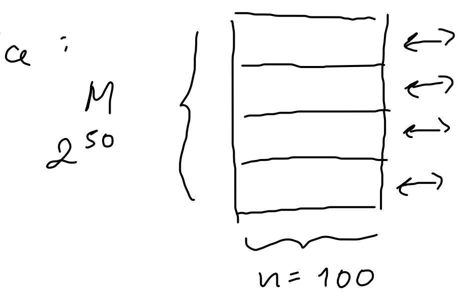
Codici correttori d'errore

Codici aleatori ("destrutturati") non sono pratici

Es. $n = 100$, $R = 1/2$ $\rightarrow$ $R = \dfrac{\log_q M}{n} = \dfrac{\log_2 M}{n} \leftrightarrow M = 2^{nR} \rightarrow M = 2^{100 \cdot 1/2} = 2^{50} \approx 10^{15}$

$q = 2$

Tabelle del codice:



$\rightarrow$ Struttura algebrica sull'insieme di parole di codice $\mathcal{C}$

$$M = |\mathcal{C}| \leq q^n$$

Assumeremo che $A = \{a_1, a_2, \dots, a_q\}$ sia un campo finito con $q = p^r$ potenza di un numero primo p
$GF(q)$

e A^n $(\vec{q}^{\,n})$ sia uno spazio vettoriale su $GF(q)$.

Esempio: $A = \{0, 1\}$ $q = 2$

$GF(2)$: $+$ $\cdot$ $\rightarrow$ $0+0=0$, $0+1=1$, $1+0=1$, $1+1=0$

$0 \cdot 0 = 0$, $0 \cdot 1 = 0$, $1 \cdot 0 = 0$, $1 \cdot 1 = 1$

Sequenze lunghe n : $A^n = \{0,1\}^n$ spazio vettoriale su $GF(2)$

Esempio: $x = 001 \in A^n$, $y = 101 \in A^n$ $\rightarrow$ $x + y = 100$

Richiami di strutture algebriche

Insieme S, legge di composizione interna per S è una funzione $f: B \rightarrow S$ con $B \subseteq S \times S$

Semigruppo: $(S, *)$ con $*$ associativa

Esempio: $(A^+, \circ)$ con $\circ$ la concatenazione tra sequenze

$\uparrow$ insieme di tutte le sequenze su A di lunghezza ≥ 1

$A = \{a, b, c\}$

$A^+ = \{a, b, c, aa, ab, ac, ba, bb, \dots, aaa, aab, \dots\}$ $ab \circ cca = abcca$

Monoide : semigruppo dotato di elemento neutro

($u \in S$ è elemento neutro : $x * u = u * x = x \quad \forall x \in S$).

Gruppo : monoide in cui ogni $g \in S$ ha un inverso g^{-1} :

$$g * g^{-1} = g^{-1} * g = 1 \leftarrow \text{(l'elemento neutro)}$$

Esempio : $S = \{0, 1, 2\}$

$*$ = somma modulo 3

Elemento neutro : 0

g		$-g$	
0	$\to$	0	$0+0 = 0 \pmod 3$
1	$\to$	2	$1+2 = 0 \pmod 3$
2	$\to$	1	$2+1 = 0 \pmod 3$

Sottogruppo H di un gruppo G è un sottoinsieme $H \subseteq G$ tale che :

$$a * b^{-1} \in H \quad \forall a, b \in H$$

Esempio : $G = (\{0,1,2,3\}, +_{mod 4})$ $\to$ somma modulo 4

$H = (\{0, 2\}, +_{mod 4})$

$0 +_{mod 4} (-2) \overset{?}{\in} H \longleftrightarrow \overbrace{0+2}^{2} \pmod 4 \in H$

$0 + (-0) \in H$

$2 + (-0) \in H$

$2 + (-2) \in H$

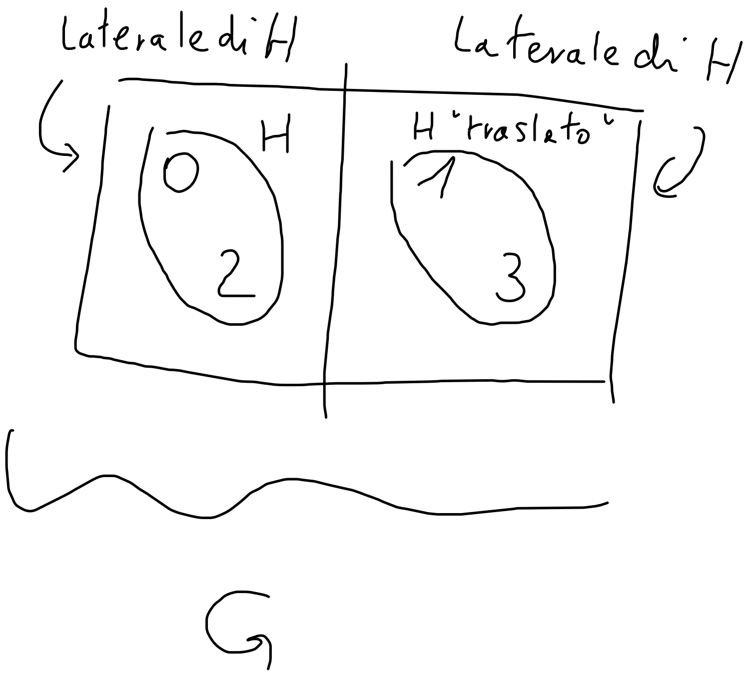
Laterali di un sottogruppo :

