Síndrome:

Recibimos $w = \overset{c}{\cancel{m}} + e \iff c = w - e$.

Síndrome:

Recibimos $w = \overset{c}{\cancel{m}} + e \iff c = w - e$.

Buscamos f lineal que sea 0 sobre C y 1-1 ~~afuera~~ en los errores:

$$f(w) = f(c+e) = f(c) + f(e) = f(e)$$

Síndrome:

Recibimos $w = \overset{c}{\cancel{m}} + e \iff c = w - e$.

Buscamos f lineal que sea 0 sobre C y 1-1 ~~afuera~~ en los errores:

$$f(w) = f(c+e) = f(c) + f(e) = f(e)$$

Sea C un código lineal de long. n y dim k.

Una matriz de control H para C es una matriz $(n-k)\times n$ t.q.

$$w \in F^n : \underbrace{w H^T}_{\text{síndrome de } w} = 0 \iff w \in C$$

Síndrome:

Recibimos $w = \overset{c}{\cancel{m}} + e \iff c = w - e$.

Buscamos f lineal que sea 0 sobre C y 1-1 ~~afuera~~ en los errores:

$$f(w) = f(c+e) = f(c) + f(e) = f(e)$$

Sea C un código lineal de long. n y dim k.

Una matriz de control H para C es una matriz $(n-k) \times n$ t.q.

$$w \in F^n : \underbrace{w H^T}_{\text{síndrome de } w} = 0 \iff w \in C$$

Prop:

Sea H una matriz de control para un código lineal e-corrector. Entonces, si w_1, w_2 son palabras con peso menor o igual a e con la misma síndrome, $w_1 = w_2$.

Síndrome:

Recibimos $w = \overset{c}{\cancel{m}} + e \iff c = w - e$.

Buscamos f lineal que sea 0 sobre C y 1-1 ~~afuera~~ en los errores:

$$f(w) = f(c+e) = f(c) + f(e) = f(e)$$

Sea C un código lineal de long. n y dim k.

Una **matriz de control** H para C es una matriz $(n-k) \times n$ t.q.

$$w \in F^n : \underbrace{w H^T}_{\text{síndrome de } w} = 0 \iff w \in C$$

Prop:

Sea H una matriz de control para un código lineal e-corrector. Entonces, si w_1, w_2 son palabras con peso menor o igual a e con la misma síndrome, $w_1 = w_2$.

Dem: Si $w_1 H^T = w_2 H^T$ entonces $(w_1 - w_2) H^T = 0$ y $w_1 - w_2 \in C$.

Síndrome:

Recibimos $w = \overset{c}{\cancel{m}} + e \iff c = w - e$.

Buscamos f lineal que sea 0 sobre C y 1-1 ~~afuera~~ en los errores:

$$f(w) = f(c+e) = f(c) + f(e) = f(e)$$

Sea C un código lineal de long. n y dim k.

Una <u>matriz de control</u> H para C es una matriz $(n-k)\times n$ t.q.

$$w \in F^n : \underset{\substack{\uparrow \\ \text{síndrome de } w}}{w H^T} = 0 \iff w \in C$$

Prop:

Sea H una matriz de control para un código lineal e-corrector. Entonces, si w_1, w_2 son palabras con peso menor o igual a e con la misma síndrome, $w_1 = w_2$.

Dem:

Si $w_1 H^T = w_2 H^T$ entonces $(w_1 - w_2) H^T = 0$ y $w_1 - w_2 \in C$.
Ahora $wt(w_1 - w_2) \le 2e$ y, siendo C e-corrector, su peso mínimo es $2e+1$. Necesariamente $w_1 - w_2 = 0$. $\square$

Síndrome:

Recibimos $w = \overset{c}{\cancel{m}} + e \iff c = w - e$.

Buscamos f lineal que sea 0 sobre C y 1-1 ~~afuera~~ en los errores:

$$f(w) = f(c+e) = f(c) + f(e) = f(e)$$

Sea C un código lineal de long. n y dim k.

