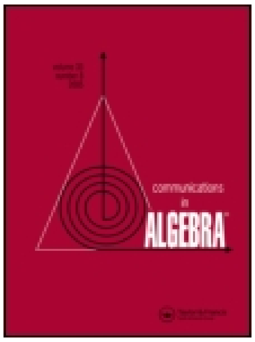

Communications in Algebra

ISSN: 0092-7872 (Print) 1532-4125 (Online) Journal homepage: http://www.tandfonline.com/loi/lagb20

A note on towers of function fields over finite fields

Ferruh Özbudak & Michael Thomas

COMMUNICATIONS IN ALGEBRA, 26(11), 3737-3741(1998)

A NOTE ON TOWERS OF FUNCTION FIELDS OVER FINITE FIELDS

FERRUH ÖZBUDAK AND MICHAEL THOMAS

BILKENT UNIVERSITY, DEPARTMENT OF MATHEMATICS, 06533 ANKARA, TURKEY

E-mail address: ozbudak@fen.bilkent.edu.tr

UNIVERSITÄT GH ESSEN, FB 6 MATHEMATIK UND INFORMATIK, D-45117 ESSEN, GERMANY

E-mail address: michael.thomas@uni-essen.de

ABSTRACT. For a tower $F_1 \subseteq F_2 \subseteq \cdots$ of algebraic function fields $F_i/\mathbb{F}_q$, define $\lambda := \lim_{i\to\infty} N(F_i)/g(F_i)$, where $N(F_i)$ is the number of rational places and $g(F_i)$ is the genus of $F_i/\mathbb{F}_q$. The purpose of this note is to calculate λ for a class of towers which was studied in [1], [2] and [3].

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field with q elements and $F/\mathbb{F}_q$ an algebraic function field, i.e. an algebraic extension of the rational function field $\mathbb{F}_q(x)$ of finite degree such that $\mathbb{F}_q$ is algebraically closed in F. We denote by $N(F)$ the number of rational places of $F/\mathbb{F}_q$ and by $g(F)$ the genus of the function field. Weil's theorem states that

$$|N(F) - (q+1)| \leq 2g(F)q^{1/2}.$$

Fixing q, for large genera g this bound could be improved. Namely let $N_q(g) = \max\{N(F)|F \text{ is a function field over } \mathbb{F}_q \text{ of genus } g\}$ and $A(q) =$

This paper was written while the first author was visiting the University of Essen under a grant of TÜBİTAK (Turkish Scientific and Technological Research Council).

Correspondence to the first author.

$\limsup_{g\to\infty} N_q(g)/g$, then by Drinfeld-Vladut bound

$$A(q) \leq \sqrt{q} - 1.$$

If q is a square, Ihara and Tsfasman-Vladut-Zink proved that

$$A(q) = \sqrt{q} - 1.$$

If q is not square, the exact value of $A(q)$ is unknown. Serre showed

$$A(q) \geq c \log q > 0 \text{ for all } q$$

with some small constant $c > 0$.

A *tower of function fields* over $\mathbb{F}_q$ is a sequence $\mathcal{F} = (F_1, F_2, \dots)$ of function fields $F_i/\mathbb{F}_q$ having the following properties: (i) $F_1 \subseteq F_2 \subseteq F_3 \subseteq \cdots$, (ii) for every $n \geq 1$, the extension F_{n+1}/F_n is separable of degree > 1, and (iii) $g(F_j) > 1$ for some $j \geq 1$. Let $\lambda(\mathcal{F}) := \lim_{n\to\infty} N(F_n)/g(F_n)$. $\mathcal{F}$ is called *asymptotically good* if $\lambda(\mathcal{F}) > 0$.

It is clear that $\lambda(\mathcal{F}) \leq A(q)$. Garcia-Stichtenoth-Thomas [2] have recently given examples for any $q = p^e$, $e \geq 2$ such that $\lambda(\mathcal{F}) \geq \frac{2}{q-2}$. Namely they constructed a tower of function fields over $\mathbb{F}_q$, $q = p^e$, where $F_n = \mathbb{F}_q(x_1, \dots, x_n)$ and

$$x_{i+1}^m + (x_i + 1)^m = 1,\ i = 1, \dots, n-1,\ m = \frac{p^e - 1}{p - 1}.$$

It would be interesting if the actual value of $\lambda(\mathcal{F})$ was large.

Thomas [3] showed $\lambda(\mathcal{F}) = \frac{2}{q-2}$ for a few fixed values of q.

In this note we prove the equality for a class of towers for any value of q when q is a square.

