Galois Towers over Non-prime Finite Fields

Alp Bassa*, Peter Beelen†, Arnaldo Garcia‡ and Henning Stichtenoth§

Abstract

In this paper we construct Galois towers with good asymptotic properties over any non-prime finite field $\mathbb{F}_\ell$; i.e., we construct sequences of function fields $\mathcal{N} = (N_1 \subset N_2 \subset \cdots)$ over $\mathbb{F}_\ell$ of increasing genus, such that all the extensions N_i/N_1 are Galois extensions and the number of rational places of these function fields grows linearly with the genus. The limits of the towers satisfy the same lower bounds as the best currently known lower bounds for the Ihara constant for non-prime finite fields. Towers with these properties are important for applications in various fields including coding theory and cryptography.

1 Introduction

The question of how many rational points a curve over a finite field can have is not only interesting from a purely number-theoretical perspective, but also has become an important question for applications in computer science, coding theory, cryptography and other areas of discrete mathematics. Curves with many rational points have been successfully applied in the construction of codes, sequences, hash functions, secret sharing and multiparty computation schemes and other combinatorial objects. One of the landmark results in this direction is the work of Tsfasman–Vladut–Zink [10], where sequences of curves of increasing genus with good asymptotic behavior and a construction of codes from curves with many points due to Goppa are combined to construct codes better than the Gilbert–Varshamov bound. This was a big surprise, as the Gilbert–Varshamov bound had resisted any attempt of improvement for many years.

Although several such sequences of curves with the same good asymptotic behavior exist, some turn out to be more suitable for applications than others. Recent work has shown that various additional properties enjoyed by the curves in some of these sequences turn out to be very beneficial for applications. These additional properties satisfied by the curves in the sequence reflect themselves in further features or better parameters of the objects constructed from them. For instance, Stichtenoth [9] showed how sequences of curves with many points together with the additional property that each of them is a Galois covering of the first one can be used to construct self-dual and transitive codes attaining the Tsfasman–Vladut–Zink bound. Also, in [4] Cascudo, Cramer and Xing showed how, in the construction of arithmetic secret sharing schemes from sequences of curves with many rational points, a better control on the d-torsion in the class group of the curves involved leads to better bounds for the constructed schemes (see also [1]).

With these and similar applications in mind, we construct in this paper over any non-prime finite field $\mathbb{F}_\ell$ sequences of curves with increasing genus and many rational points, such that each

*Alp Bassa is supported by Tübitak Proj. No. 112T233.

†Peter Beelen gratefully acknowledges the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No.11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography.

‡Arnaldo Garcia is partially supported by CNPq (Brazil).

§Henning Stichtenoth is supported by Tübitak Proj. No. 111T234.

curve in the sequence is a Galois covering of the first one. Instead of the geometric language of curves over finite fields, we will use the equivalent language of algebraic function fields with finite constant fields. So, more precisely, over any non-prime finite field $\mathbb{F}_\ell$ we will construct sequences of function fields $\mathcal{N} = (N_1 \subset N_2 \subset \cdots)$ such that for each $i > 0$ the extension N_i/N_1 is a Galois extension and moreover $\mathcal{N}$ has a large limit. For a more precise statement, see Theorem 1 below.

Let $\mathcal{G} = (G_1 \subset G_2 \subset \cdots)$ be a sequence of functions fields with full constant field $\mathbb{F}_\ell$. Such a sequence is called a tower over $\mathbb{F}_\ell$. Let $f(x,y) \in \mathbb{F}_\ell[x,y]$. We say that the tower $\mathcal{G}$ satisfies the equation $f(x,y) = 0$ recursively, if for all $i \geq 1$ there exists $x_i \in G_i$ such that

- x_1 is transcendental over $\mathbb{F}_\ell$,
- $G_i = G_{i-1}(x_i)$ and $f(x_{i-1}, x_i) = 0$ for $i > 1$.

Such a tower is simply called a recursive tower. The main ingredients for this paper are the recursive towers that were introduced by the authors in [2].

For a function field F over $\mathbb{F}_\ell$ we denote by $N(F)$ the number of rational paces and by $g(F)$ its genus. Let q be a power of a prime p, $1 \leq k < n$ be integers such that $\gcd(k, n-k) = 1$, and let $\ell = q^n$. In [2] we introduced and studied the towers $\mathcal{F} = (F_1 \subset F_2 \subset \cdots)$ over $\mathbb{F}_\ell$ satisfying the recursive equation

$$\frac{y}{x^{q^k}} + \frac{y^q}{x^{q^{k+1}}} + \cdots + \frac{y^{q^{n-k-1}}}{x^{q^{n-1}}} + \frac{y^{q^{n-k}}}{x} + \frac{y^{q^{n-k+1}}}{x^q} + \cdots + \frac{y^{q^{n-1}}}{x^{q^{k-1}}} = 1. \tag{1}$$

We showed that the limit

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

of this tower satisfies

$$\lambda(\mathcal{F}) \geq 2\left(\frac{1}{q^k - 1} + \frac{1}{q^{n-k} - 1}\right)^{-1}. \tag{2}$$

Consider a tower $\mathcal{G} = (G_1 \subset G_2 \subset \cdots)$ over $\mathbb{F}_\ell$. Assume that for all $i \geq 1$ the extensions G_{i+1}/G_i are separable (hence so are the extensions G_i/G_1). Let $\tilde{G}_i$ be the Galois closure of the extension G_i/G_1 and assume that $\mathbb{F}_\ell$ is algebraically closed in all $\tilde{G}_i$. The tower $\tilde{\mathcal{G}} = (\tilde{G}_1 \subset \tilde{G}_2 \subset \cdots)$ is called the Galois closure of $\mathcal{G}$.

In this paper we investigate the Galois closure of the tower $\mathcal{F}$ and of some of its subtowers introduced in [2]. We investigate the splitting and ramification behavior of places in these towers, study the Galois groups of the extensions and show that each of these Galois towers has a limit satisfying Inequality (2). Along the way, we also show that there exists a finite extension E/F_1 such that each step in the composite tower $E\mathcal{F} = (EF_1 \subset EF_2 \subset \cdots)$ is Galois with an elementary abelian p-group as Galois group. We collect the main results of this paper in the following theorem:

Theorem 1 *Let q be a prime power. For any integer $n > 1$ and $1 \leq k < n$ with $\gcd(k, n-k) = 1$ there exists a tower $\mathcal{N} = (N_1 \subset N_2 \subset \cdots)$ over $\mathbb{F}_\ell$, where $\ell = q^n$, such that*

i) $N_1 = \mathbb{F}_\ell(z_1)$ is a rational function field.

ii) For each $i \geq 2$, the extension N_i/N_1 is a Galois extension having as Galois group an extension of a subgroup of $\mathrm{GL}_{n-1}(\mathbb{F}_q)$ by a p-group. The extension N_i/N_2 is a p-extension.

iii) The place $[z_1 = -1]$ of N_1 splits completely in $\mathcal{N}$; i.e., it splits completely in each extension N_i/N_1.

iv) The only places of N_1 which are ramified in $\mathcal{N}$ are $P_0 := [z_1 = 0]$ and $P_\infty := [z_1 = \infty]$, and they are weakly ramified (i.e., their second ramification groups are trivial).

v) For each $i > 1$, the extension N_i/N_2 is 2-bounded; more precisely, for any place P of N_2 the ramification index $e(P)$ and different exponent $d(P)$ of P in the extension N_i/N_2 satisfy

$$d(P) = 2(e(P) - 1).$$

vi) Let $e_i(P_0)$ and $e_i(P_\infty)$ denote the ramification indices in the extension N_i/N_1 of the places P_0 and P_∞ respectively and assume that $i > 1$. We have

$$e_i(P_0) = (q^k - 1)q^{(i-1)(n-k)-k}p^{\epsilon_1(i)}$$

and

$$e_i(P_\infty) = (q^{n-k} - 1)q^{(i-1)(n-k)}p^{\epsilon_2(i)},$$

with $\epsilon_1(i), \epsilon_2(i) \geq 0$.

vii) The limit of the tower satisfies

$$\lambda(\mathcal{N}) \geq 2\left(\frac{1}{q^k - 1} + \frac{1}{q^{n-k} - 1}\right)^{-1}.$$

2 Preliminaries

In this section we establish some preliminaries and recall some notations and results from [2].

