

Teoria dell'Informazione e della Trasmissione

Appunti

Scandella Matteo

Pezzoli Matteo

Galizzi Francesco

12 aprile 2016

Indice

Introduzione	1
I. Codifica di sorgente	2
1. Introduzione	3
2. Sorgenti senza memoria	5
2.1. Introduzione all'entropia di sorgente	5
2.2. Codifica per sorgenti senza memoria	8
2.2.1. Disuguaglianza di Kraft	9
2.2.2. Codifica di Shannon	11
2.2.3. Codifica di Huffman	15
3. Sorgenti con memoria	20
3.1. Entropia condizionata	20
3.2. Entropia congiunta	23
3.3. Entropia di sorgenti con memoria	25
3.4. Codifica per sorgenti con memoria	25
3.5. Codifica di Lempel-Ziv	27
II. Codifica di canale	29
4. Capacità di canale	30
4.1. Definizione di canale	30
4.2. Mutua informazione	30
4.3. Canali discreti	32
4.3.1. Canale BSC (Binary Symmetric Channel)	32
4.3.2. Canale BEC (Binary Erasure Channel)	35
4.4. Canali continui	38
4.4.1. Introduzione alle variabili casuali continue	38
4.4.2. Canale AGN (Additive Gaussian Noise) con trasmettitore continuo (analogico)	43
4.4.3. Canale AGN (Additive Gaussian Noise) con trasmettitore discreto (digitale)	44
5. Teorema della codifica di canale	49
5.1. Modalità di invio dei messaggi sul canale	49
5.2. Modalità di ricezione dei messaggi sul canale	49
5.3. Probabilità di sbagliare di un ricevitore ML	50
5.3.1. Formulazione	50
5.3.2. Limite superiore	51
5.3.3. Maggiorazione del valor medio	52
5.3.4. Maggiorazione del valor medio in un canale senza memoria	54
5.4. Analisi della maggiorazione dell'errore medio	55
5.5. Conclusioni sul teorema	59
6. Codici per la trasmissione	61
6.1. Concetti generali	61

6.2. Codifiche lineari	61
6.2.1. Notazione matriciale	62
6.2.2. Notazione polinomiale	63
6.2.3. Codificatore di un codice lineare sistematico	65
6.2.4. Decodificatore di un codice lineare sistematico	66
7. Algebra dei campi finiti di Galois	68
7.1. Definizione di campo finito	68
7.2. Equazioni nei campi finiti	69
7.3. Campi finiti di Galois primi	70
7.4. Campi finiti di Galois estesi	71
7.5. Notazione esponenziale	72
7.6. Proprietà speciali	76
7.7. Trasformata di Fourier discreta	77
8. Codifica per la trasmissione su un canale BSC	84
8.1. Considerazioni generali e distanza di Hamming	84
8.2. Prestazioni di un codice per canali BSC	86
8.3. Codici derivati	88
8.4. Codice a parità semplice (Simple Parity Check)	89
8.5. Codici di Hamming	90
8.6. Codici ciclici	92
8.6.1. Introduzione	92
8.6.2. Codici BCH primitivi	94
8.6.3. Codici BCH non primitivi	96
8.6.4. Codici Reed-Solomon	97
8.7. Decodifica algebrica di codici ciclici	98
8.7.1. Introduzione	98
8.7.2. Polinomio locatore dell'errore e calcolo delle posizioni degli errori	99
8.7.3. Polinomio valutatore dell'errore e calcolo del valore degli errori	101
8.7.4. Algoritmo di Euclide	105
9. Codifica per la trasmissione su un canale BEC	107
9.1. Considerazioni generali	107
9.2. Codici LDPC	110
9.2.1. Introduzione	110
9.2.2. Grafo di Tanner	111
9.2.3. Risolvibilità del decodificatore tramite grafo di Tanner	112
9.3. Codici LDPC irregolari	116
III. Teoria della trasmissione	120
10. Segnali	121
10.1. Forme d'onda	121
10.1.1. Caratteristiche delle forme d'onda	121
10.1.2. Categorie di forme d'onda	121
10.1.3. Forme d'onda notevoli	123
10.1.3.1. Forma d'onda costante	123
10.1.3.2. Forma d'onda a scalino	123
10.1.3.3. Forma d'onda a rettangolo	124
10.1.3.4. Forma d'onda a delta di Dirac	125
10.1.4. Manipolazione di forme d'onda	126

10.2. Trasformata di Fourier	127
10.2.1. Serie di Fourier	127
10.2.2. Trasformata di Fourier	127
10.2.3. Trasformate notevoli	128
10.2.3.1. Trasformata dello scalino	128
10.2.3.2. Trasformata della forma d'onda rettangolare	129
10.2.3.3. Trasformata della delta di Dirac	129
10.2.4. Proprietà della trasformata di Fourier	129
10.2.4.1. Linearità	129
10.2.4.2. Simmetria	130
10.2.4.3. Trasformata e antitrasformata in 0	130
10.2.4.4. Dualità	131
10.2.4.5. Scalatura	131
10.2.4.6. Traslazione	131
10.2.4.7. Traslazione in frequenza	132
10.2.4.8. Convoluzione	132
10.2.4.9. Relazione di Parseval	137
10.2.5. Trasformata di Fourier di un segnale periodico	139
10.3. Notazione geometrica delle forme d'onda	140
10.4. Canali di trasmissione	143
10.4.1. Introduzione	143
10.4.2. Sistemi LTI	144
10.4.3. Risposta in frequenza dei sistemi LTI	148
10.5. Processi casuali	149
10.5.1. Definizione	149
10.5.2. Densità di probabilità	150
10.5.3. Funzione di autocorrelazione	152
10.5.4. Funzione di densità di potenza spettrale	152
10.5.5. Processi casuali bianchi	153
10.5.6. Processi casuali in un sistema LTI	153
10.5.7. Rappresentazione geometrica	155
11. Trasmissione multicanale	158
11.1. Trasmissione di un simbolo tramite un canale passa-basso	158
11.1.1. Introduzione	158
11.1.2. Trasmissione 2-PAM	161
11.1.3. Trasmissione 4-PAM	162
11.1.4. Trasmissione M-PAM	165
11.2. Trasmissione di una sequenza di simboli tramite un canale passa-basso	168
11.2.1. Introduzione	168
11.2.2. Condizione di Nyquist	169
11.3. Trasmissione tramite una canale passa-banda	172
11.3.1. Introduzione	172
11.3.2. Trasmissione M-QAM	175
11.4. Capacità di canale	176

Introduzione

La teoria dell'informazione è una disciplina che si occupa di quantificare i dati che è necessario trasmettere o memorizzare su un certo mezzo. Il padre della disciplina è considerato Claude Shannon, che nel 1948 pubblicò il testo considerato alla base della teoria dell'informazione: «A Mathematical Theory of Communication», che tratta, in sostanza, di come trasferire informazioni.

Questo obiettivo presenta immediatamente due problemi:

- la scelta di quale sia il modo più efficiente per rappresentare le informazioni, sia che queste siano destinate alla trasmissione che alla memorizzazione;
- la scelta di un metodo per trasmettere o memorizzare le informazioni stesse su un supporto potenzialmente poco affidabile, in quanto disturbato (soggetto a errori/rumore).

Questi problemi vengono affrontati con due approcci diversi: il primo con la codifica detta «di sorgente», mentre il secondo attraverso la codifica «di canale».

Marcos.ferrari@polimi.it
Marcos.ferrari@quest.unibg.it

- Teorie dell'informazione codici "Bellini"
- Teorie delle trasmissione "Petti"
"sequenze e modelli per le telecomunicazioni"

Essere:

- Scritto 30m
- Orale 60m

Prerequisiti:

- Analisi
- Calcolo probabilità

Codifica di sorgente

- misura dell'informazione
- modo più economico per memorizzare o trasmettere l'informazione

Codifica di canale

quanta informazione si può trasmettere su un canale non ideale (non affidabile, ossia rumoroso) e in che modo

Parte I.

Codifica di sorgente

1. Introduzione

Definizione intuitiva di sorgente di informazione Una sorgente d'informazione è un'entità che emette una grandezza osservabile (**variabile dipendente**) aleatoria che varia nel tempo o nello spazio (variabile indipendente).

Esempi

- Una persona che parla emette una variazione di pressione dell'aria misurabile tramite i timpani che varia nel tempo e quindi è una sorgente di informazione.
- Un testo scritto sono dei simboli leggibili che variano nello spazio e quindi è una sorgente di informazione.
 - caratteri che provengono da un alfabeto messi in fila secondo un determinato ordine
 - associamo chiaramente un significato a ciascuna sequenza di caratteri
- Un'immagine è costituita da un insieme di colori osservabili che variano nello spazio e quindi è una sorgente.
- Un film sono delle immagini osservabili che variano nel tempo e quindi è una sorgente.

• continue / discrete nel tempo
• continue / discrete nelle ampiezze

• var indipendente
• var dipendente

Tipi di sorgente Le sorgenti si possono dividere in base alla forma **delle due grandezze**, che possono essere continue, ossia appartenere a un intervallo di \mathbb{R} , o discrete, ossia i suoi valori appartengono a un insieme finito o al più numerabile. In base a questo si distinguono 3 tipi di sorgente:

Continue Se entrambe le grandezze sono continue, come ad esempio un segnale audio o una persona che parla.

Discrete Se entrambe le grandezze sono discrete, come ad esempio un testo scritto che dispone di un limitato alfabeto e si legge simbolo per simbolo.

Ibride Sono quelle che hanno una grandezza continua e una discreta; ad esempio un film analogico (quelli su cassetta) è una serie di diapositive che avanzano in modo discreto (variabile indipendente discreta), ma l'immagine visualizzata può assumere qualsiasi scala di colore (variabile indipendente).

al giorno d'oggi tutti i segnali vengono digitalizzati => campionamento + quantizzazione

discrete

Osservazione Tipicamente questo testo verrà a contatto principalmente con il **secondo tipo**, in quanto l'evoluzione ha portato le sorgenti ad essere principalmente discrete. Un altro motivo di questa scelta sta nel fatto che si può dimostrare che si può passare da una sorgente continua a una discreta commettendo un errore piccolo a piacere (come si vedrà in dettaglio più avanti).

nel tempo e
nelle ampiezze

Definizione di sorgente di informazione discreta Una sorgente d'informazione discreta è un'entità che emette una sequenza di variabili casuali X_k di messaggi presi da un alfabeto finito o numerabile $\{x_1, x_2, x_3, \dots, x_M\}$.

• perché non so quale sarà il prossimo carattere
• variabile casuale X con pedice indica il tempo
• x minuscola si indica i valori che la variabile casuale può assumere

$\mathcal{X} = \{x_1, \dots, x_M\}$

la loro posizione nell'alfabeto

alfabeto X ma in corsivo

Osservazioni

- k è un indice temporale discreto e quindi X_k e X_{k+1} sono due messaggi successivi.
- M è il numero di simboli presenti nell'alfabeto.
- Tutte le sorgenti si considerano stazionarie; se non lo fossero sarebbe come se un testo cambiasse lingua a un certo punto.

$$P_{X_k}(x_i) = P_{\text{Prob}}[X_k = x_i]$$

distribuzione di probabilità di X_k o ddp

- qual è la probabilità o la distribuzione di probabilità
- dove a pedice indico la variabile casuale di cui sto descrivendo la distribuzione di probabilità
- argomento x_i rappresenta uno dei valori tratti dall'alfabeto
- Prob quando uso questa funzione indico un evento tra [...], ossia la probabilità che questo evento sia vero.
- L'evento è che il messaggio k -esimo assuma il valore x_i

Esempio di sorgente discreta

Si consideri come sorgente una sequenza di lanci di una moneta: questa genererà una successione di messaggi (lanci) che attingeranno dall'alfabeto $\{T, C\}$. Una possibile sequenza X_k di messaggi potrebbe essere $X_k = \{T, C, T, T, T, C, T, C, C\}$. Questo significa che verrà indicato con $X_1 = x_1 = T$ il primo messaggio, $X_2 = x_2 = C$ il secondo messaggio, $X_3 = x_3 = T$ il terzo messaggio, e così via.

$$\begin{aligned} X &= \{T, C\} \text{ alfabeto} \\ X_k &= \{T, C, T\} \text{ msg} \end{aligned}$$

$x_1 = x_1$
 $x_2 = x_2$
 $x_3 = x_3$

Caratterizzazione di una sorgente discreta Per descrivere una sorgente è quindi necessario conoscere:

- l'alfabeto dei possibili messaggi $\{x_1, x_2, x_3, \dots, x_M\}$;
- la distribuzione di probabilità dei messaggi:
 - nel caso i messaggi siano indipendenti, basta solo la probabilità che X_k assuma il valore x_i , rappresentata come $P_{X_k}(x_i)$. Questa funzione di probabilità è necessaria $\forall i$ con $0 < i \leq M$;
 - nel caso i messaggi non siano indipendenti, è necessaria anche la distribuzione di probabilità congiunta, ovvero la probabilità che X_k assuma il valore x_i e X_{k+1} assuma il valore x_j , rappresentata come $P_{X_k, X_{k+1}}(x_i, x_j)$. In generale, in base a quanto le variabili sono correlate è necessario fornire

$$P_{X_k, X_{k+1}, \dots}(x_i, x_j, \dots)$$

per poter rappresentare appieno la distribuzione.

Osservazioni

assumeremo sempre che le sorgenti siano stazionarie cioè che le sue caratteristiche statistiche non cambiano nel tempo

- Per l'ipotesi di stazionarietà le distribuzioni P non dipendono dall'indice temporale e quindi

$$P_{X_k}(x_i) = P_{X_{k+1}}(x_i) = P_{X_{k+2}}(x_i) = \dots = P_X(x_i)$$

• fissato il carattere dell'alfabeto
 • indipendentemente dal messaggio

mentre per le distribuzioni congiunte conta solo la distanza tra i due indici temporali e quindi

$$P_{X_k, X_{k+\tau}}(x_i, x_j) = P_{X_{k+1}, X_{k+1+\tau}}(x_i, x_j) = P_{X_{k+2}, X_{k+2+\tau}}(x_i, x_j) = \dots = P_{X, \tau}(x_i, x_j)$$

fissati i caratteri dell'alfabeto
 fissata la var casuale =
 fissato il messaggio X

- Dato che $P_X(x_i)$ è una probabilità deve valere che $\sum_{i=1}^N P_X(x_i) = 1$ e che $P_X(x_i) \geq 0 \forall i$ tale che $1 \leq i \leq M$
- Nel caso in cui gli X_k siano indipendenti non è necessario fornire la distribuzione di probabilità congiunta in quanto la si può ricavare facilmente da quella marginale:

$$P_{X, \tau}(x_i, x_j) = P_X(x_i) \cdot P_X(x_j) \quad \text{fissata la sorgente}$$

$\forall \tau \in \mathbb{N}$

Ciò non vale se le variabili sono correlate.

- Le sorgenti con variabili casuali correlate sono dette con memoria mentre le altre sono dette senza memoria (nel senso che al tempo k «si dimenticano» di quello che è successo al tempo $k - 1$).

Una sorgente stazionaria senza memoria è univocamente specificata da:

- \mathcal{X} alfabeto
- $P_{X_k}(x_i)$

distribuzione congiunta di X_1 e X_2 : la probabilità che si verifichi il doppio evento simultaneo le due variabili indipendenti è il prodotto delle due

$$P_{X_1, X_2}(x'_1, x''_2) = \text{Prob}(x_1 = x'_1 \cap x_2 = x''_2)$$

probabilità condizionata: mi metto solo nel sottospazio degli eventi in cui X_2 in cui si verifica X_1

$$P_{X_2|X_1}(x''_2|x'_1) \triangleq \frac{P_{X_1, X_2}(x'_1, x''_2)}{P_{X_1}(x'_1)}$$

se invece a memoria dovremmo assegnare le distribuzioni congiunte o condizionate

Se indipendenti:
 $P_{X_1, X_2}(x'_1, x''_2) = P_{X_1}(x'_1) \cdot P_{X_2}(x''_2)$
 $P_{X_2|X_1}(x''_2|x'_1) = P_{X_2}(x''_2)$

- se i messaggi X_1, X_2, \dots, X_k sono indipendenti tra loro
- Indipendenti vuol dire che il fatto che il k -esimo messaggio assume un certo valore non cambia la distribuzione di probabilità dei successivi
- con memoria invece il valore assunto di un messaggio cambia la ddp degli altri

2. Sorgenti senza memoria

2.1. Introduzione all'entropia di sorgente

Sia S una sorgente senza memoria con sequenza di messaggi $X_k \in \{x_1, x_2, x_3, \dots, x_M\}$ e distribuzione di probabilità $P_X(x_i)$. È utile determinare in modo quantitativo quanta informazione può erogare questa sorgente, ma per farlo è necessario definire il concetto di informazione. Shannon, per definire l'informazione di un messaggio, assume che:

$$\uparrow I(x_i)$$

siamo in condizioni stazionarie: stessa probabilità per ogni variabile casuale

$$\rho_{x_k}(x_i)$$

$$\rho_{x_k}(x_m) = P(x_i)$$

in condizioni stazionarie: l'informazione definita da x_i è uguale per tutti i msm

- L'informazione legata a un messaggio che assuma il valore x_i , definita come $I(x_i)$, è tanto più grande quanto $P_X(x_i)$ è piccola. Ciò significa che più un messaggio è raro, più informazione contiene e conseguentemente vale anche il contrario;
- l'informazione di due messaggi indipendenti è la somma delle singole informazioni.

Definizione di informazione secondo Shannon Si definisce l'informazione contenuta in un messaggio x_i come

$$I(x_i) \stackrel{\text{DEF}}{=} \log \left(\frac{1}{P_X(x_i)} \right)$$

Osservazioni

- Questa formulazione rispetta le due assunzioni di Shannon.

$$\circ \text{ rarità del messaggio} \downarrow \Rightarrow P_X(x_i) \uparrow \Rightarrow \frac{1}{P_X(x_i)} \downarrow \Rightarrow \log \left(\frac{1}{P_X(x_i)} \right) \downarrow$$

$$\circ \text{ L'informazione legata a due messaggi } x_i \text{ e } x_j, \text{ secondo questa definizione, è } I(x_i, x_j) = \log \left(\frac{1}{P_{X,\tau}(x_i, x_j)} \right); \\ \text{ quando i due messaggi sono scorrelati vale quindi:}$$

$$\begin{aligned} I(x_i, x_j) &= \log \left(\frac{1}{P_{X,\tau}(x_i, x_j)} \right) = \\ &= \log \left(\frac{1}{P_X(x_i) \cdot P_X(x_j)} \right) = \\ &= \log \left(\frac{1}{P_X(x_i)} \right) + \log \left(\frac{1}{P_X(x_j)} \right) = \\ &= I(x_i) + I(x_j) \end{aligned}$$

- Partendo dalle due assunzioni di Shannon si possono trovare diverse formulazioni di informazione che le rispettano, ma si è scelto di usare questa che porta dei vantaggi nei teoremi successivi.
- Anche questa formulazione ha una parte indefinita che può essere scelta a piacere senza andare contro le due assunzioni; questo parametro è la base del logaritmo. Solitamente vengono utilizzate due notazioni:

Il simbolo $\stackrel{\text{DEF}}{=}$ significa «uguale per definizione».

2. Sorgenti senza memoria

- Se la base è e l'informazione viene misurata in [nat].
- Se la base è 2 l'informazione viene misurata in [bit]. Questa è la notazione più usata ed è anche quella che verrà utilizzata all'interno di questo testo. Da questo momento in poi verrà assunta come convenzione $\log X = \log_2 X$.

Definizione di entropia della sorgente Si definisce entropia della sorgente la quantità di informazione emessa dalla sorgente

$$H(X) = \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} = \mathbb{E}_X \left[\log \frac{1}{P_X(x_i)} \right] = \mathbb{E}[I(x_i)]$$

L'informazione media per messaggio emessa da X sarà
valore atteso

ovvero il valore medio dell'informazione dei messaggi pesato sulla base delle probabilità.

Osservazione È noto che $P_X(x_i) \leq 1$ in quanto esse sono probabilità: da questo si ha che $\log \frac{1}{P_X(x_i)} \geq 0$ e quindi $H(X) \geq 0$.

Oss: se $P_X(x_i) = 0$ segnando $\lim_{x \rightarrow 0} \log x = -\infty$
osserviamo che non dà contributo ad $H(X)$.

Esempi

- Si consideri come sorgente il lancio di una moneta e quindi:

<ul style="list-style-type: none"> $M = 2$ e l'alfabeto è $\{T, C\}$ $P_X(T) = P_X(C) = \frac{1}{2}$ 	<p>Sorgente: $X = \{T, C\}$ $P_X(x) = \{\frac{1}{2}, \frac{1}{2}\}$</p>
---	---

Si può ricavare che:

- $I(T) = I(C) = \log \frac{1}{\frac{1}{2}} = 1$ bit
- $H(X) = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = 1$ bit

Intuitivamente questo risultato sembra appropriato: per memorizzare il lancio di una moneta basta un singolo bit.

- Si consideri come sorgente l'estrazione, con re-immissione, di una carta da un mazzo, dove l'informazione considerata è il seme della carta e quindi:

<ul style="list-style-type: none"> $M = 4$ e l'alfabeto è $\{O, C, S, B\}$ $P_X(O) = P_X(C) = P_X(S) = P_X(B) = \frac{1}{4}$ 	<p>Sorgente: $X = \{O, C, S, B\}$ // 4 msg possibili $P_X(x) = \{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\}$</p>
---	--

Si può ricavare che:

- $I(O) = I(C) = I(S) = I(B) = \log \frac{1}{\frac{1}{4}} = 2$ bit
- $H(X) = \sum_{i=1}^4 P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} = \sum_{i=1}^4 \frac{1}{4} \cdot \log \frac{1}{\frac{1}{4}} = 2$ bit

Anche in questo esempio, la soluzione è intuitiva, in quanto servirebbero effettivamente 2 bit per salvare un messaggio contenente uno dei quattro semi.

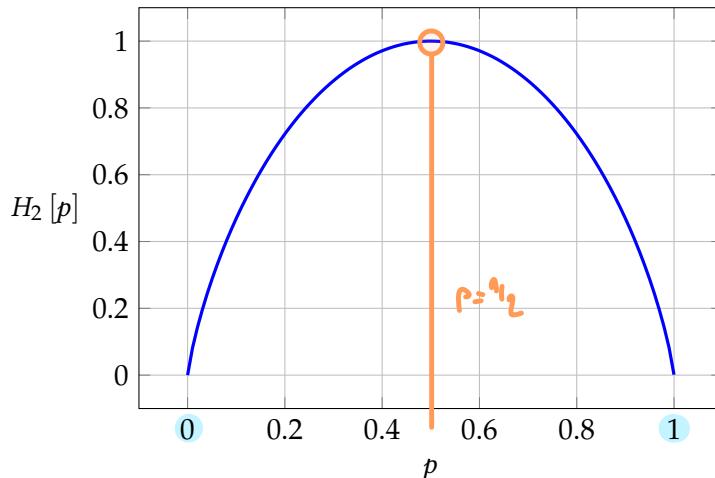
- Si consideri come sorgente il lancio di una moneta truccata in cui la probabilità di ottenere testa è diversa da quella di ottenere croce e quindi:

<ul style="list-style-type: none"> $M = 2$ e l'alfabeto è $\{T, C\}$ $P_X(T) = p$ e $P_X(C) = 1 - p$, dove $p \in [0, 1]$ 	<p>$X = \{T, C\}$ $P_X(x) = \{p, 1-p\}$</p>
--	--

2. Sorgenti senza memoria

Si può ricavare che:

- $I(T) = \log \frac{1}{p}$ bit e $I(C) = \log \frac{1}{1-p}$ bit; da notare che il numero di bit non è necessariamente un numero naturale.
- $H(X) = p \cdot \log \frac{1}{p} + (1-p) \cdot \log \frac{1}{(1-p)} \triangleq H_2[p]$, il cui grafico è rappresentato in figura 2.1.



[$0 < p < 1$]

- messaggi sono deterministici \Rightarrow conosco quale sarà il contenuto del mio messaggio X_k , dunque non mi porta lacuna infomazione
- entropia massima quando ho più incertezza ossia per $p=1/2$
- rarità non è incertezza, incertezza massima vuol dire che io quando trasmetto non so quale messaggio io stiamo trasmettendo

Figura 2.1.: Funzione $H_2[p]$. entropia di una variabile binaria (2) di parametro P

Dal grafico si può notare che:

- la funzione ha un massimo per $p = \frac{1}{2}$, ossia quando i due messaggi sono equiprobabili, dove vale $H(X) = 1$ (come dimostrato in un precedente esempio);
- la funzione è pari rispetto a $\frac{1}{2}$ (invertire T e C nella moneta non varia l'informazione contenuta nella sorgente);
- la funzione ha minimo per $p = 0$ e $p = 1$ dove vale $H(X) = 0$. Questo si ha perché se è certo che capiti T (per $p = 1$) o C (per $p = 0$) allora non c'è nessuna informazione da archiviare dato che l'esito lo si conosce a priori;
- per valori intermedi la funzione ha valori nell'intervallo $[0, 1]$.
- Ha derivata pari a:

derivo + punto critico/stazionario (derivata = 0)
• massimo se $f''(x) > 0$
• minimo se $f''(x) < 0$

$$\frac{d}{dp} H_2[p] = \log \frac{1-p}{p}$$

$$H(x) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$$

caso
buone
= $\frac{1}{\ln 2} [-p \ln p - (1-p) \ln (1-p)]$

$$\frac{dH(x)}{dp} = -\frac{1}{\ln 2} [\ln p + 1 - \ln(1-p) - 1] = \ln \frac{1-p}{p}$$

Ora: La $H(x)$ è massima quando la ddp è uniforme ed il risultato è generale.

Teorema Sia X una sorgente con un alfabeto di M simboli, allora $H(X) \leq \log M$.

Sia X di alfabeto $X = \{x_1, \dots, x_M\}$
senza memoria con ddp $P_X(x_i)$

Dimostrazione Dalla definizione di entropia:

$$H(X) = \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{P_X(x_i)}$$

Dimostrazione
alternativa:

$$\begin{aligned} H(X) - \log M &= \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} - \sum_{i=1}^M P_X(x_i) \log M \\ &= \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{P_X(x_i) \cdot M} \leq \frac{1}{\ln 2} \left[\sum_{i=1}^M P_X(x_i) \left(\frac{1}{P_X(x_i) \cdot M} - 1 \right) \right] \\ &= \frac{1}{\ln 2} \left(\sum_{i=1}^M \frac{1}{M} - \sum_{i=1}^M P_X(x_i) \right) \\ &= \frac{1}{\ln 2} (1 - 1) = 0 \end{aligned}$$

dove:

$$\sum_{i=1}^M P_X(x_i) = 1$$

Note bene:
• casuale cioè
• $\odot \Rightarrow \text{ogni } x \in X - 1$

2. Sorgenti senza memoria

Moltiplicando numeratore e denominatore dell'argomento del logaritmo per M non cambia nulla

$$\begin{aligned}
 H(X) &= \sum_{i=1}^M P_X(x_i) \cdot \log \frac{M}{M \cdot P_X(x_i)} = \\
 &= \sum_{i=1}^M P_X(x_i) \cdot \log M + \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{M \cdot P_X(x_i)} = \\
 &= \log M \cdot \underbrace{\sum_{i=1}^M P_X(x_i)}_1 + \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{M \cdot P_X(x_i)}
 \end{aligned}$$

$\frac{\log_2(x)}{\log_2(e)} = \log(x)$

considerando ora che $\log(x) \leq (x - 1) \cdot \log e$:

$$\begin{aligned}
 H(X) &= \log M + \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{M \cdot P_X(x_i)} \leq \\
 &\leq \log M + \sum_{i=1}^M P_X(x_i) \cdot \log e \cdot \left(\frac{1}{M \cdot P_X(x_i)} - 1 \right) = \\
 &= \log M + \log e \cdot \left(\underbrace{\sum_{i=1}^M P_X(x_i) \cdot \frac{1}{M \cdot P_X(x_i)}}_1 - \underbrace{\sum_{i=1}^M P_X(x_i)}_1 \right) = \\
 &= \log M
 \end{aligned}$$

quindi si ha che

$$H(X) \leq \log M$$

Osservazioni

- Questo fatto pone un limite massimo al valore che l'entropia può assumere. Considerandolo insieme al limite minimo si ottiene un range limitato di valori:

$$0 \leq H(X) \leq \log M$$

- Si può notare che la diseguaglianza diventa uguaglianza quando, riprendendo dalla dimostrazione:

$$\sum_{i=1}^M P_X(x_i) \cdot \log \left(\frac{1}{M \cdot P_X(x_i)} \right) = 0$$

$\log(x) = 0$
 $x = 1$

vuol dire che la probabilità deve essere $1/M$ indipendentemente da i

e quindi quando il valore del logaritmo vale 0 in modo che la sommatoria diventi una somma di 0 e quindi:

$$\frac{1}{M \cdot P_X(x_i)} = 1 \Rightarrow \sum_{i=1}^M P_X(x_i) \cdot \boxed{\log \frac{1}{M \cdot P_X(x_i)}} = 0$$

$\forall i$ tale che $1 \leq i \leq M$

Questo avviene quando $P_X(x_i) = \frac{1}{M}$, $\forall i$ tale che $1 \leq i \leq M$, ovvero quando i messaggi sono tutti equiprobabili.

2.2. Codifica per sorgenti senza memoria

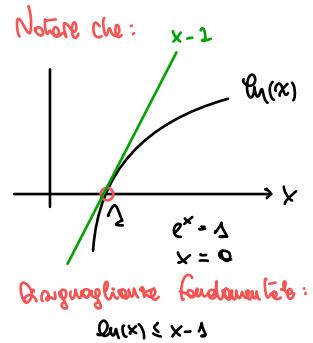
Definizione di codice Si definisce codice una M -upla di sequenze di bit dove $C(x_i)$ è la sequenza associata al messaggio x_i , lunga n_i bit^{II}. La lunghezza di $C(x_i)$ si indica $n(x_i)$.

^{II}Possono esistere anche codifiche a più di 2 simboli, ma per ora si considerano solo quelle a 2 simboli. ossia le binarie

$x = \{x_1, \dots, x_M\}$ m caratteri alfabeto
 $C = (C(x_1), \dots, C(x_M))$ m-upla di sequenze di bit.

data una sequenza di msm consecutivi x , ossia sto inviando in successione sms x^1, x^2, \dots

Ora: $C(x^1, x^2, x^3, \dots) = C(x^1), C(x^2), \dots$
 Notazione $= C(x)$



2. Sorgenti senza memoria

Definizione di codice univocamente decodificabile Un codice si dice univocamente decodificabile (o lossless) se dalla sequenza dei codici è possibile ricreare la sequenza dei messaggi. $\Rightarrow C(x') \neq C(x'')$ **non** $x' \neq x''$

date due sequenze di simboli in successione x' e x'' diversi tra loro quindi in almeno un singolo msm, la sequenza di bit associata è diversa

Osservazione Per quanto questa proprietà sembri imprescindibile esiste un'intera branca della teoria dell'informazione dedicata a creare codici in cui si può perdere un po' di informazione in modo da diminuire la lunghezza delle sequenze.

Definizione di codice istantaneamente decodificabile Un codice si dice istantaneamente (o immediatamente) decodificabile se nessuna sequenza $C(x_i)$ inizia con un'altra sequenza $C(x_j)$.

nessuna sequenza coincide con l'inizio di un'altra sequenza

Osservazione Se un codice è istantaneamente decodificabile allora il codice $C(x_i)$ non può iniziare con nessuna sequenza associata agli altri messaggi e quindi non può essere uguale; quindi questo codice è anche univocamente decodificabile, cioè:

voglio usare delle sequenze molto lunghe è facile fare un codice univocamente decodificabile però il costo è più alto

instantanea decodificabilità \Rightarrow univoca decodificabilità

codici istantaneamente decodificabili
Codici univocamente decodificabili

2.2.1. Disuguaglianza di Kraft

Condizione sufficiente della disuguaglianza di Kraft Siano $n(x_1), n(x_2), n(x_3), \dots, n(x_M)$ le lunghezze delle sequenze di bit di un codice, allora si ha che

noi abbiamo base due nella disuguaglianza di Kraft perché si tratta di codici binari

$$\sum_{i=1}^M 2^{-n(x_i)} \leq 1 \Rightarrow \exists \text{ un codice istantaneamente decodificabile}$$

rappresenta la frazione dello spazio totale occupata da una sequenza di lunghezza $n(x_i)$

La disuguaglianza garantisce che la totalità delle sequenze codificate non eccede lo spazio totale disponibile ossia l'insieme di tutte le possibili sequenze binarie assicurando che ogni codice possa essere assegnato in modo univoco

dove $\sum_{i=1}^M 2^{-n(x_i)} \leq 1$ viene chiamata disuguaglianza di Kraft e fornisce una condizione sufficiente per l'esistenza di un codice istantaneamente decodificabile.

Dimostrazione Si supponga di voler creare un codice istantaneamente decodificabile per una sorgente X con un alfabeto di M elementi in modo che:

$$n(x_1) \leq n(x_2) \leq n(x_3) \leq \dots \leq n(x_M)$$

$$L^N = \sum^{N \text{ (combinazioni)}}$$

Per farlo si può procedere con il seguente metodo iterativo:

- Si scelga arbitrariamente il codice di $C(x_1)$ con una lunghezza $n(x_1)$
- Per mantenere il codice istantaneamente decodificabile è necessario scegliere $C(x_2)$ in modo che non inizi con i valori assunti da $C(x_1)$. Per questo motivo non tutti i codici sono leciti, in particolare la quantità dei codici esclusi si può ricavare facilmente: sono infatti tutti i codici lunghi $n(x_2)$ tali che abbiano i primi $n(x_1)$ bit uguali da $C(x_1)$, e quindi sono $2^{n(x_2)-n(x_1)}$. Quindi si sceglie $C(x_2)$ arbitrariamente tra i codici non esclusi.
Se $n(x_2) = n(x_1)$ allora si esclude solo una combinazione, quella abbinata al codice $C(x_1)$.
- Per mantenere il codice istantaneamente decodificabile è necessario che $C(x_3)$ non inizi con i valori assunti da $C(x_1)$ e da $C(x_2)$. La quantità dei codici esclusi è facilmente calcolabile come la somma di quelli che vengono esclusi da $C(x_1)$ e quelli di $C(x_2)$ e quindi $2^{n(x_3)-n(x_1)} + 2^{n(x_3)-n(x_2)}$. Quindi si sceglie $C(x_3)$ arbitrariamente tra i codici non esclusi.
- Si procede in questo modo fino al codice di $C(x_M)$ che avrà una quantità di sequenze escluse di

$$2^{n(x_M)-n(x_1)} + 2^{n(x_M)-n(x_2)} + 2^{n(x_M)-n(x_3)} + \dots + 2^{n(x_M)-n(x_{M-1})}$$

2^M combinazioni:

0 0 0	0 0 1
0 1 0	0 1 1
1 0 0	1 0 1
1 1 0	1 1 1

3 bit

il codice $C(x_i) \Rightarrow n(x_i) = 3$

$$2^3 - 2^1 = 2^2 = 4$$

Supponendo che $n(x_1) = 3$ allora altre tre combinazioni di quattro:

2. Sorgenti senza memoria

Per fare in modo che il codice esista questo numero deve essere minore del numero di combinazioni possibili con $n(x_M)$ bit e quindi:

$$\begin{aligned}
 2^{n(x_M)-n(x_1)} + 2^{n(x_M)-n(x_2)} + 2^{n(x_M)-n(x_3)} + \dots + 2^{n(x_M)-n(x_{M-1})} &\leq 2^{n(x_M)} - 1 \\
 2^{n(x_M)} \cdot (2^{-n(x_1)} + 2^{-n(x_2)} + 2^{-n(x_3)} + \dots + 2^{-n(x_{M-1})}) &\leq 2^{n(x_M)} - 1 \\
 2^{-n(x_1)} + 2^{-n(x_2)} + 2^{-n(x_3)} + \dots + 2^{-n(x_{M-1})} &\leq \frac{2^{n(x_M)} - 1}{2^{n(x_M)}} \\
 2^{-n(x_1)} + 2^{-n(x_2)} + 2^{-n(x_3)} + \dots + 2^{-n(x_{M-1})} &\leq 1 - 2^{-n(x_M)} \\
 2^{-n(x_1)} + 2^{-n(x_2)} + 2^{-n(x_3)} + \dots + 2^{-n(x_{M-1})} + 2^{-n(x_M)} &\leq 1 \\
 \sum_{i=1}^M 2^{-n(x_i)} &\leq 1
 \end{aligned}$$

ho trovato un limite superiore alle lunghezze di cui devo disporre per costruire un codice istantaneamente decodificabile che so che è anche univocamente decodificabile

Quindi se le lunghezze assegnate inizialmente rispettano la disegualanza di Kraft è possibile trovare un codice istantaneamente decodificabile sfruttando questa procedura iterativa.

Condizione necessaria della disegualanza di Kraft Sia C un codice con lunghezze $n(x_1), n(x_2), n(x_3), \dots, n(x_M)$ univocamente decodificabile: vale allora la disegualanza di Kraft.

Dimostrazione Sia $(C(x_{i_1}), C(x_{i_2}), \dots, C(x_{i_N}))$ una $N - upla$ di sequenze, in cui:

- Le singole sequenze hanno lunghezza $n(x_{i_1}), n(x_{i_2}), \dots, n(x_{i_N})$.
- La $N - upla$ ha una lunghezza totale pari a $n_{seq} = n(x_{i_1}) + n(x_{i_2}) + \dots + n(x_{i_N})$.

Si consideri la somma del valore $2^{-n_{seq}}$ di tutte le possibili tuple lunghe N ossia:

$$\sum_{i_1=1}^M \sum_{i_2=1}^M \dots \sum_{i_N=1}^M 2^{-n_{seq}}$$

Tramite qualche passaggio matematico si ottiene:

$$\begin{aligned}
 \sum_{i_1=1}^M \sum_{i_2=1}^M \dots \sum_{i_N=1}^M 2^{-n_{seq}} &= \sum_{i_1=1}^M \sum_{i_2=1}^M \dots \sum_{i_N=1}^M 2^{-(n(x_{i_1})+n(x_{i_2})+\dots+n(x_{i_N}))} = \\
 &= \sum_{i_1=1}^M \sum_{i_2=1}^M \dots \sum_{i_N=1}^M 2^{-n(x_{i_1})} \cdot 2^{-n(x_{i_2})} \dots \cdot 2^{-n(x_{i_N})} = \\
 &= \left(\sum_{i_1=1}^M 2^{-n(x_{i_1})} \right) \cdot \left(\sum_{i_2=1}^M 2^{-n(x_{i_2})} \right) \dots \cdot \left(\sum_{i_N=1}^M 2^{-n(x_{i_N})} \right)
 \end{aligned}$$

Dato che le sommatorie non sono più annidate si può usare l'indice i (senza pedice) per tutte le sommatorie e quindi:

$$\begin{aligned}
 \sum_{i_1=1}^M \sum_{i_2=1}^M \dots \sum_{i_N=1}^M 2^{-n_{seq}} &= \left(\sum_{i_1=1}^M 2^{-n(x_{i_1})} \right) \cdot \left(\sum_{i_2=1}^M 2^{-n(x_{i_2})} \right) \dots \cdot \left(\sum_{i_N=1}^M 2^{-n(x_{i_N})} \right) = \\
 &= \left(\sum_{i=1}^M 2^{-n(x_i)} \right)^N
 \end{aligned}$$

Siano:

- A_n il numero delle possibili sequenze di messaggi per cui $n_{seq} = n$.

2. Sorgenti senza memoria

- $n_{max} = \max_{i=1, \dots, M} n(x_i)$, ossia la lunghezza della sequenza più lunga.

Allora si ha che:

$$\sum_{i_1=1}^M \sum_{i_2=1}^M \cdots \sum_{i_N=1}^M 2^{-n_{seq}} = \sum_{n=1}^{N \cdot n_{max}} A_n \cdot 2^{-n}$$

Ossia per ogni possibile lunghezza totale della $N - upla$ ($N \cdot n_{max}$) è il la lunghezza della totale della $N - upla$ massima possibile, ottenibile ponendo ogni elemento della tupla stessa uguale alla sequenza più lunga) si conta il valore $2^{-n} A_n$ volte, dato che per quella lunghezza n ci saranno A_n possibili messaggi.

Dato che il codice C è univocamente decodificabile si ha che $A_n \leq 2^n$ perché se così non fosse ci sarebbe una sequenza di bit lunga n che può essere interpretata in più di una sequenza di messaggi. In altre parole se si hanno a disposizione n bit allora ci sono solo 2^n possibili codici e quindi ci devono essere massimo 2^n sequenze da decodificare se si vuole mantenere l'univoca decodificabilità e quindi $A_n \leq 2^n$. Si ha che:

$$\begin{aligned} \sum_{n=1}^{N \cdot n_{max}} A_n \cdot 2^{-n} &\stackrel{\text{C univocamente decodificabile}}{\leq} \sum_{n=1}^{N \cdot n_{max}} 2^n \cdot 2^{-n} = \\ &= \sum_{n=1}^{N \cdot n_{max}} 1 = \\ &= N \cdot n_{max} \end{aligned}$$

e quindi:

$$\begin{aligned} \left(\sum_{i=1}^M 2^{-n(x_i)} \right)^N &\leq N \cdot n_{max} \\ \sum_{i=1}^M 2^{-n(x_i)} &\leq (N \cdot n_{max})^{\frac{1}{N}} = e^{\frac{1}{N} \log(N \cdot n_{max})} \rightarrow \downarrow \end{aligned}$$

Questa espressione vale $\forall N \geq 1$ e:

- Essendo una radice è $\geq 1 \forall N \in \mathbb{N}$
- $\lim_{N \rightarrow \infty} (N \cdot n_{max})^{\frac{1}{N}} = \lim_{N \rightarrow \infty} 2^{\frac{1}{N} \cdot \log(N \cdot n_{max})} = 2^0 = 1$

quindi assume valori decrescenti con limite inferiore uguale a 1 e quindi si ha che:

$$\sum_{i=1}^M 2^{-n(x_i)} \leq 1$$

che è quello che si voleva dimostrare.

Osservazione Sia C un codice univocamente decodificabile, per la dimostrazione appena fatta, vale la disuguaglianza di Kraft e dato che se vale la disuguaglianza di Kraft si può dimostrare che esiste un codice istantaneamente decodificabile si ha che se esiste un codice univocamente decodificabile esiste anche un codice istantaneamente decodificabile con le stesse lunghezze dei messaggi. Per questo motivo è inutile cercare un codice solo univocamente decodificabile dato che si può trovare un codice istantaneamente decodificabile che occupi lo stesso spazio.

2.2.2. Codifica di Shannon

Primo teorema di Shannon sulla codifica di sorgente Sia C un codice univocamente decodificabile di lunghezze $n(x_1), n(x_2), n(x_3), \dots, n(x_M)$ per la sorgente X , allora si ha che

$$\sum_{i=1}^M P_X(x_i) \cdot n(x_i) = \bar{n}_C \geq H(X) \quad [\text{bit}]$$

• costo medio del codice
 lunghezza media della mia codifica

↓
 ddp della sorgente
 da decodificare

2. Sorgenti senza memoria

Dimostrazione È necessario mostrare che $H(X) - \bar{n}_C \leq 0$. Sviluppando la differenza si ottiene

$$\begin{aligned}
 H(X) - \bar{n}_C &= \sum_{i=1}^M \left(P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} \right) - \sum_{i=1}^M (P_X(x_i) \cdot n(x_i)) \\
 &= \sum_{i=1}^M \left(P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} - P_X(x_i) \cdot n(x_i) \right) = \\
 &= \sum_{i=1}^M \left(P_X(x_i) \cdot \left(\log \frac{1}{P_X(x_i)} - n(x_i) \right) \right) = \\
 &= \sum_{i=1}^M \left(P_X(x_i) \cdot \left(\log \frac{1}{P_X(x_i)} - \log 2^{n(x_i)} \right) \right) = \\
 &= \sum_{i=1}^M \left(P_X(x_i) \cdot \left(\log \frac{2^{-n(x_i)}}{P_X(x_i)} \right) \right)
 \end{aligned}$$

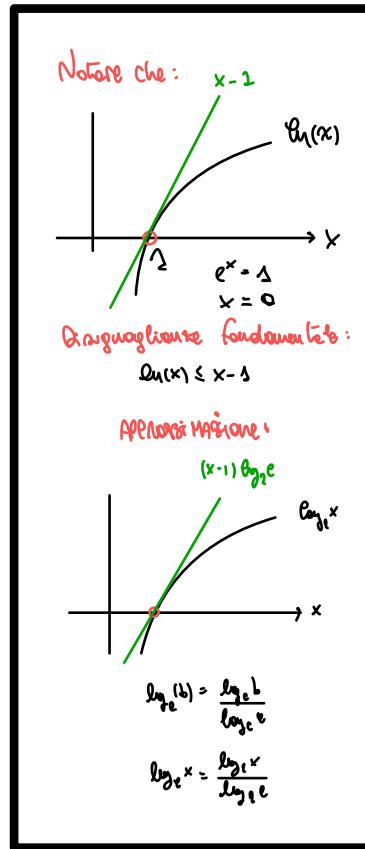
Sfruttando ancora la relazione $\log(x) \leq (x-1) \cdot \log e$:

Dimostrazione II°)

$$\begin{aligned}
 H(X) - \bar{n}_C &= \sum_{i=1}^n P_X(x_i) \log \frac{1}{P_X(x_i)} - \sum_{i=1}^n P_X(x_i) \cdot n_i \\
 &= \sum_{i=1}^n P_X(x_i) \log \frac{2^{-n_i}}{P_X(x_i)} \quad \text{log}(1) \Rightarrow \\
 &\stackrel{\text{Per } x \leq x-1}{=} \sum_{i=1}^n P_X(x_i) \left[\frac{2^{-n_i}}{P_X(x_i)} - 1 \right] \leq 0
 \end{aligned}$$

Oss: se $P_X(x_i) = 2^{-n_i}$ $\forall i \Rightarrow H(X) = \bar{n}_C$ e fatto
di conseguenza $n_i = \log \frac{1}{P_X(x_i)}$

$$\begin{aligned}
 H(X) - \bar{n}_C &\stackrel{x \leq x-1}{\leq} \sum_{i=1}^M \left(P_X(x_i) \cdot \log e \cdot \left(\frac{2^{-n(x_i)}}{P_X(x_i)} - 1 \right) \right) = \\
 &= \log e \cdot \left(\sum_{i=1}^M 2^{-n(x_i)} - \underbrace{\sum_{i=1}^M P_X(x_i)}_1 \right) = \\
 &= \log e \cdot \left(\sum_{i=1}^M 2^{-n(x_i)} - 1 \right)
 \end{aligned}$$



Dato che il codice è univocamente decodificabile vale la diseguaglianza di Kraft e quindi $\sum_{i=1}^M 2^{-n(x_i)} \leq 1$ e quindi si ha che:

$$H(X) - \bar{n}_C \leq \log e \cdot (1 - 1) = 0$$

e quindi:

$$H(X) \leq \bar{n}_C$$

Osservazioni

$$H(X) = \bar{n}_C$$

- La diseguaglianza diventa uguaglianza quando, riprendendo dalla dimostrazione:

$$\sum_{i=1}^M \left(P_X(x_i) \cdot \left(\log \frac{2^{-n(x_i)}}{P_X(x_i)} \right) \right) = 0$$

visto che i termini nella sommatoria sono sempre ≥ 0 deve valere:

$$P_X(x_i) \cdot \left(\log \frac{2^{-n(x_i)}}{P_X(x_i)} \right) = 0$$

Dato che $P_X(x_i)$ è sempre maggiore di zero (se così non fosse sarebbe presente un messaggio impossibile che si può rimuovere dall'alfabeto) l'unico termine che può azzerarsi è il logaritmo. Questo si azzera

2. Sorgenti senza memoria

quando l'argomento è uguale a 1 e quindi quando:

$$\begin{aligned} \frac{2^{-n(x_i)}}{P_X(x_i)} &= 1 \\ 2^{-n(x_i)} &= P_X(x_i) \\ -n(x_i) &= \log P_X(x_i) \\ n(x_i) &= -\log P_X(x_i) \\ n(x_i) &= \log \frac{1}{P_X(x_i)} \end{aligned}$$

codifica ottima: $H(x) = \bar{n}c$

- L'unico modo per ottenere la massima efficienza possibile da una codifica è fare in modo che quei logaritmi assumano un valore intero assegnabile a $n(x_i)$.
- Nel caso la codifica ottima non sia possibile allora Shannon suggerisce di utilizzare l' $n(x_i)$ intero immediatamente superiore a quello che sarebbe ottimo

codifica non ottima

$$n(x_i) = \left\lceil \log \frac{1}{P_X(x_i)} \right\rceil$$

- codifica nel caso non ottimo
- a msrn più probabili con contenuto informatico basso assegno una lunghezza di codifica bassa

in questo modo si ha che:

$$\log \frac{1}{P_X(x_i)} < n(x_i) < \log \frac{1}{P_X(x_i)} + 1$$

e quindi:

$$\begin{aligned} \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} &< \sum_{i=1}^M P_X(x_i) \cdot n(x_i) < \sum_{i=1}^M P_X(x_i) \cdot \left(\log \frac{1}{P_X(x_i)} + 1 \right) \\ H(X) &< \bar{n}_C < \sum_{i=1}^M P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} + \sum_{i=1}^M P_X(x_i) \\ H(X) &< \bar{n}_C < H(X) + 1 \end{aligned}$$

$\rho_k(x_i)$ $\rho_{K_1, K_2}(x_i, x_j)$
 $\Sigma(x_i) \rightarrow \Sigma(x_i, x_j)$

a due simboli x_i, x_j dell'alfabeto
associa una sola sequenza $C(xij)$

con questa scelta posso costruire un codice univocamente decodificabile che ha una lunghezza media maggiore dell'entropia e inferiore all'entropia +1 bit

- Codificando i messaggi a coppie è come se si codificasse da una sorgente di entropia $2 \cdot H(X)$. Questo codice possiede il doppio dell'informazione in quanto contiene due messaggi. Quindi anche la lunghezza media \bar{n}_{C2} di questa codifica a coppie sarà il doppio rispetto a quella della codifica normale e quindi usando l'osservazione precedente si ha che:

in caso di codifica non ottima significa che si sta usando più bit in media di quelli strettamente necessari per rappresentare ogni simbolo della sorgente
ossia che la codifica adottata introduce overhead inutile è inefficiente e c'è margine di miglioramento

$$2 \cdot H(X) < \bar{n}_{C2} < 2 \cdot H(X) + 1$$

$$H(X) < \bar{n}_C < H(X) + \frac{1}{2}$$

se però immagino di codificare a L-uple con lo stesso criterio ho:

$$L \cdot \bar{H}(x) \leq \bar{C} \leq L \cdot H(x) + 1$$

$$\bar{H}(x) \leq \bar{n} = \frac{\bar{C}}{L} \leq \bar{H}(x) + \frac{1}{L}$$

E quindi tende a diventare ottimo per L che prende all'infinito.
Ma per L finito la codifica ottima è quella di Huffman

quindi ci si può avvicinare di più al valore ottimo.

- Seguendo il ragionamento dell'osservazione precedente si nota che si possono codificare i messaggi in N-uple con N a piacere ottenendo una lunghezza media sempre più vicina al valore ottimo.

Esempio codifica di Shannon Sia X una sorgente binaria con alfabeto {1, 0} e con $P(1) = 0.8$ e $P(0) = 0.2$; si può ricavare facilmente l'entropia:

$$H(X) = 0.8 \cdot \log \frac{1}{0.8} + 0.2 \cdot \log \frac{1}{0.2} = 0.722 \text{ bit}$$

2. Sorgenti senza memoria

Codifica di Shannon a coppie

X_k	X_{k+1}	P congiunta	n_i	Codice
0	0	$0.8 \cdot 0.8 = 0.64$	1	0
0	1	$0.8 \cdot 0.2 = 0.16$	3	100
1	0	$0.2 \cdot 0.8 = 0.16$	3	101
1	1	$0.2 \cdot 0.2 = 0.04$	5	11111
Somma P		$0.64 + 0.16 + 0.16 + 0.04 = 1$		

- assegno a Messaggi, più probabili un codice di lunghezza inferiore
- in questo modo, i simboli più probabili hanno codici più corti e quelli meno probabili hanno codici più lunghi
- questo riduce al minimo la lunghezza media del codice, rendendo uguale all'entropia

Per riempire la tabella:

- Si scrivono tutte le possibili combinazioni che si possono ottenere con delle coppie di messaggi, in questo caso 4.
- Si ricava la probabilità congiunta che capiti la determinata sequenza. Dato che sono tutti messaggi indipendenti questa è uguale al prodotto delle singole probabilità e, data la loro natura, la somma di questa colonna è sempre uguale a 1.
- Si ricava la lunghezza del messaggio usando la regola proposta da Shannon, ossia

$$n_i = \left\lceil \log \frac{1}{P_X(x_i)} \right\rceil$$

- Si scrive il codice in modo che sia istantaneamente decodificabile e che rispetti le lunghezze calcolate.

Si può ricavare

$$\bar{n} = \frac{0.64 \cdot 1 + 0.16 \cdot 3 + 0.16 \cdot 3 + 0.04 \cdot 5}{2} = 0.9 \text{ bit} > H(X) = 0.722 \text{ bit}$$

rispettando il teorema di Shannon.

Codifica di Shannon a triple Si procede costruendo la stessa tabella del caso a coppie.

X_k	X_{k+1}	X_{k+2}	P congiunta	n_i	Codice
0	0	0	$0.8 \cdot 0.8 \cdot 0.8 = 0.512$	1	0
0	0	1	$0.8 \cdot 0.8 \cdot 0.2 = 0.128$	3	100
0	1	0	$0.8 \cdot 0.2 \cdot 0.8 = 0.128$	3	101
0	1	1	$0.8 \cdot 0.2 \cdot 0.2 = 0.032$	5	11100
1	0	0	$0.2 \cdot 0.8 \cdot 0.8 = 0.128$	3	110
1	0	1	$0.8 \cdot 0.2 \cdot 0.2 = 0.032$	5	11101
1	1	0	$0.8 \cdot 0.2 \cdot 0.2 = 0.032$	5	11110
1	1	1	$0.2 \cdot 0.2 \cdot 0.2 = 0.008$	7	1111111
Somma P		$0.512 + 0.128 \cdot 3 + 0.032 \cdot 3 + 0.008 = 1$			

ottenendo

$$\bar{n} = \frac{2.2}{3} = 0.733 \text{ bit} > H(X) = 0.722 \text{ bit}$$

. Si nota che è meglio della codifica a coppie.

2.2.3. Codifica di Huffman

Definizione di codice ottimo Un codice C con lunghezza media \bar{n}_C si definisce ottimo per una sorgente se per ogni altro codice C' di lunghezza media $\bar{n}_{C'}$ vale:

$$\bar{n}_C \leq \bar{n}_{C'}$$

un codice ottimo per una sorgente X se non esiste nessun altro codice che riesce a garantire una lunghezza media minore dei messaggi

ossia non esiste un codice di lunghezza minore (ma potrebbe esistere un codice con la stessa lunghezza).

Primo teorema sull'ottimalità Sia C un codice ottimo e istantaneamente decodificabile per una sorgente X , allora:

$$\forall x_a, x_b \text{ tali che } P(x_a) \leq P(x_b) \rightarrow n(x_a) \geq n(x_b)$$

vado ad assegnare ai messaggi più probabili una lunghezza minore, affinché la lunghezza media si abbassi

Tratta da Covers Thomas: "Elements of I.T. - Wiley '89"

Dimostrazione per assurdo Siano x_a e x_b tali che $P(x_a) \leq P(x_b)$ e C un codice ottimo che per assurdo ha $n(x_a) \leq n(x_b)$ allora il suo valore medio vale:

$$\bar{n} = \sum_{i=1}^M P_X(x_i) \cdot n(x_i) = r + P(x_a) \cdot n(x_a) + P(x_b) \cdot n(x_b)$$

dove r è la sommatoria degli altri valori dell'alfabeto. Si può definire un codice C' partendo da C scambiando $C(x_a)$ con $C(x_b)$ e quindi ottenendo $n'(x_a) = n(x_b)$ e $n'(x_b) = n(x_a)$. Questo codice ha lunghezza media pari a:

$$\begin{aligned} \bar{n}' &= r + P(x_a) \cdot n'(x_a) + P(x_b) \cdot n'(x_b) = \\ &= r + P(x_a) \cdot n(x_b) + P(x_b) \cdot n(x_a) \end{aligned}$$

Paragonando le due lunghezze:

$$\begin{aligned} \bar{n} - \bar{n}' &= r + P(x_a) \cdot n(x_a) + P(x_b) \cdot n(x_b) - r - P(x_a) \cdot n(x_b) - P(x_b) \cdot n(x_a) = \\ &= P(x_a) \cdot (n(x_a) - n(x_b)) + P(x_b) \cdot (n(x_b) - n(x_a)) = \\ &= P(x_a) \cdot (n(x_a) - n(x_b)) - P(x_b) \cdot (n(x_a) - n(x_b)) = \\ &= \underbrace{(n(x_a) - n(x_b))}_{\geq 0} \cdot \underbrace{(P(x_a) - P(x_b))}_{\geq 0} \end{aligned}$$

quindi $\bar{n} - \bar{n}' \geq 0$, cioè $\bar{n}' \leq \bar{n}$, e quindi C' è un codice migliore di C e quindi C non è ottimo.

Secondo teorema sull'ottimalità Sia C un codice ottimo e istantaneamente decodificabile per una sorgente X in cui $n(x_1) \leq n(x_2) \leq \dots \leq n(x_{M-1}) \leq n(x_M)$ allora:

messaggi meno probabili => secondo teorema !

$$n(x_M) = n(x_{M-1})$$

Dimostrazione Per l'istantanea decodificabilità $C(x_M)$ deve avere i primi $n(x_{M-1})$ bit diversi da quelli di $C(x_{M-1})$ e quindi non è necessario aggiungere altri bit per differenziare i due codici.

Terzo teorema sull'ottimalità Sia C un codice ottimo e istantaneamente decodificabile per una sorgente X in cui $n(x_1) \leq n(x_2) \leq \dots \leq n(x_{M-1}) \leq n(x_M)$ allora $C(x_M)$ e $C(x_{M-1})$ possono essere diversi solo nell'ultimo bit.

Dimostrazione Per scegliere $C(x_M)$ bisogna scegliere un codice che non inizi come tutti gli altri e, per il secondo teorema, che sia lungo quanto $C(x_{M-1})$. Dato che il codice $C(x_{M-1})$ inizia in modo diverso da tutti gli altri codici di lunghezza inferiore si ha che modificando l'ultimo bit si ottiene un codice che inizia ancora diversamente da tutti quelli di lunghezza inferiore, e inoltre differisce anche da $C(x_{M-1})$ e quindi può essere usato per $C(x_M)$.

senza modificare n medio

Ad esempio:

- Se abbiamo un codice con $C(x_1) = 10$ e $C(x_2) = 100$, $C(x_1)$ è un prefisso di $C(x_2)$, il che rende il codice non istantaneamente decodificabile. Infatti, leggendo il "10" iniziale di $C(x_2)$, non sappiamo se si tratta di $C(x_1)$ o dell'inizio di $C(x_2)$.

2. Sorgenti senza memoria

Codifica di Huffman Il metodo di Huffman permette di ottenere sempre la codifica ottima ed è un metodo iterativo che sfrutta i tre teoremi appena visti. Ad ogni passo:

1. Si riordinano i termini dell'alfabeto dal più probabile al meno probabile, in modo che, per il primo teorema, i codici saranno in ordine di lunghezza dal più corto al più lungo.
2. Si selezionano gli ultimi due elementi x_M e x_{M-1} , ossia i meno probabili, e si assegna un bit diverso a ognuno. Questo bit sarà il bit finale della loro codifica che per il terzo teorema è l'unico che deve differire.
3. Si crea una nuova sorgente S' con un alfabeto lungo $M - 1$ in cui tutti i termini rimangono uguali con la stessa probabilità escluso x'_{M-1} in cui si ha $P'(x'_{M-1}) = P(x_{M-1}) + P(x_M)$. Il codice di S si ottiene concatenando il codice di S' con i bit aggiunti al passo precedente e quindi la lunghezza del codice è:

$$\begin{aligned}\bar{n} &= \bar{n}' + 1 \cdot P(x_{M-1}) + 1 \cdot P(x_M) = \\ &= \bar{n}' + P(x_{M-1}) + P(x_M)\end{aligned}$$

4. Si ripetono i primi 3 passaggi con la nuova sorgente finché non si arriva a una sorgente con un alfabeto con un solo elemento (dopo $M - 1$ passaggi).

Esempio di codifica di Huffman Si riprenda l'esempio sulla codifica di Shannon, sia X una sorgente binaria con alfabeto $\{1, 0\}$ e con $P(1) = \underline{0.8}$ e $P(0) = \underline{0.2}$; si può ricavare facilmente l'entropia:

$$H(X) = 0.8 \cdot \log \frac{1}{0.8} + 0.2 \cdot \log \frac{1}{0.2} = 0.722 \text{ bit}$$

Codifica di Huffman a coppie Si rappresentano nella tabella i dati ordinati in ordine di probabilità:

X_k	X_{k+1}	P congiunta	bit aggiunto
0	0	$0.8 \cdot 0.8 = 0.64$	
0	1	$0.8 \cdot 0.2 = 0.16$	
1	0	$0.2 \cdot 0.8 = 0.16$	1
1	1	$0.2 \cdot 0.2 = 0.04$	0

Si crea una nuova sorgente con 3 elementi con gli ultimi due combinati e la sia riordina in ordine di probabilità:

X_k	X_{k+1}	P congiunta	bit aggiunto	bit di prima
0	0	0.64		
1	0			1
1	1	$0.16 + 0.04 = 0.20$	1	0
0	1	0.16	0	

Si crea una nuova sorgente con 2 elementi con gli ultimi due combinati e la sia riordina in ordine di probabilità:

X_k	X_{k+1}	P congiunta	bit aggiunto	bit di prima
0	0	0.64	1	
1	0			11
1	1	$0.20 + 0.16 = 0.36$	0	10
0	1			0

Unendo gli ultimi due elementi si ottiene un alfabeto con un solo elemento quindi la codifica è ultimata. Si è ottenuta la seguente codifica:

2. Sorgenti senza memoria

X_k	X_{k+1}	P congiunta	codice	n_i
0	0	0.64	1	1
0	1	0.16	00	2
1	0	0.16	011	3
1	1	0.04	010	3

da cui si ricava che:

$$\bar{n} = \frac{1 \cdot 0.64 + 2 \cdot 0.16 + 3 \cdot 0.16 + 3 \cdot 0.04}{2} = 0.78 \text{ bit}$$

che è meglio della codifica di Shannon a coppie e inoltre si può notare che i 3 teoremi di ottimalità sono rispettati.

Codifica di Huffman a triple Si rappresentano nella tabella i dati ordinati in ordine di probabilità:

X_k	X_{k+1}	X_{k+2}	P congiunta	bit aggiunto
0	0	0	0.512	
0	0	1	0.128	
0	1	0	0.128	
1	0	0	0.128	
0	1	1	0.032	
1	0	1	0.032	
1	1	0	0.032	1
1	1	1	0.008	0

Si crea una nuova sorgente con 7 elementi con gli ultimi due combinati e la sia riordina in ordine di probabilità:

X_k	X_{k+1}	X_{k+2}	P congiunta	bit aggiunto	bit di prima
0	0	0	0.512		
0	0	1	0.128		
0	1	0	0.128		
1	0	0	0.128		
1	1	0	0.032 + 0.08 = 0.040		1
1	1	1	0.032 + 0.08 = 0.040		0
0	1	1	0.032	1	
1	0	1	0.032	0	

Si crea una nuova sorgente con 6 elementi con gli ultimi due combinati e la sia riordina in ordine di probabilità:

X_k	X_{k+1}	X_{k+2}	P congiunta	bit aggiunto	bit di prima
0	0	0	0.512		
0	0	1	0.128		
0	1	0	0.128		
1	0	0	0.128		
0	1	1	0.032 + 0.032 = 0.064	1	1
1	0	1	0.032 + 0.032 = 0.064	0	0
1	1	0	0.032 + 0.08 = 0.040	0	1
1	1	1	0.032 + 0.08 = 0.040	0	0

Si crea una nuova sorgente con 5 elementi con gli ultimi due combinati e la sia riordina in ordine di probabilità:

2. Sorgenti senza memoria

X_k	X_{k+1}	X_{k+2}	P congiunta	bit aggiunto	bit di prima
0	0	0	0.512		
0	0	1	0.128		
0	1	0	0.128		
1	0	0	0.128	1	
0	1	1			11
1	0	1			10
1	1	0			01
1	1	1			00

Si crea una nuova sorgente con 4 elementi con gli ultimi due combinati e la sia riordina in ordine di probabilità:

X_k	X_{k+1}	X_{k+2}	P congiunta	bit aggiunto	bit di prima
0	0	0	0.512		
1	0	0			1
0	1	1			011
1	0	1	0.104 + 0.128 = 0.232		110
1	1	0			001
1	1	1			000
0	0	1	0.128	1	
0	1	0	0.128	0	

Si crea una nuova sorgente con 3 elementi con gli ultimi due combinati e la sia riordina in ordine di probabilità:

X_k	X_{k+1}	X_{k+2}	P congiunta	bit aggiunto	bit di prima
0	0	0	0.512		
0	0	1			1
0	1	0	0.128 + 0.128 = 0.256	1	0
1	0	0			1
0	1	1			011
1	0	1	0.104 + 0.128 = 0.232	0	110
1	1	0			001
1	1	1			000

Si crea una nuova sorgente con 2 elementi con gli ultimi due combinati e la sia riordina in ordine di probabilità:

X_k	X_{k+1}	X_{k+2}	P congiunta	bit aggiunto	bit di prima
0	0	0	0.512	1	
0	0	1			11
0	1	0			10
1	0	0			01
0	1	1	0.256 + 0.232 = 0.488	0	0011
1	0	1			0110
1	1	0			0001
1	1	1			0000

Unendo gli ultimi due elementi si ottiene un alfabeto con un solo elemento quindi la codifica è ultimata. Si è ottenuta la seguente codifica:

2. Sorgenti senza memoria

X_k	X_{k+1}	X_{k+2}	P congiunta	Codice	n_i
0	0	0	0.512	1	1
0	0	1	0.128	011	3
0	1	0	0.128	010	3
0	1	1	0.032	00011	5
1	0	0	0.128	001	3
1	0	1	0.032	00110	5
1	1	0	0.032	00001	5
1	1	1	0.008	00000	5

da cui si ricava che:

$$\bar{n} = \frac{2.184}{3} = 0.728 \text{ bit}$$

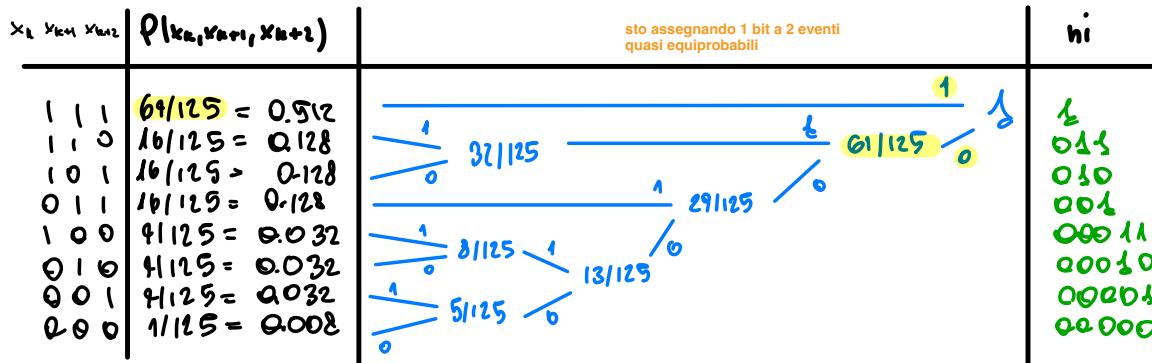
che è meglio della codifica di Shannon a triple e inoltre si può notare che i 3 teoremi di ottimalità sono rispettati.

Osservazioni sulla codifica

- La sequenza di un messaggio generata tramite un buon codice contiene 0 e 1 equiprobabili, in modo che ogni bit contenga la stessa quantità di informazione e quindi l'informazione contenuta nel messaggio viene massimizzata.
- Per l'osservazione precedente la codifica di Huffman cerca di dividere l'informazione sempre in due parti equiprobabili cercando di massimizzare l'informazione contenuta in ogni bit.

• guardare esercizio con dado T,C
• $H(X)$ massima e nc medio intero

- se volessimo misurare l'informazione che porta ciascuno di questi messaggi il costo di rappresentazione del messaggio è $\log M$ bit, dove M è il numero di messaggi sono sufficienti per rappresentare questi messaggi
- se i messaggi non sono equi probabili possiamo risparmiare qualcosa in termini di costo sfruttando la non equi probabilità dei messaggi, cioè: associando sequenze di bit più lunghe a messaggi più rari e sequenze di bit più brevi a messaggi più frequenti
- 1 bit vale davvero 1 bit finché ha una probabilità 1/2 di assumere un valore piuttosto che l'altro altrimenti vale meno di 1 bit \Rightarrow la codifica di Huffman fondamentalmente se noi guardiamo l'albero consiste nel scegliere un valore di 1 bit andando a frazionare lo spazio possibile degli eventi che sono equi probabili e che si meritano effettivamente il valore di 1 bit. E si procede in questo modo iterando



$X_k X_{k+1}$	$P(X_k, X_{k+1})$	C_i	h_i
0 0	$1/25$	010	3
0 1	$4/25$	011	3
1 0	$4/25$	00	2
1 1	$16/25$	1	1

- La memoria toglie informazione ai messaggi
- Questo perché essendo che i messaggi sono legati tra di loro l'osservazione del messaggio precedente va a modificare la distribuzione di probabilità del messaggio successivo
- dunque introduce quella che viene definita la distribuzione di probabilità condizionata

la probabilità dell'evento $X_k = x_k$ dato che X_{k-1} è stato uguale a x_{k-1}

$$P_{X_k|X_{k-1}}(x_k|x_{k-1}) = \text{Prob}[X_k = x_k | X_{k-1} = x_{k-1}]$$

- messaggio corrente
- messaggio precedente
- caratteri dell'alfabeto X qualsiasi non necessariamente il k -esimo e il $(k-1)$ -esimo

3. Sorgenti con memoria

Introduzione Se la sorgente contiene memoria allora la conoscenza della sequenza di messaggi antecedenti X_1, X_2, \dots, X_{k-1} modifica l'informazione contenuta nel messaggio X_k riducendone l'incertezza e quindi diminuendone l'informazione.

Per esempio nella lingua italiana se al tempo $k - 1$ è presente la lettera L le probabilità delle lettere al tempo k variano, infatti è molto probabile che ci sia una vocale e molto meno probabile che ci sia una consonante e quindi l'informazione legata all'arrivo di una consonante è maggiore. Un caso estremo è la Q in cui la lettera dopo non contiene informazione dato che si è certi che ci sarà la U .

Si può anche notare che se al tempo $k - 2$ è presente la lettera G e al tempo $k - 1$ la lettera L , è quasi certo che al tempo k ci sarà la lettera I e quindi l'informazione contenuta nella I sarà molto inferiore a quella contenuta nella O .

In generale più eventi passati si conoscono più si può abbassare l'informazione contenuta nell'evento successivo e quindi si può creare una codifica sempre migliore.

Per questo motivo è possibile dare una definizione più completa di entropia in cui viene considerata la memoria della sorgente.

3.1. Entropia condizionata

Definizione di probabilità condizionata La probabilità condizionata $P_{A|B}(a_i|b_j)$ indica la probabilità che l'esito dell'evento A sia a_i sapendo che l'esito dell'evento B è b_j . Questa definizione si può generalizzare anche per più eventi di cui si conosce l'esito: $P_{A|B,C,\dots}(a_i|b_j, c_k, \dots)$.

Definizione di probabilità congiunta La probabilità congiunta $P_{A,B}(a_i, b_j)$ indica la probabilità che l'evento A abbia esito a_i e l'evento B abbia esito b_j . Questa definizione si può generalizzare anche per più eventi: $P_{A,B,C,\dots}(a_i, b_j, c_k, \dots)$.

Definizione di probabilità marginale La probabilità marginale $P_A(a_i)$ è la probabilità che l'evento A abbia esito a_i ignorando l'esito degli altri eventi. Analogamente si può definire la probabilità marginale $P_B(b_j)$ e si può generalizzare anche per un gruppo di variabili, per esempio $P_{A,B}(a_i, b_j)$ è la probabilità marginale di A e B supponendo che esistano altri eventi.

Osservazioni

- La probabilità che si verifichino gli eventi a_i e b_j insieme è uguale alla probabilità che si verifichi l'evento b_j moltiplicata per la probabilità che si verifichi l'evento a_i sapendo che è avvenuto l'evento b_j , ossia:

$$P_{A,B}(a_i, b_j) = P_{A|B}(a_i|b_j) \cdot P_B(b_j)$$

quindi:

come si comporta o distribuisce A nei casi in cui si verifica B e poi normalizzo questa distribuzione di probabilità dividendo per la probabilità di B

$$P_{A|B}(a_i|b_j) = \frac{P_{A,B}(a_i, b_j)}{P_B(b_j)}$$

congiuntamente gli eventi A e B
probabilità del condizionante B

- Per l'osservazione precedente si ha che:

$$P_{A|B}(a_i|b_j) \geq P_{A,B}(a_i, b_j)$$

3. Sorgenti con memoria

- Se due esiti sono indipendenti si ha:

$$P_{A|B}(a_i|b_j) = P_A(a_i)$$

e quindi

$$\begin{aligned} P_{A,B}(a_i, b_j) &= P_{A|B}(a_i|b_j) \cdot P_B(b_j) = \\ &= P_A(a_i) \cdot P_B(b_j) \end{aligned}$$

- Se ci sono N possibili esiti dell'evento B si ha:

$$\sum_{j=1}^N P_{A,B}(a_i, b_j) = P_A(a_i)$$

- Se i due esiti a_i e b_j sono dipendenti allora:

$$P_{A,B}(a_i, b_j) = P_{A|B}(a_i|b_j) \cdot P_B(b_j) \geq P_A(a_i) \cdot P_B(b_j)$$

Informazione condizionata Supponendo che esistano due eventi X (con M possibili esiti) e Y (con N possibili esiti):

- L'informazione contenuta nell'esito x_i dell'evento X sapendo che l'evento Y ha avuto esito y_j vale:

$$I(x_i | y_j) \triangleq \log \frac{1}{P_{X|Y}(x_i | y_j)}$$

- L'informazione media contenuta nell'esito dell'evento X sapendo che l'evento Y ha avuto esito y_j :

- entropia condizionata da y_j
tutti i possibili esiti di X , dato il verificarsi di y_j
- fissato sito $Y = y_j$

$$H(X|y_j) \triangleq \sum_{i=1}^M P_{X|Y}(x_i | y_j) \cdot I(x_i | y_j) = \sum_{i=1}^M P_{X|Y}(x_i | y_j) \cdot \log \frac{1}{P_{X|Y}(x_i | y_j)}$$

- Proprietà:
- $H(X|y_j) \geq 0$
 - $H(X|y_j) \in \text{Log}_2 M$ dove $M = |Y|$
 - $H(x_i | y_j) = \log_2 M$ se $P_{X|Y}(x_i | y_j)$ è una forma

- L'entropia condizionata è l'informazione media contenuta nell'esito dell'evento X conoscendo l'esito dell'evento Y vale:

$$H(X|Y) \triangleq \sum_{j=1}^N P_Y(y_j) \cdot H(X|y_j) \quad (\text{bit}) \text{ per } \log_2$$

con qualche passaggio matematico si ottiene:

- entropia condizionata media misura in bit l'informazione che porta X quando già conosco Y

$$\begin{aligned} H(X|Y) &= \sum_{j=1}^N P_Y(y_j) \cdot H(X|y_j) \triangleq \sum_{j=1}^N P_Y(y_j) \cdot I(X|y_j) \\ &= \sum_{j=1}^N P_Y(y_j) \cdot \sum_{i=1}^M P_{X|Y}(x_i | y_j) \cdot \log \frac{1}{P_{X|Y}(x_i | y_j)} = \\ &= \sum_{j=1}^N \sum_{i=1}^M P_Y(y_j) \cdot P_{X|Y}(x_i | y_j) \cdot \log \frac{1}{P_{X|Y}(x_i | y_j)} = \\ &= \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{X|Y}(x_i | y_j)} = \\ &= \mathbb{E}_{X,Y} \left[\log \frac{1}{P_{X|Y}(x_i | y_j)} \right] = \\ &= \mathbb{E}_{X,Y} [I(x_i | y_j)] \end{aligned}$$

Proprietà:

- $I(X|Y) \geq 0$ perché $H(X|y_j) \geq 0$
- $H(X|Y) \leq H(X)$ se più Y può ridurre l'incertezza circa l'info che porta X .

