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

Juan Francisco Gottig

Trabajo en colaboración con: Mariana Pérez y Melina Privitelli
CONICET, UNGS, UNAHUR

7 de junio de 2023

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos y p su característica.

Consideraremos un sistema de ecuaciones diagonales de la forma

$$\begin{cases} X_1^{d_1} + X_2^{d_1} + \cdots + X_k^{d_1} = b_1 \\ \vdots \\ X_1^{d_m} + X_2^{d_m} + \cdots + X_k^{d_m} = b_m \end{cases}$$

donde $b_i \in \mathbb{F}_q$, $d_1 > d_2 > \cdots > d_m$, $d_i \in \mathbb{N}$.

Soluciones $\mathbb{F}_q$-racionales: soluciones con coordenadas en $\mathbb{F}_q$.

Resultados previos:

- X. Cao, W-S. Chou and J. Gu, On the number of solutions of certain diagonal equations over finite fields, Finite Fields Appl. 42 (2016), 225–252.
- F. N. Castro, I. Rubio, P. Guan and R. Figueroa, On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p, Finite Fields Appl. 14 (2008), no. 3, 648–657.
- K. W. Spackman, Simultaneous solutions to diagonal equations over finite fields, J. Number Theory 11 (1979), no. 1, 100–115.
- K. W. Spackman, On the number and distribution of simultaneous solutions to diagonal congruences, Canadian J. Math. 33 (1981), no. 2, 421–436.
- M. Perez and M. Privitelli, On the number of simultaneous solutions of certain diagonal equations over finite fields, J. Number Theory 236 (2022), 160–187.

¿Por qué nos interesa estimar las soluciones $\mathbb{F}_q$ racionales?

- En general tiene aplicaciones en criptografía, combinatoria, teoría de códigos, entre otras.
- En particular se puede aplicar en teoría de ciclotómicos, el problema de Waring sobre cuerpos finitos, el subset sum problem, problema de coloreo de grafos, etc.
- Problema NP-completo.

Estrategia:

$$f_i := X_1^{d_i} + \cdots + X_k^{d_i} - b_i,\ 1 \leq i \leq m.$$

$$V := \boldsymbol{V}(f_1, \ldots, f_m) = \{x \in \mathbb{A}^k / f_1(x) = f_2(x) = \cdots = f_m(x) = 0\}.$$

Propiedades geométricas de V:

- Si $m \leq \frac{k-1}{2}$ entonces la codimensión de $sing(V) \geq 2$, (la dimensión de $sing(V) \leq m-1$) y $\langle f_1, \ldots, f_s \rangle$ es radical.
- V es una intersección completa de grado menor o igual a $d_1 \cdots d_m$ y dimensión pura $k-m$.

Dada una variedad afín $W \subset K^n$, la **clausura proyectiva** de W es la variedad proyectiva $\overline{W} = \boldsymbol{V}(\boldsymbol{I}(W)^h)) \subset \mathbb{P}^n(K)$. Se notará como $pcl(W)$.

Propiedades de la clausura proyectiva:

- $V_\infty := pcl(V) \cap \{\boldsymbol{x} \in \mathbb{P}^n / x_0 = 0\} = \boldsymbol{V}(f_1 + b_1, \ldots, f_m + b_m) \subset \mathbb{P}^{k-1}$ es absolutamente irreducible de dimensión $k - m - 1$.
- $pcl(V) = \boldsymbol{V}(f_1^h, \ldots, f_m^h) \subset \mathbb{P}^k$ es intersección completa absolutamente irreducible de dimensión $k - m$ y grado $d_1 \cdots d_m$ y $codim(sing(pcl(V))) \geq 2$ (es normal).

