Appunti di Teoria dei Codici

Fabio Rinnone

12 giugno 2013

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

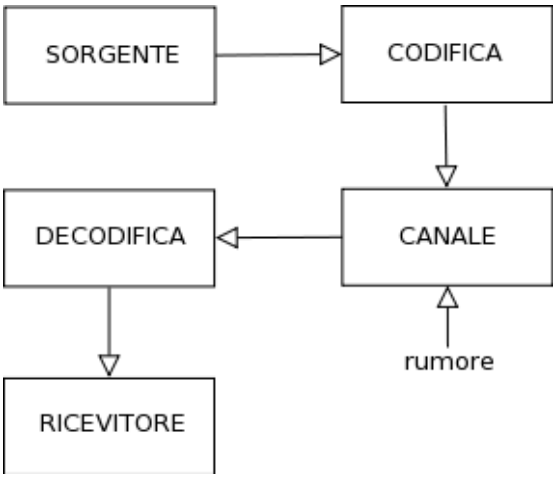

Figura 1.1: Schema comunicazione tra sorgente e ricevitore.

Definizione 1.1 (Alfabeto)**.** Un alfabeto $\mathcal{A}$ è un insieme *finito* di simboli.

Esempio 1.1. $\mathcal{A} = \{a_1, \ldots, a_n\}$.

Definizione 1.2 (Parola)**.** Una parola è una *sequenza* finita di elementi dell'alfabeto.

Esempio 1.2. $\mathcal{A}_k =$ insieme delle parole di lunghezza k, $k \in \mathbb{N}$.

Esempio 1.3. $\mathcal{A}_1 = \mathcal{A}$.

Esempio 1.4. $\mathcal{A}_2 = \{a_1a_1, a_1a_2, \ldots, a_na_n\} = \{\ldots, a_ia_j \ldots\}$, $1 \leq i, j \leq n$.

Osservazione 1.1. L'insieme di tutte le parole è infinito.

Definizione 1.3. Una parola formata da k simboli (dell'alfabeto) si dirà di lunghezza k.

Osservazione 1.2. A_n è l'insieme delle parole di lunghezza n.

Definizione 1.4. Un sottoinsieme di $\mathcal{A}_n$ si dirà *codice* (a blocchi di lunghezza n).

Esempio 1.5. Sia $\mathcal{C} = \{00\ldots0\}$. In questo caso tutte le parole contententi 1 sarebbero corrette.

Esempio 1.6. Sia $\mathcal{C}' = \mathcal{A}_n$. In questo caso tutte le parole sarebbero interpretate come corrette.

Un codice deve garantire le seguenti proprietà.

1. Codifica veloce.
2. Facile trasmissione del messaggio.
3. Decodifica veloce del messaggio ricevuto.
4. Rilevazione e correzione degli errori.
5. Massimo trasferimento dell'informazione.

Esempio 1.7. $\mathcal{C} = \{0, 1\}$.

Esempio 1.8. $\mathcal{A}_2 = \{00, 01, 10, 11\},\ \mathcal{C} = \{00, 11\}$.

Osservazione 1.3. Il codice dell'esempio 3.1 è in grado di rilevare errori di lunghezza 1. Tale codice non rileva errori di lunghezza 2.

Esempio 1.9. $\mathcal{A}_3 \supseteq C = \{000, 111\}$.

Osservazione 1.4. Il codice dell'esempio 1.9 è in grado di rilevare errori di lunghezza 1 e di correggerli.

Definizione 1.5. Un codice a blocchi è un codice in cui tutte le parole sono della stessa lunghezza.

Definizione 1.6. Un codice binario è un codice in cui l'alfabeto utilizzato è $\{0, 1\}$.

Capitolo 2

Codici lineari

Definizione 2.1. Un campo $\mathbb{K}$ è una struttura algebrica nella quale sono definite due operazioni: somma e prodotto $(+, \cdot)$ tali che:

- La somma $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ gode delle seguenti proprietà.
  - $\forall x, y, z \in \mathbb{K}$ si ha $(x + y) + z = x + (y + z)$.
  - Esiste lo zero, indicato con $0 \in \mathbb{K}$, tale che $x + 0 = 0 + x = x \ \forall x \in \mathbb{K}$.
  - Esiste l'opposto: $\forall x \in \mathbb{K} \ \exists y \in \mathbb{K}$ tale che $x+y = y+x = 0$. Solitamente l'opposto si indica con il simbolo $-x$.
  - $x + y = y + x \ \forall x, y \in \mathbb{K}$.
- Il prodotto $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ gode delle seguenti proprietà.
  - $\forall x, y, z \in \mathbb{K}$ si ha $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
  - Esiste l'unità, indicata con $1 \in \mathbb{K}$, tale che $x \cdot 1 = 1 \cdot x = x$.
  - Esiste l'inverso: $\forall x \in \mathbb{K} \ \exists y \in \mathbb{K}, x \neq 0 \exists$ tale che $x \cdot y = y \cdot x = 1$. Solitamente l'inverso si indica con il simbolo x^{-1}.
  - $x \cdot y = y \cdot x \ \forall x, y \in \mathbb{K}$.
- Vale la proprietà della distributività del prodotto rispetto alla somma:

$$x \cdot (y + z) = x \cdot y + x \cdot z \ \forall x, y, z \in \mathbb{K}$$
$$(x + y) \cdot z = x \cdot z + y \cdot z \ \forall x, y, z \in \mathbb{K}.$$

Esempio 2.1. $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Esempio 2.2. Campi finiti, ad esempio $\mathbb{K} = \{0, 1\}$.

$+$	0	1
0	0	1
1	1	0

Tabella 2.1: Operazione addizione nel campo finito $\mathbb{K} = \{0, 1\}$.

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

Tabella 2.2: Operazione moltiplicazione nel campo finito $\mathbb{K} = \{0, 1\}$.

Definizione 2.2. Uno spazio vettoriale è una quaterna $(V, +, \mathbb{K}, \cdot)$, dove V è un insieme (i cui elementi si chiamano vettori) su cui è definita un'operazione $+ : V \times V \to V$ che rende V un gruppo abeliano. Ovvero:

- $\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ si ha $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$.
- $\exists \theta \in V : \theta + \mathbf{v} = \mathbf{v} + \theta \ \ \forall \theta \in V$.
- $\forall \mathbf{v} \in V \exists \mathbf{w} \in V : \mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v} = \theta$.
- $\forall \mathbf{v}, \mathbf{w} \in V$ si ha $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$.

Inoltre definiamo $\cdot : \mathbb{K} \times V \to V$ prodotto *esterno* (tra uno scalare ed un vettore), tale che:

- $\forall \mathbf{v}, \mathbf{w}, \mathbf{z} \in V$ si ha $(\mathbf{v} + \mathbf{w}) \cdot \mathbf{z} = \mathbf{v} \cdot \mathbf{z} + \mathbf{w} \cdot \mathbf{z}$.
- $\forall \alpha \in \mathbb{K}, \forall \mathbf{v}, \mathbf{w} \in V$ si ha $\alpha \cdot (\mathbf{v} + \mathbf{w}) = \alpha \cdot \mathbf{v} + \alpha \cdot \mathbf{w}$.
- Detto $1 \in \mathbb{K}$ l'elemento identico si ha $1 \cdot \mathbf{v} = \mathbf{v} \cdot 1 = \mathbf{v} \ \ \forall \mathbf{v} \in V$.
- $\forall \mathbf{v} \in V, \forall \alpha, \beta \in \mathbb{K}$ si ha $(\alpha \cdot \beta) \cdot \mathbf{v} = \alpha \cdot (\beta \cdot \mathbf{v})$.

Esempio 2.3 (Spazio vettoriale numerico)**.** $\mathbb{K}^n = \underbrace{\mathbb{K} \times \mathbb{K} \times \cdot \times \mathbb{K}}_{n \text{ volte}} = \{(x_1, \cdots, x_n) : x_1, \cdots, x_n \in \mathbb{K}\}$ (insieme delle n-uple ordinate che stanno in $\mathbb{K}$).

Esempio 2.4. $\mathbb{K}^{n,m}$ è l'insieme delle matrici i cui elementi stanno nel campo $\mathbb{K}$ con n righe ed m colonne.

$$\begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & a_{ij} & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}, \quad a_{ij} \in \mathbb{K}.$$

Somma tra matrici Siano $A, B \in \mathbb{K}^{n,m}$ matrici dello stesso tipo. Se $A = (a_{ij}), B = (b_{i,j})$, $1 \leq i \leq n, 1 \leq j \leq m$ allora la somma tra le matrici A e B sarà

$$A + B = (a_{i,j}) + (b_{i,j}) = (a_{i,j} + b_{i,j}) = \begin{bmatrix} a_{11} + b11 & \cdots & \cdots \\ \vdots & a_{ij} + b_{ij} & \vdots \\ \cdots & \cdots & a_{nm} + b_{nm} \end{bmatrix}.$$

Prodotto esterno tra matrici Siano $\alpha \in \mathbb{K}, A \in \mathbb{K}^{n,m}$. Il prodotto esterno tra lo scalare α e la matrice A sarà

$$\alpha \cdot A = (\alpha \cdot a_{i,j}) = \begin{bmatrix} \alpha \cdot a_{11} & \cdots & \cdots \\ \vdots & \alpha \cdot a_{ij} & \vdots \\ \cdots & \cdots & \alpha \cdot a_{nm} \end{bmatrix}.$$

Osservazione 2.1. Se $\mathbb{K} = \{0, 1\}$ il prodotto esterno si riduce a due sole possibilità:

$$0 \cdot \mathbf{v} = \mathbf{0}$$
$$1 \cdot \mathbf{v} = \mathbf{v}$$

Inoltre l'opposto di un vettore $\mathbf{v}$ è ancora $\mathbf{v}$:

$$\mathbf{v} + \mathbf{v} = \mathbf{0}$$
$$\mathbf{v} - \mathbf{v} = \mathbf{v} + \mathbf{v}$$

Definizione 2.3. Un sottospazio vettoriale di V è un sottoinsieme $S \subseteq V$ che è chiuso rispetto alla somma e al prodotto esterno:

- $\forall \mathbf{v}, \mathbf{w} \in S$ si ha $\mathbf{v} + \mathbf{w} \in V$.
- $\forall \alpha \in \mathbb{K}, \forall \mathbf{v} \in S$ si ha $\alpha \cdot \mathbf{v} \in S$.

Osservazione 2.2. Se $\mathbb{K} = \{0, 1\}, V = \mathbb{K}^n$ affinché $S \subseteq V$ sia un sottospazio è sufficiente che $\forall \mathbf{v}, \mathbf{w} \in S$ si abbia $\mathbf{v} + \mathbf{w} \in V$.

Definizione 2.4. Un codice lineare (di lunghezza n) è un sottospazio di $\mathbb{K}^n$.

Il vettore nullo appartiene ad ogni sottospazio.

Esempio 2.5. $\mathbb{K}^2 = \{(0,0),(0,1),(1,0),(1,1)\} = \{00,01,10,11\}$.

Esempio 2.6. $\mathbb{K}^3 = \{000,001,010,\ldots,111\}$.

Esempio 2.7. Verifichiamo che $C = \{000,111\} \subseteq \mathbb{K}^3$ sia un sottospazio. $000 \in C$, se così non fosse non avremmo sicuramente in sottospazio. Verifichiamo poi che $000 + 111 = 111 \in C$ e quindi C è un sottospazio.

Esempio 2.8. Verifichiamo che $C = \{000,001,101\}$ sia un codice lineare. $000 \in C, 001 + 101 = 100 \notin C_1$ quindi C_1 non è un codice lineare.

Esempio 2.9. Verifichiamo che $C = \{101,111,011\}$ sia un codice lineare. Poiché $000 \notin C$, C non è certamente un codice lineare (né un sottospazio).

Esempio 2.10. Verifichiamo che $C = \{101,111,011,000\}$ sia un codice lineare. $000 \in C, 101 + 111 = 010 \notin C$, quindi C non è un codice lineare.

Esempio 2.11. Verifichiamo che $C = \{000,001,010,011\}$ sia un codice lineare. $000 \in C, 001 + 010 = 011 \in C, 001 + 0110 = 010 \in C, 010 + 011 = 001 \in C$, quindi C è un codice lineare.

