Teoria dei codici

Introduzione

Applicazioni dei codici nel mondo che ci circonda

- Messaggi possono essere codificati per vari motivi
  - *Compressione dell'informazione*: Comprimere l'informazione eliminando tutta la ridondanza e risparmiare banda o spazio di memoria;
  - *Crittografia*: Nascondere il contenuto di un messaggio ad utenti diversi da quello desiderato;
  - *Rivelazione o correzione di errore*: Viene aggiunta ridondanza ad hoc per aumentare la resistenza a rumore e ad interferenza.

Applicazioni dei codici nel mondo che ci circonda

- Codici per applicazioni commerciali
  - Codici a rivelazione di errore: ISBN, carte di credito, TCP (16 bit checksum), codice ASCII (1 bit checksum).
  - Codici a correzione di errore: Hard disk (RS), cd (RS), comunicazioni cellulari, comunicazioni satellitari.

Applicazioni dei codici nel mondo che ci circonda: ridondanza nella lingua italiana

Sneocdo uno sdtiuo dlel'Untisverà di Cabmbrige, non irmptoa cmoe snoo sctrite le plaroe, tutte le letetre posnsoo esesre al pstoo sbgalaito, è ipmtortane sloo che la prmia e l'umiltia letrtea saino al ptoso gtsiuo, il rteso non ctona, il cerlvelo è comquune semrpe in gdrao di decraifre tttuo qtueso coas, pcheré non lgege ongi silngoa ltetrea, ma lgege la palroa nel suo insmiee...

Tassonomia dei codici

- Codici lineari:
  - Codici a blocco
  - Codici convoluzionali
- Definizione di un codice a blocco
  - Rate $R = k/n$ del codice
    - Esempio: quale è il rate di un codice che ha 1024 parole di lunghezza 15 bit?
- Rivelazione di errore
- Correzione di errore

Un esempio di codici a blocco: codici a ripetizione

- Codici a ripetizione: codici a blocco più semplici che esistano.
- Esempio: codice a ripetizione con $R = 1/3$
  - $m = 0 \rightarrow c = [000]$
  - $m = 1 \rightarrow c = [111]$
- Ricevitore effettua decodifica a maggioranza
  - decide per il bit che compare nella maggioranza delle posizioni della parola ricevuta.
- Esempio:
  - $r = [000] \rightarrow \hat{c} = [000], \hat{m} = 0$
  - $r = [010] \rightarrow \hat{c} = [000], \hat{m} = 0$
  - $r = [101] \rightarrow \hat{c} = [111], \hat{m} = 1$

Un esempio di codici a blocco: codici a ripetizione

- In BSC, la probabilità di sbagliare t bit in una parola di n bit è

$$p(t, n) = \binom{n}{t} p^t (1-p)^{(n-t)},$$

dove il coefficiente binomiale

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

indica tutti i possibili pattern di errore (il numero di tutte le possibili combinazioni di t errori su n bit).

- Un codice a ripetizione con $R = 1/n$ può rivelare fino a $n - 1$ errori e correggere $(n-1)/2$ errori (per n dispari).

Un esempio di codici a blocco: codici a ripetizione

- L'evento errore per un codice a correzione di errore consiste nel non essere in grado di correggere tutti gli errori (introdotti dal canale).
- Se la probabilità di errore sul bit $p_{e,b}$ è sufficientemente piccola, la probabilità di errore $p_{e,W}$ per il codice può essere approssimata dal primo evento che determina la ricezione errata (ad esempio dall'aver fatto 2 errori per $R = 1/3$).
  - Codice a ripetizione $R = 1/3$
    1. Se $p_{e,b} = 0.1 \implies p_{e,W} \approx 2.7 * 10^{-2}$ ($p_{e,W} = 2.8 * 10^{-2}$)
    2. Se $p_{e,b} = 0.01 \implies p_{e,W} \approx 2.97 * 10^{-4}$ ($p_{e,W} = 2.98 * 10^{-4}$).
  - Codice a ripetizione $R = 1/5$
    1. Se $p_{e,b} = 0.1 \implies p_{e,W} \approx 8.1 * 10^{-3}$
    2. Se $p_{e,b} = 0.01 \implies p_{e,W} \approx 9.8 * 10^{-6}$.

Un esempio di codici a blocco: codici a controllo di parità

- Codice con rate $R = k/(k+1)$: k bit informativi + 1 di parità (1 se #bit dispari, 0 altrimenti)

k	n	Stringa di bit	Bit di parità	Parola codificata
2	3	[10]	1	[101]
7	8	[1010101]	0	[10101010]

- Esempio 1: Codice ASCII 128 caratteri rappresentati da 7 bit, l'ottavo bit è di controllo di parità (contenuto in un byte).

Un esempio di codici a blocco: codici a controllo di parità

- Esempio 2: Trasmetto parole di 11 bit con rate $R_b = 10Mb/s$ e probabilità di errore sul bit trasmesso $p_{e,b} = 10^{-8}$.
  - Senza controllo di parità è sufficiente che sia sbagliato anche un solo bit per sbagliare tutta la parola:

$$p_{e,W} = \sum_{j=1}^{11} \binom{11}{j} p_{e,b}^{j} (1-p_{e,b})^{(11-j)} \approx 11 p_{e,b} (1-p_{e,b})^{10} \approx 11p,$$

ed il rate di parole sbagliate al secondo è

$$R_{e,w} = R_b/11 * p_{e,W} \approx (10^7/11) * 11p = 0.1w/s.$$

Sbaglio una parola ogni $T_{e,w} = 1/R_{e,w} = 10$ s!

