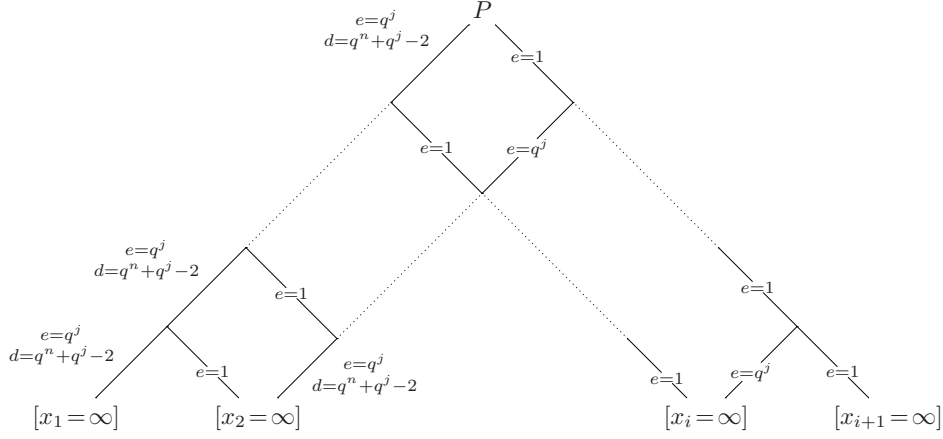
FIGURE 6. Ramification over $[x_1 = \infty]$

We conclude that F_i has places with residue class field K, so K is the full constant field of F_i. Thus we have shown items (i) and (ii). By Corollary 2.7, the genus of $F_2 = K(x_1, x_2)$ satisfies $g(F_2) \geqslant 1$. Since there is some ramified place in every extension F_{i+1}/F_i, it follows from Hurwitz' genus formula that $g(F_i) \to \infty$ as $i \to \infty$. $\qquad\square$

As a consequence of the proof above we get:

Corollary 3.2. *All places $[x_1 = \beta]$ with $\beta \in \mathbb{F}_\ell^\times$ split completely in F_i/F_1. In particular in the case $K = \mathbb{F}_\ell$, the number $N(F_i)$ of rational places of $F_i/\mathbb{F}_\ell$ satisfies the inequality*

$$N(F_i) \geqslant (\ell - 1) \cdot [F_i : F_1].$$

In order to prove Theorem 1.2, one needs an estimate for the genus $g(F_i)$, as $i \to \infty$. Since ramification indices, different exponents and genera are invariant under separable constant field extensions, we will assume from now on that

$$K = \overline{\mathbb{F}}_\ell \text{ is algebraically closed.}$$

Then all places of F_i/K are rational.

Definition 3.3. (i) Let E/H be a separable extension of function fields over K, P a place of H and $b \in \mathbb{R}^+$. We say that P is b-bounded in E if for any place P' of E above P, the different exponent $d(P'|P)$ satisfies

$$d(P'|P) \leqslant b \cdot (e(P'|P) - 1).$$

(ii) Let $\mathcal{H} = (H_1, H_2, \dots)$ be a tower of function fields over K, P a place of H_1 and $b \in \mathbb{R}^+$. We say that P is b-bounded in $\mathcal{H}$, if it is b-bounded in all extensions H_i/H_1.

Proposition 3.4. Let $\mathcal{H} = (H_1, H_2, \dots)$ be a tower of function fields over K, with $g(H_1) = 0$. Assume that $P_1, \dots, P_r$ are places of H_1 and $b_1, \dots, b_r \in \mathbb{R}^+$ are positive real numbers such that the following hold:

(i) P_s is b_s-bounded in $\mathcal{H}$, for $1 \leqslant s \leqslant r$.
(ii) All places of H_1, except for $P_1, \ldots, P_r$, are unramified in H_i/H_1.

Then the genus $g(H_i)$ is bounded by

$$g(H_i) - 1 \leqslant \left(-1 + \frac{1}{2} \sum_{s=1}^{r} b_s \right) \cdot [H_i : H_1].$$

Proof. This is an immediate consequence of Hurwitz' genus formula, see also [7]. $\square$

We want to apply Proposition 3.4 to the tower $\mathcal{F}$. By Proposition 2.6, only the places $[x_1 = 0]$ and $[x_1 = \infty]$ of $F_1 = K(x_1)$ are ramified in $\mathcal{F}$ (see Figures 2, 3 and 4). From Figure 6 and the transitivity of different exponents, the place $[x_1 = \infty]$ is b_∞-bounded with

$$b_\infty := \frac{q^n - 1}{q^j - 1} + 1. \tag{24}$$

Main Claim. *The place $[x_1 = 0]$ is b_0-bounded with*

$$b_0 := \frac{q^n - 1}{q^k - 1} + 1. \tag{25}$$

Assuming this claim, Proposition 3.4 yields the estimate

$$g(F_i) - 1 \leqslant \left(-1 + \frac{1}{2} (b_0 + b_\infty) \right) [F_i : F_1] = \frac{[F_i : F_1]}{2} \left(\frac{q^n - 1}{q^k - 1} + \frac{q^n - 1}{q^j - 1} \right). \tag{26}$$

For the tower $\mathcal{F}$ over the field $K = \mathbb{F}_\ell$, we combine Equation (26) with Corollary 3.2 and then we obtain for all $i \geqslant 2$,

$$\frac{N(F_i)}{g(F_i) - 1} \geqslant 2 \left(\frac{1}{q^j - 1} + \frac{1}{q^k - 1} \right)^{-1}.$$

Letting $i \to \infty$, this gives a lower bound for the limit $\lambda(\mathcal{F}) = \lim_{i \to \infty} N(F_i)/g(F_i)$,

$$\lambda(\mathcal{F}) \geqslant 2 \left(\frac{1}{q^j - 1} + \frac{1}{q^k - 1} \right)^{-1},$$

and thus proves Theorem 1.2.

So it remains to prove the Main Claim, which means: for every $i \geqslant 1$ and every place $\widetilde{P}$ of F_{i+1} lying above the place $[x_1 = 0]$, we have to estimate the different exponent $d(\widetilde{P}|[x_1 = 0])$.

The restriction of $\widetilde{P}$ to the rational subfield $K(x_{i+1})$ is either the place $[x_{i+1} = 0]$ or $[x_{i+1} = \infty]$, as follows from Figures 2, 3 and 4. In the case $[x_{i+1} = 0]$, the place $\widetilde{P}$ is a zero of all x_h with $1 \leqslant h \leqslant i + 1$, and we see from Figure 2 that $\widetilde{P}$ is unramified over $[x_1 = 0]$; hence we have $0 = d(\widetilde{P}|[x_1 = 0]) \leqslant b \cdot (e(\widetilde{P}|[x_1 = 0]) - 1)$ for every $b \in \mathbb{R}^+$.