Una matriz de control H para C es una matriz $(n-k)\times n$ t.q.

$$w \in F^n : \underbrace{wH^T}_{\text{síndrome de } w} = 0 \iff w \in C$$

Prop:

Sea H una matriz de control para un código lineal e-corrector. Entonces, si w_1, w_2 son palabras con peso menor o igual a e con la misma síndrome, $w_1 = w_2$.

Dem:

Si $w_1 H^T = w_2 H^T$ entonces $(w_1 - w_2)H^T = 0$ y $w_1 - w_2 \in C$.

Ahora $wt(w_1 - w_2) \leq 2e$ y, siendo C e-corrector, su peso mínimo es $2e+1$. Necesariamente $w_1 - w_2 = 0$. □

Para decodificar hacemos así:

- recibimos w;
- cálculamos la síndrome wH^T;
- buscamos qué error e genera esa síndrome;
- $c = w - e$.

Podemos pensar en el síndrome en otra manera.

Podemos pensar en el síndrome en otra manera.

H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x)=w$, i.e. cada coset tiene una sola imagen bajo H^T.

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x)=w$, i.e. cada coset tiene una sola imagen bajo H^T.
Podemos corregir un error por coset, por eso elegimos un representante en cada coset (el de peso mínimo) y lo llamamos <u>coset leader</u>.

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x)=w$, i.e. cada coset tiene una sola imagen bajo H^T.
Podemos corregir un error por coset, por eso elegimos un representante en cada coset (el de peso mínimo) y lo llamamos <u>coset leader</u>.

<u>Prop</u>: Sea C un código lineal con matriz de control H. Luego C tiene peso mínimo mayor o igual a δ sii cualesquiera $\delta-1$ columnas de H son linearmente independientes.

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x)=w$, i.e. cada coset tiene una sola imagen bajo H^T.
Podemos corregir un error por coset, por eso elegimos un representante en cada coset (el de peso mínimo) y lo llamamos <u>coset leader</u>.

<u>Prop</u>: Sea C un código lineal con matriz de control H. Luego C tiene peso mínimo mayor o igual a δ sii cualesquiera $\delta-1$ columnas de H son linearmente independientes.

<u>Dem</u>: Llamamos $h_1, \dots, h_n$ las columnas de H.

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x) = w$, i.e. cada coset tiene una sola imagen bajo H^T.
Podemos corregir un error por coset, por eso elegimos un representante en cada coset (el de peso mínimo) y lo llamamos <u>coset leader</u>.

<u>Prop</u>: Sea C un código lineal con matriz de control H. Luego C tiene peso mínimo mayor o igual a δ sii cualesquiera $\delta-1$ columnas de H son linearmente independientes.

<u>Dem</u>: Llamamos $h_1, \dots, h_n$ las columnas de H.
$c_1 \cdots c_n \in C \iff c_1 h_1 + \cdots + c_n h_n = 0$

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x) = w$, i.e. cada coset tiene una sola imagen bajo H^T.
Podemos corregir un error por coset, por eso elegimos un representante en cada coset (el de peso mínimo) y lo llamamos <u>coset leader</u>.

<u>Prop:</u> Sea C un código lineal con matriz de control H. Luego C tiene peso mínimo mayor o igual a δ sii cualesquiera $\delta-1$ columnas de H son linearmente independientes.

<u>Dem:</u> Llamamos $h_1, \dots, h_n$ las columnas de H.
$c_1 \cdots c_n \in C \iff c_1 h_1 + \cdots + c_n h_n = 0$
Por eso, si $wt(c) = f$, tenemos una dependencia lineal entre f columnas de H. $\square$

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x)=w$, i.e. cada coset tiene una sola imagen bajo H^T.
Podemos corregir un error por coset, por eso elegimos un representante en cada coset (el de peso mínimo) y lo llamamos <u>coset leader</u>.

<u>Prop</u>: Sea C un código lineal con matriz de control H. Luego C tiene peso mínimo mayor o igual a δ sii cualesquiera $\delta-1$ columnas de H son linearmente independientes.

