(1) Il codice binario (su $GF(2)$) $\mathcal{C} = \{ \underbrace{000, \boxed{\underset{x}{010}, \underset{x'}{100}}, 111}_{\text{parole di codice}} \}$, $n = 3$

Il codice è lineare ?

$n = 3$

$$\underset{A^n}{V^{(n)}} = \underbrace{\{0,1\}}_{A}^{3}$$

$a_1 a_2 a_3 \in V^{(3)}$

$b_1 b_2 b_3 \in V^{(3)}$ $\rightarrow (a_1 + b_1, a_2 + b_2, a_3 + b_3) \in V^{(3)}$

$|\mathcal{C}| = |V^{(k)}|$ per qualche k intero ≥ 0

$= 2^k$ $\rightarrow$ in questo ok per $\boxed{k = 2}$

Devo verificare che $\forall \underline{x \in \mathcal{C}}$, $\left.\begin{array}{l} 0 \cdot x \in \mathcal{C} \\ 1 \cdot x \in \mathcal{C} \end{array}\right\}$ $\begin{array}{l} 0 \cdot x = 00\ldots0 \in \mathcal{C} \\ 1 \cdot x = x \in \mathcal{C} \end{array}$

$\forall x, x' \in \mathcal{C}$, $x + x' \in \mathcal{C}$

$x = 010$
$x' = 100$ $\rightarrow$ $x + x' = 110 \notin \mathcal{C}$ $\rightarrow$ il codice non è lineare.

② Il codice binario $\mathcal{C} = \{0000, 0101, 1010, 1111\}$ è lineare?

$(n=4)$

$V^{(n)} = \{0,1\}^4$

$|\mathcal{C}| = 4 = 2^2 \to$ Se $\mathcal{C}$ è lineare, la sua dimensione (dim. di $V^{(k)}$) è 2 (k)

$\mathcal{C} \ni 0000 + x = x \in \mathcal{C}$

$0101 + 0101 = 0000 \in \mathcal{C}$

$0101 + 1010 = 1111 \in \mathcal{C}$

$1111 + 0101 = 1010 \in \mathcal{C}$

$1111 + 1010 = 0101 \in \mathcal{C}$

$$G = \begin{bmatrix} \boxed{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}} & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{bmatrix}$$

Matrice generatrice

$\mathcal{C} \ni x = u \cdot G$

- G è una matrice a elementi in $GF(2)$ di dimensione $k \times n \to 2 \times 4$
- Ciascuna riga di G deve essere una parola di codice
- Il rango di G deve essere k

$$G' = \begin{bmatrix} \boxed{\begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}} & \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix} \end{bmatrix}$$

$2^k \times n$

$$\begin{bmatrix} \cancel{0\,0\,0\,0} \\ 0\,1\,0\,1 \\ 1\,0\,1\,0 \\ \cancel{1\,1\,1\,1} \end{bmatrix}$$

$GF(q)$ esiste se e solo se $q = p^s$ con p primo, $s \geq 1$ intero

~~$GF(6)$~~

$GF(2)$

$GF(3)$

$GF(4)$

In $GF(p)$ con p primo: $GF(p) = \{0, 1, ..., p-1\}$

- l'addizione è l'addizione modulo p : $(\mathbb{Z}_p, +)$ è un gruppo
- la moltiplicazione è la moltiplicazione modulo p : $(\mathbb{Z}_p^*, *)$ è un gruppo

$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

$GF(3)$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$GF(4)$

$\{0, 1, \underset{\alpha}{2}, \underset{1+\alpha}{3}\}$

$2 \overset{?}{=} 1+1$ NO

Non posso avere ciò

$\underset{\neq 0}{x} \cdot \underset{\neq 0}{x'} = 0$ Moltiplico per x^{-1}

$x' = x^{-1} \cdot 0 = 0$

$\boxed{1+1=0}$

+	0	1	2 (α)	3 ($1+\alpha$)
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x \cdot x' = y$

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$\mathbb{Z}_4^*$

③ Il codice ternario ($\equiv$ in $GF(3)$) $\mathcal{C} = \{\overbrace{000000}^{n=6}, 012112, 021221\}$ è lineare?

