Functiones et Approximatio
57.1 (2017), 47–60
doi: 10.7169/facm/1615

A NOTE ON A TOWER BY BASSA, GARCIA AND STICHTENOTH

Nurdagül Anbar, Peter Beelen

Abstract: In this note, we prove that the tower given by Bassa, Garcia and Stichtenoth in [4] is a subtower of the one given by Anbar, Beelen and Nguyen in [2]. This completes the study initiated in [16, 2] to relate all known towers over cubic finite fields meeting Zink's bound with each other.

Keywords: tower of function fields, number of rational places, Zink's bound.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements, and let F be a function field with (full) constant field $\mathbb{F}_q$. The number $N(F)$ of $\mathbb{F}_q$-rational places of F is bounded in terms of the genus $g(F)$ and the cardinality of the finite field; namely

$$N(F) \leqslant 1 + q + 2g(F)\sqrt{q},$$

which is a well-known Hasse–Weil bound. It was noticed by Ihara [10] and Manin [12] that this bound is not optimal when $g(F)$ is large compared with the cardinality of the finite field. This initiated the study of asymptotic behaviour of the number of rational places of a function field over its genus as genus goes to infinity, and resulted in *Ihara's constant*:

$$A(q) := \limsup_{g(F)\to\infty} \frac{N(F)}{g(F)},$$

where "lim sup" runs over function fields with constant field $\mathbb{F}_q$. To investigate this constant, one considers towers of function fields. A *(recursive) tower* $\mathcal{F}/\mathbb{F}_q = (F_1 \subset F_2 \subset \cdots)$ *over* $\mathbb{F}_q$ is a sequence of function fields with constant field $\mathbb{F}_q$ such that

(i) $F_1 = \mathbb{F}_q(x_1)$ for some $x_1 \in F_1$, which is transcendental over $\mathbb{F}_q$,

2010 Mathematics Subject Classification: primary: 14H05, 11G20; secondary: 14G50

(ii) for each $i \geqslant 1$, we have $F_{i+1} = F_i(x_{i+1})$ with $[F_{i+1} : F_i] > 1$ and $\varphi(x_i, x_{i+1}) = 0$ for some separable polynomial $\varphi(x_i, T) \in \mathbb{F}_q(x_i)[T]$, and

(iii) $g(F_i) \to \infty$ as $i \to \infty$.

One says that the tower satisfies the recursion $\varphi(x_i, x_{i+1}) = 0$. For a tower $\mathcal{F}/\mathbb{F}_q$ satisfying the recursion $\varphi(x_i, x_{i+1}) = 0$, we call a tower $\mathcal{G}/\mathbb{F}_q$ the *dual tower* of $\mathcal{F}/\mathbb{F}_q$ if $\mathcal{G}/\mathbb{F}_q$ satisfies the recursion $\varphi(x_{i+1}, x_i) = 0$. Note that we do not assume that $\varphi(x_i, T)$ is irreducible over F_i for all i. As a result, a full characterization of the function fields in the tower may require further information. A tower $\mathcal{F}/\mathbb{F}_q$ is called *good* if its *limit*

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

is a positive real number. As the value of $\lambda(\mathcal{F}/\mathbb{F}_q)$ gives a lower bound for Ihara's constant $A(q)$, we are interested in towers having a limit as large as possible.

Drinfeld and Vladut [15] showed that $A(q) \leqslant \sqrt{q} - 1$ for any finite field $\mathbb{F}_q$. Therefore, this inequality is called the Drinfeld–Vladut bound. On the other hand, Ihara [9], Tsfasman, Vladut and Zink [14] used modular curves to show that $A(q) \geqslant \sqrt{q} - 1$ for square q. As a result, they proved that $A(q) = \sqrt{q} - 1$ if q is square. Then Garcia and Stichtenoth [7] gave another proof for the exact value of $A(q)$ for square q by constructing explicitly defined recursive tower.

Even though the exact value of $A(q)$ is still an open problem for non-square q, there are many lower bounds for it. Zink [17] used degenerations of Shimura surfaces to show

$$A(p^3) \geqslant 2(p^2 - 1)/(p + 2),$$

for p prime. Then van der Geer and van der Vlugt [8] gave an example of an explicitly defined tower over $\mathbb{F}_8$ whose limit is $3/2$; i.e. they gave an example of a tower meeting Zink's bound for the case $p = 2$. The bound was generalized for any cubic fields $\mathbb{F}_{q^3}$ as

$$A(q^3) \geqslant 2(q^2 - 1)/(q + 2) \tag{1}$$

by Bezerra, Garcia and Stichtenoth [5] by constructing an explicitly defined tower $\mathcal{A}/\mathbb{F}_{q^3}$ meeting Zink's bound. After that, a simpler proof for the bound (1) was given by Bassa, Garcia and Stichtenoth [4] with another explicitly defined tower $\mathcal{C}/\mathbb{F}_{q^3}$. Then it was shown by Zieve in [16] that $\mathcal{C}/\mathbb{F}_{q^3}$ is a partial Galois closure of $\mathcal{A}/\mathbb{F}_{q^3}$.

For any non-prime finite field $\mathbb{F}_{q^n}$, a new explicit tower BBGS was introduced by Bassa, Beelen, Garcia and Stichtenoth [3]. The tower's limit gave the following lower bound for $A(q^n)$:

$$A(q^n) \geqslant 2\left(\frac{1}{q^j - 1} + \frac{1}{q^{n-j} - 1}\right)^{-1},$$

where $1 \leqslant j \leqslant n - 1$. In fact, this resulted in the currently best known lower bound for $A(q^n)$ in the case $j = \lfloor n/2 \rfloor$, where $\lfloor x \rfloor$ denotes the integer part of x. Note that for $n = 3$, the bound coincides with Zink's bound.

