Métodos del álgebra conmutativa aplicados a la Teoría de Códigos

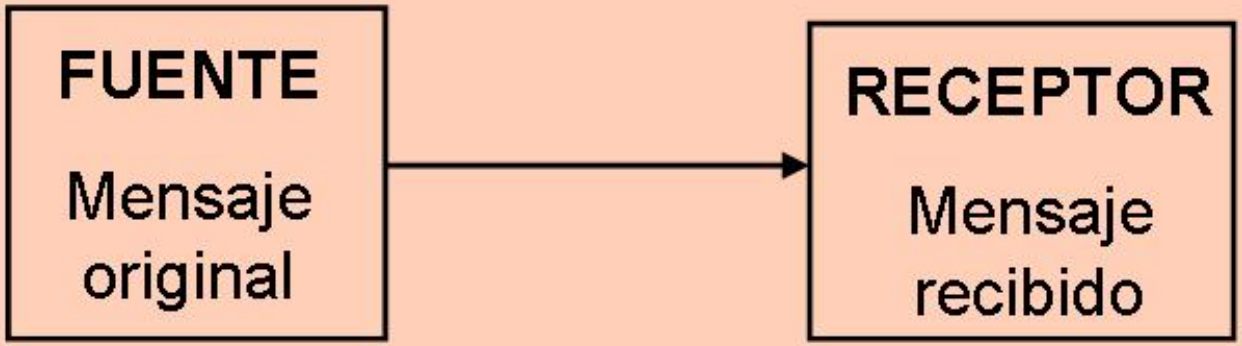
Eliseo Sarmiento Rosales
Departamento de Matemáticas
ESFM-IPN

Seminario de Estudiantes, 30 de septiembre de 2013
CINVESTAV IPN

Índice de la plática

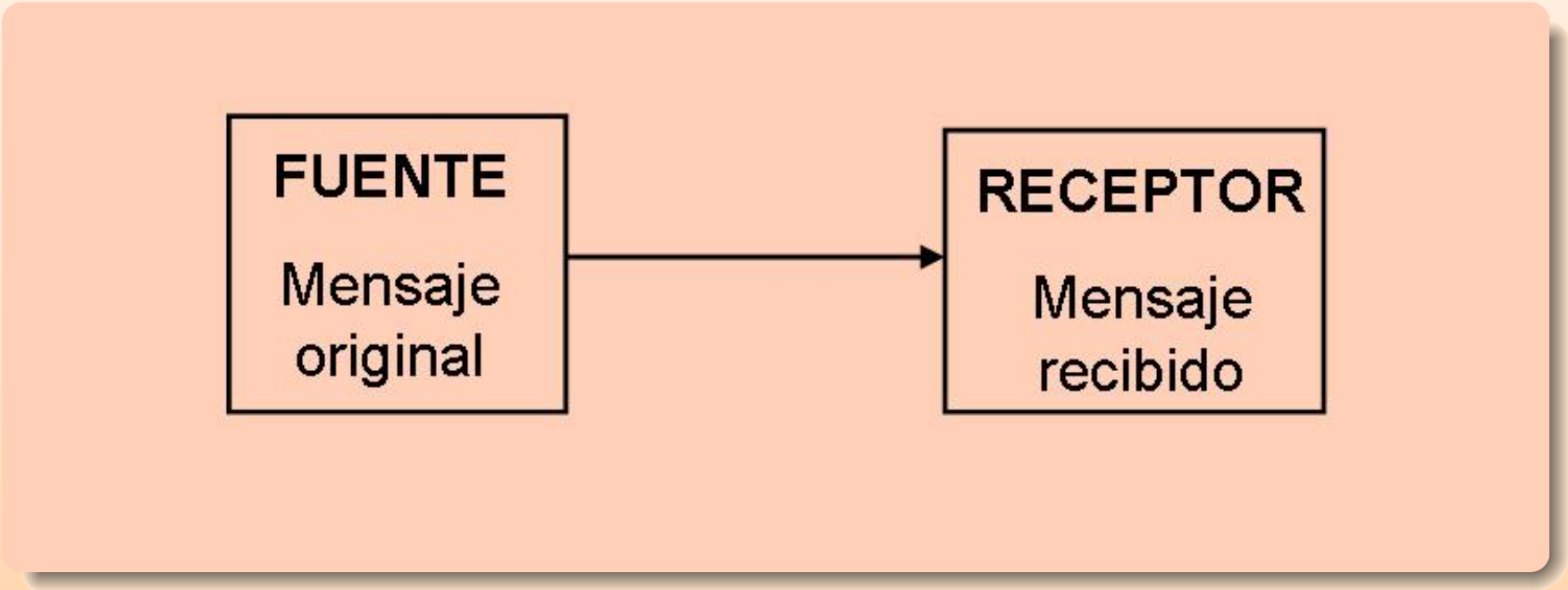
Justificación

Deseamos enviar un mensaje:



Justificación

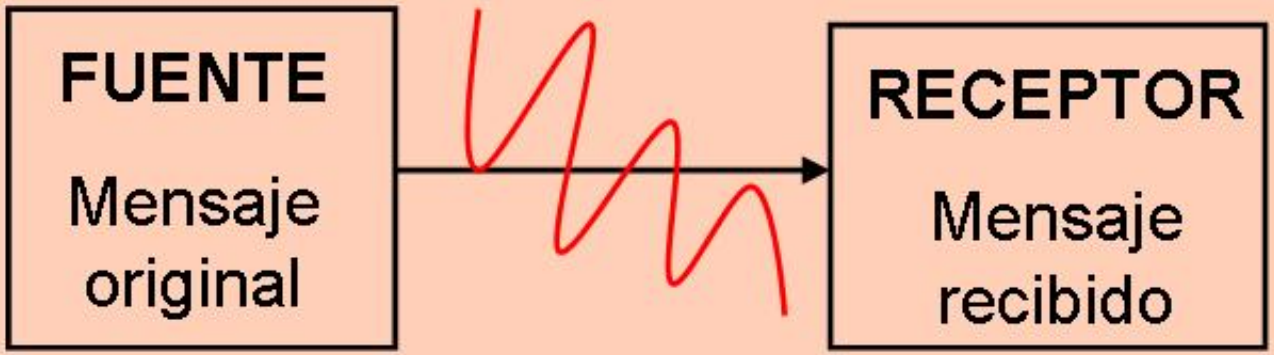
Deseamos enviar un mensaje:



Note que tenemos dos problemas con respecto a la información que se envía.

