A tower with non-Galois steps which attains the Drinfeld-Vladut bound

Juscelino Bezerra and Arnaldo Garcia[1,2]

IMPA, Estrada Dona Castorina 110, 22.460-320, Rio de Janeiro-Brazil

Abstract

We introduce a new tower of function fields over a finite field of square cardinality, which attains the Drinfeld-Vladut bound. One new feature of this new tower is that it is constructed with non-Galois steps; i.e., with non-Galois function field extensions. The exact value of the genus $g(F_n)$ is also given (see Lemma 4).

Keywords: Towers of Function Fields, Finite Fields, Rational Places, Drinfeld-Vladut bound, genus.

1 Introduction

The interest on the determination of the rational points on curves over finite fields (equivalently, the determination of the places of degree one of function fields over finite fields) has a long history, going back to C.F. Gauss. It was renewed recently after Goppa's construction of codes from algebraic curves, and also after Tsfasman-Vladut-Zink showed that (through Goppa's construction) one can find infinite sequences of codes with limit parameters above the so-called Gilbert-Varshamov bound.

Let K be a finite field. A function field F over K is a field extension F/K such that:

a) F is finitely generated over K.
b) The transcendence degree of F/K is one.
c) K is algebraically closed in the field F.

[1] Corresponding author.
E-mail address: garcia@impa.br (Arnaldo Garcia)

[2] This work started while the second author was visiting Sabanci Univ.-Turkey, and it was also partially supported by PRONEX # 662408/1996-3, Brazil.

A tower $\mathcal{F}$ over K is an infinite sequence $F_1 \subsetneqq F_2 \subsetneqq F_3 \subsetneqq \dots$ of function fields F_n over K such that

$$g(F_n) \to \infty \quad \text{as} \quad n \to \infty,$$

where $g(F_n)$ denotes the genus of the field F_n. We denote by $N(F_n)$ the number of K-rational places of the field F_n; i.e.,

$$N(F_n) = \#\{P \text{ place of } F_n;\ \deg(P) = 1\}.$$

The limit $\lambda(\mathcal{F})$ below exists (see [3])

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

It follows from the Drinfeld-Vladut bound (see [2]) that we have

$$\lambda(\mathcal{F}) \leq (\#K)^{1/2} - 1.$$

When $K = \mathbb{F}_{q^2}$ is the finite field with q^2 elements, q a prime power, there are towers $\mathcal{F}$ over K attaining the Drinfeld-Vladut bound; i.e., such that

$$\lambda(\mathcal{F}) = q - 1.$$

See, for example, [6], [9], [4] and [5]. One usually tries to construct explicit towers $\mathcal{F}$ over K with Galois steps; i.e., the extensions F_{n+1}/F_n are Galois extensions for all $n \geq 1$. The purpose here is to present a new tower $\mathcal{F}$ over $K = \mathbb{F}_{q^2}$ (see Theorem 1) attaining the Drinfeld-Vladut bound, but with non-Galois steps (except for the case $q = 2$). This new tower $\mathcal{F}$ will have both wild and tame ramifications, and the difficulty lies in the determination of the genus $g(F_n)$, for each value of $n \in \mathbb{N}$ (see Lemma 4). The exact value of the genus $g(F_n)$ is very important in applications (see for example [7] and [1]).

One can also deduce that this new tower $\mathcal{F}$ attains the Drinfeld-Vladut bound from [3] (see Remark 1) but the direct proof given here is simpler, avoiding in particular the tiresome pole-order reductions in [3], and it illustrates a method for computing the genus $g(F_n)$ which will certainly be useful for other non-Galois towers of function fields over finite fields of nonsquare cardinalities. Moreover to obtain the genus $g(F_n)$ from the tower in [3] one is naturally led to the key computations done in Lemma 3 (see Remark 1).

Another new feature of this tower $\mathcal{F}$ is that it is recursively given by an equation where each side of it is not a polynomial (see Equation (1) in Section 3).

