Udine, 24 Febbraio 2005

Principi di Teoria dei Codici

Andrea Tonello

e-mail: tonello@uniud.it

http://www.diegm.uniud.it/tlc/tonello

UNIVERSITÀ DEGLI STUDI DI UDINE

DIEGM DIPARTIMENTO DI INGEGNERIA ELETTRICA, GESTIONALE E MECCANICA

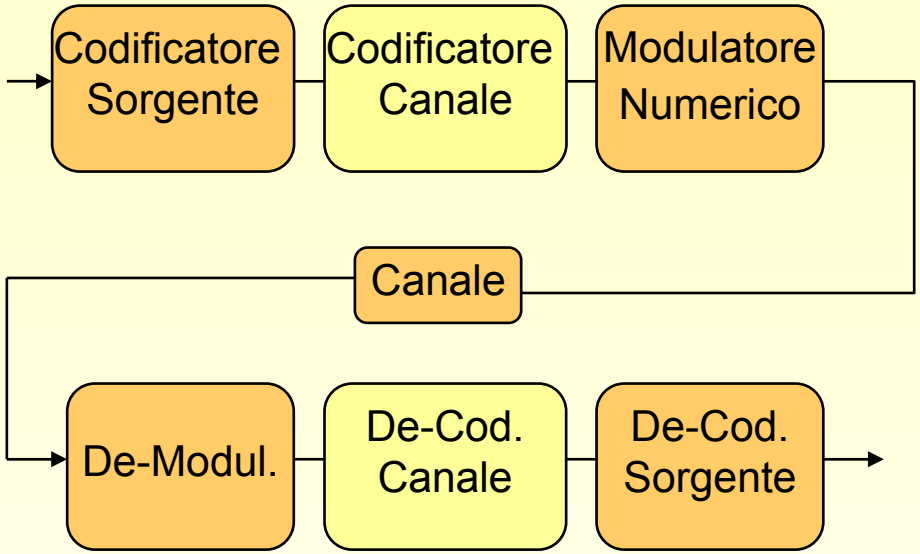
Sommario

- Approcci alla Codifica di Canale
- Codici a Blocco
- Prestazioni Codici a Blocco
- Codici Convoluzionali

Bibliografia:

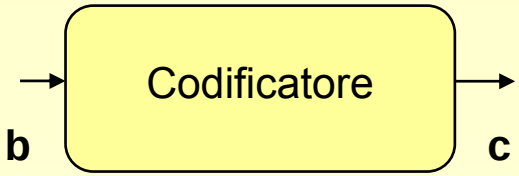
- J. Proakis, *Digital Communications*
- S. Lin, D. Costello, *Error Control Coding*

Modello Sistema di Comunicazione



- Lo scopo della Codifica di Canale e` di consentire la correzione e/o rivelazione degli errori introdotti dal canale.

Codifica di Canale



- ***Idea:*** Introdurre ridondanza in trasmissione, ad. es. ripetere l'informazione.
- Il **codificatore** attua una trasformazione dalle parole di ingresso **b** alle parole di uscita **c** con una certa legge:

$$\mathbf{b}=[\ldots,b_i,\ b_{i+1},\ldots] \ \rightarrow\ \mathbf{c}=[\ldots,c_i,\ c_{i+1},\ldots]$$

- **Alfabeto:** il campo cui appartengono gli elementi delle parole di ingresso, ad. es. GF(2).
- **Codice:** insieme delle parole codificate.
- **Rate:** rapporto tra numero di simboli di ingresso e quello di uscita (<1).

Approcci alla Codifica di Canale

- Codici Algebrici a Blocco
- Codici Convoluzionali
- Codifica e Modulazione Congiunta
  - Modulazione codificata a traliccio (TCM)
- Turbo Codici

Codici a Blocco

Codici a Blocco

- **Codice a blocco (n, k):**
  - Parole (Vettori) di ingresso hanno lunghezza k : $\mathbf{b}=[b_1,\ldots,b_k]$
  - Parole di uscita hanno lunghezza n>k : $\mathbf{c}=[c_1,\ldots,c_n]$
  - Alfabeto e` q-ario e le operazioni sono definite su un campo finito GF(q) con q primo o potenza di un numero primo.
  - Se q e` primo, l'algebra e` modulo q.
- **Definizione**: e` un insieme di q^k parole di n elementi.