$V^{(n)} = \{0,1,2\}^6 \qquad |\mathcal{C}| = 3 = |V^{(k)}| = 3^k \Rightarrow$ dobbiamo avere $k = 1$

$C(n,k)$

$C(6,1)$

$\forall x \in \mathcal{C}, \quad \forall a \in \{0,1,2\} \qquad a \cdot x \in \mathcal{C}$

$a \cdot 000000 = 000000 \in \mathcal{C}$

$a \cdot 012112$

$a \cdot 021221$

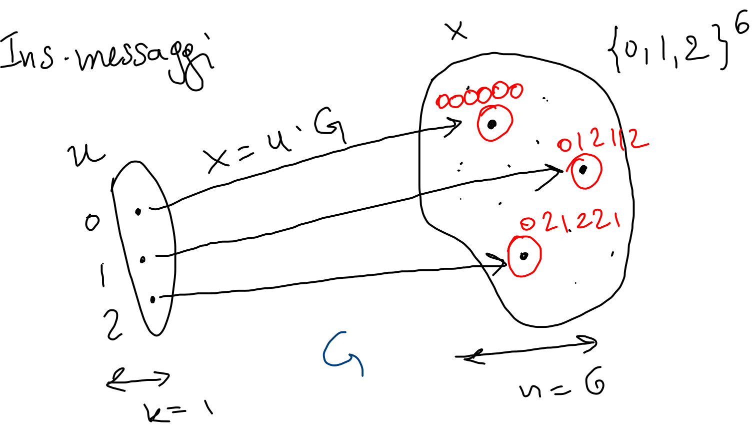
+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Se $a = 1$: $1 \cdot 012112 = 012112 \in \mathcal{C}$, $1 \cdot 021221 = 021221 \in \mathcal{C}$

$a = 2$: $\boxed{2 \cdot 012112 = 021221} \in \mathcal{C}$, $2 \cdot 021221 = 012112 \in \mathcal{C}$

ok



$\forall x, x' \in \mathcal{C}, \quad x + x' \in \mathcal{C}$

$012112 + 021221 = 000000 \in \mathcal{C}$

$012112 + 012112 = 2 \cdot 012112 \in \mathcal{C}$

$021221 + 021221 = 2 \cdot 021221 \in \mathcal{C}$

$\rightarrow \mathcal{C}$ è lineare.

$$\begin{bmatrix} \cancel{000000} \\ 012112 \\ \cancel{021221} \end{bmatrix}$$

$$u \longleftrightarrow k = 1$$

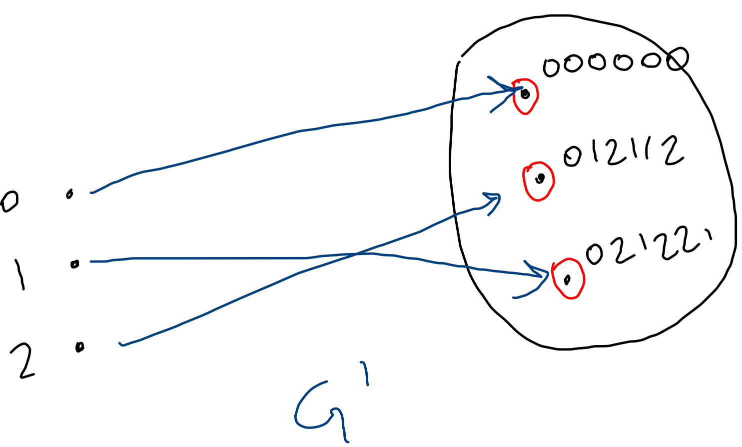
$$(k \times n)$$

$$G = [\,0 \;\; 1 \;\; 2 \;\; 1 \;\; 1 \;\; 2\,] \in \mathbb{F}_3^{1 \times 6}$$

G ha rango $1 = k$ ← x

$\underline{u}$			
0	$\cdot\ 012112$	$=$	000000
1	$\cdot\ 012112$	$=$	012112
2	$\cdot\ 012112$	$=$	021221

Se invece avessi scelto $G' = [\,0 \;\; 2 \;\; 1 \;\; 2 \;\; 2 \;\; 1\,]$



$$0 \cdot 021221 = 000000$$

$$1 \cdot 021221 = 021221$$

$$2 \cdot 021221 = 012112$$

④ Un codice binario di tipo $C(7,4)$ ha:

lineare

- 7 parole contenenti 3 simboli '1'
- 7 parole " 4 simboli '1'
- 1 parola " 7 simboli '1'

(a) Se il codice è usato solo per rilevare errori, quanti errori può rilevare?

(b) Qual è la probabilità di mancata rilevazione di errore nel canale $BSC(\varepsilon)$?

