UNIVERSITÀ DEGLI STUDI DI PISA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
CORSO DI LAUREA IN MATEMATICA

Polarizzazione dei canali B-DMC e Polar Codes

TESI DI LAUREA MAGISTRALE

Giulia Cervia

Relatore
Prof. Paolo Acquistapace
UNIVERSITÀ DI PISA

Relatore
Ing. Salvatore Corvo
THALES ALENIA SPACE

Relatore
Prof. Marco Luise
UNIVERSITÀ DI PISA

Controrelatore
Dott. Massimo Caboara
UNIVERSITÀ DI PISA

ANNO ACCADEMICO 2013/2014

Indice

Introduzione **1**

1 Teoria dell'informazione **5**

1.1 Entropia, mutua informazione e capacità 5

1.2 Canali discreti senza memoria 7

1.3 Casi particolari: canali BSC e BEC 10

1.4 Decodifica 12

1.5 Teorema fondamentale 13

1.6 Inverso debole del teorema fondamentale 17

1.7 Inverso forte del teorema fondamentale nel caso del canale simmetrico 20

2 Polarizzazione dei canali binari **23**

2.1 Polarizzazione 26

2.2 Struttura ricorsiva di $W_N^{(i)}$ 30

2.3 Trasformazione di $I\left(W_N^{(i)}\right)$ e $Z\left(W_N^{(i)}\right)$ 33

2.4 Convergenza di $I\left(W_N^{(i)}\right)$ e $Z\left(W_N^{(i)}\right)$ 38

2.5 Caso del canale simmetrico 43

3 Polar Codes per canali binari **47**

3.1 Codifica 47

3.1.1 Costruzione di G_N 48

3.1.2 Scelta di $\mathcal{A}$ 54

3.2 Decodifica 55

3.2.1 Un primo algoritmo di decodifica 55

3.2.2 Implementazione dell'algoritmo di decodifica 56

3.3 Errori di blocco 63
3.4 Costruzione di Polar Codes dai codici RM 73
3.5 Simulazioni 77

4 Polarizzazione come fenomeno più generale **79**
4.1 Alfabeto di input arbitrario 79
4.2 Matrice di trasformazione dei canali 90

Bibliografia **99**

Introduzione

Col presente lavoro si è inteso ricercare ed analizzare, con i metodi della teoria dell'informazione, una soluzione a un problema di trasmissione afferente a un progetto di larga portata e di alto livello tecnologico, GALILEO.

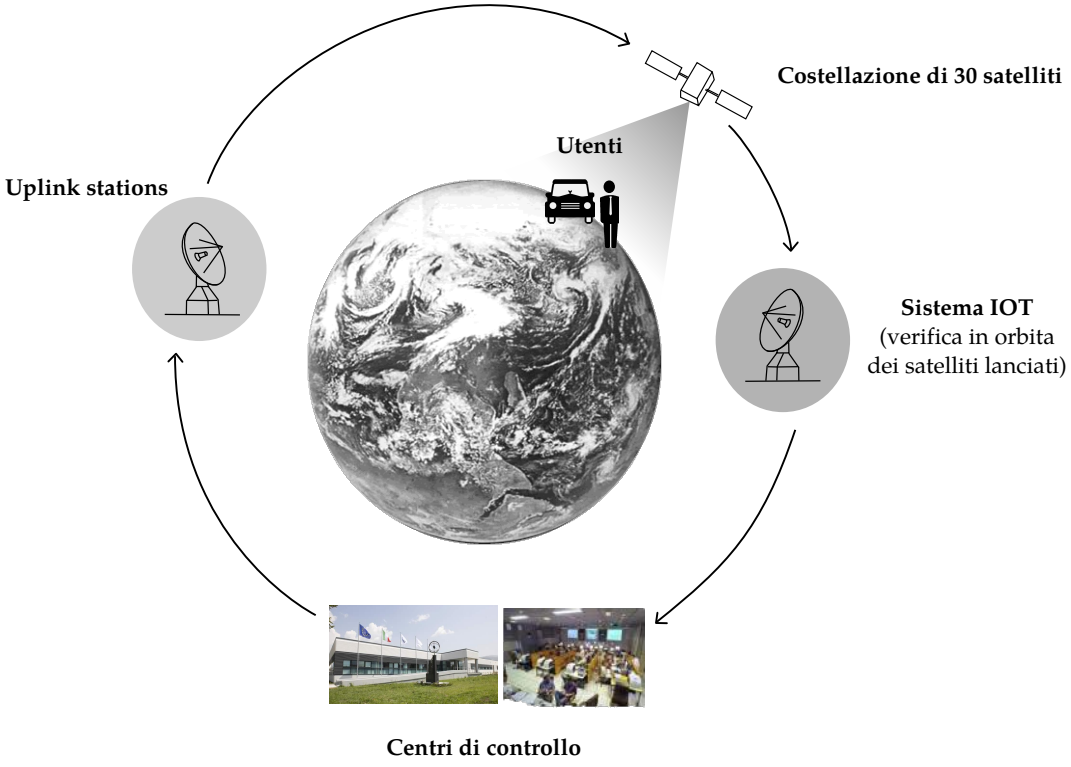

Figura 1: Architettura di Galileo

GALILEO è un'iniziativa dell'Unione Europea, in collaborazione con l'agenzia spaziale europea (ESA) e alcune industrie europee, come Thales Alenia Space che è uno dei partner fondamentali. L'idea è di creare un sistema di posizionamento e navigazione satellitare civile europeo, compatibile con il GPS (controllato dal Dipartimento della Difesa degli Stati Uniti) e con il GLONASS russo, ma indipendente da essi. I principali scopi di Galileo sono:

- maggiore accuratezza nella geo-localizzazione degli utenti;
- aumento della copertura globale dei segnali dei satelliti;
- elevata disponibilità del servizio, di particolare rilevanza per applicazioni che richiedono alti standard di sicurezza.

