Introducción a los códigos correctores de errores

Mathematics sin fronteras

María Chara

Universidad Nacional del Litoral

12 de mayo 2021

FIQ UNL. FACULTAD DE INGENIERÍA QUÍMICA

Mariner 9, 1971

Mariner 9 (**Mariner Mars '71** / **Mariner-I**) fue una sonda espacial no tripulada de la NASA que contribuyó en gran medida a la exploración de Marte y fue parte del programa Mariner . El Mariner 9 fue lanzado hacia Marte el 30 de mayo de 1971 desde la Estación de la Fuerza Aérea de Cabo Cañaveral y llegó al planeta el 14 de noviembre del mismo año, convirtiéndose en la primera nave espacial en orbitar otro planeta, superando por poco a los soviéticos Mars 2 y Mars 3 . que ambos llegaron dentro de un mes. Después de meses de tormentas de polvo, logró enviar imágenes claras de la superficie.

Mariner 9 devolvió 7329 imágenes durante el transcurso de su misión, que concluyó en octubre de 1972.

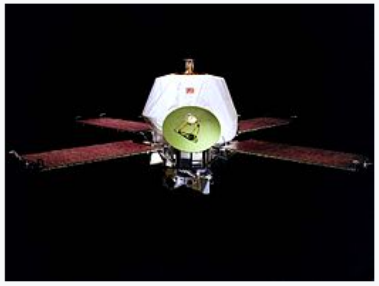
Contenido [hide]

Objetivos

El Mariner 9 fue diseñado para continuar los estudios atmosféricos iniciados por los Mariner 6 y 7 , y para mapear más del 70% de la superficie marciana desde la altitud más baja (1.500 kilómetros (930 millas)) y en las resoluciones más altas (desde 1 kilómetro por píxel hasta 100 metros por píxel) de cualquier misión a Marte hasta ese punto. Se incluyó un radiómetro infrarrojo para detectar fuentes de calor en busca de evidencia de actividad volcánica . Fue para estudiar los cambios temporales en la atmósfera y la superficie marcianas. También se analizarían las dos lunas de Marte. Mariner 9 cumplió con creces sus objetivos.

Según los planes originales, se volaría una misión dual como los Marineros 6–7, sin embargo, el fracaso del lanzamiento del Mariner 8 arruinó este plan y obligó a los planificadores de la NASA a recurrir a una misión más simple de una sola sonda. La NASA

Marinero 9



La nave espacial Mariner 9

Tipo de misión	Orbitador de Marte
Operador	NASA / JPL
ID COSPAR	1971-051A
SATCAT no.	5261
Duración de la misión	1 año, 4 meses, 27 días
Propiedades de la nave espacial	
Fabricante	Laboratorio de propulsión a chorro
Masa de lanzamiento	997,9 kilogramos (2200 libras)
Secado masivo	558,8 kilogramos (1232 libras)
Poder	500 vatios
Inicio de la misión	
Fecha de lanzamiento	30 de mayo de 1971 22:23:04 UTC

Figure: https://es.qwe.wiki/wiki/Mariner_9

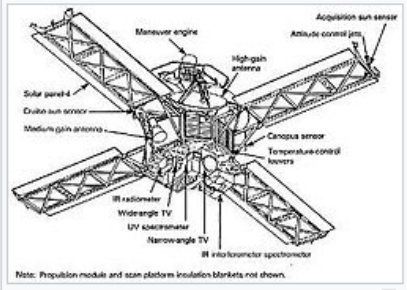
Mariner 9, 1971

Construcción

El espectrómetro ultravioleta a bordo del Mariner 9 fue construido por el Laboratorio de Física Atmosférica y Espacial de la Universidad de Colorado , Boulder, Colorado . El equipo del espectrómetro ultravioleta fue dirigido por el profesor Charles Barth.

El equipo del espectrómetro de interferómetro infrarrojo (IRIS) fue dirigido por el Dr. Rudolf A. Hanel del Centro de vuelos espaciales Goddard de la NASA (GSFC). El instrumento IRIS fue construido por Texas Instruments , Dallas, Texas .

El equipo del radiómetro infrarrojo (IRR) fue dirigido por el profesor Gerald Neugebauer del Instituto de Tecnología de California (Caltech).



Un esquema de Mariner 9, que muestra los principales componentes y características.

Logros de códigos de corrección de errores

Para controlar los errores en la recepción de los datos de imagen en escala de grises enviados por Mariner 9 (causados por una baja relación señal / ruido), los datos tenían que codificarse antes de la transmisión utilizando un llamado código de corrección de errores hacia adelante (FEC) . Sin FEC, el ruido habría constituido aproximadamente una cuarta parte de una imagen recibida, mientras que FEC codificaba los datos de forma redundante, lo que permitió la reconstrucción de la mayoría de los datos de la imagen enviada en la recepción.

Dado que el hardware volado estaba restringido con respecto al peso, el consumo de energía, el almacenamiento y la potencia de cálculo, se tuvieron que tomar algunas consideraciones al elegir un FEC, y se decidió usar un código Hadamard para Mariner 9. Cada píxel de la imagen se representó como un valor binario de seis bits, que tenía 64 niveles de escala de grises posibles . Debido a las limitaciones del transmisor, la longitud máxima de datos útiles fue de unos 30 bits. En lugar de usar un código de repetición , se usó un código Hadamard perforado [32, 6, 16], que también es un código Reed-Muller de primer orden . Los errores de hasta siete bits por cada palabra de 32 bits podrían corregirse utilizando este esquema. En comparación con un código de cinco repeticiones, las propiedades de corrección de errores de este código Hadamard eran mucho mejores, pero su velocidad de datos era comparable. El algoritmo de decodificación eficiente fue un factor importante en la decisión de utilizar este código. El circuito utilizado se denominó "Máquina

Figure: https://es.qwe.wiki/wiki/Mariner_9

Mariner 9: Imagen de la caldera central del volcán Marciano Olympus Mons.

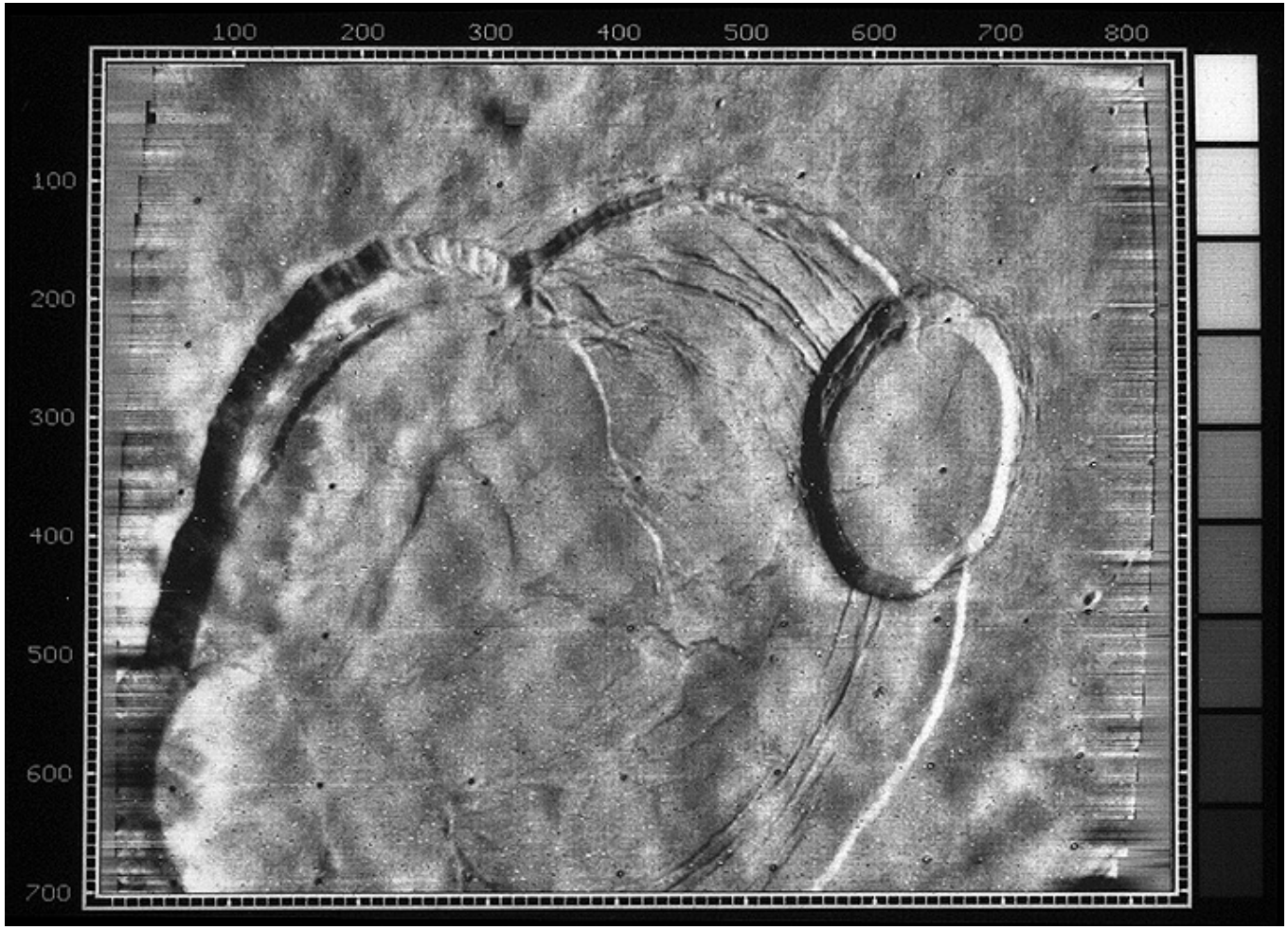


Figure: https://nssdc.gsfc.nasa.gov/imgcat/html/object_page/m09_mtvs4265_52.html

Patricia “Patsy” Conklin, una empleada de la sección de Biociencia y Planetología del Laboratorio de Propulsión de la NASA ensambla fotos de Mariner 9 en mosaicos grandes.

Figure: https://www.upi.com/Top_News/2020/05/30/On-This-Day-Mariner-9-launched-toward-Mars/4991590342141/

Ejemplo: Transmisión de fotografías desde naves espaciales de la NASA

Ejemplo: Transmisión de fotografías desde naves espaciales de la NASA

El Mariner 4 (1964/1965) fue la primera nave espacial en tomar fotografías de otro planeta. Tomó 22 fotografías completas de Marte.

Ejemplo: Transmisión de fotografías desde naves espaciales de la NASA

El Mariner 4 (1964/1965) fue la primera nave espacial en tomar fotografías de otro planeta. Tomó 22 fotografías completas de Marte.

Cada fotografía se desarmó en 200×200 elementos y a cada elemento se le asignó una $6-$upla binaria que representaba uno de los 64 niveles de brillantez de blanco (000000) a negro (111111).

Ejemplo: Transmisión de fotografías desde naves espaciales de la NASA

El Mariner 4 (1964/1965) fue la primera nave espacial en tomar fotografías de otro planeta. Tomó 22 fotografías completas de Marte.

Cada fotografía se desarmó en 200×200 elementos y a cada elemento se le asignó una $6-$upla binaria que representaba uno de los 64 niveles de brillantez de blanco (000000) a negro (111111).

El número total de bits (dígitos binarios) por foto fue de 240000. Fueron necesarias 8 horas para trasmitir cada una de las imágenes.

Ejemplo: Transmisión de fotografías desde naves espaciales de la NASA

El Mariner 4 (1964/1965) fue la primera nave espacial en tomar fotografías de otro planeta. Tomó 22 fotografías completas de Marte.

Cada fotografía se desarmó en 200×200 elementos y a cada elemento se le asignó una $6-$upla binaria que representaba uno de los 64 niveles de brillantez de blanco (000000) a negro (111111).

El número total de bits (dígitos binarios) por foto fue de 240000. Fueron necesarias 8 horas para trasmitir cada una de las imágenes.

Todas las imágenes fueron almacenadas en la cinta de a bordo y luego enviadas a nuestro planeta. Todas las imágenes se enviaron por duplicado.

