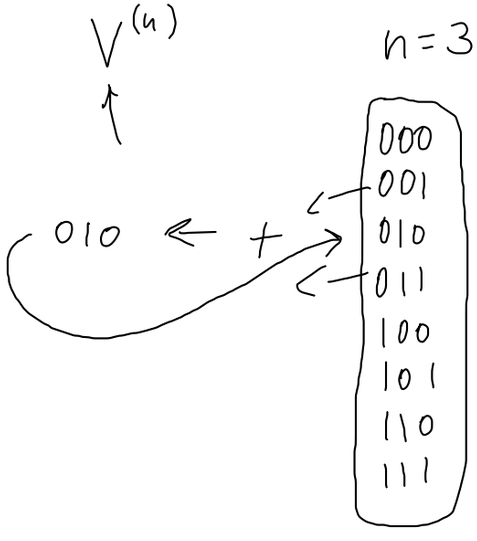
① Il codice binario (su $GF(2)$) $C = \{000, 010, 100, 111\}$ è lineare?



0 1

000

Se $x \in C$ allora $0 \cdot x \in C$ ✓ ←
$1 \cdot x \in C$ ✓

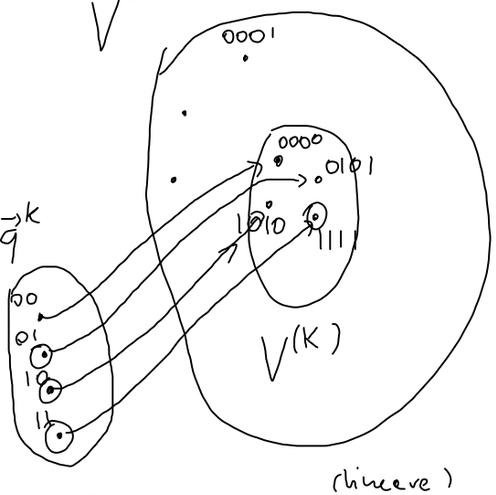
Se $x \in C, y \in C$ allora $x + y \in C$

$0 + y \in C \quad \forall y \in C$, banalmente

$010 + 100 = 110 \notin C$ ✗ $\Rightarrow$ C non è lineare

Galois Field	$GF(2)$	$+$ | 0 1 0 | 0 1 1 | 1 0	$\cdot$ | 0 1 0 | 0 0 1 | 0 1
Field	$\mathbb{F}_2$		

$\mathbb{F}_2^n$ ↓ $V^{(n)}$



(lineare)

Per un codice binario, $|C| = 2^K$ $\quad q^k$

Messaggi φ → Parole di codice

k → n

2^k

$+ \begin{bmatrix} 0101 \\ 1010 \\ 1111 \end{bmatrix}$ ↔ n

$k = 2$

Messaggi:

00 10

01 11

↔ 2

---

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

$\overleftrightarrow{n}$

$|C| = 4$

$0000 \in C$ ✓

$0101 + 1010 = 1111 \in C$ ✓

$0101 + 1111 = 1010 \in C$ ✓

$1010 + 1111 = 0101 \in C$ ✓

$0101 + 0101 = 0000 \in C$

$1010 + 1010 = 0000 \in C$

$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ ↕ $k = 2$

$k \times n$

↔ $n = 4$

$(0\,1)G = (0\,1\,0\,1)$

$(1\,0)G = (1\,0\,1\,0)$

$(1\,1)G = (1\,1\,1\,1)$

$0101 \leftarrow$

$1111 \leftarrow$

$0 \cdot 1111 = 0000$

$1 \cdot 1111 = 1111$

$0 \cdot 0101 = 0000$

$1 \cdot 0101 = 0101$

Dim $V^{(K)} \geq 2$

(esistono due vettori di C linearmente indipendenti)

Dim $V^{(K)} \leq 2$

(qualunque triple di vettori di C è linearmente dipendente)