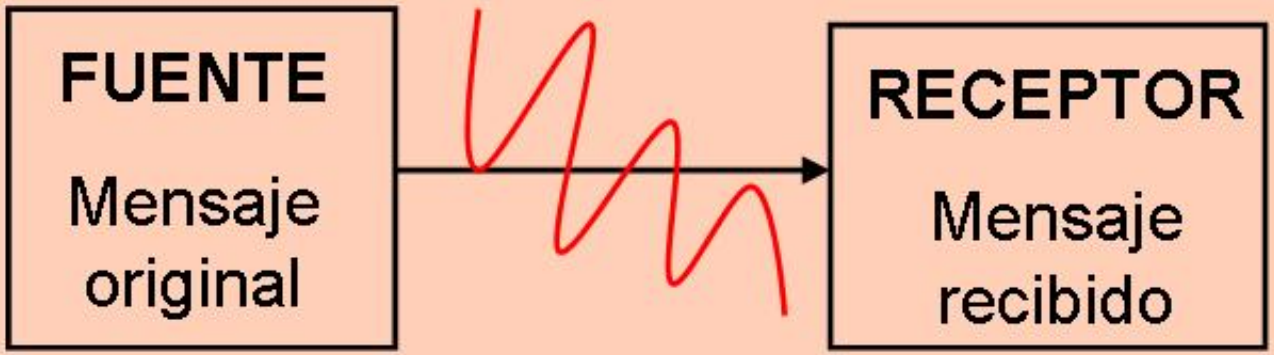
Transmisión de Información

Existencia de factores sexternos que hacen que la información enviada pueda no ser privada o confiable.



Transmisión de Información

Existencia de factores sexternos que hacen que la información enviada pueda no ser privada o confiable.



Para resolver este problema están la Teoría de Códigos y la Criptografía.

Aclaraciones

1. **¿Qué es la Teoría de Códigos?**

Aclaraciones

1. **¿Qué es la Teoría de Códigos?**

   La Teoría de Códigos es un área de las matemáticas que se encarga de corregir errores en la información que se envía en canales de comunicación ruidosos.

Aclaraciones

1. **¿Qué es la Teoría de Códigos?**

   La Teoría de Códigos es un área de las matemáticas que se encarga de corregir errores en la información que se envía en canales de comunicación ruidosos.

2. **¿y la Criptografía?**

Aclaraciones

1. **¿Qué es la Teoría de Códigos?**

   La Teoría de Códigos es un área de las matemáticas que se encarga de corregir errores en la información que se envía en canales de comunicación ruidosos.

2. **¿y la Criptografía?**

   Se encarga de la seguridad de la información que se transmite por un canal no seguro.

Aclaraciones

1. **¿Qué es la Teoría de Códigos?**

   La Teoría de Códigos es un área de las matemáticas que se encarga de corregir errores en la información que se envía en canales de comunicación ruidosos.

2. **¿y la Criptografía?**

   Se encarga de la seguridad de la información que se transmite por un canal no seguro.

3. **¿Cuál es el origen de los códigos lineales?**

Aclaraciones

1. **¿Qué es la Teoría de Códigos?**

   La Teoría de Códigos es un área de las matemáticas que se encarga de corregir errores en la información que se envía en canales de comunicación ruidosos.

2. **¿y la Criptografía?**

   Se encarga de la seguridad de la información que se transmite por un canal no seguro.

3. **¿Cuál es el origen de los códigos lineales?**

   En 1948 Claude Shannon, trabajando en los Laboratorios Bell (Estados Unidos), publicó un trabajo llamado “The Mathematical Theory of Communication”.

Códigos de repetición

Deseo transmitir un mensaje que sólo contenga 0's y 1's.
¿Cómo puedo enviar el mensaje 1?

Códigos de repetición

Deseo transmitir un mensaje que sólo contenga 0's y 1's. ¿Cómo puedo enviar el mensaje 1?

1. Puedo enviar el mensaje 1.

Códigos de repetición

Deseo transmitir un mensaje que sólo contenga 0's y 1's. ¿Cómo puedo enviar el mensaje 1?

1. Puedo enviar el mensaje 1.
2. Puedo enviar el mensaje 111.

Códigos de repetición

Deseo transmitir un mensaje que sólo contenga 0's y 1's.
¿Cómo puedo enviar el mensaje 1?

1. Puedo enviar el mensaje 1.
2. Puedo enviar el mensaje 111.
3. Puedo enviar el mensaje 11111.

Códigos de repetición

Deseo transmitir un mensaje que sólo contenga 0's y 1's.
¿Cómo puedo enviar el mensaje 1?

1. Puedo enviar el mensaje 1.
2. Puedo enviar el mensaje 111.
3. Puedo enviar el mensaje 11111.

El segundo caso es llamado un código de repetición $[3, 1]$, sus elementos o *palabras código* son: 111 y 000.
Pero los elementos que puedo recibir son:

$$111\ 110\ 101\ 011\ 100\ 010\ 001\ 000.$$

Códigos de repetición

Entonces tengo dos tipos de palábras. Las que son factibles y son las únicas que pueden ser enviadas (palabras-código): 111, 000; y las demás 110, 101, 011, 100, 010, 001.

Códigos de repetición

Entonces tengo dos tipos de palábras. Las que son factibles y son las únicas que pueden ser enviadas (palabras-código): $111, 000$; y las demás $110, 101, 011, 100, 010, 001$.

1. Si después de que se ha transmitido cierta de información me llega la palabra: 110. ¿Qué palabras podríamos suponer que se envió originalmente?

Códigos de repetición

Entonces tengo dos tipos de palábras. Las que son factibles y son las únicas que pueden ser enviadas (palabras-código): 111, 000; y las demás 110, 101, 011, 100, 010, 001.

1. Si después de que se ha transmitido cierta de información me llega la palabra: 110. ¿Qué palabras podríamos suponer que se envió originalmente?

   Esperaríamos que se haya enviado 111, porque es la más parecida de las palabras-código.

Códigos de repetición

Entonces tengo dos tipos de palábras. Las que son factibles y son las únicas que pueden ser enviadas (palabras-código): 111, 000; y las demás 110, 101, 011, 100, 010, 001.

1. Si después de que se ha transmitido cierta de información me llega la palabra: 110. ¿Qué palabras podríamos suponer que se envió originalmente?

   Esperaríamos que se haya enviado 111, porque es la más parecida de las palabras-código.