The non-trivial case is when $\widetilde{P}$ is a pole of x_{i+1}. Then there exists a unique $m \in \{1, \ldots, i\}$ such that $\widetilde{P}$ is a zero of x_m and a pole of x_{m+1}. The situation is shown in Figure 7. The question marks indicate that one cannot read off the ramification index and different exponent from ramification data in the basic function field,
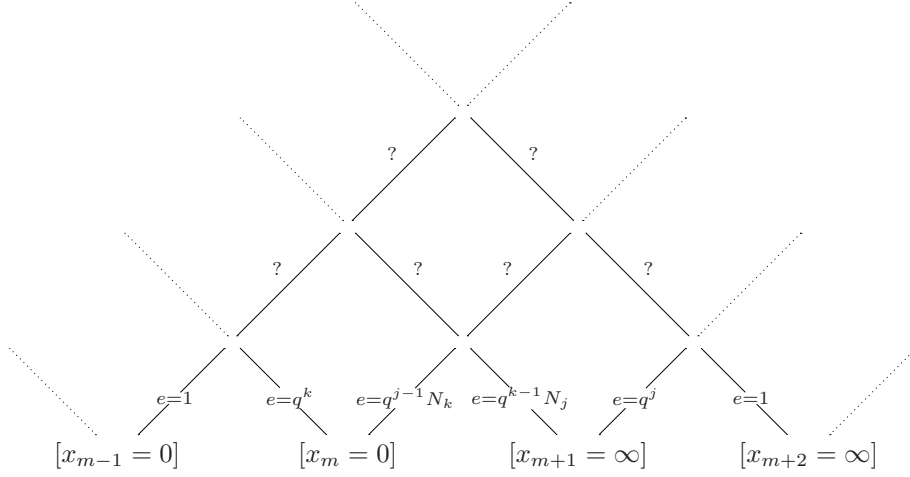
FIGURE 7. Ramification of $\tilde{P}$ over $[x_1 = 0]$: the non-trivial case

since both 'lower' ramifications are wild and therefore Abhyankar's lemma does not apply.

In order to analyze this situation, we introduce the 'u-subtower' of $\mathcal{F}$. Let $u_i \in K(x_i, x_{i+1})$ be the unique element which satisfies the conditions (see Proposition 2.2)

$$\mathrm{Tr}_k(u_i) + \alpha = \frac{x_{i+1}}{x_i^{q^k}} \quad \text{and} \quad \mathrm{Tr}_j(u_i) = -\frac{x_{i+1}^{q^j}}{x_i}.$$

We set $z_i := -x_i^{q^n - 1}$ and we then have for all $i \geqslant 1$ the equations

$$z_{i+1} = -x_{i+1}^{q^n - 1} = \frac{\mathrm{Tr}_j(u_{i+1})}{(\mathrm{Tr}_k(u_{i+1}) + \alpha)^{q^j}} = \frac{\mathrm{Tr}_j(u_i)^{q^k}}{\mathrm{Tr}_k(u_i) + \alpha}. \tag{27}$$

Equation (27) defines a subtower $\mathcal{E} = (E_1 \subseteq E_2 \subseteq \dots)$ of $\mathcal{F}$ (see Figure 8), where

$$E_i := K(u_1, u_2, \dots, u_i).$$

By Proposition 2.2 we know that $F_2 = K(x_1, x_2) = K(x_1, u_1)$, and it follows by induction that

$$F_{i+1} = E_i(x_1) \quad \text{for all } i \geqslant 1.$$

Let $\tilde{P}$ be a place of the field F_{i+1} as in Figure 7 (the 'non-trivial case'), and let P be the restriction of $\tilde{P}$ to the subfield E_i. The restrictions of P to the subfields $K(u_1), \dots, K(u_i)$ are

$$\begin{aligned}
&[u_s = \gamma_s] && \text{with } \gamma_s \in \Gamma \text{ for } 1 \leqslant s \leqslant m - 1, \\
&[u_m = \infty], && \text{and} \\
&[u_s = \delta_s] && \text{with } \delta_s \in \Delta \text{ for } m + 1 \leqslant s \leqslant i.
\end{aligned} \tag{28}$$
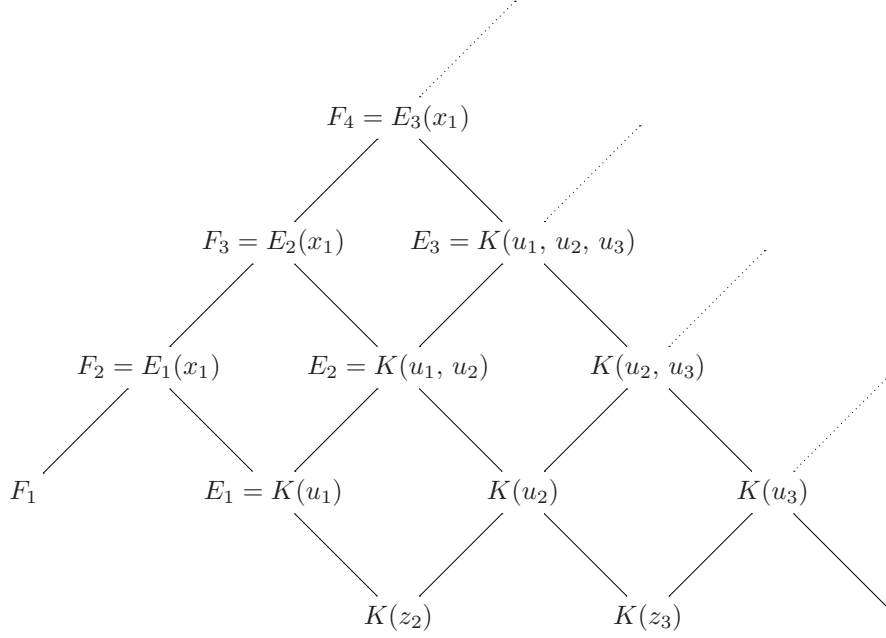
FIGURE 8. The subtower $\mathcal{E} = (E_1 \subseteq E_2 \subseteq \dots)$.

THE CASE $m = 1$.

We will see that this case already comprises most problems that occur in the general case. The situation is shown in Figure 9, where ramifications come from Figures 3 and 4.
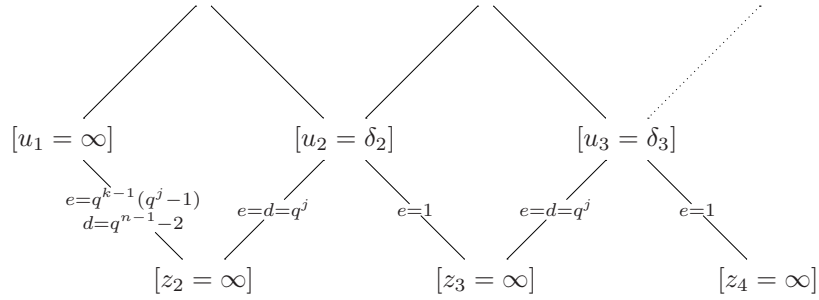
FIGURE 9. The case $m = 1$

Ramification indices and different exponents do not change under completion; we will therefore replace the fields F_s, E_s, $K(u_s)$ etc. by their completions $\widehat{F}_s$, $\widehat{E}_s$, $\widehat{K(u_s)}$ etc. (of course, completions are understood at the restrictions of $\widetilde{P}$ to the corresponding fields). As the field K is assumed to be algebraically closed, the ramification indices are then equal to the degrees of the corresponding field

extensions. To simplify notation, we set

$$u := u_1, \quad z := z_2, \quad H := \widehat{K(z)}, \quad \text{and} \quad E := \widehat{E}_1 = \widehat{K(u)} = H(u). \tag{29}$$

The next two propositions are of vital importance for the proof of the Main Claim.