- **Codice Lineare:** se $\mathbf{c}_1$ e $\mathbf{c}_2$ sono di codice allora $a\mathbf{c}_1 + b\mathbf{c}_2=\mathbf{c}_3$ e` di codice.
  - La parola nulla appartiene al codice.

Matrice di Codice

- **Matrice di Codice** $\underset{1\times n}{\mathbf{c}} = \underset{1\times k}{\mathbf{b}}\ \underset{k\times n}{\mathbf{G}}$. Elementi appartenti a GF(q)

- Le k righe di **G** sono vettori linearmente indipendenti e sono di codice.

- I vettori di codice appartengono al sottospazio k-dimensionale generato dalle righe di **G**.

- **Forma sistematica**

$$\mathbf{c} = [\mathbf{b} \,|c_{k+1},\ldots,c_n] \qquad \mathbf{G} = \begin{bmatrix} 1 & \ldots & 0 & p_{11} & \ldots & p_{1n-k} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 1 & p_{k1} & \ldots & p_{kn-k} \end{bmatrix} = [\mathbf{I} \,|\mathbf{P}]$$

Matrice di Controllo Parita`

- **Matrice di Controllo Parita`**

$$\underset{k\times n}{(\mathbf{G})}\ \underset{(n-k)\times n}{(\mathbf{H})^{T}} = \underset{k\times(n-k)}{\mathbf{0}}$$

- Le n-k righe di **H** sono vettori linearmente indipendenti e generano il codice duale (n-k,n)
- Le parole del codice duale sono ortogonali a quelle del codice (n,k)
- Se il codice e` in forma sistematica:

$$\underbrace{[\mathbf{I}_k \mid \mathbf{P}]}_{\mathbf{G}} \underbrace{\begin{bmatrix} -\mathbf{P} \\ \mathbf{I}_{n-k} \end{bmatrix}}_{\mathbf{H}^T} = \mathbf{0}$$

$$\mathbf{H} = \begin{bmatrix} -\mathbf{P}^T & \mathbf{I}_{n-k} \end{bmatrix}$$

Matrice di Controllo Parita`

- Matrice di Controllo Parita`ci consente di verificare se un vettore e` di codice

$$\mathbf{cH}^T \begin{cases} = 0 \ \text{se} \ \ c \in \mathbb{C} \\ \neq 0 \ \text{se} \ \ c \notin \mathbb{C} \end{cases}$$

- **Vettore Sindrome:** $\underset{1\times(n-k)}{\mathbf{s}} = \mathbf{cH}^T$

- Assumendo il codice binario abbiamo:
  - 2^k vettori di ingresso e di codice.
  - 2^n possibile vettori di dimensione n, quindi $2^n - 2^k$ non sono di codice.
  - 2^{n-k} sindromi.

Distanza e Peso di Hamming

- **Distanza di Hamming:** numero di simboli di cui differiscono due parole con alfabeto q-ario

$$d_H(\mathbf{r}_1,\mathbf{r}_2)$$

- **Peso di Hamming:** numero di simboli diversi da zero

$$w_H(\mathbf{r}_1)$$

- **Vale la seguente:** $d_H(\mathbf{c}_1,\mathbf{c}_2) = w_H(\mathbf{c}_1 - \mathbf{c}_2)$

Distanza Minima

- **Distanza Minima di Hamming:** e` la minima distanza tra parole di codice

$$d_{H,min} = \min_{\mathbf{c}_1,\mathbf{c}_2} \left\{ d_H(\mathbf{c}_1, \mathbf{c}_2) \right\}$$