Theorem 1.1. *Let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements. Let $F_n = \mathbb{F}_{q^2}(x_1, x_2, \dots, x_n)$ be the algebraic function field where*

$$x_{i+1}^{q+1} + (x_i + 1)^{q+1} = 1,\ i = 1, 2, \dots, n-1.$$

Let $\mathcal{F}$ be the tower of function fields over $\mathbb{F}_{q^2}$ given by $\mathcal{F} = (F_1, F_2, \dots, F_n, \dots)$. Then

$$\lambda(\mathcal{F}) = \frac{2}{q^2 - 2}.$$

2. Proof of the Theorem

Let $\mathbb{P}_{F_n}$ denote the set of places of F_n, $n \geq 1$, P_∞ be the place of F_1 where $v_{P_\infty}(x_1) = -1$. Let

$$S(\mathcal{F}) = \{P \in \mathbb{P}_{F_1} | P \text{ is ramified in } F_n/F_1 \text{ for some } n \geq 2\}.$$

It is known that ([2], Example 2.3)

(2.2) $S(\mathcal{F}) \subseteq \{P \in \mathbb{P}_{F_1} | P \text{ is a rational place and } P \neq P_\infty\}$.

Let

$$A_n = \sum_{\substack{P\in \mathbb{P}_{F_1} \\ P \neq P_\infty}} \sum_{\substack{P' \in \mathbb{P}_{F_n} \\ P'|P}} P'.$$

Claim. $\lim_{n\to\infty} \frac{\deg A_n}{(q+1)^n} = 0$.

The claim shows the equality of two sets in 2.2, since otherwise there would be a finite place which is unramified in all extensions and hence the limit would be positive.

By Riemann-Hurwitz genus formula

$$2g(F_n) - 2 = [F_n : F_1](2g(F_1) - 2) + \deg Diff(F_n/F_1).$$

From the claim above, more precisely from the equality of the two sets in 2.2 we have

$$\deg Diff(F_n/F_1) = [F_n : F_1]q^2 - \deg A_n$$

and therefore

$$g(F_n) = [F_n : F_1](g(F_1) - 1) + \frac{q^2[F_n : F_1]}{2} - \frac{\deg A_n}{2} + 1.$$

Moreover since P_∞ splits completely in all extensions F_n/F_1 we have $[F_n : F_1] \leq N(F_n) \leq [F_n : F_1] + \deg A_n$. Consequently our claim also proves the theorem since $[F_n : F_1] = (q+1)^{n-1}$.

Now we prove the claim. For α, $\beta \in \mathbb{F}_q$ let $f(\alpha,\beta) = \#\{x \in \mathbb{F}_{q^2} | x^{q+1} = \alpha,\ x^{q+1} + x^q + x = -\beta\}$. Then

$$\#\{(x_1, x_2) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} | x_2^{q+1} = 1 - (x_1+1)^{q+1}\} = \sum_{\alpha_1\in\mathbb{F}_q} \sum_{\beta_1\in\mathbb{F}_q} \sum_{\beta_2\in\mathbb{F}_q} f(\alpha_1,\beta_1)f(\beta_1,\beta_2)$$

since $x_2^{q+1} = -(x_1^{q+1} + x_1^q + x_1)$. Similarly

$$\#\{(x_1,x_2,x_3) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} | x_2^{q+1} = 1 - (x_1+1)^{q+1} \text{ and } x_3^{q+1} = 1 - (x_2+1)^{q+1}\}$$
$$= \textstyle\sum_{\alpha_1\in\mathbb{F}_q} \sum_{\beta_1\in\mathbb{F}_q} \sum_{\beta_2\in\mathbb{F}_q} \sum_{\beta_3\in\mathbb{F}_q} f(\alpha_1,\beta_1)f(\beta_1,\beta_2)f(\beta_2,\beta_3)$$

By induction

$$\deg A_n = \sum_{\alpha\in\mathbb{F}_q} \sum_{\beta\in\mathbb{F}_q} f^n(\alpha,\beta)$$

where $f^{i+1}(\alpha,\beta) = \sum_{h\in F_q} f^i(\alpha,h)f(h,\beta)$ $i \geq 1$.

Let $h : \{1,2,\ldots,q\} \to \mathbb{F}_q$ be a bijection such that $h(1) = 1$ and $h(q) = 0$. Define $G := [G_{i,j}]_{1\leq i\leq q, 1\leq j\leq q}$ where $G_{i,j} = f(h(i),h(j))$. Considering $G : \mathbb{C}^q \to \mathbb{C}^q$ and using L_1 norm we have $||G|| = \max_{1\leq j\leq n} \sum_{i=1}^q |G_{i,j}|$ (see for example [4] page 165).