L'architettura di Galileo, analoga a quella di altri sistemi satellitari globali di navigazione (in inglese GNSS), è composta da tre segmenti, illustrati in Figura 1:

- il segmento spaziale, che comprende una costellazione di 30 satelliti suddivisi in 3 diverse orbite MEO (Medium Earth Orbit),
- il segmento di terra, composto dai centri di controllo e dalle stazioni di uplink che monitorano il segmento spaziale,
- il segmento degli utenti.

I primi due satelliti operativi della costellazione sono stati messi in orbita il 21 ottobre 2011 e altri due sono stati lanciati il 13 ottobre 2012, per testare il sistema Galileo nelle sue strutture di terra e spaziali (fase In-Orbit Validation).

La necessità di rimpiazzare i satelliti della costellazione dopo 10-12 anni fornisce l'opportunità di realizzare alcune migliorie. Per questo motivo, nel 2007 l'ESA ha dato vita all'*European GNSS Evolution Programme* (EGEP) con l'obiettivo di apportare a Galileo modifiche permesse da innovazioni tecnologiche e studi scientifici approfonditi.

Dal *Galileo 2nd Generation* (G2G) ci si aspetta che i satelliti supportino un alto flusso di dati tra terra e spazio e che la comunicazione sia più affidabile rispetto alla prima generazione. A questo proposito vi è la necessità di identificare tecniche di codifica avanzate, quali Turbo-LDPC e Polar coding. Quest'ultima è considerata la più promettente per canali privi di memoria e costituisce l'oggetto di studio di questa tesi.

Uno dei problemi centrali della teoria dell'informazione è riuscire ad inviare messaggi attraverso un canale affetto da rumore con probabilità d'errore arbitrariamente piccola. Da quando Shannon ([22]) ha formalizzato questo problema e ne ha dimostrato la realizzabilità, uno degli obiettivi è stato quello di trovare schemi di codifica che si avvicinino a quest'ideale.
I Polar Codes, introdotti da Arıkan nel 2009 ([3]), sono i primi codici che raggiungono la capacità di canale. La loro costruzione è basata su un metodo, chiamato *polarizzazione dei canali*.
Il canale di partenza, W, è un canale binario discreto e privo di memoria (DMC), con alfabeto di input binario $\mathcal{X} = \{0, 1\}$ e alfabeto di output $\mathcal{Y}$,

$$W : \mathcal{X} \to \mathcal{Y}$$

ed è caratterizzato dalla probabilità di transizione $W(y \mid x)$ (con probabilità di transizione si intende la probabilità che, ricevuto y, sia stato inviato x). La tecnica di polarizzazione dei canali consiste nel costruire ricorsivamente, a partire da W, $N = 2^n$ canali a input binario $\left(W_N^{(1)}, \ldots, W_N^{(N)}\right)$. Questi canali si dicono *polarizzati*, nel senso che si comportano asintoticamente come canali perfetti (l'output ricevuto determina in modo univoco l'input) o inutili

(l'output non fornisce alcuna informazione sull'input), permettendo di creare un metodo di codifica che invii informazioni solo attraverso i canali *asintoticamente perfetti*.
Nel primo capitolo della tesi introduciamo i concetti basilari della teoria dell'informazione, tra i quali:

- l'entropia H, a valori compresi tra 0 e 1, che misura l'incertezza o informazione presente in un segnale aleatorio,
- la mutua informazione I, a sua volta a valori compresi tra 0 e 1, che misura la mutua dipendenza di due variabili aleatorie e permette di quantificare quanto l'output del canale riveli sull'input.

Sempre nel primo capitolo, esaminiamo canali affetti da rumore dimostrando il risultato di Shannon.
Nel secondo capitolo illustriamo il metodo ricorsivo di polarizzazione dei canali. La struttura ricorsiva di $W_N^{(i)}$ può essere pensata come un albero binario in cui, partendo dal canale W, ad ogni passo costruiamo due canali W^- e W^+ fino ad ottenere gli N canali desiderati:

$$W^{-\cdots-} \dots W^{+\cdots+}.$$

Definiamo il processo stocastico $\{K_n(\omega) \mid n \geq 0\}$ come il processo che scorre l'albero e ad ogni nodo sceglie in modo equiprobabile tra il ramo superiore e quello inferiore. La successione di variabili aleatorie $\{I_n \mid n \geq 0\}$, dove I_n è la mutua informazione di K_n, converge ad una variabile aleatoria che assume quasi ovunque i valori 0 o 1, dimostrando che i canali sono stati polarizzati.
Il terzo capitolo è suddiviso in tre parti: codifica, decodifica e stima dell'errore.
Nella prima parte definiamo la matrice di codifica G_N e ne mostriamo la struttura ricorsiva:

$$G_N = B_N G_2^{\otimes \log_2 N} = B_N G_2^{\otimes n}$$

dove B_N è un operatore di inversione di bit e $G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ è la matrice di codifica per $N = 2$.
Successivamente definiamo i Polar Codes come codici a quattro parametri, $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$, dove:

- N è la lunghezza della sequenza di bit da inviare,
- K è il numero di bit della sequenza di input che contengono informazione,
- $\mathcal{A}$ è un'insieme di indici che indica su quali componenti del vettore da inviare si deve inserire informazione, ossia gli indici i per i quali $I(W_N^{(i)})$ è massimo,
- $u_{\mathcal{A}^c}$ è la porzione di vettore da inviare che non contiene informazione, detto insieme dei *frozen bit*

La decodifica mostrata è una decodifica a cancellazione successiva (SC decoder) della quale indaghiamo alcune implementazioni, con particolare attenzione alla classe di canali *a erasure*

(BEC). I Polar Codes sono codici con complessità di codifica e decodifica $O(N \log N)$ la cui probabilità di errore di blocco è molto bassa:

Teorema . Sia W un canale DMC binario con $I(W) > 0$ e siano $N/K < I(W)$ e $\beta < \frac{1}{2}$ fissati. Allora per ogni $N = 2^n$, $n \geq 0$, la migliore la probabilità di errore di blocco per dei polar codes tramite un SC decoder soddisfa

$$P_e(N, R) = O\left(2^{-N^\beta}\right).$$

Nel quarto e ultimo capitolo studiamo la polarizzazione come fenomeno più generale. Se, al posto di un alfabeto binario, l'alfabeto di input è $\{0, \ldots, q-1\}$, si possono definire in modo analogo i parametri di canale e ottenere dei canali polarizzati. Se q è primo, come nel caso binario

$$P_e \leq 2^{-N^\beta} \quad \forall \beta < 1/2.$$

Infine dimostriamo che, presa una qualunque matrice G $n \times n$ con $n \geq 3$ ed un canale DMC binario simmetrico, G è polarizzante (ovvero una sua potenza di Kroeneker polarizza il canale) se e solo se non è triangolare superiore.

1 | Teoria dell'informazione

La teoria dell'informazione studia i *sistemi di comunicazione*, che possiamo rappresentare schematicamente come in Figura 1.1. Il messaggio da trasmettere viene trasformato in una sequenza binaria inviata attraverso il canale. La decodifica interviene sull'output del canale nel tentativo di ritrovare il messaggio originale, operazione che non può essere completamente affidabile a causa del *rumore*, che è un termine generico per indicare qualunque cosa disturbi la trasmissione.

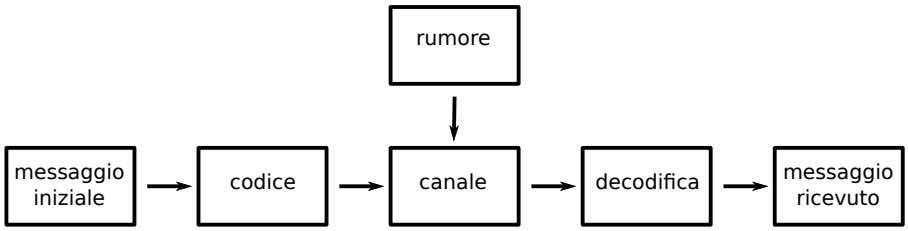

Figura 1.1: Sistema di comunicazione.

Nel corso di questo capitolo analizzeremo i parametri principali di un canale, definiremo classi di canali e arriveremo al teorema fondamentale della teoria dell'informazione, dimostrato da Claude Shannon nel 1948, che garantisce che, per quanto il canale sia affetto da rumore, è possibile trasmettere dati con probabilità d'errore piccola a piacere fino ad una certa frequenza. Tutti i risultati di questo capitolo sono dimostrati in [8].

1.1 Entropia, mutua informazione e capacità

Definizione 1.1. Sia X una variabile aleatoria discreta che può assumere valori $\{x_1, \ldots, x_n\}$ con probabilità $p(x_i)$ rispettivamente, l'entropia (o incertezza) di X è la quantità H definita da

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i).$$

Definizione 1.2. Siano X e Y due variabili aleatorie discrete che possono assumere valori $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_m\}$ rispettivamente; definiamo sia $p(x_i, y_j) = P\{X = x_i, Y = y_j\}$,

definiamo l'entropia congiunta di (X, Y) come

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j) \log p(x_i, y_j).$$

In modo del tutto analogo definiamo l'entropia condizionata di $(X \mid Y = y_j)$ e di $(X \mid Y)$.

Definizione 1.3. Siano X e Y due variabili aleatorie discrete che possono assumere valori $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_m\}$ rispettivamente,

$$H(X \mid Y = y_j) := -\sum_{i=1}^{n} p(x_i \mid y_j) \log p(x_i \mid y_j),$$

$$H(X \mid Y) := -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i \mid y_j) \log p(x_i \mid y_j).$$

Si noti che le definizioni sono ambigue dal momento che la base del logaritmo non è specificata. In realtà, poiché la più comune unità di misura in quest'ambito è il bit, in questo caso tutti i logaritmi andranno intesi in base 2.

