Decodifica dei codici a blocco

Decodifica per i codici a blocco

Dato il vettore ricevuto

$$\mathbf{y} = \mathbf{x} + \mathbf{e}, \tag{1}$$

Il decisore ottimo seleziona la parola di codice $\hat{\mathbf{x}}$ tale che

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x} \in \mathcal{C}} p(\mathbf{y}|\mathbf{x}) = \arg\min_{\mathbf{x} \in \mathcal{C}} d_H(\mathbf{y}, \mathbf{x}), \tag{2}$$

- Per ottenere $\hat{\mathbf{x}}$ è necessario fare 2^k confronti fra il vettore ricevuto $\mathbf{y}$ e tutte le parole di codice di $\mathcal{C}(k, n)$;
- La complessità cresce esponenzialmente con k.

Decodifica per i codici a blocco

Un approccio alternativo consiste nell'osservare che, poiché si ha

$$\mathbf{y} = \mathbf{x} + \mathbf{e} \implies \mathbf{x} = \mathbf{y} + \mathbf{e}, \mathbf{e} = \mathbf{y} - \mathbf{x},$$

la probabilità condizionata può essere riscritta come

$$p(\mathbf{y}|\mathbf{x}) = p(\mathbf{x} + \mathbf{e}|\mathbf{x}) = p(\mathbf{e}|\mathbf{y} + \mathbf{e} \in \mathcal{C}) \tag{3}$$

e quindi, la stima di $\mathbf{x}$ può essere ottenuta come

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x} \in \mathcal{C}} p(\mathbf{y}|\mathbf{x}) = \mathbf{y} + \arg\max_{\mathbf{e}} p(\mathbf{e}|\left\{\mathbf{y} + \mathbf{e} \in \mathcal{C}\right\}) \tag{4}$$

Decodifica per i codici a blocco

Invece di stimare $\hat{\mathbf{x}}$, si stima il vettore errore $\hat{\mathbf{e}}$ più probabile

$$\begin{aligned}\hat{\mathbf{e}} &= \arg\max_{\mathbf{e}} p(\mathbf{e}|\{\mathbf{y}+\mathbf{e}\in\mathcal{C}\}) \\ &= \arg\max_{\mathbf{e}|\{\mathbf{y}+\mathbf{e}\in\mathcal{C}\}} p^{w(\mathbf{e})}(1-p)^{n-w(\mathbf{e})} \\ &= \arg\max_{\mathbf{e}|\{\mathbf{y}+\mathbf{e}\in\mathcal{C}\}} \left(\frac{1-p}{p}\right)^{-w(\mathbf{e})} = \arg\min_{\mathbf{e}|\{\mathbf{y}+\mathbf{e}\in\mathcal{C}\}} w(\mathbf{e})\end{aligned} \tag{5}$$

- La decodifica sceglie fra tutti i possibili vettori errore $\mathbf{e}$ tali che $\mathbf{y}+\mathbf{e}\in\mathcal{C}$ quello che ha il peso di Hamming minimo, il minimo numero di errori (*massima verosimiglianza*).
- Una volta stimato $\hat{\mathbf{e}}$, si ottiene

$$\hat{\mathbf{x}} = \mathbf{y}-\hat{\mathbf{e}} = \mathbf{y}+\hat{\mathbf{e}} = \mathbf{x}+(\mathbf{e}+\hat{\mathbf{e}}) = \begin{cases}\mathbf{x} & \text{if } \hat{\mathbf{e}}=\mathbf{e} \\ \mathbf{x}_1\neq\mathbf{x} & \text{if } \hat{\mathbf{e}}\neq\mathbf{e}\end{cases}. \tag{6}$$

Decodifica per i codici a blocco

- *Definizione*: Coset. Sia $\mathcal{C}(k, n)$ un codice a blocco e sia $\mathbf{v} \in \mathcal{V}_n$ un vettore di n cifre binarie, si definisce il *coset* di $\mathcal{C}(k, n)$ individuato da $\mathbf{v}$ l'insieme

$$C_{\mathbf{v}} = C + \mathbf{v} = \{\mathbf{x} + \mathbf{v} : \mathbf{x} \in \mathcal{C}\} \tag{7}$$

