A new tower with good p-rank meeting Zink's bound

Anbar Meidl, Nurdagül; Beelen, Peter ; Nguyen, Nhut

Published in:
Acta Arithmetica

Link to article, DOI:
10.4064/aa8388-6-2016

Publication date:
2017

Document Version
Peer reviewed version

A NEW TOWER WITH GOOD p-RANK MEETING ZINK'S BOUND

NURDAGÜL ANBAR, PETER BEELEN, AND NHUT NGUYEN

ABSTRACT. In this article we investigate the asymptotic p-rank of a new tower of function fields defined over cubic finite fields. Its limit meets Zink's bound, but the new feature of this tower is that its asymptotic p-rank for small cubic finite fields is much smaller than that of other cubic towers for which the asymptotic p-rank is known. This is of independent interest, but also makes this new tower more interesting for theoretical applications in cryptography.

1. INTRODUCTION

Let $\overline{\mathbb{F}}_q$ be the algebraic closure of the finite field $\mathbb{F}_q$ with q elements. If $\bar{F}$ is an algebraic function field with constant field $\overline{\mathbb{F}}_q$, then its *p-rank* $\gamma(\bar{F})$ is defined as the $\mathbb{F}_p$-dimension of the group consisting of the divisor classes of degree zero of order p, where p is the characteristic of $\overline{\mathbb{F}}_q$. In the case that F is a function field with constant field $\mathbb{F}_q$, we define its p-rank as the p-rank of the compositum $F \cdot \overline{\mathbb{F}}_q$ of F and $\overline{\mathbb{F}}_q$. The p-rank is of independent interest and occurs in for example class field theory to estimate how many distinct unramified Artin–Schreier extensions of degree p a function field F can have. The p-rank also appears in [7] to analyse the theoretical behaviour of various constructions related to multi-party computations and fast multiplication algorithms. For such constructions a tower of function fields with low p-rank is better than a tower of function fields with high p-rank. The main contribution in this article is to define a new tower of function fields defined over cubic finite fields $\mathbb{F}_q$ with excellent asymptotic behaviour.

To put our results in context, we introduce some notation and background. Following [16], we introduce $\mathcal{F}/\mathbb{F}_q = (F_1 \subset F_2 \subset \cdots)$ a tower of function fields over $\mathbb{F}_q$. The *limit* $\lambda(\mathcal{F}/\mathbb{F}_q)$ of the tower $\mathcal{F}/\mathbb{F}_q$ is defined as

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

where $N(F_n)$ and $g(F_n)$ are the number of $\mathbb{F}_q$-rational places and the genus of the function field F_n, respectively. It is a well-known fact that the limit

2010 *Mathematics Subject Classification.* Primary 14H05, 11G20; Secondary 14G50.

Key words and phrases. tower of function fields, number of rational places, Ihara's constant, Cartier operator, p-rank.

of the tower $\mathcal{F}/\mathbb{F}_q$ satisfies

$$0 \leq \lambda(\mathcal{F}/\mathbb{F}_q) \leq \sqrt{q} - 1 \ ,$$

which is called the Drinfeld–Vladut bound. Towers with $\lambda(\mathcal{F}/\mathbb{F}_q) = \sqrt{q} - 1$ are called *optimal*.

The *asymptotic p-rank*, or in short the *p-rank* of the tower $\mathcal{F}/\mathbb{F}_q$ is defined as

$$\varphi(\mathcal{F}/\mathbb{F}_q) := \liminf_{n\to\infty} \frac{\gamma(F_n)}{g(F_n)} \ .$$

Note that this quantity is defined in [7], where it is called the p-torsion limit of the tower. Since for any function field $0 \leq \gamma(F) \leq g(F)$, we conclude that $0 \leq \varphi(\mathcal{F}/\mathbb{F}_q) \leq 1$. Towers with $\varphi(\mathcal{F}/\mathbb{F}_q) = 1$ are called *ordinary*. It was for example shown in [2] that the optimal tower in [9] is ordinary.

Motivated by [7], one is especially interested in towers $\mathcal{F}/\mathbb{F}_q$ having a large limit and p-rank as small as possible. The best would be to find an optimal tower with zero p-rank, but it is not known if such towers exist. What is known [7, 2] is that if q is a square, the explicit tower from [8] has p-rank $1/(\sqrt{q}+1)$. This gives the currently best known upper bound for the minimal p-rank of a tower of function fields defined over square finite fields. For non-square finite fields, much less is known. It is for example not known if optimal towers exist. For non-prime values of q the towers $\mathcal{F}/\mathbb{F}_q$ introduced in [3] have the currently largest known limits for a given value of q. Before this construction, the best known bound was Zink's bound over cubic fields $\mathbb{F}_{p^{3e}}$; namely

$$A(p^{3e}) \geq \frac{2(p^{2e}-1)}{p^e+2} \ .$$

Even though the limit of the tower [3] coincides with Zink's bound for $e = 1$, it strictly exceeds Zink's bound for $e > 1$. Therefore, after the square q case, computing the p-rank of a tower over $\mathbb{F}_{p^3}$ with limit at least Zink's bound is the next obvious case to study. So far in [2] only the p-rank of a tower $\mathrm{BaGS}/\mathbb{F}_{p^{3e}}$ introduced in [4], has been computed. There, it was shown that its p-rank equals

$$\varphi(\mathrm{BaGS}/\mathbb{F}_{p^{3e}}) = \frac{2\binom{p+1}{2}^e - 2}{(p^e-1)(p^e+2)} \ ,$$

where $\binom{*}{*}$ denotes the binomial coefficient. This shows that the p-rank of $\mathrm{BaGS}/\mathbb{F}_{p^{3e}}$ is strictly less than 1 for $e > 1$, while it is ordinary for $e = 1$.

In this article, we will introduce a new tower $\mathcal{F}/\mathbb{F}_{p^{3e}}$ satisfying the same reducible recursive equation as the one used in [3] (see Equation (10)). However, the defining equation of $\mathcal{F}/\mathbb{F}_{p^{3e}}$ is coming from a different factor;

namely the unique factor of degree q^2-1 (see Equation (11)), where $q=p^e$. In this respect, we can see $\mathcal{F}/\mathbb{F}_{p^{3e}}$ as a variant of the tower given in [3]. It turns out that our tower contains the tower given by Bezerra Garcia and Stichtenoth in [5] as a subtower. The limit of our tower is the same as the limit of BaGS/$\mathbb{F}_{p^{3e}}$; i.e. it meets Zink's bound, but it has better p-rank properties. In particular we will show that its p-rank satisfies

$$\varphi(\mathcal{F}/\mathbb{F}_{p^{3e}}) \leq \frac{p^{2e}+p^e+4}{4(p^{2e}+p^e+1)},$$

and in fact equality holds in the case $e=1$ (see Theorem 4 and Remark 2). Note that for $e=1$, the p-rank of the new tower is significantly less than that of the tower BaGS/$\mathbb{F}_{p^3}$.

The article is organized as follows. First in the next section we give the necessary preliminaries concerning the computation of p-rank. After that we will in the third section introduce the new tower and compute its exact limit using previous work on related towers. While doing so we compute the exact genus of all the function fields occurring in the new tower and completely describe its ramification structure. In the fourth section, we compute the p-rank of the tower. The main effort there will be spent on computing the p-rank of the second function field in the tower. After that the p-rank of the tower will be computed using the Deuring–Shafarevich theorem and the ramification structure described in section 3.

2. Preliminaries

Let E/F be a finite separable extension of function fields with the same constant field. We denote by $\mathbb{P}(F)$ the set of places of F. For a place $Q \in \mathbb{P}(E)$ lying above a place $P \in \mathbb{P}(F)$, we write $Q|P$ and denote by $e(Q|P)$ the ramification index and by $d(Q|P)$ the different exponent of $Q|P$. The following formula is a crucial tool to compute the p-rank in p-extensions of function fields.

Theorem 1 (Deuring-Shafarevich [11])**.** *Let E/F be a Galois extension of function fields over an algebraically closed field of characteristic p. Suppose that the Galois group of the extension is a p-group. Then*

$$\gamma(E)-1=[E:F](\gamma(F)-1)+\sum_{P\in\mathbb{P}(F)}\sum_{\substack{Q\in\mathbb{P}(E)\\ Q|P}}(e(Q|P)-1)\ . \tag{1}$$

Using the Riemann-Hurwitz genus formula

$$2g(E)-2=[E:F](2g(F)-2)+\deg(\operatorname{Diff}(E/F))\ , \tag{2}$$

where $\mathrm{Diff}(E/F)$ is the different divisor of E/F, we can compute the values $\gamma(E)$ and $g(E)$ from Equations (1) and (2) once we have the following information.

(1) The degree $[E : F]$ of the field extension E/F
(2) The values $\gamma(F)$ and $g(F)$
(3) The ramification structure in E/F; i.e. $e(Q|P)$ and $d(Q|P)$ for any $Q \in \mathbb{P}(E)$ and $P \in \mathbb{P}(F)$ with $Q|P$

Computing the p-rank of a tower $\mathcal{F}/\mathbb{F}_q = (F_1 \subset F_2 \subset \cdots)$ of function fields is in general a difficult task. However, if each step F_{i+1}/F_i in the tower is Galois with a p-group as its Galois group, then the Deuring–Shafarevich theorem can be applied recursively in the tower. This requires knowing the exact ramification structure for each of the steps F_{i+1}/F_i. Moreover, it requires that the genus and p-rank of the "basis" function field F_1 are known. Some towers have this property [8, 4] and as mentioned in the introduction, for these the exact p-rank is known. Especially in [4], the main difficulty was to determine the p-rank of the basis function field. A similar phenomenon occurs in this paper. We will therefore need some tools for the p-rank computation of a specific function field.

The tool that we will use to compute the p-rank of a function field F with constant field $\mathbb{F}_q$ of characteristic p is to study the Cartier operator and its action on the space of regular differentials of F. Therefore we will briefly describe the main properties of the Cartier operator. Denote by Ω_F the space of differentials of F. If we fix a separating element $x \in F$, then each differential $\omega \in \Omega_F$ has a unique representation of the form

$$\omega = (z_0^p + z_1^p x + \cdots + z_{p-1}^p x^{p-1})dx \ ,$$

for some $z_0, z_1, ..., z_{p-1} \in F$. We then define the *Cartier operator* as a map $C : \Omega_F \to \Omega_F$ by

$$C(\omega) := z_{p-1}dx \ .$$

We refer to [10] for more information on the properties of the Cartier operator. For us it will be more convenient to use powers of the Cartier operator. The above definition implies directly the following [2, Lemma 4]. With notation as above, assume that

$$\omega = \left(\sum_{i=0}^{p^f-1} z_i^{p^f} x^i \right) dx \ ,$$

for some $z_0, \ldots, z_{p^f-1} \in F$. Then

$$C^f(\omega) = z_{p^f-1}dx \ .$$

Moreover, if $q = p^f$, then C^f acts $\mathbb{F}_q$-linear on the space of regular differentials. The relation between the p-rank $\gamma(F)$ of a function field F and the Cartier operator is the following.

Lemma 1. *Let F be a function field with genus $g(F)$ and constant field $\mathbb{F}_q$ of characteristic p. Suppose that $q = p^f$ and that there exists a basis of regular differentials such that with respect to this basis C^f is represented by a matrix with coefficients in $\mathbb{F}_p$. Then $g(F) - \gamma(F)$ is equal to the algebraic multiplicity of the eigenvalue zero of C^f under the action on the space of regular differentials of F.*

Proof. This lemma is implicit in [2]. More precisely, the statements in the lemma can directly be derived combining Lemma 3, Remark 5 and the first paragraph in the proof of Theorem 19 in [2]. □

Later on we will see that some special binomial coefficients occur as eigenvalues. Since we are working in characteristic p, it will be useful to have a tool to investigate binomial coefficients modulo a prime. The following classical lemma by Lucas [14] will be very useful.

