messaggio (k) → u — parola di codice (n) → x

$u \cdot G = x$

$1\times k \quad k\times n \quad 1\times n$

x → canale → x'

Codice C Codifica : Matrice generatrice G $k \times n$

$V^{(n)} \supseteq C$

$V^{(n)} = C \oplus C^\perp$

$C^\perp$ Per ogni $y \in C^\perp$, vale l'equazione di controllo:

$$y \cdot x^T = x_1 y_1 + x_2 y_2 + \dots + x_n y_n = 0 \qquad \forall x \in C$$

$\dim C = k$

$\dim C^\perp = n - k$ Prendiamo $n-k$ vettori in $C^\perp$ linearmente indipendenti e formiamo la matrice

$$H_{(n-k)\times n} = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \vdots & & & \\ h_{n-k,1} & h_{n-k,2} & \dots & h_{n-k,n} \end{bmatrix}$$

H è la matrice generatrice di $C^\perp$

Inoltre, per ogni $x \in C$ vale che:

$$H \cdot x^T = \vec{0}$$

$$\underset{(n-k)\times n}{H} \underset{n\times 1}{x^T} = \begin{bmatrix} \\ \\ \\ \end{bmatrix} \begin{bmatrix} \\ \\ \\ \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \dots \end{bmatrix} = \underbrace{\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}}_{(n-k)\times 1}$$

$x \in C \iff H \cdot x^T = \vec{0}$

Se la matrice G è in forma canonica (codice sistematico):

$$G = \underset{k\times n}{\left[\; \underbrace{I_k}_{\text{mat. identità}} \quad A \;\right]}$$

$k \times k$, $n-k$, n

A è $k \times (n-k)$

allora posso prendere $H = \underset{(n-k)\times n}{\left[\; \underset{(n-k)\times k}{-A^T} \quad \underset{(n-k)\times(n-k)}{I_{n-k}} \;\right]}$

(1) H ha rango $n-k$

(2) Per ogni $x \in C$, $x = u \cdot G$ per qualche u (messaggio)

quindi $x^T = G^T u^T$

quindi $Hx^T = \underbrace{H \cdot G^T}_{\text{è sempre nullo}} \cdot u^T = \vec{0}$

Infatti

$$H \cdot G^T = \overbrace{\left[-A^T \;\; I_{n-k}\right]}^{H} \overbrace{\begin{bmatrix} I_k \\ A^T \end{bmatrix}}^{G^T} = \left[-A^T I_k + I_{n-k} A^T\right] = \left[-A^T + A^T\right] = \left[0\right]$$

Se decomponiamo H in colonne:

$$H = \begin{bmatrix} \vec{h}_1 & \vec{h}_2 & \cdots & \vec{h}_n \\ 0 & 0 & \cdots & 0 \end{bmatrix} \qquad (\vec{h}_i = i\text{-esima colonna di } H)$$

$H \cdot x^T$ può essere interpretato come somma pesata di alcune colonne di H, tante quante il peso del vettore x.

$$x \in C \iff \boxed{Hx^T = \vec{0}} \iff \sum_{i=1}^{n} x_i \vec{h}_i$$

→ le colonne di H sono linearmente dipendenti

$$d_{min} = \min_{\substack{x,y \in C \\ x \neq y}} d(x,y) = \min_{\substack{x,y \in C \\ x \neq y}} \underbrace{d(x-y, \vec{0})}_{wt(x-y)} = \min_{\substack{z \in C \\ z \neq \vec{0}}} wt(z)$$

peso di $x-y$

La d_{min} corrisponde al peso minimo di una parola di codice non nulla

→ Se il peso di $x \in C$ è $wt(x)$, in H ci sono $wt(x)$ colonne la cui combinazione lineare è nulla.

→ E viceversa, per ogni combinazione lineare nulla di w colonne di H esiste $x \in C$ tale che $wt(x) = w$.

Quindi d_{min} è anche pari al numero minimo di colonne di H linearmente dipendenti.

Esempio.