Esempio 2.12. Verifichiamo che $C = \{0000,0001,1110\}$ sia un codice lineare. $0000 \in C, 0001 + 1110 = 1111 \notin C$, quindi C non è un codice lineare.

Esempio 2.13. $C = \{0000,0001,1110,1111\}$ è un codice lineare.

Osservazione 2.3. Se C_1, C_2 sono codici lineari di lunghezza n ($C_1, C_2 \in \mathbb{K}^n$ sottospazi) allora $C_1 \cap C_2$ è ancora un codice lineare.

Definizione 2.5. Siano C_1, C_2 due sottospazi. Definiamo sottospazo somma, e lo indichiamo come $C_1 + C_2$, il sottospazio definito nel modo seguente.

$$C_1 + C_2 = \{\mathbf{v} + \mathbf{w} : \mathbf{v} \in C_1, \mathbf{w} \in C_2\}.$$

Osservazione 2.4. $C_1 \subseteq C_1 + C_2, C_2 \subseteq C_1 + C_2$. Inoltre $C_1 + C_2$ è un sottospazio.

Definizione 2.6. Una combinazione lineare dei vettori $\mathbf{v_1}, \cdots, \mathbf{v_k}$ è una espressione della forma $a_1\mathbf{v_1} + \cdots + a_k\mathbf{v_k}$ con $a_1, \ldots, a_k \in \mathbb{K}$.

Definizione 2.7. Dato un insieme $S \subseteq V$, diremo sottospazio generato da S, e lo indichiamo con $< S >$, il sottoinsieme formato da tutte le combinazioni lineari di vettori appartenenti ad S. Concretamente

$$S \subseteq V, \langle S \rangle = \{a_1\mathbf{v_1} + \ldots a_k\mathbf{v_k} : \mathbf{v_1}, \ldots, \mathbf{v_k} \in S a_1, \ldots, a_k \in \mathbb{K}\}.$$

Osservazione 2.5. $\langle S \rangle$ è un sottospazio vettoriale.

Teorema 2.1. *Sia* $f(\mathbf{x_1}, \ldots, \mathbf{x_n})$ *una forma lineare, ovvero*

$$f(\mathbf{x_1}, \ldots, \mathbf{x_n}) = a_1\mathbf{x_1} + \cdots + a_n\mathbf{x_n}$$

con $a_1, \ldots a_n \in \mathbb{K}$. *L'insieme dei vettori di* $\mathbb{K}^n$ *che soddisfano l'equazione* $f(\mathbf{x_1}, \ldots, \mathbf{x_n}) = 0$ *è un sottospazio.*

Definizione 2.8 (Dipendenza lineare)**.** Dati k vettori $\mathbf{v_1}, \ldots, \mathbf{v_k} \in V$, diremo che sono linearmente dipendenti (l.d.) se esistono scalari $a_1, \ldots, a_k \in \mathbb{K}$ *non tutti nulli* tali che $a_1\mathbf{v_1} + \cdots + a_k\mathbf{v_k} = 0$, ovvero tali che la loro combinazione lineare sia nulla.
Analogamente, diremo che i vettori $\mathbf{v_1}, \cdot, \mathbf{v_k} \in V$ sono linearmente indipendenti (l.i.) se l'unica loro combinazione lineare è quella banale, ovvero

$$a_1\mathbf{v_1} + \cdots + a_k\mathbf{v_k} = 0 \Rightarrow a_1, \ldots, a_k = 0.$$

Osservazione 2.6. $0\mathbf{v_1} + \cdots + 0\mathbf{v_k} = \mathbf{0}$.

Esempio 2.14. Siano $\mathbf{v_1} = (1, 2, 5, -1), \mathbf{v_2} = (2, 0, 1, 4), \mathbf{v_3} = (4, 4, 11, 2)$. Mostriamo se esistono $x, y, z \in \mathbb{Q}$ *non tutti nulli* tali che

$$x\mathbf{v_1} + y\mathbf{v_2} + z\mathbf{v_3} = (0, 0, 0, 0) \tag{2.1}$$

sia verificata.
L'equazione (2.1) è un sistema lineare omogeneo di 4 equazioni in 3 incognite. Tuttavia, poiché in questo caso vale

$$2\mathbf{v_1} + \mathbf{v_2} = \mathbf{v_3} \Rightarrow 2\mathbf{v_1} + \mathbf{v_2} - \mathbf{v_3} = 0,$$

segue che

$$x = 2, y = 1, z = -1.$$

Definizione 2.9. Diremo che l'insieme $S \subseteq V$ genera V se $\langle S \rangle = V$.

Definizione 2.10. Se esiste S finito, tale che $\langle S \rangle = V$ avremo che V è uno spazio vettoriale finitamente generato.

Definizione 2.11 (Base)**.** Dato $S \subseteq V$ se S è un insieme di generatori per V ed inoltre S è l.i. diremo che S è una base di V.

$S = \{\mathbf{v_1}, \ldots, \mathbf{v_k}\}$ è una base se

- $\langle S \rangle = V$.

- S è l.i., ovvero: $a_1\mathbf{v_1} + \cdots + a_n\mathbf{v_n} = \mathbf{0} \Rightarrow a_1 = \cdots = a_n = 0$.

Da ora in poi tutti gli spazi vettoriali (a meno che non sia esplicitamente detto) saranno considerati finitamente generati.

Teorema 2.2 (Caratterizzazione delle basi)**.** *$S = \{\mathbf{v_1}, \ldots, \mathbf{v_k}\}$ è una base se e solo se ogni vettore $\mathbf{v} \in V$ si può esprimere in modo unico come combinazione lineare di vettori della base. Ovvero*

$$\forall \mathbf{v} \in V \ \exists! a_1, \ldots, a_n \in \mathbb{K} : a_1\mathbf{v_1} + \cdots + a_n\mathbf{v_n} = \mathbf{v}.$$

Esempio 2.15. $V = \mathbb{Q}^3, B = \{\mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3}\}$ dove

$$\mathbf{e_1} = (1, 0, 0), \mathbf{e_2} = (0, 1, 0), \mathbf{e_3} = (0, 0, 1)$$

è detta base canonica. In questo caso ogni vettore può essere generato dalla base canonica.

$$(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathbb{Q}^3 : x\mathbf{e_1} + y\mathbf{e_2} + z\mathbf{e_3} = (\mathbf{x}, \mathbf{y}, \mathbf{z}).$$

B è un insieme di generatori; Inoltre B è l.i.; dunque B è una base.

Esempio 2.16. Siano

$$\mathcal{D} = \{\mathbf{v_1}, \mathbf{v_2}, \mathbf{v_3}\} \subseteq \mathbb{Q}^3$$

e

$$\mathbf{v_1} = (1, 0, 1), \mathbf{v_2} = (1, 2, -1), \mathbf{v_3} = (1, 1, 2). \tag{2.2}$$

Calcoliamo le componenti del vettore $(2, 1, 0)$ rispetto alla base $\mathcal{D}$. Avremo

$$x\mathbf{v_1} + y\mathbf{v_2} + z\mathbf{v_3} = (2, 1, 0).$$

Il sistema lineare da risolvere sarà

$$\begin{cases} x + y + z = 2 \\ 2y + z = 1 \\ x - y + 2z = 0 \end{cases} \tag{2.3}$$

Lo risolveremo con il metodo di riduzione. Costruiamo la matrice completa del sistema.

$$B = \begin{bmatrix} 1 & 1 & 1 & 2 \\ 0 & 2 & 1 & 1 \\ 1 & -1 & 2 & 0 \end{bmatrix}.$$

Applichiamo la prima sostituzione: $R_3 \mapsto R_3 - R_1$. Otterremo la matrice B':

$$B' = \begin{bmatrix} 1 & 1 & 1 & 2 \\ 0 & 2 & 1 & 1 \\ 0 & -2 & 1 & -2 \end{bmatrix}.$$

Applichiamo la seconda sostituzione: $R_3 \mapsto R_3 + R_2$. Otterremo la matrice B'':

$$B'' = \begin{bmatrix} 1 & 1 & 1 & 2 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 2 & -1 \end{bmatrix}.$$

La matrice adesso è ridotta, quindi possiamo riscrivere il sistema (2.3) in forma triangolare:

$$\begin{cases} x + y + z = 2 \\ 2y + z = 1 \\ 2z = -1 \end{cases}$$

la cui risoluzione è banale.

Lo scambio tra due righe di una matrice e l'aggiunta alla riga di una matrice del multiplo di una riga parallela si chiamano operazioni elementari di riga.

Definizione 2.12. Due matrici che si possono ottenere l'una dall'altra mediante trasformazioni elementari di riga si dicono equivalenti.

Teorema 2.3. *Dato V spazio vettoriale finitamente genereato. Se B e B' sono basi di V allora*

$$|B| = |B'|$$

Definizione 2.13. Definiamo dimensione di uno spazio vettoriale V e la indichiamo con $\dim V$ il numero di elementi di una sua base.

Dato un insieme S di generatori di un sottospazio $W \subseteq \mathbb{K}^n$. Come estraiamo da tale insieme una base di W? Sia B la matrice avente per righe gli elementi di S. Effettuiamo le medesime operazioni di riduzione nel modo consueto e, ottenuta la matrice ridotta, ne scartiamo tutte le righe nulle. Le righe rimanenti determinano la base per W e rappresentano vettori linearmente indipendenti.

Esempio 2.17. Sia $S = \{1101, 1110, 1011\}$ in $\mathbb{Z}_2 = \{0, 1\}$. Costruiamo la matrice B avente per righe gli elementi di S:

$$B = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

Applichiamo le sostituzioni: $R_2 \mapsto R_2 + R_1; R_3 \mapsto R_3 + R_1$. Otterremo la matrice B':

$$B' = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Scambiamo, infine, le righe R_2 ed R_3 ottenendo la matrice B'':

$$B'' = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

In questo caso avremo ottenuto 3 vettori l.i. che costituiscono una base del sottospazio generato dai 3 vettori iniziali.

Esempio 2.18. Sia $S = \{101, 011, 110, 010\}$ in $\mathbb{Z}_2 = \{0, 1\}$. Costruiamo la matrice B avente per righe gli elementi di S:

$$B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

La matrice ridotta, in questo caso, sarà:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

In questo caso avremo 3 vettori l.i. che costituiscono una base del sottospazio generato dai vettori iniziali.

Definizione 2.14. Data $A \in \mathbb{K}^m, n$ diremo rango d A e lo indicheremo con rk$A$ la dimensione del sottospazio vettoriale generato dalle colonne di A:

$$\text{rk}A = \dim\langle R_1, \ldots, R_n\rangle = \dim\langle C_1, \ldots, C_n\rangle.$$

Definizione 2.15. Diremo che la caratteristica (rango) di A è il numero r tale che esiste un minore M estratto da A di ordine r con det$M \neq 0$ e tutti i minori di ordine maggiore o uguale a $r + 1$ sono nulli.

Sia $S \subseteq \mathbb{K}^n$ e $\langle S\rangle$ il sottospazio generato da S. Allora $\dim\langle S\rangle$ è il rango della matrice che si ottiene mettendo nelle sue righe gli elementi di S.

Definizione 2.16 (Prodotto scalare)**.** Siano $\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$, il prodotto scalare $\cdot : \mathbb{K}^n \times \mathbb{K} \to \mathbb{K}$ di $\mathbf{x}, \mathbf{y}$, che indichiamo $\mathbf{x} \cdot \mathbf{y}$ (si legge $\mathbf{x}$ *scalare* $\mathbf{y}$) dove

$$\mathbf{x} = (x_1, \ldots, x_n), \;\; x_1, \ldots, x_n \in \mathbb{K}$$
$$\mathbf{y} = (y_1, \ldots, y_n), \;\; y_1, \ldots, y_n \in \mathbb{K}$$

sarà

$$\mathbf{x} \cdot \mathbf{y} = x_1 \cdot y_1 + \cdots + x_n \cdot y_n.$$

Il prodotto scalare gode delle seguenti proprietà.