2 Preliminaries and Notations

Let F/K be a function field over a finite field K. For two functions $z, w \in F$ and a place P of F we write

$$z = w + \mathcal{O}(n) \quad \text{at } P$$

meaning that

$$v_P(z - w) \geq n, \quad \text{where } v_P \text{ is the valuation at } P.$$

Let E/F be a separable extension of function fields over K and let P be a place of F. Denote by θ_P the local ring at P and by $\tilde{\theta}_P$ its integral closure in the field E. Suppose we can find a function $f \in \tilde{\theta}_P$ such that $E = F(f)$ and such that the minimal polynomial $P_{f|F}(T) \in \theta_P[T]$ of the function f over the field F is separable modulo the place P. Then we have clearly that P is unramified in the extension E/F; i.e., we have that the ramification index $e(Q|P)$ satisfies:

$$e(Q|P) = 1, \quad \text{for each place } Q \text{ of } E \text{ above } P.$$

We will also need some facts about different exponents. Let again E/F be a separable function field extension, Q be a place of E and P be the restriction of the place Q to the field F. We denote by $d(Q|P)$ and also by $d(Q)$ the differente exponent at Q for the extension E/F.

Proposition 1. *Suppose that $Q|P$ is totally ramified in the extension E/F. Let $t \in E$ be a Q-prime element and let $\varphi(T) \in F[T]$ denote the minimal polynomial of t over F. Then*

$$d(Q|P) = v_Q(\varphi'(t)),$$

where φ' denotes the derivative.

Proof: See [8, Proposition III.5.12]. □

Proposition 2: *Let E/F be a separable extension of function fields and suppose E_1, E_2 are intermediate fields such that $E = E_1 \cdot E_2$. Let Q be a place of E and let Q_1, Q_2 and P be its restrictions to the fields E_1, E_2 and F. Moreover denote by*

$$e_i = e(Q_i|P), \quad \text{for } i = 1 \text{ and } i = 2.$$

Assuming that e_1 and e_2 are coprime, we have:

a) $e(Q|P) = e_1 \cdot e_2$.

b) *If $Q_1|P$ is tame; i.e., if e_1 is not a multiple of the characteristic of K, then*

$$d(Q|Q_1) = e_1 \cdot d(Q_2|P) - (e_1 - 1)(e_2 - 1).$$

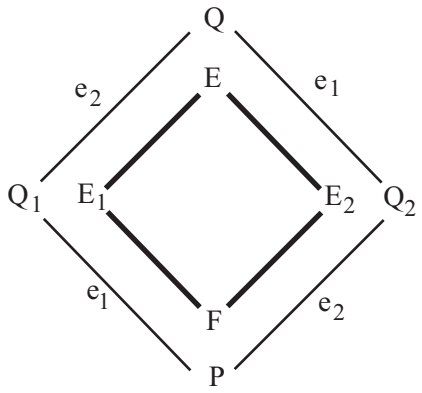

Figure 1

Proof: The item a) follows from the multiplicativity of ramification indices in field extensions, and the item b) follows from the transitivity of different exponents in field extensions. □

Figure 1 above illustrates Proposition 2.

3 The New Tower

Let $K = \mathbb{F}_{q^2}$ and consider the tower $\mathcal{F}$ over K defined inductively by:

$F_1 = K(x_1)$ is the rational function field and, for each $n \geq 1$, we have that $F_{n+1} = F_n(x_{n+1})$ with the relation

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

Our main result is the following

Theorem 1. *The tower $\mathcal{F}$ over K above attains the Drinfeld-Vladut bound; i.e.,*

$$\lambda(\mathcal{F}) = q - 1.$$

We will need some lemmas for the proof of Theorem 1. The key result is Lemma 3, which gives the main information needed for the exact computation of the genera in Lemma 4.

Lemma 1. *Let $F = K(x, y)$ be the function field over $K = \mathbb{F}_{q^2}$ defined by*

$$\frac{y - 1}{y^q} = \frac{x^q - 1}{x}. \tag{2}$$

Then the following holds:

a) $[F : K(x)] = [F : K(y)] = q$.

b) *The place of* $K(x)$ *corresponding to* $x = 0$ *is totally ramified in* F. *The place of* $K(x)$ *corresponding to* $x = \infty$ *is also totally ramified in* F. *The place of* $K(x)$ *corresponding to* $x = 1$ *has two places in* F *above it; one is denoted by* Q_1 *and corresponds to* $y = 1$, *and the other is denoted by* Q_∞ *and corresponds to* $y = \infty$. *The ramification indices in* $F/K(x)$ *are* $e(Q_1) = 1$ *and* $e(Q_\infty) = q-1$.