In [1], another tower $\mathcal{X}$ was introduced over cubic fields resulting in Zink's bound. It was noticed that all steps in $\mathcal{X}/\mathbb{F}_{q^3}$ are Galois except the first one and that $\mathcal{X}/\mathbb{F}_{q^3}$ contains $\mathcal{A}/\mathbb{F}_{q^3}$ as a subtower. In this article, we show that $\mathcal{C}/\mathbb{F}_{q^3}$ is also a subtower of $\mathcal{X}/\mathbb{F}_{q^3}$. This completes the work started in [16] to relate the various towers over $\mathbb{F}_{q^3}$ to each other. The article is organised as follows: In Section 2, we give recursive equations of several towers over $\mathbb{F}_{q^3}$ and discuss the relationship between them. In Section 3 we prove our main result that $\mathcal{C}/\mathbb{F}_{q^3}$ is a subtower of $\mathcal{X}/\mathbb{F}_{q^3}$.

2. Relationship between some cubic towers

In this section we formulate the defining equations of previously introduced towers over cubic fields and the relationship between them. For convenience, we set $\mathbb{F} := \mathbb{F}_{q^3}$. Recently in [1], the authors introduced a tower $\mathcal{X}/\mathbb{F}$ satisfying the same reducible recursive equation as the BBGS Tower for $n = 3$, but arising from a different factor. More precisely, the reducible recursive equation and its factorization are given as follows.

$$\begin{aligned} x_1^{q^3-q}(x_2^{q^3}-x_2)-(x_1^{q^3-1}-1)x_2^{q^2} &= x_2(x_1^{q^2-1}x_2^{q^2-1}+x_2^{q-1}+x_1^{q^2-q})\cdot \\ &\quad \times \prod_{\alpha\in\mathbb{F}_q\setminus\{0\}} (x_1^{q^2-1}x_2^{q^2}+x_2^q+x_1^{q^2-q}x_2-\alpha x_1^{q^2}). \end{aligned}$$

While the factor $x_1^{q^2-1}x_2^{q^2}+x_2^q+x_1^{q^2-q}x_2-\alpha x_1^{q^2}$ is used as the defining equation of BBGS/$\mathbb{F}$ for some $\alpha \in \mathbb{F}_q \setminus \{0\}$, the tower

$$\mathcal{X}/\mathbb{F} = (X_1 = \mathbb{F}(x_1) \subset X_2 = \mathbb{F}(x_1, x_2) \subset \cdots)$$

is defined by the following equations:

$$x_1^{q^2-1}x_2^{q^2-1}+x_2^{q-1}+x_1^{q^2-q}=0 \qquad \text{and} \qquad x_{n+1}^q-\frac{x_{n+1}}{(x_{n-1}x_n)^{q-1}}=x_{n-1} \quad \text{for } n \geqslant 2. \tag{2}$$

Tower $\mathcal{X}/\mathbb{F}$ is investigated through its subtower

$$\mathcal{Z}/\mathbb{F} = (Z_1 = \mathbb{F}(z_1) \subset Z_2 = \mathbb{F}(z_1, z_2) \subset \cdots),$$

where $z_i := x_i^{q^3-1}$. This is the same tower investigated in [2]. Tower $\mathcal{Z}/\mathbb{F}$ is defined by the following equations:

$$(z_2-1)^{q+1}+\frac{z_1-1}{z_1}(z_2-1)^q-\left(\frac{z_1-1}{z_1}\right)^{q+1}z_2=0 \quad \text{and}$$

$$(z_nz_{n+1}-1)\left(z_nz_{n+1}+\frac{1}{z_{n-1}}\right)^{q-1}-\frac{(z_n+1)^q}{z_n}-\left(\frac{z_{n-1}+1}{z_{n-1}}\right)^q=0 \quad \text{for } n \geqslant 2.$$

Moreover, it is shown in [2] that there exists an element $\alpha_n \in \mathbb{F}(z_n, z_{n+1})$ such that

$$z_n = -\frac{1+\alpha_n}{\alpha_n^{q+1}} \qquad \text{and} \qquad z_{n+1} = -(\alpha_n + \alpha_n^{q+1}) \qquad \text{for } n \geqslant 1;$$

that is, $\mathbb{F}(\alpha_n) = \mathbb{F}(z_n, z_{n+1})$ for all $n \geqslant 1$. This implies that by deleting the first function field Z_1 of $\mathcal{Z}$ we obtain the dual tower of Caro–Garcia ([6])

$$\mathcal{B}/\mathbb{F} = (B_1 = \mathbb{F}(b_1) \subset B_2 = \mathbb{F}(b_1, b_2) \subset \cdots),$$

which is the same as the one given by Ihara ([11])

$$\mathcal{Y}/\mathbb{F} = (Y_1 = \mathbb{F}(y_1) \subset Y_2 = \mathbb{F}(y_1, y_2) \subset \cdots)$$

with the change of variable $y_n := 1/(1 + b_n)$ for all $n \geqslant 1$, and its reducible recursive equation is

$$\frac{y_{n+1} - 1}{y_{n+1}^{q+1}} = -\frac{y_n^q}{(1-y_n)^{q+1}} \qquad \text{for } n \geqslant 1.$$