Lemma 2 (Lucas)**.** *Let n and m be two non-negative integers and p be a prime number. Suppose that in base p the integers m and n are written as follows.*

$$n := n_0 + n_1 p + \cdots + n_l p^l$$

and

$$m := m_0 + m_1 p + \cdots + m_l p^l \ ,$$

with $0 \leq n_i, m_i \leq p-1$ for $0 \leq i \leq l$. Then

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\cdots\binom{n_l}{m_l} \mod p \ .$$

In particular, we see that $\binom{n}{m} \not\equiv 0 \mod p$ if and only if $m_i \leq n_i$ for all $i \in \{0, ..., l\}$.

In the remainder of the preliminary section, we collect and cite several facts from [5, 13, 6, 1] on a tower of function fields defined over a cubic field $\mathbb{F}_{q^3}$. This tower will be useful in later sections for computing the genera of the function fields in our new tower. We start by considering the function fields $Z_1 := \mathbb{F}_{q^3}(z_1)$ and $Z_2 := \mathbb{F}_{q^3}(z_1, z_2)$, where

$$(z_2 - 1)^{q+1} + \frac{z_1 - 1}{z_1}(z_2 - 1)^q - \left(\frac{z_1 - 1}{z_1}\right)^{q+1} z_2 = 0 \ . \tag{3}$$

From (the proof of) Lemma 3 in [1], we cite that the only ramified places of Z_1 in Z_2/Z_1 are $(z_1 = 0)$ and $(z_1 = \infty)$. More precisely, the following holds:

Lemma 3. *Let $Z_2 = \mathbb{F}_{q^3}(z_1, z_2)$ be the function field defined by Equation (3). Then we have:*

(i) *There is a unique place P of Z_2 lying over $(z_1 = \infty)$, which is totally ramified.*

(ii) *There are two places of Z_2 lying over $(z_1 = 0)$, say P_1 and P_2, with $e(P_1|(z_1 = 0)) = 1$ and $e(P_2|(z_1 = 0)) = d(P_2|(z_1 = 0)) = q$.*

The first part implies in particular that Equation (3) is absolutely irreducible. It is also shown in [1] that there exists an element $\alpha_0 \in Z_2$, namely

$$\alpha_0 := \frac{1 - z_1 z_2}{z_1 - 1} \ , \tag{4}$$

such that $Z_2 = \mathbb{F}_{q^3}(\alpha_0)$. Moreover, the elements z_1 and z_2 can be expressed in α_0 as follows

$$z_1 = -\frac{1 + \alpha_0}{\alpha_0^{q+1}} \quad \text{and} \quad z_2 = -(\alpha_0 + \alpha_0^{q+1}) \ .$$

With this change of variables, the ramified places P, P_1 and P_2 of Z_2 can be given as

$$P = (\alpha_0 = 0) \ , \ \ P_1 = (\alpha_0 = -1) \ , \ \text{ and } \ P_2 = (\alpha_0 = \infty) \ . \tag{5}$$

We now wish to define a tower $\mathcal{Z}/\mathbb{F}_{q^3} = (Z_1 \subset Z_2 \subset \cdots)$, where for $n \geq 1$, $Z_{n+1} := Z_n(z_{n+1})$ and the quantities z_n satisfy the recursive equation

$$(z_{n+1} - 1)^{q+1} + \frac{z_n - 1}{z_n}(z_{n+1} - 1)^q - \left(\frac{z_n - 1}{z_n}\right)^{q+1} z_{n+1} = 0 \ . \tag{6}$$

However, it turns out that this recursion does not determine the tower uniquely. We will describe in detail what happens and then define the tower $\mathcal{Z}/\mathbb{F}_{q^3}$ uniquely. Similarly as for Z_2, for each $n > 1$ there exist variables α_{n-1} such that $\mathbb{F}_{q^3}(z_n, z_{n+1}) = \mathbb{F}_{q^3}(\alpha_{n-1})$ and

$$z_n = -\frac{1 + \alpha_{n-1}}{\alpha_{n-1}^{q+1}} \quad \text{and} \quad z_{n+1} = -(\alpha_{n-1} + \alpha_{n-1}^{q+1}) \ . \tag{7}$$

Considering $Z_3 = \mathbb{F}_{q^3}(z_1, z_2, z_3)$, we conclude that $Z_3 = \mathbb{F}_{q^3}(\alpha_0, \alpha_1)$ and that α_1 is a root of the polynomial

$$T^{q+1} - \frac{1}{\alpha_n^{q+1} + \alpha_n} T - \frac{1}{\alpha_n^{q+1} + \alpha_n} \ ; \tag{8}$$

if we set $n = 0$. This polynomial has a linear factor; namely

$$T + \frac{1}{\alpha_n + 1} \tag{9}$$

and an absolutely irreducible factor of degree q [6]. Using the degree q factor, one can define recursively $A_0 := \mathbb{F}_{q^3}(\alpha_0)$ and $A_n := A_{n-1}(\alpha_n)$ and obtain the tower $\mathcal{A}/\mathbb{F}_{q^3} = (A_0 \subset A_1 \subset \cdots)$ studied in [6] (or to be very precise: the dual of the tower studied there). We can now also uniquely define the tower $\mathcal{Z}/\mathbb{F}_{q^3} = (Z_1 \subset Z_2 \subset \cdots)$ using Equation (7) by $Z_n := \mathbb{F}_{q^3}(z_1, \ldots, z_n)$. Note that $Z_{n+2} = A_n$ for all $n \geq 0$, so the towers $\mathcal{Z}/\mathbb{F}_{q^3}$ and $\mathcal{A}/\mathbb{F}_{q^3}$ are essentially the same. Moreover as observed in [6], it is also the same as a tower given by Ihara [13] as a subtower of a tower given by Bezerra, Garcia and Stichtenoth [5]. As a result, the genera $g(A_n)$ of the function fields A_n in $\mathcal{A}/\mathbb{F}_{q^3}$ are given as follows.

Lemma 4. *Let $\mathcal{A}/\mathbb{F}_{q^3} = (A_0 \subset A_1 \subset \cdots)$ be the sequence of function fields defined as above. Then for all $n \geq 0$ the following holds:*

(i) A_{n+1}/A_n is a separable extension of degree q.
(ii) $\mathbb{F}_{q^3}$ is the full constant field of A_n.
(iii) The genus $g(A_n)$ of A_n is given as follows.

If $n \equiv 0 \mod 4$, then

$$g(A_n) = \frac{1}{2(q-1)}\left(q^{n+1} + 2q^n - 2q^{\frac{n+2}{2}} - 2q^{\frac{n}{2}} + q\right) - \frac{n}{4}q^{\frac{n-2}{2}}(q+1).$$

If $n \equiv 2 \mod 4$, then

$$g(A_n) = \frac{1}{2(q-1)}\left(q^{n+1} + 2q^n - 4q^{\frac{n+2}{2}} + q\right) - \frac{n-2}{4}q^{\frac{n-2}{2}}(q+1).$$

If $n \equiv 1 \mod 2$, then

$$g(A_n) = \frac{1}{2(q-1)}\left(q^{n+1} + 2q^n - q^{\frac{n+3}{2}} - 3q^{\frac{n+1}{2}} + q\right) - \frac{n-1}{2}q^{\frac{n-1}{2}}.$$

Proof. See [6] and Theorem 2.9 in [5]. □

The precise ramification structure of the tower $\mathcal{A}/\mathbb{F}_{q^3}$ has been determined in [6] and is restated for future reference in the following lemma.

Lemma 5. *Let $\mathcal{A}/\mathbb{F}_{q^3} = (A_0 \subset A_1 \subset \cdots)$ be the sequence of function fields defined as above. Further let Q be a place of A_n and P_i be the restriction of Q to $\mathbb{F}_{q^3}(\alpha_i)$; i.e. $P_i = Q \cap \mathbb{F}_{q^3}(\alpha_i)$, for all $i = 0, \ldots, n$. Then the following holds:*

If $P_i = (\alpha_i = -1)$ then $P_{i+1} = (\alpha_{i+1} = -1)$ or $P_{i+1} = (\alpha_{i+1} = \infty)$. In the first case, P_i is unramified in $\mathbb{F}_{q^3}(\alpha_i, \alpha_{i+1})/\mathbb{F}_{q^3}(\alpha_i)$ and P_{i+1} is totally ramified in $\mathbb{F}_{q^3}(\alpha_i, \alpha_{i+1})/\mathbb{F}_{q^3}(\alpha_{i+1})$ with different exponent q. However in the second case, both P_i and P_{i+1} ramified with ramification index $q-1$ in $\mathbb{F}_{q^3}(\alpha_i, \alpha_{i+1})/\mathbb{F}_{q^3}(\alpha_i)$ and $\mathbb{F}_{q^3}(\alpha_i, \alpha_{i+1})/\mathbb{F}_{q^3}(\alpha_{i+1})$, respectively.

If $P_i = (\alpha_i = \infty)$ then $P_{i+1} = (\alpha_{i+1} = 0)$. In this case, both P_i and P_{i+1} are unramified in $\mathbb{F}_{q^3}(\alpha_i, \alpha_{i+1})/\mathbb{F}_{q^3}(\alpha_i)$ and $\mathbb{F}_{q^3}(\alpha_i, \alpha_{i+1})/\mathbb{F}_{q^3}(\alpha_{i+1})$, respectively.

If $P_i = (\alpha_i = 0)$ then $P_{i+1} = (\alpha_{i+1} = \infty)$. Further, P_i is totally ramified in $\mathbb{F}_{q^3}(\alpha_i, \alpha_{i+1})/\mathbb{F}_{q^3}(\alpha_i)$ with different exponent q and P_{i+1} is unramified in $\mathbb{F}_{q^3}(\alpha_i, \alpha_{i+1})/\mathbb{F}_{q^3}(\alpha_{i+1})$.

In particular, we see that there are four types of sequences $(P_i)_{i\geq 0}$, with ramification structure as indicated in Figure 1.

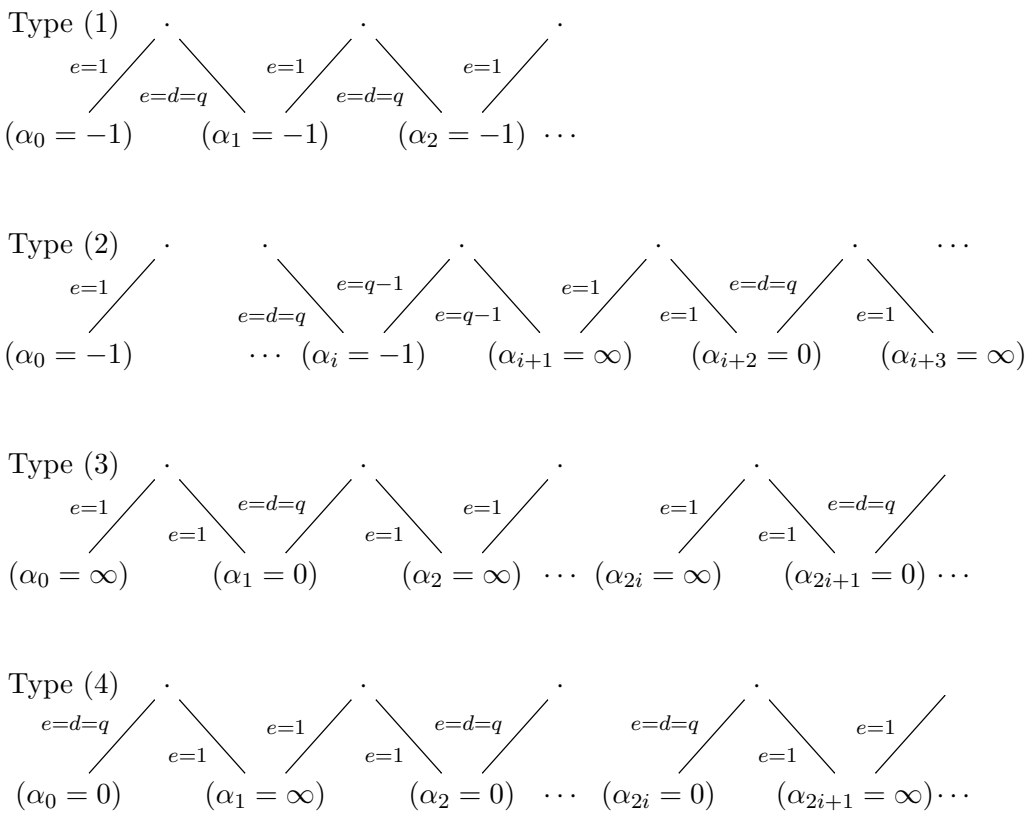

FIGURE 1. Ramification Structure of $\mathcal{A}$.