un laterale di un sottogruppo H di un gruppo G è un insieme di elementi di G della forma $y = x + h$ con h fissato e $h \in H$ $(x, y \in G)$

Due elementi di G sono nello stesso laterale (di H) se e solo se $y - x \in H$.

Nell'esempio precedente : $G = (\{0,1,2,3\}, +_{\text{mod } 4})$

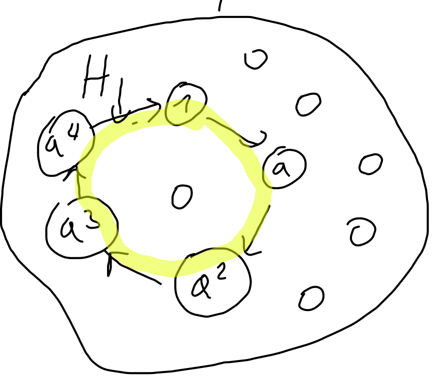
$H = (\{0,2\}, +_{\text{mod } 4})$



$x = 0$

$y - 0 \in H$

$1 - 3 = 2 \mod 4$



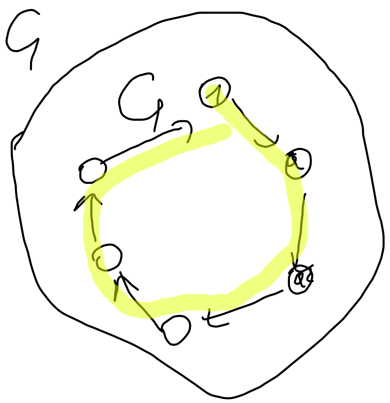
Gruppo ciclici : $(G, \cdot)$ gruppo <u>finito</u> ($\rightarrow$ numero di elementi di G è finito)

Per qualunque $a \in G$,

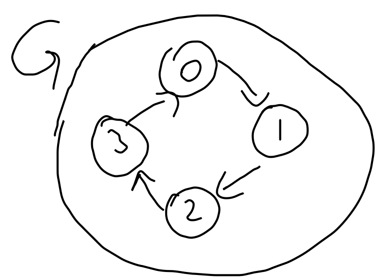
$H = \{1, a, a^2, a^3, \dots\}$ forma un sottogruppo di G (sottogruppo ciclico)

$$a \cdot a^{-3} = a^{-2} = (\underbrace{a^2}_{\in H})^{-1} \in H$$

Se perqualche a ottengo tutto G, allora G è un gruppo ciclico.



Esempio. $G = (\{0, 1, 2, 3\}, +_{mod\,4})$ è un gruppo ciclico:



Prendo $a = 1$

$a + a \mod 4 = 2$

$a + a + a \mod 4 = 3$

$a + a + a + a \mod 4 = 0$

$H = \{0, 1, 2, 3, 0\}$

$= \{0, 1, 2, 3\} = G$

Anello: $(R, +, \cdot)$ con $(R, +)$ gruppo commutativo
e $(R, \cdot)$ semigruppo
e inoltre: $a(b+c) = ab + ac \quad \forall a,b,c \in R$
$(b+c)a = ba + ca \quad \forall a,b,c \in R$

<u>Campo</u>: un anello $(R, +, \cdot)$ in cui $(R \setminus \{0\}, \cdot)$ è un gruppo commutativo
($\rightarrow$ ogni elemento $\neq 0$ ha un inverso moltiplicativo)

Esempio: $GF(2)$ $R = \{0, 1\}$ $R \setminus \{0\} = \{1\}$ è un gruppo commutativo
è un campo

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$x \cdot 0 = 1$
$0 \cdot x = 1$

$\cdot$	1
1	1

$1^{-1} = 1$

Spazio vettoriali G su un campo F:

$\forall \alpha, \beta \in F \quad \forall x, y \in G$:
$$\alpha(x+y) = \alpha x + \alpha y \in G$$
$$\alpha(\beta x) = (\alpha\beta) \cdot x \in G$$
$$(\alpha+\beta) x = \alpha x + \beta x \in G$$

$\vec{x}$ $\longrightarrow$ Canale $\longrightarrow$ $\vec{y}$

In termini di vettori, posso scrivere

$$\vec{y} = \vec{x} + \vec{e}$$

vettore di errore

$$\boxed{\vec{e} = \vec{y} - \vec{x}}$$

Esempio su GF(2) : $x = 01101$
$y = 10101$

$e = 11000 = y - x$
$\vec{0} = 00000$

Nel caso binario, la differenza modulo 2 equivale alla somma modulo 2.

