TOKYO J. MATH.
VOL. 30, NO. 2, 2007

A Note on Optimal Towers over Finite Fields

Takehiro HASEGAWA

Waseda University

(Communicated by K. Taniyama)

Abstract. Recently, under the influence of Elkies' conjecture [2], the optimal recursive towers of algebraic function fields (of one variable) over the finite fields with square cardinality are studied [3, 5, 6]. In this paper, we define the limit

$$\lim_{i\to\infty} \text{(the number of places of degree } n \text{ in } F_i/\mathbf{F}_q\text{)/(genus of } F_i)$$

of a tower $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$ over the finite field $\mathbf{F}_q$. Using this limit, we prove that all the proper constant field extensions of all the optimal towers over the finite fields with square cardinality are not optimal, and we show a simple criterion whether a tower is optimal or not. Moreover, we give many new recursive towers of finite ramification type.

1. Introduction

Let q be a power of a prime p, and $\mathbf{F}_q$ the finite field of cardinality q. In this paper, we deal with (algebraic) function fields F (of one variable) with full constant field $\mathbf{F}_q$. Let $B_n(F) := B_n(F/\mathbf{F}_q)$ be the number of places of degree n of $F/\mathbf{F}_q$. We denote by $g(F)$ the genus of F. A. Garcia and H. Stichtenoth [3] introduced the notion of towers: A tower of function fields over $\mathbf{F}_q$ is a sequence

$$\mathcal{F} := (F_0, F_1, F_2, \ldots)$$

of function fields $F_0/\mathbf{F}_q, F_1/\mathbf{F}_q, F_2/\mathbf{F}_q, \ldots$ with the following properties:

i) each field F_{i+1} is a finite separable extension of F_i of degree> 1.

ii) the genus of F_s is greater than 1 for some s.

They also defined the limit of a tower $\lambda(\mathcal{F}) = \lambda(\mathcal{F}/\mathbf{F}_q) := \lim_{i\to\infty} B_1(F_i)/g(F_i)$. A tower $\mathcal{F}$ is said to be asymptotically good (resp. asymptotically bad) if $\lambda(\mathcal{F}) > 0$ (resp. $\lambda(\mathcal{F}) = 0$). Here we present the value $A(q) := \limsup_{g\to\infty} N_q(g)/g$, where $N_q(g) := \max\{B_1(F) \mid F/\mathbf{F}_q \text{ is a function field of genus } g\}$. Note that $A(q)$ provides an upper bound for $\lambda(\mathcal{F}/\mathbf{F}_q)$. A tower $\mathcal{F}/\mathbf{F}_q$ is said to be (asymptotically) optimal if $\lambda(\mathcal{F}/\mathbf{F}_q) = A(q)$. Y. Ihara [8] (independently, M. A. Tsfasman, S. G. Vlăduţ and T. Zink [12] in some cases) showed that

$$A(q) = \sqrt{q} - 1 \quad \text{for a square } q\,, \tag{1}$$

Received March 24, 2006; revised August 2, 2006
2000 *Mathematics Subject Classifications*: 11R58 (14G15, 14H05).
Key words: finite fields; towers of function fields; the congruence zeta functions.

and V. G. Drinfeld and Vlăduţ [1] proved the so-called Drinfeld-Vlăduţ bound $A(q) \leq \sqrt{q}-1$ for a unconditional q.

Now we generalize the notion of the limit $\lambda(\mathcal{F})$, and present the notation of composite tower (cf, [10] for asymptotically exact families):

DEFINITION 1.1. Let $\mathcal{F} = (F_0, F_1, F_2, \dots)$ be a tower of function fields over $\mathbf{F}_q$, and $\mathbf{F}_{q^n}$ the n-th cyclic Galois extension of $\mathbf{F}_q$. We define the compositum

$$\mathcal{F}\mathbf{F}_{q^n} := (F_0\mathbf{F}_{q^n}, F_1\mathbf{F}_{q^n}, F_2\mathbf{F}_{q^n}, \dots)$$

of $\mathcal{F}$ and $\mathbf{F}_{q^n}$, and the limit of a tower

$$\Delta_n(\mathcal{F}) := \Delta_n(\mathcal{F}/\mathbf{F}_q) := \lim_{i\to\infty} B_n(F_i)/g(F_i)\,.$$

We call $\mathcal{F}\mathbf{F}_{q^n}/\mathbf{F}_{q^n}$ the *composite tower* of $\mathcal{F}/\mathbf{F}_q$ and $\mathbf{F}_{q^n}$, and $\Delta_n(\mathcal{F}/\mathbf{F}_q)$ the *generalized Garcia-Stichtenoth number* (of degree n) of $\mathcal{F}/\mathbf{F}_q$. (The sequence $\mathcal{F}\mathbf{F}_{q^n}$ is a tower over $\mathbf{F}_{q^n}$ and the sequence $(B_n(F_i)/g(F_i))_{i\geq 0}$ is convergent, see Section 2.)

