

Códigos binarios auto-duales doblemente pares.

Carlos Segovia González

Instituto de Matemáticas UNAM Oaxaca, México

en colaboración con Rafael Ochoa

Congreso de la SMM
Villahermosa, Tabasco

La motivación,

cuántas esferas del mismo tamaño pueden tocar una esfera?

- ▶ en dimensión uno, la respuesta es 2,
- ▶ en dimensión dos, las abejas descubrieron la respuesta dada por 6,
- ▶ en dimensión tres, la respuesta es 12 a pesar de la controversia de Isaac Newton y David Gregory.
- ▶ en dimensión cuatro, la respuesta es 24 (ref. Oleg R. Musin),
- ▶ en dimensiones ocho, la respuesta es 240 y es rígida y dada por la retícula de Gosset,
- ▶ en dimensiones veinticuatro, la respuesta es 196560 y es rígida y es dada por la retícula de Leech.

Códigos

- ▶ Un **código** binario C de la forma $[n, k, d]$ es un subespacio lineal de $\mathbb{Z}_2^n$ (longitud n , dimensión k y distancia mínima d). Tendremos matriz de paridad H ó matriz generadora G .
- ▶ Tenemos los **códigos de Hamming** H_r de la forma $[2^r - 1, 2^r - 1 - r, 3]$, donde para $r = 3$ tenemos un código $[7, 4, 3]$ con matriz chequeo

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Éste código tiene 7 elementos de peso tres, 7 elementos de peso cuatro, y su polinomio de pesos es

$$W_{H_3}(x, y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7.$$

- ▶ Los códigos de Hamming son perfectos.

- Agregando un chequeo a H_3 obtenemos el **código de Hamming extendido** h_8 que es un código $[8, 4, 4]$ con matriz de chequeo

$$\hat{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

En la forma estandar podemos ver que

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

donde $AA^{tr} = I$ implica que $h_8 = \hat{H}_3$ es **autodual**. Debido a su definición tiene 14 elementos de peso 4 y su polinomio de pesos es

$$W_{h_8}(x, y) = x^8 + 14x^4y^4 + y^8.$$

- El **código de Golay** G_{23} está generado por el polinomio irreducible en $\mathbb{F}_2$,

$$g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1,$$

luego estamos considerando $f(x)$ con grado $m \leq n - 1$ tal que $g(x)$ lo divide. Los codigos son dados por los coeficientes.

- Tenemos que G_{23} es de la forma $[23, 12, 7]$ y además junto con el código de Hamming son los únicos códigos perfectos no triviales. Su polinomio de pesos es

$$W_{G_{23}}(x, y) = x^{23} + 253x^7y^{16} + 506x^8y^{15} + 1288x^{11}y^{12} + 1288x^{12}y^{11} + 506x^{15}y^8 + 253x^{16}y^7 + y^{23}.$$

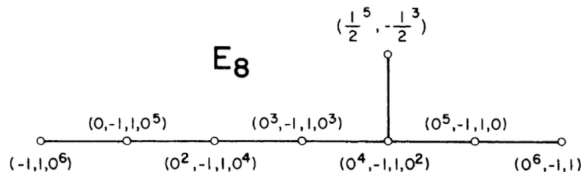
- El **código de Golay extendido** G_{24} está dado por añadir un chequeo a G_{23} y tiene matriz generadora,

Retículas

- ▶ Una **retícula** L de un espacio vectorial real V (con V de dimensión finita) es un subgrupo de V tal que genera a V como $\mathbb{R}$ espacio.
- ▶ Consideramos la **retícula Gosset** E_8 dada por el subgrupo de $\mathbb{R}^8$,

$$\left\{ (x_i) \in \mathbb{Z}^8 \sqcup \left(\mathbb{Z} + \frac{1}{2} \right)^8 : \sum_i x_i = 0 \pmod{2} \right\}$$

Una base entera en términos de un sistema de raíces es,



Los vectores mínimos son $2^4(14)$ vectores $((\pm 1/2)^4, 0^4)$, 16 vectores $(\pm 1, 0^7)$ dando un total de 240.