2. ¿Podemos dar una regla para decidir qué palabra es enviada?

Códigos de repetición

Entonces tengo dos tipos de palábras. Las que son factibles y son las únicas que pueden ser enviadas (palabras-código): 111, 000; y las demás 110, 101, 011, 100, 010, 001.

1. Si después de que se ha transmitido cierta de información me llega la palabra: 110. ¿Qué palabras podríamos suponer que se envió originalmente?

   Esperaríamos que se haya enviado 111, porque es la más parecida de las palabras-código.

2. ¿Podemos dar una regla para decidir qué palabra es enviada?

   Sí, utilizando la distancia de Hamming.

Definición

Sea K un campo. La distancia de Hamming se define como la función $\delta : K^n \times K^n \to \mathbb{N} \cup \{0\}$ definida de la siguiente forma:

$$\delta\left((a_1, \ldots, a_n), (b_1, \ldots, b_n)\right) := \left|\{i : a_i \neq b_i\}\right|.$$

la cual es una métrica.

Definición

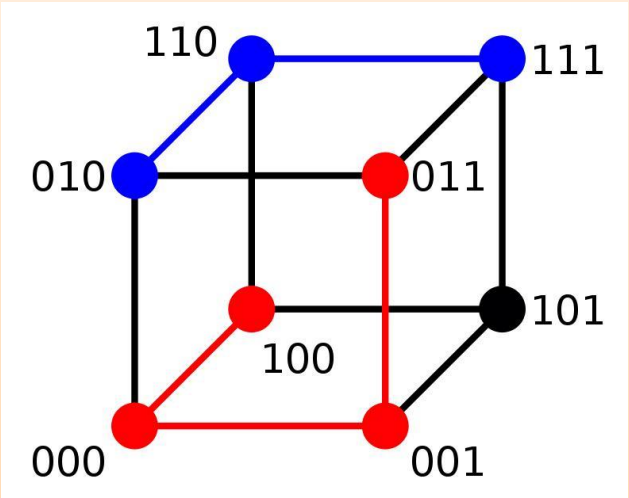
El peso de Hamming de $a = (a_1, \ldots, a_n) \in K^n$ es $w(a) := \delta(a, 0) = \left|\{i : a_i \neq 0\}\right|$.

Códigos de repetición

Para nuestro código de repetición tenemos la siguiente representación de nuestros elementos:

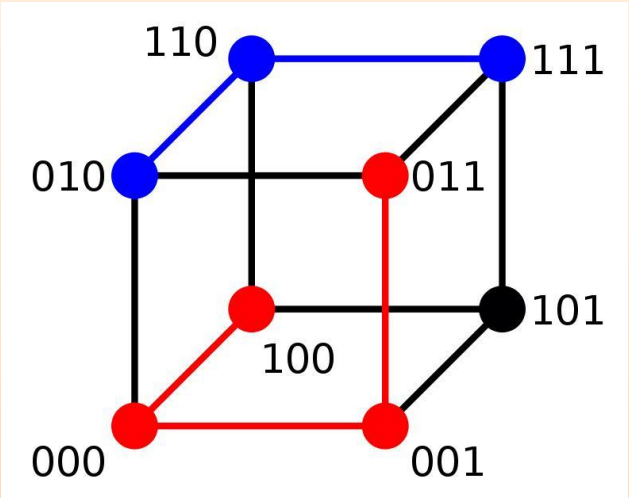
Códigos de repetición

Para nuestro código de repetición tenemos la siguiente representación de nuestros elementos:



Códigos de repetición

Para nuestro código de repetición tenemos la siguiente representación de nuestros elementos:



¿Puedo *detectar* errores? ¿Puedo *corregir* errores? ¿Cuántos? ¿En el tercer caso $[1, 5]$?

Historia de los Códigos Lineales

- En 1948 Claude Shannon, trabajando en los Laboratorios Bell (Estados Unidos), publicó un trabajo llamado “The Mathematical Theory of Communication”.

Historia de los Códigos Lineales

- En 1948 Claude Shannon, trabajando en los Laboratorios Bell (Estados Unidos), publicó un trabajo llamado “The Mathematical Theory of Communication”.
- En 1960 por Irving S. Reed y Gustave Solomon, miembros en aquel tiempo del MIT Lincoln Laboratory, publican un artículo llamado ”Polynomial Codes over Certain Finite Fields”, en el ”Journal of the Society for Industrial and Applied Mathematics”.

Historia de los Códigos Lineales

- En 1948 Claude Shannon, trabajando en los Laboratorios Bell (Estados Unidos), publicó un trabajo llamado “The Mathematical Theory of Communication”.
- En 1960 por Irving S. Reed y Gustave Solomon, miembros en aquel tiempo del MIT Lincoln Laboratory, publican un artículo llamado ”Polynomial Codes over Certain Finite Fields”, en el ”Journal of the Society for Industrial and Applied Mathematics”.
- A partir de 1990 se inicia el uso de herramientas de Geometría Algebraica y Algebra Conmutativa en la Teoría de Códigos.

Códigos Lineales

Definición

Sea K un campo, un código lineal C es un subespacio lineal de K^n.

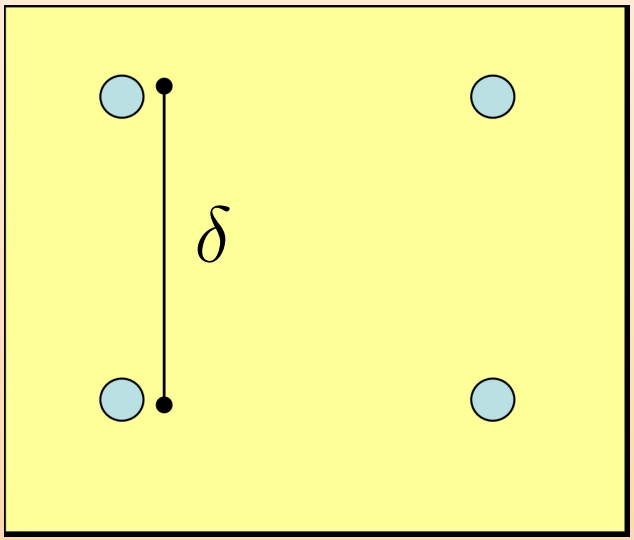
Observación

A los elementos del código C les llamaremos palabras código o simplemente palabras. El campo que usaremos será finito, o sea, $K = \mathbb{F}_q$ con $q = p^n$ y p primo.