3. Sorgenti con memoria

Osservazioni

- Dato che la probabilità condizionata è un valore sempre inferiore a 1 l'informazione è sempre un valore positivo in quanto logaritmo di un valore positivo e quindi l'entropia condizionata è sempre un valore positivo:

$$H(X|Y) \geq 0$$

- L'entropia condizionata è nulla quando

$$\sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{X|Y}(x_i|y_j)} = 0$$

- la probabilità condizionata risulta essere uguale a 1, quando il verificarsi dell'evento Y mi elimina qualsiasi incertezza su X
- probabilità al 100% che si verifichi un determinato evento => determinismo

Questo avviene quando o la probabilità congiunta è nulla, e quindi lo è anche quella condizionata, o quando quella condizionata vale 1 ossia quando conoscendo l'esito dell'evento Y non si ha incertezza sull'esito dell'evento X.

Teorema L'entropia condizionata è sempre minore o uguale all'entropia non condizionata:

$$H(X|Y) \leq H(X)$$

conoscendo l'esito dell'evento Y mi va a diminuire l'incertezza o contenuto informativo e dunque l'entropia diminuisce

Dimostrazione Ricavando la differenza tra i due valori si ottiene:

$$\begin{aligned}
 H(X|Y) - H(X) &= \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{X|Y}(x_i|y_j)} - \sum_{i=1}^M P_X(x_i) \log \frac{1}{P_X(x_i)} = \\
 &= \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{X|Y}(x_i|y_j)} - \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_X(x_i)} = \\
 &= \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \left[\log \frac{1}{P_{X|Y}(x_i|y_j)} - \log \frac{1}{P_X(x_i)} \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \left[\log \frac{P_X(x_i)}{P_{X|Y}(x_i|y_j)} \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \left[\log \frac{P_X(x_i)}{P_{X|Y}(x_i|y_j)} \cdot \frac{P_Y(y_j)}{P_Y(y_j)} \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \left[\log \frac{P_X(x_i) \cdot P_Y(y_j)}{P_{X,Y}(x_i, y_j)} \right]
 \end{aligned}$$

se prendo la distribuzione congiunta di due variabili casuali e sommo su tutti i valori di una delle due calcolo la marginale dell'altra

Ricordando che $\log x \leq (x-1) \cdot \log e$ si ottiene:

$$\begin{aligned}
 H(X|Y) - H(X) &= \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \left[\log \frac{P_X(x_i) \cdot P_Y(y_j)}{P_{X,Y}(x_i, y_j)} \right] \leq \\
 &\leq \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \log e \cdot \left(\frac{P_X(x_i) \cdot P_Y(y_j)}{P_{X,Y}(x_i, y_j)} - 1 \right) = \\
 &= \log e \cdot \sum_{j=1}^N \sum_{i=1}^M \left[\frac{P_{X,Y}(x_i, y_j)}{P_{X,Y}(x_i, y_j)} \cdot P_X(x_i) \cdot P_Y(y_j) - P_{X,Y}(x_i, y_j) \right] = \\
 &= \log e \cdot \sum_{j=1}^N \sum_{i=1}^M \underbrace{\left[P_X(x_i) \cdot P_Y(y_j) - P_{X,Y}(x_i, y_j) \right]}_{\leq 0} \leq \\
 &\leq 0
 \end{aligned}$$

$$P_{A,B}(a_i, b_j) = P_{A|B}(a_i|b_j) \cdot P_B(b_j) \geq P_A(a_i) \cdot P_B(b_j)$$

3. Sorgenti con memoria

~~Def:~~: può invece captare che $H(X|y) > H(X)$ se $P_{X|Y}(x|y)$ è più uniforme di $P_x(x)$.

e quindi:

$$\begin{aligned} H(X|Y) - H(X) &\leq 0 \\ H(X|Y) &\leq H(X) \end{aligned}$$

il condizionamento in media può solo diminuire l'informazione.

Osservazione Si può notare che la disegualanza diventa uguaglianza quando, riprendendo la dimostrazione:

$$\sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \left[\log \frac{P_X(x_i) \cdot P_Y(y_j)}{P_{X,Y}(x_i, y_j)} \right] = 0 \quad | \quad H(X|Y) = H(X)$$

dato che la probabilità congiunta è sempre un valore positivo si ha che il logaritmo deve essere nullo e quindi il termine dentro deve valere 1 e quindi il numeratore e il denominatore devono essere uguali ossia:

$$P_X(x_i) \cdot P_Y(y_j) = P_{X,Y}(x_i, y_j)$$

che significa che gli eventi sono indipendenti. \Rightarrow ossia che $Y = y$ non modifica la ddp di X

Oss3: il caso opposto è quello in cui X e Y sono deterministicamente legate $X = f(Y)$ per ogni y

$$P_{X|Y}(x|y) = \begin{cases} 1 & \text{se } x = f(y) \\ 0 & \text{altrimenti} \end{cases} \Rightarrow H(X|Y) = 0$$

Alla conoscenza di Y esaurisce tutta l'informazione su X

Estensione a più variabili La definizione di entropia condizionata si può estendere a un numero superiore di variabili:

$$H(X|Y, \dots, Z) \triangleq \mathbb{E}_{X,Y,\dots,Z} \left[\log \frac{1}{P_{X|Y,\dots,Z}(x_i|y_j, \dots, z_k)} \right]$$

rappresenta l'informazione che porta X quando ho osservato sia Y che Z

e vale:

$$0 \leq H(X|Y, \dots, Z) \leq H(X|Y, \dots) \leq \dots \leq H(X|Y) \leq H(X)$$

3.2. Entropia congiunta

L'entropia congiunta è l'informazione media associata alla coppia di esiti degli eventi X e Y :

$$\begin{aligned} H(X, Y) &\triangleq \sum_{j=1}^N \sum_{i=1}^M P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{X,Y}(x_i, y_j)} = \\ &= \mathbb{E}_{X,Y} \left[\log \frac{1}{P_{X,Y}(x_i, y_j)} \right] = \\ &= \mathbb{E}_{X,Y} [I(x_i, y_j)] \end{aligned}$$

Proprietà:

- $H(X, Y) \geq 0$
- $H(X, Y) = H(Y) + H(X|Y)$
 $= H(X) + H(Y|X)$

Osservazioni

- Se tutte le coppie di esiti di X e Y sono indipendenti allora si ha che:

$$H(X, Y) = H(X) + H(Y)$$

Dim:

$$\begin{aligned} \mathbb{E}_{XY} \left[\log \frac{1}{P_{XY}(x,y)} \right] &= \mathbb{E}_{XY} \left[\log \frac{1}{P_Y(y) \cdot P_{X|Y}(x|y)} \right] \\ &= \mathbb{E}_{XY} \left[\log \frac{1}{P_Y(y)} \right] + \mathbb{E}_{XY} \left[\log \frac{1}{P_{X|Y}(x|y)} \right] \\ &= H(Y) + H(X|Y) \end{aligned}$$

non c'è nulla che dipende da X dunque

Le stesse dimostrazioni sono elencate sotto ma con le sommatorie dove esprimono allo stesso modo la media

3. Sorgenti con memoria

infatti:

$$\begin{aligned}
 H(X, Y) &= \sum_{j=1}^N \sum_{i=1}^M \left[P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{X,Y}(x_i, y_j)} \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M \left[P_X(x_i) \cdot P_Y(y_j) \cdot \log \frac{1}{P_X(x_i) \cdot P_Y(y_j)} \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M \left[P_X(x_i) \cdot P_Y(y_j) \cdot \left(\log \frac{1}{P_X(x_i)} + \log \frac{1}{P_Y(y_j)} \right) \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M \left[P_X(x_i) \cdot P_Y(y_j) \cdot \log \frac{1}{P_X(x_i)} \right] + \sum_{j=1}^N \sum_{i=1}^M \left[P_X(x_i) \cdot P_Y(y_j) \cdot \log \frac{1}{P_Y(y_j)} \right] = \\
 &= \sum_{j=1}^N \left[P_Y(y_j) \cdot \sum_{i=1}^M \left(P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} \right) \right] + \sum_{i=1}^M \left[P_X(x_i) \cdot \sum_{j=1}^N \left(P_Y(y_j) \cdot \log \frac{1}{P_Y(y_j)} \right) \right] = \\
 &= \sum_{j=1}^N [P_Y(y_j) \cdot H(X)] + \sum_{i=1}^M [P_X(x_i) \cdot H(Y)] = \\
 &= H(X) \cdot \underbrace{\sum_{j=1}^N P_Y(y_j)}_1 + H(Y) \cdot \underbrace{\sum_{i=1}^M P_X(x_i)}_1 = \\
 &= H(X) + H(Y)
 \end{aligned}$$

- Altrimenti:

$$\begin{aligned}
 H(X, Y) &= H(X|Y) + H(Y) = \\
 &= H(Y|X) + H(X)
 \end{aligned}$$

infatti:

$$\begin{aligned}
 H(X, Y) &= \sum_{j=1}^N \sum_{i=1}^M \left[P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{X,Y}(x_i, y_j)} \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M \left[P_{X|Y}(x_i|y_j) \cdot P_Y(y_j) \cdot \log \frac{1}{P_{X|Y}(x_i|y_j) \cdot P_Y(y_j)} \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M \left[P_{X|Y}(x_i|y_j) \cdot P_Y(y_j) \cdot \left(\log \frac{1}{P_{X|Y}(x_i|y_j)} + \log \frac{1}{P_Y(y_j)} \right) \right] = \\
 &= \sum_{j=1}^N \sum_{i=1}^M \left[P_{X|Y}(x_i|y_j) \cdot P_Y(y_j) \cdot \log \frac{1}{P_{X|Y}(x_i|y_j)} \right] + \sum_{j=1}^N \sum_{i=1}^M \left[P_{X|Y}(x_i|y_j) \cdot P_Y(y_j) \cdot \log \frac{1}{P_Y(y_j)} \right] = \\
 &= \sum_{j=1}^N \left[P_Y(y_j) \cdot \sum_{i=1}^M \left(P_{X|Y}(x_i|y_j) \cdot \log \frac{1}{P_{X|Y}(x_i|y_j)} \right) \right] + \sum_{j=1}^N \left[\log \frac{1}{P_Y(y_j)} \cdot P_Y(y_j) \cdot \underbrace{\sum_{i=1}^M P_{X|Y}(x_i|y_j)}_1 \right] = \\
 &= \sum_{j=1}^N [P_Y(y_j) \cdot H(X|y_j)] + \sum_{j=1}^N \left[\log \frac{1}{P_Y(y_j)} \cdot P_Y(y_j) \right] = \\
 &= H(X|Y) + H(Y) =
 \end{aligned}$$

II° versione:
 $H(Y|Y) = H(Y|X) + H(X)$
 $\frac{Q_X(x_i)}{Q_{X|Y}(x_i)} \cdot \frac{1}{Q_{Y|X}(y_j|x_i)}$

analogamente si ricava l'altra versione.

3. Sorgenti con memoria

Estensione a più variabili La definizione di entropia congiunta si può estendere a un numero superiore di variabili:

$$H(X, Y, \dots, Z) \triangleq \mathbb{E}_{X, Y, \dots, Z} \left[\log \frac{1}{P_{X, Y, \dots, Z}(x_i, y_j, \dots, z_k)} \right]$$

misura l'informazione che portano X, Y e Z insieme

e vale:

$$H(X, Y, Z) = H(X, Y|Z) + H(Z) = H(X|Y, Z) + H(Y|Z) + H(Z)$$

3.3. Entropia di sorgenti con memoria

Definizione di entropia di sorgente utilizzando l'entropia condizionata Data una sorgente X con memoria l'entropia della sorgente si definisce come:

$$H(X) = \lim_{L \rightarrow +\infty} H(X_k | X_{k-1}, \dots, X_{k-L})$$

ogni messaggio precedente può condizionare la distribuzione del messaggio corrente

ossia è l'informazione media contenuta nel messaggio X_k conoscendo tutti i messaggi precedenti.

Definizione di entropia di sorgente utilizzando l'entropia congiunta Data una sorgente X con memoria l'entropia della sorgente si definisce come:

$$H(X) = \lim_{L \rightarrow +\infty} \frac{1}{L} \cdot H(X_k, X_{k-1}, \dots, X_{k-L})$$

ossia l'entropia è l'informazione media contenuta nella L-upla di messaggi divisa per la lunghezza del messaggio L, perché la L-upla di messaggi conterrà in media L volte più informazione del singolo messaggio.

Osservazione Le due definizioni sono equivalenti e restituiscono lo stesso risultato. La prima è più intuitiva mentre la seconda permette di dimostrare più facilmente alcuni teoremi.

Definizione Una sorgente si dice di Markov se ha memoria finita, ossia se esiste m tale che:

$$P(X_k | X_{k-1}, \dots, X_{k-m-1}) = P(X_k | X_{k-1}, \dots, X_{k-m})$$

dove m è il numero di msm precedenti che influenzano l'esito X_k attuale

Osservazione Data una sorgente di Markov di memoria m si ha:

$$\begin{aligned} H(X) &= H(X_k | X_{k-1}, \dots, X_{k-m}) = \\ &= \frac{1}{m} \cdot H(X_k, X_{k-1}, \dots, X_{k-m}) \end{aligned}$$

- sorgente con memoria finita m (sorgente di Markov)
- Utilizzo diagramma di Markov per trovare le probabilità di stato

3.4. Codifica per sorgenti con memoria

I concetti esposti riguardo ai codici univocamente e istantaneamente decodificabili valgono anche per codici di sorgenti con memoria in quanto riguardano solo il codice in sé e non l'informazione contenuta nel singolo messaggio e quindi rispettare l'uguaglianza di Kraft rimane una condizione necessaria per un codice univocamente decodificabile e una condizione sufficiente per un codice istantaneamente decodificabile. Inoltre vale anche il primo teorema di Shannon.

Primo teorema di Shannon sulla codifica di sorgente Sia C un codice univocamente decodificabile di lunghezze $n_1, n_2, n_3, \dots, n_M$ per la sorgente X , allora si ha che

$$\sum_{i=1}^M P_X(x_i) \cdot n_i = \bar{n}_C \geq H(X)$$

3. Sorgenti con memoria

Dimostrazione Bisogna dimostrare che $H(X) - \bar{n}_C$ è minore o uguale a 0.

Per farlo si considerano i messaggi di una sorgente Y che raggruppa L messaggi di X che possono venir codificati con il codice C , in questo modo la sorgente Y ha un alfabeto di M^L simboli, la codifica dei messaggi ha lunghezza media pari a $L \cdot \bar{n}_C$ e l'entropia della sorgente di Y è L volte quella di X . Quindi:

alfabeto $X = \{x_1, \dots, x_M\}$

messaggi consecutivi di $X \Rightarrow$ parole composte da L simboli

con $L=1 : (x_1, x_1), (x_1, x_2), (x_1, x_3), \dots, (x_M, x_M)$

n^{a} tabelle confusioni H^L

nuova sorgente Y

- alfabeto composto da M^L simboli, cioè una rappresentazione che raggruppa le L messaggi X
- lunghezza massima: $L \cdot \bar{n}_C$
- entropia: $H(Y) = L \cdot H(X)$

$$H(X) - \bar{n}_C = \frac{1}{L} \cdot H(Y) - \frac{1}{L} \cdot \sum_{i=1}^{M^L} P_Y(y_i) \cdot n(y_i) =$$

$$H(X) - \bar{n}_C = \frac{1}{L} \cdot \left(H(Y) - \sum_{i=1}^{M^L} P_Y(y_i) \cdot n(y_i) \right) =$$

$$(H(X) - \bar{n}_C) \cdot L = \sum_{i=1}^{M^L} P_Y(y_i) \cdot \log \frac{1}{P_Y(y_i)} - \sum_{i=1}^{M^L} P_Y(y_i) \cdot n(y_i)$$

raggruppando L messaggi consecutivi di una sorgente X
si creano tutte le possibili combinazioni di L messaggi
presi dall'alfabeto originario di X che ha cardinalità M

Questa uguaglianza vale $\forall L$ e inoltre si può notare che la parte a destra è la stessa espressione che si è ottenuta nella dimostrazione con una sorgente senza memoria e quindi seguendo analoghi passaggi si può dire che è ≤ 0 e quindi:

$$\begin{aligned} L \cdot (H(X) - \bar{n}_C) &\leq 0 && \text{grazie a Kraft} \\ H(X) - \bar{n}_C &\leq 0 \\ H(X) &\leq \bar{n}_C \end{aligned}$$

che è quello che si voleva dimostrare.

Osservazione Un buon codice oltre ad avere zeri e uni equiprobabili deve anche essere senza memoria, altrimenti si potrebbe considerare tale memoria ottenendo un'entropia minore e quindi rendendo possibile un codice migliore.

Codifica d'esempio: fax Il fax è una codifica di fogli in bianco e nero in cui solitamente è rappresentato del testo, ossia codifica una matrice di punti che possono essere bianchi o neri dove il bianco è molto più probabile del nero dato che contiene del testo. Questa sorgente può essere caratterizzata:

- La sorgente ha un alfabeto binario $\{B, N\}$.
- Per ipotesi il fax utilizza $P(B) = 0.95$ e $P(N) = 0.05$.

- con codifica Huffman $\rightarrow 0.25$ bit/pixel
- con codifica per sorgenti con memoria 1D $\rightarrow 0.1$ bit/pixel
- con codifica per sorgenti con memoria 2D $\rightarrow 0.04$ bit/pixel

ottenendo un'entropia pari a:

$$H(X) = H_2[0.95] = 0.25 \text{ bit/pixel}$$

e quindi si può risparmiare il 75% usando la codifica di sorgente senza memoria, ma in un foglio scritto è presente anche della memoria perché vicino a un bianco è più probabile trovare un altro bianco che un nero dato che sono presenti intere file bianche per esempio e quindi sfruttando la presenza della memoria si ottiene il valore di entropia usato per lo standard fax che è:

$$H(X) = 0.04 \text{ bit/pixel}$$

ottenendo un ulteriore risparmio rispetto alla codifica di sorgente che non sfrutta la memoria.

Codifica d'esempio: testo in italiano

- La sorgente ha un alfabeto di 21 caratteri $\{A, B, \dots, Z\}$, considerando minuscole e maiuscole come la stessa lettera e ignorando la punteggiatura per semplicità.
- Analizzando un libro si possono ottenere le probabilità associate ad ogni lettera, nella tabella sottostante sono indicate alcune probabilità in ordine decrescente:

3. Sorgenti con memoria

- senza sfruttare la memoria $H(x) < 4$ bit/carattere
- con codifica per sorgenti con memoria $H(X) < 1$ bit/carattere

x_i	A	E	I	O	N	T	...	U	...	Q
$P_X(x_i)$	0.1	0.1	0.08	0.08	0.07	0.07	...	0.025	...	0.003

ottenendo un'entropia pari a:

$$H(X) \cong 4 \text{ bit/lettera}$$

ottenendo un guadagno di un bit a lettera, dato che per codificare 21 lettere equiprobabili servono 5 bit. Un testo può però essere considerato come una sorgente con memoria, perché le lettere non si susseguono in ordine casuale, e usando queste informazioni è possibile diminuire l'entropia. Analizzando sempre lo stesso libro, sfruttando la codifica di sorgente con memoria si ottiene che:

$$H(X) \leq 1 \text{ bit/lettera}$$

riducendo drasticamente il numero di bit necessari per salvare il testo. Da questo si può intuire che la lingua italiana è molto ridondante e poco ottimizzata; è lecito chiedersi perché l'evoluzione della lingua abbia portato ad un linguaggio così ridondante invece che ad uno ottimizzato. La risposta va ricercata nella sicurezza del linguaggio: avere poca informazione per lettera, e quindi molta ridondanza, permette di perdere poca informazione ognqualvolta si perde una frazione del testo, e quindi è possibile ricostruire facilmente tale informazione aumentando la sicurezza, ma pagando con la lunghezza. Viceversa un linguaggio con tanta informazione per carattere è molto più corto, ma la perdita di una frazione rende irrecuperabile il senso del testo.

Si crea, quindi, un trade-off tra sicurezza e lunghezza che trova soluzione nel contesto in cui il linguaggio è utilizzato.

La codifica di sorgente si occupa di esprimere un messaggio condensando più informazione possibile per simbolo e quindi non si interessa della sicurezza, la codifica di canale, invece, aggiunge ridondanza al messaggio per aumentare la sicurezza allungando il messaggio.

N.B.: | $h(x_i) = k$ bit di informazione \rightarrow codifica sorgente
 $h(x_i) = N = k + (N-k) \rightarrow$ codifica di canale

3.5. Codifica di Lempel-Ziv

é asintoticamente ottimo

L'algoritmo di Lempel-Ziv è un algoritmo per la codifica universale di sorgenti con memoria. Data una sequenza di simboli da codificare:

Non necessita della conoscenza delle statistiche della sorgente \Rightarrow applicabile a qualunque sorgente

binarie

1. Si divide la sequenza in sotto-sequenze inedite, ossia si «taglia» la sequenza data appena si trova una sequenza mai trovata.
2. Ogni sotto-sequenza si codifica tramite:
 - a) un puntatore alla sotto-sequenza che si ottiene togliendo l'ultimo simbolo;
 - b) l'ultimo simbolo.

Per comprendere meglio il procedimento si consideri l'esempio seguente.

Esempio di codifica Si vuole codificare la sequenza di bit:

011101101111001000

Si divide in sotto-sequenza inedite:

0|1|11|01|10|111|100|1000

Per il secondo passo si consideri la seguente tabella:

Numero	0	1	2	3	4	5	6	7	8
Sequenza	vuota	0	1	11	01	10	111	100	1000
Puntatore	0	0	2	1	2	3	5	7	
Puntatore codificato	0	0	10	01	010	011	101	111	
Nuovo bit	0	1	1	1	0	1	0	0	
Codifica sequenza	. 0	0 1	10 1	01 1	010 0	011 1	101 0	111 0	

3. Sorgenti con memoria

Osservazioni sulla costruzione della tabella:

- La sequenza 0 è sempre la sequenza vuota in modo che le sequenze con un solo carattere abbiano una sequenza precedente a cui aggiungere un carattere.
- Il numero di bit con cui bisogna codificare il puntatore alla sequenza precedente dipende da quante possibilità ci sono, per esempio la sequenza 4 può avere come puntatore solo altre 4 sequenze e quindi bastano 2 bit per codificare il puntatore, mentre la sequenza 6 può avere 6 diversi valori del puntatore e quindi necessita di 3 bit per codificare il puntatore correttamente. In genere la n -esima sequenza ha un puntatore codificato con:

$$\lceil \log n \rceil \text{ bit}$$

- La sequenza codificata si ottiene concatenando la codifica del puntatore al bit che viene aggiunto in quella sequenza.

Da questo si ottiene una sequenza codificata pari a:

0011010110100011110101110

ottenuta concatenando le codifiche delle varie sequenze.

Esempio di decodifica Partendo dalla sequenza codificata precedentemente:

0011010110100011110101110

Per decodificarla bisogna ricordare che tutte le sequenze sono scritte come la concatenazione di un puntatore e di un nuovo bit. Inoltre si sa che esistono sempre:

- 1 puntatore lungo un bit (per la sequenza 2)
- 2 puntatori lunghi due bit (per le sequenze 3 e 4)
- 4 puntatori lunghi tre bit (per le sequenze 5, 6, 7 e 8)
- 8 puntatori lunghi quattro bit
- ...

Quindi si può dividere il messaggio:

.|0||0|1||10|1||01|1||010|0||011|1||101|0||111|0

ricordando che la sequenza 0 è sempre quella vuota si può costruire la seguente tabella:

Numero	0	1	2	3	4	5	6	7	8
Sequenza codificata	. 0	0 1	10 1	01 1	010 0	011 1	101 0	111 0	
Puntatore codificato	0	0	10	01	010	011	101	111	
bit aggiunto	0	1	1	1	0	1	0	0	
Puntatore decodificato	0	0	2	1	2	3	5	7	
Sequenza	vuota	0	1	11	01	10	111	100	1000

da cui si ottiene la sequenza decodificata unendo le varie sotto-sequenze:

011101101111001000

Parte II.

Codifica di canale

- è modello matematico
- spazio in cui il segnale si propaga
- esiste chiaramente del rumore/noise e quello che io ho trasmesso non arriva destinazione come inteso
- Il canale può modellizzare tutti gli effetti casuali che possono capitare sono aleatori ossia che non sono sotto controllo del trasmettitore e ricevitore

4. Capacità di canale

- un canale discreto nel tempo senza memoria con ingresso X e uscita Y è univocamente specificato da:
- alfabeto X dei messaggi in ingresso
 $X = \{x_1, x_2, \dots, x_M\}$ elenco numerabile di simboli
 $X = [x_{\min}, x_{\max}]$ range di simboli
 - analogamente alfabeto Y dei messaggi in uscita
 $\mathcal{Y} = \{y_1, y_2, \dots, y_N\}$
 $Y = [y_{\min}, y_{\max}]$
 - il legame probabilistico tra X e Y
- (dopo) $P_{Y|X}(y_i|x_i)$ ingresso discreto/uscita discreta
 (dovuto al prob) $P_{Y|X}(y_i|x_i)$ ingresso discreto/uscita continua
 $P_{Y|X}(y_i|x_i)$ ingresso continuo/uscita continua

Prima di capire come funziona la codifica di canale bisogna definire con chiarezza cosa si intende con canale e come stabilire quanto il canale sia buono.

4.1. Definizione di canale

Un canale di comunicazione è il mezzo usato per trasmettere informazione da un trasmettitore a un ricevitore. Sul mezzo fisico si creano dei disturbi a causa dei quali l'informazione trasmessa è diversa da quella ricevuta, ma spesso l'informazione ricevuta è legata a quella trasmessa ed è possibile interpretarla per ricavare l'informazione che è stata inviata; altre volte invece dall'informazione ricevuta non è possibile ricavare l'informazione trasmessa con certezza creando quindi errori nella trasmissione.

In genere l'alfabeto dei messaggi che possono essere trasmessi è diverso dall'alfabeto dei messaggi che possono essere ricevuti perché, per esempio, si possono ricevere messaggi che indicano semplicemente la perdita dell'informazione o semplicemente i messaggi ricevuti non sono gli stessi di quelli trasmessi.

Analoghi ragionamenti si possono fare anche sulla memorizzazione di informazione su un mezzo fisico (tipo un hard disk): quando è necessario rileggere quell'informazione, potrebbe capitare che essa abbia subito delle modifiche e bisognerebbe reinterpretarla; in questo caso invece di trasmettitore e di ricevente si parla di scrittore e lettore, ma la sostanza non cambia e la teoria sui canali rimane invariata.

Definizione di canale Un canale di comunicazione è un modello matematico che comprende il canale fisico e tutto ciò che sfugge al perfetto controllo tra trasmettitore TX e ricevitore RX.

Ogni canale è caratterizzato da:

dovuto ai disturbi
sul canale fisico

variabile casuale, perché pesca
da un alfabeto di messaggi
messaggio trasmesso

variabile casuale
messaggio ricevuto

- Un alfabeto di messaggi che possono essere inviati, descritti da una sorgente X.
- Un alfabeto di messaggi che possono essere ricevuti, descritti da una sorgente Y.
- Un legame probabilistico tra ingresso e uscita, ossia la probabilità di ricevere un determinato y_i sapendo che è stato inviato un certo x_j .



- X e Y possono avere alfabeti o discreti
- ingresso-uscita continuo/discreto
- canali con memoria/senza memoria

Classificazione dei canali In base alla numerosità degli alfabeti si possono avere diversi tipi di canali, infatti sia l'alfabeto di trasmissione che quello di ricezione possono essere sia continui che discreti.

nel tempo

4.2. Mutua informazione

Introduzione Bisogna trovare un parametro che indichi la bontà di un canale indipendentemente dalla quantità di informazione inviata: il primo modo che viene in mente è di usare l'entropia dell'uscita $H(Y)$, ma questa misura dipende fortemente da quanta informazione viene inviata e quindi non è un buon indicatore.

Si consideri per esempio una sorgente di trasmissione X che trasmette sempre e solo lo stesso simbolo e quindi sta trasmettendo 0 bit di informazione, in questo caso l'entropia della variabile di ricezione sarà anch'essa nulla, ma questo non da nessuna informazione sulla bontà del canale perché non è colpa del canale se $H(Y)$ è nulla.

Per risolvere questo problema si potrebbe pensare di massimizzare l'informazione inviata in modo che $H(Y)$ indichi l'informazione massima ricevibile, ma anche questo non è un buon indicatore.

Si consideri ad esempio una sorgente che invia simboli in modo equiprobabile, e quindi massimizza l'informazione inviata, e che il canale vari con una certa probabilità ϵ un simbolo in un altro simbolo (scelto in

$$X = \{x_1, x_2\} \Rightarrow H(x) \text{ max}$$

$$P_X = \{p_1, p_2\}$$

4. Capacità di canale

maniera equiprobabile), in questo caso sull'uscita si riceveranno tutti i simboli in modo equiprobabile, ottenendo un'entropia $H(Y)$ massima per qualsiasi valore di ε , ma preso un determinato simbolo non si sa quale simbolo sia stato realmente inviato. Inoltre è abbastanza intuitivo pensare che si vuole avere un valore di ε basso in modo che la probabilità di ricevere il simbolo inviato è alta e quindi un indicatore deve dipendere da tale quantità e non è il caso di $H(Y)$.

Per trovare tale indicatore si introduce quindi il concetto di mutua informazione.

Definizione di mutua informazione Dato un canale di trasmissione si definisce mutua informazione $I(X; Y)$ la quantità:

$$I(X; Y) \triangleq H(X) - H(X|Y) = H(Y) - H(Y|X)$$

• informazione media portata dall'evento X sul canale, ossia indica quanto il suo esito è incerto
 • la quantità media di informazione trasmessa sul canale
 • incertezza di X avendo osservato Y
 • incertezza di Y avendo osservato X
 • quanto incertezza non c'è dopo aver osservato Y
 • se esiste incertezza che non stata catturata vuol dire che ho perso dell'informazione sul canale
 • perché quello che ho in uscita non corrisponde a quello che le ho inviato

Significato di mutua informazione Si è visto che $H(X|Y)$ indica l'informazione media che porta X quando si è già osservato Y, ossia indica quanto incerto è l'esito dell'evento X (ossia il simbolo trasmesso) avendo osservato quello di Y (ossia quello ricevuto). In un canale ottimo si vuole che l'esito di X sia totalmente certo, ossia che non porti nessuna informazione, dopo aver osservato Y e quindi che $H(X|Y)$ sia il più piccolo possibile.

L'entropia $H(X)$ indica l'informazione media portata da X ossia indica quanto il suo esito è incerto; osservando Y questa incertezza diminuisce diventando $H(X|Y)$ e quindi la differenza $H(X) - H(X|Y)$ indica di quanto la variabile X sia meno incerta avendo osservato l'esito di Y.

In un canale ottimo si desidera conoscere esattamente l'esito di X avendo osservato Y e quindi si vuole che la sua incertezza si annulli e di conseguenza si vuole che la differenza $H(X) - H(X|Y)$ sia massima.

Per questo motivo si definisce la mutua informazione $I(X; Y)$ che indica la quantità di incertezza sul simbolo inviato che scompare osservando il simbolo ricevuto.

Osservazioni

- La mutua informazione $I(X; Y)$ è data dalla differenza di due entropie e quindi si misura in bit, ma solitamente si usa l'unità di misura bit/uso canale ossia i bit di infomazione (o frazioni di esso) trasmessi ogni volta che si usa il canale.

- Precedentemente si è dimostrato che:

$$0 \leq H(X|Y) \leq H(X)$$

e quindi si ha che:

$$\text{Solo se } X \text{ e } Y \text{ sono indipendenti} \quad 0 \leq I(X; Y) \leq H(X) \quad \text{L'informazione che attraversa il canale è al massimo pari a quella dell'ingresso}$$

e dato che l'entropia massima di una variabile X è $\log M$ (dove M è la lunghezza del suo alfabeto) si ottiene:

$$0 \leq I(X; Y) \leq \log M$$

- Se $I(X; Y) = 0$ allora $H(X|Y) = H(X)$ e quindi Y non contiene informazione sulla variabile X e quindi non transita nessuna informazione sul canale.
- Se $I(X; Y) = H(X)$ allora $H(X|Y) = 0$ e quindi X e Y sono legate deterministicamente e quindi tutta l'informazione inviata viene ricevuta senza perdita.
- Dato che:

$$\begin{aligned} H(X, Y) &= H(X) + H(Y|X) = H(Y) + H(X|Y) \\ H(X) + H(Y|X) - H(Y) &= H(X|Y) \end{aligned}$$

e quindi:

$$\begin{aligned} I(X; Y) &= H(X) - H(X|Y) = \\ &= H(X) - H(X) - H(Y|X) + H(Y) = \\ &= H(Y) - H(Y|X) \end{aligned}$$

4. Capacità di canale

e quindi la mutua informazione si può scrivere anche invertendo X e Y : questa definizione è meno intuitiva della precedente, però è spesso molto più comoda nei calcoli.

Definizione di equivocazione Dato che $H(X)$ è la quantità di informazione inviata nel canale e $I(X; Y)$ è l'informazione ricevuta allora si può dire che l'informazione persa sul canale vale:

$$H(X) - I(X; Y) = H(X) - H(X) + H(X|Y) = H(X|Y)$$

quantità media di informazione
che emessa dal ricevitore

quantità di informazione
che transita sul canale

$$\begin{aligned} H(X|Y) &= H(X) + H(Y|X) \\ &= H(Y) + H(Y|X) \end{aligned}$$

e viene definita equivocazione.

Definizione di capacità del canale La capacità del canale è la massima mutua informazione ottenibile dal canale al variare delle probabilità della sorgente in ingresso, ossia:

$$C = \max_{P_X(X)} I(X; Y)$$

(biti Jm di canale)

e si misura in bit/uso canale come la mutua informazione.

Significato di capacità Come visto precedentemente, la mutua informazione indica l'informazione che transita nel canale e quindi potrebbe essere un buon indicatore della bontà del canale; è però legata alla quantità di informazione che la sorgente invia, la quale non dipende dal canale: per eliminare questa dipendenza dalla scelta della sorgente si definisce la capacità del canale come la massima mutua informazione ottenibile dal canale facendo variare la sorgente in ingresso.

4.3. Canali discreti

4.3.1. Canale BSC (Binary Symmetric Channel)

BSC(ϵ)

Definizione Questo canale è caratterizzato da una sorgente di trasmissione X binaria e una di ricezione Y anch'essa binaria in cui:

x	y	$P_{Y X}(y x)$	Note
0	0	$1 - \epsilon$	Probabilità di leggere uno 0 in uscita avendo inviato uno 0
0	1	ϵ	Probabilità di leggere uno 0 in uscita avendo inviato un 1
1	0	ϵ	Probabilità di leggere un 1 in uscita avendo inviato uno 0
1	1	$1 - \epsilon$	Probabilità di leggere un 1 in uscita avendo inviato un 1

$x = y = \{0, 1\}$

ingresso uscita discreti
possiedono lo stesso
alfabeto per cui quello che
mando dovrebbe essere
quello che ricevo

Quindi si può dire che in questo canale c'è una probabilità ϵ di ricevere il bit sbagliato e di conseguenza una probabilità $1 - \epsilon$ di ricevere il bit corretto.

Diagramma Dato che entrambi gli alfabeti X e Y sono discreti con un numero finito di elementi si può rappresentare tramite un grafo il funzionamento di questo canale, come mostrato in figura 4.1, che permette di comprenderne meglio il funzionamento.

Trasmettitore
 X Ricevitore
 Y

Diagramma di
transizione del
canale

Il diagramma è simmetrico
quello che possiedo sono le $P(Y|X)$

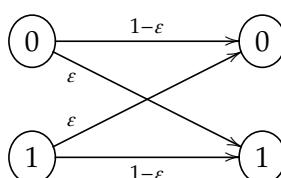


Figura 4.1.: Rappresentazione del modello BSC.

4. Capacità di canale

Calcolo entropia di ricezione $H(Y)$ Dato che la sorgente X è binaria si può generalizzare considerando $P_X(0) = p$ e $P_X(1) = 1 - p$ e ricordando che:

$$\sum_{i=1}^n P_{X_i}(x_i) \cdot P_{Y|X}(y_i|x_i) = \sum_{i=1}^n P_{X_i}(x_i) \cdot P_{Y|X}(y_i|0) + P_X(1) \cdot P_{Y|X}(y_i|1)$$

si ottiene che:

$$\begin{aligned} P_Y(0) &= P_X(0) \cdot P_{Y|X}(0|0) + P_X(1) \cdot P_{Y|X}(0|1) = \\ &= p \cdot (1 - \varepsilon) + (1 - p) \cdot \varepsilon = \\ &= p - p \cdot \varepsilon + \varepsilon - p \cdot \varepsilon = \\ &= p + \varepsilon - 2 \cdot p \cdot \varepsilon \end{aligned}$$

$$\begin{aligned} P_Y(1) &= P_X(0) \cdot P_{Y|X}(1|0) + P_X(1) \cdot P_{Y|X}(1|1) = \\ &= p \cdot \varepsilon + (1 - p) \cdot (1 - \varepsilon) = \\ &= p \cdot \varepsilon + 1 - p - \varepsilon + p \cdot \varepsilon = \\ &= 1 - (p + \varepsilon - 2 \cdot p \cdot \varepsilon) \end{aligned}$$

Giustamente si può notare che $P_Y(1) + P_Y(0) = 1$.

Conoscendo le probabilità si può ricavare facilmente $H(Y)$: infatti si può notare che Y è una sorgente binaria in cui $P_Y(0) = q$ e $P_Y(1) = 1 - q$ dove $q = p + \varepsilon - 2 \cdot p \cdot \varepsilon$ e quindi:

$$H(Y) = H_2[p + \varepsilon - 2 \cdot p \cdot \varepsilon]$$

Calcolo dell'entropia condizionata $H(Y|X)$ Per calcolare l'entropia condizionata $H(Y|X)$ bisogna conoscere le probabilità congiunte, ma queste si possono ricavare facilmente ricordando che:

$$P_{X,Y}(x,y) = P_{Y|X}(y|x) \cdot P_X(x)$$

si ricava che:

x	y	$P_{Y X}(y x)$	$P_X(x)$	$P_{X,Y}(x,y)$
0	0	$1 - \varepsilon$	p	$(1 - \varepsilon) \cdot p$
0	1	ε	p	$\varepsilon \cdot p$
1	0	ε	$1 - p$	$\varepsilon \cdot (1 - p)$
1	1	$1 - \varepsilon$	$1 - p$	$(1 - \varepsilon) \cdot (1 - p)$

• proviene dall'alfabeto
dal diagramma di transizione

$$\begin{aligned} \sum_{i=1}^n P_{X,Y}(x_i, y_i) \cdot \log \frac{1}{P_{Y|X}(y_i|x_i)} &= \\ = q \cdot \log \left(\frac{1}{q} \right) + (1-q) \cdot \log \left(\frac{1}{1-q} \right) & \end{aligned}$$

e quindi:

$$\begin{aligned} H(Y|X) &= \sum_{i=0}^1 \sum_{j=0}^1 P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{Y|X}(y_j|x_i)} = \\ &= (1 - \varepsilon) \cdot p \cdot \log \frac{1}{1 - \varepsilon} + \varepsilon \cdot p \cdot \log \frac{1}{\varepsilon} + \varepsilon \cdot (1 - p) \cdot \log \frac{1}{\varepsilon} + (1 - \varepsilon) \cdot (1 - p) \cdot \log \frac{1}{1 - \varepsilon} = \\ &= p \cdot \left((1 - \varepsilon) \cdot \log \frac{1}{1 - \varepsilon} + \varepsilon \cdot \log \frac{1}{\varepsilon} \right) + (1 - p) \cdot \left((1 - \varepsilon) \cdot \log \frac{1}{1 - \varepsilon} + \varepsilon \cdot \log \frac{1}{\varepsilon} \right) = \\ &= (p + 1 - p) \cdot \left((1 - \varepsilon) \cdot \log \frac{1}{1 - \varepsilon} + \varepsilon \cdot \log \frac{1}{\varepsilon} \right) = \\ &= H_2[\varepsilon] \end{aligned}$$

Calcolo della mutua informazione $I(X;Y)$ Dato che si conosce sia $H(Y)$ che $H(Y|X)$ conviene usare la formula meno intuitiva ricavata nelle osservazioni e quindi:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) = \\ &= H_2[p + \varepsilon - 2 \cdot p \cdot \varepsilon] - H_2[\varepsilon] \end{aligned}$$

$$\begin{aligned} H(Y) &= 1 \text{ bit} \\ H(Y|X) &= \sum_{x=0}^1 P_X(x) \cdot H(Y|x) \\ &= \sum_{x=0}^1 P_X(x) \cdot (\varepsilon \log \frac{1}{\varepsilon} + (1-\varepsilon) \log \frac{1}{1-\varepsilon}) \\ &= H_2(\varepsilon) \\ f(x,y) &= 1 - H_2(\varepsilon) \end{aligned}$$

Il triste caso degli 8 sempre neri.
come quando non sei abile mai.
Pensando bene il mio canale invierte tutti i dati per trasmettere, ma funziona
inverso che probabilistico

con probabilità di errore 0.1 di inviare un 0 e riceverne un 1. Il canale invierte tutti i dati per trasmettere, ma funziona inverso che probabilistico

con probabilità di errore 0.1 di inviare un 0 e riceverne un 1. Il canale invierte tutti i dati per trasmettere, ma funziona inverso che probabilistico

4. Capacità di canale

Calcolo dell'equivocazione $H(X|Y)$ Conoscendo la mutua informazione è facile ricavare l'equivocazione infatti:

$$\begin{aligned} I(X; Y) &= H(X) - H(X|Y) \\ H(X|Y) &= H(X) - I(X; Y) \\ H(X|Y) &= H_2[p] - H_2[p + \varepsilon - 2 \cdot p \cdot \varepsilon] + H_2[\varepsilon] \end{aligned}$$

$$I(X; Y) = H_2(p + \varepsilon - 2 \cdot p \cdot \varepsilon) - H_2[\varepsilon]$$

Calcolo della capacità del canale Per ricavare la capacità del canale bisogna trovare la distribuzione di probabilità di X tale da massimizzare la mutua informazione, quindi in questo caso bisogna:

rispetto a qualsiasi distribuzione di probabilità in ingresso

$$\begin{aligned} C &= \max_p I(X; Y) = \\ &= \max_p H_2[p + \varepsilon - 2 \cdot p \cdot \varepsilon] - H_2[\varepsilon] \end{aligned}$$

non dipende da p

Dato che il secondo termine non dipende da p bisogna massimizzare il primo, ed essendo che la funzione H_2 ha massimo in $\frac{1}{2}$:

$$\begin{aligned} p + \varepsilon - 2 \cdot p \cdot \varepsilon &= \frac{1}{2} \\ p \cdot (1 - 2 \cdot \varepsilon) &= \frac{1}{2} - \varepsilon \\ p &= \frac{1 - 2 \cdot \varepsilon}{2} \cdot \frac{1}{1 - 2 \cdot \varepsilon} \\ p &= \frac{1}{2} \end{aligned}$$

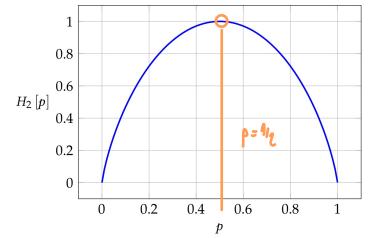


Figura 2.1.: Funzione $H_2[p]$.

da cui si ottiene che:

$$\begin{aligned} C &= H_2 \left[\frac{1}{2} + \varepsilon - 2 \cdot \frac{1}{2} \cdot \varepsilon \right] - H_2[\varepsilon] = \\ &= H_2 \left[\frac{1}{2} \right] - H_2[\varepsilon] = \\ &= 1 - H_2[\varepsilon] \end{aligned}$$

Osservazioni sulla capacità del canale La funzione della capacità è raffigurata nel grafico in figura 4.2 e si può notare che:

- Il caso peggiore è quando $\varepsilon = \frac{1}{2}$, per cui la capacità è nulla e quindi nel canale non passa nessuna informazione: in questa situazione preso un messaggio in uscita non si può dedurre nulla di come era quello trasmesso.
- Il caso migliore si ha quando c'è una relazione deterministica tra messaggio trasmesso e ricevuto e questo avviene in due casi:
 - Il messaggio arriva sempre corretto e quindi $\varepsilon = 0$.
 - Il messaggio arriva sempre sbagliato e quindi $\varepsilon = 1$, perché sapendo che il messaggio è sempre sbagliato si può sempre ricavare il messaggio giusto.
- La capacità del canale cala drasticamente allontanandosi dai due casi ottimi.

4. Capacità di canale

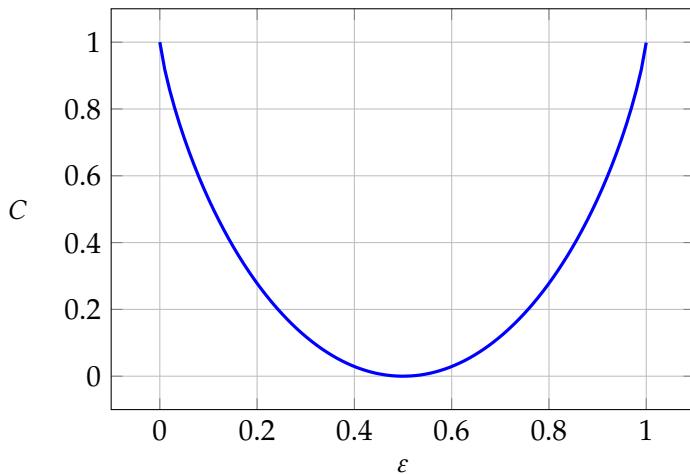


Figura 4.2.: Capacità di un canale BSC.

4.3.2. Canale BEC (Binary Erasure Channel)

BEC(ε)

Definizione Questo canale è caratterizzato da una sorgente di trasmissione X binaria e una di ricezione Y di 3 simboli $\{0, 1, E\}$.

$X = \{0, 1\}$
 $Y = \{0, 1, E\}$

dove E è una cancellazione detta erasure

x	y	$P_{Y X}(y x)$	Note
0	0	$1 - \epsilon$	Probabilità di leggere uno 0 in uscita avendo inviato uno 0
0	E	ϵ	Probabilità di leggere una E in uscita avendo inviato uno 0
0	1	0	Inviando uno 0 non è possibile ricevere un 1
1	0	0	Inviando un 1 non è possibile ricevere uno 0
1	E	ϵ	Probabilità di leggere una E in uscita avendo inviato un 1
1	1	$1 - \epsilon$	Probabilità di leggere un 1 in uscita avendo inviato un 1

Quindi si può dire che questo canale non può sbagliare, ma può perdere dei messaggi con una probabilità ϵ , che equivale a ricevere il messaggio E .

Diagramma Dato che entrambi gli alfabeti X e Y sono discreti con un numero finito di elementi si può rappresentare tramite un grafo il funzionamento di questo canale, come mostrato in figura 4.3, che permette di comprenderne meglio il funzionamento.

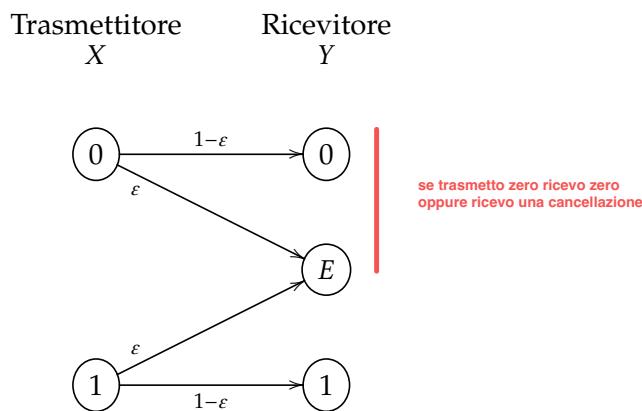


Figura 4.3.: Rappresentazione del modello BEC.

4. Capacità di canale

Calcolo entropia di ricezione $H(Y)$ Dato che la sorgente X è binaria si può generalizzare considerando $P_X(0) = p$ e $P_X(1) = 1 - p$ e ricordando che:

$$P_Y(y_i) = P_X(0) \cdot P_{Y|X}(y_1|0) + P_X(1) \cdot P_{Y|X}(y_1|1)$$

si ottiene che:

$$\begin{aligned} P_Y(0) &= P_X(0) \cdot P_{Y|X}(0|0) + P_X(1) \cdot P_{Y|X}(0|1) = \\ &= p \cdot (1 - \varepsilon) + (1 - p) \cdot 0 = \\ &= p \cdot (1 - \varepsilon) \end{aligned}$$

$$\begin{aligned} P_Y(E) &= P_X(0) \cdot P_{Y|X}(E|0) + P_X(1) \cdot P_{Y|X}(E|1) = \\ &= p \cdot \varepsilon + (1 - p) \cdot \varepsilon = \\ &= \varepsilon \cdot (p + 1 - p) = \\ &= \varepsilon \end{aligned}$$

$$\begin{aligned} P_Y(1) &= P_X(0) \cdot P_{Y|X}(1|0) + P_X(1) \cdot P_{Y|X}(1|1) \\ &= p \cdot 0 + (1 - p) \cdot (1 - \varepsilon) = \\ &= (1 - p) \cdot (1 - \varepsilon) \end{aligned}$$

giustamente si può notare che:

$$\begin{aligned} P_Y(0) + P_Y(E) + P_Y(1) &= p \cdot (1 - \varepsilon) + \varepsilon + (1 - p) \cdot (1 - \varepsilon) = \\ &= (1 - \varepsilon) \cdot (p + 1 - p) + \varepsilon = \\ &= (1 - \varepsilon) + \varepsilon = \\ &= 1 \end{aligned}$$

Conoscendo le probabilità si può ricavare facilmente $H(Y)$:

$$\begin{aligned} H(Y) &= p \cdot (1 - \varepsilon) \cdot \log \frac{1}{p \cdot (1 - \varepsilon)} + \varepsilon \cdot \log \frac{1}{\varepsilon} + (1 - p) \cdot (1 - \varepsilon) \cdot \log \frac{1}{(1 - p) \cdot (1 - \varepsilon)} = \\ &= (1 - \varepsilon) \cdot \left(p \cdot \log \frac{1}{p} + p \cdot \log \frac{1}{1 - \varepsilon} + (1 - p) \cdot \log \frac{1}{(1 - p)} + (1 - p) \cdot \log \frac{1}{1 - \varepsilon} \right) + \varepsilon \cdot \log \frac{1}{\varepsilon} = \\ &= (1 - \varepsilon) \cdot \left(p \cdot \log \frac{1}{p} + (1 - p) \cdot \log \frac{1}{(1 - p)} + \log \frac{1}{1 - \varepsilon} \cdot (p + 1 - p) \right) + \varepsilon \cdot \log \frac{1}{\varepsilon} = \\ &= (1 - \varepsilon) \cdot \underbrace{\left(p \cdot \log \frac{1}{p} + (1 - p) \cdot \log \frac{1}{(1 - p)} \right)}_{H_2[p]} + \underbrace{(1 - \varepsilon) \cdot \log \frac{1}{1 - \varepsilon} + \varepsilon \cdot \log \frac{1}{\varepsilon}}_{H_2[\varepsilon]} = \\ &= (1 - \varepsilon) \cdot H_2[p] + H_2[\varepsilon] \end{aligned}$$

Dato che questa espressione non è semplice è meglio procedere calcolando prima l'equivocazione.

Calcolo dell'equivocazione $H(X|Y)$ Per calcolare l'entropia condizionata $H(X|Y)$ bisogna conoscere le probabilità congiunte, ma queste si possono ricavare facilmente ricordando che:

$$P_{X,Y}(x,y) = P_{Y|X}(y|x) \cdot P_X(x)$$

Inoltre bisogna calcolare le probabilità condizionate $P_{X|Y}(x|y)$ che possono ricavare facilmente ricordando che:

$$P_{X|Y}(x|y) = \frac{P_{X,Y}(x,y)}{P_Y(y)}$$

quindi:

4. Capacità di canale

x	y	$P_{Y X}(y x)$	$P_X(x)$	$P_{X,Y}(x,y)$	$P_Y(y)$	$P_{X Y}(x y)$
0	0	$1 - \varepsilon$	p	$p \cdot (1 - \varepsilon)$	$p \cdot (1 - \varepsilon)$	1
0	E	ε	p	$p \cdot \varepsilon$	ε	p
0	1	0	p	0	$(1 - p) \cdot (1 - \varepsilon)$	0
1	0	0	$1 - p$	0	$p \cdot (1 - \varepsilon)$	0
1	E	ε	$1 - p$	$(1 - p) \cdot \varepsilon$	ε	$1 - p$
1	1	$1 - \varepsilon$	$1 - p$	$(1 - p) \cdot (1 - \varepsilon)$	$(1 - p) \cdot (1 - \varepsilon)$	1

e quindi:

$$\begin{aligned}
H(X|Y) &= \sum_{i=0}^1 \sum_{j=0}^1 P_{X,Y}(x_i, y_j) \cdot \log \frac{1}{P_{X|Y}(x_i|y_j)} = \\
&= p \cdot (1 - \varepsilon) \cdot \log \frac{1}{p} + p \cdot \varepsilon \cdot \log \frac{1}{p} + 0 + 0 + (1 - p) \cdot \varepsilon \cdot \log \frac{1}{1-p} + (1 - p) \cdot (1 - \varepsilon) \cdot \log \frac{1}{1-p} = \\
&= \varepsilon \cdot \left(p \cdot \log \frac{1}{p} + (1 - p) \cdot \log \frac{1}{1-p} \right) = \\
&= \varepsilon \cdot H_2[p]
\end{aligned}$$

Calcolo della mutua informazione $I(X; Y)$ Dato che si conosce l'equivocazione conviene usare la formula della definizione e quindi:

$$\begin{aligned}
I(X; Y) &= H(X) - H(X|Y) = \\
&= H_2[p] - \varepsilon \cdot H_2[p] = \\
&= (1 - \varepsilon) \cdot H_2[p]
\end{aligned}$$

Calcolo della capacità del canale Per ricavare la capacità del canale bisogna trovare la distribuzione di probabilità di X tale da massimizzare la mutua informazione, quindi in questo caso bisogna:

$$\begin{aligned}
C &= \max_p I(X; Y) = \\
&= \max_p \underline{(1 - \varepsilon)} \cdot H_2[p] \quad \text{Costante moltiplicativa che non dipende da } p
\end{aligned}$$

quindi bisogna massimizzare la funzione $H_2[p]$ che è massima quando $p = \frac{1}{2}$, ottenendo:

$$C = 1 - \varepsilon$$

Osservazioni sulla capacità del canale La funzione della capacità è raffigurata nel grafico in figura 4.4 e si può notare che:

- Il caso peggiore si ha con $\varepsilon = 1$ ossia quando tutti i messaggi vengono cancellati e quindi ovviamente non arriva nessuna informazione.
- Il caso migliore si ha con $\varepsilon = 0$ ossia quando tutti i messaggi arrivano.
- A differenza del canale BSC spostandosi dal caso ottimo la capacità varia in maniera lineare; questo è dovuto al fatto che in questo tipo di canale se arriva un messaggio «leggibile» (0 o 1) si è certi di quale sia il messaggio inviato.

4. Capacità di canale

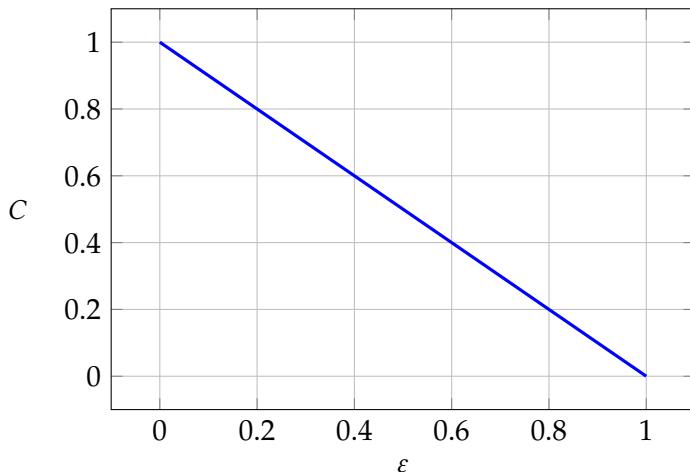


Figura 4.4.: Capacità di un canale BEC.

4.4. Canali continui

4.4.1. Introduzione alle variabili casuali continue

Nei canali continui almeno una delle sorgenti è continua e quindi per poterle analizzare bisogna utilizzare delle variabili casuali continue invece di quelle discrete usate finora; è necessario scrivere le definizioni date per le variabili discrete anche per quelle continue.

Variabili casuali continue Le variabili casuali continue sono caratterizzate da una funzione di densità che solitamente si indica con la lettera p minuscola da cui è possibile ricavare la probabilità che la variabile assuma un valore compreso in un determinato range. Per esempio data la variabile casuale continua A con funzione di densità continua p_A la probabilità che la variabile A assuma un valore compreso tra r e t è:

$$P(r \leq A \leq t) = \int_r^t p_A(a) da$$

Osservazioni

- Come per il caso discreto tutte le probabilità devono essere comprese tra 0 e 1 e somma delle probabilità di tutti gli eventi deve essere 1 e quindi:

$$\int_{-\infty}^{+\infty} p_A(a) da = 1$$

- NB** • Anche se le varie probabilità devono sempre essere inferiori a 1 non è detto che lo sia anche la funzione di densità che invece può assumere qualsiasi valore positivo.

Valore atteso delle variabili continue Come per le variabili continue si può definire il valore atteso, l'unica differenza è che invece di essere una sommatoria è un'integrale e quindi si definisce:

$$\mathbb{E}_A [f(a)] = \int_{-\infty}^{+\infty} p_A(a) \cdot f(a) da$$

In particolare esistono due valori attesi d'interesse:

4. Capacità di canale

- Il valore atteso μ_A :

$$\mu_A = \mathbb{E}_A [a] = \int_{-\infty}^{+\infty} p_A(a) \cdot a \, da$$

che indica il valore intorno a cui la variabile si sviluppa.

- La varianza σ_A^2 :

$$\sigma_A^2 = \mathbb{E}_A [(a - \mu)^2] = \int_{-\infty}^{+\infty} p_A(a) \cdot (a - \mu)^2 \, da$$

che indica quanto la variabile si scosta dal valore atteso.

Funzione di densità congiunta Come per le variabili casuali discrete esiste un concetto di probabilità congiunta anche nel caso continuo. Date due variabili A e B si definisce la funzione di densità congiunta come la funzione di densità che indica le probabilità che **le variabili A e B siano interne a un determinato range e si indica con:**

$$p_{A,B}(a, b)$$

e vale:

$$P(a_1 \leq A \leq a_2, b_1 \leq B \leq b_2) = \int_{a_1}^{a_2} \left[\int_{b_1}^{b_2} p_{A,B}(a, b) \, db \right] da$$

e come per il caso scalare vale:

$$p_A(a) = \int_{-\infty}^{+\infty} p_{A,B}(a, b) \, db$$

fissato a integro su tutti i valori possibili di b

Questa definizione si può generalizzare a più variabili casuali. Inoltre può capitare il caso in cui una delle due variabili sia discreta: in quel caso si può sostituire l'integrale con una sommatoria.

Funzione di densità condizionata Come per le variabili casuali discrete esiste un concetto di probabilità condizionata. Date due variabili A e B si definisce la funzione di densità condizionata come la funzione di densità che indica la probabilità che A sia all'interno di un range avendo già osservato l'esito dell'evento B e si indica con:

$$p_{A|B}(a|b)$$

e come per il caso discreto vale:

$$p_A(a) = p_{A|B}(a|b) \cdot p_B(b)$$

Variabile gaussiana La variabile casuale gaussiana o normale è una variabile casuale N che si definisce a partire dalla sua media μ_N e dalla sua varianza σ_N^2 con una funzione di densità:

$$p_Z(a) = \frac{1}{\sqrt{2 \cdot \pi \cdot \sigma_N^2}} \cdot e^{-\frac{(a-\mu_N)^2}{2 \cdot \sigma_N^2}} = Z_{\mu_N, \sigma_N^2}(a)$$

$$\mu = E(Y)$$

$$\sigma^2 = \text{Var}(Y) = E[(Y - \mu)^2]$$

La funzione $Z_{0,1}(a)$ è mostrata in figura 4.5.

4. Capacità di canale

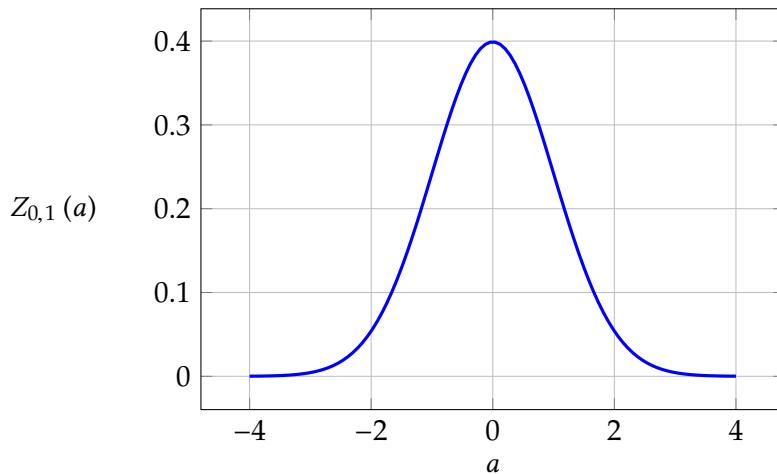
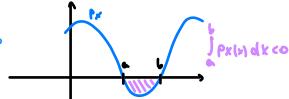


Figura 4.5.: Funzione di densità della variabile gaussiana.

Entropia L'entropia di una sorgente X si definisce come quella discreta tramite un valore atteso:

$$H(X) = \mathbb{E}_X \left[\log \frac{1}{p_X(x)} \right] = \int_{-\infty}^{+\infty} p_X(x) \cdot \log \frac{1}{p_X(x)} dx$$

- la funzione di densità può assumere qualsiasi valore, la restrizione rimane che l'intervallo infinito sia uguale a 1
- il problema rimane il logaritmo



Bisogna notare che a differenza del caso discreto questo valore non ha significato fisico: dato che $p_A(a)$ può assumere valori superiori a 1 questo valore può essere anche negativo.

non è detto che $H(Y) \geq 0$, mentre resta vero che $H(Y) - H(Y|X) \geq 0$

Entropia condizionata L'entropia condizionata $H(X|Y)$ si definisce in modo analogo a quella discreta tramite un valore atteso:

$$\begin{aligned} H(X|Y) &= \mathbb{E}_{X,Y} \left[\log \frac{1}{p_{X|Y}(x|y)} \right] = \\ &= \int_{-\infty}^{+\infty} \left[\int_{-\infty}^{+\infty} p_{X,Y}(x,y) \cdot \log \frac{1}{p_{X|Y}(x|y)} dx \right] dy = \\ &= \int_{-\infty}^{+\infty} p_Y(y) \cdot \left[\int_{-\infty}^{+\infty} p_{X|Y}(x|y) \cdot \log \frac{1}{p_{X|Y}(x|y)} dx \right] dy \end{aligned}$$

Se il valore di Y è discreto diventa:

$$H(X|Y) = \sum_{i=0}^M P_Y(y_i) \cdot \left[\int_{-\infty}^{+\infty} p_{X|Y}(x|y_i) \cdot \log \frac{1}{p_{X|Y}(x|y_i)} dx \right]$$

Mutua informazione e capacità del canale Data la definizione di entropia condizionata continua la mutua informazione e la capacità del canale si definiscono in modo analogo al caso discreto.

4. Capacità di canale

Entropia di una variabile gaussiana Sia X una variabile casuale gaussiana generica con funzione di densità Z_{μ, σ^2} allora:

$$\begin{aligned}
 H(X) &= \int_{-\infty}^{+\infty} Z_{\mu, \sigma^2}(x) \cdot \log \frac{1}{Z_{\mu, \sigma^2}(x)} dx = \\
 &= \int_{-\infty}^{+\infty} Z_{\mu, \sigma^2}(x) \cdot \log \frac{1}{\frac{1}{\sqrt{2 \cdot \pi \cdot \sigma^2}} \cdot e^{-\frac{(x-\mu)^2}{2 \cdot \sigma^2}}} dx = \\
 &= \int_{-\infty}^{+\infty} Z_{\mu, \sigma^2}(x) \cdot \log \left(\sqrt{2 \cdot \pi \cdot \sigma^2} \cdot e^{\frac{(x-\mu)^2}{2 \cdot \sigma^2}} \right) dx = \\
 &= \int_{-\infty}^{+\infty} Z_{\mu, \sigma^2}(x) \cdot \left(\frac{1}{2} \cdot \log(2 \cdot \pi \cdot \sigma^2) + \frac{(x-\mu)^2}{2 \cdot \sigma^2} \cdot \log e \right) dx = \\
 &= \frac{1}{2} \cdot \log(2 \cdot \pi \cdot \sigma^2) \cdot \underbrace{\int_{-\infty}^{+\infty} Z_{\mu, \sigma^2}(x) dx}_{1} + \frac{\log e}{2 \cdot \sigma_N^2} \cdot \underbrace{\int_{-\infty}^{+\infty} Z_{\mu, \sigma^2}(x) \cdot (x-\mu)^2 dx}_{\sigma_N^2} = \\
 &= \frac{1}{2} \cdot \log(2 \cdot \pi \cdot \sigma^2) + \frac{\log e}{2 \cdot \sigma^2} = \\
 &= \frac{1}{2} \cdot (\log(2 \cdot \pi \cdot \sigma^2) + \log e) = \\
 &= \frac{1}{2} \cdot \log(2 \cdot e \cdot \pi \cdot \sigma^2)
 \end{aligned}$$

quindi l'entropia di una gaussiana non dipende dal suo valore atteso ma solo dalla sua varianza, inoltre si nota che un aumento della varianza comporta un aumento dell'entropia.

Massimizzazione dell'entropia a pari varianza Nel caso discreto si è visto che una sorgente a pari cardinalità dell'alfabeto massimizza l'entropia quando tutti gli eventi sono equiprobabili; esiste un caso analogo anche nel continuo: infatti a pari varianza σ^2 la gaussiana massimizza l'entropia. Questo si può dimostrare calcolando la differenza tra l'entropia di una variabile casuale generica Y di varianza σ^2 e valore atteso μ e quella di una gaussiana X avente anch'essa varianza σ^2 e valore atteso μ .

$$\begin{aligned}
 H(Y) - H(X) &= \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{1}{p_Y(y)} dy - \int_{-\infty}^{+\infty} Z_{\mu, \sigma^2}(x) \cdot \log \frac{1}{Z_{\mu, \sigma^2}(x)} dx = \\
 &= \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{1}{p_Y(y)} dy - \frac{1}{2} \cdot \log(2 \cdot e \cdot \pi \cdot \sigma^2)
 \end{aligned}$$

H(Y) è massima fissata la varianza se la densità di probabilità è gaussiana

Si può notare che, ripetendo i passaggi fatti nel calcolo dell'entropia della gaussiana:

$$\begin{aligned}
 \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{1}{Z_{\mu, \sigma^2}(y)} dy &= \frac{\log(2 \cdot \pi \cdot \sigma^2)}{2} \cdot \underbrace{\int_{-\infty}^{+\infty} p_Y(y) dx}_{1} + \frac{\log e}{2 \cdot \sigma_N^2} \cdot \underbrace{\int_{-\infty}^{+\infty} p_Y(y) \cdot (y-\mu)^2 dx}_{\sigma^2} = \\
 &= \frac{\log(2 \cdot \pi \cdot \sigma^2)}{2} + \frac{\log e}{2 \cdot \sigma^2} = \\
 &= \frac{1}{2} \cdot \log(2 \cdot e \cdot \pi \cdot \sigma^2)
 \end{aligned}$$

4. Capacità di canale

Per questo motivo vale:

$$\begin{aligned}
 H(Y) - H(X) &= \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{1}{p_Y(y)} dy - \frac{1}{2} \cdot \log (2 \cdot e \cdot \pi \cdot \sigma^2) = \\
 &= \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{1}{p_Y(y)} dy - \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{1}{Z_{\mu, \sigma^2}(y)} dy = \\
 &= \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{Z_{\mu, \sigma^2}(y)}{p_Y(y)} dy
 \end{aligned}$$

indipendentemente dalla forma della distribuzione nella dimostrazione sopra è 1

$$\frac{\log(2 \cdot \pi \cdot \sigma^2)}{2} \int_{-\infty}^{+\infty} p_Y(y) dy + \frac{\log e}{2 \cdot \sigma_N^2} \int_{-\infty}^{+\infty} p_Y(y) \cdot (y - \mu)^2 dy =$$

Ricordando che $\log x \leq (x - 1) \cdot \log e$ si ottiene:

$$\begin{aligned}
 H(Y) - H(X) &= \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{Z_{\mu, \sigma^2}(y)}{p_Y(y)} dy \leq \text{Lnx} \leq x - 1 \\
 &\leq \int_{-\infty}^{+\infty} p_Y(y) \cdot \left(\frac{Z_{\mu, \sigma^2}(y)}{p_Y(y)} - 1 \right) \cdot \log e dy = \\
 &= \log e \cdot \left(\int_{-\infty}^{+\infty} p_Y(y) \cdot \frac{Z_{\mu, \sigma^2}(y)}{p_Y(y)} dy - \int_{-\infty}^{+\infty} p_Y(y) dy \right) = \\
 &= \log e \cdot (1 - 1) = \\
 &= 0
 \end{aligned}$$

e quindi:

$$\begin{aligned}
 H(Y) - H(X) &\leq 0 \\
 H(Y) &\leq H(X)
 \end{aligned}$$

e quindi la variabile gaussiana massimizza l'entropia a pari varianza e pari valore atteso. Inoltre si può notare che se si prendesse una variabile casuale generica W con varianza σ e valore atteso $\mu_W \neq \mu$ allora:

$$H(W) \leq H(Z_{\mu_W, \sigma}) = H(Z_{\mu, \sigma})$$

e quindi la variabile gaussiana massimizza l'entropia anche solo a pari varianza e con valore atteso diverso.

Entropia condizionata di variabili additive indipendenti Si supponga di avere due variabili casuali indipendenti X e N e una terza definita come $Y = X + N$ e di voler ricavare l'entropia condizionata $H(Y|X)$. Dato che $N = Y - X$ vale che:

$$p_{Y|X}(y|x) = p_N(y-x|x) \quad \begin{array}{l} \text{osservo } y \text{ dato che conosco } x \\ \text{osservare } y - x \text{ è la medesima cosa di} \\ \text{quello sopra perché io conosco già } x \end{array} \quad \begin{array}{l} y = Y + N \\ y = y - x \end{array} \quad \begin{array}{l} \text{con } X, N \\ \text{indipendenti} \end{array}$$

perché la y vale un determinato valore solo se N assume il valore $y - x$, ma N e X sono indipendenti e quindi:

$$p_{Y|X}(y|x) = p_N(y-x|x) = p_N(y-x)$$

mostra che la distribuzione condizionata di Y dato X è semplicemente la distribuzione di N traslata di x

$$\begin{aligned}
 p_{Y|X}(y|x) &= p_{N|X}(y-x|x) \\
 &= p_{N|X}(N=y-x|x) \\
 &= p_N(N|x) \\
 &= p_N(N) = p_N(y-x)
 \end{aligned}$$

Ricavando l'entropia condizionata si ottiene:

$$\begin{aligned}
 H(Y|X) &= \int_{-\infty}^{+\infty} p_X(x) \cdot \left[\int_{-\infty}^{+\infty} p_{Y|X}(y|x) \cdot \log \frac{1}{p_{Y|X}(y|x)} dy \right] dx \\
 &= \int_{-\infty}^{+\infty} p_X(x) \cdot \left[\int_{-\infty}^{+\infty} p_N(y-x) \cdot \log \frac{1}{p_N(y-x)} dy \right] dx
 \end{aligned}$$

4. Capacità di canale

Facendo il cambio di variabile $n = y - x$ nell'integrale interno i valori di integrazione non cambiano e si ottiene:

$$\begin{aligned}
 H(Y|X) &= \int_{-\infty}^{+\infty} p_X(x) \cdot \left[\int_{-\infty}^{+\infty} p_N(y-x) \cdot \log \frac{1}{p_N(y-x)} dy \right] dx = \\
 &= \int_{-\infty}^{+\infty} p_X(x) \cdot \left[\int_{-\infty}^{+\infty} p_N(n) \cdot \log \frac{1}{p_N(n)} dn \right] dx = \\
 &= \int_{-\infty}^{+\infty} p_X(x) \cdot H(N) dx = \\
 &= H(N) \cdot \int_{-\infty}^{+\infty} p_X(x) \cdot dx = \\
 &= H(N)
 \end{aligned}$$

Questo è un risultato generale che vale anche nel caso in cui la variabile X sia discreta: basta ripetere i passaggi sostituendo l'integrale esterna (quella su x) con una sommatoria di tutti i possibili valori di X .

Questo semplifica parecchio il calcolo della mutua informazione tra X e Y infatti:

$$I(X; Y) = H(Y) - H(Y|X) = H(Y) - H(N)$$

e dato che N e X sono indipendenti $H(N)$ non dipende da X e quindi per calcolare la capacità basta massimizzare l'entropia di Y .