The aim of this paper is to study exact values of $\Delta_n(\mathcal{F})$, and upper and lower bounds for $\Delta_n(\mathcal{F})$. Our main theorems are:

THEOREM 1.2. *Let q be a square. Suppose that $\mathcal{F}$ is an optimal tower of function fields over $\mathbf{F}_q$. Then, for all $n \geq 2$, we obtain*

$$\Delta_n(\mathcal{F}/\mathbf{F}_q) = 0 \quad \text{and} \quad \lambda(\mathcal{F}\mathbf{F}_{q^n}/\mathbf{F}_{q^n}) = \sqrt{q}-1\,.$$

In particular, the composite tower $\mathcal{F}\mathbf{F}_{q^n}$ is not optimal.

Let $\mathbf{P}_F$ denote the set of places of $F/\mathbf{F}_q$. A tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ is said to be tame if each extension F_{i+1}/F_i is tame.

COROLLARY 1.3. *Assume that $\mathcal{F} = (F_0, F_1, F_2, \dots)$ is a tame tower of function fields over $\mathbf{F}_q$ satisfying conditions*

(i) $V_{F_0} := \{P \in \mathbf{P}_{F_0} \mid P$ *is ramified in* F_i/F_0 *for some* $i > 0\}$ *is finite*;

(ii) $Spl_n(\mathcal{F}/\mathbf{F}_q) := \{P \in \mathbf{P}_{F_0} \mid P$ *splits completely in all* F_i/F_0, *and* $\deg P = n\}$ *is non-empty for some* $n \geq 2$. (*For brevity, we write* Spl_n *as* $Spl_n(\mathcal{F}/\mathbf{F}_q)$.)

Then $\lambda(\mathcal{F}) < \sqrt{q}-1$. *Moreover, if q is a square, then $\mathcal{F}$ is not optimal.*

A tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ is said to be of finite ramification type if $V_{F_0} < \infty$.

Perhaps, whether a recursive tower of the Kummer type [5], [7] (resp. the Artin-Schreier type [3]) is optimal or not is dependent on the characteristic p (resp. the defining equation). So optimal recursive towers (of degree 2) of the Kummer type should be constructed as follows (see Section 4):

- First: Set two polynomials $ax^2+bx+c, \alpha x+\beta \in \mathbf{Z}[x]$ with $a\cdot\alpha \neq 0$;
- Second: Choose one prime number p such that the reduction $\bar{a}x^2+\bar{b}x+\bar{c}$ at p is a separable polynomial over $\mathbf{F}_p$, $\bar{a}\cdot\bar{\alpha} \neq 0$ and $\bar{\alpha}x+\bar{\beta} \nmid \bar{a}x^2+\bar{b}x+\bar{c}$;

- Third: By increasing the value of n from 1, find a finite field $\mathbf{F}_{p^{2n}}$ over which the recursive tower $\mathcal{F}$ given by $y^2 = (\bar{a}x^2 + \bar{b}x + \bar{c})/(\bar{\alpha}x + \bar{\beta})$ is optimal.

In general, this algorithm is not deterministic. However, if a tower $\mathcal{F}$ over $\mathbf{F}_{p^{2n}}$ is optimal for some n, this finishes by Theorem 1.2, because the composite towers $\mathcal{F}\mathbf{F}_{p^{2nm}}$ over $\mathbf{F}_{p^{2nm}}$ are no longer optimal for all $m > 1$.

The contents of this paper are as follows: In Section 2, we show the convergence of the sequence in Definition 1.1 (see Proposition 2.2), and we present some simple properties about the generalized Garcia-Stichtenoth numbers $\Delta_n(\mathcal{F})$ without proofs, which are generalizations of the results [4, 6] and [7] in the ordinary cases $\lambda(\mathcal{F})$ (see Propositions 2.3 and 2.4 and 2.5). The first half of Section 3 gives Keylemma in order to prove the main theorems. A similar result to this keylemma can be obtained from Corollary 1 in [10]. However, our proof that uses the same techniques as that of the Drinfeld-Vlăduţ bound is completely different from his, and ours is very elementary. The latter half of Section 3 shows Theorem 1.2 and Corollary 1.3. In Section 4, we compute several examples. From them, we see that the lower and upper bounds in Section 2 and 3 can not be improved (see Examples 4.2 and 4.3).

In this paper, we use the notation of the textbook [9] of Stichtenoth.

2. Preliminaries

In the section, we will prove that there exists the limit of a tower $\Delta_n(\mathcal{F})$, and we give three elementary properties of this limit. First, we recall some facts about constant field extensions (cf, [9] Chap. III.6). Let F be a function field over $\mathbf{F}_q$ of genus g. Fix an algebraic closure $\bar{\mathbf{F}}_q$ of $\mathbf{F}_q$ and the constant field extension $F\bar{\mathbf{F}}_q$ of F. By $F\mathbf{F}_{q^n} (\subseteq F\bar{\mathbf{F}}_q)$, we denote the compositum of the fields F and $\mathbf{F}_{q^n}$. Then $F\mathbf{F}_{q^n}$ is a function field with full constant field $\mathbf{F}_{q^n}$, and its genus $g(F\mathbf{F}_{q^n})$ is equal to g (see, [9] III.6.1 and III.6.3). Hence, if $\mathcal{F}$ is a tower over $\mathbf{F}_q$, then so $\mathcal{F}\mathbf{F}_{q^n}$ is over $\mathbf{F}_{q^n}$ from Galois Theory. Second, we show that the sequence $(B_n(F_i)/g(F_i))$ is convergent.

