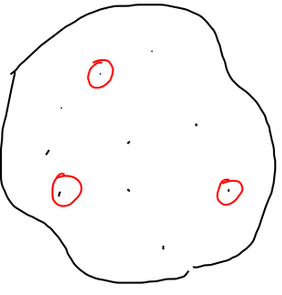
CODICI LINEARI

$\mathcal{C}$

Def. Un codice lineare di lunghezza n e dimensione k ($\leq n$) è un sottospazio lineare $V^{(k)}$ dello spazio vettoriale $V^{(n)} \hat{=} A^n$.

→ Il numero di parole di codice è $|V^{(k)}| = q^k$.

In genere scriviamo $C(n,k)$ per denotare un codice lineare di lunghezza n e dimensione k. Oppure $C(n,k,d_{min})$ se si vuole specificare anche la distanza minima del codice.



A^n spazio vettoriale (q^n)

$|A| = q$

Conseguenza:

- la somma di due parole di codice è una parola di codice
  $(x^{(1)}, x^{(2)} \in \mathcal{C} \Rightarrow x^{(1)} + x^{(2)} \in \mathcal{C})$
- il prodotto di una parola di codice per un elemento $a \in A$ del campo è ancora una parola di codice.
  $(x \in \mathcal{C},\ a \in A \Rightarrow a \cdot x \in \mathcal{C})$

$A = \{0,1\}$

$\underbrace{000\ldots0}_{n} = 0 \cdot \underbrace{x}_{n}$

$x = 1 \cdot x$

Esempio. $C = \{001, 111\}$ (su $GF(2)$) non è un codice lineare:

$000 \notin C$; $001 + 111 = 110 \notin C$ (001 ∈ C, 111 ∈ C)

$C = \{000, 111\}$ è un codice lineare:

(su $GF(2)$)

$q = 2$

Lunghezza $n = 3$

Dimensione $K = 1$

$000 + 000 = 000 \in C$

$000 + 111 = 111 \in C$

$111 + 111 = 000 \in C$

Base di C: $\{111\}$

$(000 = 0 \cdot 111$

$111 = 1 \cdot 111)$

è un codice di tipo $C(3, 1)$.

Distanza minima: $d_{min} = 3$ $C(3, 1, 3)$.

Per descrivere un codice lineare determiniamo una base di $V^{(K)}$ e formiamo una matrice di dimensioni $k \times n$ in cui ciascuna riga rappresenta il vettore riga corrispondente ad uno degli elementi della base.
Quindi ho k righe linearmente indipendenti; ciascuna riga è un vettore di $V^{(n)}$ (ha elementi in $GF(q)$).

La matrice risultante si indica con G ed è detta matrice generatrice del codice.

Otteniamo le parole del codice come combinazione lineare delle righe di G.

Esempio. $G = (1\ 1\ 1) \in GF(2)^{1\times 3}$

Codice a ripetizione; codice di tipo $C(3,1)$.
$q=2,\ n=3,\ k=1$

Esempio. Matrice generatrice:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{matrix} \leftarrow x^{(1)} \cdot 0/1 \\ \leftarrow x^{(2)} \cdot 0/1 \\ \leftarrow x^{(3)} \cdot 0/1 \\ \leftarrow x^{(4)} \cdot 0/1 \end{matrix}$$

Sottomatrice di rango k

$\in A = GF(q)$

$a_1 x^{(1)} + a_2 x^{(2)} + a_3 x^{(3)} + a_4 x^{(4)}$

q^4

$q = 2 \rightarrow k = 4, \; n = 7$ Codice $C(7,4)$

Quante sono le parole del codice? Sono $q^k = 2^4 = 16$

$$\begin{cases} 0\,0\,0\,0\,0\,0\,0 \in C = V^{(k)} \\ 1\,0\,0\,0\,0\,1\,1 \in C = V^{(k)} \\ 1\,1\,0\,0\,1\,1\,0 \in C = V^{(k)} \\ \vdots \\ ; \end{cases}$$

Se la matrice è della forma

$G = (I_k \; A)$ con

I_k matrice identità di ordine k

e A matrice $k \times (n-k)$

allora si parla di matrice in forma canonica.

o in forma sistematica.

Tasso di un codice: $R = \frac{\log_q M}{n} = \frac{k}{n}$

↖ codice lineare; $M = q^k$

n simboli di una parola di codice { k sono informativi; $n-k$ sono simboli di controllo

CODIFICA IN UN CODICE LINEARE

$u = u_1 u_2 \dots u_k$ → CC → $x = x_1 \dots x_n$

Per codificare $u = u_1 \dots u_k$ (vettore riga di lunghezza k) $\in A^k$

in $x = x_1 \dots x_n$ (vettore riga di lunghezza n) $\in A^n$

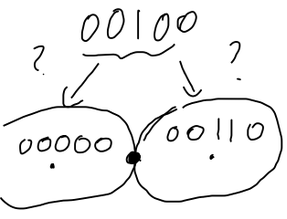
calcolo $\boxed{x = u \cdot G}$

$(1 \times n) \quad (1 \times k) \quad (k \times n)$

Quindi la codifica è una trasformazione lineare da A^k a A^n

$G : V^{(k)} \to V^{(n)}$

Esempio. $G_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ sul campo $GF(2)$



