Codici lineari

$\mathcal{A} = GF(q)$ $\quad V^{(n)}$

$\mathbb{F}_q \quad C \subseteq \quad C^\perp$

Matrice generatrice $k \times n$ $\qquad G = \begin{bmatrix} x^{(1)} \\ x^{(2)} \\ \vdots \\ x^{(k)} \end{bmatrix} = \begin{bmatrix} x_1^{(1)} & x_2^{(1)} & \dots & x_n^{(1)} \\ & \dots & & \\ x_1^{(k)} & & \dots & x_n^{(k)} \end{bmatrix}$

Codifica : $x = u \cdot G$

$\cap \qquad \cap$

$\mathbb{F}_q^n \qquad \mathbb{F}_q^k$

$\dim(C) = k$

$\dim(C^\perp) = n - k$

$y \in C^\perp \iff \forall x \in C, \ \underbrace{x_1 y_1 + x_2 y_2 + \dots + x_n y_n}_{\in \mathbb{F}_q} = 0 \in \mathbb{F}_q$

$\quad \| \quad y \cdot x^T$

Ciascun y corrisponde ad una equazione di controllo

$$x \in C \iff \forall y \in C^\perp, \ y \cdot x^T = 0$$

Sia $\{h^{(1)}, h^{(2)}, \dots, h^{(n-k)}\}$ una base di $C^\perp$; considero la matrice

$$H = \begin{bmatrix} h_1^{(1)} & h_2^{(1)} & h_3^{(1)} & \dots & h_n^{(1)} \\ \vdots & & & & \\ h_1^{(n-k)} & h_2^{(n-k)} & & \dots & h_n^{(n-k)} \end{bmatrix}$$

matrice $(n-k) \times n$.

H è chiamata matrice di controllo (di C).

Per costruzione ho :

Se $x \in C$, ho $\underbrace{H}_{(n-k)\times n} \cdot \underbrace{x^T}_{n \times 1} = \underbrace{\begin{bmatrix} \quad \\ \quad \\ \quad \end{bmatrix}}_{H} \underbrace{\begin{bmatrix} \quad \\ \quad \\ \quad \end{bmatrix}}_{x^T} = \underbrace{\begin{bmatrix} \quad \\ \quad \\ \quad \end{bmatrix}}_{(n-k)\times 1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \vec{0}$

Se $x \notin C$, $H \cdot x^T \neq \vec{0}$

$x = \underbrace{z}_{\in C} + \underbrace{w}_{\in C^\perp \neq \vec{0}}$

Se G è in forma canonica: (codice sistematico)

$$G = \underbrace{\left[\underbrace{I_k}_{k\times k} \,\middle\vdots\, \underbrace{A}_{k\times(n-k)}\right]}_{\text{k righe}}$$

allora posso prendere $H = \underbrace{\left[-A^T \,\middle\vdots\, I_{n-k}\right]}_{\text{n colonne}}$ } n-k righe

$-A^T$ è $(n-k)\times k$

Osservazioni:

(1) H ha rango $n-k$ (in quanto contiene I_{n-k} come sottomatrice)

(2) Per ogni $x \in \mathcal{C}$, $x = u \cdot G$ per qualche messaggio $u \in \mathbb{F}_q^k$

$\rightarrow x^T = G^T u^T \rightarrow \underline{Hx^T} = (H G^T)u$

$$H \cdot G^T = \left[-A^T \,\middle\vdots\, I_{n-k}\right]\begin{bmatrix} I_k \\ \cdots \\ A^T \end{bmatrix} = \left[-A^T \cdot I_k + I_{n-k} A^T\right] = \underbrace{\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 \end{bmatrix}}_{\text{k colonne}} \Big\} \text{n-k righe}$$

$$\Rightarrow HG^T u = \underbrace{\begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}}_{\text{1 colonna}} \Big\} \text{n-k righe}$$

Dalla matrice di controllo H si può anche inferire la distanza minima (d_{min}) del codice $\mathcal{C}$.

Se decomponiamo H per colonne:

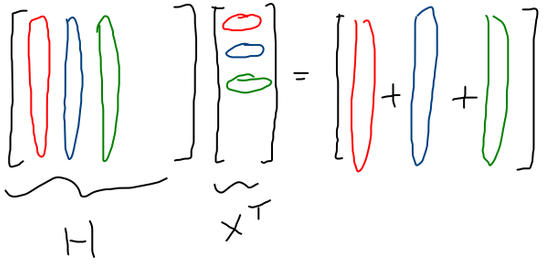
$$H = [\vec{h}_1 \quad \vec{h}_2 \quad \cdots \quad \vec{h}_n]$$

$$H = \left[\begin{array}{c|c|c|c} & & & \\ & & & \\ & & & \\ & & & \end{array}\right]$$

, allora il prodotto $H \cdot x^T = \sum_{i=1}^{n} \vec{h}_i \cdot x_i$

In particolare ho $x \in \mathcal{C}$

$$\Leftrightarrow \sum_{i=1}^{n} \vec{h}_i x_i = \vec{0} \Rightarrow \text{le colonne di } H \text{ sono linearmente dipendenti}$$



$$d_{min} = \min_{\substack{x,y \in \mathcal{C} \\ x \neq y}} d_H(x,y) = \min_{\substack{e \in \mathcal{C} \\ e \neq \vec{0} \\ (e = y - x)}} d_H(e,\vec{0}) = \min_{\substack{e \in \mathcal{C} \\ e \neq \vec{0}}} \underline{wt(e)}$$