LEMMA 2.1. *For any tower $\mathcal{F}$, the sequence $(B_1(F_i)/g(F_i))_{i\geq 0}$ is convergent.*

PROOF. See Corollary 2.2 in [3]. □

PROPOSITION 2.2. *For every $n > 0$ and any tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$, the sequence $(B_n(F_i)/g(F_i))_{i\geq 0}$ is convergent.*

PROOF. We proceed by induction on n. The assertion is trivial for $n = 1$ by Lemma 2.1. Recall the formula

$$B_1(F_i\mathbf{F}_{q^n}/\mathbf{F}_{q^n}) = B_1(F_i/\mathbf{F}_q) + \sum_{d|n, d\neq 1} d \cdot B_d(F_i/\mathbf{F}_q) \tag{2}$$

(see, [9] p178). Assume that $n > 1$ and that the limits $\Delta_m(\mathcal{F}/\mathbf{F}_q)$ exist for all $m < n$. By dividing both sides of the formula (2) by the genus $g(F_i)$ (note that $g(F_i) > 1$ for a sufficiently large i), we get $B_1(F_i\mathbf{F}_{q^n}/\mathbf{F}_{q^n})/g(F_i) = B_1(F_i/\mathbf{F}_q)/g(F_i) + \sum_{d|n,d\neq 1} d \cdot B_d(F_i/\mathbf{F}_q)/g(F_i)$.

Since $(B_1(F_i\mathbf{F}_{q^n}/\mathbf{F}_{q^n})/g(F_i))$ and $(B_m(F_i)/g(F_i))$ are convergent (for all $m < n$) from Lemma 2.1 and the assumption of induction, the sequence $(B_n(F_i)/g(F_i))$ is also convergent from the above equation and we obtain

$$\lambda(\mathcal{F}\mathbf{F}_{q^n}/\mathbf{F}_{q^n}) = \lambda(\mathcal{F}/\mathbf{F}_q) + \sum_{d|n, d\neq 1} d \cdot \Delta_d(\mathcal{F}/\mathbf{F}_q)\,. \tag{3}$$

This completes the proof of this proposition. □

REMARK. (a) It follows from the formula (3) and the Drinfeld-Vlăduţ bound that if $\mathcal{F}/\mathbf{F}_q$ is asymptotically good, then so $\mathcal{F}\mathbf{F}_{q^n}/\mathbf{F}_{q^n}$ is (for each n) and that

$$\Delta_n(\mathcal{F}/\mathbf{F}_q) \leq (\sqrt{q^n} - 1)/n\,.$$

(b) By using the formula (2) and the Möbius inversion formula (see, [9] p178), it can be also shown that $(B_n(F_i)/g(F_i))$ is convergent.

Last, we generalize the theorems in [4, 6] and [7]. Their proofs are the same as the original. The Key is to use $B_1(F\mathbf{F}_{q^n}) \geq n \cdot B_n(F)$ obtained from the formula (2).

PROPOSITION 2.3. *Suppose that a tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ over $\mathbf{F}_q$ is given by*

$$F_i = F_{i-1}(x_i) = \mathbf{F}_q(x_0, x_1, \dots, x_i)\,,$$

where x_0 is transcendental over $\mathbf{F}_q$ and x_i (for each $i \geq 1$) satisfies an absolutely irreducible polynomial $\Phi(x_{i-1}, Y) \in F_{i-1}[Y]$ with $\Phi(X, Y) \in \mathbf{F}_q[X, Y]$. Assume that Φ is separable both in X and Y, and $\deg_X \Phi \neq \deg_Y \Phi$. Then $\Delta_n(\mathcal{F}) = 0$ for all n.

We do not know whether the converse of this proposition is true or not, namely, if Φ is separable both in X and Y, $\deg_X \Phi = \deg_Y \Phi$ and $\#V_{F_0} < \infty$, then $\lambda(\mathcal{F}\mathbf{F}_{q^n}/\mathbf{F}_{q^n}) > 0$ for a sufficiently large n? Several numerical computations of this question can be seen in Example 4.3 and Remark of the last section.

The following is the best possible lower bound for tame towers (see Example 4.3).

PROPOSITION 2.4. *Let $n > 0$. Suppose that $\mathcal{F}/\mathbf{F}_q$ is a tame tower with $\#V_{F_0} < \infty$ and $\#Spl_n \neq 0$. Then $\Delta_n(\mathcal{F}) \geq 2 \cdot \#Spl_n/(2g(F_0) - 2 + \sum_{P\in V_{F_0}} \deg P) > 0$.*

Next, we give an upper bound of $\Delta_n(\mathcal{F})$.

PROPOSITION 2.5. *Let $s > 0$ and $n > 0$. Assume that $\mathcal{F}$ is a tower satisfying the condition: the set $\Sigma_s = \left\{l \in \mathbf{N} \,\middle|\, \mathcal{F} \text{ satisfies the inequalities } \frac{\deg \mathrm{Diff}(F_{s+j}/F_{s+j-1})}{[F_{s+j}:F_{s+j-1}]-1} \geq [F_{s+j-1} : F_0] + [F_1 : F_0],\ \text{for all } 1 \leq j \leq l\right\}$ is non-empty. Then, for every $l \in \Sigma_s$, we obtain $\Delta_n(\mathcal{F}) \leq 2t_n/(2g(F_0) - 2 + R(s,l) + d_s)$, where $R(s,l) := l + \frac{[F_{s+l}:F_s]-1}{[F_{s+l}:F_1]} - \sum_{j=1}^{l} \frac{1}{[F_{s+j}:F_{s+j-1}]}$, $t_n := \lim_{i\to\infty} \frac{B_n(F_i)}{[F_i:F_0]}$ and $d_s := \frac{\deg \mathrm{Diff}(F_s/F_0)}{[F_s:F_0]}$.*

3. Proofs of the main theorems

We show the main results. In their courses, we need three lemmas which will be proved first. Let q be a power of a prime.