Mariner 4, 1964 1965

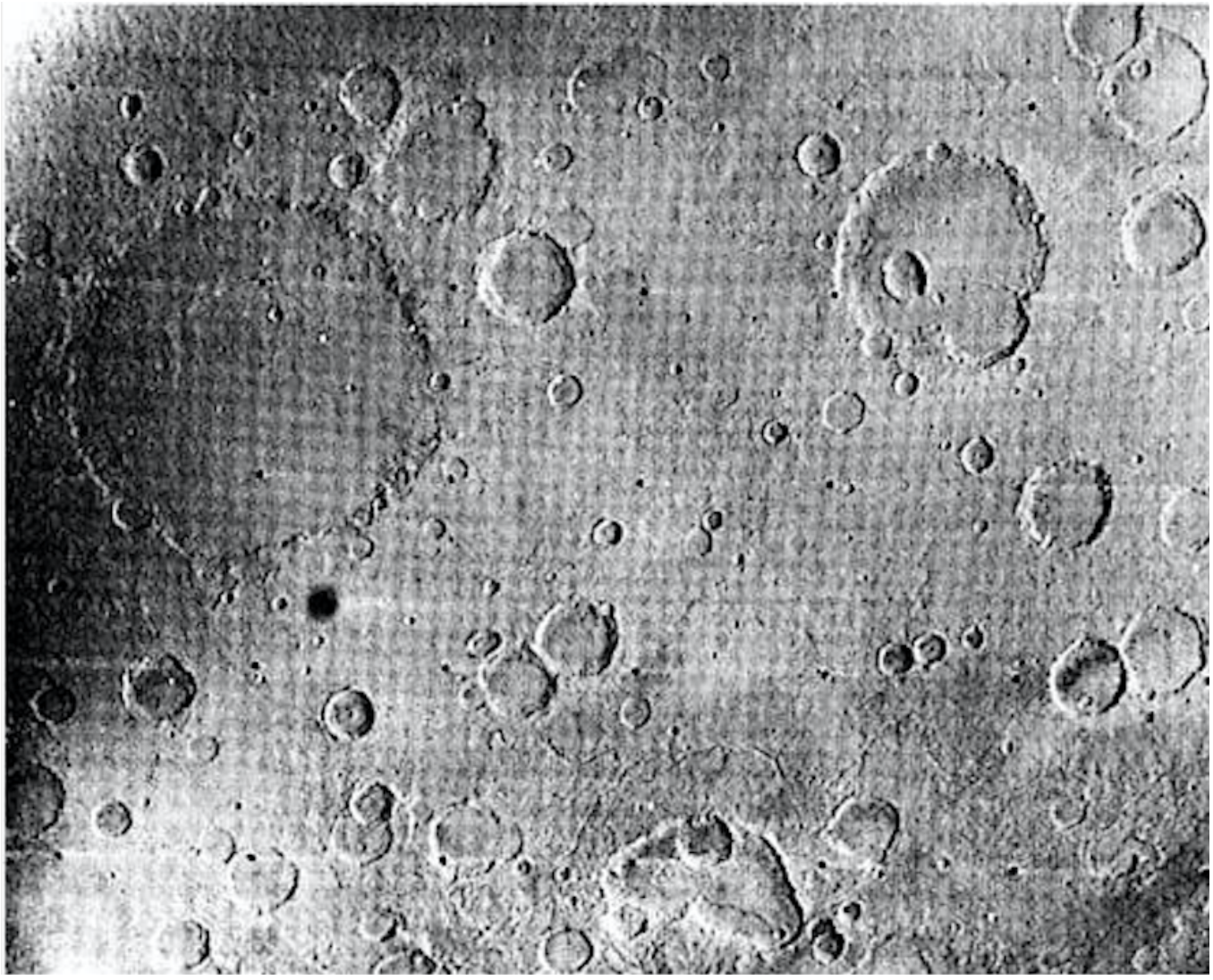
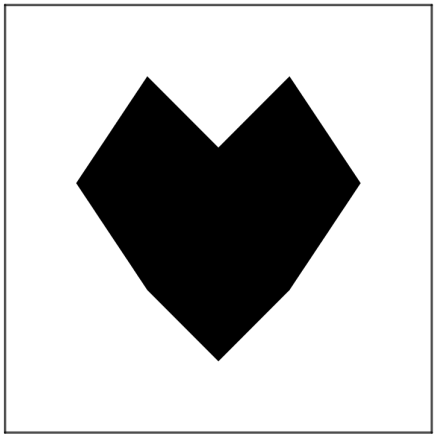


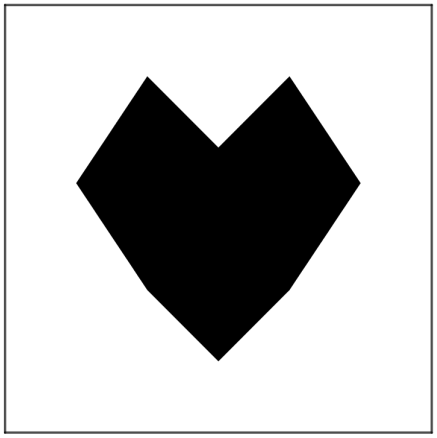
Figure: Photo:NASA

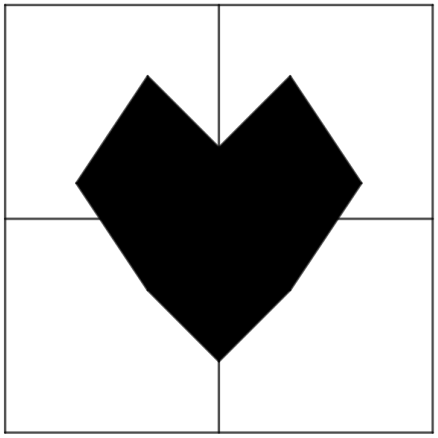
Cómo lo hacemos?

Cómo lo hacemos?

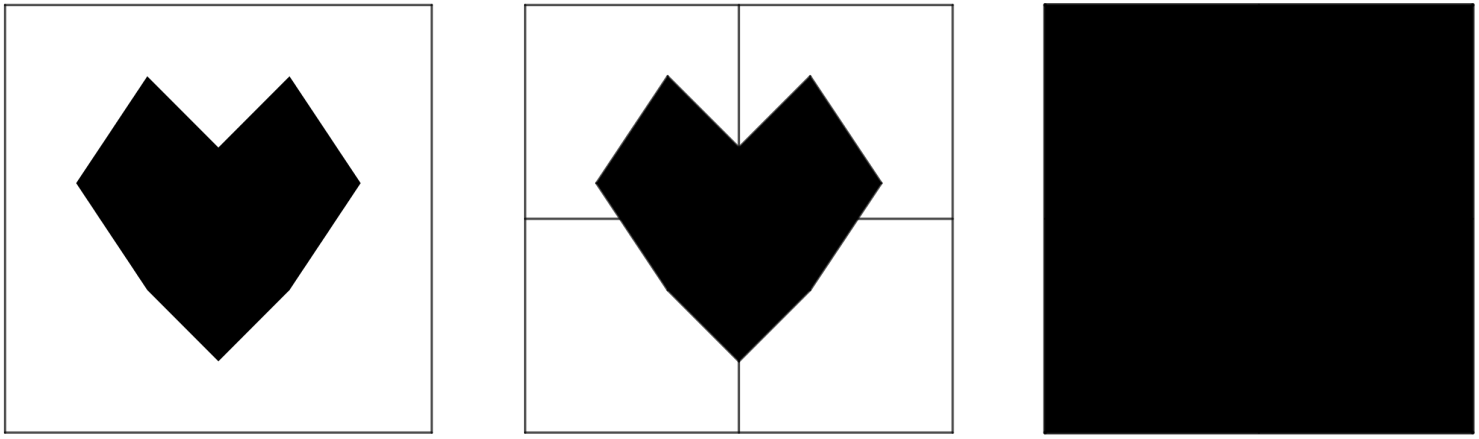


Cómo lo hacemos?

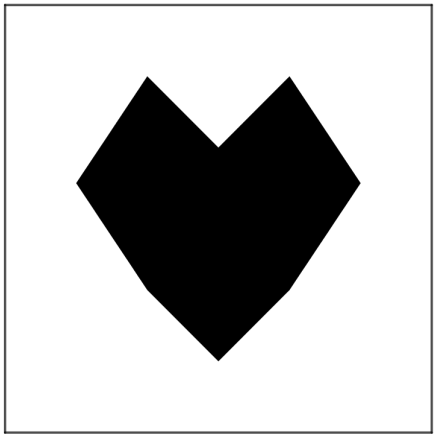


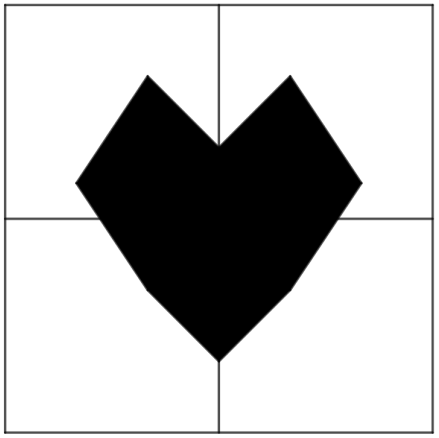


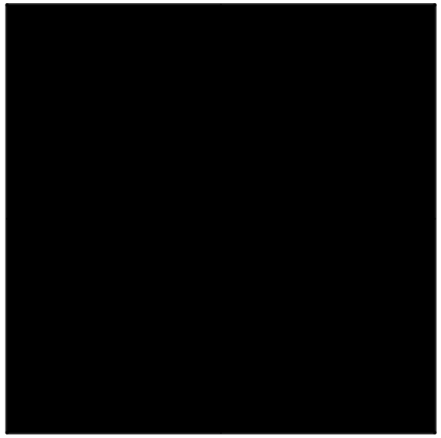
Cómo lo hacemos?

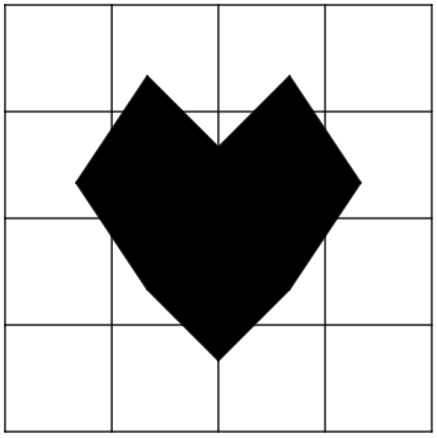


Cómo lo hacemos?