In [11] the author shows that the tower given by Bezerra, Garcia and Stichtenoth ([5])

$$\mathcal{A}/\mathbb{F} = (A_1 = \mathbb{F}(a_1) \subset A_2 = \mathbb{F}(a_1, a_2) \subset \cdots)$$

is a subtower of $\mathcal{Y}/\mathbb{F}$. In fact, $Y_2 = \mathbb{F}(y_1, y_2) = \mathbb{F}(a_2)$ with

$$y_1 = \frac{1-a_2}{a_2^q}, \qquad y_2 = \frac{a_2^q + a_2 - 1}{a_2} \qquad \text{and} \qquad a_2 = \frac{1-y_1}{y_1 y_2 - y_1 + 1}.$$

In order to give a simple proof for the fact that Zink's bound holds for any cubic fields, Bassa, Garcia and Stichtenoth investigate the tower

$$\mathcal{C}/\mathbb{F} = (C_1 = \mathbb{F}(c_1) \subset C_2 = \mathbb{F}(c_1, c_2) \subset \cdots),$$

whose recursive equation is given by

$$\left(c_{n+1}^q - c_{n+1}\right)^{q-1} + 1 = -\frac{c_n^{q(q-1)}}{\left(c_n^{q-1} - 1\right)^{q-1}}. \tag{3}$$

The complete picture for towers $\mathcal{X}$, $\mathcal{Z}$ and $\mathcal{C}$ can be seen in Figure 4.1. We refer to [1] for the investigation of $\mathcal{Z}/\mathbb{F}$ as a subtower of $\mathcal{X}/\mathbb{F}$ and to [16] for the investigation of $\mathcal{A}/\mathbb{F}$ as a subtower of $\mathcal{C}/\mathbb{F}$. In particular, the extension degrees stated in Figure 4.1 have been determined there.

We finish this section by giving the ramification structure of the extension $X_3/\mathbb{F}(a_2)$. For details we refer to Section 2.1 in [2] and Proposition 2 in [1]. A place P of $\mathbb{F}(a_2)$ is ramified in the extension $X_3/\mathbb{F}(a_2)$ only if $P \cap \mathbb{F}(z_1)$ is $(z_1 = \infty)$ or $(z_1 = 0)$. Hence we give the ramification into two cases (see also Figure 4.4).

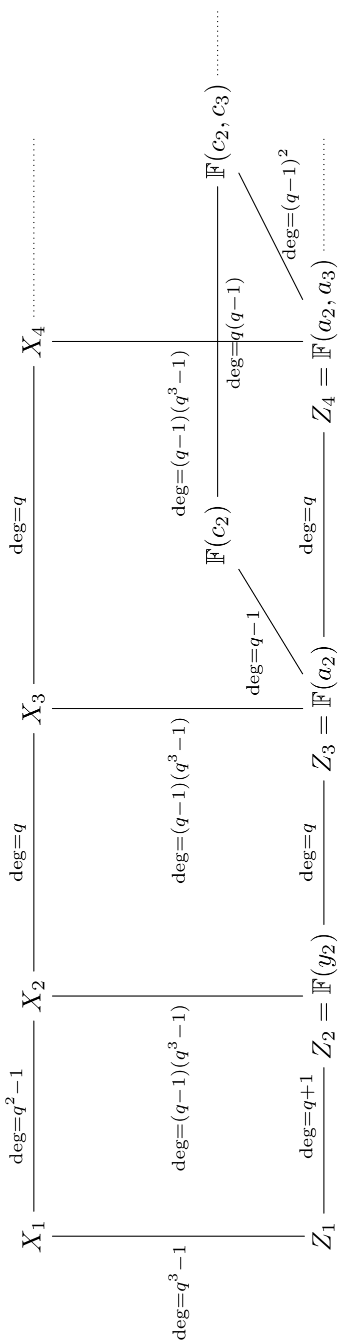

Figure 4.1. Relationship between Towers $\mathcal{X}$, $\mathcal{Z}$ and $\mathcal{C}$

- The place $(a_2 = 1)$ is the unique place lying over $(z_1 = \infty)$; i.e. $e((a_2 = 1)|(z_1 = \infty)) = q(q+1)$. Hence there are $q-1$ places of X_3 lying over $(a_2 = 1)$, and each of them has ramification index $q^3 - 1$.
- The places of $\mathbb{F}(a_2)$ lying over $(z_1 = 0)$ are $(a_2 = 0)$, $(a_2 = \infty)$ and $(a_2 = \beta_i)$, where β_i's are distinct roots of the polynomial $T^q + T - 1$ for $i \in \{1, \ldots, q\}$. They have the following ramification in $\mathbb{F}(a_2)/\mathbb{F}(z_1)$.

$$e((a_2 = 0)|(z_1 = 0)) = q - 1, \qquad e((a_2 = \infty)|(z_1 = 0)) = 1 \quad \text{and}$$
$$e((a_2 = \beta_i)|(z_1 = 0)) = q \qquad \text{for all } i \in \{1, \ldots, q\}.$$

Hence X_3 has $q-1$ many places lying over $(a_2 = \infty)$, $(a_2 = \beta_i)$, and it has $(q-1)^2$ many places lying over $(a_2 = 0)$.

3. Main result

In this section we prove that Tower $\mathcal{X}/\mathbb{F}$ has a subtower which is essentially the same as Tower $\mathcal{C}/\mathbb{F}$. To prove this, we use the fact that a divisor of a nonzero element f of a function field is zero if and only if f belongs to the constant field. Then our strategy is to show that the divisor of $c_2x_1x_2x_3$ is zero in the compositum $X_3 \cdot \mathbb{F}(c_2)$ of the function fields X_3 and $\mathbb{F}(c_2)$ over $\mathbb{F}(a_2)$. In other words, the element $c_2x_1x_2x_3$ belongs to the constant field of $X_3 \cdot \mathbb{F}(c_2)$. Then the argument that the constant field of $X_3 \cdot \mathbb{F}(c_2)$ is $\mathbb{F}_{q^3}$ implies that $c_2 \in X_3$, and hence $\mathbb{F}(c_2) \subseteq X_3$. This gives the desired result.