LEMMA 3.1. *Let m be a non-negative integer. Then,*

(a) $\sum_{s=0}^{m}(m+1-s)\cdot(\sqrt{q})^{-s} = \frac{(m+1)\cdot q-(m+2)\cdot\sqrt{q}+(1/\sqrt{q})^m}{(\sqrt{q}-1)^2}$;

(b) $\sum_{s=0}^{m}(m+1-s)\cdot(\sqrt{q})^{s} = \frac{(\sqrt{q})^{m+2}-(m+2)\cdot\sqrt{q}+m+1}{(\sqrt{q}-1)^2}$.

PROOF. (a) First recall an equation $\sum_{s=0}^{m+1} T^s = (1-T^{m+2})/(1-T)$, where T is an indeterminate element. Next the derivative of the equation (at T) is given by $\sum_{s=0}^{m}(s+1)\cdot T^s = \frac{(m+1)\cdot T^{m+2}-(m+2)\cdot T^{m+1}+1}{(1-T)^2}$. Multiplying both sides of the equation by $1/T^m$, we get $\sum_{s=0}^{m}(s+1)\cdot T^{s-m} = \frac{(m+1)\cdot T^2-(m+2)\cdot T+(1/T)^m}{(1-T)^2}$; that is, $\sum_{s=0}^{m}(m+1-s)\cdot T^{-s} = \frac{(m+1)\cdot T^2-(m+2)\cdot T+(1/T)^m}{(1-T)^2}$. Now substituting $\sqrt{q}$ for T of the equation, we obtain the result.

(b) Replacing T of the same equation by $1/\sqrt{q}$, we obtain the other result. □

Here $|r|$ (resp. $\bar{r}$) denotes the absolute value (resp. the complex conjugate) of a complex number r.

LEMMA 3.2. *Let $m > 0$, and let β be a complex number with $|\beta| = 1$. Then, $m+1+\sum_{s=1}^{m}(m+1-s)\cdot\beta^s+\sum_{s=1}^{m}(m+1-s)\cdot\beta^{-s}$ is a non-negative real number.*

PROOF. Note that $m+1+\sum_{s=1}^{m}(m+1-s)\cdot\beta^s+\sum_{s=1}^{m}(m+1-s)\cdot\beta^{-s} = \sum_{s=-m}^{m}(m+1-|s|)\cdot\beta^s$. Since $\beta\cdot\bar{\beta} = 1$ by our assumption, we obtain $|\sum_{s=0}^{m}\beta^s|^2 = \left(\sum_{s=0}^{m}\beta^s\right)\cdot\left(\sum_{t=0}^{m}\bar{\beta}^t\right) = \left(\sum_{s=0}^{m}\beta^s\right)\cdot\left(\sum_{t=0}^{m}\beta^{-t}\right)$, i.e. $\left(\sum_{s=0}^{m}\beta^s\right)\cdot\left(\sum_{t=0}^{m}\beta^{-t}\right) = \sum_{s,t=0}^{m}\beta^{s-t} = \sum_{s=-m}^{m}(m+1-|s|)\cdot\beta^s$. As a consequence, we get $m+1+\sum_{s=1}^{m}(m+1-s)\cdot\beta^s+\sum_{s=1}^{m}(m+1-s)\cdot\beta^{-s} = |\sum_{s=0}^{m}\beta^s|^2 \geq 0$. This completes the proof of the claim. □

The congruence zeta function $Z(t) = Z_F(t)$ (resp. L-polynomial $L(t) = L_F(t)$) of a function field $F/\mathbf{F}_q$ is defined as follows: $Z(0) := 1$ and $Z(t) := \sum_{n=1}^{\infty} B_1(F\mathbf{F}_{q^n})t^{n-1}$ (resp. $L(t) := (1-t)(1-qt)\cdot Z(t)$). We know that $L(t)$ factors in $\mathbf{C}[t]$ in the form $L(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$, $\alpha_j\cdot\alpha_{g+j} = q$ for $j = 1,\ldots,g$, where g is the genus of F (see, [9] V.1.15 (e)), and the reciprocals of the roots of $L(t)$ satisfy $|\alpha_i| = \sqrt{q}$ for $i = 1,\ldots,2g$ from the Hasse-Weil theorem. Putting $\beta_i := \alpha_i/\sqrt{q}$ for $i = 1,\ldots,2g$, we see that $\beta_j\cdot\beta_{g+j} = 1$ holds for $j = 1,\ldots,g$, and $|\beta_i| = 1$ for $i = 1,\ldots,2g$. Thus we obtain

$$\sum_{i=1}^{2g}\beta_i^s = \sum_{i=1}^{2g}\left(\frac{1}{\beta_i}\right)^s \tag{4}$$

for all positive integers s. By ([9] V.1.16), we have $B_1(F\mathbf{F}_{q^s}) = q^s + 1 - \sum_{i=1}^{2g}(\beta_i \cdot \sqrt{q})^s$ for all s. Multiplying both sides of this equation by $(1/\sqrt{q})^s$, we get

$$\frac{B_1(F\mathbf{F}_{q^s})}{(\sqrt{q})^s} = (\sqrt{q})^s + \left(\frac{1}{\sqrt{q}}\right)^s - \sum_{i=1}^{2g} \beta_i^s . \tag{5}$$