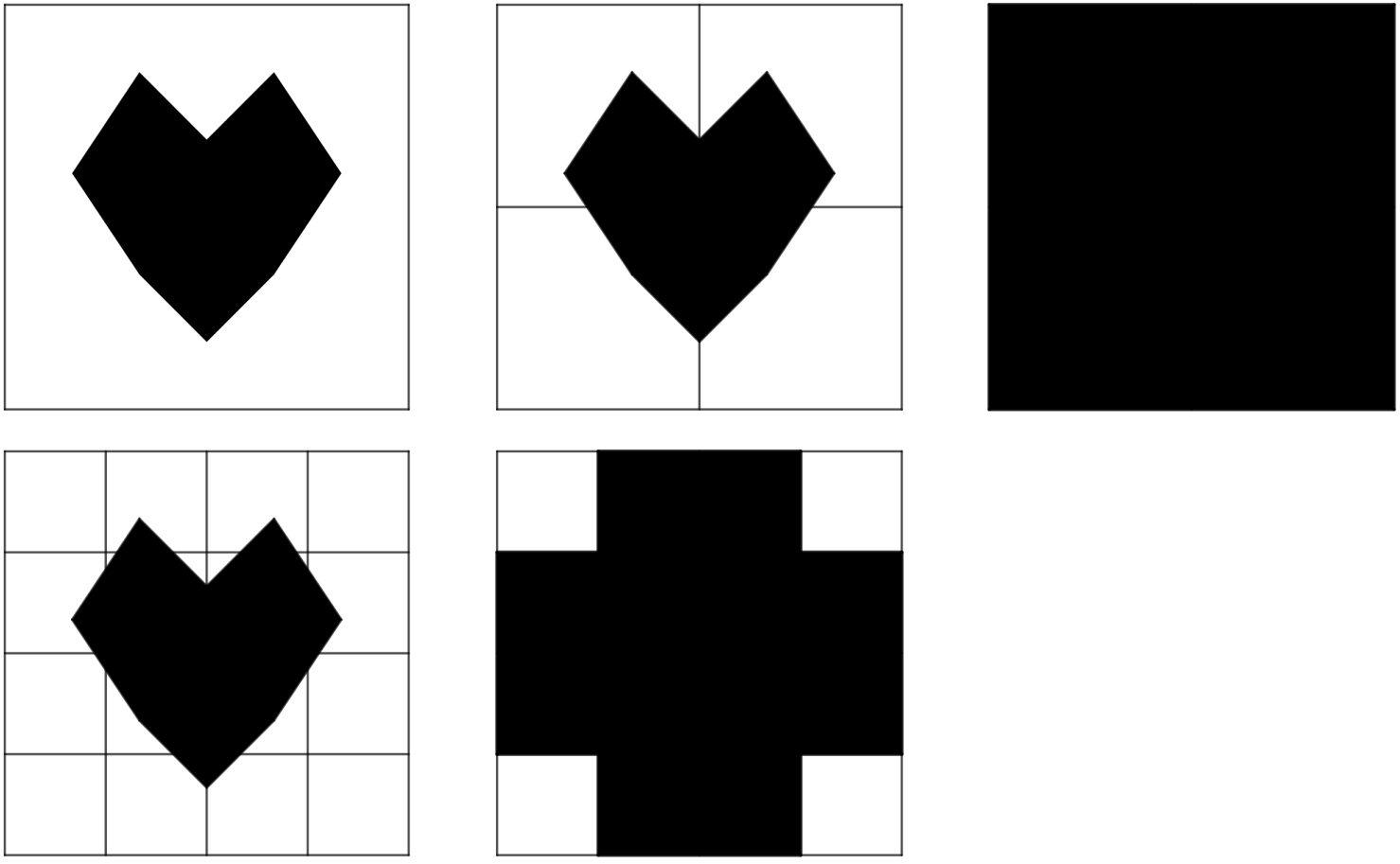


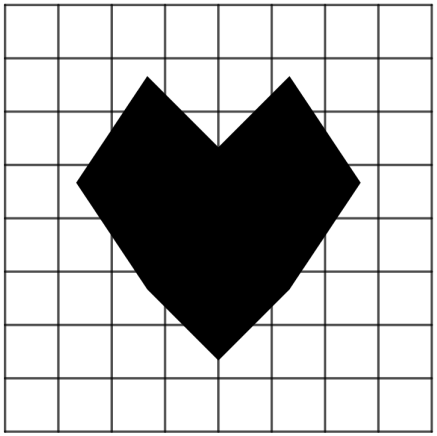


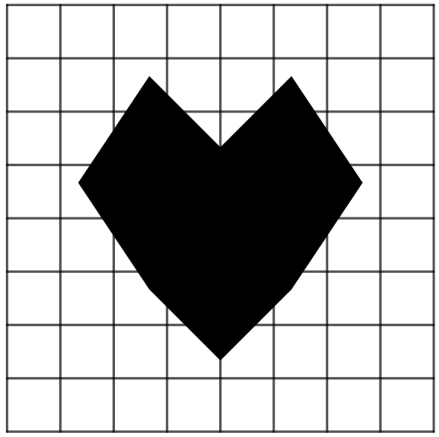


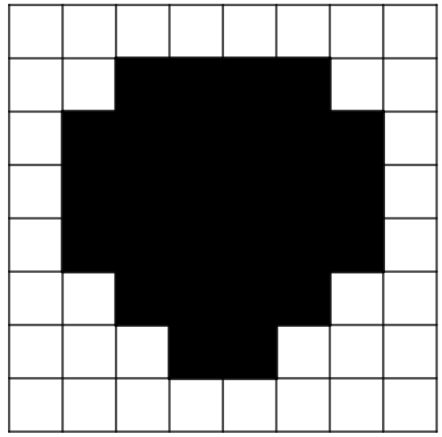


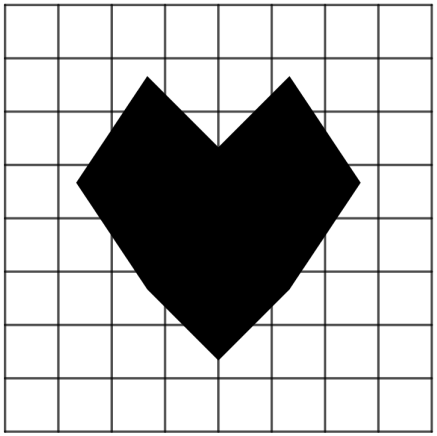
Cómo lo hacemos?

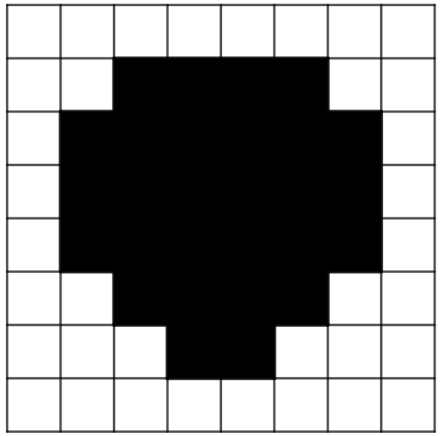


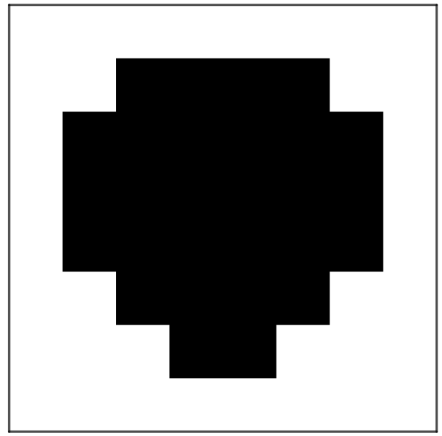


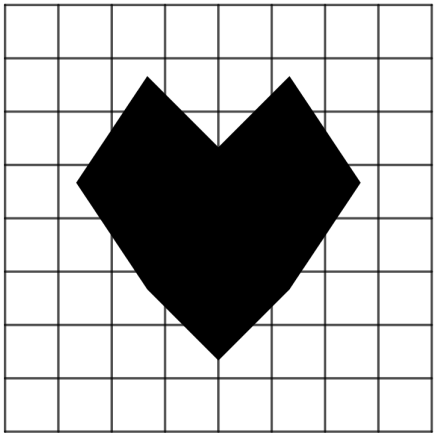


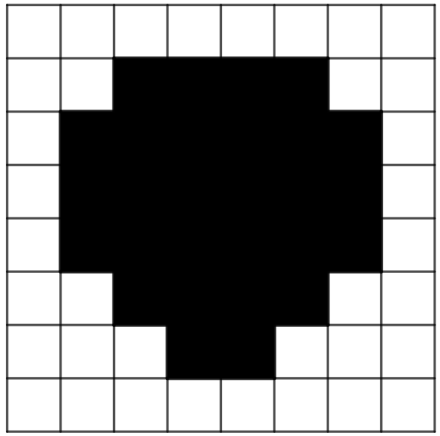


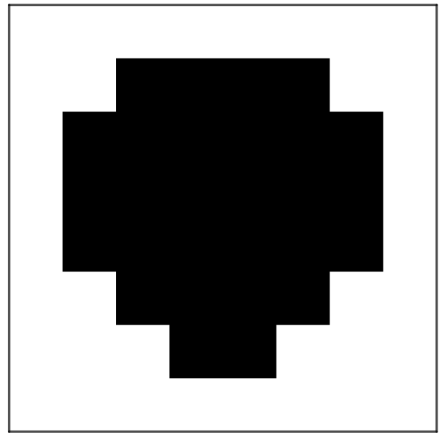


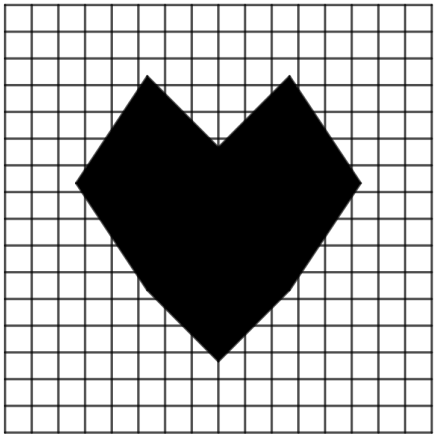


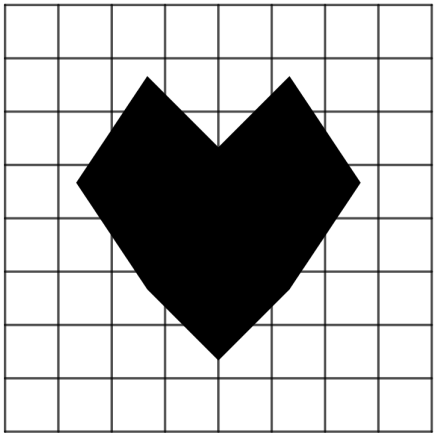


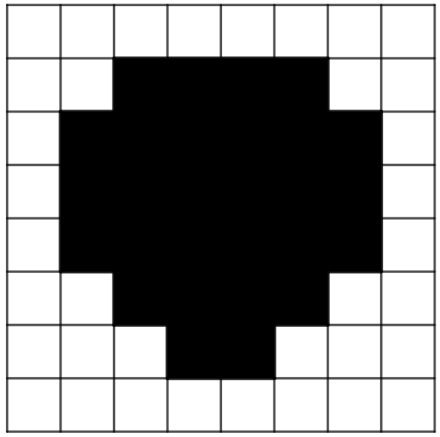


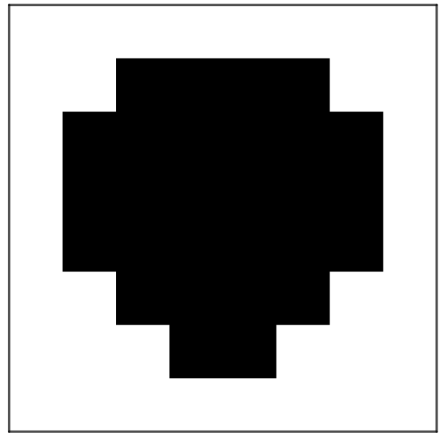


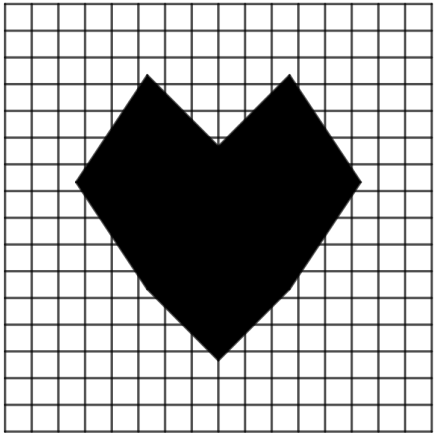


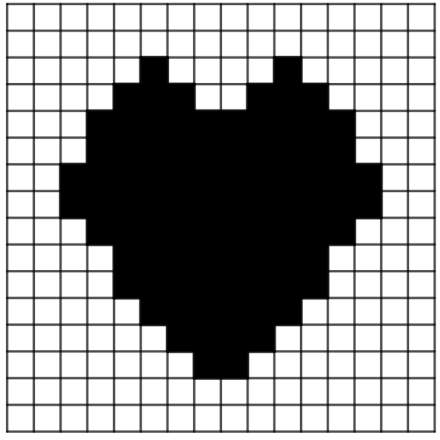


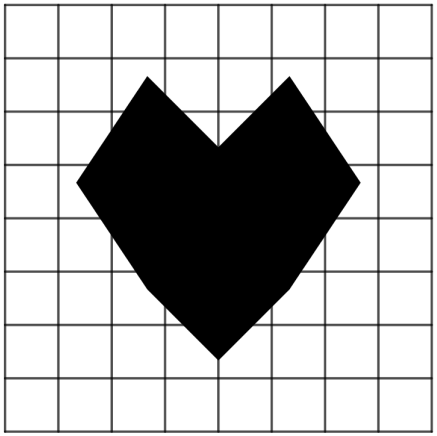
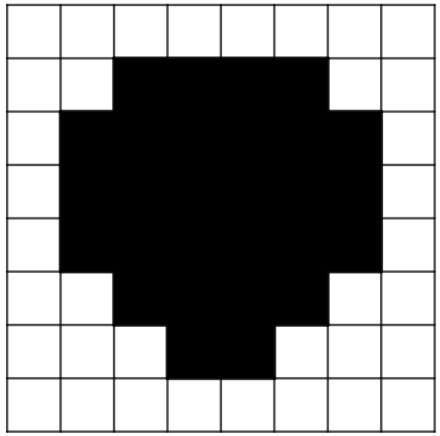
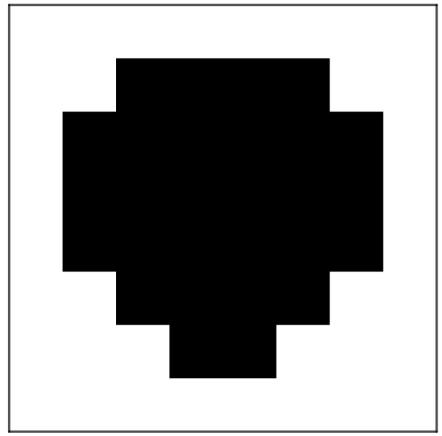
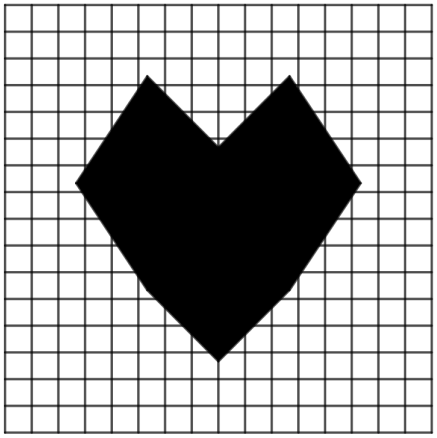
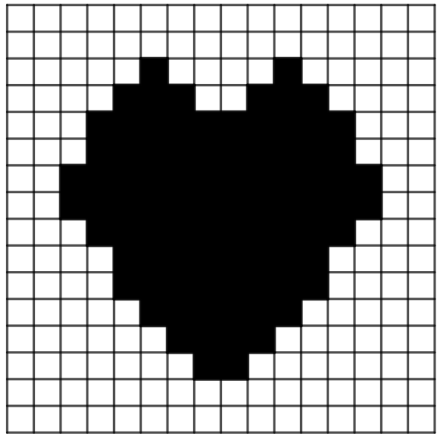
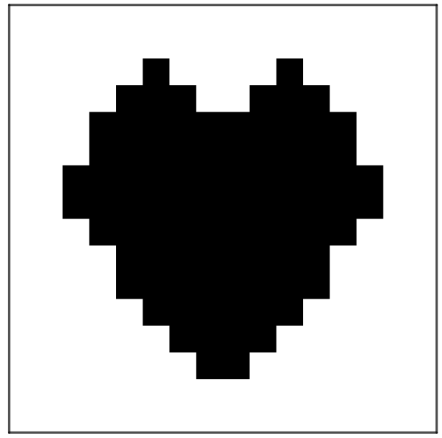