Teorema 1.4. *Siano X e Y variabili aleatorie discrete, allora*

$$H(X,Y) \leq H(X) + H(Y)$$

e vale l'uguaglianza se e solo se X e Y sono variabili aleatorie indipendenti.

Corollario 1.5. *Siano $X_1, \ldots, X_n$ variabili aleatorie, allora*

$$H(X_1, \ldots, X_n) \leq H(X_1) + \ldots + H(X_n)$$

e vale l'uguaglianza se e solo se $X_1, \ldots, X_n$ sono variabili aleatorie indipendenti.

Corollario 1.6. *Siano $X = (X_1, \ldots, X_n)$ e $Y = (Y_1, \ldots, Y_m)$ variabili aleatorie vettoriali, allora*

$$H(X_1, \ldots, X_n, Y_1, \ldots, X_m) \leq H(X_1, \ldots, X_n) + H(Y_1, \ldots, Y_m)$$

e vale l'uguaglianza se e solo se X e Y sono indipendenti, ovvero se e solo se

$$P\{X_1 = \alpha_1, \ldots, X_n = \alpha_n, Y_1 = \beta_1, \ldots, Y_m = \beta_m\} =$$

$$P\{X_1 = \alpha_1, \ldots, X_n = \alpha_n\} P\{Y_1 = \beta_1, \ldots, Y_m = \beta_m\}$$

per ogni $\alpha_1, \ldots, \alpha_n$ $\beta_1, \ldots, \beta_m$.

Teorema 1.7. *Siano X e Y due variabili aleatorie, allora*

$$H(X,Y) = H(X) + H(Y \mid X) = H(Y) + H(X \mid Y).$$

A questo punto possiamo introdurre la definizione di *mutua informazione* di due variabili aleatorie, ovvero quella funzione che misura la mutua dipendenza delle due variabili.

Definizione 1.8. Siano X e Y due variabili aleatorie, definiamo la mutua informazione di X relativa a Y come

$$I(X \mid Y) = H(X) - H(X \mid Y).$$

Proposizione 1.9. *La mutua informazione I ha le seguenti proprietà:*

(i) $I(X \mid Y) \geq 0 \quad e \quad I(X \mid Y) = 0$ *se e solo se X e Y sono indipendenti;*

(ii) $I(X \mid Y) = I(Y \mid X)$*;*

(iii) $I(X_1, \ldots, X_n \mid Y_1, \ldots, Y_m) = H(X_1, \ldots, X_n) - H(X_1, \ldots, X_n \mid Y_1, \ldots, Y_m)$*;*

(iv) $I(X_1, \ldots, X_n \mid Y_1, \ldots, Y_m) = I(Y_1, \ldots, Y_m \mid X_1, \ldots, X_n)$.

Osserviamo che, se ci immaginiamo il canale come un input X e un output Y, l'informazione processata dal canale dipende dalla distribuzione di input p. Possiamo variare la distribuzione di input affinché l'informazione raggiunga un massimo, che chiamiamo *capacità del canale*.

Definizione 1.10. Definiamo la capacità del canale $C = \max_{p(x)} I(X \mid Y)$.

Ci resta un'ultima definizione, quella della *divergenza di Kullback-Leibler*.

Definizione 1.11. Siano p, q due distribuzioni di probabilità discrete, la divergenza di Kullback-Leibler è definita da:

$$D(p\|q) = \sum_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)}.$$

Osservazione 1.12. Possiamo esprimere la mutua informazione in funzione della divergenza di Kullback-Leibler:

$$\begin{aligned} I(X \mid Y) &= E\left[D(p(X \mid Y)\|p(X)\right] \\ &= D(p(X,Y)\|p(X)p(Y)). \end{aligned}$$

1.2 Canali discreti senza memoria

Fino a questo punto abbiamo dato dei canali una definizione intuitiva, diamone una più formale e completa.

Definizione 1.13. Siano Γ e Γ' insiemi finiti, chiamati rispettivamente alfabeto di input e alfabeto di output, e sia S un insieme che chiamiamo insieme degli stati; un canale discreto è un sistema di distribuzioni di probabilità

$$p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n; s)$$

$$\text{ove } \alpha_1, \dots, \alpha_n \in \Gamma, \quad \beta_1, \dots, \beta_n \in \Gamma', \quad s \in S \quad \text{e} \quad n \in \mathbb{N}\,.$$

Possiamo interpretare $p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n; s)$ come la probabilità che la sequenza $\beta_1, \dots, \beta_n$ sia l'output della sequenza di input $\alpha_1, \dots, \alpha_n$ e lo stato iniziale (ovvero lo stato prima di α_1) sia s.

Definizione 1.14. Un canale discreto è privo di memoria se:

(i) $p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n; s)$ non dipende dallo stato s per ogni scelta di $\alpha_1, \dots, \alpha_n$ in Γ e di $\beta_1, \dots, \beta_n$ in Γ'. In tal caso possiamo scrivere $p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n)$ omettendo il simbolo s;

(ii) $p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n) = p_1(\beta_1 \mid \alpha_1) \dots p_n(\beta_n \mid \alpha_n)$ per ogni scelta di $\alpha_1, \dots, \alpha_n$ in Γ e di $\beta_1, \dots, \beta_n$ in Γ'.

