ESTÍMULO DEL TALENTO MATEMÁTICO

ESTALMAT
Comunidad de Madrid

Transmitiendo mensajes

María Jesús Vázquez Gallo (UPM)/Pablo Fernández Gallardo (UAM)

Seminario Estalmat 05-04-2025

ESTÍMULO DEL TALENTO MATEMÁTICO

REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE ESPAÑA

UNIVERSIDAD COMPLUTENSE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

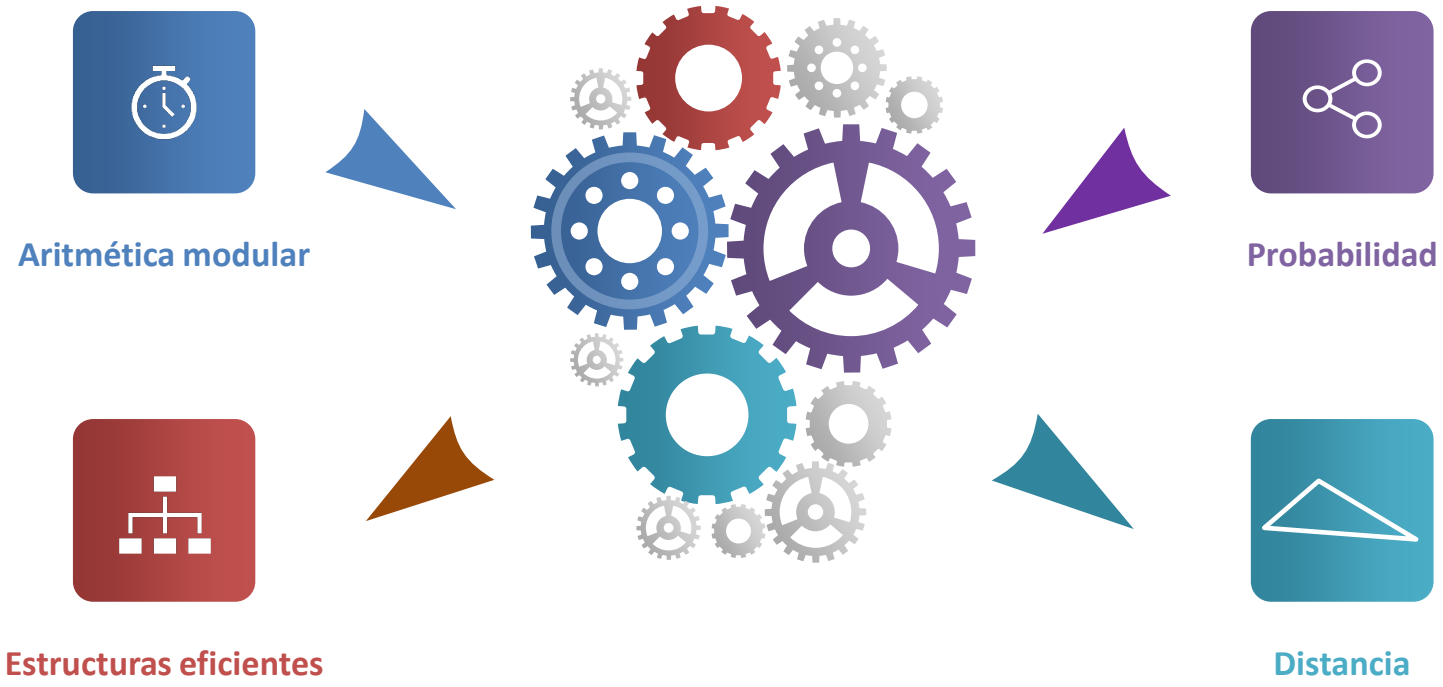
FECYT INNOVACIÓN

Purposeful Ventures

ESTALMAT
Comunidad de Madrid

Segundo año: A vueltas con el azar + **Transmitiendo mensajes**

$\approx 75\ min.$



ESTÍMULO DEL TALENTO MATEMÁTICO

Motivación

Imagina que tienes que transmitir instrucciones a un robot para que encienda o apague cierto sistema o para que se mueva en dirección Norte/Sur/Este/Oeste.