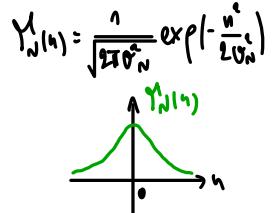
4.4.2. Canale AGN (Additive Gaussian Noise) con trasmettitore continuo (analogico) AGN

Definizione In questo canale si aggiunge un rumore gaussiano N additivo sul segnale inviato e quindi

$$Y = X + N$$

con le seguenti ipotesi:

- X è una variabile casuale continua;
- il rumore N e il segnale trasmesso X sono scorrelati;
- il rumore N ha valore atteso nullo: $\mu_N = 0$.



Calcolo della varianza di Y Dalla definizione di varianza si ottiene che:

$$\begin{aligned}
 \text{Var}(Y) &= \mathbb{E}[(Y - \mathbb{E}[Y])^2] \\
 &= \mathbb{E}[Y^2 - 2\mathbb{E}[Y]\mathbb{E}[Y] + (\mathbb{E}[Y])^2] \\
 &= \mathbb{E}[Y^2] - 2\mathbb{E}[Y]\mathbb{E}[Y] + (\mathbb{E}[Y])^2 \\
 &= \mathbb{E}[Y^2] - 2(\mathbb{E}[Y])^2 + (\mathbb{E}[Y])^2 \\
 &= \mathbb{E}[Y^2] - (\mathbb{E}[Y])^2
 \end{aligned}$$

$$\begin{aligned}
 \sigma_Y^2 &= \mathbb{E}[y^2] - (\mathbb{E}[y])^2 = \underbrace{(\mathbb{E}(x+n))^2}_{=\mathbb{E}(x)^2 + \mathbb{E}(n)^2} - (\mathbb{E}(x) + \mathbb{E}(n))^2 = \underbrace{\mathbb{E}(x)^2 + \mathbb{E}(n)^2}_{\text{scorrelati}} + 2\mathbb{E}(x)\mathbb{E}(n) = \\
 &= \mathbb{E}[(x+n)^2] - (\mathbb{E}[x+n])^2 = \\
 &= \underbrace{\mathbb{E}[x^2]}_{\sigma_X^2} - \underbrace{\mathbb{E}[x]^2}_{\sigma_X^2} + \underbrace{\mathbb{E}[n^2]}_{\sigma_N^2} + 2 \cdot \underbrace{\mathbb{E}[x \cdot n]}_0 = \\
 &= \sigma_X^2 + \sigma_N^2
 \end{aligned}$$

$$\begin{aligned}
 \text{Var}_N &= \text{Varianza di } N \\
 \mathbb{E}[n^2] &= \int_{-\infty}^{+\infty} n^2 \cdot \mathbb{P}_N(n) dn
 \end{aligned}$$

Calcolo della mutua informazione Dato che X e N sono indipendenti vale che:

$$I(Y; X) = H(Y) - H(N)$$

Dato che il rumore N è gaussiano si ottiene:

$$I(Y; X) = H(Y) - \frac{1}{2} \cdot \log(2 \cdot e \cdot \pi \cdot \sigma_N^2)$$

4. Capacità di canale

Calcolo della capacità Per calcolare la capacità bisogna massimizzare la mutua informazione che in questo caso corrisponde a massimizzare l'entropia di $H(Y)$. Dato che Y è una variabile a varianza costante pari a $\sigma_X^2 + \sigma_N^2$, la si può massimizzare facendo diventare la variabile Y una gaussiana. Questo può avvenire ponendo X gaussiana, infatti la somma di più gaussiane è ancora una gaussiana. Quindi si ottiene:

$$\begin{aligned}
 C &= \frac{1}{2} \cdot \log \left(2 \cdot e \cdot \pi \cdot (\sigma_X^2 + \sigma_N^2) \right) - \frac{1}{2} \cdot \log \left(2 \cdot e \cdot \pi \cdot \sigma_N^2 \right) = \\
 &= \frac{1}{2} \cdot \log \frac{2 \cdot e \cdot \pi \cdot (\sigma_X^2 + \sigma_N^2)}{2 \cdot e \cdot \pi \cdot \sigma_N^2} = \\
 &= \frac{1}{2} \cdot \log \frac{\sigma_X^2 + \sigma_N^2}{\sigma_N^2} = \\
 &= \frac{1}{2} \cdot \log \left(1 + \frac{\sigma_X^2}{\sigma_N^2} \right)
 \end{aligned}$$

dove il termine $\frac{\sigma_X^2}{\sigma_N^2}$ si chiama rapporto segnale rumore e solitamente si misura in decibel.

Osservazioni sulla capacità Il grafico di C al variare del rapporto segnale rumore (espresso in decibel) è rappresentato in figura 4.6; si può notare che:

- Più il rapporto segnale rumore è basso più si abbassa la capacità del canale, come è intuitivo pensare dato che se il rapporto è basso allora il rumore è molto rilevante rispetto al segnale.
- Più il rapporto è alto più la capacità del canale è alta, come è intuitivo pensare visto che il rumore diventa sempre più piccolo rispetto al segnale.
- Questo modello è molto utilizzato perché rappresenta la modellizzazione del trasferimento analogico con rumore elettronico.

(bit/jo di canale)

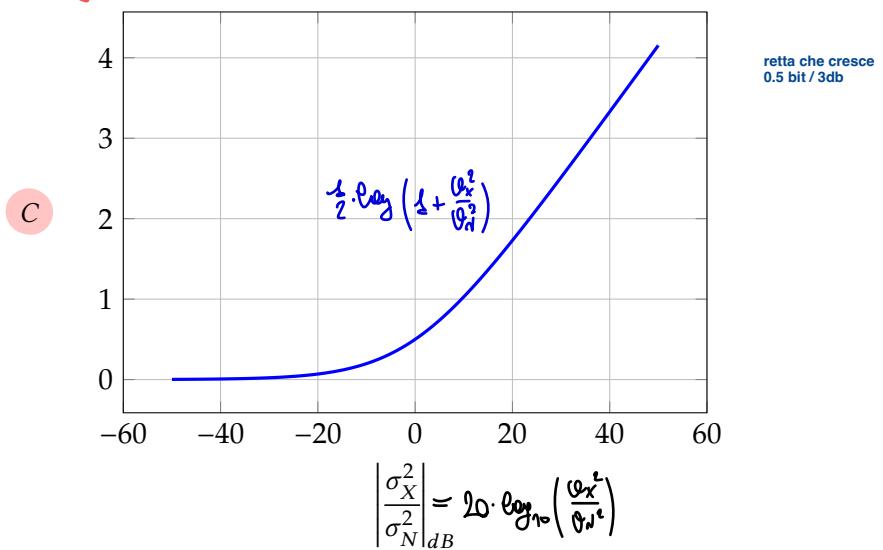


Figura 4.6.: Capacità di un canale AGN con trasmettitore continuo al variare del rapporto segnale rumore.

4.4.3. Canale AGN (Additive Gaussian Noise) con trasmettitore discreto (digitale)

Definizione In questo canale si aggiunge un rumore gaussiano N additivo sul segnale inviato e quindi

$$Y = X + N \quad N \sim \mathcal{N}(0, \sigma_N^2)$$

con le seguenti ipotesi:

4. Capacità di canale

- X è una variabile casuale discreta con un alfabeto di M simboli;
- il rumore N e il segnale trasmesso X sono scorrelati;
- il rumore N ha valore atteso nullo: $\mu_N = 0$.

Calcolo della probabilità p_Y Per la marginalità vale che:

$$p_Y(y) = \sum_{i=1}^M P_X(x_i) \cdot p_{Y|X}(y|x_i)$$

e dato che il rumore è additivo e indipendente da X vale che:

$$p_{Y|X}(y|x_i) = p_N(y - x_i)$$

e quindi:

$$p_Y(y) = \sum_{i=1}^M P_X(x_i) \cdot p_N(y - x_i)$$

Calcolo dell'entropia di Y Per la definizione si ha che:

$$H(Y) = \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{1}{p_Y(y)} dy$$

che non è integrabile analiticamente, ma solo numericamente.

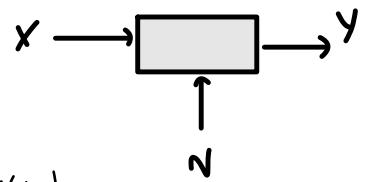
Calcolo della mutua informazione e della capacità Dato che X e N sono indipendenti vale che:

$$I(Y;X) = H(Y) - H(N)$$

Dato che non si possono fare calcoli analitici non si può scrivere meglio questa espressione, ma si può dedurre che anche in questo caso il valore di capacità dipende dal rapporto segnale rumore.

Osservazioni sulla capacità Prima di fare delle osservazioni si consideri X equiprobabile, ovvero con $P_X(x_i) = \frac{1}{M}$ e quindi:

$$\begin{aligned} p_Y(y) &= \sum_{i=1}^M \frac{1}{M} \cdot p_N(y - x_i) = \\ &= \frac{1}{M} \cdot \sum_{i=1}^M p_N(y - x_i) \end{aligned}$$



$$\begin{aligned} y &= x + n \\ p_{y|x} &= p_{n|x} \\ &= p_N(y-x) \\ H(y|x) &= \sum_y p_{y|x} \cdot \log \frac{1}{p_{y|x}} \\ &= \sum_y p_N(y-x) \cdot \log \frac{1}{p_N(y-x)} \\ &= \sum_n p_N(n) \cdot \log \frac{1}{p_N(n)} = H(n) = H(y|x) \end{aligned}$$

4. Capacità di canale

L'entropia diventa:

$$\begin{aligned}
H(Y) &= \int_{-\infty}^{+\infty} p_Y(y) \cdot \log \frac{1}{p_Y(y)} dy = \\
&= \int_{-\infty}^{+\infty} \frac{1}{M} \cdot \sum_{i=1}^M p_N(y - x_i) \cdot \log \frac{1}{\frac{1}{M} \cdot \sum_{j=1}^M p_N(y - x_j)} dy = \\
&= \frac{1}{M} \cdot \int_{-\infty}^{+\infty} \left(\sum_{i=1}^M p_N(y - x_i) \right) \cdot \log \frac{M}{\sum_{j=1}^M p_N(y - x_j)} dy = \\
&= \frac{1}{M} \cdot \int_{-\infty}^{+\infty} \left[\left(\sum_{i=1}^M p_N(y - x_i) \right) \cdot \log M + \left(\sum_{i=1}^M p_N(y - x_i) \right) \cdot \log \frac{1}{\sum_{j=1}^M p_N(y - x_j)} \right] dy = \\
&= \frac{1}{M} \cdot \int_{-\infty}^{+\infty} \left(\sum_{i=1}^M p_N(y - x_i) \right) \cdot \log M dy + \frac{1}{M} \cdot \int_{-\infty}^{+\infty} \left(\sum_{i=1}^M p_N(y - x_i) \right) \cdot \log \frac{1}{\sum_{j=1}^M p_N(y - x_j)} dy = \\
&= \frac{\log M}{M} \cdot \int_{-\infty}^{+\infty} \left(\sum_{i=1}^M p_N(y - x_i) \right) dy + \frac{1}{M} \cdot \int_{-\infty}^{+\infty} \left(\sum_{i=1}^M p_N(y - x_i) \cdot \log \frac{1}{\sum_{j=1}^M p_N(y - x_j)} \right) dy = \\
&= \frac{\log M}{M} \cdot \sum_{i=1}^M \underbrace{\int_{-\infty}^{+\infty} p_N(y - x_i) dy}_{1} + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y - x_i) \cdot \log \frac{1}{\sum_{j=1}^M p_N(y - x_j)} dy = \\
&= \frac{\log M}{M} \cdot \mathcal{M} + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y - x_i) \cdot \log \frac{1}{\sum_{j=1}^M p_N(y - x_j)} dy = \\
&= \log M + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y - x_i) \cdot \log \frac{1}{\sum_{j=1}^M p_N(y - x_j)} dy
\end{aligned}$$

che rimane non integrabile, ma si può notare che:

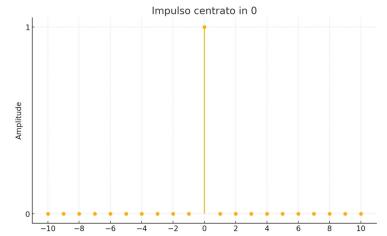
- Se il rapporto segnale rumore è molto basso ($\frac{\sigma_X^2}{\sigma_N^2} \rightarrow 0$) allora $\sigma_N^2 \rightarrow +\infty$ e quindi la funzione p_N diventa

4. Capacità di canale

ho solo rumore

costante perché tutti i valori diventano equiprobabili; vale che $p_N(y - x_i) = p_N(y) \forall x_i$ e quindi:

$$\begin{aligned}
H(Y) &= \log M + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y) \cdot \log \frac{1}{\sum_{j=1}^M p_N(y)} dy = \\
&= \log M + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y) \cdot \log \frac{1}{M \cdot p_N(y)} dy = \\
&= \log M + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} \left[p_N(y) \cdot \log \frac{1}{M} + p_N(y) \cdot \log \frac{1}{p_N(y)} \right] dy = \\
&= \log M + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y) \cdot \log \frac{1}{M} dy + \underbrace{\frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y) \cdot \log \frac{1}{p_N(y)} dy}_{H(N)} \\
&= \log M + \frac{1}{M} \cdot \log \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y) dy + \frac{1}{M} \cdot M \cdot H(N) = \\
&= -\log \frac{1}{M} + \frac{1}{M} \cdot \log \frac{1}{M} \cdot M + H(N) = \\
&= H(N)
\end{aligned}$$



- Se il rapporto segnale rumore è molto alto ($\frac{\sigma_X^2}{\sigma_N^2} \rightarrow +\infty$) allora $\sigma_N^2 \rightarrow 0$ e quindi la funzione p_N diventa simile ad un impulso centrato in 0. Quindi si ha che gli unici termini che valgono sono quelli per cui $i = j$ e quindi:

$$H(Y) = \log M + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(y - x_i) \cdot \log \frac{M}{p_N(y - x_i)} dy =$$

la ddp diventa significativa nei punti x_i e non significativa nei punti esterni perché il rumore risulta essere molto basso

Tramite il cambio di variabile $n = y - x_i$, che fa rimanere gli estremi invariati, si ha:

$$\begin{aligned}
H(Y) &= \log M + \frac{1}{M} \cdot \sum_{i=1}^M \int_{-\infty}^{+\infty} p_N(n) \cdot \log \frac{1}{p_N(n)} dn = \\
&= \log M + \frac{1}{M} \cdot M \cdot H(N) = \\
&= \log M + H(N)
\end{aligned}$$

Dato che la capacità in questo caso corrisponde al valore della mutua informazione con il valore di $H(Y)$ massimizzato queste due osservazioni valgono anche per la capacità e quindi:

- Con $\frac{\sigma_X^2}{\sigma_N^2} \rightarrow 0$ si ha che:
 - $\sigma_N^2 \rightarrow +\infty$
 - $H(Y) \rightarrow H(N)$

e quindi

$$\begin{aligned}
C &= H(Y) - H(N) \rightarrow \\
&\rightarrow H(N) - H(N) = \\
&= 0
\end{aligned}$$

4. Capacità di canale

- Con $\frac{\sigma_X^2}{\sigma_N^2} \rightarrow +\infty$ si ha che:

$$\circ \sigma_N^2 \rightarrow 0$$

$$\circ H(Y) \rightarrow \log M + H(N)$$

e quindi

$$\begin{aligned} C &= H(Y) - H(N) \rightarrow \\ &\rightarrow \log M + H(N) - H(N) = \\ &= \log M \end{aligned}$$

$$\frac{\sigma_X^2}{\sigma_N^2} \rightarrow 0$$

Quindi la capacità per rapporti segnali rumori bassi rimane simile a quella vista nel caso in cui X è analogico, ma pone un limite superiore per rapporti segnali rumore alti pari a $\log M$ che è l'informazione media di X , ovvero quella trasmessa e ovviamente risulta logico che non possa arrivare più informazione di quella inviata.

Quindi per rapporti segnale rumore alti usare un trasmettitore analogico permette di inviare più informazione media, per via del limite superiore del caso digitale, ma per rapporti segnale rumore bassi un trasmettitore digitale permette di avere una capacità maggiore.

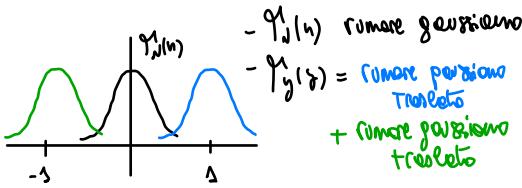
Caso AGN con X discreto:

$$Y = X + N, \quad N \sim N(0, \sigma_N^2), \quad X \in \{-1, 1\} \rightarrow P_x^2 = E[X^2] = \xi$$

indipendente
da X

equiprobabilità

$$\begin{aligned} I(x; Y) &= H(Y) - H(N) \\ &= H(Y) - \frac{1}{2} \log(2\pi e \sigma_N^2) \end{aligned}$$



Stante alle componenti discrete che si accuacciano alle componenti continue.

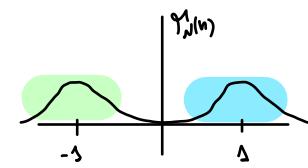
$$\begin{aligned} P_Y(y) &= P_{Y|X}(y|1) \cdot P_X(1) + P_{Y|X}(y|-1) \cdot P_X(-1) \\ &= \frac{1}{2} P_N(y+1) + \frac{1}{2} P_N(y-1) \quad \sum_{x=-1}^1 P_X(y-x) \end{aligned}$$

$$P_N(y+1) = P_{Y|X}(y|1)$$

$$P_N(y-1) = P_{Y|X}(y|-1)$$

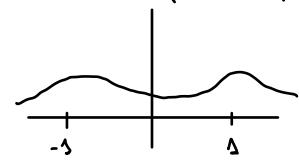
$$\begin{aligned} H(Y) &= \int_{-\infty}^{+\infty} P_Y(y) \cdot \log \frac{1}{P_Y(y)} dy = \\ &= \sum_{x=-1}^1 \frac{1}{2} \int_{-\infty}^{+\infty} P_N(y-x) \cdot \log \frac{2}{P_N(y-x) + P_N(y+x)} dy \\ &= \int_{-\infty}^{+\infty} P_N(y-1) \cdot \log \frac{2}{P_N(y+1) + P_N(y-1)} dy \end{aligned}$$

Risultato molto $H=Y$ per le case $x=-1$ mi ottiene lo stesso integrale perché $P_N(y) = P_N(-y)$.

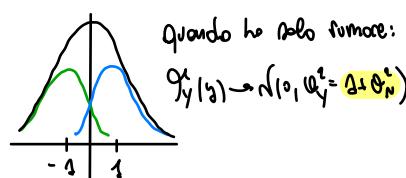


ne la var del rumore si riduce:

se la var del rumore aumenta le due andranno a confondersi se centri dipende da σ_N^2



$$\begin{aligned} &\frac{\sigma_X^2}{\sigma_N^2} \rightarrow \infty \rightarrow 1 + H(N) \Rightarrow I(x; Y) \rightarrow 1 \\ &\frac{\sigma_X^2}{\sigma_N^2} \rightarrow 0 \rightarrow \frac{1}{2} \log(2\pi e (1 + \sigma_N^2)) \\ &\Rightarrow I(x; Y) \rightarrow \frac{1}{2} \log \left(\frac{\sigma_N^2}{\sigma_N^2} \right) \end{aligned}$$

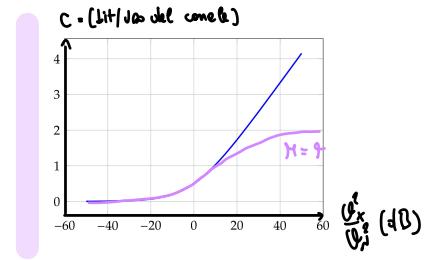
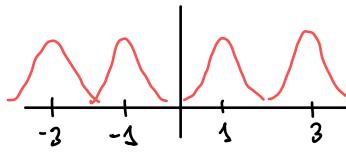


$$X \in \{-1, 1, 3\} \rightarrow P_X(x) = \left\{ \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4} \right\} \text{ equiprobabile}$$

$$P_Y(y) = \sum_{x=-3}^3 P_{Y|X}(y|x) = \sum_{x=-3}^3 \frac{1}{4} P_N(y-x)$$

$$P_{Y|X}(y|x) = P_N(y-x)$$

$$\begin{aligned} I(x; Y) &= H(Y) - H(N) = \\ &\frac{\sigma_X^2}{\sigma_N^2} \rightarrow 0 \rightarrow 2 + H(N) - H(N) = 2 \end{aligned}$$



5. Teorema della codifica di canale

5.1. Modalità di invio dei messaggi sul canale

Dato che si vuole inviare dell'informazione su un canale che presenta una probabilità di errore, la codifica di canale propone di inviare un codice più lungo che si crea tramite operazioni sui bit di informazione che si vuole inviare. In questo modo si crea ridondanza nel codice trasmesso e l'errore su un singolo bit è meno determinante rispetto all'invio senza ridondanza perché potrebbe essere ricavato tramite gli altri bit ricevuti.

Si supponga di voler inviare K bit di informazione utilizzando un canale con L simboli in ingresso utilizzando delle sequenze di simboli $\underline{x} = (x_1, x_2, \dots, x_N)$ lunghe N . Dato che si vogliono inviare K bit di informazione servono 2^K combinazioni, e il codice ne ha a disposizione L^N ; per poter inviare tutti i K bit di informazione devono esserci più combinazioni possibili rispetto a quelle necessarie, ossia

- Voglio inviare K bit di informazioni sul canale, utilizzando delle sequenze lunghe N con simboli in L
- combinazioni possibili del codice
- K bit di informazione in binario sono tot sequenze

$$\begin{aligned} L^N &\geq 2^K \\ 2^{N \cdot \log L} &\geq 2^K \\ N \cdot \log L &\geq K \end{aligned}$$

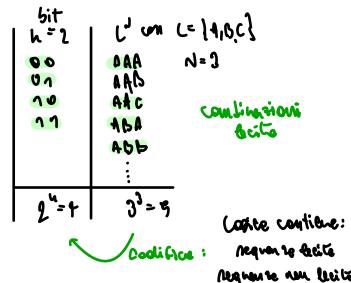
$L = \{A, B, C, D\}$ simboli distinti: alfabeto
 $\underline{x} = (x_1, \dots, x_N) \quad \forall x_i \in L$

Se vale questa considerazione ci sono più combinazioni rispetto a quelle che servono e quindi si può imporre che non tutte le combinazioni siano lecite e abbiano un significato associato.

Definizione Si definisce rate (ritmo in italiano) di invio R il rapporto:

$$R = \frac{K}{N}$$

ossia la quantità di informazione contenuta in ogni simbolo inviato sul canale.



Osservazioni

- Dato che $K \leq N \cdot \log L$ e che $K > 0$ (altrimenti non si invierebbe nessuna informazione), si ottiene che:

$$0 < R \leq \log L$$

- Se l'alfabeto è binario, come nella maggior parte dei casi:

$$\{0,1\} \Rightarrow L=2 \quad \begin{matrix} |C| \leq N \cdot \log_2 L \\ \frac{|C|}{N} \leq \frac{N \cdot \log_2 L}{N} \Rightarrow R \leq 1 \end{matrix} \quad 0 < R \leq 1$$

- Se $R = \log L$ significa che si sta inviando senza aggiungere ridondanza.

- Il numero di combinazioni lecite del codice C è:

$$M = 2^K = 2^{R \cdot N}$$

- Più il rate R è basso più si sta aggiungendo ridondanza, quindi meno densità di informazione si sta inviando sul canale. Al contrario della codifica della sorgente

5.2. Modalità di ricezione dei messaggi sul canale

R: ricevitore
T: trasmettitore

Dato che il canale non è perfetto le sequenze ricevute $\underline{y}_R = (y_{R1}, y_{R2}, \dots, y_{RN})$ non sono uguali alle sequenze inviate $\underline{x}_T = (x_{T1}, x_{T2}, \dots, x_{TN})$, quindi bisogna stabilire un metodo per ricavare la sequenza \underline{x}_T inviata conoscendo la sequenza \underline{y}_R ricevuta. I ricevitori si dividono in base alla tecnica utilizzata per fare questa scelta.

5. Teorema della codifica di canale

Ricevitori MAP (Massima probabilità A Posteriori) Scelgono la sequenza \hat{x}_{MAP} lecita che massimizza la probabilità condizionata a posteriori, ossia:

$$\hat{x}_{MAP} = \arg \max_{\underline{x} \text{ lecita}} P_{\underline{X}|\underline{Y}}(\underline{x}|\underline{y}_R)$$

quindi scelgono la sequenza \hat{x}_{MAP} lecita che ha la maggior probabilità di essere quella inviata sapendo che è stata ricevuta la sequenza \underline{y}_R .

Ricevitori ML (Massima Verosimiglianza - Maximum Likelihood) Scelgono la sequenza \hat{x}_{ML} lecita che massimizza la probabilità condizionata, ossia:

$$\hat{x}_{ML} = \arg \max_{\underline{x} \text{ lecita}} P_{\underline{Y}|\underline{X}}(\underline{y}_R|\underline{x}) \quad \begin{array}{l} \text{probabilità di yr dato} \\ \text{che ho inviato } \underline{x} \end{array}$$

quindi scelgono la sequenza \hat{x}_{ML} lecita che massimizza la probabilità di ricevere la sequenza \underline{y}_R ricevuta.

Osservazione Nel caso in cui le sequenze \underline{x} siano inviate equiprobabilmente allora i due ricevitori scelgono sempre lo stesso messaggio e sono quindi equivalenti, infatti:

$$\begin{aligned} \hat{x}_{MAP} &= \arg \max_{\underline{x} \text{ lecita}} P_{\underline{X}|\underline{Y}}(\underline{x}|\underline{y}_R) = \\ &= \arg \max_{\underline{x} \text{ lecita}} \frac{P_{\underline{X}, \underline{Y}}(\underline{x}, \underline{y}_R)}{P_{\underline{Y}}(\underline{y}_R)} = \\ &= \arg \max_{\underline{x} \text{ lecita}} P_{\underline{Y}|\underline{X}}(\underline{y}_R|\underline{x}) \cdot \frac{P_{\underline{X}}(\underline{x})}{P_{\underline{Y}}(\underline{y}_R)} \end{aligned}$$

- Se esiste equi probabilità sulle sequenze inviate nel canale e quindi che sono codificate allo stesso modo dal canale
- le invia il canale
- vengono codificate dal canale

dato che le sequenze \underline{x} sono equiprobabili:

$$P_{\underline{X}}(\underline{x}) = k, \forall \underline{x}$$

e quindi:

$$\hat{x}_{MAP} = \arg \max_{\underline{x} \text{ lecita}} P_{\underline{Y}|\underline{X}}(\underline{y}_R|\underline{x}) \cdot \frac{k}{P_{\underline{Y}}(\underline{y}_R)}$$

e dato che il termine

$$\frac{k}{P_{\underline{Y}}(\underline{y}_R)}$$

non dipende dalla \underline{x} si ha:

$$\begin{aligned} \hat{x}_{MAP} &= \arg \max_{\underline{x} \text{ lecita}} P_{\underline{Y}|\underline{X}}(\underline{y}_R|\underline{x}) = \\ &= \hat{x}_{ML} \end{aligned}$$

5.3. Probabilità di sbagliare di un ricevitore ML

5.3.1. Formulazione

Supponendo di inviare una sequenza \underline{x}_T ad un ricevitore *ML* che riceve un messaggio \underline{y}_R , il ricevitore sceglie la sequenza \hat{x}_{ML} tale che:

$$\hat{x}_{ML} = \arg \max_{\underline{x} \text{ lecita}} P_{\underline{Y}|\underline{X}}(\underline{y}_R|\underline{x})$$

- nella maggior parte dei casi io conosco quella probabilità ecco perché ci stiamo concentrando su questo ricevitore

5. Teorema della codifica di canale

Quindi il ricevitore sbaglia se esiste una sequenza lecita \underline{x}_m tale che:

$$P_{\underline{Y}|\underline{X}}(\underline{y}_R|\underline{x}_m) > P_{\underline{Y}|\underline{X}}(\underline{y}_R|\underline{x}_T)$$

generalizzato per la definizione sotto

Dato che il trasmettitore ha inviato una sequenza \underline{x}_T la probabilità di ricevere una sequenza \underline{y} è pari a:

$$P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T)$$

e quindi la probabilità di ricevere una \underline{y} tale che:

$$\mathcal{P}(\text{ricevere } \underline{y} \text{ t.c. } \exists \underline{x}_m \text{ lecita tale che } P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_m) > P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T)) = \sum_{\underline{y} \in \underline{Y}} [P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T) \cdot I_e(\underline{y}|\underline{x}_T)]$$

ricevitore ML sbaglia

si sommano le probabilità di tutte le sequenze che potrebbero indurre un errore

è pari a:

$$\sum_{\underline{y} \in \underline{Y}} [P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T) \cdot I_e(\underline{y}|\underline{x}_T)]$$

fissata la sequenza trasmessa
la probabilità totale di errore del ricevitore
ML quando la sequenza \underline{x}_T viene trasmessa

quanto è probabile che quella
specifica sequenza venga ricevuta

dove $I_e(\underline{y}|\underline{x}_T)$ è una funzione indicatrice e vale:

$$I_e(\underline{y}|\underline{x}_T) = \begin{cases} 1 & \text{se } \exists \underline{x}_m \text{ lecita tale che } P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_m) > P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T) \\ 0 & \text{altrimenti} \end{cases}$$

Quindi la probabilità che il ricevitore *ML* sbagli avendo inviato la sequenza \underline{x}_T è pari a:

$$P_{eML}(\underline{x}_T) = \sum_{\underline{y} \in \underline{Y}} [P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T) \cdot I_e(\underline{y}|\underline{x}_T)]$$

- trasmessa \underline{x}_T controllo su tutte le sequenze possibili in uscita se il mio ricevitore *ML* sbaglia o meno
- sequenze a bassa probabilità di essere ricevute dato aver trasmesso \underline{x}_T hanno poco rilevanza al contrario le altre

5.3.2. Limite superiore

Maggiorazione della funzione indicatrice Questa probabilità è difficile da ricavare perché la funzione indicatrice non è facilmente calcolabile, però è possibile maggiorarla in modo da trovare un limite superiore. Infatti:

$$I_e(\underline{y}|\underline{x}_T) \leq \frac{\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x})}{P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T)}$$

tutte le probabilità che competono con \underline{x}_T
la probabilità trasmessa genera quella ricevuta

Infatti:

- se $I_e(\underline{y}|\underline{x}_T) = 1$ allora $\exists \underline{x}_m \neq \underline{x}_T$ tale che $P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_m) > P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T)$ e quindi il numeratore è sicuramente maggiore di $P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T)$ e quindi:

$$\frac{\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x})}{P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T)} > 1 = I_e(\underline{y}|\underline{x}_T)$$

- se $I_e(\underline{y}|\underline{x}_T) = 0$ allora si può notare che il numeratore è una somma di probabilità e quindi è sempre positivo mentre il denominatore è sempre positivo perché anch'esso una probabilità e quindi:

$$\frac{\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x})}{P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T)} \geq 0 = I_e(\underline{y}|\underline{x}_T)$$

5. Teorema della codifica di canale

Dato che l'espressione è la somma di tante frazioni positive si possono elevare tutte ad una potenza positiva mantenendo corretta la disegualanza. Si introduce quindi il parametro $\rho \in [0, 1]$ tale che:

$$I_e(\underline{y}|\underline{x}_T) \leq \frac{\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}))^{\frac{1}{1+\rho}} \right]}{(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T))^{\frac{1}{1+\rho}}}$$

Inoltre dato che l'unica cosa importante è che la maggiorazione rimanga maggiore di 1 quando lo è la frazione lo si può elevare a una potenza positiva senza invalidare la disegualanza:

$$I_e(\underline{y}|\underline{x}_T) \leq \left(\frac{\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}))^{\frac{1}{1+\rho}} \right]}{(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T))^{\frac{1}{1+\rho}}} \right)^{\rho} = \frac{\left(\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}))^{\frac{1}{1+\rho}} \right] \right)^{\rho}}{(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T))^{\frac{\rho}{1+\rho}}}$$

Maggiorazione della funzione di probabilità Utilizzando la maggiorazione appena trovata:

$$\begin{aligned} P_{eML}(\underline{x}_T) &= \sum_{\underline{y} \in \underline{Y}} \left[P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T) \cdot I_e(\underline{y}|\underline{x}_T) \right] \leq \\ &\leq \sum_{\underline{y} \in \underline{Y}} P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T) \cdot \left[\left(\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}))^{\frac{1}{1+\rho}} \right] \right)^{\rho} \right] = \\ &= \sum_{\underline{y} \in \underline{Y}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T))^{1-\frac{\rho}{1+\rho}} \cdot \left(\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}))^{\frac{1}{1+\rho}} \right] \right)^{\rho} \right] = \\ &= \sum_{\underline{y} \in \underline{Y}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_T))^{\frac{1}{1+\rho}} \cdot \left(\sum_{\substack{\underline{x} \in \underline{X} \\ \underline{x} \neq \underline{x}_T}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}))^{\frac{1}{1+\rho}} \right] \right)^{\rho} \right] \end{aligned}$$

5.3.3. Maggiorazione del valor medio

Si è trovata una maggiorazione della probabilità di commettere un errore inviando un messaggio \underline{x}_T , ossia $P_{eML}(\underline{x}_T)$, ma è più utile trovare la maggiorazione del valor medio dell'errore ossia $\mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})]$ quindi:

$$\mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] \leq \mathbb{E}_{\underline{x}} \left[\sum_{\underline{y} \in \underline{Y}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}))^{\frac{1}{1+\rho}} \cdot \left(\sum_{\substack{\underline{x}_m \in \underline{X} \\ \underline{x}_m \neq \underline{x}}} \left[(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_m))^{\frac{1}{1+\rho}} \right] \right)^{\rho} \right] \right]$$

X e Y sono indipendenti:
 $E(X \cdot Y) = E(X) \cdot E(Y)$

5. Teorema della codifica di canale

Dato che \underline{x} è indipendente dai vari \underline{x}_m si può scrivere:

$$\mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] \leq \sum_{\underline{y} \in \underline{Y}} \left[\mathbb{E}_{\underline{x}} \left[\left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) \right)^{\frac{1}{1+\rho}} \right] \cdot \mathbb{E}_{\underline{x}} \left[\left(\sum_{\substack{\underline{x}_m \in \underline{X} \\ \underline{x}_m \neq \underline{x}}} \left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_m) \right)^{\frac{1}{1+\rho}} \right)^\rho \right] \right]$$

Per la diseguaglianza di Jensen si ha che se $\rho < 1$ vale che $\mathbb{E}_{\underline{x}}[(f(\underline{x}))^\rho] \leq (\mathbb{E}_{\underline{x}}[f(\underline{x})])^\rho$ e quindi:

$$\begin{aligned} \mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] &\leq \sum_{\underline{y} \in \underline{Y}} \mathbb{E}_{\underline{x}} \left[\left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) \right)^{\frac{1}{1+\rho}} \right] \cdot \mathbb{E}_{\underline{x}} \left[\sum_{\substack{\underline{x}_m \in \underline{X} \\ \underline{x}_m \neq \underline{x}}} \left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_m) \right)^{\frac{1}{1+\rho}} \right]^\rho = \\ &= \sum_{\underline{y} \in \underline{Y}} \mathbb{E}_{\underline{x}} \left[\left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) \right)^{\frac{1}{1+\rho}} \right] \cdot \left(\sum_{\substack{\underline{x}_m \in \underline{X} \\ \underline{x}_m \neq \underline{x}}} \left[\mathbb{E}_{\underline{x}} \left[\left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_m) \right)^{\frac{1}{1+\rho}} \right] \right] \right)^\rho \end{aligned}$$

Per semplicità definiamo:

$$E = \mathbb{E}_{\underline{x}} \left[\left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) \right)^{\frac{1}{1+\rho}} \right] = \mathbb{E}_{\underline{x}} \left[\left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}_m) \right)^{\frac{1}{1+\rho}} \right]$$

e sostituendolo nella maggiorazione:

$$\mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] \leq \sum_{\underline{y} \in \underline{Y}} \left[E \cdot \left(\sum_{\substack{\underline{x}_m \in \underline{X} \\ \underline{x}_m \neq \underline{x}}} [E] \right)^\rho \right]$$

Si può notare che E non dipende dal valore di \underline{x} e quindi lo si può tirare fuori dalla sommatoria, ottenendo:

$$\begin{aligned} \mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] &\leq \sum_{\underline{y} \in \underline{Y}} [E \cdot (M-1)^\rho \cdot E^\rho] = && : M \text{ rappresenta le sequenze lecite} \\ &= (M-1)^\rho \cdot \sum_{\underline{y} \in \underline{Y}} [E^{\rho+1}] && : M-1 \text{ perché tolgo quella trasmessa } \underline{x} \end{aligned}$$

Ricordando che:

$$\begin{aligned} E &= \mathbb{E}_{\underline{x}} \left[\left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) \right)^{\frac{1}{1+\rho}} \right] = \\ &= \sum_{\underline{x} \in \underline{X}} \left[P_{\underline{X}}(\underline{x}) \cdot \left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) \right)^{\frac{1}{1+\rho}} \right] \end{aligned}$$

si ottiene:

$$\begin{aligned} \mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] &\leq (M-1)^\rho \cdot \sum_{\underline{y} \in \underline{Y}} \left[\left(\sum_{\underline{x} \in \underline{X}} \left[P_{\underline{X}}(\underline{x}) \cdot \left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) \right)^{\frac{1}{1+\rho}} \right] \right)^{\rho+1} \right] \leq \\ &\leq M^\rho \cdot \sum_{\underline{y} \in \underline{Y}} \left[\left(\sum_{\underline{x} \in \underline{X}} \left[P_{\underline{X}}(\underline{x}) \cdot \left(P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) \right)^{\frac{1}{1+\rho}} \right] \right)^{\rho+1} \right] \end{aligned}$$

lo maggiore togliendo il termine

5. Teorema della codifica di canale

5.3.4. Maggiorazione del valor medio in un canale senza memoria

In un canale senza memoria vale:

$$P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) = \prod_{n=1}^N P_{Y_n|X_n}(y_n|x_n)$$

- la sequenza è lunga N con simboli in L
- i gli N simboli sono tra loro indipendenti

inoltre per ipotesi le sequenze \underline{x} inviate sono composte da simboli indipendenti e quindi:

$$P_{\underline{X}}(\underline{x}) = \prod_{n=1}^N P_{X_n}(x_n)$$

inoltre il canale e la variabile X sono stazionari e quindi la loro probabilità non dipende dalla posizione all'interno della sequenza in cui si trovano:

$$P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) = \prod_{n=1}^N P_{Y|X}(y_n|x_n)$$

il valore che assume la variabile casuale non dipende/non è influenzata dalla posizione in cui si trova

$$P_{\underline{X}}(\underline{x}) = \prod_{n=1}^N P_X(x_n)$$

Con queste considerazioni:

$$\begin{aligned} \mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] &\leq M^\rho \cdot \sum_{\underline{y} \in \underline{Y}} \left[\left(\sum_{\underline{x} \in \underline{X}} \left[P_{\underline{X}}(\underline{x}) \cdot (P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}))^{\frac{1}{1+\rho}} \right] \right)^{\rho+1} \right] = \\ &= M^\rho \cdot \sum_{\underline{y} \in \underline{Y}} \left[\left(\sum_{\underline{x} \in \underline{X}} \left[\prod_{n=1}^N \left[P_X(x_n) \cdot (P_{Y|X}(y_n|x_n))^{\frac{1}{1+\rho}} \right] \right] \right)^{\rho+1} \right] = \quad \text{data una sequenza lunga N lo invio N simboli} \\ &= M^\rho \cdot \sum_{\underline{y} \in \underline{Y}} \left[\left(\sum_{x_1 \in X} \sum_{x_2 \in X} \dots \sum_{x_N \in X} \left[\prod_{n=1}^N \left[P_X(x_n) \cdot (P_{Y|X}(y_n|x_n))^{\frac{1}{1+\rho}} \right] \right] \right)^{\rho+1} \right] = \quad \text{tutte le sequenze inviabili} \Rightarrow \text{ossia su tutti i possibili messaggi inviabili} \end{aligned}$$

La produttoria esegue il prodotto di termini che dipendono solamente dal valore assunto da una sola delle sommatorie precedenti; in generale l'unica sommatoria che influisce sull' n -esimo termine della produttoria è quella che scorre i possibili valori di x_n . Per questo motivo si può scrivere:

$$\mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] \leq M^\rho \cdot \sum_{\underline{y} \in \underline{Y}} \left[\left(\prod_{n=1}^N \left[\sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y_n|x))^{\frac{1}{1+\rho}} \right] \right] \right)^{\rho+1} \right]$$

Con questa formulazione si calcola il prodotto della somma di tutti i termini generati scorrendo tutto l'alfabeto della variabile X (se X è binaria questo corrisponde a fare la somma di due termini). Dato che l'esponenziale della produttoria è la produttoria degli esponenziali si ha che:

$$\mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] \leq M^\rho \cdot \sum_{\underline{y} \in \underline{Y}} \left[\prod_{n=1}^N \left[\left(\sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y_n|x))^{\frac{1}{1+\rho}} \right] \right)^{\rho+1} \right] \right]$$

disugualanza di Jensen

Tramite lo stesso ragionamento fatto prima:

$$\mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] \leq M^\rho \cdot \prod_{n=1}^N \left[\sum_{y \in Y} \left[\left(\sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1+\rho}} \right] \right)^{\rho+1} \right] \right]$$

Si può notare che il contenuto della produttoria non dipende dal valore di n e quindi:

$$\mathbb{E}_{\underline{x}}[P_{eML}(\underline{x})] \leq M^\rho \cdot \left(\sum_{y \in Y} \left[\left(\sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1+\rho}} \right] \right)^{\rho+1} \right] \right)^N$$

5. Teorema della codifica di canale

Ricordando che il numero delle sequenze lecite M è:

$$M = 2^{N \cdot R}$$

chiamiamo questa somma: $\{-E_0(\rho)\}$

si ottiene:

$$\mathbb{E}_x [P_{eML}(x)] \leq 2^{N \cdot R \cdot \rho} \cdot \left(\sum_{y \in Y} \left[\left(\sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1+\rho}} \right] \right)^{\rho+1} \right]^N \right)$$

Per comodità si può definire la funzione $E_0(\rho)$:

$$E_0(\rho) = -\log \left(\sum_{y \in Y} \left[\left(\sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1+\rho}} \right] \right)^{\rho+1} \right] \right)$$

e quindi:

$$\begin{aligned} \mathbb{E}_x [P_{eML}(x)] &\leq 2^{N \cdot R \cdot \rho} \cdot 2^{-E_0(\rho) \cdot N} = \\ &= 2^{-N \cdot (E_0(\rho) - R \cdot \rho)} \end{aligned}$$

: vogliamo la maggioranza più stringente
ossia trovare il più grande di rho tale per cui continua a valere tale maggioranza

Dato che questa maggiorazione vale per ogni $\rho \in [0, 1]$, si può trovare quella più stringente calcolando il valore di ρ che la minimizza (ovvero il valore più grande che l'esponente può assumere con $0 \leq \rho \leq 1$). Dato che N non dipende da ρ bisogna massimizzare solamente il contenuto della parentesi all'esponente e quindi la maggiorazione più stringente è:

$$\mathbb{E}_x [P_{eML}(x)] \leq 2^{-N \cdot E(R)}$$

dove:

$$E(R) = \max_{0 \leq \rho \leq 1} [E_0(\rho) - R \cdot \rho]$$

esponente d'errore

$$E(R) < 2^{-N \cdot E(R)} \xrightarrow[N \rightarrow \infty]{} 0 \quad \forall R: E(R) > 0$$

abbiamo un canale che introduce errori che però utilizzando anche un codice scelto casualmente e un ricevitore a massima verosimiglianza possiamo far tendere la probabilità dell'errore dei decisoni a zero, aumentando di uso del canale che facciamo pur mantenendo costante il rapporto tra l'informazione che trasmettiamo e gli usi del canale che facciamo

5.4. Analisi della maggiorazione dell'errore medio

Primo risultato Per poter analizzare il risultato si ricorda che si vuole inviare K bit di informazioni utilizzando messaggi lunghi $N > K$ simboli (in genere bit) dove

$$R = \frac{K}{N}$$

Quindi dalla formulazione ottenuta:

$$\mathbb{E}_x [P_{eML}(x)] \leq 2^{-N \cdot E(R)}$$

$\rho < E(R) > 0$	$\uparrow N$	$\mathbb{E}_x [P_{eML}(x)] \downarrow$
$\rho < E(R) < 0$	$\uparrow N$	$\mathbb{E}_x [P_{eML}(x)] \uparrow$
$\rho < E(R) = 0$	$\uparrow N$	$\mathbb{E}_x [P_{eML}(x)]$ influisce a p. fine

Si può notare che l'errore medio si può diminuire a piacere alzando il valore di N , ma questo però vale solo se $E(R)$ è strettamente positivo, perché se fosse negativo l'errore aumenterebbe con N e se fosse nullo il valore di N non influirebbe affatto. Per questo motivo è necessario analizzare più in dettaglio la funzione $E(R)$.

Analisi di $E(R)$

La funzione $E(R)$ è definita tramite un massimo e quindi è necessario valutare ogni singolo possibile termine e poi prenderne il maggiore. Dalla funzione all'interno del massimo:

$$E(R) = \boxed{E_0(\rho) - R \cdot \rho}$$

quantità che dipende da R

si può notare che:

- È una retta con coefficiente angolare $-\rho$, e quindi ha massimo per $R = 0$.
- Ha valore massimo per $R = 0$, in cui vale $E_0(\rho)$.

in questi tre punti, vado a definire 2 punti fissi della mia retta e faccio variare rho che è la pendenza della mia retta

5. Teorema della codifica di canale

- Incrocia l'asse orizzontale quando:

$$\begin{aligned} E_0(\rho) - R \cdot \rho &= 0 \\ E_0(\rho) &= R \cdot \rho \\ R &= \frac{E_0(\rho)}{\rho} \end{aligned}$$

Oss: $\sum_x p_x(x) \cdot P_{Y|X}(y|x)^{\frac{1}{n+\rho}} = \left[\sum_x p_x(x) P_{Y|X}(y|x)^{\frac{1}{n+\rho}} \right]^{\frac{1}{n+\rho}}$

Jensen inequality $\Rightarrow \left[\sum_x p_x(x) P_{Y|X}(y|x)^{\frac{1}{n+\rho}} \right]^{\frac{1}{n+\rho}} \leq \sum_x p_x(x) \left[P_{Y|X}(y|x)^{\frac{1}{n+\rho}} \right]$

- esponente $< 1 \Rightarrow$ funzione convessa
- il valore medio di una funzione convessa è sempre minore o uguale dalla funzione convessa applicata al valore medio

$\Rightarrow E_0(\rho) \geq -\log_2 \sum_y \left(\sum_x p_x(x) P_{Y|X}(y|x)^{\frac{1}{n+\rho}} \right)^{\frac{1}{n+\rho}} = 0$

La funzione $E_0(\rho)$ è una funzione decrescente con un massimo per $\rho = 1$ e un minimo per $\rho = 0$ e inoltre:

$$\begin{aligned} E_0(0) &= -\log \left(\sum_{y \in Y} \left[\left(\sum_{x \in X} [P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1}}] \right)^1 \right] \right) = \\ &= -\log \left(\sum_{y \in Y} \sum_{x \in X} [P_X(x) \cdot P_{Y|X}(y|x)] \right) = \\ &= -\log \left(\sum_{y \in Y} \sum_{x \in X} [P_{X,Y}(x,y)] \right) = \\ &= -\log 1 = \\ &= 0 \end{aligned}$$

Quindi la retta che si ottiene con $\rho = 0$ è orizzontale e corrisponde all'asse. Aumentando ρ si aumenta la pendenza e si alza il valore massimo fino ad arrivare alla curva per $\rho = 1$ che ha il massimo più alto e ha pendenza massima pari a -1 . Questo andamento è mostrato in figura 5.1.

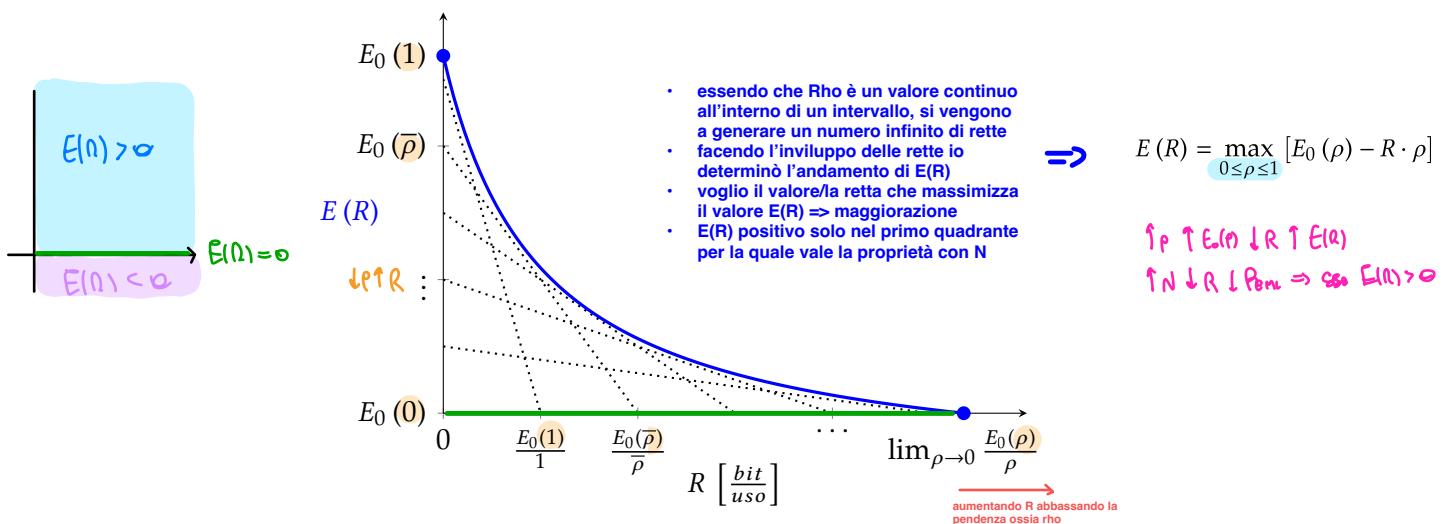


Figura 5.1.: Andamento delle rette $E_0(\rho) - R \cdot \rho$.

La funzione $E(R)$ si ricava selezionando la retta più alta per ogni valore di R e quindi la si ottiene facendo l'involuppo di tutte le varie rette. Si può notare che la funzione è decrescente e quindi:

$$R \uparrow \Rightarrow E(R) \downarrow \Rightarrow 2^{-N \cdot E(R)} \uparrow \Rightarrow \mathbb{E}_x [P_{eML}(\underline{x})] \uparrow$$

aumentando il rate R, io diminuisco la ridondanza e i possibili sbagli che io faccio sono più alti

quindi aumentando il rate di invio la probabilità di commettere errori aumenta come è facilmente intuibile.

La proprietà che aumentando N si può abbassare a piacere la media dell'errore rimane vera finché $E(R) > 0$, per cui le singole rette $E_0(\rho) - R \cdot \rho$ rimangono positive fino a che non incrociano l'asse delle ascisse per:

$$R = \frac{E_0(\rho)}{\rho}$$

5. Teorema della codifica di canale

Quindi se si prende l'incrocio con le ascisse della retta con pendenza minore, ossia quella più bassa, si ottiene il rate massimo per cui vale quella proprietà. Prima si è visto che la pendenza diminuisce con il diminuire di ρ e quindi questo limite è dato da:

$$\lim_{\rho \rightarrow 0} \frac{E_0(\rho)}{\rho}$$

voglio trovare il rate massimo per cui vale questa proprietà

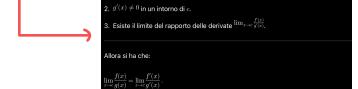
Proprietà:
 $E_x(\rho_{\text{max}}) \downarrow \text{ma } E(0) > 0$
 basta non riuscire una traiettoria dove $E(0) = 0$

Nice! Bene:
 Se $E(0) > 0$
 retta più bassa

Se questo limite diverge all'infinito allora nel canale non si perde mai la proprietà per cui aumentando la N diminuisce la probabilità media di errore; se invece questo limite esiste utilizzando rate più alti si perde questa buona proprietà del canale.

Calcolo del limite È possibile ricavare il valore del limite grazie al **teorema di De l'Hôpital**:

$$\lim_{\rho \rightarrow 0} \frac{E_0(\rho)}{\rho} = \left. \frac{d}{d\rho} E_0(\rho) \right|_{\rho=0}$$



Il calcolo di questa derivata non è semplicissimo quindi per semplicità si introducono le seguenti funzioni di appoggio:

$$f(\rho) = \sum_{y \in Y} \left[\left(\sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1+\rho}} \right] \right)^{1+\rho} \right]$$

$$g_y(\rho) = \sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1+\rho}} \right]$$

per cui:

$$\begin{aligned} E_0(\rho) &= -\log(f(\rho)) = \\ &= -\frac{1}{\ln 2} \cdot \ln(f(\rho)) \end{aligned}$$

cambio base:
 $\log_2(f(\rho)) = \frac{\ln(f(\rho))}{\ln(2)}$

$$f(\rho) = \sum_{y \in Y} \left[(g_y(\rho))^{\rho+1} \right]$$

Per semplicità si sostituisce la ρ con lo 0 il prima possibile. Quindi:

$$\begin{aligned} \left. \frac{d}{d\rho} E_0(\rho) \right|_{\rho=0} &= -\frac{1}{\ln 2} \cdot \left. \frac{d}{d\rho} \ln(f(\rho)) \right|_{\rho=0} = \\ &= -\frac{1}{\ln 2} \cdot \left. \frac{1}{f(\rho)} \cdot \frac{d}{d\rho} f(\rho) \right|_{\rho=0} \end{aligned}$$

$\frac{d \ln(f(\rho))}{d \rho} = \frac{1}{f(\rho)} \cdot \frac{df(\rho)}{d\rho}$

Dato che:

$$\begin{aligned} f(0) &= \sum_{y \in Y} \left[\left(\sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1}} \right] \right)^1 \right] = \\ &= \sum_{y \in Y} \sum_{x \in X} [P_X(x) \cdot P_{Y|X}(y|x)] = \\ &= \sum_{y \in Y} \sum_{x \in X} [P_{Y,X}(y,x)] = \\ &= 1 \end{aligned}$$

5. Teorema della codifica di canale

si ottiene:

$$\begin{aligned}
 \frac{d}{d\rho} E_0(\rho) \Big|_{\rho=0} &= -\frac{1}{\ln 2} \cdot \frac{1}{f(0)} \frac{d}{d\rho} \left[\sum_{y \in Y} \left[(g_y(\rho))^{\rho+1} \right] \right] \Big|_{\rho=0} \\
 \text{riscrivo con esponenziale} &= -\frac{1}{\ln 2} \cdot \sum_{y \in Y} \left[\frac{d}{d\rho} (g_y(\rho))^{\rho+1} \Big|_{\rho=0} \right] = \\
 \text{derivo rispetto a rho} &= -\frac{1}{\ln 2} \cdot \sum_{y \in Y} \left[\frac{d}{d\rho} e^{(\rho+1) \cdot \ln(g_y(\rho))} \Big|_{\rho=0} \right] = \quad \left| \begin{array}{l} y = e^{g(x) \cdot \ln(f(x))} \\ y' = e^{g(x) \cdot \ln(f(x))} \cdot [g'(x) \cdot \ln(f(x)) + g(x) \cdot \frac{1}{f(x)} \cdot f'(x)] \end{array} \right. \\
 \text{riscrivo l'esponenziale come} &= -\frac{1}{\ln 2} \cdot \sum_{y \in Y} \left[e^{(\rho+1) \cdot \ln(g_y(\rho))} \cdot \left(\ln(g_y(\rho)) + \frac{\rho+1}{g_y(\rho)} \cdot \frac{d}{d\rho} g_y(\rho) \right) \Big|_{\rho=0} \right] = \\
 &= -\frac{1}{\ln 2} \cdot \sum_{y \in Y} \left[g_y(\rho)^{\rho+1} \cdot \left(\ln(g_y(\rho)) + \frac{\rho+1}{g_y(\rho)} \cdot \frac{d}{d\rho} g_y(\rho) \right) \Big|_{\rho=0} \right]
 \end{aligned}$$

Dato che:

$$\begin{aligned}
 g_y(0) &= \sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1}} \right] = \\
 &= \sum_{x \in X} [P_X(x) \cdot P_{Y|X}(y|x)] = \\
 &= \sum_{x \in X} [P_{Y,X}(y,x)] = \\
 &= P_Y(y)
 \end{aligned}$$

si ottiene:

Piccole parentesi:

e quindi

$$E[\bar{P}_e] \leq 2^{-N \cdot E(R)} \xrightarrow[N \rightarrow \infty]{} 0 \quad \forall R: E(R) > 0$$

Quindi: $E(R) > 0 \quad \forall R < \lim_{\rho \rightarrow 0} \frac{E_0(\rho)}{\rho}$, che vale:

$$\begin{aligned}
 &\underbrace{\sum_y P_Y(y) \log_2 \frac{1}{P_Y(y)}}_{H(Y)} - \underbrace{\sum_y \sum_x P_X(x) P_{Y|X}(y|x) \log_2 \frac{1}{P_{Y|X}(y|x)}}_{H(Y|X)} = \\
 &= H(Y) - H(Y|X) = I(X;Y)
 \end{aligned}$$

È ne neopliemo $f_X(x)$ in modo da massimizzare $I(X;Y)$ si può concludere che:

$$E(\bar{P}_e) \leq 2^{-N E(R)} \xrightarrow[N \rightarrow \infty]{} 0 \quad \forall R < C$$

5. Teorema della codifica di canale

$$\begin{aligned}
 \frac{d}{d\rho} E_0(\rho) \Big|_{\rho=0} &= -\frac{1}{\ln 2} \cdot \sum_{y \in Y} \left[g_y(0)^{0+1} \cdot \left(\ln(g_y(0)) + \frac{1}{g_y(0)} \cdot \frac{d}{d\rho} g_y(\rho) \Big|_{\rho=0} \right) \right] = \\
 &= -\frac{1}{\ln 2} \cdot \sum_{y \in Y} \left[P_Y(y) \cdot \left(\ln(P_Y(y)) + \frac{1}{P_Y(y)} \cdot \frac{d}{d\rho} g_y(\rho) \Big|_{\rho=0} \right) \right] = \text{riscrivo la funzione secondo la formula precedente} \\
 &= -\frac{1}{\ln 2} \cdot \sum_{y \in Y} [P_Y(y) \cdot \ln(P_Y(y))] - \frac{1}{\ln 2} \cdot \sum_{y \in Y} \left[\frac{d}{d\rho} \sum_{x \in X} \left[P_X(x) \cdot (P_{Y|X}(y|x))^{\frac{1}{1+\rho}} \right] \right]_{\rho=0} = \\
 \text{1) } \frac{C_0(P_Y(y))}{\ln 2} &= \log_2(P_Y(y)) \\
 \text{2) } -\log_2(P_Y(y)) &= \log_2(P_Y(y)^{-1}) \\
 &= \log_2(\frac{1}{P_Y(y)}) \quad \Bigg| = \underbrace{\sum_{y \in Y} \left[P_Y(y) \cdot \log \frac{1}{P_Y(y)} \right]}_{H(Y)} - \frac{1}{\ln 2} \cdot \sum_{y \in Y} \sum_{x \in X} \left[P_X(x) \cdot \frac{d}{d\rho} e^{\frac{1}{1+\rho} \cdot \ln P_{Y|X}(y|x)} \Big|_{\rho=0} \right] = \text{riscrivo la funzione come esponenziale} \\
 &= H(Y) - \frac{1}{\ln 2} \cdot \sum_{y \in Y} \sum_{x \in X} \left[P_X(x) \cdot e^{\frac{1}{1+\rho} \cdot \ln P_{Y|X}(y|x)} \cdot \ln P_{Y|X}(y|x) \cdot \frac{d}{d\rho} \frac{1}{1+\rho} \Big|_{\rho=0} \right] = \Bigg| \frac{d}{d\rho} (e^{f(\rho)}) = e^{f(\rho)} \cdot f'(\rho) \\
 &= H(Y) - \frac{1}{\ln 2} \cdot \sum_{y \in Y} \sum_{x \in X} \left[P_X(x) \cdot P_{Y|X}(y|x) \cdot \ln P_{Y|X}(y|x) \cdot \frac{d}{d\rho} (1+\rho)^{-1} \Big|_{\rho=0} \right] = \\
 \text{1) } \frac{C_0(P_Y(y))}{\ln 2} &= \log_2(P_Y(y)) \\
 \text{2) } -\log_2(P_Y(y)) &= \log_2(P_Y(y)^{-1}) \\
 &= \log_2(\frac{1}{P_Y(y)}) \quad \Bigg| = \underbrace{\frac{1}{\ln 2} \cdot \sum_{y \in Y} \sum_{x \in X} \left[P_{Y,X}(y,x) \cdot \ln P_{Y|X}(y|x) \cdot -(1+\rho)^{-2} \Big|_{\rho=0} \right]}_{H(Y|X)} = \\
 &= H(Y) - \underbrace{\sum_{y \in Y} \sum_{x \in X} \left[P_{Y,X}(y,x) \cdot \log \frac{1}{P_{Y|X}(y|x)} \right]}_{H(Y|X)} = \\
 &= H(Y) - H(Y|X) = \\
 &= I(X; Y)
 \end{aligned}$$

Quindi nel migliore dei casi, ossia scegliendo una distribuzione di X che massimizza questo limite, si ottiene che:

$$\max_{P_X} \lim_{\rho \rightarrow 0} \frac{E_0(\rho)}{\rho} = \max_{P_X} I(X; Y) = C$$

- è il limite massimo oltre al quale $E(R) = 0$
- questo perché aumentando R oltre a C l'errore medio non cambia

dove C è la capacità del canale, quindi:

- Se $R > C$ non è possibile diminuire a piacere l'errore medio.
- Se $R \leq C$ è possibile diminuire a piacere l'errore medio aumentando il valore della lunghezza delle sequenze N .

5.5. Conclusioni sul teorema

Il teorema di Shannon propone una soluzione che permette di trasmettere informazione su un canale che presenta delle imperfezioni. Tale soluzione consiste nell'inviare sequenze lunghe N contenenti $N \cdot R$ (con $0 < R \leq C$) bit di informazione, in questo modo alzando N è possibile diminuire a piacimento l'errore medio di trasmissione, come dimostrato precedentemente.

Questa soluzione richiede che il ricevitore conosca quali siano le sequenze lecite e quali siano quelle sbagliate, in modo da distinguerle. Questo crea un problema realizzativo in quanto Shannon non propone nessun modo per generare i codici: teoricamente questi possono essere scelti casualmente e salvati in una tabella di conversione e se l'errore medio è troppo alto allora basta cambiare codifica e sceglierne altri casualmente, ma più lunghi.

5. Teorema della codifica di canale

Questo approccio non è attuabile in pratica perché richiederebbe l'utilizzo di tabelle lunghissime e quindi di dispositivi che tengano in memoria tantissimi dati; anche computazionalmente la ricerca di una sequenza all'interno di una tabella così grande sarebbe molto dispendiosa. Per questo motivo è necessario trovare un altro sistema per la generazione di codici, ossia qualcosa che permetta di generarli partendo dall'informazione che si vuole inviare e che allo stesso modo sia possibile estrarre dal codice ricevuto l'informazione contenuta.

$$N = 10^4 \quad R = 0.9 \rightarrow N = 2^{NL} = 2^{8000}$$

sequenze che 10^4 bit sono, cioè circa

$$10^4 \cdot (10^4)^{800} = 10^4 \cdot (10^3)^{800} = 10^{1600} \text{ bit} \approx 10^{1491} \text{ TB}$$

N : lunghezza sequenze codificate

R : rete $R = \frac{K}{N}$

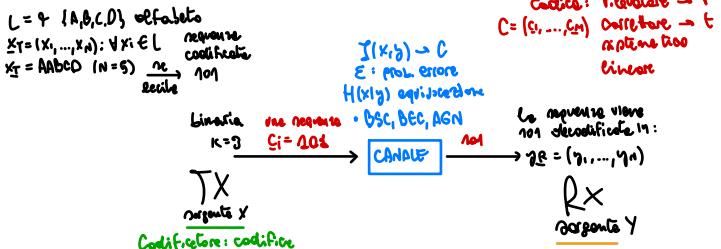
N : $2^K = q^{L \cdot N}$ = combinazioni sequenze lette in ingresso, prima delle codifiche

L : q binario {0,1}

Abbia finito il capitolo 1
del professore Bellini

- riordinare le sequenze in maniera tale che ogni adiacente differiscono di 1 bit, dove in totale sono 2^N sequenze
- il codice rappresenta in questa catena di sequenze tutte le possibili sequenze che sono quelle valide
- quelle che rimangono fuori, sono tutte le sequenze che posso ricevere dal canale se $d = 5$ le sequenze intermedie non possono appartenere a C
- introducendo la 4 e la 5 sequenza sicuramente la sequenza corretta è al 6 la stessa cosa sopra il massimo numero di errori che sono sicuro di poter correggere è circa $t = \lfloor (d-1)/2 \rfloor$ solo questo caso se $d = 5$ allora $t = 2$, cioè d pari il codificatore a ML quando trova un paragone sceglie a caso e può sbagliare

DEF: Un codice $C = \{c_1, c_2, \dots, c_N\}$ dove $c_i = [c_{i1}, c_{i2}, \dots, c_{iN}]$ è una sequenza di N bit. c_i è LINEARE se ogni bit c_{ij} si può calcolare come combinazione lineare delle (algebra 2018) dei bit in informazione $\underline{x} = [x_1, x_2, \dots, x_K]$, dove $K = N - t$ e $R = K/t$ è il tasso di trasmissione, nel canale, associato alla sequenza \underline{x} .



6. Codici per la trasmissione

6.1. Concetti generali

Codici usati come rivelatori I decodificatori di questi codici si limitano ad identificare l'errore di trasmissione, controllando solo che la sequenza ricevuta sia lecita oppure no. In genere in caso di errore di trasmissione viene richiesta la ritrasmissione.

$$r = d - 1, \text{ dove } d = \text{distanza minima di } C$$

Per questa tipologia di codici viene definito il potere rivelatore r come il numero massimo di errori che il decodificatore è in grado di rilevare.

Se il decodificatore riceve un messaggio con più di r errori non si può avere la certezza che questo sia in grado di capire che il messaggio è sbagliato.

Codici usati come correttori I decodificatori di questi codici sono in grado di correggere gli eventuali errori di trasmissione, scegliendo la sequenza lecita che massimizza la verosimiglianza.

Per questa tipologia di codici viene definito il potere correttore t come il numero massimo di errori che il decodificatore è in grado di correggere.

$$\text{con } t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

Se il decodificatore riceve un messaggio con più di t errori non si può avere la certezza che la sequenza scelta dal decodificatore sia corretta.

Osservazioni

- Solitamente il potere correttore è inferiore a quello rivelatore in quanto la correzione è un'operazione più complicata.
- La scelta di quale ricevitore usare si basa sul tipo di applicazione; per esempio se la ritrasmissione non è possibile i codici correttori sono essenziali, se invece questa è molto veloce potrebbe essere più comodo usare un codice rivelatore in quanto ha un potere maggiore (per l'osservazione precedente).

Definizione di codice sistematico Un codice si dice sistematico se e solo se i bit di informazione i sono un sottoinsieme dei bit del codice corrispettivo c . \Rightarrow $c = \begin{bmatrix} u \\ p \end{bmatrix}$ p sono i bit di parità

con u in posizioni prefissate, di solito nella parte dx di c ma di seguito sono considerate a sx

Definizione di bit di parità In un codice sistematico i bit di c aggiunti a quelli di i si definiscono bit di parità.

Osservazione In un codice binario sistematico ci sono sempre $N - K$ bit di parità.

6.2. Codifiche lineari

$C = \{c_1, \dots, c_M\}$: codice è determinato da M (sequenze lecite) ci
 $c_i = (c_{i1}, \dots, c_{iN})$: ogni ci è una sequenza di N bit

È una sequenza di N bit
 $C = (c_0, c_1, \dots, c_{N-1})$

Definizione di codice lineare Un codice si dice lineare se le sequenze lecite del codice $c = (c_1, c_2, \dots, c_N)$ sono calcolate attraverso una combinazione lineare dei bit di informazione $i = (i_1, i_2, \dots, i_K)$.

dove la somma e il prodotto seguono la logica dell'algebra XOR

il professore al posto di i usa u, infatti: $u = (u_0, u_1, \dots, u_{K-1})$

Osservazione Dato che i simboli delle sequenze i sono bit i coefficienti della combinazione lineare sono anch'essi bit e quindi ogni elemento c_n del codice si ricava tramite la somma di qualche bit della sequenza i , utilizzando la logica XOR, ossia:

$$0 + 0 = 1 + 1 = 0$$

$$1 + 0 = 0 + 1 = 1$$

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

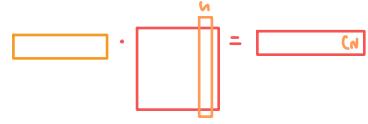
$$1 \cdot 1 = 1$$

6.2.1. Notazione matriciale

Definizione di matrice generatrice Per ogni codice lineare si definisce la matrice generatrice $\underline{\underline{G}}$ tale che, data una sequenza \underline{i} , si può ottenere il codice corrispondente facendo:

$$\underline{c} = \underline{i} \cdot \underline{\underline{G}}_{1 \times N \text{ } 1 \times K \text{ } K \times N}$$

l'immagine mostra un
quadrato con le cifre 1, 0, 1, 1
e questo è lineare.



Osservazioni

$L=2 \quad \{0,1\}$

- Dato che i simboli delle sequenze sono bit i coefficienti della matrice $\underline{\underline{G}}$ sono anch'essi bit.
- L' n -esima colonna della matrice $\underline{\underline{G}}$ è un vettore che contiene un 1 in corrispondenza dei bit che vanno sommati per formare l'elemento c_n .
- Dato che esiste la sequenza $\underline{i} = \underline{0}$ in un codice lineare il codice $\underline{c} = \underline{0}$ è sempre lecito.
- Tutte le righe della matrice generatrice fanno parte del codice perché basta scegliere $\underline{i} = \underline{e}_n$. : vettore base canonica sto scegliendo come codice la riga n -esima
- Se \underline{c} è un codice lecito allora esiste \underline{i} tale che $\underline{c} = \underline{i} \cdot \underline{\underline{G}}$.

Proposizione Se \underline{c}_1 e \underline{c}_2 sono codici leciti per un codice lineare allora $\underline{c}_1 + \underline{c}_2$ è anch'esso un codice lecito.

stiamo sommando i bit di informazioni di due sequenze lecrite. Si tratta di una combinazione lineare.

Dimostrazione Dato che \underline{c}_1 e \underline{c}_2 sono codici leciti allora esistono due sequenze \underline{i}_1 e \underline{i}_2 tali che:

$$\underline{c}_1 = \underline{i}_1 \cdot \underline{\underline{G}}$$

$$\underline{c}_2 = \underline{i}_2 \cdot \underline{\underline{G}}$$

quindi:

$$\underline{c}_1 + \underline{c}_2 = \underline{i}_1 \cdot \underline{\underline{G}} + \underline{i}_2 \cdot \underline{\underline{G}} = (\underline{i}_1 + \underline{i}_2) \cdot \underline{\underline{G}}$$

e quindi anche $\underline{c}_1 + \underline{c}_2$ è un codice lecito.

Osservazione Tutte le sequenze \underline{i} possono essere viste come:

$$\underline{i} = \sum_{j=1}^K i_j \cdot \underline{e}_j$$

combinazione lineare

: a causa dell'algebra XOR
: $0 \times 1 = 0$
: $1 \times 1 = 1$

e quindi:

$$\begin{aligned} \underline{c} &= \underline{i} \cdot \underline{\underline{G}} = \\ &= \left(\sum_{j=1}^K i_j \cdot \underline{e}_j \right) \cdot \underline{\underline{G}} = \\ &= \sum_{j=1}^K (i_j \cdot \underline{e}_j \cdot \underline{\underline{G}}) \end{aligned}$$

quindi tutte le sequenze lecite \underline{c} possono essere ottenute sommando varie combinazioni delle righe della matrice $\underline{\underline{G}}$.

Definizione di matrice di parità Per ogni codice lineare si definisce matrice di parità $\underline{\underline{H}}$ la matrice $N \times (N - K)$ tale che:

$$\underline{c}_{1 \times N} \cdot \underline{\underline{H}}_{N \times (N-K)} = \underline{w}_{1 \times (N-K)}$$

dove $\underline{w} = \underline{0}$ se e solo se il codice \underline{c} è lecito.

oss: $\underline{c} \cdot \underline{\underline{H}} = (\underline{A} \cdot \underline{\underline{G}}) \cdot \underline{\underline{H}} = \underline{0}$
 $\underline{A} \cdot \underline{\underline{G}} = \underline{c}$ $\Rightarrow \underline{\underline{G}} \cdot \underline{\underline{H}} = \underline{0}$

Osservazione

- Questa matrice viene usata dal ricevitore per capire se la sequenza arrivata è corretta oppure no.
- A volte viene usata la sua versione trasposta, ossia $\underline{\underline{H}}^T$:

$$\begin{aligned} \left(\underline{c} \cdot \underline{\underline{H}} \right)^T &= \underline{w}^T \\ \underline{\underline{H}}^T \cdot \underline{c}^T &= \underline{w}^T \end{aligned}$$

che è del tutto equivalente.

Matrice di generazione di un codice lineare sistematico Dato che i bit di i sono un sottoinsieme dei bit del codice \underline{c} la matrice generatrice deve contenere la matrice identità $\underline{\underline{I}}$ di dimensione $K \times K$ affiancata da una matrice $\underline{\underline{P}}$ di dimensione $K \times (N - K)$ per la generazione dei bit di parità, ossia:

$$\underline{\underline{G}} = \begin{bmatrix} \underline{\underline{I}} & \underline{\underline{P}} \\ K \times K & K \times (N-K) \end{bmatrix}$$

Injetive
le matrici

Osservazione Dato una sequenza \underline{i} il codice corrispettivo è:

$$\begin{aligned} \underline{c} &= \underline{i} \cdot \underline{\underline{G}} = \\ &= \underline{i} \cdot \begin{bmatrix} \underline{\underline{I}} & \underline{\underline{P}} \end{bmatrix} = \\ &= \begin{bmatrix} \underline{i} \cdot \underline{\underline{I}} & \underline{i} \cdot \underline{\underline{P}} \end{bmatrix} = \\ &= \begin{bmatrix} \underline{i} & \underline{i} \cdot \underline{\underline{P}} \end{bmatrix} \end{aligned}$$

Matrice di parità di un codice lineare sistematico In un codice sistematico lineare la matrice di parità è:

$$\underline{\underline{H}} = \begin{bmatrix} \underline{\underline{P}} \\ K \times (N-K) \\ \underline{\underline{I}} \\ (N-K) \times (N-K) \end{bmatrix}$$

Dimostrazione Sia \underline{c} un codice lecito allora esiste una sequenza \underline{i} tale che:

$$\underline{c} = \begin{bmatrix} \underline{i} & \underline{i} \cdot \underline{\underline{P}} \end{bmatrix}$$

quindi:

$$\begin{aligned} \underline{c} \cdot \underline{\underline{H}} &= \begin{bmatrix} \underline{i} & \underline{i} \cdot \underline{\underline{P}} \end{bmatrix} \cdot \begin{bmatrix} \underline{\underline{P}} \\ \underline{\underline{I}} \end{bmatrix} = \\ &= \begin{bmatrix} \underline{i} \cdot \underline{\underline{P}} + \underline{i} \cdot \underline{\underline{P}} \end{bmatrix} \end{aligned}$$

dato che sono tutti bit e che $0 + 0 = 0$ e $1 + 1 = 0$ si ha che:

$$\underline{c} \cdot \underline{\underline{H}} = \underline{\underline{0}}$$

6.2.2. Notazione polinomiale

- data una sequenza binaria con coefficienti GF(2)
- il prodotto tra polinomi deve avere coefficienti binari ossia devo ridurli modulo 2

Definizione di notazione polinomiale Dato un codice $(c_0, c_1, \dots, c_{N-2}, c_{N-1})$ in notazione polinomiale si associa il polinomio

$$c(x) = c_{N-1} \cdot x^{N-1} + c_{N-2} \cdot x^{N-2} + \dots + c_1 \cdot x + c_0$$

questo polinomio ha sempre grado inferiore a N . Analogamente si può associare un polinomio anche ai bit di informazione

$$i(x) = i_{K-1} \cdot x^{K-1} + i_{K-2} \cdot x^{K-2} + \dots + i_1 \cdot x + i_0$$

ottenendo un polinomio di grado inferiore a K .