Proposition 3.5. There exists an element $t \in E$ such that

$$t^{q^j - 1} = z^{-1}. \tag{30}$$

The extension $H(t)/H$ is cyclic of degree $[H(t) : H] = q^j - 1$, and the extension $E/H(t)$ is Galois of degree $[E : H(t)] = q^{k-1}$. The ramification indices and different exponents in the extensions $E \supseteq H(t) \supseteq H$ are as shown in Figure 10.

$$E = H(u)$$

galois of
degree q^{k-1}
$$e = q^{k-1}$$
$$d = 2(q^{k-1} - 1) = 2(e - 1)$$

$$H(t)$$

cyclic of
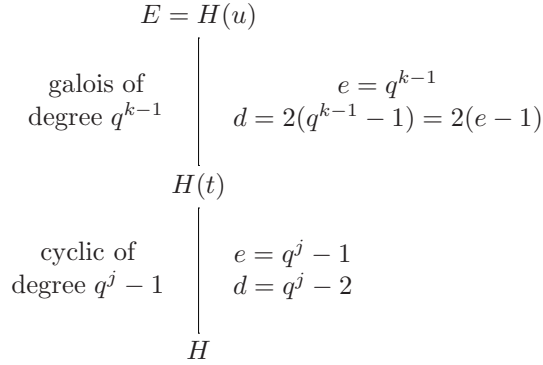degree $q^j - 1$
$$e = q^j - 1$$
$$d = q^j - 2$$

$$H$$

FIGURE 10. The intermediate field $H(t)$

Proof. Notations as in Equation (29). The extension E/H of degree $[E : H] = q^{k-1}(q^j - 1)$ is totally ramified, z^{-1} is a prime element of H and u^{-1} is a prime element of E. Hence we have

$$z^{-1} = \epsilon \cdot (u^{-1})^{q^{k-1}(q^j - 1)}$$

with a unit $\epsilon \in E$. As an easy consequence of Hensel's lemma, we can write ϵ as

$$\epsilon = \epsilon_0^{q^j - 1} \quad \text{with a unit } \epsilon_0 \in E.$$

Then the element $t := \epsilon_0 \cdot (u^{-1})^{q^{k-1}}$ satisfies the equation $t^{q^j - 1} = z^{-1}$.

It is clear that $H(t)/H$ is a cyclic extension of degree $q^j - 1$, and hence the degree of the field extension $E/H(t)$ is $[E : H(t)] = q^{k-1}$.

Next we show that $E/H(t)$ is Galois. From Equation (27) follows that u is a root of the polynomial

$$\varphi(T) := z^{-1} \cdot \mathrm{Tr}_j(T)^{q^k} - (\mathrm{Tr}_k(T) + \alpha) \in H[T].$$

Its reduction $\varphi^*(T)$ modulo the valuation ideal of H is the polynomial

$$\varphi^*(T) = -(\mathrm{Tr}_k(T) + \alpha) \in K[T].$$

We set $\eta_1(T) := \mathrm{Tr}_k(T) + \alpha$ and $\eta_2(T) := -1$, then Hensel's lemma gives a factorization

$$\varphi(T) = \varphi_1(T) \cdot \varphi_2(T) \quad \text{with } \varphi_1(T), \varphi_2(T) \in H[T],$$

$\varphi_1(T)$ is monic of degree q^{k-1} and with reduction $\varphi_1^*(T) = \mathrm{Tr}_k(T) + \alpha$. Again by Hensel's lemma, the polynomial $\varphi_1(T)$ splits into linear factors over H. As $u \notin H$ is a root of $\varphi(T)$, it follows that $\varphi_2(u) = 0$. The degree of the field extension $E = H(u)$ over H is

$$[E : H] = q^{n-1} - q^{k-1} = \deg \varphi_2(T),$$

and therefore the monic polynomial $z \cdot \varphi_2(T) \in H[T]$ is the minimal polynomial of u over H.

We can construct some other roots of $\varphi_2(T)$ in E as follows. By Hensel's lemma, the polynomial

$$\psi(T) := z^{-1} \cdot \mathrm{Tr}_j(T)^{q^k} - \mathrm{Tr}_k(T) \in H[T]$$

has q^{k-1} distinct roots $\Theta \in H$. For any such Θ we have

$$\varphi(u + \Theta) = z^{-1} \cdot \mathrm{Tr}_j(u + \Theta)^{q^k} - (\mathrm{Tr}_k(u + \Theta) + \alpha) = \varphi(u) + \psi(\Theta) = 0.$$

Since $u + \Theta \notin H$, we conclude that $u + \Theta$ is a root of $\varphi_2(T)$; hence we obtain an automorphism of the field E over H by setting $u \mapsto u + \Theta$. For $\Theta \neq 0$, this automorphism has order $p = \mathrm{char}(K)$. As $[H(t) : H] = q^j - 1$ is relatively prime to p, the restriction of this automorphism to $H(t)$ is the identity. We have thus constructed q^{k-1} distinct automorphisms of E over $H(t)$. This proves that the extension $E/H(t)$ is Galois, since its degree is $[E : H(t)] = q^{k-1}$.

The different exponent of E/H is $q^{n-1} - 2$, see Figure 9. Since $H(t)/H$ is tamely ramified with different exponent $q^j - 2$, one obtains easily that $E/H(t)$ has different exponent $2(q^{k-1} - 1)$, by transitivity of the different. □

Note that we are still considering the case $m = 1$ with completions at the corresponding places. We define now subfields $G_s \subseteq \widehat{E}_s$ (see Figure 11) by setting:

$$G_1 := H(t), \quad \text{and} \quad G_{s+1} := G_s(u_{s+1}) \text{ for } s \geqslant 1.$$

Ramification indices and different exponents in Figure 11 can be read off from Figures 9 and 10. From this it follows in particular that $\widehat{K(u_2)} = \widehat{K(z_3)}$, $\widehat{K(u_2, u_3)} = \widehat{K(u_3)} = \widehat{K(z_4)}$, etc.

Proposition 3.6. For all $s \geqslant 1$, the extension G_{s+1}/G_s is Galois of degree q^j. The ramification index of G_{s+1}/G_s is $e = q^j$, and the different exponent is $d = 2(q^j - 1) = 2(e - 1)$.

Proof. It is clear that $[G_{s+1} : G_s] = q^j$. From transitivity of the different, the different exponent of G_{s+1}/G_s is $d = 2(q^j - 1)$. It remains to prove that the extension G_{s+1}/G_s is Galois. For simplicity we write $v := u_{s+1}$, $w := z_{s+1}$ and $G := G_s$. Then $G_{s+1} = G(v)$.

Denote by $\mathcal{O}_G$ and $\mathfrak{m}_G$ the valuation ring of G and its maximal ideal. By Equation (27), the element v is a root of the polynomial

$$\Phi(T) := (\mathrm{Tr}_k(T) + \alpha)^{q^j} - w^{-1} \cdot \mathrm{Tr}_j(T) \in \mathcal{O}_G[T].$$
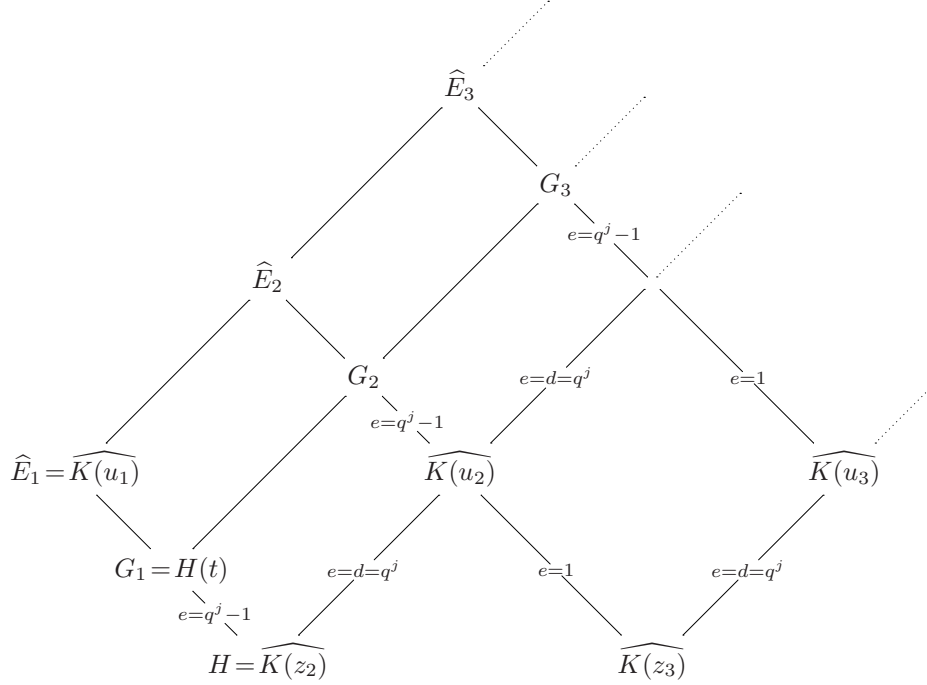
FIGURE 11. The subfields G_s

