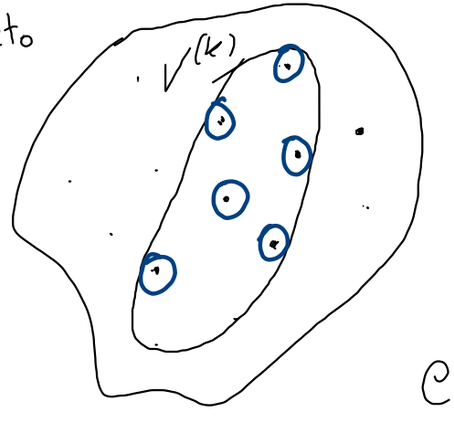
Codici lineari

Def. Un codice lineare di lunghezza n e dimensione k è un sottospazio $V^{(k)}$ (di cardinalità q^k) dello spazio vettoriale $V^{(n)} = \vec{q}^{\,n}$.

In genere è denotato con $C(n,k)$ o con $C(n,k,d_{min})$.

$\Leftrightarrow$ La somma (coordinata per coordinata, su $GF(q)$) di due parole di codice è una parola di codice.

Se $x \in \mathcal{C} \Rightarrow c \cdot x = \underbrace{x+x+\dots+x}_{c \text{ volte}} \in \mathcal{C}$ $(c \in GF(q))$



n-ple su alfabeto q-ario

$V^{(n)} = \vec{q}^{\,n}$

$q=3$ $GF(3)$

02212
10211
12120

$\mathcal{C} = \{001, 111\}$ non è lineare : su $GF(2)$, $001+111 = 110 \notin \mathcal{C}$

$\rightarrow \mathcal{C} = \{000, 111\}$ è lineare : $000+000=000 \in \mathcal{C}$
$000+111=111 \in \mathcal{C}$
$111+111=000 \in \mathcal{C}$
$111+000=111 \in \mathcal{C}$

q^k parole di codice | $C(3,1)$ $n=3$ $k=1$ $q=2$

Per descrivere un codice lineare formiamo una base di $V^{(K)}$ attraverso una matrice, di dimensione $k \times n$, con k vettori riga linearmente indipendenti di lunghezza n (a elementi su $GF(q)$).

$\rightarrow$ Matrice generatrice del codice. La indichiamo con G.

Otteniamo le parole di codice come combinazioni lineari delle righe di G.

Esempio. $G = (1 \ 1 \ 1)$ è un codice $C(3,1)$ su $GF(2)$.

Parole di codice: $0 \cdot (1\ 1\ 1) = (0\ 0\ 0)$
$1 \cdot (1\ 1\ 1) = (1\ 1\ 1)$

Esempio.

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

è un codice $C(7,4)$

q^k

2^4

$1\ 0\ 0\ 0\ 0\ 1\ 1 \in C$ $\quad 1\ 1\ 0\ 0\ 1\ 1\ 0 \in C$

Quando G è esprimibile nella forma $G = [\, I_k \;\; A \,]$ ← matrice qualunque $k \times (n-k)$

il codice è in forma sistematica. ↑ matrice identità $k \times k$

Tasso di un codice $C(n,k)$:

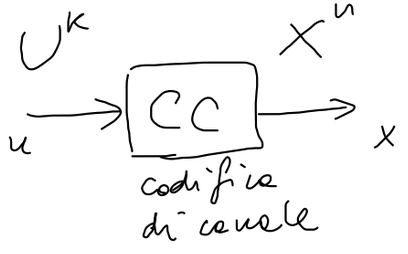
$$R = \frac{\log_q M}{n} = \frac{\log_q q^k}{n} = \frac{k}{n} \rightarrow \begin{cases} k \text{ simboli danno informazione} \\ n-k \text{ simboli ridondanti di controllo} \end{cases}$$

$M = q^k$ per quanto detto prima

CODIFICA

Per codificare $u = u_1 u_2 \dots u_k$ (vettore riga di lungh. k)

in $x = x_1 x_2 \dots x_n$ (vettore riga di lungh. n)



formo il prodotto $x = u \cdot G$

$1 \times n$; $1 \times k$; $k \times n$; $1 \times n$

La codifica è una trasformazione lineare $G: V^{(K)} \rightarrow V^{(n)}$

Esempio. $G_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ è un codice $C(5,3)$

3 ② 5 0 3 3 ② ②

$C = \{ 11100, 00110, 11111, 00000, 11010, 11001, 00011, 00101 \}$

$q^k \quad 2^3 = 8 \qquad d_{min} = 2 \rightarrow$ Può rivelare errori di peso 1 $(d_{min} - 1)$

$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{2-1}{2} \right\rfloor = \lfloor 0.5 \rfloor = 0 \rightarrow$ Non può correggere tutte le configurazioni di errore di peso 1 (servirebbe $d_{min} \geq 2 \cdot \underset{\sim}{1} + 1 = 3$)

$\underset{\sim}{t}$

Esempi di codifica.

