New towers over finite fields

Henning Stichtenoth, Sabanci University, Istanbul, Turkey

The aim of this talk is to present a recent result by A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth, which includes and generalizes all previous asymptotic bounds on curves over non-prime finite fields.

For a curve $C$ over the finite field $\mathbb{F}_q$, denote by $N(C)$ and $g(C)$ the number of rational points and the genus of $C$. The Drinfeld-Vladut bound is an asymptotic upper bound for $N(C)$ in terms of the genus:

$$N(C) \lesssim g(C) \cdot (\sqrt{q} - 1) \quad \text{for} \quad g(C) \gg 0.$$ 

For many applications, but also as a mathematical challenge, we are interested in lower bounds as well. Lower bounds are usually obtained by constructing an infinite family of curves with increasing genus, for which the limit $N(C)/g(C)$ exists and is $> 0$. Methods for such constructions include classfield towers, modular towers and explicit recursive towers.

We present over every non-prime field $\mathbb{F}_q$, $q = p^n$, $n \geq 2$ a recursive tower of curves $C_0, C_1, C_2, \ldots$ with

$$\lim_{n \to \infty} \frac{N(C_n)}{g(C_n)} \geq H(p^{\lceil \frac{n}{2} \rceil} - 1, p^{\lfloor \frac{n}{2} \rfloor} - 1),$$

where $H(., .)$ denotes the harmonic mean of two real numbers.

This lower bound coincides for even $n$ (i.e., square $q$) with the upper Drinfeld-Vladut bound and has been obtained previously by Ihara and Tsfasman-Vladut-Zink (via reduction of modular curves). For $q = p^3$, our bound coincides with Zink’s bound (obtained via reduction of modular surfaces). For all other non-prime fields, our bound is much better than all previous lower asymptotic bounds.

The asymptotic Gilbert-Varshamov bound is a fundamental result in Coding theory. It was improved by Tsfasman-Vladut-Zink for codes over quadratic fields $\mathbb{F}_q$, $q \geq 49$, a square. As a consequence of our result we obtain an improvement of the asymptotic Gilbert-Varshamov bound over any non-prime field $\mathbb{F}_q$ with $q \neq 4, 8, 9, 16, 25, 27, 32, 125$.

Reference