<u>Dem</u>: Llamamos $h_1, \dots, h_n$ las columnas de H.
$c_1 \cdots c_n \in C \iff c_1 h_1 + \dots + c_n h_n = 0$
Por eso, si $wt(c) = f$, tenemos una dependencia lineal entre f columnas de H.
$\square$

¿Cómo encontramos H?

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x)=w$, i.e. cada coset tiene una sola imagen bajo H^T.
Podemos corregir un error por coset, por eso elegimos un representante en cada coset (el de peso mínimo) y lo llamamos <u>coset leader</u>.

<u>Prop:</u> Sea C un código lineal con matriz de control H. Luego C tiene peso mínimo mayor o igual a δ sii cualesquiera $\delta-1$ columnas de H son linearmente independientes.

<u>Dem:</u> Llamamos $h_1, \dots, h_n$ las columnas de H.
$c_1 \cdots c_n \in C \iff c_1 h_1 + \dots + c_n h_n = 0$
Por eso, si $wt(c)=f$, tenemos una dependencia lineal entre f columnas de H. $\square$

¿Cómo encontramos H?

<u>Teorema:</u> ① Sean G y H matrices $k \times n$ y $(n-k)\times n$ sobre F, con lineas linealmente independientes. Luego G es la matriz generadora de un código y H la de control sii $GH^T=0$

Podemos pensar en el síndrome en otra manera.
H^T es una aplicación lineal de F^n a F^{n-k}, cuyo nucleo es el subespacio C.
Si en la transimisión se produce un error x, la palabra enviada pertenece al coset $C+x$.
Ahora, $H^T(C+x)=w$, i.e. cada coset tiene una sola imagen bajo H^T.
Podemos corregir un error por coset, por eso elegimos un representante en cada coset (el de peso mínimo) y lo llamamos <u>coset leader</u>.

<u>Prop</u>: Sea C un código lineal con matriz de control H. Luego C tiene peso mínimo mayor o igual a δ sii cualesquiera $\delta-1$ columnas de H son linearmente independientes.

<u>Dem</u>: Llamamos $h_1, \dots, h_n$ las columnas de H.
$c_1 \cdots c_n \in C \iff c_1 h_1 + \dots + c_n h_n = 0$
Por eso, si $wt(c)=f$, tenemos una dependencia lineal entre f columnas de H.
$\square$

¿Cómo encontramos H?

<u>Teorema</u>: ① Sean G y H matrices $k \times n$ y $(n-k) \times n$ sobre F, con lineas linealmente independientes. Luego G es la matriz generadora de un código y H la de control sii $GH^T=0$

② Sea $G=(I\ A)$ una matriz generadora para un código C en forma estándar. Luego una matriz de control es $H=(-A^T\ I)$.

Dem: ① Por hipótesis el espacio generado por las líneas

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.
También el nucleo C' de H tiene dimension k.

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.
También el nucleo C' de H tiene dimension k.
Ahora
$$GH^T = 0$$
es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.
También el nucleo C' de H tiene dimension k.
Ahora

$$GH^T = 0$$

es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

② G y H, ~~tie~~ tienen ambas k líneas lin. ind.

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.

También el nucleo C' de H tiene dimension k.

Ahora

$$GH^T = 0$$

es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

② G y H, tienen ambas k líneas lin. ind.

Ahora, por ①

$$(I\ A)(-A^T\ I)^T = (I\ A)\begin{pmatrix} -A \\ I \end{pmatrix} = -A + A = 0 \qquad \square$$

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.

También el nucleo C' de H tiene dimension k.

Ahora

$$GH^T = 0$$

es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

② G y H, tienen ambas k líneas lin. ind.

Ahora, por ①

$$(I\ A)(-A^T\ I)^T = (I\ A)\begin{pmatrix} -A \\ I \end{pmatrix} = -A + A = 0 \qquad \square$$

Volvemos al ejemplo $(7,4)$ de Hamming.

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.

