Lattices y Códigos

Juan Pablo Rossetti

FaMAF-CIEM, Córdoba, Argentina

Octubre de 2017
Córdoba

Introducción

Veremos 3 instancias donde se utiliza el cuerpo finito $\mathbf{F}_q$ para obtener importantes resultados en lattices:

• $\mathbf{F}_3$ y el *tetracode* para construir lattices *isospectrales* en la dimensión más baja posible: 4;

• $\mathbf{F}_4$ y el *hexacode* para construir el célebre *Leech lattice*, en dimensión 24;

• $\mathbf{F}_q$ (o el anillo $\mathbf{Z}_q$) para construir lattices *isospectrales en norma uno*, que producen ejemplos de espacios lentes isospectrales.

Introducción

Veremos 3 instancias donde se utiliza el cuerpo finito $\mathbf{F}_q$ para obtener importantes resultados en lattices:

• $\mathbf{F}_3$ y el *tetracode* para construir lattices *isospectrales* en la dimensión más baja posible: 4;

• $\mathbf{F}_4$ y el *hexacode* para construir el célebre *Leech lattice*, en dimensión 24;

• $\mathbf{F}_q$ (o el anillo $\mathbf{Z}_q$) para construir lattices *isospectrales en norma uno*, que producen ejemplos de espacios lentes isospectrales.

Introducción

Veremos 3 instancias donde se utiliza el cuerpo finito $\mathbf{F}_q$ para obtener importantes resultados en lattices:

• $\mathbf{F}_3$ y el *tetracode* para construir lattices *isospectrales* en la dimensión más baja posible: 4;

• $\mathbf{F}_4$ y el *hexacode* para construir el célebre *Leech lattice*, en dimensión 24;

• $\mathbf{F}_q$ (o el anillo $\mathbf{Z}_q$) para construir lattices *isospectrales en norma uno*, que producen ejemplos de espacios lentes isospectrales.

Introducción

Veremos 3 instancias donde se utiliza el cuerpo finito $\mathbf{F}_q$ para obtener importantes resultados en lattices:

• $\mathbf{F}_3$ y el *tetracode* para construir lattices *isospectrales* en la dimensión más baja posible: 4;

• $\mathbf{F}_4$ y el *hexacode* para construir el célebre *Leech lattice*, en dimensión 24;

• $\mathbf{F}_q$ (o el anillo $\mathbf{Z}_q$) para construir lattices *isospectrales en norma uno*, que producen ejemplos de espacios lentes isospectrales.

Isospectralidad

Geometría Espectral Inversa

Definición de *isospectralidad* para

- códigos
- lattices
- formas cuadráticas definidas positivas
- variedades Riemannianas

Isospectralidad

Geometría Espectral Inversa

Definición de *isospectralidad* para

- códigos
- lattices
- formas cuadráticas definidas positivas
- variedades Riemannianas

Isospectralidad

Geometría Espectral Inversa

Definición de *isospectralidad* para

- códigos
- lattices
- formas cuadráticas definidas positivas
- variedades Riemannianas

Isospectralidad

Geometría Espectral Inversa

Definición de *isospectralidad* para

- códigos
- lattices
- formas cuadráticas definidas positivas
- variedades Riemannianas

Isospectralidad

Geometría Espectral Inversa

Definición de *isospectralidad* para

- códigos
- lattices
- formas cuadráticas definidas positivas
- variedades Riemannianas

Isospectralidad

Geometría Espectral Inversa

Definición de *isospectralidad* para

- códigos
- lattices
- formas cuadráticas definidas positivas
- variedades Riemannianas

Isospectralidad

Geometría Espectral Inversa

Definición de *isospectralidad* para

- códigos
- lattices
- formas cuadráticas definidas positivas
- variedades Riemannianas

Ejemplo de Conway-Sloane en dim 6

códigos lineales binarios de longitud 6:

C_1						peso	C_2					
0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	2	1	0	1	0	0	0
0	0	1	1	0	0	2	0	0	1	0	1	0
0	0	0	0	1	1	2	1	0	0	0	1	0
1	1	1	1	1	1	6	1	1	1	1	1	1
0	0	1	1	1	1	4	0	1	0	1	1	1
1	1	0	0	1	1	4	1	1	0	1	0	1
1	1	1	1	0	0	4	0	1	1	1	0	1

C_1 y C_2 son 'isospectrales' pero no son isomorfos

Ejemplo de Conway-Sloane en dim 6

códigos lineales binarios de longitud 6:

$$
\begin{array}{ccc}
\mathcal{C}_1 & \text{peso} & \mathcal{C}_2 \\
\begin{array}{|cccccc|}
\hline
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 \\
\hline
\end{array}
&
\begin{array}{c}
0 \\ 2 \\ 2 \\ 2 \\ 6 \\ 4 \\ 4 \\ 4
\end{array}
&
\begin{array}{|cccccc|}
\hline
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 \\
\hline
\end{array}
\end{array}
$$

$\mathcal{C}_1$ y $\mathcal{C}_2$ son 'isospectrales' pero no son isomorfos

Ejemplo de Conway-Sloane en dim 6

códigos lineales binarios de longitud 6:

$\mathcal{C}_1$						peso	$\mathcal{C}_2$					
0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	2	1	0	1	0	0	0
0	0	1	1	0	0	2	0	0	1	0	1	0
0	0	0	0	1	1	2	1	0	0	0	1	0
1	1	1	1	1	1	6	1	1	1	1	1	1
0	0	1	1	1	1	4	0	1	0	1	1	1
1	1	0	0	1	1	4	1	1	0	1	0	1
1	1	1	1	0	0	4	0	1	1	1	0	1

$\mathcal{C}_1$ y $\mathcal{C}_2$ son 'isospectrales' pero no son isomorfos

Ejemplo de Conway-Sloane en dim 6

códigos lineales binarios de longitud 6:

$\mathcal{C}_1$						peso	$\mathcal{C}_2$					
0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	2	1	0	1	0	0	0
0	0	1	1	0	0	2	0	0	1	0	1	0
0	0	0	0	1	1	2	1	0	0	0	1	0
1	1	1	1	1	1	6	1	1	1	1	1	1
0	0	1	1	1	1	4	0	1	0	1	1	1
1	1	0	0	1	1	4	1	1	0	1	0	1
1	1	1	1	0	0	4	0	1	1	1	0	1

$\mathcal{C}_1$ y $\mathcal{C}_2$ son 'isospectrales' pero no son isomorfos

Ejemplo de Conway-Sloane en dim 6

códigos lineales binarios de longitud 6:

$\mathcal{C}_1$						peso	$\mathcal{C}_2$					
0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	2	1	0	1	0	0	0
0	0	1	1	0	0	2	0	0	1	0	1	0
0	0	0	0	1	1	2	1	0	0	0	1	0
1	1	1	1	1	1	6	1	1	1	1	1	1
0	0	1	1	1	1	4	0	1	0	1	1	1
1	1	0	0	1	1	4	1	1	0	1	0	1
1	1	1	1	0	0	4	0	1	1	1	0	1

$\mathcal{C}_1$ y $\mathcal{C}_2$ son 'isospectrales' pero no son isomorfos

$$\begin{array}{rccc} \varphi : & \mathbf{Z}^n & \longrightarrow & \mathbf{Z}_2^n \\ & (x_1, \ldots, x_n) & \longmapsto & (\bar{x}_1, \ldots, \bar{x}_n) \end{array}$$

$$L_i := \left\{ \bar{x} = (x_1, x_2, \ldots, x_6) \in \mathbf{Z}^6 \,:\, \varphi(\bar{x}) \in \mathcal{C}_i \right\}, \qquad i = 1, 2.$$

O lo mismo, $\quad L_i = \varphi^{-1}(C_i)$

Teorema. L_1 y L_2 son lattices isospectrales y no isométricos.

Veamos a continuación la construcción en dimensión 4

$$\begin{array}{rccc} \varphi: & \mathbf{Z}^n & \longrightarrow & \mathbf{Z}_2^n \\ & (x_1,\dots,x_n) & \longmapsto & (\bar{x}_1,\dots,\bar{x}_n) \end{array}$$

$$L_i := \left\{ \bar{x} = (x_1, x_2, \dots, x_6) \in \mathbf{Z}^6 \,:\, \varphi(\bar{x}) \in \mathcal{C}_i \right\}, \qquad i = 1, 2.$$

O lo mismo, $\quad L_i = \varphi^{-1}(C_i)$

Teorema. L_1 y L_2 son lattices isospectrales y no isométricos.

Veamos a continuación la construcción en dimensión 4

Lattices en dimensión 4

Consideramos el código lineal ternario de longitud 4 con 9 palabras:

$$(0,0,0,0) \qquad \pm(0,1,1,1)$$

$$\pm(1,0,1,-1) \qquad \pm(1,-1,0,1) \qquad \pm(1,1,-1,0)$$

Sean e_a, e_b, e_c y e_d 4 vectores mutuamente ortogonales de distintas longitudes, con

$$e_a \cdot e_a = \frac{a}{12} \qquad e_b \cdot e_b = \frac{b}{12} \qquad e_c \cdot e_c = \frac{c}{12} \qquad e_d \cdot e_d = \frac{d}{12}$$

Notación: $[w,x,y,z]$ para $w\, e_a + x\, e_b + y\, e_c + z\, e_d$. Se definen los lattices $L^+ = L^+(a,b,c,d)$ y $L^- = L^-(a,b,c,d)$ como los generado por

$$\begin{aligned} v_1^+ &= [+3,-1,-1,-1] & v_1^- &= [-3,-1,-1,-1] \\ v_2^+ &= [+1,+3,+1,-1] & v_2^- &= [+1,-3,+1,-1] \\ v_3^+ &= [+1,-1,+3,+1] & v_3^- &= [+1,-1,-3,+1] \\ v_4^+ &= [+1,+1,-1,+3] & v_4^- &= [+1,+1,-1,-3]. \end{aligned}$$

Los vectores de un tetralattice módulo 3 son una palabra en el tetracode, y toda palabra del tetracode es igual, módulo 3, a uno de los vectores generadores de un tetralattice.

El núcleo del mapeo de L^+ en el tetracode da un sublattice M^+ de índice 9 en L^+, que a su vez es congruente al correspondiente sublattice M^- en L^-.
Además, la otras 8 coclases en L^+ son $\pm v_i + M^+$, para $i = 1, 2, 3, 4$, y con estos datos se prueba la isospectralidad.
Se esperaba que para $0 < a < b < c < d$, $L^+(a, b, c, d)$ y $L^-(a, b, c, d)$ fueran siempre no isométricos, pero solo se probó inicialmente para valores enteros hasta un cierto número grande.
Cerviño y Hein completaron la prueba.