For the convenience of reader we first fix some notation. Let F be a function field with a constant field $\mathbb{F}$ and let E/F be a finite separable extension. We denote by

- $\mathbb{P}_F$ the set of places of F,
- Div(F) the divisor group of F
- $P|Q$ for a place $P \in \mathbb{P}_E$ lying over a place $Q \in \mathbb{P}_F$,
- $e(P|Q)$ the ramification index of $P|Q$,
- $d(P|Q)$ the different exponent of $P|Q$,
- $(f)^F$ the divisor of a nonzero $f \in F$ in F, and
- $\mathrm{Con}_{E/F}(D) \in \mathrm{Div(E)}$ the conorm of a divisor $D \in \mathrm{Div(F)}$.

For finite separable extensions $F \subseteq E \subseteq H$ and $D \in \mathrm{Div(F)}$ we have

$$\mathrm{Con}_{H/F}(D) = \mathrm{Con}_{H/E}\left(\mathrm{Con}_{E/F}(D)\right);$$

i.e., "Con" has the transitivity property. For a rational function field $\mathbb{F}(x)$ and $\gamma \in \mathbb{F}$, we denote by $(x = \gamma)$ and $(x = \infty)$ the places corresponding to the unique zero and the pole of $x - \gamma$, respectively.

Since we mainly use Abhyankar's Lemma in our proofs, we state the lemma below.

Lemma 1 (Abhyankar's Lemma ([13],Theorem 3.9.1)). *Let E/F be a finite separable extension. Suppose that $E = F_1 \cdot F_2$ is the compositum of the intermediate* *fields $F \subseteq F_1, F_2 \subseteq E$. Let $P \in \mathbb{P}_E$ lying over $Q \in \mathbb{P}_F$. We set $P_i := P \cap F_i$ for $i = 1, 2$. If one of $P_i|Q$ is tame, then*

$$e(P|Q) = \operatorname{lcm}\{e(P_1|Q), e(P_2|Q)\},$$

where lcm *denotes the least common multiple.*

In our cases, one of the extensions is always tame, say F_1/F. Then Abhyankar's Lemma implies:

$$e(P|P_1) = \frac{e(P_2|Q)}{\gcd\{e(P_1|Q), e(P_2|Q)\}},$$

where gcd denotes the greatest common divisor.

As mentioned above, our strategy is to investigate the compositum of $X_3 = \mathbb{F}(x_1, x_2, x_3)$ and $\mathbb{F}(c_2)$ over $\mathbb{F}(a_2)$, which is equivalent to the compositum of X_3 and $\mathbb{F}(x_1, c_2)$ over $\mathbb{F}(a_2)$ (see Figure 4.2). We know the exact ramification in $\mathbb{F}(x_1, x_2, x_3)/\mathbb{F}(a_2)$ as stated at the end of Section 2. Hence we only need to find out the ramification in $\mathbb{F}(x_1, c_2)$ over $\mathbb{F}(a_2)$. During the ramification investigation, we assume without loss of generality that $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_{q^3}$. We first consider $\mathbb{F}(x_1, c_2)$ over $\mathbb{F}(z_1)$. For this, we investigate the ramification structure of the rational function field extension $\mathbb{F}(c_2)/\mathbb{F}(z_1)$.

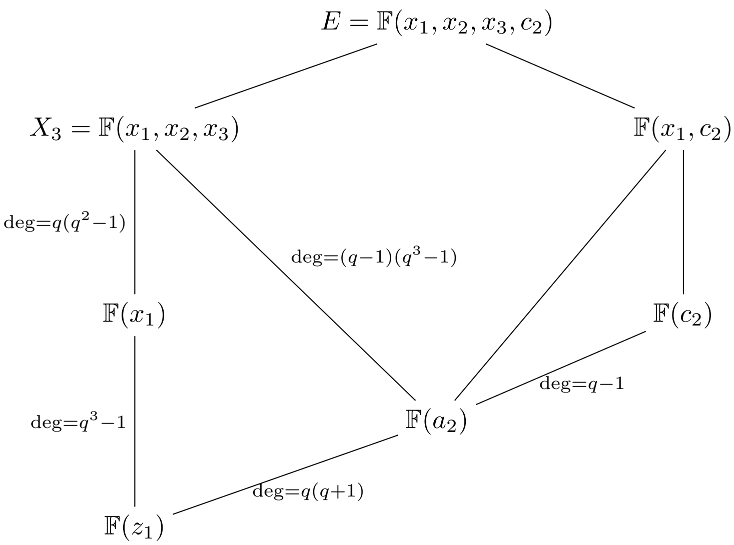

Figure 4.2. The compositum of $\mathbb{F}(x_1, x_2, x_3)$ and $\mathbb{F}(x_1, c_2)$

The ramification structure of $\mathbb{F}(c_2)/\mathbb{F}(z_1)$

By using the relations between the towers in Section 2; i.e.,

$$z_1 = -\frac{1+\alpha_1}{\alpha_1^{q+1}}, \qquad \alpha_1 = b_2 \qquad \text{and} \qquad b_2 = \frac{1}{y_2} - 1,$$

we can express z_1 in terms of y_2 as follows:

$$z_1 = -\frac{y_2^q}{(1-y_2)^{q+1}}.$$

As a result, we have extensions of rational function fields

$$\mathbb{F}(z_1) \ \subseteq \ \mathbb{F}(y_2) \ \subseteq \ \mathbb{F}(a_2) \ \subseteq \ \mathbb{F}(c_2)$$

whose defining equations are given in Figure 4.3. From the defining equations of the extensions, we have the following conclusions.