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \qquad C(7,4)$$

(I_4 | A)

Quindi la matrice di controllo è:

$$H = [-A^T \; I_{n-k}] = \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

$2^3 - 1$ colonne; 3 righe

$-A^T$ | I_{n-k}

Quanto vale d_{min}? $\Rightarrow d_{min} = 3$

d_{min} = # min. di colonne di H linearmente dipendenti

- $d_{min} > 1$ perché nessuna colonna è nulla
- $d_{min} > 2$ perché non ci sono 2 colonne identiche (e quindi non posso avere $\vec{h_i}, \vec{h_j}$ tali che $\vec{h_i} + \vec{h_j} = \vec{0}$)
- $d_{min} \leq 3$ perché ci sono 3 colonne linearmente dipendenti (la 1ª, la 2ª, la 3ª)

$$\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

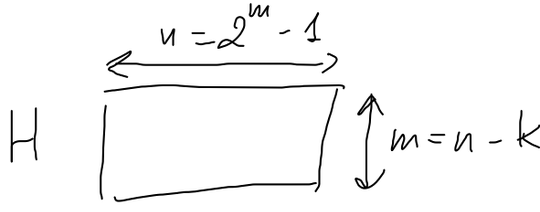
(In $GF(2)$: $-1 = +1$)

0, 1

Codice di Hamming: (Hamming 1950)

In generale, per $m = 2, 3, 4, \ldots$ posso costruire una matrice di controllo H con $n = 2^m - 1$ colonne m-ple distinte eccetto quella nulle.

In tal caso $k = n - m = 2^m - 1 - m$



Questo è un codice di Hamming $C(\underbrace{2^m - 1}_{n}, \underbrace{2^m - 1 - m}_{k})$

che ha sempre $d_{min} = 3$. (e permette di rilevare 2 errori o di correggere 1 errore).

Per esempio con $m = 2$ ottengo $k = 2^2 - 1 - 2 = 1$, $n = 2^2 - 1 = 3$ $\rightarrow$ un codice $C(3, 1, 3)$ (n, k, d_{min})

(che è il codice a ripetizione con $n = 3$)

Con $m = 3$ ottengo $k = 4$, $n = 7$ $\rightarrow$ un codice $C(7, 4, 3)$

In generale, il tasso di un codice di Hamming è $k/n = \dfrac{2^m - 1 - m}{2^m - 1}$ $\left(\triangleq R\right)$

La capacità di correzione è $\lambda = \dfrac{d_{min}}{n} = \dfrac{3}{2^m - 1}$

Con $m = 2 \rightarrow R = 1/3$, $\lambda = 1$

Con $m = 3 \rightarrow R = 4/7$, $\lambda = 3/7$

Con $m \to \infty \rightarrow R \to 1$, $\lambda \to 0$

Decodifica di un codice lineare

Parole Trasmessa : $x \in C \quad (V^{(k)})$

Seq. Ricevuta : $y = x + e \quad (V^{(n)})$

n-pla di errore : $e \quad (V^{(n)})$

Def. La sindrome di $y \in V^{(n)}$ è :

$$\underbrace{s(y)}_{(n-k)\times 1} \triangleq \underbrace{H}_{(n-k)\times n} \cdot \underbrace{y^T}_{n\times 1}$$

Abbiamo già mostrato che $x \in C \iff Hx^T = \vec{0} \iff s(x) = \vec{0}$.

La dimensione della sindrome è $n-k \Rightarrow$ ci sono q^{n-k} sindromi distinte

(il campo è $\mathbb{F}_q$)

Per linearità di H,

$$s(y) = s(x+e) = H(x+e)^T = \overbrace{Hx^T}^{\vec{0} \text{ perché } x \in C} + He^T = He^T = s(e)$$

$\rightarrow$ la sindrome di y coincide con la sindrome della configurazione di errore e.

conosco
↓
$y - e = x$
↑ ↗
?

Per rilevare errore:

1. Ricevi y e calcola $s(y)$
2. Se $s(y) = \vec{0}$, poni $\hat{x} = y$
3. Se $s(y) \neq \vec{0}$, riporta errore di trasmissione.