Los vectores de un tetralattice módulo 3 son una palabra en el tetracode, y toda palabra del tetracode es igual, módulo 3, a uno de los vectores generadores de un tetralattice.

El núcleo del mapeo de L^+ en el tetracode da un sublattice M^+ de índice 9 en L^+, que a su vez es congruente al correspondiente sublattice M^- en L^-.
Además, la otras 8 coclases en L^+ son $\pm v_i + M^+$, para $i = 1, 2, 3, 4$, y con estos datos se prueba la isospectralidad.
Se esperaba que para $0 < a < b < c < d$, $L^+(a, b, c, d)$ y $L^-(a, b, c, d)$ fueran siempre no isométricos, pero solo se probó inicialmente para valores enteros hasta un cierto número grande.
Cerviño y Hein completaron la prueba.

Los vectores de un tetralattice módulo 3 son una palabra en el tetracode, y toda palabra del tetracode es igual, módulo 3, a uno de los vectores generadores de un tetralattice.

El núcleo del mapeo de L^+ en el tetracode da un sublattice M^+ de índice 9 en L^+, que a su vez es congruente al correspondiente sublattice M^- en L^-.
Además, la otras 8 coclases en L^+ son $\pm v_i + M^+$, para $i = 1, 2, 3, 4$, y con estos datos se prueba la isospectralidad.
Se esperaba que para $0 < a < b < c < d$, $L^+(a, b, c, d)$ y $L^-(a, b, c, d)$ fueran siempre no isométricos, pero solo se probó inicialmente para valores enteros hasta un cierto número grande.
Cerviño y Hein completaron la prueba.

Lattices enteros

Un lattice L es **entero** si $\mathbf{v} \cdot \mathbf{w}$ es entero $\forall\, \mathbf{v}, \mathbf{w} \in L$;

un lattice entero L es **par** si $\mathbf{v} \cdot \mathbf{v}$ es par $\forall\, \mathbf{v} \in L$;

un lattice entero L es **unimodular** si su volumen es uno.

Si $\mathcal{C}$ es un código lineal binario de tipo $[n, k]$, entonces

$$\mathcal{C}^{\perp} := \{\bar{x} \in Z_2^n \,:\, \bar{x} \cdot c = 0 \ \ \forall c \in \mathcal{C}\}$$

es el (código) **dual** de $\mathcal{C}$ (de tipo $[n, n-k]$).

Lattices enteros

Un lattice L es **entero** si $\mathbf{v} \cdot \mathbf{w}$ es entero $\forall\, \mathbf{v}, \mathbf{w} \in L$;

un lattice entero L es **par** si $\mathbf{v} \cdot \mathbf{v}$ es par $\forall\, \mathbf{v} \in L$;

un lattice entero L es **unimodular** si su volumen es uno.

Si $\mathcal{C}$ es un código lineal binario de tipo $[n, k]$, entonces

$$\mathcal{C}^{\perp} := \{\bar{x} \in Z_2^n \;:\; \bar{x} \cdot c = 0 \;\; \forall c \in \mathcal{C}\}$$

es el (código) **dual** de $\mathcal{C}$ (de tipo $[n, n-k]$).

Lattices enteros

Un lattice L es **entero** si $\mathbf{v} \cdot \mathbf{w}$ es entero $\forall\, \mathbf{v}, \mathbf{w} \in L$;

un lattice entero L es **par** si $\mathbf{v} \cdot \mathbf{v}$ es par $\forall\, \mathbf{v} \in L$;

un lattice entero L es **unimodular** si su volumen es uno.

Si $\mathcal{C}$ es un código lineal binario de tipo $[n, k]$, entonces

$$\mathcal{C}^{\perp} := \{\bar{x} \in Z_2^n \,:\, \bar{x} \cdot c = 0 \;\; \forall c \in \mathcal{C}\}$$

es el (código) **dual** de $\mathcal{C}$ (de tipo $[n, n-k]$).

Lattices enteros

Un lattice L es **entero** si $\mathbf{v} \cdot \mathbf{w}$ es entero $\forall \, \mathbf{v}, \mathbf{w} \in L$;

un lattice entero L es **par** si $\mathbf{v} \cdot \mathbf{v}$ es par $\forall \, \mathbf{v} \in L$;

un lattice entero L es **unimodular** si su volumen es uno.

Si $\mathcal{C}$ es un código lineal binario de tipo $[n, k]$, entonces

$$\mathcal{C}^{\perp} := \{\bar{x} \in Z_2^n \, : \, \bar{x} \cdot c = 0 \;\; \forall c \in \mathcal{C}\}$$

es el (código) **dual** de $\mathcal{C}$ (de tipo $[n, n-k]$).

Lattices enteros

Un lattice L es **entero** si $\mathbf{v} \cdot \mathbf{w}$ es entero $\forall\, \mathbf{v}, \mathbf{w} \in L$;

un lattice entero L es **par** si $\mathbf{v} \cdot \mathbf{v}$ es par $\forall\, \mathbf{v} \in L$;

un lattice entero L es **unimodular** si su volumen es uno.

Si $\mathcal{C}$ es un código lineal binario de tipo $[n, k]$, entonces

$$\mathcal{C}^{\perp} := \{\bar{x} \in Z_2^n \ : \ \bar{x} \cdot c = 0 \ \ \forall c \in \mathcal{C}\}$$

es el (código) **dual** de $\mathcal{C}$ (de tipo $[n, n-k]$).

Si $\mathcal{C}$ es un código lineal binario de tipo, se define $L_{\mathcal{C}} := \frac{1}{\sqrt{2}}\varphi^{-1}(\mathcal{C})$

Proposición.

- $\mathcal{C} \subset \mathcal{C}^{\perp} \iff L_{\mathcal{C}}$ es entero.
- $\mathcal{C}$ es doblemente par $\iff L_{\mathcal{C}}$ es par.
- C es autodual $\iff L_{\mathcal{C}}$ es unimodular.

Si $\mathcal{C}$ es un código lineal binario de tipo, se define $L_{\mathcal{C}} := \frac{1}{\sqrt{2}}\varphi^{-1}(\mathcal{C})$

Proposición.

- $\mathcal{C} \subset \mathcal{C}^{\perp} \iff L_{\mathcal{C}}$ es entero.
- $\mathcal{C}$ es doblemente par $\iff L_{\mathcal{C}}$ es par.
- C es autodual $\iff L_{\mathcal{C}}$ es unimodular.

Si $\mathcal{C}$ es un código lineal binario de tipo, se define $L_{\mathcal{C}} := \frac{1}{\sqrt{2}}\varphi^{-1}(\mathcal{C})$

Proposición.

- $\mathcal{C} \subset \mathcal{C}^{\perp} \iff L_{\mathcal{C}}$ es entero.
- $\mathcal{C}$ es doblemente par $\iff L_{\mathcal{C}}$ es par.
- C es autodual $\iff L_{\mathcal{C}}$ es unimodular.

Si $\mathcal{C}$ es un código lineal binario de tipo, se define $L_{\mathcal{C}} := \frac{1}{\sqrt{2}}\varphi^{-1}(\mathcal{C})$

Proposición.

- $\mathcal{C} \subset \mathcal{C}^{\perp} \iff L_{\mathcal{C}}$ es entero.
- $\mathcal{C}$ es doblemente par $\iff L_{\mathcal{C}}$ es par.
- $\mathcal{C}$ es autodual $\iff L_{\mathcal{C}}$ es unimodular.

Si $\mathcal{C}$ es un código lineal binario de tipo, se define $L_{\mathcal{C}} := \frac{1}{\sqrt{2}}\varphi^{-1}(\mathcal{C})$

Proposición.

- $\mathcal{C} \subset \mathcal{C}^{\perp} \iff L_{\mathcal{C}}$ es entero.
- $\mathcal{C}$ es doblemente par $\iff L_{\mathcal{C}}$ es par.
- C es autodual $\iff L_{\mathcal{C}}$ es unimodular.

Ejemplo: E_8 y el código de Hamming extendido

El retículo de raíces E_8 (mejor lattice packing y óptimo kissing number: 240. Recientemente, el mejor packing!!) se puede obtener a partir de códigos.

Con la construcción anterior, es el obtenido a partir de $\mathcal{H}_8$.

También se puede con la llamada Construcción B,
ésta es para códigos lineales pares, y uno solo se queda con los elementos de la forma
$\frac{1}{\sqrt{2}}(x_1, \ldots, x_n)$ tales que $\sum_{i=1}^{n} x_i$ es múltiplo de 4.

Ejemplo: E_8 y el código de Hamming extendido

El retículo de raíces E_8 (mejor lattice packing y óptimo kissing number: 240. Recientemente, el mejor packing!!) se puede obtener a partir de códigos.

Con la construcción anterior, es el obtenido a partir de $\mathcal{H}_8$.

También se puede con la llamada Construcción B,
ésta es para códigos lineales pares, y uno solo se queda con los elementos de la forma
$\frac{1}{\sqrt{2}}(x_1, \ldots, x_n)$ tales que $\sum_{i=1}^{n} x_i$ es múltiplo de 4.

Ejemplo: E_8 y el código de Hamming extendido

El retículo de raíces E_8 (mejor lattice packing y óptimo kissing number: 240. Recientemente, el mejor packing!!) se puede obtener a partir de códigos.

Con la construcción anterior, es el obtenido a partir de $\mathcal{H}_8$.

También se puede con la llamada Construcción B, ésta es para códigos lineales pares, y uno solo se queda con los elementos de la forma $\frac{1}{\sqrt{2}}(x_1, \dots, x_n)$ tales que $\sum_{i=1}^{n} x_i$ es múltiplo de 4.

Ejemplo: E_8 y el código de Hamming extendido

El retículo de raíces E_8 (mejor lattice packing y óptimo kissing number: 240. Recientemente, el mejor packing!!) se puede obtener a partir de códigos.

Con la construcción anterior, es el obtenido a partir de $\mathcal{H}_8$.

También se puede con la llamada Construcción B,
ésta es para códigos lineales pares, y uno solo se queda con los elementos de la forma
$\frac{1}{\sqrt{2}}(x_1, \ldots, x_n)$ tales que $\sum_{i=1}^{n} x_i$ es múltiplo de 4.