- In un codice lineare la distanza minima e` pari al peso minimo:

$$d_{H,min} = w_{H,min}$$

Dim:

$$\begin{aligned} d_{H,min} &= \min_{\mathbf{c}_1,\mathbf{c}_2} \left\{ d_H(\mathbf{c}_1, \mathbf{c}_2) \right\} \\ &= \min_{\mathbf{c}_1,\mathbf{c}_2} \left\{ w_H(\mathbf{c}_1 - \mathbf{c}_2) \right\} \\ &= \min_{\mathbf{c} \neq \mathbf{0}} \left\{ w_H(\mathbf{c}) \right\} \end{aligned}$$

Singleton Bound

- **Bound di Singleton:** In un codice lineare a blocco

$$d_{H,min} \leq n - k + 1$$

- **Codici a massima distanza** verificano

$$d_{H,min} = n - k + 1$$

Dim: Basta pensare alla forma sistematica.

- Gli unici codici binari a massima distanza sono quelli ripetitivi altrimenti ci sono quelli di Reed Solomon su GF(q).

Esempi di Codici Lineari a Blocco

- Codici di Hamming.
- Codici di Hadamard.
- Codici BCH (Bose, Chaudhuri, Hocquenghem) e di Reed Solomon .

Codici di Hamming Binari

- $(n,k) = (2^{m-1}, 2^{m-1}-m)$ $m>1$ intero $n-k=m$
- La matrice **H** ha le n colonne ottenute prendendo tutti i vettori di m elementi binari escluso il vettore nullo.
- Codice di Hamming (7,4)

$$\mathbf{H} = [\mathbf{P}^T \mid \mathbf{I}_{n-k}] = \left[\begin{array}{cccc|ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

$$\mathbf{G} = [\mathbf{I}_k \mid \mathbf{P}] = \left[\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

- Il peso minimo e` uguale a 3

Codici di Hadamard

- $(n,k) = (2^m, m+1)$ $m>1$ intero
- Si ottengono dalle matrici di Hadamard cosi` definite

$$M_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad M_4 = \begin{bmatrix} M_2 & M_2 \\ M_2 & \overline{M}_2 \end{bmatrix}$$

- L'insieme delle parole di lunghezza n=4 ottenute dalle 4+4 righe di M_4 e di $\overline{M}_4$ sono un codice a blocco lineare con k=3 e peso minimo $d_{min}=n/2=2$

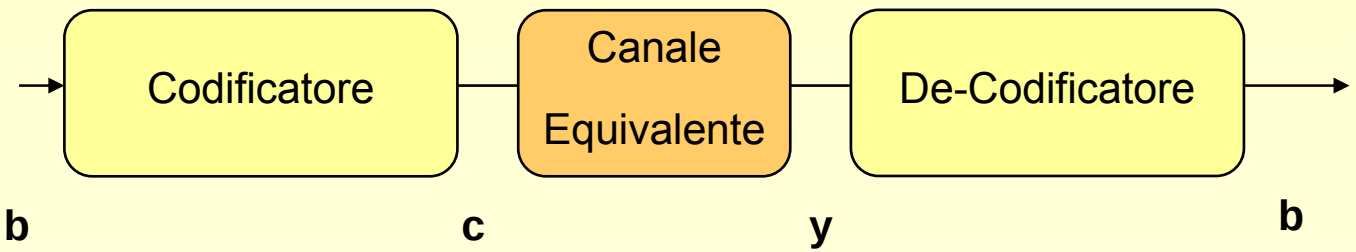
Codici BCH e Reed Solomon

- Binari (n,k) hanno parametri
  - $n=2^m-1$
  - $n-k \leq mt \quad con \quad m \geq 3 \quad t \geq 1$
  - $d_{min}=2t+1$

- Reed Solomon sono una sottoclasse non binaria.