- $(\mathbf{x}+\mathbf{y})\cdot\mathbf{z} = \mathbf{x}\cdot\mathbf{z}+\mathbf{y}\cdot\mathbf{z}\ \ \forall \mathbf{x},\mathbf{y},\mathbf{z}\in\mathbb{K}^n$.
- $\mathbf{x}\cdot(\mathbf{y}+\mathbf{z}) = \mathbf{x}\cdot\mathbf{y}+\mathbf{x}\cdot\mathbf{z}\ \ \forall \mathbf{x},\mathbf{y},\mathbf{z}\in\mathbb{K}^n$.
- $(a\cdot\mathbf{x})\cdot\mathbf{y} = a\cdot(\mathbf{x}\cdot\mathbf{y}) = \mathbf{x}\cdot(a\cdot\mathbf{y})\ \ \forall a\in\mathbb{K}, \forall \mathbf{x},\mathbf{y}\in\mathbb{K}^n$.

Definizione 2.17. Diremo che due vettori $\mathbf{x},\mathbf{y}$ sono ortogonali se $\mathbf{x}\cdot\mathbf{y}=0$.

Esempio 2.19. Sia $\mathbb{K}=\mathbb{Z}_2$.

$$11011\cdot 11011 = 1\cdot 1+1\cdot 1+0\cdot 0+1\cdot 1+1\cdot 1 = \\ 1+1+0+1+1=0.$$

Definizione 2.18. Dato $S\subseteq\mathbb{K}^n$, indicheremo con $S^\perp$ il seguente sottoinsieme

$$S^\perp = \{\mathbf{x}\in\mathbb{K}^n : \mathbf{x}\cdot\mathbf{s}=0\ \ \forall \mathbf{s}\in S\}.$$

Teorema 2.4. *$S^\perp$ è un sottospazio (detto ortogonale o duale).*
Inoltre $S^\perp = \langle S\rangle^\perp$.

Esempio 2.20. Sia $S=\{\mathbf{v_1},\mathbf{v_2}\}$. L'insieme dei vettori ortogonali a S è costituito da tutti i vettori appartenenti alla retta perpendicolare a $\mathbf{v_1}$ e $\mathbf{v_2}$.

Sia $S\subseteq\mathbb{K}^n$. In particolare $S=\{\mathbf{s_1},\dots,\mathbf{s_k}\}$. Supponiamo che i vettori appartenenti a S siano linearmente indipendenti. Allora

$$S^\perp = \{\mathbf{x}\in\mathbb{K}^n : \mathbf{s_1}\cdot\mathbf{x}=\mathbf{0},\dots,\mathbf{s_k}\cdot\mathbf{x}=\mathbf{0}\}. \tag{2.4}$$

In particolare l'equazione (2.4) rappresenta un sistema lineare omogeneo nelle incognite $x_1,\dots,x_n$ i cui coefficienti sono $s_1,\dots,s_k$, cioè

$$\mathbf{s_1}=(s_{11},\dots,s_{1n}),\dots,\mathbf{s_k}=(s_{k1},\dots,s_{kn}).$$

Quindi

$$\begin{cases} s_{11}x_1+\dots+s_{1n}x_n=0 \\ \dots \\ s_{k1}x_1+\dots+s_{kn}x_n=0. \end{cases}$$

Inoltre $\dim\langle S\rangle = k$.
$S^\perp$ è descritto da k equazioni lineari ed omogenee e linearmente indipendenti.

Esempio 2.21. Consideriamo il sistema

$$\begin{cases} 2x - 3y + z = 0 \\ x - y + z = 0 \\ 3x - 4y + 2z = 0 \end{cases}$$

In questo caso le equazioni che compongono il sistema sono linearmente indipendenti, in quanto la terza equazione è combinazione lineare delle prime due. Quindi, se scartiamo la terza equazione, il sistema

$$\begin{cases} 2x - 3y + z = 0 \\ x - y + z = 0 \end{cases}$$

sarà equivalente. Avremo

$$\dim\langle S\rangle^{\perp} = \dim S^{\perp} = n - \dim\langle S\rangle$$

dove $\dim\langle S\rangle$ corrisponde al numero di equzioni linearmente indipendenti del sistema.

Esempio 2.22. Sia $S = \{1010, 0101, 1111\}$. Calcoliamo $\dim\langle S\rangle$. Avremo

$$\dim\langle S\rangle = \mathrm{rk}\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} = 2.$$

Una base di S è $\{1010, 0101\}$.
$S^{\perp}$ è descritto dalle seguenti equazioni cartesiane

$$\begin{cases} x + z = 0 \\ y + t = 0 \end{cases} \tag{2.5}$$

da cui $\dim S^{\perp} = 4 - 2 = 2$.
Risolviamo le equazioni (2.5)[1]

$$\begin{cases} x = z \\ y = t \end{cases}$$

Posto $z = \alpha, t = \beta$ con $\alpha, \beta \in \mathbb{Z}_2$, le soluzioni saranno della forma

$$(\alpha, \beta, \alpha, \beta) \ \forall \alpha, \beta \in \mathbb{Z}_2.$$

Definizione 2.19. Diremo che G è una matrice generatrice del codice (lineare) C se le sue righe sono formate da una base di C.

[1]Si ricordi che siamo nel campo $\mathbb{Z}_2$

Vi sono, pertanto, tante matrici generatrici quante sono le basi del codice. Sia $l(C) = n$ la lunghezza del codice C e dim$C$ la sua lunghezza (con $C \in \mathbb{K}^n$. Allora $G \in \mathbb{K}^{k,n}$.
Al variare di $\mathbf{u} \in \mathbb{K}^n$, i prodotti $\mathbf{u} \cdot G$ formano tutti gli elementi del codice C; $\mathbf{u}$ è la k-upla delle componenti del vettore $\mathbf{u} \cdot G \in C$ rispetto alla base B.
Per le proprietà delle basi la matrice G permette di ottenere una corrispondenza biunivoca tra l'insieme di tutte le k-uple (in K^k) e il codice C.

Teorema 2.5. *Una matrice G è una matrice generatrice se e solo se le sue righe sono linearmente indipendenti.*

Definizione 2.20. Due matrici che generano lo stesso codice si dicono equivalenti.

Definizione 2.21. Una matrice è in *Row Echelon Form* (REF) se è nella seguente forma

$$\begin{bmatrix} 1 & 0 & \cdots & a_k & x_{11} & \cdots & x_{1n} \\ 0 & 1 & \cdots & a_{2k} & x_{21} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & x_{k_1} & \cdots & x_{2k} \end{bmatrix}$$

Definizione 2.22. Una matrice è in *Reduced Row Echelon Form* (RREF) se è nella seguente forma

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & x_{11} & \cdots & x_{1n} \\ 0 & 1 & \cdots & 0 & x_{21} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & x_{k_1} & \cdots & x_{2k} \end{bmatrix}$$

Esempio 2.23. La matrice

$$G' = \begin{bmatrix} 0 & 1 & 0 & \alpha & \beta \\ 0 & 0 & 1 & \gamma & \delta \end{bmatrix}$$

è in RREF, a meno di una permutazione delle colonne.

Il controllo di parità serve a capire se una parola (n-upla) appartiene ad un codice C. Tipicamente, dato K^n si costruisce un codice $C \subseteq K^{n+1}$, in cui per ogni parola, i primi n bit rappresentano l'informazione vera e propria che si vuole trasmettere attraverso il canale, mentre l'$(n+1)$-esimo bit è il cosiddetto bit di parità. L'$(n+1)$-esimo bit sarà la somma dei primi n bit della parola. In questo caso la $(n+1)$-upla conterrà sempre un numero pari di bit pari ad 1. Quindi se $x_1 + \cdots + x_n = 0$ allora la parola apparterrà al codice.

Definizione 2.23. H è una matrice controllo di parità (*parity-check matrix*) del codice C se $\mathbf{u} \cdot H = \mathbf{0} \ \forall \mathbf{u} \in C$.

Sia C un codice lineare. Sia

$$H = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n-k} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n-k} \end{bmatrix} \in \mathbb{K}^{n,n-k}.$$

In questo caso le equazioni cartesiane del codice C saranno

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{n,1}x_n = 0 \\ \cdots \\ a_{n,1-k}x_1 + \cdots + a_{n,n-k}x_n = 0 \end{cases}$$

Le colonne di H formano una base del codice duale di C ed inoltre

$$\dim C = k \Rightarrow \dim C^{\perp} = n - k.$$

Teorema 2.6. *Una matrice H è una matrice controllo di parità se e solo se le colonne di H sono linearmente indipendenti.*

Dato un codice C vediamo come fare a costruire una matrice controllo di parità, il che equivale a trovare una base del codice duale.
Il metodo utilizzato è il metodo di eliminazione dei parametri che mostriamo mediante un esempio.

Esempio 2.24. Siano

$$C \subseteq \mathbb{Q}^3, \ \dim C = 1.$$

In questo avremo un solo bit di informazione e 2 bit di ridondanza. Sia

$$C = \langle (2, 1, -5) \rangle = \{(2\lambda, \lambda, -5\lambda : \lambda \in \mathbb{Q}\}$$

ovvero il codice formato da tutte le possibili combinazioni lineari della terna $(2, 1, -5)$. In questo caso il codice duale sarà il sottospazio seguente

$$C^{\perp} = \{(a, b, c) \in \mathbb{Q}^3 : 2a + 1b - 5c = 0\}.$$

Il numero di equazioni linearmente indipendenti sarà $3 - 1 = 2$, dunque dobbiamo trovare una coppia di soluzioni indipendenti per

$$2a + 1b - 5c = 0.$$

Avremo

$$b = -2a + 5c \Rightarrow b = -2\alpha + 5\gamma$$

da cui le soluzioni saranno del tipo

$$(\alpha, -2\alpha + 5\gamma, \gamma) \;\; \alpha, \gamma \in \mathbb{Q}.$$

Una base di $C^\perp$ sarà

$$(1, -2, 0), \;\; (0, 5, 1).$$

Quindi una matrice controllo di parità per il codice C sarà

$$H = \begin{bmatrix} 1 & 0 \\ -2 & 5 \\ 0 & 1 \end{bmatrix}$$

H è una matrice controllo di parità per il codice C (generato da G) se $G \cdot H = 0$, con $G \in \mathbb{K}^{k,n}$, $H \in \mathbb{K}^{n,n-k}$.

Esempio 2.25. Siano

$$C = \langle (1, 0, 2), (3, 1, -4) \rangle, \; \dim C = 3.$$

In questo caso $\dim C^\perp = 3 - \dim C = 3 - 2 = 1$, quindi stavolta cercheremo una sola equazione, di conseguenza la matrice controllo di parità sarà costituita da una sola colonna. Il codice C si può pensare come l'insieme delle soluzioni di *una* equazione in 3 incognite. Se $ax + by + cz = 0$ è una di queste equazioni allora avremo

$$\begin{cases} a + 2c = 0 \\ 3a + b - 4c = 0 \end{cases}$$

Risolviamo il sistema per sostituzione.

$$\begin{cases} a = -2c \\ 3(-2c) + b - 4c = 0 \end{cases} \Rightarrow \begin{cases} a = -2c \\ -10c + b = 0 \end{cases} \Rightarrow \begin{cases} a = -2c \\ b = 10c \\ c = c \end{cases}$$

Se $c = 1$ una terna è $(-2, 10, 1)$. In definitiva abbiamo trovato i coefficienti del sistema lineare che descrive il sottospazio C, ma, come abbiamo detto prima, è costituito da una sola equazione: $-2x + 10y + z = 0$. La matrice controllo di parità sarà

$$H = \begin{bmatrix} -2 \\ 10 \\ 1 \end{bmatrix}$$

H è una matrice controllo di parità per il codice $C \subseteq \mathbb{K}^n$, $\dim C = k$ se

- $H \in \mathbb{K}^{n,n-k}$.

- Le colonne di H sono linearmente indipendenti e $\forall \mathbf{v} \in C$ si deve avere $\mathbf{v} \cdot H = \mathbf{0}$.

