Estimates on the average cardinality of the value set of general families of univariate polynomials over a finite field

Melina Privitelli
Instituto de Ciencias, UNGS, Argentina
mprivite@ungs.edu.ar

The aim of this work is to estimate the average cardinality of the value set of a general family of monic univariate polynomials with coefficients in a finite field. This is a classical combinatorial problem with several applications in coding theory, interpolation problems and the analysis of the cost of algorithms for computing $\mathbb{F}_q$-rational zeros of multivariate polynomials with coefficients in a finite field, among others.

Let $\mathbb{F}_q$ be the finite field of $q = p^k$ elements and let $\mathcal{P}_d$ be the set of monic polynomials of degree d with coefficients in $\mathbb{F}_q$. For $f \in \mathcal{P}_d$ we denote by $\mathcal{V}(f) := |\{f(c) : c \in \mathbb{F}_q\}|$ the cardinality of the value set of f. Let $\mathcal{A} \subset \mathcal{P}_d$ be a general family, namely the set of elements of $\mathcal{P}_d$ whose coefficients belong to an $\mathbb{F}_q$–algebraic variety. S. D. Cohen studied the particular case when $\mathcal{A}$ is a linear family and proved that if $p > d$ and $\mathcal{A}$ satisfies certain technical conditions, the average cardinality $\mathcal{V}(\mathcal{A})$ of the value set in $\mathcal{A}$ is

$$\mathcal{V}(\mathcal{A}) = \mu_d q + \mathcal{O}(q^{1/2}),$$

where $\mu_d := \sum_{j=1}^{d} (-1)^{j-1}/j!$.

In our work we significantly generalize this result to rather general (eventually nonlinear) families $\mathcal{A} \subset \mathcal{P}_d$. We establish conditions on $\mathcal{A}$ which allow us to obtain an explicit version of this estimate. Our result provides an expression for the constant underlying the $\mathcal{O}$-notation in terms of d. We obtain a combinatorial expression for $\mathcal{V}(\mathcal{A})$ in terms of certain "interpolating sets" $\mathcal{S}_r^{\mathcal{A}}$ $(1 \leq r \leq d)$ and we associate to each $\mathcal{S}_r^{\mathcal{A}}$ an $\mathbb{F}_q$–algebraic variety Γ_r. We reduce the question to estimate the number of $\mathbb{F}_q$–rational points of Γ_r. We also exhibit linear and non linear families of polynomials which satisfy our requirements. In the particular case of linear families we improve the estimate given by Cohen in several aspects.

Joint work with Guillermo Matera (Instituto del Desarrollo Humano, UNGS, Argentina) and Mariana Pérez (Instituto del Desarrollo Humano, UNGS, Argentina).