- *Proprietà dei coset*:
  1. Qualsiasi vettore in $\mathcal{V}_n$ appartiene ad un coset di $\mathcal{C}(k, n)$;
  2. Ciascun coset contiene 2^k elementi;
  3. Due coset o sono coincidenti o hanno intersezione nulla;
  4. Ci sono 2^{n-k} coset distinti;
  5. Se $\mathbf{v}_1$ e $\mathbf{v}_2$ appartengono allo stesso coset, $\mathbf{v}_1 + \mathbf{v}_2 \in \mathcal{C}(k, n)$ è una parola di codice;

Esempio di coset

Sia $\mathcal{C}(2,3) = \{000, 101, 010, 111\}$. I coset di $\mathcal{C}(2,3)$ sono

$$
\begin{aligned}
C + 000 &= \{000, 101, 010, 111\} = C_0 \\
C + 001 &= \{001, 100, 011, 110\} = C_1 \\
C + 010 &= \{010, 111, 000, 101\} = C_0 \\
C + 011 &= \{011, 110, 001, 100\} = C_1 \\
C + 100 &= \{100, 001, 110, 011\} = C_1 \\
C + 101 &= \{101, 000, 111, 010\} = C_0 \\
C + 110 &= \{110, 011, 100, 001\} = C_1 \\
C + 111 &= \{111, 010, 101, 000\} = C_0
\end{aligned}
\tag{8}
$$

Decodifica per i codici a blocco

Si può utilizzare il concetto di coset per effettuare la decodifica.

- Poiché $\mathbf{y} = \mathbf{x} + \mathbf{e}$, dalla definizione di coset discende che i vettori $\mathbf{e}$ e $\mathbf{y}$ appartengono allo stesso coset $C_{\mathbf{y}}$ e che i coset $C_{\mathbf{y}}$ e $C_{\mathbf{e}}$ sono coincidenti.
- Grazie alle proprietà dei coset, la somma qualsiasi elemento di $C_{\mathbf{y}}$ con $\mathbf{y}$ individua una parola di codice.
- Il vettore $\mathbf{e}$ va scelto fra gli elementi di $C_{\mathbf{y}}$ e la regola di decisione diventa

$$\hat{\mathbf{e}} = \arg\max_{\mathbf{e}} p(\mathbf{e} |\, \{\mathbf{y} + \mathbf{e} \in \mathcal{C}\}) = \arg\max_{\mathbf{e} \in \mathbf{C}_{\mathbf{y}}} p(\mathbf{e}) = \arg\min_{\mathbf{v} \in \mathbf{C}_{\mathbf{y}}} w(\mathbf{v}) \tag{9}$$

- Tra tutti i 2^k possibili vettori di $C_{\mathbf{y}}$, il principio di massima verosimiglianza ci dice che devo scegliere quello di peso minimo.

Decodifica per i codici a blocco

Algoritmo di decodifica:

1. Avendo ricevuto il vettore $\mathbf{y}$, si trova il coset di appartenenza $C_{\mathbf{y}}$;
2. Si identifica il *coset leader*, la parola di peso minimo del coset $C_{\mathbf{y}}$, che è anche la parola di peso minimo del coset $C_{\mathbf{e}}$;
3. Il coset leader è la stima del vettore di errore $\hat{\mathbf{e}}$.

Esempio di decodifica utilizzando i coset

Sia $\mathcal{C}(2,4) = \{0000, 1011, 0101, 1110\}$ la cui $d_{min} = 2$.
I coset sono

$$\begin{aligned}
C + 0000 &= \{0000, 1011, 0101, 1110\} \\
C + 0001 &= \{0001, 1010, 0100, 1111\} \\
C + 0010 &= \{0010, 1001, 0111, 1100\} \\
C + 1000 &= \{1000, 0011, 1101, 0110\}
\end{aligned}$$

Decodificare i due vettori ricevuti

1. $\mathbf{y} = [1101]$
2. $\mathbf{y} = [1111]$

Decodifica mediante sindrome per i codici a blocco

Si definisce *sindrome* di $\mathbf{y}$, il vettore $\mathbf{s}$ ottenuto dal prodotto di $\mathbf{y}$ con la matrice di controllo di parità

$$\mathbf{s} = \mathbf{y}\mathbf{H}^T = (\mathbf{x} + \mathbf{e})\,\mathbf{H}^T = \mathbf{x}\mathbf{H}^T + \mathbf{e}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T \tag{10}$$

- Tutti i membri di uno stesso coset hanno la stessa sindrome;
- La sindrome $\mathbf{s}$ è composta da $n - k$ cifre binarie;
- Le 2^{n-k} sindromi sono associate ai 2^{n-k} diversi coset del codice $\mathcal{C}(k, n)$;
- Ciascuna sindrome è associata ai 2^k pattern di errore appartenenti allo stesso coset.