Throughout the rest of the paper, q will be a power of a prime p and $\ell = q^n$ for some $n \geq 2$. Let E/F be a Galois extension of function fields over $\mathbb{F}_\ell$. Let P be a place of F and Q a place of E lying over P. We say that $Q|P$ is weakly ramified, if $G_2(Q|P) = \{e\}$, where $G_2(Q|P)$ denotes the second ramification group of $Q|P$. The Galois extension E/F is said to be weakly ramified, if for all places P of F and all places Q lying above P, $Q|P$ is weakly ramified. A weakly ramified p-extension E/F is 2-bounded. For such an extension, for every place P of F and every place Q above P we have $d(Q|P) = 2 \cdot (e(Q|P) - 1)$.

For convenience we define for any positive integer i the *trace polynomial*

$$\mathrm{Tr}_i(x) = x + x^q + x^{q^2} + \cdots + x^{q^{i-1}}$$

The trace polynomials $\mathrm{Tr}_i(x)$ are examples of q-additive polynomials. The following lemma will be useful later on:

Lemma 2 *Let i and j be positive integers.*

i) We have

$$\mathrm{Tr}_i(\mathrm{Tr}_j(x)) = \mathrm{Tr}_j(\mathrm{Tr}_i(x)).$$

More generally, any two q-additive polynomials with coefficients in $\mathbb{F}_q$ commute.

ii) Setting $r = \gcd(i, j)$, for any field $L \supset \mathbb{F}_q$ we have

$$L(\mathrm{Tr}_i(x), \mathrm{Tr}_j(x)) = L(\mathrm{Tr}_r(x)) \subseteq L(x).$$

In particular, if $\gcd(i, j) = 1$, then $L(\mathrm{Tr}_i(x), \mathrm{Tr}_j(x)) = L(x)$.

Proof. The first part follows by a direct computation. For the second part we assume w.l.o.g. that $i > j$ (the case $i = j$ is trivial). Then

$$\mathrm{Tr}_i(x) = \mathrm{Tr}_{i-j}(x) + (\mathrm{Tr}_j(x))^{q^{i-j}},$$

so

$$L(\mathrm{Tr}_i(x), \mathrm{Tr}_j(x)) = L(\mathrm{Tr}_j(x), \mathrm{Tr}_{i-j}(x)).$$

The claim then follows from the properties of the Euclidean Algorithm. ■

The second claim of the lemma is equivalent to saying that $\mathrm{Tr}_r(x)$ can be expressed in terms of $\mathrm{Tr}_i(x)$ and $\mathrm{Tr}_j(x)$. This can be shown more explicitly: Let a and b be positive integers such that $ai - bj = r$ (note that such a and b always exist). Then $\mathrm{Tr}_{ai}(x) - \mathrm{Tr}_{bj}(x)^{q^r} = \mathrm{Tr}_r(x)$, which implies that

$$\sum_{\alpha=0}^{a-1} \mathrm{Tr}_i(x)^{q^{\alpha i}} - \left(\sum_{\beta=0}^{b-1} \mathrm{Tr}_j(x)^{q^{\beta j}}\right)^{q^r} = \mathrm{Tr}_r(x). \tag{3}$$

Now let $0 < k < n$ with $\gcd(n, k) = 1$ be given. Let a, b be non-negative integers such that

$$a \cdot k - b \cdot (n - k) = 1. \tag{4}$$

Suppose x and y satisfy Equation (1) and let

$$R := \frac{y}{x^{q^k}} \qquad \text{and} \qquad S := \frac{y^{q^{n-k}}}{x}.$$

The quantities R and S occur in Equation (1):

$$\underbrace{\frac{y}{x^{q^k}}}_{R} + \frac{y^q}{x^{q^{k+1}}} + \cdots + \underbrace{\frac{y^{q^{n-k-1}}}{x^{q^{n-1}}}}_{R^{q^{n-k-1}}} + \underbrace{\frac{y^{q^{n-k}}}{x}}_{S} + \frac{y^{q^{n-k+1}}}{x^q} + \cdots + \underbrace{\frac{y^{q^{n-1}}}{x^{q^{k-1}}}}_{S^{q^{k-1}}} = 1.$$

And therefore we obtain

$$\mathrm{Tr}_{n-k}(R) + \mathrm{Tr}_k(S) = 1. \tag{5}$$

Proposition 3 *The function field $\mathbb{F}_\ell(R, S)$ is a rational function field. More precisely, letting*

$$u := \sum_{\alpha=0}^{a-1} R^{q^{\alpha k}} + \left(\sum_{\beta=0}^{b-1} S^{q^{\beta(n-k)}}\right)^q,$$

we have $R = \mathrm{Tr}_k(u) - b$, $S = -\mathrm{Tr}_{n-k}(u) + a$ and hence $\mathbb{F}_\ell(R, S) = \mathbb{F}_\ell(u)$.

Proof. We have

$$\begin{aligned}
\mathrm{Tr}_k(u) &= \sum_{\alpha=0}^{a-1} \mathrm{Tr}_k(R)^{q^{\alpha k}} + \left(\sum_{\beta=0}^{b-1} \mathrm{Tr}_k(S)^{q^{\beta(n-k)}}\right)^q \\
&= \sum_{\alpha=0}^{a-1} \mathrm{Tr}_k(R)^{q^{\alpha k}} + \left(\sum_{\beta=0}^{b-1} (1 - \mathrm{Tr}_{n-k}(R))^{q^{\beta(n-k)}}\right)^q && \text{by Equation (5)} \\
&= \mathrm{Tr}_{ak}(R) - \mathrm{Tr}_{b(n-k)}(R)^q + b \\
&= R + b. && \text{by Equation (4)}
\end{aligned}$$

Similarly $\mathrm{Tr}_{n-k}(u) = -S + a$. It follows that $\mathbb{F}_\ell(R, S) = \mathbb{F}_\ell(u)$. ■

From the above it is clear how to express u explicitly in terms of x and y. Note that

$$y^{q^n-1} = \frac{S^{q^k}}{R} = -\frac{\mathrm{Tr}_{n-k}(u)^{q^k} - a}{\mathrm{Tr}_k(u) - b} \text{ and } x^{q^n-1} = \frac{S}{R^{q^{n-k}}} = -\frac{\mathrm{Tr}_{n-k}(u) - a}{\mathrm{Tr}_k(u)^{q^{n-k}} - b}. \tag{6}$$