LEMMA 3.3 (Keylemma). *Let $\mathcal{F}/\mathbf{F}_q$ be a tower. Then, for each $n \geq 2$, we obtain $\Delta_n(\mathcal{F}) \leq c \cdot \big(1 - \lambda(\mathcal{F})/(\sqrt{q} - 1)\big) \leq c$ for some constant $c > 0$ (depending on n).*

PROOF. Fix any integer $n \geq 2$. As the genus $g(F_i)$ tends to ∞ for $i \to \infty$ from definition of towers and the Hurwitz Genus Formula, there exists the function field $F_j/\mathbf{F}_q$ such that $n < \log[\log_q g(F_j)^2]$, where $[r]$ denotes the integer part of the real number r. Here we set $m := m(j) := [\log_q g(F_j)^2]$, $l := l(j) := [(\log m)/n] \geq 1$ and $g = g(F_j)$. Let $\alpha_1, \ldots, \alpha_{2g}$ be the reciprocals of the roots of $L_{F_j}(t)$, and $\beta_i = \alpha_i/\sqrt{q}$ for $i = 1, \ldots, 2g$. Note that each β_i satisfies the condition in Lemma 3.2. Summing the values in the lemma over $i = 1, \ldots, 2g$, we obtain $2g(m+1) + \sum_{s=1}^{m}(m+1-s)\sum_{i=1}^{2g}\beta_i^s + \sum_{s=1}^{m}(m+1-s)\sum_{i=1}^{2g}\beta_i^{-s} \geq 0$; that is, by Eq.(4), $g(m+1) + \sum_{s=1}^{m}(m+1-s)\sum_{i=1}^{2g}\beta_i^s \geq 0$. From Eq. (5), we get

$$g(m+1) + \sum_{s=1}^{m}(m+1-s)\left((\sqrt{q})^s + \left(\frac{1}{\sqrt{q}}\right)^s - \frac{B_1(F\mathbf{F}_{q^s})}{(\sqrt{q})^s}\right) \geq 0 ;$$

thus,

$$g(m+1) + \sum_{s=1}^{m}(m+1-s)\left((\sqrt{q})^s + \left(\frac{1}{\sqrt{q}}\right)^s\right) \geq \sum_{s=1}^{m}(m+1-s)\frac{B_1(F_j\mathbf{F}_{q^s})}{(\sqrt{q})^s} . \tag{6}$$

On the other hand, by the formula (2), we obtain

$$\begin{aligned} g(m+1) &+ \sum_{s=1}^{m}(m+1-s)\left((\sqrt{q})^s + \left(\frac{1}{\sqrt{q}}\right)^s\right) - B_1(F_j) \cdot \sum_{s=1}^{m}\frac{m+1-s}{(\sqrt{q})^s} \\ &\geq \sum_{s=2}^{m}\frac{m+1-s}{(\sqrt{q})^s} \cdot \sum_{d|s,d>1} d \cdot B_d(F_j) . \end{aligned}$$

Noting that $n \geq 2, l \geq 1$ and $B_s(F_j)$ is a non-negative integer for all s, we obtain

$$\begin{aligned} \sum_{s=2}^{m}\frac{m+1-s}{(\sqrt{q})^s} \cdot \sum_{d|s,d>1} d \cdot B_d(F_j) &\geq n \cdot B_n(F_j) \cdot \sum_{t=1}^{l}\frac{m+1-tn}{(\sqrt{q})^{tn}} \\ &\geq (m+1-ln)n \cdot B_n(F_j) \cdot \sum_{t=1}^{l}\left(\frac{1}{\sqrt{q^n}}\right)^t \\ &= \frac{m+1-ln}{c} \cdot \left(1 - \left(\frac{1}{\sqrt{q^n}}\right)^l\right) \cdot B_n(F_j) , \end{aligned}$$

where $c = (\sqrt{q^n} - 1)/n$. From Lemma 3.1, we get

$$\begin{aligned} g(m+1) &+ \frac{(\sqrt{q})^{m+2} - (m+2)\sqrt{q} + m + 1}{(\sqrt{q}-1)^2} \\ &+ \frac{(m+1)q - (m+2)\sqrt{q} + (1/\sqrt{q})^m}{(\sqrt{q}-1)^2} - 2(m+1) \\ &- B_1(F_j) \cdot \left(\frac{(m+1)q - (m+2)\sqrt{q} + (1/\sqrt{q})^m}{(\sqrt{q}-1)^2} - (m+1) \right) \\ &\geq \frac{m+1-ln}{c} \cdot \left(1 - \left(\frac{1}{\sqrt{q^n}} \right)^l \right) \cdot B_n(F_j)\,. \end{aligned}$$