Ejemplo: E_8 y el código de Hamming extendido

El retículo de raíces E_8 (mejor lattice packing y óptimo kissing number: 240. Recientemente, el mejor packing!!) se puede obtener a partir de códigos.

Con la construcción anterior, es el obtenido a partir de $\mathcal{H}_8$.

También se puede con la llamada Construcción B,
ésta es para códigos lineales pares, y uno solo se queda con los elementos de la forma
$\frac{1}{\sqrt{2}}(x_1, \ldots, x_n)$ tales que $\sum_{i=1}^{n} x_i$ es múltiplo de 4.

Una construcción de Λ_{24}, el Leech lattice

Consideramos el cuerpo de 4 elementos $\mathbf{F}_4 = \{0, 1, \omega, \overline{\omega}\}$, tiene característica 2, y $1 + \omega + \overline{\omega} = 0$.

El **Hexacode** $\mathcal{C}_6$ es un código lineal de longitud 6 sobre $\mathbf{F}_4$:

para cada función cuadrática $\phi(x) = ax^2 + bx + c$ sobre $\mathbf{F}_4$ consideramos la 6-upla en $\mathbf{F}_4^6$

$$\big(a\,,\ b\,,\ c,\ d = \phi(1)\,,\ e = \phi(\omega)\,,\ f = \phi(\overline{\omega}) \big),$$

definimos $\mathcal{C}_6$ como el conjunto de palabras de esta forma.

Notemos que es un código lineal en $\mathbf{F}_4$, de dimensión 3 y peso mínimo 4.

Una construcción de Λ_{24}, el Leech lattice

Consideramos el cuerpo de 4 elementos $\mathbf{F}_4 = \{0, 1, \omega, \overline{\omega}\}$, tiene característica 2, y $1 + \omega + \overline{\omega} = 0$.

El **Hexacode** $\mathcal{C}_6$ es un código lineal de longitud 6 sobre $\mathbf{F}_4$:

para cada función cuadrática $\phi(x) = ax^2 + bx + c$ sobre $\mathbf{F}_4$ consideramos la 6-upla en $\mathbf{F}_4^6$

$$\big(a\,,\ b\,,\ c,\ d = \phi(1)\,,\ e = \phi(\omega)\,,\ f = \phi(\overline{\omega}) \big),$$

definimos $\mathcal{C}_6$ como el conjunto de palabras de esta forma.

Notemos que es un código lineal en $\mathbf{F}_4$, de dimensión 3 y peso mínimo 4.

Una construcción de Λ_{24}, el Leech lattice

Consideramos el cuerpo de 4 elementos $\mathbf{F}_4 = \{0, 1, \omega, \overline{\omega}\}$, tiene característica 2, y $1 + \omega + \overline{\omega} = 0$.

El **Hexacode** $\mathcal{C}_6$ es un código lineal de longitud 6 sobre $\mathbf{F}_4$:

para cada función cuadrática $\phi(x) = ax^2 + bx + c$ sobre $\mathbf{F}_4$ consideramos la 6-upla en $\mathbf{F}_4^6$

$$\big(\, a\,,\ b\,,\ c,\ d = \phi(1)\,,\ e = \phi(\omega)\,,\ f = \phi(\overline{\omega})\big),$$

definimos $\mathcal{C}_6$ como el conjunto de palabras de esta forma.

Notemos que es un código lineal en $\mathbf{F}_4$, de dimensión 3 y peso mínimo 4.

Una construcción de Λ_{24}, el Leech lattice

Consideramos el cuerpo de 4 elementos $\mathbf{F}_4 = \{0, 1, \omega, \overline{\omega}\}$,
tiene característica 2, y $1 + \omega + \overline{\omega} = 0$.

El **Hexacode** $\mathcal{C}_6$ es un código lineal de longitud 6 sobre $\mathbf{F}_4$:

para cada función cuadrática $\phi(x) = ax^2 + bx + c$ sobre $\mathbf{F}_4$
consideramos la 6-upla en $\mathbf{F}_4^6$

$$\big(\, a\,,\ b\,,\ c,\ d = \phi(1)\,,\ e = \phi(\omega)\,,\ f = \phi(\overline{\omega})\big),$$

definimos $\mathcal{C}_6$ como el conjunto de palabras de esta forma.

Notemos que es un código lineal en $\mathbf{F}_4$, de dimensión 3 y peso mínimo 4.

Una construcción de Λ_{24}, el Leech lattice

Consideramos el cuerpo de 4 elementos $\mathbf{F}_4 = \{0, 1, \omega, \overline{\omega}\}$, tiene característica 2, y $1 + \omega + \overline{\omega} = 0$.

El **Hexacode** $\mathcal{C}_6$ es un código lineal de longitud 6 sobre $\mathbf{F}_4$:

para cada función cuadrática $\phi(x) = ax^2 + bx + c$ sobre $\mathbf{F}_4$ consideramos la 6-upla en $\mathbf{F}_4^6$

$$\big(\, a\,,\; b\,,\; c,\; d = \phi(1)\,,\; e = \phi(\omega)\,,\; f = \phi(\overline{\omega})\big),$$

definimos $\mathcal{C}_6$ como el conjunto de palabras de esta forma.

Notemos que es un código lineal en $\mathbf{F}_4$, de dimensión 3 y peso mínimo 4.

El Hexacode

Ordenando la 6-upla $ab\,cd\,ef$ en $\mathcal{C}_6$ en tres pares $\begin{array}{|cc|} \hline a & b \\ c & d \\ e & f \\ \hline \end{array}$ se observa que $\mathcal{C}_6$ tiene las siguientes reglas:

- Regla 1. $\quad a + b = c + d = e + f = s.$
- Regla 2. $\begin{array}{|cc|}\hline \bullet & \\ \bullet & \\ \bullet & \\ \hline\end{array} = \begin{array}{|cc|}\hline \bullet & \\ & \bullet \\ & \bullet \\ \hline\end{array} = \begin{array}{|cc|}\hline & \bullet \\ \bullet & \\ & \bullet \\ \hline\end{array} = \begin{array}{|cc|}\hline & \bullet \\ & \bullet \\ \bullet & \\ \hline\end{array} = \omega s.$
- Regla 3. $\begin{array}{|cc|}\hline & \bullet \\ & \bullet \\ & \bullet \\ \hline\end{array} = \begin{array}{|cc|}\hline & \bullet \\ \bullet & \\ \bullet & \\ \hline\end{array} = \begin{array}{|cc|}\hline \bullet & \\ & \bullet \\ \bullet & \\ \hline\end{array} = \begin{array}{|cc|}\hline \bullet & \\ \bullet & \\ & \bullet \\ \hline\end{array} = \overline{\omega} s.$

El Hexacode

Ordenando la 6-upla $ab\,cd\,ef$ en $\mathcal{C}_6$ en tres pares $\begin{array}{|cc|}\hline a & b \\ c & d \\ e & f \\ \hline\end{array}$ se observa que $\mathcal{C}_6$ tiene las siguientes reglas:

- Regla 1. $\quad a + b = c + d = e + f = s.$
- Regla 2. $\begin{array}{|cc|}\hline \bullet & \\ \bullet & \\ \bullet & \\ \hline\end{array} = \begin{array}{|cc|}\hline \bullet & \\ & \bullet \\ & \bullet \\ \hline\end{array} = \begin{array}{|cc|}\hline & \bullet \\ \bullet & \\ & \bullet \\ \hline\end{array} = \begin{array}{|cc|}\hline & \bullet \\ & \bullet \\ \bullet & \\ \hline\end{array} = \omega s.$
- Regla 3. $\begin{array}{|cc|}\hline & \bullet \\ & \bullet \\ & \bullet \\ \hline\end{array} = \begin{array}{|cc|}\hline & \bullet \\ \bullet & \\ \bullet & \\ \hline\end{array} = \begin{array}{|cc|}\hline \bullet & \\ & \bullet \\ \bullet & \\ \hline\end{array} = \begin{array}{|cc|}\hline \bullet & \\ \bullet & \\ & \bullet \\ \hline\end{array} = \overline{\omega} s.$

El Hexacode

Ordenando la 6-upla $ab\,cd\,ef$ en $\mathcal{C}_6$ en tres pares $\boxed{\begin{array}{cc} a & b \\ c & d \\ e & f \end{array}}$ se observa que $\mathcal{C}_6$ tiene las siguientes reglas:

- Regla 1. $\quad a + b = c + d = e + f = s.$
- Regla 2. $\boxed{\begin{array}{cc} \bullet & \\ \bullet & \\ \bullet & \end{array}} = \boxed{\begin{array}{cc} \bullet & \\ & \bullet \\ & \bullet \end{array}} = \boxed{\begin{array}{cc} & \bullet \\ \bullet & \\ & \bullet \end{array}} = \boxed{\begin{array}{cc} & \bullet \\ & \bullet \\ \bullet & \end{array}} = \omega s.$
- Regla 3. $\boxed{\begin{array}{cc} & \bullet \\ & \bullet \\ & \bullet \end{array}} = \boxed{\begin{array}{cc} & \bullet \\ \bullet & \\ \bullet & \end{array}} = \boxed{\begin{array}{cc} \bullet & \\ & \bullet \\ \bullet & \end{array}} = \boxed{\begin{array}{cc} \bullet & \\ \bullet & \\ & \bullet \end{array}} = \overline{\omega} s.$

El Hexacode

En $\mathcal{C}_6$ se cumplen las siguientes reglas de simetría:

se puede

- 1. multiplicar una palabra de $\mathcal{C}_6$ por cualquier potencia de ω,
- 2. intercambiar los dígitos en dos parejas de una palabra,
- 3. permutar las tres parejas de dígitos en cualquier palabra.

y el resultado vuelve a estar en $\mathcal{C}_6$

Importante: tres coordenadas cualesquiera determinan una palabra en $\mathcal{C}_6$

y cinco coordenadas cualesquiera de una palabra de $\mathcal{C}_6$, con a lo sumo una coordenada incorrecta, determinan la palabra.