The reduction of $\Phi(T)$ modulo $\mathfrak{m}_G$ decomposes in $K[T]$ as follows:

$$\Phi^*(T) := (\operatorname{Tr}_k(T) + \alpha)^{q^j} = \prod_{\delta \in \Delta} \eta_\delta(T) \quad \text{with } \eta_\delta(T) = T^{q^j} - \delta^{q^j} \in K[T]. \qquad (31)$$

The polynomials $\eta_\delta(T)$ are relatively prime, for distinct $\delta \in \Delta$. By Hensel's lemma we can lift the decomposition of $\Phi^*(T)$ to a decomposition of $\Phi(T)$ as follows:

$$\Phi(T) = \prod_{\delta \in \Delta} \Phi_\delta(T),$$

with monic polynomials $\Phi_\delta(T) \in \mathcal{O}_G[T]$ of degree $\deg \Phi_\delta(T) = q^j$, and

$$\Phi_\delta^*(T) = T^{q^j} - \delta^{q^j} \quad \text{for all } \delta \in \Delta. \qquad (32)$$

As v is a root of $\Phi(T)$ and $[G(v) : G] = q^j$, we conclude that there is a unique $\epsilon \in \Delta$ such that

$$\Phi_\epsilon(T) \text{ is the minimal polynomial of } v \text{ over } G.$$

We will now show that the polynomial $\Phi_\epsilon(T)$ has q^j distinct roots in G_{s+1} and hence that the field extension G_{s+1}/G_s is Galois. To this end we consider

$$\chi(T) := \operatorname{Tr}_j(T) - w \cdot \operatorname{Tr}_k(T)^{q^j} \in G[T].$$

From Figure 11 we see that w has a pole of order $q^j - 1$ in G, and hence we can write

$$w = \left(\frac{1}{w_0}\right)^{q^j - 1} \quad \text{with some prime element } w_0 \in G.$$

Then

$$\chi(T) = \mathrm{Tr}_j(T) - \left(\frac{1}{w_0}\right)^{q^j - 1} \mathrm{Tr}_k(T)^{q^j} = w_0 \left[\frac{T}{w_0} - \left(\frac{T}{w_0}\right)^{q^j} + w_0 \cdot \Lambda\left(\frac{T}{w_0}\right)\right],$$

with $\Lambda(Z)$ a polynomial in the ring $\mathcal{O}_G[Z]$. Again by Hensel's lemma, there exist q^j distinct elements $\xi \in \mathcal{O}_G$ such that

$$\xi - \xi^{q^j} + w_0 \cdot \Lambda(\xi) = 0,$$

and for these elements we have $\chi(w_0\xi) = 0$. Now it follows that

$$\Phi(v + w_0\xi) = (\mathrm{Tr}_k(v + w_0\xi) + \alpha)^{q^j} - w^{-1}\mathrm{Tr}_j(v + w_0\xi) = \Phi(v) - w^{-1}\chi(w_0\xi) = 0 - 0 = 0.$$

For every $\delta \in \Delta\backslash\{\epsilon\}$ we have $\Phi_\delta^*(v + w_0\xi)^* = \Phi_\delta^*(v^*) = \epsilon^{q^j} - \delta^{q^j}$, and therefore $v + w_0\xi$ cannot be a root of the polynomial $\Phi_\delta(T)$. Hence the element $v + w_0\xi$ is a root of $\Phi_\epsilon(T)$, which is the minimal polynomial of v over G. $\qquad\square$

In the following we need the concept of weakly ramified extensions of valuations. For simplicity, we consider only the case of complete fields.

Definition 3.7. Let L be a field which is complete with respect to a discrete valuation and has an algebraically closed residue class field of characteristic $p > 0$. A finite separable extension L'/L is said to be weakly ramified if the following hold:

(i) There exists a chain of intermediate fields

$$L = L_0 \subseteq L_1 \subseteq L_2 \cdots \subseteq L_m = L'$$

such that all extensions L_{i+1}/L_i are Galois p-extensions.

(ii) The different exponent $d(L'|L)$ satisfies

$$d(L'|L) = 2(e(L'|L) - 1),$$

where $e(L'|L)$ denotes the ramification index of L'/L.

Proposition 3.8. Let L be a field, complete with respect to a discrete valuation, with an algebraically closed residue field of characteristic $p > 0$, and let L'/L be a finite separable extension.

(i) Let H be an intermediate field, $L \subseteq H \subseteq L'$. Then L'/L is weakly ramified if and only if both extensions H/L and L'/H are weakly ramified.

(ii) Assume that $L' = H_1 \cdot H_2$ is the composite field of two intermediate fields $L \subseteq H_1, H_2 \subseteq L'$. If both extensions H_1/L and H_2/L are weakly ramified, then also L'/L is weakly ramified.

Proof. This follows using techniques from [7]. $\qquad\square$

By Propositions 3.5, 3.6 and item (i) of Proposition 3.8, the extensions $\widehat{E}_1/G_1$ and G_s/G_1 are weakly ramified. We conclude from item (ii) of Proposition 3.8 that

$$\widehat{E}_s/\widehat{E}_1 \quad \text{is weakly ramified, for all } s \geqslant 1. \tag{33}$$

Now we can calculate the different exponent of a place $\widetilde{P}$ of F_{i+1} over $P_1 := [x_1 = 0]$ in the case $m = 1$ (see Figures 8 and 11). As before, the place P is the restriction of $\widetilde{P}$ to the field E_i, and we denote by P_2 the restriction of $\widetilde{P}$ to the field $F_2 = E_1(x_1)$. The situation is represented in Figure 12, where we set $e_0 := e(P_2|P_1)$ and $e_1 := e(P|[u_1 = \infty])$. By Equation (33), e_1 is a power of p, and $d(P|[u_1 = \infty]) = 2(e_1 - 1)$.
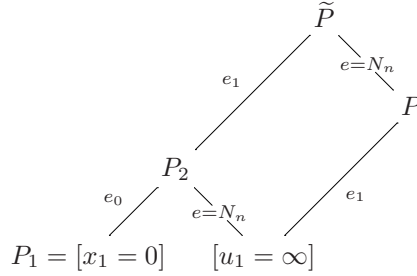

FIGURE 12. The place extension $\widetilde{P}|P_1$ in the case $m = 1$.