Decodifica mediante sindrome per i codici a blocco

- Il decodificatore a sindrome compie quindi le seguenti operazioni:
  1. Calcola la sindrome $\mathbf{s} = \mathbf{y}\mathbf{H}^T$;
  2. Associa la sindrome al coset leader corrispondente $\mathbf{s} \to \mathbf{e}_{CL}(\mathbf{s})$;
  3. Corregge l'errore sommando il coset leader alla n-upla $\mathbf{y}$

$$\hat{\mathbf{x}} = \mathbf{y} + \mathbf{e}_{CL}(\mathbf{s}). \tag{11}$$

- La parola $\hat{\mathbf{x}}$ è una parola di codice:

$$\hat{\mathbf{x}}\mathbf{H}^T = (\mathbf{y} + \mathbf{e}_{CL}(\mathbf{s}))\mathbf{H}^T = \mathbf{s} + \mathbf{s} = 0 \tag{12}$$

- Per costruzione, la parola di codice $\hat{\mathbf{x}}$ minimizza la distanza di Hamming da $\mathbf{y}$!

Decodifica a sindrome per il codice di Hamming $m = 3$

Il codice ha $d_{min} = 3$ ed è in grado di correggere *esattamente* un errore.

- Si sceglie la matrice $\mathbf{H}$ in maniera che la *tabella di decodifica* associ alla sindrome il pattern di errore a peso 1 in cui il bit messo a 1 sia nella posizione corrispondente alla conversione della sindrome in decimale.

Codice non sistematico

Syndrome	Coset leader
[000]	[0000000]
[100]	[1000000]
[010]	[0100000]
[110]	[0010000]
[001]	[0001000]
[101]	[0000100]
[011]	[0000010]
[111]	[0000001]

Codice non sistematico

Syndrome	Coset leader
[000]	[0000000]
[100]	[0000100]
[010]	[0000010]
[110]	[1000000]
[001]	[0000001]
[101]	[0100000]
[011]	[0010000]
[111]	[0001000]

Esercizio

- Un codice lineare a blocchi ha la seguente matrice di controllo di parità:

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

  1. Determinare la matrice generatrice del codice;
  2. Decodificare mediante decodifica a sindrome la parola $\mathbf{y} = [110110]$ ed identificare la parola di codice trasmessa.

Prestazioni sistemi codificati

Calcolo della probabilità di errore sulle parole di codice

Un codice a blocco $\mathcal{C}(k, n)$ con $d_{min} = 2t + 1$ è in grado di correggere fino a t errori.

- Una parola ricevuta $\mathbf{y} = \mathbf{x} + \mathbf{e}$ è errata quando il canale introduce un numero di errori maggiore di t.
- La probabilità di errore $P_w(e) = \Pr\{w(\mathbf{e}) > t\}$ si calcola

$$P_w(e) = \sum_{j=t+1}^{n} \binom{n}{j} p^j (1-p)^{n-j}$$

- $P_w(e)$ può essere lower-bounded dalla probabilità dell'evento più probabile: aver commesso $t + 1$ errori

$$P_w(e) \approx \binom{n}{t+1} p^{t+1} (1-p)^{n-(t+1)}$$

Bound per il calcolo della probabilità di errore sul bit

Mentre la $P_w(e)$ si riesce a calcolare con precisione, nel caso del calcolo della probabilità di errore su bit codificato si deve per forza ricorrere ad approssimazioni.

- Il numero di bit errati in $\hat{\mathbf{x}}$ dopo la decodifica dipende dal vettore di errore $\mathbf{e}$ e da come agisce la decodifica a sindrome, che, in presenza di un numero di errori maggiore di t, aggiunge altri errori a quelli introdotti dal canale.
- La decodifica a sindrome restituisce sempre una parola di codice, quindi ogni volta che al ricevitore c'è un errore nella decodifica i bit errati sono almeno d_{min} degli n trasmessi.
- In questo caso la $P_b(e)$ si approssima

$$P_b(e) \approx \frac{d_{min}}{n} P_w(e) \approx \frac{d_{min}}{n} \binom{n}{t+1} p^{t+1} (1-p)^{n-(t+1)}. \quad (1)$$