El Hexacode

En $\mathcal{C}_6$ se cumplen las siguientes reglas de simetría:
se puede

- 1. multiplicar una palabra de $\mathcal{C}_6$ por cualquier potencia de ω,
- 2. intercambiar los dígitos en dos parejas de una palabra,
- 3. permutar las tres parejas de dígitos en cualquier palabra.

y el resultado vuelve a estar en $\mathcal{C}_6$

Importante: tres coordenadas cualesquiera determinan una palabra en $\mathcal{C}_6$

y cinco coordenadas cualesquiera de una palabra de $\mathcal{C}_6$, con a lo sumo una coordenada incorrecta, determinan la palabra.

El Hexacode

En $\mathcal{C}_6$ se cumplen las siguientes reglas de simetría:
se puede

- 1. multiplicar una palabra de $\mathcal{C}_6$ por cualquier potencia de ω,
- 2. intercambiar los dígitos en dos parejas de una palabra,
- 3. permutar las tres parejas de dígitos en cualquier palabra.

y el resultado vuelve a estar en $\mathcal{C}_6$

Importante: tres coordenadas cualesquiera determinan una palabra en $\mathcal{C}_6$

y cinco coordenadas cualesquiera de una palabra de $\mathcal{C}_6$, con a lo sumo una coordenada incorrecta, determinan la palabra.

El Hexacode

En $\mathcal{C}_6$ se cumplen las siguientes reglas de simetría:
se puede

- 1. multiplicar una palabra de $\mathcal{C}_6$ por cualquier potencia de ω,
- 2. intercambiar los dígitos en dos parejas de una palabra,
- 3. permutar las tres parejas de dígitos en cualquier palabra.

y el resultado vuelve a estar en $\mathcal{C}_6$

Importante: tres coordenadas cualesquiera determinan una palabra en $\mathcal{C}_6$

y cinco coordenadas cualesquiera de una palabra de $\mathcal{C}_6$, con a lo sumo una coordenada incorrecta, determinan la palabra.

El Hexacode

En $\mathcal{C}_6$ se cumplen las siguientes reglas de simetría:
se puede

- 1. multiplicar una palabra de $\mathcal{C}_6$ por cualquier potencia de ω,
- 2. intercambiar los dígitos en dos parejas de una palabra,
- 3. permutar las tres parejas de dígitos en cualquier palabra.

y el resultado vuelve a estar en $\mathcal{C}_6$

Importante: tres coordenadas cualesquiera determinan una palabra en $\mathcal{C}_6$

y cinco coordenadas cualesquiera de una palabra de $\mathcal{C}_6$, con a lo sumo una coordenada incorrecta, determinan la palabra.

El Hexacode

En $\mathcal{C}_6$ se cumplen las siguientes reglas de simetría:
se puede

- 1. multiplicar una palabra de $\mathcal{C}_6$ por cualquier potencia de ω,
- 2. intercambiar los dígitos en dos parejas de una palabra,
- 3. permutar las tres parejas de dígitos en cualquier palabra.

y el resultado vuelve a estar en $\mathcal{C}_6$

Importante: tres coordenadas cualesquiera determinan una palabra en $\mathcal{C}_6$

y cinco coordenadas cualesquiera de una palabra de $\mathcal{C}_6$, con a lo sumo una coordenada incorrecta, determinan la palabra.

El Hexacode

En $\mathcal{C}_6$ se cumplen las siguientes reglas de simetría:
se puede

- 1. multiplicar una palabra de $\mathcal{C}_6$ por cualquier potencia de ω,
- 2. intercambiar los dígitos en dos parejas de una palabra,
- 3. permutar las tres parejas de dígitos en cualquier palabra.

y el resultado vuelve a estar en $\mathcal{C}_6$

Importante: tres coordenadas cualesquiera determinan una palabra en $\mathcal{C}_6$

y cinco coordenadas cualesquiera de una palabra de $\mathcal{C}_6$, con a lo sumo una coordenada incorrecta, determinan la palabra.

Cada elemento de $\mathbf{F}_4$ se puede representar de 4 formas distintas como combinación lineal (con coeficientes 0 ó 1) de los elementos de $\mathbf{F}_4$:

	0				1				ω				$\overline{\omega}$			
0	0	1	1	0	1	0	0	1	1	0	0	1	1	0	0	1
1	0	1	0	1	1	0	1	0	0	1	0	1	0	1	0	1
ω	0	1	0	1	0	1	0	1	1	0	1	0	0	1	0	1
$\overline{\omega}$	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0
	par		impar		par		impar		par		impar		par		impar	

Ahora con palabras de $\mathcal{C}_6$ armaremos matrices 4×6 de ceros y unos.

Cada elemento de $\mathbf{F}_4$ se puede representar de 4 formas distintas como combinación lineal (con coeficientes 0 ó 1) de los elementos de $\mathbf{F}_4$:

	0				1				ω				$\overline{\omega}$			
0	0	1	1	0	1	0	0	1	1	0	0	1	1	0	0	1
1	0	1	0	1	1	0	1	0	0	1	0	1	0	1	0	1
ω	0	1	0	1	0	1	0	1	1	0	1	0	0	1	0	1
$\overline{\omega}$	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0
	par		impar		par		impar		par		impar		par		impar	

Ahora con palabras de $\mathcal{C}_6$ armaremos matrices 4×6 de ceros y unos.

Cada elemento de $\mathbf{F}_4$ se puede representar de 4 formas distintas como combinación lineal (con coeficientes 0 ó 1) de los elementos de $\mathbf{F}_4$:

	0				1				ω				$\overline{\omega}$			
0	0	1	1	0	1	0	0	1	1	0	0	1	1	0	0	1
1	0	1	0	1	1	0	1	0	0	1	0	1	0	1	0	1
ω	0	1	0	1	0	1	0	1	1	0	1	0	0	1	0	1
$\overline{\omega}$	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0
	par		impar		par		impar		par		impar		par		impar	

Ahora con palabras de $\mathcal{C}_6$ armaremos matrices 4×6 de ceros y unos.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos
– una palabra de $\mathcal{C}_6$;
– una paridad (par o impar);
– una representación con la paridad elegida para cada letra de la palabra;
– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es $01\ \omega\overline{\omega}\ 01$ y elegimos la paridad 'par',

una matriz posible es

	0	1	ω	$\overline{\omega}$	0	1
0	0	1	1	1	0	1
1	0	1	0	0	0	1
ω	0	0	1	0	0	0
$\overline{\omega}$	0	0	0	1	0	0

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos

– una palabra de $\mathcal{C}_6$;

– una paridad (par o impar);

– una representación con la paridad elegida para cada letra de la palabra;

– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es 01 $\omega\overline{\omega}$ 01 y elegimos la paridad 'par',

una matriz posible es

	0	1	ω	$\overline{\omega}$	0	1
0	0	1	1	1	0	1
1	0	1	0	0	0	1
ω	0	0	1	0	0	0
$\overline{\omega}$	0	0	0	1	0	0

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos
– una palabra de $\mathcal{C}_6$;
– una paridad (par o impar);
– una representación con la paridad elegida para cada letra de la palabra;
– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es $01\ \omega\overline{\omega}\ 01$ y elegimos la paridad 'par', una matriz posible es

$$\begin{array}{c|cccccc|} & 0 & 1 & \omega & \overline{\omega} & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \omega & 0 & 0 & 1 & 0 & 0 & 0 \\ \overline{\omega} & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline \end{array}$$

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos
– una palabra de $\mathcal{C}_6$;
– una paridad (par o impar);
– una representación con la paridad elegida para cada letra de la palabra;
– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es 01 $\omega\overline{\omega}$ 01 y elegimos la paridad 'par',

una matriz posible es

$$\begin{array}{c|cccccc} & 0 & 1 & \omega & \overline{\omega} & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \omega & 0 & 0 & 1 & 0 & 0 & 0 \\ \overline{\omega} & 0 & 0 & 0 & 1 & 0 & 0 \end{array}$$

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos
– una palabra de $\mathcal{C}_6$;
– una paridad (par o impar);
– una representación con la paridad elegida para cada letra de la palabra;
– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es $01\ \omega\overline{\omega}\ 01$ y elegimos la paridad 'par',

una matriz posible es

	0	1	ω	$\overline{\omega}$	0	1
0	0	1	1	1	0	1
1	0	1	0	0	0	1
ω	0	0	1	0	0	0
$\overline{\omega}$	0	0	0	1	0	0

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos
– una palabra de $\mathcal{C}_6$;
– una paridad (par o impar);
– una representación con la paridad elegida para cada letra de la palabra;
– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es $01\ \omega\overline{\omega}\ 01$ y elegimos la paridad 'par',

una matriz posible es

$$\begin{array}{c|cccccc|} & 0 & 1 & \omega & \overline{\omega} & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \omega & 0 & 0 & 1 & 0 & 0 & 0 \\ \overline{\omega} & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline \end{array}$$

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos
– una palabra de $\mathcal{C}_6$;
– una paridad (par o impar);
– una representación con la paridad elegida para cada letra de la palabra;
– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es 01 $\omega\overline{\omega}$ 01 y elegimos la paridad 'par',

una matriz posible es

$$\begin{array}{c|cccccc} & 0 & 1 & \omega & \overline{\omega} & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \omega & 0 & 0 & 1 & 0 & 0 & 0 \\ \overline{\omega} & 0 & 0 & 0 & 1 & 0 & 0 \end{array}$$

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos
– una palabra de $\mathcal{C}_6$;
– una paridad (par o impar);
– una representación con la paridad elegida para cada letra de la palabra;
– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es $\;01\;\omega\overline{\omega}\;01$ y elegimos la paridad 'par',

una matriz posible es

	0	1	ω	$\overline{\omega}$	0	1
0	0	1	1	1	0	1
1	0	1	0	0	0	1
ω	0	0	1	0	0	0
$\overline{\omega}$	0	0	0	1	0	0

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

El código de Golay extendido $\mathcal{C}_{24}$

Para construir $\mathcal{C}_{24}$ elegimos
– una palabra de $\mathcal{C}_6$;
– una paridad (par o impar);
– una representación con la paridad elegida para cada letra de la palabra;
– la primera fila también debe tener la paridad elegida

Ejemplo: si la palabra es $01\ \omega\overline{\omega}\ 01$ y elegimos la paridad 'par', una matriz posible es

$$\begin{array}{c|cccccc|} & 0 & 1 & \omega & \overline{\omega} & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \omega & 0 & 0 & 1 & 0 & 0 & 0 \\ \overline{\omega} & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline \end{array}$$

Cada matriz 4×6 obtenida será un elemento de $\mathcal{C}_{24}$.

