Códigos tóricos sobre hipersimplejos

Jesica Rubí Lara Rosales, Nuria Sydykova Méndez
Néstor Fabián Bravo Hernández, Omar Alfredo Jaloma López
José de Jesús Liceaga Martínez, Jonatan García Pernia.
CIMAT/DEMAT, Universidad de Guanajuato.

Introducción

Problema.
Encontrar fórmulas para los parámetros básicos sobre un código tórico sobre un hipersimplejo, $\mathcal{C}_{\mathcal{P}}(d)$.

Configuración.
Sea $S = K[t_1, \dots, t_s] = \oplus_{d=0}^{\infty} S_d$ un anillo polinomial sobre un campo finito $K = \mathbb{F}_q$ con la clasificación estándar. El *toro afín* del espacio afín $\mathbb{A}^s := K^s$ está dado por $T := (K^*)^s$, donde K^* es el grupo multiplicativo de K. La cardinalidad de T es igual a $(q-1)^s$. Si $g \in S$, denotamos al conjunto de raíces de g in T por $V_T(g)$.
Definición.
Para $s \geq 2$, sea $1 \leq d \leq s$ un entero, y sea $\mathcal{P}$ la envolvente convexa en $\mathbb{R}^s$ de todos los puntos enteros

$$\mathcal{A}_d = \{\mathbf{e}_{i_1} + \cdots + \mathbf{e}_{i_d} | 1 \leq i_1 < \cdots < i_d \leq s\},$$

donde $\mathbf{e}_i$ es el i-ésimo vector en $\mathbb{R}^s$. El retículo politópico $\mathcal{P}$ es llamado el d-ésimo hipersimplejo de $\mathbb{R}^s$ [1, p.84].
Ejemplo 1.
Sea $s = 3$, entonces el primer hipersimplejo

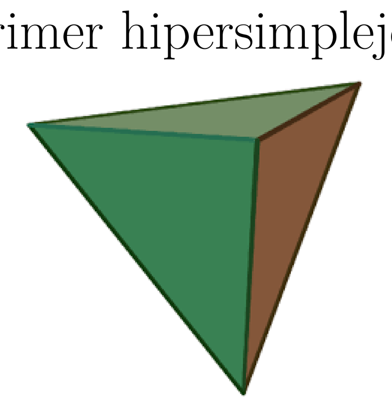

Figura 1:Tetraedro.

Códigos sobre hipersimplejos

El *código tórico* de $\mathcal{P}$ de grado d, denotado por $\mathcal{C}_{\mathcal{P}}(d)$ o simplemente $\mathcal{C}_{\mathcal{P}}$, es la imagen del mapeo de evaluación

$$\mathrm{ev}_d : \mathcal{L}_d \to \mathbb{K}^m, \quad f \mapsto (f(P_1), \dots, f(P_m)),$$

donde $\mathcal{L}_d$ es el K-subespacio vectorial de S_d generado por todos los $t^a := t_1^{a_1} \cdots t_s^{a_s}$, $a = (a_1, \dots, a_s)$, tal que $a \in \mathcal{P} \cap \mathbb{Z}^s$ y $\{P_1, \dots, P_m\}$ es el conjunto de todos los puntos del toro afín T de $\mathbb{A}^s$.
Los *parámetros básicos* de $\mathcal{C}_{\mathcal{P}}(d)$ son

- La *longitud* m.
- La *dimensión* $\dim_K(\mathcal{C}_{\mathcal{P}}(d))$.
- La mínima distancia

$$\delta\left(\mathcal{C}_{\mathcal{P}}(d)\right) := \text{mín}\left\{|T \setminus V_T(g)| \quad | \quad g \in \mathcal{L}_d \setminus I(T)\right\}.$$

Los códigos tóricos fueron introducidos por Hansen [2] y han sido activamente estudiados la última década, ver [**?**].
Observaciones.

