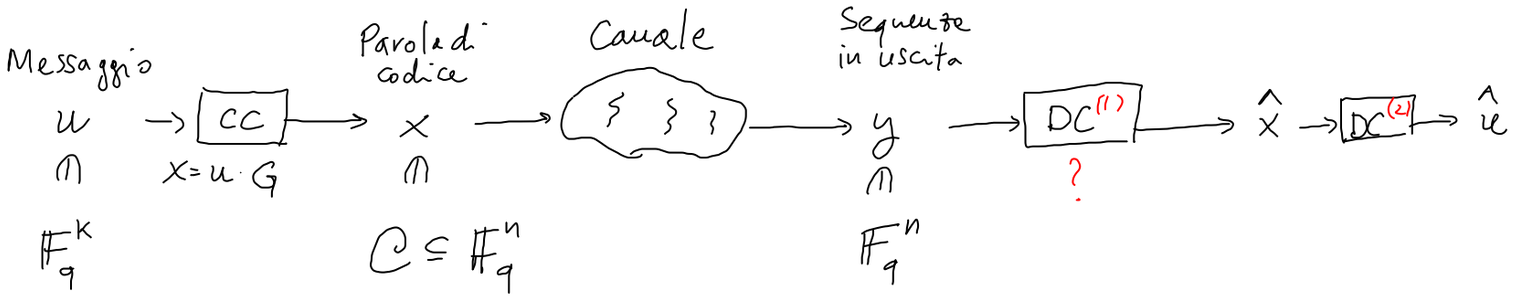
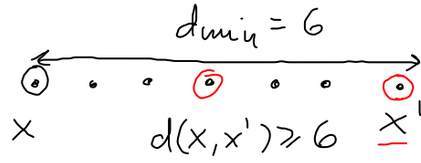
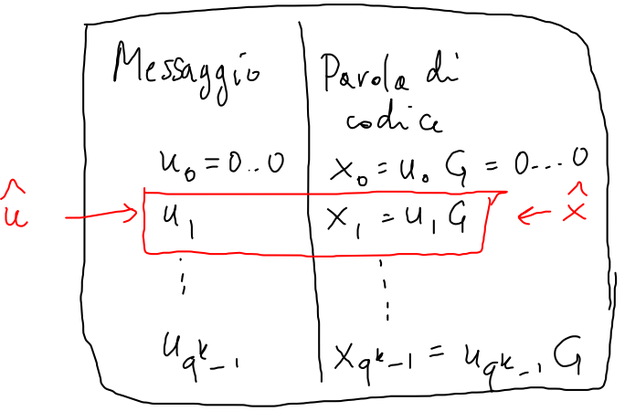
Decodifica di Codici Lineari







Matrice di controllo H $\quad (n-k) \times n$

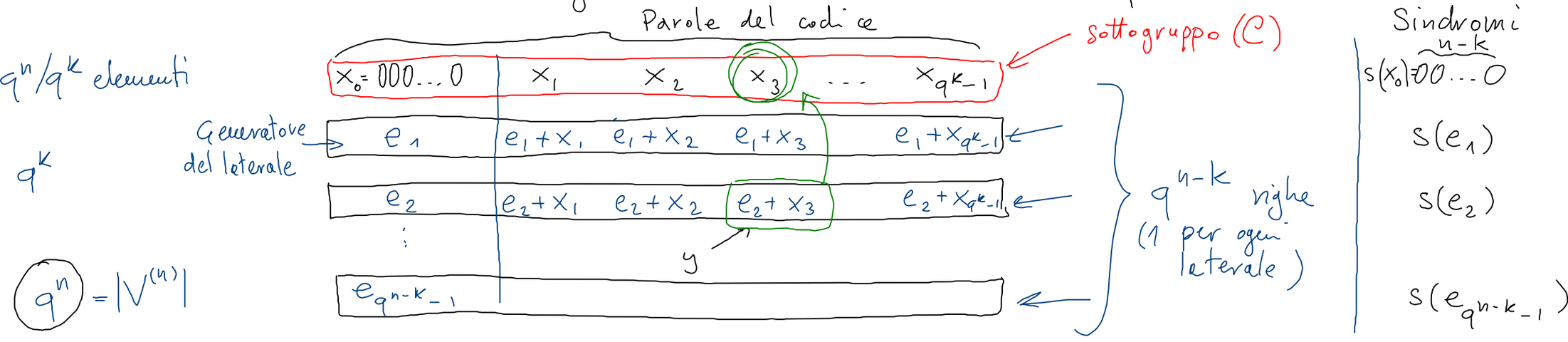
$$\underset{(n-k)\times n}{H}\ \underset{(n\times 1)}{y^T} = \underset{(n-k)\times 1}{s(y)}$$ sindrome di y

Le equaz. di controllo sono tutte soddisfatte $\iff s(y) = \vec{0}$

$$s(e_i + x_j) = H(e_i + x_j)^T = H e_i^T + \cancel{H x_j^T}^{0} = s(e_i)$$

Come correggere gli errori ?

Costruiamo la seguente tabella (tabella di Slepian)



$(V^{(n)}, +)$ è un gruppo

$V^{(n)}$ è uno spazio vettoriale; $\mathcal{C}$ è un sottospazio di $V^{(n)}$

$(\mathcal{C}, +)$ è un sottogruppo di $(V^{(n)}, +)$; qualunque gruppo è partizionabile attraverso i suoi laterali: laterale rispetto a un sottogruppo $\mathcal{H}$ è un sottoinsieme del gruppo i cui elementi y possono essere scritti nella forma $y = x + e$ dove e (fissato) è un elemento del gruppo e $x \in \mathcal{H}$

↑ addizione tra sequenze

Due elementi e ed y sono sulla stessa riga della tabella

$\Leftrightarrow \quad y - e \in C \quad \Leftrightarrow \quad s(y-e) = \vec{0}$

Ricostruiamo $\hat{x}$ cercando le parole di codice nelle stesse colonne della sequenza ricevuta y. ($\hat{x}$ è nella prima riga).