3. The new tower

We will now introduce a new tower over cubic finite fields. In this section we investigate the genera of the function fields in the tower as well as its limit and ramification structure. The new tower is a variation of a class of towers introduced in [3]. In particular a class of towers was given with function fields $(\mathbb{F}_{q^e}(x_1, \ldots, x_n))_{n\geq 1}$ whose variables for $n \geq 1$ satisfy the

following recursive equation

$$\frac{x_{n+1}^{q^e-1}-1}{x_{n+1}^{q^j-1}} = \frac{x_n^{q^e-1}-1}{x_n^{q^e-q^{e-j}}} \ .$$

These equations were explained using the theory of Drinfeld modules and turn out not to be irreducible in general. The towers studied in [3] correspond to choosing specific factors. Whereas for $e > 2$ the resulting towers in [3] will not have Galois steps, we will see that for $e = 3$ by choosing different factors, one can obtain a tower $\mathcal{F}/\mathbb{F}_{q^3} = (F_1 \subset F_2 \subset \cdots)$ with Galois steps. While $F_1 := \mathbb{F}_{q^3}(x_1)$, the other function fields will need to be described carefully.

3.1. **The defining equations of the new tower:** For $e = 3$ and $j = 2$, the equation given above reduces to

$$\frac{x_{n+1}^{q^3-1}-1}{x_{n+1}^{q^2-1}} = \frac{x_n^{q^3-1}-1}{x_n^{q^3-q}} \ . \tag{10}$$

However Equation (10) is not irreducible. More precisely,

$$\begin{aligned} X^{q^3-q}(Y^{q^3}-Y) - (X^{q^3-1}-1)Y^{q^2} &= (X^{q^2-1}Y^{q^2} + Y^q + X^{q^2-q}Y)^q \\ &\quad - X^{q^3-q^2}(X^{q^2-1}Y^{q^2} + Y^q + X^{q^2-q}Y) \ ; \end{aligned}$$

and hence

$$\begin{aligned} &X^{q^3-q}(Y^{q^3}-Y) - (X^{q^3-1}-1)Y^{q^2} \\ &\qquad = \prod_{\alpha\in\mathbb{F}_q} (X^{q^2-1}Y^{q^2} + Y^q + X^{q^2-q}Y - \alpha X^{q^2}) \\ &\qquad = Y(X^{q^2-1}Y^{q^2-1} + Y^{q-1} + X^{q^2-q})\times \\ &\qquad\quad \prod_{\alpha\in\mathbb{F}_q\setminus\{0\}} (X^{q^2-1}Y^{q^2} + Y^q + X^{q^2-q}Y - \alpha X^{q^2}) \ . \end{aligned} \tag{11}$$

For the construction of the second function field F_2 of $\mathcal{F}/\mathbb{F}_{q^3}$ we consider the factor, which has Y-degree q^2-1. Items (i) and (ii) from the following proposition imply that this factor is absolutely irreducible.

Proposition 1. *Let $F_2 = \mathbb{F}_{q^3}(x_1, x_2)$ be an extension of the rational function field $\mathbb{F}_{q^3}(x_1)$ such that x_1 and x_2 satisfy*

$$x_1^{q^2-1}x_2^{q^2-1} + x_2^{q-1} + x_1^{q^2-q} = 0 \ . \tag{12}$$

Then the following holds.

(i) *The extension degree $[F_2 : \mathbb{F}_{q^3}(x_1)]$ is q^2-1.*
(ii) *$\mathbb{F}_{q^3}$ is the full constant field of F_2.*
(iii) *The genus $g(F_2)$ of F_2 is $(q^4-q^3-4q+6)/2$.*

Proof. We multiply Equation (12) by $x_2/x_1^{q^2}$ to obtain that

$$\frac{x_2^{q^2}}{x_1} + \frac{x_2^q}{x_1^{q^2}} + \frac{x_2}{x_1^q} \;=\; \frac{x_2^{q^2}}{x_1} + \left(\frac{x_2}{x_1^q}\right)^q + \frac{x_2}{x_1^q} = 0 \ .$$

This implies that for $\alpha \in \mathbb{F}_{q^3}\backslash\{0\}$ the place $(x_1 = \alpha)$ splits completely in the extension $F_2/\mathbb{F}_{q^3}(x_1)$, since the equation

$$0 = \frac{x_2^{q^2}}{\alpha} + \left(\frac{x_2}{\alpha^q}\right)^q + \frac{x_2}{\alpha^q} = \left(\frac{x_2}{\alpha^q}\right)^{q^2} + \left(\frac{x_2}{\alpha^q}\right)^q + \frac{x_2}{\alpha^q}$$

has q^2 distinct solutions for x_2 in $\mathbb{F}_{q^3}$. This implies item *(ii)*.

Moreover, if we set $R := x_2/x_1^q$ and $S := x_2^{q^2}/x_1$, then the following equalities hold.

$$z_1 := x_1^{q^3-1} = \frac{S}{R^{q^2}} = -\frac{R^q + R}{R^{q^2}} = -\frac{R^{q-1}+1}{R^{q^2-1}} \ .$$

Since $F_2 = \mathbb{F}_{q^3}(x_1, R)$, we can write F_2 as the compositum of $\mathbb{F}_{q^3}(x_1)$ and $\mathbb{F}_{q^3}(R)$. Note that $\mathbb{F}_{q^3}(x_1)/\mathbb{F}_{q^3}(z_1)$ is a Kummer extension and therefore in particular a tame extension. The only ramified places of $\mathbb{F}_{q^3}(z_1)$ in this extension are $(z_1 = 0)$ and $(z_1 = \infty)$ both with ramification index $q^3 - 1$. To compute the ramification in $F/\mathbb{F}_{q^3}(x_1)$ we only need to find the ramification behaviour in the extension $\mathbb{F}_{q^3}(R)/\mathbb{F}_{q^3}(z_1)$. To investigate the ramification it will be convenient to extend the constant field to $\mathbb{F} := \overline{\mathbb{F}}_{q^3}$.

The minimal polynomial $p(T)$ of R over $\mathbb{F}(z_1)$ is equal to

$$p(T) = T^{q^2-1} + \frac{1}{z_1}T^{q-1} + \frac{1}{z_1} \ .$$

For $\alpha \in \mathbb{F} \setminus \{0\}$, we denote by $p_\alpha(T)$ the polynomial given by

$$p_\alpha(T) = T^{q^2-1} + \frac{1}{\alpha}T^{q-1} + \frac{1}{\alpha} \ .$$

We observe that $p_\alpha(T)$ and its derivative $p'_\alpha(T)$ cannot have a common zero in $\mathbb{F}$. This implies that none of the places $P \in \mathbb{P}(\mathbb{F}(z_1))$ other than $(z_1 = 0)$ and $(z_1 = \infty)$ ramify in $\mathbb{F}(R)/\mathbb{F}(z_1)$. From the defining equation of $\mathbb{F}(R)$ over $\mathbb{F}(z_1)$; i.e. $z_1 = -(R^{q-1}+1)/R^{q^2-1}$, we see that the following holds.

(a) Set $\mathcal{B} := \{\beta \in \mathbb{F} \mid \beta^{q-1} + 1 = 0\}$. There are q places of $\mathbb{F}(R)$ lying over $(z_1 = 0)$; namely $(R = \beta)$ for $\beta \in \mathcal{B}$ each of them satisfying $e((R = \beta)|(z_1 = 0)) = 1$ and $(R = \infty)$ with $e((R = \infty)|(z_1 = 0)) = q^2 - q$.

(b) $(R = 0)$ is the unique place lying over $(z_1 = \infty)$. In particular, $e((R = 0)|(z_1 = \infty)) = q^2 - 1$.

Let Q be a place of F_2 lying over $(R = \beta)$ for some $\beta \in \mathcal{B}$. Then by Abhyankar's lemma we can conclude that Q is ramified in $F_2/\mathbb{F}(R)$ with $e(Q|(R = \beta)) = q^3 - 1$. This implies that the extension degree F_2 over $\mathbb{F}(R)$

is equal to q^3-1. Equivalently, we can conclude that the extension degree F_2 over $\mathbb{F}(x_1)$ is q^2-1, which proves item *(i)*.

Now we compute the genus of F_2 using the Riemann-Hurwitz genus formula applied to the extension $F_2/\mathbb{F}(R)$. We have already established that the ramified places of F_2 other than the ones lying over $(R=\beta)$ for $\beta \in \mathcal{B}$, which are totally ramified in $F_2/\mathbb{F}(R)$, can only lie over the places $(R=\infty)$ and $(R=0)$. Let Q_1 and Q_2 be places of F_2 lying over $(R=\infty)$ and $(R=0)$, respectively. Then by Abhyankar's lemma we deduce that $e(Q_1|(R=\infty)) = e(Q_2|(R=0)) = q^2+q+1$. Since $[F_2:\mathbb{F}(R)] = q^3-1$, we also deduce that there are $q-1$ possibilities for Q_1 as well as for Q_2. Then $2g(F_2)-2$ is given by

$$(q^3-1)(-2)+(q-1)(q^3-2)+(q-1)(q^2+q)+(q-1)(q^2+q)\ .$$

Item *(iii)* now follows. □

The equation

$$X^{q^2-1}Y^{q^2-1}+Y^{q-1}+X^{q^2-q} = \frac{X^{q^2-1}}{Y}\left(Y^{q^2}+\frac{Y^q}{X^{q^2-1}}+\frac{Y}{X^{q-1}}\right)\ .$$

was used to define $F_2 = \mathbb{F}_{q^3}(x_1,x_2)$, but using the same equation to recursively define $F_3 = F_2(x_3)$ is somewhat subtle. The reason is that over F_2 we have the following factorization.

$$\begin{aligned} x_3^{q^2}+\frac{x_3^q}{x_2^{q^2-1}}+\frac{x_3}{x_2^{q-1}} &= \left(x_3^q-\frac{x_3}{(x_1x_2)^{q-1}}\right)^q - x_1^{q-1}\left(x_3^q-\frac{x_3}{(x_1x_2)^{q-1}}\right) \\ &= \prod_{\alpha\in\mathbb{F}_q}\left(x_3-\frac{\alpha}{x_1x_2}\right)\prod_{\alpha\in\mathbb{F}_q\setminus\{0\}}\left(x_3^q-\frac{x_3}{(x_1x_2)^{q-1}}-\alpha x_1\right)\ . \end{aligned}$$

Fortunately, we can choose any of the degree q factors to define $F_3 = F_2(x_3)$. Moreover any choice gives rise to the same extension, since for any element $\alpha \in \mathbb{F}_q \setminus \{0\}$ we have

$$x_3^q-\frac{x_3}{(x_1x_2)^{q-1}}-\alpha x_1 = x_3^q-\frac{x_3}{(\alpha x_1x_2)^{q-1}}-\alpha x_1\ .$$

For convenience we will assume that for $n>1$ we have

$$x_{n+1}^q-\frac{x_{n+1}}{(x_{n-1}x_n)^{q-1}}-x_{n-1}=0\ . \tag{13}$$

In principle, this equation could be reducible over F_n for some $n\geq 2$ (though we later will see that this does not happen). In either case, Equation (13) gives rise to an Artin–Schreier polynomial, thus defines an Artin–Schreier extension of F_n. Therefore, it is either absolutely irreducible, or it factors completely, in which case F_{n+1} would be equal to F_n. Regardless of what

happens, we can uniquely define a tower of function fields by $F_1 := \mathbb{F}_{q^3}(x_1)$, $F_2 := \mathbb{F}_{q^3}(x_1, x_2)$ as in Proposition 1 and for $n \geq 2$ $F_{n+1} := F_n(x_{n+1})$, with x_{n+1} satisfying Equation (13). In the following lemma, we will see that Equation (13) in fact for $n = 2$ defines an Artin–Schreier extension $F_3 = F_2(x_3)$ of F_2 of degree q. Later on we will see that also for all $n \geq 3$, the extension degree $[F_{n+1} : F_n]$ equals q.