By Proposition 2.6 the place P_2 is tame over $[u_1 = \infty]$ with ramification index

$$e(P_2|[u_1 = \infty]) = \frac{q^n - 1}{q - 1}.$$

From transitivity we obtain

$$d(\widetilde{P}|[u_1 = \infty]) = e_1\left(\frac{q^n - 1}{q - 1} - 1\right) + d(\widetilde{P}|P_2) = \frac{q^n - 1}{q - 1} \cdot 2(e_1 - 1) + \left(\frac{q^n - 1}{q - 1} - 1\right);$$

hence

$$d(\widetilde{P}|P_2) = \left(\frac{q^n - 1}{q - 1} + 1\right)(e_1 - 1) = (N_n + 1)(e_1 - 1). \tag{34}$$

By Figure 4,

$$e_0 = e(P_2|P_1) = q^{j-1}N_k \quad \text{and} \quad d(P_2|P_1) = (q^{j-1} - 1)N_n + (e_0 - 1). \tag{35}$$

Combining Equations (34) and (35) one gets

$$d(\widetilde{P}|P_1) = e_1\left((q^{j-1} - 1)N_n + (e_0 - 1)\right) + (N_n + 1)(e_1 - 1)$$

$$= N_n(e_1 q^{j-1} - 1) + (e_0 e_1 - 1) = \left(\frac{N_n}{N_k} + 1\right)(e_0 e_1 - 1) + \frac{N_n}{N_k} - N_n$$

$$\leqslant \left(\frac{q^n - 1}{q^k - 1} + 1\right)(e(\tilde{P}|P_1) - 1).$$

This inequality shows the Main Claim in case $m = 1$; i.e., the place extension $\tilde{P}|P_1$ satisfies

$$d(\tilde{P}|P_1) \leqslant \left(\frac{q^n - 1}{q^k - 1} + 1 \right)(e(\tilde{P}|P_1) - 1) = b_0 \cdot (e(\tilde{P}|P_1) - 1).$$

It remains to prove the Main Claim for:

THE CASE $m \geqslant 2$.

Now we have a place $\widetilde{P}$ of the field F_{i+1} such that its restriction P to the field $E_i = K(u_1, \ldots, u_i)$ satisfies the condition in Equation (28) for some integer m, with $2 \leqslant m \leqslant i$. The restrictions of P to the rational subfields $K(u_1), \ldots, K(u_m)$ and $K(z_2), \ldots, K(z_m)$ are shown in Figure 13.
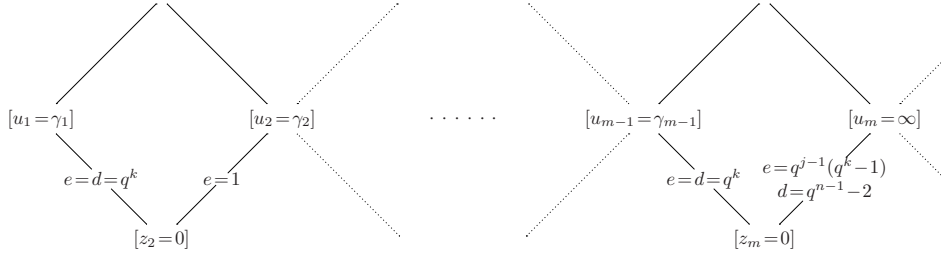

FIGURE 13. The case $m \geqslant 2$

There is a strong analogy between Figures 9 and 13 that interchanges the roles of j and k. In fact, after passing to the completions one proves that there is a field L_1 with $\widehat{K(z_m)} \subseteq L_1 \subseteq \widehat{K(u_m)}$ such that:

(i) $L_1/\widehat{K(z_m)}$ is cyclic with ramification index $e = q^k - 1$.
(ii) $\widehat{K(u_m)}/L_1$ is a weakly ramified p-extension.
(iii) The extension $L := \widehat{E}_{m-1} \cdot L_1$ is weakly ramified over L_1.

The proof is exactly as in the case of $m = 1$; we leave the details to the reader. Note that L_1 corresponds to the field G_1 in Figure 11. From the case of $m = 1$, we know that the extension $\widehat{G}/\widehat{K(u_m)}$ with $G = K(u_m, \ldots, u_i)$ is weakly ramified (see Equation (33)), and then it follows from Proposition 3.8 that also $\widehat{E}_i = \widehat{E}_m \cdot \widehat{G}$ is weakly ramified over L. From item (i) above we see that the extension $L/\widehat{E}_{m-1}$ has ramification index $e = q^k - 1$. The extensions $\widehat{E}_{m-1}/\widehat{E}_1$ and $\widehat{F}_2/\widehat{F}_1$ are unramified. Figure 14 represents the situation (in Figure 14, 'w.r.' means 'weakly ramified'). The degree of $M := L \cdot \widehat{F}_2$ over $\widehat{F}_2$ follows from Abhyankar's lemma.

Finally we consider the composite field $\widehat{F}_{i+1} = \widehat{E}_i \cdot \widehat{F}_2 = \widehat{E}_i(x_1)$ and determine ramification index and different exponent of $\widetilde{P}$ over $P_1 = [x_1 = 0]$. We have

$$e(\widetilde{P}|P_1) = \frac{q^k - 1}{q - 1} \cdot \widetilde{e}, \quad \text{with } \tilde{e} \text{ a power of } p.$$

Denoting by $\widetilde{d}$ the different of $\widehat{F}_{i+1}$ over M,

$$\widetilde{d} + \widetilde{e} \cdot (N_n - 1) = (N_n - 1) + N_n \cdot (2\widetilde{e} - 2), \quad \text{and hence } \widetilde{d} = (N_n + 1)(\widetilde{e} - 1).$$
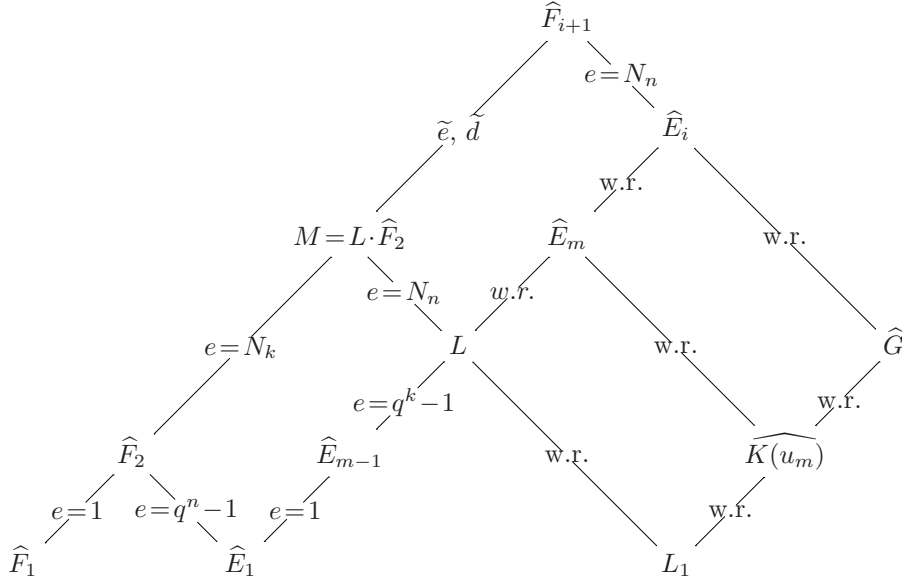
FIGURE 14. Ramification over $\widehat{F}_1$ in case $m \geqslant 2$

We finally obtain that

$$
\begin{aligned}
d(\widetilde{P}|P_1) &= \widetilde{d} + \widetilde{e} \cdot (N_k - 1) \\
&= \left(\frac{q^n - 1}{q^k - 1} + 1 \right)(e(\widetilde{P}|P_1) - 1) - \left(\frac{q^n - 1}{q - 1} - \frac{q^n - 1}{q^k - 1} \right) \leqslant b_0 \cdot (e(\widetilde{P}|P_1) - 1).
\end{aligned}
$$

This finishes the proof of the Main Claim and hence also the proof of Theorem 1.2. $\square$

Remark 3.9. The u-tower $\mathcal{E} = (E_1 \subseteq E_2 \subseteq \cdots)$ is recursively defined by (see Equation (27))

$$
\frac{\mathrm{Tr}_j(Y)}{(\mathrm{Tr}_k(Y) + \alpha)^{q^j}} = \frac{\mathrm{Tr}_j(X)^{q^k}}{\mathrm{Tr}_k(X) + \alpha}. \tag{36}
$$

This equation has 'separated variables'.