We show $||G^3|| < (q+1)^3$ which finishes the proof since $\deg A_n = \sum_{i=1}^{q}\sum_{j=1}^{q} G_{i,j}^n$. Firstly observe that $0 \le G_{i,j} \le 2$. The right hand side follows from the fact that if $a, b \in \mathbb{F}_q$ and $f(x) = gcd(x^{q+1}+a, x^{q+1}+x^q+x+b)$, then $\deg f \le 2$. Moreover

(2.3) $$\sum_{i=1}^{q} G_{i,j} = \begin{cases} q+1 & \text{if } j \ne 1, \\ 1 & \text{if } j = 1, \end{cases}$$

since

$$\begin{aligned} \sum_{i=1}^{q} G_{i,j} &= \#\{x \in \mathbb{F}_{q^2} | x^{q+1}+x^q+x = -h(j)\} \\ &= \#\{x \in \mathbb{F}_{q^2} | (x+1)^{q+1} = 1-h(j)\} \\ &= \#\{x \in \mathbb{F}_{q^2} | x^{q+1} = 1-h(j)\}. \end{aligned}$$

In fact $G_{i,1} = \begin{cases} 1 & \text{if } i = 1, \\ 0 & \text{if } i \ne 1. \end{cases}$ Similarly

(2.4) $\sum_{j=1}^{q} G_{i,j} = \begin{cases} q+1 & \text{if } i \ne q, \\ 1 & \text{if } i = q, \end{cases}$ and $G_{q,j} = \begin{cases} 1 & \text{if } j = q, \\ 0 & \text{if } j \ne q. \end{cases}$

Using 2.3 we get

$$\begin{aligned} \sum_{i=1}^{q} G_{i,j}^2 &= \sum_{i=1}^{q}\sum_{l=1}^{q} G_{i,l}G_{l,j} = \sum_{l=1}^{q} G_{l,j}\sum_{i=1}^{q} G_{i,l} \\ &= (q+1)\sum_{l=1}^{q} G_{l,j} - qG_{1,j} \\ &= \begin{cases} (q+1)^2 - qG_{1,j} & \text{if } j \ne 1, \\ 1 & \text{if } j = 1. \end{cases} \end{aligned}$$

Moreover we also get

$$\begin{aligned} \sum_{i=1}^{q} G_{i,j}^3 &= \sum_{i=1}^{q}\sum_{l=1}^{q} G_{i,l}G_{l,j}^2 = \sum_{l=1}^{q} G_{l,j}^2\sum_{i=1}^{q} G_{i,l} \\ &= (q+1)\sum_{l=1}^{q} G_{l,j}^2 - qG_{1,j}^2 \\ &= \begin{cases} (q+1)^3 - q(q+1)G_{1,j} - qG_{1,j}^2 & \text{if } j \ne 1, \\ 1 & \text{if } j = 1. \end{cases} \end{aligned}$$

However there exists no $2 \le j \le q$ such that $G_{1,j}^2 = 0$. Indeed if $G_{1,j}^2 = 0$, then

$$G_{1,l}G_{l,j} = 0 \text{ for } l = 1, \ldots, q$$

since the entries are nonnegative. Moreover the entries are bounded from above by 2 and using the properties 2.3 and 2.4, we get $G_{1,l} = 0$ for at most $\frac{q-1}{2}$ many values of l and $G_{l,j} = 0$ for at most $\frac{q-1}{2}$ many values of l. This gives a contradiction to $G_{1,j}^2 = 0$ and completes the proof.

3. Acknowledgments

We would like to thank Arnolda Garcia, Henning Stichtenoth, and Fernando Torres for the stimulating conversations. Moreover the first author thanks to Fachbereich 6 Universität Essen for their hospitality.

References

[1] Garcia A. and Stichtenoth H., "Asymptotically good towers of function fields over finite fields", C.R. Acad. Sci. Paris 322, Ser. I, pp. 1067-1070, 1996.

[2] Garcia A., Stichtenoth H. and Thomas M., "On towers and composita of towers of function fields over finite fields", Finite Fields and Their Applications, vol. 3, no. 3, pp. 257-274, 1997.
[3] Thomas M, "Türme und Pyramiden algebraischer Funktionenkörper", Ph.D. Dissertation, University of Essen, 1997.
[4] Elaydi S. N., "An introduction to difference equations", Springer-Verlag, New York, 1996.

Received: June 1997

Revised: February 1998