Quest'ultima condizione è equivalente a $G \cdot H = 0$.
Una matrice controllo di parità, per un codice C, si può interpretare come una matrice nelle cui colonne c'è una base duale $C^{\perp}$, dove $\dim C^{\perp} = n - \dim C$. Se le colonne di H sono k, allora $\dim C = n - k$.
Vediamo un algoritmo per la costruzione di una matrice controllo di parità a partire da una matrice generatrice. Sia G una matrice generatrice del codice C ($\dim C = k$).
Sia G una matrice generatrice del codice C ($\dim C = k$). Riduciamo la matrice in forma RREF, ovvero otteniamo una nuova matrice G' nella forma $(1, X)$, a meno di una permutazione delle colonne. Avremo

$$G' = \begin{bmatrix} 1 & 0 & \cdots & 0 & x_{11} & \cdots & x_{1n} \\ 0 & 1 & \cdots & 0 & x_{21} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & x_{k_1} & \cdots & x_{2k} \end{bmatrix} = (I, X)$$

La matrice controllo di parità H sarà

$$H = \begin{bmatrix} X \\ I \end{bmatrix}$$

Chiaramente, poichè lavoriamo nel campo finito $\mathbb{Z}_2$ avremo $G' \cdot H = \mathbf{0}$.

Esempio 2.26. Consideriamo la matrice

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

Eseguiamo operazioni elementari di riga su G. Inizialmente applichiamo la riduzione di riga $R_2 \mapsto R_2 + R_1$ ottenendo

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

Applichiamo quindi la riduzione di riga $R_3 \mapsto R_2 + R_3$ ottenendo

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

La terza riga di G'' è nulla quindi il codice è di dimensione 2, il che significa che le righe di G non è erano tutte linearmente indipendenti. Possiamo quindi scartare la terza riga di G'' ottenendo

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

La matrice $\bar{G}$ è in REF, quindi proseguiamo con le operazioni elemetari di riga nel tentativo di trasformarla in RREF. Applichiamo $R_1 \mapsto R_1 + R_2$ ottenendo

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

La matrice $\bar{\bar{G}}$ è in RREF. La costruzione di H è immediata.

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

Verifichiamo, infine, che $\bar{\bar{G}} \cdot H = \mathbf{0}$.

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

Esempio 2.27. Sia

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

Applichiamo le riduzioni $R_2 \mapsto R_2 + R_1, R_3 \mapsto R_3 + R_1$ ottenendo

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

Applichiamo la riduzione $R_4 \mapsto R_4 + R_2$ ottenendo

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

Scartiamo la quarta riga e quindi otteniamo

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

in REF. Applichiamo la riduzione $R_1 \mapsto R_1 + R_3$ ottenendo

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

Infine $R_1 \mapsto R_1 + R_2$ e otteneniamo

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

in RREF. La matrice controllo di parità sarà

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

Poiché $\dim C = 3$ avremo $\dim C^{\perp} = 5 - \dim C = 5 - 3 = 2$. Inoltre

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

Definizione 2.24 (Distanza di Hamming)**.** Siano $u, v \in \mathbb{K}^n$ con $\mathbb{K} = \mathbb{Z}_2$, indichiamo con $\mathrm{d}(\mathbf{u}, \mathbf{v})$ il numero di post in cui $\mathbf{u}$ e $\mathbf{v}$ differiscono:

$$\mathrm{d}(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i\}|.$$

Definizione 2.25 (Peso)**.** Sia $\mathbf{u} \in \mathbb{K}^n$. Il peso di $\mathbf{u}$ è

$$\mathrm{wt}(\mathbf{u}) = \mathrm{d}(\mathbf{u}, \mathbf{0})$$

ovvero il numero di 1 presenti nella parola (o la distanza della parola dalla parola vuota).

Osservazione 2.7. Vale $\mathrm{d}(\mathbf{u}, \mathbf{v}) = \mathrm{wt}(\mathbf{u} + \mathbf{v})\ \forall \mathbf{u}, \mathbf{v} \in \mathbb{Z}_2$.

Esempio 2.28. Siano

$$\mathbf{u} = (0110111), \mathbf{v} = (00111010)$$

Avremo

$$\begin{gathered} \mathrm{d}(\mathbf{u}, \mathbf{v}) = 3 \\ \mathrm{wt}(\mathbf{u}) = \mathrm{d}(\mathbf{u}, \mathbf{0}) = 5 \\ \mathrm{wt}(\mathbf{v}) = \mathrm{d}(\mathbf{v}, \mathbf{0}) = 4 \end{gathered}$$

La distanza gode delle seguenti proprietà.

- $\mathrm{d}(\mathbf{u}, \mathbf{v}) = 0 \Leftrightarrow \mathbf{u} = \mathbf{v}\ \ \forall \mathbf{u}, \mathbf{v} \in \mathbb{K}^n$.
- $\mathrm{d}(\mathbf{u}, \mathbf{v}) = \mathrm{d}(\mathbf{v}, \mathbf{u})\ \ \forall \mathbf{u}, \mathbf{v} \in \mathbb{K}^n$.
- $\mathrm{d}(\mathbf{u}, \mathbf{v}) \leq \mathrm{d}(\mathbf{u}, \mathbf{w}) + \mathrm{d}(\mathbf{v}, \mathbf{w})\ \ \forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{K}^n$ (Disuguaglianza triangolare).

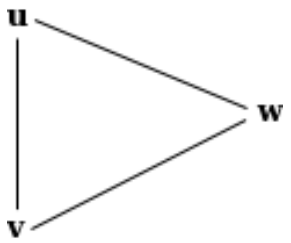

Figura 2.1: Disuguaglianza triangolare.

Definizione 2.26 (Distanza di un codice)**.** La distanza di un codice C è

$$\mathrm{d}(C) = d = \min\{\mathrm{d}(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$$

Nel caso di un codice lineare C avremo

$$\mathrm{d}(C) = \min\{\mathrm{d}(\mathbf{u}, \mathbf{0}) : \mathbf{u} \in C, \mathbf{u} \neq \mathbf{0}\} = \min\{\mathrm{wt}(\mathbf{u}) : \mathbf{u} \in C, \mathbf{u} \neq \mathbf{0}\}$$

Inoltre $\mathbf{u}, \mathbf{v} \in C \Rightarrow \mathbf{u} + \mathbf{v} \in C$.

Supponiamo di considerare il codice $C = \{000, 111\}$. Supponiamo che il ricevitore riceva la parola $010 \in C$: in questo caso è stato commesso un errore. In questo caso o il ricevitore, constatato l'errore, richiede al trasmettitore il reinvio della parola, o cerca di correggere l'errore. In questo caso abbiamo due possibilità: o

l'errore si è verificato in un solo bit o in due bit. In particolare l'errore verificatosi o è $\mathbf{u} = 010$ ed in questo caso la parola trasmessa era $000 \in C$, infatti $000 + \mathbf{u} = 000 + 010 = 010$; o è $\mathbf{u} = 101$ ed in questo caso la parola trasmessa era $111 \in C$, infatti $111 + \mathbf{u} = 111 + 101 = 010$. In questi casi si suppone che la parola inviata sia quella avente distanza minore, quindi, in questo caso 000.

Teorema 2.7. *Sia C un codice di distanza $d(C) = d$. Il codice C corregge tutti gli errori $\mathbf{u}$ di peso*

$$wt(\mathbf{u}) = \left\lfloor \frac{d-1}{2} \right\rfloor$$

Dimostrazione. Bisogna dimostrare che dato $\mathbf{v} \in C$ e un qualunque $\mathbf{u} \in \mathbb{K}^n$ di peso

$$\mathrm{wt}(\mathbf{u}) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

allora $\forall \mathbf{w} \in C$ si avrà

$$\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) > \mathrm{d}(\mathbf{v}, \mathbf{v} + \mathbf{u})$$

Consideriamo

$$\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) + \mathrm{d}(\mathbf{v} + \mathbf{u}, \mathbf{v}) \geq \mathrm{d}(\mathbf{w}, \mathbf{v}) \geq d \tag{2.6}$$

con $\mathbf{w} \in C$. La (2.6) è una disuguaglianza triangolare: l'ultimo membro della disequazione è possibile poiché d, per la definizione 2.26, è la minore tra tutte le possibili distanza del codice C. Poiché

$$\mathrm{d}(\mathbf{v} + \mathbf{u}, \mathbf{v}) = \mathrm{wt}(\mathbf{v} + \mathbf{u} + \mathbf{v}) = \mathrm{wt}(\mathbf{u})$$

sostituendo nella (2.6) otteniamo

$$\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) + \mathrm{wt}(\mathbf{u}) \geq d$$

Ma

$$\mathrm{wt}(\mathbf{u}) \leq \left\lfloor \frac{d-1}{2} \right\rfloor \leq \frac{d-1}{2} \Rightarrow d \geq 2\mathrm{wt}(\mathbf{u}) + 1$$

quindi

$$\begin{gathered}
\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) + \mathrm{wt}(\mathbf{u}) \geq 2\mathrm{wt}(\mathbf{u}) + 1 \Rightarrow \\
\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) \geq 2\mathrm{wt}(\mathbf{u}) - \mathrm{wt}(\mathbf{u}) + 1 \Rightarrow \\
\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) \geq \mathrm{wt}(\mathbf{u}) + 1 > \mathrm{wt}(\mathbf{u}) = \mathrm{d}(\mathbf{v} + \mathbf{u}, \mathbf{v}) \Rightarrow \\
\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) > \mathrm{d}(\mathbf{v} + \mathbf{u}, \mathbf{v}).
\end{gathered}$$

Abbiamo, quindi, dimostrato la prima parte del teorema. Rimane da dimostrare che per errori $\mathbf{u}$ il cui peso è almeno

$$\mathrm{wt}(\mathbf{u}) = \left\lfloor \frac{d-1}{2} \right\rfloor + 1$$

non possono essere corretti.
Siano $\mathbf{u}, \mathbf{v} \in C$ tali che $\mathrm{d}(\mathbf{v}, \mathbf{w}) = d$. Questo significa che la parola $\mathbf{v} + \mathbf{w}$ contiene esattamente d bit 1 e rimanenti bit sono 0. Costruiamo una parola $\mathbf{u} \in \mathbb{K}^n$ ottenuta trasformando in 0 esattamente $d - 1 - \lfloor \frac{d-1}{2} \rfloor$ dei suoi 1. Facciamo vedere che, in questo caso, l'errore non può essere corretto. Avremo

$$\mathrm{d}(\mathbf{v}, \mathbf{v} + \mathbf{u}) = \mathrm{wt}(\mathbf{u}) = 1 + \left\lfloor \frac{d-1}{2} \right\rfloor$$

e

$$\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) = \mathrm{wt}(\mathbf{w} + \mathbf{v} + \mathbf{u}) = d - \left(1 + \left\lfloor \frac{d-1}{2} \right\rfloor\right) = d - 1 - \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Se $d = 2t + 1$ (d dispari) avremo

$$\mathrm{d}(\mathbf{v}, \mathbf{v} + \mathbf{u}) = 1 + \left\lfloor \frac{2t + 1 - 1}{2} \right\rfloor = 1 - \lfloor t \rfloor = 1 + t$$

e

$$\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) = 2t + 1 - 1 - \left\lfloor \frac{2t + 1 - 1}{2} \right\rfloor = 2t - \lfloor t \rfloor = 2t - t = t.$$

quindi

$$\mathrm{d}(\mathbf{v}, \mathbf{v} + \mathbf{u}) > \mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}).$$

In maniera analoga se $d = 2t$ (d pari) avremo

$$\mathrm{d}(\mathbf{v}, \mathbf{v} + \mathbf{u}) = 1 + \left\lfloor \frac{2t - 1}{2} \right\rfloor = 1 + \left\lfloor t - \frac{1}{2} \right\rfloor = 1 + t - 1 = t$$

e

$$\mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}) = 2t - 1 - \left\lfloor \frac{2t - 1}{2} \right\rfloor = 2t - 1 - \left\lfloor t - \frac{1}{2} \right\rfloor = 2t - 1 - t + 1 = 2t$$

quindi, in questo caso

$$\mathrm{d}(\mathbf{v}, \mathbf{v} + \mathbf{u}) > \mathrm{d}(\mathbf{w}, \mathbf{v} + \mathbf{u}).$$

In entrambi i casi, pertanto, l'errore non verrà corretto. □

Teorema 2.8. *Sia H una matrice controllo di parità per il codice (lineare) C. La distanza di C è d se e solo se comunque si scelgono $d-1$ righe di H, tali righe sono linearmente indipendenti ed inoltre esistono d righe di H che sono linearmente dipendenti.*

Definizione 2.27. Un coset d C (codice lineare di lunghezza n) è un insieme della forma

$$\mathbf{u} + C = \{\mathbf{u} + \mathbf{v} : \mathbf{v} \in C\}$$

Un sottospazio C induce una relazione di equivalenza su $\mathbb{K}^n$ nel modo seguente

$$\mathbf{v} \sim \mathbf{w} \ (\mathbf{v} \equiv \mathbf{w} \bmod C) \text{ se } \mathbf{v} - \mathbf{w} \in C. \tag{2.7}$$

Se $\mathbb{K} = \mathbb{Z}_2$ $\mathbf{v} \sim \mathbf{w}$ se $\mathbf{v} - \mathbf{w} \in C$. Tale relazione di equivalenza permette di dividere $\mathbb{K}^n$ in sottoclassi di equivalenza (disgiunte). Esse si chiamano *cosets* o laterali. L'unione di tutti i cosets coincide con $\mathbb{K}^n$. In particolare, il coset che contiene il vettore nullo è C.
Vale

$$\mathbf{u} + C = \mathbf{v} + C \Leftrightarrow \mathbf{u} + \mathbf{v} \in C.$$

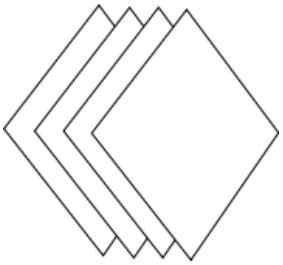

Figura 2.2: Cosets.