The x-tower $\mathcal{F} = (F_1 \subseteq F_2 \subseteq \cdots)$ is recursively defined by Equation (23), which does not have separated variables. Subtracting Equation (23) from its q-th power, one sees that the tower $\mathcal{F}$ also satisfies the recursive equation

$$
\frac{Y^{q^n} - Y}{Y^{q^j}} = \frac{X^{q^n} - X}{X^{q^n - q^k + 1}}. \tag{37}
$$

Equation (37) has separated variables but it is not irreducible. One can get from this equation a very simple proof of Corollary 3.2.

The z-tower $\mathcal{H} = (H_1 \subseteq H_2 \subseteq \cdots)$ with z_i as in Equation (27) and $H_i :=$ $K(z_1, \ldots, z_i)$ satisfies the recursion

$$\frac{(Y+1)^{N_n}}{Y^{N_j}} = \frac{(X+1)^{N_n}}{X^{q^k N_j}}, \tag{38}$$

which has separated variables and is reducible. Equation (38) can be deduced from Equation (37).

Since $\mathcal{H}$ is a subtower of $\mathcal{E}$ and $\mathcal{E}$ is a subtower of $\mathcal{F}$, we have (see [6])

$$\lambda(\mathcal{H}) \geqslant \lambda(\mathcal{E}) \geqslant \lambda(\mathcal{F}) \geqslant 2\left(\frac{1}{q^j - 1} + \frac{1}{q^k - 1}\right)^{-1}. \tag{39}$$

It would be interesting to have a direct proof for the limit $\lambda(\mathcal{H})$ just using Equation (38).

4. A Drinfeld Modular Motivation for the Equations

In this section we show that Equations (37) and (38) can be obtained using a Drinfeld modular construction. More precisely, we show that curves in the towers are related to one-dimensional varieties parametrizing certain classes of Drinfeld modules of characteristic $T - 1$ and rank $n \geqslant 2$ together with some varying additional structure. For definitions and results about Drinfeld modules, we refer to [14]. We will restrict to the case of Drinfeld $\mathbb{F}_q[T]$-modules of rank n and characteristic $T - 1$.

It is well known that Drinfeld modular curves which parametrize Drinfeld modules of rank two together with some level structure, have many $\mathbb{F}_{q^2}$-rational points after suitable reductions. These rational points correspond to supersingular Drinfeld modules. In fact, it was shown in [13] that curves obtained in this way are asymptotically optimal; i.e., they attain the Drinfeld–Vlăduţ bound. More generally, after reduction, the variety parametrizing Drinfeld modules of rank n (again with some additional structure) has points corresponding to supersingular Drinfeld modules, which were shown to be $\mathbb{F}_{q^n}$-rational in [12]. This variety however, has dimension $n - 1$. Hence we will consider one-dimensional subvarieties containing the supersingular points, to obtain curves with many $\mathbb{F}_{q^n}$-rational points. We will consider a one-dimensional sub-locus corresponding to particular Drinfeld modules (including all supers ingular ones, in order to get many rational points), together with particular isogenies leaving this sub-locus invariant (in order to get recursive equations).

More precisely, let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$. Let L be a field containing $\mathbb{F}_q$ together with a fixed $\mathbb{F}_q$-algebra homomorphism $\iota \colon A \to L$. The kernel of ι is called the characteristic of L. We will always assume that the characteristic is the ideal generated by $T - 1$. Further denote by τ the q-Frobenius map and let $L\{\tau\}$ be the ring of additive polynomials over L under operations of addition and composition (also called twisted polynomial ring or Ore ring). Given $f(\tau) = a_0 + a_1\tau + \cdots + a_n\tau^n \in L\{\tau\}$, we define $D(f) := a_0$. Note that the map $D \colon L\{\tau\} \to L$ is a homomorphism of $\mathbb{F}_q$-algebras.

A homomorphism of $\mathbb{F}_q$-algebras $\phi \colon A \to L\{\tau\}$ (where one usually writes ϕ_a for the image of $a \in A$ under ϕ) is called a Drinfeld A-module ϕ of characteristic $T - 1$

over L, if $D \circ \phi = \iota$ and if there exists $a \in A$ such that $\phi_a \neq \iota(a)$. It is determined by the additive polynomial ϕ_T. If $\phi_T = g_0 \tau^n + g_1 \tau^{n-1} + \cdots + g_{n-1}\tau + 1 \in L\{\tau\}$, with $g_i \in L$ and $g_0 \neq 0$, the Drinfeld module is said to have rank n. A Drinfeld module ϕ given by $\phi_T = g_0 \tau^n + g_1 \tau^{n-1} + \cdots + g_{n-1}\tau + 1$ is called supersingular (in characteristic $T - 1$) if $g_1 = \cdots = g_{n-1} = 0$. Note that this corresponds to the situation that the additive polynomial ϕ_{T-1} is purely inseparable.

For Drinfeld modules ϕ and ψ as above, an isogeny $\lambda \colon \phi \to \psi$ over L is an element $\lambda \in L\{\tau\}$ satisfying

$$\lambda \cdot \phi_a = \psi_a \cdot \lambda \quad \text{for all } a \in A. \tag{40}$$

We say that the kernel of the isogeny is annihilated by multiplication with $P(T) \in \mathbb{F}_q[T]$, if there exists $\mu \in L\{\tau\}$ such that

$$\mu \cdot \lambda = \phi_{P(T)}.$$

Over the algebraically closed field $\bar{L}$, Drinfeld modules ϕ and ψ are isomorphic, if they are related by an invertible isogeny; i.e., if there exists $\lambda \in \bar{L}^{\times}$ such that Equation (40) holds.

In analogy to normalized Drinfeld modules in [4], for $1 \leqslant j \leqslant n$, let $\mathfrak{D}_{n,j}$ be the set of rank n Drinfeld A-modules of characteristic $T - 1$ of the form $\phi_T = -\tau^n + g\tau^j + 1$. We will call such Drinfeld modules normalized. As before, we assume that $\gcd(n, j) = 1$ and write $k = n - j$. Note that $\mathfrak{D}_{n,j}$ contains the supersingular Drinfeld module ϕ with $\phi_T = -\tau^n + 1$. First we exhibit certain isogenies for $\phi \in \mathfrak{D}_{n,j}$ and show that the isogenous Drinfeld module is again in $\mathfrak{D}_{n,j}$:

Proposition 4.1. Let $\phi \in \mathfrak{D}_{n,j}$ be a Drinfeld module defined by $\phi_T = -\tau^n + g\tau^j + 1$ and let λ be an additive polynomial of the form $\lambda = \tau^k - a$. Then there exists a Drinfeld module ψ such that λ defines an isogeny from ϕ to ψ if and only if

$$\frac{1}{a} g^{q^k} - \frac{1}{a^{q^j}} g - a^{q^n - 1} + 1 = 0. \tag{41}$$

Moreover $\psi \in \mathfrak{D}_{n,j}$ and more precisely, $\psi_T = -\tau^n + h\tau^j + 1$ with

$$h = -a^{q^n} + a + g^{q^k}. \tag{42}$$

Proof. The existence of a Drinfeld module ψ such that λ defines an isogeny from ϕ to ψ, is equivalent to the existence of an additive polynomial $\psi_T = h_0 \tau^n + h_1 \tau^{n-1} + \cdots + h_{n-1}\tau + h_n$ such that $\lambda \cdot \phi_T = \psi_T \cdot \lambda$. Clearly one needs to choose $h_0 = -1$ and $h_n = 1$.