$$\begin{array}{ccc}
 & \mathbb{F}(c_2) & \\
\text{deg}{=}q-1 & \Big| & c_2^{q-1} = 1 - \frac{1}{a_2} \\
 & \mathbb{F}(a_2) & \\
\text{deg}{=}q & \Big| & y_2 = \frac{a_2^q + a_2 - 1}{a_2} \\
 & \mathbb{F}(y_2) & \\
\text{deg}{=}q+1 & \Big| & z_1 = -\frac{y_2^q}{(1-y_2)^{q+1}} \\
 & \mathbb{F}(z_1) &
\end{array}$$

Figure 4.3. Subfields of $\mathbb{F}(c_2)/\mathbb{F}(z_1)$

- In the extension $\mathbb{F}(y_2)/\mathbb{F}(z_1)$, the ramified places are $(z_1 = 0)$ and $(z_1 = \infty)$. More precisely, there are two places of $\mathbb{F}(y_2)$ lying over $(z_1 = 0)$, namely

$(y_2 = 0)$ and $(y_2 = \infty)$ with $e((y_2 = 0)|(z_1 = 0)) = d((y_2 = 0)|(z_1 = 0)) = q$ and $e((y_2 = \infty)|(z_1 = 0)) = 1$. The place $(y_2 = 1)$ is the unique place lying over $(z_1 = \infty)$; i.e., it is totally ramified in $\mathbb{F}(y_2)$.

- In the extension $\mathbb{F}(a_2)/\mathbb{F}(y_2)$, the ramified places are $(y_2 = 1)$ and $(y_2 = \infty)$. More precisely, there are two places of $\mathbb{F}(a_2)$ lying over $(y_2 = \infty)$; namely $(a_2 = 0)$ and $(a_2 = \infty)$ with $e((a_2 = 0)|(y_2 = \infty)) = 1$ and $e((a_2 = \infty)|(y_2 = \infty)) = q - 1$. The place $(y_2 = 1)$ totally ramifies in $\mathbb{F}(a_2)$, and $(a_2 = 1)$ is the unique place lying over it.
- It can be easily seen that $(c_2 = \infty)$ and $(c_2 = 0)$ are the unique places lying over $(a_2 = 0)$ and $(a_2 = 1)$, respectively. There is no other ramification. ■

In particular, we conclude that $(z_1 = 0)$ and $(z_1 = \infty)$ are the only ramified places of $\mathbb{F}(z_1)$ in the extension $\mathbb{F}(c_2)/\mathbb{F}(z_1)$. The exact ramification structure of $\mathbb{F}(c_2)/\mathbb{F}(z_1)$ is given in Figure 4.4.

Corollary 1. *The extension degree of* $\mathbb{F}(x_1, c_2)/\mathbb{F}(c_2)$ *is equal to* $q^3 - 1$, *and hence the extension degree of* $\mathbb{F}(x_1, c_2)/\mathbb{F}(a_2)$ *is* $(q - 1)(q^3 - 1)$.

Proof. We consider $\mathbb{F}(x_1, c_2)$ as a compositum of $\mathbb{F}(x_1)$ and $\mathbb{F}(c_2)$ over $\mathbb{F}(z_1)$ (see Figure 4.2). Let R be a place of $\mathbb{F}(x_1, c_2)$ lying over $R_{i,j}$ for some $i \in \{1, \ldots, q\}$ and $j \in \{1, \ldots, q - 1\}$ (see Figure 4.4). Note that we have $R|R_{i,j}|(z_1 = 0)$ and $R|(x_1 = 0)|(z_1 = 0)$. Since $z_1 = x_1^{q^3-1}$, the ramification index $e((x_1 = 0)|(z_1 = 0) = q^3 - 1$, which is relatively prime to the ramification index $e(R_{i,j}|(z_1 = 0)) = q$. By Abhyankar's Lemma we conclude that $e(R|R_i) = q^3 - 1$. This implies that the extension degree of $\mathbb{F}(x_1, c_2)/\mathbb{F}(c_2)$ is at least $q^3 - 1$, which gives the desired result. ■

Note that by Corollary 1 we conclude that $[\mathbb{F}(x_1, c_2) : \mathbb{F}(a_2)] = [\mathbb{F}(x_1, x_2, x_3) : \mathbb{F}(a_2)]$. As a result, we have $[E : \mathbb{F}(x_1, x_2, x_3)] = [E : \mathbb{F}(x_1, c_2)]$.

The ramification structure of $\mathbb{F}(x_1, c_2)/\mathbb{F}(c_2)$

We have seen that $(z_1 = 0)$ and $(z_1 = \infty)$ are the only places of $\mathbb{F}(z_1)$ ramified in the extensions $\mathbb{F}(x_1)/\mathbb{F}(z_1)$ and $\mathbb{F}(c_2)/\mathbb{F}(z_1)$. Hence a place of $\mathbb{F}(x_1, c_2)$ is ramified only if it lies over $(z_1 = 0)$ or $(z_1 = \infty)$. Hence, we investigate the ramification $\mathbb{F}(x_1, c_2)/\mathbb{F}(c_2)$ into two cases.