6. Codici per la trasmissione

Definizione di polinomio generatore

Il polinomio $g(x)$ si dice generatore del codice $c(x)$ se e solo se $c(x)$ è divisibile per $g(x)$.

$$C(x) \in \mathbb{C} \iff c(x) \text{ è divisibile per } g(x)$$

Osservazione

- Il codice lecito $c(x)$ abbinato a $i(x)$ è:

grado $\leq N - 1$ grado $\leq N - K$ grado $\leq K - 1$

$$c(x) = g(x) \cdot i(x)$$

OSS: i bit ci sono combinazioni lineari di bit ui con coefficienti si \Rightarrow C è lineare \Rightarrow potrei descriverlo tramite la sua matrice. Ma non è vero il viceversa, cioè che qualsiasi codice lineare si possa rappresentare in forma polinomiale.

- Dato che i $c(x)$ hanno grado inferiore a N e che $i(x)$ ha grado inferiore a K il polinomio generatore $g(x)$ deve avere grado $N - K$.
- La notazione matriciale e polinomiale sono equivalenti e ogni codice può essere definito sia tramite la matrice generatrice G sia tramite il polinomio generatore $g(x)$.

Codici sistematici in notazione polinomiale Utilizzando la formula espressa prima, i codici generati non sono sistematici e quindi per poter generare un codice sistematico dal polinomio generatore $g(x)$ si utilizza la formula:

$$c(x) = x^{N-K} \cdot i(x) - \text{Resto} \left[\frac{x^{N-K} \cdot i(x)}{g(x)} \right] \quad \begin{array}{l} \text{generazione di} \\ \text{un codice lecito} \end{array}$$

che è divisibile per $g(x)$ perché al polinomio $x^{N-K} \cdot i(x)$ viene rimosso il resto delle divisione tra lui e $g(x)$, ottenendo un valore divisibile per $g(x)$.

Osservazioni

- Dato che i simboli sono tutti binari fare la sottrazione o la somma è equivalente e quindi:

$$\begin{aligned} c(x) &= x^{N-K} \cdot i(x) - \text{Resto} \left[\frac{x^{N-K} \cdot i(x)}{g(x)} \right] = \\ &= x^{N-K} \cdot i(x) + \text{Resto} \left[\frac{x^{N-K} \cdot i(x)}{g(x)} \right] \end{aligned}$$

- Moltiplicare per x^{N-K} equivale a shiftare di $N - K$ posti i bit e quindi si pongono in testa i bit di informazione, come si vuole in un codice sistematico, mentre gli altri bit vengono definiti dal resto che è sicuramente un polinomio di grado inferiore a quello di $g(x)$ ossia $N - K$, che sono i bit di parità.

Definizione Un codice si definisce ciclico se il polinomio generatore $g(x)$ è un divisore di $x^N - 1$.

$$(x^N - 1) \text{ mod } g(x) = 0$$

Significato di codice ciclico Un codice ciclico ha la proprietà che preso un codice lecito, eseguendo un numero qualsiasi di shift si ottiene ancora un codice lecito, infatti dato un codice lecito $c(x) = c_{N-1} \cdot x^{N-1} + \dots + c_1 \cdot x + c_0$ per fare un uno shift:

- Si moltiplica per x in modo da ottenere $c_{N-1} \cdot x^N + \dots + c_1 \cdot x^2 + c_0 \cdot x$ | **eseguo lo shift del codice**
- Si aggiunge il bit c_{N-1} all'inizio della sequenza quindi facendo $c(x) \cdot x + c_{N-1}$ | **Riduzione modulo x^N :**
se sommo/tolgo il termine di più alto grado e aggiungo la costante tolta grazie alla proprietà del codice ciclico
- Si toglie il termine $c_{N-1} \cdot x^N$ facendo $c(x) \cdot x + c_{N-1} + c_{N-1} \cdot x^N$

quindi la nuova sequenza si ottiene facendo

$$\begin{aligned} c'(x) &= c(x) \cdot x + c_{N-1} + c_{N-1} \cdot x^N \\ &= c(x) \cdot x + c_{N-1} \cdot (1 + x^N) \quad \equiv (1-x^N) \end{aligned}$$

$$\begin{array}{l} \text{C}'(x) \text{ è una notazione ciclica se:} \\ \text{C}'(x) \text{ mod } (x^N + 1) = C(x) \cdot x \\ C(x) \cdot x \text{ mod } g(x) = 0 \\ C(x) \subseteq C \end{array}$$

Si può notare che $c'(x)$ è divisibile per $g(x)$ infatti:

- $c(x)$ è un codice lecito e quindi è divisibile per $g(x)$ e di conseguenza lo è anche $c(x) \cdot x$
 - Per definizione $1 + x^N$ è divisibile per $g(x)$ e quindi lo è anche $c_{N-1} \cdot (1 + x^N)$
- quindi anche $c'(x)$ è divisibile per $g(x)$ e quindi è un codice lecito.

6.2.3. Codificatore di un codice lineare sistematico

Circuito di codifica Dato un codice $C(N, K)$ lineare con polinomio generatore $g(x) = g_{N-K} \cdot x^{N-K} + \dots + g_1 \cdot x + g_0$ allora data una sequenza di informazione $i(x) = i_{K-1} \cdot x^{K-1} + \dots + i_1 \cdot x + i_0$ è possibile ricavare la sequenza di codice sistematico corrispettiva tramite un circuito con $N - K$ flip-flop. Il circuito è mostrato schematicamente in figura 6.1.

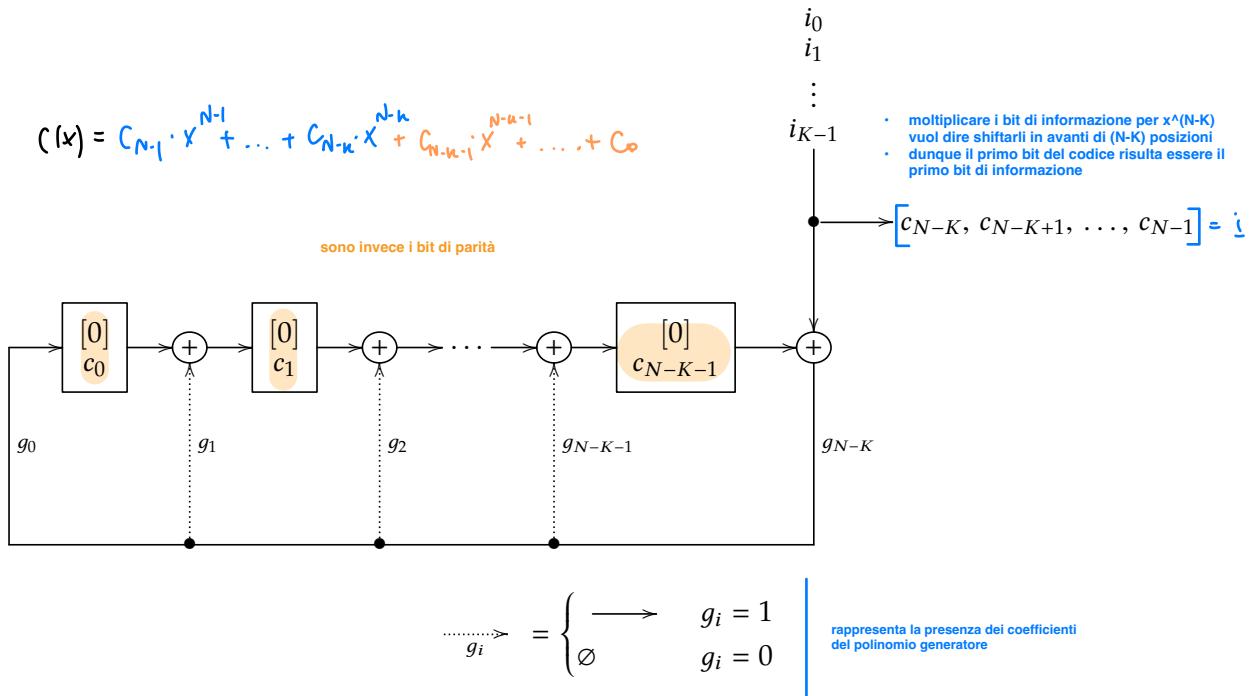


Figura 6.1.: Circuito per la codifica di un codice lineare sistematico; il valore tra parentesi quadre è il valore di inizializzazione dei flip-flop.

Esempio di funzionamento del codificatore Per comprendere meglio il funzionamento di questo circuito si consideri un codice di Hamming $C(7, 4)$ con $g(x) = x^3 + x + 1$ e si supponga di voler codificare la sequenza $i(x) = x^3 + x$. Analiticamente bisogna trovare il resto tra $i(x) \cdot x^{N-K} = x^6 + x^4$ e $g(x)$:

$$c(x) = x^{N-K} \cdot i(x) - \text{Resto} \left[\frac{x^{N-K} \cdot i(x)}{g(x)} \right] = x^{N-K} \cdot i(x) + \text{Resto} \left[\frac{x^{N-K} \cdot i(x)}{g(x)} \right]$$

x^6	$+x^4$	x^3	$x^3 + x + 1$
x^6	$+x^4$	$+x^3$	$x^3 + 1$
<hr/>			$x^3 + 1$
x^3	x^3	$+x$	$+1$
<hr/>			x
			$+1$

$f(x) = x^3 + x + 1$ grado $N-k$
 $i(x) = x^3 + x$ grado $k-1$
 $C(x)$ grado $N-1$
 da cui $C(N, k)$
 $\begin{cases} N=7 \\ k=4 \end{cases} \Rightarrow \begin{cases} i primi 4 bit saranno i bit di informazione \\ mentre gli ultimi 3 biti di parità \end{cases}$

e quindi si ha che:

$$c(x) = x^6 + x^4 + x + 1$$
 $c = (1, 0, 1, 0, 0, 1, 1)$

Il funzionamento del circuito è mostrato in figura 6.2.

6. Codici per la trasmissione

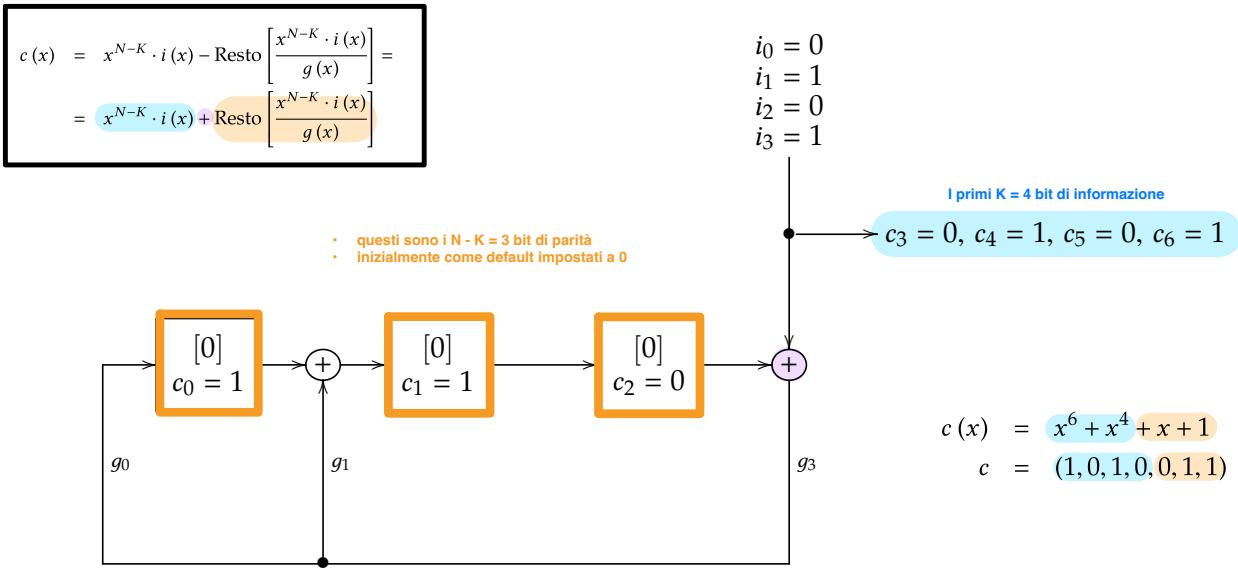


Figura 6.2.: Circuito per la codifica di un codice di Hamming.

6.2.4. Decodificatore di un codice lineare sistematico

Circuito di codifica Dato un codice $C(N, K)$ lineare con polinomio generatore $g(x) = g_{N-K} \cdot x^{N-K} + \dots + g_1 \cdot x + g_0$ allora data una sequenza generica $v(x) = v_{N-1} \cdot x^{N-1} + \dots + v_1 \cdot x + v_0$ è possibile ricavare il resto della divisione tra $v(x)$ e $g(x)$ che può essere usato per capire se $v(x)$ è una sequenza di codice tramite un circuito con $N - K$ flip-flop. Il circuito è mostrato schematicamente in figura 6.3.

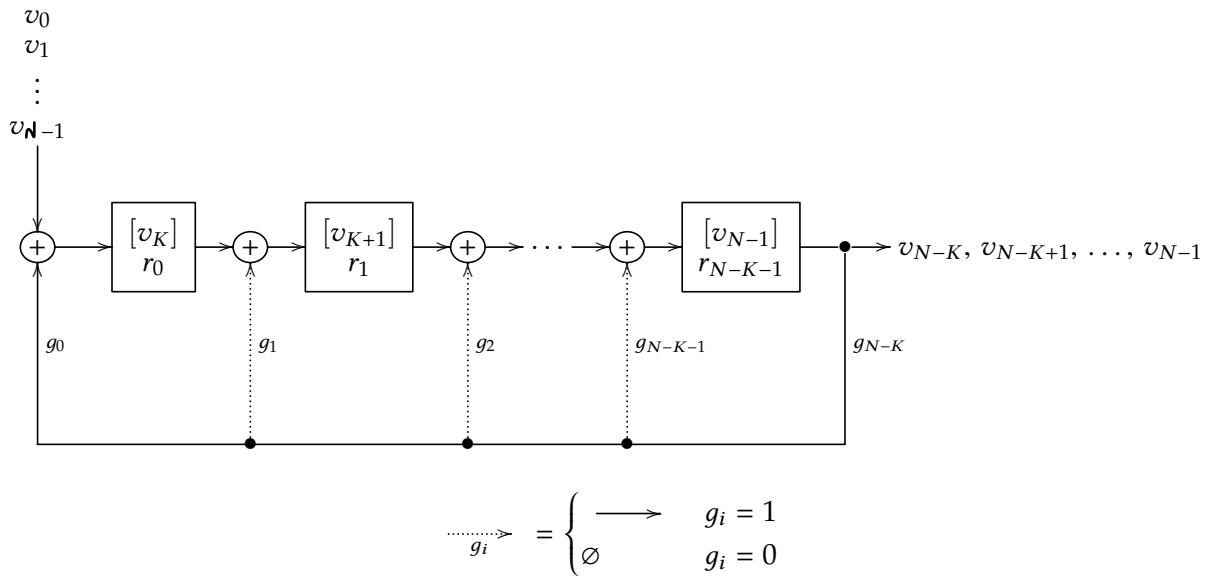


Figura 6.3.: Circuito per la decodifica di un codice lineare sistematico; il valore tra parentesi quadre è il valore di inizializzazione dei flip-flop.

Il circuito mostrato, tuttavia, in genere non è grado di correggere la sequenza, l'unica eccezione sono i codici di Hamming in cui il resto indica la riga della matrice di parità del bit da cambiare.

Esempio di funzionamento del codificatore Per comprendere meglio il funzionamento di questo circuito si consideri un codice di Hamming $C(7, 4)$ con $g(x) = x^3 + x + 1$ e si supponga di aver ricevuto la sequenza $v(x) = x^6 + x^4 + x^2 + 1$. Analiticamente si ottiene:

data una sequenza di ordine $N - 1$ capire se è di codice lecito o meno

6. Codici per la trasmissione

$$\begin{array}{r}
 \begin{array}{ccccc}
 x^6 & +x^4 & +x^2 & & \\
 x^6 & +x^4 & +x^3 & & \\
 \hline
 & & x^3 & +x^2 & 1 \\
 & & x^3 & +x & +1 \\
 \hline
 & & x^2 & +x &
 \end{array} & \left| \begin{array}{c} 1 \\ x^3+x+1 \\ x^3+1 \\ \hline \end{array} \right.
 \end{array}$$

e quindi si ha che:

$$r(x) = x^2 + x$$

Il funzionamento del circuito è mostrato in figura 6.4.

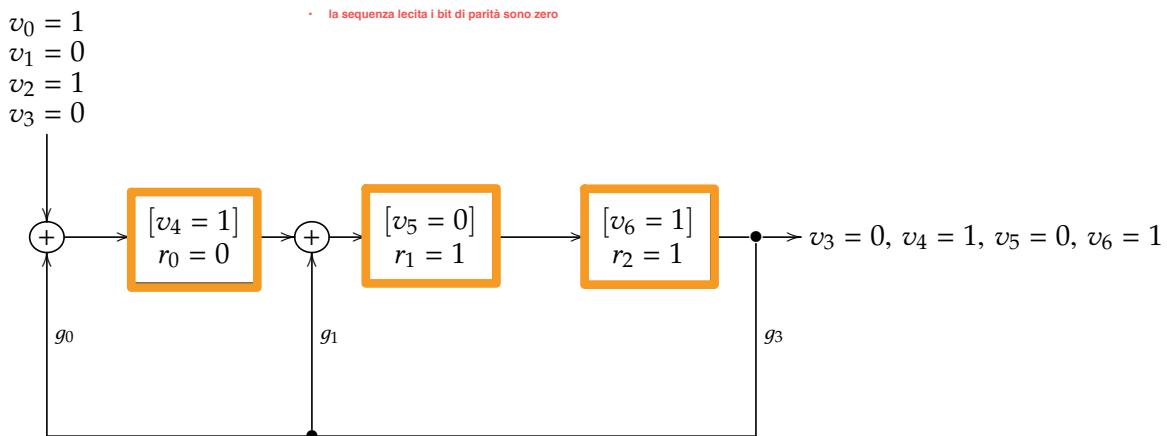


Figura 6.4.: Circuito per il calcolo del resto di un codice di Hamming.

Oss: ogni codice polinomiale in quanto lineare ammette la rappresentazione matriciale, ma non viceversa

Perfondendo che un codice $C(N, K, d)$ mi permetta ottenere

2 versioni:

- 1) ACCORDATE (Now mi vanno bene N e K definite da questo codice): se codice C di parametri $(N-a, K-a, d)$, utilizzando solo K -e bit e restando a bit e rimanenti;

- 2) ESENTE: se codice C di parametri $(N-t, K, d)$ aggiungendo un bit di parità complessivo somma di tutti i bit delle paritate di C , con $t > d$ e in particolare $t=d+1$ se d è dispari (che avviene spesso)

Esempio: se un $H(31, 26, 3) \rightarrow H(31, 26, 3)$ per avere K potenze di 2.

Esempio: se un $H(63, 57, 3) \rightarrow H(64, 57, 4)$

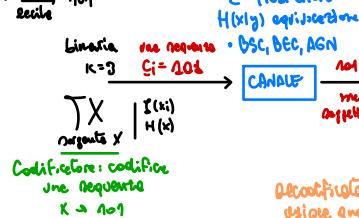
Rivelatore di $t=3$ err.

Connettore di errore e rivelatore di $t=2$ err.

Protezioni di codici binari:

- 1) Probabilità di mancata correzione $\rightarrow P_e$
- 2) Probabilità di errore nel bit all'uscita del decodificatore $\rightarrow P_d$
- 3) Probabilità di mancata rivelazione di errore $\rightarrow P_r$

$L = \{A, B, C, D\}$ alfabeto
 $X_T = (X_1, \dots, X_N); \forall X_i \in L$ sequenze
 $X_T = AABCD (N=5) \xrightarrow{\text{decodificare}} 101$



N lunghezza sequenza
 k bit di info col in canale
 R rate: $\frac{k}{N}$
 M combinazioni legate: 2^k

$$(N \geq 2^k \quad n \log L \geq k)$$

Codice: rilevabile $\rightarrow r$
 $C = \{c_1, \dots, c_m\}$ correttore $\rightarrow t$
 rappresentato $\forall c \in C \Rightarrow c = \sum_{i=1}^{N-r} f_i$
 binario: G, H
 circolare: $(x^d + 1) \text{ mod } g(x) = 0$

Lo sorgente viene
 noi decodificata in:
 $\xrightarrow{\text{C decodifica } G}$
 $\xrightarrow{\text{S, H}}$

$$R_X \xrightarrow{\text{sorgente } Y}$$

Il codificatore è integrato nel ricevitore che
 ha il compito di verificare e se necessario
 correggere la sequenza ricevuta durante la
 trasmissione

- Riconducente
- errore nel singolo bit

Secondo Shannon:

$$I(X) = \log \left(\frac{1}{P(X)} \right)$$

• Teoria di Shannon:

$$\sum P_i(x_i) \cdot h(x_i) = \bar{h}(x) \geq H(x)$$

(limite di Shannon)

Teoria delle codifiche del canale:

$$\begin{aligned} E_p(P_{\text{canale}}(x)) &\leq 2^{N \cdot R_p - E_p(R_p) \cdot N} \\ &= 2^{-N(E_p(R_p) - R_p)} \\ &= 2^{-N E(R_p)} \end{aligned}$$

- $E_p(P_{\text{canale}}(x)) \leq N \uparrow \text{per } E(R_p) > 0$
 - $R_p \uparrow E(R_p) \downarrow \text{per } E(p) \downarrow E_p(P_{\text{canale}}(x)) \uparrow$
- ma $\lim_{p \rightarrow 0} \frac{E_p(R_p)}{p} = \lim_{p \rightarrow 0} I(x|p) = C$
- $\rightarrow \text{se } R_p > C \uparrow N \quad E_p(P_{\text{canale}}(x)) \text{ invariato}$
- $\rightarrow \text{se } R_p \leq C \uparrow N \quad E_p(P_{\text{canale}}(x)) \downarrow$

Codice Lineare:

$\exists C \subseteq \mathbb{F}$ matrice da generazione: $\underline{c} = \underline{i} \cdot \underline{G}$
 $\&$ decodico me: $\underline{c} \cdot \underline{H} = \underline{w}$ dove $\underline{w} = \underline{u} - \underline{v}$

Codice Lineare riassettivo:

$$\underline{G} = \begin{bmatrix} \underline{I} & \underline{P} \end{bmatrix}_{n \times n} \quad \underline{H} = \begin{bmatrix} \underline{P} \\ \underline{I} \end{bmatrix}_{(N-n) \times (N-n)}$$

$$\underline{H} = \begin{bmatrix} \underline{P} \\ \underline{I} \end{bmatrix}_{(N-n) \times (N-n)}$$

No borsone esponentiale

$\underline{c} = (c_1, \dots, c_{N-n})$ lungo n

$$\begin{aligned} C(x) &= c_{N-n} x^{N-n} + \dots + c_1 x + c_0 & (N-n) \\ i(x) &= i_{N-n} x^{N-n} + \dots + i_1 x + i_0 & (N-n) \end{aligned}$$

Polinomio generatore: $\exists \underline{g} \in C \Rightarrow C(x) \text{ mod } g(x) = 0$
 del codice C $g(x)$ ha grado $(N-n)$

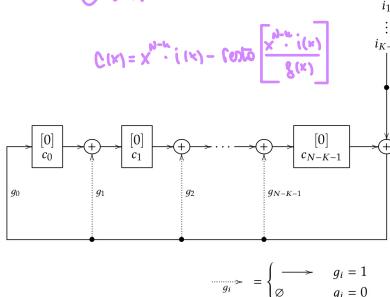
codice: $C(x) = i(x) \cdot g(x)$

bit di info.

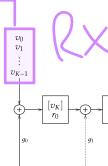
codice: $C(x) = x \cdot i(x) \sim \text{resto} \left[\frac{x^{N-n}; i(x)}{g(x)} \right]$

bit di parità

Codificatore



TX



Decodificatore:

$$\text{Se } \frac{J(x)}{g(x)} = 0 \Rightarrow J(x) \text{ decodito} \quad J(x) \in C$$

Campi finiti di Galois

Proprietà	Galois
ciclico	\Rightarrow generatore α^n

$$E_j = \sum_{h=0}^{N-1} e_h \cdot \beta^{jh}$$

$$E = [e_0, \dots, e_{N-1}] \rightarrow E = [E_0, \dots, E_{N-1}]$$

$$E = [0, \dots, 1, \dots, 1, \dots, 0]$$

Dato un codice di Hamming:
 $d \rightarrow d-n$ elementi nulli
 consecutivi in E

$$e(x) = e_{m-1} x^{m-1} + \dots + e_0$$

$$e(\beta) = 0 \Rightarrow E_j = 0 \rightarrow$$

$$y(x) = \prod_{j=1}^{N-1} (x - \beta^j) + \text{polinomio minimo } v(\beta)$$

l'essere viene rivelato proprio \uparrow
 la posizione (j)

$$E = [E_0, \dots, E_1, \dots, E_{N-1}]$$

de ho un errore
 in posizione E_6
 \downarrow
 allora le termini
 β^6 appaiono nelle
 finalizzate
 \Downarrow
 posso dunque correggere
 E_6 con l'info di S

$$\begin{array}{cc} \text{incognite:} & \begin{array}{c} E_1 \\ \vdots \\ E_6 \\ \vdots \\ E_{N-1} \end{array} \\ \begin{array}{c} E_1 \\ \vdots \\ E_6 \\ \vdots \\ E_{N-1} \end{array} & \end{array}$$

$$\begin{array}{cc} \text{incognite:} & \begin{array}{c} E_1 \\ \vdots \\ E_6 \\ \vdots \\ E_{N-1} \end{array} \\ \begin{array}{c} E_1 \\ \vdots \\ E_6 \\ \vdots \\ E_{N-1} \end{array} & \end{array}$$

$$E_6 = d^2 \rightarrow \begin{array}{c} \text{posizione } \beta^6 \\ \text{Jolare } = d^2 \end{array}$$

$$g(x) = (x-\lambda)(x-d_1)$$

$$J_1 = E_1 + C_1 = E_1 \quad \text{Sintesi } J_0 = 1$$

$$J_2 = E_2 + C_2 = E_2 \quad \text{Sintesi } J_1 = 0$$

$$J_3 = E_3 + C_3 = E_3 \quad \text{Sintesi } J_2 = 0$$

$$J_4 = E_4 + C_4 = E_4 \quad \text{Sintesi } J_3 = 0$$

$$J_5 = E_5 + C_5 = E_5 \quad \text{Sintesi } J_4 = 0$$

$$J_6 = E_6 + C_6 = E_6 \quad \text{Sintesi } J_5 = 0$$

$$J_7 = E_7 + C_7 = E_7 \quad \text{Sintesi } J_6 = 0$$

$$J_8 = E_8 + C_8 = E_8 \quad \text{Sintesi } J_7 = 0$$

7. Algebra dei campi finiti di Galois

7.1. Definizione di campo finito

Un campo $GF(q)$ è un gruppo di q elementi^{dunque finito} su cui sono definite le operazioni binarie «+» (somma) e «·» (prodotto) per cui valgono le seguenti proprietà:

- Chiusura:

$$\begin{aligned}\forall a, b \in GF(q) &\Rightarrow a + b \in GF(q) \\ &\Rightarrow a \cdot b \in GF(q)\end{aligned}$$

- Esistenza degli elementi neutri:

$$\exists 0 \in GF(q) \text{ tale che } \forall a \in GF(q) \text{ vale } a + 0 = a$$

$$\exists 1 \in GF(q) \text{ tale che } \forall a \in GF(q) \text{ vale } a \cdot 1 = a$$

- Esistenza dell'opposto:

$$\forall a \in GF(q), \exists b \in GF(q) \text{ tale che } a + b = 0 \quad \begin{smallmatrix} \text{elemento neutro} \\ \text{della somma} \end{smallmatrix}$$

l'elemento b è detto opposto di a e si indica con $-a$.

- Esistenza dell'inverso:

$$\forall a \in GF(q) \text{ con } a \neq 0, \exists b \in GF(q) \text{ tale che } a \cdot b = 1 \quad \begin{smallmatrix} \text{elemento neutro} \\ \text{del prodotto} \end{smallmatrix}$$

l'elemento b è detto inverso di a e si indica con a^{-1} .

- Per le operazioni valgono le seguenti proprietà:

- Commutativa: $a + b = b + a$ e $a \cdot b = b \cdot a$
- Associativa: $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Distributività del prodotto sulla somma: $(a + b) \cdot c = a \cdot c + b \cdot c$

Osservazione L'elemento 0 funge da elemento assorbente per il prodotto ossia:

$$\forall a \in GF(q), a \cdot 0 = 0$$

Dimostrazione Considerando $a \cdot 0 + a \cdot 1$ per la proprietà distributiva vale:

$$a \cdot 0 + a \cdot 1 = a \cdot (0 + 1)$$

Dato che lo 0 è l'elemento neutro della somma vale:

$$a \cdot (0 + 1) = a \cdot 1 = a \cdot 0 + a \cdot 1$$

Dato che $a \cdot 1$ appartiene al campo per la proprietà di chiusura, esiste il suo opposto $-a \cdot 1$; lo si può sommare a destra e a sinistra ottenendo:

$$\begin{aligned}a \cdot 0 + a \cdot 1 - a \cdot 1 &= a \cdot 1 - a \cdot 1 \\ a \cdot 0 &= 0\end{aligned}$$

7. Algebra dei campi finiti di Galois

Osservazione Dati $a, b \in GF(q)$ allora se $a \cdot b = 0$ allora $a = 0 \vee b = 0$.

Dimostrazione Se $a \neq 0$ allora esiste il suo inverso $a^{-1} \in GF(q)$ e quindi:

$$\begin{aligned} a \cdot b &= 0 \\ a \cdot b \cdot a^{-1} &= 0 \cdot a^{-1} \end{aligned}$$

Dato che vale la proprietà commutativa si ha:

$$\begin{aligned} a \cdot a^{-1} \cdot b &= 0 \\ 1 \cdot b &= 0 \\ b &= 0 \end{aligned}$$

Se invece $b \neq 0$ allora si arriva alla conclusione che $a = 0$ tramite analoghi passaggi.

Osservazione Dati $a, b, c \in GF(q)$ con $c \neq 0$, se $a \cdot c = b \cdot c$ allora $a = b$.

Dimostrazione Sommando a destra e a sinistra l'opposto di $b \cdot c$ si ottiene:

$$\begin{aligned} a \cdot c &= b \cdot c \\ a \cdot c - b \cdot c &= b \cdot c - b \cdot c \\ a \cdot c - b \cdot c &= 0 \end{aligned}$$

Per la proprietà distributiva vale:

$$(a - b) \cdot c = 0$$

Dato che $c \neq 0$ allora esiste il suo inverso c^{-1} e quindi:

$$\begin{aligned} (a - b) \cdot c \cdot c^{-1} &= 0 \cdot c^{-1} \\ a - b &= 0 \\ a &= b \end{aligned}$$

7.2. Equazioni nei campi finiti

Equazioni di primo grado Si consideri l'equazione di primo grado:

$$a \cdot x = b$$

Se $a \neq 0$ allora esiste e il suo inverso e vale:

$$x = a^{-1} \cdot b$$

Equazioni di secondo grado Si consideri l'equazione di secondo grado:

$$a \cdot x^2 + b \cdot x + c = 0$$

Se $a \neq 0$ allora esiste il suo inverso e vale:

$$x^2 + b \cdot a^{-1} \cdot x + c \cdot a^{-1} = 0$$

Questa equazione ha soluzioni se esistono due valori $x_1, x_2 \in GF(q)$ tali che:

$$\begin{aligned} x^2 + b \cdot a^{-1} \cdot x + c \cdot a^{-1} &= (x - x_1) \cdot (x - x_2) && \text{1) metodo di scomposizione: tramite le radici} \\ x^2 + b \cdot a^{-1} \cdot x + c \cdot a^{-1} &= x^2 - x \cdot x_1 - x \cdot x_2 + x_1 \cdot x_2 \\ x^2 + b \cdot a^{-1} \cdot x + c \cdot a^{-1} &= x^2 - x \cdot (x_1 + x_2) + x_1 \cdot x_2 && \text{2) metodo di scomposizione: somma prodotto} \end{aligned}$$

ossia se:

$$\begin{cases} x_1 + x_2 = -b \cdot a^{-1} \\ x_1 \cdot x_2 = c \cdot a^{-1} \end{cases}$$

Sistemi di equazioni I sistemi di equazioni si possono risolvere usando i normali metodi dell'algebra reale dato che è possibile farlo per le equazioni, come appena visto.

Osservazione In ogni campo finito $GF(q)$ vale il teorema fondamentale dell'algebra ossia un'equazione di grado N ha al più N soluzioni e un polinomio con N radici ha almeno grado N .

7.3. Campi finiti di Galois primi

Definizione Un campo finito di Galois primo è un campo finito $GF(p) = \{0, 1, \dots, p-1\}$ dove p è un numero primo e in cui le operazioni sono definite come in algebra reale ridotte a modulo p . | Es: $7 \bmod 3 = 1$ mi restituisce il resto

Proposizione I campi finiti di Galois primi sono effettivamente dei campi finiti.

Dimostrazione

- Le operazioni di somma e prodotto in algebra reale sono ben definite e l'applicazione dell'operazione di modulo p consente di rispettare la chiusura.
- L'elemento 0 funge da elemento neutro anche per la somma ridotta a modulo p infatti:

$$(a + 0) \bmod p = a, \forall a \in GF(p)$$

- L'elemento 1 funge da elemento neutro anche per la moltiplicazione ridotta a modulo p infatti:

$$(a \cdot 1) \bmod p = a, \forall a \in GF(p)$$

- Le proprietà di commutatività, associatività e distributività sono ereditate da quelle dell'algebra reale.
- L'opposto esiste sempre infatti dato $a \in GF(p)$ allora il suo opposto è b se:

$$(a + b) \bmod p = 0$$

e quindi b esiste se esiste $k \in \mathbb{Z}$ tale che:

$$\begin{aligned} a + b + k \cdot p &= 0 \\ a + b &= -k \cdot p \end{aligned}$$

$$\begin{aligned} (-a) \bmod p &= (-a) \\ \Rightarrow -a + np &= -a \\ \text{Se } a \in GF(p) \rightarrow b \in GF(p) : \\ (-a + b) \bmod p &= 0 \\ \Rightarrow 0 + np &= a+b \end{aligned}$$

e quindi se esiste $h \in \mathbb{Z}$ tale che:

$$a + b = h \cdot p$$

questa equazione diofantea ha soluzione se e solo se $h \cdot p$ è divisibile per $MCD(1, 1) = 1$, ma tutti i numeri sono divisibili per 1 e quindi h esiste e quindi l'opposto b esiste.

- L'inverso esiste sempre infatti dato che $a \in GF(p)$ allora il suo inverso è b se:

$$a \cdot b \bmod p = 1$$

ossia se:

$$a \cdot b + k \cdot p = 1 \quad \begin{array}{l} \text{: Può essere sia positivo che negativo} \\ \text{: mi indica quante volte aggiungiamo o sottraiamo } P \text{ per ottenere uno} \end{array}$$

che ha soluzione se e solo se 1 è divisibile per $MCD(a, p)$ ossia se $MCD(a, p) = 1$, ma dato che p è primo questo è sempre vero e quindi l'inverso esiste sempre.

Esempio $GF(2)$ In $GF(2)$ ci sono solo due elementi ossia $\{0, 1\}$ e le operazioni sono definite come:

+	0	1
0	0	1
1	1	0

$$(1+1) \bmod 2 = 0$$

*	0	1
0	0	0
1	0	1

Che sono le normali operazioni binarie in cui 1 è il neutro del prodotto e 0 è il neutro della somma.

7. Algebra dei campi finiti di Galois

Esempio $GF(3)$ In $GF(3)$ ci sono solo tre elementi ossia $\{0, 1, 2\}$ e le operazioni sono definite come:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$$(2+1) \bmod 3 = 0$$

$$(1+2) \bmod 3 = 1$$

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

7.4. Campi finiti di Galois estesi

- contiene p^m elementi (campo finito)
- ho tuple di elementi lunghe $m \Rightarrow m\text{-uple}$
- rappresentazione polinomiale

Definizione Un campo finito di Galois esteso è un campo finito $GF(p^m)$ dove p è un numero primo e m un numero naturale. Gli elementi del campo sono m -uple $(a_0, a_1, \dots, a_{m-1})$ di elementi di $GF(p)$ che vengono rappresentati tramite dei polinomi $a(\alpha) = a_0 + a_1 \cdot \alpha + \dots + a_{m-1} \cdot \alpha^{m-1}$ e le operazioni sono:

- La somma è la normale somma di polinomi.
- Il prodotto si ottiene calcolando il resto della divisione tra il normale prodotto tra polinomi e un polinomio $p(\alpha)$

- L'elemento neutro è il polinomio con coefficiente tutti a zero
- L'opposto di un polinomio è il polinomio con coefficienti tutti opposti a quelli del polinomio di partenza

$$q(\alpha) \cdot r(\alpha) = \text{Resto} \left[\frac{q(\alpha) \cdot r(\alpha)}{p(\alpha)} \right] \Rightarrow [q(\alpha) \cdot r(\alpha)] \bmod p(\alpha)$$

dove $p(\alpha)$ è un polinomio irriducibile di grado m e coefficienti in $GF(p)$ ed è detto polinomio generatore del campo.

ossia, non è possibile fattorizzarlo in polinomi a coefficienti in $GF(p)$

Proposizione I campi finiti di Galois estesi sono effettivamente dei campi finiti.

Dimostrazione parziale

devo solo controllare i coefficienti che siano in $GF(p)$

- La somma mantiene la chiusura perché sommando due polinomi con grado inferiore a m , usando la somma definita in $GF(p)$, si ottiene un polinomio di grado al più m e quindi un elemento di $GF(p^m)$.
- Il prodotto normale tra due polinomi non mantiene la chiusura perché il grado può aumentare. Per risolvere il problema si utilizza il resto della divisione per un polinomio di grado m , infatti il resto può avere grado massimo di $m - 1$. Il polinomio scelto deve anche essere irriducibile, ossia non si può ricavare tramite il prodotto di due polinomi di grado inferiore, in modo che moltiplicando due polinomi di grado inferiore non si può ottenere un multiplo di $p(\alpha)$ e quindi il resto è sempre diverso da 0.

Osservazione Ogni campo finito esteso di Galois $GF(p^m)$ ha come sottocampi i campi $GF(p^n)$ con $0 < n < m$, ossia gli elementi di $GF(p^n)$ sono interamente contenuti in $GF(p^m)$ con le operazioni che restituiscono gli stessi risultati.

4 non è primo

Esempio: $GF(4) = GF(2^2)$ ossia è un campo formato da tutti i polinomi di grado inferiore a 2 con coefficienti in $GF(2)$ e quindi:

$$GF(2^2) = \{0, 1, \alpha, \alpha + 1\}$$

$$\text{1) } GF(2) = \{0, 1\}$$

le tuple sono lunghe $m=2$, con elementi in $GF(2)$
ossia: $\alpha(\omega) = \alpha_0 = 0 \text{ e } \alpha_1 = \alpha = 1$

$$\text{2) } GF(2^2) =$$

con elementi in $GF(2)$
combinazioni:

α_0	α_1
0	0
0	1
1	0
1	1

+	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

$$(\alpha + \alpha) \bmod 2 = (\alpha \alpha) \bmod 2 = 0 \cdot \alpha = 0$$

$$((\alpha + 1) + \alpha) \bmod 2 = ((\alpha + 1) \alpha) \bmod 2 + (\alpha + 1) \bmod 2$$

$$= (2\alpha) \bmod 1 + 1 = 1$$

$$((\alpha + 1) + (\alpha + 1)) \bmod 2 = ((\alpha + 1) \alpha) \bmod 2 + ((\alpha + 1) \bmod 2)$$

$$= 0$$

- Il risultato della somma mi deve restituire un elemento appartenente al campo
- i coefficienti sono in $GF(2)$ dunque devo mod(2) i coefficienti
- gli elementi del polinomio vengono sommati separatamente, somma i termini simili rispettando $GF(2)$ per i coefficienti
- le operazioni si fanno combinando i termini applicando modulo 2

7. Algebra dei campi finiti di Galois

da cui si può notare che ogni elemento è l'opposto di se stesso, caratteristica tipica dei gruppi finiti estesi $GF(2^m)$.

La tabella del prodotto richiede qualche calcolo aggiuntivo e in particolare bisogna trovare il polinomio generatore. Dato che il polinomio deve avere grado $m = 2$ l'elemento α^2 deve essere per forza presente:

$$p(\alpha) = \alpha^2$$

• il polinomio ha grado m
deve essere irriducibile: ossia non deve avere radici
contenute nel campo ossia alpha, alpha + 1

Per fare in modo che non sia divisibile per i termini di primo grado bisogna garantire che non condividano delle radici e quindi dato che il polinomio α si annulla per $\alpha = 0$ e il polinomio $\alpha + 1$ si annulla per $\alpha = 1$ deve valere:

polinomio:
 $p(\alpha) = p_2\alpha^2 + p_1\alpha + p_0$
 1) α^2 minore rispetto a $m=2$
 $p(\alpha) = \alpha^2 + p_1\alpha + p_0$

$$\begin{array}{lll} p(0) = 1 & & \text{1) } p(0) = p_0 \Rightarrow p_0 = 1 \Rightarrow p(x) = \alpha^2 + p_1\alpha + 1 \\ p(1) = 1 & & \text{3) } p(1) = 1 + p_1 \Rightarrow p_1 = 1 \Rightarrow p(x) = \alpha^2 + \alpha + 1 \\ & & = 1 + p_1 \\ & & = p_1 \end{array}$$

il che si ottiene ponendo:

$$p(\alpha) = \alpha^2 + \alpha + 1$$

Ottenuto il polinomio generatore si può costruire la tabella del prodotto:

.	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

Molti termini non richiedono il calcolo del resto perché hanno grado inferiore a 2; per gli altri:

- $\alpha \cdot \alpha = \alpha^2$:

$$\begin{array}{r|rrr}
 \alpha^2 & & & \alpha^2 + \alpha + 1 \\
 \alpha^2 & +\alpha & +1 & \\
 \hline
 \alpha & +1 & &
 \end{array}$$

- $(\alpha + 1) \cdot \alpha = \alpha^2 + \alpha$:

$$\begin{array}{r|rrr}
 \alpha^2 & +\alpha & & \alpha^2 + \alpha + 1 \\
 \alpha^2 & +\alpha & +1 & \\
 \hline
 1 & & &
 \end{array}$$

- $(\alpha + 1) \cdot (\alpha + 1) = \alpha^2 + 1$:

$$\begin{array}{r|rrr}
 \alpha^2 & & +1 & \alpha^2 + \alpha + 1 \\
 \alpha^2 & +\alpha & +1 & \\
 \hline
 \alpha & & &
 \end{array}$$

7.5. Notazione esponenziale

• q vale per entrambi
p assumo che il campo sia primo
p^m assumo campo esteso

Definizione Dato $a \in GF(q)$ con $a \neq 0$ e $a \neq 1$, si definisce **ordine di a** il più piccolo numero naturale $m > 1$ tale che:

$$a^m = 1 \quad | \quad \alpha^{\frac{m}{\text{ordine}}} \rightarrow x$$

note: ordine naturale (potenze)

Definizione Un elemento $a \in GF(q)$ si definisce **primitivo** se ha **ordine $q - 1$** .

Esempio Si considerino gli elementi di $GF(5) = \{0, 1, 2, 3, 4\}$:

- L'ordine di 2 lo si ricava calcolando le varie potenze:

$$2^2 = 4$$

$$2^3 = 2^2 \cdot 2 = 4 \cdot 2 = 8 \mod 5 = 3$$

ordine n indica che possono essere assunti n valori distinti

$$2^4 = 2^3 \cdot 2 = 3 \cdot 2 = 6 \mod 5 = 1$$

quindi l'ordine di 2 è 4 e visto che $4 = 5 - 1$ è anche un elemento primitivo.

- L'ordine di 3 lo si ricava calcolando le varie potenze:

$$3^2 = 9 \mod 5 = 4$$

$$3^3 = 3^2 \cdot 3 = 4 \cdot 3 = 12 \mod 5 = 2$$

$$3^4 = 3^3 \cdot 3 = 2 \cdot 3 = 6 \mod 5 = 1$$

quindi l'ordine di 3 è 4 e visto che $4 = 5 - 1$ è anche un elemento primitivo.

- L'ordine di 4 lo si ricava calcolando le varie potenze:

$$4^2 = 16 \mod 5 = 1$$

quindi l'ordine di 4 è 2 e quindi non è un elemento primitivo.

dunque io ho $m - 1$ elementi diversi rappresentabili tramite rappresentazione esponenziale + 0

Osservazione Le potenze di un elemento primitivo coprono tutti gli elementi del campo escluso lo 0.

Esempio Si è visto che 2 è un elemento primo di $GF(5)$ e si può notare che:

$$1 = 2^0$$

$$2 = 2^1$$

$$3 = 2^3$$

$$4 = 2^2$$

Osservazione Le potenze di un elemento di ordine o sono cicliche e si ripetono ogni o volte.

Dimostrazione Si consideri la potenza a^m con $m > o$:

$$a^m = a^o \cdot a^{m-o} = 1 \cdot a^{m-o} = a^{m-o}$$

e si può procedere in modo analogo fintanto che $m > o$.

Teorema Ogni campo finito di Galois $GF(q)$ ha almeno un elemento primitivo α .

• Presentazione generica di un elemento primitivo
 • Io indicheremo sempre in questa maniera negli esercizi

7. Algebra dei campi finiti di Galois

Dimostrazione Dato che tutti gli elementi hanno potenze cicliche si ha che l'ordine massimo è $q - 1$; infatti se un elemento avesse ordine $v > q - 1$ servirebbero $v + 1$ elementi all'interno del campo per completare il ciclo; questo vorrebbe dire avere un numero di elementi $v + 1 > q$, il che è impossibile. Si ha quindi che l'elemento con ordine $v > q - 1$ non esiste, rendendo $q - 1$ il massimo ordine presente nel campo.

Sia $\beta \in GF(q)$ di ordine n e $\gamma \in GF(q)$ di ordine m con $\gamma \neq \beta^{-1}$; l'ordine k di $\delta = \beta \cdot \gamma$ è il minor numero > 1 tale che:

$$\begin{aligned} (\beta \cdot \gamma)^k &= 1 \\ \beta^k \cdot \gamma^k &= 1 \end{aligned}$$

Dato che $\beta \neq \gamma^{-1}$ questo avviene se e solo se k è un multiplo sia di n che di m , ed essendo il minore possibile: $k = \text{lcm}(n, m)$.

Si può procedere in modo analogo per ricavare l'ordine di un altro elemento e così via per tutti gli elementi del campo; dato che l'ordine può solo aumentare, così facendo si trova l'ordine o massimo del campo che è un numero multiplo di tutti gli ordini dei vari elementi del campo.

Per questo motivo si ha che $\forall \beta \in GF(q) \beta^o = 1$ e quindi considerando l'equazione:

$$\beta^o - 1 = 0$$

si nota che tutti gli elementi del campo (escluso lo 0) sono soluzioni: l'equazione ha quindi $q - 1$ soluzioni e deve avere almeno grado $q - 1$ per il teorema fondamentale dell'algebra. Si ha quindi $o \geq q - 1$ e in conclusione:

$$q - 1 \leq o \leq q - 1$$

$$o = q - 1$$

e quindi esiste sempre almeno un elemento di ordine $q - 1$ e quindi un elemento primitivo.

Osservazione Tutti gli ordini possibili devono essere dei divisori di $q - 1$.

Teorema Dato un campo finito di Galois $GF(q)$, se $q - 1$ è primo tutti i suoi elementi sono primitivi.

Dimostrazione Si è visto che tutti gli ordini possibili sono divisibili per $q - 1$, ma essendo primo è divisibile solo per se stesso e 1. Dato che non è possibile avere ordine 1, si ha che tutti gli elementi hanno ordine $q - 1$ e quindi sono tutti primitivi.

Definizione di notazione esponenziale Dato un campo finito di Galois $GF(q)$ e un suo elemento primitivo α la notazione esponenziale rappresenta tutti gli elementi (escluso lo 0) come potenze di α :

$$GF(q) = \left\{ 0, \alpha^0, \alpha^1, \dots, \alpha^{q-2} \right\} \quad \begin{array}{l} \parallel \\ \alpha^{q-1} = 1 \end{array} \quad \begin{array}{l} \text{- ho } q \text{ elementi all'interno del campo} \\ \text{- tramite elevazione di alpha rappresentiamo } q - 1 \text{ elementi + lo 0 = } q \\ \text{- gli esponenti in notazione esponenziale sono ridotti a modulo } q - 1 \Leftrightarrow \text{mod } (q - 1) \end{array}$$

Osservazioni

- La notazione esponenziale funziona sia per campi primi che per campi estesi e per questo è molto usata.
- Le moltiplicazioni e le divisioni sono molto più semplici da fare usando la notazione esponenziale perché basta sommare gli esponenti, mentre la somma è più complicata rispetto alla normale notazione.
- Lo 0 è l'unico elemento non rappresentabile e solitamente viene indicato con l'esponente $-\infty$ anche se non ha un reale significato.

Esempio Si è visto che 2 è un elemento primitivo di $GF(5)$ infatti:

n	$-\infty$	0	1	2	3
2^n	0	1	2	4	3

$$2^3 \bmod 5 = 3$$

Teorema: In un campo GF(q) esiste sempre almeno un elemento primitivo

Dimostrazione: sia κ l'ordine dell'elemento di ordine massimo $\Rightarrow K \geq q-1$. Se β è di ordine b , per $\text{GF}(q)$ c'è $\gamma \in \text{GF}(q)$ di ordine c con $b < c$ relativamente primi (ogni parte fattori in comune). L'ordine $d = b \cdot c$ è il minimo tale che $(\beta \gamma)^d = 1$. Se $b < c$ sono relativamente primi, $b \nmid \gamma^{-1}$ (che hanno lo stesso ordine, necessariamente)

$$\begin{aligned} \Rightarrow \alpha (\beta \gamma)^d = 1 &\Rightarrow \beta^d \gamma^d = 1 \Rightarrow \beta^d = 1 \wedge \gamma^d = 1 \\ \Rightarrow d > b &\wedge d > c \quad \text{in particolare} \quad d = b \cdot c \end{aligned}$$

Sia η di ordine r non relativamente primo con d ma fatti $a = r \cdot b$ con r relativamente primo con d .

$$\begin{aligned} \Rightarrow \eta = \gamma^a &\text{ ha ordine } r \text{ relativamente primo con } d \\ \Rightarrow \lambda = \eta \cdot \beta &\text{ avrà ordine } m = r \cdot d \geq r \text{ di } d \end{aligned}$$

Procedendo così troviamo che elemento e elemento trovando ordine sempre maggiore fino ad ottenere un elemento α di ordine K tale che ogni altro elemento $\mu \in \text{GF}(q)$ ha ordine divisorio di K .

$$\begin{aligned} \Rightarrow \mu^K = 1 \quad \forall \mu \in \text{GF}(q) &\Rightarrow x^K - 1 = 0 \\ \text{avremo } q-1 &\text{ soluzioni distinte in } \text{GF}(q) \\ \Rightarrow K \geq q-1 &\text{ per la teorema fondamentale dell'algebra} \\ \Rightarrow K = q-1 & \end{aligned}$$

7. Algebra dei campi finiti di Galois

$$p(\alpha) = p_0 + p_1 \alpha + p_2 \alpha^2 + \dots + p_{m-1} \alpha^{m-1}$$

Definizione Sia $GF(p^m)$ un campo finito esteso di Galois con polinomio generatore $p(\alpha)$; se α è un elemento primitivo allora il polinomio generatore $p(\alpha)$ si definisce primitivo.

se un elemento risulta essere primitivo, appartiene al campo esteso di riferimento e a nessun sottocampo

un polinomio generatore viene chiamato primitivo se solo se la riduzione modulo $p(\alpha)$ mi permette di generare tutti i polinomi del campo $GF(p^m)$

Osservazioni

- Dato un campo finito esteso di Galois $GF(p^m)$ esiste sempre almeno un polinomio generatore $p(\alpha)$ primitivo.
- Dato che esiste sempre un polinomio generatore primitivo solitamente lo si usa in modo da rendere più semplice l'individuazione dell'elemento primitivo.
- Dato un elemento α^k del campo $GF(q)$ il suo ordine è:

elemento del campo rappresentato
tramite notazione esponenziale

$$n = \frac{q-1}{MCD(k, q-1)}$$

$$\alpha = 0, \dots, q-1 \quad \alpha^{q-1} = 1$$

$$\alpha^{q-1} = 1$$

- Dato un elemento α^k del campo $GF(q)$ il suo inverso è α^{q-1-k} infatti:

$$\alpha^k \cdot \alpha^{q-1-k} = \alpha^{k+q-1-k} = \alpha^{q-1} = 1$$

INVERSO
 α^{-k}

$$-W \bmod (q-1) = r$$

$$(q-1) - W = r$$

nella maggior parte delle volte $n = r$

$$0 \leq r < q-1$$

Logartimo di Zech Dato un campo finito di Galois con elemento primitivo α , si definisce il logaritmo di Zech come la funzione che dato l'esponente n di un elemento restituisce l'esponente dell'elemento successivo, cioè k tale che $\alpha^k = \alpha^n + 1$, e si indica con $z(n)$.

Utilizzo del logaritmo di Zech Il logaritmo di Zech permette di semplificare il calcolo delle somme usando gli elementi in notazione esponenziale. Supponendo di voler sommare due elementi α^k e α^j , con $k > j$:

$$\alpha^k + \alpha^j = \alpha^j \cdot (\alpha^{k-j} + 1) = \alpha^j \cdot \alpha^{z(k-j)} = \alpha^{j+z(k-j)}$$

Osservazione Non esiste un metodo matematico per ricavare il logaritmo di Zech e quindi è necessario tabulare i vari risultati; rimane comunque molto comodo perché richiede meno spazio rispetto a tabulare tutti i possibili esponenti di tutte le possibili somme.

il campo ha coeff. in $GF(2) = \{0, 1\}$
mentre deve avere 8 elementi al suo interno
 $(0, 1, \alpha, \alpha + 1) \Rightarrow \ell(n) = 0 + 0 \cdot \alpha + 0 \cdot \alpha^2$

Esempio Si consideri il campo $GF(8) = GF(2^3)$ con polinomio generatore $p(\alpha) = \alpha^3 + \alpha + 1$, ossia il campo che ha come elementi i polinomi di grado inferiore a 3 ossia:

$$GF(2^3) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

tab. in $GF(8)$, $g(x) = x^3 + x + 1$, $2^3 = 8$ combinazioni

000	0
001	1
010	α
011	$\alpha + 1$
100	α^2
101	$\alpha^2 + 1$
110	$\alpha^2 + \alpha$
111	$\alpha^2 + \alpha + 1$

Dato che $8 - 1 = 7$ è primo tutti gli elementi sono primitivi e quindi lo si può scrivere in notazione esponenziale usando α come elemento primitivo. Quindi tabulando la notazione esponenziale si ottiene:

n	$-\infty$	0	1	2	3	4	5	6
α^n	0	α^0	α^1	α^2	α^3	$\alpha \cdot (\alpha + 1)$	$\alpha \cdot (\alpha^2 + \alpha)$	$\alpha \cdot (\alpha^2 + \alpha + 1)$
$\alpha^n \bmod p(x)$	0	1	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$

da cui si può ricavare il logaritmo di Zech:

$\left[\frac{\alpha}{\alpha^n} \right] \text{ è grande}$

$$\alpha^4 = \alpha^2 \alpha = (\alpha + 1) \alpha$$

$$\alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$$

n	$-\infty$	0	1	2	3	4	5	6
$\alpha^n \bmod p(x)$	0	1	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$
$\alpha^n + 1$	1	0	$\alpha + 1$	$\alpha^2 + 1$	α	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$	α^2
$z(n)$	0	$-\infty$	3	6	= 1	5	4	2

che si può usare per fare delle somme in forma esponenziale, per esempio:

$$\alpha^5 + \alpha^3 = \alpha^{3+z(5-3)} = \alpha^{3+z(2)} = \alpha^{3+6} = \alpha^9 = \alpha^7 \cdot \alpha^2 = \alpha^2$$

In notazione normale la stessa somma equivale a:

$$\alpha^2 + \alpha + 1 + \alpha + 1 = \alpha^2$$

esempio:
elemento α
 $\alpha^0 = 1$
 $\alpha^1 = \alpha$
 $\alpha^2 = \alpha^2$
 $\alpha^3 = \alpha + 1$
 $\alpha^4 = \alpha^2 + 1$
 $\alpha^5 = \alpha + 1$

mi serve trovare l'esponente $z(n)$ tale
per cui ho la condizione di destra

7.6. Proprietà speciali

- Siano $\alpha, \beta \in GF(p^m)$ con $m > 0$, allora $(\alpha + \beta)^p = \sum_{i=0}^p \binom{p}{i} \cdot \alpha^{p-i} \cdot \beta^i = \alpha^p + \beta^p$. Infatti analizzando:

$$\left| \binom{p}{i} = \frac{p!}{i! \cdot (p-i)!} \right. \quad \text{coefficiente binomiale}$$

si nota che:

- se $i = 0$:

mi rimangono solo gli estremi $i = 0$ e p , perché nel mezzo sono tutti 0

$$\binom{p}{0} = \frac{p!}{0! \cdot p!} = \frac{1}{0!} = 1$$

- se $i = p$:

$$\binom{p}{p} = \frac{p!}{p! \cdot (p-p)!} = \frac{1}{0!} = 1$$

- negli altri casi:

$$\binom{p}{i} = \frac{p!}{i! \cdot (p-i)!} = p \cdot \frac{(p-1)!}{i! \cdot (p-i)!}$$

che è un multiplo di p e quindi è nullo in $GF(p)$.

- $(\alpha + \beta + \gamma)^p = (\alpha + \beta)^p + \gamma^p = \alpha^p + \beta^p + \gamma^p$ e quindi si può estendere per un numero qualsiasi di elementi:

$$\Rightarrow \left(\sum_i \beta_i \right)^p = \sum_i \beta_i^p, \beta_i \in GF(p^m)$$

- $(\alpha + \beta)^{p^2} = [(\alpha + \beta)^p]^p = [\alpha^p + \beta^p]^p = \alpha^{p^2} + \beta^{p^2}$ e anche questa proprietà si può estendere per qualsiasi esponente dell'esponente, ottenendo:

$$\Rightarrow \left(\sum_i \beta_i \right)^{p^k} = \sum_i \beta_i^{p^k}, \beta_i \in GF(p^m), k \in \mathbb{N}$$

$\beta \in GF(q) = GF(p^k)$

- Sia $\beta \in GF(q)$ con q potenza di un numero primo, allora:

Dunque visto:
• $\forall \beta \in GF(q) : \beta \in GF(p^k)$
 $\Rightarrow \beta^q = \beta$
 $\downarrow \beta \in GF(p^k) \Rightarrow \beta^{p^k} = \beta$

$$\beta^{q^k} = (\beta^q)^{q^{k-1}} = (\beta^{q-1} \cdot \beta)^{q^{k-1}} = \beta^{q^{k-1}} = \dots = \beta$$

l'ordine di ogni elemento del campo è divisore di $q - 1$
Teorema di Lagrange applicato al campo finito
(moltiplicativo + ciclico) ordine $q - 1$

$$\begin{aligned} \forall \beta \in GF(q) &\Rightarrow \beta^{q-1} = 1 \\ \downarrow \beta \in GF(q) &\Rightarrow \beta^q \cdot \beta^{q-1} = \beta \end{aligned}$$

- Dato che $GF(q)$ è un sotto campo dei campi estesi $GF(q^m)$ con $m > 1$ questa proprietà vale anche per gli elementi di questi campi che appartengono anche al sottocampo.

- Dato un polinomio $F(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots$ dove $a_i \in GF(q)$ e $x \in GF(q^m)$ con q potenza di un numero primo e $m \in \mathbb{N}$, allora:

$$\begin{aligned} F(x)^{q^k} &= a_0^{q^k} + a_1^{q^k} \cdot x^{q^k} + a_2^{q^k} \cdot x^{2 \cdot q^k} + \dots = \\ &= a_0^{q^k} + a_1^{q^k} \cdot x^{q^k} + a_2^{q^k} \cdot (x^{q^k})^2 + \dots = \\ &= F(x^{q^k}) \end{aligned}$$

- se $\beta \in GF(q^m)$ è una radice di $F(x)$ si ha che:

$$\begin{aligned} F(\beta) &= 0 \\ F(\beta)^{q^k} &= 0 \\ F(\beta^{q^k}) &= 0 \end{aligned}$$

e quindi anche tutte le potenze β^{q^k} sono radici.

In $GF(2^m)$:

$$\begin{aligned} (\alpha + \beta)^2 &= \alpha^2 + 2\alpha\beta + \beta^2 = \alpha^2 + \beta^2 \\ (\alpha + \beta + \gamma)^2 &= (\alpha + \beta)^2 + \gamma^2 = \alpha^2 + \beta^2 + \gamma^2 \\ (\alpha + \beta)^4 &= ((\alpha + \beta)^2)^2 = (\alpha^2 + \beta^2)^2 = \alpha^4 + \beta^4 \end{aligned}$$

Quindi in $GF(2^m)$, se considero un qualsiasi n° di elementi β_i :

$$(\sum_i \beta_i)^{2^k} = \sum_i \beta_i^{2^k} \quad \forall n$$

Le proprietà si può generalizzare in $GF(2^m)$:

$$\begin{aligned} (\alpha + \beta)^p &= \sum_{i=0}^p \binom{p}{i} \alpha^i \cdot \beta^{p-i} = \alpha^p + \beta^p \\ \Rightarrow (\sum_i \beta_i)^p &= \sum_i \beta_i^p \end{aligned}$$

7. Algebra dei campi finiti di Galois

Definizione Siano:

- q una potenza di un numero primo;
- m un numero naturale;
- $b \in GF(q^m)$;
- $T(x) = t_0 + t_1 \cdot x + t_2 \cdot x^2 + \dots$ un polinomio per cui $t_i \in GF(q)$ $\forall i$ e $x \in GF(q^m)$;

Allora $T(x)$ si definisce polinomio minimo di b in $GF(q^m)$ se e solo se:

- Non è il polinomio nullo;
- Ha b come radice;
- Non esiste un polinomio di grado minore che rispetti tutte le proprietà esposte.

Individuazione del polinomio minimo Per definizione un **polinomio minimo di b** deve essere divisibile per b e quindi si ha che $T(b) = 0$. Idealmente si vorrebbe che tale polinomio non avesse altre radici in modo che sia di grado unitario, ma per le proprietà viste prima si sa che se $T(b) = 0$ anche $T(b^{q^k}) = 0$ e quindi ci sono anche altre radici. Per questo motivo il polinomio minimo di b è:

$$T(x) = (x - b) \cdot (x - b^q) \cdot (x - b^{q^2}) \cdot \dots$$

vuol dire che esiste un generatore
(elemento primitivo) che mi determina
tutti gli elementi non nulli del campo

Dato che b è un elemento di $GF(q^m)$ è ciclico e quindi il numero di radici è finito. Inoltre questo polinomio ha i coefficienti in $GF(q)$ e quindi si può scrivere:

$$T(x) = \prod_{k=0}^{n-1} (x - b^{q^k})$$

: se $n = m$ se e solo se b appartiene solo a $GF(q^m)$
altrimenti $n < m$, ossia b proviene da un sottocampo

n è definito come: l'ordine
moltiplicativo di b

NB: gli elementi all'interno di un campo, possono essere elementi che provengono dai
sottocampi, oppure sono elementi nuovi generati dal campo esteso di riferimento e dunque

1) $b \in GF(q) \Rightarrow b^q = b$
2) $\forall b \in GF(q) \Rightarrow b \in GF(q^n)$
3) l'ordine moltiplicativo n : $b^n = b$
 $\forall b \in GF(q): b \in GF(q^n) \Rightarrow b^n = b$ ($n=n$) | sottocampi di
 $\forall b \in GF(q^n): b \in GF(q^n) \Rightarrow b^n = b$ ($n=n$) | $GF(q^n)$
 $\forall b \notin GF(q), b \in GF(q^n) \Rightarrow b^n = b$ ($n=m$) | con $0 < n < m$

Osservazioni

- Si è visto che il polinomio minimo di b ha come divisori anche i termini del tipo b^{q^k} e quindi è il polinomio minimo anche di questi valori.
- Sia α un elemento primitivo di $GF(q^m)$, allora si può rappresentare il polinomio minimo in forma esponenziale di un elemento α^k :

$$T(x) = (x - \alpha^k) \cdot (x - \alpha^{k+q}) \cdot (x - \alpha^{k+q^2}) \cdot \dots = \sum_{i=0}^{n-1} (x - (\alpha^k)^{q^i})$$

dⁿ = b
rotazione
esponentiale

tal polinomio si può chiamare $m_k(x)$ dove k è l'esponente dell'elemento.

- Dall'osservazione fatta prima si ha che:

$$m_k(x) = m_{k+q}(x) = m_{k+q^2}(x) = \dots$$

- L'insieme delle radici del polinomio minimo di b è detto **set ciclotomico di b** .

7.7. Trasformata di Fourier discreta

Definizione di trasformata di Fourier discreta Sia $v = (v_0, v_1, \dots, v_{N-1})$ una sequenza di N elementi tali che $v_i \in GF(q)$; la trasformata discreta di Fourier (FDT) associata biunivocamente a v è una sequenza $V = (V_0, V_1, \dots, V_{N-1})$ di N elementi tale che $V_i \in GF(q)$. Data la sequenza v è possibile ricavare V tramite la seguente formula:

$$V_j = \sum_{i=0}^{N-1} v_i \cdot \beta^{i \cdot j}$$

dove $\beta \in GF(q)$.

$$q = p^m$$

$$V(k) \xrightarrow{\sim} \sqrt{k} \text{ dove:}$$

$$\begin{aligned} V(k) &= V_0 + V_1 k + V_2 k^2 + \dots \\ J(k) &= J_0 + J_1 k + J_2 k^2 + \dots \end{aligned}$$

7. Algebra dei campi finiti di Galois

Definizione di antitrasformata di Fourier discreta L'antitrasformata o trasformata inversa di Fourier è l'operazione che permette di ricavare la sequenza v che trasformata dà V . Data V si può ricavare che:

$$v_j = \frac{1}{N} \cdot \sum_{i=0}^{N-1} V_i \cdot \beta^{-i \cdot j}$$

dove $\frac{1}{N}$ intero e $\beta = \frac{1}{N^{\text{mod } p}}$

Condizione di esistenza della trasformata discreta di Fourier La trasformata esiste se l'associazione effettuata tra v e V è davvero biunivoca quindi se l'antitrasformata della trasformata di una sequenza v è v stessa, quindi:

$$v_j = \frac{1}{N} \cdot \sum_{i=0}^{N-1} \left[\sum_{k=0}^{N-1} v_k \cdot \beta^{i \cdot k} \right] \cdot \beta^{-i \cdot j}$$

$\forall j < N$

↓

↑

Riordinando le sommatorie si ottiene:

$$\begin{aligned} v_j &= \frac{1}{N} \cdot \sum_{k=0}^{N-1} v_k \cdot \left[\sum_{i=0}^{N-1} (\beta^{i \cdot k} \cdot \beta^{-i \cdot j}) \right] = \\ &= \frac{1}{N} \cdot \sum_{k=0}^{N-1} v_k \cdot \left[\sum_{i=0}^{N-1} \beta^{i \cdot k - i \cdot j} \right] = \\ &= \frac{1}{N} \cdot \sum_{k=0}^{N-1} v_k \cdot \left[\sum_{i=0}^{N-1} \beta^{i \cdot (k-j)} \right] \end{aligned}$$

Considerando l'elemento j -esimo dalla sommatoria esterna

$$\begin{aligned} \text{per ogni } v_j \text{ esterno} \\ \text{fissato della sommatoria} \\ \frac{1}{N} \sum_{k=0}^{N-1} v_k \cdot \sum_{i=0}^{N-1} \beta^{i \cdot (j-k)} &= \frac{1}{N} \cdot v_j \cdot \sum_{i=0}^{N-1} \beta^0 = \\ \text{fisso } k=j \\ &= \frac{1}{N} \cdot v_j \cdot N = \\ &= v_j \end{aligned}$$

Definendo $r = k - j$, per semplicità, si ottiene:

$$\begin{aligned} v_j &= v_j + \frac{1}{N} \cdot \sum_{\substack{k=0 \\ k \neq j}}^{N-1} v_k \cdot \left[\sum_{i=0}^{N-1} \beta^{i \cdot r} \right] \\ 0 &= 0 + \frac{1}{N} \cdot \sum_{\substack{k=0 \\ k \neq j}}^{N-1} v_k \cdot \left[\sum_{i=0}^{N-1} \beta^{i \cdot r} \right] \\ \frac{1}{N} \cdot \sum_{\substack{k=0 \\ k \neq j}}^{N-1} v_k \cdot \left[\sum_{i=0}^{N-1} \beta^{i \cdot r} \right] &= 0 \\ \forall j < N & \end{aligned}$$

7. Algebra dei campi finiti di Galois

Dato che i valori della sequenza v sono tipicamente non nulli, l'unico modo per garantire la nullità di questo valore è imporre:

$$\begin{aligned} \sum_{i=0}^{N-1} \beta^{i \cdot r} &= 0 \\ \sum_{i=0}^{N-1} \beta^{i \cdot (k-j)} &= 0 \\ \forall (j, k) \text{ tali che } j < N, k < N, k \neq j \end{aligned}$$

Si consideri il valore: Calcolando il valore (senza alcuna relazione rispetto ai calcoli precedenti) ottengo:

$$\begin{aligned} (\beta^r - 1) \cdot \sum_{i=0}^{N-1} \beta^{i \cdot r} &= (\beta^r - 1) \cdot (\beta^0 + \beta^r + \beta^{2 \cdot r} + \dots + \beta^{(N-1) \cdot r}) = \\ &= \cancel{\beta^r + \beta^{2 \cdot r} + \dots + \beta^{(N-1) \cdot r}} + \cancel{\beta^{N \cdot r}} - \cancel{\beta^0} - \cancel{\beta^r} - \cancel{\beta^{2 \cdot r}} - \dots - \cancel{\beta^{(N-1) \cdot r}} = \\ &= \cancel{\beta^{N \cdot r} - 1} \quad \cancel{\beta^r \cdot \Sigma} \quad (-1) \cdot \cancel{\Sigma} \end{aligned}$$

Se $\beta^r - 1 \neq 0$ si ha che:

$$\sum_{i=0}^{N-1} \beta^{i \cdot r} = \frac{\beta^{N \cdot r} - 1}{\beta^r - 1}$$

Una frazione è nulla se il numeratore è nullo mentre il denominatore non lo è (altrimenti è indeterminata) e quindi quando:

$$\beta^{N \cdot r} - 1 = 0 \Rightarrow \beta^{Nr} = 1$$

Questo si verifica quando N è multiplo dell'ordine di β infatti:

$$\begin{array}{l} \beta \in GF(q) \\ \beta^N \text{ mod } q = 1 \end{array} \quad (\beta^N)^r - 1 = 1^r - 1 = 0$$

Bisogna però verificare che il denominatore non sia nullo, ossia se:

$$\begin{aligned} \beta^r - 1 &\neq 0 \\ \beta^{k-j} - 1 &\neq 0 \\ \forall (j, k) \text{ tali che } j < N, k < N, k \neq j \end{aligned}$$

Si può garantire che questo sia vero se e solo se N è esattamente l'ordine di β , infatti in questo caso si ha che:

- $r \neq 0$ dato che $k \neq j$.
- $-N < k - j < N$ dato che sia k che j sono minori di N .

e quindi si ha che $\beta^r \neq 1$ e quindi che $\beta^r - 1 \neq 0$ come si voleva dimostrare.

dove N risulta essere la lunghezza delle sequenze

In conclusione la trasformata di una sequenza di N elementi esiste solo usando un elemento β il cui ordine è N .

Osservazioni

- La sequenza v di elementi di $GF(q)$ più lunga di cui si può ricavare la trasformata ha $q - 1$ elementi utilizzando un β primitivo.

7. Algebra dei campi finiti di Galois

- Se si sta trasformando una sequenza lunga N allora $\beta^N = 1$, dato che N è l'ordine di β questo implica che se si provasse a calcolare:

$$\begin{aligned}
 V_{N+j} &= \sum_{i=0}^{N-1} v_i \cdot \beta^{i \cdot (N+j)} = \\
 &= \sum_{i=0}^{N-1} v_i \cdot \beta^{i \cdot N} \cdot \beta^{i \cdot j} = \\
 &= \sum_{i=0}^{N-1} v_i \cdot (\beta^N)^i \cdot \beta^{i \cdot j} = \\
 &= \sum_{i=0}^{N-1} v_i \cdot 1^i \cdot \beta^{i \cdot j} = \\
 &= \sum_{i=0}^{N-1} v_i \cdot \beta^{i \cdot j} = \\
 &= V_j
 \end{aligned}$$

struttura ciclica

e quindi si può traslare la sequenza semplicemente scorrendo gli indici dato che $V_N = V_0$.

- Siano $v = (v_0, v_1, \dots, v_{N-1})$ e $z = (z_0, z_1, \dots, z_{N-1})$ due sequenze con coefficienti in $GF(q)$ ed e la sequenza tale che:

$$\begin{aligned}
 e_i &= a \cdot v_i + b \cdot z_i \\
 \forall i < N \\
 a, b &\in GF(q)
 \end{aligned}$$

allora si nota che:

$$\begin{aligned}
 E_j &= \sum_{i=0}^{N-1} e_i \cdot \beta^{i \cdot j} = \\
 &= \sum_{i=0}^{N-1} (a \cdot v_i + b \cdot z_i) \cdot \beta^{i \cdot j} = \\
 &= a \cdot \sum_{i=0}^{N-1} v_i \cdot \beta^{i \cdot j} + b \cdot \sum_{i=0}^{N-1} z_i \cdot \beta^{i \cdot j} = \\
 &= a \cdot V_j + b \cdot Z_j
 \end{aligned}$$

e quindi la trasformata di Fourier è un operatore lineare.