Sia V un sottospazio. Per ogni $\mathbf{v} \in V$ esiste una ed una sola classe di equivalenza contenente $\mathbf{v}$. Indichiamo con $\bar{\mathbf{v}}$ la classe di equivalenza di $\mathbf{v}$, ovvero l'insieme di tutti gli elementi equivalenti a $\mathbf{v}$. Cio

$$\bar{\mathbf{v}} = \{\mathbf{w} \in V : \mathbf{w} \equiv \mathbf{v} \bmod C\}$$

Tutte le classi di equivalenza sono costituite dallo stesso numero di elementi.
Valgono le seguenti proprietà.

- C è esso stesso un coset.
- $C = C + \mathbf{u}$ $\forall u \in C$.

- $C + \mathbf{u} = C + \mathbf{v} \Leftrightarrow \mathbf{u} \equiv \mathbf{v} \bmod C$.
- $\mathbf{u} \in C + \mathbf{u}$.

Due cosets, inoltre, hanno lo stesso numero di elementi, il che significa che esiste un'applicazione

$$\phi : C \to C + \mathbf{u} \tag{2.8}$$

biunivoca, tale che $\phi(\mathbf{v}) = \mathbf{v} + \mathbf{u}\ \forall \mathbf{v} \in C$.
Indicato con $\frac{V}{C}$ l'insieme di tutti i cosets, si può dotare $\frac{V}{C}$ della struttura di spazio vettoriale. Inoltre

$$\dim\frac{V}{C} = \dim V - \dim C = n - k.$$

Esempio 2.29. Sia $C = \langle 1011, 0101\rangle, C \in \mathbb{K}^4$. C conterrà $2^{\dim C}$ elementi

$$C = \{0000, 1011, 0101, 1110\} \tag{2.9}$$

Il numero di cosets $C + \mathbf{u}$, in questo caso sarà $2^{4-2} = 2^2 = 4$. I cosets $C + 0000$, $C + 1000, C + 0100, C + 0010$ sono

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100

Per ciascun coset, chiameremo elemento *leader*, la parola (o le parole) di peso minimo.
Supponiamo che $\mathbf{u} \in \mathbb{K}^4$ sia un errore (*error pattern*). Questo significa che se trasmettiamo attraverso un canale un certo messaggio $\mathbf{v}$ sarà ricevuto un messaggio $\mathbf{w} = \mathbf{v} + \mathbf{u}$. Banalmente, se conoscessimo $\mathbf{u}$ potremmo riottenere $\mathbf{v}$ calcolando $\mathbf{v} = \mathbf{w} + \mathbf{u}$. Tuttavia l'errore non si conosce a priori. Facciamo l'ipotesi che l'errore sia quello di peso minimo.
Se $\mathbf{v} \in C$ si ha

$$C + \mathbf{v} = C + \mathbf{w}$$

ovvero l'*error pattern* e la parola stanno nello stesso coset.
Supponiamo, quindi, che la parola ricevuta sia $\mathbf{w} = 1101 \notin C$. In questo caso è stato certamente commesso un errore durante la trasmissione. Applicando la cosiddetta *decodifica per massima verosomiglianza* (MLD) supporremo che l'errore commesso sia il coset leader di $C + \mathbf{w}$ cioè 1000. Si avrà

$$\mathbf{w} + 1000 = 1101 + 1000 = 0101 \in C$$

quindi 0101 sarà la parola decodificata.
Supponiamo, adesso, che $w = 1111$ e che l'error pattern sia $u = 0100$. Decodificando con MLD avremo

$$\mathbf{w} + 0100 = 1111 + 0100 = 1011 \in C$$

Ma, in questo caso, potremmo decodificare anche con il secondo coset leader (0001) ottenendo un altro risultato.

Definizione 2.28 (Sindrome)**.** Sia H una matrice controllo di parità di C. Definiamo sindrome di una parola $\mathbf{w} \in \mathbb{K}^n$, la parola $\mathbf{w} \cdot H \in \mathbb{K}^{n-k}$.

Supponendo che gli errori di peso minimo siano i più probabili si può utilizzare il seguente schema (MLD).

- Ricevuta $\mathbf{w}$ calcoliamo la sindrome (se $\mathbf{w} \cdot H = \mathbf{0}$ non c'è errore).
- Elenchiamo all'inizio le sindromi dei coset leader.
- Cerchiamo tra le sindromi dei coset leader quella che coincide con $\mathbf{w} \cdot H$.
- Decodifichiamo come $\mathbf{w} + \mathbf{u}$, dove $\mathbf{u}$ è il coset leader individuato.

Il numero di parole di di lunghezza n e peso t è

$$\binom{n}{t} = \frac{n!}{t!(n-t)!}$$

Lemma 2.9. *Sia* $\mathbf{v} \in \mathbb{K}^n$*. Il numero di parole* $\mathbf{u} \in \mathbb{K}^n$ *tali che* $\mathrm{d}(\mathbf{u}, \mathbf{v}) \leq t$ *è*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}$$

Dimostrazione. L'unica parola distante 0 da $\mathbf{v}$ è la parola $\mathbf{v}$ stessa. Le parole distanti esattamente 1 da $\mathbf{v}$ sono $\binom{n}{1} = n$, quelle distanti esattamente 2 sono $\binom{n}{2}$ e così via. L'insieme delle parole distanti al più t da $\mathbf{v}$ è quindi

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}$$

□

Consideriamo un codice (non necessariamente lineare) di distanza $2t+1$ (oppure $2t+2$). Siano $\mathbf{v}_1, \mathbf{v}_2 \in C$, non esiste $\mathbf{w}$ tale che $\mathrm{d}(\mathbf{v_1}, \mathbf{w}) \leq t$ e $\mathrm{d}(\mathbf{v_2}, \mathbf{w}) \leq t$. Infatti $d(\mathbf{v}_1, \mathbf{v}_2) \leq \mathrm{d}(\mathbf{v}_1, \mathbf{w}) + \mathrm{d}(\mathbf{v}_2, \mathbf{w}) \leq t + t = 2$. Avremmo così trovato due parole $\mathbf{v}_1, \mathbf{v_2} \in C$ la cui distanza è $\leq 2t$ ma il codice ha distanza $2t+1$ (o $2t+2$) e questo sarebbe assurdo. Indicato con

$$B(\mathbf{v}_1, t) = \{\mathbf{w} \in \mathbb{K}^n : \mathrm{d}(\mathbf{w}, \mathbf{v_1}) \leq t\}$$

ne segue

$$\mathbb{K}^n \supseteq \bigcup_{\mathbf{v} \in C} B(\mathbf{v}, t)$$

e poiché i sottoinsiemi sono a due a due disgiunti segue che

$$|\mathbb{K}^n| \geq \bigcup_{\mathbf{v} \in C} B(\mathbf{v}, t)| =$$

$$\sum_{\mathbf{v} \in C} |B(\mathbf{v}, t)| = |C| \cdot |B(\mathbf{v}, t)| \leq$$

$$|C| \cdot [\binom{n}{0} + \cdots + \binom{n}{t}]$$

da cui

$$|C| \leq \frac{2^n}{\binom{n}{0} + \cdots + \binom{n}{t}} = \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}} \tag{2.10}$$

L'equazione (2.10) è la disuguaglianza o *limite di Hamming* e vale per tutti i codici (anche quelli non lineari).
Dato il codice lineare C con $\dim C = k, \mathrm{length} C = n, d(C) = d$ allora

$$d - 1 \leq n - k \tag{2.11}$$

La condizione dell'equazione (2.13) è detta *singleton bound* ed è meno forte del limite di Hamming. Condideriamo una matrice controllo di parità H per il codice C: la distanza di C è d se, comunque si scelgono $d-1$ righe di H, queste righe saranno linearmente indipendenti. Se le prime $d-1$ righe sono linearmente dipendenti allora nel codice è contenuta la parola con le prime $d-1$ componenti uguali a 1 e le rimanenti uguali a 0. Poiché il rango per righe è uguale al rango per colonne ci possono essere al più $n-k$ righe linearmente indipedenti dai cui il limite (2.13).

Definizione 2.29. Un codice lineare tale che $d-1 = n-k$ si dirà MDS (Maximum Distance Separable).

Teorema 2.10. *Per un codice C (lineare) i seguenti fatti sono equivalenti.*

- $d = n - k + 1$.
- *Comunque si scelgono $n - k$ righe nella matrice controllo di parità tali righe sono linearmente indipendenti.*
- *Comunque si scelgono k colonne nella matrice generatrice tali colonne sono linearmente indipendenti.*
- *C è MDS.*

Corollario 2.11. *Se C è MDS allora anche $C^{\perp}$ è MDS.*

Teorema 2.12 (Limite di Gilbert-Varshamov)**.** *Un codice lineare di lunghezza n, dimensione k e distanza d esiste se la seguente disuguaglianza è soddisfatta.*

$$\binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2} < 2^{n-k}.$$

Esempio 2.30. Sia $S = \{0110, 1010, 1100, 00110, 1111\}$. Estraiamo da S un sottoinsieme di parole linearmente indipendenti.

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

Poiché $R_2 + R_3 = R_4$ si potrebbe già scartare R_4. Riduciamo la matrice ottenuta per righe e otterremo

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

Scartando le ultime due righe

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \tag{2.12}$$

L'insieme di tutte le combinazioni lineari delle parole ottenute è un codice lineare:

$$C = \langle 1010, 0110, 0011 \rangle \tag{2.13}$$

con dim$C = 3$. Calcoliamo, infine, una tra tutte le possibili matrici controllo di parità per il codice C. Chiaramente $H \in \mathbb{K}^{4,1}$. Riduciamo la matrice (2.12) in RREF ottenendo

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} = (1, X)$$

quindi

$$H = \begin{bmatrix} X \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Dalla disuguaglianza di Hamming abbiamo che

$$C \leq \frac{2^n}{\binom{n}{0} + \cdots + \binom{n}{t}} \tag{2.14}$$

dove t è tale che $d = 2t + 1$ (d è la distanza del codice che è dispari).

Capitolo 3

Codici perfetti

Definizione 3.1. Diremo che un codice C di lunghezza n e distanza $d = 2t + 1$ è *perfetto* se vale l'uguaglianza nell'equazione (2.14).

Fissato $r \geq 2$ consideriamo $n = 2^r - 1$. Sia H la matrice le cui righe sono tutte le parole non nulle di lunghezza r. Ne segue che le righe di H sono $2^r - 1$.