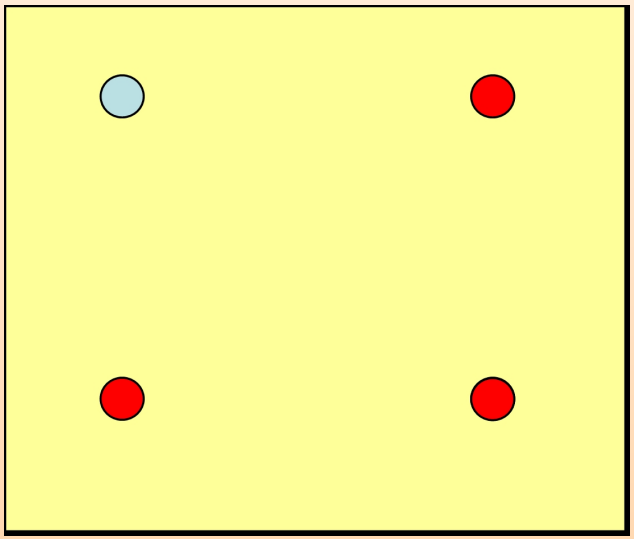
Los **parámetros básicos** de un código $C \subseteq K^n$

- La *longitud* de C es n.
- La *dimension* de C es $k = \dim_K C$.
- La *distancia mínima* $\delta = \min\{w(v) \colon 0 \neq v \in C\}$.