Prima proprietà della DFT Sia $v = (v_0, v_1, \dots, v_{N-1})$ una sequenza con coefficienti in $GF(q)$ allora si può associare una notazione polinomiale

$$v(x) = \sum_{i=0}^{N-1} v_i \cdot x^i$$

notazione polinomiale:

$$\begin{aligned}
 v(x) &= v_0 + v_1 x + \dots + v_{N-1} x^{N-1} \\
 V(x) &= V_0 + V_1 x + \dots + V_{N-1} x^{N-1}
 \end{aligned}$$

da cui si può notare che:

$$\begin{aligned}
 V_j &= \sum_{i=0}^{N-1} v_i \cdot \beta^{i \cdot j} = v(\beta^j) \\
 v_j &= \frac{1}{N} \cdot \sum_{i=0}^{N-1} V_i \cdot \beta^{-i \cdot j} = \frac{1}{N} \cdot V(\beta^{-j})
 \end{aligned}$$

$$\begin{aligned}
 v(x) &= 0 \text{ con } x = \beta^j \\
 V(\beta^j) &= 0 = V_j
 \end{aligned}$$

da cui si può notare che:

$$V_j = 0 \Leftrightarrow \beta^j \text{ è radice di } v(x)$$

Analogamente:

$$V(\beta^{-j}) = 0 \equiv V_j$$

7. Algebra dei campi finiti di Galois

Seconda proprietà della DFT Siano $v = (v_0, v_1, \dots, v_{N-1})$ e $z = (z_0, z_1, \dots, z_{N-1})$ due sequenze con coefficienti in $GF(q)$ e la sequenza e tale che:

$$\begin{aligned} e_i &= v_i \cdot z_i \\ \forall i < N \end{aligned}$$

L'elemento $j < N$ della trasformata di e si ottiene tramite convoluzione circolare di V e Z , trasformate di v e z , ossia:

$$E_j = \frac{1}{N} \cdot \sum_{k=0}^{N-1} V_k \cdot Z_{j-k}$$

Infatti:

$$\begin{aligned} E_j &= \sum_{i=0}^{N-1} e_i \cdot \beta^{i \cdot j} = \\ &= \sum_{i=0}^{N-1} z_i \cdot v_i \cdot \beta^{i \cdot j} = \\ &= \sum_{i=0}^{N-1} z_i \cdot \left[\frac{1}{N} \cdot \sum_{k=0}^{N-1} V_k \cdot \beta^{-k \cdot i} \right] \cdot \beta^{i \cdot j} = \\ &= \frac{1}{N} \cdot \sum_{k=0}^{N-1} V_k \cdot \sum_{i=0}^{N-1} (z_i \cdot \beta^{-k \cdot i} \cdot \beta^{i \cdot j}) = \\ &= \frac{1}{N} \cdot \sum_{k=0}^{N-1} V_k \cdot \underbrace{\sum_{i=0}^{N-1} (z_i \cdot \beta^{i \cdot (j-k)})}_{Z_{j-k}} = \\ &= \frac{1}{N} \cdot \sum_{k=0}^{N-1} V_k \cdot Z_{j-k} \end{aligned}$$

Terza proprietà della DFT Sia $v = (v_0, v_1, \dots, v_{N-1})$ una sequenza con coefficienti in $GF(q)$ e z la sequenza tale che:

$$\begin{aligned} z_i &= v_i \cdot \beta^i \\ \forall i < N \end{aligned}$$

dove β è l'elemento con cui si esegue la trasformata allora si ha che:

$$\begin{aligned} Z_j &= \sum_{i=0}^{N-1} z_i \cdot \beta^{i \cdot j} = \\ &= \sum_{i=0}^{N-1} v_i \cdot \beta^i \cdot \beta^{i \cdot j} = \\ &= \sum_{i=0}^{N-1} v_i \cdot \beta^{(j+1) \cdot i} = \\ &= V_{j+1} \end{aligned}$$

Oss: la rotazione circolare di V non modifica la nullità o non nullità dei v_i e viceversa (gli elementi nulli della TDF Restano nulli)

$$\begin{array}{ccc} J_i = V_i \alpha^i & \iff & J_j = J_{i+1} \\ J_i = V_{i \text{ mod } N} & \iff & J_j = J_i \cdot \alpha^{j-i} \end{array}$$

ossia la trasformata di z è quella di v traslata di una posizione. Dualmente si ha che data una $V = (V_0, V_1, \dots, V_{N-1})$ sequenza trasformata dalla sequenza v con elementi in $GF(q)$ e la sequenza trasformata Z tale che:

$$\begin{aligned} Z_i &= V_i \cdot \beta^i \\ \forall i < N \end{aligned}$$

7. Algebra dei campi finiti di Galois

si ha che:

$$\begin{aligned} z_j &= \sum_{i=0}^{N-1} Z_i \cdot \beta^{-i \cdot j} = \\ &= \sum_{i=0}^{N-1} V_i \cdot \beta^i \cdot \beta^{-i \cdot j} = \\ &= \sum_{i=0}^{N-1} V_i \cdot \beta^{-(j-1) \cdot i} = \\ &= v_{j-1} \end{aligned}$$

Primo corollario della terza proprietà Sia $v = (v_0, v_1, \dots, v_{N-1})$ una sequenza con coefficienti in $GF(q)$ e z la sequenza ruotata di una posizione ossia tale che:

$$\begin{aligned} z_i &= v_{i-1} && \text{la rotazione ciclica dell'antitrasformata si ottiene come} \\ &\forall i < N && \\ Z_i &= V_i \cdot \beta^i && \begin{array}{l} \text{9} \\ \text{||} \end{array} \quad \sum_{i=0}^{N-1} v_i \cdot \beta^{iu} \Rightarrow v_k \text{ ha come radice } \beta^i \Rightarrow \sqrt[i]{v_k} \end{aligned}$$

Dalla terza proprietà si è visto che:

quindi se esiste un indice k tale che $V_k = 0$ allora anche $Z_k = 0$, e quindi anche tutte le altre versioni ruotate di v hanno la trasformata nulla nella posizione k .

Secondo corollario della terza proprietà Dualmente si ha che data una $V = (V_0, V_1, \dots, V_{N-1})$ sequenza trasformata dalla sequenza v con elementi in $GF(q)$ e la sequenza trasformata Z tale che:

$$Z_i = V_{i+1} \quad \forall i < N \quad \text{rotazione ciclica della trasformata}$$

dalla terza proprietà si è visto che:

$$z_i = v_i \cdot \beta^i \quad \forall i < N$$

e quindi se esiste un indice k tale che $v_k = 0$ allora anche $z_k = 0$ e quindi anche tutte le altre versioni ruotate di V hanno l'antitrasformata nulla nella posizione k .

Quarta proprietà della DFT Sia $v = (v_0, v_1, \dots, v_{N-1})$ una sequenza con elementi in $GF(q)$ con trasformata $V = (V_0, V_1, \dots, V_{N-d}, 0, \dots, 0)$ (ossia con gli ultimi $d - 1$ elementi nulli) calcolata con β di ordine N , allora si ha che il polinomio $V(x)$ ha al più grado $N - d$ e quindi per il teorema fondamentale dell'algebra ha al più $N - d$ radici. Tutte le radici di $V(x)$ possono essere rappresentate in notazione esponenziale β^{-i} , dato che β ha ordine N , e quindi dalla prima proprietà si ottiene che:

$$\text{Ha al più } N - d \text{ radici cioè: } \sqrt[d]{(\beta^i)} = 0 \Leftrightarrow j_i = 0 \quad v_i = V(\beta^{-i}) = 0$$

- teorema si basa da rappresentazione polinomiale di grado $N - 1$ con gli elementi della sequenza che sono N
- c'è un fattore 1 che balza a causa di v_0

e quindi ci sono al più $N - d$ elementi nulli nella sequenza e quindi ci sono almeno d elementi non nulli.

Corollario della quarta proprietà Per il secondo corollario della terza proprietà si ha che la quarta proprietà vale anche se i $d - 1$ elementi nulli della trasformata non sono gli ultimi e basta che siano consecutivi (ciclicamente) poiché si è visto che se la sequenza v ha un elemento nullo in posizione k anche l'antitrasformata della sua trasformata ruotata ha l'elemento in posizione k nullo. Quindi se v ha L elementi nulli li hanno anche le antitrasformate delle versioni ruotate della trasformata di v .

dipendenza da beta k

7. Algebra dei campi finiti di Galois

Quinta proprietà Sia $v = (v_0, v_1, \dots, v_{N-1})$ una sequenza con elementi in $GF(p)$ con p primo, allora:

$$\begin{aligned} V_{j \cdot p^k} &= v\left(\beta^{j \cdot p^k}\right) = \\ &= v\left(\beta^j\right)^{p^k} = \\ &= V_j^{p^k} \end{aligned}$$

8. Codifica per la trasmissione su un canale BSC

8.1. Considerazioni generali e distanza di Hamming

Ripasso canale $BSC(\varepsilon)$ Il canale $BSC(\varepsilon)$ è un canale con alfabeto binario in cui:

$$P_{Y|X}(y|x) = \begin{cases} \varepsilon & x \neq y \\ 1 - \varepsilon & x = y \end{cases}$$

la cui capacità è:

$$C = 1 - H_2[\varepsilon]$$

Si era visto che il caso peggiore si ha con $\varepsilon = \frac{1}{2}$ e che spostandosi in entrambe le direzioni il comportamento del canale è identico, infatti avendo $\varepsilon > \frac{1}{2}$ si possono invertire i bit di uscita ottenendo una probabilità di errore pari a $1 - \varepsilon < \frac{1}{2}$. Per questo motivo si può ipotizzare che $0 \leq \varepsilon \leq \frac{1}{2}$.

Definizione di distanza di Hamming Date due sequenze binarie \underline{x}_1 e \underline{x}_2 si definisce distanza di Hamming $d_H(\underline{x}_1, \underline{x}_2)$ il numero di bit diversi tra \underline{x}_1 e \underline{x}_2 ^I.

Definizione di peso di Hamming Data una sequenza binaria lecita \underline{c} si definisce peso di Hamming $W(\underline{c})$ il numero di bit a 1 della sequenza^{II}, ossia:

$$W(\underline{c}) = d_H(\underline{c}, \underline{0})$$

Probabilità condizionata di una sequenza Se si considera un canale senza memoria la probabilità condizionata sulle sequenze è pari al prodotto di quelle dei singoli segnali e quindi:

$$P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) = \prod_{n=1}^N P_{Y|X}(y_n|x_n)$$

e quindi se ci sono d bit trasmessi con errore, ossia la distanza di Hamming tra \underline{x} e \underline{y} , si ottiene:

$$\begin{aligned} P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) &= \prod_{n=1}^N P_{Y|X}(y_n|x_n) = \\ &= \prod_{n=1}^d \varepsilon \cdot \prod_{n=1}^{N-d} (1-\varepsilon) = \\ &= \varepsilon^d \cdot (1-\varepsilon)^{N-d} \end{aligned}$$

Decodificatore ML di un canale BSC Un decodificatore ML sceglie la sequenza che massimizza la probabilità condizionata:

$$\begin{aligned} \hat{\underline{x}}_{ML} &= \arg \max_{\underline{x} \text{ lecito}} P_{\underline{Y}|\underline{X}}(\underline{y}_R|\underline{x}) = \\ &= \arg \max_{\underline{x} \text{ lecito}} \varepsilon^d \cdot (1-\varepsilon)^{N-d} \end{aligned}$$

^IIn generale, date due sequenze \underline{x}_1 e \underline{x}_2 la distanza di Hamming è il numero di simboli diversi tra \underline{x}_1 e \underline{x}_2 .

^{II}In generale, il peso di Hamming di una sequenza è il numero di simboli diversi da 0 della sequenza stessa.

8. Codifica per la trasmissione su un canale BSC

con $d = d_H(\underline{y}_R, \underline{x})$; dato che $0 \leq \varepsilon \leq \frac{1}{2}$ (e quindi $\varepsilon < 1 - \varepsilon$) si ha che:

$$\begin{aligned}\hat{\underline{x}}_{ML} &= \arg \max_{\underline{x} \text{ lecita}} \varepsilon^d \cdot (1 - \varepsilon)^{N-d} = \\ &= \arg \min_{\underline{x} \text{ lecita}} d = \\ &= \arg \min_{\underline{x} \text{ lecita}} d_H(\underline{y}_R, \underline{x})\end{aligned}$$

e quindi il decodificatore a massima verosimiglianza in un canale *BSC* corrisponde al decodificatore a minima distanza di Hamming, ossia il decodificatore prende la sequenza legittima che si ottiene variando meno bit possibili rispetto alla sequenza ricevuta.

Per questo motivo nei codici per canali *BSC* si cerca di massimizzare la distanza di Hamming tra le varie sequenze legittime in modo che servano tanti errori per portare un codice legittimo «più vicino» a un altro codice legittimo, riducendo quindi la probabilità di errore.

aumentare la distanza di hamming tra sequenze lecite del codice

Codici a distanza di Hamming d Un codice si definisce a distanza di Hamming d se prese due sequenze lecite \underline{c}_1 e \underline{c}_2 vale:

$$d_H(\underline{c}_1, \underline{c}_2) \geq d \quad \boxed{\text{distanza tra codici leciti}}$$

ossia data una sequenza legittima qualsiasi bisogna almeno fare d variazioni per ottenerne un'altra legittima.

Potere rivelatore di un codice a distanza di Hamming d In un codice a distanza di Hamming d per poter ottenere un codice lecito partendo da un altro codice lecito bisogna modificare d bit e quindi se nella trasmissione avvengono meno di d errori al ricevitore arriva sicuramente una sequenza non lecita e quindi è in grado di rivelare l'errore. Per questo motivo la sua potenza rivelatrice è pari a:

$$r = d - 1$$

yR è lecita? il rivelatore mi dice se la sequenza risulta essere lecita oppure no:
 • se commetto $d - 1$ variazioni rispetto all'ingresso arriva una sequenza non lecita
 • altrimenti non sono in grado di dire nulla

Potere correttore di un codice a distanza di Hamming d In un codice a distanza di Hamming d se si commettono $m < d$ errori la sequenza ricevuta si trova a una distanza di Hamming di m dalla sequenza inviata e a $d - m$ dalla sequenza sbagliata «più vicina». Dato che il ricevitore seleziona la sequenza con la distanza di Hamming minore sceglie la sequenza corretta se:

La correzione avviene durante la codifica ML, quando le ricevitore sceglie la sequenza lecita più vicina

$$m < \underline{d - m} \quad \boxed{\text{La più vicina sequenza lecita sbagliata}}$$

ossia se:

$$m < \frac{d}{2}$$

quindi se d è dispari il ricevitore può correggere un numero massimo di errori di:

$$\frac{d}{2} - \frac{1}{2}$$

mentre se d è pari:

$$\frac{d}{2} - 1 = \left\lfloor \frac{d}{2} - \frac{1}{2} \right\rfloor$$

quindi il potere correttore vale:

$$t = \left\lfloor \frac{d}{2} - \frac{1}{2} \right\rfloor = \left\lfloor \frac{d - 1}{2} \right\rfloor$$

4. In che ordine avviene tutto?

1. Il ricevitore controlla se la sequenza ricevuta è lecita.
 - Se è una sequenza valida → nessun errore.
 - Se non è lecita, significa che c'è stato almeno un errore → interviene la rivelazione.
2. Se la sequenza ricevuta è errata, il decodificatore ML cerca la sequenza lecita più vicina.
 - Se il numero di errori m è minore di t , si corregge con successo.
 - Se $m \geq t$, il decoder potrebbe sbagliare, introducendo un errore di decodifica.

Conclusione

- La rivelazione degli errori avviene prima della decodifica ML e identifica le sequenze sicuramente errate.
- La correzione avviene durante la decodifica ML, selezionando la sequenza più vicina tra quelle lecite.

8. Codifica per la trasmissione su un canale BSC

Distanza di Hamming dei codici lineari Siano \underline{c}_1 una sequenza legittima con n bit a uno e $N - n$ bit a zero e \underline{c}_2 un'altra sequenza lecita. Allora $\underline{c}_3 = \underline{c}_1 + \underline{c}_2$ è ancora una sequenza lecita, ma \underline{c}_3 si ottiene modificando n bit della sequenza \underline{c}_2 e quindi la distanza di Hamming tra \underline{c}_3 e \underline{c}_2 è pari a n . Inoltre si può notare che n è la distanza di Hamming tra la sequenza \underline{c}_1 e la sequenza nulla $\underline{0}$, quindi:

$$d_H(\underline{c}_1 + \underline{c}_2, \underline{c}_2) = d_H(\underline{c}_1, \underline{0})$$

dato un codice lineare, la sequenza nulla è sempre una sequenza lecita

Applicando questo risultato con $\underline{c}_1 = \underline{c}_a + \underline{c}_b$ e $\underline{c}_2 = \underline{c}_a$ (dove \underline{c}_a e \underline{c}_b sono lecite) si ottiene:

$$\begin{aligned} d_H(\underline{c}_a + \underline{c}_b + \underline{c}_a, \underline{c}_a) &= d_H(\underline{c}_a + \underline{c}_b, \underline{0}) \\ d_H(\underline{c}_b, \underline{c}_a) &= d_H(\underline{c}_a + \underline{c}_b, \underline{0}) \end{aligned}$$

quindi la distanza di Hamming tra due sequenze lecite è uguale alla distanza di Hamming della loro somma dalla sequenza nulla. Quindi il numero n di 1 nella sequenza con il minor numero di 1 (esclusa quella nulla) è anche la distanza di Hamming del codice.

Osservazione In un codice lineare la distanza di Hamming d vale:

$$d = \min_{\substack{\underline{c} \in C \\ \underline{c} \neq \underline{0}}} W(\underline{c})$$

8.2. Prestazioni di un codice per canali BSC

Le prestazioni di un codice si possono calcolare tramite la probabilità che ha il decodificatore di fallire e quindi dipende dal valore di t e di r e quindi dalla distanza di Hamming d .

probabilità di mancata rivelazione di errore (Pr)

Probabilità di errore di un codice rivelatore La probabilità di sbagliare a rivelare una parola (word in inglese) si può ottenere sommando le probabilità che capiti una sequenza che non si sa rivelare, ossia con almeno $r + 1 = d$ errori.

- ho un'ambiguità tra due sequenze
- distanza di hamming tra codici = d

$$P_{rw} = \sum_{e=d}^N P_{\text{di ricevere}} \cdot P_{\text{avere } e \text{ errori}}$$

- r = numero massimo di errori rilevabili
- N = lunghezza della parola o del codice trasmesso
- A_e = numero di sequenze possibili con esattamente e errori

La probabilità di ricevere una determinata sequenza con e errori è:

$$\varepsilon^e \cdot (1 - \varepsilon)^{N-e}$$

e questo va moltiplicato per il numero A_e di sequenze possibili con e errori, ottenendo:

probabilità totale di errore nella rivelazione di una parola (word)

$$P_{rw} = \sum_{e=d}^N A_e \cdot \varepsilon^e \cdot (1 - \varepsilon)^{N-e}$$

| • A_e : numero di parole C di peso di Hamming e => spettro di Hamming di C
• ossia numero di sequenze di lunghezza N che differiscono in esattamente e posizioni rispetto alla sequenza originale

Avere e errori corrisponde a ricevere una sequenza con distanza di Hamming e rispetto alla sequenza inviata e dato che:

$$\begin{aligned} d_H(\underline{c}_R, \underline{c}_T) &= d_H(\underline{c}_R + \underline{c}_T, \underline{0}) \\ e &\leftarrow d_H(\underline{c}_R + \underline{c}_T, \underline{0}) \\ e &= W(\underline{c}_R + \underline{c}_T) \end{aligned}$$

Quindi per ogni coppia di messaggi \underline{c}_R e \underline{c}_T con distanza di Hamming e esiste un codice \underline{c} con peso di Hamming e e quindi il numero A_e di possibili sequenze con e errori corrisponde al numero di sequenze con peso di Hamming di e .

$$P_{rw} = \sum_{e=d}^N A_e \cdot \varepsilon^e \cdot (1 - \varepsilon)^{N-e} \quad \textcolor{red}{\approx A_d \cdot \varepsilon^d \cdot (1 - \varepsilon)^{N-d}}$$

e dominante
 $e = d$

8. Codifica per la trasmissione su un canale BSC

probabilità di mancata correzione (P_e)

Probabilità di errore di un codice correttore La probabilità di sbagliare a correggere una parola (word in inglese) si può ottenere sommando le probabilità che capiti una sequenza che non si sa correggere, ossia con almeno $t + 1$ errori.

$$P_{tw} = \sum_{e=t+1}^N P_{\text{di avere } e \text{ errori}}$$

La probabilità di avere una determinata sequenza con e errori è:

$$\varepsilon^e \cdot (1 - \varepsilon)^{N-e}$$

mentre il numero di possibili sequenze con e errori è dato dalla binomiale e quindi:

- numero di combinazioni (o disposizioni senza ripetizione chiamata anche semplice) di e elementi scelti da un insieme di N oggetti
- NB: rappresenta il numero di modi/sequenze in cui possono verificarsi i errori nelle N posizioni della sequenza trasmessa
- ⇒ Non deve ripetersi un elemento perché rappresenta la posizione effettiva all'interno della sequenza lunga N
- ⇒ identifica tutte le sequenze con e errori tramite disposizione, dove e del coefficiente è la posizione dell'errore

variabile casuale discreta chiamata anche bernulliana

$$\begin{aligned} P_{tw} &= \sum_{e=t+1}^N \binom{N}{e} \cdot \varepsilon^e \cdot (1 - \varepsilon)^{N-e} = \\ &= \sum_{e=t+1}^N N_e \quad \text{probabilità} \quad 0 \leq N_e \leq 1 \end{aligned}$$

La variabile casuale N_e è una distribuzione binomiale e quindi ha valore atteso $\mathbb{E}_e [N_e] = N \cdot \varepsilon$ e il suo andamento cresce fino a raggiungere questo valore e poi decresce tendendo a 0, come mostrato in figura 8.1.

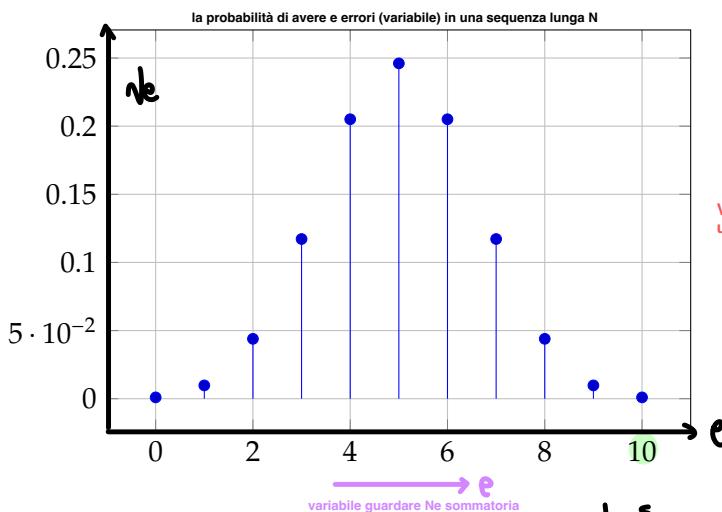


Figura 8.1.: Andamento di una binomiale $B(10, 0.5)$.

- fissa la probabilità di errore su canale
- lunghezza N sequenza massima fissata
- e (numero di bit sbagliati) variabile fino ad N

La probabilità P_{tw} è la somma di tutti valori che assume N_e quando $e > t + 1$ e quindi più $t + 1$ è grande più piccoli sono questi valori e quindi più bassa è la probabilità che il correttore sbagli, per questo motivo si può supporre che $t + 1 \gg N \cdot \varepsilon$. Con questa approssimazione si può scrivere:

Sono molto più a destra della media
quindi la probabilità di sbagliare è molto bassa

$$P_{tw} \approx \binom{N}{t+1} \cdot \varepsilon^{t+1} \cdot (1 - \varepsilon)^{N-t-1}$$

ossia si considera che la probabilità di avere $t + 1$ errori sia quella dominante dato che quelle successive sono sempre più piccole. Si può anche supporre che $N \gg t + 1$ e quindi:

$$\begin{aligned} P_{tw} &\approx \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \cdot (1 - \varepsilon)^{N-t-1} \approx \\ &\approx \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \cdot (1 - \varepsilon)^N \end{aligned}$$

dato che $N \gg t + 1$ e $t + 1 \gg N \cdot \varepsilon$ allora $\varepsilon \approx 0$ e quindi:

$$\begin{aligned} P_{tw} &\approx \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \cdot 1^N = \\ &= \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \end{aligned}$$

8. Codifica per la trasmissione su un canale BSC

probabilità di errore sul singolo all'uscita del decodificatore (P_b)

Probabilità di sbagliare la correzione di un singolo bit Questo valore non è facilmente calcolabile, ma si possono ricavare degli estremi, infatti nel peggior dei casi data una sequenza sbagliata il correttore esegue al massimo t modifiche e quindi:

$$P_{tb} \leq \sum_{e=t+1}^N \frac{e+t}{N} \cdot \binom{N}{e} \cdot \varepsilon^e \cdot (1-\varepsilon)^{N-e}$$

ossia si aggiungono t bit sbagliati agli e già sbagliati, mentre nel migliore dei casi il correttore si accorge che non può correggere la sequenza e quindi non prova nemmeno a correggere:

$$P_{tb} \geq \sum_{e=t+1}^N \frac{e}{N} \cdot \binom{N}{e} \cdot \varepsilon^e \cdot (1-\varepsilon)^{N-e}$$

Usando le stesse approssimazioni fatte precedentemente ($N \gg t+1$ e $t+1 \gg N \cdot \varepsilon$) si ottiene:

questa approssimazione porta a considerare la probabilità dominante $e = t+1$ nella somma

$$\begin{aligned} P_{tb} &\leq \frac{t+1+t}{N} \cdot \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \approx \\ &\approx \frac{2 \cdot t + 2}{N} \cdot \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \approx \\ &\approx 2 \cdot \frac{N^t}{t!} \cdot \varepsilon^{t+1} \end{aligned}$$

aggiunto
 $t+2 = 2(t+1)$
per semplificare
il fattoriale
 $(t+1)! = (t+1) \cdot (t)$.

$$\begin{aligned} P_{tb} &\geq \frac{t}{N} \cdot \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \approx \\ &\approx \frac{t+1}{N} \cdot \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \approx \\ &\approx \frac{N^t}{t!} \cdot \varepsilon^{t+1} \end{aligned}$$

e quindi:

$$\frac{N^t}{t!} \cdot \varepsilon^{t+1} \leq P_{tb} \leq 2 \cdot \frac{N^t}{t!} \cdot \varepsilon^{t+1}$$

- N : numero totale di bit
- t : numero massimo di errori correggibili
- ε : probabilità di errore per bit

8.3. Codici derivati

Codici estesi Dato un codice $C(N, K, d)$ ^{III} si può ricavare il codice $C_e(N+1, K, d_e)$ esteso aggiungendo un bit di parità complessivo a ogni codice (ossia si aggiunge un bit che è pari alla somma di tutti gli altri bit). Questo codice ha le seguenti proprietà:

- $R_e = \frac{K}{N+1} < R$ e quindi il ritmo diminuisce.
- Se C è lineare lo è anche C_e dato che si aggiunge un bit che si calcola tramite una combinazione lineare degli altri.
- Se il numero di 1 del codice è dispari si aggiunge un 1, mentre se è pari si aggiunge uno 0.
- Per l'osservazione fatta prima la distanza di Hamming d_e è sicuramente pari e quindi:
 - Se d è dispari allora:
 - $d_e = d + 1$
 - $r_e = d_e - 1 = d + 1 - 1 = r + 1$

^{III}Un codice che trasmette sequenze lunghe N simboli con K bit di informazione per sequenza trasmessa e distanza di Hamming d .

8. Codifica per la trasmissione su un canale BSC

$$- t_e = \left\lceil \frac{d_e + 1}{2} \right\rceil = \left\lceil \frac{d + 1}{2} + \frac{1}{2} \right\rceil = \left\lceil \frac{d + 1}{2} \right\rceil = t$$

o Se d è pari allora:

$$\begin{aligned} - d_e &= d \\ - r_e &= d_e - 1 = d - 1 = r \\ - t_e &= \left\lceil \frac{d_e + 1}{2} \right\rceil = \left\lceil \frac{d + 1}{2} \right\rceil = t \end{aligned}$$

Codici accorciati Dato un codice $C(N, K, d)$ ^{IV} si può ricavare il codice $C_A(N - a, K - a, d_a)$ accorciato forzando a a bit e non trasmettendoli e quindi usando un sottoinsieme dei valori originari; in genere la distanza di Hamming non varia, ma in alcuni casi può diminuire o aumentare.

Codici ibridi I codici visti fino a ora venivano usati o come correttori o come rivelatori, ma si possono usare anche come ibridi. Si consideri un codice in cui si desidera avere potere correttore t : se $2 \cdot t < d$ allora ci sono $d - 2 \cdot t$ codici che non vengono corretti, ma si riesce a capire se sono sbagliati oppure no. Per questo motivo dato un codice a distanza di Hamming d , perché questo possa essere usato come codice ibrido deve valere:

$$d > 2 \cdot t + r$$

e quindi nel caso migliore:

$$d - 1 = 2 \cdot t + r$$

Da questo si possono anche ricavare i codici non ibridi infatti:

- Un codice rivelatore ha $t = 0$ e quindi:

$$d - 1 = r$$

- Un codice correttore ha $r = 0$ e quindi:

$$d - 1 = 2 \cdot t$$

8.4. Codice a parità semplice (Simple Parity Check)

Definizione Il codice a parità semplice è un codice sistematico lineare con sequenze lunghe $N = K + 1$ e quindi con un solo bit di parità, che si ricava sommando tutti gli elementi della sequenza i .

In questo codice il numero di sequenze lecite è:

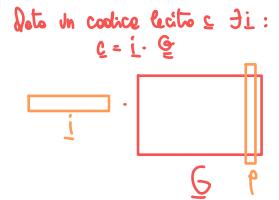
$$2^K = 2^{N-1} = \frac{2^N}{2}$$

Matrice generatrice Dato che è un codice sistematico la matrice generatrice contiene la matrice identità $K \times K$ e una matrice \underline{P} di dimensione $K \times (N - K)$ che permette la costruzione del bit di parità. In questo caso la matrice \underline{P} ha una sola colonna, infatti $N - K = K + 1 - K = 1$ e dato che il bit di parità è sempre uguale alla somma di tutte le cifre, questa matrice sarà formata da una colonna di soli 1 e quindi:

$$\underline{P} = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

$$\underline{G} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \end{bmatrix} = \begin{bmatrix} \underline{I} & \underline{P} \end{bmatrix}$$

• con la matrice generatrice, io creo un codice lecito
• con la matrice di parità, identifico se il codice sia lecito o meno



^{IV}Un codice che trasmette sequenze lunghe N simboli con K bit di informazione per sequenza trasmessa e distanza di Hamming d .

8. Codifica per la trasmissione su un canale BSC

Matrice di parità La matrice di parità si può costruire conoscendo \underline{P} e quindi vale:

$$\underline{H} = \begin{bmatrix} \underline{P} \\ \underline{\underline{I}} \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{bmatrix}$$

Dato una sequenza \underline{u} v'è solo:

$$\underline{u} \cdot \underline{H} = \underline{r} \quad \text{se } \underline{u} = 0 \Rightarrow \underline{u} \text{ è lecito (bit a 0 pari)}$$

se $\underline{u} \neq 0$ ottimamente

intendo che $\underline{H} = (\underline{1})$ ord:

$$\sum_i r_i = 0 \Rightarrow \underline{u} \text{ lecito} \Rightarrow n \text{ a pari}$$

Quindi per stabilire se una sequenza fa parte del codice basta contare gli 1 nel codice, i quali devono sempre essere in numero pari in modo che la loro somma si annulli, rendendo questo codice molto semplice da controllare e da decodificare.

- dato il mio codice K bit di informazione, è 1 bit di parità
- il bit di parità che aggiungo è dato dalla somma di tutti gli altri elementi all'interno del codice
- se ho un numero pari di 1 allora il bit che aggiungo è 0
- se ho un numero dispari di 1 il bit che aggiungo è 1

Distanza di Hamming Dato che sono legittime solo le sequenze con un numero di 1 pari è facile capire che il minimo peso di Hamming è 2 e quindi questo codice ha una distanza di Hamming di 2. Da questo si può ricavare che:

- Dato che le sequenze lecrite hanno numero di UNI pari
- da una sequenza lecita all'altra devo cambiare 2 bit

$$r = d - 1 = 1$$

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0$$

dato un \underline{u} è lecito dimostro che:

$$W(\underline{u}) = d_H(\underline{u}, \underline{0}) = 2$$

$$r = d - 1 = 1$$

$$d - 1 = 2 \cdot 1 + 1 \Rightarrow t = 0$$

quindi questo codice è in grado di rilevare solo un errore e non è in grado di correggerne alcuno.

8.5. Codici di Hamming

non posso includere il vettore 0 perché qualsiasi cosa moltiplicata per zero restituisce zero ed è il vettore che mi permette di capire che ho una sequenza lecita

Definizione I codici di Hamming sono codici sistematici lineari la cui matrice di parità \underline{H} contiene tutte le combinazioni di $N - K$ bit esclusa quella nulla. I codici di Hamming possono essere usati a diversi valori di N : l'unico vincolo è che la matrice \underline{H} abbia $2^{N-K} - 1$ righe, e dato che la matrice \underline{H} ha sempre N righe si ha:

Il numero delle righe della matrice H deve essere uguale al numero totale di combinazioni che si possono comporre con la parte destra dell'equazione

$$N = 2^{N-K} - 1$$

$$\underline{J} \cdot \underline{H} = \underline{0}$$

$C \times N$ $C \times (N-K)$
 $C \times N$ $C \times (d-n)$

e quindi si possono formare codici di Hamming a diverse lunghezze N , come mostrato nella tabella 8.1.

$N - K$	N	K	R
2	$2^2 - 1 = 3$	$3 - 2 = 1$	$\frac{1}{3} = 0.333$
3	$2^3 - 1 = 7$	$7 - 3 = 4$	$\frac{4}{7} = 0.571$
4	$2^4 - 1 = 15$	$15 - 4 = 11$	$\frac{11}{15} = 0.733$
5	$2^5 - 1 = 31$	$31 - 5 = 26$	$\frac{26}{31} = 0.838$
\vdots	\vdots	\vdots	\vdots

Tabella 8.1.: Tabella delle lunghezze dei codici di Hamming.

Inoltre, fissata una lunghezza l'ordine delle righe della matrice \underline{H} non è determinante e quindi si possono creare diverse varianti del codice.

Idea alla base dei codici di Hamming Sia \underline{c} una sequenza lecita e \underline{c}_1 la sequenza che si ottiene introducendo un errore all' n -esimo bit c_n , ossia:

$$\underline{c}_1 = \underline{c} + \underline{e}_n$$

dove \underline{e}_n è un vettore $1 \times N$ con tutti i bit a 0 tranne l' n -esimo bit. Moltiplicando questa sequenza con la matrice di parità:

$$\begin{aligned} \underline{c}_1 \cdot \underline{H} &= (\underline{c} + \underline{e}_n) \cdot \underline{H} = \\ &= \underline{c} \cdot \underline{H} + \underline{e}_n \cdot \underline{H} \\ &\stackrel{H}{=} \underline{0} \end{aligned}$$

8. Codifica per la trasmissione su un canale BSC

e dato che \underline{c} è una sequenza lecita:

$$\underline{c}_1 \cdot \underline{\underline{H}} = \underline{e}_n \cdot \underline{\underline{H}}$$

ossia \underline{c}_1 è l' n -esima riga della matrice $\underline{\underline{H}}$ e dato che nei codici di Hamming la matrice $\underline{\underline{H}}$ ha tutte le righe diverse si riesce a capire che l'errore è presente sull' n -esimo bit, permettendo quindi la correzione.

Introducendo due errori, invece, si ha che (con $m \neq n$):

$$\underline{c}_1 = \underline{c} + \underline{e}_n + \underline{e}_m$$

$$\underline{c}_1 \cdot \underline{\underline{H}} = \underline{e}_n \cdot \underline{\underline{H}} + \underline{e}_m \cdot \underline{\underline{H}}$$

|| In uscita ottengo la somma di due vettori

e quindi non è più possibile capire la posizione dell'errore e di conseguenza correggerlo.

Matrice di parità Dato che i codici di Hamming sono lineari e sistematici, la matrice di parità deve contenere tutte le possibili combinazioni a $N - K$ bit esclusa quella nulla e si presenta nella forma:

$$\underline{\underline{H}} = \begin{bmatrix} P \\ \vdots \\ I \\ \vdots \end{bmatrix}$$

risiedono le combinazioni con un solo bit 1

quindi, dato che la matrice identità contiene tutte le combinazioni con un un solo bit a 1, la matrice $\underline{\underline{P}}$ dovrà contenere tutte le altre combinazioni, ossia quelle con almeno 2 bit a 1.

Matrice generatrice Dato che è un codice lineare sistematico la matrice generatrice è sempre nella forma:

$$\underline{\underline{G}} = \begin{bmatrix} I & P \end{bmatrix}$$

dove $\underline{\underline{P}}$ contiene tutte le combinazioni con almeno 2 bit a 1.

Distanza di Hamming Dato che tutte le righe della matrice generatrice fanno parte del codice allora esiste almeno una sequenza lecita \underline{c}_1 tale che $W(\underline{c}_1) = 3$ dato che:

- La matrice di identità ha uno e uno solo bit a 1 per riga.
- In $\underline{\underline{P}}$ sono presenti tutte le combinazioni con almeno due bit a 1 e quindi sono presenti delle righe con solo 2 bit a 1.

Inoltre si può dimostrare che non ci sono sequenze legittime con peso minore e quindi:

$$d = \min_{\substack{\underline{c} \in \underline{C} \\ \underline{c} \neq \underline{0}}} W(\underline{c}) = 3$$

da cui si nota che:

$$\begin{aligned} r &= d - 1 = 2 \\ t &= \left\lceil \frac{d-1}{2} \right\rceil = 1 \end{aligned}$$

quindi il potere correttore è 1 come si era mostrato precedentemente.

- nota bene**
- quando faccio il prodotto tra vettori e matrice, la somma risulta essere binaria
 - quindi P contiene tutte le possibili combinazioni

8. Codifica per la trasmissione su un canale BSC

Osservazione La decodifica funziona in modo analogo anche utilizzando la notazione esponenziale; infatti, dato il polinomio generatore $g(x)$, se si riceve una sequenza con un errore in posizione j :

$$v(x) = c(x) + x^j \quad \begin{aligned} e_j &= (0 \dots \underset{j}{1} \dots 0) \\ g(x) &= 1 x^j = x^j \end{aligned}$$

si ottiene:

$$\begin{aligned} \text{Resto} \left[\frac{c(x) + x^j}{g(x)} \right] &= \text{Resto} \left[\frac{c(x)}{g(x)} \right] + \text{Resto} \left[\frac{x^j}{g(x)} \right] \\ &= \text{Resto} \left[\frac{x^j}{g(x)} \right] = r_j \end{aligned}$$

Questo resto è unico perché se esistesse un'altra posizione $i \neq j$ tale che $r_i = r_j$ allora si avrebbe che la sequenza $x^j + x^i$ è lecita:

$$\begin{aligned} \text{Resto} \left[\frac{x^i + x^j}{g(x)} \right] &= \text{Resto} \left[\frac{x^i}{g(x)} \right] + \text{Resto} \left[\frac{x^j}{g(x)} \right] \\ &= r_i + r_j = 0 \end{aligned}$$

ma questo non è possibile perché la distanza di Hamming del codice, e quindi anche il peso minimo, è 3. Quindi tramite la sequenza ottenuta calcolando il resto si può individuare la posizione dell'errore.

Conclusioni sui codici di Hamming Come si è visto dalla tabella 8.1 si può alzare N e R del codice a piacimento mantenendo il potere correttore di 1 e distanza di Hamming di 3, il che è un'ottima proprietà, in quanto il teorema di Shannon suggerisce che aumentando N è possibile diminuire la probabilità che il ricevitore ML sbagli e quindi, nei codici BSC , il potere correttore (e di conseguenza anche la distanza di Hamming).

Esempio di codice di Hamming Si consideri il codice di Hamming con $N = 7$ e quindi $K = 4$, ossia il caso della seconda riga della tabella 8.1, con:

$$\underline{\underline{P}} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

e quindi:

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

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

8.6. Codici ciclici

8.6.1. Introduzione

Definizione Un codice circolare C è un insieme di sequenze \underline{c} di elementi in $GF(q)$ tali che la loro trasformata di Fourier, usando un coefficiente $\beta \in GF(q)$, è nulla per tutti e soli gli indici j_1, \dots, j_L stabiliti.

8. Codifica per la trasmissione su un canale BSC

Osservazioni

- L'insieme $L = \{j_1, \dots, j_L\}$ degli indici per cui la trasformata delle sequenze lecite è nulla, insieme a q , definisce univocamente il codice.
- La lunghezza del codice N è stabilita dalla lunghezza delle sequenze e quindi all'ordine di β .

Il numero di elementi distinti che beta può generare ciclicamente prima di tornare a uno è N
 è necessario che sia N per
 beta è il generatore del gruppo
 moltiplicativo finito (finito di
 elementi) di ordine N

Polinomio generatore Dire che $C_j = 0$ implica che β^j è una radice di $c(x)$ per la prima proprietà delle trasformate e quindi:

$$c(\beta^j) = 0 = C_j \\ \forall j \in L \\ \forall c(x) \text{ polinomio associato a } c \in C$$

per tutte le sequenze lecite appartenenti al codice hanno come radici beta di L

dato che un polinomio si può sempre scrivere come $c(x) = (x - x_1) \cdot (x - x_2) \cdot \dots$ dove x_1, x_2, \dots sono le radici del polinomio si ha che tutti i $c(x) \in C$ sono divisibili per:

$$\prod_{j \in L} (x - \beta^j)$$

esempio:
 $x^4 - 1 = (x+1)(x-1)$
 $x^2 - 1 \Rightarrow x = \pm 1$

e quindi il polinomio generatore del codice è:

$$g(x) = \prod_{j \in L} (x - \beta^j)$$

tutte le radici di $g(x)$ appartengono a X^{N-1}

$$X^4 - 1 = (\beta^j)^4 - 1 \quad \forall j \in L \\ = 1 - 1 = 0$$

$\beta^{j \cdot N}$ multiplo della ordine

Osservazioni sul polinomio generatore

Per mantenere le proprietà cicliche di un codice

- $g(x)$ è sicuramente un divisore di $X^N - 1$ poiché per qualsiasi radice β^j di $g(x)$ si ha che $(\beta^j)^N = 1$ e quindi tutte le radici di $g(x)$ sono anche radici di $X^N - 1$, anche se quest'ultimo potrebbe avere anche altre radici.
- Dato che il grado del polinomio generatore corrisponde a $N - K$ e quindi al numero di bit di parità, il numero di elementi di L definisce il numero di bit di parità del codice.
- Dato che $g(x)$ è il polinomio associato a una sequenza lecita di codice si ha che la distanza di Hamming del codice è inferiore al peso di Hamming di $g(x)$, ossia $d \leq W(g(x))$.

il numero delle radici di $g(x)$ è $N - K$
 (teorema fondamentale dell'algebra)

Ciclicità del codice Sia $c(x)$ una sequenza lecita, allora:

$$C_j = 0 \\ \forall j \in L$$

$\forall c \in C \Rightarrow c(x)$ con ordine massimo
 $f(x)$ di C ha ordine $N - k \Rightarrow N - k$ radici $\beta^{j \cdot k}$ con $j \in L$
 \Rightarrow le $N - k$ radici fanno $\beta^{j \cdot k} + \dots + \beta^{(N-1)k}$

quindi per il secondo corollario della terza proprietà delle trasformate tutte le sequenze che si ottengono ruotando la sequenza $c(x)$ sono lecite, per questo motivo questi codici sono detti ciclici.

Linearità del codice I codici ciclici sono sempre codici lineari infatti:

- $c(x) = 0$ dato che la sua trasformata è la sequenza nulla che è nulla negli indici stabiliti.
- Siano $a(x)$ e $b(x)$ due sequenze lecite del codice, allora anche $c(x) = a(x) + b(x) \in C$ dato che

$$C_j = A_j + B_j$$

quindi se A_j e B_j sono nulli lo è anche C_j e di conseguenza la trasformata di $c(x)$ è nulla negli indici contenuti in L .

Quindi la distanza di Hamming del codice corrisponde al minimo peso di Hamming possibile.

8. Codifica per la trasmissione su un canale BSC

BCH bound Se in L ci sono k indici consecutivi allora tutte le sequenze lecite hanno trasformata con k elementi consecutivi nulli e quindi, per il corollario della quarta proprietà delle trasformate, nel codice ci sono almeno $k+1$ elementi non nulli e quindi la distanza di Hamming del codice è almeno $d = k+1$.

Per questa proprietà è possibile creare codici con una distanza di Hamming a piacere infatti se si vuole avere una distanza di Hamming di almeno d basta mettere $d-1$ elementi nulli consecutivi nella trasformata.

8.6.2. Codici BCH^V primitivi

Definizione Dati:

- q una potenza di un numero primo;
- m un numero naturale;

si definisce il codice BCH come il codice con sequenze lunghe $N = q^m - 1$ tali che:

- hanno elementi in $GF(q)$;
- è ciclico considerando le trasformate dei codici in $GF(q^m)$ utilizzando un elemento α primitivo di $GF(q^m)$, ossia uno di ordine $q^m - 1$.

Osservazione Dato che gli elementi di una sequenza di codice sono in $GF(q)$ si ha che questi sono anche elementi di $GF(q^m)$ dato che $GF(q)$ è un sottocampo di $GF(q^m)$.

Codici BCH con distanza di Hamming d Per avere un codice BCH con distanza di Hamming d bisogna che valga:

$$L \subseteq \{j_0, j_0 + 1, \dots, j_0 + d - 2\} \quad \begin{array}{l} \text{d - 1 elementi nulli nella sequenza della trasformata} \\ \text{d - 1 indici} \\ \text{bit di parità N - K = d - 1} \end{array}$$

però, per la quinta proprietà delle trasformate, se questi elementi sono nulli lo sono anche quelli con indici del tipo:

$$(\alpha^{j_0})^k \mid j_0 \cdot q^k \quad (j_0 + 1) \cdot q^k \quad \dots \quad (j_0 + d - 2) \cdot q^k$$

con k qualsiasi. Per questo motivo oltre ai bit di parità necessari per avere la distanza di Hamming voluta se ne aggiungono altri non voluti, ma necessari per le proprietà della trasformata.

Questo garantisce che la distanza di Hamming del codice sia maggiore di d , per esempio se per caso anche $j_0 + d - 1$ è nullo la distanza di Hamming è almeno $d + 1$.

Polinomio generatore di un codice BCH con distanza di Hamming d Dato che i codici BCH sono codici ciclici si ha che:

$$g(x) = \prod_{j \in L} (x - \alpha^j)$$

devo includere
gli indici delle radici per cui le $d-1$ trasformate sono nulle
è dato un indice per le proprietà del campo devo includere anche
tutti i polinomi minimi di tutte le radici

Dato che in L sono presenti gli elementi $j_0, j_0 \cdot q, j_0 \cdot q^2, \dots$ si ha che nel polinomio generatore sono presenti tutte le radici del polinomio minimo di j_0 e analogamente anche quelle di $j_0 + 1, \dots, j_0 + d - 2$ e si può ottenere dalla produttoria di tutti fattori dei vari polinomi minimi (escludendo i fattori doppi) e questo equivale a fare il minimo comune multiplo:

$$g(x) = \text{mcm} [m_{j_0}(x), m_{j_0+1}(x), \dots, m_{j_0+d-2}(x)]$$

$$\alpha^{j_0} \Rightarrow T(x) = \prod_{i=0}^{d-2} (x - \alpha^{j_0+i})$$

- alcuni polinomi possono condividere radici, perché le radici nel campo sono cicliche (finite)
- per evitare duplicati, calcoliamo il minimo comune multiplo (mcm) dei polinomi minimi
- permette di includere tutte le radici necessarie senza ripetizioni
- mcm: scomposizione fattori primi, sono inclusi i fattori comuni con un esponente più grande e tutti quelli non comuni

I coefficienti del polinomio generatore sono in $GF(q)$, come ci si aspettava.

Solitamente si pone $j_0 = 1$ perché la generalizzazione non porta reali vantaggi e quindi si ha che:

Varia da esercizio a esercizio

$$g(x) = \text{mcm} [m_1(x), m_2(x), \dots, m_{d-1}(x)]$$

- data distanza di Hamming d avrà $d-1$ radici consecutive
- per ogni radice abbiamo un polinomio minimo
- escludendo fattori doppi prendo mcm dei vari polinomi minimi

VI codici BCH prendono il nome dai 3 matematici che per primi li hanno proposti, ossia il francese Hocquenghem e i tedeschi Bose e Chaudhuri.

8. Codifica per la trasmissione su un canale BSC

Osservazioni

- Il polinomio $m_1(x)$ è:

$$m_1(x) = (x - \alpha) \cdot (x - \alpha^q) \cdot (x - \alpha^{q^2}) \cdots$$

trasformate consecutive nelle radici consecutive
 $d-1=2$

quindi se $q = 2$ si ha che usando $m_1(x)$ come polinomio generatore si ottiene una distanza di Hamming pari a 3 dato che $m_2(x) = m_1(x)$ e quindi si ottiene un codice di Hamming. Per questo motivo i codici di Hamming sono codici ciclici ed il loro polinomio generatore è sempre uguale al polinomio minimo di α .

- Soltanente il polinomio generatore dei codici binari è espresso in forma ottale, ossia si divide in gruppi da 3 la sequenza data $(g_{N-K}, g_{N-K-2}, \dots, g_0)$, e si convertono i gruppi in ottale; per esempio dato il polinomio generatore $g(x) = x^5 + x^4 + x + 1$ si ottiene:

$$\begin{array}{c|cc|cc|cc} & x^0 & x^1 & x^2 & x^3 & x^4 & x^5 \\ \hline 110 & 011 & & & & & \\ \hline 6 & 3 & & & & & \\ & 1 & 1 & 0 & 0 & 1 & 1 \end{array}$$

Esempio di codice BCH binario Si consideri il codice BCH con $q = 2$ e $m = 4$, per definizione si ha che:

- $N = 2^4 - 1 = 15$. è primo, tutti gli elementi del campo sono elementi primitivi $\Rightarrow \alpha$

$$\alpha^m \Rightarrow \text{tuple di } m-1 = 3 \\ (g_0, g_1, g_2, g_3) = g_0 + \alpha g_1 + \alpha^2 g_2 + \alpha^3 g_3$$

- I codici hanno elementi in $GF(2)$, ossia è un codice BCH binario.

Per poter ricavare i vari polinomi è utile esplicare la notazione esponenziale in $GF(2^4)$; dato il polinomio generatore del campo $p(\alpha) = \alpha^4 + \alpha + 1$ si ottiene:

n	0	1	2	3	4	5	6	7	8	9
$\alpha^n \bmod p(\alpha)$	1	α	α^2	α^3	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^3 + \alpha^2$	$\alpha^3 + \alpha + 1$	$\alpha^2 + 1$	$\alpha^3 + \alpha$

n	10	11	12	13	14	15
$\alpha^n \bmod p(\alpha)$	$\alpha^2 + \alpha + 1$	$\alpha^3 + \alpha^2 + \alpha$	$\alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^3 + \alpha^2 + 1$	$\alpha^3 + 1$	α^2

Per poter ricavare il polinomio generatore del codice bisogna ricavare i polinomi minimi:

$$m_1(x) = m_2(x) = m_4(x) = m_8(x) = (x - \alpha) \cdot (x - \alpha^2) \cdot (x - \alpha^4) \cdot (x - \alpha^8) = x^4 + x + 1$$

un binomio avrebbe dovuto:
 $(x - \alpha^i) = (x - \alpha^{16})$
16 mod $q-1 = 1$
• Stesso $(x - \alpha)$ è già presente.
• dunque $n=4 \Rightarrow$ min. termo è $n=3$

$$m_3(x) = m_6(x) = m_9(x) = m_{12}(x) = (x - \alpha^3) \cdot (x - \alpha^6) \cdot (x - \alpha^{12}) \cdot (x - \alpha^9) = x^4 + x^3 + x^2 + x + 1$$

- espandere i polinomi moltiplicandoli tra di loro
- e semplificarli utilizzando la tabella definita sopra
- coefficiente polinomi va ridotto mod(2)

$$m_5(x) = m_{10}(x) = (x - \alpha^5) \cdot (x - \alpha^{10}) = x^2 + x + 1$$

$$= x^2 + x + 1$$

$$= x^2 - (\alpha^5 + \alpha^{10})x - (\alpha^5 \cdot \alpha^{10})x + 1$$

$$= x^2 - \alpha^{15}x - 2\alpha^{15}x + 1 \rightarrow (-2) \bmod 2 = 0$$

$$= x^2 + x + 1 \quad (\text{neg o positivo stesso cosa})$$

$$m_7(x) = m_{14}(x) = m_{13}(x) = m_{11}(x) = (x - \alpha^7) \cdot (x - \alpha^{14}) \cdot (x - \alpha^{13}) \cdot (x - \alpha^{11}) = x^4 + x^3 + 1$$

Quindi per garantire una distanza di Hamming di 3 bisogna usare come polinomio generatore il minimo comune multiplo dei primi $d-1=2$ polinomi minimi e quindi:

$$g(x) = \text{mcm}[m_1(x), m_2(x)] = m_1(x) = x^4 + x + 1 \quad : \quad \begin{aligned} & d=3 \\ & \text{devo includere } d-1 \text{ polinomi minimi} \end{aligned}$$

ottenendo un codice di Hamming con $N = 15$, $N - K = 4$ e $K = 11$.

- distanza di Hamming $d = 3$
- ho $d-1$ radici consecutive $\Rightarrow 2$
- i bit di parità con corrisponde come prima al numero di radici del polinomio a causa della proprietà dei campi il grado è più alto

8. Codifica per la trasmissione su un canale BSC

Si può notare che se si vuole aumentare la distanza bisogna aggiungere i fattori di $m_3(x)$ e questo permette di avere 4 indici consecutivi e quindi $d = 5$:

- mcm: prendo fattori comune con indice più grande e tutti quelli non comuni grado $m_1(x) > m_8(x)$

$$\begin{aligned} g(x) &= \text{mcm}[m_1(x), m_2(x), m_3(x)] = \\ &= (x^4 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) = \\ &= x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

• se voglio avere una distanza di Hamming d devo avere
 • se voglio avere $d = 5 \Rightarrow 4$ radici consecutive

$$\begin{aligned} m_1(x) = m_2(x) = m_4(x) = m_8(x) &= (x - \alpha) \cdot (x - \alpha^2) \cdot (x - \alpha^4) \cdot (x - \alpha^8) \\ &= x^4 + x + 1 \end{aligned}$$

$$\begin{aligned} m_3(x) = m_6(x) = m_9(x) = m_{12}(x) &= (x - \alpha^3) \cdot (x - \alpha^6) \cdot (x - \alpha^{12}) \cdot (x - \alpha^9) \\ &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

che è un codice con $N = 15$, $N - K = 8$ e $K = 7$.

Allo stesso modo si può aumentare ulteriormente la distanza di Hamming aggiungendo anche i fattori di $m_5(x)$:

$$\begin{aligned} g(x) &= \text{mcm}[m_1(x), m_3(x), m_5(x)] = \\ &= (x^4 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) \cdot (x^2 + x + 1) = \\ &= (x^8 + x^7 + x^6 + x^4 + 1) \cdot (x^2 + x + 1) = \\ &= x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1 \end{aligned}$$

Le radici consecutive sarebbero:

$\alpha^1, \alpha^4, \alpha^3, \alpha^7, \alpha^9, \alpha^6$

Includendo $m_1(x), m_2(x), m_3(x), m_5(x), m_6(x)$

ottenendo un codice con $d = 7$, $N = 15$, $N - K = 10$ e $K = 5$.

Aggiungendo anche i fattori di $m_7(x)$ si ottiene un codice con $d = 15$, $N = 15$, $N - K = 14$ e $K = 1$ che è un codice con solo $2^1 = 2$ sequenze lecite, che sono quella nulla e quella di soli 1.

Osservazione Generalmente in un codice BCH binario in $GF(2^m)$ ogni unità di potere correttore t «costa» circa m bit di parità, che è molto vicino all'ottimo; infatti per avere un potere correttore t servono $\log \binom{N}{t}$ bit di parità e quindi supponendo $N \gg t$ si ha:

$$\begin{aligned} \log \binom{N}{t} &= \log \left(\frac{N!}{t! \cdot (N-t)!} \right) = \\ &= \log \left(\frac{N!}{(N-t)!} \right) - \log(t!) = \\ &= \log \left(\prod_{i=N-t+1}^N i \right) - \log \left(\prod_{i=1}^t i \right) = \\ &= \sum_{i=N-t+1}^N \log i - \sum_{i=1}^t \log i \approx \\ &\approx t \cdot \log N = \\ &= t \cdot \log 2^m = \\ &= t \cdot m \end{aligned}$$

OBS: $N - K = m \cdot t$ in $GF(2^m)$

8.6.3. Codici BCH non primitivi

Definizione Dati:

- q una potenza di un numero primo;
- m un numero naturale;
- $\beta \in GF(q^m)$ non primitivo di ordine $N < q^m - 1$; essendo beta un elemento non primitivo del campo esteso, genera solo un sottogruppo ciclico proprio del campo

si definisce il codice BCH come il codice con sequenze lunghe N tali che:

- hanno elementi in $GF(q)$;
- è ciclico considerando le trasformate dei codici in $GF(q^m)$ utilizzando un elemento β di $GF(q^m)$.

8. Codifica per la trasmissione su un canale BSC

Osservazione La differenza tra questi codici e i BCH primitivi è che l'elemento usato per il calcolo della trasformata non è un elemento primitivo di $GF(q^m)$. Questo non comporta grandi differenze nella procedura:

- Il polinomio generatore per garantire una distanza di Hamming pari a d è il medesimo.
- Nel polinomio rimangono i termini non voluti.

Esempio di codice BCH non primitivo: codice di Golay Il codice di Golay è un codice BCH non primitivo con $q = 2$, $m = 11$ e $\beta = \alpha^{89}$ dove α è un elemento primitivo di $GF(2^{11})$.

Si può notare che β ha ordine 23 infatti $\alpha^{23 \cdot 89} = \alpha^{2047} = 1$ e quindi il codice di Golay ha $N = 23$ e il polinomio $g(x)$ ha come radici:

$$\underline{\beta}, \underline{\beta^2}, \underline{\beta^4}, \underline{\beta^8}, \beta^{16}, \beta^9, \beta^{18}, \beta^{13}, \underline{\beta^3}, \beta^6, \beta^{12}$$

che sono 11 radici. Per questo motivo il codice di Golay ha $N = 23$, $N - K = 11$ e quindi $K = 12$. Si può notare che la distanza di Hamming garantita dal BCH bound è 5 dato che sono presenti 4 elementi consecutivi (quelli sottolineati nell'elenco), ma nei codici BCH non primitivi questo limite è molto lasco infatti questo codice ha una distanza di Hamming pari a 7.

8.6.4. Codici Reed-Solomon

Definizione Dati:

- q una potenza di un numero primo;
- m un numero naturale;

Si definisce il codice Reed-Solomon (BRS) come il codice con sequenze tali che:

- Hanno elementi in $GF(q^m)$;
- È ciclico considerando le trasformate dei codici in $GF(q^m)$ utilizzando un elemento β qualsiasi di $GF(q^m)$.

Osservazioni

- La differenza tra i codici BCH e i codici BRS è che per questi ultimi ogni simbolo di codice è in realtà una sequenza di simboli in $GF(q)$, quindi per esempio se $q = 2$ e $m = 8$ ogni simbolo della sequenza è un byte e non un bit.
- Tutti i parametri del codice N , K e d sono riferiti alle sequenze di simboli, quindi per esempio se $q = 2$ e $m = 8$ con N si intende il numero di byte inviati per singolo messaggio.
- La lunghezza N del messaggio dipende dall'elemento β scelto per la trasformata, infatti come per i codici BCH N è esattamente l'ordine dell'elemento β . Per questo motivo l' N massimo si raggiunge usando un β primitivo per cui vale $N = q^m - 1$.

Polinomio generatore Per garantire una distanza d bisogna che la trasformata sia nulla in $d - 1$ indici consecutivi, come per tutti i codici ciclici, ma la grossa differenza rispetto ai codici BCH è che non vale più la proprietà dei campi di Galois per cui si devono aggiungere al polinomio generatore i termini non voluti del tipo $\beta^{k \cdot q^m}$ e quindi si può raggiungere il minimo grado del polinomio generatore a pari distanza di Hamming, ossia il minimo numero di simboli di parità, infatti:

$$d - 1 = N - K \longrightarrow d - N + K + 1 \quad \text{minima distanza possibile}$$

Bisogna, però, tener presente che ogni simbolo di parità è una sequenza di simboli in $GF(q)$; nell'esempio $q = 2$ e $m = 8$ ogni simbolo di parità è un byte.

Per questo motivo questi codici sono usati quando gli errori tendono ad accumularsi in una piccola regione del messaggio ricevuto (errori a burst) perché i codici BRS correggono byte per byte e non bit per bit (nel caso $q = 2$ e $m = 8$); se gli errori sono distribuiti uniformemente non conviene usare un codice BRS rispetto a un normale BCH perché, a pari distanza di Hamming (sui simboli in $GF(q)$), il numero di simboli in $GF(q)$ è generalmente maggiore.

8.7. Decodifica algebrica di codici ciclici

8.7.1. Introduzione

Nelle sezioni precedenti si è visto come ricavare il polinomio generatore di un codice circolare con distanza di Hamming a piacimento; in questa sezione invece si vuole trovare un metodo per poter decodificare un messaggio, capire se ci sono errori ed eventualmente correggerli.

Metodo generale Si supponga di utilizzare un codice circolare definito in $GF(q)$ in cui la trasformata è calcolata tramite un elemento $\beta \in GF(q)$ e sia L l'insieme degli indici per cui la trasformata è nulla e d la distanza di Hamming del codice. Si supponga di ricevere una sequenza v con v errori, algebricamente si può rappresentare come:

$$\begin{aligned} v_i &= c_i + e_i \\ \forall i < N \end{aligned}$$

dove $\beta^{N-1} = 1$
N lung. sequenza

dove:

- c è la sequenza trasmessa, e quindi quella corretta, con trasformata C .
- e è una sequenza che è diversa da 0 dove sono ci sono degli errori, con trasformata E .

Eseguendo la trasformata di v , usando lo stesso elemento β , si ottiene:

$$V_i = \underline{C}_i + E_i$$

Se questa trasformata ha dei valori non nulli in almeno un indice presente in L si è rilevato un errore in trasmissione e il decodificatore è in grado di capirlo. Inoltre è possibile ricavare il valore della trasformata dell'errore negli indici presenti in L in quanto la trasformata della sequenza trasmessa deve essere nulla e quindi:

$$\begin{aligned} E_i &= V_i \\ \forall i \in L \end{aligned}$$

Posso identificare gli errori solo
per ogni valore, i che fa parte di L

Per la definizione di trasformata si ha che:

$$E_i = \sum_{j=1}^N e_j \cdot \beta^{i-j}$$

ricevo una sequenza con al massimo v errori

La sequenza e è non nulla negli indici $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_v$ dove sono presenti degli errori, mentre in tutti gli altri è nulla, e quindi si può scrivere:

- data una sequenza e ho v errori su N bit
- Sapendo che nella posizione della radice $E_i = V_i$ e dunque posso trovare l'errore delle varie posizioni
- per determinare la TDF scorro tutti i valori e che si sommano tra di loro

$$E_i = \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{i-\varepsilon_n}$$

valore posizione

$$\begin{array}{c} \varepsilon_1 \quad \varepsilon_v \\ \beta \quad \beta \\ \uparrow \quad \uparrow \\ e = [e_0, \dots, 0, \dots, e_{v-1}] \\ \downarrow \quad \downarrow \\ e_{\varepsilon_1} \quad e_{\varepsilon_v} \end{array}$$

- utilizzo semplicemente E_i perché nel punto dove fare V_i perché $C_i = 0$
- in questo modo posso calcolare tutte le posizioni dei miei errori
- dunque utilizzo i vari $E_i = V_i$ per determinare le equazioni da cui determino le posizioni
- per risolvere v incognite \Rightarrow v equazioni indipendenti

$$\begin{aligned} g(x) &= (x-\lambda)(x-\lambda_v) \\ j_1 &= \varepsilon_1 + C_1 = E_1 \\ \text{eq I)} \quad E_1 &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{1-\varepsilon_n} \\ \text{eq II)} \quad E_2 &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{2-\varepsilon_n} \\ \text{eq III)} \quad E_3 &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{3-\varepsilon_n} \end{aligned}$$

Questo è un sistema con L equazioni e ha come incognite:

- I v valori degli errori e_{ε_i} ; per queste incognite il sistema è lineare.
- Le v posizioni degli errori ε_i ; per queste incognite il sistema non è lineare dato che si trovano all'esponente.

Dato che il sistema non è lineare bisogna trovare un **metodo alternativo** in modo da semplificare l'individuazione dell'errore.

Si preferisce allora ridursi ad un problema lineare utilizzando il **polinomio locatore degli errori**

8. Codifica per la trasmissione su un canale BSC

Definizione di sindrome La sindrome è una sequenza $S = (S_0, S_1, \dots, S_{d-2})$ di $d - 1$ elementi tale che:

$$S_k = E_{k+j_0} \quad \forall k < j_0 + d - 2$$

- rappresenta il punto di partenza dal quale in poi sono presenti le radici delle posizioni sbagliate
- gli errori si possono trovare nelle $d - 1$ trasformate consecutive nulle nelle posizioni k
- le sindromi vanno a prendere $d - 1$ trasformate nulle a parte da j_0

ossia la sindrome è la sequenza delle trasformate degli errori note. Come tutte le sequenze le si può associare un polinomio di grado $d - 2$ tale che:

$$S(x) = S_0 + S_1 \cdot x + \dots + S_{d-2} \cdot x^{d-2} = \sum_{k=0}^{d-2} S_k \cdot x^k$$

Osservazioni

- Dato che per questi indici la trasformata dell'errore è uguale a quella della trasformata della sequenza ricevuta si ha che:

$$S_k = E_{k+j_0} = V_{k+j_0} \quad \forall k < j_0 + d - 2$$

- Se la sindrome è nulla allora la sequenza ricevuta è corretta.

8.7.2. Polinomio locatore dell'errore e calcolo delle posizioni degli errori

Definizione Il polinomio locatore dell'errore (ELP - Error Locator Polynomial) è un polinomio Λ che si definisce come:

$$\Lambda(x) = \prod_{n=1}^{\nu} (1 - \beta^{\epsilon_n} \cdot x) = \Lambda_0 + \Lambda_1 \cdot x + \dots + \Lambda_{\nu} \cdot x^{\nu}$$

date le radici, io riesco a capire dove sono posizionate gli errori e se ho la posizione degli errori, riesco a calcolare i coefficienti perché si tratta di un problema lineare \Rightarrow problemi equivalenti

$\epsilon_1, \epsilon_{\nu}$

ossia il polinomio che ha come radici gli elementi di $GF(q)$:

$$\beta^{-\epsilon_1}, \beta^{-\epsilon_2}, \dots, \beta^{-\epsilon_{\nu}} \quad \text{dove solo collocati i vari errori (posizione)}$$

Osservazioni

- Per come è definito il polinomio locatore è sempre monico e quindi $\Lambda_0 = 1$.
indice all'interno di una sequenza lunga $N = [0..N-1] \Rightarrow$ inoltre $i = 0$
- Si noti che $\epsilon_i < N \ \forall i < \nu$ in quanto sono indici di una sequenza lunga N e quindi tutte queste radici sono valori distinti in quanto si sta elevando un elemento di $GF(q)$ per un valore inferiore al proprio ordine. Quindi ricavare le radici del polinomio locatore equivale a trovare le ν posizioni degli eventuali errori.

Antitrasformata del polinomio locatore Antitrasformando il polinomio locatore si ottiene il polinomio $\lambda(x)$ e per le proprietà della trasformata si ha che:

$$\lambda_i = \Lambda(\beta^{-i})$$

e quindi si ha che:

$$\lambda_{\epsilon_i} = 0 \quad \forall i < \nu$$

Nelle posizioni qui c'è l'errore, si annulla

e quindi è un polinomio che è nullo negli indici in cui c'è un errore.

8. Codifica per la trasmissione su un canale BSC

Valutazione del termine $\lambda \cdot e$ Si consideri:

$$\begin{array}{c} \text{jolla} \\ \text{sempre} \\ \text{sempre} \end{array} \quad \frac{\lambda_k \cdot e_k}{\forall k < N} = 0 \quad \begin{array}{c} \text{caso a) c'è errore} \\ \lambda_k \cdot e_k = 0 \\ 0 \ 0 \end{array} \quad \begin{array}{c} \text{caso b) non c'è errore} \\ \lambda_k \cdot e_k = 0 \\ 0 \ 0 \end{array}$$

perché se in posizione k non c'è un errore allora $e_k = 0$ altrimenti $\lambda_k = 0$, per la proprietà vista prima.

Facendo la trasformata a destra e a sinistra si ottiene:

$$\sum_{n=0}^{N-1} \Lambda_n \cdot E_{k-n} = 0 \quad \forall k < N \quad \begin{array}{c} \text{Proprietà} \\ \text{trasformate} \end{array}$$

$$e_i = v_i \cdot z_i \quad \forall i < N$$

$$E_j = \frac{1}{N} \cdot \sum_{k=0}^{N-1} V_k \cdot Z_{j-k}$$

da questa espressione è possibile eseguire alcune semplificazioni:

- Osservando che $\Lambda_n = 0 \forall n > v$ si ottiene:

$$\sum_{n=0}^v \Lambda_n \cdot E_{k-n} = 0 \quad \forall k < N$$

: il polinomio locatore dell'errore ha grado massimo oltre a n è tutto nullo

- Osservando che $\Lambda_0 = 1$ dato che il polinomio è monico si ottiene:

$$\begin{aligned} \sum_{n=0}^v \Lambda_n \cdot E_{k-n} &= 0 \\ \Lambda_0 \cdot E_{k-0} + \sum_{n=1}^v \Lambda_n \cdot E_{k-n} &= 0 \\ \sum_{n=1}^v \Lambda_n \cdot E_{k-n} &= -E_k \\ &\forall k < N \end{aligned}$$

se comprende un indice al di fuori di L , la trasformata di C e di E si sommano

BCH bound:
 - distanza di Hamming d
 - corrisponde ad avere $d-1$ trasformate nulle consecutive

Número di equazioni Il valore E_x è noto solo se $x \in L$ quindi supponendo di avere una distanza di Hamming pari a d il termine è calcolabile se $j_0 \leq x \leq j_0 + d - 2$.

Nell'equazione scritta precedentemente bisogna conoscere E_k e E_{k-n} per $n = 0, 1, \dots, v$ e quindi si ha che:

$$\begin{aligned} j_0 \leq k &\leq j_0 + d - 2 \\ j_0 \leq k-1 &\leq j_0 + d - 2 \\ &\vdots \\ j_0 \leq k-v &\leq j_0 + d - 2 \end{aligned}$$

Dato che $k > k-1 > \dots > k-v$ si può notare che i due casi critici sono:

$$\begin{aligned} k &< j_0 + d - 2 \\ k-v &\geq j_0 \Rightarrow k > j_0 + v \end{aligned}$$

e quindi:

$$\begin{aligned} j_0 + v &\leq k \leq j_0 + d - 2 \\ j_0 + v &\leq k \leq j_0 + d - 1 \end{aligned}$$

per togliere l'inclusione

da cui si deduce che si possono scrivere solo:

$$j_0 + d - 1 - j_0 - v = d - v - 1$$

trovo l'ampiezza/intervallo di k

equazioni.

8. Codifica per la trasmissione su un canale BSC

Key equation e risolvibilità La Key equation è il sistema di equazioni:

$$\sum_{n=1}^v \Lambda_n \cdot E_{k-n} = -E_k$$

$$\forall k \text{ tale che } j_0 + v \leq k \leq j_0 + d - 2$$

che è un sistema lineare le cui incognite sono i coefficienti $\Lambda_1, \Lambda_2, \dots, \Lambda_v$ ed è composto da $d - v - 1$ equazioni. Un sistema lineare è risolvibile se e solo se il numero di equazioni è maggiore o uguale a quello di incognite e quindi se:

$$\begin{aligned} v &\leq d - v - 1 \\ 2 \cdot v &\leq d - 1 \\ v &\leq \frac{d - 1}{2} \end{aligned}$$

e quindi se il numero di errori è inferiore a $\frac{d-1}{2}$, ma in un canale BSC questo equivale al potere correttore di un codice a distanza di Hamming d e quindi questo sistema permette di ricavare la posizione del massimo numero di errori risolvibili dal codice.

Key equation usando la sindrome Dato che le trasformate dell'errore usate nella Key equation sono quelle note si può utilizzare la sindrome:

$$\sum_{n=1}^v \Lambda_n \cdot S_{k-n} = -S_k$$

$$\forall k \text{ tale che } v \leq k \leq d - 2$$

$$S_k = E_{k+j_0} \quad \forall k < j_0 + d - 2$$

Io è incluso nella sindrome

Algoritmo per risolvere la Key equation Per impostare la Key equation bisogna conoscere il numero di errori v effettuati, ma questo non è possibile e quindi si procede come segue:

- Si imposta la Key equation con $v = \frac{d-1}{2}$, che è il valore massimo di errori per cui si può sperare che la Key equation abbia soluzione.
- Se la Key equation ha soluzione allora si sono trovati i vari coefficienti $\Lambda_1, \Lambda_2, \dots, \Lambda_v$, se invece il sistema è indeterminato si diminuisce il numero di errori v e si riprova.

Calcolo delle posizioni degli errori Le soluzioni della Key equation non sono direttamente le posizioni, ma i coefficienti del polinomio locatore Λ ; le posizioni sono le soluzioni dell'equazione:

$$\Lambda(\beta^{-\epsilon}) = 0$$

- Il polinomio si può risolvere per sostituzione
- non c'è bisogno di fattorizzarlo
- essendo che beta a grado N le radici sono finite

ossia gli esponenti ϵ di β che annullano il polinomio; il modo migliore per trovarli è effettuare una ricerca esaustiva (per tentativi) che è possibile perché si sa che $\epsilon < N$. Questo metodo prende il nome di ricerca di Chen.