c) *The place of* $K(y)$ *corresponding to* $y = 0$ *has two places in* F *above it; one is denoted by* P_0 *and it is the unique zero of the function* x *in* F, *and the other is denoted by* P_∞ *and it is the unique pole of the function* x *in* F. *The ramification indices in* $F/K(y)$ *are* $e(P_0) = 1$ *and* $e(P_\infty) = q - 1$. *The place of* $K(y)$ *corresponding to* $y = \infty$ *is totally ramified in* F *and* Q_∞ *is the unique place above it. The place of* $K(y)$ *corresponding to* $y = 1$ *is also totally ramified in* F *and* Q_1 *is the unique place above it.*

d) *The principal divisors in* F *of the functions* $x, y, x-1$ *and* $y-1$ *are:* $div(x) = qP_0 - qP_\infty$; $div(y) = P_0 + (q-1)P_\infty - qQ_\infty$; $div(x-1) = Q_1 + (q-1)Q_\infty - qP_\infty$; $div(y-1) = qQ_1 - qQ_\infty$.

e) *The places of* F *that are ramified over* $K(x)$ *are exactly the places* P_0, P_∞ *and* Q_∞. *Their different exponents with respect to the extension* $F/K(x)$ *are* $d(P_0) = q$, $d(P_\infty) = 2(q-1)$ *and* $d(Q_\infty) = q - 2$.

Proof: Follows directly from Equation (2). We will only prove here the assertions about the different exponents in item e). The assertion $d(Q_\infty) = q - 2$ is easy since Q_∞ is tamely ramified over $K(x)$ with $e(Q_\infty) = q - 1$ (see item c)). The other two places P_0 and P_∞ are totally ramified in the extension $F/K(x)$ and we will use Proposition 1 to determine their different exponents. The function $y \in F$ is a P_0-prime element and its minimal polynomial $\varphi(T)$ over $K(x)$ is given below

$$\varphi(T) = T^q - \frac{x}{x^q - 1} \cdot T + \frac{x}{x^q - 1}.$$

Hence $d(P_0) = v_{P_0}(\varphi'(y)) = v_{P_0}(x) = q$. Now at the place P_∞ of F we have that $t = 1/xy$ is a P_∞-prime element and its minimal polynomial $\psi(T)$ over $K(x)$ is

$$\psi(T) = T^q - \frac{1}{x} \cdot T^{q-1} + \frac{x^q - 1}{x^{q+1}}.$$

Hence

$$d(P_\infty) = v_{P_\infty}(\psi'(t)) = v_{P_\infty}(\frac{1}{x}t^{q-2}) = v_{P_\infty}(\frac{1}{x}) + q - 2 = 2(q-1).$$

□

The place of $K(x_1)$ corresponding to $x_1 = 0$ has a unique place above it in F_2 and this place is a simple zero for the function x_2, as follows from Lemma 1. Repeating this argument for F_{n+1}/F_n with $n \geq 2$, inductively, we see that $x_1 = 0$ is totally ramified in F_n/F_1 for all values of $n \in \mathbb{N}$. This shows that Equation (1) really defines a tower (see [8, Proposition III.7.10]).

Lemma 2. *For the tower $\mathcal{F}$ over K we have:*

a) $[F_n : K(x_i)] = q^{n-1}$, *for each* $i = 1, 2, \ldots, n$.

b) *The function x_1 has a unique zero P in the field F_n, for each $n \in \mathbb{N}$. The different exponent $d(P)$ with respect to the extension F_n/F_{n-1} is $d(P) = q$. Futhermore, the place P of F_n is unramified in the extension $F_n/K(x_n)$.*

c) *The function x_1 has a unique pole P' in the field F_n, for each $n \in \mathbb{N}$. The different exponent $d(P')$ with respect to the extension F_n/F_{n-1} is $d(P') = 2(q-1)$. Futhermore, the place P' of F_n has ramification index $(q-1)$ with respect to the extension $F_n/K(x_n)$.*

d) *If a place of F_n is neither a zero nor a pole for the function $x_1(x_1 - 1)$, then it is unramified in the extension F_n/F_1.*

Proof: Follows directly from Lemma 1 and Proposition 2. We will just prove here the item c). Consider the following picture (see Figure 2) where the numbers over the edges represent the ramification indices in the corresponding field extensions for the various restrictions of the place P'.