The equation $\lambda \cdot \phi = \psi \cdot \lambda$ implies that

$$-\tau^{n+k} + (a + g^{q^k})\tau^n - ag\tau^j + \tau^k - a = \sum_{i=k}^{n+k} h_{n-i+k}\tau^i - \sum_{i=0}^{n} h_{n-i} a^{q^i} \tau^i.$$

Consequently we have

$$(-a^{q^n} + a + g^{q^k})\tau^n - ag\tau^j = \sum_{i=k+1}^{n+k-1} h_{n-i+k}\tau^i - \sum_{i=1}^{n-1} h_{n-i} a^{q^i} \tau^i. \tag{43}$$

By comparing coefficients of τ^i in Equation (43) for $n + k - 1 \leqslant i \leqslant n + 1$, we see that $h_i = 0$ for all $1 \leqslant i < k$. By considering coefficients of τ^i in Equation (43) for $i \not\equiv n \pmod{k}$, we then conclude that $h_i = 0$ for all $i \not\equiv 0 \pmod{k}$. We are left to determine the coefficients of the form h_i, with $1 \leqslant i < n$ a multiple of k. Again by Equation (43) we conclude that for such i, $h_i = 0$ if $k < i < n$. This leaves two equations in the coefficient h_k, namely the ones in Equation (43) relating the coefficients of τ^n and τ^j:

$$-a^{q^n} + a + g^{q^k} = h_k \quad \text{and} \quad -ag = -h_k a^{q^j}.$$

The proposition now follows. $\qquad\square$

Now we determine all solutions of Equation (41):

Proposition 4.2. Let $X \in \bar{L}$ be such that $X^{q^k-1} = a$. All solutions of Equation (41) are given by

$$g = \frac{X^{q^n-1} + c}{X^{q^j-1}}, \quad \text{with } c \in \mathbb{F}_{q^k}. \tag{44}$$

The corresponding h in Equation (42) is given by

$$h = \frac{X^{q^n-1} + c}{X^{q^n-q^k}}. \tag{45}$$

Proof. Multiplying both sides of Equation (41) with X^{q^n-1} and using that $a = X^{q^k-1}$, we find that

$$-X^{(q^n-1)q^k} + X^{q^n-1} + X^{(q^j-1)q^k} g^{q^k} - X^{q^j-1} g = 0,$$

which can be rewritten as

$$(-X^{q^n-1} + gX^{q^j-1})^{q^k} - (-X^{q^n-1} + gX^{q^j-1}) = 0.$$

The possible solutions for g now follow. Inserting these solutions in Equation (42), the formula for h is obtained readily. $\qquad\square$

Note that in fact X corresponds to a choice of a nonzero element in the kernel of the isogeny $\lambda = \tau^k - a$. The kernel of λ is just $\mathbb{F}_{q^k} X$. Exactly in the case that $c = -1$, the element X can be chosen to be a T-torsion point of the Drinfeld module ϕ. We will assume from now on that this is the case. The equations relating g, h and X then simplify to

$$g = \frac{X^{q^n} - X}{X^{q^j}} \quad \text{and} \quad h = \frac{X^{q^n} - X}{X^{q^n-q^k+1}}. \tag{46}$$

Therefore we have obtained exactly the same correspondence as the one described in Equation (37). Through this correspondence, we are parametrizing normalized rank n Drinfeld modules together with an isogeny of the form $\lambda = \tau^k - a$ and a nonzero T-torsion point in its kernel.

In the particular case of $n = 2$ and $k = 1$, these are just normalized Drinfeld modules together with T-isogenies (together with a T-torsion point in their kernel) as studied by Elkies in [4]. For general n and k, not all of the kernel of λ will be

annihilated by multiplication with T anymore, but by multiplication with the polynomial $(T-1)^{N_k} - (-1)^k$ (which is obviously relatively prime to the characteristic $T-1$):

Proposition 4.3. Let ϕ and ψ be two Drinfeld modules given by $\phi_T = -\tau^n + g\tau^j + 1$ and $\psi_T = -\tau^n + h\tau^j + 1$. Further let $\lambda = \tau^k - X^{q^k-1}$ be an isogeny from ϕ to ψ. Then the kernel of λ is annihilated by the polynomial $P_k(T) = (T-1)^{N_k} - (-1)^k$.

Proof. Any additive polynomial of the form $\tau - (\alpha X)^{q-1}$ with $\alpha \in \mathbb{F}_{q^k}^{\times}$ is a right factor of $\tau^k - X^{q^k-1}$. In total this gives N_k distinct right factors, since $\#\{\alpha^{q-1} \colon \alpha \in \mathbb{F}_{q^k}^{\times}\} = N_k$. Clearly the kernel of such a right factor is contained in the kernel of $\tau^k - X^{q^k-1}$. This gives rise to $N_k(q-1) = q^k - 1$ nonzero elements of the kernel of $\tau^k - X^{q^k-1}$. Therefore the union of the kernels of the right factors $\tau - (\alpha X)^{q-1}$, with $\alpha \in \mathbb{F}_{q^k}^{\times}/\mathbb{F}_q^{\times}$, is equal to the kernel of $\tau^k - X^{q^k-1}$.

We claim that the kernel of $\tau - (\alpha X)^{q-1}$ is annihilated by $T - 1 + \alpha^{q^j-1}$. Indeed, $\phi_{T-1+\alpha^{q^j-1}} = -\tau^n + g\tau^j + \alpha^{q^j-1}$ can be written as $\mu(\tau - (\alpha X)^{q-1})$ for some additive polynomial μ if and only if $-(\alpha X)^{q^n-1} + g(\alpha X)^{q^j-1} + \alpha^{q^j-1} = 0$. This equality is satisfied, as can be seen by using Equation (46) and the fact that $\alpha \in \mathbb{F}_{q^k}^{\times}$.

Two right factors $\tau - (\alpha X)^{q-1}$ and $\tau - (\alpha' X)^{q-1}$ are equal if and only if $\alpha^{q-1} = \alpha'^{q-1}$. Therefore the proposition follows once we show that the product of $T - 1 + \alpha^{q^j-1}$ over all $\alpha \in \mathbb{F}_{q^k}^{\times}/\mathbb{F}_q^{\times}$ equals $(T-1)^{N_k} - (-1)^k$. This is the case, since

$$\prod_{\beta \in (\mathbb{F}_{q^k}^{\times})^{q-1}} (T - 1 + \beta^{N_j}) = \prod_{\beta \in (\mathbb{F}_{q^k}^{\times})^{q-1}} (T - 1 + \beta) = (-1)^k \prod_{\beta \in (\mathbb{F}_{q^k}^{\times})^{q-1}} (-T + 1 - \beta)$$

$$= (-1)^k ((-T+1)^{N_k} - 1) = (T-1)^{N_k} - (-1)^k.$$

In the first equality we used that since $\gcd(j, k) = 1$, the map from $(\mathbb{F}_{q^k}^{\times})^{q-1}$ to itself given by $\beta \mapsto \beta^{N_j}$ is a bijection. In the third equality we used that $(\mathbb{F}_{q^k}^{\times})^{q-1}$ consists of exactly all elements of $\mathbb{F}_{q^k}^{\times}$ of multiplicative order dividing N_k. $\qquad \square$

From the proof of Proposition 4.3 we also see that $P_k(T)$ is the lowest degree polynomial annihilating the kernel of $\lambda = \tau^k - X^{q^k-1}$. For $k = 1$, we have $P_1(T) = T$, so the kernel of the isogeny λ is annihilated by multiplication with T.