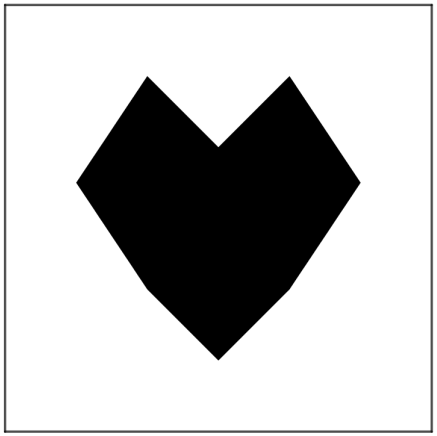


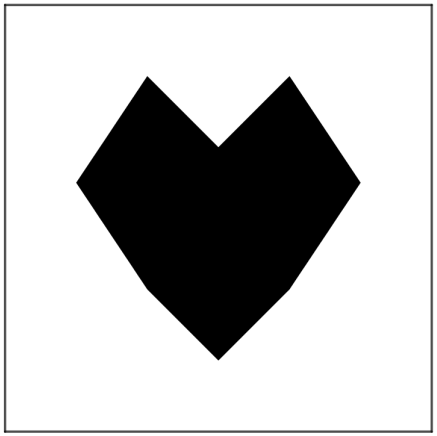


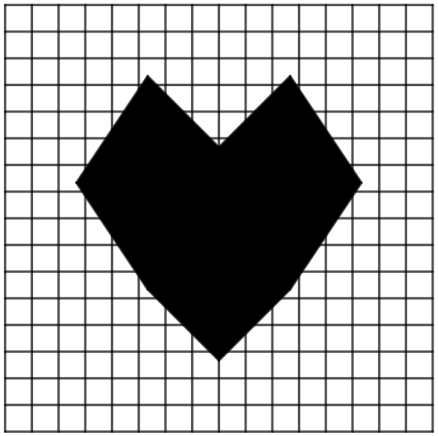


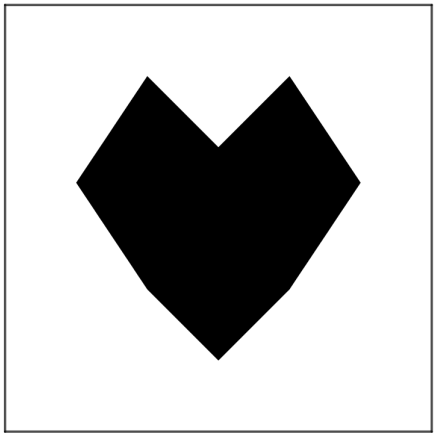


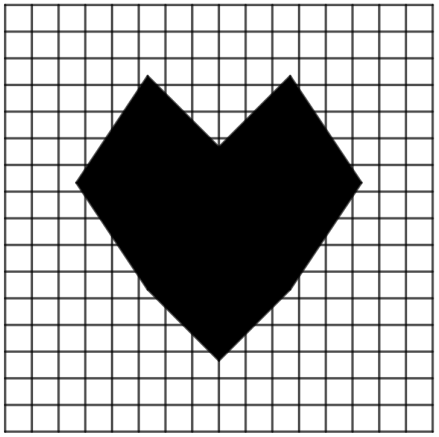







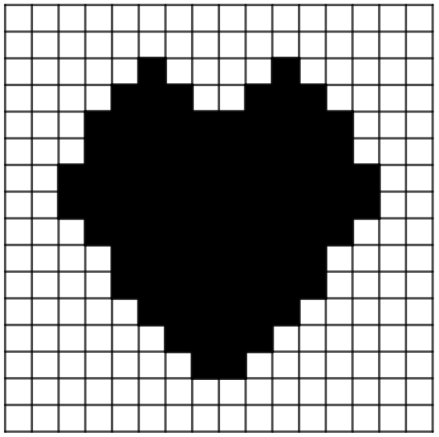


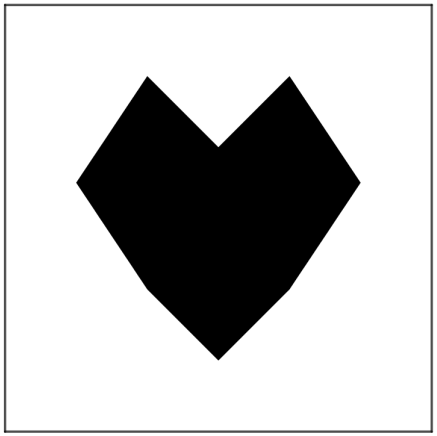


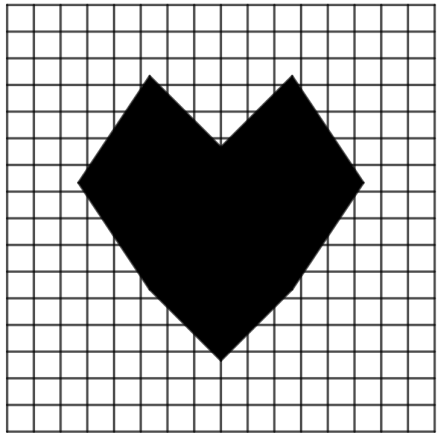


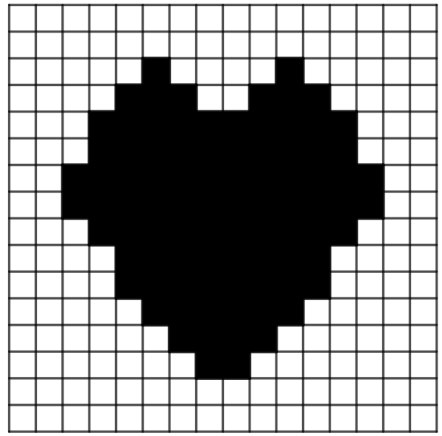


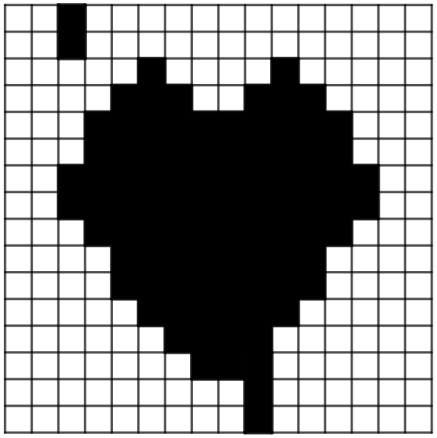


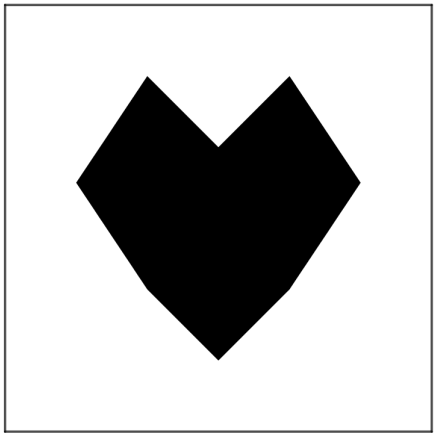
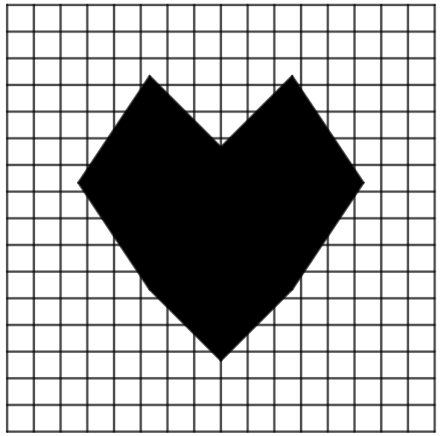
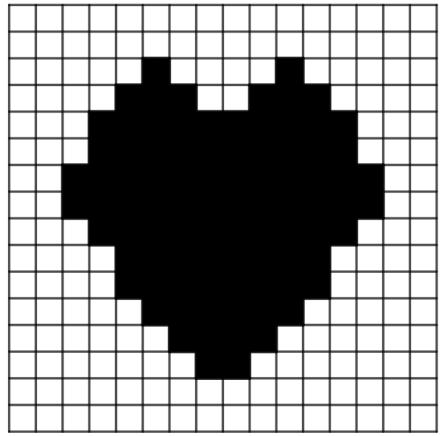
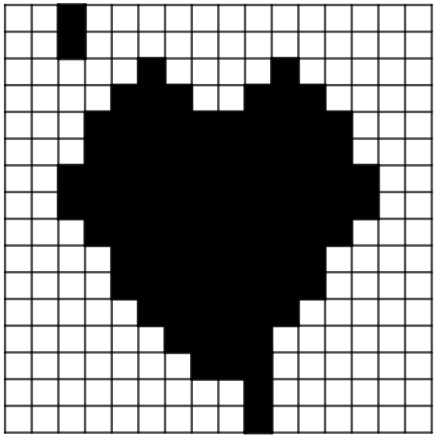
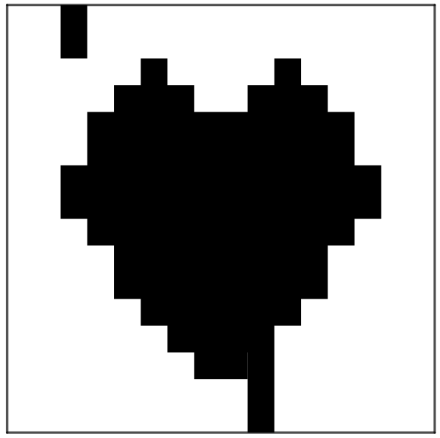










Ejemplo: $\mathcal{C} = \{0, 1\}$

Ejemplo: $\mathcal{C} = \{0, 1\}$

Mensaje ‘blanco’ o ‘negro’

Ejemplo: $\mathcal{C} = \{0, 1\}$

Mensaje ‘blanco’ o ‘negro’

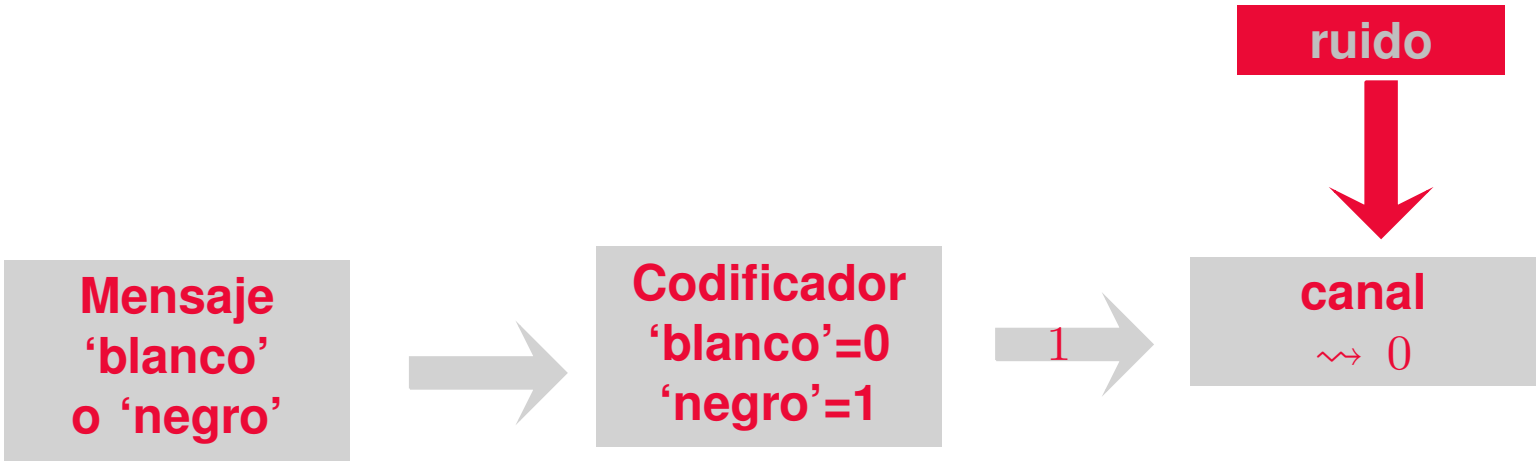
Ejemplo: $\mathcal{C} = \{0, 1\}$

Mensaje
‘blanco’
o ‘negro’