8.7.3. Polinomio valutatore dell'errore e calcolo del valore degli errori

- Se il codice binario basta complementare i vin per ottenere i cin GF(q) = 2 = {0,1}
- altrimenti devi scegliere il simboli in GF(q)

Introduzione Una volta note le posizioni $\epsilon_1, \epsilon_2, \dots, \epsilon_v$ degli errori se il codice è binario la correzione è immediata, mentre se il codice non è binario sono richiesti calcoli aggiuntivi. Bisogna ottenere la sequenza degli errori $e = (e_1, e_2, \dots, e_v)$ per poter trovare la sequenza corrette:

$$\begin{aligned} c_{\epsilon_i} &= v_{\epsilon_i} - e_{\epsilon_i} \\ \forall i < v \end{aligned}$$

Tramite la Key-equation è possibile ricavare l'intera sindrome S che si può antitrasformare per ottenere la sequenza e voluta, ma questo sistema è molto complicato dal punto di vista computazione. Per poter semplificare la decodifica si utilizza il polinomio rivelatore.

8. Codifica per la trasmissione su un canale BSC

Definizione di polinomio valutatore Il polinomio valutatore $\Omega(x)$ è il polinomio definito come:

$$\Omega(x) = [\Lambda(x) \cdot S(x)] \mod x^{d-1}$$

- $S(x)$ polinomio di grado $d-2$
- $\Lambda(x)$ polinomio di grado v
- $\Rightarrow (d-2)(v)$ grado

Significato del polinomio valutatore Ricordando la definizione del polinomio delle sindromi si può notare che:

questa dimostrazione mi concentra sulla dinamica non sui calcoli

$$\begin{aligned} S(x) &= \sum_{k=0}^{d-2} S_k \cdot x^k = \\ &= \sum_{k=0}^{d-2} E_{k+j_0} \cdot x^k = \\ &= \sum_{k=0}^{d-2} \left[\sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{(k+j_0) \cdot \varepsilon_n} \right] \cdot x^k = \\ &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \left[\sum_{k=0}^{d-2} \beta^{(k+j_0) \cdot \varepsilon_n} \cdot x^k \right] = \\ &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \left[\sum_{k=0}^{d-2} \beta^{k \cdot \varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot x^k \right] = \\ &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot \left[\sum_{k=0}^{d-2} (\beta^{\varepsilon_n} \cdot x)^k \right] \end{aligned}$$

Obs: Si noti che
 $\Omega_k = \sum_{j=0}^v \Lambda_j \cdot S_{k-j} = 0 \quad k = 1, \dots, d-2$
 quindi per costruzione grado($\Omega(x)$) è:
 $j-1 < \text{grado}(\Lambda(x))$

Si può notare che la parte tra le quadre è una serie geometrica finita e quindi vale:

$$\sum_{k=0}^{d-2} (\beta^{\varepsilon_n} \cdot x)^k = \frac{1 - (\beta^{\varepsilon_n} \cdot x)^{d-1}}{1 - \beta^{\varepsilon_n} \cdot x}$$

convergenza della geometria:

$$\sum_{k=0}^{\infty} x^k = \frac{1-x^{n+1}}{1-x}$$

ottenendo:

$$\begin{aligned} S(x) &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot \frac{1 - (\beta^{\varepsilon_n} \cdot x)^{d-1}}{1 - \beta^{\varepsilon_n} \cdot x} = \\ &= \sum_{n=1}^v \frac{e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot (1 - (\beta^{\varepsilon_n} \cdot x)^{d-1})}{1 - \beta^{\varepsilon_n} \cdot x} \end{aligned}$$

Ricordando che il polinomio locatore è definito come:

$$\Lambda(x) = \prod_{k=1}^v (1 - \beta^{\varepsilon_k} \cdot x)$$

si può notare che:

$$\begin{aligned} \Omega(x) &= \Lambda(x) \cdot S(x) = \\ &= \left[\prod_{k=1}^v (1 - \beta^{\varepsilon_k} \cdot x) \right] \cdot \left[\sum_{n=1}^v \frac{e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot (1 - (\beta^{\varepsilon_n} \cdot x)^{d-1})}{1 - \beta^{\varepsilon_n} \cdot x} \right] \\ &\quad \text{blue bracket: } (1 - \beta^{\varepsilon_n} \cdot x) \end{aligned}$$

8. Codifica per la trasmissione su un canale BSC

Dato che gli elementi della produttoria sono i vari denominatori della sommatoria, questi si semplificano e si ottiene:

$$\begin{aligned}
 \Lambda(x) \cdot S(x) &= \sum_{n=1}^v \left[e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot \left(1 - (\beta^{\varepsilon_n} \cdot x)^{d-1}\right) \cdot \left(\prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k} \cdot x) \right) \right] = \\
 &= \sum_{n=1}^v \left[e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot \left(\prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k} \cdot x) \right) - e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot (\beta^{\varepsilon_n} \cdot x)^{d-1} \cdot \left(\prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k} \cdot x) \right) \right] = \\
 &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot \left(\prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k} \cdot x) \right) - \underbrace{\sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot (\beta^{\varepsilon_n} \cdot x)^{d-1} \cdot \left(\prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k} \cdot x) \right)}_{\text{termini di grado } >d-1}
 \end{aligned}$$

Dato che:

$$\Omega(x) = [\Lambda(x) \cdot S(x)] \mod x^{d-1}$$

si ha che $\Omega(x)$ si ottiene togliendo tutti i termini di grado $d-1$ o maggiore e quindi la parte evidenziata dalla graffa, ottenendo:

$$\Omega(x) = \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot \left(\prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k} \cdot x) \right)$$

Calcolando il polinomio valutatore in $\beta^{-\varepsilon_i}$ ossia in β elevato all'opposto della posizione di un errore si ottiene:

$$\begin{aligned}
 \Omega(\beta^{-\varepsilon_i}) &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot \left(\prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k} \cdot \beta^{-\varepsilon_i}) \right) = \\
 &= \sum_{n=1}^v e_{\varepsilon_n} \cdot \beta^{j_0 \cdot \varepsilon_n} \cdot \left(\prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k - \varepsilon_i}) \right)
 \end{aligned}$$

la sommatoria va a 0 sempre tranne nel caso in cui k sia diverso da i

Si può notare che se nella produttoria c'è un valore nullo, si annulla l'intera sommatoria. Questo succede se $k = i$, dato che la produttoria scorre tutti gli indici escluso uno questa si annulla tutte le volte escluso il caso in cui la condizione $k = i$ non si verifica e quindi:

$$\Omega(\beta^{-\varepsilon_i}) = e_{\varepsilon_i} \cdot \beta^{j_0 \cdot \varepsilon_i} \cdot \prod_{\substack{k=1 \\ k \neq i}}^v (1 - \beta^{\varepsilon_k - \varepsilon_i}) \neq 0$$

a me interessa il valore dell'errore nella posizione i

e quindi è un valore proporzionale al valore dell'errore in posizione ε_i .

8. Codifica per la trasmissione su un canale BSC

Osservazione Si può notare che il polinomio valutatore è composto da un prodotto di $v - 1$ fattori (la produttoria) di primo grado e quindi il grado del polinomio valutatore è al più $v - 1$. | tolgo $k = i$

Calcolo del valore dell'errore Si è visto che $\Omega(\beta^{-\varepsilon_i})$ è proporzionale al valore dell'errore e quindi si può ottenere il valore dell'errore facendo:

$$e_{\varepsilon_i} = \frac{\Omega(\beta^{-\varepsilon_i})}{\beta^{j_0 \cdot \varepsilon_i} \cdot \prod_{\substack{k=1 \\ k \neq i}}^v (1 - \beta^{\varepsilon_k - \varepsilon_i})}$$

Bisogna quindi trovare un modo per ricavare il denominatore. Calcolando la derivata del polinomio locatore si ottiene:

$$\begin{aligned} \frac{d}{dx} \Lambda(x) &= \frac{d}{dx} \prod_{n=1}^v (1 - \beta^{\varepsilon_n} \cdot x) = \\ &= \sum_{n=1}^v -\beta^{\varepsilon_n} \cdot \prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k} \cdot x) \end{aligned}$$

e quindi:

$$\begin{aligned} \left. \frac{d}{dx} \Lambda(x) \right|_{x=\beta^{-\varepsilon_i}} &= \sum_{n=1}^v -\beta^{\varepsilon_n} \cdot \prod_{\substack{k=1 \\ k \neq n}}^v (1 - \beta^{\varepsilon_k - \varepsilon_i}) = \quad \text{non ho mai la derivata del polinomio } x \\ &= -\beta^{\varepsilon_i} \cdot \prod_{\substack{k=1 \\ k \neq i}}^v (1 - \beta^{\varepsilon_k - \varepsilon_i}) = \\ &= \Lambda'(\beta^{-\varepsilon_i}) \end{aligned}$$

$\frac{d f(x) \cdot f'(x)}{dx} = f'(x) \cdot f(x) + f(x) \cdot f'(x)$

per ragionamenti analoghi a prima. In questo modo si può notare che:

$$\begin{aligned} e_{\varepsilon_i} &= \frac{\Omega(\beta^{-\varepsilon_i})}{\beta^{j_0 \cdot \varepsilon_i} \cdot \prod_{\substack{k=1 \\ k \neq i}}^v (1 - \beta^{\varepsilon_k - \varepsilon_i})} = \\ &= \frac{\Omega(\beta^{-\varepsilon_i})}{\beta^{\varepsilon_i \cdot (j_0 - 1)} \cdot \beta^{\varepsilon_i} \cdot \prod_{\substack{k=1 \\ k \neq i}}^v (1 - \beta^{\varepsilon_k - \varepsilon_i})} = \quad \text{ricostruisco il valore necessario} \\ &= -\frac{\Omega(\beta^{-\varepsilon_i})}{\beta^{\varepsilon_i \cdot (j_0 - 1)} \cdot \Lambda'(\beta^{-\varepsilon_i})} \quad -\Lambda'(\beta^{-\varepsilon_i}) \end{aligned}$$

Dato che normalmente si ha che $j_0 = 1$ si ottiene:

$$e_{\varepsilon_i} = -\frac{\Omega(\beta^{-\varepsilon_i})}{\Lambda'(\beta^{-\varepsilon_i})} \quad \frac{\text{grado: } v-1}{\text{grado: } v-1} = \text{valente}$$

Calcolo della derivata Il calcolo della derivata del polinomio locatore è molto semplice, infatti:

$$\Lambda(x) = \prod_{n=1}^v (1 - \beta^{\varepsilon_n} \cdot x) = \Lambda_0 + \Lambda_1 \cdot x + \Lambda_2 \cdot x^2 + \Lambda_3 \cdot x^3 + \dots + \Lambda_v \cdot x^v$$

8. Codifica per la trasmissione su un canale BSC

e quindi:

$$\begin{aligned}\Lambda'(x) &= \Lambda_1 + 2 \cdot \Lambda_2 \cdot x + 3 \cdot \Lambda_3 \cdot x^2 + \dots + v \cdot \Lambda_v \cdot x^{v-1} = \\ &= \sum_{i=1}^v i \cdot \Lambda_i \cdot x^{i-1}\end{aligned}$$

8.7.4. Algoritmo di Euclide

Introduzione L'algoritmo di Euclide è un metodo che permette di ricavare il polinomio locatore $\Lambda(x)$ e il polinomio valutatore $\Omega(x)$ in modo iterativo partendo dal valore del polinomio della sindrome $S(x)$. Dalla definizione di polinomio valutatore si ha che:

$$\begin{array}{lcl} \text{incognite} \\ \text{nodo} \end{array} \quad \Omega(x) &= \Lambda(x) \cdot S(x) \mod x^{d-1} = & \xrightarrow{\quad} = \text{v} \\ \text{grado } d-1 &= \Lambda(x) \cdot S(x) + x^{d-1} \cdot \Phi(x) & = x - q x^{d-1} \\ \text{grado } v & \text{grado } d-1 \end{array}$$

dove $\Phi(x)$ è il quoziente della divisione tra $\Lambda(x) \cdot S(x)$ e x^{d-1} . L'algoritmo di Euclide calcola iterativamente i polinomi $\Omega(x)$, $\Lambda(x)$ e $\Phi(x)$ e quindi si definiscono le seguenti successioni:

- $\Omega_k(x)$ è il valore del polinomio $\Omega(x)$ al passo k dell'algoritmo.
- $\Lambda_k(x)$ è il valore del polinomio $\Lambda(x)$ al passo k dell'algoritmo.
- $\Phi_k(x)$ è il valore del polinomio $\Phi(x)$ al passo k dell'algoritmo.

Inoltre a ogni passo k vale:

$$\Omega_k(x) = \Lambda_k(x) \cdot S(x) + x^{d-1} \cdot \Phi_k(x)$$

Stato iniziale L'algoritmo di Euclide richiede l'inizializzazione dei primi due valori della successione:

OSS: l'iterazione si ferma quando:
grado $\Omega(x) >$ grado $\Delta(x)$

$$\begin{cases} \Omega_{-1}(x) = x^{d-1} & \text{grado massimo possibile} \Rightarrow \text{grado decrescente} \\ \Lambda_{-1}(x) = 0 & \text{grado minimo possibile} \Rightarrow \text{grado crescente} \\ \Phi_{-1}(x) = 1 \end{cases}$$

$$\begin{cases} \Omega_0(x) = S(x) \\ \Lambda_0(x) = 1 \\ \Phi_0(x) = 0 \end{cases}$$

che sono due passi che rispettano l'equazione, infatti:

$$\begin{aligned}\Omega_{-1}(x) &= \Lambda_{-1}(x) \cdot S(x) + x^{d-1} \cdot \Phi_{-1}(x) \\ x^{d-1} &= 0 \cdot S(x) + x^{d-1} \cdot 1 \\ x^{d-1} &= x^{d-1}\end{aligned}$$

$$\begin{aligned}\Omega_0(x) &= \Lambda_0(x) \cdot S(x) + x^{d-1} \cdot \Phi_0(x) \\ S(x) &= 1 \cdot S(x) + x^{d-1} \cdot 0 \\ S(x) &= S(x)\end{aligned}$$

Inoltre si ha che:

polinomio	grado
$\Omega_{-1}(x)$	$d-1$
$\Omega_0(x)$	$d-2$
$\Lambda_{-1}(x)$	0
$\Lambda_0(x)$	0

quindi il grado di $\Omega(x)$ è diminuito di 1.

8. Codifica per la trasmissione su un canale BSC

Passo iterativo Dati due passi $k-2$ e $k-1$ per calcolare il valore delle successioni al passo k si deve calcolare il quoziente $q_k(x)$ tra $\Omega_{k-2}(x)$ e $\Omega_{k-1}(x)$, ossia:

$$q_k(x) = \frac{\Omega_{k-2}(x)}{\Omega_{k-1}(x)}$$

e porre:

$$\begin{cases} \Omega_k(x) = \Omega_{k-2}(x) - q_k(x) \cdot \Omega_{k-1}(x) \\ \Lambda_k(x) = \Lambda_{k-2}(x) - q_k(x) \cdot \Lambda_{k-1}(x) \\ \Phi_k(x) = \Phi_{k-2}(x) - q_k(x) \cdot \Phi_{k-1}(x) \end{cases}$$

Dato che il grado di $q_1(x)$ è 1 si ha che $\Omega_1(x)$ ha grado $d-3$, ossia uno in meno di $\Omega_0(x)$, mentre $\Lambda_1(x)$ ha grado 1, ossia uno in più di $\Lambda_0(x)$. Quindi quando si calcola il quoziente $q_2(x)$ si ottiene ancora un polinomio di grado 1 e quindi a ogni passo il grado di $\Omega(x)$ diminuisce di 1 mentre quello di $\Lambda(x)$ aumenta di 1. Per questo motivo si ha che:

polinomio	grado
$\Omega_k(x)$	$d-2-k$
$\Lambda_k(x)$	k

per $k \neq -1$

Potrebbe succedere che l'algoritmo prosegua più velocemente del caso illustrato, infatti se si annulla qualche termine di $\Omega(x)$ nel prodotto potrebbe succedere che il quoziente $q_k(x)$ sia di grado maggiore di 1 e quindi il grado di $\Omega(x)$ decresce più velocemente, e analogamente quello di $\Lambda(x)$ aumenta più velocemente.

Condizione di terminazione L'algoritmo si deve fermare quando i polinomi raggiungono il grado corretto, ossia quando $\Omega_k(x)$ ha grado v e $\Lambda_k(x)$ ha grado $v-1$, e quindi quando:

numero iterazioni è uguale
al numero di errori

$$\begin{cases} d-2-k = v \\ k \leq v-1 \end{cases}$$

$$\begin{cases} d-2-k = v \\ k < v \end{cases}$$

condizione di terminazione:
 $\deg(\Omega(x)) < \deg(\Lambda(x))$

ovvie olte prossima iterazione mi
fermo dunque nell'ultima ho:

$\deg(\Omega(x)) = v$
 $\deg(\Lambda(x)) = v-1$

ossia:

$$\begin{aligned} k &< d-2-k \\ 2 \cdot k &< d-2 \\ 2 \cdot k &\leq d-1 \\ k &\leq \frac{d-1}{2} = t \end{aligned}$$

e quindi per risolvere l'algoritmo ci vogliono al più t passi, dove t è il potere correttore dell'algoritmo.

Osservazione L'algoritmo di Euclide non garantisce che il polinomio locatore trovato sia monico, ma comunque garantisce che le sue radici siano quelle desiderate. Questo comporta una variazione anche del polinomio valutatore dato che si ricava facendo $\Omega(x) = S(x) \cdot \Lambda(x)$.

9. Codifica per la trasmissione su un canale BEC

9.1. Considerazioni generali

Ripasso canale BEC (ε) Il canale BEC (ε) è un canale con X binario e Y ternario a cui si aggiunge, rispetto a X , un elemento che indica che il simbolo ricevuto è sbagliato chiamato E e si ha che:

$$P_{Y|X}(y|x) = \begin{cases} 1 - \varepsilon & y = x \\ \varepsilon & y = E \end{cases}$$

la cui capacità è:

$$C = 1 - \varepsilon$$

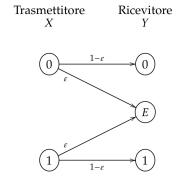


Figura 4.3.: Rappresentazione del modello BEC.

che è molto maggiore di quella di un canale BSC (ε), come mostrato in figura 9.1, e quindi è utile ricavare codici diversi per questo tipo di canale.

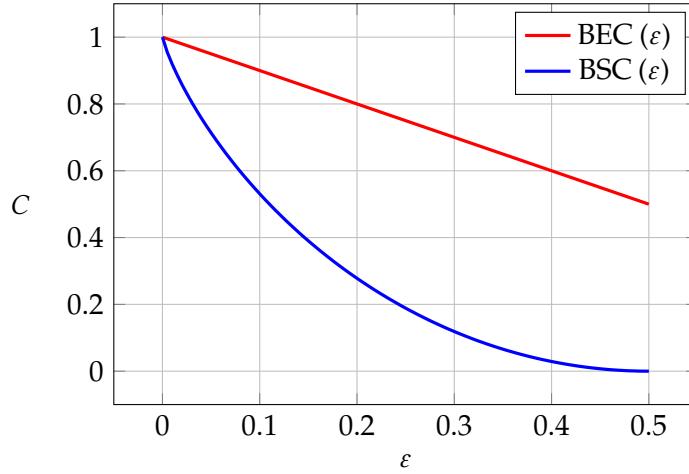


Figura 9.1.: Capacità dei canali BSC e BEC al variare di ε tra 0 e 0.5.

Probabilità condizionata di una sequenza Ipotizzando che il canale non abbia memoria si ha che:

$$P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) = \prod_{n=1}^N P_{Y|X}(y_n|x_n)$$

numero di cancellazioni in y

quindi ipotizzando di aver ricevuto N_e simboli E si ha che:

$$P_{\underline{Y}|\underline{X}}(\underline{y}|\underline{x}) = \begin{cases} \varepsilon^{N_e} \cdot (1 - \varepsilon)^{\underline{N} - N_e} & \text{se } \underline{y} \text{ è compatibile con } \underline{x} \\ 0 & \text{altrimenti} \end{cases}$$

• sequenza incompatibile
se differisce in una sola posizione
dove x e y è diversa da E

Ciò è dovuto al fatto che se si riceve un simbolo diverso da E questo è sicuramente giusto e quindi è impossibile che la sequenza trasmessa abbia quel simbolo diverso. Per questo motivo esistono sequenze incompatibili con altre per esempio se si invia $(0, 1, 1, 0)$ non si può ricevere $(1, E, 1, E)$ perché il primo simbolo è incompatibile.

Inoltre si può notare che la probabilità di ricevere una qualsiasi sequenza compatibile non dipende dalla sequenza ricevuta, ma solo dal numero di simboli cancellati ricevuti; questo è dovuto al fatto che se si riceve un simbolo cancellato la probabilità che questo fosse uno 0 o un 1 è uguale.

9. Codifica per la trasmissione su un canale BEC

Decodificatore ML di un canale BEC Data la $P_{Y|X}(\underline{y}|\underline{x})$ si può notare che le sequenze ricevute si dividono in due categorie:

- Quelle impossibili, ossia incompatibili.
- Quelle possibili, ossia tutte le altre.

La decodifica ML consiste nell'individuazione della sequenza compatibile quando è unica, oppure bisogna dichiarare fallimento o scegliere a caso

Inoltre tutte quelle possibili hanno uguale verosimiglianza dato che la probabilità $P_{Y|X}(\underline{y}|\underline{x})$ dipende solamente dal numero di elementi cancellati ricevuti e non al messaggio stesso. Per questi motivi il decodificatore a massima verosimiglianza si limita a scegliere una sequenza compatibile casualmente.

Quindi un decodificatore a massima verosimiglianza può sbagliare tutte le volte che ci sono più sequenze compatibili lecite nel codice.

Codici lineari Utilizzando un codice lineare con matrice di parità $\underline{\underline{H}}$ si ha che una sequenza \underline{x} è di codice se:

$$\underline{\underline{H}}_{(N-K) \times N}^T \cdot \underline{x}_{N \times 1}^T = \underline{0}$$

Il vettore \underline{x} si può dividere in due parti: una con i simboli noti \underline{x}_{NE} e una con i simboli non noti \underline{x}_E , analogamente si può dividere la matrice di parità in due matrici, di cui una avrà N_e colonne corrispondenti alle colonne dei simboli cancellati ricevuti, ottenendo:

$$\begin{bmatrix} \underline{\underline{H}}_{(N-K) \times (N-N_e)}^T & \underline{\underline{H}}_{(N-K) \times N_e}^T \end{bmatrix} \cdot \begin{bmatrix} \underline{x}_{NE}^T \\ \underline{x}_E^T \end{bmatrix}_{(N-N_e) \times 1} = \underline{0}$$

$$\underline{\underline{H}}_{(N-K) \times N_e}^T \cdot \underline{x}_{NE} + \underline{\underline{H}}_{N_e \times 1}^T \cdot \underline{x}_E = \underline{0}$$

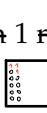
Dato che il termine $\underline{\underline{H}}_{(N-K) \times N_e}^T \cdot \underline{x}_{NE}$ è calcolabile in quanto si conoscono i bit della sequenza lo si può chiamare s , ottenendo:

$$\begin{aligned} s + \underline{\underline{H}}_{N_e \times 1}^T \cdot \underline{x}_E &= \underline{0} \\ \underline{\underline{H}}_{N_e \times 1}^T \cdot \underline{x}_E &= s \end{aligned}$$

Quindi il decodificatore a massima verosimiglianza deve risolvere un sistema con $N - K$ equazioni e N_e incognite.

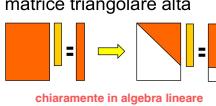
Risoluzione del sistema di decodifica Esistono diversi modi per risolvere un sistema di questo genere, ma il più rapido consiste nel:

1. eliminazione gaussiana seguita da sostituzione all'indietro (back substitution)

- Effettuare delle operazioni lineari tra righe per avere un 1 nella posizione (0, 0) della matrice e avere solo 0 nel resto della prima colonna. 
- Effettuare delle operazioni lineari tra righe per avere un un 1 nella posizione (1, 1) della matrice e avere solo 0 dalla terza posizione in poi nella seconda colonna. 
- Ripetere questa procedura per N_e volte in modo da avere una matrice triangolare alta, dove tutti gli 1 sono al di sopra della diagonale principale.

In questo modo è possibile ricavare l'ultima incognita, dato che nell'ultima riga compare solo un 1 e quindi si ha un'equazione di facile soluzione, e poi sostituendo all'indietro si ricavano anche le altre incognite (questo procedimento è noto come back substitution).

1) • L'eliminazione gaussiana trasforma H_e in una matrice triangolare alta complessità $O(N^3)$ con matrice H_e piena.



2) • Si possono poi ricavare le incognite una ad una (o più) partendo dalle equazioni con una sola incognita (ce n'è per forza almeno una) e sostituendo i valori trovati via via riducendo il numero delle incognite nelle equazioni precedenti

complessità $O(N^2)$ con matrice H_e piena.



9. Codifica per la trasmissione su un canale BEC

Complessità della decodifica Ipotizzando di avere una matrice piena, ossia:

- In media le righe sono composte da 0 e 1 in egual numero.
- In media le colonne sono composte da 0 e 1 in egual numero.

Per poter rendere la matrice triangolare per ogni variabile bisogna eseguire una operazione tra righe per ogni riga con un 1 nella colonna in esame e dato che ogni operazione di riga necessita di una commutazione per ogni uno nella riga si ha che:

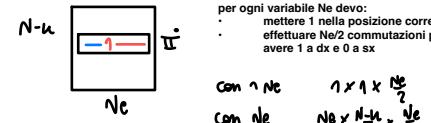
$$\underbrace{N_e}_{\text{numero di variabili}} \cdot \underbrace{\frac{N-K}{2}}_{\substack{\text{numero di zeri in una colonna} \\ \text{ossia il numero di operazioni di riga da fare}}} \cdot \underbrace{\frac{N_e}{2}}_{\substack{\text{numero di zeri in una riga} \\ \text{ossia il numero di commutazioni da fare}}} = O(N^3)$$

portare da 1 a 0 la
colonna i-esima

una commutazione, una matrice, lo scambio di righe o colonne per
riorganizzare la matrice, semplificare la risoluzione del sistema lineare

dato che di media si ha che $N_e = \varepsilon \cdot N$ si ottiene:

$$O\left(N_e \cdot \frac{N_e}{2} \cdot \frac{N-K}{2}\right) = O(N^3)$$



Una volta ottenuta una matrice triangolare bisogna eseguire la back substitution, per ogni variabile calcolata bisogna sostituirla in tutte le altre equazioni in cui compare e quindi:

$$\underbrace{N_e}_{\text{numero variabili}} \cdot \underbrace{\frac{N_e}{2}}_{\substack{\text{numero di zeri in una riga} \\ \text{ossia il numero di equazioni in cui compare la variabile}}} = O(N^2)$$



dato che di media si ha che $N_e = \varepsilon \cdot N$ si ottiene:

$$O\left(N_e \cdot \frac{N_e}{2}\right) = O(N^2)$$

e quindi in totale si ha una complessità computazionale di:

$$O(N^3 + N^2) = O(N^3)$$

che è abbastanza alta.

Utilizzo di matrici sparse Per abbassare questa complessità computazionale si possono usare matrici sparse, ossia matrici tali che:

- In media in ogni riga ci siano pochi uni e di un numero indipendente da N .
- In media in ogni colonna ci siano pochi uni e di un numero indipendente da N .

Rinunciamo alla eliminazione gaussiana
decodificando solo quando riusciamo a farlo
tramite sola back Substitution

In questo modo c'è la possibilità che la matrice diventi triangolare senza fare nessuna operazione di riga, ma solo (o quasi solo) delle sostituzioni, riducendo il costo computazionale a $O(N)$; inoltre in questa situazione si può sperare che nella back substitution tutte le equazioni abbiano solo un'incognita e quindi non ci sia bisogno di effettuare delle sostituzioni, riducendo il costo a $O(N)$.

Ovviamente questo è un costo medio e si basa sull'ipotesi di avere matrici con poca probabilità di avere degli 1; inoltre, un algoritmo che dà per scontato di poter far le due operazioni in questo modo potrebbe fallire in casi in cui questo non avviene e in cui il decodificatore a massima verosimiglianza, con l'algoritmo esposto prima, non fallirebbe.

Quindi l'utilizzo di matrici sparse permette di abbassare notevolmente la complessità computazionale sacrificando la decodifica a massima verosimiglianza.

9.2. Codici LDPC

9.2.1. Introduzione

Introduzione I codici LDPC (Low Density Parity Check) sono dei codici che sfruttano delle matrici di parità sparse per diminuire il costo computazionale della decodifica, come illustrato prima.

I codici LDPC sono stati proposti negli anni 60 da Gallagher, ma sono stati usati solo a partire dagli anni 90; ora sono usati in molti standard, come il wi-fi 802.11N.

Definizione Un codice LDPC è un codice con matrice di parità in cui:

- In ogni riga ci sono j uni, con $j \ll N$.
- In ogni colonna ci sono k uni, con $k \ll N - K$.

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

$\underline{H} \in \mathbb{R}^{(N-K) \times N}$

se j e k sono costanti per ogni riga
e colonna il codice si dice regolare

$$\underline{H}^T \cdot \underline{x}^T = 0$$

$(N-K) \times N \quad N \times 1$

Si presta attenzione al fatto che k minuscolo è il numero di uni per colonna mentre K maiuscolo è la quantità di informazione per messaggio, il solito parametro.

Rate di un codice LDPC Il numero di uni U nella matrice di parità può essere calcolata in due modi diversi:

$$U = j \cdot N = k \cdot (N - K) \rightarrow \cancel{N = N - u} \quad \text{"colonne"} \\ = \frac{j \cdot N}{k}$$

e quindi si ha:

$$\frac{j}{k} = \frac{N - K}{N} = 1 - \frac{K}{N} = 1 - R \quad \cancel{j \cdot N = u \cdot (N - u)}$$

e quindi:

$$R = 1 - \frac{j}{k}$$

Esempio Si consideri un codice LDPC con $j = 2$, $k = 3$ e $N = 6$ con matrice di parità:

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

Si supponga di ricevere la sequenza $y = (0, E, E, E, 0, 0)$: per decodificarla bisogna per prima cosa ricavare il vettore \underline{s} :

$$\begin{aligned} \underline{s} &= \underline{\underline{H}}_{NE}^T \cdot \underline{y}_{NE}^T = \\ &= \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \end{aligned}$$

e quindi il sistema è:

$$\begin{aligned} \underline{\underline{H}}_E^T \cdot \underline{y}_E^T &= \underline{s} \\ \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} &= \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \end{aligned}$$

9. Codifica per la trasmissione su un canale BEC

quindi in forma non matriciale:

$$\begin{cases} y_4 = 0 \\ y_2 = 0 \\ y_2 + y_3 = 0 \\ y_3 + y_4 = 0 \end{cases}$$

Si può notare che il sistema è facilmente risolvibile perché ci sono due equazioni immediatamente risolvibili e poi rimane solo un'incognita da calcolare, ma il problema è trovare un procedimento algoritmico che sfrutti questa caratteristica.

9.2.2. Grafo di Tanner

ad ogni codice con matrice di parità H
si può associare il grafo di Tanner

prendo come riferimento la H trasposta, dove j e k
rappresentano gli 1 su riga e colonna

Introduzione Il grafo di Tanner è un supporto grafico per l'algoritmo che si può usare per risolvere in modo efficiente il sistema per la decodifica. È un grafo bipartito con due tipi di nodi:

- **Check node (CN)** nodi di parità

Ogni check node rappresenta un'equazione di parità e quindi ce ne sono $N - K$. Si indicano con un quadrato \square .

- **Variable node (VN)** nodi variabili

Ogni variable node rappresenta una variabile del sistema e quindi ce ne sono N . Si indicano con un pallino \circ .

Ogni check node è collegato a tutte le variabili che compaiono in quell'equazione e quindi a k variable node, mentre ogni variable node è collegato a j check node.

Funzionamento L'algoritmo è composto da due fasi alterne: una di attivazione dei variable node e una di attivazione dei check node. Per il corretto funzionamento si parte con l'attivazione dei variable node e si procede in questo modo:

• decodifica iterativa dei codici LDPC

- Ogni variable node che conosce il proprio valore lo comunica a tutti i check node a cui è collegato e si disattiva.
- Ogni check node che conosce tutti i valori dei variable node a cui è collegato escluso uno, ricava opportunamente l'unico valore che non conosce e lo comunica al variable node.

I variable node sono inizializzati con i valori delle variabili conosciute e si procede alternando le due fasi finché tutti i nodi sono disattivati.

Problemi dell'algoritmo Questo algoritmo non è in grado di risolvere tutti i sistemi perché se nella fase di attivazione dei check node nessuno è in grado di attivarsi perché tutti hanno almeno due variabili ancora sconosciute, l'algoritmo si blocca e non è in grado di risolvere il sistema.

Per questo motivo usando questo sistema si riesce a risolvere solo una parte dei sistemi che sarebbero risolvibili usando un normale decodificatore a massima verosimiglianza, ma questo algoritmo è molto più efficiente e quindi è utile valutare:

- Quanto potere correttore si perde utilizzando questo algoritmo rispetto alla decodifica a massima verosimiglianza.
- Come si può minimizzare tale differenza lavorando sui parametri del codice j e k .

9. Codifica per la trasmissione su un canale BEC

questo vale sempre:
 - le righe sono rappresentate da i
 - le colonne da k
 adesso prendo come riferimento H^T : dunque i rappresenta sempre la riga e k la colonna

Esempio Riprendendo l'esempio precedente, si può provare ad applicare l'algoritmo appena esposto; il sistema da risolvere è:

$$\text{ch} \rightarrow j \quad \begin{matrix} \text{n varie node} \\ \text{check node} \end{matrix} \quad \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \Rightarrow \underline{H^T} \cdot \underline{y^T} = \underline{0}$$

e quindi ci sono 6 variable node e 4 check node come mostrato in figura 9.2.

Ricevuta la sequenza $y = (0, E, E, E, 0, 0)$ si può inizializzare l'algoritmo mettendo a 0 i 3 variable node corrispondenti.

$\text{N} - \text{Nb} + \text{E}$

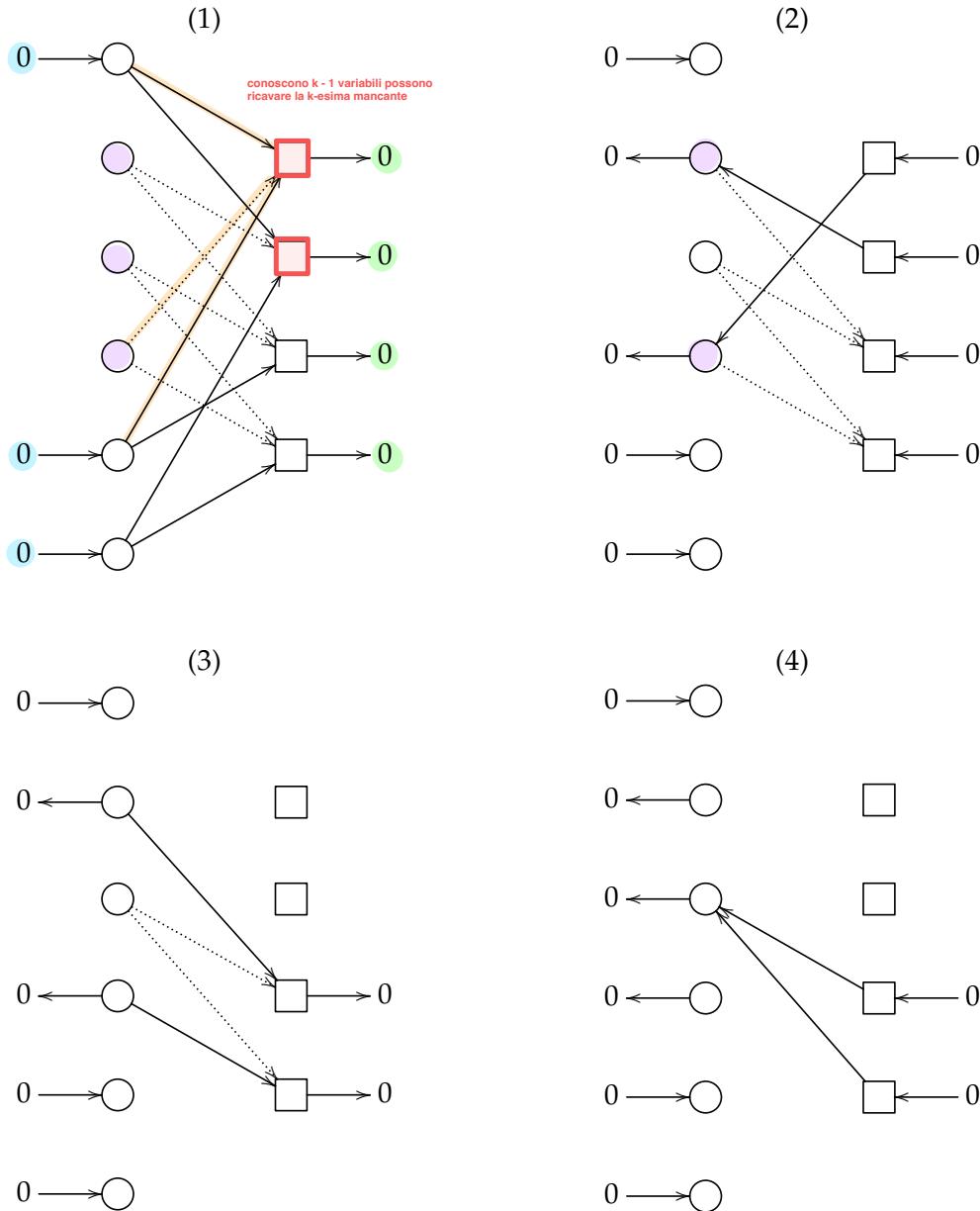
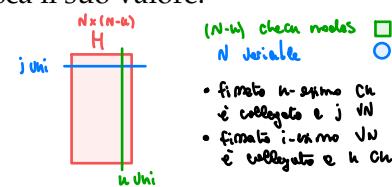


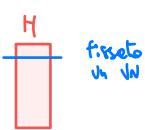
Figura 9.2.: Passaggi dell'algoritmo di decodifica tramite grafo di Tanner.

9.2.3. Risolvibilità del decodificatore tramite grafo di Tanner

convergenza

Per analizzare la risolvibilità bisogna calcolare la probabilità che l'algoritmo ha di risolvere il sistema e quindi di non bloccarsi, per farlo si può calcolare la probabilità che un variable node x conosca il suo valore.





9. Codifica per la trasmissione su un canale BEC

dopo un'interazione alla proprietà di recuperare il valore di un VN x qualsiasi la proprietà di riceverlo dal canale da uno dei j CN connessi

$$P_k(x \neq e) = 1 - \varepsilon [1 - (1 - \varepsilon)^{k-1}]$$

La probabilità che x conosca il suo valore all'inizializzazione dipende dal canale e vale:

$$P_0 = 1 - \varepsilon$$

2 fonte) se avvenuta una cancellazione, lo determino tramite grafo

1 fonte) non è avvenuta una cancellazione e dunque conosco il valore della mia variabile x

mentre la probabilità che lo conosca al secondo passo aumenta e dipende dal resto del grafo; per conoscere il valore al secondo passo deve riceverlo direttamente da uno dei j check node a cui è collegato, e ognuno di questi check node può comunicare tale valore se gli altri $k-1$ variable node a cui è collegato conoscono il loro valore. Quindi:

Vuol dire che un CK conosce $k-1$ VN a cui è collegato e questi valori sono stati ottenuti dal canale

solo grafo

- $(1 - \varepsilon)^{k-1}$ è la probabilità che uno dei j check node a cui è collegato conosca il valore del variable node x .
- $1 - (1 - \varepsilon)^{k-1}$ è la probabilità che uno dei j check node non conosca il valore del variable node x .
- $(1 - (1 - \varepsilon)^{k-1})^j$ è la probabilità che nessun dei j check node a cui è collegato conosca il valore del variable node x .
non me lo dice nemmeno il canale
- $\varepsilon \cdot (1 - (1 - \varepsilon)^{k-1})^j$ è la probabilità che il nodo x non conosca ancora il proprio valore al secondo passo e nessuno è in grado di comunicarglielo.
1 - non si sappia o che si sappia al secondo passo, o dal canale o dai check nodes collegati
- $1 - \varepsilon \cdot (1 - (1 - \varepsilon)^{k-1})^j$ è la probabilità che il nodo x conosca il proprio valore al secondo passo.
la probabilità complementare, ovvero che x conosca il suo valore al secondo passo

Né il canale né i check nodes possono determinare il valore del variable node x

secondo passo:
canale + grafo

Proseguendo in questo modo i valori di probabilità si complicano molto perché si formano dei cicli nel grafo e quindi è utile ipotizzare che non si formino cicli ossia che $N \rightarrow \infty$, in questo caso è possibile calcolare tali probabilità ad un passo generico.

sto supponendo di ricevere informazioni dal canale all'infinito

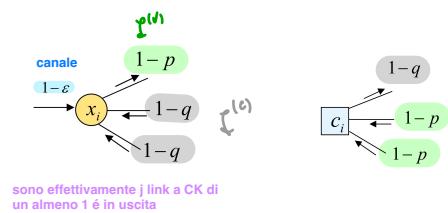
la presenza di cicli mi complica il calcolo
dunque le probabilità che ho trattato mi facilmente perché erano indipendenti tra di loro perché tutti i messaggi arrivati dal canale sono indipendenti già dalla seconda interazione possono non essere indipendenti per N che tende all'infinito il grafo tende a diventare un albero e dunque i cicli tendono ad annullarsi e considero le probabilità indipendenti

Calcolo della probabilità ad un passo generico Se si assume che $N \rightarrow \infty$ allora si può assumere che tutti i nodi abbiano la stessa probabilità di ricevere dell'informazione a tutti i passi, e quindi si definisce:

- p : probabilità che un variable node non sia in grado di comunicare a un check node il valore della variabile.
- q : probabilità che un check node non sia in grado di comunicare a un variable node il valore della sua variabile.
- $I^{(v)} = 1 - p$, ossia la probabilità che un variable node sia in grado di comunicare a un check node il valore della variabile.
- $I^{(c)} = 1 - q$, ossia la probabilità che un check node sia in grado di comunicare a un variable node il valore della variabile.

Un variable node può ricevere il valore della propria variabile da:

- Il canale, con probabilità $1 - \varepsilon$.
- Uno dei $j - 1$ check node a cui è collegato, con probabilità $1 - q$.



Dato che un variable node riesce a comunicare il valore della propria variabile se almeno una delle fonti lo comunica si ha che:

$$p = \varepsilon \cdot q^{j-1}$$

ossia la probabilità che non riesca a comunicare il valore è uguale alla probabilità che tutte le fonti falliscano a comunicare il valore e quindi si ha:

$$I^{(v)} = 1 - \varepsilon \cdot (1 - I^{(c)})^{j-1} \quad \text{probabilità di ricevere informazione al secondo passo}$$

Un check node può comunicare il valore di una variabile se riceve tutte le altre $k-1$ variabili dei variable node a cui è collegato e quindi:

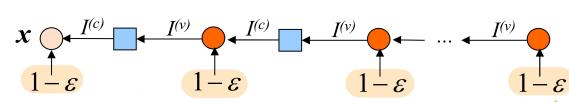
il nodo calcola l'informazione sulla base della conoscenza a priori definita dai $k-1$ connessi al check node

$$I^{(c)} = (I^{(v)}_a)^{k-1}$$

L'informazione a priori di $k-1$ variable nodes

con N che tende all'infinito il grafo tende a un albero: le probabilità sono indipendenti
I(e) informazione a priori rappresenta la conoscenza che un nodo (variable o check) ha all'inizio di una certa interazione prima di ricevere nuovi messaggi dai nodi vicini
I(e): informazione estrinseca è l'informazione che un nodo calcola e propaga all'esterno verso i nodi vicini, basandosi solo sulle informazioni degli altri nodi a cui è collegato escludendo se stesso e quindi dedotta dalla rete

I grafici di questi due andamenti sono mostrati in figura 9.3.



9. Codifica per la trasmissione su un canale BEC

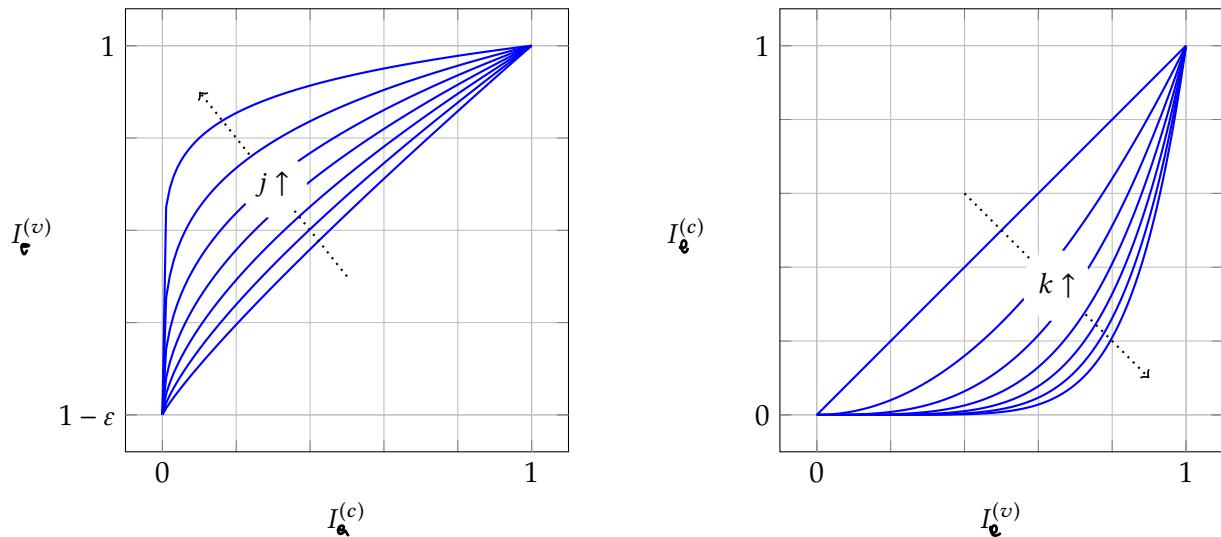


Figura 9.3.: Grafici dei valori $I_e^{(c)}$ e $I_e^{(v)}$ al variare di j e k .

Dati grafici si può notare che:

- Più j è alto più la $I^{(v)}$ aumenta velocemente con l'aumentare di $I^{(c)}$ che è abbastanza intuitivo, infatti più check node sono collegati al variable node più è probabile che questo conosca il proprio valore.
- Più k è alto più $I^{(c)}$ aumenta lentamente con l'aumentare di $I^{(v)}$ che è anch'esso abbastanza intuitivo, infatti più variable node sono collegati al check node più si abbassa la probabilità che tutti conoscano il proprio valore.
- Anche se i check node non hanno nessuna possibilità di comunicare il risultato ($I^{(c)} = 0$) i variable node hanno una probabilità di comunicare un valore pari alla capacità del canale: $I^{(v)} = 1 - \epsilon$.

Queste probabilità $I^{(c)}$ e $I^{(v)}$ possono anche essere considerate come la frazione media dei nodi disattivi, quelli che conoscono il valore, conoscendo la frazione di nodi disattivi all'iterazione precedente.

Analisi di convergenza Perché l'algoritmo converga la probabilità che i variable node conoscano il loro valore deve tendere a 1, ossia tutti i nodi conoscono la variabile e il sistema è stato risolto. Si può notare che il valore di $I^{(v)}$ dipende dal valore di $I^{(c)}$ che a sua volta dipende dal valore di $I^{(v)}$.

Quindi per ricavare il valore di queste probabilità ai vari passi bisogna procedere iterativamente partendo da $I^{(v)} = 1 - \epsilon$ e usandolo come input della funzione $I^{(c)} = (I^{(v)})^{k-1}$, ottenendo un valore che si può usare come input del passo successivo per ricavare nuovamente la nuova $I^{(v)}$. Questo procedimento si può eseguire graficamente se si mettono le due espressioni nello stesso grafico e procedendo a «zig-zag» come mostrato nel diagramma EXIT (EXtrinsic Information Transfer) di figura 9.4.

9. Codifica per la trasmissione su un canale BEC

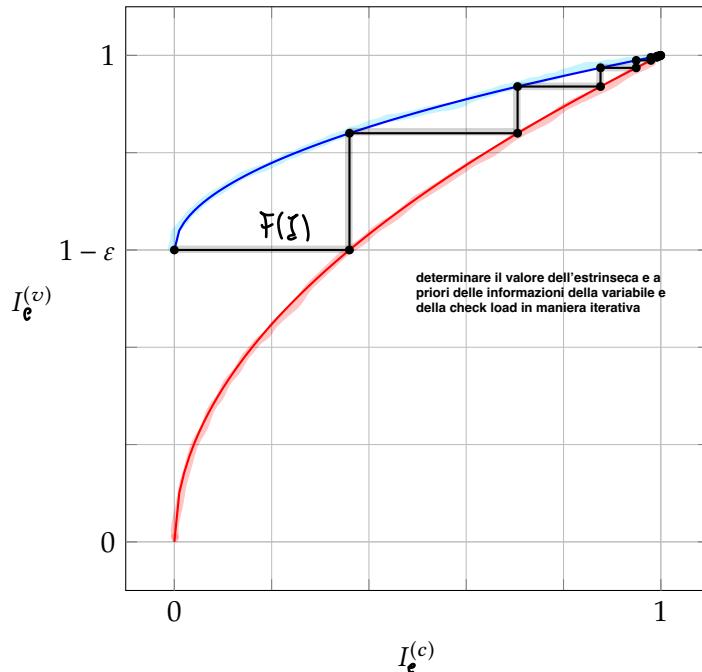


Figura 9.4.: Diagramma EXIT di analisi della convergenza di un algoritmo LDPC.

Dal grafico si può notare che $I^{(v)}$ converge a 1 solo se i due grafici non si incrociano; dato che la curva inferiore è l'inversa di $I^{(c)}$ si ha che per poter convergere deve valere:

$$F(I) = 1 - \varepsilon \cdot (1 - I)^{j-1} - I^{\frac{1}{k-1}} > 0 \quad \forall I \in [0, 1)$$

la condizione per la convergenza per la codifica iterativa

la decodifica iterativa converge se c'è un tunnel aperto tra le due curve che danno lo scambio di informazioni tra VNs e CNs

Considerazioni sulla convergenza Analizzare la funzione $F(I)$ non è semplice, ma si possono fare alcune considerazioni:

- Più la probabilità di errore del canale ε è piccola più la curva $I^{(v)}$ parte alta e quindi è più probabile che la funzione $F(I)$ sia positiva; si può quindi definire ε_T come l' ε massimo per cui vale la condizione di convergenza.
- Dato che la funzione $F(I)$ dipende dai parametri j e k è lecito chiedersi quali siano i j e k che rendono la ε_T più grande possibile a pari rate.

Non si riesce a rispondere analiticamente a queste domande data la complessità di $F(I)$, però si possono effettuare delle simulazioni.

Esempio Tramite simulazioni si può ricavare che con un rate $R = 0.5$ i valori di k e j che massimizzano la ε_T sono:

$$\begin{aligned} j &= 3 \\ k &= 6 \end{aligned}$$

da cui si ricava che:

$$\varepsilon_T = 0.43$$

da cui si può notare che la capacità di canale minima richiesta per inviare con un rate di $R = 0.5$ è $C = 1 - \varepsilon_T = 0.57$ e quindi si ha perdita ^{sensibile} rispetto alla codifica ottima, in cui per inviare con $R = 0.5$ basta un canale con $C = 0.5$.

NB: dunque la perdita tra ML e decodifica iterativa è sensibile

9.3. Codici LDPC irregolari

Introduzione I codici LDPC irregolari sono codici che generalizzano gli LDPC visti nella sezione precedente e sono stati introdotti negli anni 90 per migliorare le prestazioni dei codici. In questi codici j e k non sono parametri costanti e quindi ogni variable node e check node è collegato ad un numero diverso di nodi.

Si definiscono i seguenti valori:

- E è il numero di rami totali nel grafo, ossia il numero di uni nella matrice di parità.
- λ_i è la frazione di rami collegati ai variable node connessi a i check node, a cui si può associare il polinomio

$$\lambda(x) = \sum_{i=1}^{i_{max}} \lambda_i \cdot x^{i-1}$$

frazione dei rami collegati ai variable nodes che hanno esattamente grado i

dove i_{max} è il massimo numero di rami collegati ad un variable node.

- ρ_j è la frazione di rami collegati ai check node connessi a j variable node, a cui si può associare il polinomio

$$\rho(x) = \sum_{j=1}^{j_{max}} \rho_j \cdot x^{j-1}$$

frazione dei rami collegati a check nodes che hanno esattamente grado j

dove j_{max} è il massimo numero di rami collegati ad un check node.

Rate del codice Il numero di righe $N - K$ e di colonne N della matrice di parità si può ricavare come segue:

$$N = E \cdot \sum_{i=1}^{i_{max}} \frac{\lambda_i}{i} = E \cdot \int_0^1 \lambda(x) dx$$

$$N - K = E \cdot \sum_{j=1}^{j_{max}} \frac{\rho_j}{j} = E \cdot \int_0^1 \rho(x) dx$$

e quindi:

$$R = \frac{K}{N} = 1 - \frac{N - K}{N} = 1 - \frac{E \cdot \int_0^1 \rho(x) dx}{E \cdot \int_0^1 \lambda(x) dx} = 1 - \frac{\int_0^1 \rho(x) dx}{\int_0^1 \lambda(x) dx}$$

Analisi di convergenza Per l'analisi della convergenza si può procedere in modo analogo ai LDPC regolari, ossia si suppone che $N \rightarrow \infty$ in modo che i nodi abbiano la stessa probabilità di ricevere dell'informazione a tutti i passi, ma a differenza dei LDPC regolari tale probabilità dipende dal grado del nodo. Per questo si definiscono:

- $I_i^{(v)}$ la probabilità che un variable node di grado i possa comunicare il proprio valore.
- $I_i^{(c)}$ la probabilità che un check node di grado i sia in grado di comunicare a un variable node il valore della variabile.

Dato che i calcoli possono diventare complessi si usano le probabilità medie, ossia:

$$I_m^{(v)} = \sum_{i=1}^{i_{max}} \lambda_i \cdot I_i^{(v)}$$

$$I_m^{(c)} = \sum_{j=1}^{j_{max}} \rho_j \cdot I_j^{(c)}$$

Sfruttando tale semplificazione valgono le stesse espressioni usate per i LDPC regolari, ossia:

9. Codifica per la trasmissione su un canale BEC

$$I_i^{(v)} = 1 - \varepsilon \cdot \left(1 - I_m^{(c)}\right)^{i-1}$$

$$I_j^{(c)} = \left(I_m^{(v)}\right)^{j-1}$$

e quindi:

$$\begin{aligned} I_m^{(v)} &= \sum_{i=1}^{i_{max}} \lambda_i \cdot I_i^{(v)} = \\ &= \sum_{i=1}^{i_{max}} \lambda_i \cdot \left(1 - \varepsilon \cdot \left(1 - I_m^{(c)}\right)^{i-1}\right) = \\ &= \sum_{i=1}^{i_{max}} \lambda_i \cdot 1 - \varepsilon \cdot \sum_{i=1}^{i_{max}} \lambda_i \cdot \left(1 - I_m^{(c)}\right)^{i-1} = \\ &= 1 - \varepsilon \cdot \lambda \left(1 - I_m^{(c)}\right) \end{aligned}$$

$$\begin{aligned} I_m^{(c)} &= \sum_{i=1}^{i_{max}} \rho_i \cdot I_i^{(c)} = \\ &= \sum_{i=1}^{i_{max}} \rho_i \cdot \left(I_m^{(v)}\right)^{j-1} = \\ &= \rho \left(I_m^{(v)}\right) \end{aligned}$$

da cui si può costruire l'EXIT diagram in modo analogo ai LDPC, da cui si nota che la condizione per la convergenza è analoga e dove le due curve sono:

Exit $\Sigma_m^{(v)}$ $I_m^{(v)} = 1 - \varepsilon \cdot \lambda \left(1 - I_m^{(c)}\right)$ \Rightarrow la condizione per la convergenza della codifica iterativa diventa:
 $1 - \varepsilon \cdot \lambda(1 - x) > \rho(x) \quad \forall x \in [0, 1]$
 $\Sigma_m^{(c)}$ $I_m^{(c)} = \rho \left(I_m^{(v)}\right)$

Il vantaggio di questo codice è che avendo più gradi di libertà si può ottenere una ε_T maggiore a pari rate.

Esempio Per paragone agli LDPC regolari si consideri un LDPC irregolare con $R = 0.5$; tramite simulazione si può ottenere che:

e quindi una capacità minima richiesta:

$\varepsilon_T = 0.47$	$ $	$\varepsilon_T = 0.48$ $C_T = 0.53$
------------------------	-----	--

Regolare

che è minore di quella ottenuta con un LDPC regolare.

Criterio per la scelta di $\lambda(x)$ e $\rho(x)$ Dalle formule di $I_m^{(v)}$ e $I_m^{(c)}$ si può notare che le curve dipendono dai polinomi $\lambda(x)$ e $\rho(x)$ e quindi è utile trovare un criterio di scelta per cui si ottiene una ε_T massima.

Per farlo si può notare che una condizione necessaria per avere la convergenza è che l'area tra le due curve sia positiva, ossia:

$$A(\varepsilon) > 0$$

Tale area si può ricavare calcolando l'area al di sotto della curva superiore A_1 , sottrattogli l'area al di sopra della curva inferiore A_2 e sottraendogli l'intera area A_3 , come mostrato in figura 9.5.

9. Codifica per la trasmissione su un canale BEC

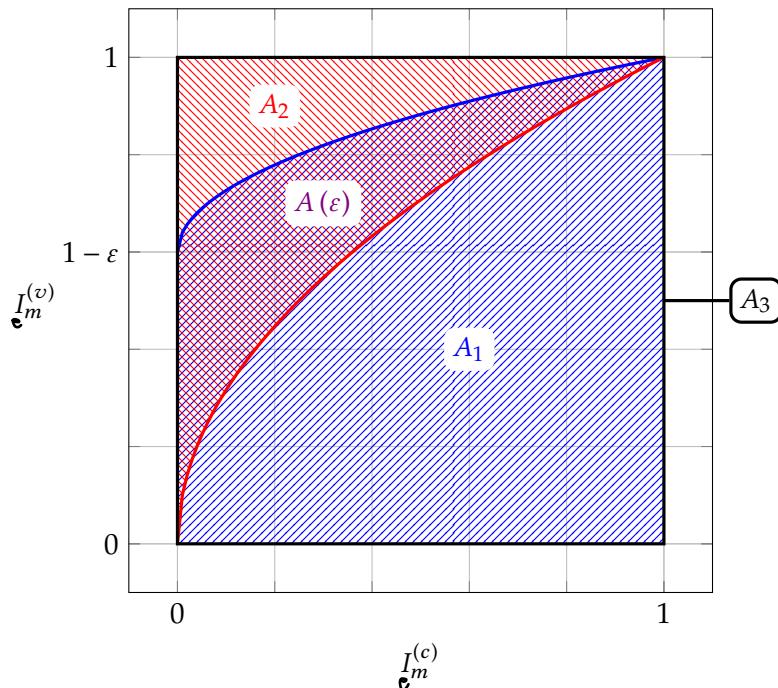


Figura 9.5.: Calcolo dell'area $A(\varepsilon)$.

La prima area A_1 è quella sottesa dalla curva $I_m^{(v)}$ e quindi:

$$\begin{aligned} A_1 &= \int_0^1 I_m^{(v)} dI_m^{(c)} = \\ &= 1 - \varepsilon \cdot \int_0^1 \lambda(1 - I_m^{(c)}) dI_m^{(c)} \end{aligned}$$

Tramite il cambio di variabile $1 - I_m^{(c)} = x$ si ottiene $dx = -dI_m^{(c)}$ e gli estremi diventano $x_1 = 1 - 1 = 0$ e $x_2 = 1 - 0 = 1$ e quindi:

$$\begin{aligned} A_1 &= 1 - \varepsilon \cdot \int_0^1 \lambda(1 - I_m^{(c)}) dI_m^{(c)} = \\ &= 1 - \varepsilon \cdot \int_1^0 -\lambda(x) dx = \\ &= 1 - \varepsilon \cdot \int_0^1 \lambda(x) dx \end{aligned}$$

La seconda area A_2 è quella sottesa dalla curva $I_m^{(c)}$ (questo si può notare meglio se si scambiano tra loro gli

9. Codifica per la trasmissione su un canale BEC

assi) e quindi:

$$\begin{aligned} A_2 &= \int_0^1 I_m^{(J)} dI_m^{(v)} = \\ &= \int_0^1 \rho(I_m^{(v)}) dI_m^{(v)} = \\ &= \int_0^1 \rho(x) dx \end{aligned}$$

La terza area A_3 corrisponde a quella di un quadrato di lato unitario e quindi:

$$A_3 = 1$$

e quindi si ha:

$$\begin{aligned} A(\varepsilon) &= A_1 + A_2 - A_3 = \\ &= 1 - \varepsilon \cdot \int_0^1 \lambda(x) dx + \int_0^1 \rho(x) dx - 1 = \\ &= \int_0^1 \lambda(x) dx \cdot \left(-\varepsilon + \frac{\int_0^1 \rho(x) dx}{\int_0^1 \lambda(x) dx} \right) = \\ &= \frac{N}{E} \cdot \left(\underbrace{1 - \varepsilon}_{C(\varepsilon)} + \underbrace{\frac{\int_0^1 \rho(x) dx}{\int_0^1 \lambda(x) dx} - 1}_{-R} \right) = \\ &= \frac{N}{E} \cdot (C(\varepsilon) - R) \end{aligned}$$

Dato che quest'area deve essere positiva si ha che:

$$C(\varepsilon) > R$$

che è la condizione necessaria data dal teorema di Shannon, ma si può notare che se si vuole avere $R = C(\varepsilon)$ bisogna ridurre quest'area a 0, ossia rendere le due curve coincidenti. In questo modo si ottiene il codice LDPC migliore possibile.

Analiticamente questa condizione corrisponde ad avere:

$$\rho^{-1}(x) = 1 - \varepsilon \cdot \lambda(1-x) \quad \forall x \in [0,1]$$

Questa condizione però non è sempre raggiungibile, ma comunque è possibile arrivare molto vicini e si ha che

$$A(\varepsilon_T)$$

è la perdita di capacità che si ha nel caso migliore.

Guardare le slide + appunti

Parte III.

Teoria della trasmissione

10. Segnali

Un segnale è una funzione di una (o più) variabili indipendenti che descrive l'andamento di una (o più) grandezze fisiche. Nella maggior parte dei casi di studio che verranno presentati, la variabile indipendente sarà il tempo. I segnali si possono dividere principalmente in due categorie:

Deterministici Un segnale deterministico è un segnale che può essere descritto in modo rigoroso, per esempio tramite una funzione, una tabella o un grafico. Questi segnali sono comunemente definiti forme d'onda.

Casuali Non noti a priori (processi casuali o forme d'onda funzioni di variabili casuali).

10.1. Forme d'onda

Introduzione Il modo più semplice per descrivere una forma d'onda è tramite una funzione $x(t)$.

10.1.1. Caratteristiche delle forme d'onda

Potenza istantanea La potenza istantanea è definita come:

$$W(t) = |x(t)|^2$$

che è una funzione che varia nel tempo che è legata alla forma d'onda. Questo parametro è definito così perché si basa sul concetto di potenza istantanea in elettrotecnica dove la potenza è proporzionale al quadrato della tensione.

Energia L'energia è definita come l'integrale nel tempo della potenza, ossia:

$$E = \int_{-\infty}^{+\infty} |x(t)|^2 dt$$

Potenza media La potenza media è la potenza istantanea media calcolata in un intervallo temporale T , solitamente si prende come intervallo l'intero dominio del tempo e quindi si ottiene:

$$W_m = \lim_{T \rightarrow \infty} \frac{1}{T} \cdot \int_{-T/2}^{+T/2} |x(t)|^2 dt$$

10.1.2. Categorie di forme d'onda

Definizione di forma d'onda reale È una forma d'onda con ampiezza reale, ossia:

$$\begin{aligned} x(t) &\in \mathbb{R} \\ t &\in \mathbb{R} \end{aligned}$$

Definizione di forma d'onda complessa È una forma d'onda con ampiezza complessa, ossia:

$$\begin{aligned} x(t) &\in \mathbb{C} \\ t &\in \mathbb{R} \end{aligned}$$

10. Segnali

Osservazione È utile notare che un segnale complesso può essere descritto da una coppia di segnali reali, che possono rappresentare parte reale e parte immaginaria dell'ampiezza del corrispondente segnale complesso oppure il suo modulo e la sua fase. Ossia:

$$\begin{aligned} x(t) &= x_R(t) + j \cdot x_I(t) = \\ &= \rho(t) \cdot e^{j \cdot \varphi(t)} \end{aligned}$$

Esempio Il più semplice esempio di forma d'onda complessa è:

$$x(t) = e^{j \cdot \omega \cdot t}$$

che è un segnale descritto da un modulo costante e da una fase che aumenta linearmente nel tempo:

$$\rho(t) = 1$$

$$\varphi(t) = \omega \cdot t$$

Inoltre tramite le formule di Eulero si ottiene:

$$\begin{aligned} x(t) &= e^{j \cdot \omega \cdot t} = \\ &= \cos(\omega \cdot t) + j \cdot \sin(\omega \cdot t) \end{aligned}$$

da cui si ricava che può essere descritto da una parte reale cosinusoidale e da una parte immaginaria sinusoidale:

$$\begin{aligned} x_R(t) &= \cos(\omega \cdot t) \\ x_I(t) &= \sin(\omega \cdot t) \end{aligned}$$

Definizione di forma d'onda periodica Le forme d'onda periodiche sono forme d'onda che, definito un intervallo temporale T detto periodo, questa si ripete all'infinito, ossia:

$$\begin{aligned} x(t) &= x(t + n \cdot T) \\ \forall n \in \mathbb{Z} \end{aligned}$$

Osservazione Se $g(t)$ è una funzione non periodica allora si può ricavare da essa un segnale periodico facendo:

$$x_P(t) = \sum_{n=-\infty}^{n=+\infty} g(t - n \cdot T_0)$$

dove T_0 è il periodo che si impone al segnale. Si può facilmente intuire che sia vero se si pensa a una forma d'onda $g(t)$ con ampiezza non nulla solamente in $\left[-\frac{T_0}{2}, \frac{T_0}{2}\right]$, ma questo funziona con qualsiasi forma d'onda.

Definizione di forme d'onda a energia finita Una forma d'onda si definisce a energia finita se:

$$E = \int_{-\infty}^{+\infty} |x(t)|^2 dt$$

converge e quindi assume un valore finito.

Definizione di forma d'onda a potenza media non nulla I segnali a potenza non nulla sono segnali in cui:

$$W_m \neq 0$$

Osservazioni

- Sia $x(t)$ una forma d'onda a energia finita, allora si ha:

$$\begin{aligned}
 W_m &= \lim_{T \rightarrow +\infty} \frac{1}{T} \cdot \int_{-T/2}^{+T/2} |x(t)|^2 dt = \\
 &= \lim_{T \rightarrow +\infty} \frac{1}{T} \cdot \int_{-\infty}^{+\infty} |x(t)|^2 dt = \\
 &= \lim_{T \rightarrow +\infty} \frac{E}{T} = \\
 &= 0
 \end{aligned}$$

Quindi le forme d'onda a energia finita hanno sempre potenza media nulla, e quindi le categorie di forme d'onda a energia finita e di forma d'onda a potenza media non nulla sono mutuamente esclusive.

- Per come è definita l'energia se un segnale è limitato nel tempo ha sicuramente energia finita.

10.1.3. Forme d'onda notevoli

10.1.3.1. Forma d'onda costante

Definizione Una forma d'onda costante è definita dalla funzione:

$$x(t) = c$$

Categorie

- Questa forma d'onda può essere sia reale che complessa, in base all'insieme numerico a cui appartiene la costante c .
- Questa forma d'onda è periodica per qualsiasi periodo T .

Potenza istantanea La potenza istantanea si può ricavare facilmente:

$$W(t) = c^2$$

Potenza media

$$\begin{aligned}
 W_m &= \lim_{T \rightarrow +\infty} \frac{1}{T} \cdot \int_{-T/2}^{+T/2} c^2 dt = \\
 &= c^2
 \end{aligned}$$

e quindi è una forma d'onda a potenza media non nulla e quindi non è una forma d'onda a energia finita.

10.1.3.2. Forma d'onda a scalino

Definizione Una forma d'onda a scalino $sca(t)$ è definita dalla funzione:

$$sca(t) = \begin{cases} 1 & \text{se } t \geq 0 \\ 0 & \text{altrimenti} \end{cases}$$

Categorie

- Questa forma d'onda è reale.
- Questa forma d'onda non è periodica.

Potenza istantanea La potenza istantanea si può ricavare facilmente:

$$W(t) = \begin{cases} 1 & \text{se } x \geq 0 \\ 0 & \text{altrimenti} \end{cases} = \text{sca}(t)$$

Potenza media

$$\begin{aligned} W_m &= \lim_{T \rightarrow \infty} \frac{1}{T} \cdot \int_{-T/2}^{+T/2} \text{sca}(t) dt = \\ &= \lim_{T \rightarrow \infty} \frac{1}{T} \cdot \int_0^{+T/2} 1 dt = \\ &= \lim_{T \rightarrow \infty} \frac{1}{T} \cdot \frac{T}{2} = \\ &= \frac{1}{2} \end{aligned}$$

e quindi è una forma d'onda a potenza media non nulla e quindi non è una forma d'onda a energia finita.

10.1.3.3. Forma d'onda a rettangolo

Definizione Una forma d'onda a rettangolo $\text{rect}(t)$ è definita dalla funzione:

$$\text{rect}(t) = \begin{cases} 1 & \text{se } -\frac{1}{2} \leq t \leq \frac{1}{2} \\ 0 & \text{altrimenti} \end{cases}$$

Categorie

- Questa forma d'onda è reale.
- Questa forma d'onda non è periodica.

Potenza istantanea La potenza istantanea si può ricavare facilmente:

$$\begin{aligned} W(t) &= \begin{cases} 1 & \text{se } -\frac{1}{2} \leq t \leq \frac{1}{2} \\ 0 & \text{altrimenti} \end{cases} \\ &= \text{rect}(t) \end{aligned}$$

Energia

$$\begin{aligned}
 E &= \int_{-\infty}^{+\infty} \text{rect}(t) dt = \\
 &= \int_{-1/2}^{+1/2} 1 dt = \\
 &= \frac{1}{2} + \frac{1}{2} = \\
 &= 1
 \end{aligned}$$

e quindi è una forma d'onda a energia finita e quindi ha potenza media nulla.

10.1.3.4. Forma d'onda a delta di Dirac

Definizione Una delta di Dirac si definisce come una forma d'onda tale che:

$$\begin{aligned}
 \delta(t) &= 0 \\
 \forall t \neq 0 & \\
 \int_{-\infty}^{+\infty} \delta(t) dt &= 1
 \end{aligned}$$

Questo segnale si può considerare come un segnale rettangolare con una base larga T e altezza $1/T$ con $T \rightarrow 0$. Graficamente si indica con una freccia di altezza 1.

Categorie

- Questa forma d'onda è reale.
- Questa forma d'onda non è periodica.
- Questa forma d'onda è pari, ossia:

$$\delta(t) = \delta(-t)$$

Proprietà speciali

- Data una forma d'onda qualsiasi $x(t)$ si ha che:

$$\begin{aligned}
 x(t) \cdot \delta(t) &= 0 \\
 \forall t \neq 0 &
 \end{aligned}$$

$$\int_{-\infty}^{+\infty} x(t) \cdot \delta(t) dt = x(0)$$

e quindi si ha che:

$$x(t) \cdot \delta(t) = x(0) \cdot \delta(t)$$

- Data una forma d'onda qualsiasi $x(t)$ si ha che:

$$\int_{-\infty}^{+\infty} x(t) \cdot \delta(t - \tau) dt = x(\tau)$$

10.1.4. Manipolazione di forme d'onda

Ritardo e anticipo Dato un segnale $x(t)$ si può ottenere il segnale $y(t)$ ritardato di t_0 sottraendo alla variabile indipendente il ritardo t_0 :

$$y(t) = x(t - t_0)$$

Se $t_0 < 0$ si ottiene l'effetto opposto, ossia un anticipo.

Dilatazione e contrazione Dato un segnale $x(t)$ si può ottenere il segnale $y(t)$ dilatato di un fattore $\tau > 1$ dividendo la variabile indipendente per il fattore di dilatazione τ :

$$y(t) = x\left(\frac{t}{\tau}\right)$$

Se $0 < \tau < 1$ si ottiene l'effetto opposto, ossia una contrazione. Se $\tau < 0$ si ha come effetto aggiuntivo quello di specchiare il segnale rispetto all'asse y .

Amplificazione e attenuazione Dato un segnale $x(t)$ si può ottenere il segnale $y(t)$ amplificato di un fattore $A > 1$ moltiplicando la forma d'onda per il fattore di amplificazione A :

$$y(t) = A \cdot x(t)$$

se $0 < A < 1$ si ottiene l'effetto opposto, ossia un'attenuazione. Se $A < 0$ si ha come effetto aggiuntivo quello di specchiare il segnale rispetto all'asse x .

Osservazione Tutte le manipolazioni viste possono essere combinate tra di loro, per esempio: se si vuole ottenere il segnale $y(t)$ dal segnale $x(t)$ ritardandolo di t_0 , contraendo l'asse dei tempi di un fattore τ e amplificando il segnale stesso di un fattore A si può scrivere:

$$y(t) = A \cdot x\left(\frac{t - t_0}{\tau}\right)$$

Da notare che il segnale:

$$\begin{aligned} z(t) &= x\left(\frac{t}{\tau} - t_0\right) = \\ &= x\left(\frac{t - t_0 \cdot \tau}{\tau}\right) \end{aligned}$$

subisce in realtà un ritardo di $t_0 \cdot \tau$ e non di t_0 .