¿Cómo lo harías?

C. Shannon (1948):

unidad de información binaria: BIT *(binary digit)*

1 bit: 0, 1 — **2** posibles valores/mensajes

2 bits: 00, 01, 10, 11 — **4** posibles: 00, 01, 10, 11

…

8 bits (1 BYTE) → 256 mensajes

…

n bits → ¿cuántos posibles mensajes?

En la era de la transmisión de la información:
millones de dispositivos comunicándose a través de la red.
Compras, secretos, transacciones… **Ruidos, interferencias**…

Si se producen **errores** en la transmisión…

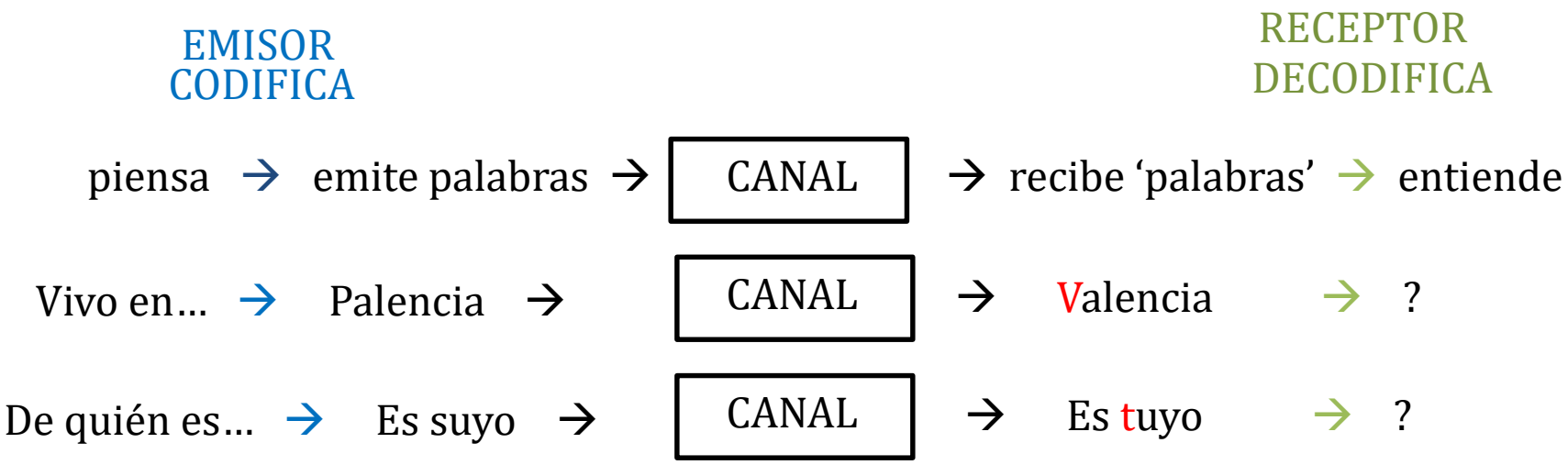
¿Cómo detectar errores automáticamente?
¿Y cómo corregirlos?

¿Cómo transmitir información de manera fiable y eficiente?

Ingeniero y matemático C. Shannon (trabajó para la telefónica Bell, hoy AT&T):
"Teoría matemática de la comunicación" en 1948.
(Internet nació hacia 1970!!!)

Ejemplos sencillos

Ejemplo: Al comunicarnos en un idioma usamos palabras del diccionario –código-.