La seconda condizione può essere sostituita da altre due condizioni, come mostra il seguente risultato.

Lemma 1.15. *Siano $p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n; s)$ funzioni di probabilità che soddisfino la condizione (i) della Definizione 1.14, definiamo*

- *la probabilità che i primi $n-k$ simboli di output siano $\beta_1, \dots, \beta_{n-k}$ se la sequenza di input è $\alpha_1, \dots, \alpha_n$*

$$p_n(\beta_1, \dots, \beta_{n-k} \mid \alpha_1, \dots, \alpha_n) := \sum_{\beta_{n-k+1}, \dots, \beta_n \in \Gamma'} p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n) \quad 1 \le k \le n-1;$$

- *la probabilità che l'n-simo simbolo di output sia β_n sapendo che la sequenza di input è $\alpha_1, \dots, \alpha_n$ e i primi $n-1$ simboli di output sono $\beta_1, \dots, \beta_{n-1}$*

$$p_n(\beta_n \mid \alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_{n-1}) := \frac{p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n)}{p_n(\beta_1, \dots, \beta_{n-1} \mid \alpha_1, \dots, \alpha_n)}.$$

Le probabilità p_n soddisfano la condizione (ii) della Definizione 1.14 se e solo se per ogni $n \ge 1$, $n \in \mathbb{N}$ sono soddisfatte entrambe le seguenti:

(a) $p_n(\beta_n \mid \alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_{n-1}) = p_1(\beta_n \mid \alpha_n)$ *per ogni* $\alpha_1, \dots \alpha_n \in \Gamma, \quad \beta_1, \dots, \beta_n \in \Gamma'$, *ovvero la probabilità che l'n-simo simbolo di output sia β_n dipende solo dall'n-simo simbolo di input α_n*

(b) $p_n(\beta_1, \dots, \beta_{n-k} \mid \alpha_1, \dots, \alpha_n) = p_{n-k}(\beta_1, \dots, \beta_{n-k} \mid \alpha_1, \dots, \alpha_{n-k})$ *per ogni* $\alpha_1, \dots \alpha_n \in \Gamma$, $\beta_1, \dots, \beta_{n-k} \in \Gamma' \quad e \quad 1 \le k \le n-1$, *ovvero la probabilità che i primi $n-k$ simboli di output siano $\beta_1, \dots, \beta_{n-k}$ dipende solo dai primi $n-k$ simboli di input $\alpha_1, \dots, \alpha_{n-k}$.*

Dimostrazione. Supponiamo che la condizione (ii) della Definizione 1.14 sia soddisfatta. Allora vale

$$\begin{aligned} p_n(\beta_n \mid \alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_{n-1}) &= \frac{p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n)}{p_n(\beta_1, \dots, \beta_{n-1} \mid \alpha_1, \dots, \alpha_n)} \\ &= \frac{\prod_{k=1}^{n} p_1(\beta_k \mid \alpha_k)}{\sum_{\beta_n \in \Gamma'} p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n)} \\ &= \frac{\prod_{k=1}^{n} p_1(\beta_k \mid \alpha_k)}{\sum_{\beta_n \in \Gamma'} \prod_{k=1}^{n} p_1(\beta_k \mid \alpha_k)} \\ &= \frac{\prod_{k=1}^{n} p_1(\beta_k \mid \alpha_k)}{\prod_{k=1}^{n-1} p_1(\beta_k \mid \alpha_k) \sum_{\beta_n \in \Gamma'} p_1(\beta_n \mid \alpha_n)} \\ &= p_1(\beta_n \mid \alpha_n) \end{aligned}$$

e al condizione (a) è provata.
Per dimostrare la condizone (b), osserviamo che il ragionamento appena visto mostra che

$$p_n(\beta_1, \dots, \beta_{n-1} \mid \alpha_1, \dots, \alpha_n) = \prod_{k=1}^{n-1} p_1(\beta_k \mid \alpha_k) = p_{n-1}(\beta_1, \dots, \beta_{n-1} \mid \alpha_1, \dots, \alpha_{n-1})$$

e quindi possiamo dimostrare (b) per induzione.
Viceversa, se (a) e (b) sono verificate, abbiamo

$$\begin{aligned} p_n(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n) &= p_n(\beta_1, \dots, \beta_{n-1} \mid \alpha_1, \dots, \alpha_n) p_n(\beta_n \mid \alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_{n-1}) \\ &= p_{n-1}(\beta_1, \dots, \beta_{n-1} \mid \alpha_1, \dots, \alpha_{n-1}) p_1(\beta_n \mid \alpha_n) \end{aligned}$$

e induttivamente ttroviamo la condizione (ii) della Definizione 1.14. □

Un canale discreto privo di memoria è caratterizzato da una matrice in cui l'elemento di posto (i, j) è $p_1(\beta_j \mid \alpha_i)$, dove $\beta_j \in \Gamma'$ e $\alpha_i \in \Gamma$ (d'ora in poi scriveremo $p(\beta_j \mid \alpha_i)$ al posto di $p_1(\beta_j \mid \alpha_i)$).