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego
$A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego
$A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego
$A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego
$A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego
$A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego
$A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego
$A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

- su cardinal es 2^{12};
- es lineal;
- $(1^{24}) \in \mathcal{C}_{24}$;
- el peso mínimo es 8;
- de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
- Es par, más aún es doblemente par;
- $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
- las palabras de peso 8 corresponden a *octads*.
- veremos que hay 759 de éstas;
- así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego $A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego $A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

- su cardinal es 2^{12};
- es lineal;
- $(1^{24}) \in \mathcal{C}_{24}$;
- el peso mínimo es 8;
- de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
- Es par, más aún es doblemente par;
- $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
- las palabras de peso 8 corresponden a *octads*.
- veremos que hay 759 de éstas;
- así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego $A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego $A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

De este modo, en $\mathcal{C}_{24}$ se verifica lo siguiente:

– su cardinal es 2^{12};
– es lineal;
– $(1^{24}) \in \mathcal{C}_{24}$;
– el peso mínimo es 8;
– de modo que $\mathcal{C}_{24}$ es un código lineal binario de tipo $[24, 12, 8]$.
– Es par, más aún es doblemente par;
– $A_i = 0$ para $i \neq 0, 8, 12, 16, 24$;
– las palabras de peso 8 corresponden a *octads*.
– veremos que hay 759 de éstas;
– así, $A_0 = A_{24} = 1$, $A_8 = A_{16} = 759$, luego
$A_{12} = |\mathcal{C}_{24}| - 2\,A_0 - 2\,A_8 = 2576$;

Octads

– **Afirmación:** las octads forman un sistema de Steiner $S(5, 8, 24)$.

Es un lindo ejercicio encontar la octad correspondiente a cinco unos elegidos al azar.

Por lo tanto, la cantidad de octads es exactamente $\binom{24}{5}/\binom{8}{5} = 23 \cdot 4 \cdot 3 = 759$.

Octads

– **Afirmación:** las octads forman un sistema de Steiner $S(5,8,24)$.

Es un lindo ejercicio encontar la octad correspondiente a cinco unos elegidos al azar.

Por lo tanto, la cantidad de octads es exactamente $\binom{24}{5}/\binom{8}{5} = 23 \cdot 4 \cdot 3 = 759$.

Ejercicios:

1. Completar a palabras de $\mathcal{C}_6$:
$$(1, 1, \_, 0, \_, \_) \text{ y } (\_, \omega, \_, 1, \omega, \_)$$

2. Hallar dos palabras de $\mathcal{C}_6$ que tengan respectivamente a lo sumo una diferencia con las dos siguientes:
$$(\overline{\omega}, 0, \_, \omega, 1, 1) \quad \text{y} \quad (\omega, 0, \omega, 0, 0, \_).$$

3. Hallar las octads correspondientes a:

			*		
		*	*	*	
*					

y

*	*	*			
	*				
*					

4. Está

0	1	1	1	0	0
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	1	0	0

en $\mathcal{C}_{24}$?

Ejercicios:

1. Completar a palabras de $\mathcal{C}_6$:

$$(1, 1, \_, 0, \_, \_) \text{ y } (\_, \omega, \_, 1, \omega, \_)$$

2. Hallar dos palabras de $\mathcal{C}_6$ que tengan respectivamente a lo sumo una diferencia con las dos siguientes:

$$(\overline{\omega}, 0, \_, \omega, 1, 1) \quad \text{y} \quad (\omega, 0, \omega, 0, 0, \_).$$

3. Hallar las octads correspondientes a:

			*		
		*	*	*	
*					

y

*	*	*			
	*				
*					

4. Está

0	1	1	1	0	0
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	1	0	0

en $\mathcal{C}_{24}$?

Ejercicios:

1. Completar a palabras de $\mathcal{C}_6$:

$$(1, 1, \_, 0, \_, \_) \text{ y } (\_, \omega, \_, 1, \omega, \_)$$

2. Hallar dos palabras de $\mathcal{C}_6$ que tengan respectivamente a lo sumo una diferencia con las dos siguientes:

$$(\overline{\omega}, 0, \_, \omega, 1, 1) \quad \text{y} \quad (\omega, 0, \omega, 0, 0, \_).$$

3. Hallar las octads correspondientes a:

			*		
		*	*	*	
*					

y

*	*	*			
	*				
*					

4. Está

0	1	1	1	0	0
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	1	0	0

en $\mathcal{C}_{24}$?

Ejercicios:

1. Completar a palabras de $\mathcal{C}_6$:

$$(1, 1, \_, 0, \_, \_) \text{ y } (\_, \omega, \_, 1, \omega, \_)$$

2. Hallar dos palabras de $\mathcal{C}_6$ que tengan respectivamente a lo sumo una diferencia con las dos siguientes:

$$(\overline{\omega}, 0, \_, \omega, 1, 1) \quad \text{y} \quad (\omega, 0, \omega, 0, 0, \_).$$

3. Hallar las octads correspondientes a:

			*		
		*	*	*	
*					

y

*	*	*			
	*				
*					

4. Está

0	1	1	1	0	0
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	1	0	0

en $\mathcal{C}_{24}$?

Ejercicios:

1. Completar a palabras de $\mathcal{C}_6$:
$$(1, 1, \_, 0, \_, \_) \text{ y } (\_, \omega, \_, 1, \omega, \_)$$
2. Hallar dos palabras de $\mathcal{C}_6$ que tengan respectivamente a lo sumo una diferencia con las dos siguientes:
$$(\overline{\omega}, 0, \_, \omega, 1, 1) \quad \text{y} \quad (\omega, 0, \omega, 0, 0, \_).$$
3. Hallar las octads correspondientes a:

			*		
		*	*	*	
*					

y

*	*	*			
	*				
*					

4. Está

0	1	1	1	0	0
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	1	0	0

en $\mathcal{C}_{24}$?

Ejercicios:

1. Completar a palabras de $\mathcal{C}_6$:

$$(1, 1, \_, 0, \_, \_) \text{ y } (\_, \omega, \_, 1, \omega, \_)$$

2. Hallar dos palabras de $\mathcal{C}_6$ que tengan respectivamente a lo sumo una diferencia con las dos siguientes:

$$(\overline{\omega}, 0, \_, \omega, 1, 1) \quad \text{y} \quad (\omega, 0, \omega, 0, 0, \_).$$

3. Hallar las octads correspondientes a:

			$*$		
		$*$	$*$	$*$	
$*$					

y

$*$	$*$	$*$			
	$*$				
$*$					

4. Está

0	1	1	1	0	0
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	1	0	0

en $\mathcal{C}_{24}$?

de Golay a Leech

Sea $\quad L := \varphi^{-1}(\mathcal{C}_{24})$;

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $\quad 2 \cdot 24 = 48$;

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $\quad 2^8\, A_8 = 2^8 \cdot 759 = 194304$;

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\quad \binom{24}{2} \cdot 2^2 = 1104$;

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

de Golay a Leech

Sea $L := \varphi^{-1}(\mathcal{C}_{24})$;

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $2 \cdot 24 = 48$;

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $2^8\, A_8 = 2^8 \cdot 759 = 194304$;

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\binom{24}{2} \cdot 2^2 = 1104$;

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

de Golay a Leech

Sea $L := \varphi^{-1}(\mathcal{C}_{24})$;

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $2 \cdot 24 = 48$;

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $2^8 A_8 = 2^8 \cdot 759 = 194304$;

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\binom{24}{2} \cdot 2^2 = 1104$;

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

de Golay a Leech

Sea $L := \varphi^{-1}(\mathcal{C}_{24})$;

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $2 \cdot 24 = 48$;

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $2^8\, A_8 = 2^8 \cdot 759 = 194304$;

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\binom{24}{2} \cdot 2^2 = 1104$;

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

de Golay a Leech

Sea $L := \varphi^{-1}(\mathcal{C}_{24})$;

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $2 \cdot 24 = 48$;

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $2^8\, A_8 = 2^8 \cdot 759 = 194304$;

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\binom{24}{2} \cdot 2^2 = 1104$;

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

de Golay a Leech

Sea $L := \varphi^{-1}(\mathcal{C}_{24})$;

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $2 \cdot 24 = 48$;

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $2^8\, A_8 = 2^8 \cdot 759 = 194304$;

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\binom{24}{2} \cdot 2^2 = 1104$;

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

de Golay a Leech

Sea $\quad L := \varphi^{-1}(\mathcal{C}_{24});$

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $\quad 2 \cdot 24 = 48;$

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $\quad 2^8\, A_8 = 2^8 \cdot 759 = 194304;$

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\quad \binom{24}{2} \cdot 2^2 = 1104;$

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

de Golay a Leech

Sea $L := \varphi^{-1}(\mathcal{C}_{24})$;

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $2 \cdot 24 = 48$;

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $2^8\, A_8 = 2^8 \cdot 759 = 194304$;

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\binom{24}{2} \cdot 2^2 = 1104$;

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

de Golay a Leech

Sea $L := \varphi^{-1}(\mathcal{C}_{24})$;

L tiene vectores de tipo $(\pm 2, 0^{23})$, de norma 4, hay: $2 \cdot 24 = 48$;

de tipo $(\pm 1^8, 0^{16})$, de norma 8, hay: $2^8\, A_8 = 2^8 \cdot 759 = 194304$;

y de tipo $(\pm 2^2, 0^{22})$, de norma 8, hay: $\binom{24}{2} \cdot 2^2 = 1104$;

L tiene pocos vectores mínimos...

pero muchísimos de la siguiente norma!

En este caso, hay un truco que funciona: pasar a un *lattice vecino*.

Primero una reducción

Sea

$$\begin{array}{rccc} \alpha : & L & \longrightarrow & \mathbf{Z}_2 \\ & (x_1, \ldots, x_n) & \longmapsto & \frac{1}{2}\sum_i x_i \mod 2 \end{array}$$

Sea

$$A := \ker(\alpha) = \alpha^{-1}(0).$$

A es un sublattice de L de índice 2.

Notemos que al quedarnos con A, "eliminamos" los 48 vectores cortos que tenía L.
Aunque también hemos perdido casi la mitad de los segundos vectores más cortos.

Lo notable es que se podrá duplicar la cantidad de vectores mínimos.

Primero una reducción

Sea

$$\begin{array}{rccl} \alpha : & L & \longrightarrow & \mathbf{Z}_2 \\ & (x_1, \ldots, x_n) & \longmapsto & \frac{1}{2}\sum_i x_i \mod 2 \end{array}$$

Sea

$$A := \ker(\alpha) = \alpha^{-1}(0).$$

A es un sublattice de L de índice 2.