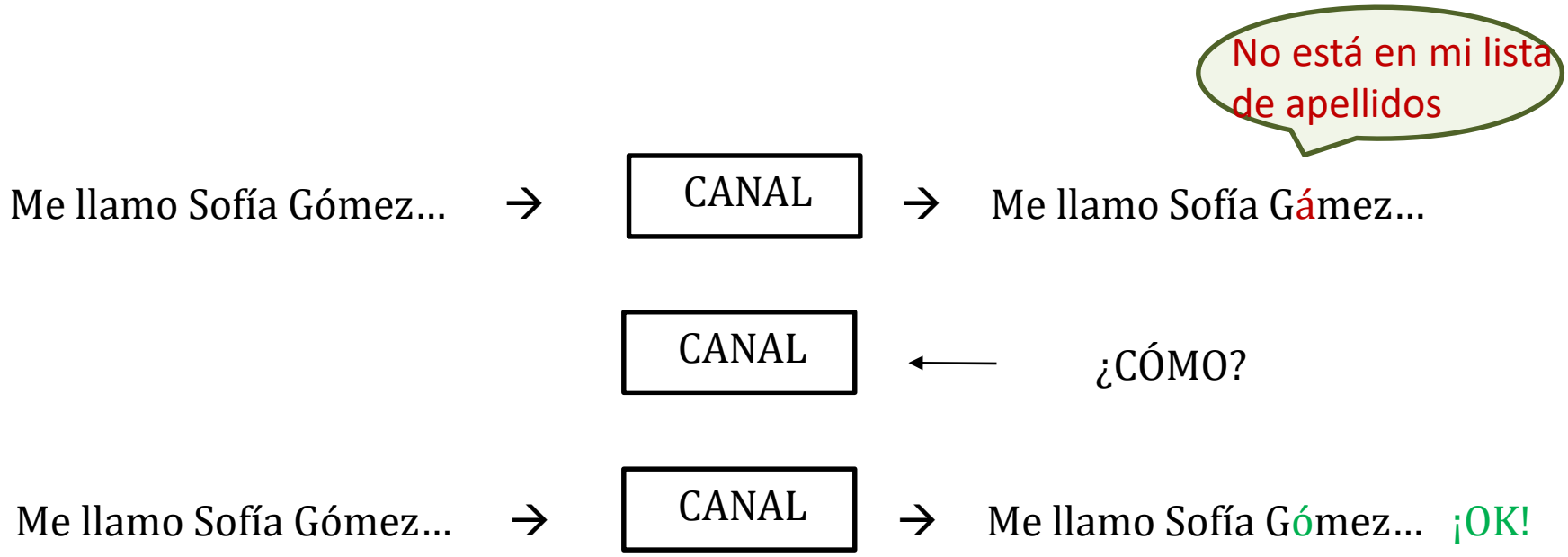


Queremos codificar y decodificar para detectar y corregir errores automáticamente

¿Cómo hacerlo?

Imagina que te han invitado a un concierto privado y tienes que dar tu nombre en la entrada…

¿Cómo detectamos y corregimos errores al comunicarnos?



Ideas del lenguaje común:

Detecta errores si una palabra no está en diccionario.

Corrige errores repitiendo, añadiendo redundancia.

Idea: ¡repetir!

- Codificar: 0 → 00, 1→11. **Código de repetición 2** : {00,11}

Detecta: No está en el diccionario

1101 → 11 11 00 11 → CANAL → 11 10 00 11 → 1 ? 0 1

codificación

¿Decodificación?

- Codificar: 0 → 000, 1→111. **Código de repetición 3** : {000,111}

Detecta: No está en el diccionario

1101 → 111 111 000 111 → CANAL → 111 110 000 111 → 1101

codificación

Decodificamos a la palabra más cercana

También en un idioma:

Mi bisidleta es negra…

Pues mi bicicleta es azul…

Idea: detectamos error si no está en diccionario y corregimos con la palabra más cercana.

¡Detección y corrección automática!

Ejercicio 1:

Código de repetición 3 para transmitir no (0) o sí (1).
¿Qué mensajes se pueden recibir? ¡Decodifícalos!