- Let T be a place of $\mathbb{F}(x_1, c_2)$ lying over $(z_1 = \infty)$. Since $(z_1 = \infty)$ is totally ramified in both extensions $\mathbb{F}(x_1)$ and $\mathbb{F}(c_2)$, we have $T|(x_1 = \infty)|(z_1 = \infty)$ and $T|(c_2 = 0)|(z_1 = \infty)$. Then we conclude that $e(T|(c_2 = 0)) = q^2 + q + 1$.
- Let S be a place of $\mathbb{F}(x_1, c_2)$ lying over $(z_1 = 0)$. Then there are two cases.
  - (i) If S is a place lying over $R_{i,j}$ for some $i \in \{1, \ldots, q\}$ and $j \in \{1, \ldots, q - 1\}$ (see Figure 4.4), then we have $S|(x_1 = 0)|(z_1 = 0)$ and $S|R_{i,j}|(z_1 = 0)$. By Abhyankar's Lemma, we conclude that $e(S|R_{i,j}) = q^3 - 1$; i.e. $R_{i,j}$ is totally ramified $\mathbb{F}(x_1, c_2)$ for each $i \in \{1, \ldots, q\}$ and $j \in \{1, \ldots, q - 1\}$.
  - (ii) If S is a place lying over $(c_2 = \infty)$ or P_i for some $i \in \{1, \ldots, q - 1\}$, then we have $e(S|(c_2 = \infty)) = e(S|P_i) = q^2 + q + 1$. ■

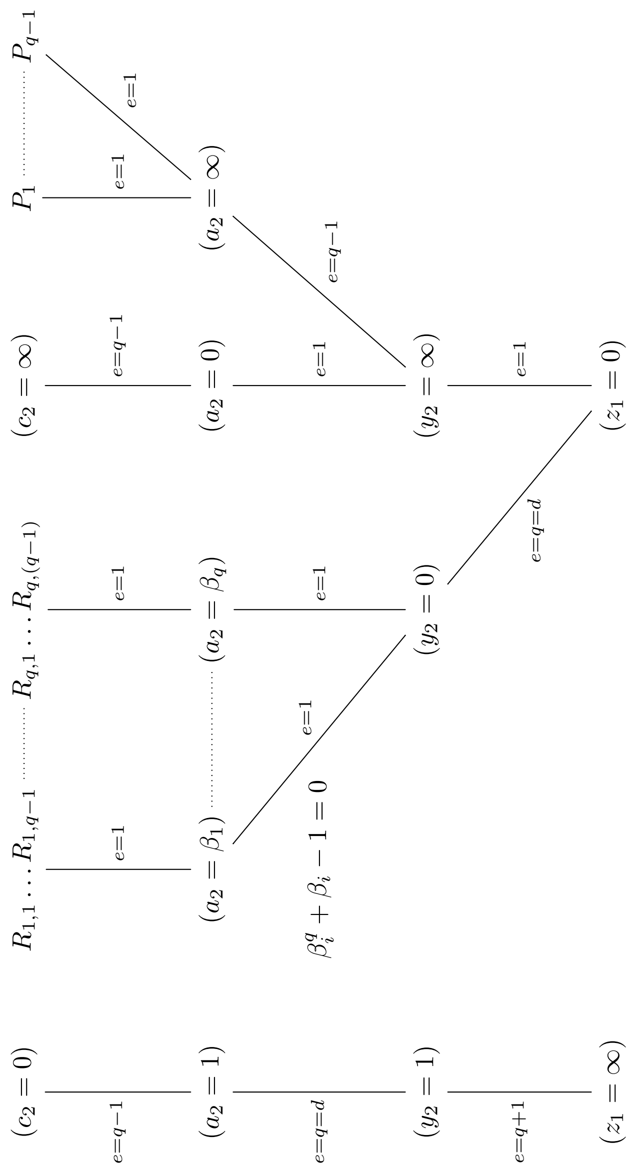

Figure 4.4. The ramification structure in $\mathbb{F}(c_2)/\mathbb{F}(z_1)$

Now we can explicitly state the ramification structure of the extension $\mathbb{F}(x_1, c_2)/\mathbb{F}(a_2)$. We first note that $\mathbb{F}(x_1, c_2)/\mathbb{F}(a_2)$ is a Galois extension of degree $(q-1)(q^3-1)$ since it is the compositum of two Kummer extensions $\mathbb{F}(x_1, a_1)$ and $\mathbb{F}(c_2)$ of $\mathbb{F}(a_2)$. From the above discussions on the ramification structures of the extensions $\mathbb{F}(c_2)/\mathbb{F}(z_1)$ and $\mathbb{F}(x_1, c_2)/\mathbb{F}(c_2)$, we conclude the following ramification structure of $\mathbb{F}(x_1, c_2)$ over $\mathbb{F}(a_2)$: The ramified places of $\mathbb{F}(a_2)$ are $(a_2 = 1)$, $(a_2 = 0)$, $(a_2 = \infty)$ and $(a_2 = \beta_i)$ for $i = 1, \ldots, q$, where β_i's are distinct roots of the polynomial $T^q + T - 1$. More precisely, there are $q-1$ many places of $\mathbb{F}(x_1, c_2)$ lying over each of the places $(a_2 = 1)$, $(a_2 = 0)$ and $(a_2 = \beta_i)$ for $i = 1, \ldots, q$, and hence each of them has ramification index $q^3 - 1$. Furthermore, there are $(q-1)^2$ places lying over $(a_2 = \infty)$ each of which has a ramification index $q^2 + q + 1$. On the other hand, we know that the same tame ramification structure holds in $\mathbb{F}(x_1, x_2, x_3)/\mathbb{F}(a_2)$. We consider the compositum $E := X_3 \cdot \mathbb{F}(x_1, c_2)$ of the fields X_3 and $\mathbb{F}(x_1, c_2)$ over $\mathbb{F}(a_2)$. The same ramification structure of $\mathbb{F}(x_1, c_2)/\mathbb{F}(a_2)$ and $X_3/\mathbb{F}(a_2)$ implies that E is an unramified extension of both X_3 and $\mathbb{F}(x_1, c_2)$ of the same degree.