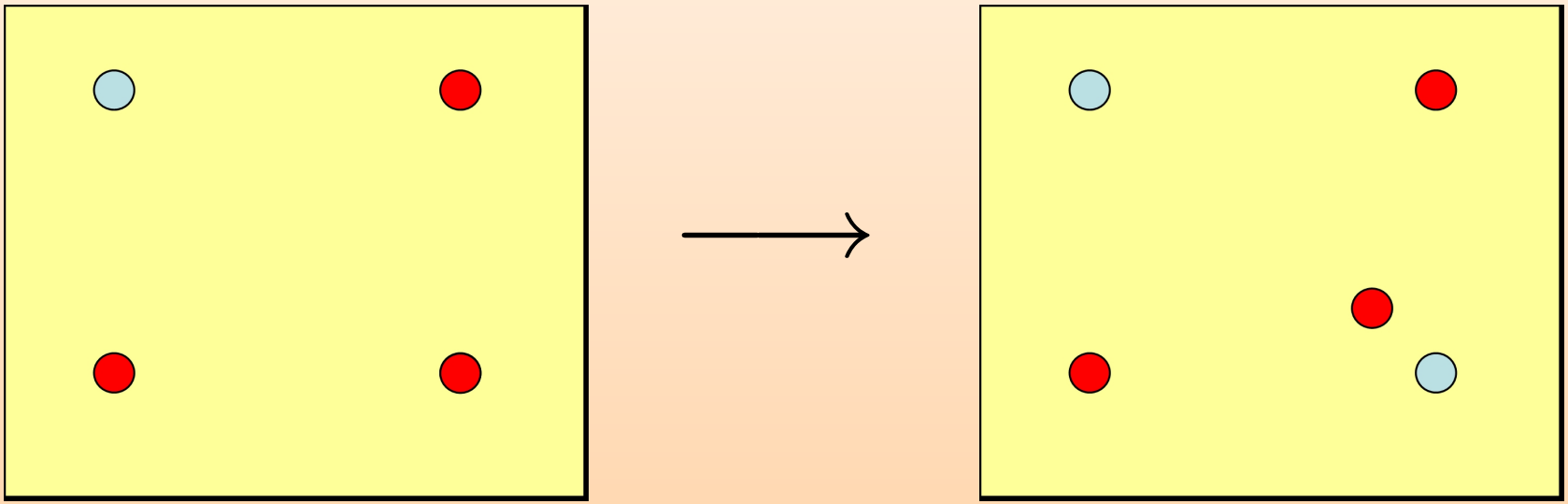
Código detector-corrector de errores



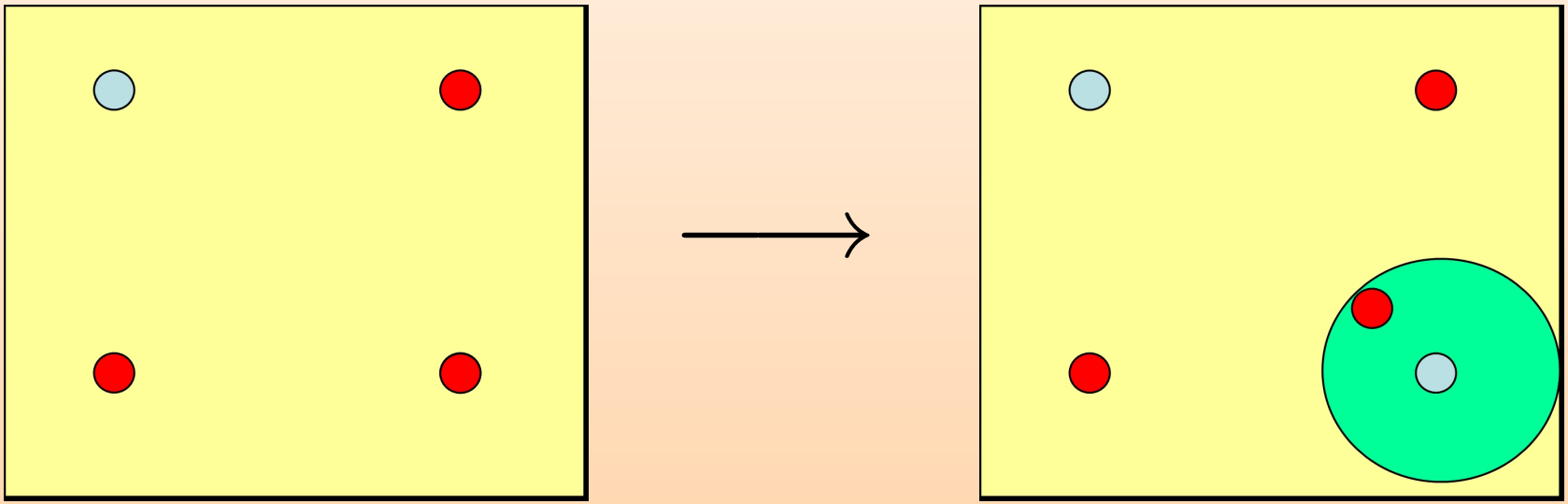
Código detector-corrector de errores



Código detector-corrector de errores

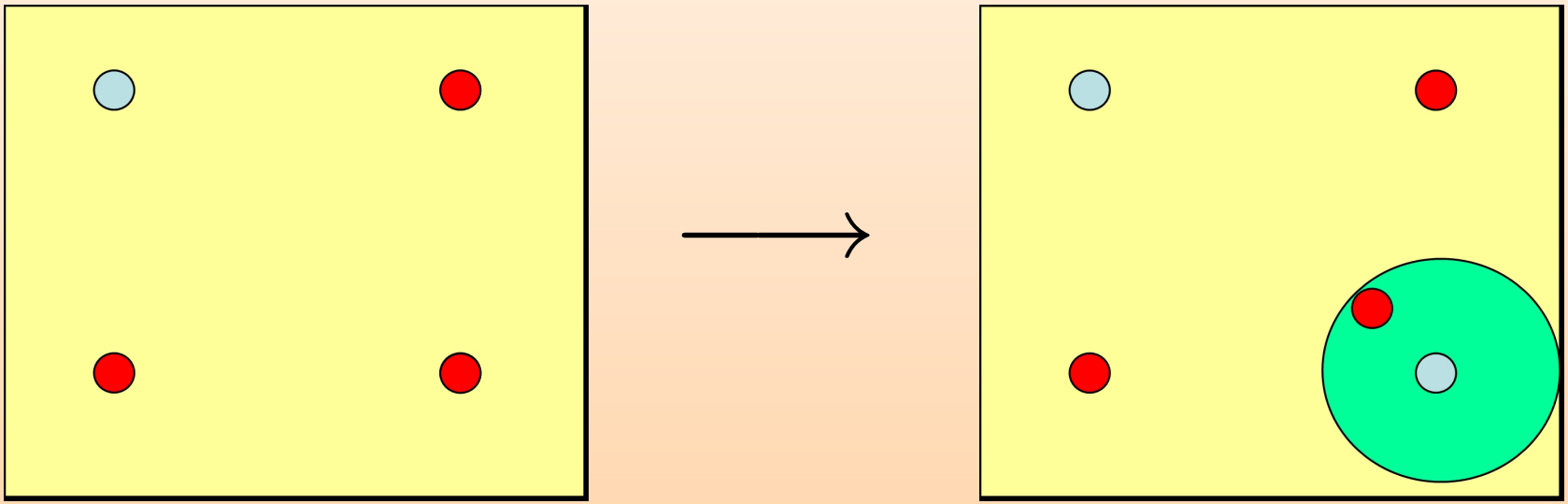


Código detector-corrector de errores



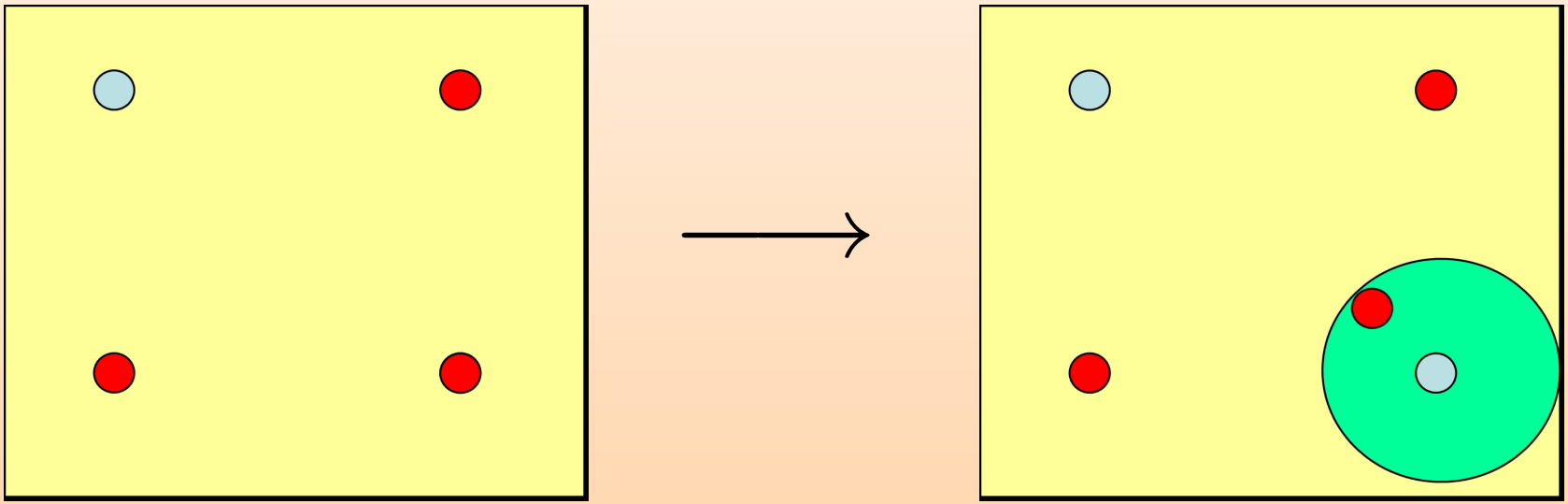
Código detector-corrector de errores

Sea $t := \left[\frac{\delta-1}{2}\right]$. Si un elemento $a \in K^n$ cumple que $\delta(a, c) \leq t$ para algún $c \in C$, entonces c es la única palabra con dicha propiedad.



Código detector-corrector de errores

Sea $t := \left[\frac{\delta-1}{2}\right]$. Si un elemento $a \in K^n$ cumple que $\delta(a, c) \leq t$ para algún $c \in C$, entonces c es la única palabra con dicha propiedad.



El código C se llamará un código detector-corrector de $t-$errores.

Códigos Lineales

1. ¿Cuáles son los parámetros básicos del código de repetición repitiendo r veces?

Códigos Lineales

1. ¿Cuáles son los parámetros básicos del código de repetición repitiendo r veces? $[r, 1, r]$

Códigos Lineales

1. ¿Cuáles son los parámetros básicos del código de repetición repitiendo r veces? $[r, 1, r]$
2. ¿Los parámetros básicos guardarán alguna relación entre ellos?

Códigos Lineales

1. ¿Cuáles son los parámetros básicos del código de repetición repitiendo r veces? $[r, 1, r]$
2. ¿Los parámetros básicos guardarán alguna relación entre ellos?