Ejercicio 1:

Código de repetición 3 para transmitir no (0) o sí (1).
¿Qué mensajes se pueden recibir? ¡Decodifícalos!

decodificación

000	→	000
100	→	000
010	→	000
001	→	000
110	→	111
101	→	111
011	→	111
111	→	111

¡OJO! Cuanta más repetición, mejor detección y corrección, pero ocupamos más espacio

ESTÍMULO DEL TALENTO MATEMÁTICO

ESTALMAT
Comunidad de Madrid

Reflexión

ESTÍMULO DEL TALENTO MATEMÁTICO

REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE ESPAÑA

UNIVERSIDAD COMPLUTENSE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

FECYT INNOVACIÓN

Purposeful Ventures

ESTALMAT
Comunidad de Madrid

¿Siempre podemos corregir con la palabra más cercana?

Me dejas tu cafa …

¿casa?, ¿caja?, ¿cama?, ¿gafa?…

Detectamos que ha habido un error pero
no siempre podemos corregir automáticamente

Idea: no sabemos corregir porque
hay varias palabras a *distancia mínima*
(y el contexto no decide).

Pero: ¿Y si se produce más de un error?
Si al codificar 1 bit con repetición 3, se recibe 110
¿decodificamos a 111 o a 000?

Incertidumbre… recuerda las ideas de probabilidad

Ejemplo: Sabemos que en cierto canal el 99% de los bits se transmiten correctamente.
Al aplicar un código de repetición 3 y decodificar a la palabra más cercana:

¿Nuevo porcentaje de transmisión correcta?

Ejemplo: Canal con **transmisión correcta del 99% de los bits**.

Sin código: Emitiendo

Probabilidad p: número entre 0 y 1

- **1 bit**: probabilidad(transmisión correcta)= **0.99**

  (probabilidad(error en 1 bit) $= 1 - 0.99 = 0.01 = p$).

- **100 bits**: transmisión correcta en los 100 bits

  $0.99^{100} \approx 0.3660 \rightarrow 36.60\%$

- **200 bits**: transmisión correcta en los 200 bits

  $0.99^{200} \approx 0.1334 \rightarrow 13.34\%$

Ejemplo: Canal con **transmisión correcta del 99% de los bits**.

Con código de repetición 3: Emitiendo

- **1 bit**: probabilidad(transmisión correcta)=

$$p(0\ errores) + p(1\ error^{*}) =$$

$$0.99^3 + 3\ 0.99^2\ 0.01 =$$

$$0.970299 + 0.029403 = 0.999702 \rightarrow \approx \mathbf{99.97\%}$$

* Decodificamos a la palabra más cercana.

- **100 bits**: transmisión correcta en los 100 bits

$$0.999702^{100} \approx 0.9706 \rightarrow \approx \mathbf{97.06\%}$$

- **200 bits**: transmisión correcta en los 200 bits

$$0.999702^{200} \approx 0.9421 \rightarrow \approx \mathbf{94.21\%}!!!$$

Mucho mejor que el $\approx 13.34\%$ *sin código*

ESTÍMULO DEL TALENTO MATEMÁTICO

ESTALMAT
Comunidad de Madrid

Buscando soluciones más eficientes

ESTÍMULO DEL TALENTO MATEMÁTICO
REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE ESPAÑA
UNIVERSIDAD COMPLUTENSE MADRID
FACULTAD DE CIENCIAS MATEMÁTICAS
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
FECYT INNOVACIÓN
Purposeful Ventures
ESTALMAT
Comunidad de Madrid

Problema 1 :

Quieres enviar al Perseverance en Marte:
muévete en dirección Sur
(N: 00, S: 01, E: 10, O:11)

Sur → 01 → CANAL → 11 → Oeste ¡GLUB!

Codifica para ser capaz de detectar 1 error, minimizando la longitud de los mensajes.

Pista: no es un código de repetición.

00 → ? 01 → ? 10 →? 11 →?

