- Codifica di sorgente
  - Possibilità teoriche — CAP. 3
  - Costruzione di codici di sorgente — CAP. 5
- Codifica di canale
  - Possibilità teoriche — CAP. 4
  - Costruzione di codici di canale (codici correttori d'errore) — CAP. 6

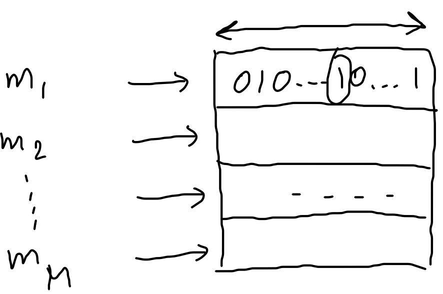
CODICI CORRETTORI D'ERRORE

Esempio. Vogliamo un codice di canale con $q = 2$ (binario)

$R = 1/2$, $n = 100$

Spazio delle possibili sequenze: $\{0,1\}^n$ $\quad |\{0,1\}^n| = 2^{100}$

Quante parole di codice ci occorrono? M $\qquad R = \frac{\log_q M}{n}$



$2^{50} \approx 10^{15}$ parole di codice

$$M = 2^{50} \xleftarrow[n=100]{R=1/2} M = 2^{nR} \xleftarrow{q=2} nR = \log_q M$$

Abbiamo bisogno di <u>struttura</u>

Introdurremo una struttura algebrica:

Assumeremo che l'alfabeto di canale $\mathcal{A}$ sia un campo finito

$\mathcal{A} = \{a_1, a_2, \dots, a_q\}$

Galois field

Indichiamo un campo finito su q elementi con $GF(q)$

q deve essere una potenza di un primo: $q = p^k$ per qualche numero primo p e qualche intero $k \geq 1$

somma di elementi nel campo

$\longrightarrow$ $(\mathcal{A}, +, \cdot)$

prodotto di elementi nel campo

Conseguenze: l'insieme $\mathcal{A}^n$ può essere dotato di una struttura di spazio vettoriale

$(\mathcal{A}^n, +, \cdot)$ prodotto tra un elemento del campo e un elemento dello spazio vettoriale

somma di elementi (sequenze) dello spazio vettorale

$$(a_{i_1}, a_{i_2}, \dots, a_{i_n}) + (b_{j_1}, b_{j_2}, \dots, b_{j_n}) = (a_{i_1}+b_{j_1}, a_{i_2}+b_{j_2}, \dots, a_{i_n}+b_{j_n})$$

$GF(q)$

prodotto nel campo

$$\alpha \cdot (a_{i_1}, \dots, a_{i_n}) = (\alpha \cdot a_{i_1}, \dots, \alpha a_{i_n})$$

prodotto nello spazio vettoriale per uno scalare

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

$GF(2)$

$+$	0	1
0	0	1
1	1	0

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

Sequenze di lunghe~~zza~~ n:

(A^n) $\quad n = 3$:

$x = 001 \in A^n$

$y = 101 \in A^n$

$x + y = 100$

$1 \cdot y = 101$

$0 \cdot y = 000$

Richiami di strutture algebriche

Insieme S, una legge di composizione interna per S è una funzione $f : B \to S$

$B \subseteq S \times S$

Semigruppo : $(S, *)$ $\quad * : S \times S \to S$

con $*$ associativa : $a * (b * c) = (a * b) * c$

$\forall a, b, c \in S$

Esempio : $S = A^+$, per qualche alfabeto A

$*$ = concatenazione di sequenze

$A = \{a, b, c\}$ $\quad aba \in S$

$cc \in S$ $\quad \rightarrow \quad aba * cc = abacc$

$((aba)cc)b = (aba)(cc(b))$

Monoide : un semigruppo $(S, *)$ dotato di elemento neutro :

elemento 1_S tale che : $1_S \cdot a = a \cdot 1_S \quad \forall a \in S$

Esempio : Insieme A^* di tutte le sequenze sull'alfabeto A di lunghezza maggiore o uguale a zero.

sequenza vuota λ : $(aba) * \lambda = aba$

Gruppo : un monoide $(S, *, 1_S)$ tale che ogni elemento $a \in S$ ammette un inverso a^{-1} tale che : $a * a^{-1} = 1_S$

$$a^{-1} * a = 1_S$$

A volte, per i gruppi si usa alternativamente la notazione additiva:
(specialmente per gruppi commutativi)

