Codici a blocco

Introduzione ai codici lineari: definizione di campo

- Un campo è una struttura composta da un insieme non vuoto F e da due operazioni binarie *interne*: *somma* e *prodotto*. Per ogni $\alpha, \beta, \gamma \in F$ vale

Somma

$$\alpha + \beta \in F$$
$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$
$$\alpha + \beta = \beta + \alpha$$
$$0 \in F, \alpha + 0 = \alpha, \alpha - \alpha = 0$$

Prodotto (2)

$$\alpha * \beta \in F$$
$$(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$$
$$\alpha * \beta = \beta * \alpha$$
$$1 \in F, \alpha * 1 = \alpha, \forall \alpha \neq 0 \; \alpha * \alpha^{-1} = 1$$
$$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$$

Introduzione ai codici lineari: i campi di Galois

- Un campo di Galois GF(q) è un campo con un *numero finito* q di elementi.
- GF(2) è il campo definito su $\{0, 1\}$ con somma modulo 2 ("XOR") e prodotto modulo 2 ("AND").
- Una volta definito GF(2), si può costruire lo spazio vettoriale $\mathcal{V}_n = \text{GF}(2)^n$, lo spazio di tutte i possibili 2^n vettori di n cifre binarie su cui valgono le operazioni definite per GF(2).

Codici a blocco lineari su GF(2)

- Sia $\mathbf{u} = [u_1, u_2, \ldots, u_k]$ una generica parola di k cifre binarie. Il codice a blocco lineare $\mathcal{C}(k, n) \subset \mathcal{V}_n$ è l'insieme delle 2^k parole $\mathbf{x} = [x_1, x_2, \ldots, x_n]$ di n cifre binarie ottenute con la trasformazione lineare

$$\mathbf{x} = \mathbf{uG} \tag{3}$$

  dove $\mathbf{G}$ è una matrice $k \times n$ di cifre binarie.
- $\mathbf{G}$ è la *matrice generatrice* del codice.

Codici a blocco lineari su GF(2)

- Siano $\mathbf{g}_i$ $(i = 1, 2, \ldots, k)$ le righe di $\mathbf{G}$, $\mathbf{x}$ è la combinazione lineare delle righe $\mathbf{g}_i$.

$$\mathbf{x} = \sum_{i=1}^{k} u_i \mathbf{g}_i \tag{4}$$

- Perché ci siano 2^k parole di codice distinte è necessario che $\mathbf{G}$ abbia rango $k \implies$ le righe di $\mathbf{G}$ sono linearmente indipendenti e costituiscono una *base* per il *sottospazio vettoriale* $\mathcal{C} \subset \mathcal{V}_n$.

Proprietà dei codici lineari a blocchi

- Alcune semplici proprietà derivano direttamente dalla linearietà dei codici:
  1. Ogni parola di codice è una combinazione lineare di righe della matrice generatrice.
  2. Il codice a blocchi è costituito da tutte le possibili combinazioni delle righe della matrice generatrice.
  3. La somma di due parole di codice è ancora una parola di codice.
  4. La n-pla di tutti zeri è sempre una parola di codice.
  5. Se $\mathbf{x}$ è una parola di codice, anche $-\mathbf{x}$ è una parola di codice.

Distanza di Hamming

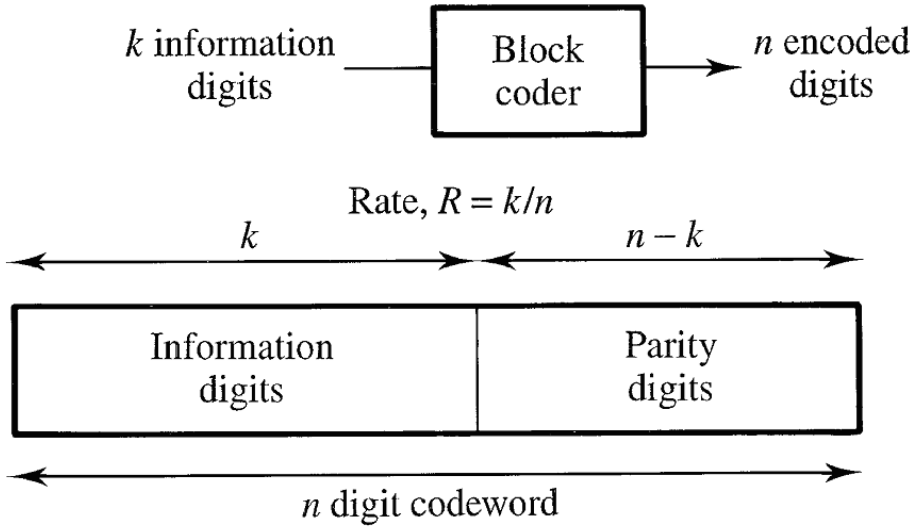
- La distanza di Hamming $d(\mathbf{x}_1, \mathbf{x}_2)$ tra due vettori di n elementi $\mathbf{x}_1$ e $\mathbf{x}_2$ è il numero di posizioni in cui le due parole sono diverse tra loro.
- La distanza di Hamming è una metrica.
  1. $d(\mathbf{x}_1, \mathbf{x}_2) \geq 0$
  2. $d(\mathbf{x}_1, \mathbf{x}_2) = 0 \Leftrightarrow \mathbf{x}_1 = \mathbf{x}_2$
  3. $d(\mathbf{x}_1, \mathbf{x}_2) = d(\mathbf{x}_2, \mathbf{x}_1)$
  4. $d(\mathbf{x}_1, \mathbf{x}_3) \leq d(\mathbf{x}_1, \mathbf{x}_2) + d(\mathbf{x}_2, \mathbf{x}_3)$
- Il peso di Hamming di un vettore $\mathbf{x}_0 \in \mathcal{V}_n$ è $w(\mathbf{x}_0) = d(\mathbf{x}_0, \mathbf{0}_n)$
- La *distanza minima* di un codice $\mathcal{C}$ è la minima distanza di Hamming calcolata fra tutte le possibili parole che appartengono a $\mathcal{C}$.