Esempio 3.1.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Un codice che ha H come matrice controllo di parità si dice codice di Hamming. In questo caso $H \in \mathbb{K}^{2^r-1,r}$. Calcoliamo la distanza di tale codice.

$$\mathrm{d} = \min\{k : \text{in } H \text{ ci sono } k \text{ righe l.d.}\}.$$

Esistono due righe in H linearmente dipendenti? No, poiché in H non ci sono due righe uguali. Esistono tre righe in H linearmente dipendenti? Sì, basta scegliere come terza riga la somma delle prime due. Quindi la distanza in un codice di Hamming è 3.

Osservazione 3.1. I codici di Hamming sono perfetti.

Sia G la matrice generatrie di un codice C. La matrice generatrice del codice esteso da C è

$$G^\star = (G, \mathbf{b})$$

con $\mathbf{b}$ vettore colonna, dove $\mathbf{b}_i$ è 1 se il peso della riga i-esima di G è dispari, mentre è 0 in caso contrario.

Definizione 3.2. Sia $G \in \mathbb{K}^{k,n}$ una matrice generatrice del codice C ($\dim C = \mathrm{rk}G = k$). Se G è della forma seguente

$$G = (I, A), \;\; I \in \mathbb{K}^{n,n}$$

si dirà in forma standard.

Esempio 3.2. La matrice

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

non si può portare in forma standard.

Definizione 3.3. Un codice C che possiede una matrice generatrice in forma standard si dirà *sistematico*.

In questo caso l'informazione inviata codificando la parola mediante G in forma standard è contenuta nelle prime k cifre:

$$(x_1, \ldots, x_k) \cdot G = (x_1, \ldots, x_k, y_{k+1}, \ldots, y_n)$$

Definizione 3.4. Due codici $C, C' \in \mathbb{K}^n$ si dicono *equivalenti* se esiste una permutazione $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ tale che

$$\sigma C = C'$$

Considerata una parola $(x_1, \ldots, x_n)$ una permutazione è del tipo

$$\sigma(x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Esempio 3.3. Consideriamo il codice lineare $C = \{000, 001, 010, 110\}$. Un codice equivalente è

$$C' = \{000, 100, 010, 011\}$$

Osservazione 3.2. Codici equivalenti hanno stessa dimensione e distanza.

Definizione 3.5 (Codice di Golay esteso)**.** Un codice di Golay esteso, che indichiamo con C_{24}, è un codice generato dalla matrice $G = (1, B) \in \mathbb{K}^{12,24}$ tale che

$\dim C_{24} = 12$ e la lunghezza di C_{24} è 24. La matrice B è la seguente.

$$B = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \tag{3.1}$$

Una matrice controllo di parità del codice esteso C_{24} è

$$H = \begin{bmatrix} B \\ I \end{bmatrix}.$$

Vale

$$G \cdot H = (I, B) \cdot \begin{bmatrix} B \\ I \end{bmatrix} = \mathbf{0}$$

Un'altra matrice controllo di parità è

$$H' = \begin{bmatrix} I \\ B \end{bmatrix}.$$

Questo è possibile perché

$$B = {}^tB$$

e quindi

$$B \cdot {}^tB = B \cdot B = \mathbf{1} \tag{3.2}$$

Avremo

$$G \cdot H' = (I, B) \cdot \begin{bmatrix} I \\ B \end{bmatrix} = I + B \cdot {}^tB = I + B \cdot B = I + B^2 = I + I = \mathbf{0}.$$

Anche la matrice $G' = (B, I)$ è una matrice generatrice di C_{24}. Per verificare che G' è una matrice generatrice di C_{24} è sufficiente verificare che $G' \cdot H = \mathbf{0}$ oppure $G' \cdot H' = \mathbf{0}$.
Inoltre C_{24} è autoduale, quindi C_24 coincide con il proprio duale. Ovvero vale

$$C_{24}^{\perp} = C_{24} \tag{3.3}$$

La distanza di C_{24} è 8. C_{24} è un codice 3-correttore.

Dimostriamo che il codice C_{24} ha distanza 8.
Passo 1. Dimostriamo che il peso di ogni parola di C_{24} è un multiplo di 4. Nella matrice G tutte le righe hanno un peso multiplo di 4. Dall'osservazione che le righe di G sono ortogonali segue che il numero di posti in cui le due righe hanno entrambe degli 1 è pari.
Siano, infatti, $\mathbf{r}_i, \mathbf{r}_j$ due righe di G, segue che

$$\mathrm{wt}(\mathbf{r}_i + \mathbf{r}_j) = \mathrm{wt}(\mathbf{r}_i) + \mathrm{wt}(\mathbf{r}_j) - 2(2x)$$

dove x è il numero di posizioni in cui i bit 1 delle due parole si sovrappongono. Siano ad esempio $\mathbf{r}_i = (0111010), \mathbf{r}_j = (1110001)$, le due parole sono tali che i bit 1 si sovrappongono nelle posizioni 1 e 2.

$$\begin{array}{c} 0\ \mathbf{1}\ \mathbf{1}\ 1\ 0\ 1\ 0 \\ 1\ \mathbf{1}\ \mathbf{1}\ 0\ 0\ 0\ 1 \end{array}$$

Quindi sommando due qualunque parole della matrice G si ottiene ancora una parola il cui peso è un multiplo di 4. Procedendo per induzione sommiamo tre parole di G.

$$\mathbf{r}_i + \mathbf{r}_j + \mathbf{r}_k = (\mathbf{r}_i + \mathbf{r}_j) + \mathbf{r}_k$$

In questo caso $\mathbf{r}_i + \mathbf{r}_j$ è di peso multiplo di 4 ed è quindi ancora ortogonale a $\mathbf{r}_k$. Quindi per lo stesso ragionamento fatto in precedenza anche $\mathbf{r}_i + \mathbf{r}_j + \mathbf{r}_k$ ha peso che è un multiplo di 4. Da un semplice sguardo alle righe di G segue che la distanza di C_{24} deve essere 4 oppure 8.
Passo 2. Supponiamo che $\mathbf{v} \in C_{24}$ sia tale che $\mathrm{wt}(\mathbf{v}) = 4$ (vogliamo dimostrare che tale parola non può esistere). Esisteranno $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{K}^{12}$ tali che $\mathbf{v} = \mathbf{u}_1(I, B)$ e $\mathbf{v} = \mathbf{u}_2(B, I)$. Se $\mathrm{wt}(\mathbf{v}) = 4$ segue necessariamente che $\mathrm{wt}(\mathbf{u}_1) \leq 2$ oppure $\mathrm{wt}(\mathbf{u}_2) \leq 2$. Supponiamo che $\mathrm{wt}(\mathbf{u}_1) \leq 2$ allora $\mathbf{u}_1 \cdot G$ è la somma di al più due righe di G. Poiché tutte le righe di G hanno peso 8 oppure 12 segue che $\mathrm{wt}(\mathbf{u}_1) = 2$. A questo punto basterà controllare che la somma di due qualunque parole di G ha peso ≥ 8. Ne segue che *non* possono esistere parole di peso 4 in C_{24}.

Decodifica di C_{24}. Sia $\mathbf{w} \in \mathbb{K}^{24}$ la parola ricevuta. Sia $\mathbf{v} \in \mathbb{C}_{24}$ tale che $\mathrm{d}(v, w) = \min\{\mathrm{d}(\mathbf{x}, \mathbf{v}) : x \in \mathbb{C}_{24}\}$. Sia $\mathbf{u} \in \mathbb{K}^{24}$ tale che $\mathbf{v} + \mathbf{u} = \mathbf{w}$. Se $\mathrm{wt}(\mathbf{u}) \leq 3$ saremo in grado di correggere l'errore. Sia $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2)$ con $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{K}^{12}$. Poiché stiamo supponendo che $\mathrm{wt}(\mathbf{u}) \leq 3$ ne segue che $\mathrm{wt}(\mathbf{u}_1) \leq 1$ oppure $\mathrm{wt}(\mathbf{u}_2) \leq 1$.
Sia $\mathbf{s}_1 = \mathbf{w} \cdot \begin{bmatrix} I \\ B \end{bmatrix}$ una sindrome.

Avremo

$$\mathbf{s}_1 = \mathbf{w} \cdot \begin{bmatrix} I \\ B \end{bmatrix} = \mathbf{u} \cdot \begin{bmatrix} I \\ B \end{bmatrix} = [\mathbf{u}_1, \mathbf{u}_2] \cdot \begin{bmatrix} I \\ B \end{bmatrix} = \mathbf{u}_1 + \mathbf{u}_2 B.$$

Se $\mathrm{wt}(\mathbf{u}_2) \leq 1$ allora $\mathrm{wt}(\mathbf{u}_2) = 0$ oppure $\mathrm{wt}(\mathbf{u}_2) = 1$.
Se $\mathrm{wt}(\mathbf{u}_2) = 1$ allora $\mathbf{s}_1 = \mathbf{u}_1 + \mathbf{0} \cdot B = \mathbf{u}_1$ da cui $\mathrm{wt}(\mathbf{s}_1) = \mathrm{wt}(\mathbf{v}_1) \leq 3$.
Se $\mathrm{wt}(\mathbf{u}_2) = 1$ allora $\mathbf{s}_1 = \mathbf{u}_1 + \mathbf{u}_2 \cdot B = \mathbf{u}_1 + \mathbf{r}_i$, dove $\mathbf{r}_i$ è la i-esima riga di B, da cui $\mathrm{wt}(\mathbf{v}_1) \leq 2$. In tal caso la sindrome $\mathbf{s}_1$ è una riga di B con al più due bit scambiati.

Osservazione 3.3. Poiché $B^2 = I$ segue che

$$\mathbf{s}_1 = \mathbf{u}_1 + \mathbf{u}_2 \cdot B$$

e

$$\mathbf{s}_2 = \mathbf{u}_1 \cdot B + \mathbf{u}_2 = (\mathbf{u}_1 + \mathbf{u}_2 \cdot B) = \mathbf{u}_1 \cdot B + \mathbf{u}_2 \cdot B^2 = \mathbf{u}_1 \cdot \mathbf{u}_1 \cdot B + \mathbf{u}_2$$

Procedura di decodifica.

- Calcoliamo la sindrome $\mathbf{s} = \mathbf{w} \cdot \begin{bmatrix} I \\ B \end{bmatrix}$.
- Se $\mathrm{wt}(\mathbf{s}) \leq 3 \Rightarrow \mathbf{u} = (\mathbf{s}, \mathbf{0})$.

Altrimenti

- Se $\mathrm{wt}(\mathbf{s} + \mathbf{r}_i) \leq 2$ per qualche riga di $B \Rightarrow \mathbf{u} = [\mathbf{s} + \mathbf{r}_i, \mathbf{e}_i]$.

Altrimenti

- Calcoliamo $\mathbf{s}_2 = \mathbf{s}B$.
- Se $\mathrm{wt}(\mathbf{s}B) \leq 3 \Rightarrow \mathbf{u} = [\mathbf{0}, \mathbf{s}B]$.

Altrimenti

- Se $\mathrm{wt}(\mathbf{s}B + \mathbf{r}_i) \leq 2$ per qualche riga della matrice $B \Rightarrow \mathbf{u} = [\mathbf{e}_i, \mathbf{s}B + \mathbf{r}_i]$.

Sia $C \in \mathbb{K}^n$ un codice lineare di lunghezza n, la proiezione i-esima $\pi : \mathbb{K}^n \to \mathbb{K}^{n-1}$ trasforma il codice $C \in \mathbb{K}^n$ in un codice lineare $\pi_i(C) \in \mathbb{K}^{n-1}$ nel seguente modo.

$$\pi_i(x_1, \ldots, x_i, x_{i+1}, \ldots, x_n) = (x_1, \ldots, x_{i+1}, \ldots, x_n)$$

Esempio 3.4.

$$\pi_1(x, y, z, t) = (y, z, t)$$
$$\pi_2(x, y, z, t) = (x, z, t)$$

Definizione 3.6 (Codice di Golay)**.** Il codice di Golay C_{23} ha lunghezza 23 e si ottiene dal codice di Golay esteso eliminando l'ultimo bit di ogni parola di C_{24}.