Modello di Canale

Modello di Canale



- Modulatore – Canale – Demodulatore possono essere visti come un blocco equivalente.
- Bisogna definire la relazione ingresso-uscita. Essa dipende dal tipo di modulazione e demodulazione/decodifica:
  - **Demodulazione/Decodifica Congiunta**.
  - **Demodulazione/Decodifiva disgiunta**:
    - ***HARD***
    - ***SOFT***

Modello di Canale

- Alfabeto di codice binario, Modulazione 2-PAM, Rumore Additivo Gaussiano Bianco

$$y_i = \sqrt{E_S}\, x_i + n_i$$

$$x_i = 2c_i - 1$$
$$c_i \in \{0,1\}$$
$$x_i \in \{+1,-1\}$$
$$n_i = N(0, N_0/2) \text{ ed indip.}$$

- In forma vettoriale possiamo raccogliere le n osservazioni in un vettore e scrivere

$$\mathbf{y} = \sqrt{E_S}\,\mathbf{x} + \mathbf{n}$$

- C'e` una relazione biunivoca tra c ed x

$$\mathbf{x} = 2\mathbf{c} - 1$$

Decodifica Soft

Decodifica Ottima a Massima Verosimiglianza

- Il decodificatore ML decide per la parola di codice che massimizza la densita` di probabilita` del vettore ricevuto condizionata dal vettore trasmesso:

$$p_{Y|X}(\mathbf{y}\,|\,\mathbf{x}) = \prod_{i=1}^{n} p_{Y_i|X_i}(y_i\,|\,x_i)$$

$$= \prod_{i=1}^{n} \frac{1}{\sqrt{\pi N_0}} e^{-\frac{1}{N_0}(y_i - \sqrt{E_S}x_i)^2}$$

$$= (\pi N_0)^{n/2} e^{-\frac{1}{N_0}\|\mathbf{y} - \sqrt{E_S}\mathbf{x}\|^2}$$

- Il decodificatore ML decide per il vettore di codice che e` a distanza Euclidea minima dal vettore ricevuto

$$\hat{\mathbf{x}} = \underset{\mathbf{x}\in\mathbb{C}}{\arg\min}\{\| \mathbf{y} - \sqrt{E_S}\mathbf{x} \|^2\} \qquad \| \mathbf{y} - \sqrt{E_S}\mathbf{x} \|^2 = \sum_{i=1}^{n} (y_i - \sqrt{E_S}x_i)^2$$

Probabilita` Errore con Decodifica Soft

$$P_e = P[\hat{\mathbf{c}} \neq \mathbf{c}] = P[\hat{\mathbf{x}} \neq \mathbf{x}]$$
$$= \sum_{\mathbf{x}_i \in \mathbb{C}} P[\mathbf{x} = \mathbf{x}_i] P[\hat{\mathbf{x}} \neq \mathbf{x} \mid \mathbf{x} = \mathbf{x}_i]$$

$$P[E_{ij}] \leq P[\hat{\mathbf{x}} \neq \mathbf{x} \mid \mathbf{x} = \mathbf{x}_i] = P[\bigcup_j E_{ij}] \leq \sum_j P[E_{ij}]$$

$$E_{ij} = \{\hat{\mathbf{x}} = \mathbf{x}_j \neq \mathbf{x} = \mathbf{x}_i\}$$

Probabilita` Errore a Coppie

$$
\begin{aligned}
P[E_{ij}] &= P[\mathbf{x} = \mathbf{x}_i \rightarrow \hat{\mathbf{x}} = \mathbf{x}_j] \\
&= P[d_E(\mathbf{y}, \sqrt{E_S}\hat{\mathbf{x}}) < d_E(\mathbf{y}, \sqrt{E_S}\mathbf{x})] \\
&= P[||\sqrt{E_S}(\mathbf{x} - \hat{\mathbf{x}}) + \mathbf{n}||^2 - ||\mathbf{n}||^2 < 0] \\
&= P[E_S ||\mathbf{x} - \hat{\mathbf{x}}||^2 - 2\sqrt{E_S}(\mathbf{x} - \hat{\mathbf{x}})\mathbf{n}^T < 0]
\end{aligned}
$$