We denote by $Q_1, \ldots, Q_{q-1}$ the places of X_3 lying over $(a_2 = 1)$, by $A_1, \ldots, A_{q-1}$ the ones lying over $(a_2 = 0)$, by $S_{i,1}, \ldots, S_{i,q-1}$ the ones lying over $(a_2 = \beta_i)$ for each $i \in \{1, \ldots, q\}$ and $B_1, \ldots, B_{(q-1)^2}$ the ones lying over $(a_2 = \infty)$. Moreover, for convenience we define the divisors $\mathcal{Q}$, $\mathcal{A}$, $\mathcal{S}$ and $\mathcal{B}$ as follows:

$$\mathcal{Q} := \sum_{i=1}^{q-1} Q_i, \qquad \mathcal{A} := \sum_{i=1}^{q-1} A_i, \qquad \mathcal{S} := \sum_{j=1}^{q} \sum_{i=1}^{q-1} S_{i,j} \qquad \text{and} \qquad \mathcal{B} := \sum_{i=1}^{(q-1)^2} B_i.$$

Now we compute the divisors of x_1, x_2 and x_3 in X_3 with this convention.

- **The divisor of $\boldsymbol{x_1}$:** We have seen that $z_1 = -y_2^q/(1-y_2)^{q+1}$, and hence the divisor of z_1 in $\mathbb{F}(y_2)$ is given by

$$(z_1)^{\mathbb{F}(y_2)} = q(y_2 = 0) + (y_2 = \infty) - (q+1)(y_2 = 1).$$

By using Figure 4.4 and the transitivity of the Con mapping, we conclude the following equalities.

$$\begin{aligned} \mathrm{Con}_{X_3/\mathbb{F}(y_2)}((y_2 = 0)) &= \mathrm{Con}_{X_3/\mathbb{F}(a_2)}\left(\mathrm{Con}_{\mathbb{F}(a_2)/\mathbb{F}(y_2)}(y_2 = 0)\right) \qquad (4)\\ &= \sum_{j=1}^{q} \mathrm{Con}_{X_3/\mathbb{F}(a_2)}((a_2 = \beta_j)) \\ &= (q^3 - 1)\mathcal{S}. \\ \mathrm{Con}_{X_3/\mathbb{F}(y_2)}((y_2 = \infty)) &= \mathrm{Con}_{X_3/\mathbb{F}(a_2)}\left(\mathrm{Con}_{\mathbb{F}(a_2)/\mathbb{F}(y_2)}(y_2 = \infty)\right) \\ &= \mathrm{Con}_{X_3/\mathbb{F}(a_2)}((a_2 = 0)) \\ &\quad + (q-1)\mathrm{Con}_{F/\mathbb{F}(a_2)}((a_2 = \infty)) \\ &= (q^3 - 1)\mathcal{A} + (q^3 - 1)\mathcal{B} \\ \mathrm{Con}_{X_3/\mathbb{F}(y_2)}((y_2 = 1)) &= \mathrm{Con}_{X_3/\mathbb{F}(a_2)}\left(\mathrm{Con}_{\mathbb{F}(a_2)/\mathbb{F}(y_2)}(y_2 = 1)\right) \\ &= q\mathrm{Con}_{X_3/\mathbb{F}(a_2)}((a_2 = 1)) \\ &= q(q^3 - 1)\mathcal{Q} \end{aligned}$$

As a result, we conclude that

$$(z_1)^{X_3} = (q^3-1)\left(q\mathcal{S}+\mathcal{A}+\mathcal{B}-q(q+1)\mathcal{Q}\right).$$

Since $z_1 = x_1^{q^3-1}$, this implies that $(x_1)^{X_3} = q\mathcal{S}+\mathcal{A}+\mathcal{B}-q(q+1)\mathcal{Q}$.

- **The divisor of $\boldsymbol{x_2}$:** Similarly we can compute z_2 in terms of y_2 by using the relations given in Section 2 as follows.

$$z_2 = -(\alpha_1+\alpha_1^{q+1}) = -(b_2+b_2^{q+1}) = \frac{y_2-1}{y_2^{q+1}}$$

Hence, the divisor of z_2 in $\mathbb{F}(y_2)$ is given by

$$(z_2)^{\mathbb{F}(y_2)} = (y_2=1)+q(y_2=\infty)-(q+1)(y_2=0).$$

By Equations (4), we conclude that

$$(z_2)^{X_3} = (q^3-1)\left(q\mathcal{Q}+q\mathcal{A}+q\mathcal{B}-(q+1)\mathcal{S}\right),$$

which implies that $(x_2)^{X_3} = q\mathcal{Q}+q\mathcal{A}+q\mathcal{B}-(q+1)\mathcal{S}$.

- **The divisor of $\boldsymbol{x_3}$:** By the fact that $y_1=(1-a_2)/a_2^q$, we have

$$z_3 = \frac{y_1-1}{y_1^{q+1}} = \frac{a_2^{q^2}(a_2^q+a_2-1)}{(a_2-1)^{q+1}}.$$

In other words, the divisor of z_3 in $\mathbb{F}(a_2)$ is

$$(z_3)^{\mathbb{F}(a_2)} = q^2(a_2=0)+\sum_{j=1}^{q}(a_2=\beta_j)-(q+1)(a_2=1)-(q^2-1)(a_2=\infty),$$

where β_j's are distinct roots of T^q+T-1 as before. As a result, we conclude that

$$(z_3)^{X_3} = (q^3-1)\left(q^2\mathcal{A}+\mathcal{S}-(q+1)\mathcal{Q}-(q+1)\mathcal{B}\right),$$

or equivalently this means that $(x_3)^{X_3} = q^2\mathcal{A}+\mathcal{S}-(q+1)\mathcal{Q}-(q+1)\mathcal{B}$.