Cota de Singleton

Los parámetros básicos de un código C están relacionados de la siguiente manera:

$$\delta + k \leq n + 1.$$

En caso que la igualdad se cumpla, se dirá que los Códigos son de *Máxima Distancia Separable*.

Espacio proyectivo y del ideal $I(X)$

Sea $K = \mathbb{F}_q$ un campo finito con q elementos y sea $\mathbb{P}^{s-1}$ el *espacio proyectivo* de dimensión $s-1$ sobre K. Sea $S = K[t_1, \ldots, t_s]$ un anillo de polinomios con la graduación natural

$$S = \bigoplus_{d=0}^{\infty} S_d.$$

Para un subconjunto $X \subset \mathbb{P}^{s-1}$, definimos al ideal anulador de X como el ideal generado por los polinomios homogéneos de S que se anulan en X. Note que se puede graduar

$$I(X) = \bigoplus_{d=0}^{\infty} I(X)_d \subset S.$$

Códigos parametrizados

Definición

Sea $K = \mathbb{F}_q$ un campo finito con q elementos, y tomamos $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{Z}^n, \quad i = 1, \ldots, s$. Sea A la matriz con columnas $v_i, \quad i = 1, \ldots, s$, y sea $x^{v_i} := x_1^{v_{i1}} \cdots x_n^{v_{in}}$ el monomio defino por v_i. El *conjunto paremetrizado por A* está definido por

$$X := \{[(x^{v_1}, \ldots, x^{v_s})] | \, x_i \in K^* = K \setminus \{0\} \; \forall \, i\} \subset \mathbb{P}^{s-1}$$

Toro proyectivo

Cuando A es la matriz identidad de orden s, al conjunto que obtenemos le llamamos *Toro proyectivo*

$$\mathbb{T}^{s-1} := \{[(x_1, \ldots, x_s)] | \, x_i \in K^* \text{ for all } i\} \subset \mathbb{P}^{s-1}.$$

El anillo coordenado homogéneo $S/I(X)$

Definición

La Función de Hilbert de $S/I(X)$ *se define como:*

$$H_X(d) := \dim_K (S/I(X))_d = \dim_K S_d/I(X)_d.$$

Observación (Geramita, Kreuzer, Robbiano, TAMS, 1993)

Hay un entero $r \geq 0$*, llamado el índice de regularidad de* $S/I(X)$*, denotado por* $\operatorname{reg}(S/I(X))$ *tal que*

- $H_X(d-1) < H_X(d)$ *for* $d = 1 \ldots r-1$.
- $H_X(d) = |X|$ *for* $d \geq r$.

Códigos lineales parametrizados por X

Definición

Sea $X = \{[P_1], \ldots, [P_m]\}$ *y sea* $f_0(t_1, \ldots, t_s) = t_1^d$, *con* $d \geq 1$. *El mapero lineal de* $K-$*espacios vectoriales:*

$$\mathrm{ev}_d \colon K[t_1, \ldots, t_s]_d \to K^{|X|}, \qquad f \mapsto \left(\frac{f(P_1)}{f_0(P_1)}, \ldots, \frac{f(P_m)}{f_0(P_m)} \right)$$

es llamado un mapeo de evaluación.

- *La imagen de* ev_d, *denotada por* $C_X(d)$, *es un código lineal.*
- $C_X(d)$ *es llamado el código de evaluación de orden* d *asociado a* X.

Códigos lineales parametrizados por X

Observación

- *El núcleo de* ev_d *es precisamente* $I(X)_d$*. Por lo tanto existe un isomorfismo de* $K-$*espacios vectoriales*

$$S_d/I(X)_d \simeq C_X(d).$$

- $\dim_K C_X(d) = \dim(S_d/I(X)_d) = \dim(S/I(X))_d = H_X(d).$
- *La longitud de* $C_X(d)$ *es igual a* $\mathrm{degree}(S/I(X)) = |X|$.

Los **parámetros básicos** de un código de evaluación son:

- La *longitud* de $C_X(d) \subseteq K^{|X|}$ es $|X|$.
- La *dimension* de $C_X(d)$ es $H_X(d)$.
- La *distancia mínima* $\delta_d := \min\{w(v) \colon 0 \neq v \in C_X(d)\}$ $*$.

Códigos lineales parametrizados por X

Cota de Singleton

La relación de los parámetros básicos de $C_X(d)$ se relacionan según la cota de Singleton de la siguiente forma:

$$\delta_d + H_X(d) \leq |X| + 1$$

$$* \ \ 1 \leq \delta_d \leq |X| - H_X(d) + 1.$$

Códigos lineales parametrizados por X

Cota de Singleton

La relación de los parámetros básicos de $C_X(d)$ se relacionan según la cota de Singleton de la siguiente forma:

$$\delta_d + H_X(d) \leq |X| + 1$$

$$* \ \ 1 \leq \delta_d \leq |X| - H_X(d) + 1.$$

Preguntas

Entonces, ¿qué nos falta saber de los parámetros básicos?, ¿existe una mejor cota superior para la distancia mínima?

Códigos asociados a gráficas

Observación

Podemos generar códigos a partir de gráficas de la siguiente forma:

- *Se toma la matriz de incidencia de una gráfica G.*
- *Se genera el subconjunto X del espacio proyectivo parametrizado por la matriz A.*
- *El mapeo evaluación sobre el conjunto X nos generará un código lineal parametrizado.*

Definición

En el caso anterior el código $C_X(d)$ es llamado el código de evaluación asociado con la gráfica G.

Ejemplo

Sea $K = \mathbb{F}_{81} = \{0, 1, a, a^2, \ldots, a^{79}\}$ y consideremos la siguiente matriz .