Alternatively, instead of studying normalized rank n Drinfeld modules, one can consider the corresponding $\bar{L}$-isomorphism classes. More precisely, we look at isomorphism classes of rank n Drinfeld modules ϕ with $\phi_T = g_0\tau^n + g_1\tau^{n-1} + \cdots + g_{n-1}\tau + 1$ such that

$$g_1 = \ldots = g_{j-1} = g_{j+1} = \ldots = g_{n-1} = 0.$$

Clearly every such class contains a normalized Drinfeld module, and two normalized Drinfeld modules $\phi, \phi' \in \mathfrak{D}_{n,j}$, with $\phi_T = -\tau^n + g\tau^j + 1$ and $\phi'_T = -\tau^n + g'\tau^j + 1$ are isomorphic over $\bar{L}$ if and only if $g' = g \cdot \lambda^{q^j-1}$ for some $\lambda \in \mathbb{F}_{q^n}^{\times}$.

Since $\gcd(n, j) = 1$, the image of the map $\lambda \mapsto \lambda^{q^j-1}$ is $(\mathbb{F}_{q^n}^{\times})^{q-1}$. We see that ϕ and ϕ' as above are isomorphic if and only if

$$g'^{N_n} = g^{N_n}.$$

We denote $J(\phi) = g^{N_n}$, since it plays the analogous role of the j-invariant for normalized Drinfeld modules (also compare with [22]). It is now easy to relate $J(\phi)$ and $J(\psi)$ for Drinfeld modules ϕ and ψ which are related by an isogeny of the form $\tau^k - X^{q^k-1}$. By Equation (46) we have

$$J(\phi) = g^{N_n} = \left(\frac{X^{q^n-1} - 1}{X^{q^j-1}} \right)^{N_n} = \frac{(X^{q^n-1} - 1)^{N_n}}{(X^{q^n-1})^{N_j}}$$

and similarly

$$J(\psi) = h^{N_n} = \frac{(X^{q^n-1} - 1)^{N_n}}{(X^{q^n-1})^{q^k N_j}}.$$

Letting $Z = -X^{q^n-1}$, we have

$$J(\phi) = (-1)^k \frac{(Z+1)^{N_n}}{Z^{N_j}}, \quad J(\psi) = (-1)^k \frac{(Z+1)^{N_n}}{Z^{q^k N_j}},$$

which is the same correspondence as the one described in Equation (38).

REFERENCES

[1] J. Bezerra, A. Garcia, and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. **589** (2005), 159–199. MR 2194682

[2] V. G. Drinfeld and S. G. Vlăduţ, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), no. 1, 68–69 (Russian). MR 695100. English translation: Functional Anal. Appl. **17** (1983), no. 1, 53–54.

[3] I. Duursma and K.-H. Mak, *On lower bounds for the Ihara constants $A(2)$ and $A(3)$*, Compos. Math. **149** (2013), no. 7, 1108–1128. MR 3078640

[4] N. D. Elkies, *Explicit towers of Drinfeld modular curves*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 189–198. MR 1905359

[5] A. García and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound*, Invent. Math. **121** (1995), no. 1, 211–222. MR 1345289

[6] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61** (1996), no. 2, 248–273. MR 1423052

[7] A. Garcia and H. Stichtenoth, *On the Galois closure of towers*, Recent trends in coding theory and its applications, AMS/IP Stud. Adv. Math., vol. 41, Amer. Math. Soc., Providence, RI, 2007, pp. 83–92. MR 2348945

[8] A. Garcia, H. Stichtenoth, and H.-G. Rück, *On tame towers over finite fields*, J. Reine Angew.   not cited? Math. **557** (2003), 53–80. MR 1978402

[9] G. van der Geer, *Curves over finite fields and codes*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 225–238. MR 1905363

[10] G. van der Geer and J. H. van Lint, *Introduction to coding theory and algebraic geometry*, DMV Seminar, vol. 12, Birkhäuser Verlag, Basel, 1988. MR 1015293

[11] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34** (2002), no. 3, 291–300. MR 1887701

[12] E.-U. Gekeler, *On finite Drinfeld modules*, J. Algebra **141** (1991), no. 1, 187–203. MR 1118323

[13] E.-U. Gekeler, *Invariants of some algebraic curves related to Drinfeld modular curves*, J. Number Theory **90** (2001), no. 1, 166–183. MR 1850880

[14] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 35, Springer-Verlag, Berlin, 1996. MR 1423131

[15] Y. Ihara, *Congruence relations and Shimūra curves*, Automorphic forms, representations and *L*-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 291–311. MR 546621

[16] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 721–724 (1982). MR 656048

[17] N. Jacobson, *Lectures in abstract algebra. Vol III: Theory of fields and Galois theory*, D. Van Nostrand Co., Inc., Princeton, N.J.-Toronto, Ont.-London-New York, 1964. MR 0172871

[18] W.-C. W. Li, *Upper and lower bounds for $A(q)$*, Recent trends in coding theory and its applications, AMS/IP Stud. Adv. Math., vol. 41, Amer. Math. Soc., Providence, RI, 2007, pp. 15–23. MR 2348941

[19] W.-C. W. Li and H. Maharaj, *Coverings of curves with asymptotically many rational points*, J. Number Theory **96** (2002), no. 2, 232–256. MR 1932454

[20] Yu. I. Manin, *What is the maximum number of points on a curve over $\mathbb{F}_2$?*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 715–720 (1982). MR 656047

[21] H. Niederreiter and C. Xing, *Rational points on curves over finite fields: theory and applications*, London Mathematical Society Lecture Note Series, vol. 285, Cambridge University Press, Cambridge, 2001. MR 1837382

[22] I. Y. Potemine, *Minimal terminal Q-factorial models of Drinfeld coarse moduli schemes*, Math. Phys. Anal. Geom. **1** (1998), no. 2, 171–191. MR 1690499

[23] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), no. 9, 397–402. MR 703906

[24] H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR 2464941

[25] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28. MR 705893

[26] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Fundamentals of computation theory (Cottbus, 1985), Lecture Notes in Comput. Sci., vol. 199, Springer, Berlin, 1985, pp. 503–511. MR 821267

A.B.: Sabanci University, MDBF, 34956 Tuzla, İstanbul, Turkey
E-mail address: bassa@sabanciuniv.edu

P.B.: Technical University of Denmark, Department of Applied Mathematics and Computer Science, Matematiktorvet, Building 303B, DK-2800, Lyngby, Denmark
E-mail address: p.beelen@mat.dtu.dk

A.G.: Instituto Nacional de Matemática Pura e Aplicada, IMPA, Estrada Dona Castorina 110, 22460-320, Rio de Janeiro, RJ, Brazil
E-mail address: garcia@impa.br

H.S.: Sabanci University, MDBF, 34956 Tuzla, İstanbul, Turkey
E-mail address: henning@sabanciuniv.edu