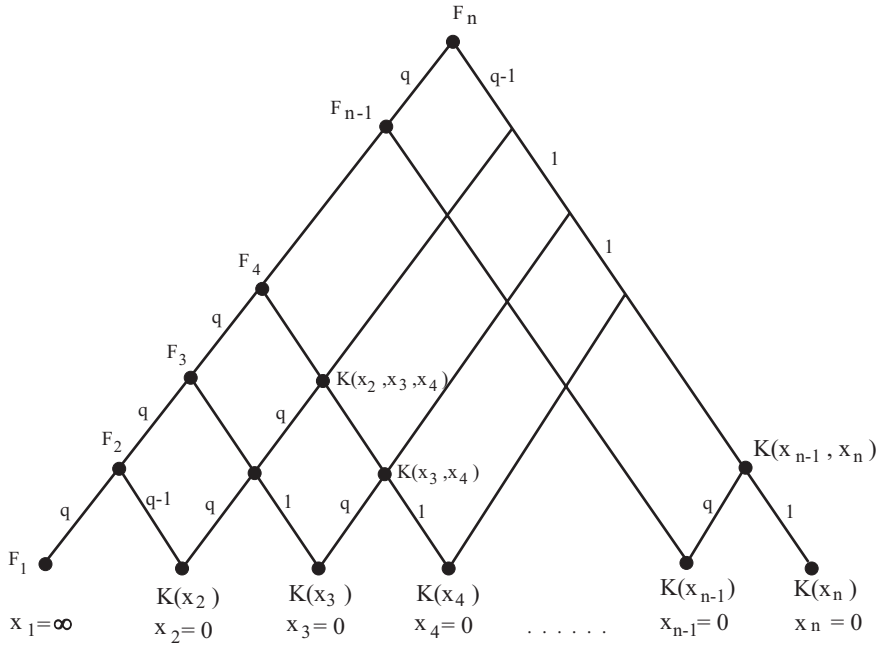

Figure 2

The picture above follows directly from Lemma 1 and explains the assertions concerning ramification indices. Now we determine $d(P')$. For $n = 2$, it follows from the item e) in Lemma 1. Assume now that $n \geq 3$ and consider the following picture:

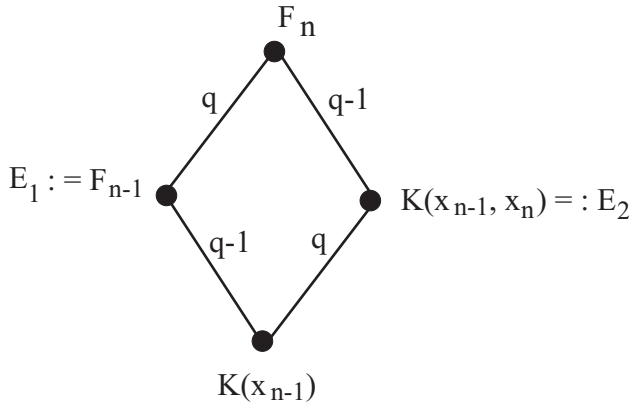

Figure 3

As in Proposition 2, we denote by Q_1, Q_2 and P the restrictions of the place P' of F_n to the subfields E_1, E_2 and $K(x_{n-1})$. We have $d(Q_2|P) = q$, as follows from the item e) in Lemma 1. Since $e(Q_1|P) = q - 1$, it now follows from the item b) in Proposition 2 that

$$d(P'|Q_1) = (q-1) \cdot q - (q-2)(q-1) = 2(q-1).$$

□

From Lemma 2 we still need to analyze the ramification behaviour in the extensions F_n/F_{n-1} of the zeros in F_n for the function $(x_1 - 1)$. Again from Lemma 1 we have two possibilities for a place Q of F_n which is a zero of $(x_1 - 1)$:

Possibility 1: The place Q is a common zero for the functions $(x_i - 1)$, for each $i = 1, 2, \ldots, n$.

In this case Q is unramified in F_n/F_1 and it is totally ramified in the extension $F_n/K(x_n)$.