Teorema (Ghorpade & Lachaud 2002)

Sea $V \subset \mathbb{P}^n$ una intersección completa absolutamente irreducible de dimensión r y cuyo lugar singular tiene dimensión menor o igual a s, con $0 \leq s \leq r-1$, multigrado $(d_1, \ldots, d_{m-r})$ y sea $d = \max\{d_1, \ldots, d_{m-r}\}$ entonces

$$\left| |V(\mathbb{F}_q)| - p_r \right| \leq \binom{m-s}{r-s-1} (d+1)^{m-s-1} q^{\frac{r+s+1}{2}} + 9 \cdot 2^{m-r} ((m-r)d+3)^{m+1} q^{\frac{r+s}{2}}$$

En la clausura proyectiva:

$$\left||pcl(V(\mathbb{F}_q))| - p_{k-m}\right| \leq \binom{k-m+1}{k-2m}(d_1+1)^{k-m}q^{\frac{k}{2}} + 9\cdot 2^m(md_1+3)^{k+1}q^{\frac{k-1}{2}} \quad (1)$$

En los puntos del infinito:

$$\left||V_\infty(\mathbb{F}_q)| - p_{k-m-1}\right| \leq \binom{k-m}{k-2m-1}(d_1+1)^{k-m-1}q^{\frac{k-1}{2}} + 9\cdot 2^m(md_1+3)^{k}q^{\frac{k-2}{2}} \quad (2)$$

(3)

Juntando ambas estimaciones:

$$\left||V(\mathbb{F}_q)| - q^{k-m}\right| \leq 3^4 \cdot 2^{m-2}(3 + d_1 \cdot m)^{k+1} \cdot q^{\frac{k}{2}}$$

- En la literatura no hay resultados acerca de este tipo de sistemas.
- El orden del error es el mismo que en el caso de exponentes igualados en columna. Esto fue trabajado en:

  M. Perez and M. Privitelli, On the number of simultaneous solutions of certain diagonal equations over finite fields, J. Number Theory 236 (2022), 160–187.

Subset sum problem:

Sea $D \subset \mathbb{F}_q$. Sea $m \in \mathbb{N}$ y $k \in \mathbb{Z}$ tal que $1 \leq k \leq |D|$. Sea $(b_1, \ldots, b_m) := b \in \mathbb{F}_q^m$, $N_m(k, b)$ el número de subconjuntos $S \subset D$ con cardinal k tal que para $i = 1, \ldots, m$, $\sum_{a \in S} a^i = b_i$.

Ejemplo:

Consideremos $\mathbb{F}_{43}$, $D = \{1, 2, 3, 4\}$, $k = 3$ $b := (6, 14)$.
Estamos buscando todos los subconjuntos de tres elementos tales que verifiquen que:

$$a_1 + a_2 + a_3 = 6$$
$$a_1^2 + a_2^2 + a_3^2 = 14$$

Consideraciones a tener en cuenta:

- Consideramos $D = \mathbb{F}_q$.
- Estamos contando de más. Hay que corregir la cantidad.

Resultados previos:

Li & Wan (2010)

$$\left| N_m(k,b) - \frac{1}{q^m}\binom{q}{k} \right| < \binom{\frac{q}{p} + (m-1)\sqrt{q} + k - 1}{k}$$

Li & Wan (2010)

$\forall \varepsilon > 0$, $\exists C_\varepsilon > 0$ tal que si $m < \varepsilon\sqrt{k}$, $4\varepsilon^2 \ln q^2 < k \leq C_\varepsilon q$ entonces $N_m(k,b) > 0$ para todo $b \in \mathbb{F}_q^m$.

Notación:

- $X := V$
- $\overline{X} := \{(X_1, \ldots, X_k) \in X : X_i \neq X_j \ \forall i \neq j\}$.
- Sea S_k el grupo simétrico de k elementos.
- Una permutación τ se dice de tipo $(c_1, c_2, \ldots, c_k)$ si tiene exactamente c_i ciclos de longitud i.
- Cada $\tau \in S_k$ se factoriza como producto de ciclos disjuntos.
- Llamaremos $l(\tau)$ al número de ciclos de τ.
- Notaremos $C(\tau)$ al número de permutaciones conjugadas a τ.
- Dado $\tau = (i_1 i_2 \cdots i_{\alpha_1}) \cdots (l_1 l_2 \cdots l_{\alpha_s})$
  $X_\tau := \{(x_1, \ldots, x_k) \in X, x_{i_1} = \cdots = x_{i_{\alpha_1}}, \ldots, x_{l_1} = \cdots = x_{l_{\alpha_s}}\}$
  Ej: $\tau = (12)(34)$ $X_\tau = \{(x_1, \ldots, x_k) \in X, x_1 = x_2, x_3 = x_4\}$.