Problema 1: Posible idea añadir un solo bit que controla la "paridad" de la suma de dígitos

$0 + 0 = 0$

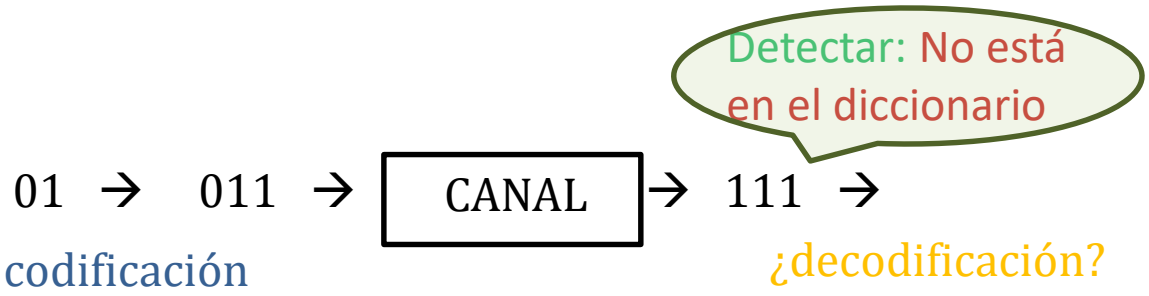
$0 + 1 = 1$

$1 + 0 = 1$

$1 + 1 = 0$ (impar+impar=par)

Codificamos:

00 → 000, 01 → 011 , 10 →101, 11 →110



En general: $a_1 a_2 \rightarrow a_1 a_2 a_3 \ con \ a_3 \equiv a_1 + a_2 \ mod \ 2$

ESTÍMULO DEL TALENTO MATEMÁTICO

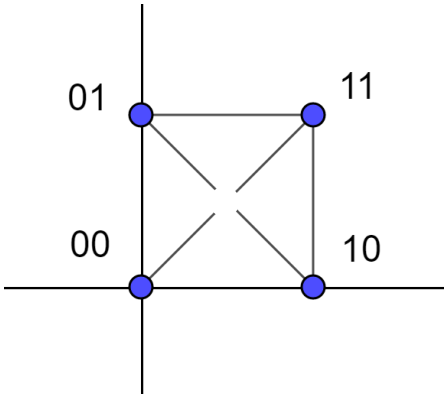
ESTALMAT
Comunidad de Madrid

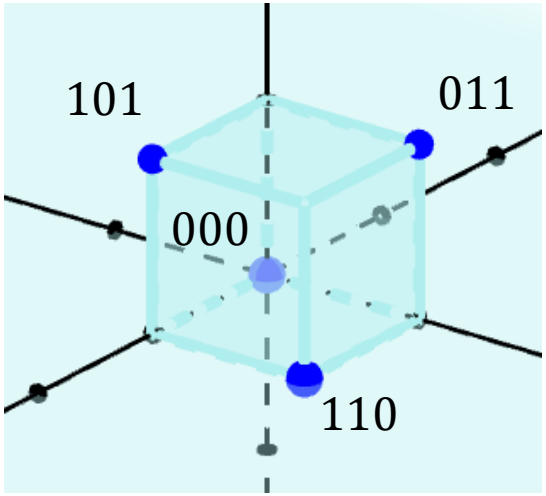
Visualizando

ESTÍMULO DEL TALENTO MATEMÁTICO
REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE ESPAÑA
UNIVERSIDAD COMPLUTENSE MADRID
FACULTAD DE CIENCIAS MATEMÁTICAS
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
FECYT INNOVACIÓN
Purposeful Ventures
ESTALMAT
Comunidad de Madrid

Problema 2: Código de paridad ={000, 011, 101, 110}

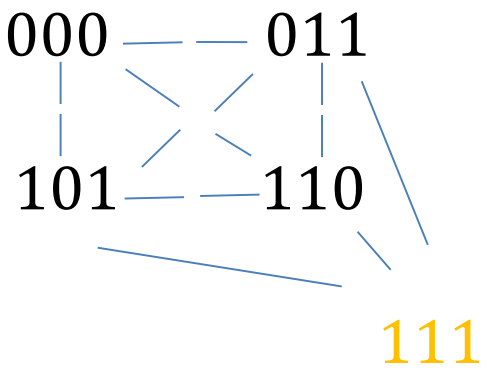
Sin código





1. ¿Por qué este código detecta 1 error?
2. ¿Puede corregirlo?
3. ¿Puede detectar 2 errores?