Lemma 6. *The polynomial $T^q - T/(x_1x_2)^{q-1} - x_1$ is absolutely irreducible over F_2.*

Proof. As we consider the absolute irreducibility of a polynomial, we can continue to assume that F_2 is a function field with the full constant field $\mathbb{F} = \overline{\mathbb{F}}_{q^3}$. With the same notation as in the proof of Proposition 1, we have $Q_1 \cap \mathbb{F}(x_1) = (x_1 = 0)$ and $Q_2 \cap \mathbb{F}(x_1) = (x_1 = \infty)$. We use the transitivity of ramification index and the transitivity of different exponent to conclude that

$$e(Q_1|(x_1 = 0)) = q\,,\ e(Q_2|(x_1 = \infty)) = q{+}1 \text{ and } d(Q_1|(x_1 = 0)) = q^3{+}q{-}2\,.$$

We now count the number of ramified places lying over $(x_1 = \infty)$ and $(x_1 = 0)$. Since any place Q of F_2 lying over $(x_1 = \infty)$ lies over $(R = 0)$ with ramification index $e(Q|(x_1 = \infty)) = q{+}1$, we conclude by Fundamental Equality (see [16], Theorem 3.1.11) that there are $q - 1$ places lying over $(x_1 = \infty)$, say $Q_{1\ell}$ for $\ell = 1, \ldots, q - 1$. Now suppose that Q is a place of F_2 lying over $(x_1 = 0)$. We note that there exist $q - 1$ places of F_2 lying over $(R = \beta)$ for $\beta \in \mathcal{B}$, which are not ramified in $F_2/\mathbb{F}(x_1)$. We denote by Q_β the unique place of F_2 lying over $(R = \beta)$. On the other hand, any place of F_2 lying over the place $(R = \infty)$ ramifies with ramification index q and different exponent $q^3 + q - 2$. From Fundamental Equality, we conclude that there are $q - 1$ places of F_2 lying over $(x_1 = 0)$, which are ramified, say $Q_{2\ell}$ for $\ell = 1, \ldots, q - 1$. Then we can give the principal divisors of x_1 and R in F_2 as follows:

$$(x_1) = \sum_{\beta\in\mathcal{B}} Q_\beta + q\sum_{\ell=1}^{q-1} Q_{1\ell} - (q+1)\sum_{\ell=1}^{q-1} Q_{2\ell}$$

$$(R) = (q^2+q+1)\sum_{\ell=1}^{q-1} Q_{2\ell} - (q^2+q+1)\sum_{\ell=1}^{q-1} Q_{1\ell}\ .$$

Denote by v_i the valuation at the place Q_{2i} for some $i \in \{1, \ldots, q-1\}$. Now we substitute T by $T/(x_1x_2)$ in $T^q - T/(x_1x_2)^{q-1} - x_1$ and then multiply the polynomial by $(x_1x_2)^q$ to obtain $T^q - T - x_1^{q+1}x_2^q$. It is enough to show that the Artin-Schreier polynomial $T^q - T - x_1^{q+1}x_2^q$ is absolutely irreducible.

However this comes from the valuation of $x_1^{q+1}x_2^q$ at the place Q_{2i} for some $i \in \{1, \ldots, q-1\}$ (see [16], Proposition 3.7.8) since

$$v_i(x_1^{q+1}x_2^q) = v_i(x_1^{q^2+q+1}R^q) = -(q^2+q+1) \ ,$$

where $R = x_2/x_1^q$. □

We will now establish a relation between the tower $\mathcal{F}/\mathbb{F}_{q^3}$ and a known cubic tower $\mathcal{Z}/\mathbb{F}_{q^3} = (Z_1 \subset Z_2 \subset \cdots)$ described in Section 2. Using this relation, we will show that indeed $\mathcal{F}/\mathbb{F}_{q^3}$ is a tower.

Theorem 2. *Let $\mathcal{F}/\mathbb{F}_{q^3} = (F_1 \subset F_2 \subset \cdots)$ be the sequence of function fields given by $F_1 = \mathbb{F}_{q^3}(x_1)$ and $F_{n+1} = F_n(x_{n+1})$ where*

$$x_1^{q^2-1}x_2^{q^2-1} + x_2^{q-1} + x_1^{q^2-q} = 0 \quad \text{and} \quad x_{n+1}^q - \frac{x_{n+1}}{(x_{n-1}x_n)^{q-1}} = x_{n-1} \ , \tag{14}$$

for $n \geq 2$. Then $\mathcal{F}/\mathbb{F}_{q^3}$ is a tower.

Proof. We introduce $z_n := x_n^{q^3-1}$ for $n > 0$, and define $Z_n := \mathbb{F}_{q^3}(z_1, \ldots, z_n)$. It can easily be seen from Equation (10) that the z_n satisfy the following recursive equation

$$\frac{(z_{n+1}-1)^{q^2+q+1}}{z_{n+1}^{q+1}} = \frac{(z_n-1)^{q^2+q+1}}{z_n^{q^2+q}} \ .$$

In [1] it was shown that this equation (seen as a function in two independent variables) has two absolutely irreducible factors, one of degree $q+1$ and one of degree q^2. The one of degree $q+1$ is the following:

$$(z_{n+1}-1)^{q+1} + \frac{z_n-1}{z_n}(z_{n+1}-1)^q - \left(\frac{z_n-1}{z_n}\right)^{q+1} z_{n+1} = 0 \ .$$

Note that this is exactly Equation (6). Now we show that z_1 and z_2 cannot satisfy an irreducible equation of degree q^2 in z_2. If that would be the case, then the extension degree $[F_2 : Z_1]$ would be divisible by q^2. However this is not possible since by Proposition 1 we have

$$[F_2 : Z_1] = [F_2 : F_1] \cdot [F_1 : Z_1] = (q^2-1)(q^3-1) \ .$$

From this we conclude that $[F_2 : Z_2] = [F_2 : Z_1]/[Z_2 : Z_1] = (q-1)(q^3-1)$.

We have seen in the discussion after Equation (8) that $[Z_3 : Z_2]$ equals either 1 or q. Since $F_3 = Z_3(x_1, x_2, x_3)$ is a multiple Kummer extension (given by $x_i^{q^3-1} = z_i$), its degree is a divisor of $(q^3-1)^3$. Hence the degree $[F_3 : Z_3]$ is relatively prime to q.

If $[Z_3 : Z_2] = 1$, then on the one hand the extension degree $[F_3 : Z_2] = [F_3 : Z_3]$ is relatively prime to q. But, on the other hand we know by Lemma

6 that $[F_3 : F_2] = q$, which implies that the degree $[F_3 : Z_2]$ is divisible by q, since

$$[F_3 : Z_2] = [F_3 : F_2][F_2 : Z_2] = q(q-1)(q^3-1) \ .$$

Hence we conclude that $[Z_3 : Z_2] = q$ and $[F_3 : Z_3] = (q-1)(q^3-1)$. This equivalently means that the tower $\mathcal{Z}/\mathbb{F}_{q^3}$ can be defined first using Equation (6) for $n = 1$ and afterwards for $n \geq 2$ recursively by the degree q factor of Equation (6). As a result we see that the tower $\mathcal{Z}/\mathbb{F}_{q^3}$ is indeed the tower $\mathcal{Z}/\mathbb{F}_{q^3}$ from Section 2. In particular, we then have that $[Z_{n+1} : Z_n] = q$ for all $n \geq 2$. As $\mathcal{Z}/\mathbb{F}_{q^3}$ is a subtower of $\mathcal{F}/\mathbb{F}_{q^3}$ and F_{n+1} is the compositum $F_n \cdot Z_{n+1}$ of F_n and Z_{n+1} for all $n \geq 2$, by comparing degrees we conclude the following using induction:

$$[F_{n+1} : F_n] = q \ \text{ and } \ [F_{n+1} : Z_{n+1}] = (q-1)(q^3-1) \text{ for all } n \geq 2.$$

Furthermore we know that any extension Z_{n+1}/Z_n contains a totally ramified place for $n \geq 2$ (see Figure 1), which by Abhyankar's lemma (since all ramification in the multiple Kummer extension F_n/Z_n is tame) shows the existence of a totally ramified place in the extension F_{n+1}/F_n for $n \geq 2$. In particular, this shows that Equation (13) is absolutely irreducible for all $n \geq 2$ and hence that $\mathbb{F}_{q^3}$ is the full constant field of F_n for any $n \geq 2$. All in all we have shown that $\mathcal{F}/\mathbb{F}_{q^3}$ is indeed a tower defined over $\mathbb{F}_{q^3}$. □

Remark 1. Combining Lemma 3 with the ramification behaviour in the proof of Proposition 1, it is not hard to see that the ramification in the extension F_2/Z_2 is as follows:

$$e(Q|Q \cap Z_2) = e(Q_1|Q_1 \cap Z_2) = e(Q_2|Q_2 \cap Z_2) = q^3 - 1 \ .$$

Moreover, each of Q, Q_1 and Q_2 can be chosen in $q-1$ distinct ways.

3.2. **Genus and limit of the new tower:** We now compute the exact genera of the function fields in the tower $\mathcal{F}/\mathbb{F}_{q^3}$. Using this, we will determine the limit of $\mathcal{F}/\mathbb{F}_{q^3}$ as well. Since the exact genus of each function field $A_n = Z_{n+2}$ is known by Lemma 4, our approach in the following proposition is to compute the exact genus of F_n by using the Riemann-Hurwitz genus formula for the extension F_n/Z_n.

Proposition 2. *Let $\mathcal{F}/\mathbb{F}_{q^3} = (F_1 \subset F_2 \subset \cdots)$ be the tower of function fields given by Equation 14 in Theorem 2. Then*

$$g(F_n) = 1 + (q-1)\frac{(q^2+q+1)(q+2)q^{n-2} - (q+1)q^2 - r_n}{2} \ ,$$

with

(i) *For* $n = 2k + 3$ *and* $k \geq 0$,

$$r_n = \left((2k+1)q^3 + 2q^2 + 5q - 2k + 2\right) q^k.$$

(ii) *For* $n = 2k + 2$, $k \equiv 0 \pmod 2$ *and* $k \geq 0$,

$$r_n = \left((k-1)q^4 + (k+2)q^3 + 3q^2 - (k-6)q - k\right) q^{k-1}.$$

(iii) *For* $n = 2k + 2$, $k \equiv 1 \pmod 2$ *and* $k > 0$,

$$r_n = \left(kq^4 + (k+1)q^3 + 3q^2 - (k-5)q - (k-1)\right) q^{k-1}.$$

Proof. As we are interested in the genus of a function field, we can without loss of generality extend the field of constants to $\mathbb{F} := \overline{\mathbb{F}}_{q^3}$. The facts that F_{n+2} is the compositum of F_2 and A_n over A_0, and that the extension degree q^n of F_{n+2}/F_2 is relatively prime to the extension degree $(q-1)(q^3-1)$ of F_2/A_0 for each $n \geq 0$ imply that a place Q of A_n is ramified in F_{n+2}/A_n if and only if $Q \cap A_0$ is ramified in F_2/A_0. Equivalently, this holds if and only if Q lies over a place of A_0 in the set $\{(\alpha_0 = \infty), (\alpha_0 = 0), (\alpha_0 = -1)\}$ (see Figure 1).