- Un monomio t^a de S pertenece a $\mathcal{L}_d$ si y solo si t^a es libre de cuadrados y tiene grado d, esto es, un punto entero a de $\mathbb{N}^s$ pertenece a $\mathcal{P}$ si y solo si t^a está en $\mathcal{L}_d$, donde $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- Si reemplazamos $\mathcal{L}_d$ por $S_{\leq d}$ en el mapeo de evaluación, la imagen del mapeo resultante es un código de tipo Reed-Muller $\mathcal{C}_T(d)$ sobre el toro afín T. la mínima distancia de $\mathcal{C}_T(d)$ fue determinada en [3]

Parámetros básicos de $\mathcal{C}_{\mathcal{P}}(d)$ [6]

Sea $\mathcal{C}_{\mathcal{P}}(d)$ el código tórico sobre el hipersimplejo $\mathcal{P}$ de grado d. Luego, la longitud de $\mathcal{C}_{\mathcal{P}}(d)$ es $m = (q-1)^s$,

$$\dim_{\mathbb{K}}(\mathcal{C}_{\mathcal{P}}(d)) = \begin{cases} \binom{s}{d}, \text{ if } q \geq 3, \\ \\ 1, \quad \text{if } q = 2. \end{cases} \tag{1}$$

,

$$\delta_d = \begin{cases} (q-2)^d(q-1)^{s-d}, \text{ si} & d \leq s/2, q \geq 3, \\ (q-1)^d(q-2)^{s-d}, \text{ si} & s/2 < d < s, q \geq 3, \\ (q-1)^s, \quad \text{si} & d = s, \\ 1, \quad \text{si} & q = 2, \end{cases} \tag{2}$$

Ejemplo 2

Para $s = 3$, $d = 1$, y $q = 3$, tenememos que el primer hipersimplejo está dado por la envolvente convexa de (ver Figura 1)

$$\mathcal{A}_1 = \{\mathbf{e}_i | 1 \leq i \leq 3\} = \{(1,0,0), (0,1,0), (0,0,1)\}.$$

Entonces, $\mathcal{L}_1$ es generado por t_1, t_2, t_3 como $\mathbb{F}_3$-espacio vectorial. Dado que $T = \{(1,1,1), (1,1,2), (1,2,1), (1,2,2), (2,1,1), (2,1,2), (2,2,1), (2,2,2)\}$
Tenemos que

$$\mathcal{C}_{\mathcal{P}}(1) = \mathrm{im}(\mathrm{ev}_1) = ((1,1,1,1,2,2,2,2), (1,2,1,2,1,2,1,2), (1,1,2,2,1,1,2,2)).$$

Los parámetros básicos $\mathcal{C}_{\mathcal{P}}(1)$ están dados por las formulas (1) y (2), $\dim_{\mathbb{K}}(\mathcal{C}_{\mathcal{P}}(1)) = 3$, $\delta_1 = 4$, y longitud $(\mathcal{C}_{\mathcal{P}}(1)) = 2^3 = 8$.

Ejemplo 3

Para $s = 4$ y $q = 3$, la lista de los valores de la longitud, dimensión, y distancia mínima de $\mathcal{C}_{\mathcal{P}}(d)$ está dada en la siguiente tabla

d	1	2	3	4
m	16	16	16	16
$\dim_{\mathbb{K}}(\mathcal{C}_{\mathcal{P}}(d))$	4	6	4	1
δ_d	8	4	8	16

Referencias

[1] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series **8**, American Mathematical Society, Rhode Island, 1996.

[2] J. Hansen, *Toric surfaces and error-correcting codes* in Coding Theory, Cryptography, and Related Areas, Springer, 132-142, 2000.

[3] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, The minimum distance of parameterized codes on projective tori, Appl. Algebra Engrg. Comm. Comput. **22** (2011), no. 4, 249–264.

[4] J. Martínez-Bernal, Y. Pitones and R. H. Villarreal, Minimum distance functions of complete intersections, J. Algebra Appl. **17** (2018), no. 11, 1850204 (22 pages).

[5] J. Martínez-Bernal, Y. Pitones and R. H. Villarreal, Minimum distance functions of graded ideals and Reed-Muller-type codes, J. Pure Appl. Algebra **221** (2017), 251–275.

[6] D. Jaramillo, M. Vaz Pinto, and R. H. Villarreal, Evaluation codes and their basic parameters, Des. Codes Cryptogr. **89** (2021), 269–300.