A questo punto possiamo introdurre alcune classi di canali di più facile trattazione. Un canale è:

- *privo di perdite* se $H(X \mid Y) = 0$ per ogni distribuzione di input;
- *deterministico* se $p(y_j \mid x_i)$ assume solo i valori 0 e 1 per ogni i e per ogni j;
- *privo di rumore* se è privo di perdite e deterministico;
- *a capacità zero* se $I(X \mid Y) = 0$ per ogni distribuzione di input;
- *simmetrico* se tutte le righe della matrice di canale contengono gli stessi elementi $p'_1, \dots, p'_n$ e tutte le colonne contengono gli stessi elementi $q'_1, \dots, q'_m$.

La classe di canali discreti privi di memoria sarà particolarmente significativa per questo lavoro e la denotiamo con DMC, B-DMC nel caso l'alfabeto sia binario.

1.3 Casi particolari: canali BSC e BEC

Canali BSC

Un *canale binario simmetrico* è un canale che può trasmettere solo 0 o 1 e che riceve correttamente con probabilità $1-p$ e riceve il digit sbagliato con probabilità p. Questa probabilità p prende il nome di *probabilità di crossover*.
Questi canali sono il modello più semplice di canale affetto da rumore.

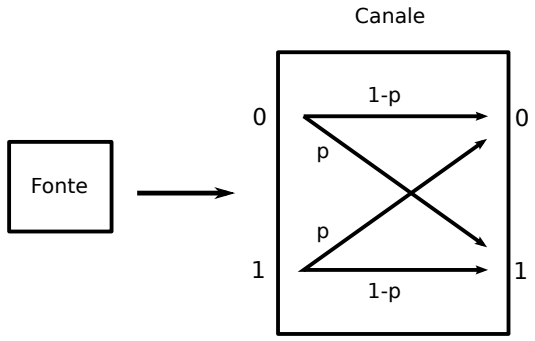

Figura 1.2: Esempio di canale binario simmetrico (BSC).

Diamo la definizione più formale.

Definizione 1.16. Un BSC con probabilità di crossover p è un canale caratterizzato da:

- alfabeto di input $\mathcal{X} = \{0, 1\}$;
- alfabeto di output $\mathcal{Y} = \{0, 1\}$;
- probabilità condizionali

$$\begin{aligned} P\{Y = 0 \mid X = 0\} &= 1 - p \\ P\{Y = 1 \mid X = 0\} &= p \\ P\{Y = 0 \mid X = 1\} &= p \\ P\{Y = 1 \mid X = 1\} &= 1 - p. \end{aligned}$$

  dove X è la variabile aleatoria che rappresenta l'input e Y la variabile aleatoria che rappresenta l'output.

Osservazione 1.17. La capacità di un canale BSC è $1 - H(p)$, dove H è la funzione di entropia binaria.

Canali BEC

Un *canale a erasure binario* o *binary erasure channel* (BEC) è un modello di canale in cui viene inviato un bit e il ricevente o riceve il bit inviato oppure riceve un messaggio che lo informa del fatto che il bit non è stato ricevuto.

Il canale BEC è, in un certo senso, privo di errore. Infatti, quando viene ricevuto 0 o 1, si ha la certezza che la trasmissione sia stata corretta e vi è ambiguità solo quando arriva il messaggio che informa dell'errore. Tale messaggio è rappresentato dal *simbolo di erasure*.

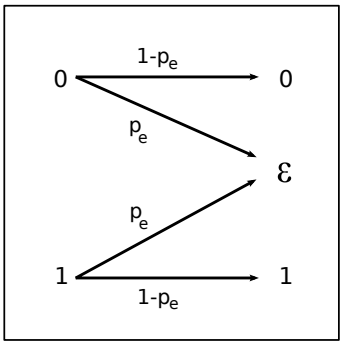

Figura 1.3: Canale a erasure (BEC)

Diamo la definizione di questa classe di canali in modo più formale.

Definizione 1.18. Un canale BEC con probabilità di cancellazione (anche detta probabilità di erasure) p_e è un canale caratterizzato da:

- alfabeto di input binario $\mathcal{X} = \{0, 1\}$;
- alfabeto di output ternario $\mathcal{Y} = \{0, 1, \varepsilon\}$, dove ε è il simbolo di erasure;
- probabilità condizionali

$$\begin{aligned} P\{Y = 0 \mid X = 0\} &= 1 - p_e \\ P\{Y = \varepsilon \mid X = 0\} &= p_e \\ P\{Y = 1 \mid X = 0\} &= 0 \\ P\{Y = 0 \mid X = 1\} &= 0 \\ P\{Y = \varepsilon \mid X = 1\} &= p_e \\ P\{Y = 1 \mid X = 1\} &= 1 - p_e. \end{aligned}$$

dove X è la variabile aleatoria che rappresenta l'input e Y la variabile aleatoria che rappresenta l'output.

Osservazione 1.19. La capacità di un canale BEC è $1 - p_e$.

1.4 Decodifica

Consideriamo adesso il problema dell'affidabilità della trasmissione se il canale è disturbato da un rumore: ricevuta una sequenza di output cerchiamo il modo migliore per risalire alla corretta sequenza di input.

Definizione 1.20. Supponiamo di avere un canale con alfabeto di input $x_1, \dots, x_M$, alfabeto di output $y_1, \dots, y_L$ e matrice $[p(y_j \mid x_i)]$. Uno schema di decodifica è l'assegnamento ad un simbolo di output y_j di un simbolo di input x_j^* dell'alfabeto $x_1, \dots, x_M$.