We differentiate the investigation of the ramified places of A_n in the extension F_{n+2}/A_n into three cases.

Case (1): Let Q be a place of A_n lying over the set $\{(\alpha_0 = \infty), (\alpha_0 = 0)\}$. Using Figure 1, we see that $(\alpha_0 = \infty)$ and $(\alpha_0 = 0)$ ramify and split in an alternating way in the tower $\mathcal{A}/\mathbb{F}$. By induction, we show that there are $q^{k+1} + q^k$ places of A_n if $n = 2k+1$, and there are $2q^k$ places of A_n if $n = 2k$ lying over $\{(\alpha_0 = \infty), (\alpha_0 = 0)\}$. By Remark 1 for each place of A_n lying over $\{(\alpha_0 = \infty), (\alpha_0 = 0)\}$ there are $q-1$ places of F_{n+2} lying over it, all with ramification index $q^3 - 1$. All in all this gives a contribution to the different $\mathrm{Diff}(F_{n+2}/A_n)$ of degree $(q^{k+1} + q^k)(q-1)(q^3-2)$ if $n = 2k+1$ and of degree $2q^k(q-1)(q^3-2)$ if $n = 2k$.

Case (2): There is a unique place Q of A_n lying over $(\alpha_0 = -1)$ with $Q \cap \mathbb{F}(\alpha_i) = (\alpha_i = -1)$ for all $i = 0, \ldots, n$. Since $(\alpha_0 = -1)$ is ramified with ramification index $q^3 - 1$ in the extension $F_2/Z_2 = F_2/A_0$ and it is unramified in A_n/A_0 (see Figure 1), by Abhyankar's lemma we can conclude that the ramification index of a place of F_{n+2} lying over Q is equal to $q^3 - 1$. Hence there are $q-1$ places lying over Q each with ramification index $q^3 - 1$ in F_{n+2}/A_n. All in all this gives a contribution to $\mathrm{Diff}(F_{n+2}/A_n)$ of degree $(q-1)(q^3-2)$.

Case (3): From Remark 1 and Abhyankar's lemma we conclude that for each place Q of A_n lying over $(\alpha_0 = -1)$ other than the one from Case (2), the ramification index in the extension F_{n+2}/A_n is equal to $q^2 + q + 1$ and hence there are $(q-1)^2$ places of F_{n+2} lying over Q. Note that for any $i \geq 0$

the place $(\alpha_i = -1)$ of $\mathbb{F}(\alpha_i)$ splits into two places R_1 and R_2 in $\mathbb{F}(\alpha_i, \alpha_{i+1})$ with $e((\alpha_i = -1)|R_1) = 1$ and $e((\alpha_i = -1)|R_2) = q - 1$ (see Lemma 5). In fact R_1 and R_2 are the places of $\mathbb{F}(\alpha_i, \alpha_{i+1})$ lying over $(\alpha_{i+1} = -1)$ and $(\alpha_{i+1} = \infty)$, respectively. The precise ramification behaviour in the tower $\mathcal{A}/\mathbb{F}$ is complicated, but was settled completely in [5, 6]. Using their results one can directly determine the number of places of A_n lying above $(\alpha_0 = -1)$ not occurring in Case (2). For $n = 2k + 1$ this number equals $2(q^{k+1} - 1)/(q - 1) - 1$, while if $n = 2k$ we have $q^k + 2(q^k - 1)/(q - 1) - 1$ such places. This gives a contribution to $\mathrm{Diff}(F_{n+2}/A_n)$ of degree

$$(2(q^{k+1} - 1)(q - 1) - (q - 1)^2)(q^2 + q) = (2q^{k+1} - q - 1)(q^3 - q)$$

if $n = 2k + 1$, and of degree

$$(q^k(q-1)^2 + 2(q^k - 1)(q-1) - (q-1)^2)(q^2+q) = (q^{k+1} + q^k - q - 1)(q^3 - q)$$

if $n = 2k$.

Adding all contributions we calculate the degree of the different divisor $\mathrm{Diff}(F_{n+2}/A_n)$ of F_{n+2}/A_n.

$$\begin{aligned} \deg(\mathrm{Diff}(F_{2k+3}/A_{2k+1})) &= (q^{k+1} + q^k)(q-1)(q^3-2) + (q-1)(q^3-2) \\ &\quad +(2q^{k+1} - q - 1)(q^3 - q) \\ &= (q-1)(q^{k+4} + 3q^{k+3} + 2q^{k+2} - 2q^{k+1} - 2q^k) \\ &\quad -(q-1)(2q^2 + q + 2) \end{aligned} \tag{15}$$

$$\begin{aligned} \deg(\mathrm{Diff}(F_{2k+2}/A_{2k})) &= 2q^k(q-1)(q^3-2) + (q-1)(q^3-2) \\ &\quad +(q^{k+1} + q^k - q - 1)(q^3 - q) \\ &= (q-1)(3q^{k+3} + 2q^{k+2} + q^{k+1} - 4q^k) \\ &\quad -(q-1)(2q^2 + q + 2)\ . \end{aligned}$$

Then by the Riemann-Hurwitz genus formula together with Lemma 4 we obtain the desired result. □

Theorem 3. *Let $\mathcal{F}/\mathbb{F}_{q^3} = (F_1 \subset F_2 \subset \cdots)$ be the tower of function fields given by $F_1 = \mathbb{F}_{q^3}(x_1)$ and $F_{n+1} = F_n(x_{n+1})$ where*

$$x_1^{q^2-1}x_2^{q^2-1} + x_2^{q-1} + x_1^{q^2-q} = 0 \quad \textit{and} \quad x_{n+1}^q - \frac{x_{n+1}}{(x_{n-1}x_n)^{q-1}} = x_{n-1}\ ,$$

Then

$$\lambda(\mathcal{F}/\mathbb{F}_{q^3}) = \frac{2(q^2-1)}{q+2}.$$

Proof. Since $\mathcal{Z}/\mathbb{F}_{q^3}$ is a subtower of $\mathcal{F}/\mathbb{F}_{q^3}$ with exact limit $2(q^2-1)/(q+2)$ (see[1]), we obtain that $\lambda(\mathcal{F}/\mathbb{F}_{q^3}) \le \lambda(\mathcal{Z}/\mathbb{F}_{q^3}) = 2(q^2-1)/(q+2)$. On the

other hand, a place of the form $(x_1 = \beta)$ with $\beta \in \mathbb{F}_{q^3}\backslash\{0\}$ splits in the tower $\mathcal{F}/\mathbb{F}_{q^3}$, as can be seen directly from Equation (10). Combined with the genus formulas from Proposition 2 we see that

$$\lambda(\mathcal{F}/\mathbb{F}_{q^3}) \geq \lim_{n\to\infty} \frac{(q^3-1)(q^2-1)q^{n-2}}{(q-1)\frac{(q^2+q+1)(q+2)q^{n-2}}{2}} = \frac{2(q^2-1)}{q+2}.$$

□

3.3. **The ramification:** Even though we have already computed the limit of the tower $\mathcal{F}/\mathbb{F}_{q^3}$, it is required to know the exact ramification in F_{n+1}/F_n for $n \geq 2$ to compute the p-rank of the tower. In this section we first show that the tower is (q^2+q+2)-bounded, which will be crucial to calculate the number of ramified places in F_{n+1}/F_n.

Proposition 3. *Let $Q \in \mathbb{P}(F_{n+1})$ be the place lying above $P \in \mathbb{P}(F_n)$ for $n \geq 2$. Then $d(Q|P) = (q^2+q+2)(e(Q|P)-1)$. In other words, the extension F_{n+1}/F_n is (q^2+q+2)-bounded.*

Proof. As the argument trivially holds if $Q|P$ is unramified, we only consider the case in which there is a ramification. We know that for $n \geq 2$, F_{n+1}/F_n is a Galois extension of degree q and that F_n/A_{n-2} is a tame extension. Then by Abhyankar's lemma we deduce that a place Q of F_{n+1} is ramified in F_{n+1}/F_n only if $Q \cap A_{n-2}$ is ramified in A_{n-1}/A_{n-2}. In turn, $Q \cap A_{n-2}$ is ramified in A_{n-1}/A_{n-2} only if $Q \cap \mathbb{F}_{q^3}(\alpha_{n-2})$ is ramified in $\mathbb{F}_{q^3}(\alpha_{n-2}, \alpha_{n-1})/\mathbb{F}_{q^3}(\alpha_{n-2})$. By Figure 1, we see that (still assuming $n \geq 2$) the place Q lies above a place of A_0 in $\{(\alpha_0 = \infty), (\alpha_0 = 0), (\alpha_0 = -1)\}$ as well as that either $\alpha_{n-2}(Q) = -1$ and $\alpha_{n-1}(Q) = \infty$ or $\alpha_{n-2}(Q) = 0$ and $\alpha_{n-1}(Q) = \infty$. Moreover, in the former case we have $e(Q\cap A_{n-1}|Q\cap A_{n-2}) = q-1$ and in the latter $e(Q\cap A_{n-1}|Q\cap A_{n-2}) = d(Q\cap A_{n-1}|Q\cap A_{n-2}) = q$. We analyse the ramification structure of such places distinguishing two cases.

Case (1): Suppose that Q is a place of F_{n+1} that ramifies in F_{n+1}/F_n lying over either $(\alpha_0 = \infty)$ or $(\alpha_0 = 0)$. Then by Figure 1 and the assumption that Q is ramified, we see that we are in the case where $\alpha_{n-2}(Q) = 0$ and $\alpha_{n-1}(Q) = \infty$. From the proof of Proposition 2, we see that $Q\cap A_{n-2}$ is ramified in F_n/A_{n-2} with ramification index q^3-1. By Abhyankar's lemma and transitivity of different we conclude that Q is also totally ramified in F_{n+1}/F_n with different exponent $q^3+q-2 = (q^2+q+2)(q-1)$.

Case (2): Now suppose that Q is a place of F_{n+1} that ramifies in F_{n+1}/F_n lying over $(\alpha_0 = -1)$. In this case, there are two possibilities as given below.

(i) $\alpha_{n-2}(Q) = -1$ and $\alpha_{n-1}(Q) = \infty$
(ii) $\alpha_{n-2}(Q) = 0$ and $\alpha_{n-1}(Q) = \infty$

In case (i), $Q \cap A_{n-2}$ is ramified in A_{n-1}/A_{n-2} with ramification index $q-1$. This place is also ramified in F_n/A_{n-2} with ramification index q^3-1 and hence by Abhyankar's lemma Q is not ramified in F_{n+1}/F_n. In case (ii), we know that the ramification of $Q \cap A_{n-2}$ is 2-bounded in A_{n-1}/A_{n-2} (see [6]) with ramification index 1 or q. That is to say $e \in \{1, q\}$ and $d = 2(e-1)$ for the ramification index e and different exponent d of any possible place of A_{n-1} lying above $Q \cap A_{n-2}$. On the other hand $Q \cap A_{n-2}$ is ramified in F_n/A_{n-2} with ramification index q^2+q+1. By transitivity of different, we conclude that either Q is not ramified or that it is totally ramified in F_{n+1}/F_n with different exponent $q^3+q-2 = (q^2+q+2)(q-1)$.