V.a. gaussia a media nulla e varianza: $2N_0E_S ||\mathbf{x} - \hat{\mathbf{x}}||^2$

$$
P[E_{ij}] = Q\left(\sqrt{\frac{E_S ||\mathbf{x} - \hat{\mathbf{x}}||^2}{2N_0}}\right) = Q\left(\sqrt{\frac{E_S d_E^2(\mathbf{x}, \hat{\mathbf{x}})}{2N_0}}\right)
$$

Q(a) distribuzione gaussiana complementare

Probabilita` Errore Condizionata

$$P[\hat{\mathbf{x}} \neq \mathbf{x} \mid \mathbf{x} = \mathbf{x}_i] \leq \sum_j P[E_{ij}]$$

$$\leq \sum_{\hat{\mathbf{x}}_j \neq \mathbf{x}_i} Q\left(\sqrt{\frac{E_S d_E^2(\mathbf{x}_i, \hat{\mathbf{x}}_j)}{2N_0}}\right)$$

$$\leq \sum_{\hat{\mathbf{x}}_j \neq \mathbf{x}_i} Q\left(\sqrt{\frac{E_S d_{E,min}^2}{2N_0}}\right)$$

$$\leq (2^k - 1) Q\left(\sqrt{\frac{E_S d_{E,min}^2}{2N_0}}\right)$$

$$d_{E,min} = \min_{\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{C}} \{|| \mathbf{x}_1 - \mathbf{x}_2 ||\}$$

Minima distanza Euclidea tra parole di codice 2-PAM

Probabilita` Errore

$$P_e = \sum_{\mathbf{x}_i \in \mathbb{C}} P[\mathbf{x} = \mathbf{x}_i] P[\hat{\mathbf{x}} \neq \mathbf{x} \mid \mathbf{x} = \mathbf{x}_i]$$

$$\leq (2^k - 1) \sum_{\mathbf{x}_i \in \mathbb{C}} P[\mathbf{x} = \mathbf{x}_i] Q\left(\sqrt{\frac{E_S d_{E,min}^2}{2N_0}}\right)$$

$$\leq (2^k - 1) Q\left(\sqrt{\frac{E_S d_{E,min}^2}{2N_0}}\right)$$

P_e blocco

$$LQ\left(\sqrt{\frac{E_S d_{E,min}^2}{2N_0}}\right) \leq P_e \leq (2^k - 1) Q\left(\sqrt{\frac{E_S d_{E,min}^2}{2N_0}}\right)$$

$$L = \frac{\text{n. parole a } d_{E,min}}{2^k} \leq 1$$

P_e bit

$$\frac{L}{k} Q\left(\sqrt{\frac{E_S d_{E,min}^2}{2N_0}}\right) \leq P_b \leq (2^k - 1) Q\left(\sqrt{\frac{E_S d_{E,min}^2}{2N_0}}\right)$$

Confronto Sistema Codificato e Non Codificato

$$P_{b,COD} = Q\left(\sqrt{\frac{2E_b Rd_{H.min}}{N_0}}\right) \qquad P_{b,UNCOD} = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

$$d_{E,min} = 2d_{H,min} \qquad E_b = E_S / R = E_S n / k$$

Per mantenere la velocita` di TX uguale bisogna incrementare la banda di 1/R ⇒ $G = Rd_{H,min}$

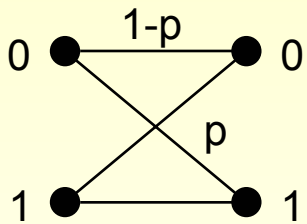
Esempio: Hamming (7,4) ⇒ $G = 3 \times 4 / 7 = 2.34$ dB

Canale Binario Simmetrico

Modello di Canale Binario Simmetrico (BSC)