Notemos que al quedarnos con A, "eliminamos" los 48 vectores cortos que tenía L.
Aunque también hemos perdido casi la mitad de los segundos vectores más cortos.

Lo notable es que se podrá duplicar la cantidad de vectores mínimos.

Primero una reducción

Sea

$$\begin{array}{rccl} \alpha : & L & \longrightarrow & \mathbf{Z}_2 \\ & (x_1, \ldots, x_n) & \longmapsto & \frac{1}{2}\sum_i x_i \mod 2 \end{array}$$

Sea

$$A := \ker(\alpha) = \alpha^{-1}(0).$$

A es un sublattice de L de índice 2.

Notemos que al quedarnos con A, “eliminamos” los 48 vectores cortos que tenía L.
Aunque también hemos perdido casi la mitad de los segundos vectores más cortos.

Lo notable es que se podrá duplicar la cantidad de vectores mínimos.

Primero una reducción

Sea

$$\begin{array}{rccl} \alpha : & L & \longrightarrow & \mathbf{Z}_2 \\ & (x_1, \ldots, x_n) & \longmapsto & \frac{1}{2}\sum_i x_i \mod 2 \end{array}$$

Sea

$$A := \ker(\alpha) = \alpha^{-1}(0).$$

A es un sublattice de L de índice 2.

Notemos que al quedarnos con A, "eliminamos" los 48 vectores cortos que tenía L.

Aunque también hemos perdido casi la mitad de los segundos vectores más cortos.

Lo notable es que se podrá duplicar la cantidad de vectores mínimos.

Primero una reducción

Sea

$$\begin{array}{rccl} \alpha : & L & \longrightarrow & \mathbf{Z}_2 \\ & (x_1, \ldots, x_n) & \longmapsto & \frac{1}{2}\sum_i x_i \mod 2 \end{array}$$

Sea

$$A := \ker(\alpha) = \alpha^{-1}(0).$$

A es un sublattice de L de índice 2.

Notemos que al quedarnos con A, "eliminamos" los 48 vectores cortos que tenía L.
Aunque también hemos perdido casi la mitad de los segundos vectores más cortos.

Lo notable es que se podrá duplicar la cantidad de vectores mínimos.

Primero una reducción

Sea

$$\begin{array}{rccl} \alpha : & L & \longrightarrow & \mathbf{Z}_2 \\ & (x_1, \ldots, x_n) & \longmapsto & \frac{1}{2}\sum_i x_i \mod 2 \end{array}$$

Sea

$$A := \ker(\alpha) = \alpha^{-1}(0).$$

A es un sublattice de L de índice 2.

Notemos que al quedarnos con A, "eliminamos" los 48 vectores cortos que tenía L.
Aunque también hemos perdido casi la mitad de los segundos vectores más cortos.

Lo notable es que se podrá duplicar la cantidad de vectores mínimos.

Lattice vecino

Consideremos el vector $(-3, 1^{23})$.

Tenemos que $(-3, 1^{23}) \in A$ pues:

$\varphi((-3, 1^{23})) = (1^{24}) \in \mathcal{C}_{24}$,
y $\alpha((-3, 1^{23})) = \frac{1}{2}(-3 + 23) \equiv 0 \mod 2$.

Y además $\frac{1}{2}(-3, 1^{23}) \notin A$.

Por lo tanto, podemos agregar $\frac{1}{2}(-3, 1^{23})$ a A y así agrandar el lattice A al doble de puntos.

Lattice vecino

Consideremos el vector $(-3, 1^{23})$.

Tenemos que $(-3, 1^{23}) \in A$ pues:

$\varphi((-3, 1^{23})) = (1^{24}) \in \mathcal{C}_{24}$,
y $\alpha((-3, 1^{23})) = \frac{1}{2}(-3 + 23) \equiv 0 \mod 2$.

Y además $\frac{1}{2}(-3, 1^{23}) \notin A$.

Por lo tanto, podemos agregar $\frac{1}{2}(-3, 1^{23})$ a A y así agrandar el lattice A al doble de puntos.

Lattice vecino

Consideremos el vector $(-3, 1^{23})$.

Tenemos que $(-3, 1^{23}) \in A$ pues:

$\varphi((-3, 1^{23})) = (1^{24}) \in \mathcal{C}_{24}$,
y $\alpha((-3, 1^{23})) = \frac{1}{2}(-3 + 23) \equiv 0 \mod 2$.

Y además $\frac{1}{2}(-3, 1^{23}) \notin A$.

Por lo tanto, podemos agregar $\frac{1}{2}(-3, 1^{23})$ a A y así agrandar el lattice A al doble de puntos.

Lattice vecino

Consideremos el vector $(-3, 1^{23})$.

Tenemos que $(-3, 1^{23}) \in A$ pues:

$\varphi((-3, 1^{23})) = (1^{24}) \in \mathcal{C}_{24}$,
y $\alpha((-3, 1^{23})) = \frac{1}{2}(-3 + 23) \equiv 0 \mod 2$.

Y además $\frac{1}{2}(-3, 1^{23}) \notin A$.

Por lo tanto, podemos agregar $\frac{1}{2}(-3, 1^{23})$ a A y así agrandar el lattice A al doble de puntos.

Lattice vecino

Consideremos el vector $(-3, 1^{23})$.

Tenemos que $(-3, 1^{23}) \in A$ pues:

$\varphi((-3, 1^{23})) = (1^{24}) \in \mathcal{C}_{24}$,
y $\alpha((-3, 1^{23})) = \frac{1}{2}(-3 + 23) \equiv 0 \mod 2$.

Y además $\frac{1}{2}(-3, 1^{23}) \notin A$.

Por lo tanto, podemos agregar $\frac{1}{2}(-3, 1^{23})$ a A y así agrandar el lattice A al doble de puntos.

Lattice vecino

Consideremos el vector $(-3, 1^{23})$.

Tenemos que $(-3, 1^{23}) \in A$ pues:

$\varphi((-3, 1^{23})) = (1^{24}) \in \mathcal{C}_{24}$,
y $\alpha((-3, 1^{23})) = \frac{1}{2}(-3 + 23) \equiv 0 \mod 2$.

Y además $\frac{1}{2}(-3, 1^{23}) \notin A$.

Por lo tanto, podemos agregar $\frac{1}{2}(-3, 1^{23})$ a A y así agrandar el lattice A al doble de puntos.

El Leech Lattice Λ_{24}

Definimos

$$\Lambda_{24} := \frac{1}{\sqrt{2}} \langle A, \tfrac{1}{2}(-3, 1^{23}) \rangle_{\mathbf{Z}}$$

contemos los vectores mínimos: 196560

Por lo tanto, hemos verificado el siguiente

Teorema. Λ_{24} es un lattice par unimodular sin vectores de norma 2, y tiene 196560 vectores mínimos (de norma 4).

Hay varios teoremas donde se prueba la unicidad del Leech lattice con respecto a alguna propiedad.

El Leech Lattice Λ_{24}

Definimos

$$\Lambda_{24} := \frac{1}{\sqrt{2}} \langle A, \tfrac{1}{2}(-3, 1^{23}) \rangle_{\mathbf{Z}}$$

contemos los vectores mínimos: 196560

Por lo tanto, hemos verificado el siguiente

Teorema. Λ_{24} es un lattice par unimodular sin vectores de norma 2, y tiene 196560 vectores mínimos (de norma 4).

Hay varios teoremas donde se prueba la unicidad del Leech lattice con respecto a alguna propiedad.

El Leech Lattice Λ_{24}

Definimos

$$\Lambda_{24} := \frac{1}{\sqrt{2}} \langle A, \tfrac{1}{2}(-3, 1^{23}) \rangle_{\mathbf{Z}}$$

contemos los vectores mínimos: 196560

Por lo tanto, hemos verificado el siguiente

Teorema. Λ_{24} es un lattice par unimodular sin vectores de norma 2, y tiene 196560 vectores mínimos (de norma 4).

Hay varios teoremas donde se prueba la unicidad del Leech lattice con respecto a alguna propiedad.

Lattices isospectrales en norma uno

- Para $n \geq 5$, construimos pares de variedades Riemannianas en dimensión n, p-isospectrales para todo p que no son *fuertemente isospectrales*

- infinitos pares de espacios lentes n-dimensionales.

Los espacios lentes son *spherical space forms* con grupo fundamental cíclico. Para $q \in \mathbf{N}$ y $s_1, \ldots, s_m \in \mathbf{Z}$ coprimos con q, sea

$$L(q; s_1, \ldots, s_m) = \langle\gamma\rangle \backslash S^{2m-1}, \qquad \text{donde}$$

$$\gamma = \operatorname{diag}\left(\begin{bmatrix} \cos(2\pi s_1/q) & \sin(2\pi s_1/q) \\ -\sin(2\pi s_1/q) & \cos(2\pi s_1/q) \end{bmatrix}, \ldots, \begin{bmatrix} \cos(2\pi s_m/q) & \sin(2\pi s_m/q) \\ -\sin(2\pi s_m/q) & \cos(2\pi s_m/q) \end{bmatrix} \right).$$

Al espacio lente $L(q; s_1, \ldots, s_m)$ le asociamos el lattice de congruencia $\mathcal{L}(q, s) = \mathcal{L}(q; s_1, \ldots, s_m)$ de los $(a_1, \ldots, a_m) \in \mathbf{Z}^m$ tales que

$$a_1 s_1 + \cdots + a_m s_m \equiv 0 \pmod{q}$$

Lattices isospectrales en norma uno

- Para $n \geq 5$, construimos pares de variedades Riemannianas en dimensión n, p-isospectrales para todo p que no son *fuertemente isospectrales*

- infinitos pares de espacios lentes n-dimensionales.