(Esempio : $1-1=0 = 1+1=0$
$1-0=1 = 1+0=1$)

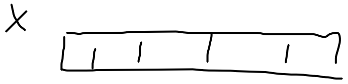
Distanza di Hamming

$$d_H(\vec{x},\vec{y}) = d_H(\vec{y}-\vec{x}, \vec{0}) = d_H(\vec{e}, \vec{0}) =$$ numero di componenti diverse da 0 nel vettore $\vec{e}$
("peso" del vettore $\vec{e}$)

Peso di $\vec{e}$ è indicato con $wt(\vec{e})$
("weight")

Alfabeto di q simboli

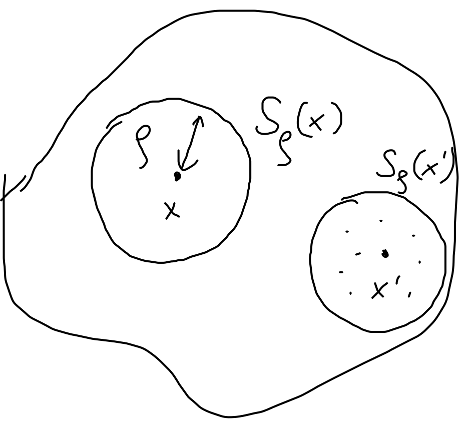
Sfera di Hamming $\quad S_\rho(x) = \{ y : d_H(x,y) \le \rho \}$

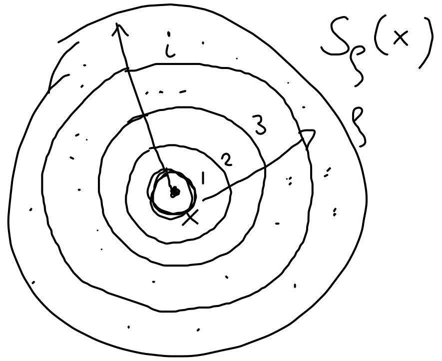


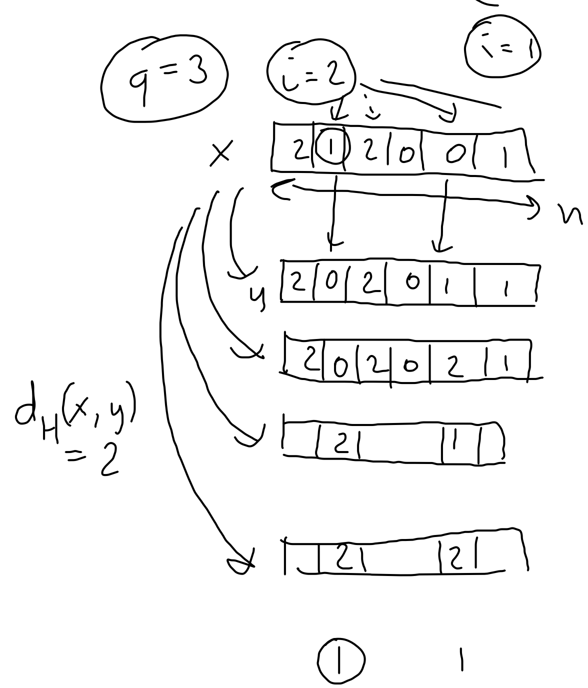
$\le \rho$ simboli modificati
Quante diverse sequenze posso ottenere?
Questo è $Vol(S_\rho(x))$

Volume : $\quad Vol(S_\rho(x)) = |S_\rho(x)| = \sum_{i=0}^{\rho} \binom{n}{i} (q-1)^i$

Se x è lunga n
Se ho q simboli







Stime : per ogni n sufficientemente grande

$$Vol(S_\rho) \le q^{n h_q(\rho/n)}$$

$$h_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$$

$$h_q(x) = x \log_q (q-1) - x \log_q x - (1-x) \log_q (1-x)$$

$q = 2$

$$Vol(S_\rho) \le 2^{n h_2(\rho/n)}$$

$\rho \le n/2$