Now we can state our main result.

Theorem 1. *Let $\mathcal{X}/\mathbb{F}_{q^3} = (X_1=\mathbb{F}(x_1)\subset X_2=\mathbb{F}(x_1,x_2)\subset\cdots)$ be the tower defined by Equation* (2). *Then $\mathcal{X}/\mathbb{F}_{q^3}$ contains a tower, which is essentially the same as the tower $\mathcal{C}/\mathbb{F}_{q^3}=(C_1=\mathbb{F}(c_1)\subset C_2=\mathbb{F}(c_1,c_2)\subset\cdots)$ given by Equation* (3). *In other words, the Bassa–Garcia–Stichtenoth Tower is a subtower of $\mathcal{X}/\mathbb{F}_{q^3}$.*

Proof. We know that $c_2^{q-1}=(a_2-1)/a_2$; i.e. the divisor of c_2^{q-1} in $\mathbb{F}(a_2)$ is given by

$$(c_2^{q-1})^{\mathbb{F}(a_2)} = (a_2=1)-(a_2=0).$$

Hence we conclude that

$$(c_2^{q-1})^{X_3} = (q^3-1)(\mathcal{Q}-\mathcal{A}).$$

On the other hand, we have computed the divisors of x_1, x_2, x_3 in X_3. With these computations we conclude that

$$(x_1x_2x_3)^{X_3} = (x_1)^{X_3} + (x_2)^{X_3} + (x_3)^{X_3} = (q^2+q+1)\mathcal{A} - (q^2+q+1)\mathcal{Q}.$$

Since the compositum E of $X_3 = \mathbb{F}(x_1, x_2, x_3)$ and $\mathbb{F}(x_1, c_2)$ is an unramified extension of X_3, we conclude that $(x_1x_2x_3)^E + (c_2)^E = 0$. This holds if and only if $x_1x_2x_3c_2 = \gamma$ for some nonzero $\gamma \in \mathbb{F}$. Note that the place $(z_1 = 1)$ of $\mathbb{F}(z_1)$ splits in both extension X_3 and $\mathbb{F}(c_2)$. Hence $(z_1 = 1)$ splits in the compositum $X_3 \cdot \mathbb{F}(c_2) = E$. This implies that the full constant field of E is $\mathbb{F}_{q^3}$. Similarly, for all $i > 2$ we can show that

$$c_i x_{i-1} x_i x_{i+1} = \gamma_i \qquad \text{for some nonzero } \gamma_i \in \mathbb{F}_{q^3},$$

which shows that $\mathcal{C}/\mathbb{F}$ is contained in $\mathcal{X}/\mathbb{F}$. ■

Acknowledgment. Nurdagül Anbar and Peter Beelen gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF–4002-00367). Nurdagül Anbar is also supported by H.C. Ørsted COFUND Post-doc Fellowship from the project “Algebraic curves with many rational points".

References

[1] N. Anbar, P. Beelen, N. Nguyen, *A new tower meeting Zink's bound with good p-rank*, appeared online 18 January 2017 in Acta Arithmetica.

[2] N. Anbar, P. Beelen, N. Nguyen, *The exact limit of some cubic towers*, to appear in Contemporary Mathematics, proceedings of AGCT-15.

[3] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, *Towers of function fields over non-prime finite fields*, Mosc. Math. J. **15(1)** (2015), 1–29.

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

[5] 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.

[6] N. Caro, A. Garcia, *On a tower of Ihara and its limit*, Acta Arith. **151** (2012), 191–200.

[7] A. Garcia, H. Stichtenoth, *A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound*, Invent. Math. **121** (1995), 211–222.

[8] G. van der Geer, M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34** (2002), 291–300.

[9] Y. Ihara, *Congruence relations and Shimūra curves. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25(3)** (1979), 301–361.

[10] 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(3)** (1982), 721–724.

[11] Y. Ihara, *Some remarks on the BGS tower over finite cubic fields*, Proceedings of the workshop "Arithmetic Geometry, Related Areas and Applications", Chuo University, (2007), 127–131.

[12] J.I. Manin, *The Hasse-Witt matrix of an algebraic curve*, Amer. Math. Soc. Transl. **45** (1965), 245–264.

[13] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 2009.

[14] M.A. Tsfasman, S.G. Vladut, Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov–Gilbert bound*, Mathematische Nachrichten **109(1)** (1982), 21–28.

[15] S.G. Vladut and V.G. Drinfel'd, *Number of points of an algebraic curve*, Functional analysis and its applications **17(1)** (1983), 53–54.

[16] M.E. Zieve, *An equality between two towers over cubic fields*, to appear in Bull. Braz. Math. Soc., arXiv:0905.4921.

[17] Th. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, In: Fundamentals of computation theory (Cottbus, 1985), Lecture Notes in Comput. Sci. **199** (1985), 503–511.

Address: Nurdagül Anbar and Peter Beelen: Department for Applied Mathematics and Computer Science, Technical University of Denmark, Matematiktorvet 303B, 2800 Kongens Lyngby, Denmark.

E-mail: nurdagulanbar2@gmail.com, pabe@dtu.dk

Received: 4 May 2016; **revised:** 15 July 2016