Osservazione Tutte le proprietà ricavate per le forme d'onda notevoli sono valide anche a seguito di manipolazioni, l'unica differenza è che possono variare i valori di energia e potenza. Per esempio si consideri la forma d'onda:

$$x(t) = A \cdot \text{rect}\left(\frac{t - t_0}{\tau}\right)$$

dato che il rettangolo è una forma d'onda a energia finita lo è anche $x(t)$, ma vale che:

$$\begin{aligned} E &= \int_{-\infty}^{+\infty} x(t)^2 dt = \\ &= \int_{t_0 - \tau/2}^{t_0 + \tau/2} A^2 dt = \\ &= A^2 \cdot \left[t_0 + \frac{\tau}{2} - t_0 - \frac{\tau}{2} \right] = \\ &= A^2 \cdot \tau \end{aligned}$$

Altre forme d'onda Partendo da queste si possono costruire diverse forme d'onda con diverse proprietà, per esempio si consideri la forma d'onda:

$$x(t) = \text{sca}(t) \cdot A \cdot e^{-\frac{t}{\tau}}$$

Questo segnale non è limitato nel tempo e non è neppure periodico, però è a energia limitata, infatti:

$$\begin{aligned} E &= \int_{-\infty}^{+\infty} x(t)^2 dt = \\ &= \int_{-\infty}^{+\infty} \left(\text{sca}(t) \cdot A \cdot e^{-\frac{t}{\tau}} \right)^2 dt \\ &= \int_0^{+\infty} A^2 \cdot e^{-\frac{2 \cdot t}{\tau}} dt = \\ &= A^2 \cdot \int_0^{+\infty} e^{-\frac{2 \cdot t}{\tau}} dt = \\ &= A^2 \cdot \left[-\frac{\tau}{2} \cdot e^{-\frac{2 \cdot t}{\tau}} \right]_0^{+\infty} = \\ &= -\frac{A^2 \cdot \tau}{2} \cdot [0 - 1] = \\ &= \frac{A^2 \cdot \tau}{2} \end{aligned}$$

10.2. Trasformata di Fourier

10.2.1. Serie di Fourier

Definizione La serie di Fourier permette di rappresentare un segnale periodico $x_p(t)$ di periodo T_0 come una somma di infinite sinusoidi di diversa ampiezza e di periodo multiplo di T_0 . In forma compatta si può scrivere:

$$x_p(t) = \sum_{n=-\infty}^{\infty} C_n \cdot e^{j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t}$$

dove:

$$C_n = \frac{1}{T_0} \cdot \int_{-T_0/2}^{T_0/2} x_p(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t} dt$$

Osservazioni

- La frequenza $f_0 = T_0^{-1}$ è detta frequenza fondamentale e si ha che tutte le componenti sinusoidali hanno frequenza multipla di f_0 , ossia del tipo $n \cdot f_0$ con $n \in \mathbb{Z}$.
- Ogni componente sinusoidale prende il nome di armonica del segnale.

10.2.2. Trasformata di Fourier

Definizione La trasformata di Fourier è una generalizzazione per segnali non periodici della serie di Fourier. I segnali non periodici possono essere considerati come dei segnali periodici di periodo infinito e quindi con

10. Segnali

$T_0 = \infty$. Si può pensare che ogni armonica sia distanziata dalla successiva da un infinitesimo e quindi la successione C_n dei coefficienti diventa una funzione continua definita come:

$$x(t) = \int_{-\infty}^{+\infty} X(f) \cdot e^{j \cdot 2 \cdot \pi \cdot f \cdot t} df$$

e:

$$X(f) = \int_{-\infty}^{+\infty} x(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt$$

Osservazioni

- La funzione $X(f)$ è detta funzione trasformata di Fourier ed è definita nel dominio delle frequenze.
- La rappresentazione grafica di $X(f)$ è detta spettro di $x(t)$.
- Si indica $X(f) = \mathcal{F} x(t)$ o $x(t) \Leftarrow X(f)$.

10.2.3. Trasformate notevoli

10.2.3.1. Trasformata dello scalino

Sia $x(t) = \text{sca}(t)$ allora si ha:

$$\begin{aligned} X(t) &= \int_{-\infty}^{+\infty} \text{sca}(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\ &= \int_0^{+\infty} e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\ &= \left[-\frac{e^{-j \cdot 2 \cdot \pi \cdot f \cdot t}}{j \cdot 2 \cdot \pi \cdot f} \right]_0^{+\infty} = \\ &= 0 - \left(-\frac{1}{j \cdot 2 \cdot \pi \cdot f} \right) = \\ &= \frac{1}{j \cdot 2 \cdot \pi \cdot f} \end{aligned}$$

10.2.3.2. Trasformata della forma d'onda rettangolare

Sia $x(t) = \text{rect}(t)$ allora si ha:

$$\begin{aligned}
 X(t) &= \int_{-\infty}^{+\infty} \text{rect}(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\
 &= \int_{-1/2}^{1/2} e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\
 &= \left[-\frac{e^{-j \cdot 2 \cdot \pi \cdot f \cdot t}}{j \cdot 2 \cdot \pi \cdot f} \right]_{-1/2}^{1/2} = \\
 &= \frac{e^{-j \cdot \pi \cdot f}}{j \cdot 2 \cdot \pi \cdot f} + \frac{e^{j \cdot \pi \cdot f}}{j \cdot 2 \cdot \pi \cdot f} = \\
 &= \frac{e^{j \cdot \pi \cdot f} - e^{-j \cdot \pi \cdot f}}{j \cdot 2 \cdot \pi \cdot f} = \\
 &= \frac{1}{\pi \cdot f} \cdot \frac{e^{j \cdot \pi \cdot f} - e^{-j \cdot \pi \cdot f}}{2 \cdot j} = \\
 &= \frac{\sin(\pi \cdot f)}{\pi \cdot f} = \\
 &= \text{sinc}(f)
 \end{aligned}$$

quindi la trasformata del rettangolo è il seno cardinale^I.

10.2.3.3. Trasformata della delta di Dirac

Sia $x(t) = \delta(t)$ allora si ha:

$$\begin{aligned}
 X(t) &= \int_{-\infty}^{+\infty} \delta(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\
 &= e^{-j \cdot 2 \cdot \pi \cdot f \cdot 0} = \\
 &= 1
 \end{aligned}$$

e quindi la trasformata della delta di Dirac è una costante.

10.2.4. Proprietà della trasformata di Fourier

10.2.4.1. Linearità

La trasformata di Fourier è un operatore lineare e quindi si ha che:

$$\mathcal{F} [\alpha \cdot x_1(t) + \beta \cdot x_2(t)] = \alpha \cdot X_1(f) + \beta \cdot X_2(f)$$

$\forall \alpha, \beta \in \mathbb{R}$

^IIl seno cardinale può essere definito in due modi:

- Il seno cardinale normalizzato, utilizzato in questa trattazione, in cui si ha:

$$\text{sinc}(x) = \begin{cases} \frac{\sin(\pi \cdot x)}{\pi \cdot x} & \text{se } x \neq 0 \\ 1 & \text{se } x = 0 \end{cases}$$

- Il seno cardinale non normalizzato in cui si ha:

$$\text{sinc}(x) = \begin{cases} \frac{\sin(x)}{x} & \text{se } x \neq 0 \\ 1 & \text{se } x = 0 \end{cases}$$

10.2.4.2. Simmetria

Proprietà generali Data una funzione $x(t)$ con trasformata $X(f)$ si ha che^{II}:

$$x(-t) \Leftrightarrow X(-f)$$

$$x(t)^* \Leftrightarrow X(-f)^*$$

Proprietà su modulo e fase della trasformata di un segnale reale Queste proprietà si possono estendere se $x(t) \in \mathbb{R}$, infatti si ha che:

$$\begin{aligned} |X(f)| &= |X(f)^*| = \\ &= |\mathcal{F} x(-t)^*| = \\ &= |\mathcal{F} x(-t)| = \\ &= |X(-f)| \end{aligned}$$

e quindi la trasformata è pari in modulo e inoltre:

$$\begin{aligned} \angle X(f) &= -\angle X(f)^* = \\ &= -\angle \mathcal{F} x(-t)^* = \\ &= -\angle \mathcal{F} x(-t) = \\ &= -\angle X(-f) \end{aligned}$$

e quindi è dispari in fase.

Proprietà sulle componenti reali e immaginarie della trasformata di un segnale reale Si possono fare considerazioni solo se la funzione è pari o dispari:

- Se $x(t)$ è pari allora si ha che:

$$X(f) = \mathcal{F} x(t) = \mathcal{F} x(-t) = X(-f)$$

e quindi anche la trasformata è pari, inoltre:

$$X(f) = \mathcal{F} x(t) = \mathcal{F} x(t)^* = \mathcal{F} x(-t)^* = X(f)^*$$

e quindi la trasformata e il suo coniugato sono uguali e quindi deve essere per forza reale, cioè $X(f) \in \mathbb{R}$.

- Se $x(t)$ è dispari allora si ha che:

$$X(f) = \mathcal{F} x(t) = \mathcal{F} -x(-t) = -X(-f)$$

e quindi anche la trasformata è dispari, inoltre:

$$X(f) = \mathcal{F} x(t) = \mathcal{F} x(t)^* = \mathcal{F} -x(-t)^* = -X(f)^*$$

e quindi la trasformata è l'opposto del suo coniugato e quindi deve essere per forza puramente immaginaria.

10.2.4.3. Trasformata e antitrasformata in 0

Principio Un'importante proprietà della trasformata è la seguente:

$$\begin{aligned} X(0) &= \int_{-\infty}^{+\infty} x(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot t \cdot 0} dt = \int_{-\infty}^{+\infty} x(t) dt \\ x(0) &= \int_{-\infty}^{+\infty} X(f) \cdot e^{j \cdot 2 \cdot \pi \cdot 0 \cdot f} df = \int_{-\infty}^{+\infty} X(f) df \end{aligned}$$

e quindi l'area sottesa della trasformata corrisponde al valore assunto dalla funzione in 0 e viceversa.

^{II}Dato un numero complesso z , z^* indica il suo coniugato.

Esempio: segnale rettangolare Si è visto che:

$$\text{rect}(t) \Leftrightarrow \text{sinc}(f)$$

quindi l'area sottesa dal seno cardinale è:

$$\text{rect}(0) = 1$$

10.2.4.4. Dualità

Principio La dualità permette di ricavare delle trasformate da quelle che già si conoscono, infatti data una forma d'onda $x(t)$ con trasformata $X(f)$ si ha che:

$$X(t) \Leftrightarrow x(-f)$$

Esempio: trasformata del seno cardinale Si è visto che:

$$\text{rect}(t) \Leftrightarrow \text{sinc}(f)$$

quindi per la proprietà di dualità si ha che:

$$\mathcal{F} \text{sinc}(t) = \text{rect}(-f) = \text{rect}(f)$$

10.2.4.5. Scalatura

Principio Sia $x(t)$ una forma d'onda con trasformata $X(f)$ e $\alpha \in \mathbb{R}$ allora si ha che:

$$x(\alpha \cdot t) \Leftrightarrow \frac{1}{|\alpha|} \cdot X\left(\frac{f}{\alpha}\right)$$

Esempio Si è visto che:

$$\mathcal{F} \text{rect}(t) = \text{sinc}(f)$$

e quindi:

$$\mathcal{F} \text{rect}\left(\frac{t}{T}\right) = T \cdot \text{sinc}(T \cdot f)$$

10.2.4.6. Traslazione

Sia $x(t)$ una forma d'onda con trasformata $X(f)$ e $\alpha \in \mathbb{R}$ allora si ha che:

$$x(t - \alpha) \Leftrightarrow X(f) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot \alpha}$$

Esempi Si è visto che:

$$\delta(t) \Leftrightarrow 1$$

e quindi:

$$\mathcal{F} \delta(t - t_0) = 1 \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t_0} = e^{-j \cdot 2 \cdot \pi \cdot f \cdot t_0}$$

Questo è un risultato molto importante perché per la dualità si ottiene:

$$\mathcal{F} e^{-j \cdot 2 \cdot \pi \cdot f_0 \cdot t} = \delta(f_0 - f) = \delta(f - f_0)$$

Tramite questo risultato, utilizzando le formule di Eulero, è possibile ricavare la trasformata della cosinusoide:

$$\begin{aligned} \mathcal{F} A \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t) &= \mathcal{F} \frac{A}{2} \cdot [e^{j \cdot 2 \cdot \pi \cdot f_0 \cdot t} + e^{-j \cdot 2 \cdot \pi \cdot f_0 \cdot t}] = \\ &= \frac{A}{2} \cdot [\mathcal{F} e^{j \cdot 2 \cdot \pi \cdot f_0 \cdot t} + \mathcal{F} e^{-j \cdot 2 \cdot \pi \cdot f_0 \cdot t}] = \\ &= \frac{A}{2} \cdot [\delta(f - f_0) + \delta(f + f_0)] \end{aligned}$$

e quindi la trasformata di una cosinusoide è la somma di due delta di Dirac posizionate alla frequenza della cosinusoide stessa e alla sua opposta. Tramite analoghi passaggi si può ricavare la trasformata di una sinusoide:

$$\begin{aligned}\mathcal{F} A \cdot \sin(2 \cdot \pi \cdot f_0 \cdot t) &= \mathcal{F} \frac{A}{2 \cdot j} \cdot [e^{j \cdot 2 \cdot \pi \cdot f_0 \cdot t} - e^{-j \cdot 2 \cdot \pi \cdot f_0 \cdot t}] = \\ &= \frac{A}{2 \cdot j} \cdot [\mathcal{F} e^{j \cdot 2 \cdot \pi \cdot f_0 \cdot t} - \mathcal{F} e^{-j \cdot 2 \cdot \pi \cdot f_0 \cdot t}] = \\ &= \frac{A}{2 \cdot j} \cdot [\delta(f - f_0) - \delta(f + f_0)]\end{aligned}$$

10.2.4.7. Traslazione in frequenza

Principio Sia $x(t)$ una forma d'onda con trasformata $X(f)$ allora si ha che:

$$X(f - f_0) \Leftrightarrow x(t) \cdot e^{j \cdot 2 \cdot \pi \cdot f_0 \cdot t}$$

Osservazione La traslazione in frequenza è anche chiamata modulazione del segnale dato che permette di spostare in frequenza il segnale.

10.2.4.8. Convoluzione

Definizione di convoluzione Dati due segnali $x(t)$ e $y(t)$ si può definire l'operatore di convoluzione:

$$[x * y](t) = \int_{-\infty}^{+\infty} x(\tau) \cdot y(t - \tau) d\tau$$

Proprietà commutativa La convoluzione gode della proprietà commutativa, infatti ponendo $k = t - \tau$ si ottiene:

$$\begin{aligned}[x * y](t) &= \int_{-\infty}^{+\infty} x(\tau) \cdot y(t - \tau) d\tau = \\ &= \int_{-\infty}^{+\infty} -x(t - k) \cdot y(k) dk = \\ &= \int_{-\infty}^{+\infty} x(t - k) \cdot y(k) dk = \\ &= [y * x](t)\end{aligned}$$

Altre proprietà

- $[(\alpha \cdot x) * (\beta \cdot y)](t) = \alpha \cdot \beta \cdot [x * y](t)$
- Data una forma d'onda qualsiasi $y(t)$ e una forma d'onda pari $x(t)$ allora la loro convoluzione è pari, infatti:

$$k(t) = [x * y](t) = \int_{-\infty}^{+\infty} x(\tau) \cdot y(t - \tau) d\tau$$

tramite il cambio di variabile $u = -\tau$ si ottiene:

$$\begin{aligned} k(t) &= \int_{+\infty}^{-\infty} -x(-u) \cdot y(t - (-u)) du = \\ &= \int_{-\infty}^{+\infty} x(u) \cdot y(t - (-u)) du = \\ &= k(-t) \end{aligned}$$

- Sia $x(t)$ una forma d'onda qualsiasi allora definendo

$$\text{comb}_T(t) = \sum_{n=-\infty}^{+\infty} \delta(t - n \cdot T)$$

si ha:

$$\begin{aligned} k(t) &= [x * \text{comb}_T](t) = \\ &= \int_{-\infty}^{+\infty} x(t - \tau) \cdot \text{comb}_T(\tau) d\tau = \\ &= \int_{-\infty}^{+\infty} x(t - \tau) \cdot \left[\sum_{n=-\infty}^{+\infty} \delta(\tau - n \cdot T) \right] d\tau = \\ &= \sum_{n=-\infty}^{+\infty} \left[\int_{-\infty}^{+\infty} x(t - \tau) \cdot \delta(\tau - n \cdot T) d\tau \right] = \\ &= \sum_{n=-\infty}^{+\infty} x(t - n \cdot T) \end{aligned}$$

- La convoluzione di segnali costanti a tratti è una funzione lineare a tratti con punti spigolosi in prossimità delle discontinuità dei segnali convoluti; è quindi possibile ricavare la convoluzione calcolando solamente i valori dei punti spigolosi.

Per comprendere meglio questo secondo punto si consideri la convoluzione:

$$\begin{aligned} x(t) &= [\text{rect} * \text{rect}](t) = \\ &= \int_{-\infty}^{+\infty} \text{rect}(\tau) \cdot \text{rect}(t - \tau) d\tau = \\ &= \int_{t-1/2}^{t+1/2} \text{rect}(\tau) d\tau \end{aligned}$$

Quindi:

- se $t + \frac{1}{2} < -\frac{1}{2}$ la funzione integranda è nulla in tutto l'intervallo d'integrazione e quindi:

$$\begin{aligned} x(t) &= 0 \\ \forall t \in (-\infty, -1] \end{aligned}$$

10. Segnali

- se $-\frac{1}{2} < t + \frac{1}{2} < \frac{1}{2}$ allora l'integrale diventa:

$$\begin{aligned} x(t) &= \int_{-1/2}^{t+1/2} 1 d\tau \\ &= t + \frac{1}{2} + \frac{1}{2} = t + 1 \\ &\forall t \in (-1, 0] \end{aligned}$$

- se $-\frac{1}{2} < t - \frac{1}{2} < \frac{1}{2}$ allora l'integrale diventa:

$$\begin{aligned} x(t) &= \int_{t-1/2}^{1/2} 1 d\tau \\ &= \frac{1}{2} - t + \frac{1}{2} = 1 - t \\ &\forall t \in (0, 1) \end{aligned}$$

- se $t - \frac{1}{2} > \frac{1}{2}$ allora la funzione integranda è nulla in tutto l'intervallo d'integrazione e quindi:

$$\begin{aligned} x(t) &= 0 \\ &\forall t \in [1, +\infty) \end{aligned}$$

e quindi:

$$x(t) = \begin{cases} 0 & \text{se } t \leq -1 \\ t + 1 & \text{se } -1 < t \leq 0 \\ 1 - t & \text{se } 0 < t < 1 \\ 0 & \text{se } t \geq 1 \end{cases} = \text{tr}(t)$$

che è una funzione lineare a tratti.

Convoluzione dell'impulso Sia $x(t)$ una forma d'onda, allora definendo

$$\delta_A(a) = \delta(a - A)$$

si ha che:

$$\begin{aligned} [x * \delta_{t_0}](t) &= \int_{-\infty}^{+\infty} x(\tau) \cdot \delta(t - t_0 - \tau) d\tau = \\ &= x(t - t_0) \end{aligned}$$

Trasformata della convoluzione Dati due segnali $x(t)$ e $y(t)$ con trasformata $X(f)$ e $Y(f)$ si ha che:

$$\begin{aligned}
 \mathcal{F}[x * y](t) &= \int_{-\infty}^{+\infty} [x * y](t) \cdot e^{-j \cdot 2 \cdot \pi \cdot t \cdot f} dt = \\
 &= \int_{-\infty}^{+\infty} \left[\int_{-\infty}^{+\infty} x(\tau) \cdot y(t - \tau) d\tau \right] \cdot e^{-j \cdot 2 \cdot \pi \cdot t \cdot f} dt = \\
 &= \int_{-\infty}^{+\infty} x(\tau) \cdot \left[\int_{-\infty}^{+\infty} y(t - \tau) \cdot e^{-j \cdot 2 \cdot \pi \cdot t \cdot f} dt \right] d\tau = \\
 &= \int_{-\infty}^{+\infty} x(\tau) \cdot e^{-j \cdot 2 \cdot \pi \cdot \tau \cdot f} \left[\int_{-\infty}^{+\infty} y(t - \tau) \cdot e^{-j \cdot 2 \cdot \pi \cdot t \cdot f} \cdot e^{j \cdot 2 \cdot \pi \cdot \tau \cdot f} dt \right] d\tau = \\
 &= \int_{-\infty}^{+\infty} x(\tau) \cdot e^{-j \cdot 2 \cdot \pi \cdot \tau \cdot f} \left[\int_{-\infty}^{+\infty} y(t - \tau) \cdot e^{-j \cdot 2 \cdot \pi \cdot (t - \tau) \cdot f} dt \right] d\tau = \\
 &= \int_{-\infty}^{+\infty} x(\tau) \cdot e^{-j \cdot 2 \cdot \pi \cdot \tau \cdot f} \cdot Y(f) d\tau = \\
 &= Y(f) \cdot \int_{-\infty}^{+\infty} x(\tau) \cdot e^{-j \cdot 2 \cdot \pi \cdot \tau \cdot f} d\tau = \\
 &= X(f) \cdot Y(f)
 \end{aligned}$$

Antitrasformata della convoluzione Dati due segnali $x(t)$ e $y(t)$ con trasformata $X(f)$ e $Y(f)$ si ha che:

$$\begin{aligned}
 \mathcal{F} x(t) \cdot y(t) &= \int_{-\infty}^{+\infty} x(t) \cdot y(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\
 &= \int_{-\infty}^{+\infty} x(t) \cdot \left[\int_{-\infty}^{+\infty} Y(\tau) \cdot e^{j \cdot 2 \cdot \pi \cdot \tau \cdot t} d\tau \right] \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\
 &= \int_{-\infty}^{+\infty} x(t) \cdot \left[\int_{-\infty}^{+\infty} Y(\tau) \cdot e^{j \cdot 2 \cdot \pi \cdot \tau \cdot t} d\tau \right] \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\
 &= \int_{-\infty}^{+\infty} Y(\tau) \cdot \left[\int_{-\infty}^{+\infty} x(t) \cdot e^{j \cdot 2 \cdot \pi \cdot \tau \cdot t} \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt \right] d\tau = \\
 &= \int_{-\infty}^{+\infty} Y(\tau) \cdot \left[\int_{-\infty}^{+\infty} x(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot (f - \tau) \cdot t} dt \right] d\tau = \\
 &= \int_{-\infty}^{+\infty} Y(\tau) \cdot X(f - \tau) d\tau = \\
 &= [X * Y](f)
 \end{aligned}$$

Esempio di modulazione in ampiezza Sia $x(t)$ un segnale con trasformata $X(f)$ e $y(t) = A \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t)$, allora sapendo che

$$\begin{aligned} Y(f) &= \frac{A}{2} \cdot [\delta(f - f_0) + \delta(f + f_0)] = \\ &= \frac{A}{2} \cdot [\delta_{f_0}(f) + \delta_{-f_0}(f)] \end{aligned}$$

si può calcolare:

$$\begin{aligned} \mathcal{F}[x(t) \cdot y(t)] &= [X * Y](f) = \\ &= \frac{A}{2} \cdot [[X * \delta_{f_0}](f) + [X * \delta_{-f_0}](f)] = \\ &= \frac{A}{2} \cdot [X(f - f_0) + X(f + f_0)] \end{aligned}$$

In figura 10.1 viene mostrato un esempio di modulazione in ampiezza.

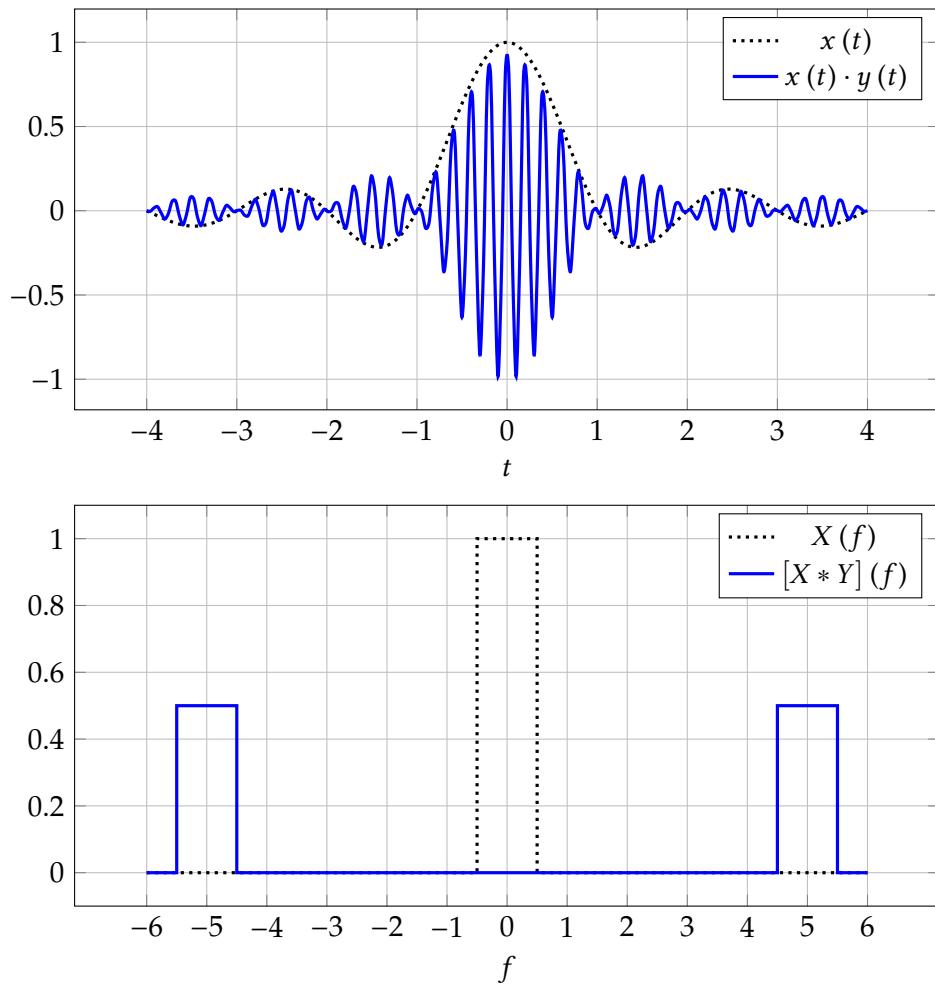


Figura 10.1.: Modulazione di un segnale in ampiezza: $x(t) = \text{sinc}(t)$, $y(t) = \cos(2 \cdot \pi \cdot 5 \cdot t)$.

Esempio di trasformata della convoluzione Si consideri il segnale triangolare visto prima $\text{tr}(t)$ definito come:

$$\text{tr}(t) = [\text{rect} * \text{rect}](t)$$

Si ha che:

$$\begin{aligned} \mathcal{F}[\text{tr}(t)] &= \mathcal{F}[\text{rect}(t) * \text{rect}(t)] = \\ &= \text{sinc}(t)^2 \end{aligned}$$

10.2.4.9. Relazione di Parseval

Principio Data una forma d'onda $x(t)$ a energia finita E allora:

$$E = \int_{-\infty}^{+\infty} |X(f)|^2 df$$

Dimostrazione Si consideri il segnale ($x_-(t) = x(-t)$):

$$\begin{aligned} k(t) &= [x * x_-^*](t) = \\ &= \int_{-\infty}^{+\infty} x(\tau) \cdot x_-(t - \tau)^* d\tau = \\ &= \int_{-\infty}^{+\infty} x(\tau) \cdot x(\tau - t)^* d\tau \end{aligned}$$

che ha come trasformata:

$$\begin{aligned} K(f) &= X(f) \cdot X_-(f)^* = \\ &= X(f) \cdot X(-f)^* = \\ &= X(f) \cdot X(f)^* = \\ &= |X(f)|^2 \end{aligned}$$

Si può ricavare $k(0)$ nel dominio del tempo:

$$\begin{aligned} k(0) &= \int_{-\infty}^{+\infty} x(\tau) \cdot x(\tau)^* d\tau = \\ &= \int_{-\infty}^{+\infty} |x(\tau)|^2 d\tau = \\ &= E \end{aligned}$$

Inoltre per la proprietà 10.2.4.3 si ha che:

$$\begin{aligned} k(0) &= \int_{-\infty}^{+\infty} K(f) df = \\ &= \int_{-\infty}^{+\infty} |X(f)|^2 df = \\ &= E \end{aligned}$$

e quindi:

$$k(0) = \int_{-\infty}^{+\infty} |x(t)|^2 dt = \int_{-\infty}^{+\infty} |X(f)|^2 df = E$$

Osservazione La funzione $|X(f)|^2$ è definita funzione di densità spettrale d'energia perché rappresenta il modo in cui l'energia del segnale è distribuita sulle varie frequenze.

Segnali a energia finita passa-basso Un segnale $x(t)$ a energia finita si dice segnale passa-basso (low-pass, LP) se tutta l'energia è concentrata intorno alla frequenza nulla.

Per i segnali passa-basso si definisce il concetto di banda B che si misura in Hz come il minimo valore di frequenza tale che la densità spettrale di energia è nulla, ossia:

$$\begin{aligned} |X(f)|^2 &= 0 \\ \forall f > B \end{aligned}$$

Solitamente la funzione di densità spettrale di energia non è mai nulla, ma se va a 0 asintoticamente il segnale si può considerare comunque di tipo passa-basso.

Segnali a energia finita passa-banda Un segnale $x(t)$ a energia finita si dice segnale passa-banda (band-pass, BP) se tutta l'energia è concentrata intorno a una frequenza f_0 .

Per i segnali passa-banda si definisce il concetto di banda B che si misura in Hz come la larghezza dell'intervallo in cui la densità spettrale di energia non è nulla, ossia:

$$\begin{aligned} |X(f)|^2 &\neq 0 \\ |f - f_0| &< \frac{B}{2} \end{aligned}$$

Solitamente la funzione di densità spettrale di energia non è mai nulla, ma se va asintoticamente a 0 in entrambe le direzioni allora si può considerare comunque di tipo passa-banda.

Esempio di segnale passa-basso Si consideri il segnale $x(t) = \text{sca}(t) \cdot e^{-\frac{t}{\tau}}$ allora:

$$\begin{aligned} \mathcal{F} x(t) &= \int_{-\infty}^{+\infty} \text{sca}(t) \cdot e^{-\frac{t}{\tau}} \cdot e^{-j \cdot 2 \cdot \pi \cdot t \cdot f} dt = \\ &= \int_0^{+\infty} e^{-j \cdot 2 \cdot \pi \cdot t \cdot f - \frac{t}{\tau}} dt = \\ &= \int_0^{+\infty} e^{-(j \cdot 2 \cdot \pi \cdot f + \frac{1}{\tau}) \cdot t} dt = \\ &= \left[\frac{e^{-(j \cdot 2 \cdot \pi \cdot f + \frac{1}{\tau}) \cdot t}}{-\left(j \cdot 2 \cdot \pi \cdot f + \frac{1}{\tau}\right)} \right]_0^{+\infty} = \\ &= 0 + \frac{1}{j \cdot 2 \cdot \pi \cdot f + \frac{1}{\tau}} = \\ &= \frac{\tau}{1 + j \cdot 2 \cdot \pi \cdot f \cdot \tau} \end{aligned}$$

e quindi la densità spettrale di energia è:

$$|X(f)|^2 = \frac{\tau^2}{1 + 4 \cdot \pi^2 \cdot f^2 \cdot \tau^2}$$

da cui si nota che:

$$\begin{aligned} f \rightarrow 0 &\Rightarrow |X(f)|^2 \rightarrow \tau^2 \\ f \rightarrow +\infty &\Rightarrow |X(f)|^2 \rightarrow 0 \end{aligned}$$

e quindi è un segnale di tipo passa-basso.

10.2.5. Trasformata di Fourier di un segnale periodico

Definizione dei segnali periodici Dato un segnale periodico $x_p(t)$, di periodo T_0 , questo può sempre essere visto come la ripetizione nel tempo di un segnale non periodico $x(t)$ con trasformata $X(f)$, infatti definendo:

$$x(t) = \begin{cases} x_p(t) & |t| \leq \frac{T_0}{2} \\ 0 & |t| > \frac{T_0}{2} \end{cases}$$

si nota che:

$$x_p(t) = \sum_{n=-\infty}^{\infty} x(t - n \cdot T_0)$$

Calcolo dei coefficienti C_n Utilizzando questa notazione si ha che:

$$\begin{aligned} C_n &= \frac{1}{T_0} \cdot \int_{-T_0/2}^{T_0/2} x_p(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t} dt = \\ &= \frac{1}{T_0} \cdot \int_{-T_0/2}^{T_0/2} x(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t} dt = \\ &= \frac{1}{T_0} \cdot \int_{-\infty}^{+\infty} x(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t} dt = \\ &= \frac{1}{T_0} \cdot X\left(\frac{n}{T_0}\right) \end{aligned}$$

Trasformata di $x_p(t)$ Dalla definizione di serie di Fourier si ha che:

$$\begin{aligned} x_p(t) &= \sum_{n=-\infty}^{\infty} C_n \cdot e^{j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t} = \\ &= \sum_{n=-\infty}^{\infty} \frac{1}{T_0} \cdot X\left(\frac{n}{T_0}\right) \cdot e^{j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t} = \\ &= \frac{1}{T_0} \cdot \sum_{n=-\infty}^{\infty} X\left(\frac{n}{T_0}\right) \cdot e^{j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t} \end{aligned}$$

da cui è semplice ricavare la trasformata:

$$\begin{aligned} \mathcal{F} x_p(t) &= X_p(f) = \\ &= \int_{-\infty}^{+\infty} x_p(t) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\ &= \int_{-\infty}^{+\infty} \left(\frac{1}{T_0} \cdot \sum_{n=-\infty}^{\infty} X\left(\frac{n}{T_0}\right) \cdot e^{j \cdot 2 \cdot \pi \cdot \frac{n}{T_0} \cdot t} \right) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot t} dt = \\ &= \frac{1}{T_0} \cdot \sum_{n=-\infty}^{\infty} X\left(\frac{n}{T_0}\right) \cdot \int_{-\infty}^{+\infty} e^{-j \cdot 2 \cdot \pi \cdot \left(f - \frac{n}{T_0}\right) \cdot t} dt = \\ &= \frac{1}{T_0} \cdot \sum_{n=-\infty}^{\infty} X\left(\frac{n}{T_0}\right) \cdot \delta\left(f - \frac{n}{T_0}\right) = \\ &= f_0 \cdot \sum_{n=-\infty}^{\infty} X(n \cdot f_0) \cdot \delta(f - n \cdot f_0) \end{aligned}$$

Considerazioni Dai calcoli fatti la trasformata di Fourier di un segnale periodico è la somma di infinite delta di Dirac di ampiezza pari all'ampiezza della trasformata del segnale che viene ripetuto nel tempo.

Esempio Si consideri un segnale periodico $x_p(t)$ ricavato dalla ripetizione, con periodo T_0 , di forme d'onda rettangolari:

$$x_p(t) = \sum_{n=-\infty}^{\infty} \text{rect}(t - n \cdot T_0)$$

allora si ha che:

$$\mathcal{F} x_p(t) = \frac{1}{T_0} \cdot \sum_{n=-\infty}^{\infty} \text{sinc}\left(\frac{n}{T_0}\right) \cdot \delta\left(f - \frac{n}{T_0}\right)$$

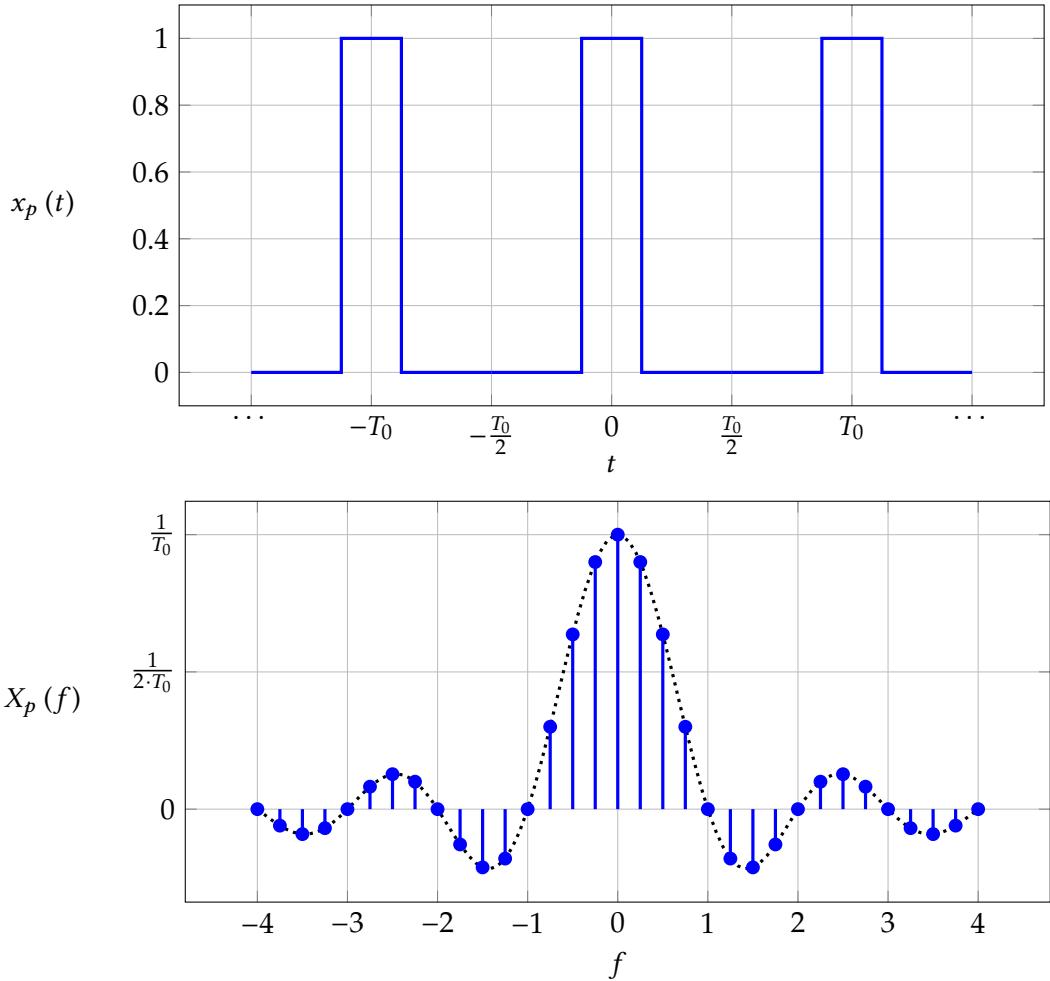


Figura 10.2.: Trasformata della ripetizione di segnali rettangolari.

10.3. Notazione geometrica delle forme d'onda

Definizione di forma d'onda limitata nel tempo Una forma d'onda $s(t)$ si definisce limitata nel tempo se esiste T tale che:

$$\begin{aligned} s(t) &= 0 \\ \forall t > T \end{aligned}$$

Definizione di prodotto interno tra forme d'onda Siano $s_1(t)$ e $s_2(t)$ due forme d'onda limitate nel tempo allora si definisce prodotto interno:

$$\langle s_1(t), s_2(t) \rangle = \int_{-\infty}^{+\infty} s_1(t) \cdot s_2(t) dt$$

Definizione di ortogonalità Due forme d'onda $s_1(t)$ e $s_2(t)$ limitate nel tempo si dicono ortogonali se:

$$\langle s_1(t), s_2(t) \rangle = 0$$

Definizione di norma di una forma d'onda Data una forma d'onda $s(t)$ si definisce norma il valore:

$$\sqrt{\langle s(t), s(t) \rangle} = \sqrt{\int_{-\infty}^{+\infty} s(t)^2 dt} = \sqrt{E}$$

dove E è l'energia della forma d'onda.

Definizione di distanza di due forme d'onda Siano $s_1(t)$ e $s_2(t)$ due forme d'onda limitate nel tempo, allora si definisce la distanza tra $s_1(t)$ e $s_2(t)$ come segue:

$$\begin{aligned} d(s_1(t), s_2(t)) &= \sqrt{\int_{-\infty}^{+\infty} (s_1(t) - s_2(t))^2 dt} = \\ &= \sqrt{\langle s_1(t) - s_2(t), s_1(t) - s_2(t) \rangle} \end{aligned}$$

ossia la norma della differenza delle due forme d'onda.

Definizione di normalità Una forma d'onda $s(t)$ limitata nel tempo si dice normale se ha norma unitaria, ossia se ha energia unitaria.

Definizione di ortonormalità Due forme d'onda $s_1(t)$ e $s_2(t)$ limitate nel tempo si dicono ortonormali se sono ortogonali tra loro ed entrambe normali, ossia:

$$\langle s_1(t), s_2(t) \rangle = 0$$

$$\langle s_1(t), s_1(t) \rangle = 1$$

$$\langle s_2(t), s_2(t) \rangle = 1$$

Definizione di base ortonormale Un insieme $\{s_1(t), s_2(t), \dots, s_v(t)\}$ di forme d'onda limitate si dice base ortonormale v -dimensionale se le varie forme d'onda sono ortonormali fra di loro, ossia:

$$\langle s_i(t), s_j(t) \rangle = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

Rappresentazione vettoriale delle forme d'onda Dato un insieme $\{s_1(t), s_2(t), \dots, s_N(t)\}$ di N forme d'onda limitate nel tempo, questo ammette rappresentazione vettoriale se esiste una base ortonormale $\{\varphi_1(t), \varphi_2(t), \dots, \varphi_v\}$ tale che:

$$\forall s_i(t) \exists \underline{S}_i = (S_{i1}, \dots, S_{iv}) \text{ tale che } s_i(t) = \sum_{k=1}^v S_{ik} \cdot \varphi_k(t)$$

quindi se ad ogni forma d'onda $s_i(t)$ si può associare un vettore \underline{S}_i v -dimensionale.

Osservazione Grazie alla rappresentazione vettoriale si ottiene che:

$$\begin{aligned}
 \langle s_x(t), s_y(t) \rangle &= \int_{-\infty}^{+\infty} s_x(t) \cdot s_y(t) dt = \\
 &= \int_{-\infty}^{+\infty} \left[\sum_{k=1}^v S_{xk} \cdot \varphi_k(t) \right] \cdot \left[\sum_{j=1}^v S_{yj} \cdot \varphi_j(t) \right] dt = \\
 &= \int_{-\infty}^{+\infty} \sum_{k=1}^v \sum_{j=1}^v [(S_{xk} \cdot \varphi_k(t)) \cdot (S_{yj} \cdot \varphi_j(t))] dt = \\
 &= \sum_{k=1}^v \sum_{j=1}^v S_{xk} \cdot S_{yj} \cdot \left[\int_{-\infty}^{+\infty} \varphi_k(t) \cdot \varphi_j(t) dt \right] = \\
 &= \sum_{k=1}^v \sum_{j=1}^v S_{xk} \cdot S_{yj} \cdot \langle \varphi_k(t), \varphi_j(t) \rangle
 \end{aligned}$$

Dato che la base è ortonormale il prodotto interno $\langle \varphi_k(t), \varphi_j(t) \rangle$ è uguale a 1 se $k = j$ e 0 altrimenti, si ottiene:

$$\langle s_x(t), s_y(t) \rangle = \sum_{k=1}^v S_{xk} \cdot S_{yk}$$

che è il prodotto scalare tra i vettori \underline{s}_x e \underline{s}_y . Questo permette di comprendere meglio le definizioni date precedentemente dato che il prodotto interno tra due forme d'onda corrisponde al prodotto scalare tra i loro corrispettivi vettori nella rappresentazione geometrica, infatti:

- Norma: $|S_x|^2 = |S_x \cdot S_x| = \langle s_x(t), s_x(t) \rangle = E^2$
- Distanza: $d(\underline{s}_x, \underline{s}_y)^2 = |\underline{s}_x - \underline{s}_y|^2 = \langle s_x(t) - s_y(t), s_x(t) - s_y(t) \rangle$

Componenti del vettore associato a una forma d'onda Di un vettore si può ottenere il valore della componente parallela rispetto ad un altro vettore facendo il prodotto scalare tra i due. Dato che il prodotto scalare corrisponde al prodotto interno si ha che la componente S_{xk} parallela a $\varphi_k(t)$ appartenente alla base vale:

$$S_{xk} = \langle s_x(t), \varphi_k(t) \rangle = \int_{-\infty}^{+\infty} s_x(t) \cdot \varphi_k(t) dt$$

e quindi si ha che:

$$\begin{aligned}
 s_x(t) &= \sum_{k=1}^v S_{xk} \cdot \varphi_k(t) = \\
 &= \sum_{k=1}^v \langle s_x(t), \varphi_k(t) \rangle \cdot \varphi_k(t)
 \end{aligned}$$

Determinazione della base ortonormale Tutto questo è possibile solo se esiste la base ortonormale; tramite il procedimento di ortogonalizzazione di Gram-Schmidt si può dimostrare che la base ortonormale esiste sempre ed è al più N -dimensionale. Tale costruzione si svolge iterativamente:

$$\varphi_1(t) = \frac{s_1(t)}{\sqrt{E}} = \frac{s_1(t)}{\sqrt{\langle s_1(t), s_1(t) \rangle}}$$

è la funzione associata al versore del vettore associato alla prima forma d'onda. La forma d'onda $s_2(t)$ si può scomporre in due forme d'onda: $s_{2\parallel}(t)$ parallela a $\varphi_1(t)$ e $s_{2\perp}(t)$ ortogonale.

$$s_2(t) = s_{2\parallel}(t) + s_{2\perp}(t)$$

La componente parallela si può ricavare tramite il prodotto interno:

$$s_{2\parallel}(t) = \langle s_2(t), \varphi_1(t) \rangle \cdot \varphi_1(t)$$

e quindi si ha che la componente ortogonale vale:

$$s_{2\perp}(t) = s_2(t) - s_{2\parallel}(t)$$

se tale componente non è nulla si assegna:

$$\begin{aligned} \varphi_2(t) &= \frac{s_{2\perp}(t)}{\sqrt{\langle s_{2\perp}(t), s_{2\perp}(t) \rangle}} = \\ &= \frac{s_2(t) - s_{2\parallel}(t)}{\sqrt{\langle s_2(t) - s_{2\parallel}(t), s_2(t) - s_{2\parallel}(t) \rangle}} \end{aligned}$$

Se invece la componente ortogonale è nulla si prosegue alla terza forma d'onda senza aggiungere elementi alla base.

Tale procedimento si può generalizzare per l' x -esimo passo:

- Si scomponete la forma d'onda $s_x(t)$ nella sua componente parallela e ortogonale con $\varphi_1(t)$.
- Si scomponete la componente ortogonale ottenuta nella sua componente parallela e ortogonale con le successive forme d'onda di base e si procede in questo modo finché la componente ortogonale ottenuta è nulla o sono finite le forme d'onda di base.
- Se la componente ortogonale ottenuta è nulla non si fa nulla e si passa alla $s_{x+1}(t)$, altrimenti si aggiunge alla base la forma d'onda:

$$\varphi(t) = \frac{s_{x\perp}(t)}{\sqrt{\langle s_{x\perp}(t), s_{x\perp}(t) \rangle}}$$

Si può notare che questa procedura si ripete N volte e a ogni passo si aggiunge al più una forma d'onda alla base e quindi alla fine nella base ci saranno al più N forme d'onda ortonormali.

10.4. Canali di trasmissione

10.4.1. Introduzione

Idealmente, un canale di trasmissione dovrebbe essere in grado di trasferire una tensione (o una corrente) da un punto «trasmettitore» ad un altro punto «ricevitore» senza alcuna perdita. Analizzando i canali di trasmissione si può però scoprire che essi sono ben lontani dall'idealità: una coppia di fili per esempio, può essere modellizzata come rappresentato in figura 10.3, dove la resistenza R modellizza la resistenza del filo, mentre C è la capacità parassita che viene a trovarsi tra i due fili, essendo effettivamente conduttori separati da un isolante.

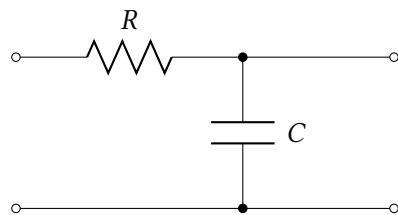


Figura 10.3.: Modellizzazione di una coppia di fili.

È quindi necessaria una modellizzazione completa di un canale di trasmissione per potere capire come i segnali che viaggiano su di esso verranno influenzati prima di arrivare al ricevitore; per fare ciò i canali di trasmissione vengono descritti tramite sistemi Lineari Tempo Invarianti (LTI). Uno schema a blocchi generale è riportato in figura 10.4.

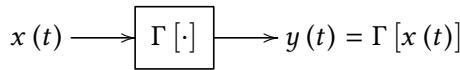


Figura 10.4.: Schema a blocchi di un sistema LTI.

10.4.2. Sistemi LTI

Introduzione Un sistema LTI è un sistema che dato in ingresso una forma d'onda $x(t)$ ne restituisce in uscita una $y(t)$ calcolabile tramite l'applicazione di una trasformazione Γ , ossia:

$$y(t) = \Gamma[x(t)]$$

dove la trasformazione Γ possiede le seguenti proprietà:

- Γ è lineare ossia:

$$\Gamma[\alpha \cdot x_1(t) + \beta \cdot x_2(t)] = \alpha \cdot \Gamma[x_1(t)] + \beta \cdot \Gamma[x_2(t)]$$

- Γ è tempo invariante ossia:

$$\Gamma[x(t - t_0)] = y(t - t_0)$$

cioè la risposta non dipende dall'istante in cui il sistema è eccitato.

Descrizione tramite risposta all'impulso Un sistema LTI può essere descritto esaustivamente dalla forma d'onda $h(t)$ risposta dell'impulso, ossia:

$$h(t) = \Gamma[\delta(t)]$$

Considerando una forma d'onda generica $x(t)$, per le proprietà della delta di Dirac si ha che:

$$x(t) = \int_{-\infty}^{+\infty} x(\tau) \cdot \delta(t - \tau) d\tau$$

e quindi, dato che Γ è lineare, si ha:

$$\begin{aligned} y(t) &= \Gamma[x(t)] = \\ &= \Gamma \left[\int_{-\infty}^{+\infty} x(\tau) \cdot \delta(t - \tau) d\tau \right] = \\ &= \int_{-\infty}^{+\infty} x(\tau) \cdot \Gamma[\delta(t - \tau)] d\tau \end{aligned}$$

Dato che Γ è tempo invariante:

$$\begin{aligned} y(t) &= \int_{-\infty}^{+\infty} x(\tau) \cdot h(t - \tau) d\tau = \\ &= [x * h](t) \end{aligned}$$

Esempio di sistema LTI Si consideri un sistema LTI con risposta all'impulso:

$$h(t) = \text{rect}\left(\frac{t - T/2}{T}\right) = \begin{cases} 1 & 0 \leq t \leq T \\ 0 & \text{altrimenti} \end{cases}$$

allora la risposta allo scalino $x(t) = \text{sca}(t)$ è:

$$\begin{aligned} y(t) &= [x * h](t) = \\ &= \int_{-\infty}^{+\infty} x(t - \tau) \cdot h(\tau) d\tau = \\ &= \int_{-\infty}^{+\infty} \text{sca}(t - \tau) \cdot \text{rect}\left(\frac{t - T/2}{T}\right) d\tau = \\ &= \int_{-\infty}^t \text{rect}\left(\frac{t - T/2}{T}\right) d\tau \end{aligned}$$

Per risolvere questa integrale si possono distinguere i 3 casi in cui:

- Se $t < 0$ allora la funzione d'integrazione è nulla su tutto l'intervallo e quindi:

$$y(t) = 0$$

- Se $0 < t < T$ allora:

$$\begin{aligned} y(t) &= \int_{-\infty}^t \text{rect}\left(\frac{\tau - T/2}{T}\right) d\tau = \\ &= \int_0^t 1 d\tau = \\ &= t \end{aligned}$$

- Se $t > T$ allora:

$$\begin{aligned} y(t) &= \int_{-\infty}^t \text{rect}\left(\frac{\tau - T/2}{T}\right) d\tau = \\ &= \int_0^T 1 d\tau = \\ &= T \end{aligned}$$

e quindi si ottiene:

$$y(t) = \begin{cases} 0 & t < 0 \\ t & 0 \leq t \leq T \\ T & t > T \end{cases}$$

Calcolo della risposta all'impulso del circuito RC Per prima cosa bisogna ricavare la risposta all'impulso $h(t)$ di un circuito RC; durante l'impulso il condensatore si carica a:

$$Q = \int \frac{x(t)}{R} dt = \frac{1}{R}$$

e quindi raggiunge una tensione pari a:

$$\begin{aligned} Q &= C \cdot y(0) \\ \frac{1}{R} &= C \cdot y(0) \\ \frac{1}{R \cdot C} &= y(0) \end{aligned}$$

dopodiché il condensatore inizia a scaricarsi con una corrente $i(t)$ e tramite il bilancio delle correnti sul nodo di uscita si ottiene:

$$\frac{x(t) - y(t)}{R} = C \cdot \frac{d}{dt} y(t)$$

che è una equazione differenziale in cui la tensione $x(t) = 0$ e quindi:

$$\begin{aligned} \frac{0 - y(t)}{R} &= C \cdot \frac{d}{dt} y(t) \\ y(t) &= -R \cdot C \cdot \frac{d}{dt} y(t) \\ y(t) &= \text{sca}(t) \cdot y(0) \cdot e^{-\frac{t}{R \cdot C}} \\ y(t) &= \text{sca}(t) \cdot \frac{1}{R \cdot C} \cdot e^{-\frac{t}{R \cdot C}} \end{aligned}$$

e quindi:

$$h(t) = \text{sca}(t) \cdot \frac{1}{R \cdot C} \cdot e^{-\frac{t}{R \cdot C}}$$

Calcolo della risposta allo scalino del circuito RC Se si vuole calcolare la risposta a uno scalino $x(t) = \text{sca}(t)$ si ottiene:

$$\begin{aligned} y(t) &= [x * h](t) = \\ &= \int_{-\infty}^{+\infty} x(t - \tau) \cdot h(\tau) d\tau = \\ &= \int_{-\infty}^{+\infty} \text{sca}(t - \tau) \cdot \text{sca}(\tau) \cdot \frac{1}{R \cdot C} \cdot e^{-\frac{\tau}{R \cdot C}} d\tau = \\ &= \int_{-\infty}^t \text{sca}(\tau) \cdot \frac{1}{R \cdot C} \cdot e^{-\frac{\tau}{R \cdot C}} d\tau = \\ &= \frac{1}{R \cdot C} \cdot \int_{-\infty}^t \text{sca}(\tau) \cdot e^{-\frac{\tau}{R \cdot C}} d\tau \end{aligned}$$

Per risolvere questa integrale si possono distinguere i 2 casi in cui:

10. Segnali

- Se $t < 0$ allora la funzione è nulla in tutto l'intervallo di integrazione e quindi:

$$\begin{aligned} y(t) &= \frac{1}{R \cdot C} \cdot \int_{-\infty}^t \text{sca}(\tau) \cdot e^{-\frac{\tau}{R \cdot C}} d\tau = \\ &= \frac{1}{R \cdot C} \cdot 0 = \\ &= 0 \end{aligned}$$

- Se $t > 0$ allora:

$$\begin{aligned} y(t) &= \frac{1}{R \cdot C} \cdot \int_{-\infty}^t \text{sca}(\tau) \cdot e^{-\frac{\tau}{R \cdot C}} d\tau = \\ &= \frac{1}{R \cdot C} \cdot \int_0^t e^{-\frac{\tau}{R \cdot C}} d\tau = \\ &= \frac{1}{R \cdot C} \cdot \left[-R \cdot C \cdot e^{-\frac{\tau}{R \cdot C}} \right]_0^t = \\ &= -e^{-\frac{t}{R \cdot C}} + 1 \end{aligned}$$

che è la normale funzione della carica di un condensatore.

$$y(t) = \text{sca}(t) \cdot \left(1 - e^{-\frac{t}{R \cdot C}} \right)$$

Calcolo della risposta al rettangolo del circuito RC Si vuole ricavare la risposta al rettangolo

$$x(t) = \text{rect}\left(\frac{t - T/2}{T}\right)$$

del circuito RC. Per poterlo fare si può notare che:

$$x(t) = \text{rect}\left(\frac{t - T/2}{T}\right) = \text{sca}(t) - \text{sca}(t - T)$$

e dato che la risposta allo scalino è stata ricavata nel paragrafo precedente e che il sistema è lineare si ha:

$$\begin{aligned} y(t) &= \text{sca}(t) \cdot \left(1 - e^{-\frac{t}{R \cdot C}} \right) - \text{sca}(t - T) \cdot \left(1 - e^{-\frac{t-T}{R \cdot C}} \right) = \\ &= \begin{cases} 0 & t < 0 \\ 1 - e^{-\frac{t}{R \cdot C}} & 0 \leq t < T \\ 1 - e^{-\frac{t}{R \cdot C}} - 1 + e^{-\frac{t-T}{R \cdot C}} & t \geq T \end{cases} = \\ &= \begin{cases} 0 & t < 0 \\ 1 - e^{-\frac{t}{R \cdot C}} & 0 \leq t < T \\ e^{-\frac{t-T}{R \cdot C}} - e^{-\frac{t}{R \cdot C}} & t \geq T \end{cases} \end{aligned}$$

Da questo risultato si nota che se $R \cdot C \gg T$ il condensatore non riesce a caricarsi e quindi ad arrivare a 1, viceversa se $R \cdot C \ll T$ allora l'uscita ha un andamento molto simile a quello del rettangolo in ingresso, solo leggermente smussato.

10.4.3. Risposta in frequenza dei sistemi LTI

Risposta di un sistema LTI a un esponenziale complesso Si consideri un generico sistema LTI con risposta all'impulso $h(t)$, allora si può ricavare la risposta a un esponenziale complesso generico:

$$x(t) = A \cdot e^{j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta)}$$

e si può ricavare per convoluzione:

$$\begin{aligned} y(t) &= [x * h](t) = \\ &= A \cdot \int_{-\infty}^{+\infty} h(\tau) \cdot e^{j \cdot (2 \cdot \pi \cdot f \cdot (t - \tau) + \vartheta)} d\tau = \\ &= A \cdot \int_{-\infty}^{+\infty} h(\tau) \cdot e^{j \cdot 2 \cdot \pi \cdot f \cdot (t - \tau)} \cdot e^{j \cdot \vartheta} d\tau = \\ &= A \cdot e^{j \cdot \vartheta} \cdot e^{j \cdot 2 \cdot \pi \cdot f \cdot t} \cdot \int_{-\infty}^{+\infty} h(\tau) \cdot e^{-j \cdot 2 \cdot \pi \cdot f \cdot \tau} d\tau = \\ &= A \cdot e^{j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta)} \cdot [\mathcal{F} h(t)] = \\ &= x(t) \cdot [\mathcal{F} h(t)] \end{aligned}$$

Chiamando $H(f) = \mathcal{F} h(t)$ si ottiene che:

$$\begin{aligned} y(t) &= x(t) \cdot H(f) = \\ &= A \cdot e^{j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta)} \cdot |H(f)| \cdot e^{j \cdot \angle H(f)} = \\ &= A \cdot |H(f)| \cdot e^{j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta + \angle H(f))} \end{aligned}$$

Quindi la risposta ad un esponenziale complesso è un altro esponenziale complesso con la stessa frequenza che ha subito le seguenti variazioni:

- È amplificato di un fattore $|H(f)|$.
- È sfasato di un fattore $\angle H(f)$.

Inoltre dato che $h(t) \in \mathbb{R}$ si ha che:

- $|H(f)| = |H(-f)|$.
- $\angle H(f) = -\angle H(-f)$.

Risposta di un sistema LTI ad una cosinusoide Si consideri la cosinusoide generica:

$$x(t) = A \cdot \cos(2 \cdot \pi \cdot f \cdot t + \vartheta)$$

allora per le formule di Eulero si ricava che:

$$\begin{aligned} x(t) &= A \cdot \cos(2 \cdot \pi \cdot f \cdot t + \vartheta) = \\ &= \frac{A}{2} \cdot [e^{j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta)} + e^{-j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta)}] = \\ &= \frac{A}{2} \cdot [e^{j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta)} + e^{j \cdot (2 \cdot \pi \cdot (-f) \cdot t - \vartheta)}] \end{aligned}$$

Dato che i sistemi LTI sono lineari la risposta alla cosinusoide può essere vista come la somma dei contributi dati dalle due esponenziali e quindi:

$$\begin{aligned} y(t) &= \frac{A}{2} \cdot [|H(f)| \cdot e^{j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta + \angle H(f))} + |H(-f)| \cdot e^{j \cdot (2 \cdot \pi \cdot (-f) \cdot t - \vartheta + \angle H(-f))}] = \\ &= \frac{A}{2} \cdot |H(f)| \cdot [e^{j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta + \angle H(f))} + e^{-j \cdot (2 \cdot \pi \cdot f \cdot t + \vartheta + \angle H(f))}] = \\ &= A \cdot |H(f)| \cdot \cos(2 \cdot \pi \cdot f \cdot t + \vartheta + \angle H(f)) \end{aligned}$$

ossia la risposta è una cosinusoide con la stessa frequenza ma che ha subito le seguenti variazioni:

- È amplificato di un fattore $|H(f)|$.
- È sfasato di un fattore $\angle H(f)$.

Risposta a un segnale generico Sia $x(t)$ una forma d'onda generica con trasformata $X(f)$ e Γ un sistema LTI, allora si ha che la risposta alla forma d'onda $x(t)$ del sistema LTI Γ vale:

$$\begin{aligned} y(t) &= \Gamma[x(t)] = \\ &= \Gamma \left[\int_{-\infty}^{+\infty} X(f) \cdot e^{j \cdot 2 \cdot \pi \cdot f \cdot t} df \right] \end{aligned}$$

dato che Γ è lineare si ha che:

$$\begin{aligned} y(t) &= \int_{-\infty}^{+\infty} \Gamma[X(f) \cdot e^{j \cdot 2 \cdot \pi \cdot f \cdot t}] df = \\ &= \int_{-\infty}^{+\infty} X(f) \cdot \Gamma[e^{j \cdot 2 \cdot \pi \cdot f \cdot t}] df = \\ &= \int_{-\infty}^{+\infty} X(f) \cdot e^{j \cdot 2 \cdot \pi \cdot f \cdot t} \cdot H(f) df = \\ &= \int_{-\infty}^{+\infty} X(f) \cdot H(f) \cdot e^{j \cdot 2 \cdot \pi \cdot f \cdot t} df \end{aligned}$$

e quindi $y(t)$ è l'antitrasformata del prodotto $X(f) \cdot H(f)$ e quindi si ha che:

$$Y(f) = X(f) \cdot H(f)$$

come si poteva immaginare dato che la trasformata della convoluzione è il prodotto delle trasformate.

Osservazione Si può notare che lavorando nel dominio delle frequenze i calcoli nei sistemi LTI diventano molto più semplici dato che la convoluzione diventa un semplice prodotto.

10.5. Processi casuali

10.5.1. Definizione

Definizione Un processo casuale è un segnale $x(t)$, variabile nel tempo, la cui ampiezza ad ogni istante è una variabile casuale. Possono quindi essere visti come una collezione di possibili realizzazioni di cui si possono descrivere le caratteristiche comuni.

Stazionarietà Per semplicità solitamente vengono usati processi stazionari, ossia processi in cui la distribuzione di probabilità e le varie statistiche (valore atteso e varianza) non variano nel tempo.

Osservazione I processi casuali sono usati per rappresentare il rumore casuale che si sovrappone ad una forma d'onda deterministica.

10.5.2. Densità di probabilità

La densità di probabilità dell'ampiezza del processo è una caratteristica fondamentale per descrivere il processo. Teoricamente può essere usata qualsiasi distribuzione, ma ingegneristicamente sono rilevanti solo la distribuzione gaussiana e la distribuzione uniforme.

Ogni distribuzione è caratterizzata da un valore atteso e da una varianza che sono funzioni del tempo, ma in genere si ha che:

$$\mathbb{E}[x(t)] = 0$$

Densità di probabilità gaussiana La funzione di probabilità gaussiana è definita a partire dalla sua media e dalla sua varianza; dato che si suppone che il valore atteso sia nullo allora data una varianza σ^2 si ha che:

$$p_{x(t)}(\alpha) = \frac{1}{\sqrt{2 \cdot \pi \cdot \sigma^2}} \cdot e^{-\frac{\alpha^2}{2 \cdot \sigma^2}}$$

Il parametro σ rappresenta la dispersione della campana, infatti si ha che:

- Nell'intervallo $[-\sigma, +\sigma]$ è presente circa il 68% della massa di probabilità complessiva.
- Nell'intervallo $[-2 \cdot \sigma, +2 \cdot \sigma]$ è presente circa il 95% della massa di probabilità complessiva.

In una variabile gaussiana si ha che:

$$P(a < \alpha < b) = \int_a^b \frac{1}{\sqrt{2 \cdot \pi \cdot \sigma^2}} \cdot e^{-\frac{\alpha^2}{2 \cdot \sigma^2}} d\alpha$$

che è un integrale che dipende da 3 valori a , b e σ e non è risolvibile analiticamente. Per questo motivo si definisce la funzione $Q(x)$:

$$Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2 \cdot \pi}} \cdot e^{-\frac{\alpha^2}{2}} d\alpha$$

i cui valori sono calcolati numericamente e tabulati. Sfruttando la $Q(x)$ è possibile calcolare il valore di $P(a < \alpha < b)$; attuando il cambio di variabile:

$$\begin{aligned} t &= \frac{\alpha}{\sigma} \\ dt &= \frac{d\alpha}{\sigma} \\ t_a &= \frac{a}{\sigma} \\ t_b &= \frac{b}{\sigma} \end{aligned}$$

si ottiene:

$$\begin{aligned}
 P(a < \alpha < b) &= \int_a^b \frac{1}{\sqrt{2 \cdot \pi \cdot \sigma^2}} \cdot e^{-\frac{\alpha^2}{2 \cdot \sigma^2}} d\alpha = \\
 &= \int_{a/\sigma}^{b/\sigma} \frac{1}{\sqrt{2 \cdot \pi \cdot \sigma^2}} \cdot e^{-\frac{t^2}{2}} \cdot \sigma dt = \\
 &= \int_{a/\sigma}^{b/\sigma} \frac{1}{\sqrt{2 \cdot \pi}} \cdot e^{-\frac{t^2}{2}} dt = \\
 &= \int_{a/\sigma}^{+\infty} \frac{1}{\sqrt{2 \cdot \pi}} \cdot e^{-\frac{t^2}{2}} dt - \int_{b/\sigma}^{+\infty} \frac{1}{\sqrt{2 \cdot \pi}} \cdot e^{-\frac{t^2}{2}} dt = \\
 &= Q\left(\frac{a}{\sigma}\right) - Q\left(\frac{b}{\sigma}\right)
 \end{aligned}$$

Densità di probabilità uniforme La densità di probabilità uniforme è caratterizzata da un intervallo compatto in cui la probabilità è costante diversa da 0 mentre per tutti gli altri valori la funzione è nulla.

Dato che il valore atteso è nullo la densità di probabilità uniforme è definita a partire dalla larghezza Δ dell'intervallo:

$$p_{x(t)}(\alpha) = \begin{cases} \frac{1}{\Delta} & \text{se } |\alpha| < \frac{\Delta}{2} \\ 0 & \text{altrimenti} \end{cases}$$

da cui si può ricavare la varianza:

$$\begin{aligned}
 \sigma^2 &= \int_{-\infty}^{+\infty} \alpha^2 \cdot \rho(\alpha) d\alpha = \\
 &= \int_{-\Delta/2}^{\Delta/2} \alpha^2 \cdot \frac{1}{\Delta} d\alpha = \\
 &= \frac{1}{\Delta} \cdot \left[\frac{\alpha^3}{3} \right]_{-\Delta/2}^{\Delta/2} = \\
 &= \frac{1}{3 \cdot \Delta} \cdot \left[\frac{\Delta^3}{8} + \frac{\Delta^3}{8} \right] = \\
 &= \frac{1}{3 \cdot \Delta} \cdot \frac{\Delta^3}{4} = \\
 &= \frac{\Delta^2}{12}
 \end{aligned}$$

Confronto

- La distribuzione uniforme è usata nei casi in cui si conosce un limite fisico per cui si sa che il segnale non può andare oltre certi limiti, ma non si conosce nessuna caratteristica del segnale che renda più probabili certi valori rispetto ad altri.
- La distribuzione gaussiana è usata quando si ha un valore più probabile e la probabilità diminuisce allontanandosi da quel valore, ma tutti i valori sono comunque possibili.

10.5.3. Funzione di autocorrelazione

Definizione Dato un processo $x(t)$ si definisce la funzione di autocorrelazione come:

$$R_x(t_1, t_2) = \mathbb{E}[x(t_1) \cdot x(t_2)]$$

dato che i valori attesi sono assunti nulli la funzione di autocorrelazione corrisponde alla covarianza tra due distribuzioni prese agli istanti t_1 e t_2 . Per l'ipotesi di stazionarietà la funzione $R_x(t_1, t_2)$ dipende solo dalla distanza tra i due istanti e quindi si può esprimere:

$$R_x(\tau) = \mathbb{E}[x(t) \cdot x(t + \tau)]$$

Osservazione Si può notare che:

$$R_x(0) = \mathbb{E}[x(t) \cdot x(t)] = \sigma_x^2$$

Ergodicità Un processo si dice ergodico se le statistiche temporali su una singola realizzazione coincidono con quelle del processo per ogni realizzazione, ossia:

$$\begin{aligned} & \underbrace{\lim_{T \rightarrow \infty} \frac{1}{T} \cdot \int_{-T/2}^{T/2} x(t) dt}_{\text{media temporale}} = \underbrace{\mathbb{E}[x(t)]}_{\text{media delle realizzazioni}} \\ & \underbrace{\lim_{T \rightarrow \infty} \frac{1}{T} \cdot \int_{-T/2}^{T/2} x(t) \cdot x(t + \tau) dt}_{\text{correlazione temporale}} = \underbrace{\mathbb{E}[x(t) \cdot x(t + \tau)]}_{\text{correlazione nelle realizzazioni}} \end{aligned}$$

Osservazione In un processo ergodico si può notare che:

$$\lim_{T \rightarrow \infty} \frac{1}{T} \cdot \int_{-T/2}^{T/2} x(t)^2 dt = \mathbb{E}[x(t)^2] = R_x(0)$$

e quindi la potenza media del segnale è data da $R_x(0)$.

Proprietà della funzione di autocorrelazione

$$R_x(\tau) = R_x(-\tau)$$

$$R_x(0) = \sigma_x^2 = P \geq 0$$

$$|R_x(\tau)| \leq R_x(0)$$

10.5.4. Funzione di densità di potenza spettrale

Concetto La funzione di densità di potenza spettrale $S_x(f)$ è una funzione che vuole esprimere come la potenza si distribuisce sulle varie frequenze del processo. Per questo motivo una prima proprietà che questa funzione deve avere è che l'integrale in tutto il dominio dia tutta la potenza del segnale e quindi:

$$\int_{-\infty}^{+\infty} S_x(f) df = P = R_x(0)$$

Una funzione con questa proprietà è la trasformata di Fourier della funzione di autocorrelazione:

$$S_x(f) = \mathcal{F} R_x(f)$$

Definizione La funzione di densità spettrale di potenza $S_x(f)$ è la trasformata di Fourier della funzione di autocorrelazione del processo casuale.

10.5.5. Processi casuali bianchi

Definizione Un processo casuale x si dice bianco se:

$$S_x(f) = \frac{N_0}{2}$$

ossia se la sua funzione di densità spettrale è costante.

Funzione di autocorrelazione Conoscendo la funzione di densità spettrale si può ricavare la funzione di autocorrelazione:

$$\begin{aligned} R_x(\tau) &= \mathcal{F}^{-1} S_x(f) = \\ &= \mathcal{F}^{-1} \frac{N_0}{2} = \\ &= \frac{N_0}{2} \cdot \delta(\tau) \end{aligned}$$

questo significa che ad ogni istante la variabile casuale è indipendente da tutti gli altri istanti temporali.

Osservazione Si può notare che questo processo ha potenza infinita e quindi non è realizzabile, ma è comunque un'ottima approssimazione quando il processo riesce a rimanere bianco per una banda maggiore di quella di tutti gli altri segnali nel sistema.

10.5.6. Processi casuali in un sistema LTI

Introduzione Dato un sistema LTI con $h(t)$ risposta all'impulso e $x(t)$ realizzazione del processo casuale in ingresso, allora l'uscita vale:

$$y(t) = [x * h](t)$$

Dato che $x(t)$ è un processo casuale anche $y(t)$ è un processo casuale; se ne possono ricavare le caratteristiche conoscendo quelle del processo casuale in ingresso.

Valore atteso Se il processo in ingresso ha valore atteso μ_x allora si ha che:

$$\begin{aligned}
 \mu_y &= \mathbb{E}[y(t)] = \\
 &= \mathbb{E}[[x * h](t)] = \\
 &= \mathbb{E}\left[\int_{-\infty}^{+\infty} x(\tau) \cdot h(t - \tau) d\tau\right] = \\
 &= \int_{-\infty}^{+\infty} \mathbb{E}[x(\tau)] \cdot h(t - \tau) d\tau = \\
 &= \int_{-\infty}^{+\infty} \mu_x \cdot h(t - \tau) d\tau = \\
 &= \mu_x \cdot \int_{-\infty}^{+\infty} h(t - \tau) d\tau = \\
 &= \mu_x \cdot \int_{-\infty}^{+\infty} -h(y) dy = \\
 &= \mu_x \cdot \int_{-\infty}^{+\infty} h(y) \cdot e^{-j \cdot 2 \cdot \pi \cdot 0 \cdot y} dy = \\
 &= \mu_x \cdot H(0)
 \end{aligned}$$

Quindi se $\mu_x = 0$ anche μ_y è nullo.

Autocorrelazione Se il processo in ingresso ha funzione di autocorrelazione $R_x(\tau)$ allora si ha che:

$$\begin{aligned}
 R_y(\tau) &= \mathbb{E}[y(t) \cdot y(t + \tau)] = \\
 &= \mathbb{E}[[x * h](t) \cdot [x * h](t + \tau)] = \\
 &= \mathbb{E}\left[\left(\int_{-\infty}^{+\infty} x(t - \alpha) \cdot h(\alpha) d\alpha\right) \cdot \left(\int_{-\infty}^{+\infty} x(t + \tau - \beta) \cdot h(\beta) d\beta\right)\right] = \\
 &= \mathbb{E}\left[\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} x(t - \alpha) \cdot x(t + \tau - \beta) \cdot h(\alpha) \cdot h(\beta) d\beta d\alpha\right] = \\
 &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \mathbb{E}[x(t - \alpha) \cdot x(t + \tau - \beta)] \cdot h(\alpha) \cdot h(\beta) d\beta d\alpha = \\
 &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} R_x(t + \tau - \beta - t + \alpha) \cdot h(\alpha) \cdot h(\beta) d\beta d\alpha = \\
 &= \int_{-\infty}^{+\infty} \left[\int_{-\infty}^{+\infty} R_x(\tau + \alpha - \beta) \cdot h(\beta) d\beta \right] \cdot h(\alpha) d\alpha
 \end{aligned}$$

Ponendo $F(t) = [h * R_x](t)$ si ottiene:

$$R_y(\tau) = \int_{-\infty}^{+\infty} F(\tau + \alpha) \cdot h(\alpha) d\alpha$$

10. Segnali

Dato che $R_x(t)$ è una funzione pari lo è anche $F(t)$ e quindi:

$$\begin{aligned} R_y(\tau) &= \int_{-\infty}^{+\infty} F(-\tau - \alpha) \cdot h(\alpha) d\alpha = \\ &= [F * h](-\tau) \end{aligned}$$

e quindi definendo $h_-(t) = h(-t)$:

$$\begin{aligned} R_y(\tau) &= [F * h_-](\tau) = \\ &= [R_x * h * h_-](\tau) \end{aligned}$$

Densità di potenza spettrale Dato che la densità di potenza spettrale è la trasformata di Fourier della funzione di autocorrelazione si ottiene:

$$\begin{aligned} S_y(f) &= \mathcal{F} R_y(\tau) = \\ &= \mathcal{F} [R_x * h * h_-](\tau) = \\ &= (\mathcal{F} R_x(\tau)) \cdot (\mathcal{F} h(\tau)) \cdot (\mathcal{F} h(-\tau)) = \\ &= S_x(f) \cdot H(f) \cdot H(-f) \end{aligned}$$

Dato che $h(t) \in \mathbb{R}$ si ha che $H(-f) = H(f)^*$ e quindi:

$$S_y(f) = S_x(f) \cdot |H(f)|^2$$

Da questa conclusione si può capire perché la densità spettrale di potenza fornisca un'informazione su come è distribuita la potenza a varie frequenze, infatti prendendo un sistema LTI che fa da filtro passa-banda con una banda Δf intorno alle frequenze f_0 e $-f_0$ molto stretta, ossia come un impulso a quelle frequenze, si ottiene che:

$$S_y(f) = S_x(-f_0) + S_x(f_0)$$

Dato che ci si aspetta che in questo filtro passi solo la potenza sulle frequenze f_0 e $-f_0$ si ha che tale potenza deve essere uguale a $S_x(f_0)$ e che il filtro la sparge su tutte le frequenze.