Codici a blocco in forma sistematica

- Quando il codice è in *forma sistematica* la matrice generatrice del codice ha la seguente forma

$$\mathbf{G} = [\mathbf{I}_k, \mathbf{P}] \tag{5}$$

- La matrice $\mathbf{P}$, di dimensioni $k \times (n-k)$ è la *matrice di parità*.



Esempio: codice a ripetizione $R = 1/3$

- Codice a ripetizione $R = 1/3$

Bit in ingresso	Parola codificata
1	[111]
0	[000]

- La matrice generatrice del codice è

$$\mathbf{G} = [111] \tag{6}$$

- La distanza minima del codice è $d_{min} = 3$.

Esempio: codice a controllo di parità $R = 7/8$

- Codice a a controllo di parità $R = 7/8$. Ogni 7 bit ne aggiunge uno di controllo di parità: 1 se il numero di '1' è dispari, 0 se il numero di '1' è pari.
- La matrice generatrice del codice è

$$\mathbf{G} = [\mathbf{I}_7, \mathbf{1}_7] \tag{7}$$

- il prodotto $\mathbf{u}\mathbf{1}_7 = \sum_{i=1}^{7} u_i$ può essere scritto come una somma modulo 2 e quindi vale 0 se il il numero di '1' è pari e 1 altrimenti.
- La distanza minima del codice è $d_{min} = 2$. Dimostrazione.

Codici a blocco in forma sistematica

Definizione: Due codici lineari $\mathcal{C}_1(k, n)$ e $\mathcal{C}_2(k, n)$ in $GF(2)$ sono *equivalenti* se uno è ottenuto dall'altro attraverso una permutazione delle posizioni del codice;
Teorema 1: Due matrici generatici $\mathbf{G}_1$ and $\mathbf{G}_2$ in $GF(2)$ generano due codici equivalenti se una può essere ottenuta dall'altra da una sequenza di operazioni di questo tipo:

1. Permutazione delle righe;
2. Combinazione lineare di righe;
3. Permutazione delle colonne.

Teorema 2: Qualsiasi codice lineare a blocchi è equivalente ad un codice in forma sistematica.

Codici a blocco in forma sistematica

- Dato il sottospazio $\mathcal{C} \subset \mathcal{V}_n$ di dimensione k esiste un sottospazio ortogonale (null space) $\mathcal{C}^{\perp} \subset \mathcal{V}_n$ di dimensione $n-k$, definito dalla matrice $\mathbf{H}$ di dimensioni $n-k \times n$ tale che

$$\mathbf{G}\mathbf{H}^T = \mathbf{0}_{k,n-k} \tag{8}$$

- La base di $\mathcal{C}^{\perp}$ è costituita dalle $n-k$ righe della matrice $\mathbf{H}$, per cui ogni elemento $\mathbf{t} \in \mathcal{C}^{\perp}$ può essere rappresentato

$$\mathbf{t} = \mathbf{v}\mathbf{H} = \sum_{i=1}^{n-k} v_i \mathbf{h}_i \tag{9}$$

- Per ogni $\mathbf{x} \in \mathcal{C}$ e per ogni $\mathbf{t} \in \mathcal{C}^{\perp}$ si ha

$$\mathbf{x}\mathbf{t}^T = \mathbf{u}\mathbf{G}\mathbf{H}^T\mathbf{v}^T = 0 \tag{10}$$

Matrice di controllo di parità

- La matrice $\mathbf{H}$ è la *matrice di controllo di parità* del codice.
- Per costruzione, per ciascun $\mathbf{x} \in \mathcal{C}$ vale

$$\mathbf{x}\mathbf{H}^T = \mathbf{u}\mathbf{G}\mathbf{H}^T = \mathbf{0}. \tag{11}$$

- La matrice la matrice di controllo di parità non è unica. Se $\mathbf{G}$ è sistematica si può utilizzare la relazione

$$[\mathbf{A}, \mathbf{B}] \begin{bmatrix} \mathbf{C} \\ \mathbf{D} \end{bmatrix} = \mathbf{AC} + \mathbf{BD} \tag{12}$$

per trovare

$$\mathbf{H} = \left[\mathbf{P}^T, \mathbf{I}_{n-k}\right]. \tag{13}$$

Esempi: codice a ripetizione e a controllo di parità

- Per il codice a ripetizione $R = 1/3$ si ha $k = 1, n = 3$ e $n - k = 2$, per cui la matrice la matrice di controllo di parità è

$$\mathbf{H} = \left[\mathbf{P}^T, \mathbf{I}_2\right] = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}. \tag{14}$$

- Per il codice a controllo di parità $R = 7/8$ si ha $k = 7, n = 8$ e $n - k = 1$, per cui la matrice la matrice di controllo di parità è

$$\mathbf{H} = \left[\mathbf{P}^T, \mathbf{I}_1\right] = \mathbf{1}_8^T. \tag{15}$$