$GF(q)$ esiste per ogni q della forma $q = p^s$, con p primo e $s \geq 1$ intero

$\mathbb{F}_2 \rightarrow GF(2)$ ✓

$\mathbb{F}_3 \rightarrow GF(3)$ ✓

$\mathbb{F}_7 \rightarrow GF(7)$ ✓

~~$\mathbb{F}_6$~~ ✗ $GF(6)$ No perché $6 = 2 \cdot 3$ non è potenza di un primo

$\mathbb{F}_{49}$ $GF(49)$ ✓ $49 = 7^2$

$\mathbb{F}_{2^s} \rightarrow (2^s)$ elementi

$\rightarrow GF(p)$ con p primo

Somma modulo p ↙ ↘ Prodotto modulo p

$\mathbb{F}_p = (\{0, 1, 2, \dots, p-1\}, +_p, \cdot_p)$

$\mathbb{F}_7$ $\quad -3 \stackrel{?}{=} 7 - 3 = 4 \pmod 7$

3^{-1} ? $\quad 3 \cdot 5 = 15 = 1 \pmod 7$ quindi $3^{-1} = 5$ in $\mathbb{F}_7$

③ Il codice ternario (su $\mathbb{F}_3$) $C = \{000000, 012112, 021221\}$ è lineare?

($n = 6$)

$V^{(n)} = \mathbb{F}_3^{\,6}$

$\forall x \in C \quad \forall \alpha \in \mathbb{F}_3 \quad \alpha \cdot x \in C$? ✓

$\forall x \in C \quad \forall y \in C \quad x + y \in C$? ✓

} sì, è lineare

$\alpha \in \{0, 1, 2\}$ $(\mathbb{F}_3)$

✓ ✓

$2 \cdot 000000 = 000000$ ✓

$\rightarrow 2 \cdot 012112 = 021221 \in C$ ✓

$2 \cdot 021221 = 012112 \in C$ ✓

Se $y \in C$ $\quad 0 + y \in C$ ✓

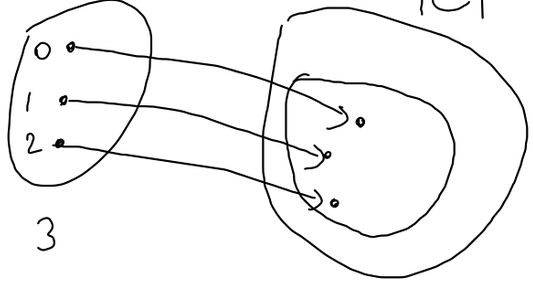
$012112 + 021221 = 000000 \in C$ ✓

$012112 + 012112 = 2 \cdot 012112$ ✓

$021221 + 012112$ ✓

$021221 + 021221 = 2 \cdot 021221$ ✓

Messaggi



$k = 1$

④ Un codice binario (lineare) $C(7,4)$ ($n=7$, $k=4$) {
- ha 7 parole con 3 '1' ← peso minimo è 3
- ha 7 parole con 4 '1'
- e 1 parole con 7 '1'

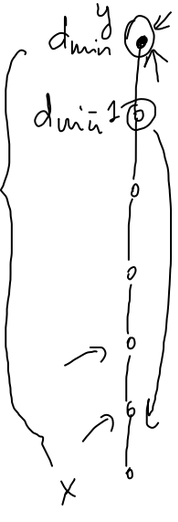
(a) Se il codice è usato solo per rilevare errori, quanti errori può rilevare?

(b) Qual è la probabilità di mancato rilevazione in un canale binario simmetrico $BS(\varepsilon)$?