Multiplying both sides of this inequality by $1/g(m+1)$, we get

$$\begin{aligned} 1 &+ \frac{(\sqrt{q})^{m+2} - (m+2)\sqrt{q} + m + 1}{g(m+1)(\sqrt{q}-1)^2} \\ &+ \frac{(m+1)q - (m+2)\sqrt{q} + (1/\sqrt{q})^m}{g(m+1)(\sqrt{q}-1)^2} - \frac{2}{g} \\ &- \frac{B_1(F_j)}{g} \cdot \left(\frac{(m+1)q - (m+2)\sqrt{q} + (1/\sqrt{q})^m}{(m+1)(\sqrt{q}-1)^2} - 1 \right) \\ &\geq \frac{1}{c} \cdot \frac{B_n(F_j)}{g} \cdot \frac{m+1-ln}{m+1} \cdot \left(1 - \left(\frac{1}{\sqrt{q^n}} \right)^l \right). \end{aligned}$$

This shows that $1 - \lambda(\mathcal{F})/(\sqrt{q}-1) \geq (1/c) \cdot \Delta_n(\mathcal{F})$, because it is easily seen that

$$\frac{(\sqrt{q})^{m+2} - (m+2)\sqrt{q} + m + 1}{g(m+1)(\sqrt{q}-1)^2} \to 0\,;$$

$$\frac{(m+1)q - (m+2)\sqrt{q} + (1/\sqrt{q})^m}{g(m+1)(\sqrt{q}-1)^2} \to 0\,;$$

$$\frac{(m+1)q - (m+2)\sqrt{q} + (1/\sqrt{q})^m}{(m+1)(\sqrt{q}-1)^2} - 1 \to \frac{1}{\sqrt{q}-1}$$

for $j \to \infty$. This finishes the proof of Lemma 3.3. □

We now begin the proofs of the main theorems.

PROOF OF THEOREM 1.2. Recall that $A(q) = \sqrt{q} - 1$ by Eq. (1). Since $\mathcal{F}$ is optimal, we obtain $\lambda(\mathcal{F}/\mathbf{F}_q) = A(q) = \sqrt{q} - 1$. It follows from Lemma 3.3 that $\Delta_n(\mathcal{F}/\mathbf{F}_q) = 0$ for all $n \geq 2$. So, from the formula (3), we obtain

$$\lambda(\mathcal{F}\mathbf{F}_{q^n}/\mathbf{F}_{q^n}) = \lambda(\mathcal{F}/\mathbf{F}_q) = \sqrt{q} - 1 \qquad \text{for all} \quad n \geq 2\,.$$

Hence $\mathcal{F}\mathbf{F}_{q^n}$ is not optimal since $\lambda(\mathcal{F}\mathbf{F}_{q^n}/\mathbf{F}_{q^n}) = \sqrt{q} - 1 < A(q^n) = \sqrt{q^n} - 1$. □

PROOF OF COROLLARY 1.3. It follows from Proposition 2.4 and Lemma 3.3 that

$$0 < \Delta_n(\mathcal{F}) \leq c \cdot \frac{\sqrt{q}-1-\lambda(\mathcal{F})}{\sqrt{q}-1}.$$

Thus we obtain $\sqrt{q}-1-\lambda(\mathcal{F}) > 0$. If q is a square, then $\lambda(\mathcal{F}) < \sqrt{q}-1 = A(q)$ by Eq. (1). Therefore $\mathcal{F}$ is not optimal. This completes the proof of Corollary 1.3. □

4. Examples

In this section, we state several examples of our results and new recursive towers of finite ramification type. Firstly, we introduce an example of the Artin-Schreier type.

EXAMPLE 4.1 ([3]). Consider the tower $\mathcal{F}/\mathbf{F}_{q^2}$ given recursively by the so-called Garcia-Stichtenoth equation $y^q + y = x^q/(x^{q-1}+1)$. Then, since this is optimal, we obtain $\Delta_n(\mathcal{F}) = 0$ and $\lambda(\mathcal{F}\mathbf{F}_{q^{2n}}) = q-1$ for all $n \geq 2$ by Theorem 1.2.

Secondly, we give a tower that attain the upper bound of Lemma 3.3, which is of the Kummer type.

EXAMPLE 4.2 ([2] Equation 45). Let $p \geq 5$, and let $\mathcal{G}/\mathbf{F}_p$ be the tower given recursively by $y^2 = x(x+3)/(x-1)$. Then $\lambda(\mathcal{G}) = 0$ and $\Delta_2(\mathcal{G}) = (p-1)/2$.

REMARK. It can be shown that the tower $\mathcal{G}\mathbf{F}_{p^2}/\mathbf{F}_{p^2}$ is optimal.

Thirdly, we introduce a tower whose generalized Garcia-Stichtenoth number is equal to its lower bound in Proposition 2.4.

EXAMPLE 4.3 ([5] Example 4.3). Consider the tower $\mathcal{T}_1/\mathbf{F}_q$ defined recursively by the equation $y^2 = x(x-1)/(x+1)$. Then,

$$\lambda(\mathcal{T}_1/\mathbf{F}_q) = \begin{cases} 0 & \text{if } q = 3\,; \\ 2/3 & \text{if } q = 9^n\,, \end{cases} \qquad \Delta_{2n}(\mathcal{T}_1/\mathbf{F}_3) = \begin{cases} 1/3 & \text{if } n = 1\,; \\ 0 & \text{if } n \geq 2 \end{cases}$$

from the formula (3).