In either case, we see that the (q^2+q+2)-bounded condition is satisfied. □

In the above proposition we have $e(Q|P) \in \{1, q\}$ for any $Q \in \mathbb{P}(F_{n+1})$ lying over $P \in \mathbb{P}(F_n)$. Therefore, if Q is ramified in F_{n+1}/F_n, then the different exponent $d(Q|P) = q^3+q-2$. Moreover, we have the following.

Corollary 1. *For $n \geq 2$ and $k \geq 0$,*

$$\operatorname{degDiff}(F_{n+k}/F_n) = (q^2+q+2) \sum_{P \in \mathbb{P}(F_n)} \sum_{\substack{Q \in \mathbb{P}(F_{n+k}) \\ Q|P}} (e(Q|P)-1) \ .$$

Proof. The proof is by induction on k using transitivity of the different. □

4. Computing the p-rank

We now turn our attention to computing the p-rank of the function fields in the tower $\mathcal{F}/\mathbb{F}_{q^3}$ in case $q = p$. Since many of our arguments are valid for general q we will work in this generality and indicate where precisely we assume that $q = p$. Using Theorem 1 (the Deuring–Shafarevich theorem), we can compute recursively the p-rank of all function fields in the tower, as soon as the p-rank of F_2 is known. Indeed for $n \geq 2$, the extension F_{n+1}/F_n is an Artin–Schreier extension, so Theorem 1 applies. Our main effort will in fact go into the computation of the p-rank of F_2. To this end we will use the action of the Cartier operator on the space of regular differentials of F_2.

4.1. **The action of the Cartier operator on regular differentials of F_2:** We first need to determine a basis for the space of regular differentials of the function field F_2 in order to apply Lemma 1. We use a change of variable also used in Proposition 1; i.e. we set $R := x_2/x_1^q$. Then $F_2 = \mathbb{F}_{q^3}(x_1, x_2) = \mathbb{F}_{q^3}(x_1, R)$ and the defining equation of F becomes

$$x_1^{q^3-1} R^{q^2-1} + R^{q-1} + 1 = 0 \ . \tag{16}$$

We can determine an explicit basis of the space of regular differential forms as follows (also see Figure 2).

Lemma 7. *Let $F_2 = \mathbb{F}_{q^3}(x_1, R)$ be the function field with the defining equation given in Equation (16). Then a basis for the space $\Omega_{F_2}(0)$ of regular differentials of F_2 is given by the set of differentials of the form*

$$\omega_{ij} = \frac{dR}{x_1^{q^3-1-i} R^{q^2-j}} \ ,$$

where (i, j) satisfy

$$(17)\ \ i > 0, \quad j(q^2+q+1) - i(q+1) > 0, \quad \textit{and} \quad j(q^2+q+1) - iq < q^3 - 1 \ .$$

Proof. We use the same notation as in Proposition 1 and Lemma 6. In other words, we denote by Q_β the unique place of F lying over $(R = \beta)$ for $\beta \in \mathcal{B}$, by $Q_{1\ell}$ the places of F_2 lying over $(R = \infty)$ and by $Q_{2\ell}$ the places of F_2 lying over $(R = 0)$ for $\ell = 1, \ldots, q-1$. From the proof of Lemma 6 we conclude that the divisors (x_1), (R) and (dR) in F are given by

$$\begin{aligned}
(x_1) &= \sum_{\beta \in \mathcal{B}} Q_\beta + q \sum_{\ell=1}^{q-1} Q_{1\ell} - (q+1) \sum_{\ell=1}^{q-1} Q_{2\ell} \ , \\
(R) &= (q^2+q+1) \sum_{\ell=1}^{q-1} Q_{2\ell} - (q^2+q+1) \sum_{\ell=1}^{q-1} Q_{1\ell} \ , \text{ and} \\
(dR) &= -2(q^2+q+1) \sum_{\ell=1}^{q-1} Q_{1\ell} + \text{Diff}\left(F_2/\mathbb{F}_{q^3}(R)\right) \ ,
\end{aligned}$$

where $\text{Diff}\left(F_2/\mathbb{F}_{q^3}(R)\right)$ is the different divisor of $F_2/\mathbb{F}_{q^3}(R)$, see [16, Remark 4.3.7]. As

$$\text{Diff}\left(F_2/\mathbb{F}_{q^3}(R)\right) = (q^2+q) \sum_{\ell=1}^{q-1} (Q_{1\ell} + Q_{2\ell}) + (q^3-2) \sum_{\beta \in \mathcal{B}} Q_\beta \ ,$$

we compute the divisor of the differential ω_{ij} as follows.

$$\begin{aligned}
(\omega_{ij}) &= (dR) - (q^3-1-i)(x_1) - (q^2-j)(R) \\
&= (i-1) \sum_{\beta \in \mathcal{B}} Q_\beta + (iq - j(q^2+q+1) + q^3 - 2) \sum_{\ell=1}^{q-1} Q_{1\ell} \qquad (18) \\
&\quad + (j(q^2+q+1) - i(q+1) - 1) \sum_{\ell=1}^{q-1} Q_{2\ell} \ .
\end{aligned}$$

From Equality (18) we conclude that ω_{ij} is regular if and only if the following conditions hold.

$$(19)\quad i > 0 \ , \ \ j(q^2+q+1) - iq < q^3 - 1 \ \text{ and } \ \ j(q^2+q+1) - i(q+1) > 0 \ .$$

Furthermore, the set $\{\omega_{ij}\}$ is $\mathbb{F}_{q^3}$-linearly independent since we have that $[F_2 : \mathbb{F}_{q^3}(x_1)] = q^2 - 1$, $[F_2 : \mathbb{F}_{q^3}(R)] = q^3 - 1$. Determining the number of possibilities for (i, j) satisfying the conditions in (19), amounts to counting the number of interior integral points in the triangle in Figure 2. A direct computation (or using for example Pick's theorem [15]) gives that this number is equal to the genus $g(F_2)$ of F_2, which was determined in Proposition 1. Since the dimension of $\Omega_{F_2}(0)$ equals the genus, we conclude that the set of differentials ω_{ij} forms a basis. □

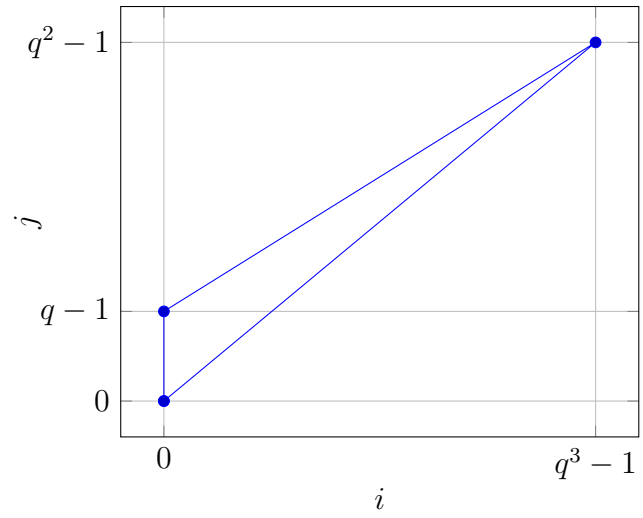

FIGURE 2. ω_{ij} is regular if (i, j) lies inside the triangle.

Next we investigate the action of the Cartier operator on the space of regular differentials $\Omega_{F_2}(0)$ of the function field F_2 using the basis found in Lemma 7. Set $q^3 := p^e$. Instead of computing the action of the Cartier operator C directly, it turns out to be very convenient to consider C^e, the e-th power of the Cartier operator. Note that by the p^{-1}-linearity of the Cartier operator, C^e defines an $\mathbb{F}_{q^3}$-linear map on $\Omega_{F_2}(0)$ and by Lemma 1 the p-rank can be determined studying C^e instead of C. The following simple lemma specifies the action of C^e on $\Omega_{F_2}(0)$ completely.

Lemma 8.

$$C^e(\omega_{ij}) = (-1)^i \binom{q^3 - i - 1}{j(q^2 + q + 1) - i(q + 1)} \omega_{ij} \ . \tag{20}$$

Proof. By p^{-1}-linearity of the Cartier operator we have

$$C^e(h^{-1}\omega) = h^{-1} C^e(h^{q^3 - 1}\omega)$$

for $h \in F$ and $\omega \in \Omega_{F_2}$. In our case, we set $h := x_1^{q^3-1-i}$ and $\omega := dR/R^{q^2-j}$; i.e. $\omega_{ij} = h^{-1}\omega$. Then we have the following equalities.

$$\begin{aligned} C^e(\omega_{ij}) &= C^e\left(\frac{1}{x_1^{q^3-1-i}}\frac{dR}{R^{q^2-j}}\right) = \frac{1}{x_1^{q^3-1-i}}C^e\left((x_1^{q^3-1-i})^{q^3-1}\frac{dR}{R^{q^2-j}}\right) \\ &= \frac{1}{x_1^{q^3-1-i}}C^e\left((x_1^{q^3-1})^{q^3-1-i}\frac{dR}{R^{q^2-j}}\right). \end{aligned}$$

Equation (16) implies that $x_1^{q^3-1} = -(1+R^{q-1})/R^{q^2-1}$. As a result, the following holds.

$$\begin{aligned} C^e(\omega_{ij}) &= \frac{1}{x_1^{q^3-1-i}}C^e\left(\left(-\frac{1+R^{q-1}}{R^{q^2-1}}\right)^{q^3-1-i}\frac{dR}{R^{q^2-j}}\right) \\ &= \frac{(-1)^i}{x_1^{q^3-1-i}}C^e\left(\frac{1}{R^{(q^2-1)(q^3-1-i)+(q^2-j)}}\sum_{a=0}^{q^3-1-i}\binom{q^3-1-i}{a}R^{a(q-1)}\right). \end{aligned}$$

By definition of the Cartier operator, we need to determine a for which the exponent is congruent to -1 modulo q^3; i.e.

$$-1 \equiv -(q^2-1)(q^3-1-i) - (q^2-j) + a(q-1) \pmod{q^3}. \tag{21}$$

Note that Equation (21) has a unique solution, since $0 \le a \le q^3-1$. To find it, we first multiply both sides of Equation (21) by q^2+q+1. Then we have

$$-(q^2+q+1) \equiv -(q+1)i + (q^2+q+1)j - (q^2+q+1) - a \pmod{q^3}.$$

Hence we see that Equation (21) holds if and only if

$$a \equiv -(q+1)i + (q^2+q+1)j \pmod{q^3}.$$

This shows that $a = -(q+1)i + (q^2+q+1)j$ as i, j satisfy the conditions in (17), which implies that

$$0 \le -(q+1)i + (q^2+q+1)j \le q^3-1-i.$$

For this value of a we have

$$C^e(\omega_{ij}) = \frac{(-1)^i}{x_1^{q^3-1-i}}\binom{q^3-i-1}{a}R^\ell dR,$$

where the exponent ℓ is given by

$$\begin{aligned} \ell &= \frac{1}{q^3}\big(-(q^2-1)(q^3-1-i)(q^2+q+1) \\ &\quad -(q^2-j)(q^2+q+1) + a(q^3-1)\big) \\ &= -q^2 + j. \end{aligned}$$

This gives the desired result. □

4.2. **The p-rank of F_2:** We now use the previous result to compute the p-rank of F_2. We set

$$b_{ij} := \binom{q^3-i-1}{j(q^2+q+1)-i(q+1)} .$$

We have seen in Lemma 8 that $(-1)^i b_{ij}$ is an eigenvalue of C^e associated with ω_{ij}. In order to calculate the p-rank of F_2 using Lemma 1, we have to determine for how many pairs (i,j), the value b_{ij} is zero (as element of F_2, that is to say zero modulo p). We will use Lemma 2 for this, but first we will rewrite b_{ij} in an easier form.