(a) $= d_{min} - 1$ (# errori rilevabili)

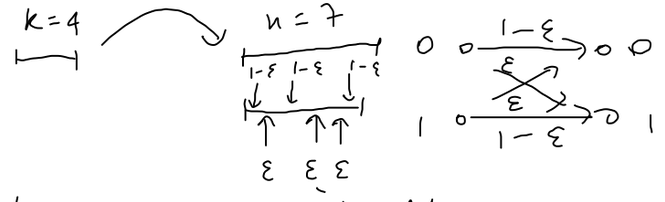
$d_{min} = \min_{x,y \in C} d_H(x,y)$

(lineare) $= \min_{\substack{z \in C \\ z \neq 000..0}} d_H(000\ldots0, z) = \min_{\substack{z \in C \\ z \neq 00..0}} wt(z) = 3$ (peso di z)



Rilevo fino a 2 errori

(b)



$0 < \varepsilon < 1/2$

Mancato rilevazione con più di 2 errori : $\binom{7}{3}\varepsilon^3(1-\varepsilon)^4 + \binom{7}{4}\varepsilon^4(1-\varepsilon)^3 + \binom{7}{5}\varepsilon^5(1-\varepsilon)^2 + \binom{7}{6}\varepsilon^6(1-\varepsilon) + \binom{7}{7}\varepsilon^7 = O(\varepsilon^3)$

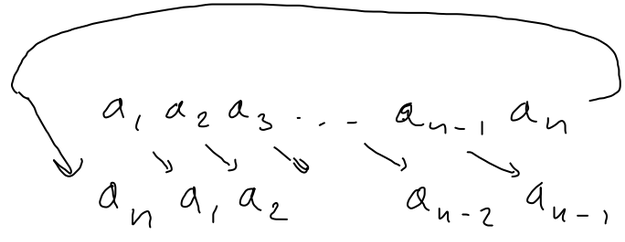
⑤ Un codice lineare di canale (binario) ha matrice generatrice

$\mathbb{F}_2$

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

$k \times n$ (2 × 9)

$u \cdot G = x \in C$



(1) Quante e quali sono le parole del codice

((2) Il codice è ciclico ?) Sì

(3) Qual è distanza minima del codice ?

(1) Le parole di codice sono $2^k = 2^2 = 4$.

Le parole di codice sono tutte e sole le n-ple binarie della forma $x = u \cdot G$ dove u è un messaggio di lunghezza k

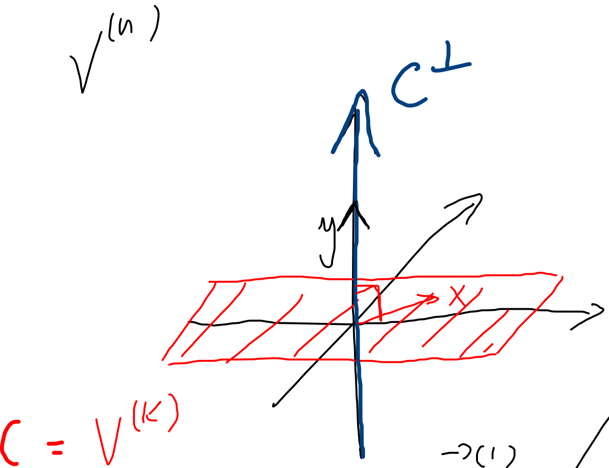
$(0\ 0)G = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$
$(0\ 1)G = (1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0)$
$(1\ 0)G = (0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1)$
$(1\ 1)G = (1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1)$

$$\left\{ \begin{array}{l} 000000000 \\ 110110110 \\ 011011011 \\ 101101101 \end{array} \right\} = C$$

6
6
6

$\rightarrow d_{min} = 6$

Data una matrice $k \times n$ G con elementi in $GF(2)$ che genera un codice lineare $C = \{ u \cdot G \mid u \in \{0,1\}^k \}$ mostrare che è sempre possibile trovare una matrice H $n \times (n-k)$ tale che $C = \{ x \in \{0,1\}^n : x \cdot H = \vec{0} \}$



$y \in C^\perp : x_1 y_1 + x_2 y_2 + \dots + x_n y_n = 0 \quad \forall x \in C$

Considero una base di $C^\perp$; $\dim(C^\perp) = \dim(V^{(n)}) - \dim(V^k) = n - k$

contiene $n-k$ vettori riga linearmente indipendenti

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

$(0\,1\,0\,0\,1\,1 \; \dots \;)$ con componenti $y_1\, y_2 \; \dots \; y_n$