Funzione di densità di probabilità Si può notare che la variabile casuale in uscita è una combinazione lineare di variabili casuali infatti:

$$y(t) = \int_{-\infty}^{+\infty} x(t) \cdot h(t - \alpha) d\alpha$$

Sapendo questo non si può dire molto sulla funzione di densità di probabilità di y , ma se x è gaussiana allora si può dire che anche y è gaussiana.

I parametri della gaussiana di uscita sono calcolabili come visto precedentemente.

10.5.7. Rappresentazione geometrica

Introduzione Come per le forme d'onda deterministiche esiste una rappresentazione geometrica i cui vettori avranno parametri casuali e per cui valgono le stesse definizioni date precedentemente.

Rappresentazione geometrica Dato un insieme di N processi casuali $\{x_1(t), x_2(t), \dots, x_N(t)\}$, questo ammette rappresentazione vettoriale se esiste una base ortonormale $\{\varphi_1(t), \varphi_2(t), \dots, \varphi_v(t)\}$ tale che:

$$\forall x_i(t) \exists \underline{X}_i = (X_{i1}, \dots, X_{iv}) \text{ tale che } x_i(t) = \sum_{k=1}^v X_{ik} \cdot \varphi_k(t)$$

quindi ad ogni processo casuale $x_i(t)$ si può associare un vettore \underline{X}_i v -dimensionale.

Componenti del vettore Ogni componente del vettore che rappresenta un processo casuale è anch'essa casuale e vale:

$$X_{ik} = \int_{-\infty}^{+\infty} x_i(t) \cdot \varphi_k(t) dt$$

Valore atteso delle componenti Sia μ_i il valore atteso del processo casuale $x_i(t)$, allora si ottiene che:

$$\begin{aligned} \mathbb{E}[X_{ik}] &= \mathbb{E}\left[\int_{-\infty}^{+\infty} x_i(t) \cdot \varphi_k(t) dt\right] = \\ &= \int_{-\infty}^{+\infty} \mathbb{E}[x_i(t)] \cdot \varphi_k(t) dt = \\ &= \mu_i \cdot \int_{-\infty}^{+\infty} \varphi_k(t) dt \end{aligned}$$

quindi se il processo casuale $x_i(t)$ ha valore atteso nullo tutte le sue componenti hanno valore atteso nullo.

Funzione di correlazione Dato il vettore \underline{X}_i che rappresenta il processo casuale $x_i(t)$, si definisce la funzione di correlazione tra due componenti del vettore:

$$R_X(k, j) = \mathbb{E}[X_{ik} \cdot X_{ij}]$$

Funzione di correlazione del vettore associato a un processo bianco Sia $n(t)$ un processo bianco con $R_n(0) = N_0/2$ e $\underline{N} = \{N_1, N_2, \dots, N_v\}$ il vettore associato a $n(t)$, allora si ha che:

$$\begin{aligned} R_N(k, j) &= \mathbb{E}[N_k \cdot N_j] = \\ &= \mathbb{E}\left[\left(\int_{-\infty}^{+\infty} n(\alpha) \cdot \varphi_k(\alpha) d\alpha\right) \cdot \left(\int_{-\infty}^{+\infty} n(\beta) \cdot \varphi_j(\beta) d\beta\right)\right] = \\ &= \mathbb{E}\left[\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} n(\alpha) \cdot \varphi_k(\alpha) \cdot n(\beta) \cdot \varphi_j(\beta) d\beta d\alpha\right] = \\ &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \mathbb{E}[n(\alpha) \cdot n(\beta)] \cdot \varphi_k(\alpha) \cdot \varphi_j(\beta) d\beta d\alpha = \\ &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} R_n(\alpha - \beta) \cdot \varphi_k(\alpha) \cdot \varphi_j(\beta) d\beta d\alpha = \\ &= \int_{-\infty}^{+\infty} \left[\int_{-\infty}^{+\infty} \frac{N_0}{2} \cdot \delta(\alpha - \beta) \cdot \varphi_k(\alpha) d\alpha \right] \cdot \varphi_j(\beta) d\beta = \\ &= \frac{N_0}{2} \cdot \int_{-\infty}^{+\infty} \varphi_k(\beta) \cdot \varphi_j(\beta) d\beta = \\ &= \frac{N_0}{2} \cdot \langle \varphi_k(t), \varphi_j(t) \rangle = \\ &= \begin{cases} \frac{N_0}{2} & \text{se } k = j \\ 0 & \text{se } k \neq j \end{cases} \end{aligned}$$

e quindi il vettore corrispondente ad un processo bianco ha componenti indipendenti tra loro e con varianza pari a quella del processo bianco stesso.

Osservazione Si può dimostrare che per rappresentare un processo bianco bisogna utilizzare una base a dimensione infinita. Questo non crea un problema perché i processi bianchi vengono usati per rappresentare il rumore che si aggiunge ad un segnale deterministico che viene rappresentato in uno spazio v -dimensionale, quindi si possono considerare solo quelle v dimensioni e ignorare le altre dato che non hanno nessun effetto sulla forma d'onda.

11. Trasmissione multicanale

11.1. Trasmissione di un simbolo tramite un canale passa-basso

11.1.1. Introduzione

Problema Si vuole trasmettere un simbolo proveniente da una sorgente $\{1, 2, \dots, M\}$ attraverso un canale passa-basso caratterizzato da un rumore bianco di varianza $N_0/2$.

Forme d'onda Per farlo si deve assegnare una forma d'onda diversa per ogni simbolo della sorgente ottenendo quindi:

$$S = \{s_1(t), s_2(t), \dots, s_M(t)\}$$

Per ragioni pratiche si scelgono sempre forme d'onda finite e quindi queste forme d'onda si possono rappresentare nella notazione vettoriale in uno spazio al più M dimensionale e quindi alla forma d'onda $s_i(t)$ corrisponde il vettore \underline{s}_i . Inoltre queste forme d'onda devono essere di tipo passa-basso con banda inferiore a quella del canale, altrimenti vengono deformate dal canale e il ricevente non riesce ad interpretare correttamente le forme d'onda.

Energie Dato che sono presenti diverse forme d'onda è comodo definire i seguenti parametri:

- E_{s_i} è l'energia della forma d'onda $s_i(t)$.
- E_s è l'energia media delle forme d'onda usate.
- E_b è l'energia media necessaria per trasmettere un bit di informazione.

Ovviamente si desidera trasmettere con una E_b più bassa possibile, ma esistono dei limiti dovuti al rumore del canale.

Effetto del canale Dato che le forme scelte hanno banda inferiore a quella del canale si può supporre che il ricevente legga dal canale la forma d'onda inviata con l'aggiunta del rumore. Chiamando $r(t)$ il segnale letto dal ricevitore e $s_x(t)$ il segnale inviato si ha che:

$$r(t) = s_x(t) + n(t)$$

oppure utilizzando la notazione vettoriale:

$$\underline{R} = \underline{s}_x + \underline{N}$$

dove \underline{N} è il vettore delle componenti utili del rumore bianco, ossia quelle nello spazio vettoriale usato per le forme d'onda definite prima. Tutte le componenti del rumore hanno la stessa varianza $N_0/2$ come dimostrato nelle sezioni precedenti.

Una rappresentazione grafica nel caso con $M = 2$ si può trovare in figura 11.1.

11. Trasmissione multicanale

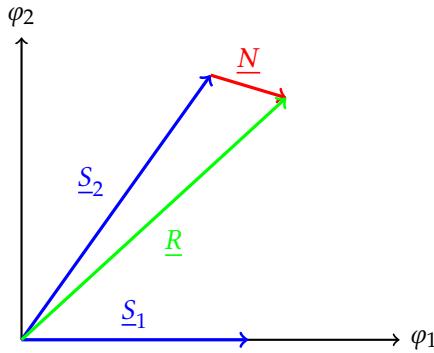


Figura 11.1.: Rappresentazione geometrica del segnale ricevuto nel caso di trasmissione binaria.

La scelta del ricevitore Nella sezione 5.2 sulla codifica di canale si è visto che il ricevitore può prendere una decisione principalmente in due modi:

- Massimizzando la probabilità a posteriori:

$$\hat{S}_{MAP} = \arg \max_{\underline{S}_x \in S} P_{S_T | S_R} (\underline{S}_x | R)$$

- Massimizzando la verosimiglianza:

$$\hat{S}_{ML} = \arg \max_{\underline{S}_x \in S} P_{S_R | S_T} (R | \underline{S}_x)$$

Inoltre si è visto che i due metodi sono equivalenti se le varie forme d'onda vengono trasmesse equiprobabilmente; questa è un'ipotesi che si può considerare corretta dato che tutta la codifica di sorgente è fatta a tale scopo, quindi si possono considerare i ricevitori MAP dato che la probabilità a posteriori è più facile da calcolare. Infatti la probabilità che sia stato inviato un certo segnale \underline{S}_x avendo ricevuto il segnale R corrisponde alla probabilità che il rumore assuma il valore:

$$R - \underline{S}_x = \underline{N}$$

e dato che il rumore è gaussiano si ha che:

$$\begin{aligned} P_{S_T | S_R} (\underline{S}_x | R) &= \frac{1}{\sqrt{2 \cdot \pi \cdot \frac{N_0}{2}}} \cdot e^{-\frac{|R - \underline{S}_x|^2}{2 \cdot \frac{N_0}{2}}} = \\ &= \frac{1}{\sqrt{\pi \cdot N_0}} \cdot e^{-\frac{|R - \underline{S}_x|^2}{N_0}} \end{aligned}$$

Dato che si vuole massimizzare tale probabilità bisogna massimizzare l'esponente della e , e quindi minimizzare il termine $|R - \underline{S}_x|^2$, ma dato che il modulo è sempre positivo si ha che:

$$\hat{S} = \arg \min_{\underline{S}_x \in S} |R - \underline{S}_x|$$

che equivale a scegliere il segnale lecito che è più vicino geometricamente al segnale ricevuto.

Regioni decisionali Dato che il ricevitore sceglie sempre il segnale più vicino geometricamente alla forma d'onda ricevuta questo può dividere lo spazio al più M -dimensionale in M zone, dove ogni zona contiene i punti che sono più vicini ad una certa forma d'onda \underline{S}_i . Tali zone sono sempre facilmente individuabili geometricamente, per esempio se $M = 2$ le due regioni sono divise dalla retta ortogonale all'asse che unisce i due vettori delle forme d'onda, come mostrato in figura 11.2.

11. Trasmissione multicanale

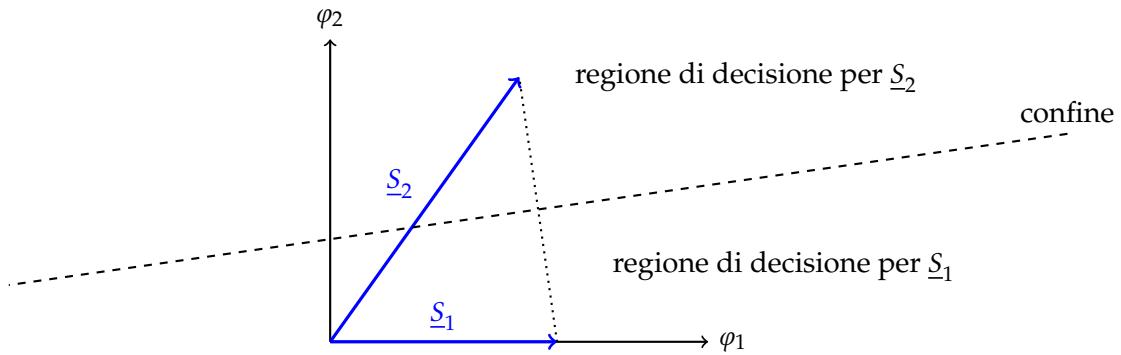


Figura 11.2.: Regioni decisionali di un ricevitore MAP.

Probabilità di errore Il ricevitore MAP sbaglia se il rumore è abbastanza grande da far superare il confine tra le due regioni decisionali. Nella maggior parte dei casi quando il ricevitore sbaglia interpreta il segnale ricevuto come appartenente ad una delle zone decisionali confinanti.

Si consideri il caso in cui si invia la forma d'onda \underline{S}_k , allora la probabilità che il ricevitore lo interpreti come la forma d'onda con regione decisionale confinante \underline{S}_j è pari alla probabilità che il rumore sia abbastanza grande da far superare tale confine.

Il vettore del rumore si può scomporre in due componenti, una parallela al confine (N_{\parallel}) e una ortogonale (N_{\perp}); quest'ultima è la componente che sposta il segnale ricevuto al confine delle regioni decisionali e quindi il ricevitore sbaglia se:

$$N_{\perp} \geq \frac{|\underline{S}_k - \underline{S}_j|}{2}$$

La componente del rumore è distribuita come una gaussiana con varianza pari a quella del rumore (dato che le componenti di un rumore gaussiano bianco hanno la stessa distribuzione del segnale composto) e quindi si ha che la probabilità di sbagliare è pari a:

$$P_{ekj} = P\left(N_{\perp} \geq \frac{|\underline{S}_k - \underline{S}_j|}{2}\right) = Q\left(\frac{\frac{|\underline{S}_k - \underline{S}_j|}{2}}{\sqrt{\frac{N_0}{2}}}\right) = Q\left(\frac{|\underline{S}_k - \underline{S}_j|}{\sqrt{2 \cdot N_0}}\right)$$

da cui si può notare che $P_{ekj} = P_{ejk}$. Supponendo che la regione decisionale di $s_k(t)$ confini con tutte le altre si ha che:

$$P_{ek} = \sum_{\substack{j=1 \\ j \neq k}}^M P_{ekj}$$

Per calcolare la probabilità complessiva si può fare la media di tutte questa probabilità, quindi supponendo che tutti confinino con tutti si ottiene:

$$\begin{aligned} P_e &= \frac{1}{M} \cdot \left[\sum_{k=1}^M P_{ek} \right] = \\ &= \frac{1}{M} \cdot \left[\sum_{k=1}^M \sum_{\substack{j=1 \\ j \neq k}}^M P_{ekj} \right] = \\ &= \frac{2}{M} \cdot \left[\sum_{k=1}^M \sum_{j=k+1}^M P_{ekj} \right] \end{aligned}$$

Analisi sulla probabilità di errore La probabilità di errore dipende quindi da:

- La varianza del rumore bianco: più il rumore è variabile più è alta la probabilità di errore.
- La distanza tra le forme d'onda: più le forme d'onda sono distanti più è bassa la probabilità di errore. Questo si può ottenere in due modi:
 - Allungando i vettori, ma questo comporterebbe l'impiego di maggiore energia.
 - Sfruttando la geometria, ossia aumentando l'angolo tra i vettori.

11.1.2. Trasmissione 2-PAM

Concetto Il sistema 2-PAM (Pulse-Amplitude Modulation) è una tecnica che permette di trasmettere un bit di informazione per simbolo; sfrutta la geometria dei segnali per diminuire la probabilità di errore.

Dato che invia un bit di informazione per simbolo basta definire la forma di due segnali.

Definizione Il sistema scelto è monodimensionale con funzione di base $\varphi(t)$ e con:

$$\begin{aligned} s_0(t) &= \sqrt{E} \cdot \varphi(t) = g(t) \\ s_1(t) &= -\sqrt{E} \cdot \varphi(t) = -g(t) \end{aligned}$$

Quindi si ha che $s_0(t) = -s_1(t)$.

Osservazione Dato un bit $a \in \{-1, 1\}$ si può ottenere la forma d'onda da trasmettere facendo semplicemente $a \cdot g(t)$.

Rate di invio Con il sistema 2-PAM si invia 1 bit/simbolo.

Scelta del ricevitore Ricevuto un segnale $r(t)$ l'unica componente interessante è quella parallela a $\varphi(t)$ e quindi si ricava:

$$r_{\parallel} = \int_{-\infty}^{+\infty} r(t) \cdot \varphi(t) dt = \frac{1}{\sqrt{E_g}} \cdot \int_{-\infty}^{+\infty} r(t) \cdot g(t) dt$$

L'oggetto che esegue questa integrale nella catena di ricezione di un sistema di trasmissione 2-PAM è detto correlatore. Le regioni decisionali sono definite dal segno di r_{\parallel} , come si può notare dalla rappresentazione grafica delle regioni decisionali mostrata in figura 11.3.

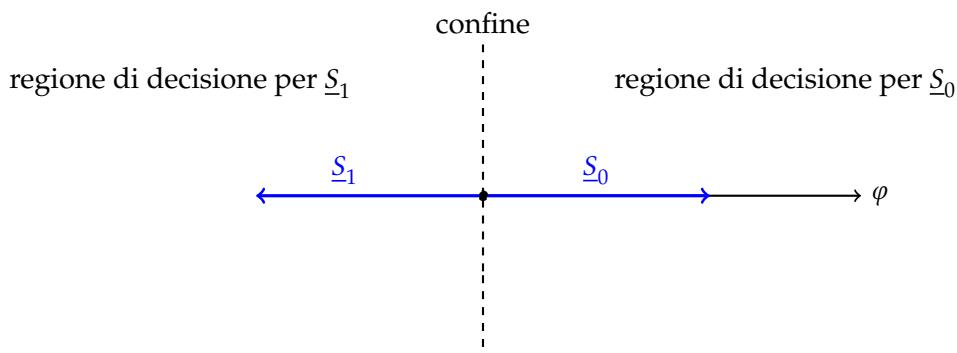


Figura 11.3.: Regioni decisionali nel 2-PAM.

Dato che le regioni decisionali sono date solo dal segno si può utilizzare:

$$r_{\parallel} = \int_{-\infty}^{+\infty} r(t) \cdot g(t) dt$$

Valore delle energie

- $E_{s_0} = E_{s_1} = E_g = E$, dato che tra i due segnali varia solo il segno.
- $E_s = E$, dato che le forme d'onda hanno tutte la stessa energia.
- $E_b = E$, dato che ogni forma d'onda trasmette un bit di informazione.

Probabilità di errore Si può ricavare la probabilità di errore tramite la formula generale, dove è presente solo un confine tra le regioni decisionali e quindi:

$$\begin{aligned} P_e &= Q\left(\frac{|S_1 - S_0|}{\sqrt{2 \cdot N_0}}\right) = \\ &= Q\left(\frac{2 \cdot \sqrt{E_b}}{\sqrt{2 \cdot N_0}}\right) = \\ &= Q\left(\sqrt{\frac{2 \cdot E_b}{N_0}}\right) \end{aligned}$$

Si può notare che la probabilità di errore non dipende in nessun modo dalla forma del segnale e quindi si può scegliere la forma del segnale in modo da migliorare altri parametri. La probabilità di errore dipende solamente dal rapporto tra l'energia del segnale e la varianza del rumore e quindi si può rappresentare questa dipendenza in un grafico, come mostrato in figura 11.4.

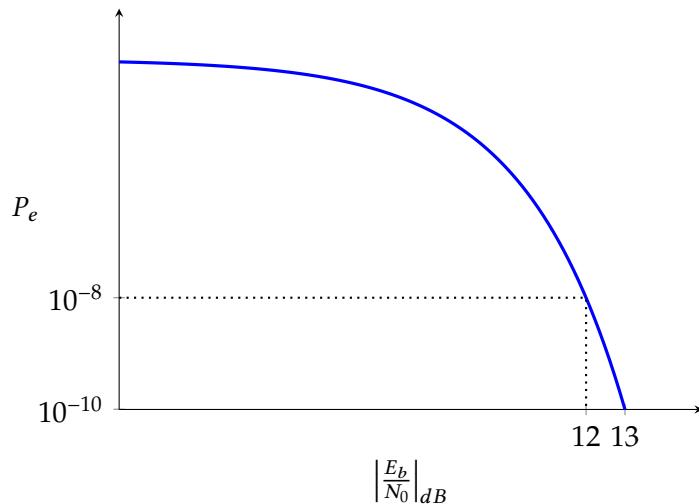


Figura 11.4.: Probabilità d'errore per il 2-PAM al variare del rapporto tra energia del segnale e varianza del rumore.

11.1.3. Trasmissione 4-PAM

Concetto Il sistema 4-PAM è una tecnica che permette di trasmettere due bit di informazione per simbolo; sfrutta la geometria dei segnali per diminuire la probabilità d'errore.

Dato che invia due bit di informazione per simbolo basta definire la forma di quattro segnali.

Definizione Il sistema scelto è monodimensionale con funzione di base $\varphi(t)$, dove le 4 forme d'onda sono:

$$\begin{aligned} s_0(t) &= -3 \cdot \sqrt{E} \cdot \varphi(t) = -3 \cdot g(t) \\ s_1(t) &= -\sqrt{E} \cdot \varphi(t) = -g(t) \\ s_2(t) &= \sqrt{E} \cdot \varphi(t) = g(t) \\ s_3(t) &= 3 \cdot \sqrt{E} \cdot \varphi(t) = 3 \cdot g(t) \end{aligned}$$

11. Trasmissione multicanale

Osservazione Dato un simbolo $a \in \{-1, 1, -3, 3\}$ si può ottenere la forma d'onda da trasmettere facendo semplicemente $a \cdot g(t)$.

Rate di invio Con il sistema 4-PAM si inviano 2 bit/simbolo.

Scelta del ricevitore Ricevuto un segnale $r(t)$ l'unica componente interessante è quella parallela a $\varphi(t)$ e quindi si ricava:

$$r_{\parallel} = \int_{-\infty}^{+\infty} r(t) \cdot \varphi(t) dt = \frac{1}{\sqrt{E_g}} \cdot \int_{-\infty}^{+\infty} r(t) \cdot g(t) dt$$

Le regioni decisionali sono mostrate in figura 11.5: due sono interne, e confinano con altre due regioni, e due esterne, e confinano solo con una regione.

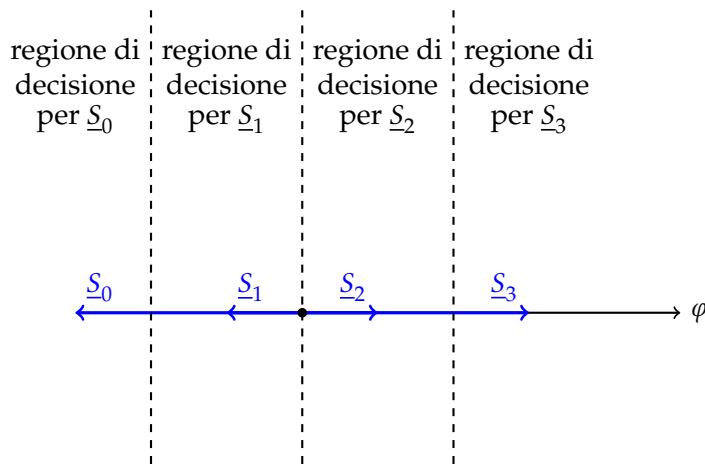


Figura 11.5.: Rappresentazione grafica delle regioni decisionali nel 4-PAM.

Si può notare che tali confini si trovano nelle posizioni $-\frac{2}{\sqrt{E_g}}, 0, \frac{2}{\sqrt{E_g}}$ e quindi si può considerare il termine:

$$r_{\parallel} = \int_{-\infty}^{+\infty} r(t) \cdot g(t) dt$$

e usare come confini i valori interi $-2, 0, 2$.

Valore delle energie

- $E_{s_1} = E_{s_2} = E_g$ e $E_{s_0} = E_{s_3} = 3^2 \cdot E_g$, come si può facilmente notare.
- Si può notare che:

$$E_s = \frac{E_g + E_g + 9 \cdot E_g + 9 \cdot E_g}{4} = \frac{20}{4} \cdot E_g = 5 \cdot E_g$$

- Dato che ogni simbolo porta 2 bit di informazione si ha che:

$$E_b = \frac{E_s}{2} = \frac{5}{2} \cdot E_g$$

11. Trasmissione multicanale

Probabilità di errore Si può ricavare la probabilità di errore tramite la formula generale, dove:

- Le zone esterne confinano solo con una zona, quindi si ha che:

$$P_{e0} = P_{e01} = Q\left(\frac{|S_0 - S_1|}{\sqrt{2 \cdot N_0}}\right) = Q\left(\frac{2 \cdot \sqrt{E_g}}{\sqrt{2 \cdot N_0}}\right) = Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right)$$

$$P_{e3} = P_{e32} = Q\left(\frac{|S_3 - S_2|}{\sqrt{2 \cdot N_0}}\right) = Q\left(\frac{2 \cdot \sqrt{E_g}}{\sqrt{2 \cdot N_0}}\right) = Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right)$$

- Le zone interne confinano con altre due regioni, quindi si ha che:

$$P_{e1} = P_{e12} + P_{e10} = Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) + Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) = 2 \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right)$$

$$P_{e2} = P_{e23} + P_{e21} = Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) + Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) = 2 \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right)$$

Quindi la probabilità di interpretare male il simbolo è:

$$\begin{aligned} P_e &= \frac{1}{M} \cdot \left[\sum_{k=1}^M P_{ek} \right] = \\ &= \frac{1}{4} \cdot [P_{e0} + P_{e1} + P_{e2} + P_{e3}] = \\ &= \frac{1}{4} \cdot \left[Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) + Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) + 2 \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) + 2 \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) \right] = \\ &= \frac{6}{4} \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) = \\ &= \frac{3}{2} \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) \end{aligned}$$

Probabilità di sbagliare un bit La P_e ricavata prima è la probabilità di sbagliare simbolo, ma dato che ogni simbolo porta 2 bit di informazione questa non corrisponde alla probabilità di sbagliare un bit. Per poter ricavare questa probabilità bisogna assegnare alle varie forme d'onda una coppia di bit.

Dato che è molto probabile che in caso di errore si sbagli con una regione confinante è comodo assegnare a regioni confinanti sequenze di bit che variano solo di un bit: questo mapping è detto di Grey. Un possibile mapping di Gray è il seguente:

$$\begin{array}{rccccc} -3 & \Leftrightarrow & s_0(t) & \Leftrightarrow & 00 \\ -1 & \Leftrightarrow & s_1(t) & \Leftrightarrow & 01 \\ 1 & \Leftrightarrow & s_2(t) & \Leftrightarrow & 11 \\ 3 & \Leftrightarrow & s_3(t) & \Leftrightarrow & 10 \end{array}$$

Utilizzando tale mapping sbagliare l'interpretazione corrisponde a sbagliare un solo bit e quindi si ha che:

$$P_{eb} = \frac{P_e}{2} = \frac{3}{4} \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right)$$

11. Trasmissione multicanale

Per poter paragonare questa probabilità di errore al 2-PAM è necessario scriverla in funzione dell'energia media necessaria per inviare un bit E_b e quindi:

$$P_{eb} = \frac{3}{4} \cdot Q\left(\sqrt{\frac{2}{5} \cdot \frac{2 \cdot E_b}{N_0}}\right)$$

Si può notare che per avere la stessa probabilità di sbagliare del sistema 2-PAM bisogna avere una energia maggiore, precisamente serve un'energia 2.5 maggiore, e quindi tramite il 4-PAM si trasmette con un bit rate maggiore, ma per avere la stessa probabilità di errore è necessario usare segnali con potenza maggiore. Si può notare la differenza con il 2-PAM nella figura 11.6.

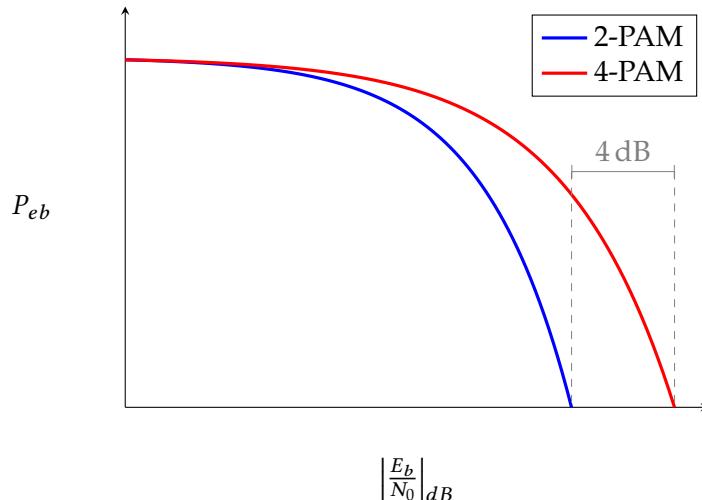


Figura 11.6.: Confronto tra 2-PAM e 4-PAM della probabilità d'errore al variare del rapporto tra energia del segnale e varianza del rumore.

11.1.4. Trasmissione M-PAM

Concetto Il sistema M -PAM (Pulse-Amplitude Modulation) è la generalizzazione dei sistemi di trasmissione visti precedentemente dove si utilizzano un numero generico M di simboli.

Definizione Il sistema scelto è monodimensionale con funzione di base $\varphi(t)$ e si ha che:

$$s_i(t) = a_i \cdot \sqrt{E_g} \cdot \varphi(t)$$

dove $a_i \in \{1, -1, 3, -3, 5, -5, \dots, M-1, -M+1\}$ e si definisce

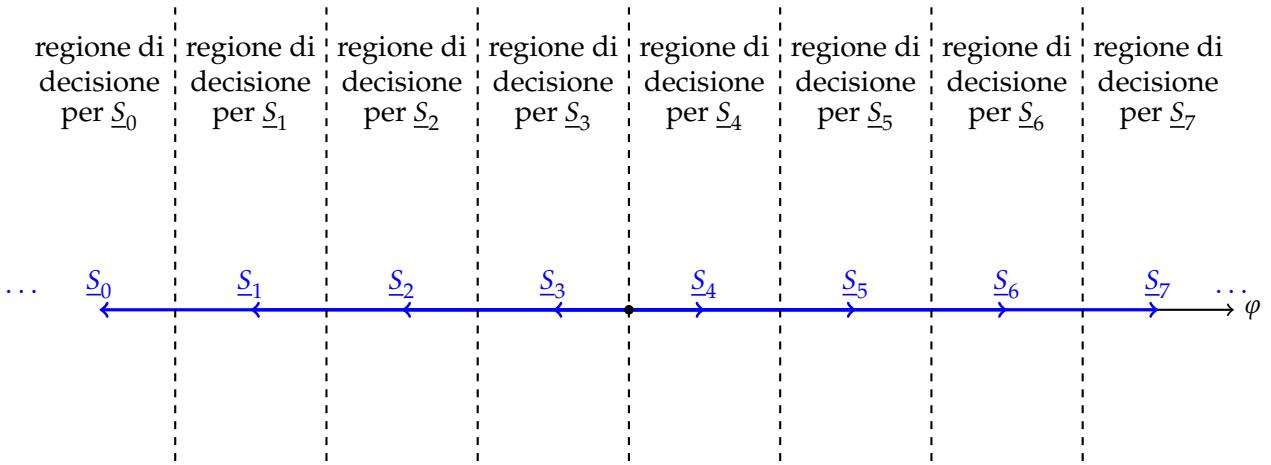
$$g(t) = \sqrt{E_g} \cdot \varphi(t)$$

Rate di invio Con il sistema M -PAM si inviano $\log M$ bit/simbolo; per questo motivo solitamente M è una potenza di 2.

Scelta del ricevitore Ricevuto un segnale $r(t)$ l'unica componente interessante è quella parallela a $\varphi(t)$ e quindi si ricava:

$$r_{||} = \int_{-\infty}^{+\infty} r(t) \cdot \varphi(t) dt = \frac{1}{\sqrt{E_g}} \cdot \int_{-\infty}^{+\infty} r(t) \cdot g(t) dt$$

Le regioni decisionali sono mostrate in figura 11.7: $M - 2$ regioni decisionali sono interne, e confinano con altre due regioni; 2 regioni sono esterne, e confinano solo con una regione.


 Figura 11.7.: Rappresentazione grafica delle regioni decisionali nel M -PAM.

Si può notare che tali confini si trovano nelle posizioni $0, \frac{2}{\sqrt{E_g}}, -\frac{2}{\sqrt{E_g}}, \frac{4}{\sqrt{E_g}}, -\frac{4}{\sqrt{E_g}}, \dots$ e quindi si può considerare il termine:

$$r_{\parallel} = \int_{-\infty}^{+\infty} r(t) \cdot g(t) dt$$

e usare come confini i valori interi $0, 2, -2, 4, -4, \dots, M-2, -2+M$.

Valore delle energie

- $E_{s_i} = a_i^2 \cdot E_g$
- Si può notare che:

$$E_s = \frac{\sum_{i=1}^M a_i^2 \cdot E_g}{M} = \frac{E_g}{M} \cdot \sum_{i=1}^M a_i^2 = \frac{M^2 - 1}{3} \cdot E_g^I$$

^IDimostrazione dell'ultimo passaggio:

La sommatoria è la somma del quadrato di tutti i numeri dispari minori di M presi due volte dato che ci sono i negativi e quindi:

$$\frac{\sum_{k=1}^M a_k^2}{M} = \frac{2 \cdot \sum_{k=1}^{\frac{M}{2}} (2 \cdot k - 1)^2}{M} = \frac{1}{M} \cdot \left[8 \cdot \sum_{k=1}^{\frac{M}{2}} k^2 - 8 \cdot \sum_{k=1}^{\frac{M}{2}} k + 2 \cdot \sum_{k=1}^{\frac{M}{2}} 1 \right]$$

Ricordando che:

$$\sum_{k=1}^{\frac{M}{2}} k^2 = \frac{1}{6} \cdot \left(\frac{M}{2} \right) \cdot \left(\frac{M}{2} + 1 \right) \cdot (M + 1)$$

$$\sum_{k=1}^{\frac{M}{2}} k = \frac{1}{2} \cdot \left(\frac{M}{2} \right) \cdot \left(\frac{M}{2} + 1 \right)$$

si ha che:

$$\begin{aligned} \frac{\sum_{k=1}^{\frac{M}{2}} a_k^2}{M} &= \frac{1}{M} \cdot \left[\frac{8}{6 \cdot 2 \cdot 2} \cdot M \cdot (M + 2) \cdot (M + 1) - \frac{8}{2 \cdot 2 \cdot 2} \cdot M \cdot (M + 2) + 2 \cdot \frac{M}{2} \right] = \\ &= \frac{M}{M} \cdot \left[\frac{1}{3} \cdot (M^2 + 3 \cdot M + 2) - M - 2 + 1 \right] = \\ &= \frac{1}{3} \cdot M^2 + M + \frac{2}{3} - M - 1 = \\ &= \frac{M^2 - 1}{3} \end{aligned}$$

11. Trasmissione multicanale

- Dato che ogni simbolo porta $\log M$ bit di informazione si ha che:

$$E_b = \frac{E_s}{\log M} = \frac{M^2 - 1}{3 \cdot \log M} \cdot E_g$$

Probabilità di errore Si può ricavare la probabilità di errore tramite la formula generale, dove:

- Le zone esterne confinano solo con le una zona, quindi per le due zone esterne si ha:

$$P_{ek} = Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right)$$

- Le zone interne confinano solo con altre due zone, quindi per le $M - 2$ zone interne si ha:

$$P_{ek} = 2 \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right)$$

Quindi la probabilità di interpretare male il simbolo è:

$$\begin{aligned} P_e &= \frac{1}{M} \cdot \left[\sum_{k=1}^M P_{ek} \right] = \\ &= \frac{1}{M} \cdot \left[2 \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) + (M - 2) \cdot 2 \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) \right] = \\ &= \frac{2 \cdot M - 4 + 2}{M} \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) = \\ &= \frac{2 \cdot (M - 1)}{M} \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right) \end{aligned}$$

Probabilità di sbagliare un bit In modo analogo al 4-PAM si può utilizzare il codice Gray per fare in modo che le zone confinanti rappresentino una sequenza di bit in cui varia solo un bit ottenendo:

$$P_{eb} = \frac{P_e}{\log M} = \frac{2 \cdot (M - 1)}{M \cdot \log M} \cdot Q\left(\sqrt{\frac{2 \cdot E_g}{N_0}}\right)$$

Per poter paragonare questa probabilità di errore al 2-PAM è necessario scriverla in funzione dell'energia media necessaria per inviare un bit E_b e quindi:

$$P_{eb} = \frac{2 \cdot (M - 1)}{M \cdot \log M} \cdot Q\left(\sqrt{\frac{3 \cdot \log M}{M^2 - 1} \cdot \frac{2 \cdot E_b}{N_0}}\right)$$

Quindi per avere la stessa probabilità di errore del 2-PAM bisogna usare più energia. Il fattore di perdita è:

$$\frac{M^2 - 1}{3 \cdot \log M}$$

Si può notare che il contributo di M^2 è più significativo di quello di $\log M$ al denominatore e quindi questo termine aumenta in modo quadratico con l'aumento di M . Inoltre si può notare che il bit rate aumenta logaritmicamente con M e quindi si arriva velocemente a una situazione in cui per aumentare di 1 bit il bit rate

bisogna aumentare di molto l'energia dei segnali, per questo motivo si tende a non usare M molto grandi. Si può notare la differenza tra i vari M -PAM nella figura 11.8.

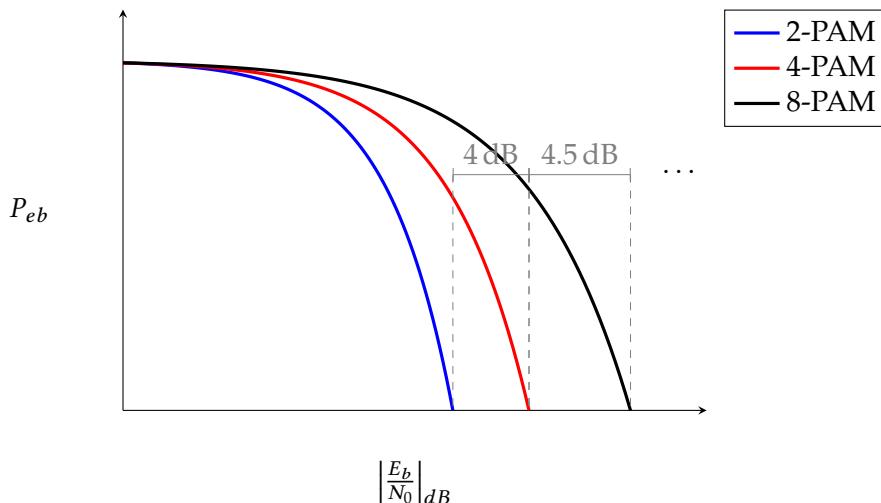


Figura 11.8.: Confronto tra M -PAM della probabilità d'errore al variare del rapporto tra energia del segnale e varianza del rumore.

11.2. Trasmissione di una sequenza di simboli tramite un canale passa-basso

11.2.1. Introduzione

Introduzione al problema Si supponga di voler trasmettere una sequenza di bit con un trasmettitore M -PAM, quindi si ha una sequenza (a_0, a_1, a_2, \dots) con $a_i \in \{1, -1, 3, -3, \dots, M-1, -M+1\}$. Supponendo di scegliere una generica forma d'onda $g(t)$ e di voler trasmettere un simbolo ogni T secondi si ha che il segnale trasmesso è:

$$\begin{aligned} s(t) &= a_0 \cdot g(t) + a_1 \cdot g(t-T) + a_2 \cdot g(t-2 \cdot T) + \dots = \\ &= \sum_k a_k \cdot g(t-k \cdot T) \end{aligned}$$

Per interpretare l' i -esimo bit il ricevitore calcola la sua componente parallela a $g(t-i \cdot T)$ ossia:

$$\begin{aligned} r_i &= \int_{-\infty}^{+\infty} r(t) \cdot g(t-i \cdot T) dt = \\ &= \int_{-\infty}^{+\infty} (s(t) + n(t)) \cdot g(t-i \cdot T) dt = \\ &= \int_{-\infty}^{+\infty} \left(\sum_k a_k \cdot g(t-k \cdot T) \right) \cdot g(t-i \cdot T) dt + \int_{-\infty}^{+\infty} n(t) \cdot g(t-i \cdot T) dt = \\ &= \sum_k a_k \cdot \left[\int_{-\infty}^{+\infty} g(t-k \cdot T) \cdot g(t-i \cdot T) dt \right] + \int_{-\infty}^{+\infty} n(t) \cdot g(t-i \cdot T) dt = \\ &= a_i \cdot \underbrace{\int_{-\infty}^{+\infty} g(t-i \cdot T)^2 dt}_E + \underbrace{\sqrt{E \cdot n_k}}_{\text{effetto del rumore}} + \sum_{k \neq i} a_k \cdot \underbrace{\left[\int_{-\infty}^{+\infty} g(t-k \cdot T) \cdot g(t-i \cdot T) dt \right]}_{\text{interferenza intersimbolica}} \end{aligned}$$

L'interferenza intersimbolica (ISI) aggiunge un errore ulteriore al segnale ricevuto.

Analisi dell'interferenza intersimbolica Facendo un cambio di variabile si nota che l'interferenza intersimbolica dipende solamente dalla distanza tra due segnali ossia:

$$\sum_{k \neq 0} a_k \cdot \left[\int_{-\infty}^{+\infty} g(t - k \cdot T) \cdot g(t) dt \right]$$

Se si usasse una forma d'onda $g(t)$ limitata nel tempo, ossia $g(t) = 0$ per $|t| > T$ questo integrale sarebbe nullo per tutto il suo dominio riducendo al minimo tale errore. Questo però comporta l'utilizzo di segnali con bande larghe e quindi verrebbero filtrati dal canale con banda più stretta, per questo motivo bisogna trovare un altro modo per ridurre tale errore.

Si può notare che la condizione appena spiegata è solo una condizione sufficiente, infatti si ha che la condizione necessaria è che:

$$\int_{-\infty}^{+\infty} g(t - k \cdot T) \cdot g(t) dt = 0 \\ \forall k \neq 0$$

che è nota come condizione di Nyquist.

11.2.2. Condizione di Nyquist

Tramite il cambio di variabile $\tau = t - k \cdot T$ si ottiene ($g_-(t) = g(-t)$):

$$\int_{-\infty}^{+\infty} g(t - k \cdot T) \cdot g(t) dt = \int_{-\infty}^{+\infty} g(\tau) \cdot g(\tau + k \cdot T) d\tau = [g * g_-](t)|_{t=-k \cdot T}$$

Quindi definendo la funzione $v(t) = [g * g_-](t)$ si può scrivere la condizione di Nyquist come:

$$v(k \cdot T) = 0 \\ \forall k \neq 0$$

Per avere $v(t)$ nulla in tutti gli istanti $k \cdot T \neq 0$ deve valere la seguente uguaglianza:

$$v(t) \cdot \left[\sum_{k=-\infty}^{+\infty} \delta(t - k \cdot T) \right] = v(0) \cdot \delta(t)$$

perché la funzione $\delta(t - k \cdot T)$ è diversa da 0 solo negli istanti dove ci sono gli impulsi ossia $0, T, 2 \cdot T, \dots$, ma la funzione $v(t)$ dev'essere nulla in tutti questi istanti escluso lo 0, e quindi questa funzione deve essere uguale al valore che assume per $k = 0$ ossia $v(0) \cdot \delta(t)$.

Applicando la trasformata di Fourier ad entrambi i termini si ottiene ($\mathcal{F} \text{ comb}_T(t) = \frac{1}{T} \cdot \text{comb}_{\frac{1}{T}}(f)$):

$$\begin{aligned} \frac{1}{T} \cdot \left[V * \text{comb}_{\frac{1}{T}} \right](f) &= v(0) \\ \frac{1}{T} \cdot \int_{-\infty}^{+\infty} V(\tau) \cdot \sum_{n=-\infty}^{+\infty} \delta\left(f - \frac{n}{T} - \tau\right) d\tau &= v(0) \\ \frac{1}{T} \cdot \sum_{n=-\infty}^{+\infty} \int_{-\infty}^{+\infty} V(\tau) \cdot \delta\left(f - \frac{n}{T} - \tau\right) d\tau &= v(0) \\ \frac{1}{T} \cdot \sum_{n=-\infty}^{+\infty} V\left(f - \frac{n}{T}\right) &= v(0) \\ \sum_{n=-\infty}^{+\infty} V\left(f - \frac{n}{T}\right) &= T \cdot v(0) \end{aligned}$$

11. Trasmissione multicanale

e quindi per rispettare la condizione di Nyquist la ripetizione con periodo $1/T$ dello spettro di $v(t)$ deve essere costante nel tempo.

Dalla definizione di $v(t)$ si ottiene che:

$$|V(f)| = |G(f)| \cdot |G(f)| = |G(f)|^2$$

e quindi anche lo spettro di $g(t)$ deve avere questa proprietà, inoltre si può notare che V e G hanno la stessa banda, perché $|G(f)| = 0 \Leftrightarrow |V(f)| = 0$.

Scelta della forma d'onda di $g(t)$ usando il sistema M-PAM Si vuole trovare la forma d'onda $g(t)$ per cui vale la condizione di Nyquist con banda più stretta possibile; in figura 11.9 sono rappresentate qualitativamente le forme d'onda che rispettano tale condizione.

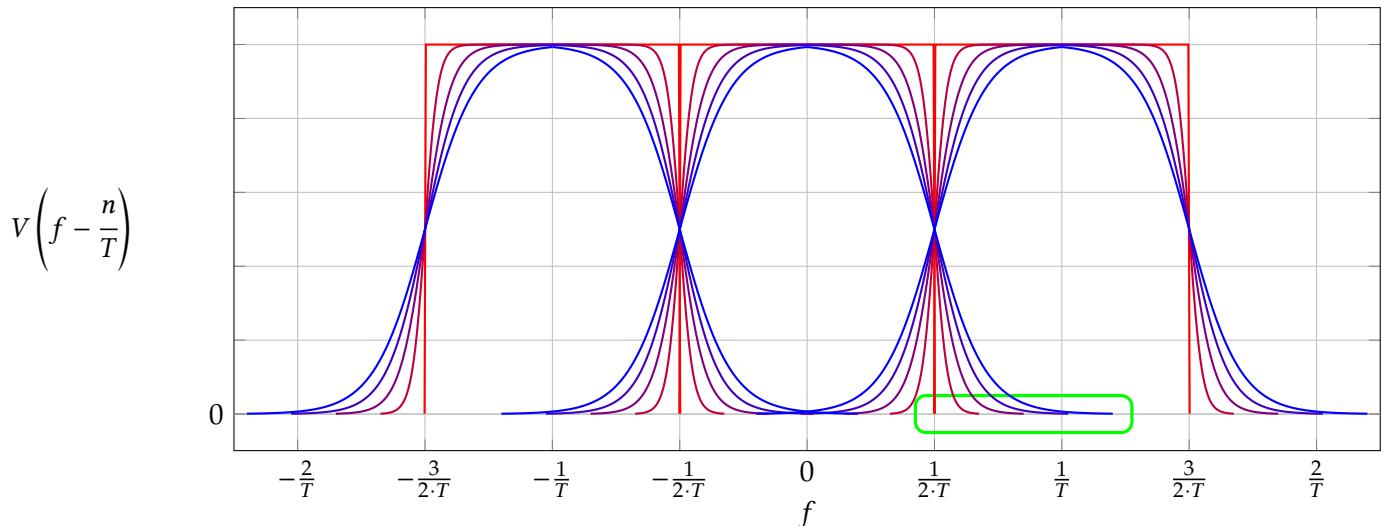


Figura 11.9.: Forme d'onda che rispettano la condizione di Nyquist.

Dall'immagine si nota che stringendo la banda la forma d'onda si avvicina sempre di più ad un rettangolo largo $1/T$; si può anche notare che non esistono forme d'onda che rispettano la condizione di Nyquist che hanno banda inferiore a questa. Per questo motivo la forma d'onda a banda minore che rispetta la condizione di Nyquist è la forma d'onda con trasformata:

$$G(f) = \text{rect}(f \cdot T)$$

che ha banda pari a

$$B = \frac{1}{2 \cdot T}$$

quindi si ha che:

$$g(t) = \text{sinc}\left(\frac{t}{T}\right)$$

Il seno cardinale è la forma d'onda con banda minore a rispettare la condizione di Nyquist, però presenta il problema che continua a oscillare per diversi periodi e quindi il rumore porta a errori molto grossi e inoltre questa forma d'onda va resa causale per essere usata.

Per questo motivo si utilizzano onde che occupano un po' più di banda ma si annullano molto più velocemente nel tempo, riducendo l'errore dovuto al rumore; la forma d'onda più usata è il «Raised-Cosine» per il quale la discesa dello spettro ha un andamento cosinusoidale del tipo:

$$G(f) \propto \cos^2\left[\left(f - \frac{1-\alpha}{2 \cdot T}\right) \cdot \frac{\pi \cdot T}{2 \cdot \alpha}\right]$$

$$f \in \left[\frac{1-\alpha}{2 \cdot T}, \frac{1+\alpha}{2 \cdot T}\right]$$

11. Trasmissione multicanale

Dove α è un parametro che indica quanto è veloce la discesa e solitamente si usa $\alpha \in [0.2, 0.5]$. Nel dominio nel tempo si ottiene una forma d'onda del tipo:

$$g(t) \propto \text{sinc}\left(\frac{t}{T}\right) \cdot \frac{1}{t^2}$$

che si annulla molto più velocemente del seno cardinale e solitamente la si può considerare avente durata pari a $6 \cdot T$.

Radice di Nyquist Una forma d'onda che rispetta la condizione di Nyquist è detta radice di Nyquist.

Banda del segnale Utilizzando una radice di Nyquist con una banda larga B il segnale $s(t)$ inviato ha anch'esso banda B , infatti:

$$\begin{aligned} s(t) &= \sum_k a_k \cdot g(t - k \cdot T) \\ S(f) &= \mathcal{F} \left[\sum_k a_k \cdot g(t - k \cdot T) \right] = \\ &= \sum_k a_k \cdot \mathcal{F}[g(t - k \cdot T)] = \\ &= \sum_k a_k \cdot G(f) \cdot e^{-j \cdot 2 \cdot \pi \cdot k \cdot T} = \\ &= G(f) \cdot \sum_k a_k \cdot e^{-j \cdot 2 \cdot \pi \cdot k \cdot T} \end{aligned}$$

Dato che i vari a_k non sono mai nulli e che l'esponenziale non può annullarsi si ha che:

$$S(f) = 0 \Leftrightarrow G(f) = 0$$

e quindi $s(t)$ ha come banda B .

Trasmissione M -PAM usando il Raised-Cosine In un M -PAM si ha che:

$$R_b = \log M \text{ bit/simbolo}$$

e dato che:

$$R_s = \frac{1}{T} \text{ simboli/s}$$

si ottiene:

$$R_b = \frac{\log M}{T} \text{ bit/s}$$

Utilizzando come forma d'onda il Raised-Cosine si ha che per trasmettere con un bit rate di R_b si deve avere a disposizione una banda pari a:

$$B = \frac{1 + \alpha}{2 \cdot T} = \frac{1 + \alpha}{2 \cdot \log M} \cdot R_b$$

e quindi più M è grande meno banda serve per trasmettere un determinato bit rate.

11.3. Trasmissione tramite una canale passa banda

11.3.1. Introduzione

Premessa trigonometrica In questa sezione vengono usate spesso le seguenti uguaglianze trigonometriche:

$$\sin^2(x) = \frac{1}{2} + \frac{1}{2} \cdot \cos(2 \cdot x)$$

$$\cos^2(x) = \frac{1}{2} - \frac{1}{2} \cdot \cos(2 \cdot x)$$

$$\sin(x) \cdot \cos(x) = \frac{1}{2} \cdot \sin(2 \cdot x)$$

Problema Si vuole trasmettere attraverso un canale passa banda con una banda B centrata sulla frequenza f_0 sfruttando la conoscenza acquisita in merito alla trasmissione su canale passa basso.

Per trasmettere la sequenza (a_0, a_1, a_2, \dots) si usa una forma d'onda con banda limitata:

$$s(t) = \sum_k a_k \cdot g(t - k \cdot T)$$

Si è visto che moltiplicando per una cosinusoide si ottiene un segnale con banda doppia centrata nella frequenza della cosinusoide e quindi si può trasmettere tale forma d'onda nel canale.

Trasmissione in fase e in quadratura Si consideri di voler trasmettere due sequenze (a_0, a_1, a_2, \dots) e (b_0, b_1, b_2, \dots) tramite i segnali:

$$s_i(t) = \sum_k a_k \cdot g(t - k \cdot T)$$

$$s_q(t) = \sum_k b_k \cdot g(t - k \cdot T)$$

Tramite un canale passa banda si possono inviare in contemporanea utilizzando il segnale:

$$s(t) = \sqrt{2} \cdot [s_i(t) \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t) + s_q(t) \cdot \sin(2 \cdot \pi \cdot f_0 \cdot t)]$$

dove la sequenza a è trasmessa in fase mentre la sequenza b è trasmessa in quadratura.

Operazione del ricevitore in fase Il ricevitore per leggere il segnale in fase basta che moltiplich di nuovo per $\sqrt{2} \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t)$ e poi applichi un filtro passa basso, infatti:

$$\begin{aligned} s(t) \cdot \sqrt{2} \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t) &= 2 \cdot [s_i(t) \cdot \cos^2(2 \cdot \pi \cdot f_0 \cdot t) + s_q(t) \cdot \sin(2 \cdot \pi \cdot f_0 \cdot t) \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t)] = \\ &= s_i(t) \cdot 2 \cdot \left[\frac{1}{2} - \frac{1}{2} \cdot \cos(2 \cdot \pi \cdot 2 \cdot f_0 \cdot t) \right] + s_q(t) \cdot 2 \cdot \left[\frac{1}{2} \cdot \sin(2 \cdot \pi \cdot 2 \cdot f_0 \cdot t) \right] = \\ &= s_i(t) - s_i(t) \cdot \cos(2 \cdot \pi \cdot 2 \cdot f_0 \cdot t) + s_q(t) \cdot \sin(2 \cdot \pi \cdot 2 \cdot f_0 \cdot t) \end{aligned}$$

quindi applicando un filtro passa basso con frequenza di taglio f_0 si eliminano le componenti non volute dato che si trovano entrambe in un intorno della frequenza $2 \cdot f_0$, e quindi in uscita dal filtro si ottiene esattamente $s_i(t)$. Successivamente si può applicare il correlatore del M-PAM usato per ottenere i vari simboli delle sequenze.

Operazione del ricevitore in quadratura Il ricevitore per leggere il segnale in quadratura basta che moltipichi di nuovo per $\sqrt{2} \cdot \sin(2 \cdot \pi \cdot f_0 \cdot t)$ e poi applichi un filtro passa-basso infatti:

$$\begin{aligned} s(t) \cdot \sqrt{2} \cdot \sin(2 \cdot \pi \cdot f_0 \cdot t) &= 2 \cdot [s_i(t) \cdot \sin(2 \cdot \pi \cdot f_0 \cdot t) \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t) + s_q(t) \cdot \sin^2(2 \cdot \pi \cdot f_0 \cdot t)] = \\ &= s_i(t) \cdot 2 \cdot \left[\frac{1}{2} \cdot \sin(2 \cdot \pi \cdot 2 \cdot f_0 \cdot t) \right] + s_q(t) \cdot 2 \cdot \left[\frac{1}{2} + \frac{1}{2} \cdot \cos(2 \cdot \pi \cdot 2 \cdot f_0 \cdot t) \right] = \\ &= s_i(t) \cdot \sin(2 \cdot \pi \cdot 2 \cdot f_0 \cdot t) + s_q(t) + s_q(t) \cdot \cos(2 \cdot \pi \cdot 2 \cdot f_0 \cdot t) \end{aligned}$$

Tramite un filtro analogo al caso precedente si riesce a ottenere $s_q(t)$ e tramite il correlatore del M-PAM si possono ottenere i bit della sequenza inviata in quadratura.

Banda usata Usando una forma d'onda $g(t)$ con banda larga B allora:

- $s_i(t)$ e $s_q(t)$ hanno anch'esse banda larga B .
- $s(t)$ ha una banda larga $2 \cdot B$ centrata in f_0 .

Quindi il canale passa-banda usato deve avere una banda pari a $2 \cdot B$.

Symbol rate di trasmissione Con questo sistema si possono inviare due sequenze con symbol rate pari $1/T$ e quindi in totale si trasmettono $2/T$ simboli/s. Quindi si ha un ritmo di trasmissione doppio rispetto alla trasmissione su un canale passa-basso, ma è richiesta una banda doppia e quindi per trasmettere ad un certo symbol rate è richiesta la stessa banda che serve per la trasmissione su un canale passa-basso. Infatti supponendo di usare un Raised-Cosine si ha:

$$\begin{aligned} \frac{B}{2} &= \frac{1+\alpha}{2 \cdot T} = \frac{1+\alpha}{2} \cdot \frac{R_s}{2} \\ B &= \frac{1+\alpha}{2} \cdot R_s \end{aligned}$$

che è lo stesso ritmo degli M-PAM.

Rappresentazione tramite schema a blocchi Tutta la catena appena descritta può essere riassunta dallo schema a blocchi in figura 11.10.

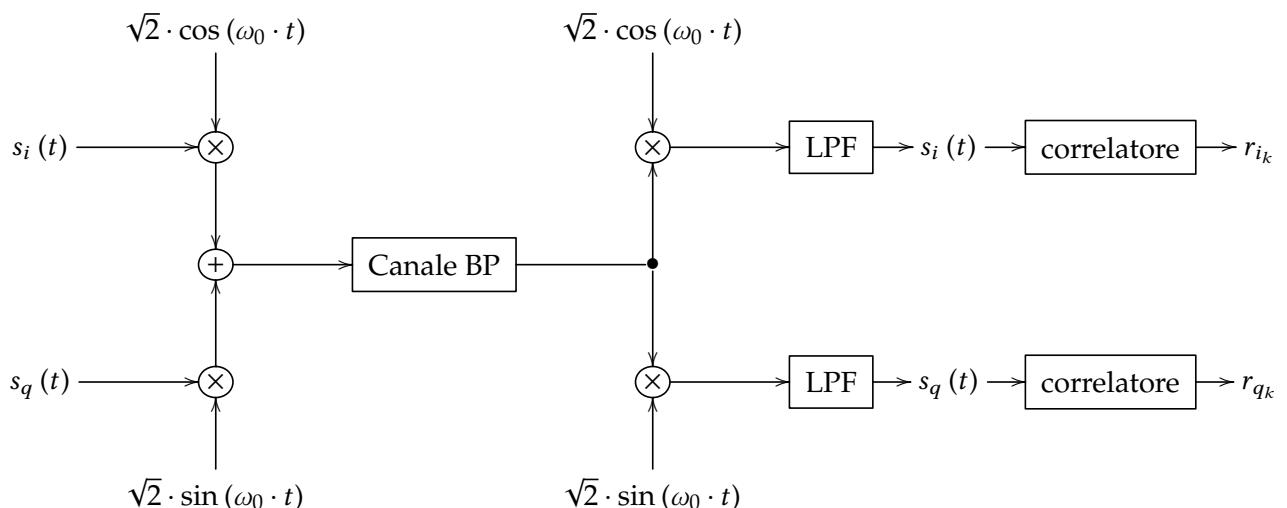


Figura 11.10.: Schema a blocchi per trasmissione e ricezione in un canale passa-banda.

11. Trasmissione multicanale

Realizzazione dei filtri passa-basso La funzione di filtro passa-basso è realizzata automaticamente dal correlatore, infatti per il k -esimo bit della forma d'onda in fase si ottiene:

$$\int_{-\infty}^{+\infty} r(t) \cdot g(t - k \cdot T) dt = \int_{-\infty}^{+\infty} (s_i(t) - s_i(t) \cdot \cos(4 \cdot \pi \cdot f_0 \cdot t) + s_q(t) \cdot \sin(4 \cdot \pi \cdot f_0 \cdot t)) \cdot g(t - k \cdot T) dt$$

quindi si ottiene il termine voluto sommato ai termini:

$$\begin{aligned} & \int_{-\infty}^{+\infty} -s_i(t) \cdot \cos(4 \cdot \pi \cdot f_0 \cdot t) \cdot g(t - k \cdot T) dt \\ & \int_{-\infty}^{+\infty} s_q(t) \cdot \sin(4 \cdot \pi \cdot f_0 \cdot t) \cdot g(t - k \cdot T) dt \end{aligned}$$

Il ragionamento sui due termini è analogo, e quindi considerando il termine con il coseno si ottiene:

$$\begin{aligned} \int_{-\infty}^{+\infty} -s_i(t) \cdot \cos(4 \cdot \pi \cdot f_0 \cdot t) \cdot g(t - k \cdot T) dt &= - \int_{-\infty}^{+\infty} \left[\sum_j a_j \cdot g(t - j \cdot T) \right] \cdot \cos(4 \cdot \pi \cdot f_0 \cdot t) \cdot g(t - k \cdot T) dt = \\ &= - \sum_j a_j \cdot \int_{-\infty}^{+\infty} g(t - j \cdot T) \cdot g(t - k \cdot T) \cdot \cos(4 \cdot \pi \cdot f_0 \cdot t) dt \end{aligned}$$

Per calcolare l'integrale appena scritto si può ricavare la trasformata di Fourier della funzione integranda e valutarla alla frequenza nulla; definendo:

$$\mathcal{F} g(t - i \cdot T) = G_i(f) = G(f) \cdot e^{-j \cdot 2 \cdot \pi \cdot i \cdot T}$$

$$\mathcal{F} \cos(A \cdot t) = \Delta_A(a) = \delta(a + A) + \delta(a - A)$$

abbiamo che:

$$\int_{-\infty}^{+\infty} g(t - j \cdot T) \cdot g(t - k \cdot T) \cdot \cos(4 \cdot \pi \cdot f_0 \cdot t) dt = [G_j * G_k * \Delta_{4 \cdot \pi \cdot f_0}](f) \Big|_{f=0}$$

Dato che i due termini esponenziali presenti in G_i e G_j non dipendono da f si possono portare davanti ottenendo:

$$\begin{aligned} [G_j * G_k * \Delta_{4 \cdot \pi \cdot f_0}](f) \Big|_{f=0} &= e^{-j \cdot 2 \cdot \pi \cdot j \cdot T} \cdot e^{-j \cdot 2 \cdot \pi \cdot k \cdot T} \cdot [G * G * \Delta_{4 \cdot \pi \cdot f_0}](f) \Big|_{f=0} = \\ &= e^{-j \cdot 2 \cdot \pi \cdot (j+k) \cdot T} \cdot [G * G * \Delta_{4 \cdot \pi \cdot f_0}](f) \Big|_{f=0} \end{aligned}$$

Dato che $\Delta_{4 \cdot \pi \cdot f_0}$ è la somma di due impulsi la sua convoluzione con $G * G$ è semplice:

$$\begin{aligned} [G_j * G_k * \Delta_{4 \cdot \pi \cdot f_0}](f) \Big|_{f=0} &= e^{-j \cdot 2 \cdot \pi \cdot (j+k) \cdot T} \cdot [[G * G](f - 4 \cdot \pi \cdot f_0) + [G * G](f + 4 \cdot \pi \cdot f_0)] \Big|_{f=0} = \\ &= e^{-j \cdot 2 \cdot \pi \cdot (j+k) \cdot T} \cdot [[G * G](-4 \cdot \pi \cdot f_0) + [G * G](4 \cdot \pi \cdot f_0)] \end{aligned}$$

Si può dimostrare che la convoluzione in frequenza raddoppia la banda del segnale e quindi dato che $f_0 \gg B$ si ha che il termine è nullo. In modo analogo si dimostra che anche il termine con il seno è anch'esso nullo e quindi il correlatore funziona da filtro.

11. Trasmissione multicanale

Analisi del rumore Si supponga che il canale passa banda usato abbia un rumore bianco gaussiano additivo con varianza $N_0/2$, allora nei segnali che si ottengono dopo il filtro va aggiunto un certo rumore additivo:

$$s_{ri}(t) = s_i(t) + n_i(t)$$

$$s_{rq}(t) = s_q(t) + n_q(t)$$

Un parametro importante del rumore è la correlazione tra le varie componenti del rumore e quindi è comodo ricavare:

$$\begin{aligned} R_n(k, j) &= \mathbb{E}[N_{ik} \cdot N_{ij}] = \\ &= \mathbb{E}\left[\frac{1}{\sqrt{E_g}} \cdot \int_{-\infty}^{+\infty} n_i(t) \cdot \sqrt{2} \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t) \cdot g(t - k \cdot T) dt \cdot \right. \\ &\quad \left. \frac{1}{\sqrt{E_g}} \cdot \int_{-\infty}^{+\infty} n_i(\tau) \cdot \sqrt{2} \cdot \cos(2 \cdot \pi \cdot f_0 \cdot \tau) \cdot g(\tau - j \cdot T) d\tau\right] = \\ &= \frac{1}{E_g} \cdot \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \mathbb{E}[n_i(t) \cdot n_i(\tau)] \cdot 2 \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t) \cdot \cos(2 \cdot \pi \cdot f_0 \cdot \tau) \cdot g(t - k \cdot T) \cdot g(\tau - j \cdot T) dt d\tau = \\ &= \frac{N_0 \cdot 2}{2 \cdot E_g} \cdot \left[\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \delta(t - \tau) \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t)^2 \cdot g(t - k \cdot T) \cdot g(\tau - j \cdot T) dt d\tau \right] = \\ &= \frac{N_0}{E_g} \cdot \left[\int_{-\infty}^{+\infty} \left(\frac{1}{2} - \frac{1}{2} \cdot \cos(4 \cdot \pi \cdot f_0 \cdot t) \right) \cdot g(t - k \cdot T) \cdot g(t - j \cdot T) dt \right] = \\ &= \frac{N_0}{E_g} \cdot \frac{1}{2} \cdot \left[\int_{-\infty}^{+\infty} g(t - k \cdot T) \cdot g(t - j \cdot T) dt - \int_{-\infty}^{+\infty} g(t - k \cdot T) \cdot g(t - j \cdot T) \cdot \cos(4 \cdot \pi \cdot f_0 \cdot t) dt \right] \end{aligned}$$

Il secondo termine viene rimosso dal filtro; inoltre dato che $g(t)$ è una radice di Nyquist si ha che:

$$\int_{-\infty}^{+\infty} g(t - k \cdot T) \cdot g(t - j \cdot T) dt = \begin{cases} E_g & \text{se } k = j \\ 0 & \text{se } k \neq j \end{cases}$$

e quindi:

$$\begin{aligned} R_n(k, j) &= \begin{cases} \cancel{\frac{E_g}{E_g}} \cdot \frac{N_0}{\cancel{E_g}} \cdot \frac{1}{2} & \text{se } k = j \\ 0 & \text{se } k \neq j \end{cases} = \\ &= \begin{cases} \frac{N_0}{2} & \text{se } k = j \\ 0 & \text{se } k \neq j \end{cases} \end{aligned}$$

e quindi è un rumore bianco con varianza uguale a quella del canale, e quindi usando questa configurazione, dal punto di vista del rumore, equivale alla trasmissione tramite un canale passa-basso. Tramite analoghi passaggi si può dimostrare che questo vale anche per il rumore in quadratura, inoltre sempre con analoghi passaggi si può dimostrare che il rumore in fase e quello in quadratura sono scorrelati.

11.3.2. Trasmissione M-QAM

Concetto La trasmissione *M-QAM* (Quadrature Amplitude Modulation) è una tecnica che sfrutta la trasmissione vista nella sezione precedente e permette di ottenere le stesse prestazioni di un \sqrt{M} -PAM.

Con questa tecnica si invia una coppia di simboli, uno in fase e uno in quadratura, con la tecnica spiegata prima, in questo modo si trasmettono il doppio dei bit utilizzando una banda doppia e quindi mantenendo le stesse prestazioni del corrispettivo PAM.

Dato che si trasmettono sempre i bit in coppia il numero totale di simboli è una potenza di 4 perché aggiungendo 2 nuovi simboli il numero di coppie va moltiplicato per $2^2 = 4$, e quindi si parla di:

- 4-QAM che corrisponde a un 2-PAM.
- 16-QAM che corrisponde a un 4-PAM.
- ...

Formalizzazione Si è visto che per trasmettere in un M -PAM si moltiplica la forma d'onda $g(t)$ per il simbolo a da trasmettere e quindi per inviare una sequenza si:

$$s(t) = \sum_k a_k \cdot g(t - k \cdot T)$$

con $a_k \in \{1, -1, 3, -3, 5, -5, \dots, M-1, -M+1\}$

Per mantenere una notazione simile nei M -QAM si può considerare la coppia di simboli da trasmettere come un numero complesso, ottenendo:

$$s(t) = \sum_k (a_k + j \cdot b_k) \cdot g(t - T \cdot k)$$

con $a_k, b_k \in \{1, -1, 3, -3, 5, -5, \dots, M-1, -M+1\}$

in questo modo si ottiene un M^2 -QAM che trasmette con un bit-rate doppio a quello di un M -PAM sfruttando il doppio della banda.

Costellazioni Se si rappresentano su un piano i numeri complessi che possono essere trasmessi tramite un M^2 -QAM si ottiene una rappresentazione grafica dei simboli possibili, come mostrato in figura 11.11.

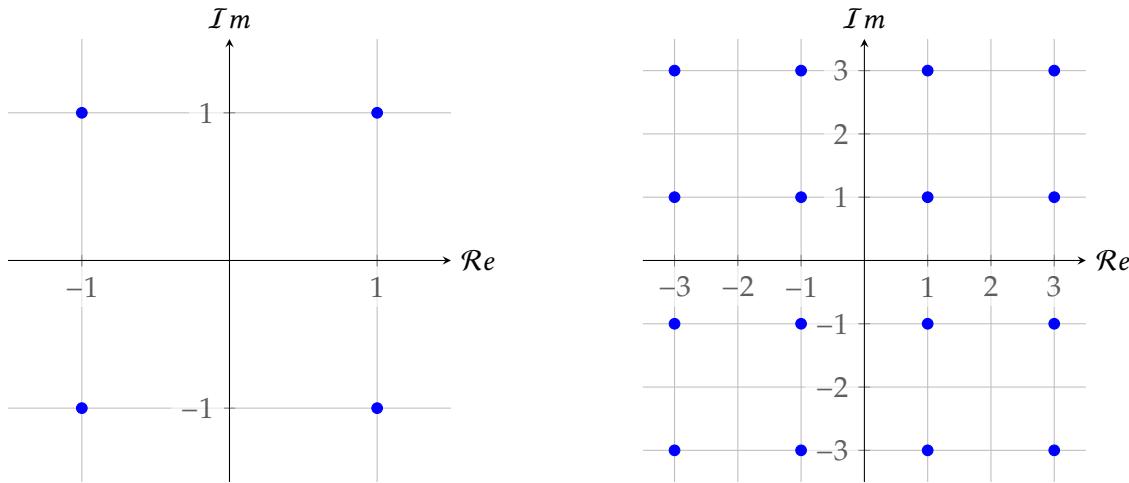


Figura 11.11.: Costellazioni di un 4-QAM e di un 16-QAM.

11.4. Capacità di canale

Modellizzazione di un canale di trasmissione Nelle sezioni precedenti si è visto un metodo per trasmettere attraverso un canale passa-basso e uno analogo per la trasmissione in un canale passa-banda; considerando un 2-PAM lo schema a blocchi della catena di trasmissione è mostrato in figura 11.12.

11. Trasmissione multicanale

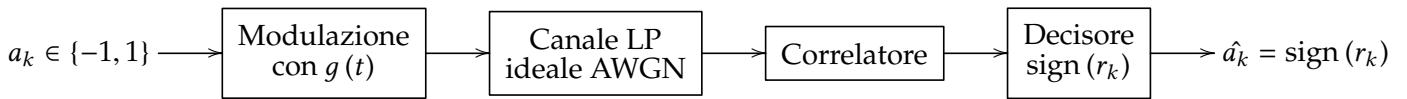


Figura 11.12.: Catena di trasmissione e ricezione di un 2-PAM.

Data questa catena è utile ricavare la capacità del canale e modellizzarlo seguendo i modelli visti nella parte sulla codifica di canale in modo da poter scegliere il giusto codice da utilizzare.

Modellizzazione come canale BSC La modellizzazione più semplice è quella che comprende tutti i blocchi e corrisponde a un BSC la cui probabilità di sbagliare vale:

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

e quindi la capacità del canale è:

$$C = 1 - H_2\left[Q\left(\sqrt{\frac{2 \cdot E_b}{N_0}}\right)\right]$$

Modellizzazione come canale con rumore gaussiano additivo Alternativamente si può escludere il blocco che analizza il segno per ottenere un canale con rumore additivo gaussiano la cui capacità dipende dal rapporto segnale rumore E_b/N_0 .

Confronto tra le due modellizzazioni Come spiegato nell'apposita sezione non si riesce a trovare una formulazione analitica della capacità di un canale con rumore additivo gaussiano e quindi si può fare solamente un confronto grafico che si può vedere in figura 11.13.

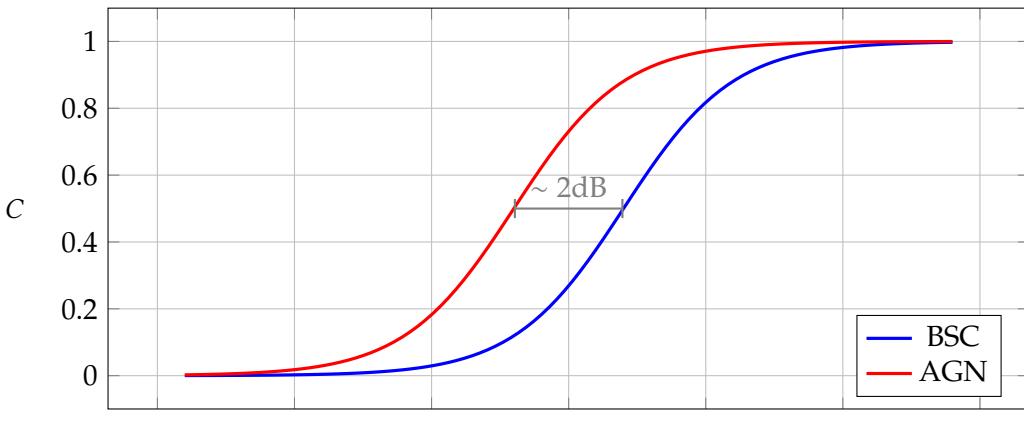


Figura 11.13.: Confronto tra le due modellizzazioni.

Dalla figura si nota che la modellizzazione tramite canale gaussiano ha sempre capacità maggiore; questo è dovuto al fatto che questo canale può sfruttare anche l'informazione sulla quantità di errore e prendere una decisione autonomamente, ma come si è visto i codici per questi canali sono più complessi da realizzare e quindi se il rapporto segnale rumore è alto, e quindi la differenza è poca (come si nota dal grafico), si possono sfruttare i codici per canali BSC molto più semplici.