Ovviamente la matrice generatrice G di C_{23} è la matrice $G = (I, \hat{B})$ dove $\hat{B} \in \mathbb{K}^{12,11}$ è ottenuta dalla matrice (3.1) eliminando l'ultima colonna. $\dim C_{23} = 12$. C_{23} ha distanza 7. C_{23} può correggere tutti gli errori di peso al più 3. È una facile verifica dimostrare che il codice di Golay è perfetto.
Decodifica di C_{23}. Sia $\mathbf{w}$ la parola ricevuta, costruiamo la parola $(\mathbf{w}, i) = \mathbf{w}i$, con $i \in \{0, 1\}$, dove si pone $i = 0$ se il peso di $\mathbf{w}$ è dispari e $i = 1$ se il peso di $\mathbf{w}$ è pari. In questo modo la parola $\mathbf{w}i \notin C_{24}$ (per come abbiamo deciso di aggiungere il bit i). Utilizziamo la procedura di decodifica del codice di Golay esteso e ottenuta la parola $\mathbf{v} \in C_{24}$ ne scartiamo l'ultimo bit (la parola così ottenuta è la più vicina alla parola $\mathbf{w}$ che cercavamo).
Se $\mathbf{w}$ arriva senza errori, $\mathbf{w}i$ avrà un errore (nell'ultima posizione).
Se $\mathbf{w}$ arriva con un errore, $\mathbf{w}i \notin C_{24}$. Decodificando come $(\mathbf{w}, i) + (\mathbf{e}_k, 0)$, dove $k = 1, \ldots, 23$, si ottiene una parola di C_{24}.
Se $\mathbf{w}$ arriva con due errori bisognerà correggere tre errori nella parola $(\mathbf{w}, i)$ di cui uno è proprio il simbolo i.
Se $\mathbf{w}$ arriva con tre errori bisognerà correggere ancora tre errori in $(\mathbf{w}, i)$.

Codici di Reed-Muller. Un codice di Reed-Muller di ordine r e lunghezza 2^m si indica con $\mathrm{RM}(r, m)$ dove r, m sono interi positivi tali che

$$0 \leq r \leq m, \;\; m \geq 0.$$

La costruzione di tali codici si può ottenere in modo ricorsivo.

- $\mathrm{RM}(0, m) = \{\underbrace{00\ldots0}_{2^m}, 11\ldots1\}$, $\mathrm{RM}(0, m) \subseteq \mathbb{K}^{2^m}, \mathrm{RM}(m, m) = \mathbb{K}^{2^m}$.
- $\mathrm{RM}(r, m) = \{(\mathbf{x}, \mathbf{x} + \mathbf{y}) : \mathbf{x} \in \mathrm{RM}(r, m-1), \mathbf{y} \in \mathrm{RM}(r-1, m-1)\}$.

La matrice generatrice del codice $\mathrm{RM}(r, m)$ è

$$G(r, m) = \begin{bmatrix} G(r, m-1) & G(r, m-1) \\ 0 & G(r-1, m-1) \end{bmatrix}.$$

$(\mathbf{x}, \mathbf{x}) \in \mathrm{RM}(r, m)$ con $\mathbf{x} \in \mathrm{RM}(r, m-1)$.
$(\mathbf{0}, \mathbf{y}) \in \mathrm{RM}(r, m)$ con $\mathbf{x} \in \mathrm{RM}(r-1, m-1)$.

Esempio 3.5. $\mathrm{RM}(0, 1) = \{00, 11\}$. Il codice ha lunghezza $2^1 = 2$.

Esempio 3.6. $\mathrm{RM}(0, 2) = \{0000, 1111\}$.

Esempio 3.7. $\mathrm{RM}(0, 3) = \{00000000, 11111111\}$.

Esempio 3.8. $\mathrm{RM}(1,2) = \{(\mathbf{x}, \mathbf{x}+\mathbf{y}) : \mathbf{x} \in \mathrm{RM}(1,1), \mathbf{y} \in \mathrm{RM}(0,1)\}$.
$\mathrm{RM}(0,1) = \{00, 11\}$.
$\mathrm{RM}(1,2) = \{0000, 0101, 1010, 1111, 0011, 0011, 0110, 1001, 1100\}$.
In termini di matrice generatrice

$$G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ \mathbf{0} & G(0,1) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} =$$

Osservazione 3.4. $G(0,m) = (\underbrace{1 \ldots 1}_{2^m})$.

Teorema 3.1. *Per il codice RM(r,m) si ha*

- *lunghezza di RM(r,m) è 2^m;*
- *distanza di RM(r,m) è 2^{m-r};*
- *dimensione di RM(r,m) è $\sum_{i=0}^{r} \binom{m}{i} = \binom{m}{0} + \cdots + \binom{m}{r}$.*

Esempio 3.9. Sia $m = 3 \Rightarrow \mathrm{RM}(1,m) = \mathrm{RM}(1,3)$.

- Lunghezza di $\mathrm{RM}(1,3)$ è $2^m = 2^3 = 8$.
- Distanza di $\mathrm{RM}(1,3)$ è $2^{m-r} = 2^{3-1} = 2^2 = 4$.
- Dimensione di $\mathrm{RM}(1,3)$ è $\sum_{i=0}^{r} \binom{m}{i} = \sum_{i=0}^{1} \binom{3}{i} = \binom{3}{0} + \binom{3}{1} = 1 + 3 = 4$.

Decodifica dei codici $\mathrm{RM}(1,m)$. Sia $\mathbf{w}$ la parola ricevuta. Se c è una parola del codice tale che $\mathrm{d}(\mathbf{w}, \mathbf{c}) \leq 2$ allora $\mathbf{w}$ si decodifica come $\mathbf{c}$.
Se $\mathrm{d}(\mathbf{w}, \mathbf{c}) > 6 \Rightarrow \mathrm{d}(\mathbf{w}, \mathbf{c}+\mathbf{1}) < 2$ (dove $\mathbf{1}$ è la parola con tutti 1). Allora decodifichiamo $\mathbf{w}$ come $\mathbf{c}+\mathbf{1}$ (ovviamente $\mathbf{c}+\mathbf{1} \in \mathrm{RM}$ perché $\mathbf{1} \in \mathrm{RM}$).
In generale consideriamo $\mathrm{RM}(1,m)$. La lunghezza è 2^m, la distanza è $2^{m-r} = 2^{m-1}$, la dimensione è $\binom{m}{0} + \binom{m}{1} = 1 + m$. Poiché $\mathrm{d}(C) = 2^{m-1}$ riusciremo a correggere circa 2^{m-2} errori ($\left\lfloor \frac{2^{m-1}-1}{2} \right\rfloor$).
Se $\mathrm{d}(\mathbf{w}, \mathbf{c}) < 2^{m-2}$ allora si decodifica come $\mathbf{c}$.
Se $\mathrm{d}(\mathbf{w}, \mathbf{c}) < 2^m - 2^{m-2}$ allora si decodifica come $\mathbf{c}+\mathbf{1}$.

Capitolo 4

Codici cicicli

Definizione 4.1 (Permutazione ciclica)**.** Chiamiamo *permutazione ciclica* l'applicazione $\pi : \mathbb{K}^n \to \mathbb{K}^n$ così definita.

$$\pi(a_0 a_1 \dots a_n) = a_n a_0 \dots a_{n-1}.$$

Esempio 4.1. $1011 \xrightarrow{\pi} 1101$.

Definizione 4.2. Un codice $C \in \mathbb{K}^n$ si dirà ciclico se è *invariante* rispetto a permutazioni cicliche, ovvero

$$\forall c \in C \Rightarrow \pi(c) \in C.$$

Esempio 4.2. $C = \{\mathbf{0}\}$.

Esempio 4.3. $C = \{\mathbf{0}, \mathbf{1}\}$.

Esempio 4.4. $C = \{101, 110, 011, 000\} = \langle 101, 110 \rangle$. ($C$ è codice lineare).
$\pi(101) = 110$.
$\pi(110) = 011$.
$\pi(011) = 101$.

Esempio 4.5. $C = \{01, 10\}$ è ciclico ma non lineare.

$\pi : \mathbb{K}^n \to \mathbb{K}^n$ è un'applicazione lineare ovvero

$$\pi(\mathbf{x} + \mathbf{y}) = \pi(\mathbf{x}) + \pi(\mathbf{y}) \ \ \forall \mathbf{x}, \mathbf{y} \in \mathbb{K}^n \quad \text{(additività)}$$

ed anche

$$\pi(\alpha + \mathbf{x}) = \alpha + \pi(\mathbf{x}) \ \ \forall \alpha \in \mathbb{K}, \mathbf{x} \in \mathbb{K}^n \quad \text{(omogeneità)}.$$

(Nel caso dei campi finiti $\mathbb{K} = \{0, 1\}$ è sufficiente che sia verificata la sola proprietà di additività).

Teorema 4.1. *$C = \langle B \rangle$ è ciclico se e solo se B è invariante rispetto a π.*

(Il teorema segue direttamente dalla definizione di linearità di π).
In particolare si può scegliere come insieme di generatori B una base di C.

Sia $\mathbf{x} \in \mathbb{K}^n$. L'insieme costituito da $\mathbf{x}, \pi(\mathbf{x}), \pi(\pi(\mathbf{x})) = \pi^2(\mathbf{x}), \ldots, \pi^{n-1}(\mathbf{x})$ è un insieme di generatori per un codice ciclico.

Polinomi a coefficienti su $\mathbb{K}$. Un polinomio di grado n è un'espressione formale di questo tipo

$$a_0 + a_1 x + \cdots + a_n x^n \text{ con } a_0, a_1, \ldots, a_n \in \mathbb{K}.$$

Se $a_n \neq 0$ diremo che $a_0 + a_1 x + \cdots + a_n x^n$ ha grado n. L'insieme di tutti i polinomi si indica con $\mathbb{K}[x]$ (il sottoinsieme dei polinomi di grado $\leq n$ si indica con $\mathbb{K}[x]_n$). Con l'operazione di somma tra polinomi e di prodotto tra uno scalare ed un polinomio gli insiemi $\mathbb{K}[x]$ e $\mathbb{K}[x]_n$ sono spazi vettoriali.
Inoltre

$$\mathbb{K}[x]_1 \subseteq \mathbb{K}[x]_2 \subseteq \ldots \mathbb{K}[x]_n \subseteq \mathbb{K}[x].$$

Corrispondenza tra polinomi e parole. Consideriamo una parola, avremo

$$a_0 a_1 \ldots a_n \mapsto a_0 + a_1 x + \cdots + a_n x^n.$$

Esempio 4.6. $x^3 + x^5 + 1 + x = \underbrace{1 + x + x^3 + x^5}_{=1+1\cdot x+0\cdot x^2+1\cdot x^3+0\cdot x^4+1\cdot x^5} \mapsto 110101.$

Esempio 4.7. $\mathbb{K}[x]_2$ è lo spazio vettoriale (insieme) dei polinomi di grado ≤ 2. $\mathbb{K}[x]_2 \ni 1 + x^2, x + x^2, 1 + x, x, 1$. L'insieme corrispondente delle parole è

$$\{101, 011, 110, 010, 100\}.$$

Moltiplichiamo un polinomio $g(x)$ per x. Avremo

$$g(x) = a_0 + a_1 x + \cdots + a_n x^n \xrightarrow{x \cdot g(x)} a_0 x + a_1 x + \cdots + a_n x^{n+1}.$$

L'operazione equivale alla permutazione ciclica

$$a_0 a_1 \ldots a_n \xrightarrow{\pi} a_n a_0 \ldots a_{n-1}.$$

Divisione tra polinomi. Dati $p(x), g(x) \in \mathbb{K}[x]$, con $p(x)$ dividendo e $g(x)$ divisore, esistono e sono unici due polinomi $q(x) \in \mathbb{K}[x]$ e $r(x) \in \mathbb{K}[x]$ con $\deg(r(x)) < \deg(g(x))$ (grado di $r(x)$ minore del grado di $g(x)$) tali che

$$p(x) = q(x) \cdot g(x) + r(x).$$

Esempio 4.8. $60 \div 7$.

$$\begin{array}{r} 8 \\ 7\overline{)\,60} \\ \underline{56} \\ 4 \end{array}$$

Esempio 4.9. $p(x) = 5x^4 + x^3 - x^2 + 2x + 4,\ \ g(x) = x^2 - x + 3.$

$$\begin{array}{rr} & 5x^2 + 6x - 10 \\ \cline{2-2} x^2 - x + 3\big) & 5x^4 + x^3 - x^2 + 2x + 4 \\ & \underline{-5x^4 + 5x^3 - 15x^2} \\ & 6x^3 - 16x^2 + 2x \\ & \underline{-6x^3 + 6x^2 - 18x} \\ & -10x^2 - 16x + 4 \\ & \underline{10x^2 - 10x + 30} \\ & -26x + 34 \end{array}$$

$q(x) = 5x^2 + 6x - 10,\ \ r(x) = -26x + 34.$

Definizione 4.3. Diremo che due polinomi $f(x)$ e $g(x)$ sono *congruenti* modulo $h(x)$ e lo indichiamo con $f(x) \equiv g(x) \bmod h(x)$ se $f(x)$ e $g(x)$ hanno lo stesso resto nella divisione per $h(x)$.

