On the number of rational points of Artin-Schreier curves and hypersurfaces

Daniela Alves de Oliveira

Let $\mathbb{F}_q$ be the finite field with $q = p^s$ elements, where p is an odd prime. An important class of curves over finite fields is the class of Artin-Schreier curves. That are given by the equation $y^q - y = f(x)$ for some $f(x) \in \mathbb{F}_q[x]$. These curves have been extensively studied in several contexts and this type of curve can be generalized for several variables, i.e., the hypersurfaces of Artin-Schreier of the form $y^q - y = f(X)$, with $f(X) \in \mathbb{F}_q[X] \setminus \{0\}$ and $X = (x_1, \ldots, x_r)$. Information about the number of affine rational points of algebraic hypersurfaces over finite fields has many applications in coding theory, cryptography, communications and related areas.

In this presentation, we will determine the number of $\mathbb{F}_{q^n}$-rational points of the Artin-Schreier curve $\mathcal{C}_i$ given by

$$\mathcal{C}_i : y^q - y = x(x^{q^i} - x) - \lambda$$

where $i \in \mathbb{N}$ and $\lambda \in \mathbb{F}_{q^n}$. We denote by $N_n(\mathcal{C}_i)$ the number of $\mathbb{F}_{q^n}$-rational points of $\mathcal{C}_i$.

For $i \in \mathbb{N}$, we define Q_i the map

$$\begin{aligned} Q_i : \mathbb{F}_{q^n} &\to \mathbb{F}_q \\ \alpha &\mapsto \mathrm{Tr}(\alpha(\alpha^{q^i} - \alpha) - \lambda), \end{aligned}$$

and $N_n(Q_i)$ denotes the number of zeroes of Q_i in $\mathbb{F}_{q^n}$. Hilbert's Theorem 90 implies that

$$N_n(\mathcal{C}_i) = q \cdot N_n(Q_i).$$

Therefore, we observe that determine $N_n(\mathcal{C}_i)$ is equivalent to calculate $N_n(Q_i)$. Using the method, that consists in determine the number of solutions of the quadratic form Q_i using appropriates permutation matrices, we compute the number $N_n(\mathcal{C}_i)$ and also determine conditions for the Artin-Schreier curve C_i to be maximal or minimal with respect the Hasse-Weil bound.

Therefore we will determine the number of $\mathbb{F}_{q^n}$-rational points of the affine Artin-Schreier hypersurface $\mathcal{H}_r$ given by

$$\mathcal{H}_r : y^q - y = \sum_{j=1}^{r} a_j x_j (x_j^{q^{i_j}} - x_j) - \lambda, \tag{1}$$

where $a_j \in \mathbb{F}_q^*$ and $0 < i_j < n$ for $1 \leq j \leq r$. We denote by $N_n(\mathcal{H}_r)$ the number of $\mathbb{F}_{q^n}$-rational points of the hypersurface $\mathcal{H}_r$. The well-known Weil bound assures us that

$$|N_n(\mathcal{H}_r) - q^{rn}| \leq (q-1) \prod_{j=1}^{r} q^{i_j} q^{\frac{nr}{2}} = (q-1) q^{\frac{nr+2I}{2}}, \tag{2}$$

where $I = \sum_{j=1}^{r} i_j$. The hypersurface $\mathcal{H}_r$ is called $\mathbb{F}_{q^n}$-maximal ($\mathbb{F}_{q^n}$-minimal) if $N_n(\mathcal{H}_r)$ attains the upper (lower) bound given in Equation (2). We provide necessary and sufficient conditions to this bound be attained. From the results about the curve $\mathcal{C}_i$, we can explicitly determine the number of rational points $N_n(\mathcal{H}_r)$ and the conditions to obtain the maximality or minimality of this hypersurface.

Departamento de Matemática, Universidade de São Paulo (ICMC- São Carlos), USP
Email address: danielaalvesoliveira@gmail.com