On characterization of certain maximal curves

by
Saeed Tafazolian
(IASBS at Zanjan, Iran)

Let $\mathcal{C}$ be a (non-singular, projective, geometrically irreducible, algebraic) curve of genus g defined over a finite field $\mathbb{F}_q$ with q elements. We know after A. Weil that the number of $\mathbb{F}_q$-points of a curve of genus g defined over $\mathbb{F}_q$ satisfies the following limitations:

$$q+1-2g\sqrt{q} \leq \#\mathcal{C}(\mathbb{F}_q) \leq 1+q+2g\sqrt{q},$$

where $\mathcal{C}(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of the curve $\mathcal{C}$.

Here we will be interested in maximal(resp. minimal) curves over $\mathbb{F}_{q^2}$, that is, we will consider curves $\mathcal{C}$ attaining Hasse-Weil's upper (resp. lower) bound:

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2+1+2gq \text{ (resp. } q^2+1-2gq).$$

Here we are interested to consider the hyperelliptic curve $\mathcal{C}$ given by the equation $y^2 = x^m + 1$ over $\mathbb{F}_{q^2}$. We are going to determine when this curve is maximal over $\mathbb{F}_{q^2}$. In fact, we show that

Theorem 0.1. *Suppose q is an odd prime power and let m be a positive integer such that $gcd(q, m) = 1$. The smooth complete hyperelliptic curve $\mathcal{C}$ corresponding to*

$$y^2 = x^m + 1$$

is maximal over $\mathbb{F}_{q^2}$ if and only if m divides $q+1$.

This generalizes [1, Propositions 2, 3 and 5]) which deals with the particular case when $m = 7, 8$ and 12.

References

[1] T. Kodama, J. Top and T. Washio, Maximal hyperelliptic curves of genus three, *Finite Fields Appl* **15** (2009), 392-403.