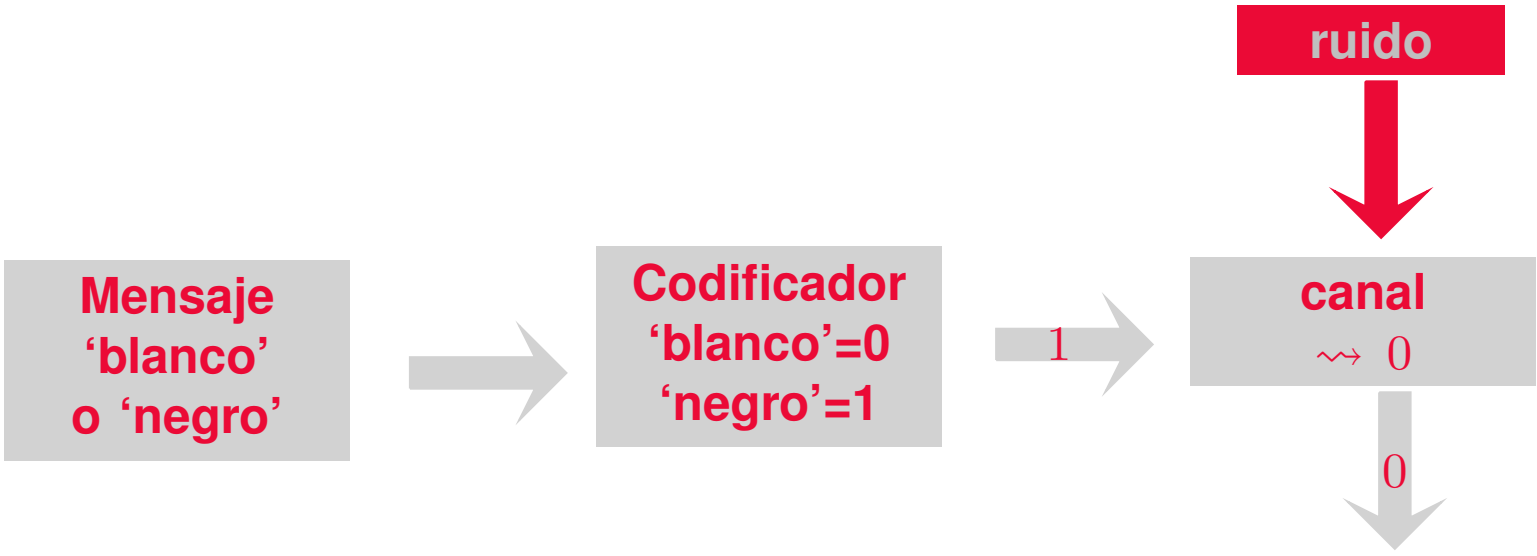
Codificador
‘blanco’=0
‘negro’=1

Ejemplo: $\mathcal{C} = \{0, 1\}$

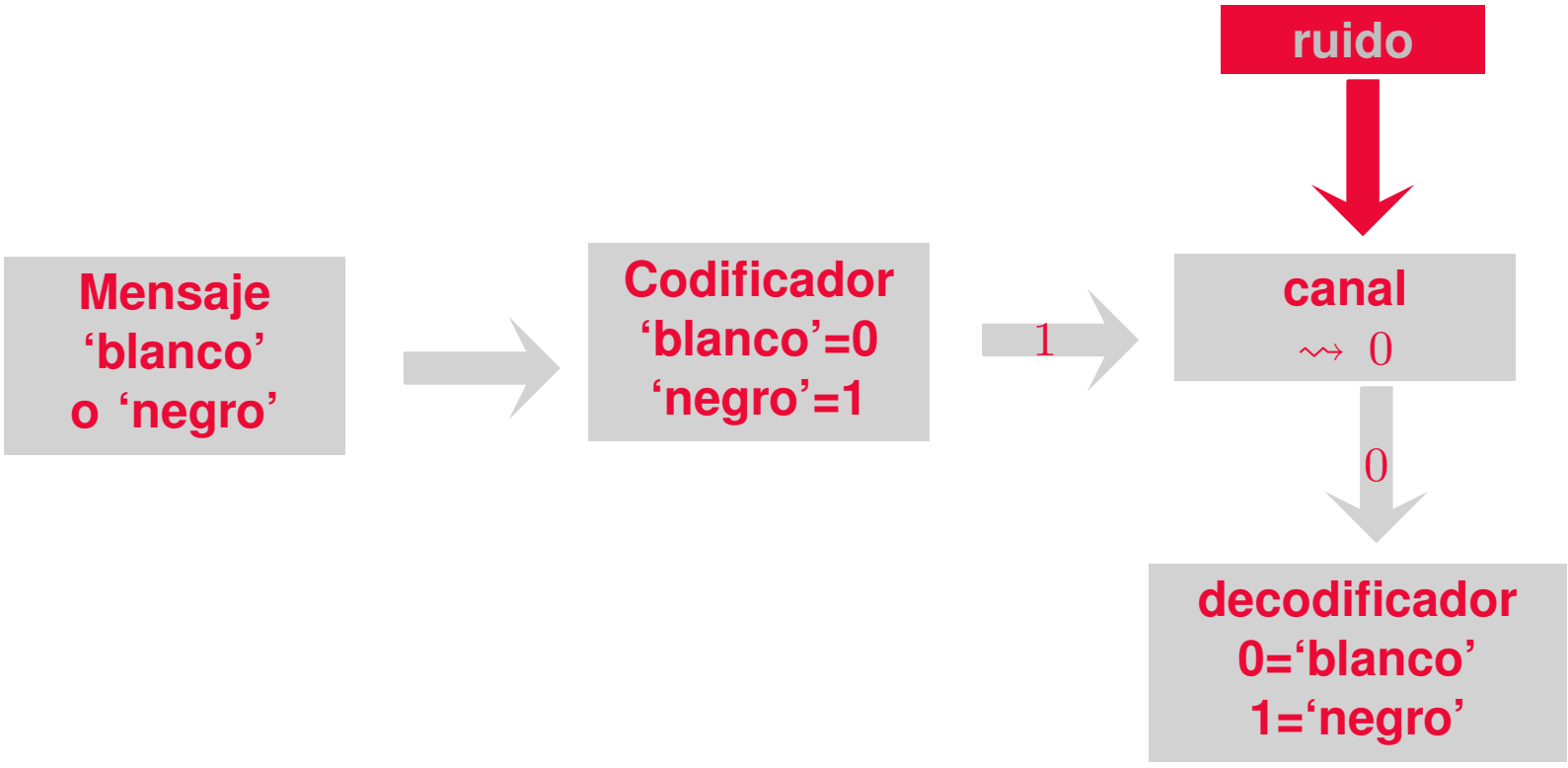
Ejemplo: $\mathcal{C} = \{0, 1\}$



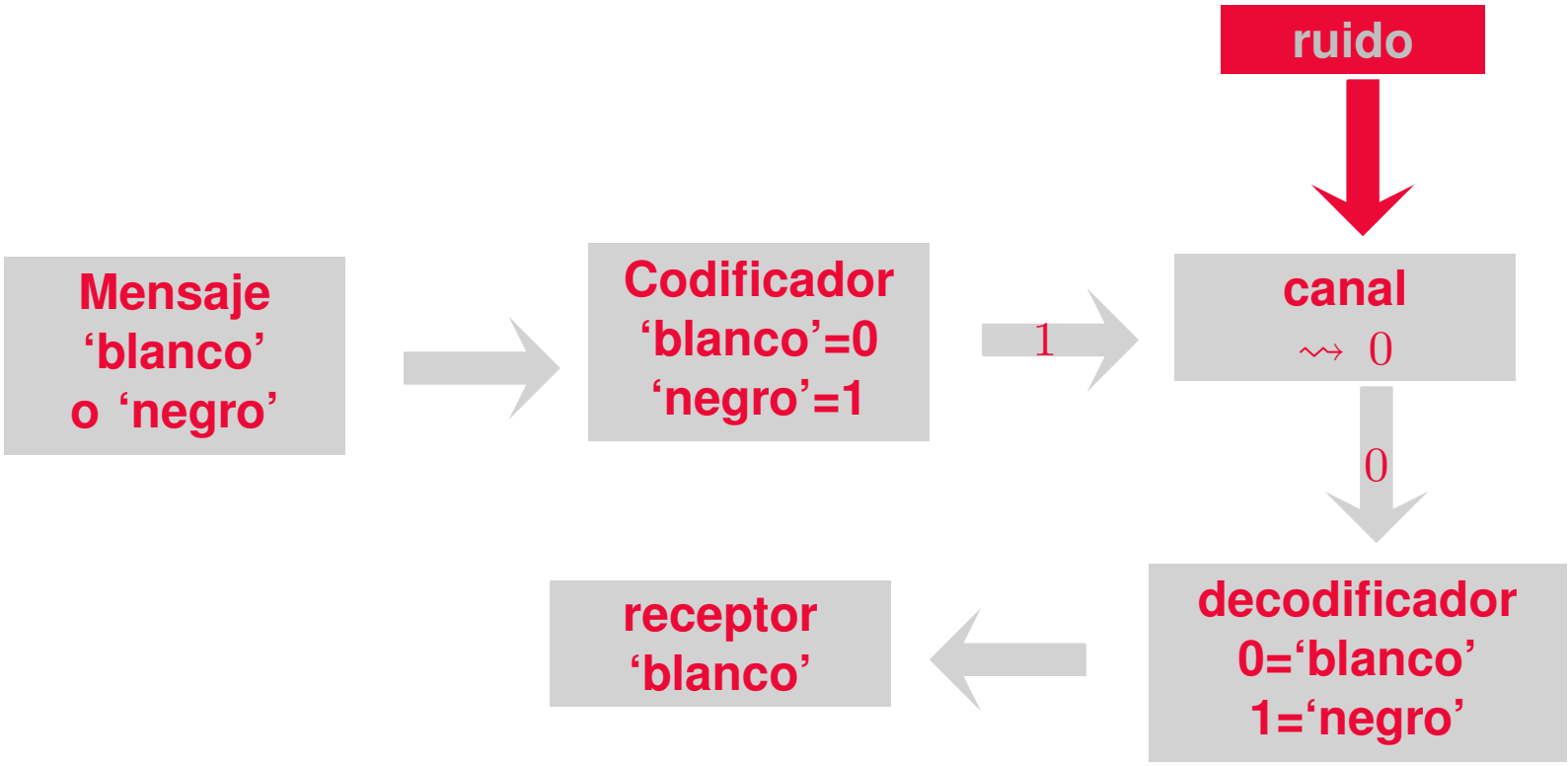
Ejemplo: $\mathcal{C} = \{0, 1\}$



Ejemplo: $\mathcal{C} = \{0, 1\}$



Ejemplo: $\mathcal{C} = \{0, 1\}$



Ejemplo: $\mathcal{C} = \{00, 11\}$

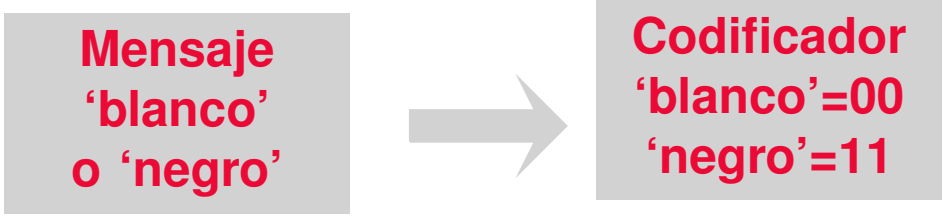
Ejemplo: $\mathcal{C} = \{00, 11\}$

Mensaje ‘blanco’ o ‘negro’

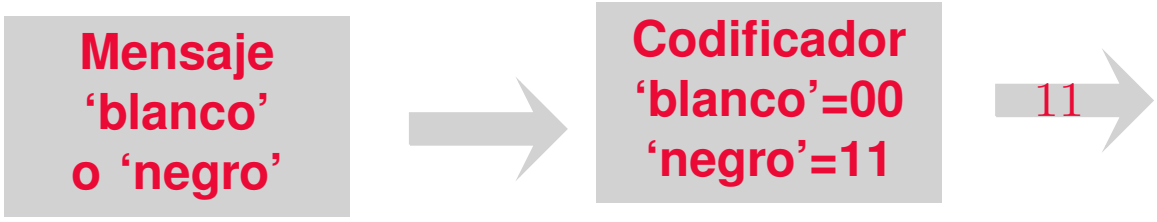
Ejemplo: $\mathcal{C} = \{00, 11\}$

Mensaje ‘blanco’ o ‘negro’