It was shown in [2, Lemma 2.9] that $\mathbb{F}_\ell(x^{q^n-1}, y^{q^n-1}) = \mathbb{F}_\ell(u)$. Therefore, one can express u not only as a rational expression in x and y, but also in x^{q^n-1} and y^{q^n-1}, say

$$u = \phi(x^{q^n-1}, y^{q^n-1}).$$

Now let $\mathcal{F} = (F_i)_{i>0}$ be a tower over $\mathbb{F}_\ell$, where $F_1 = \mathbb{F}_\ell(x_1)$ is a rational function field and for all $i > 1$, there exist $x_i \in F_i$ such that $F_i = F_{i-1}(x_i)$ with

$$\frac{x_i}{x_{i-1}^{q^k}} + \frac{x_i^q}{x_{i-1}^{q^{k+1}}} + \cdots + \frac{x_i^{q^{n-k-1}}}{x_{i-1}^{q^{n-1}}} + \frac{x_i^{q^{n-k}}}{x_{i-1}} + \cdots + \frac{x_i^{q^{n-1}}}{x_{i-1}^{q^{k-1}}} = 1. \tag{7}$$

Thus $\mathcal{F}$ satisfies the recursion given by Equation (1).

Defining $u_i := \phi(x_i^{q^n-1}, x_{i+1}^{q^n-1})$ and $z_i := -x_i^{q^n-1}$, we see from Equation (6) that

$$z_i = -x_i^{q^n-1} = \frac{\mathrm{Tr}_{n-k}(u_i) - a}{\mathrm{Tr}_k(u_i)^{q^{n-k}} - b} = \frac{\mathrm{Tr}_{n-k}(u_{i-1})^{q^k} - a}{\mathrm{Tr}_k(u_{i-1}) - b}. \tag{8}$$

Consider the subtowers $\mathcal{E} = (E_i)_{i>0}$ and $\mathcal{H} = (H_i)_{i>0}$ of $\mathcal{F}$ where $E_i = \mathbb{F}_\ell(u_1, \ldots, u_i) = \mathbb{F}_\ell(z_1, \ldots, z_{i+1})$ and $H_i = \mathbb{F}_\ell(z_1, \ldots, z_i)$. Note that for $i > 0$ we have $E_i = H_{i+1}$. See Figure 1 for a graphical overview of the fields occurring in $\mathcal{F}$, $\mathcal{E}$ and $\mathcal{H}$. From Equation (8) we see that the tower $\mathcal{E}$ satisfies a recursive equation. In [2, Equation (38)] we gave a recursive equation satisfied by the tower $\mathcal{H}$.

Remark 4 *It was shown in [2] that $E_i(x_1) = F_{i+1}$. This means that the tower $\mathcal{F}$ can be seen as the composite of the tower $\mathcal{H}$ and the field F_1.*

Remark 5 *Let $\mathcal{F}$ be a tower satisfying a recursion $f(x, y) = 0$. Define the dual polynomial $\hat{f}(x, y) := f(y, x)$. A tower $\hat{\mathcal{F}}$ satisfying the recursion $\hat{f}(x, y) = 0$ is called a dual tower of $\mathcal{F}$.*

Let $\hat{\mathcal{E}}$ be a dual tower of the tower $\mathcal{E}$ defined above. The towers $\mathcal{E}$ and $\hat{\mathcal{E}}$ have very similar behavior. Equation (8) *implies that the tower $\hat{\mathcal{E}}$ satisfies the recursive equation*

$$\frac{\mathrm{Tr}_k(u_r) - b}{\mathrm{Tr}_{n-k}(u_r)^{q^k} - a} = \frac{\mathrm{Tr}_k(u_{r-1})^{q^{n-k}} - b}{\mathrm{Tr}_{n-k}(u_{r-1}) - a}. \tag{9}$$

This equation is obtained from Equation (8) *by interchanging both k with $n - k$ and a with b.*

Remark 6 *If $\gcd(n-k, p) = 1$, we can choose $a \equiv 0 \pmod p$ in Equation* (4)*. The corresponding choice of b will satisfy $b \cdot (n - k) \equiv -1 \pmod p$. Equation* (8) *then gets the form*

$$\frac{\mathrm{Tr}_{n-k}(u_{i+1})}{\mathrm{Tr}_k(u_{i+1})^{q^{n-k}} + \alpha} = \frac{\mathrm{Tr}_{n-k}(u_i)^{q^k}}{\mathrm{Tr}_k(u_i) + \alpha},$$

with $\alpha := (n - k)^{-1} \in \mathbb{F}_p$. In this form the subtower $\mathcal{E} \subset \mathcal{F}$ appeared in [2].

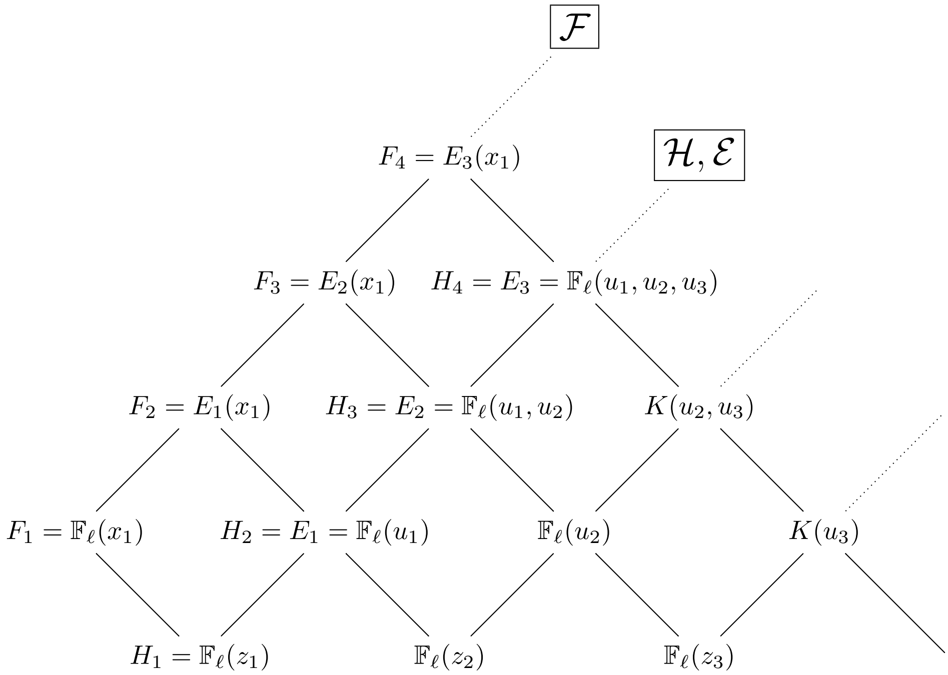

Figure 1: The towers $\mathcal{F} = (F_i)_{i>0}$, $\mathcal{E} = (E_i)_{i>0}$ and $\mathcal{H} = (H_i)_{i>0}$.

Next we collect some facts about the tower $\mathcal{H}$.