$(S, +, 0_S)$, inverso di a è denotato con $-a$

$$a + (-a) = 0_S \qquad (-a) + a = 0_S .$$

somma modulo 4

Esempio. $G = (\{0,1,2,3\}, +, 0)$

Inverso di 0 è 0 $\quad 0+0=0$
1 è 3 $\quad 1+3=0$
2 è 2 $\quad 2+2=0$
3 è 1 $\quad 3+1=0$

$\to$ è un gruppo (commutativo)

Sottogruppo H di un gruppo $(G, *, 1_G)$

È un sottoinsieme $H \subseteq G$ tale che $(H, *, 1_G)$ è a sua volta un gruppo.

In particolare, se $a \in H \to a^{-1} \in H \to * \quad a * a^{-1} = 1_G \in H$

$b \in H \to b^{-1} \in H$

$\to a * (b^{-1})^{-1} \in H$

$a * b \in H$

Esempio.

$\to G = (\{0,1,2,3\}, +, 0)$

$\{1,3\}$ $\quad H = (\{0,2\}, +, 0)$ è un sottogruppo

$(\{0,1,3\}, +, 0)$ non è un sottogruppo

$2-0=2 \in H$
$0-2=2 \in H$
$0-0=0 \in H$
$2-2=0 \in H$

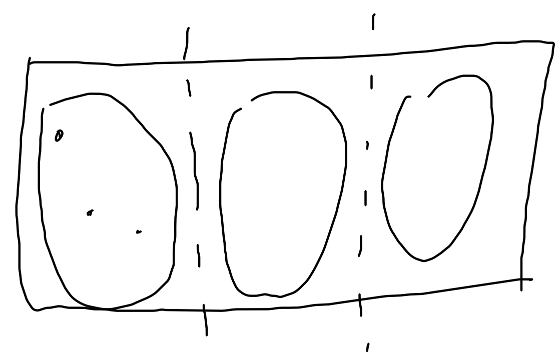
Laterali di un sottogruppo:

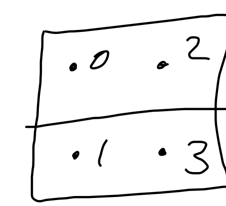
un laterale di un sottogruppo H di un gruppo G è un insieme di elementi della forma $y = x + h$ con $h \in H$, per qualche x fissato ($x \in G$).

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

Nell'esempio precedente, $G = (\{0,1,2,3\}, +, 0)$

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





Ho due laterali di H:

$\{0,2\}$ perché $\begin{cases} 0-2 \in H \\ 0-0 \in H \\ 2-0 \in H \\ 2-2 \in H \end{cases}$

$\{1,3\}$ perché $\begin{cases} 3-1 \in H \\ 1-1 \in H \\ 1-3 \in H \\ 3-3 \in H \end{cases}$

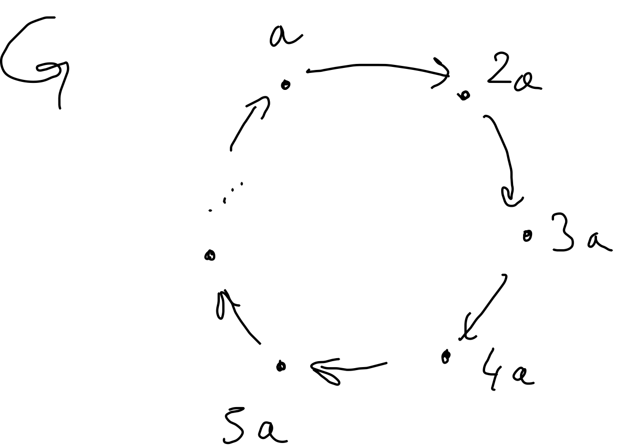
Gruppi ciclici:

Un gruppo $(G, +, 0)$ è detto <u>ciclico</u> se esiste un elemento $a \in G$ tale che l'insieme

$$\{0, a, \underbrace{2a}_{a+a}, \underbrace{3a}_{a+a+a}, 4a, 5a, \dots\}$$ coincide con G.