Decodifica hard: operiamo la demodulazione ottenendo un canale equivalente binario

$$y_i \rightarrow r_i \in \{0,1\}$$



- **Probabilita` di transizione (con trasmissione 2-PAM)** e`

$$p = P_e = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

Decodifica ML in Canale BSC

- In forma vettoriale abbiamo per il canale binario simmetrico senza memoria

$$\mathbf{r} = \mathbf{c} + \mathbf{e}$$

- **Decodifica ML hard**: massimizziamo la probabilita

$$P[\mathbf{r} = \hat{\mathbf{r}} \mid \mathbf{c} = \hat{\mathbf{c}}] = \prod_{i=1}^{n} P[r = \hat{r}_i \mid c = \hat{c}_i]$$

$$= \prod_{i=1}^{n} P[e_i = \hat{r}_i - \hat{c}_i \mid c = \hat{c}_i]$$

$$= p^{w_H(\hat{\mathbf{r}}-\hat{\mathbf{c}})}(1-p)^{n-w_H(\hat{\mathbf{r}}-\hat{\mathbf{c}})}$$

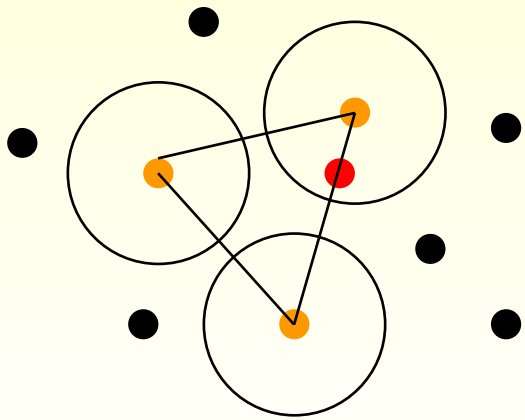
Se p<1/2, decidiamo per il vettore di codice a distanza di Hamming minima

$$\hat{\mathbf{c}} = \arg\min_{\mathbf{c}\in\mathbb{C}}\{d_H(\mathbf{r},\mathbf{c})\}$$

Correzione

- Con decodifica Hard possiamo **correggere** tutti i pattern di errore di peso minore uguale di

$$t = \left\lfloor \frac{1}{2}(d_{H,min} - 1) \right\rfloor$$



  - Puo` accadere che correggiamo errori di peso > t

Rivelazione

- Con decodifica Hard possiamo **rivelare** tutti i pattern di errore di peso minore uguale di

$$d_{H,min} - 1$$

- Con la decodifica a sindrome, un pattern di errore di peso $d_{H,min}$-1 non puo` trasformare la parola originaria in un'altra parola di codice.
- Tuttavia possiamo anche rivelare pattern errore di peso maggiore di $d_{H,min}$-1 poiche`:
  - 2^k di codice e 2^n ricevute
  - 2^n-2^k non sono di codice quindi rivelabili via decodifica a sindrome
  - 2^n -2^n+2^k = 2^k non sono rivelabili
  - Frazione di non rivelabili e` piccola: $(2^k - 1) / (2^n - 1) \sim 2^{k-n}$

Probabilita` di Errore

- Con decodifica Hard possiamo correg. tutti i pattern di errore di peso minore uguale di t

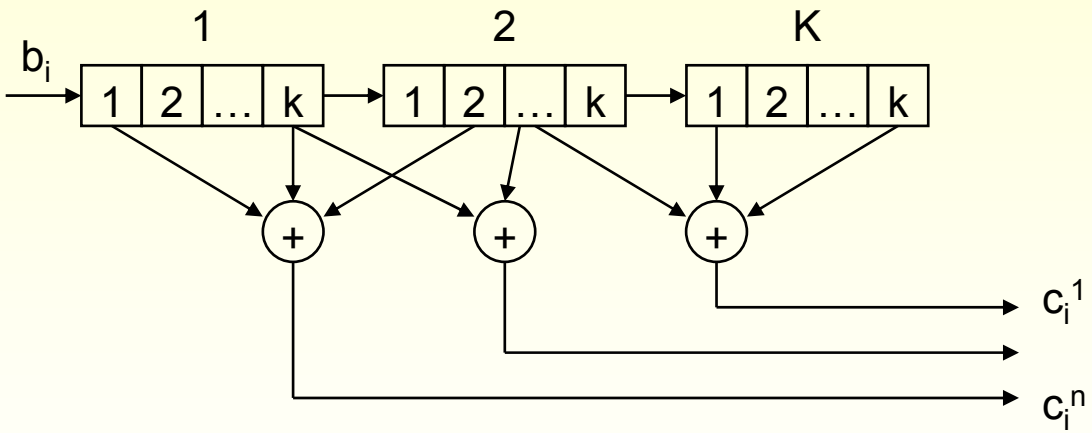
$$P_e(\text{blocco}) \leq P[w(\mathbf{e}) > t] = \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