La decodifica dipende dalla scelta dei generatori dei laterali.

Esempio (6.7). $n=4, k=2, q=2$. $G = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$; $H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ $(HG^T = 0)$

Tabelle di Slepian

				$\hat{x}$	sindromi	
	0000	0110	1011	1101	00	$= Hx^T$
$e_1 \rightarrow$	1111	1001	0100	0010	11	$= He_1^T$
$e_2 \rightarrow$	1000	1110	0011	0101	10	$= He_2^T$
$e_3 \rightarrow$	0111	0001	1100	1010	01	$= He_3^T$

$H \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$

$x = 0110$
$y = 0111$
$e_{canale} = 0001$
$e = 0111$
$\hat{x} = 0111 - 0111$
$= 0000$

Se ricevo 0010
restituisco $\hat{x} = 1101$

Ricevo $0010 = y$
Calcolo $s(y) = Hy^T$
$= H(e_1 + \hat{x})^T = He_1^T = s(e_1) = 11$
Restituisco $\hat{x} = y - e_1 = 0010 - 1111$
$= 1101$

Procedura di decodifica con sindrome (correzione d'errore per codici lineari)

1. Ricevi y dal canale e calcola la sindrome $s(y) = Hy^T$
2. Se $s(y) = \vec{0}$, restituisci $\hat{x} = y$
3. Altrimenti, identifica il generatore e tale che $s(e) = s(y)$ (attraverso la tabelle)
   Restituisci $\hat{x} = y - e$

Probabilità di corretta decodifica: $P_{corr} = \sum_{\substack{e : e \text{ è uno} \\ \text{dei generatori}}} p(\text{conf. d'errore sul canale uguale a } e)$

$$\longrightarrow = \sum_{e : \text{generatori}} \varepsilon^{wt(e)} (1-\varepsilon)^{n-wt(e)}$$

$$= \sum_{e : \text{generatori}} \left(\frac{\varepsilon}{1-\varepsilon}\right)^{wt(e)} (1-\varepsilon)^n$$

$x \longmapsto x + \textcircled{e} = y$

$y \longmapsto y - \textcircled{e}$

$\left(\frac{\varepsilon}{1-\varepsilon} < 1 \text{ in quanto } \varepsilon < 1/2\right)$

Per avere P_{corr} alta, voglio $\left(\frac{\varepsilon}{1-\varepsilon}\right)^{wt(e)}$ sia alta

$\longrightarrow$ voglio $wt(e)$ basso.

$$p_{corr} = \sum_{w=0}^{n} n_w \, \varepsilon^w (1-\varepsilon)^{n-w}$$

n_w → numero dei generatori di peso w

Osservazione: le colonne della tabella di Slepian corrispondono alle regioni di decodifica.

Def. Un codice lineare è detto **perfetto** se le sfere di Hamming di raggio $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ centrate sulle parole di codice partizionano $V^{(n)}$

$$S_t(x) \cap S_t(x') = \emptyset$$
$$\bigcup_{x \in C} S_t(x) = V^{(n)}$$

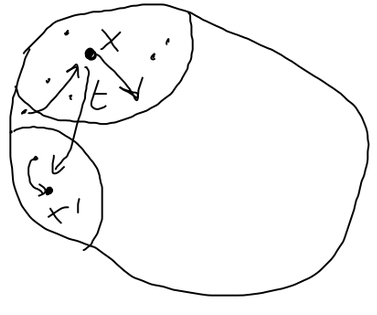
Perché questo accada:

$$q^n = \underbrace{vol(V^{(n)})}_{\#\text{ di } n\text{-ple}} = \underbrace{vol(S_t)}_{\#\text{ di elementi di } S_t} \times \underbrace{(\#\text{ di sfere})}_{|C| = q^k}$$

q^n

d_{min} → corregge sicuramente $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ errori (in qualunque configurazione)

La sfera di Hamming di raggio t centrata in $x \in C$ è contenuta nella regione di decodifica associata ad x.

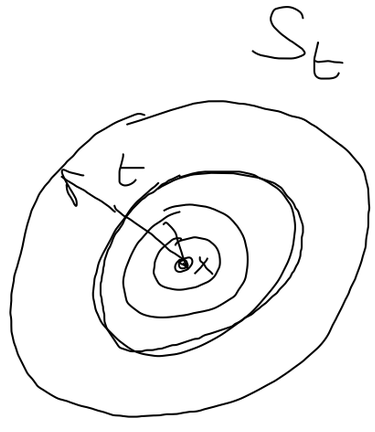


$\longrightarrow$ per avere un codice perfetto, serve che

$$vol(S_t) = q^n / q^k = q^{n-k}$$

$$\| $$

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$



Esempio. Il codice

$C(5,1)$ a ripetizione

$C = \{00000, 11111\}$

è perfetto.

$\binom{n}{1}$

$\binom{n}{2}$

$x_1 \dots x_n$ 1

0/1

Per ottenere un elemento a distanza i da x, scelgo i posizioni tra le n possibili e per ciascuna scelgo uno dei $q-1$ simboli alternativi possibili.