Esempio. $G = (\{0,1,2,3\}, +, 0)$ è ciclico in quanto scegliendo $a = 1$ ho

$$\{0, a, 2a, 3a, 4a, 5a, \dots\} = \{0,1,2,3\} = G.$$



Anello : $(R, +, \cdot)$ dove $(R, +, 0)$ è un gruppo commutativo

e $(R, \cdot, 1)$ è un semigruppo

e inoltre : $a(b+c) = ab + ac$ $\forall a, b, c \in R$

$(b+c)a = ba + ca$

Campo : un anello $(R, +, \cdot)$ in cui

$(R \setminus \{0\}, \cdot, 1)$ è un gruppo commutativo

(in particolare, ogni elemento in R diverso da 0 ha un inverso :

$a \rightsquigarrow a^{-1}$ tale che $a \cdot a^{-1} = 1$)

Esempio. $GF(2)$ $R = \{0, 1\}$ $R \setminus \{0\} = \{1\}$

$+$	0	1
0	0	1
1	1	0

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

$\cdot$	1
1	1

Spazio vettoriale G sul campo F ← field

$GF(q)$

$\mathbb{F}$

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

$$\alpha \cdot (\beta \cdot x) = (\alpha \beta) \cdot x$$

moltipl. nel campo

moltiplic. scalari
nello spazio vettoriale

$$(\alpha + \beta)\, x = \alpha x + \beta x$$

Somma nel
campo F

somma
nello spazio vettoriale G

$$\vec{x} \longrightarrow \boxed{\text{Canale}} \longrightarrow \vec{y}$$
$$\vec{x} \in \mathcal{A}^n \qquad \vec{y} \in \mathcal{A}^n$$

In termini di vettori,

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

vettore di errore (seq. di errore)

Esempio: $x = 01101$

$y = 10101$

$y - x = 11000 = e$

$\mathbb{F} = GF(2)$

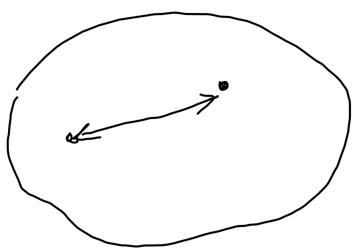
$\mathcal{A} = \{0,1\}$

Osservazione: nel caso binario, la somma di vettori coincide con la differenza di vettori:

$$y - x = y + x$$

+	0	1
0	0	1
1	1	0

Spazio delle sequenze $\mathcal{A}^n$: a questo punto lo interpretiamo come uno spazio vettoriale (Spazio di Hamming)



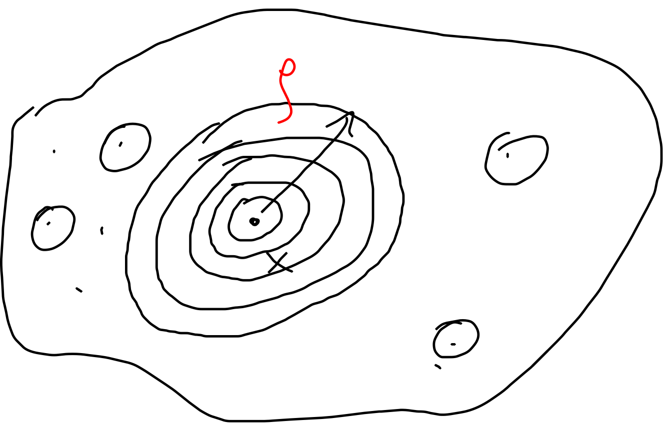
Distanza di Hamming: $d_H(x,y) = d_H(\overbrace{y-x}^{e}, \vec{0})$

\# posizioni i tali che $x_i \neq y_i$

$=:$ peso del vettore e

(\# simboli di e diversi da 0)

Alfabeto di q simboli



$S_\rho(x) =$ ins. seq. y tali che $d_H(x,y) \leq \rho$

$= \{ y \in A^n : d_H(x,y) \leq \rho \}$

$|S_\rho(x)| \leq 2^{n h_2(\rho/n)}$ nel caso binario

$|S_\rho(x)| \leq q^{n h_q(\rho/n)}$ nel caso q-ario

$(\rho \leq (1 - 1/q)\, n)$