Ejemplo: $\mathcal{C} = \{00, 11\}$

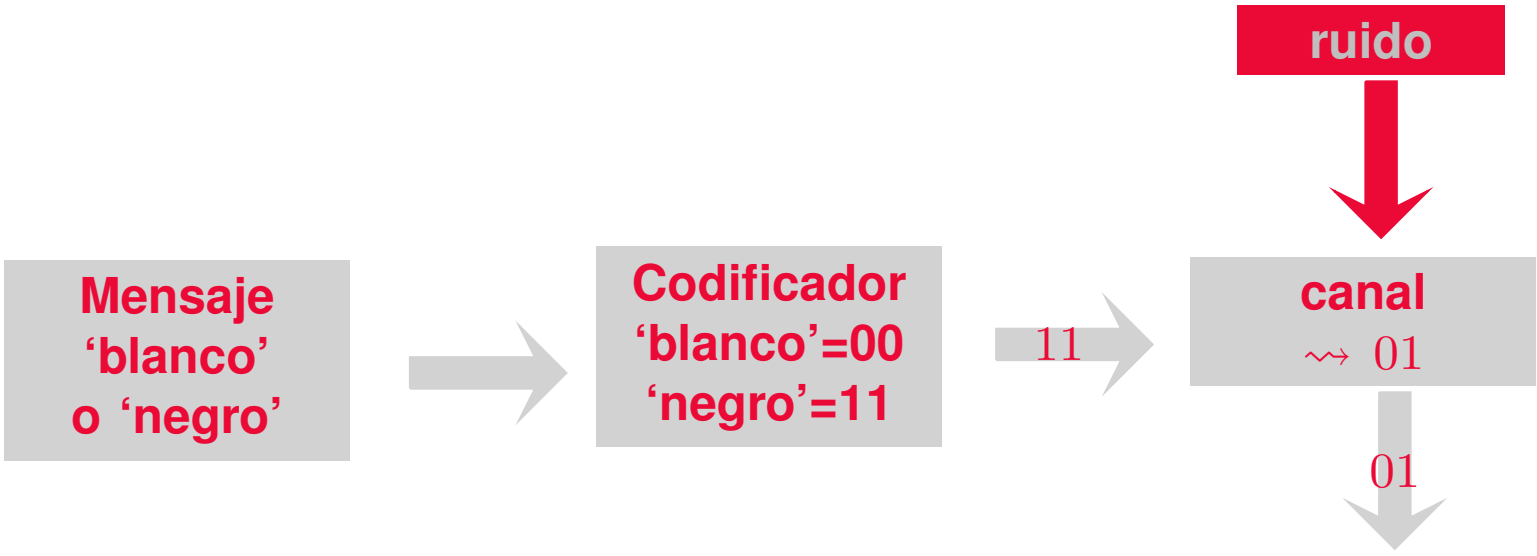


Ejemplo: $\mathcal{C} = \{00, 11\}$

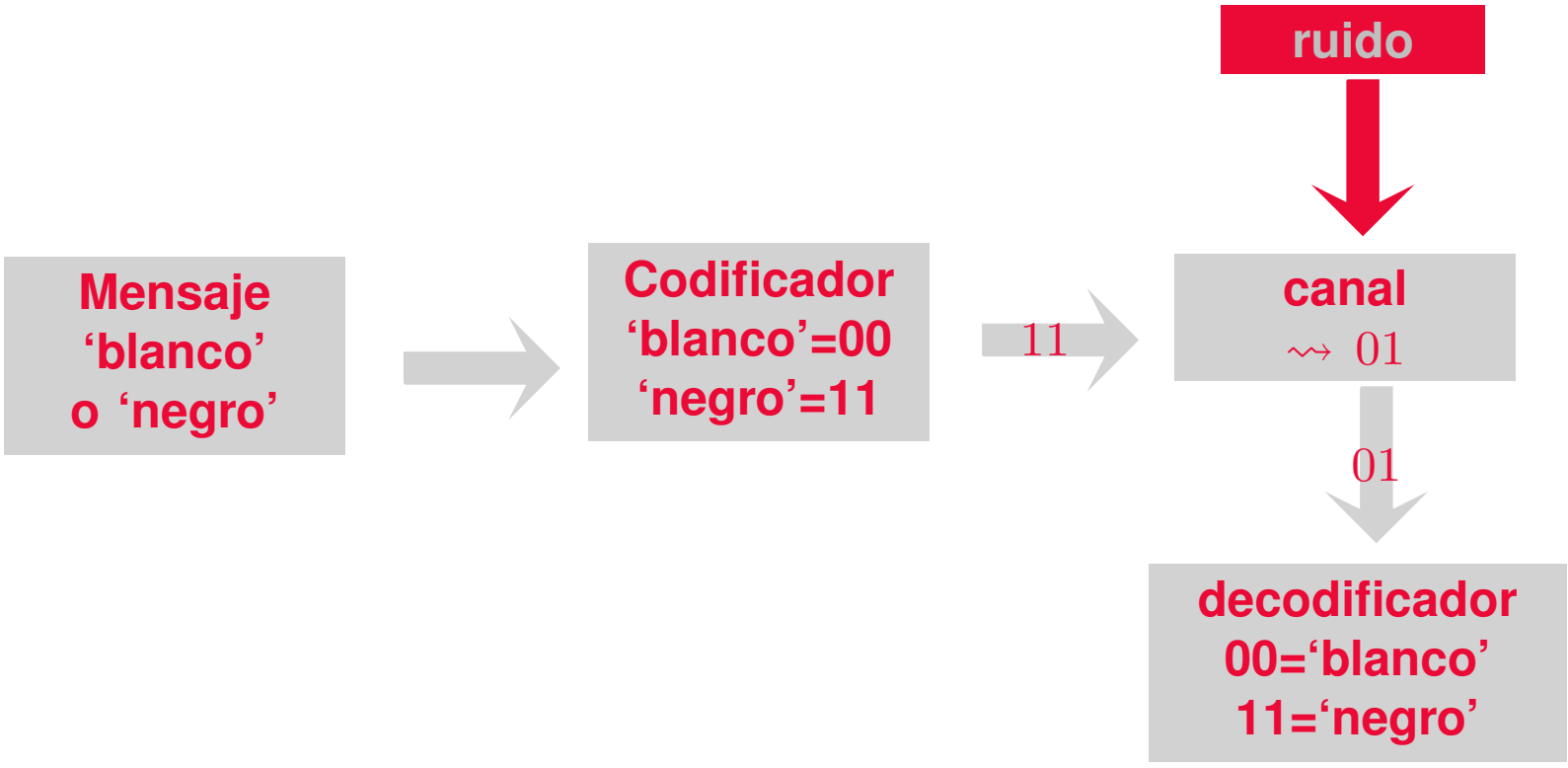


Ejemplo: $\mathcal{C} = \{00, 11\}$

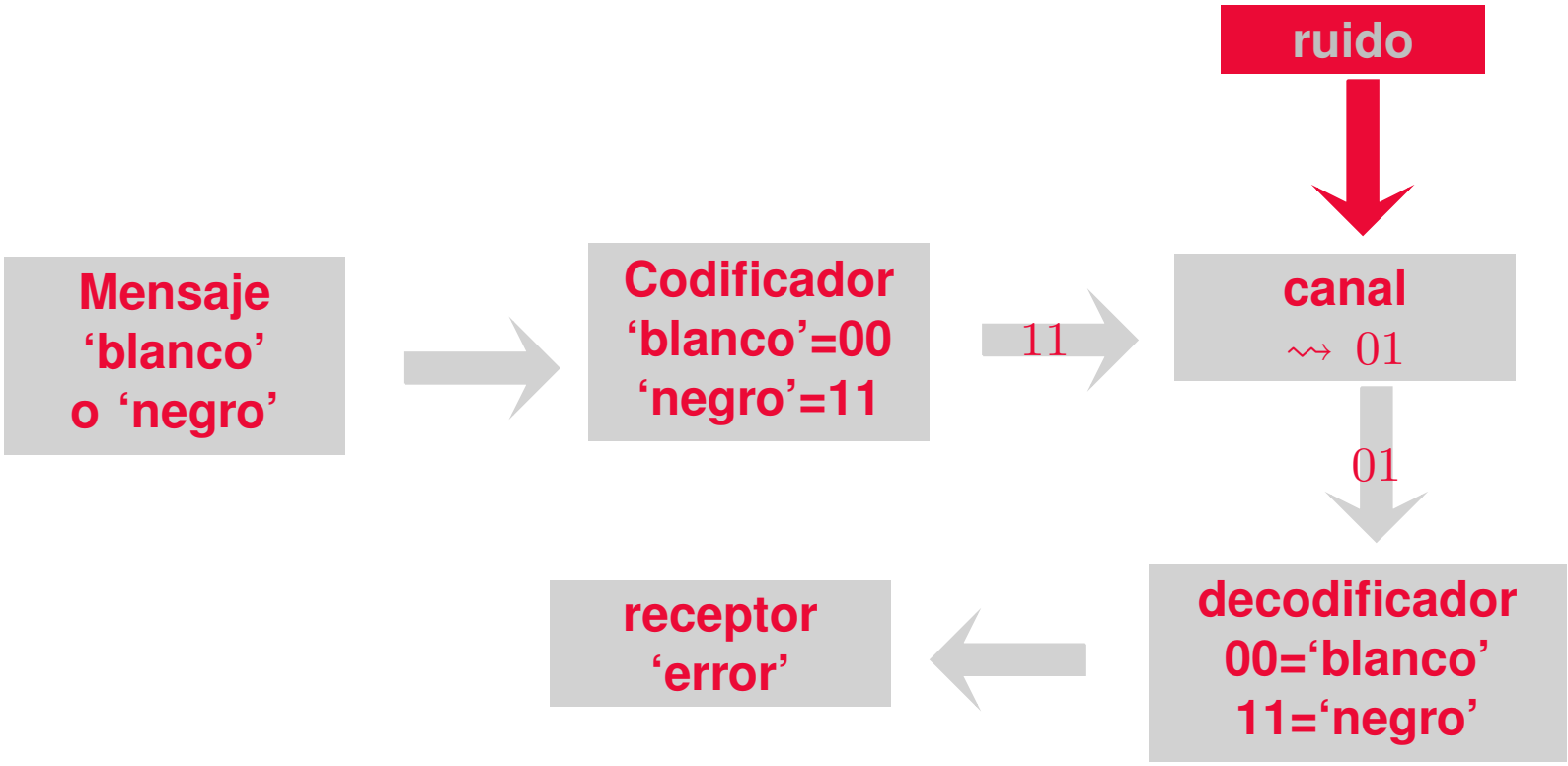
Ejemplo: $\mathcal{C} = \{00, 11\}$



Ejemplo: $\mathcal{C} = \{00, 11\}$



Ejemplo: $\mathcal{C} = \{00, 11\}$



Ejemplo: $\mathcal{C} = \{000, 111\}$

Ejemplo: $\mathcal{C} = \{000, 111\}$

Mensaje ‘blanco’ o ‘negro’

Ejemplo: $\mathcal{C} = \{000, 111\}$

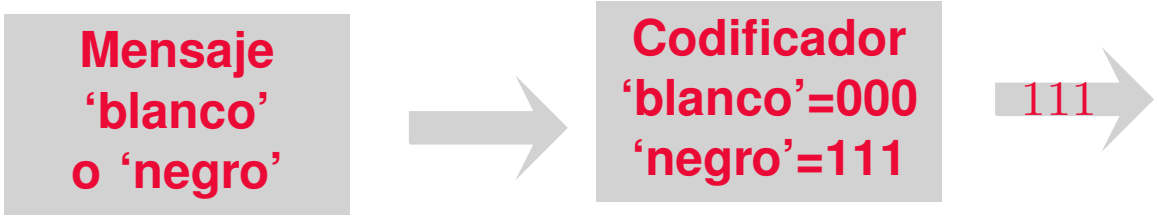
Mensaje ‘blanco’ o ‘negro’

Ejemplo: $\mathcal{C} = \{000, 111\}$

Mensaje
‘blanco’
o ‘negro’