Un esempio di codici a blocco: codici a controllo di parità

- Esempio 2 -continuazione-
  - Aggiungo un bit di parità. La parola diventa di 12 bit e sbaglio quando faccio almeno 2 errori, gli errori di 1 bit vengono rivelati e corretti (mediante ritrasmissione della parola).
    In questo caso, si ha

$$p_{e,W} = \sum_{j=2}^{12} \binom{12}{j} p_{e,b}^{j}(1-p_{e,b})^{(12-j)} \approx 66p_{e,b}^{2}(1-p_{e,b})^{10} \approx 66p_{e,b}^{2},$$

ed il rate di parole sbagliate al secondo è

$$R_{e,w} = R_b/12 * p_{e,W} \approx (10^7/12) * 66p_{e,b}^2 = 5.5 * 10^{-9} w/s.$$

Sbaglio una parola ogni $T_{e,w} = 1/R_{e,w} = 1.82 * 10^8$ s, una parola ogni sei anni circa (1 anno $\approx 3.15 * 10^7$s)!

Codici a blocco

Modulo-2 addition and multiplication

- Modulo-2 addition (subtraction is the same)
  - $0 + 0 = 0$
  - $1 + 0 = 1$
  - $0 + 1 = 1$
  - $1 + 1 = 0$
- Modulo-2 multiplication
  - $0 \times 0 = 0$
  - $1 \times 0 = 0$
  - $0 \times 1 = 0$
  - $1 \times 1 = 1$

Codici a blocco lineari

- Sia $\mathbf{m} = [m_1, m_2, \ldots, m_k]$ una parola di k cifre binarie.
- Il codice a blocco lineare $\mathcal{C}(k, n)$ è l'insieme delle 2^k parole $\mathbf{c} = [c_1, c_2, \ldots, c_n]$ di n cifre binarie ottenute con la trasformazione lineare
$$\mathbf{c} = \mathbf{mG} \tag{2}$$
dove $\mathbf{G}$ è una matrice $k \times n$ di cifre binarie.
- $\mathbf{G}$ è la *matrice generatrice* del codice.

Codici a blocco lineari

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

$$\mathbf{c} = \mathbf{m}\mathbf{G} = \sum_{i=1}^{k} m_i \mathbf{g}_i \tag{3}$$

- 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 (costituiscono una *base* di $\mathcal{C}$).

Proprietà dei codici lineari a blocchi

- Semplici proprietà che derivano direttamente dalla linearietà dei codici:
  1. Ogni parola di codice è una combinazione lineare di righe della matrice generatrice.
  2. Il codice 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.

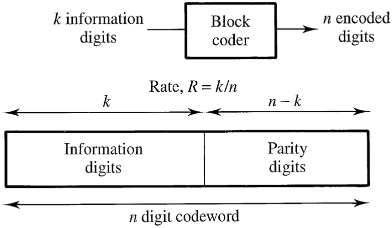
Distanza di Hamming

- La distanza di Hamming $d_H(\mathbf{c}_1, \mathbf{c}_2)$ tra due vettori di n elementi $\mathbf{c}_1$ e $\mathbf{c}_2$ è il numero di posizioni in cui le due parole sono diverse tra loro.
- La distanza di Hamming è una metrica.
  1. $d_H(\mathbf{c}_1, \mathbf{c}_2) \geq 0$
  2. $d_H(\mathbf{c}_1, \mathbf{c}_2) = 0 \Leftrightarrow \mathbf{c}_1 = \mathbf{c}_2$
  3. $d_H(\mathbf{c}_1, \mathbf{c}_2) = d(\mathbf{c}_2, \mathbf{c}_1)$
  4. $d_H(\mathbf{c}_1, \mathbf{c}_3) \leq d_H(\mathbf{c}_1, \mathbf{c}_2) + d_H(\mathbf{c}_2, \mathbf{c}_3)$
- Il peso di Hamming di $\mathbf{c}$ è

$$w(\mathbf{c}) = d_H(\mathbf{c}, \mathbf{0}_n)$$

- La *distanza minima* di un codice $\mathcal{C}$ è la minima distanza di Hamming calcolata fra tutte le possibili parole.

Codici a blocco in forma sistematica



- Quando il codice è in *forma sistematica*

$$\mathbf{G} = [\mathbf{P}, \mathbf{I}_k] \tag{4}$$

- Quindi:

$$\mathbf{c} = \mathbf{mG} = \mathbf{m}[\mathbf{P}, \mathbf{I}_k] = [\mathbf{mP}, \mathbf{m}] = [\mathbf{b}, \mathbf{m}] \tag{5}$$

- La matrice **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

$$\mathbf{G} = [111] = \mathbf{1}_{1,3} \tag{6}$$

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

Matrice di controllo di parità

- La matrice $\mathbf{H}$
$$\mathbf{H} = \left[\mathbf{I}_{n-k}, \mathbf{P}^T\right]. \tag{7}$$
è la *matrice di controllo di parità* del codice.
- Per ciascun $\mathbf{c} \in \mathcal{C}$ vale
$$\mathbf{c}\mathbf{H}^T = \mathbf{m}\mathbf{G}\mathbf{H}^T = \mathbf{0}_{1,n-k}. \tag{8}$$

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

$$\mathbf{H} = \left[\mathbf{I}_2, \mathbf{P}^T\right] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \tag{9}$$

- 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

$$\mathbf{H} = \left[\mathbf{I}_1, \mathbf{P}^T\right] = \mathbf{1}_{1,8}. \tag{10}$$