G_2: per codificare $u = u_1 u_2 u_3$ formo il prodotto

$$u \cdot G_2 = (u_1\ u_2\ u_3) \begin{bmatrix} u_1 & 1 & 1 & 1 & 0 & 0 \\ u_2 & 0 & 0 & 1 & 1 & 0 \\ u_3 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = (u_1+u_3,\ u_1+u_3,\ u_1+u_2+u_3,\ u_2+u_3,\ u_3)$$

$1 \times k$ $\qquad k \times n \qquad 1 \times n$

$u = 101 \quad (1\ 0\ 1)\ G = (0, 0, 0, 1, 1) \rightarrow 00011 = x$

$u = 111 \quad (1\ 1\ 1)\ G = (0, 0, 1, 0, 1) \rightarrow 00101 = x$

Esempio · $G_3 =$

u_1	1	0	0	0	0	1	1
u_2	0	1	0	0	1	0	1
u_3	0	0	1	0	1	1	0
u_4	0	0	0	1	1	1	1

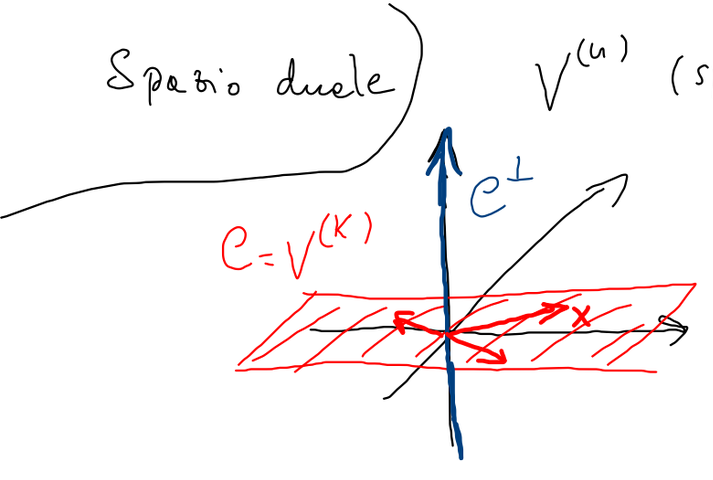
$u = (u_1\ u_2\ u_3\ u_4)$

$u \cdot G_3 = (\overbrace{u_1, u_2, u_3, u_4}^{\text{i } k \text{ elementi di } u}, u_2+u_3+u_4, u_1+u_3+u_4, u_1+u_2+u_4)$

k bit di informazione

$n-k$ bit di controllo (ridondanza)

Spazio duale $V^{(n)}$ (spazio di tutte le n-ple)



Consideriamo l'insieme $\{y \in V^{(n)} : y \perp x \quad \forall x \in \mathcal{C}\}$ (y ortogonale a x; $V^{(k)}$)

$= \{y \in V^{(n)} : \langle y, x \rangle = 0 \quad \forall x \in \mathcal{C}\} \triangleq \mathcal{C}^\perp$

↑ prodotto scalare tra y e x ($y^T x$)

$\mathcal{C}^\perp$ è il sottospazio di $V^{(n)}$ ortogonale a $\mathcal{C} = V^{(K)}$

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

$$\mathcal{C} : C(n,k) \qquad \mathcal{C}^\perp : C(n, n-k)$$

Quindi $\mathcal{C}^\perp$ rappresenta a sua volta un codice lineare $C(n, n-k)$ (detto codice duale)

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

$\Updownarrow$

Equazione di controllo $\boxed{x_1 y_1 + x_2 y_2 + \dots + x_n y_n = 0}$ (in $GF(q)$)

Poiché $\dim \mathcal{C}^\perp = n-k$, ci sono $n-k$ equazioni di controllo linearmente indipendenti.

Prendiamo una base di $C(n, n-k)$ (una base di $\mathcal{C}^\perp$) formata da $n-k$ vettori linearmente indipendenti (di lunghezza n) $\longrightarrow$ Matrice di controllo (H).