Problema 2: Código de paridad={000, 011, 101, 110}



1. Al producirse 1 error, caemos fuera del código.

2. No se puede corregir porque no existe la palabra más “cercana”

3. No se pueden detectar 2 errores porque hay palabras a “distancia” 2.

codificación decodificación

Emisor: 01 → 011 → CANAL → 101 → Receptor: NO detecta

ESTÍMULO DEL TALENTO MATEMÁTICO

ESTALMAT
Comunidad de Madrid

Abstrayendo

ESTÍMULO DEL TALENTO MATEMÁTICO
REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE ESPAÑA
UNIVERSIDAD COMPLUTENSE MADRID
FACULTAD DE CIENCIAS MATEMÁTICAS
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
FECYT INNOVACIÓN
Purposeful Ventures
ESTALMAT
Comunidad de Madrid

Definición: La DISTANCIA (de Hamming) de un código es el mínimo nº de diferencias entre dos palabras cualesquiera.

Ejemplo: Código de paridad tiene "distancia 2":
00 → 000, 01 → 011 , 10 → 101, 11 → 110

Ejemplo: Código de repetición 3 {000,111} tiene distancia 3

0 → 000, 1 → 111

$$000 \quad __ \quad __ \quad 111 \qquad d = 3$$

Idea: A mayor distancia mayor **capacidad de detección**,
pero si d es muy grande puede haber pocas palabras disponibles.

Ejercicio 3:

¿Cuántos errores podrá detectar un código de distancia n?

Ejercicio 3

¿Cuántos errores podrá detectar un código de distancia n?

Un código de distancia n
detecta como máximo $n - 1$ errores,

Entre dos palabras del código hay al menos n diferencias, luego:

- si hay hasta $n - 1$ errores, la palabra recibida no está en código.

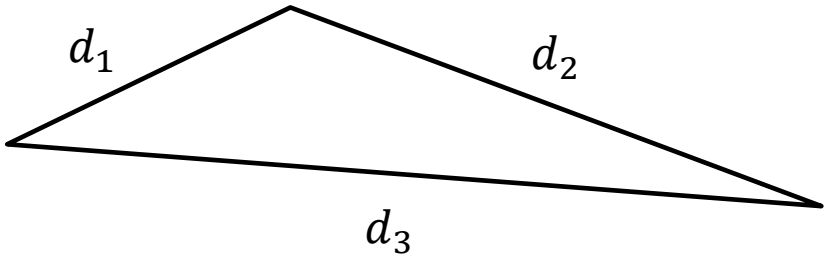
- si hay n errores o más: la palabra recibida puede estar el código (podemos haber saltado de una palabra del código a otra).

Observación:

La distancia de un código es una **distancia de verdad** (una buena manera de medir).

Explica por qué:

- ¡Nunca es negativa!
- La distancia entre dos … no depende del orden en la pareja.
- Se cumple la desigualdad *triangular*

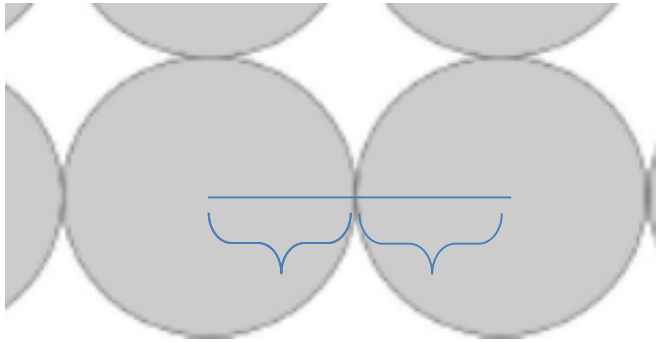


$$d_i \leq d_j + d_k$$

Problema 4: Capacidad de corrección

En general, dado un código con distancia d impar.
¿Cuántos errores será capaz de corregir?

