Soluciones racionales de sistemas de ecuaciones diagonales y su aplicación al "subset sum problem"

Juan Francisco Gottig
Universidad Nacional de General Sarmiento, Argentina
gottig21@gmail.com

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos. Un sistema de ecuaciones diagonales generalizadas es un sistema de la forma:

$$\begin{cases} a_{11}x_1^{d_{11}} + a_{12}x_2^{d_{12}} + \cdots + a_{1t}x_t^{d_{1t}} = g_1(x_1, \ldots, x_k) \\ \vdots \\ a_{n1}x_1^{d_{n1}} + a_{n2}x_2^{d_{n2}} + \cdots + a_{nt}x_t^{d_{nt}} = g_n(x_1, \ldots, x_k) \end{cases}$$

con $k \leq t$, $g_1, \ldots, g_n \in \mathbb{F}_q[x_1, \ldots, x_k]$, $grado(g_j) < d_t$ para $1 \leq j \leq n$ y $d_t > d_{t-1} > \cdots > d_1 > 1$.

Diversos problemas de teoría de códigos, criptografía y combinatoria sobre cuerpos finitos requieren estimar o poder garantizar la existencia de soluciones racionales (soluciones con coordenadas en $\mathbb{F}_q$) de sistemas de la forma (1) (ver, por ejemplo, [1] y [2]). Para el caso particular de una única ecuación diagonal existen muchos resultados, incluso hay fórmulas de conteo exacto de soluciones racionales para ecuaciones especiales. En [3] las autoras proporcionan estimaciones y resultados de existencia para variantes de ecuaciones diagonales. En cambio, cuando se trata de sistemas, se encuentran muchos menos resultados. En [4] las autoras estudian un caso particular de (1) que se trata de los sistemas en los que $d_{ji} = d_{ki}$ si $k \neq j$ para $1 \leq i \leq n$ y obtienen resultados que mejoran en diversos aspectos los de [5] y [6].

En este trabajo estudiamos la siguiente versión de (1): consideramos $d_{ij} = d_{ik}$ para $k \neq j$, $1 \leq i \leq n$ y $g_i \in \mathbb{F}_q$ para todo $1 \leq i \leq n$.

Nuestro interés en este sistema radica en que en primer lugar no se cuenta con resultados de existencia ni estimaciones de la cantidad de soluciones racionales del mismo y por otro lado en que el estudio del conjunto de sus soluciones racionales tiene aplicaciones a diferentes problemas en cuerpos finitos como, por ejemplo, el "Subset Sum Problem" y el estudio de los deep holes en el código de Reed Solomon.

Nuestra metodología consiste en considerar la variedad algebraica definida por los polinomios $f_j = a_{j1}x_1^{d_j} + \cdots + a_{jt}x_t^{d_j} - b_j$ para $1 \leq j \leq n$ y estudiar las propiedades geométricas de la misma. A partir de este estudio se obtienen estimaciones y resultados de existencia de soluciones racionales del sistema.

Finalmente aplicamos los resultados obtenidos al estudio del "Subset Sum Problem" sobre cuerpos finitos.

Trabajo en conjunto con Mariana Pérez (Universidad Nacional de Hurlingham, Argentina) y Melina Privitelli (Universidad Nacional de General Sarmiento, Argentina).

Referencias

[1] R. Lidl y H. Niederreiter. Finite fields, Adisson-Wesley, Reading, Massachusetts, 1983.

[2] Gary L. Mulln y Daniel Panario, Handbook of Finite Fields (1st ed.), Chapman and Hall/CRC, 2013.

[3] M. Pérez y M. Privitelli, Estimates on the number of rational solutions of variants of diagonal equations over finite fields, Finite Fields and Appl. 68,(2020), pp. 30.

[4] M. Pérez y M. Priivitelli, on the number of solutions of systems of certain diagonal equations over finite fields, Journal of Number Theory 236 (2022), 160-187.

[5] K. W. Spackman, Simultaneous solutions to diagonal equations over finite fields, J. Number Theory 11 (1979), 100-115.

[6] K. W. Spackman, On the number and distribution of simultaneous solutions to diagonal congruences, Canadian J. Math 33 (1981), no. 2. 421-436.