Teorema

El número de permutaciones en S_k de tipo $(c_1, c_2, \ldots, c_k)$ es $N(c_1, c_2, \ldots, c_k) = \frac{k!}{1^{c_1} c_1! \cdots k^{c_k} c_k!}$

Teorema (Li & Wan 2010)

Sea C_k el conjunto de clases de conjugación de S_k. Si X es simétrico, entonces

$$|\overline{X}| = \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau|.$$

X se dice simétrico si es invariante bajo la acción de S_k.

Buscamos estimar $|\overline{X}|$:

Separaremos en dos casos $p|k$ y $p \nmid k$. Para el primer caso trabajaremos con:
$CP_k = \{\tau \in C_k :$
τ tiene longitud $l(\tau)$ y todos los ciclos de τ tienen longitud divisible por $p\}$

Si pedimos $b \neq (0, \ldots, 0)$:

$$
\begin{aligned}
|\overline{X}| &= \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau| \\
&= \underbrace{\sum_{\substack{1 \leq l(\tau) \leq k \\ \tau \in CP_k}} (-1)^{k-l(\tau)} C(\tau) |X_\tau|}_{=0} + \sum_{\substack{1 \leq l(\tau) \leq k \\ \tau \in \overline{CP_k}}} (-1)^{k-l(\tau)} C(\tau) |X_\tau|
\end{aligned}
$$

Podemos separar en conjuntos disjuntos a $\overline{CP_k}$ del siguiente modo:

$$\overline{CP_k} = \bigcup_{i=0}^{\frac{k}{p}-1} \{\tau : \tau \text{ tiene longitud } l(\tau) \text{ y tiene exactamente } i \text{ ciclos de longitud divisibles por } p\}$$

$$\sum_{\substack{1 \leq l(\tau) \leq k \\ \tau \in \overline{CP_k}}} (-1)^{k-l(\tau)} C(\tau)|X_\tau| = \sum_{\substack{1 \leq l(\tau) \leq k \\ \tau \in D(0, l(\tau))}} (-1)^{k-l(\tau)} C(\tau)|X_\tau| + \cdots + \sum_{\substack{1 \leq l(\tau) \leq k \\ \tau \in D\left(\frac{k}{p}-1, l(\tau)\right)}} (-1)^{k-l(\tau)} C(\tau)|X_\tau|$$

$$\sum_{\substack{1\le l(\tau)\le k\\ \tau\in D(0,l(\tau))}} (-1)^{k-l(\tau)} C(\tau)|X_\tau| = \underbrace{\sum_{\substack{l(\tau)=2m+1\\ \tau\in D(0,l(\tau))}}^{k} (-1)^{k-l(\tau)} C(\tau)|X_\tau|}_{(A)} + \underbrace{\sum_{\substack{l(\tau)=1\\ \tau\in D(0,l(\tau))}}^{2m} (-1)^{k-l(\tau)} C(\tau)|X_\tau|}_{(B)}$$

$$\vdots$$

$$\sum_{\substack{1\le l(\tau)\le k\\ \tau\in D\left(\frac{k}{p}-1,l(\tau)\right)}} (-1)^{k-l(\tau)} C(\tau)|X_\tau| = \underbrace{\sum_{\substack{l(\tau)=2m+\frac{k}{p}+1\\ \tau\in D\left(\frac{k}{p}-1,l(\tau)\right)}}^{k} (-1)^{k-l(\tau)} C(\tau)|X_\tau|}_{(A)} + \underbrace{\sum_{\substack{l(\tau)=1\\ \tau\in D\left(\frac{k}{p}-1,l(\tau)\right)}}^{2m+\frac{k}{p}} (-1)^{k-l(\tau)} C(\tau)|X_\tau|}_{(B)}$$