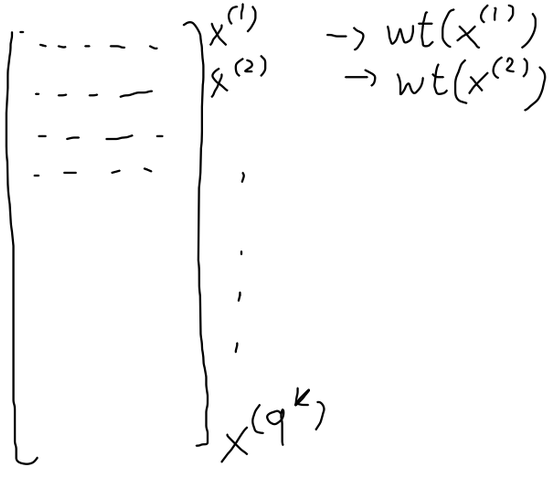
Se $x \in \mathcal{C}$ ha l componenti diverse da 0,

allora poiché $Hx^T = \sum_{i=1}^{n} \vec{h}_i x_i = \vec{0}$, esistono l vettori dell'insieme $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_n\}$ linearmente dipendenti.

→ Se il peso di $x \in C$ è $wt(x)$, in H ci sono $wt(x)$ colonne linearmente dipendenti.

$\Rightarrow$ d_{min} coincide con il minimo numero di colonne di H linearmente dipendenti.

C



$$d_{min} = \min_{j=1 \dots q^k} wt(x^{(j)})$$

Esempio.
(è un esempio di codice di Hamming) $G = \left[\begin{array}{cccc|ccc} 1&0&0&0&0&1&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&1&1&1 \end{array}\right] \rightarrow H = [-A^T I_{n-k}] = \left[\begin{array}{ccc|ccc} 0&1&1&1&1&0&0\\ 1&0&1&1&0&1&0\\ 1&1&0&1&0&0&1 \end{array}\right]$

I_4 A A^T I_3

$$H = \left[\begin{array}{ccccccc} 0&1&1&1&1&0&0\\ 1&0&1&1&0&1&0\\ 1&1&0&1&0&0&1 \end{array}\right]$$

$(2^3 - 1$ triple binarie non-nulle$)$

$k = 4$, $n = 7$
$n - k = 3$

Da H osservo che: $d_{min} > 1$: tutte le colonne di H sono non-nulle;
nessun vettore colonna di H da solo può essere lin. dipendente.

$d_{min} > 2$: tutte le colonne di H sono anche distinte;
nessuna è multiplo di un'altra.

$x \quad x'$

~~$x' = 0 \cdot x$~~
~~$x' = 1 \cdot x$~~
~~$x + x' = 0$~~
~~$x = -x' = x'$~~

$d_{min} \leq 3$: la terza colonna è uguale alla somma delle prime due.

In GF(2), $-1 = 1 \pmod 2$

$\Rightarrow$ $d_{min} = 3$.

Codici di Hamming (Hamming 1950);

In generale per $m = 2, 3, 4, \ldots$ $(m = n - k)$

posso costruire una matrice di controllo H con tutti i possibili $2^m - 1$ vettori colonna binari distinti (evitando il vettore colonna nullo)

In tal caso, H avrà dimensioni $\underbrace{m}_{n-k} \times \underbrace{(2^m - 1)}_{n}$

$m = n - k$
$k = n - m$
$= 2^m - 1 - m$

$\Rightarrow$ è un codice lineare di tipo $C(2^m - 1, 2^m - 1 - m, 3)$

$\Rightarrow$ Può rilevare fino $d_{min} - 1 = 2$ errori

Può correggere $\left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = 1$ errore.

Il tasso di un codice di Hamming è $R = \frac{\log_q M}{n} = \frac{\log_q q^k}{n} = \frac{k}{n} = \frac{2^m - 1 - m}{2^m - 1}$

Per esempio, se $m = 2$, ho $R = \frac{2^2 - 1 - 2}{2^2 - 1} = \frac{1}{3}$

il codice è del tipo $C(3, 1, 3)$; è il codice a ripetizione di lunghezza 3.

Se $m = 3$, ho $R = \frac{2^3 - 1 - 3}{2^3 - 1} = \frac{4}{7}$

il codice è del tipo $C(7, 4, 3)$

Se $m \to \infty$, ho $R = \frac{2^m - 1 - m}{2^m - 1} \xrightarrow[m \to \infty]{} 1$

Capacità di correzione: $\lambda = \frac{d_{min}}{n}$

$m = 2$, $\lambda = 3/3 = 1$ $(n = 3)$

$m = 3$, $\lambda = 3/7$

$m \to \infty$, $\lambda = 3/\infty \to 0$

Decodifica in un codice lineare: $\mathbb{F}_q^n \supseteq \mathbb{F}_q^k$

Parola trasmessa $x \in \mathcal{C}$ $(\in V^{(n)})$ $\quad x = u \cdot G$

Seq. ricevuta : $y = x + e$

n-pla di errore : $e = y - x$

Def. $s(y) \triangleq H y^T$ è chiamata la sindrome della sequenza y

Abbiamo già argomentato che $s(y) = \vec{0} \iff y \in \mathcal{C} \iff x + e \in \mathcal{C}$

Procedura di rilevazione di errore:

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

$$s(y) = H y^T = H(x+e)^T = \underbrace{H x^T}_{= \vec{0},\ x \in \mathcal{C}} + H e^T = H e^T = s(e)$$