Los espacios lentes son *spherical space forms* con grupo fundamental cíclico. Para $q \in \mathbf{N}$ y $s_1, \dots, s_m \in \mathbf{Z}$ coprimos con q, sea

$$L(q; s_1, \dots, s_m) = \langle\gamma\rangle \backslash S^{2m-1}, \qquad \text{donde}$$

$$\gamma = \operatorname{diag}\left(\begin{bmatrix} \cos(2\pi s_1/q) & \sin(2\pi s_1/q) \\ -\sin(2\pi s_1/q) & \cos(2\pi s_1/q) \end{bmatrix}, \dots, \begin{bmatrix} \cos(2\pi s_m/q) & \sin(2\pi s_m/q) \\ -\sin(2\pi s_m/q) & \cos(2\pi s_m/q) \end{bmatrix} \right).$$

Al espacio lente $L(q; s_1, \dots, s_m)$ le asociamos el lattice de congruencia $\mathcal{L}(q, s) = \mathcal{L}(q; s_1, \dots, s_m)$ de los $(a_1, \dots, a_m) \in \mathbf{Z}^m$ tales que

$$a_1 s_1 + \cdots + a_m s_m \equiv 0 \pmod{q}$$

Lattices isospectrales en norma uno

- Para $n \geq 5$, construimos pares de variedades Riemannianas en dimensión n, p-isospectrales para todo p que no son *fuertemente isospectrales*

- infinitos pares de espacios lentes n-dimensionales.

Los espacios lentes son *spherical space forms* con grupo fundamental cíclico. Para $q \in \mathbf{N}$ y $s_1, \ldots, s_m \in \mathbf{Z}$ coprimos con q, sea

$$L(q; s_1, \ldots, s_m) = \langle\gamma\rangle \backslash S^{2m-1}, \qquad \text{donde}$$

$$\gamma = \operatorname{diag}\left(\begin{bmatrix} \cos(2\pi s_1/q) & \sin(2\pi s_1/q) \\ -\sin(2\pi s_1/q) & \cos(2\pi s_1/q) \end{bmatrix}, \ldots, \begin{bmatrix} \cos(2\pi s_m/q) & \sin(2\pi s_m/q) \\ -\sin(2\pi s_m/q) & \cos(2\pi s_m/q) \end{bmatrix} \right).$$

Al espacio lente $L(q; s_1, \ldots, s_m)$ le asociamos el lattice de congruencia $\mathcal{L}(q,s) = \mathcal{L}(q; s_1, \ldots, s_m)$ de los $(a_1, \ldots, a_m) \in \mathbf{Z}^m$ tales que

$$a_1 s_1 + \cdots + a_m s_m \equiv 0 \pmod{q}$$

Lattices isospectrales en norma uno

- Para $n \geq 5$, construimos pares de variedades Riemannianas en dimensión n, p-isospectrales para todo p que no son *fuertemente isospectrales*
- infinitos pares de espacios lentes n-dimensionales.

Los espacios lentes son *spherical space forms* con grupo fundamental cíclico. Para $q \in \mathbf{N}$ y $s_1, \ldots, s_m \in \mathbf{Z}$ coprimos con q, sea

$$L(q; s_1, \ldots, s_m) = \langle\gamma\rangle \backslash S^{2m-1}, \qquad \text{donde}$$

$$\gamma = \operatorname{diag}\left(\begin{bmatrix} \cos(2\pi s_1/q) & \sin(2\pi s_1/q) \\ -\sin(2\pi s_1/q) & \cos(2\pi s_1/q) \end{bmatrix}, \ldots, \begin{bmatrix} \cos(2\pi s_m/q) & \sin(2\pi s_m/q) \\ -\sin(2\pi s_m/q) & \cos(2\pi s_m/q) \end{bmatrix} \right).$$

Al espacio lente $L(q; s_1, \ldots, s_m)$ le asociamos el lattice de congruencia $\mathcal{L}(q, s) = \mathcal{L}(q; s_1, \ldots, s_m)$ de los $(a_1, \ldots, a_m) \in \mathbf{Z}^m$ tales que

$$a_1 s_1 + \cdots + a_m s_m \equiv 0 \pmod{q}$$

Theorem

$L = \Gamma\backslash S^{2m-1}$, $L' = \Gamma'\backslash S^{2m-1}$ espacios lente con lattices de congruencia asociados $\mathcal{L}$ y $\mathcal{L}'$ respectivamente. Entonces

(i) *L y L' son 0-isospectrales $\iff$ $\mathcal{L}$ y $\mathcal{L}'$ son $\|\cdot\|_1$-isospectrales.*

(ii) *L y L' son p-isospectrales para todo p $\iff$ $\mathcal{L}$ y $\mathcal{L}'$ son $\|\cdot\|_1^*$-isospectrales.*

Nota: Ikeda'80 dio pares de espacios lente 0-isospectral, $L(11;1,2,3)$ y $L(11;1,2,4)$ en dimensión 5.
sus lattices de congruencia asociados $\mathcal{L} = \mathcal{L}(11;1,2,3)$ y $\mathcal{L}' = \mathcal{L}(11;1,2,4)$ deben ser $\|\cdot\|_1$-isospectrales.

Sin embargo, $\mathcal{L}$ and $\mathcal{L}'$ no son $\|\cdot\|_1^*$-isospectrales.

Theorem

$L = \Gamma \backslash S^{2m-1}$, $L' = \Gamma' \backslash S^{2m-1}$ espacios lente con lattices de congruencia asociados $\mathcal{L}$ y $\mathcal{L}'$ respectivamente. Entonces

(i) *L y L' son 0-isospectrales $\iff$ $\mathcal{L}$ y $\mathcal{L}'$ son $\|\cdot\|_1$-isospectrales.*

(ii) *L y L' son p-isospectrales para todo p $\iff$ $\mathcal{L}$ y $\mathcal{L}'$ son $\|\cdot\|_1^*$-isospectrales.*

Nota: Ikeda'80 dio pares de espacios lente 0-isospectral, $L(11; 1, 2, 3)$ y $L(11; 1, 2, 4)$ en dimensión 5.
sus lattices de congruencia asociados $\mathcal{L} = \mathcal{L}(11; 1, 2, 3)$ y $\mathcal{L}' = \mathcal{L}(11; 1, 2, 4)$ deben ser $\|\cdot\|_1$-isospectrales.

Sin embargo, $\mathcal{L}$ and $\mathcal{L}'$ no son $\|\cdot\|_1^*$-isospectrales.

Theorem

$L = \Gamma\backslash S^{2m-1}$, $L' = \Gamma'\backslash S^{2m-1}$ espacios lente con lattices de congruencia asociados $\mathcal{L}$ y $\mathcal{L}'$ respectivamente. Entonces

(i) *L y L' son 0-isospectrales $\iff$ $\mathcal{L}$ y $\mathcal{L}'$ son $\|\cdot\|_1$-isospectrales.*

(ii) *L y L' son p-isospectrales para todo p $\iff$ $\mathcal{L}$ y $\mathcal{L}'$ son $\|\cdot\|_1^*$-isospectrales.*

Nota: Ikeda'80 dio pares de espacios lente 0-isospectral, $L(11;1,2,3)$ y $L(11;1,2,4)$ en dimensión 5.
sus lattices de congruencia asociados $\mathcal{L} = \mathcal{L}(11;1,2,3)$ y $\mathcal{L}' = \mathcal{L}(11;1,2,4)$ deben ser $\|\cdot\|_1$-isospectrales.

Sin embargo, $\mathcal{L}$ and $\mathcal{L}'$ no son $\|\cdot\|_1^*$-isospectrales.

Theorem

$L = \Gamma\backslash S^{2m-1}$, $L' = \Gamma'\backslash S^{2m-1}$ espacios lente con lattices de congruencia asociados $\mathcal{L}$ y $\mathcal{L}'$ respectivamente. Entonces

(i) *L y L' son 0-isospectrales $\iff$ $\mathcal{L}$ y $\mathcal{L}'$ son $\|\cdot\|_1$-isospectrales.*

(ii) *L y L' son p-isospectrales para todo p $\iff$ $\mathcal{L}$ y $\mathcal{L}'$ son $\|\cdot\|_1^*$-isospectrales.*

Nota: Ikeda'80 dio pares de espacios lente 0-isospectral, $L(11; 1, 2, 3)$ y $L(11; 1, 2, 4)$ en dimensión 5.
sus lattices de congruencia asociados $\mathcal{L} = \mathcal{L}(11; 1, 2, 3)$ y $\mathcal{L}' = \mathcal{L}(11; 1, 2, 4)$ deben ser $\|\cdot\|_1$-isospectrales.

Sin embargo, $\mathcal{L}$ and $\mathcal{L}'$ no son $\|\cdot\|_1^*$-isospectrales.

Cálculos y preguntas

- Usamos un teorema de finitud para producir, con la ayuda de la computadora, muchos ejemplos de pares de lattices de congruencia no-isométricos que son $\|\cdot\|_1^*$-isospectrales.

- Lista de todos los lattices de q-congruencia $\|\cdot\|_1^*$-isospectrales en dimensión m, para $m = 3$, $q \leq 300$ y $m = 4$, $q \leq 150$:

Cálculos y preguntas

- Usamos un teorema de finitud para producir, con la ayuda de la computadora, muchos ejemplos de pares de lattices de congruencia no-isométricos que son $\|\cdot\|_1^*$-isospectrales.

- Lista de todos los lattices de q-congruencia $\|\cdot\|_1^*$-isospectrales en dimensión m, para $m = 3$, $q \leq 300$ y $m = 4$, $q \leq 150$:

q	$[s_1,\ s_2,\ s_3]$	$[s'_1,\ s'_2,\ s'_3]$	
49	[1, 6, 15]	[1, 6, 20]	*
64	[1, 7, 17]	[1, 7, 23]	*
98	[1, 13, 29]	[1, 13, 41]	*
100	[1, 9, 21]	[1, 9, 29]	*
100	[1, 9, 31]	[1, 9, 39]	
121	[1, 10, 23]	[1, 10, 32]	*
121	[1, 10, 34]	[1, 10, 43]	
121	[1, 10, 45]	[1, 10, 54]	
121	[1, 21, 34]	[1, 21, 54]	
121	[1, 21, 45]	[1, 21, 56]	
128	[1, 15, 33]	[1, 15, 47]	*
147	[1, 20, 43]	[1, 20, 62]	*
169	[1, 12, 27]	[1, 12, 38]	*
169	[1, 12, 53]	[1, 12, 64]	
169	[1, 12, 66]	[1, 12, 77]	
169	[1, 25, 40]	[1, 25, 64]	

Todos estos ejemplos responden a la siguiente descripción:

$$\mathcal{L}(q;\theta^{d_0},\theta^{d_1},\dots,\theta^{d_{m-1}}) \quad \text{and} \quad \mathcal{L}(q;\theta^{-d_0},\theta^{-d_1},\dots,\theta^{-d_{m-1}}),$$

donde $q = r^2 t$, $r > 1$, $\theta = 1 + rt$ y $0 = d_0 < d_1 < \cdots < d_{m-1} < r$.