Possibility 2: There exists $t \in \mathbb{N}$ with $1 \leq t < n$ such that:

a) The place Q is a common zero for the functions $(x_i - 1)$ for $i = 1, 2, \ldots, t$.
b) The place Q is a pole for the function x_{t+1}.
c) The place Q is a zero for the functions x_i for $i = t + 2, \ldots, n$.

Note that condition b) in Possibility 2 above implies the other two conditions a) and c). For treating the places Q satisfying Possibility 2 we consider the following picture (see Figure 4), where again the numbers over the edges are

the ramification indices of the restrictions of such places Q and where we denote $S := q - 1$.

Picture with t = 5

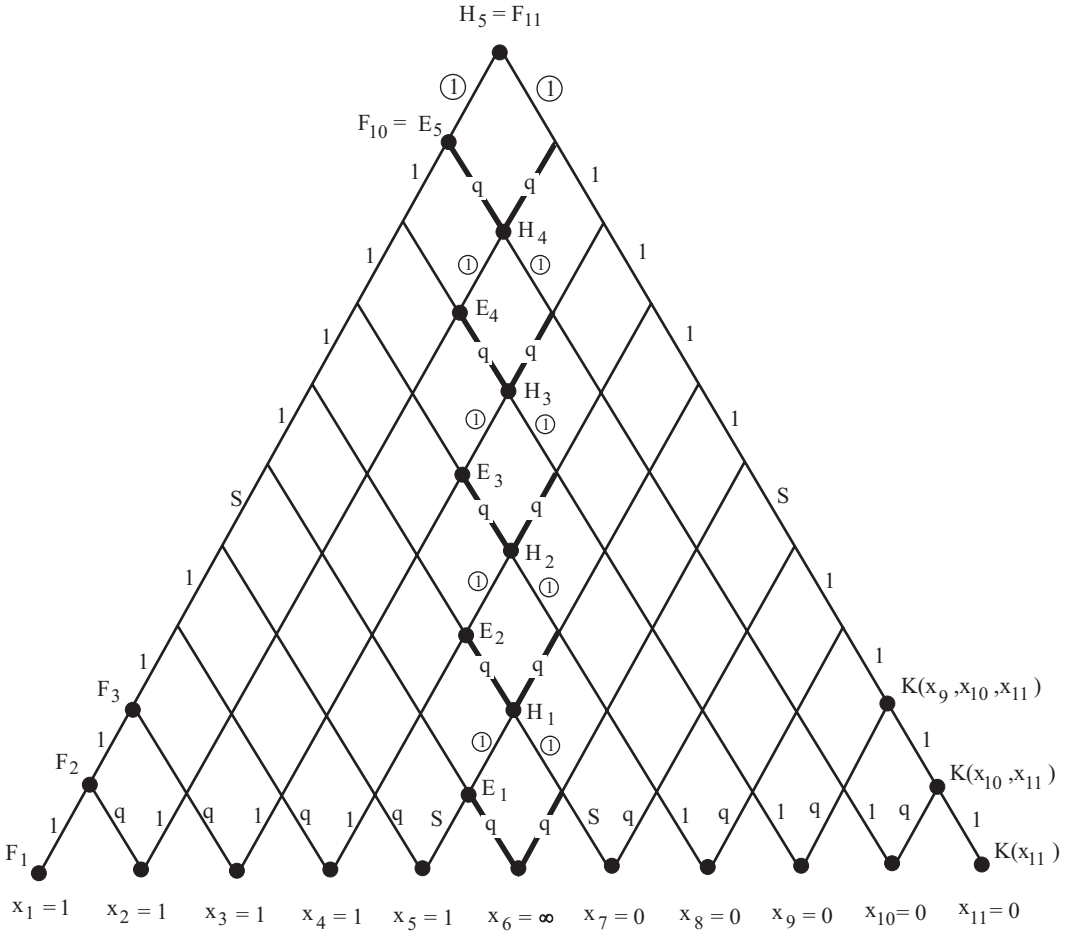

Figure 4

As already indicated in the above figure, we set for $1 \leq k \leq t$:

$$E_k := K(x_{t+1-k}, \ldots, x_{t+k}) \quad \text{and} \quad H_k := E_k(x_{t+k+1}).$$

In the next lemma we will use the following notations:

$$\begin{aligned} &X_i := (x_{i+t+1} - 1) \quad \text{for} \quad i < 0 \ \text{ and } \ X_0 := 1/x_{t+1}; \\ &X_i := -x_{i+t+1} \quad \text{for} \quad i > 0; \\ &Y_k := \prod_{i=-k}^{-1} X_i \quad \text{and} \quad Z_k := \prod_{i=1}^{k} X_i. \end{aligned}$$

Also, we denote by Q_0 the pole of the function x_{t+1} in the rational function field $H_0 := K(x_{t+1})$.