Proposition 7 *The place $[z_1 = -1]$ of H_1 splits completely in the tower $\mathcal{H}$.*

Proof. This follows from [2, Corollary 3.2] and the fact that $z_1 = -x_1^{q^n-1}$. ∎

While investigating ramification, we replace the constant field $\mathbb{F}_\ell$ by its algebraic closure $K := \overline{\mathbb{F}}_\ell$. Moreover, for completions, since the place at which we complete is clear from the context, we do not specify the place explicitly in the notation. A place and the corresponding maximal ideal of the valuation ring in the completion are by slight abuse of notation denoted by the same symbol.

Proposition 8 *Let $i > 0$ and Q be a place of H_i, let $P = Q \cap H_1$ be its restriction to H_1. If $Q|P$ is ramified, then one of the following holds:*

1. *There exists $1 \leq m < i$ such that $z_1(Q) = \cdots = z_m(Q) = 0$ and $z_{m+1}(Q) = \cdots = z_i(Q) = \infty$. Completing various fields at Q and its restrictions, there is an intermediate field L of the extension $\widehat{H_i}/\widehat{H_1}$ such that $L/\widehat{H_1}$ is cyclic of degree $q^k - 1$ and $\widehat{H_i}/L$ can be divided into 2-bounded elementary abelian p-extensions.*

2. *One has $z_1(Q) = \infty$ and $e(Q|P) = q^{(n-k)(i-1)}$. Let $t_0 \neq 0$ be chosen such that $\mathrm{Tr}_{n-k}(t_0)^{q^k} - z_1 \mathrm{Tr}_k(t_0) = 0$ and choose a place P' of $K(t_0)$ such that $t_0(P') = \infty$. Suppose that there exists a place Q' of $H_i(t_0)$ lying above both P' and Q.*

   (a) *Completing various fields at Q' and its restrictions, there is an intermediate field G_1 of the extension $\widehat{K(t_0)}/\widehat{K(z_1)}$ such that $G_1/\widehat{K(z_1)}$ is cyclic of degree $q^{n-k} - 1$ and*

$\widehat{K(t_0)}/G_1$ *is a 2-bounded elementary abelian p-extension.*

(b) Letting G_j be $G_1\widehat{H_j}$ for $1 \leq j \leq i$, the extensions G_{j+1}/G_j are 2-bounded elementary abelian p-extensions for $1 \leq j < i$.

Proof. The fact that the ramification locus of the tower $\mathcal{H}$ only consists of the zero and the pole of z_1 is a direct consequence of [2, Proposition 2.6]. The first part about the zero of z_1 follows from [2, Propositions 3.5, 3.6 and Figure 14]. The second part can be shown very similarly to these propositions. The only difference with [2, Propositions 3.5 and 3.6] is that the element t_0 satisfies the equation $\mathrm{Tr}_{n-k}(t_0)^{q^k} - z_1\mathrm{Tr}_k(t_0) = 0$, while the element u mentioned there satisfies $\mathrm{Tr}_{n-k}(u)^{q^k} - z_2\mathrm{Tr}_k(u) = a - bz_2$. ■

3 The Galois closure of the tower $\mathcal{H}$

Let us denote by N_i the Galois closure of the extension H_i/H_1. It follows easily that $\mathbb{F}_\ell$ is algebraically closed in all N_i, since there exists a rational place of H_1 splitting completely in the extension H_i/H_1 (see [7, Proposition 14]). By definition, the tower $\mathcal{N} = \tilde{\mathcal{H}} = (N_1 \subset N_2 \subset \dots)$ is the Galois closure of $\mathcal{H}$ (over $N_1 = H_1$). It is a Galois tower; i.e., each extension N_i/N_1 is a Galois extension. We will now study the limit of $\mathcal{N}$ and show that it satisfies Inequality (2).

The field N_i is obtained by taking the composite of several conjugates $\sigma(H_i)$ of H_i, with σ an element of the absolute Galois group of H_1. Since the ramification behavior in the extension $\sigma(H_i)/H_1$ is similar to that of H_i/H_1, the analysis of the tower $\mathcal{H}$ in [2] as described in Proposition 8 will be very useful. We start by studying the Galois closure of the extension H_2/H_1. We define the polynomials

$$f(T) := -z_1^{-1}\mathrm{Tr}_{n-k}(T) + \mathrm{Tr}_k(T)^{q^{n-k}} \tag{10}$$

and

$$g(T) := \mathrm{Tr}_{n-k}(T)^{q^k} - z_1\mathrm{Tr}_k(T). \tag{11}$$

Proposition 9 *The Galois closure of H_2/H_1 is equal to the composite of H_2 and the splitting field of $f(T)$ over H_1.*

Proof. The Galois closure of H_2/H_1 is obtained by adjoining to H_2 all roots of the polynomial $\mathrm{Tr}_{n-k}(T) - z_1\mathrm{Tr}_k(T)^{q^{n-k}} - a + bz_1$, or equivalently, all roots of the polynomial $f(T) + az_1^{-1} - b$. However, the differences of two roots u, v of $f(T) + az_1^{-1} - b$ are exactly the roots of $f(T)$. ■

The polynomial $g(T)$ plays the same role for a dual tower of $\mathcal{H}$ as the polynomial $f(T)$ does for $\mathcal{H}$. We will show in Proposition 12 that the splitting fields of $f(T)$ and $g(T)$ are the same, which is a fact we will use later. To show this we need the following result (see [8, Theorem 1.7.11]):

Proposition 10 *Let F be a field containing $\mathbb{F}_q$ and $h(T) = \sum_{i=0}^{t} a_i T^{q^i} \in F[T]$ be a q-additive polynomial with $a_0 \neq 0$ and $a_t \neq 0$. Define $h^{\mathrm{ad}}(T) := \sum_{i=0}^{t} a_i^{q^{t-i}} T^{q^{t-i}}$. Then the roots of $h(T)$ and $h^{\mathrm{ad}}(T)$ generate the same extension of F.*

A direct consequence of this proposition is that the extension of $\mathbb{F}_q(z_1)$ generated by the roots of $f(T)$, is the same as the extension of $\mathbb{F}_q(z_1)$ generated by the roots of

$$(z_1 f)^{\mathrm{ad}}(T) = -(T^{q^{n-1}} + \dots + T^{q^k}) + z_1^{q^{k-1}} T^{q^{k-1}} + \dots + z_1^q T^q + z_1 T.$$

To relate the roots of $f(T)$ with those of $g(T)$, we will use the following lemma:

Lemma 11 *Let t be a root of $g(T)$, then $\mathrm{Tr}_k(t)$ is a root of $(z_1 f)^{\mathrm{ad}}(T)$.*

Proof. Since $g(t) = 0$, we have $\mathrm{Tr}_{n-k}(t)^{q^k} = z_1 \mathrm{Tr}_k(t)$. Applying Tr_k and using Lemma 2, we obtain

$$\mathrm{Tr}_{n-k}(\mathrm{Tr}_k(t))^{q^k} = \mathrm{Tr}_k(z_1 \mathrm{Tr}_k(t)).$$

This proves that $\mathrm{Tr}_k(t)$ is a root of $(z_1 f)^{\mathrm{ad}}(T)$. ■

Proposition 12 *The splitting fields of the polynomials $f(T)$ and $g(T)$ over H_1 are the same.*