Pregunta

Dar condiciones sobre la secuencia $0 = d_0 < d_1 < \cdots < d_{m-1} < r$ para que los lattices de congruencia sean $\|\cdot\|_1^*$-isospectrales.

Pregunta

Hay ejemplos de lattices $\|\cdot\|_1^*$-isospectrales que no sean de este tipo para algún θ?

Pregunta

Hay familias de lattices mutuamente $\|\cdot\|_1^*$-isospectrales?

Todos estos ejemplos responden a la siguiente descripción:

$$\mathcal{L}(q;\theta^{d_0},\theta^{d_1},\ldots,\theta^{d_{m-1}}) \quad \text{and} \quad \mathcal{L}(q;\theta^{-d_0},\theta^{-d_1},\ldots,\theta^{-d_{m-1}}),$$

donde $q = r^2 t$, $r > 1$, $\theta = 1 + rt$ y $0 = d_0 < d_1 < \cdots < d_{m-1} < r$.

Pregunta

Dar condiciones sobre la secuencia $0 = d_0 < d_1 < \cdots < d_{m-1} < r$ para que los lattices de congruencia sean $\|\cdot\|_1^*$-isospectrales.

Pregunta

Hay ejemplos de lattices $\|\cdot\|_1^*$-isospectrales que no sean de este tipo para algún θ?

Pregunta

Hay familias de lattices mutuamente $\|\cdot\|_1^*$-isospectrales?

`arXiv:1404.2574` *Cyclic groups with the same Hodge series.*
Daryl R. DeFord, Peter G. Doyle

Familias de pares de lattices $\|\cdot\|_1^*$-isospectrales

Para $r, t \in \mathbf{N}$, $r > 1$, $q = r^2 t$ consideramos

$$\mathcal{L} = \mathcal{L}(q; 1, rt-1, 2rt+1), \quad \mathcal{L}' = \mathcal{L}(q; 1, rt-1, 3rt-1).$$

definido por las ecuaciones

$$\begin{aligned} \mathcal{L}: \quad & a + (rt-1)b + (2rt+1)c \equiv 0 \pmod{r^2 t}, \\ \mathcal{L}': \quad & (rt-1)a' + b' + (3rt-1)c' \equiv 0 \pmod{r^2 t}. \end{aligned}$$

El par más simple es $\mathcal{L}(49; 1, 6, 15)$, $\mathcal{L}(49; 1, 6, 20)$ $\quad (t = 1,\ r = 7$ y $q = 49)$.

Theorem

Para r, t enteros positivos impares, $r \not\equiv 0 \pmod 3$, los lattices $\mathcal{L}(q; 1, rt-1, 2rt+1)$ y $\mathcal{L}(q; 1, rt-1, 3rt-1)$ son $\|\cdot\|_1^*$-isospectrales.

Familias de pares de lattices $\|\cdot\|_1^*$-isospectrales

Para $r, t \in \mathbf{N}$, $r > 1$, $q = r^2 t$ consideramos

$$\mathcal{L} = \mathcal{L}(q; 1, rt-1, 2rt+1), \quad \mathcal{L}' = \mathcal{L}(q; 1, rt-1, 3rt-1).$$

definido por las ecuaciones

$$\begin{array}{llll} \mathcal{L}: & a + (rt-1)b + (2rt+1)c & \equiv 0 & \pmod{r^2 t}, \\ \mathcal{L}': & (rt-1)a' + b' + (3rt-1)c' & \equiv 0 & \pmod{r^2 t}. \end{array}$$

El par más simple es $\mathcal{L}(49; 1, 6, 15)$, $\mathcal{L}(49; 1, 6, 20)$ $(t = 1,\ r = 7$ y $q = 49)$.

Theorem

Para r, t enteros positivos impares, $r \not\equiv 0 \pmod 3$, los lattices $\mathcal{L}(q; 1, rt-1, 2rt+1)$ y $\mathcal{L}(q; 1, rt-1, 3rt-1)$ son $\|\cdot\|_1^*$-isospectrales.

Familias de pares de lattices $\|\cdot\|_1^*$-isospectrales

Para $r, t \in \mathbf{N}$, $r > 1$, $q = r^2 t$ consideramos

$$\mathcal{L} = \mathcal{L}(q; 1, rt-1, 2rt+1), \quad \mathcal{L}' = \mathcal{L}(q; 1, rt-1, 3rt-1).$$

definido por las ecuaciones

$$\begin{array}{lcccccc} \mathcal{L}: & a & + (rt-1)b + & (2rt+1)c & \equiv & 0 & \pmod{r^2 t}, \\ \mathcal{L}': & (rt-1)a' + & b' & + (3rt-1)c' & \equiv & 0 & \pmod{r^2 t}. \end{array}$$

El par más simple es $\mathcal{L}(49; 1, 6, 15)$, $\mathcal{L}(49; 1, 6, 20)$ $\quad (t = 1,\ r = 7$ y $q = 49)$.

Theorem

Para r, t enteros positivos impares, $r \not\equiv 0 \pmod 3$, los lattices $\mathcal{L}(q; 1, rt-1, 2rt+1)$ y $\mathcal{L}(q; 1, rt-1, 3rt-1)$ son $\|\cdot\|_1^*$-isospectrales.

Familias de pares de lattices $\|\cdot\|_1^*$-isospectrales

Para $r, t \in \mathbf{N}$, $r > 1$, $q = r^2 t$ consideramos

$$\mathcal{L} = \mathcal{L}(q; 1, rt-1, 2rt+1), \quad \mathcal{L}' = \mathcal{L}(q; 1, rt-1, 3rt-1).$$

definido por las ecuaciones

$$\begin{aligned} \mathcal{L}: \quad & a + (rt-1)b + (2rt+1)c \equiv 0 \pmod{r^2 t}, \\ \mathcal{L}': \quad & (rt-1)a' + b' + (3rt-1)c' \equiv 0 \pmod{r^2 t}. \end{aligned}$$

El par más simple es $\mathcal{L}(49; 1, 6, 15)$, $\mathcal{L}(49; 1, 6, 20)$ $\quad (t = 1,\ r = 7$ y $q = 49)$.

Theorem

Para r, t enteros positivos impares, $r \not\equiv 0 \pmod 3$, los lattices $\mathcal{L}(q; 1, rt-1, 2rt+1)$ y $\mathcal{L}(q; 1, rt-1, 3rt-1)$ son $\|\cdot\|_1^*$-isospectrales.

Problemas

- Hallar todos los ejemplos de lattices isospectfrales en dimensión 4.
- Hay una familia (más de dos) de lattices mutuamente isospectrales en dim 4? En dim 5?
- Jigsaw conjecture sobre lattices isospectrales.
- Dar una nueva prueba (más geométrica?) de la no existencia in dimension 3.
- Hallar nuevos ejemplos de lattices isospectrales con respecto a la norma uno. También $\|\cdot\|_1^*$-isospectrales.

`arXiv:1209.4916` *Representation equivalence and p-Spectrum of constant curvature space forms.* Lauret-Miatello-R. J. Geom. Anal.

Problemas

- Hallar todos los ejemplos de lattices isospectfrales en dimensión 4.
- Hay una familia (más de dos) de lattices mutuamente isospectrales en dim 4? En dim 5?
- Jigsaw conjecture sobre lattices isospectrales.
- Dar una nueva prueba (más geométrica?) de la no existencia in dimension 3.
- Hallar nuevos ejemplos de lattices isospectrales con respecto a la norma uno. También $\|\cdot\|_1^*$-isospectrales.

`arXiv:1209.4916` *Representation equivalence and p-Spectrum of constant curvature space forms.* Lauret-Miatello-R. J. Geom. Anal.

Problemas

- Hallar todos los ejemplos de lattices isospectfrales en dimensión 4.

- Hay una familia (más de dos) de lattices mutuamente isospectrales en dim 4? En dim 5?

- Jigsaw conjecture sobre lattices isospectrales.

- Dar una nueva prueba (más geométrica?) de la no existencia in dimension 3.

- Hallar nuevos ejemplos de lattices isospectrales con respecto a la norma uno. También $\|\cdot\|_1^*$-isospectrales.

`arXiv:1209.4916` *Representation equivalence and p-Spectrum of constant curvature space forms.* Lauret-Miatello-R. J. Geom. Anal.

Problemas

- Hallar todos los ejemplos de lattices isospectfrales en dimensión 4.

- Hay una familia (más de dos) de lattices mutuamente isospectrales en dim 4? En dim 5?

- Jigsaw conjecture sobre lattices isospectrales.

- Dar una nueva prueba (más geométrica?) de la no existencia in dimension 3.

- Hallar nuevos ejemplos de lattices isospectrales con respecto a la norma uno. También $\|\cdot\|_1^*$-isospectrales.

`arXiv:1209.4916` *Representation equivalence and p-Spectrum of constant curvature space forms.* Lauret-Miatello-R. J. Geom. Anal.

Problemas

- Hallar todos los ejemplos de lattices isospectfrales en dimensión 4.

- Hay una familia (más de dos) de lattices mutuamente isospectrales en dim 4? En dim 5?

- Jigsaw conjecture sobre lattices isospectrales.

- Dar una nueva prueba (más geométrica?) de la no existencia in dimension 3.

- Hallar nuevos ejemplos de lattices isospectrales con respecto a la norma uno. También $\|\cdot\|_1^*$-isospectrales.

`arXiv:1209.4916` *Representation equivalence and p-Spectrum of constant curvature space forms.* Lauret-Miatello-R. J. Geom. Anal.

[Bo] Borcherds, R. E. The Leech lattice and other lattices, Ph.D. thesis (Cambridge, 1985). *Proc. R. Soc. London. A* **398** (1985), 365–376.

[CS] Conway, J.H.; Sloane, N., Sphere Packing, Lattices and Groups. *Springer-Verlag 3rd Edition* (1999).

John H, Conway The Sensual (quadratic) form, *Carus Monographs* (1997)

[Eb] Ebeling, Wolfgang. Lattices and codes. A course partially based on lectures by F. Hirzebruch. *Second edition. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn*, Braunschweig, 2002.

E. Lauret, R. Miatello, JPR. Spectra of Lens Spaces from 1-Norm Spectra of Congruence Lattices *IMRN* (2015)