- Tipicamente la decodifica Hard differisce per 1-2 dB da quella Soft in termine di Eb/No per ottenere la stessa Pe.

Codici Convoluzionali

Codice Convoluzionale

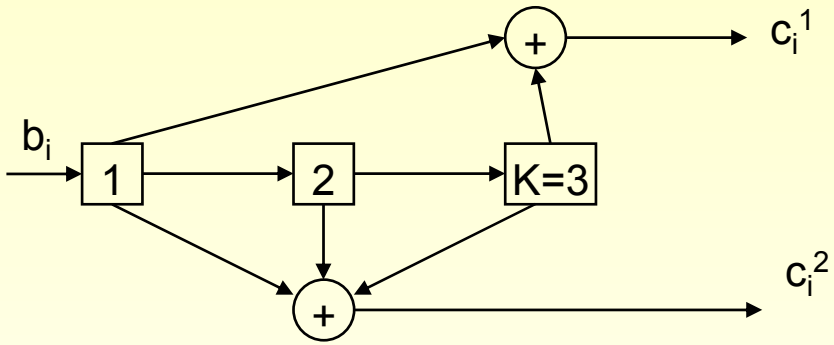
- Un codificatore convoluzionale e` una macchina a stati finiti lineare.
- Codice convoluzionale binario di rate k/n genera ogni k bit d'ingresso n bit di uscita combinando modulo 2 i contenuti di uno shif register di lunghezza kK:



- Gli shift sono k bit d'ingresso alla volta.
- K e` detta constraint length (lunghezza di vincolo).

Codice Convoluzionale Binario 1/n

- Esempio rate ½ e K=3



- Viene descritto da una sequenza generatrice (detta polinomio di codice)

$$\mathbf{g}^{(1)} = [101] \rightarrow [5] \text{ in ottale}$$

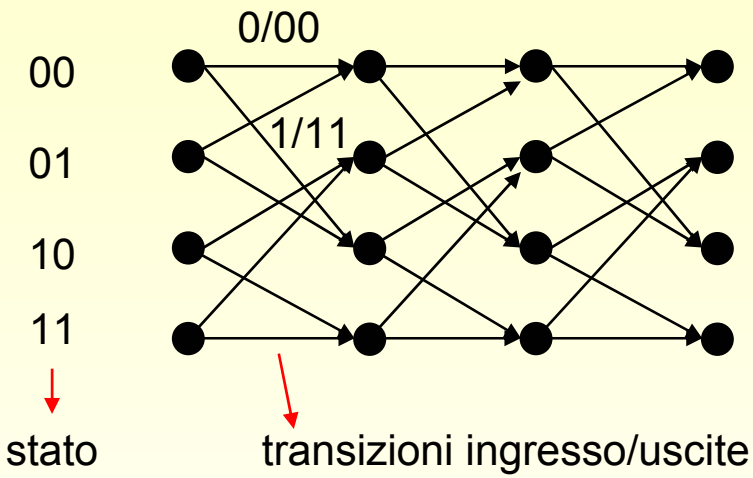
$$\mathbf{g}^{(2)} = [111] \rightarrow [7] \text{ in ottale}$$