(a) $n=7$, $k=4$, $|\mathcal{C}| = 2^4 = 16$

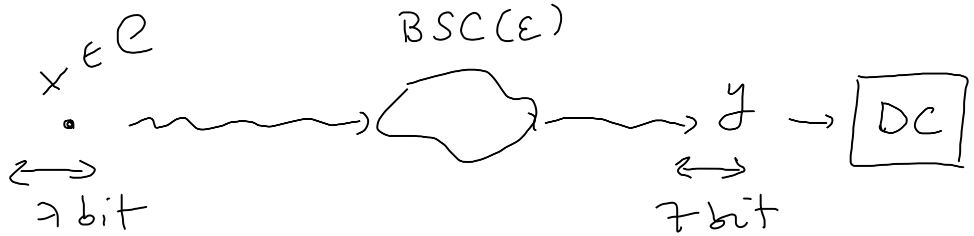
0000000	$\in \mathcal{C}$
0101001 ...	7 con 3 '1' → 3
...	7 con 4 '1' → 4
...	1 con 7 '1' → 7

$$\#\text{errori rilevabili} = d_{min} - 1$$

$$= \min_{\substack{x \neq x' \\ x, x' \in \mathcal{C}}} d_H(x, x') - 1$$

$$= \min_{e \neq \vec{0}} d_H(\underbrace{x - x'}_{e \in \mathcal{C}}, 0000000) - 1 = \min_{\substack{e \neq \vec{0} \\ e \in \mathcal{C}}} wt(e) - 1$$

$$= 3 - 1 = 2.$$



Vari casi a seconda di $d_H(x,y)$:

- Se $d_H(x,y)=0$, $y=x\in\mathcal{C}$: nessun errore rilevato

$$(1-\varepsilon)^7$$

- Se $d_H(x,y)=1$; $y\notin\mathcal{C}$ rilevo errore

$$\binom{7}{1}\varepsilon^1(1-\varepsilon)^6 = 7\varepsilon(1-\varepsilon)^6$$

- Se $d_H(x,y)=2$; $y\notin\mathcal{C}$ rilevo errore

$$\binom{7}{2}\varepsilon^2(1-\varepsilon)^5$$

Scenari in cui l'errore (se c'è) è rilevato

Se $d_H(x,y)\geq 3$

y potrebbe appartenere a $\mathcal{C}$

(non riesco a rilevare errore)

$$\left\{ \binom{7}{3}\varepsilon^3\underline{(1-\varepsilon)^4}+\binom{7}{4}\varepsilon^4(1-\varepsilon)^3+\binom{7}{5}\varepsilon^5(1-\varepsilon)^2+\binom{7}{6}\varepsilon^6(1-\varepsilon)+\binom{7}{7}\varepsilon^7 \right. = O(\varepsilon^3)$$

(5) Un codice lineare binario ha matrice generatrice:

$$G = \overset{n=2}{\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}} \; k=2$$

(1) Quante e quali sono le parole di codice? 4

(2) Qual è la distanza minima del codice? 6

(1) $V^{(n)} = \{0,1\}^9$ $n=9$ $k=2$ $V^{(k)} = \{0,1\}^2$ $|\mathcal{C}| = |V^{(k)}| = 2^2 = 4$

→ 4 parole di codice; quali sono?

$$\begin{array}{ll|l} x^{(1)} & 011011011 & 6 \\ x^{(2)} & 110110110 & 6 \\ x^{(3)} & 000000000 & \cancel{0} \\ x^{(4)} & 101101101 & 6 \end{array}$$

$d_{min} = \min_{e \neq \vec{0}} wt(e) = 6$

$01|1011011 \in \mathcal{C}$

$1011011|01 \in \mathcal{C}$

⑥ Data una matrice $k \times n$ G in $GF(2)$ che genera un codice lineare $\mathcal{C} = \{ \underbrace{u \cdot G}_{n} \mid \underbrace{u}_{k} \in \{0,1\}^k \} \subseteq \{0,1\}^n$

Mostrare che è sempre possibile trovare una matrice H di dimensioni $n \times (n-k)$ tale che $\mathcal{C} = \{ x \in \{0,1\}^n : x \cdot H = \vec{0} \}$.

Dim. $y \in \mathcal{C}^\perp$: $\boxed{x_1 y_1 + x_2 y_2 + \dots + x_n y_n = 0}$ $\forall x \in \mathcal{C}$

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

Prendo una qualunque base di $\mathcal{C}^\perp$: ottengo $n-k$ vettori di lunghezza n linearmente indipendenti

Chiamiamoli $y^{(1)}, y^{(2)}, \dots, y^{(n-k)} \in GF(2)^n$

$$H = \left[\begin{pmatrix} y^{(1)} \end{pmatrix} \begin{pmatrix} y^{(2)} \end{pmatrix} \begin{pmatrix} y^{(3)} \end{pmatrix} \begin{pmatrix} \; \end{pmatrix} \begin{pmatrix} \; \end{pmatrix} \cdots \begin{pmatrix} y^{(n-k)} \end{pmatrix} \right]$$

$\rightarrow$ ottengo $x \cdot H = \vec{0}$ $= [0 \; 0 \; \dots \; 0]$