Equivalentemente $f(x)$ e $g(x)$ sono congruenti modulo $h(x)$ se $f(x) - g(x)$ è un multiplo di $h(x)$. Per dimostrare che un polinomio è multiplo di $h(x)$ è sufficiente dividere il polinomio per $h(x)$ e verificare che il resto sia 0).

Indichiamo con $\overline{f(x)}$ la classe di equivalenza modulo $h(x)$ avente $f(x)$ come rappresentante.

$$\overline{f(x)} = \{g(x) \in \mathbb{K}[x] : g(x) \equiv f(x) \bmod h(x)\}$$

ovvero l'insieme dei polinomi $g(x)$ tali che

$$g(x) - f(x) \text{ è multiplo di } h(x)$$

ovvero

$$g(x) - f(x) = q(x) \cdot h(x) \text{ con } q(x) \in \mathbb{K}[x].$$

Sia $g(x) \in \overline{f(x)}$ tale che $\deg g(x) = \min\{\deg a(x) : a(x) \in \overline{f(x)}, a(x) \neq 0\}$ (per convenzione $a(x) = 0 \Rightarrow \deg a(x) = -1$). Tale $g(x)$ è unico, a meno di multipli, cioè se $\deg g(x) = \deg f(x) = \min\{\deg a(x) : a(x) \in \overline{f(x)}\}$ allora $g(x) = kf(x)$ con k costante moltiplicativa non nulla.

Sia $f(x) : \deg f(x) = \deg g(x)$ e applichiamo il teorema sulla divisione tra polinomi: $f(x) = q(x) \cdot g(x) + r(x)$ con $\deg r(x) < \deg g(x)$ (oppure $r(x) = 0$). Se $r(x) \neq 0$, poiché $r(x) \in \overline{f(x)} = \overline{g(x)}$ ne seguirebbe l'assurdo che

$$\deg r(x) < \min\{\deg a(x) : a(x) \in \overline{f(x)}\}.$$

Esempio 4.10. Troviamo una base del più piccolo codice ciclico contenente $\mathbf{v} = 1101000$.

$$\begin{aligned} g(x) &= 1 + x + x^3 \\ xg(x) &= x + x^2 + x^4 \\ x^2g(x) &= x^2 + x^3 + x^5 \\ x^3g(x) &= x^3 + x^4 + x^6 \\ x^4g(x) &= x^4 + x^5 + x^7 \end{aligned}$$

Per descrivere tutte le parole di $\mathbb{K}^7$ abbiamo scelto di utilizzare tutti i polinomi di grado ≤ 6 ($\mathbb{K}[x]_6$). Poiché

$$x^7 \equiv 1 \bmod (1 + x^7)$$

riduciamo il polinomio $x^4g(x)$ modulo $(1 + x^7)$. Otterremo

$$(x^4 + x^5 + x^7 \equiv x^4 + x^5 + 1) \bmod (1 + x^7)$$

Le parole del codice saranno

$$C = \langle \overline{g(x)}, \overline{xg(x)}, \overline{x^2g(x)}, \overline{x^3g(x)}, \overline{x^4g(x)} \rangle$$

dove con $\overline{x^ig(x)}$ si intende la classe di equivalenza modulo $(1 + x^7)$. Una matrice generatrice del codice (ciclico) C si otterrà riducendo per righe la seguente matrice

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

Un codice ciclico di lunghezza n si può interpretare come un insieme di classi di equivalenza di polinomi modulo $(1 + x^n)$.

Osservazione 4.1. Se $\mathbf{v} \in C$ (ciclico) e $v(x) \in \mathbb{K}[x]$ è il polinomio corrispondente allora i polinomi $c(x)$ tali che $c(x) \equiv a(x)v(x) \bmod (1 + x^n)$ sono *parole* di C e viceversa, se $c(x)$ è una *parola* di C allora $c(x) \equiv v(x) \bmod (1 + x^n)$.

Esempio 4.11. Sia $\mathbf{v} = 1101000$. Avremo

$$v(x) = 1 + x + x^3, \quad x^5 v(x) = x^5(1 + x + x^3) = x^5 + x^6 + x^8.$$

Ma

$$x^5 + x^6 + x^8 \equiv x^5 + x^6 + 1 \bmod (1 + x^7)$$

quindi

$$\overline{x^8} = \overline{x \cdot x^7} = \overline{x \cdot 1}.$$

Definizione 4.4. Sia C un codice ciclico di lunghezza n, indichiamo ancora con C l'insieme delle classi di equivalenza che rappresentano C in $\mathbb{K}[x]/_{\bmod (1+x^n)}$, chiamiamo generatore di C il polinomio $g(x)$ (diverso da 0) che ha grado minimo tra tutti quelli contenuti nelle classi di equivalenza di C.

Dato un codice ciclico C e sia $\mathbf{v} \in C$. Allora dati $a(x) \in \mathbb{K}[x]$ (volendo si può scegliere dega$(x) <$ lunghezza di C) e $v(x)$ il polinomio associato alla parola $\mathbf{v}$ allora se $c(x) \in \mathbb{K}[x]$ è tale che

$$c(x) \equiv a(x)v(x) \bmod (1 + x^n).$$

ne segue che $c(x)$ *rappresenta* una parola appartenente a C.
Il rappresentante canonico della classe di equivalenza

$$\begin{aligned}\overline{f(x)} &= \{g(x) \in \mathbb{K}[x] : g(x) \equiv f(x) \bmod (1 + x^n)\} \\ &= \{g(x) = f(x) + a(x) \cdot (1 + x^n)\}\end{aligned}$$

è il polinomio $c(x) \in \overline{f(x)}$ di grado minimo.

Esempio 4.12. Sia $f(x) = x + x^5 + x^{12}$. Troviamo il rappresentante canonico della classe di equivalenza

$$\overline{f(x)} = \{g(x) \in \mathbb{K}[x] : g(x) \equiv f(x) \bmod (1 + x^n)\}$$

fissato $n = 6$.
Avremo

$$\overline{f(x)} = \{g(x) \in \mathbb{K}[x] : g(x) \equiv f(x) \bmod (1 + x^6)\}.$$

In tal caso il rappresentante canonico di $\overline{f(x)}$ sarà il resto della divisione di $f(x)$ per $1 + x^6$.

$$\begin{array}{r|l} & x^6 \quad\quad -1 \\ \hline x^6+1 & x^{12} \quad +x^5+x \\ & -x^{12}-x^6 \\ \hline & \quad -x^6+x^5+x \\ & \quad\; x^6 \quad\quad +1 \\ \hline & \quad\quad\quad x^5+x+1 \end{array}$$

Quindi $x^5 + x + 1$ è il rappresentante canonico.

Definizione 4.5. Sia C un codice ciclico. Definiamo polinomio generatore di C, *il* polinomio *non nullo* di grado minimo.

Osservazione 4.2. Sia $g(x)$ un polinomio che *genera* un codice ciclico C. Se $\deg g(x) = n - k$ i polinomi

$$\underbrace{g(x), xg(x), x^2g(x), \ldots, x^{k-1}g(x)}_{k} \tag{4.1}$$

costituiscono una base di C.
Inoltre $\dim C = k$.

I polinomi (4.1) sono indipendenti perché sono tutti di grado diverso.

Teorema 4.2. *Il generatore di un codice ciclico (lineare) di lunghezza n è necessariamente un divisore del polinomio $1 + x^n$.*

Esempio 4.13. $1 + x^2 = (1 + x)(1 + x)$.

Definizione 4.6. Un polinomio si dice irriducibile se è divisibile soltanto per 1 o per se stesso. (Il polinomio 1 non si condidera irriducibile).

Corollario 4.3. *Dato il codice ciclico di C (lunghezza di C è n) e $v(x) \in C$, il generatore di C è il polinomio $g(x) = MCD(v(x), 1 + x^n)$.*

Esempio 4.14. Calcoliamo MCD$(18, 30)$ mediante il crivello di Eratostene. Scomponiamo 18 e 30 in fattori:

$$18 = 3^2 \cdot 2$$
$$30 = 3 \cdot 2 \cdot 5.$$

Il massimo comune divisore sarà dato dal prodotto dei fattori comuni con il minimo esponente quindi

$$\text{MCD}(18, 30) = 3 \cdot 2 = 6.$$

Esempio 4.15. Calcoliamo MCD$(18, 30)$ mediante l'algoritmo di Euclide.

$$30 = \underbrace{q_1}_{=1} \cdot 18 + \underbrace{r_2}_{=12}$$
$$30 = \underbrace{q_1}_{=2} \cdot 12 + \underbrace{r_2}_{=6}$$

Quindi

$$\text{MCD}(18, 30) = 3 \cdot 2 = 6.$$

Esempio 4.16. Sia C il codice ciclico generato da $g(x) = 1 + x + x^3, n = 7$. Si avrà

$$\mathbb{K}^7 \simeq \mathbb{K}[x]/(1 + x^7) \simeq \mathbb{K}^6.$$

Un insieme di generatori per C è

$$g(x), xg(x), x^2g(x), x^3g(x), \ldots$$

quindi

$$\begin{aligned} g(x) &= 1 + x + x^3 \\ xg(x) &= x + x^2 + x^4 \\ x^2g(x) &= x^2 + x^3 + x^5 \\ x^3g(x) &= x^3 + x^4 + x^6 \\ x^4g(x) &= x^4 + x^5 + x^7 \end{aligned}$$

ma

$$x^4 + x^5 + x^7 \equiv x^4 + x^5 + 1 (\mathrm{mod}(1 + x^7))$$

pertanto

$$1 + x^4 + x^5 \in \langle 1 + x + x^3, x + x^2 + x^4, x^2 + x^3 + x^5, x^3 + x^4 + x^6 \rangle$$

Esempio 4.17. Sia $\mathbf{v} = 010101$. Il codice ciclico più piccolo contenente $\mathbf{v}$ sarà

$$C = \langle x + x^3 + x^5, 1 + x^2 + x^4 \rangle.$$

Il polinomio generatore sarà $1 + x^2 + x^4$.

Codifica di un codice ciclico. Siano

$$a(x) \in \mathbb{K}[x]_{\dim C - 1}, \ \deg g(x) = n - k, \ \deg a(x) = n - 1.$$

Allora $a(x) \cdot g(x)$ è un polinomio di grado $n - 1$. Questo completa la codifica.

Decodifica di un codice ciclico. Se $c(x) \in C$ allora $a(x) = c(x) \div g(x)$. Un polinomio $c(x)$ appartiene al codice ciclico generato dal polinomio $g(x)$ se e solo se il resto della divisione di $c(x)$ per $g(x)$ è 0.
La matrice di parità $H = [\ldots]$ sarà tale che $x_i = r_i(x) \bmod g(x), i = 1, \ldots, n - 1$, cioè nelle righe avremo i coefficienti di $r_i(x)$.
Il polinomio $g(x)$ è un generatore di un codice ciclico di lunghezza n se e solo se $g(x)$ divide $1 + x^n$. Il problema si riconduce, quindi, a costruire tutte le fattorizzazioni di $1 + x^n$.

Esempio 4.18. $1 + x^3 = (1 + x)(1 + x + x^2)$.

Esempio 4.19. $1 + x^4 = (1 + x^2)^2 = (1 + x)^4$.

Il duale di un codice ciclico è ancora un codice ciclico.
Se π è la permutazione ciclica $\mathbf{y} \in C^\perp \Rightarrow \pi(\mathbf{y}) \in C^\perp$.