- Ciascuna uscita puo` essere ottenuta da un filtraggio modulo 2

$$c_i^{(n)} = b \otimes g^{(n)}(i)$$

Diagramma a Traliccio (Trellis)

- Ingresso-uscita puo` essere rappresentata da un traliccio



- Numero di stati uguale a 2^{K-1}
- Numero di rami entranti/uscenti per stato uguale a 2 (rate 1/n)
- Lungezza del traliccio uguale al numero totale di bit di ingresso
- Se il codice e` terminato si parte dallo stato 0 e si ritorna allo stato 0

Decodifica ML

- Il decodificatore soft a massima verosimiglinza cerca tra tutte le parole di codice quelle a distanza euclidea minima (con rumore AWGN).
- Se consideriamo trasmissione 2-PAM e rumore additivo bianco il modello e`:

$$y_i = \sqrt{E_S}x_i + n_i \qquad \| \mathbf{y} - \sqrt{E_S}\mathbf{x} \|^2 = \sum_i (y_i - \sqrt{E_S}x_i)^2$$

- Se assumiamo un codice di rate 1/n, allora

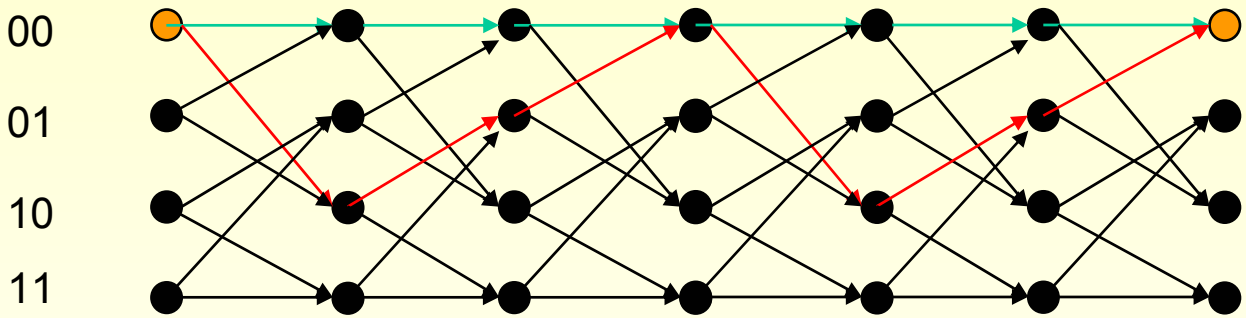
$$\| \mathbf{y} - \sqrt{E_S}\mathbf{x} \|^2 = d_E(\mathbf{y}, \sqrt{E_S}\mathbf{x}) = \sum_i \underbrace{\sum_{m=1}^{n} (y_{ni+m} - \sqrt{E_S}x_{ni+m})^2}_{BM(\mathbf{x}_i)}$$

$$= \sum_i BM(\mathbf{x}_i) = \underbrace{\sum_{j<i} BM(\mathbf{x}_j)}_{PM(i-1)} + BM(\mathbf{x}_i)$$

- La distanza totale e` ottenibile come somma di *Branch metrics*

Algoritmo di Viterbi

- La ricerca esaustiva delle sequenza a distanza minima si ottiene con una operazione ricorsiva di ADD, COMPARE, SELECT sul traliccio



- Ciascun ramo puo` essere etichettato con il bit di ingresso, gli n bit di uscita, e la metrica di ramo (Branch Metric).

- Percorsi entranti in uno stesso stato (nodo) sono competitors e sopravvive solo quello con metrica di percorso (Path Metric) piu` piccola.

- Giunti alla fine del traliccio sompravviveranno un numero di percorsi pari al numero di stati. Scelgo quello di metrica piu` piccola, da cui ottengo la sequenza di bit di ingresso (sequenza decodificata).

Conclusioni

- La codifica di canale e` essenziale per consentire comunicazioni affidabili.
- Il codice deve essere progettato in funzione dell'applicazione e del canale trasmissivo.