The next lemma is the hardest part of our proof of Theorem 1. The item a) in it explains the encircled ①'s in Figure 4 above, which is the essential point for the explicit determination of the genera (see Lemma 4).

Lemma 3. *For $1 \leq k \leq t$, let E_k and H_k be the function fields defined above. Suppose that Q_k is a place of the field H_k which is a pole for the function x_{t+1} and let P_k denote the restriction of Q_k to the field E_k. Then the following holds:*

a) *The function $f_k := (Z_k - Y_k)/X_0$ is regular at the place Q_k. The minimal polynomial of f_k over E_k is separable modulo the place P_k. In particular, the place Q_k is unramified over E_k; i.e., $e(Q_k|P_k) = 1$.*

b) *The zero-orders at Q_k of the functions X_i are:*

$$v_{Q_k}(X_i) = \begin{cases} q^{k+i} \cdot (q-1) & \text{if } -k \leq i \leq -1 \\ q^k & \text{if } i = 0 \\ q^{k-i} \cdot (q-1) & \text{if } 1 \leq i \leq k. \end{cases}$$

c) *For $i = 1, 2, \ldots, k$, we have that*

$$v_{Q_k}\left(\frac{X_i - X_{-i}}{X_i}\right) \geq q^{k-i}.$$

Proof: We are going to prove the lemma by induction over k. For $k = 1$ we have

$$E_1 = K(X_{-1}, X_0) \quad \text{and} \quad H_1 = E_1(X_1).$$

The place Q_1 is a common zero for X_{-1}, X_0 and X_1. We rewrite Equation (1) as below:

$$\frac{X_1^q}{X_1 + 1} = \frac{X_0^{q-1}}{1 - X_0^q} \tag{3}$$

and

$$\frac{X_{-1}^q}{X_{-1} + 1} = X_0^{q-1} \cdot (1 - X_0). \tag{4}$$

Clearly, $v_{P_1}(X_{-1}) = q - 1$, $v_{P_1}(X_0) = q$ and $e(P_1|Q_0) = q$. Also, the minimal polynomial of $f_1 = (X_1 - X_{-1})/X_0$ over the field E_1 is the following (as follows from Equation (3)):

$$P_{f_1|E_1}(T) = T^q - \frac{1}{1 - X_0^q} \cdot T + \left(\frac{X_{-1}}{X_0}\right)^q - \frac{X_{-1} + 1}{(1 - X_0^q)X_0}.$$

Using Equation (4) we can write

$$P_{f_1|E_1}(T) = T^q - \frac{1}{1-X_0^q} \cdot T + \left(\frac{1+X_{-1}}{1-X_0^q}\right)(X_0^q - X_0^{q-1} - 1).$$

The polynomial above is separable modulo P_1 and hence $e(Q_1|P_1) = 1$. Then we have:

$$v_{Q_1}(X_{-1}) = v_{Q_1}(X_1) = q-1, \quad v_{Q_1}(X_0) = q \text{ and } v_{Q_1}(X_1 - X_{-1}) \geq v_{Q_1}(X_0) = q.$$

Hence $v_{Q_1}\left(\frac{X_1 - X_{-1}}{X_1}\right) \geq 1 = q^0$ and Lemma 3 is proved in the case $k = 1$.

Suppose now $k \geq 2$ and that Lemma 3 holds for $1 \leq j < k$. The place Q_k is a common zero for X_i for $i = -k, \ldots, 0, \ldots, k$. We have the following relations:

$$\frac{1+X_{i+1}^q}{X_{i+1}} = \frac{1+X_i}{X_i^q} \quad \text{for } i = -k, \ldots, -2; \tag{5}$$

$$X_0^{q-1} \cdot (1 - X_0) = \frac{X_{-1}^q}{1+X_{-1}}; \tag{6}$$

$$\frac{1+X_1}{X_1^q} = \frac{1-X_0^q}{X_0^{q-1}} \tag{7}$$

and

$$\frac{1+X_{i+1}}{X_{i+1}^q} = \frac{1+X_i^q}{X_i} \quad \text{for } i = 1, \ldots, k-1. \tag{8}$$