También el nucleo C' de H tiene dimension k.

Ahora

$$GH^T = 0$$

es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

② G y H, ~~tie~~ tienen ambas k líneas lin. ind.

Ahora, por ①

$$(I\ A)(-A^T\ I)^T = (I\ A)\begin{pmatrix} -A \\ I \end{pmatrix} = -A + A = 0 \qquad \square$$

Volvemos al ejemplo $(7,4)$ de Hamming.

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

siendo el código 1-corrector, solo nos interesan las sindromes de los elemento de peso 1, i.e. los vectores de basis.

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.
También el nucleo C' de H tiene dimension k.
Ahora

$$GH^T = 0$$

es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

② G y H, ~~tie~~ tienen ambas k líneas lin. ind.
Ahora, por ①

$$(I\ A)(-A^T\ I)^T = (I\ A)\begin{pmatrix} -A \\ I \end{pmatrix} = -A + A = 0 \qquad \square$$

Volvemos al ejemplo $(7,4)$ de Hamming.

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

siendo el código 1-corrector, solo nos interesan las sindromes de los elemento de peso 1, i.e. los vectores de basis.

$e_1 H^T = 1^{era}$ línea de $H^T = 001$

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.

También el nucleo C' de H tiene dimension k.

Ahora

$$GH^T = 0$$

es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

② G y H, ~~tie~~ tienen ambas k líneas lin. ind.

Ahora, por ①

$$(I\ A)(-A^T\ I)^T = (I\ A)\begin{pmatrix} -A \\ I \end{pmatrix} = -A + A = 0$$

□

Volvemos al ejemplo $(7,4)$ de Hamming.

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

siendo el código 1-corrector, solo nos interesan las síndromes de los elemento de peso 1, i.e. los vectores de basis.

$e_1 H^T = 1^{era}$ línea de $H^T = 001$

[...]

En general, $e_i H^T$ es i en basis 2.

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.
También el nucleo C' de H tiene dimension k.
Ahora

$$GH^T = 0$$

es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

② G y H, ~~tie~~ tienen ambas k líneas lin. ind.
Ahora, por ①

$$(I\ A)(-A^T\ I)^T = (I\ A)\begin{pmatrix} -A \\ I \end{pmatrix} = -A + A = 0 \qquad \square$$

Volvemos al ejemplo $(7,4)$ de Hamming.

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

siendo el código 1-corrector, solo nos interesan las sindromes de los elemento de peso 1, i.e. los vectores de basis.

$e_1 H^T = 1^{\text{era}}$ línea de $H^T = 001$

[...]

En general, $e_i H^T$ es i en basis 2.

Si enviamos 1001, esto se codifica en 1001100.

Supongamos de recibir $w = 1001101$.

Dem: ① Por hipótesis el espacio generado por las líneas de G, que llamamos C, tiene dimension k.
También el nucleo C' de H tiene dimension k.
Ahora
$$GH^T=0$$
es equivalente al hecho que cada línea de G esté en C', es decir $C \subseteq C'$.

② G y H, ~~tie~~ tienen ambas k líneas lin. ind.
Ahora, por ①
$$(I\ A)(-A^T\ I)^T = (I\ A)\begin{pmatrix}-A\\ I\end{pmatrix} = -A+A=0$$
□

Volvemos al ejemplo $(7,4)$ de Hamming.

$$H=\begin{pmatrix}0&0&0&1&1&1\\0&1&1&0&1&1\\1&0&1&1&0&1\end{pmatrix}$$

siendo el código 1-corrector, solo nos interesan las síndromes de los elemento de peso 1, i.e. los vectores de basis.

$e_1H^T = 1^{era}$ línea de $H^T = 001$

[...]

En general, e_iH^T es i en basis 2.

Si enviamos 1001, esto se codifica en 1001100.

Supongamos de recibir $w = 1001101$.

$wH^T = 111 = 7$ en basis 2 $\Rightarrow$ hay 1 error en w_7!

Si tuvieramos más de 1 error la decodificación sería incorrecta.