Proof. Using Proposition 10 we are done once we show that the roots of $g(T)$ and $(z_1 f)^{\mathrm{ad}}(T)$ generate the same extension. We denote by V, respectively W, the $\mathbb{F}_q$-vector space consisting of the q^{n-1} roots of $g(T)$, respectively of $(z_1 f)^{\mathrm{ad}}(T)$. Lemma 11 gives rise to an $\mathbb{F}_q$-linear map ψ from V to W defined by $\psi(t) = \mathrm{Tr}_k(t)$. The proposition follows if we show that the map ψ has trivial kernel. Suppose therefore that $\mathrm{Tr}_k(t) = 0$. Since $g(t) = 0$ as well, one obtains that $\mathrm{Tr}_{n-k}(t) = 0$. Using Equations (3) and (4), we see that $t = 0$. ■

Remark 13 *As an immediate consequence of Proposition 9 and Proposition 12 we see that all roots of $f(T)$ and $g(T)$ are contained in N_i for $i \geq 2$.*

These facts will be used to determine the ramification behavior in the tower $\mathcal{N}$. Let P be a place of H_1 ramified in N_i/H_1. Since the sets of places of H_1 that ramify in N_i/H_1 and H_i/H_1 agree, P is either the pole or the zero of z_1 by Proposition 8. Let $\tilde{Q}$ be a place of N_i lying above such a place P. We have the following proposition about the ramification of $\tilde{Q}|P$:

Proposition 14 *Completing N_i at $\tilde{Q}$, there exists an intermediate field L of $\widehat{N_i}/\widehat{N_1}$ such that the extension $L/\widehat{N_1}$ is cyclic and the extension $\widehat{N_i}/L$ is a 2-bounded p-extension. If P is the zero of z_1, then $[L : \widehat{N_1}] = q^k - 1$. If P is the pole of z_1, we have $[L : \widehat{N_1}] = q^{n-k} - 1$.*

Proof. Denote by $Q_1, \ldots, Q_s$ be the restrictions of $\tilde{Q}$ to the various conjugates $\sigma_1(H_i), \ldots, \sigma_s(H_i)$ of H_i. We will consider the two cases $z_1(P) = 0$ and $z_1(P) = \infty$ separately.

Case i) $z_1(P) = 0$:
From the first part of Proposition 8 we see that after completion at $\tilde{Q}$, the extensions $\widehat{\sigma_j(H_i)}/\widehat{H_1}$ all can be divided into a cyclic part of degree $q^k - 1$ and steps of 2-bounded elementary abelian p-extensions. Taking composites we see (using Abhyankar's lemma and [7, Proposition 12]) that there exists a field $L \subset \widehat{N_i}$ such that the extension $L/\widehat{H_1}$ is cyclic of degree $q^k - 1$ and such that the extension $\widehat{N_i}/L$ can be divided into 2-bounded elementary abelian p-extensions.

Case ii) $z_1(P) = \infty$:
Let t_0 be a nonzero root of $g(T)$. By Remark 13 the element t_0 is contained in N_2 and hence in N_i. Let P' be a place of $H_1(t_0)$ lying above P such that $t_0(P') = \infty$ and $\tilde{R}$ a place of N_i lying above P'. We denote the restrictions of $\tilde{R}$ to the conjugates $\sigma_1(H_i), \ldots, \sigma_s(H_i)$ of H_i by $R_1, \ldots, R_s$ and the restrictions to $\sigma_1(H_i(t_0)), \ldots, \sigma_s(H_i(t_0))$ by $R'_1, \ldots, R'_s$. The second part of Proposition 8 implies that after completion at $\tilde{R}$, the extensions $\sigma_j(\widehat{H_i(t_0)})/\widehat{H_1}$ all can be divided into a cyclic part of degree $q^{n-k} - 1$ and steps of 2-bounded elementary abelian p-extensions. Again, using Abhyankar's lemma and [7, Proposition 12], we obtain the desired result for the place $\tilde{R}$. Since N_i/H_1 is a Galois extension and $\tilde{Q}$ and $\tilde{R}$ lie above the same place P of H_1, the same holds for $\tilde{Q}$. ■

Proposition 15 *Let $e_i(P_0)$ and $e_i(P_\infty)$ denote the ramification indices in the extension N_i/N_1 of the places P_0 and P_∞ respectively. Then for $i > 1$ we have*

$$e_i(P_0) = (q^k - 1)q^{(i-1)(n-k)-k}p^{\epsilon_1(i)}$$

and

$$e_i(P_\infty) = (q^{n-k} - 1)q^{(i-1)(n-k)}p^{\epsilon_2(i)}$$

with $\epsilon_1(i), \epsilon_2(i) \geq 0$.

Proof. We first consider the case of the place P_0. We will give a lower bound for the ramification by estimating the highest ramification index among all places of H_i lying over P_0. Since N_i/H_1 is a Galois extension, the ramification index $e(\tilde{Q}|P_0)$ does not depend on the choice of the place $\tilde{Q}$ of N_i lying over P_0. Without loss of generality we may therefore assume that $z_2(\tilde{Q}) = \infty$.

Let Q be the restriction of $\tilde{Q}$ to H_i and extend the constant field to $K := \overline{\mathbb{F}_\ell}$. We will use the notation from [2], especially the notation occurring in Figures 9 and 11 there. There the fields KH_i were completed at Q and an intermediate field G_1 of $\widehat{KH_2}/\widehat{K(z_2)}$ was introduced such that the extension $G_1/\widehat{K(z_2)}$ is cyclic of degree $q^{n-k}-1$, while the extension $\widehat{KH_2}/G_1$ is a 2-bounded Galois p-extension. Finally the field $G_i = G_1\widehat{KH_i}$ was defined.

Now let us denote by Q_2 the restriction of Q to $\widehat{KH_2}$. We obtain from [2, Figures 9 and 11] that

$$e(Q|P_0) = e(Q|Q_2)e(Q_2|P_0) = e(Q|Q_2)q^{n-k-1}(q^k - 1).$$

Further denote the restrictions of Q to G_i by S_i. Also by [2, Figures 9 and 11] we have $e(S_i|S_1) = q^{(i-2)(n-k)}$ and $e(Q_2|S_1) = q^{k-1}$. Since

$$e(Q|Q_2)q^{k-1} = e(Q|Q_2)e(Q_2|S_1) = e(Q|S_1) = e(Q|S_i)e(S_i|S_1) = e(Q|S_i)q^{(i-2)(n-k)},$$

and the extensions $\widehat{KH_2}/G_1$ and G_i/G_1 are 2-bounded Galois p-extensions, we obtain that $e(Q|Q_2)$ is the product of $q^{(i-2)(n-k)-k+1}$ with a power of the characteristic p. Combining the above, we see that $e(Q|P_0)$ is a power of p times $(q^k - 1)q^{(i-1)(n-k)-k}$. This proves first part of the proposition.