From the induction hypothesis we have $e(P_k|Q_{k-1}) = q$ and

$$v_{P_k}(X_j) = q \cdot v_{Q_{k-1}}(X_j) = \begin{cases} q^{k+j} \cdot (q-1) & \text{for } j = -(k-1), \ldots, -1 \\ q^k & \text{for } j = 0 \\ q^{k-j} \cdot (q-1) & \text{for } j = 1, \ldots, k-1. \end{cases}$$

From the relation between $X_{-(k-1)}$ and X_{-k} given in Equation (5), we also have $v_{P_k}(X_{-k}) = q - 1$. Using that $Z_k = Z_{k-1} \cdot X_k$ and Equation (8) for $i = k-1$, we see that the minimal polynomial of $f_k = (Z_k - Y_k)/X_0$ over the field E_k is given by

$$P_{f_k|E_k}(T) = T^q - A_k \cdot T + B_k, \quad \text{where}$$

$$A_k = \frac{X_{k-1} \cdot Z_{k-1}^{q-1}}{(1+X_{k-1}^q)X_0^{q-1}} \quad \text{and}$$

$$B_k = \left(\frac{Y_k}{X_0}\right)^q - \frac{X_{k-1} \cdot Z_{k-1}^{q-1} \cdot Y_k}{(1+X_{k-1}^q)X_0^q} - \frac{X_{k-1} \cdot Z_{k-1}^q}{(1+X_{k-1}^q)X_0^q}$$

It is easy to see that $v_{P_k}(Z_{k-1}) = q^k - q$ and hence that $v_{P_k}(A_k) = 0$. We are now going to show that $v_{P_k}(B_k) \geq 0$ and this will complete the proof of the item a) in Lemma 3. We can rewrite B_k as below

$$B_k = A_k \cdot \frac{1}{X_0} \left(\frac{Y_k^q (1 + X_{k-1}^q)}{Z_{k-1}^{q-1} \cdot X_{k-1}} - Y_k - Z_{k-1} \right). \tag{9}$$

From the induction hypothesis we have $v_{P_k}(f_{k-1}) \geq 0$; i.e., we have

$$Y_{k-1} = Z_{k-1} + \mathcal{O}(q^k) \quad \text{ at } P_k. \tag{10}$$

Denoting by C_k the term inside the parenthesis in Equation (9); i.e., we have $B_k = A_k \cdot C_k / X_0$, we need to show that $v_{P_k}(C_k) \geq v_{P_k}(X_0) = q^k$.

From $Y_k = Y_{k-1} \cdot X_{-k}$ and Equation (10), we have

$$C_k = \frac{X_{-k}^q \cdot Z_{k-1}}{X_{k-1}} - X_{-k} \cdot Z_{k-1} - Z_{k-1} + \mathcal{O}(q^k) \quad \text{ at } P_k. \tag{11}$$

It follows from Equation (5) with $i = -k$ that

$$\frac{X_{-k}^q}{X_{k-1}} - X_{-k} - 1 = \frac{X_{-(k-1)}}{X_{k-1}} - 1 + \mathcal{O}(q) \quad \text{ at } P_k. \tag{12}$$

Using Equations (11) and (12), the proof that $v_{P_k}(B_k) \geq 0$ will be complete if we show

$$v_{P_k} \left(\frac{X_{k-1} - X_{-(k-1)}}{X_{k-1}} \right) \geq q. \tag{13}$$

Finally the inequality in (13) above follows from the induction hypothesis since

$$v_{Q_{k-1}} \left(\frac{X_i - X_{-i}}{X_i} \right) \geq q^{(k-1)-i}, \quad \text{ for } i = 1, \ldots, k-1,$$

and since we have already observed that $e(P_k | Q_{k-1}) = q$.