- La **construcción A**: tomemos el mapa dado por modulo 2,

$$\rho : \mathbb{Z}^n \rightarrow \mathbb{Z}_2^n$$

Para un código C , tendremos la retícula $\rho^{-1}(C)$ es entera.
Tomaremos $\frac{1}{\sqrt{2}}\rho^{-1}(C)$. En particular:

- i) $\frac{1}{\sqrt{2}}\rho^{-1}(C)$ será **unimodular** cuando C es **auto-dual**, y
 - ii) $\frac{1}{\sqrt{2}}\rho^{-1}(C)$ será **par** cuando C es **doblemente par**.
- Para la retícula de Gosset tenemos la identificación multiplicando por $\frac{1}{\sqrt{2}}$ con,
 - $\frac{1}{\sqrt{2}}(\pm 1^4, 0^4) \longleftrightarrow ((\pm 1/2)^4, 0^4),$
 - $\frac{1}{\sqrt{2}}(\pm 2, 0^7) \longleftrightarrow (\pm 1, 0^7).$

donde bajo ρ , se tiene $(\pm 1^4, 0^4) \mapsto (1^4, 0^4)$ y $(\pm 2, 0^7) \mapsto (0^8).$

- Consideramos la **retícula de Leech** Γ_{24} generada por todos los elementos

$$\frac{1}{\sqrt{8}}(\mp 3, \pm 1^{23})$$

donde ∓ 3 puede ir en cualquier posición y los signos superiores se toman en una coordenada donde un código de Golay tenga 1.

- Para los vectores de peso cuatro 4 obtenemos las formas $(4^2, 0^{22})$, $(3, 1^{23})$, $(2^8, 0^{16})$ con frecuencias $2^2 \binom{24}{2}$, $2^{12} \cdot 24$, $2^7 \cdot 759$, que suma 196560.

- para m un entero positivo $r_L(m) := |\{x \in L \mid x \cdot x = 2m\}|$. La serie theta es

$$\sum_{m=0}^{\infty} r_L(m) q^m = 1 + r_L(1) + \dots$$

que converge para $|q| < 1$ (equivale a definirlo en el plano superior H con $q = e^{2\pi iz}$), así

$$\theta_L(z) = \sum_{m=0}^{\infty} r_L(m) q^m = \sum_{x \in L} q^{\frac{(x \cdot x)}{2}} = \sum_{x \in L} e^{\pi i (x \cdot x) z}$$

la función theta la cual es holomorfa en H y de peso $n/2$.

- La serie theta de la retícula de Gosset E_8 está dada por

$$\theta_{E_8} = 1 + 240q + 2160q^2 + 6720q^3 + \dots$$

- La serie theta de la retícula de Leech Γ_{24} está dada por

$$\theta_{\Gamma_{24}} = 1 + 196560q^4 + 16773120q^6 + \dots$$

Códigos-Retículas

Código

Código autodual

Doblemente par autocódigo

Polinomio de pesos

Polinomio invariante

Identidades de MacWilliams

Teorem de Gleason

Código de Hamming h_8

Código de Golay g_{24}

Retícula

Retícula unimodular

Retícula unimodular par

Serie theta

Forma modular

Identidad de Jacobi

Teorem de Hecke

Retícula de Gosset E_8

Retícula de Leech Γ_{24}

Gleason-Hecke

Un código es:

- ▶ **Type I**, si es binario auto-dual y no es doblemente par.
- ▶ **Type II**, si es binario auto-dual y doblemente par.