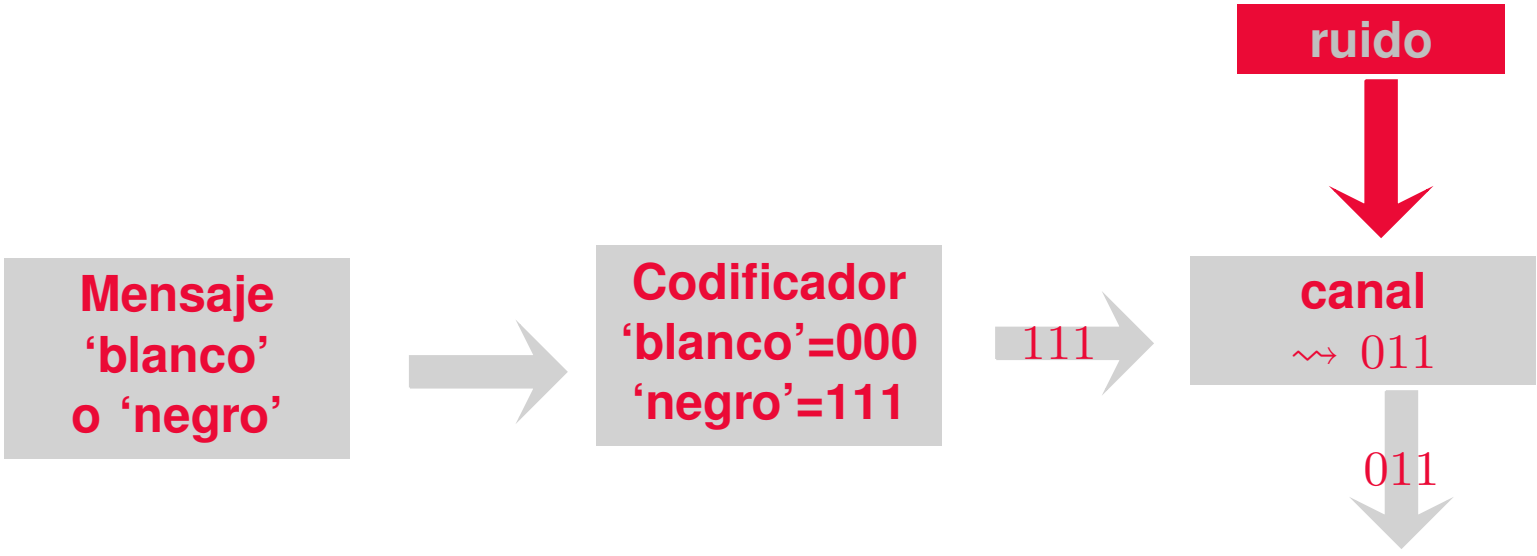
Codificador
‘blanco’=000
‘negro’=111

Ejemplo: $\mathcal{C} = \{000, 111\}$

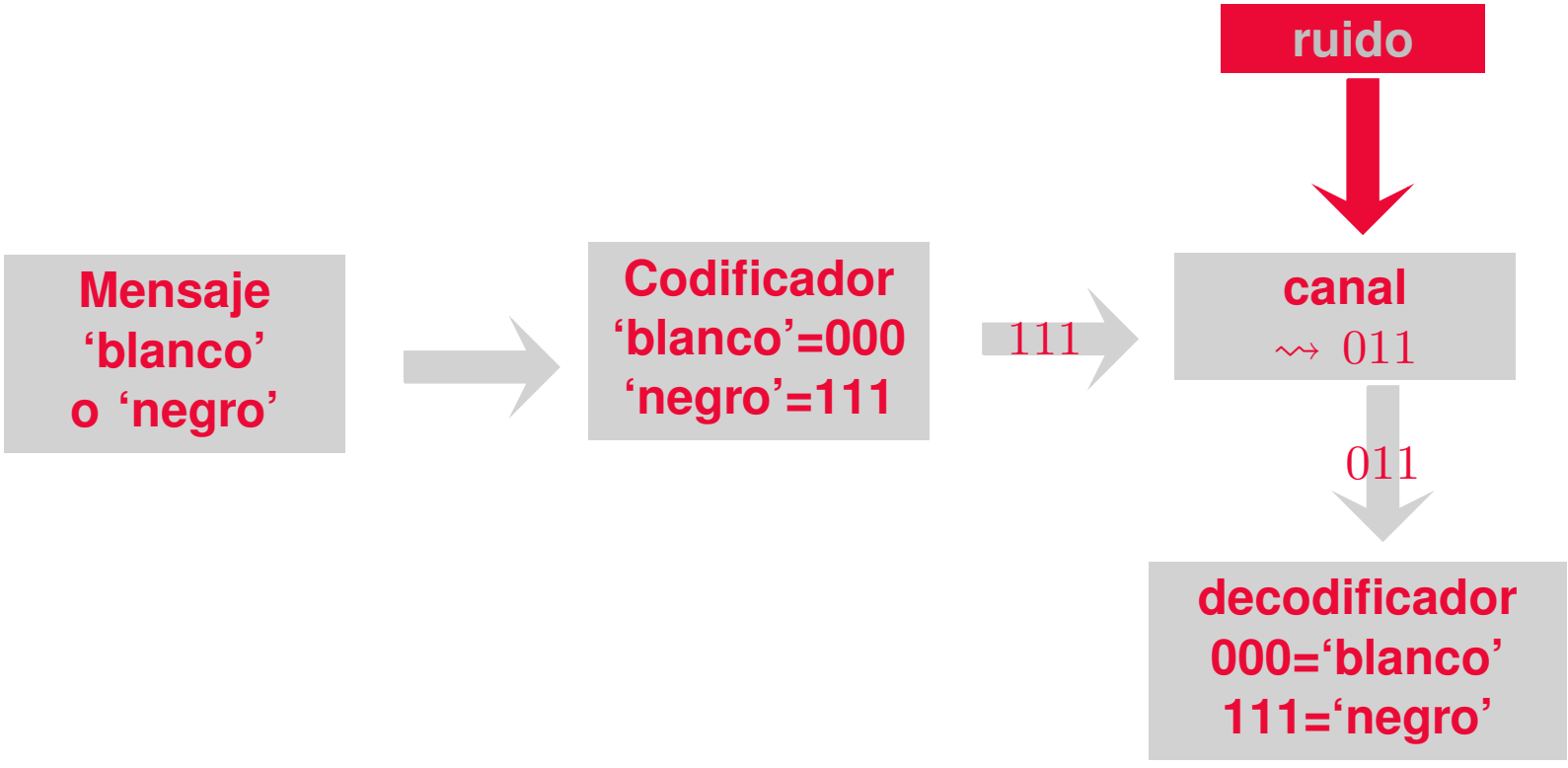


Ejemplo: $\mathcal{C} = \{000, 111\}$

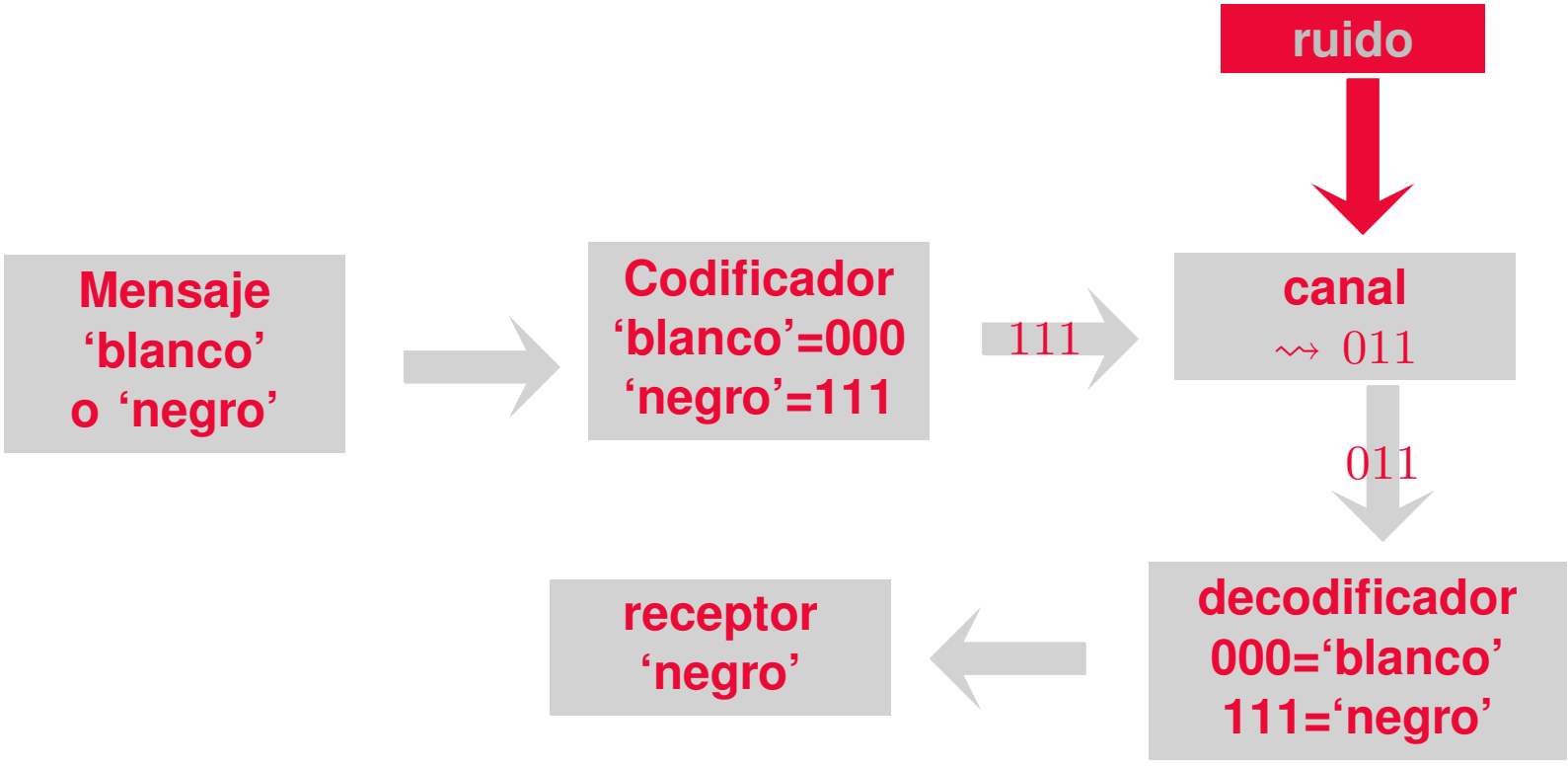
Ejemplo: $\mathcal{C} = \{000, 111\}$



Ejemplo: $\mathcal{C} = \{000, 111\}$



Ejemplo: $\mathcal{C} = \{000, 111\}$



.

- Un (n, M)-**código** $\mathcal{C}$ sobre un conjunto finito $\mathcal{A}$ es un subconjunto de $\mathcal{A}^n$ con M elementos. Decimos que $\mathcal{A}$ es el **alfabeto**.

- Un (n, M)-**código** $\mathcal{C}$ sobre un cuerpo finito $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ con M elementos. Decimos que $\mathbb{F}_q$ es el **alfabeto**.

- Un (n, M)-**código** $\mathcal{C}$ sobre un cuerpo finito $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ con M elementos. Decimos que $\mathbb{F}_q$ es el **alfabeto**.
- Los elementos de $\mathbb{F}_q^n$ se llaman **palabras** y los elementos de $\mathcal{C}$ se llaman **palabras código**.

- Un (n, M)-**código** $\mathcal{C}$ sobre un cuerpo finito $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ con M elementos. Decimos que $\mathbb{F}_q$ es el **alfabeto**.
- Los elementos de $\mathbb{F}_q^n$ se llaman **palabras** y los elementos de $\mathcal{C}$ se llaman **palabras código**.
- Para $a = (a_1, a_2, \ldots, a_n)$ y $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$ sea

$$d(a, b) = |\{i : 1 \leq i \leq n,\ a_i \neq b_i\}|.$$

  Esta función d se llama **distancia de Hamming** en $\mathbb{F}_q^n$.

- Un (n, M)-**código** $\mathcal{C}$ sobre un cuerpo finito $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ con M elementos. Decimos que $\mathbb{F}_q$ es el **alfabeto**.
- Los elementos de $\mathbb{F}_q^n$ se llaman **palabras** y los elementos de $\mathcal{C}$ se llaman **palabras código**.
- Para $a = (a_1, a_2, \ldots, a_n)$ y $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$ sea

$$d(a, b) = |\{i : 1 \leq i \leq n,\ a_i \neq b_i\}|.$$

  Esta función d se llama **distancia de Hamming** en $\mathbb{F}_q^n$.
- El **peso** de un elemento $a \in \mathbb{F}_q^n$ está definido como

$$w(a) := d(a, 0) = |\{i : 1 \leq i \leq n,\ a_i \neq 0\}|.$$

- Un (n, M)-**código** $\mathcal{C}$ sobre un cuerpo finito $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ con M elementos. Decimos que $\mathbb{F}_q$ es el **alfabeto**.
- Los elementos de $\mathbb{F}_q^n$ se llaman **palabras** y los elementos de $\mathcal{C}$ se llaman **palabras código**.
- Para $a = (a_1, a_2, \ldots, a_n)$ y $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$ sea

$$d(a, b) = |\{i : 1 \leq i \leq n,\ a_i \neq b_i\}|.$$

  Esta función d se llama **distancia de Hamming** en $\mathbb{F}_q^n$.
- El **peso** de un elemento $a \in \mathbb{F}_q^n$ está definido como

$$w(a) := d(a, 0) = |\{i : 1 \leq i \leq n,\ a_i \neq 0\}|.$$

- Por ejemplo

$$d((00000), (01010)) = 2$$

  mientras que

$$w((00000)) = 0 \qquad \text{y} \qquad w((01010)) = 2.$$

- Un (n, M)-**código** $\mathcal{C}$ sobre $\mathbb{F}_q$ es un subconjunto de $\mathbb{F}_q^n$ con M elementos. Decimos que $\mathbb{F}_q$ es el **alfabeto**.
- Los elementos de $\mathbb{F}_q^n$ se llaman **palabras** y los elementos de $\mathcal{C}$ se llaman **palabras código**.
- Para $a = (a_1, a_2, \ldots, a_n)$ y $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$ sea

$$d(a, b) = |\{i : 1 \leq i \leq n,\ a_i \neq b_i\}|.$$

  Esta función d se llama **distancia de Hamming** en $\mathbb{F}_q^n$.
- El **peso** de un elemento $a \in \mathbb{F}_q^n$ está definido como

$$w(a) := d(a, 0) = |\{i : 1 \leq i \leq n,\ a_i \neq 0\}|.$$

Obs.: La distancia de Hamming es una métrica en $\mathbb{F}_q^n$.