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 10 & 18 & 26 & 34 & 42 \\ 5 & 33 & 61 & 89 & 117 & 145 \end{pmatrix}$$

El conjunto parametrizado por A es:

$$X = \{(1,1,1,1,1,1), (1, a^{28}, a^{56}, a^4, a^{32}, a^{60}), (1, a^{56}, a^{32}, a^8, a^{64}, a^{40}), (1, a^4, a^8, a^{12}, a^{16}, a^{20}), (1, a^{32}, a^{64}, a^{16}, a^{48}, 1), (1, a^{60}, a^{40}, a^{20}, 1, a^{60}), (1, a^8, a^{16}, a^{24}, a^{32}, a^{40}), (1, a^{36}, a^{72}, a^{28}, a^{64}, a^{20}), (1, a^{64}, a^{48}, a^{32}, a^{16}, 1), (1, a^{12}, a^{24}, a^{36}, a^{48}, a^{60}), (1, a^{40}, 1, a^{40}, 1, a^{40}), (1, a^{68}, a^{56}, a^{44}, a^{32}, a^{20}), (1, a^{16}, a^{32}, a^{48}, a^{64}, 1), (1, a^{44}, a^8, a^{52}, a^{16}, a^{60}), (1, a^{72}, a^{64}, a^{56}, a^{48}, a^{40}), (1, a^{20}, a^{40}, a^{60}, 1, a^{20}), (1, a^{48}, a^{16}, a^{64}, a^{32}, 1), (1, a^{76}, a^{72}, a^{68}, a^{64}, a^{60}), (1, a^{24}, a^{48}, a^{72}, a^{16}, a^{40}), (1, a^{52}, a^{24}, a^{76}, a^{48}, a^{20})\}$$

Ejemplo

La longitud del código $C_X(d)$ es $|X| = 20$. Podemos calcular la función de Hilbert y la distancia mínima con Macaulay 2.

d	$H_X(d)$	δ_d
1	6	15
2	11	10
3	16	5
4	20	1
5	20	1

Se puede observar que los códigos son códigos MDS.

Pregunta

¿Cómo se calcula la distancia mínima? ¿Qué tan complicado se vuelve?

Ideal $I(X)$

El ideal $I(X)$ se puede expresar como:

$$I(X) = \bigcap_{[\alpha] \in X} I_{[\alpha]}$$

donde $I_{[\alpha]} = (\alpha_1 t_2 - \alpha_2 t_1, \alpha_1 t_3 - \alpha_3 t_1, \ldots, \alpha_1 t_s - \alpha_s t_1)$
es el ideal generado por los polinomios homogéneos de S que se anulan en el punto $[\alpha] = [(\alpha_1, \ldots, \alpha_s)]$.

Definición

Un ideal generado por binomios de la forma $t^a - t^b$, con $a, b \in \mathbb{N}^s$, es llamado un *ideal binomial* de S.

Ideal $I(X)$

Teorema (Rentería, Simis, Villarreal, 2010)

- $I(X) = (\{t_i - y^{v_i} z\}_{i=1}^{s} \cup \{x_i^{q-1} - 1\}_{i=1}^{n}) \cap S$.
- $I(X)$ *es un ideal binomial.*
- $t_i \notin \mathcal{Z}_S(S/I(X))$ *para todo* i.
- $I(X) = (\{t^a - t^b | \, a, b \in \mathbb{N}^s$ *with* $a - b \in \mathcal{L}\})$ *para algún subgrupo aditivo* $\mathcal{L}$ *de* $\mathbb{Z}^s$. *Lo que significa que* $I(X)$ *es un lattice ideal.*
- $S/I(X)$ *es un anillo Cohen-Macaulay de dimensión 1.*

El grado de complejidad de $I(X)$

Se ha estudiado la propiedead de cuando $I(X)$ es una intersección completa. El siguiente resultado muestra una caracterización de esta propiedad.

Teorema (- , Vaz Pinto, Villarreal, 2010)

Sea $\mathcal{C}$ un clutter con s aristas y sea $\mathbb{T}^{s-1} = \{[(x_1, \ldots, x_s)] | \, x_i \in K^*\}$ el toro proyectivo. Las siguientes condiciones son equivalente:

- *$I(X)$ es una intersección completa.*
- *$I(X) = (t_1^{q-1} - t_s^{q-1}, \ldots, t_{s-1}^{q-1} - t_s^{q-1})$.*
- *$X = \mathbb{T}^{s-1} \subset \mathbb{P}^{s-1}$.*

El grado de complejidad de $I(X)$

Definición

El grado de complejidad de un ideal I con respecto al orden $\prec$ es el máximo grado de la base de Grobner reducida de I.

Recordemos que el *orden lexicográfico inverso* (*revlex*) en los monomios de S, es el orden dado por $t^a \prec t^b$ si y sólo si la última entrada no cero de $b - a$ es negativa.

Teorema (- , Vaz Pinto, Villarreal, 2010)

Sea $\mathcal{C}$ un clutter y sea $\prec$ el orden revlex en los monomios de S. Si $\mathcal{G}$ es una base de Grobner reducida del ideal $I(X)$, entonces $t_i^{q-1} - t_s^{q-1} \in \mathcal{G}$ para $i = 1, \ldots, s-1$ y $\deg_{t_i}(g) \leq q-1$ para $g \in \mathcal{G}$ y $1 \leq i \leq s$.

El caso del toro proyectivo $X = \mathbb{T}^{s-1} \subset \mathbb{P}^{s-1}$

Definición

Sea $X = \mathbb{T}^{s-1} = \{[(x_1, \ldots, x_s)] | \, x_i \in K^*$ *for all* $i\} \subset \mathbb{P}^{s-1}$*. En este caso a* $C_X(d)$ *le llamaremos el código Reed-Solomon generalizado.*

Pregunta

¿Cuáles son los parámtros básicos del código $C_X(d)$?

El caso del toro proyectivo $X = \mathbb{T}^{s-1} \subset \mathbb{P}^{s-1}$

La longitud de $C_X(d)$

Si $X = \mathbb{T}^{s-1}$, entonces la longitud de $C_X(d)$ es $|X| = (q-1)^{s-1}$.

Proposición (González, Rentería , Congr. Numer., 2003)

Si $X = \mathbb{T}^{s-1}$, entonces

- $I(\mathbb{T}^{s-1}) = (\{t_i^{q-1} - t_1^{q-1}\}_{i=2}^{s})$.
- *La dimensión de $C_X(d)$ está dada por*

$$H_X(d) = \binom{s-1+d}{d} + \sum_{i=1}^{s-1} (-1)^i \binom{s-1}{i} \binom{s-1+d-i(q-1)}{d-i(q-1)}$$

Caso particular: $\mathbb{T}^2 \subset \mathbb{P}^2$

Proposición (González, Hansen, Rentería, Villarreal)

Si $X = \mathbb{T}^2 \subset \mathbb{P}^2$, *entonces*

$$\delta_d = \begin{cases} (q-1)(q-1-d) & \text{if} \quad 1 \leq d \leq (q-2), \\ 2q-d-3 & \text{if} \quad q-1 \leq d \leq 2(q-2)-1, \\ 1 & \text{if} \quad d \geq 2(q-2). \end{cases}$$

Distancia mínima de $\mathbb{T} \subset \mathbb{P}^{s-1}$

Para encontrar la distancia mínima de estos códigos, se acotó el número de ceros de polinomios en ciertos conjuntos.