REMARK. In the tower $\mathcal{T}_1/\mathbf{F}_3$, we know that

$$V_{T_0} = \{\infty, P_{x_0}, P_{x_0+1}, P_{x_0-1}, P_{x_0^2+x_0-1}, P_{x_0^2-x_0-1}\} \quad \text{and} \quad Spl_2 = \{P_{x_0^2+1}\}\,,$$

where ∞ is the infinite place of T_0 and $P_{p(x)}$ is the zero of $p(x)$ (see, [9] Chap. I.2). Hence we obtain $\Delta_2(\mathcal{T}_1/\mathbf{F}_3) \geq \frac{2\cdot 1}{2g(T_0)-2+8} = \frac{1}{3}$ from Proposition 2.4 since $g(T_0) = 0$ and $\sum_{P\in V_{T_0}} \deg P = 8$. As a consequence, we see that this lower bound can not be improved.

REMARK ([5] Example 4.5). Suppose that $\mathcal{T}_2/\mathbf{F}_q$ is given by the equation $y^2 = x(x+1)/(x-1)$. Then, $\lambda(\mathcal{T}_2/\mathbf{F}_3) = \lambda(\mathcal{T}_2/\mathbf{F}_9) = 0$ and $\lambda(\mathcal{T}_2/\mathbf{F}_{81^n}) = 2$ for $n \geq 1$.

Next, we list the towers over $\mathbf{F}_{p^2}$ $(p = 3, 5, 7)$ of finite ramification type defined recursively by the specific equation

$$y^2 = \;(f(x) :=)\; \frac{ax^2 + bx + c}{\alpha x + \beta}\,, \quad a, b, c, \alpha, \beta \in \mathbf{F}_p, a \cdot \alpha \neq 0\,.$$

By the following proposition, without loss of the generality, we can assume $a = \alpha = 1$.

PROPOSITION 4.4. *Let q be a power of $p \geq 3$. Suppose that $\mathcal{F}/\mathbf{F}_q$ (resp. $\mathcal{G}/\mathbf{F}_q$) is the tower given recursively by the equation*

$$y^2 = f(x) \quad \left(\textit{resp.}\quad y^2 = \frac{x^2 + b'x + c'}{x + \beta'}, \quad b' = \frac{b\alpha}{a^2}, c' = \frac{c\alpha^2}{a^3}, \beta' = \frac{\beta}{a}\right).$$

Then the generalized Garcia-Stichtenoth numbers of $\mathcal{F}$ are equal to those of $\mathcal{G}$.

PROOF. Substituting $(\frac{\alpha}{a}x, \frac{\alpha}{a}y)$ for (x, y) of the defining equation of $\mathcal{G}$, we obtain that of $\mathcal{F}$. So the asymptotic behavior of places in $\mathcal{G}$ corresponds to that in $\mathcal{F}$, that is, $B_n(G_i) = B_n(F_i)$ and $g(G_i) = g(F_i)$ for all i, and $\Delta_n(\mathcal{G}) = \Delta_n(\mathcal{F})$ for each n. □

The following recursive towers are of finite ramification type. Using Proposition 2.4, we see that the six towers $\mathcal{T}_4, \mathcal{T}_{11}, \mathcal{T}_{12}, \mathcal{T}_{17}, \mathcal{T}_{19}$ and $\mathcal{T}_{21}$ are optimal.

	$f(x)$	Reference
• Case $p = 3$		
$\mathcal{T}_1$:	$x(x-1)/(x+1)$;	[5] Example 4.3
$\mathcal{T}_2$:	$x(x+1)/(x-1)$;	[5] Example 4.5
$\mathcal{T}_3$:	$(x+1)(x-1)/x$;	
$\mathcal{T}_4$:	$(x^2+1)/x$;	[5] Notation 5.1
$\mathcal{T}_5$:	$(x^2-x-1)/(x+1)$;	
$\mathcal{T}_6$:	$(x^2+x-1)/(x-1)$.	
• Case $p = 5$		
$\mathcal{T}_7$:	$x(x+1)/(x-1)$;	[5] Example 4.5
$\mathcal{T}_8$:	$x(x+2)/(x+1)$;	[5] Example 4.7
$\mathcal{T}_9$:	$(x+1)(x-2)/(x+2)$;	
$\mathcal{T}_{10}$:	$(x+2)(x-1)/(x-2)$;	
$\mathcal{T}_{11}$:	$x(x-2)/(x-1)$;	[2] Equation 45
$\mathcal{T}_{12}$:	$(x-1)(x+1)/x$;	[5] Notation 5.1
$\mathcal{T}_{13}$:	$(x+1)(x-2)/x$;	
$\mathcal{T}_{14}$:	$(x^2-x+2)/(x+1)$;	
$\mathcal{T}_{15}$:	$(x^2-2x-1)/x$;	
$\mathcal{T}_{16}$:	$(x^2+2)/(x+2)$.	
• Case $p = 7$		
$\mathcal{T}_{17}$:	$x(x+1)/(x-1)$;	[5] Example 4.5
$\mathcal{T}_{18}$:	$x(x+2)/(x-1)$;	
$\mathcal{T}_{19}$:	$x(x+3)/(x-1)$;	[2] Equation 45