000 ___ ___ 111



Problema 4: ¿Cuántos errores corrige un código con d impar?

Como $d = 2k + 1 = k + (k + 1)$, entonces:

- Hasta k errores, la palabra más cercana a la recibida es la original;
- Si hay $k + 1$ errores o más, puede haber otra palabra distinta de la original que sea su palabra más cercana.

Código corrige hasta $k = \frac{d-1}{2}$ errores.

Ejemplo: d=3 corrige 1 error, d=5, corrige 2 errores, etc.

000 _ _ 111

Obs: Si d par, $d = 2m$, corrige $\frac{d-2}{2}$ err. 0000 _ _ _ 1111

En general, corrige la parte entera de $\frac{d-1}{2}$.

Problema 5: Escribe demostración con desigualdad triangular.

ESTÍMULO DEL TALENTO MATEMÁTICO

ESTALMAT
Comunidad de Madrid

Saber más

ESTÍMULO DEL TALENTO MATEMÁTICO

REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE ESPAÑA

UNIVERSIDAD COMPLUTENSE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

FECYT INNOVACIÓN

Purposeful Ventures

ESTALMAT
Comunidad de Madrid

Otros códigos en la vida cotidiana:

Código de barras: Sistema *EAN-13* identifica cada producto con 13 dígitos:
El último dígito, a_{13} se calcula de forma que:
$(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + 3\,(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) + a_{13}$
sea 0 (pero en la aritmética módulo 10).
Calcula a_{13} para estas 12 cifras 1 8 4 7 4 0 3 7 0 3 6 0. Comprueba. (Excel).

Código QR: (Quick Response) formado por
cuadrados negros (0) y blancos (1).
El mensaje se codifica en conjuntos de 8 cuadrados, (llamados codewords) que incluyen información y control de paridad.

Código letra NIF 00053224*W* Explora…

Y haciéndonos preguntas:

¿Cómo sistematizar los códigos de paridad? ¿Matrices?

¿Eficiencia al almacenar código?

¿Buenos códigos en relación con tasas como distancia/longitud?

¿Buenos códigos con palabras ‘bien’ colocadas?

¿Bit cuántico? ¿Continuo frente a discreto?

REFERENCIAS

- FERNÁNDEZ GALLARDO, Pablo; GIL ÁLVAREZ, Omar (2001):
  "Una introducción a los códigos detectores y correctores de errores".

- GIL, Omar (2011): *Matemáticamente tenemos chance*. Montevideo: Ed. Fin de Siglo.

- HAMMING, Richard W. (1950): "Error Detecting and Error Correcting Codes"
  en *The Bell System Technical Journal*, Vol. XXIX, Nº 2, 147-160.

- HAMMING, Richard W. (1980b): "The Unreasonable Effectiveness of Mathematics" en
  American Mathematical Monthly, Vol. 87, Nº 2,pp. 81-90.

- SHANNON, Claude E. (1948): "A Mathematical Theory of Communication"
  en *The Bell System Technical Journal*, Vol. XXVII, pp. 379-423 (Julio), 623-656.

Jugando

Terminamos jugando:

Damos un número de 4 cifras a cada persona de un grupo.

Los números son: 1024, 2005, 3130, 2113, 1600, 5020, 4210, 7232, 1544, 8411, 9230…

Después de guardarlos un rato, nos los devuelven.

Entre esos números encontramos: 1024, 4300, 2032, 5020, 8123, 3502, 2354, 1085, 6001…

¿Alguien ha querido darnos el cambiazo?

ESTÍMULO DEL TALENTO MATEMÁTICO

ESTALMAT
Comunidad de Madrid

Transmitiendo mensajes

María Jesús Vázquez Gallo/Pablo Fernández Gallardo

Seminario Estalmat 05-04-2025

ESTÍMULO DEL TALENTO MATEMÁTICO

REAL ACADEMIA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES DE ESPAÑA

UNIVERSIDAD COMPLUTENSE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

FECYT INNOVACIÓN

Purposeful Ventures

ESTALMAT
Comunidad de Madrid