Si $l(\tau)-i \geq 2m+1$ podemos acotar usando nuestra estimación Caso (A):

$$||X_\tau| - q^{l(\tau)-m}| \leq cte \cdot q^{\frac{l(\tau)}{2}}$$

Si $l(\tau)-i \leq 2m$ podemos usar una cota clásica Caso (B):

$$|X_\tau| \leq d_1^{l(\tau)-i-1} \leq d_1 q^{2m-i-1}$$

Considerar que $N_m(k,b) = \frac{|\overline{X}|}{k!}$

Cota superior:

$$N_m(k,b) \leq \frac{1}{q^m}\binom{q}{k} + \frac{1}{q^m}(-1)^{k+\frac{k}{p}-1}\binom{q/p}{k/p} + 4 \cdot cte \cdot \underbrace{(-1)^k \binom{-\sqrt{q}}{k}}_{\sim q^{\frac{k}{2}}}$$

Cota inferior:

$$N_m(k,b) \geq \frac{1}{q^m}\binom{q}{k} + \frac{1}{q^m}(-1)^{k+\frac{k}{p}-1}\binom{q/p}{k/p} - 4 \cdot cte \cdot \underbrace{(-1)^k \binom{-\sqrt{q}}{k}}_{\sim q^{\frac{k}{2}}}$$

La estimación nos queda:

Caso $p|k, (b_1, \ldots, b_n) \neq 0$,

Si $p \geq 3$, $k \geq 4m$:

$$\left| N_m(k,b) - \left(\frac{1}{q^m}\binom{q}{k} + \frac{1}{q^m}(-1)^{k+\frac{k}{p}-1}\binom{q/p}{k/p} \right) \right| \leq 4 \cdot cte \cdot \underbrace{(-1)^k \binom{-\sqrt{q}}{k}}_{\sim q^{\frac{k}{2}}}$$

Casos que faltan:

- $p|k,\ b = 0.$
- $p \nmid k,\ b = 0.$
- $p \nmid k,\ b \neq 0.$

Teorema (nuestra estimación)

Si $m \leq \frac{k-\lfloor \frac{k}{p} \rfloor}{2}$ *y* $p \geq 3$

1. *Si* $p \nmid k$

$$\left| N_m(k,b) - \frac{1}{q^m}\binom{q}{k} \right| \leq 2q^{m-1} + (-1)^k cte \binom{-\sqrt{q}}{k} + 2q^{m+\lfloor \frac{k}{p} \rfloor}$$

2. *Si* $p|k$

$$\left| N_m(k,b) - \left(\frac{1}{q^m}\binom{q}{k} + \frac{v(b)}{q^m}(-1)^{k+\frac{k}{p}} \binom{q/p}{k/p} \right) \right|$$
$$\leq 2q^{m-1} + (-1)^k cte \binom{-\sqrt{q}}{k} + 2q^{m+\frac{k}{p}}$$

donde $v(b) = q^m - 1$ *si* $b = \mathbf{0}$, $v(b) = -1$ *si* $b \neq \mathbf{0}$ *y* $cte = 3^4 2^m (3 + d_1 m)^{k+1}$.

Teorema (Li & Wan (2010))

Si $m \leq k-2$

$$\left| N_m(k,b) - \frac{1}{q^m}\binom{q}{k} \right| \leq m^k \left(\frac{3}{2}\right)^{k-1} \left(\frac{q}{p}\right)^k$$

Existencia:

Nuestro resultado

Para cualquier $\varepsilon \in (0, \frac{6}{25})$, si $2 \leq m \leq \sqrt{\frac{2}{7}} k^{\varepsilon}$ y $14^{\frac{1}{2\varepsilon}} \leq k \leq q$ entonces, $N_m(k, b) > 0$ para todo $b \in \mathbb{F}_q^m$.

Li & Wan (2010)

$\forall \varepsilon > 0$, $\exists C_\varepsilon > 0$ tal que si $m < \varepsilon\sqrt{k}$, $4\varepsilon^2 \ln q^2 < k \leq C_\varepsilon q$ entonces $N_m(k, b) > 0$.

¡Muchas gracias!