L'interpretazione è che quando il simbolo y_j viene ricevuto, è decodificato come x_j^*. Lo schema di decodifica può essere pensato come un canale deterministico con alfabeto di input $y_1, \dots, y_L$ e alfabeto di output $x_1, \dots, x_M$.
Se abbiamo una distribuzione di probabilità fissata $p(x)$, vorremmo poter costruire uno schema di decodifica che minimizza la probabilità di errore e un tale schema di decodifica prende il nome *osservatore ideale*.
A questo scopo, supponiamo che a ciascun simbolo y_j sia associato un simbolo x_j^* per $j = 1, \dots, L$, cosicché se y_j è l'output, la probabilità che la trasmissione sia avvenuta correttamente è la probabilità che x_j^* sia l'input. Se denotiamo con $p(e)$ la probabilità di errore e $p(e')$ la probabilità che la trasmissione sia stata corretta, possiamo scrivere

$$p(e') = \sum_{j=1}^{L} p(y_j)p(e' \mid y_j) = \sum_{j=1}^{L} p(y_j)P\{X = x_j^* \mid y_j\}$$

dove ricordiamo che $p(y_j)$ dipende solo dalla distribuzione di input e dalla matrice del canale.

Definizione 1.21. L'osservatore ideale è lo schema di decodifica che associa a ciascun simbolo di output y_j l'input x tale che $p(x \mid y_j)$ sia massima.

Analogamente, se consideriamo una situazione in cui una sequenza $x = (\alpha_1, \dots, \alpha_n)$ sia scelta con probabilità $p(x) = p(\alpha_1, \dots, \alpha_n)$, allora la probabilità che l'output sia $(\beta_1, \dots, \beta_n)$ è data da

$$\begin{aligned} p(\beta_1, \dots, \beta_n) &= \sum_{\alpha_1, \dots, \alpha_n} p(\alpha_1, \dots, \alpha_n)p(\beta_1, \dots, \beta_n \mid \alpha_1, \dots, \alpha_n) \\ &= \sum_{\alpha_1, \dots, \alpha_n} p(\alpha_1, \dots, \alpha_n)p(\beta_1 \mid \alpha_1) \dots p(\beta_n \mid \alpha_n). \end{aligned}$$

Lo schema di decodifica può essere definito come la funzione che assegna a ciascuna sequenza di output $(\beta_1, \dots, \beta_n)$ una sequenza in input $(\alpha_1, \dots, \alpha_n)$ e l'osservatore ideale è lo schema di decodifica che massimizza la probabilità condizionale

$$p(\alpha_1, \dots, \alpha_n \mid \beta_1, \dots, \beta_n) = \frac{p(\alpha_1, \dots, \alpha_n) \prod_{k=1}^{n} p(\beta_k \mid \alpha_k)}{p(\beta_1, \dots, \beta_n)}.$$

Un caso particolare è quello in cui tutti gli input $x_1, \ldots, x_M$ sono equiprobabili, in questo caso

$$p(x_i \mid y) = \frac{p(x_i)p(y \mid x_i)}{p(y)} = \frac{1}{M}\frac{p(y \mid x_i)}{p(y)}.$$

Quindi, se y é fissato, massimizzare $p(x_i \mid y)$ equivale a massimizzare $p(y \mid x_i)$ e lo schema di decodifica che sceglie l'input x_i tale che $p(y \mid x_i)$ sia massimo, ovvero l'osservatore ideale, prende anche il nome, in questo caso, di schema di decisione di *massima verosimiglianza*.

Osservazione 1.22. L'osservatore ideale soffre dello svantaggio dell'essere definito solo per una particolare distribuzione di input e, per di più, può accadere che certi input non siano mai ricevuti correttamente, mentre sarebbe più desiderabile avere uno schema di decodifica per il quale la probabilità di errore sia uniformemente limitata.

1.5 Teorema fondamentale

In questo paragrafo cercheremo di mostrare come sia possibile trametterе informazioni attraverso un canale ad ogni tasso d'informazione (dove il tasso è il numero di digits tramessi al secondo) minore della capacità del canale con probabilità di errore arbitrariamente piccola. A questo scopo dobbiamo prima introdurre alcune definizioni.

Definizione 1.23. Dato una canale discreto privo di memoria, una n-sequenza in input e una di output, un codice (s, n) è un insieme di s n-sequenze di input $x^{(1)}, \ldots, x^{(s)}$, chiamate codewords, e di uno schema di decodifica.

Definizione 1.24. La massima probabilità di errore di un codice è definita da

$$p_m(e) = \max_{1 \le i \le s} p(e \mid x^{(i)}).$$

Definizione 1.25. Un codice (s, n, λ) è un codice (s, n) la cui massima probabilità di errore sia minore o uguale a λ

Enunciamo ora il teorema fondamentale della teoria dell'informazione, o teorema di Shannon.