È un codice lineare di tipo $C(\overset{n}{5}, \overset{k}{3})$

L'insieme delle parole di codice è: (devono essere $q^k = 2^3 = 8$)

$$\mathcal{C} = \{ \underset{(3)}{00000}, \underset{(2)}{11100}, \underset{(5)}{00110}, \underset{(3)}{11111}, \underset{(2)}{11010}, \underset{(3)}{00011}, \underset{(2)}{11001}, 00101 \} \subset \{0,1\}^5$$

Distanza minima del codice: $d_{min} = \min_{\substack{x \neq x' \\ x, x' \in \mathcal{C}}} d_H(x, x') = \min_{\substack{x \neq x' \\ x, x' \in \mathcal{C}}} d_H(\underbrace{x - x'}_{z}, 00\ldots0)$

$= \min_{\substack{z \neq 00\ldots0 \\ z \in \mathcal{C}}} d_H(z, 00\ldots0) = \min_{\substack{z \neq 00\ldots0 \\ z \in \mathcal{C}}} wt(z)$

nel nostro caso $d_{min} = 2$ ←

⇒ possiamo rilevare fino a $d_{min} - 1 = 1$ errore

e possiamo correggere fino a $\left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0$ errori (in qualunque configurazione)

Esempio di codifica : per codificare la k-pla

$u = (u_1, u_2, u_3)$

calcolo $x = u \cdot G = (u_1, u_2, u_3) \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$

$= (u_1 + u_3 \,,\; u_1 + u_3 \,,\; u_1 + u_2 + u_3 \,,\; u_2 + u_3 \,,\; u_3) \in V^{(5)}$

Se $u = 101$ ottengo $x = 00011$

Se $u = 111$ ottengo $x = 00101$

Esempio in forma sistematica.

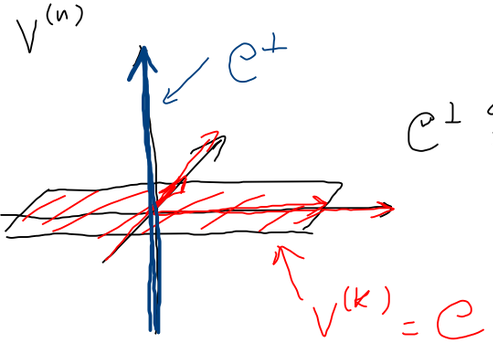
$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

$u = (u_1, u_2, u_3, u_4) \in GF(q)^4$

$u \cdot G = (\underbrace{u_1, u_2, u_3, u_4}_{k \text{ simboli "informativi"}}, \underbrace{u_2+u_3+u_4, u_1+u_3+u_4, u_1+u_2+u_4}_{n-k \text{ simboli di controllo}})$

Spazio duale / Codice duale

$V^{(n)}$: spazio vett. di tutte le n-ple ; $\mathcal{C} = V^{(K)}$: sottospazio di $V^{(n)}$



Consideriamo l'insieme : (prodotto scalare standard)

$$\mathcal{C}^\perp \overset{\text{def.}}{=} \{y \in V^{(n)} : y \perp x \ \ \forall x \in \mathcal{C}\} = \{y \in V^{(n)} : \langle y, x \rangle = 0 \ \ \forall x \in \mathcal{C}\}$$

L'insieme $\mathcal{C}^\perp$ è a sua volta un sottospazio di $V^{(n)}$

(per esempio, $\langle y + y', x \rangle = \underset{0}{\langle y, x \rangle} + \underset{0}{\langle y', x \rangle} = 0$)

$\mathcal{C}^\perp$ è il sottospazio ortogonale a $\mathcal{C} \subseteq V^{(k)}$

$$\underbrace{\dim \mathcal{C}}_{k} + \dim \mathcal{C}^\perp = \underbrace{\dim V^{(n)}}_{n} \quad \Rightarrow \quad \dim \mathcal{C}^\perp = n - k$$

Essendo $\mathcal{C}^\perp$ a sua volta un sottospazio di $V^{(n)}$, esso definisce un altro codice lineare, chiamato il codice duale di $\mathcal{C}$.

Se $\mathcal{C}$ è di tipo $C(n,k)$ allora $\mathcal{C}^\perp$ è di tipo $C(n, n-k)$.

Per ogni $x \in \mathcal{C}$, e per ogni $y \in \mathcal{C}^\perp$, per costruzione ho $\langle x, y \rangle = 0$

ovvero $x_1 y_1 + x_2 y_2 + \dots + x_n y_n = 0$ (nel campo $GF(q)$)

(equazione di controllo).

Ogni $y \in \mathcal{C}^\perp$ dà luogo ad una equazione di controllo. Ve ne sono $n-k$ linearmente indipendenti.