From Equations (5) and (8) for $i = -k$ and $i = (k-1)$, we have

$$\left(\frac{X_k - X_{-k}}{X_k} \right)^q = \left(\frac{X_{k-1} - X_{-(k-1)}}{X_{k-1}} \right) + \mathcal{O}(q-1) \quad \text{ at } P_k.$$

The proof of Lemma 3 is complete, since we have $e(Q_k | P_k) = 1$. □

Proof of Theorem 1: To finish now the proof of Theorem 1 is a simple matter. Let $1 \leq t \leq \frac{n-1}{2}$ and let Q be a place of F_n which is a pole for the function x_{t+1}. Then the place Q is totally ramified in $F_{s+1} | F_n$ for all $s \geq n$, as follows from Lemma 3. As in the proof of Lemma 2, the different exponent

is $2(q-1)$ in each step $F_{s+1}|F_s$. It also follows from Lemma 3 that there are exactly q^t places of F_n that are poles for the function x_{t+1}.

Puting this together we get that the different degree of the extension F_n/F_{n-1} is as below:

$$\deg \mathrm{Diff}(F_n|F_{n-1}) = 2(q-1) + 2(q^{[n/2]} - 1).$$

From the different degree above and Riemann-Hurwitz formula, we get

Lemma 4. For the fields F_n in the tower $\mathcal{F}$ considered here, we have:

$$(q-1)\cdot g(F_n) = \begin{cases} (q^{n/2}-1)^2, & \text{if } n \text{ is even} \\ (q^{\frac{n-1}{2}}-1)(q^{\frac{n+1}{2}}-1), & \text{if } n \text{ is odd.} \end{cases}$$

□

Continuing with the proof of Theorem 1, one sees easily that the rational places of $K(x_1)$ corresponding to the roots of $x_1^q + x_1 - 1 = 0$ are completely splitting in $\mathcal{F}$ and hence

$$N(F_n) \geq q \cdot [F_n : F_1] = q^n.$$

This then gives $\lim \dfrac{N(F_n)}{g(F_n)} = q-1.$ □

Remark 1: The tower $\mathcal{F}$ here is a subtower of the tower in [3] and hence this fact gives another proof that $\lambda(\mathcal{F}) = q-1$, as follows from [3, Corollary 2.4]. Indeed, let us denote by $\mathcal{E}$ the tower over K defined inductively as: $E_1 = K(y_1)$ is the rational function field and, for each $n \geq 1$, we have $E_{n+1} = E_n(y_{n+1})$ with the relation

$$y_{n+1}^q + y_{n+1} = \frac{y_n^q}{y_n^{q-1}+1}.$$

Taking $x_n := 1/(1+y_n^{q-1})$, $\forall\, n \in \mathbb{N}$, then one sees that the functions $x_n \in E_n$ satisfy Equation (1). But if one wants to deduce the genus formula in Lemma 4 from the tower $\mathcal{E}$ above, one should consider the following Figure 5:

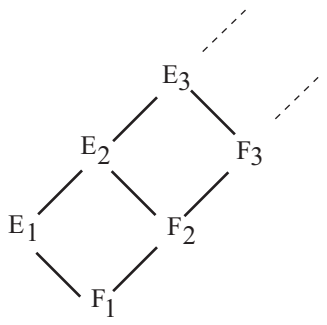

Figure 5

Each of the extensions E_n/F_n is a Kummer extension of degree $q-1$ and satisfies

$$E_n = F_n(y_1) \quad \text{with} \quad y_1^{q-1} = \frac{1-x_1}{x_1}.$$

So in order to deduce $g(F_n)$ from $g(E_n)$ we are led to consider the zeros and poles of the function $(1-x_1)/x_1$ in the field F_n, and hence we cannot avoid the considerations done in the key result here (which is Lemma 3).

References

[1] S. Ballet: Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$, *Finite Fields Appl. 5* (1999), 364–377.

[2] V.G. Drinfeld, S.G. Vladut: Number of points of an algebraic curve, *Funct. Anal. 17* (1983), 53–54.

[3] A. Garcia, H. Stichtenoth: On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory 61* (1996), 248–273.

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

[5] A. Garcia, H. Stichtenoth: On tame towers over finite fields, *J. Reine Angew. Math. 557* (2003), 53–80.

[6] Y. Ihara: Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo 28* (1981), 721–724.

[7] R. Matsumoto: Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes, *IEEE Trans. Inform. Theory 48* (2002), 2122–2124.

[8] H. Stichtenoth: "Algebraic Function Fields and Codes". Springer Universitext, Springer-Verlag, Berlin-Heidelberg, 1993.

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