For the place P_∞, we see from Proposition 14 that $(q^{n-k}-1)|e_i(P_\infty)$. On the other hand, since any place of H_i lying above P_∞ has ramification index $(q^{n-k})^{i-1}$, we have $q^{(n-k)\cdot(i-1)}|e_i(P_\infty)$. Hence $(q^{n-k} - 1) \cdot q^{(n-k)(i-1)}$ divides $e_i(P_\infty)$. ∎

Remark 16 *Note that by Proposition 14 the extension N_i/H_1 is weakly ramified.*

Proposition 17 *We have*

$$\frac{g(N_i) - 1}{[N_i : N_1]} \leq \frac{1}{2} \cdot \left(\frac{1}{q^k - 1} + \frac{1}{q^{n-k} - 1} \right).$$

Proof. Denote by P_0 (respectively P_∞) the zero (respectively pole) of z_1 in H_1. We will use the Riemann-Hurwitz formula to estimate the genus of N_i. Since only the pole and zero of z_1 ramify in the extension N_i/H_1, we only need to estimate the different of these places in the extension. Let $\tilde{Q}$ be a place of N_i lying above P_0. After completing denote by S the restriction of $\tilde{Q}$ to the intermediate field L from Proposition 14. We obtain that

$$e(\tilde{Q}|P_0) = e(\tilde{Q}|S)e(S|P_0) = e(\tilde{Q}|S)(q^k - 1)$$

and

$$d(\tilde{Q}|P_0) = e(\tilde{Q}|S)d(S|P_0) + d(\tilde{Q}|S) = e(\tilde{Q}|S)(q^k - 2) + 2e(\tilde{Q}|S) - 2 = q^k e(\tilde{Q}|S) - 2.$$

Similarly for a place $\tilde{Q}$ above P_∞ we find

$$e(\tilde{Q}|P_\infty) = e(\tilde{Q}|S)(q^{n-k} - 1)$$

and

$$d(\tilde{Q}|P_\infty) = e(\tilde{Q}|S)(q^{n-k} - 2) + 2e(\tilde{Q}|S) - 2 = q^{n-k}e(\tilde{Q}|S) - 2.$$

We see that

$$\frac{d(\tilde{Q}|P_0)}{e(\tilde{Q}|P_0)} \leq 1 + \frac{1}{q^k - 1} \tag{12}$$

and

$$\frac{d(\tilde{Q}|P_\infty)}{e(\tilde{Q}|P_\infty)} \leq 1 + \frac{1}{q^{n-k} - 1}. \tag{13}$$

Using Equations (12) and (13) together with the Riemann-Hurwitz genus formula and the fundamental equality for the extension N_i/H_1, the result follows. ■

We immediately obtain the following:

Corollary 18 *The limit of the tower $\mathcal{N}$ satisfies*

$$\lambda(\mathcal{N}) \geq 2\left(\frac{1}{q^k - 1} + \frac{1}{q^{n-k} - 1}\right)^{-1}.$$

Proof. By Proposition 7, the place $[z_1 = -1]$ of H_1 splits completely in the tower $\mathcal{H}$ and hence also in the tower $\mathcal{N}$. This together with Proposition 17 implies the result. ■

At this point we have proved all statements of Theorem 1, except ii).

Remark 19 *Estimates for the limits of the Galois closures $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{F}}$ of the towers $\mathcal{E}$ and $\mathcal{F}$ can easily be derived from the above. The lower bound given in Corollary 18 holds for all of them. More precisely, the tower $\tilde{\mathcal{E}}$ is a subtower of $\mathcal{N}$, since the Galois closure is now taken over $E_1 = H_2$. Therefore $\lambda(\tilde{\mathcal{E}}) \geq \lambda(\mathcal{N})$. Lifting the tower $\mathcal{N}$ by adjoining the element x_1, gives a Galois tower over F_1. By a direct computation, the limit of this lift is easily seen to satisfy the same lower bound as that given for $\lambda(\mathcal{N})$ in Corollary 18. Since $\tilde{\mathcal{F}}$ is a subtower of this lifted tower, its limit also satisfies the same lower bound.*

4 A recursive tower with Galois steps

In [5] and [3], recursive towers over quadratic and cubic finite fields were introduced, where every step is Galois. In this section we obtain an analogous result over any non-prime finite field. More precisely, we construct a recursive subtower $(H_2' \subset H_3' \subset \cdots)$ of the tower $\mathcal{N}$ such that for any $i > 1$ the extension H_{i+1}'/H_i' is a Galois extension with elementary abelian p-group as Galois group and such that each ramification in H_{i+1}'/H_i' is 2-bounded.

Starting with the recursive tower $\mathcal{H} = (H_1 \subset H_2 \subset H_3 \subset \cdots)$ as defined in Section 2 we will introduce an extension field M/H_1 such that the composite tower $\mathcal{H}' = (H_1 \subset H_2' \subset H_3' \subset \cdots)$ with $H_i' = M \cdot H_i$ has Galois steps and its limit satisfies Inequality (2).

Recall that for $i > 0$ we have

$$z_i = \frac{\mathrm{Tr}_{n-k}(u_i) - a}{\mathrm{Tr}_k(u_i)^{q^{n-k}} - b} = \frac{\mathrm{Tr}_{n-k}(u_{i-1})^{q^k} - a}{\mathrm{Tr}_k(u_{i-1}) - b}.$$

Hence u_i is a root of the polynomial

$$\mathrm{Tr}_{n-k}(T) - z_i \cdot \mathrm{Tr}_k(T)^{q^{n-k}} - a + z_i \cdot b \in \mathbb{F}_\ell(z_i)[T]. \tag{14}$$

The extension $\mathbb{F}_\ell(u_i)/\mathbb{F}_\ell(z_i)$ is not Galois, but by Proposition 9, the Galois closure of $\mathbb{F}_\ell(u_i)/\mathbb{F}_\ell(z_i)$ can be obtained by adjoining to $\mathbb{F}_\ell(u_i)$ all roots of the polynomial

$$\begin{aligned} f_i(T) &:= -z_i^{-1}\mathrm{Tr}_{n-k}(T) + \mathrm{Tr}_k(T)^{q^{n-k}} \\ &= \mathrm{Tr}_n(T) - (1 + z_i^{-1})\mathrm{Tr}_{n-k}(T) \\ &= \mathrm{Tr}_n(T) - \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i) - a}\mathrm{Tr}_{n-k}(T). \end{aligned} \tag{15}$$

Similarly, to obtain the Galois closure of the extension $\mathbb{F}_\ell(u_{i+1})/\mathbb{F}_\ell(z_{i+1})$, we need to adjoin all roots of

$$\begin{aligned} f_{i+1}(T) &= \mathrm{Tr}_n(T) - (1 + z_{i+1}^{-1})\mathrm{Tr}_{n-k}(T) \\ &= \mathrm{Tr}_n(T) - \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i)^{q^k} - a}\mathrm{Tr}_{n-k}(T). \end{aligned} \tag{16}$$

We will show that for each root of $f_i(T)$ we get (using u_i) a root of the polynomial $f_{i+1}(T)$ and this will give a one-to-one correspondence between roots of $f_i(T)$ and $f_{i+1}(T)$. This implies that by adjoining all roots of $f_i(T)$ to a field containing u_i, we get all roots of $f_{i+1}(T)$. Hence inductively, we obtain that by lifting the tower $\mathcal{H}$ by adjoining all roots of $f_1(T)$, we get a tower with Galois steps. First we need a preparatory lemma:

Lemma 20 *Assume that s_i is a root of $f_i(T)$, i.e., assume that*

$$\mathrm{Tr}_n(s_i) = \mathrm{Tr}_{n-k}(s_i) \cdot \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i) - a}.$$