Lemma 9.

$$b_{ij} = (-1)^j \binom{j(q^2+q+1)-iq}{i}. \tag{22}$$

Proof. First note that b_{ij} is the coefficient of $T^{j(q^2+q+1)-i(q+1)}$ in $(T+1)^{q^3-i-1}$. We write

$$(T+1)^{q^3-i-1} = (T+1)^{q^3}\frac{1}{(T+1)^{i+1}} = \frac{T^{q^3}}{(T+1)^{i+1}} + \frac{1}{(T+1)^{i+1}} .$$

Then the coefficient of $T^{j(q^2+q+1)-i(q+1)}$ only comes from the second sum as

$$\frac{1}{(T+1)^{i+1}} = (1-T+T^2+\cdots)^{i+1} \text{ and } j(q^2+q+1)-iq \le q^3-1 .$$

The fact that $1/(T+1)^{i+1} = \sum_{m\ge 0}(-1)^m\binom{i+m}{m}T^m$ (see for example [12, Chapter 5.4]) gives the following equalities for the coefficient d of $T^{j(q^2+q+1)-i(q+1)}$.

$$\begin{aligned} d &= (-1)^{j(q^2+q+1)-i(q+1)}\binom{j(q^2+q+1)-iq}{j(q^2+q+1)-i(q+1)} \\ &= (-1)^j\binom{j(q^2+q+1)-iq}{i}. \end{aligned}$$

□

For a final simplification we reparametrize the binomial coefficients from Lemma 9.

Lemma 10. *The set of binomial coefficients of the form*

$$\binom{j(q^2+q+1)-iq}{i},$$

with $(i,j)\in\mathbb{Z}^2$ satisfying the conditions in Equation (17) is the same as the set of binomial coefficients

$$\binom{aq+b}{b(q+1)-a},$$

where $(a,b) \in \mathbb{Z}^2$ *and*

$$a < b(q+1), \quad a(q+1) > bq, \quad \textit{and} \quad aq+b < q^3-1 \ . \tag{23}$$

Proof. We have

$$(j(q^2+q+1)-iq, i) = i\cdot(-q,1)+j\cdot(q^2+q+1,0) = (i-(q+1)j)\cdot(-q,1)+j\cdot(1,q+1) \ .$$

Setting $a := (q+1)j - i$ and $b := j$, we see that

$$\binom{j(q^2+q+1)-iq}{i} = \binom{aq+b}{b(q+1)-a}.$$

Since $i = (q+1)b - a$ we see that $(i,j) \in \mathbb{Z}^2$ if and only if $(a,b) \in \mathbb{Z}^2$. Further Equation (17) directly implies Equation (23) and vice versa. □

We are now ready to compute the p-rank of F_2.

Proposition 4. *Assume that $q = p$ is a prime, then the p-rank of F_2 is*

$$\gamma(F_2) = \frac{1}{8}(q^4 + 2q^3 + 3q^2 - 22q + 24) \ .$$

Proof. We have seen that binomial coefficients occur as eigenvalues of C^e and that these coefficients can be described using $(a,b) \in \mathbb{Z}^2$ lying inside a certain triangle $\triangle$ defined by Equation 23 as in Lemma 10. For (a,b) in Δ, we have to count the number of pairs (a,b) for which

$$\binom{aq+b}{bq+b-a} = \binom{aq+b}{(a-b)q+a} \equiv 0 \pmod{p}$$

in order to calculate the p-rank of F_2. We can write a, b in a unique way as

$$a = a_1q + a_0 \quad \text{and} \quad b = b_1q + b_0 \quad \text{for some } 0 \le a_0, a_1, b_0, b_1 \le q-1 \ .$$

In light of Lucas's lemma, we consider the following binomial coefficients.

$$\binom{a_1q^2 + (a_0+b_1)q + b_0}{(a_1-b_1)q^2 + (a_0-b_0+a_1)q + a_0} = \binom{a_1q^2 + (a_0+b_1)q + b_0}{b_1q^2 + (b_1-a_1+b_0)q + b_0 - a_0}. \tag{24}$$

We divide the possibilities for (a,b) up into several smaller regions, see Figure 3 for an illustration. More precisely, we divide the triangle $\triangle$ into four sub-triangles with the following boundary conditions.

Triangle I: $a < q^2 - q$, $b > q-1$ and $a > b$
Triangle II: $a \le b < q^2 - q$, $bq < a(q+1)$ and $0 < a < q^2 - q$
Triangle III: $0 < b \le q-1$, $a < b(q+1)$ and $q-1 < a < q^2 - 1$
Triangle IV: $q^2 - q \le a < q^2 - 1$, $q-1 < b < q^2 - 1$ and $aq + b < q^3 - 1$

Now we investigate each sub-triangle separately. In this investigation we mainly make use of Lemma 2. Recall that we assume that $q = p$, a prime.

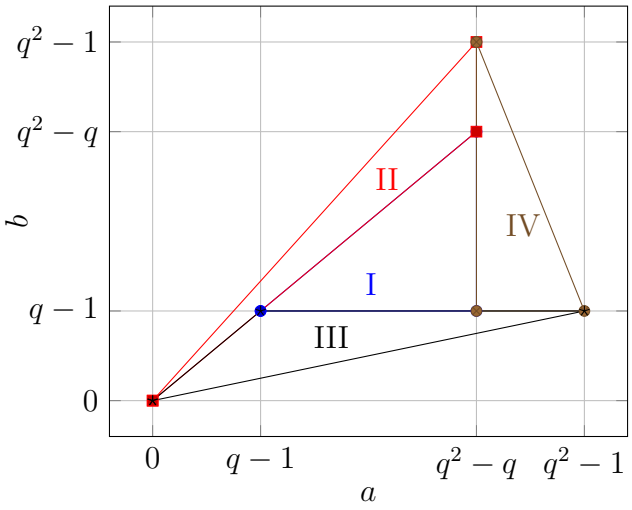

FIGURE 3. The triangle $\triangle$ and its sub-triangles.

Triangle I: First note that since $a > b$ in Triangle I, we obtain that

$$a_1 > b_1 + (b_0 - a_0)/q \geq b_1 - (q-1)/q, \tag{25}$$

implying that $a_1 \geq b_1$, since a_1 and b_1 are integers. Further, in the case that $a_0 > b_0$, we can see from Lemma 2 and Equation (24) that $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$. For this reason we first divide Triangle I into small squares whose sides have length q. For each fixed $b_1 \in \{1, \ldots q-3\}$ and $a_1 \in \{b_1, \ldots, q-2\}$ we define the square with boundary conditions

$$b_1 q \leq b = b_1 q + b_0 \leq b_1 q + q - 1 \quad \text{and} \quad a_1 q \leq a = a_1 q + a_0 \leq a_1 q + q - 1 \ .$$

Then we separate each square into two triangles according to a lower triangle $a_0 > b_0$ and an upper triangle $a_0 \leq b_0$. We have seen that in the first case, i.e. in the lower triangle part of the square, the condition that $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$ always holds. We observe that for fixed b_1 there are $q-1-b_1$ many lower triangles. In other words, there exist

$$(q-2) + (q-3) + \cdots + 1 = \frac{(q-1)(q-2)}{2}$$

many lower triangles in Triangle I.

Note that in each lower triangle part, $b_0 \in \{0, \ldots, a_0 - 1\}$ for a fixed $a_0 \in \{1, \ldots, q-1\}$. That is; for a fixed a_0 there exist a_0 many b_0's with $a_0 > b_0$. As a result, each lower triangle contains

$$1 + 2 + \cdots + q - 1 = \frac{q(q-1)}{2}$$

many pairs (a, b). This gives rise to $N_{lt} = \frac{q(q-1)^2(q-2)}{4}$ many pairs (a, b) with $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$.

Now we consider the upper triangle parts; i.e. the part for which $a_0 \leq b_0$. In this case, by Equation (24) we conclude that $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$ if and only if

$$\binom{a_1q + (a_0+b_1)}{b_1q + (b_0+b_1-a_1)} \equiv 0 \pmod{q} . \tag{26}$$

We investigate congruence (26) into four cases according to the q-adic expansions $a_1q + (a_0+b_1)$ and $b_1q + (b_0+b_1-a_1)$. We denote by $N_{ut,k}$ the number of pairs (a,b) in the upper triangles with $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$ satisfying the conditions in Case (k) for $k = 1, \ldots, 4$.

Case (1): $0 \leq b_0 + b_1 - a_1 \leq q-1$ and $0 \leq a_0 + b_1 \leq q-1$.
By Lucas's Lemma 2 we see that

$$\binom{aq+b}{b(q+1)-a} \equiv \binom{a_1}{b_1}\binom{a_0+b_1}{b_0+b_1-a_1}\binom{b_0}{b_0-a_0} \pmod{q} .$$

Then $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$ if and only if $a_0 + a_1 < b_0$. This inequality combined Equation 25 implies $a_1 > b_1$. More precisely, from our assumptions for Case (1) we have the following equivalent conditions:

$$1 \leq b_1 < a_1 \leq q-2 \quad \text{and} \quad a_0 + b_1 < b_0 \leq q-1 .$$

Note that $1 \leq b_1 \leq q-3$. For a fixed $b_1 \in \{1, \ldots, q-3\}$, we have that $a_1 \in \{b_1+1, \ldots, q-2\}$, $a_0 \in \{0, 1, \ldots, q-2-a_1\}$ and $b_0 \in \{a_0+a_1+1, \ldots, q-1\}$. Furthermore, for each such choice of (a_0, a_1, b_0, b_1) the pair (a,b) lies in an upper triangle in Triangle I. As a result, the number $N_{ut,1}$ of pairs (a,b) with $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$ is given as follow.

$$\begin{aligned}
N_{ut,1} &= \sum_{b_1=1}^{q-3} \sum_{a_1=b_1+1}^{q-2} \sum_{a_0=0}^{q-2-a_1} (q-1-a_0-a_1) = \sum_{b_1=1}^{q-3} \sum_{a_1=b_1+1}^{q-2} \sum_{t=1}^{q-1-a_1} t \\
&= \sum_{b_1=1}^{q-3} \sum_{a_1=b_1+1}^{q-2} \binom{q-a_1}{2} = \sum_{b_1=1}^{q-3} \sum_{s=2}^{q-b_1-1} \binom{s}{2} \\
&= \sum_{b=1}^{q-3} \binom{q-b_1}{3} = \sum_{u=3}^{q-1} \binom{u}{3} = \binom{q}{4}
\end{aligned}$$

Case (2): $b_0 + b_1 - a_1 < 0$ and $0 \leq a_0 + b_1 \leq q-1$.
In this case, by Lucas's Lemma 2 we have

$$\binom{aq+b}{b(q+1)-a} \equiv \binom{a_1}{b_1-1}\binom{a_0+b_1}{q+b_0+b_1-a_1}\binom{b_0}{b_0-a_0} \pmod{q} .$$

In other words, $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$ if and only if $a_0+a_1 < b_0+q$, which trivially holds as $a_0 \leq b_0$.

Then $1 \leq b_1 \leq q-3$ and for a fixed $b_1 \in \{1, \ldots, q-3\}$, we have $a_1 \in \{b_1+1, \ldots, q-2\}$, $b_0 \in \{0, \ldots, a_1-b_1-1\}$ and $a_0 \in \{0, \ldots, b_0\}$.

Furthermore, for each such choice of (a_0, a_1, b_0, b_1) the pair (a, b) lies in an upper triangle in Triangle I. Therefore there are

$$N_{ut,2} = \sum_{b_1=1}^{q-3} \sum_{a_1=b_1+1}^{q-2} \sum_{b_0=0}^{a_1-b_1-1} (b_0+1) = \binom{q}{4}$$

pairs (a, b) with $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$.

Case (3): $b_0 + b_1 - a_1 < 0$ and $a_0 + b_1 \geq q$.
We observe that the conditions $b_0 + b_1 < a_1$, $a_0 \leq b_0$ and $a_0 + b_1 \geq q$ implies $a_1 \geq q$, which is a contradiction. Therefore, there is no pair (a, b) satisfying these conditions; i.e. $N_{ut,3} = 0$.

