Estimaciones de soluciones racionales de ciertas ecuaciones polinomiales sobre cuerpos finitos

Expositor: Melina Lorena Privitelli (UNGS-CONICET, mprivite@ungs.edu.ar)
Autor/es: Melina Lorena Privitelli (UNGS-CONICET, mprivite@ungs.edu.ar); Mariana Valeria Pérez (UNAHUR-CONICET, mariana.perez@unahur.edu.ar)

Ciertos problemas de teoría de códigos, criptografía y combinatoria requieren el estudio de la geometría de variedadades “simétricas”sobre cuerpos finitos, es decir, variedades definidas por polinomios en los polinomios simétricos elementales (ver, por ejemplo [1], [2] y [3]). En este trabajo, consideramos polinomios en variables de la forma $S_k = X_1^k + \cdots + X_n^k$. Es decir, dado $f \in \mathbb{F}_q[Y_1, \ldots, Y_d]$ (donde $\mathbb{F}_q$ es el cuerpo finito de q elementos) y $S_{k_1}, \ldots, S_{k_d} \in \mathbb{F}_q[X_1, \ldots, X_n]$, definimos la variedad dada por $f(S_{k_1}, \ldots, S_{k_d})$. Bajo ciertas hipótesis sobre f, probamos que dicha variedad es absolutamente irreducible y obtenemos una cota de la dimensión de su lugar singular. A partir de este estudio, y utilizando los resultados de conteo de puntos $\mathbb{F}_q$-racionales para variedades singulares provistos en [4], obtenemos estimaciones de la cantidad de puntos $\mathbb{F}_q$-racionales de este tipo de variedades.

Nuestras estimaciones son aplicadas al problema de estimar el cardinal del conjunto de soluciones $\mathbb{F}_q$-racionales de ciertas ecuaciones polinomiales sobre $\mathbb{F}_q$. Más precisamente, obtenemos resultados de existencia y estimaciones de la cantidad de soluciones $\mathbb{F}_q$-racionales de las ecuaciones de Carlitz y de ecuaciones diagonales deformadas, entre otras. Estas estimaciones mejoran los existentes en la literatura (ver, por ejemplo, [5]).

Referencias

[1] A. Cafure, G. Matera, M. Privitelli. Singularities of symmetric hypersurfaces and Reed-Solomon codes, Adv. Math. Commun. 6 (2012). no. 1, 69–94.

[2] E.Cesaratto, G. Matera , M. Pérez y Melina Privitelli. On the value set of small families of polynomials over a finite field. I. J. Combin. Theory Ser. A 124 (2014), 203–227.

[3] G. Matera, M.Pérez y M. Privitelli. Factorization patterns on nonlinear families of univariate polynomials over a finite field, J Algebr. Comb. (2019), 1-51.

[4] S. Ghorpade and G. Lachaud, Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, Mosc. Math. J. 2 (2002), no. 3, 589–631.

[5] G. Muller y D. Panario. G. Mullen y D. Panario, Handbook of finite fields. CRC Press, Boca Raton, FL, 2013.