Lema

Sea $0 \neq G = G(t_1, \ldots, t_s) \in S$ *un polinomio con grado total* d. *Si*

$$Z_G := \{x \in (K^*)^s \mid G(x) = 0\},$$

entonces $|Z_G| \leq d(q-1)^{s-1}$.

Teorema

Sea $G = G(t_1, \ldots, t_s) \in S$ *un polinomio de grado total* $d \geq 1$ *tal que* $\deg_{t_i}(G) \leq q-2$ *para* $i = 1, \ldots, s$. *Si* $d = k(q-2) + \ell$ *con* $1 \leq \ell \leq q-2$ *y* $0 \leq k \leq s-1$, *entonces*

$$|Z_G| \leq (q-1)^{s-k-1}((q-1)^{k+1} - (q-1) + \ell).$$

Distancia mínima de $\mathbb{T} \subset \mathbb{P}^{s-1}$

Se encuentra de forma explícita la fórmula para la distancia mínima de estos códigos.

Distancia mínima de $\mathbb{T} \subset \mathbb{P}^{s-1}$

Se encuentra de forma explícita la fórmula para la distancia mínima de estos códigos.

Teorema

Si $X = \mathbb{T}$ *y* $1 \leq d = k(q-2) + \ell$ *con* $1 \leq \ell \leq q-2$ *y* $k \geq 0$, *entonces la distancia mínima es:*

$$\delta_d = \begin{cases} (q-1)^{s-(k+2)}(q-1-\ell) & \text{si} \quad d \leq (q-2)(s-1)-1, \\ 1 & \text{si} \quad d \geq (q-2)(s-1). \end{cases}$$

Distancia mínima de $\mathbb{T} \subset \mathbb{P}^{s-1}$

Se encuentra de forma explícita la fórmula para la distancia mínima de estos códigos.

Teorema

Si $X = \mathbb{T}$ *y* $1 \leq d = k(q-2) + \ell$ *con* $1 \leq \ell \leq q-2$ *y* $k \geq 0$, *entonces la distancia mínima es:*

$$\delta_d = \begin{cases} (q-1)^{s-(k+2)}(q-1-\ell) & \text{si} \quad d \leq (q-2)(s-1)-1, \\ 1 & \text{si} \quad d \geq (q-2)(s-1). \end{cases}$$

Este resultado se puede aplicar a otros casos.

Gráficas bipartitas completas

Sea $K_{m,n}$ una gráficas bipartita completa, con matriz de incidencia

$$A = \begin{pmatrix} 1 & 1 & 1 & \dots & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots & 1 & 1 & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots & 0 & 1 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

El conjunto parametrizado X que le corresponde es:

$$X = \{[(t_1t_{m+1}, t_1t_{m+2}, \dots, t_1t_{m+n}, t_2t_{m+1}, t_2t_{m+2}, \dots, t_2t_{m+n}, \dots t_mt_{m+1}, t_mt_{m+2}, \dots, t_mt_{m+n})] \; | t_i \in K^* \text{ for all } i = 1, \dots, m+n\}$$

A continuación se describen los parámetros básicos del código $C_X(d)$.
Sea $X_1 = \mathbb{T}^{n-1}$ y $X_2 = \mathbb{T}^{m-1}$ los toros proyectivos de dimensiones $n-1$ y $m-1$ respectivamente. Entonces:

Teorema (González, Rentería, Int. J. of Algebra 2008)

- *Longitud*: $(q-1)^{m+n-2}$
- *Dimensión*: $H_X(d) = H_{X_1}(d) \cdot H_{X_2}(d)$
- *a-invariante*:
  $a_X = \max\{(n-1)(q-1)-n, (m-1)(q-1)-m\}$
- *Distancia mínima*: $\delta_X(d) = \delta_{X_1}(d) \cdot \delta_{X_2}(d)$.

Ciclos impares

Sea G un ciclo impar, con matriz de incidencia $A \in M_{n\times n}[K]$. Entonces el código parametrizado asociado a G es,

$$X = \{[(t_1t_2, t_2t_3, \ldots, t_nt_1)] \mid t_i \in K^*\} \subset \mathbb{P}^{n-1}$$

como G es una conexa y no-bipartita, entonces $|X| = (q-1)^{n-1}$. Luego,

$$X = \{[(x_1, x_2, \ldots, x_n)] \mid x_i \in K^*\} = \mathbb{T}^{n-1} \subset \mathbb{P}^{n-1}$$

es un toro proyectivo.

Regularidad

Teorema

Si G es una gráfica conexa y X es el conjunto tórico proyectivo parametrizado por G, entonces:

$$\operatorname{reg}(S/I(X)) = \begin{cases} \frac{(q-2)(n-1)}{2(q-1)} & \text{si} \quad G \text{ es bipartita} \\ \frac{(q-2)(n-1)}{2} & \text{si} \quad G \text{ es no bipartita.} \end{cases}$$

Problemas abiertos

Aunque a lo largo de esta tesis se han encontrado resultados valiosos aún quedan mucho problemas sin resolver, por ejemplo:

Problemas abiertos

Aunque a lo largo de esta tesis se han encontrado resultados valiosos aún quedan mucho problemas sin resolver, por ejemplo:

- Calcular los parámetros básicos de los códigos proyectivos parametrizados asociados a gráficas.

Problemas abiertos

Aunque a lo largo de esta tesis se han encontrado resultados valiosos aún quedan mucho problemas sin resolver, por ejemplo:

- Calcular los parámetros básicos de los códigos proyectivos parametrizados asociados a gráficas.
- Calcular los parámetros básicos de los códigos proyectivos parametrizados asociados a cualquier matriz.

Problemas abiertos

Aunque a lo largo de esta tesis se han encontrado resultados valiosos aún quedan mucho problemas sin resolver, por ejemplo:

- Calcular los parámetros básicos de los códigos proyectivos parametrizados asociados a gráficas.
- Calcular los parámetros básicos de los códigos proyectivos parametrizados asociados a cualquier matriz.
- Encontrar códigos parametrizados que sean de Máxima Distancia Separable que puedan ser implementados.

GRACIAS

Contacto

Eliseo Sarmiento Rosales

$e-mail$	eliseo@esfm.ipn.mx
sitio	http : //esfm.ipn.mx/eliseo
fb	facebook.com/Curso_ESFM