Then we have

$$\left(\frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b}\right)^{q^{n-k}} = \frac{\mathrm{Tr}_{n-k}(s_i)}{\mathrm{Tr}_{n-k}(u_i) - a} \tag{17}$$

and

$$\mathrm{Tr}_{n-k}(s_i)^{q^k} = \mathrm{Tr}_{n-k}(s_i) \cdot \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i) - a} - \mathrm{Tr}_k(s_i). \tag{18}$$

Proof. Since s_i is a root of $f_i(T)$, we have

$$\begin{aligned} \mathrm{Tr}_k(s_i)^{q^{n-k}} &= \mathrm{Tr}_{n-k}(s_i) \cdot \left(\frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i) - a} - 1\right) \\ &= \mathrm{Tr}_{n-k}(s_i) \cdot \frac{\mathrm{Tr}_k(u_i)^{q^{n-k}} - b}{\mathrm{Tr}_{n-k}(u_i) - a}. \end{aligned}$$

This implies Equation (17). Equation (18) follows, since

$$\mathrm{Tr}_k(s_i) + \mathrm{Tr}_{n-k}(s_i)^{q^k} = \mathrm{Tr}_n(s_i) = \mathrm{Tr}_{n-k}(s_i) \cdot \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i) - a}.$$

■

Lemma 21 (Shifting lemma) *If s_i is a root of $f_i(T)$, then*

$$s_{i+1} := \left(\frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b}\right)^q - \left(\frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b}\right) \in \mathbb{F}_\ell(u_i, s_i)$$

is a root of $f_{i+1}(T)$.

Proof.

$$\begin{aligned}
\mathrm{Tr}_n(s_{i+1}) &= \left(\frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b}\right)^{q^n} - \left(\frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b}\right) \\
&= \left(\frac{\mathrm{Tr}_{n-k}(s_i)}{\mathrm{Tr}_{n-k}(u_i) - a}\right)^{q^k} - \frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b} && \text{by Equation (17)} \\
&= \frac{\mathrm{Tr}_{n-k}(s_i) \cdot \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i) - a} - \mathrm{Tr}_k(s_i)}{\mathrm{Tr}_{n-k}(u_i)^{q^k} - a} - \frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b} && \text{by Equation (18)} \\
&= \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i)^{q^k} - a} \cdot \left[\frac{\mathrm{Tr}_{n-k}(s_i)}{\mathrm{Tr}_{n-k}(u_i) - a} - \frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b}\right] \\
&= \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i)^{q^k} - a} \cdot \left[\left(\frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b}\right)^{q^{n-k}} - \frac{\mathrm{Tr}_k(s_i)}{\mathrm{Tr}_k(u_i) - b}\right] && \text{by Equation (17)} \\
&= \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i)^{q^k} - a} \cdot \mathrm{Tr}_{n-k}(s_{i+1}).
\end{aligned}$$

Now we see from Equation (16) that

$$f_{i+1}(s_{i+1}) = \mathrm{Tr}_n(s_{i+1}) - \frac{\mathrm{Tr}_n(u_i) - (a+b)}{\mathrm{Tr}_{n-k}(u_i)^{q^k} - a} \cdot \mathrm{Tr}_{n-k}(s_{i+1}) = 0.$$

■

We have now established that each root of $f_i(T)$ together with u_i generates a root of $f_{i+1}(T)$. Let V_i (respectively V_{i+1}) be the set of roots of $f_i(T)$ (respectively $f_{i+1}(T)$). Since $f_i(T)$ and $f_{i+1}(T)$ are separable and q-additive, V_i and V_{i+1} are $(n-1)$-dimensional $\mathbb{F}_q$-vector spaces. By Lemma 21,

$$\begin{aligned}
\varphi : V_i &\to V_{i+1} \\
s &\mapsto \left(\frac{\mathrm{Tr}_k(s)}{\mathrm{Tr}_k(u_i) - b}\right)^q - \left(\frac{\mathrm{Tr}_k(s)}{\mathrm{Tr}_k(u_i) - b}\right)
\end{aligned}$$

is a map from V_i to V_{i+1}. Because φ is q-additive in s, it is in fact an $\mathbb{F}_q$-vector space homomorphism. In fact, it will turn out that φ is a bijection.

Lemma 22 *The map $\varphi : V_i \to V_{i+1}$ defined above is a bijection.*

Proof. It is sufficient to show that $\ker(\varphi) = \{0\}$. Let $s \in V_i$, i.e., $f_i(s) = 0$. If

$$\varphi(s) = \left(\frac{\mathrm{Tr}_k(s)}{\mathrm{Tr}_k(u_i) - b}\right)^q - \left(\frac{\mathrm{Tr}_k(s)}{\mathrm{Tr}_k(u_i) - b}\right) = 0,$$

then $\mathrm{Tr}_k(s)/(\mathrm{Tr}_k(u_i) - b) \in \mathbb{F}_q$, implying that there exists $\alpha \in \mathbb{F}_q$ such that

$$\mathrm{Tr}_k(s) = \alpha(\mathrm{Tr}_k(u_i) - b). \tag{19}$$

By Equation (17), we then have

$$\frac{\mathrm{Tr}_{n-k}(s)}{\mathrm{Tr}_{n-k}(u_i) - a} = \left(\frac{\mathrm{Tr}_k(s)}{\mathrm{Tr}_k(u_i) - b}\right)^{q^{n-k}} = \alpha^{q^{n-k}} = \alpha,$$

so

$$\mathrm{Tr}_{n-k}(s) = \alpha(\mathrm{Tr}_{n-k}(u_i) - a). \tag{20}$$

Equations (19) and (20) imply that

$$\mathrm{Tr}_{n-k}(\mathrm{Tr}_k(s)) = \alpha \mathrm{Tr}_{n-k}(\mathrm{Tr}_k(u_i) - b) = \alpha \mathrm{Tr}_{n-k}(\mathrm{Tr}_k(u_i)) - \alpha \cdot b \cdot (n-k)$$

and

$$\mathrm{Tr}_k(\mathrm{Tr}_{n-k}(s)) = \alpha \mathrm{Tr}_k(\mathrm{Tr}_{n-k}(u_i) - a) = \alpha \mathrm{Tr}_k(\mathrm{Tr}_{n-k}(u_i)) - \alpha \cdot a \cdot k.$$

Using the above and Lemma 2 we obtain

$$\begin{aligned} 0 &= \mathrm{Tr}_{n-k}(\mathrm{Tr}_k(s)) - \mathrm{Tr}_k(\mathrm{Tr}_{n-k}(s)) \\ &= \alpha\left(\mathrm{Tr}_{n-k}(\mathrm{Tr}_k(u_i)) - \mathrm{Tr}_k(\mathrm{Tr}_{n-k}(u_i)) + a \cdot k - b \cdot (n-k)\right) \\ &= \alpha(a \cdot k - b \cdot (n-k)) = \alpha. \end{aligned}$$

In the last step we used Equation (4). Equations (19) and (20) now imply that $\mathrm{Tr}_{n-k}(s) = 0$ and $\mathrm{Tr}_k(s) = 0$. Using Equation (3) we conclude that $s = 0$. ∎

By the shifting lemma (Lemma 21) and Lemma 22 all roots of $f_i(T)$ together with u_i generate all roots of $f_{i+1}(T)$. Similarly all roots of $f_{i+1}(T)$ together with u_{i+1} generate all roots of $f_{i+2}(T)$, etc. So, lifting the tower $\mathcal{H}$ by the splitting field of $f_1(T)$ gives a tower with Galois steps (see also Proposition 9). More formally, denote by M be the splitting field of $f_1(T)$ over H_1 and define $H'_i = M \cdot H_i$ for $i \geq 2$. Then we consider the tower $\mathcal{H}' = (H_1 \subset H'_2 \subset H'_3 \subset \cdots)$. Note that by Remark 13, the tower $\mathcal{H}'$ is a subtower of $\mathcal{N}$ and moreover $N_2 = H'_2$. Note also that all roots of $f_i(T)$ belong to H'_i.