Case (4): $0 \leq b_0 + b_1 - a_1 \leq q - 1$ and $a_0 + b_1 \geq q$.
In this case we observe that any pair (a, b) satisfying these conditions also satisfies $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$ and with a similar argument we show that there are

$$N_{ut,4} = \sum_{b_1=1}^{q-3} \sum_{a_1=b_1+1}^{q-2} \sum_{a_0=q-b_1}^{q-1} (q - a_0) = \binom{q}{4}$$

pairs (a, b) satisfying these conditions.

To sum up, in Triangle I there are

$$\frac{q(q-1)^2(q-2)}{4} + 3\binom{q}{4} = 9\binom{q}{4} + 3\binom{q}{3}$$

pairs (a, b) with $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$.

Now we continue with the Triangle IV.

Triangle IV: The boundary conditions $a \geq q^2 - q$, $q - 1 < b$ and $aq + b < q^3 - 1$ imply that

$$a_1 = q - 1, \quad 0 < b_1 \leq q - 1 \quad \text{and} \quad a_0 + b_1 < q \ .$$

We remind that in this case

$$\binom{aq+b}{b(q+1)-a} = \binom{(q-1)q^2 + (a_0+b_1)q + b_0}{(q-1-b_1)q^2 + (a_0-b_0+q-1)q + a_0} .$$

We then investigate $\binom{aq+b}{b(q+1)-a}$ in two cases.

Case (1): Suppose that $a_0 \leq b_0$. Then by Lucas's lemma 2

$$\binom{aq+b}{b(q+1)-a} \equiv \binom{q-1}{q-1-b_1}\binom{a_0+b_1}{a_0-b_0+q-1}\binom{b_0}{a_0} \pmod{q} .$$

As a result, we see that $\binom{c}{i} \equiv 0 \pmod{q}$ if and only if $b_0 + b_1 \leq q - 2$. Here we observe that $0 \leq a_0 \leq q - 3$, and for a fixed $a_0 \in \{0, \ldots, q-3\}$, we have

$b_0 \in \{a_0, \dots, q-3\}$ and $b_1 \in \{1, \dots, q-2-b_0\}$. As a result, there are

$$\sum_{a_0=0}^{q-3} \sum_{b_0=a_0}^{q-3} (q-2-b_0) = \binom{q}{3}$$

pairs (a,b) with $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$.

Case (2): Suppose that $a_0 > b_0$. In this case $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$ as observed before. In this case $0 \le a_0 \le q-2$, and moreover, for a fixed $a_0 \in \{0, \dots, q-2\}$, we have $b_0 \in \{0, \dots, a_0-1\}$ and $b_1 \in \{1, \dots, q-2-a_0\}$. Similar calculations show that there are $\binom{q}{3}$ pairs (a,b) satisfying this case.

To sum up, Triangle IV contains exactly $2\binom{q}{3}$ pairs (a,b) satisfying that $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$.

We could calculate the number of desired pairs (a,b) in Triangles II and III similarly as in Triangle IV; however, we can related the pairs in Triangles II and III with the pairs in Triangle IV. For this we consider the affine map f defined by

$$f : (a,b) \mapsto (\tilde{a}, \tilde{b}) = (b - a + q^2 - q, -a + q^2 - 1) \ .$$

Then the map f acts on Triangles II, III and IV. More precisely, f not only permutes them but also preserves the boundary conditions. For a pair $(c,i) = (aq+b, b(q+1)-a)$, we set $(\hat{c}, \hat{i}) := (\tilde{a}q + \tilde{b}, \tilde{b}q + \tilde{b} - \tilde{a})$. Now we show that $\binom{c}{i} \equiv 0 \pmod{q}$ if and only if $\binom{\hat{c}}{\hat{i}} \equiv 0 \pmod{q}$, which proves that all triangles contain the same number of pairs (a,b) with $\binom{aq+b}{b(q+1)-a} \equiv 0 \pmod{q}$; namely $2\binom{q}{3}$.

We see by definition of f that

$$\binom{\hat{c}}{\hat{i}} = \begin{pmatrix} -a(q+1) + bq + q^3 - 1 \\ -aq - b + q^3 - 1 \end{pmatrix} = \begin{pmatrix} -a(q+1) + bq + q^3 - 1 \\ -a + b(q+1) \end{pmatrix} .$$

For convenience we set $\alpha := a(q+1) - bq$ and $\beta := -a + b(q+1)$. Then we have

$$\alpha = a(q+1) - bq = aq + b + (a - b(q+1)) = aq + b - \beta \ ,$$

and the boundary conditions $bq < a(q+1)$ and $a < b(q+1)$ (see the boundary conditions for Triangle II and III) imply that

$$0 < \alpha < q^3 - 1 \ \text{ and } \ 0 < \beta < q^3 - 1 - \alpha \ .$$

Therefore $\binom{\hat{c}}{\hat{i}} = \binom{q^3-1-\alpha}{\beta}$ is equal to the coefficient of T^β in $(T+1)^{q^3-1-\alpha}$. As we observed in the proof of Lemma 9, this is equal to the coefficient of T^β in the power series expansion of $1/(T+1)^{1+\alpha}$; i.e. we have the following

equalities.

$$\binom{\hat{c}}{\hat{i}} = (-1)^{\beta}\binom{\alpha+\beta}{\alpha} = (-1)^{\beta}\binom{\alpha+\beta}{\beta} = (-1)^{\beta}\binom{aq+b}{bq+b-a} = (-1)^{\beta}\binom{c}{i},$$

which shows that $\binom{\hat{c}}{\hat{i}} \equiv 0 \pmod{q}$ if and only if $\binom{c}{i} \equiv 0 \pmod{q}$.

From all counting arguments above we conclude that

$$g(F_2) - \gamma(F_2) = 9\binom{q}{4} + 9\binom{q}{3} = 9\binom{q+1}{4}.$$

The above equality together with Proposition 1 gives the desired result and finishes the proof. □

Theorem 4. *The p-rank $\varphi(\mathcal{F}/\mathbb{F}_{p^3})$ of the tower $\mathcal{F}/\mathbb{F}_{p^3}$ satisfies*

$$\varphi(\mathcal{F}/\mathbb{F}_{p^3}) = \frac{p^2+p+4}{4(p^2+p+1)}.$$

Proof. Let n be a non-negative integer. By transitivity of ramification index and Fundamental Equality we show

$$\gamma(F_{n+2}) - 1 = p^n(\gamma(F_2) - 1) + \sum_{P\in\mathbb{P}(F_2)} \sum_{Q\in\mathbb{P}(F_{n+2}),Q|P} (e(Q|P) - 1). \tag{27}$$

The fact that all extensions F_{i+1}/F_i for all $i > 0$ are p^2+p+2-bounded (see Proposition 3) implies that F_{n+2}/F_2 is p^2+p+2-bounded. Then by the Riemann-Hurwitz genus formula we have

$$\sum_{P\in\mathbb{P}(F_2)} \sum_{Q\in\mathbb{P}(F_{n+2}),Q|P} (e(Q|P) - 1) = \frac{2g(F_{n+2}) - 2 - p^n(2g(F_2) - 2)}{(p^2+p+2)}. \tag{28}$$

Combining Equations (27) and (28) we obtain that

$$\frac{\gamma(F_{n+2})}{g(F_{n+2})} = \frac{2}{p^2+p+2} + \frac{(p^2+p+2)\,(p^n(\gamma(F_2)-1)+1)) - 2\,(1+p^n(g(F_2)-1))}{g(F_{n+2})(p^2+p+2)}. \tag{29}$$

Using Proposition 2, we conclude that

$$\lim_{n\to\infty} \frac{\gamma(F_n)}{g(F_n)} = \frac{2}{p^2+p+2} + 2\frac{(p^2+p+2)\,(\gamma(F_2)-1) - 2\,(g(F_2)-1)}{(p^3-1)(p+2)(p^2+p+2)}.$$

Then by Proposition 1 and 4, the theorem follows. □

Remark 2. Note that from Equation (29) and Proposition 2, we directly can find a closed formula for $\gamma(F_n)$ for $n \geq 2$. Also note that going through the proof of Proposition 4 again, one easily concludes that the found pairs (a, b) for which the corresponding binomial coefficient vanishes modulo p also vanish for general q. The condition that $q = p$ was only used to ensure

that for the remaining pairs (a, b) the corresponding binomial coefficients do not vanish modulo p. In other words for general q we have:

$$\gamma(F_2) \leq \frac{1}{8}(q^4 + 2q^3 + 3q^2 - 22q + 24) \ .$$

This is enough to be able to conclude that for general q the p-rank of the tower $\mathcal{F}/\mathbb{F}_{q^3}$ satisfies

$$\varphi(\mathcal{F}/\mathbb{F}_{q^3}) \leq \frac{q^2 + q + 4}{4(q^2 + q + 1)} \ .$$

As mentioned before the case $q = p$ is the most interesting, since for non-prime q there exist towers over $\mathbb{F}_{q^3}$ with a better limit. It is future work to investigate the p-rank of these kinds of towers.

Acknowledgements: 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". The authors would also like to thank Prof. Henning Stichtenoth for his valuable comments.

References

[1] N. Anbar, P. Beelen, N. Nguyen, *The exact limit of some cubic towers*, in: Arithmetic, geometry and coding theory (AGCT 2015), submitted.

[2] A. Bassa, P. Beelen, *The Hasse-Witt invariant in some towers of function fields over finite fields*, Bulletin of the Brazilian Mathematical Society , New Series 41 (2010), no. 4, 567–582.

[3] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, *Towers of Function Fields over Non-prime Finite Fields*, Moscow Mathematical Journal 15 (2015), no. 1, 1–29.

[4] A. Bassa, A. Garcia, H. Stichtenoth, *A new tower over cubic finite fields*, Moscow Mathematical Journal 8 (2008), no. 3, 401–418.

[5] J. Bezerra, A. Garcia, H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, Journal für die reine und angewandte Mathematik 589 (2005), 159–199.

[6] N. Caro, A. Garcia, *On a tower of Ihara and its limit*, Acta Arithmetica 151 (2012), no. 2, 191–200.

[7] I. Cascudo, R. Cramer, C. Xing, *Torsion Limits and Riemann-Roch Systems for Function Fields and Applications*, IEEE Transactions on Information Theory 60 (2014), no. 7, 3871–3888.

[8] A. Garcia, H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Inventiones Mathematicae 121 (1995), no. 1, 211–222.

[9] A. Garcia, H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, Journal Of Number Theory 61 (1996), no. 2, 248–273. doi:10.1006/jnth.1996.0147.

[10] A. Garcia, S. Tafazolian, *Certain maximal curves and Cartier operators*, Acta Arithmetica 135 (2008), no. 3, 199–218.

[11] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic curves over a finite field*, Philadelphia, PA, USA: SIAM, 2008.

[12] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete mathematics*, Addison-Wesley Publishing Company, Reading, MA, 1989.

[13] Y. Ihara, *Some remarks on the BGS tower over finite cubic fields*, in: Proceedings of the conference Arithmetic Geometry, Related Area and Applications (Chuo University, April 2006) (2007) 127–131.

[14] E. Lucas, *Sur les congruences des nombers eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France 6 (1878) 49–54.

[15] G. Pick, *Geometrisches zur zahlenlehre*, Sitzungbericht Lotos (Prague) 19 (1899), 311–319.

[16] H. Stichtenoth, *Algebraic function fields and codes*, Springer, 2009.

Department of Applied Mathematics and Comp. Science, Technical University of Denmark

E-mail address: nurdagulanbar2@gmail.com

Department of Applied Mathematics and Comp. Science, Technical University of Denmark

E-mail address: pabe@dtu.dk

Department of Applied Mathematics and Comp. Science, Technical University of Denmark

E-mail address: ntnhut17@gmail.com