Old and New Towers over Finite Fields

Henning Stichtenoth

Sabancı University, MDBF
34956 Tuzla, İstanbul, Turkey
henning@sabanciuniv.edu

Abstract. The theory of recursive towers of function fields over finite fields was developed by A. Garcia and the author since 1995. In this talk we describe some of the main ideas and results, and we present old and new examples of interesting recursive towers.

1

We consider towers of algebraic function fields, i.e. sequences $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields F_i over a finite field $\mathbb{F}_q$ where $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$, all extensions F_{i+1}/F_i are separable and the genus $g(F_i)$ tends to infinity as $i \to \infty$. We denote by $N(F_i)$ the number of rational (i.e. degree one) places of F_i over $\mathbb{F}_q$. It is well-known that the limit

$$\lambda(\mathcal{F}) = \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}$$

exists, and it is bounded from above by the Drinfeld-Vladut bound

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

A tower $\mathcal{F}$ over $\mathbb{F}_q$ is said to be *asymptotically good*, if $\lambda(\mathcal{F}) > 0$, it is *asymptotically optimal* if $\lambda(\mathcal{F}) = \sqrt{q} - 1$, and it is *asymptotically bad* if $\lambda(\mathcal{F}) = 0$. The study of asymptotically good towers is of high interest because of their various applications in coding theory (Tsfasman-Vladut-Zink theorem), cryptography etc., but also as a mathematical challenge.

In order to determine the limit of a tower, it is useful to study the behaviour of the genus and of the number of rational places separately; i.e. one considers the limits

$$\gamma(\mathcal{F}/F_0) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}\ , \quad \text{the } \textit{genus} \text{ of } \mathcal{F} \text{ over } F_0,$$

and

$$\nu(\mathcal{F}/F_0) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}\ , \quad \text{the } \textit{splitting rate} \text{ of } \mathcal{F} \text{ over } F_0.$$

It is easily seen that $0 < \gamma(\mathcal{F}/F_0) \leq \infty$ and $0 \leq \nu(\mathcal{F}/F_0) < \infty$, and moreover,

$$\lambda(\mathcal{F}/F_0) = \frac{\nu(\mathcal{F}/F_0)}{\gamma(\mathcal{F}/F_0)}.$$

This implies that the tower $\mathcal{F}$ is asymptotically good if and only if its genus $\gamma(\mathcal{F}/F_0)$ is finite, and its splitting rate $\nu(\mathcal{F}/F_0)$ is strictly positive. We introduce the *ramification locus*

$$V(\mathcal{F}/F_0) := \{P \mid P \text{ is a place of } F_0 \text{ which is ramified in } F_k/F_0 \text{ for some } k > 0\}.$$

If $V(\mathcal{F}/F_0)$ is finite and all ramification in the tower is tame, it follows from the Hurwitz genus formula that the genus $\gamma(\mathcal{F}/F_0)$ is finite. The condition of tame ramification can be weakened as follows: suppose that for every place $P \in V(\mathcal{F}/F_0)$, there is a constant $c_P \in \mathbb{R}$ such that for all $k \geq 1$ and all places Q of F_k lying above P, the different exponent $d(Q|P)$ is bounded by

$$d(Q|P) \leq c_P \cdot e(Q|P)$$

(here we denote by $e(Q|P)$ the ramification index of $Q|P$). Then finiteness of the ramification locus implies again finiteness of the genus $\gamma(\mathcal{F}/F_0)$.

In a similar way, one can often make sure that the splitting rate $\nu(\mathcal{F}/F_0)$ is positive. To this aim, we define the *splitting locus*

$$Z(\mathcal{F}/F_0) = \{P \mid P \text{ is a place of } \ F_0 \text{ which splits completely in } \ \mathcal{F}\}.$$

Obviously, $\nu(\mathcal{F}/F_0) \geq |Z(\mathcal{F}/F_0)|$, and therefore a non-empty splitting locus implies that the splitting rate of the tower is positive. To conclude, we have the following result:

Lemma 1. *Suppose that the tower $\mathcal{F}$ satisfies the following conditions:*
(i) the ramification locus $V(\mathcal{F}/F_0)$ is finite,
(ii) for every $P \in V(\mathcal{F}/F_0)$, there is a constant $c_P \in \mathbb{R}$ such that $d(Q|P) \leq c_P \cdot e(Q|P)$ for all places Q above P,
(iii) the splitting locus of $\mathcal{F}/F_0$ is non-empty.
Then the tower is asymptotically good.

The conditions given in Lemma 1 are *sufficient* conditions for $\mathcal{F}$ to be asymptotically good. On the other hand, all examples of good towers that I know, satisfy all these conditions.

There are essentially three sources for towers: *class field towers* (first introduced by Serre [3]), *towers of modular curves* (first introduced by Ihara [2] and Tsfasman, Vladut and Zink [4]), and *recursive towers* (introduced by Garcia and the author [1]).

A tower $\mathcal{F} = (F_i)_{i \geq 0}$ is said to be *recursive* if there exist a non-zero polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ and elements $x_0, x_1, x_2, \ldots$ such that for all $i \geq 0$,

$$F_0 = \mathbb{F}_q(x_0) \ , F_{i+1} = F_i(x_{i+1}) \text{ and } f(x_i, x_{i+1}) = 0 \ .$$

In this talk we discuss several examples of recursive towers, some of which are well-known, some are new. In all cases we focus on the question if the conditions of Lemma 1 are satisfied.

References

1. Garcia, A., Stichtenoth, H.: On the Asymptotic Behaviour of Some Towers of Function Fields over Finite Fields, J. Number Theory 61, 248-273 (1996)
2. Ihara, Y.: Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28, 721-724 (1981)
3. Serre, J.-P.: Sur le Nombre des Points Rationnels d'une Courbe Algebrique sur un Corps Finis, C. R. Acad. Sci. Paris 296, 397-402 (1983)
4. Tsfasman, M. A., Vladut, S. G., Zink, T.: Modular Curves, Shimura Curves, and Goppa Codes, Better than the Varshamov-Gilbert Bound, Math. Nachr. 109, 21-28 (1982)