Proposition 23 *1. All steps in the tower $\mathcal{H}'$ are Galois.*

2. The Galois group of the extension H'_2/H_1 is an extension by an elementary abelian p-group of a subgroup of $\mathrm{GL}_{n-1}(\mathbb{F}_q)$.

3. For each $i > 1$, the extension H'_{i+1}/H'_i is an elementary abelian p-extension.

Proof. By Proposition 9 the field $H'_2 = M \cdot H_2$ is a Galois extension of H_1. The extension M/H_1, being the splitting field of the q-additive polynomial $f(T)$ of degree q^{n-1}, is Galois with Galois group a subgroup of $\mathrm{GL}_{n-1}(\mathbb{F}_q)$. Since $H_2 = H_1(u_1)$, u_1 is a root of $f(T) + az_1^{-1} - b$ and M contains all roots of the additive polynomial $f(T)$, the Galois group of H'_2/M is an elementary abelian p-group. This proves the second part of the proposition. Similarly, since $H'_{i+1} = H'_i(u_i)$, u_i is a root of $f_i(T) + az_i^{-1} - b$ and H'_i contains all roots of $f_i(T)$, the extension H'_{i+1}/H'_i for each $i > 1$ is Galois with an elementary abelian p-group as Galois group. ∎

Remark 24 *Note that the tower $(H'_2 \subset H'_3 \subset \cdots)$ is a recursive tower whose steps are 2-bounded elementary abelian p-extensions (starting at a non-rational function field). Let $E := M(x_1)$. The composite $E \cdot \mathcal{F} = (E \cdot F_1 \subset E \cdot F_2 \subset \cdots)$ is then also a tower whose steps are weakly ramified elementary abelian p-extensions. Since both towers are subtowers of $\mathcal{N}$, the bound from Corollary 18 applies.*

Remark 25 *The very same reasoning applies to a dual tower, by replacing k and b by $n-k$ and a, respectively. So a modified version of the shifting lemma and of Proposition 23 apply in the dual direction.*

The splitting fields over H_1 of the polynomials $f_1(T) = f(T)$ and $g(T)$ from Equations (10) and (11) are the same. Combining this with Lemma 21 and Remark 25, we see that after adjoining the roots of $f(T)$ to $\mathbb{F}_\ell(z_1)$, all extensions $M(u_{-i}, \ldots, u_1)/M(u_{-(i-1)}, \ldots, u_1)$ become Galois. Note that allowing indices $i \le 0$ in Equation (8) corresponds to a dual tower.

Since $H_i \subseteq H_i' = M \cdot H_i \subseteq N_i$ for $i > 1$, it follows that the Galois closure of H_i'/H_1 is given by N_i (the Galois closure of the tower $\mathcal{H}'$ is the tower $\mathcal{N}$). This observation enables us to describe the Galois group of N_i/N_1 and to determine the ramification in the extensions H_{i+1}'/H_i'. The Galois closure of H_i'/H_1 is obtained by taking the composite over H_1 of $\sigma(H_i')$ where σ runs over all embeddings over H_1 of H_i' into a separable closure of H_1. Since H_2'/H_1 is Galois, we have $\sigma(H_2') = H_2'$ and hence this amounts to taking the composite over H_2' of the $\sigma(H_i')$. Since all extensions $\sigma(H_i')/H_2'$ are stepwise Galois p-extensions, we see that the extension N_i/H_2' is a Galois p-extension.

So we have:

Proposition 26 *The Galois group of N_i/N_1 is an extension of a subgroup of $\mathrm{GL}_{n-1}(\mathbb{F}_q)$ by a p-group.*

We can now determine the ramification behavior in the extensions H_{i+1}'/H_i', $i > 1$. We have $N_{i+1} \supseteq H_{i+1}' \supseteq H_i' \supseteq H_2'$. Since the extension N_{i+1}/H_2' is a p-extension, so is the extension N_{i+1}/H_i'. Moreover N_{i+1}/H_i' is weakly ramified, hence 2-bounded by Remark 16. The 2-boundedness of H_{i+1}'/H_i' now follows from [7, Proposition 10]. Hence we obtain the following

Proposition 27 *For all $i > 1$, the steps H_{i+1}'/H_i' are 2-bounded Galois p-extensions.*

Collecting all results above, we finish the proof of Theorem 1.

References

[1] A. Bassa, P. Beelen, The Hasse-Witt invariant in some towers of function fields over finite fields, Bulletin of the Brazilian Mathematical Society 41, 567–582, 2010.

[2] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, Towers of Function Fields over Non-prime Finite Fields, arXiv:1202.5922v2 [math.AG], May 2013.

[3] A. Bassa, A. Garcia, H. Stichtenoth, A new tower over cubic finite fields, Mosc. Math. J. 8, 401–418, 2008.

[4] I. Cascuso, R. Cramer, C. Xing, Torsion Limits and Riemann-Roch Systems for Function Fields and Applications to Arithmetic Secret Sharing, Proc. of the 31st Annual IACR CRYPTO, LNCS vol. 6842, pp. 685–707, Springer, 2011.

[5] A. Garcia and H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, J. Number Theory 61, 248–273, 1996.

[6] A. Garcia, H. Stichtenoth, Some Artin–Schreier towers are easy, Mosc. Math. J. 5, 767–774, 2005.

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

[8] D. Goss, Basic Structures of Function Field Arithmetic, Springer, 1996.

[9] H. Stichtenoth, Transitive and self-dual codes attaining the Tsfasman–Vladut–Zink bound, IEEE Trans. Inform. Theory 52, no. 5, pp. 2218–2224, 2006.

[10] M.A. Tsfasman, S.G. Vladut and T. Zink, Modular curves, Shimura curves and Goppa codes, better than the Varshamov–Gilbert bound, Math. Nachr. 109, pp. 21–28, 1982.

Alp Bassa
Sabancı University, MDBF
34956 Tuzla, İstanbul, Turkey
bassa@sabanciuniv.edu

Peter Beelen
Technical University of Denmark, Department of Applied Mathematics and Computer Science
Matematiktorvet, Building 303B
DK-2800, Lyngby, Denmark
p.beelen@mat.dtu.dk

Arnaldo Garcia
Instituto Nacional de Matemática Pura e Aplicada, IMPA
Estrada Dona Castorina 110
22460-320, Rio de Janeiro, RJ, Brazil
garcia@impa.br

Henning Stichtenoth
Sabancı University, MDBF
34956 Tuzla, İstanbul, Turkey
henning@sabanciuniv.edu