Teorema (Gleason)

Si C es un código auto-dual de Tipo I, II, III ó IV, entonces $W_C \in \mathbb{C}[f, g]$, donde:

Type	f	g
I	$x^2 + y^2$	$x^2 y^2 (x^2 - y^2)^2$
II	$x^8 + 14x^4 y^4 + y^8$	$x^4 y^4 (x^4 - y^4)^4$
III	$x^4 + 8xy^3$	$y^3 (x^3 - y^3)^3$
IV	$x^2 + 3y^2$	$y^2 (x^2 - y^2)^2$

Una retícula es

- ▶ **Type I**, si es unimodular y no es par.
- ▶ **Type II**, si es unimodular y es par.

Teorema (Hecke)

Si L es una retícula de Type I ó II, entonces la función theta θ_Γ of Γ pertenece a $\mathbb{C}[f, g]$, donde:

Type	f	g
I	$\theta_3(z)$	$\Delta_8(z)$
II	$E_4(z)$	$\Delta_{24}(z)$

donde

$$\Delta_8(z) = \frac{1}{16} \theta_2(z)^4 \theta_4(z)^4 = q \left[\prod_{m=1}^{\infty} (1 - q^{2m-1})(1 - q^{4m}) \right]^8 = q - 8q^2 + 23q^3 - 64q^4 + 126q^5 - 224q^6 + \dots \text{ y}$$

$$\Delta_{24}(z) = \left[\frac{1}{2} \theta_2(z) \theta_3(z) \theta_4(z) \right]^8 = q^2 \prod_{m=1}^{\infty} (1 - q^{2m})^{24} = q^2 - 24q^4 + 252q^6 - 1472q^8 + \dots$$

Identidades MacWilliam-Jacobi

- ▶ Para códigos y retículas tipo I, las identidades de MacWilliam y Jacobi son:

i)

$$W_C((x+y)/\sqrt{2}, (x-y)/\sqrt{2}) = W_C(x, y),$$
$$W_C(x, -y) = W_C(x, y).$$

ii)

$$\theta_L(-1/z) = (z/i^{n/2})\theta_L(z),$$
$$\theta_L(z+2) = \theta_L(z).$$

- ▶ Para códigos y retículas tipo II, las identidades de MacWilliam y Jacobi son:

i)

$$W_C((x+y)/\sqrt{2}, (x-y)/\sqrt{2}) = W_C(x, y),$$
$$W_C(x, iy) = W_C(x, y),$$

ii)

$$\theta_L(-1/z) = (z/i^{n/2})\theta_L(z),$$
$$\theta_L(z+2) = \theta_L(z).$$

Grupo de Clifford-Weil

- ▶ Tomaremos el grupo generado por $\frac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$ y $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.
- ▶ En el caso no homogéneo por $\frac{1+i}{2} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$ y $\begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix}$.
- ▶ Tendremos grupos de orden 192 y 96. Denotemos $\mathcal{G}$ el grupo de Clifford-Weil.
- ▶ Sea $\mathcal{W} := \mathbb{C}[x, y]^{\mathcal{G}}$ y sea $\mathcal{L}_n$ el espacio de funciones holomorfas en el plano hiperbólico, periódicas junto con una condición adicional, luego $\mathcal{L} := \bigoplus_{n \geq 2} \mathcal{L}_n$.

Teorema (Michel)

Existe un isomorfismo de álgebra entre $\mathcal{W}$ y $\mathcal{L}$ dado para $p(x, y) \in \mathbb{C}[x, y]$ por $p(\theta_2, \theta_3)$, donde $\theta_2(z) = 2 \sum_{m=0}^{\infty} q^{(m+\frac{1}{2})^2}$ y $\theta_3(z) = 1 + 2 \sum_{m=1}^{\infty} q^{m^2}$.