- La **distancia mínima** $d(\mathcal{C})$ de un código $\mathcal{C}$ es la menor distancia de Hamming entre palabras código distintas, es decir,

$$d(\mathcal{C}) = \min\{d(x, y) : x \in \mathcal{C},\ y \in \mathcal{C},\ x \neq y\}.$$

- La **distancia mínima** $d(\mathcal{C})$ de un código $\mathcal{C}$ es la menor distancia de Hamming entre palabras código distintas, es decir,

$$d(\mathcal{C}) = \min\{d(x, y) : x \in \mathcal{C},\ y \in \mathcal{C},\ x \neq y\}.$$

- Si un código $\mathcal{C}$ tiene M palabras de longitud n y distancia mínima d decimos que $\mathcal{C}$ es un (n, M, d)-código.

- La **distancia mínima** $d(\mathcal{C})$ de un código $\mathcal{C}$ es la menor distancia de Hamming entre palabras código distintas, es decir,

$$d(\mathcal{C}) = \min\{d(x, y) : x \in \mathcal{C},\ y \in \mathcal{C},\ x \neq y\}.$$

- Si un código $\mathcal{C}$ tiene M palabras de longitud n y distancia mínima d decimos que $\mathcal{C}$ es un (n, M, d)-código.

- Por ejemplo, la nave espacial Mariner 9 utilizó, para trasmitir fotografías de Marte, un $(32, 64, 16)-$código binario.

- La **distancia mínima** $d(\mathcal{C})$ de un código $\mathcal{C}$ es la menor distancia de Hamming entre palabras código distintas, es decir,

$$d(\mathcal{C}) = \min\{d(x, y) : x \in \mathcal{C},\ y \in \mathcal{C},\ x \neq y\}.$$

- Si un código $\mathcal{C}$ tiene M palabras de longitud n y distancia mínima d decimos que $\mathcal{C}$ es un (n, M, d)-código.

- Por ejemplo, la nave espacial Mariner 9 utilizó, para trasmitir fotografías de Marte, un $(32, 64, 16)-$código binario.

- $C = \{(0000000), (0001111), (0010101), (0011010), (0100110), (0101001), (0110011), (0111100), (1000011), (1001100), (1010110), (1011001), (1100101), (1101010), (1110000), (1111111)\}$.

  es un $(7, 16, 3)-$ código binario.

La distancia mínima determina la capacidad de corrección

La distancia mínima determina la capacidad de corrección

Teorema

Un código $\mathcal{C}$ con distancia mínima d puede:

(i) *detectar hasta $d-1$ errores;*

(ii) *corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores.*

La distancia mínima determina la capacidad de corrección

Teorema

Un código $\mathcal{C}$ con distancia mínima d puede:

(i) *detectar hasta $d-1$ errores;*

(ii) *corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores.*

Demostración

La distancia mínima determina la capacidad de corrección

Teorema

Un código $\mathcal{C}$ con distancia mínima d puede:

(i) *detectar hasta $d-1$ errores;*

(ii) *corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores.*

Demostración

(i) Supongamos que una palabra código x es transmitida y se recibe un vector y con a lo sumo $d-1$ errores. Entonces y no puede ser una palabra del código pues la distancia mínima de $\mathcal{C}$ es d y

$$d(x,y) \leq d-1 < d(\mathcal{C}).$$

Por lo tanto, se detectó que se han cometido errores en la transmisión.

La distancia mínima determina la capacidad de corrección

Teorema

Un código $\mathcal{C}$ con distancia mínima d puede:

(i) *detectar hasta $d-1$ errores;*

(ii) *corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores.*

Demostración

(ii) Sea $t = \lfloor \frac{d-1}{2} \rfloor$ y supongamos que una palabra código x es transmitida y se recibe un vector y con a lo sumo t errores. Entonces $d(x, y) \leq t$.

La distancia mínima determina la capacidad de corrección

Teorema

Un código $\mathcal{C}$ con distancia mínima d puede:

(i) *detectar hasta $d-1$ errores;*

(ii) *corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores.*

Demostración

(ii) Sea $t = \lfloor \frac{d-1}{2} \rfloor$ y supongamos que una palabra código x es transmitida y se recibe un vector y con a lo sumo t errores. Entonces $d(x,y) \leq t$. Si z es otra palabra código cualquiera, entonces como

$$d(x,z) \leq d(x,y) + d(y,z)$$

tenemos que

$$d(y,z) \geq d(x,z) - d(x,y) \geq d - t > t$$

y por lo tanto, x es la palabra código más cercana a y.

Decodificación del vecino más cercano

Decodificar y como la palabra código x tal que $d(y, x)$ sea la menor posible:

- cada símbolo transmitido tiene la misma probabilidad p de ser recibido con error;
- si un símbolo es recibido con error, cada uno de los símbolos restantes tienen la misma probabilidad de ser el error.

Códigos Lineales

- Un **código lineal** $\mathcal{C}$ (sobre el alfabeto $\mathbb{F}_q$) es un subespacio lineal de $\mathbb{F}_q^n$.

Códigos Lineales

- Un **código lineal** $\mathcal{C}$ (sobre el alfabeto $\mathbb{F}_q$) es un subespacio lineal de $\mathbb{F}_q^n$.
- Decimos que n es la **longitud** del código y $\dim \mathcal{C}$ es la **dimensión** del código (como espacio vectorial sobre $\mathbb{F}_q$).

Códigos Lineales

- Un **código lineal** $\mathcal{C}$ (sobre el alfabeto $\mathbb{F}_q$) es un subespacio lineal de $\mathbb{F}_q^n$.
- Decimos que n es la **longitud** del código y $\dim \mathcal{C}$ es la **dimensión** del código (como espacio vectorial sobre $\mathbb{F}_q$).
- Un $[n, k]-$código $\mathcal{C}$ es un código lineal de longitud n y dimensión k.

Códigos Lineales

- Un **código lineal** $\mathcal{C}$ (sobre el alfabeto $\mathbb{F}_q$) es un subespacio lineal de $\mathbb{F}_q^n$.
- Decimos que n es la **longitud** del código y $\dim \mathcal{C}$ es la **dimensión** del código (como espacio vectorial sobre $\mathbb{F}_q$).
- Un $[n, k]-$código $\mathcal{C}$ es un código lineal de longitud n y dimensión k. Si d es la distancia mínima de $\mathcal{C}$ decimos que $\mathcal{C}$ es un $[n, k, d]-$código.
- Se dice que cada palabra de $\mathcal{C}$ contiene k símbolos de información y $n-k$ símbolos redundantes: el número k/n se llama tasa de transmisión de información de $\mathcal{C}$.

Códigos Lineales

- Un **código lineal** $\mathcal{C}$ (sobre el alfabeto $\mathbb{F}_q$) es un subespacio lineal de $\mathbb{F}_q^n$.
- Decimos que n es la **longitud** del código y $\dim \mathcal{C}$ es la **dimensión** del código (como espacio vectorial sobre $\mathbb{F}_q$).
- Un $[n,k]-$código $\mathcal{C}$ es un código lineal de longitud n y dimensión k. Si d es la distancia mínima de $\mathcal{C}$ decimos que $\mathcal{C}$ es un $[n,k,d]-$código.
- Se dice que cada palabra de $\mathcal{C}$ contiene k símbolos de información y $n-k$ símbolos redundantes: el número k/n se llama tasa de transmisión de información de $\mathcal{C}$.
- Uno de los objetivos principales de la teoría de códigos correctores de errores es encontrar *códigos buenos*, es decir, con buenos parámetro, que maximicen a la vez k/n y d/n.

Proposición (Cota de Singleton)

Para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

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

Proposición (Cota de Singleton)

Para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

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

- Los códigos cuyos parámetros verifican que $k + d = n + 1$ se denominan códigos MDS (códigos de distancia máxima separables).

Proposición (Cota de Singleton)

Para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

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

- Los códigos cuyos parámetros verifican que $k + d = n + 1$ se denominan códigos MDS (códigos de distancia máxima separables).
- En general es difícil encontrar cotas inferiores no triviales para la distancia mínima de un código o de una clase de códigos.

Proposición (Cota de Singleton)

Para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

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

Proposición (Cota de Singleton)

Para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

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

Demostración

Proposición (Cota de Singleton)

Para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

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

Demostración

- Consideremos el subespacio vectorial $E \subset \mathbb{F}_q^n$ dado por

$$E = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \ : \ a_i = 0 \text{ para todo } i \geq d\}$$

Proposición (Cota de Singleton)

Para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

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

Demostración

- Consideremos el subespacio vectorial $E \subset \mathbb{F}_q^n$ dado por

$$E = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \ : \ a_i = 0 \text{ para todo } i \geq d\}$$

Cada $a \in E$ tiene peso $w(a) \leq d - 1$, y por lo tanto $E \cap \mathcal{C} = \emptyset$.

Proposición (Cota de Singleton)

Para un $[n, k, d]-$código $\mathcal{C}$ se verifica que

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

Demostración

- Consideremos el subespacio vectorial $E \subset \mathbb{F}_q^n$ dado por

$$E = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \ : \ a_i = 0 \text{ para todo } i \geq d\}$$

Cada $a \in E$ tiene peso $w(a) \leq d - 1$, y por lo tanto $E \cap \mathcal{C} = \emptyset$. Como $\dim E = d - 1$ tenemos que

$$k+(d-1) = \dim \mathcal{C}+\dim E = \dim(\mathcal{C}+E)+\dim(\mathcal{C}\cap E) = \dim(E+\mathcal{C}) \leq n.$$

Matriz generadora de un código $\mathcal{C}$

Matriz generadora de un código $\mathcal{C}$

- Dada una base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de un $[n, k]-$código $\mathcal{C}$ definimos la matriz generadora G del código $G_{k \times n}$ como la matriz cuyas filas son los vectores v_i de la base.

Matriz generadora de un código $\mathcal{C}$

- Dada una base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de un $[n, k]-$código $\mathcal{C}$ definimos la matriz generadora G del código $G_{k \times n}$ como la matriz cuyas filas son los vectores v_i de la base.

- G depende de la base elegida.

Matriz generadora de un código $\mathcal{C}$

- Dada una base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de un $[n, k]-$código $\mathcal{C}$ definimos la matriz generadora G del código $G_{k \times n}$ como la matriz cuyas filas son los vectores v_i de la base.

- G depende de la base elegida.

- Dos matrices equivalentes por filas definen el mismo código.

Matriz generadora de un código $\mathcal{C}$

- Dada una base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de un $[n, k]-$código $\mathcal{C}$ definimos la matriz generadora G del código $G_{k\times n}$ como la matriz cuyas filas son los vectores v_i de la base.

- G depende de la base elegida.

- Dos matrices equivalentes por filas definen el mismo código.

- Decimos que una matriz generadora G de un código está en forma estándar si es de la forma

$$G = (I_k|A)$$

donde I_k es la matriz identidad de $k \times k$ y A es una matriz de $k \times n - k$.

Codificación y decodificación

Codificación y decodificación

Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ podemos definir una forma de codificar mensajes usando la matriz generadora G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \rightarrow & c = uG \end{array}$$

Codificación y decodificación

Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ podemos definir una forma de codificar mensajes usando la matriz generadora G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \rightarrow & c = uG \end{array}$$

- Ejemplo: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

Codificación y decodificación

Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ podemos definir una forma de codificar mensajes usando la matriz generadora G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \to & c = uG \end{array}$$

- Ejemplo: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

- Consideremos el $[4, 2]-$código binario $\mathcal{C}$ generado por la matriz

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Codificación y decodificación

Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ podemos definir una forma de codificar mensajes usando la matriz generadora G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \to & c = uG \end{array}$$

- Ejemplo: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

- Consideremos el $[4, 2]-$código binario $\mathcal{C}$ generado por la matriz

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

  Entonces $\mathcal{C} = \{(0000), (1011), (0101), (1110)\}$.

Si G está en forma estándar, entonces decodificar es trivial ya que en esta situación

$$u \in \mathbb{F}_q^k \quad \longrightarrow \quad c = uG = (u|uA) \in \mathbb{F}_q^n \quad \longrightarrow \quad u = c_{|_{\mathbb{F}_q^k}} \in \mathbb{F}_q^k.$$