On Two Towers of Garcia and Stichtenoth

Vinay Deolalikar
Information Theory Research Group
HP Laboratories Palo Alto
HPL-2001-208
August 29th , 2001*

E-mail: vinayd@hpl.hp.com

algebraic geometric codes, function fields, finite fields

We make the observation that two examples of towers of function fields with asymptotically positive N / g ratios given by Garcia and Stichtenoth can be generalized, each leading to $\tau(n) - 1$ such examples over $\mathbb{F}_{p^n}$, $n > 1$, where τ is the number of divisors function.

* Internal Accession Date Only
Approved for External Publication

Abstract

We make the observation that two examples of towers of function fields with asymptotically positive N/g ratios given by Garcia and Stichtenoth can be generalized, each leading to $\tau(n) - 1$ such examples over $\mathbb{F}_{p^n}$, $n > 1$, where τ is the number of divisors function.

1 Introduction

Let $\mathcal{T} = (T_1, T_2, \ldots)$ be a tower of function fields, each defined over $\mathbb{F}_q$. Let $N(T_i)$ and $g(T_i)$ denote the number of places of degree one and the genus, respectively, of T_i. It is known that the sequence $(N(T_i)/g(T_i))$ converges as $i \to \infty$ [4]. Let $\lambda(\mathcal{T}) := \lim_{i\to\infty} N(T_i)/g(T_i)$. Then, we have

$$0 \leq \lambda(\mathcal{T}) \leq \sqrt{q} - 1. \tag{1}$$

The upper bound is known as the Drinfeld-Vladut bound. Algebraic-geometric codes with good parameters can be constructed on towers with $\lambda(\mathcal{T}) > 0$. Codes constructed on towers meeting the Drinfeld-Vladut bound can have performance exceeding the Gilbert-Varshamov bound [7]. However, for use in code-construction, such towers have to be explicitly described. There are very few of these in literature [2, 3, 4, 5].

In [5], Garcia and Stichtenoth provided two examples of towers for which $\lambda(\mathcal{T}) > 0$. These two towers attain the Drinfeld-Vladut bound when the underlying field is of cardinality four or nine, respectively. In this correspondence, we generalize these examples to sets of $\tau(n) - 1$ examples each, over $\mathbb{F}_{p^n}$ $n > 1$, where τ is the number of divisors function.

2 Towers

Definition 2.1 *Let $q = p^n$ where $n > 1$. For a proper divisor d of n, let $k_d := \frac{p^n-1}{p^d-1}$. For any pair (r, s) of proper divisors of n, consider the tower of function fields given by $\mathcal{T}^{r,s} = (T_1, T_2, \ldots)$, where $T_1 = \mathbb{F}_q(x_1)$ and for $i \geq 1$, $T_{i+1} = T_i(x_{i+1})$, where x_{i+1} satisfies*

$$x_{i+1}^{k_r} + z_i^{k_s} = b_i^{k_s}, \tag{2}$$

$$z_i = a_i x_i^{m_i} + b_i, \tag{3}$$

where $a_i, b_i \in \mathbb{F}_{p^s}^*$ and m_i is a power of p.

Theorem 2.2 *For the tower $\mathcal{T}^{r,s}$:*
If $r \equiv 0 \bmod s$, P_∞ splits completely throughout the tower.
If $s \equiv 0 \bmod r$ Every ramified place in the tower lies above a rational place in T_1.
If $r = s$, $\lambda(\mathcal{T}) \geq \frac{2}{q-2}$.

Proof. Since the proof is very similar to that for the original tower, we only verify that under the hypothesis, we do indeed get a tower of function fields. Notice that at one of the places dividing x_1 in T_2, we get a zero of x_2 of order not divisible by k_r. This implies that $b_1^{k_s} - z_1^{k_s}$ is not of the form w^{k_r} for any $w \in T_1$. Further, one of the places dividing x_2 in T_3 also has the same property, and so on. Thus, each equation is irreducible and gives us an extension. □

The second tower is also generalized using similar ideas. Here we allow raising of the variables to the order of not just the total multiplicative group of the field, but all its subgroups as well.

Definition 2.3 *Let $q = p^n > 4$ and $n > 1$. For a proper divisor d of n, let $l_d := p^d - 1$. For any pair (r, s) of proper divisors of n, consider the tower of function fields in given by $\mathcal{T}^{r,s} = (T_1, T_2, \ldots)$, where $T_1 = \mathbb{F}_q\ (x_1)$ and for $i \geq 1$, $T_{i+1} = T_i(x_{i+1})$, where x_{i+1} satisfies*

$$x_{i+1}^{l_r} + z_i^{l_s} = 1, \tag{4}$$

$$z_i = a_i x_i^{m_i} + b_i, \tag{5}$$

where $a_i, b_i \in \mathbb{F}_{p^s}^*$ and m_i is a power of p.

Theorem 2.4 *For the tower $\mathcal{T}^{r,s}$:*
If $s \equiv 0 \bmod r$, P_∞ splits completely throughout the tower.
If $r \equiv 0 \bmod s$, Every ramified place in the tower lies above a rational place in T_1.
If $r = s$, we get $\lambda(\mathcal{T}) \geq \frac{2}{l_r - 1}$.

Proof. To verify that we do indeed get a tower of function fields, note that $b_i^{l_s} = 1$. The proof of the theorem is similar to that of Theorem 2.2. □

Remark 2.5 *Let $\mathcal{T}_1^{r,s}$ be the tower of Definition 2.1 with $a_i = 1$ for $i > j$ where j is a positive integer. Then*

$$\mathcal{T}_1^{r,s} \cong \mathcal{T}^{r,s},$$

since we can absorb the a_i in the equation at each stage as follows:

$$\zeta_i = x_i^{m_i} + \frac{b_i}{a_i}, \tag{6}$$

$$(x_{i+1}/a_i^{\frac{k_s}{k_r}})^{k_r} + {\zeta_i}^{k_s} = (\frac{b_i}{a_i})^{k_s}. \tag{7}$$

We can do a similar substitution for the tower of Definition 2.3.

Remark 2.6 *Elkies [2] showed that the Garcia and Stichtenoth towers were modular. It would be interesting to see what relations to modularity the generalizations have.*

References

[1] V. Deolalikar, *On splitting places of degree one in extensions of algebraic function fields, towers of function fields meeting asymptotic bounds, and explicit basis constructions for algebraic-geometric codes.*, Ph.D dissertation, Department of Electrical Engineering, University of Southern California (1999). e-print available at http://arXiv.org/abs/math.NT/0010307

[2] N. Elkies, *Explicit modular towers*, Proceedings of the Thirty Fifth Annual Allerton Conference on Communication, Control and Computing, Urbana, IL (1997).

[3] A. Garcia and H. Stichtenoth, *A Tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Inventiones Mathematicae 121, 1995, 11-222.

[4] A. Garcia and H. Stichtenoth, *On the Asymptotic Behaviour of Some Towers of Function Fields over Finite Fields*, Journal of Number Theory 61, No. 2 (1996), 248-273.

[5] A. Garcia and H. Stichtenoth, *Asymptotically good towers of function fields over finite fields*, C. R. Acad. Sci. Paris, t. 322, Série I (1996), 1067-1070.

[6] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Berlin-Heidelberg-New York (1991).

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