$\mathcal{T}_{20}$: $(x^2+1)/(x+1)$;

$\mathcal{T}_{21}$: $(x^2-3)/x$. [5] Notation 5.1

Here, in order to compute $\lambda(\mathcal{T}_1)$ and $\lambda(\mathcal{T}_8)$, we give the following result:

PROPOSITION 4.5. *Let q be a power of a prime $p \geq 3$ and let $a, b \in \mathbf{F}_q, a \neq b$. Consider the tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ over $\mathbf{F}_q$ defined recursively by the equation*

$$y^2 = \frac{(x-a)(x-b)}{x - \dfrac{ab-a-b}{a+b}}.$$

If $a+b = -\beta^2$ for some $\beta \in \mathbf{F}_q$, then the places $P_{x_0+\beta}$ and $P_{x_0-\beta}$ in $F_0/\mathbf{F}_q$ split completely in the extensions F_i/F_0 for all i.

PROOF. We show the claim by using induction on i and the Kummer's theorem ([9] III.3.7). First, put $P = P_{x_0-\beta}$ and

$$\varphi(T) = T^2 - \frac{(x_0-a)(x_0-b)}{x_0 - \dfrac{ab-a-b}{a+b}}.$$

Then $\varphi(T) \in \mathcal{O}_P[T]$ as $\frac{ab-a-b}{a+b} \neq \beta$, where $\mathcal{O}_P$ is the discrete valuation ring of P. In fact, $\frac{ab-a-b}{a+b} = \beta$ implies $\beta^2 - (a+b)\beta + ab = 0$ (since $a+b = -\beta^2$). Therefore $\beta = a$ or b, and then the defining equation of $\mathcal{F}$ is $y^2 = x - a$ or $x - b$. No towers can be constructed from such an equation, which is a contradiction.

In $\mathcal{O}_P/P[T]$ $(= \mathbf{F}_q[T])$,

$$\bar{\varphi}(T) = T^2 - \frac{(\beta-a)(\beta-b)}{\beta - \dfrac{ab-a-b}{a+b}} = T^2 - \beta^2 = (T-\beta)(T+\beta).$$

Similarly, for the other place $P_{x_0+\beta}$, we obtain

$$\bar{\varphi}(T) = T^2 - \frac{(-\beta-a)(-\beta-b)}{-\beta - \dfrac{ab-a-b}{a+b}} = (T-\beta)(T+\beta).$$

The assertion follows immediately from the Kummer's theorem. □

By this proposition and Proposition 2.4, we see that $\lambda(\mathcal{T}_1) \geq 2/3$ and $\lambda(\mathcal{T}_8) \geq 1$. It can be shown from direct computations that the equalities hold above.

ACKNOWLEDGEMENT. The author is deeply grateful to Prof. Shoichi Kondo, Weseda University, for his valuable advice, constant guidance and encouragement. The author also thanks the referee for his valuable comments and careful reviews on the first version of this paper.

References

[1] V. G. DRINFELD and S. G. VLĂDUŢ, Number of points of an algebraic curve, Functional Anal. Appl. **17** (1983), 53–54.

[2] N. D. ELKIES, Explicit modular towers, in: T. Basar and A. Vardy (eds.), Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (1997), 23–32.

[3] A. GARCIA and H. STICHTENOTH, On the asymptotic behavior of some towers of function fields over finite fields, J. Number Theory **61** (1996), 248–273.

[4] A. GARCIA and H. STICHTENOTH, Skew pyramids of function fields are asymptotically bad, in: J. BUCHMANN et al. (eds.), *Coding Theory*, *Cryptography and Related Areas*, Springer-Verlag Berlin, 2000, 111–113.

[5] A. GARCIA, H. STICHTENOTH and H. G. RÜCK, On tame towers over finite fields, J. Reine Angew. Math. **557** (2003), 53–80.

[6] A. GARCIA, H. STICHTENOTH and M. THOMAS, On towers and composita of towers of function fields over finite fields, Finite Fields Appl. **3** (1997), 257–274.

[7] T. HASEGAWA, An upper bound for the Garcia-Stichtenoth numbers of towers, Tokyo J. Math. **28** (2005), 471–481.

[8] Y. IHARA, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA. Math. **28** (1981), 721–724.

[9] H. STICHTENOTH, *Algebraic function fields and codes*, Springer-Verlag Berlin, 1993.

[10] M. A. TSFASMAN, Some remarks on the asymptotic number of points, in: H. Stichtenoth and M. A. Tsfasman (Eds.), *Coding theory and algebraic geometry*, Springer-Verlag Berlin, 1992, 178–192.

[11] M. A. TSFASMAN and S. G. VLĂDUŢ, *Algebraic-geometric codes*, Kluwer Dordrecht, 1991.

[12] M. A. TSFASMAN, S. G. VLĂDUŢ and T. ZINK, Modular curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound, Math. Nachr. **109** (1982), 21–28.

Present Address:
DEPARTMENT OF MATHEMATICS, SCHOOL OF EDUCATION,
WASEDA UNIVERSITY,
TOKYO, 169–8050 JAPAN.
e-mail: thasegawa@suou.waseda.jp