Reciprocidad de Schur-Weyl

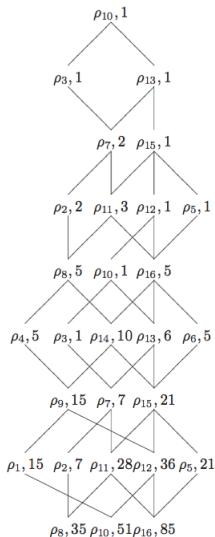
Teorema (Teoría invariante)

Considere las acciones de $GL(V)$ y Σ_m sobre $V^{\otimes m}$ y denote por $\langle GL(V) \rangle$ y $\langle S_m \rangle$ las subálgebras de $End(V^{\otimes m})$ generadas por $GL(V)$ y Σ_m , respectivamente. Entonces,

- a) $End_{S_m}(V^{\otimes m}) = \langle GL(V) \rangle$.
- b) Si $\text{char} K = 0$ entonces $End_{GL(V)}(V^{\otimes m}) = \langle S_m \rangle$.

Diagrama de Hasse

1
2
5
15
51
187
715
2795
11051
43947
:
:



$$1^2 = \mathbf{1}$$

$$1^2 + 1^2 = \mathbf{2}$$

$$2^2 + 1^2 = \mathbf{5}$$

$$2^2 + 3^2 + 1^2 + 1^2 = \mathbf{15}$$

$$5^2 + 1^2 + 5^2 = \mathbf{51}$$

$$5^2 + 1^2 + 10^2 + 6^2 + 5^2 = \mathbf{187}$$

$$15^2 + 7^2 + 21^2 = \mathbf{715}$$

$$15^2 + 7^2 + 28^2 + 36^2 + 21^2 = \mathbf{2795}$$

$$35^2 + 51^2 + 85^2 = \mathbf{11051}$$

Códigos-Retículas

Código

Código autodual

Doblemente par autocódigo

Polinomio de pesos

Polinomio invariante

Identidades de MacWilliams

Teorem de Gleason

Código de Hamming h_8

Código de Golay g_{24}

Grupo de Clifford-Weil $\mathcal{G}$

Diagrama de Bratteli de $\mathcal{G}$

Retícula

Retícula unimodular

Retícula unimodular par

Serie theta

Forma modular

Identidad de Jacobi

Teorem de Hecke

Retícula de Gosset E_8

Retícula de Leech Γ_{24}

Grupo esp. lin. $Sl_2(\mathbb{Z})$

D. Young hasta 4 cajas

-  M. KOSUDA and M. OURA, *Centralizer algebras of the primitive unitary reflection group of order 96*, 2 May 2015. arXiv:1505.00318v1 [math.RT]
-  J.P. SERRE, *A Course in Arithmetic* New York, Springer, N.J., 1973.
-  G. NEBE, E. M. RAINS and N. J. A. SLOANE, *Self-dual codes and invariant theory*. Springer-Verlag (2006).
-  E. M. RAINS and N. J. A. SLOANE, *Self-dual codes*, in Handbook of Coding Theory, ed. V. S. Pless and W. C. Huffman, Elsevier, Amsterdam, 1998, pp. 177 - 294.
-  A. M. GLEASON, *Weight polynomials of self-dual codes and the MacWilliams identities*, in: Actes Congres Internl. de Mathematique, 1970 (Gauthier-Villars. Paris, 1971) 211-215.
-  M. BROUÉ and M. ENGUEHARD, *Polinômes des poids de certains codes et fonctions thêta de certains réseaux*, Annales scientifiques de L'É.N.S. 4^e série, tome 5, n^o1, 1972, p. 157 -181.

-  J. H. CONWAY and N. J. A. SLOANE, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 2nd edition, 1993.
-  F.J. MACWILLIAMS and N.J.A. SLOANE, *The Theory of Error-Correcting Codes* North-Holland Mathematical Library, 1977.
-  J. LEECH, *Notes on sphere packings*, CJM 19, 1967.
-  M. J.E. GOLAY, *Notes on Digital Coding*, Proc. IRE 37, 657, 1949.
-  W. EBELING, *Lattices and Codes*, Vieweg, Wiesbaden, 1994