Teorema 1.26 (Teorema di Shannon)**.** *Dato un canale discreto privo di memoria con capacità $C > 0$ e tasso R, $0 < R < C$, esiste una successione di codici $\mathcal{A}_1, \mathcal{A}_2, \ldots$ tale che:*

- *ciascun $\mathcal{A}_n$ sia un $(2^{nR}, n, \lambda_n)$ codice;*
- *la massima probabilità d'errore λ_n tenda a 0 per $n \to +\infty$.*

Per dimostrare il teorema abbiamo bisogno di un risultato, che chiamiamo Lemma Fondamentale.

Lemma 1.27 (Lemma Fondamentale)**.** *Dato un canale discreto privo di memoria, sia n un intero positivo e $p(x)$ una distribuzione di probabilità sulle n-sequenza di input. Sia x una n-sequenza di*

input e y una di output, definiamo per ogni $a \in \mathcal{R}$

$$A = \left\{ (x,y) \middle| \log \frac{p(y \mid x)}{p(y)} > a \right\}.$$

Allora per ogni intero positivo s esiste un (s, n, λ) codice tale che

$$\lambda \leq \frac{s}{2^a} + P\{(X,Y) \notin A\}$$

dove $P\{(X,Y) \notin A\}$ è calcolata a partire da $p(x)$.

Dimostrazione. Il messaggio essenziale del lemma fondamentale è che, fissata una distribuzione di probabilità $p(x)$, possiamo costruire un codice la cui massima probabilità d'errore sia limitata da $\epsilon = \frac{s}{2^a} + P\{(X,Y) \notin A\}$. Procediamo quindi costruendo iterativamente il codice

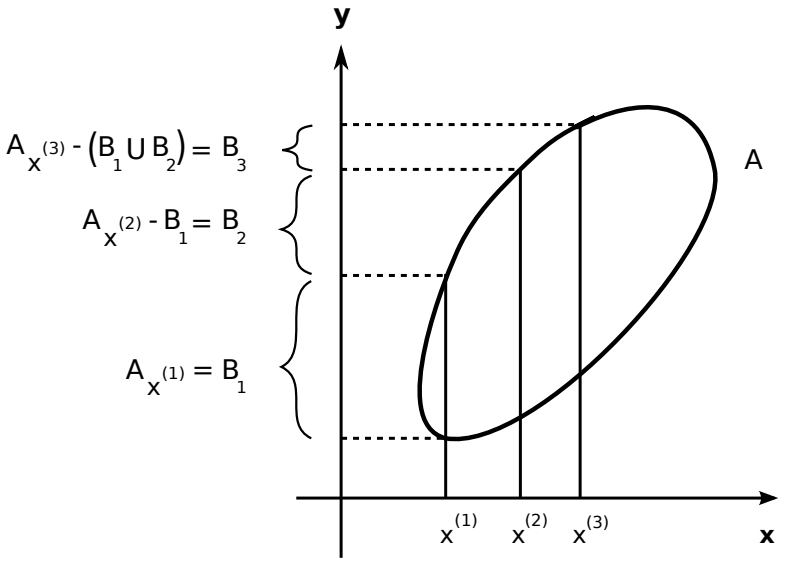

Figura 1.4: Prova del Lemma Fondamentale

come mostrato schematicamente nella Figura 1.4.
Sia x una n-sequenza di input, chiamiamo $A_x = \{y \,|(x,y) \in A\}$. Se $\epsilon \geq 1$ il lemma è banalmente vero, supponiamo quindi $0 < \epsilon < 1$.
Sia $x^{(1)}$ una qualunque n-sequenza di input tale che

$$P\left\{ Y \in A_{x(1)} \middle| X = x^{(1)} \right\} \geq 1 - \epsilon$$

e denotiamo con B_1 l'insieme $A_{x(1)}$. Scegliamo adesso $x^{(2)}$ tale che

$$P\left\{ Y \in A_{x(2)} - B_1 \middle| X = x^{(2)} \right\} \geq 1 - \epsilon$$

e denotiamo con B_2 l'insieme $A_{x(2)} - B_1$. Supponiamo di aver scelto $x^{(1)}, \ldots, x^{(k-1)}$ e di aver

definito gli insiemi $B_1, \ldots, B_{k-1}$ disgiunti tra loro, scegliamo adesso $x^{(k)}$ tale che

$$P\left\{Y \in A_{x(k)} - \bigcup_{i=1}^{k-1} B_i \,\middle|\, X = x^{(k)}\right\} \geq 1 - \epsilon$$

e definiamo $B_k = A_{x(k)} - \bigcup_{i=1}^{k-1} B_i$. Poiché le sequenze di input sono un numero finito, il processo termina dopo t passi. Se mostriamo che $t \geq s$, allora la sequenza $x^{(1)}, \ldots, x^{(s)}$ e il corrispondente schema di decodifica $B_1, \ldots, B_s$ formano per costruzione un (s, n, λ) codice con

$$\lambda \leq \max_{1 \leq i \leq s} P\{Y \notin B_i | X = x_i\} \leq \epsilon.$$

Per mostrare che $t \geq s$, proviamo che $\epsilon \leq \frac{t}{2^a} + P\{(X, Y) \notin A\}$.
Consideriamo $P\{(X, Y) \in A\}$,

$$P\{(X,Y) \in A\} = \sum_{(x,y) \in A} p(x,y) = \sum_x p(x) \left(\sum_{y \in A_x} p(y \mid x) \right).$$

Sia $B = \bigcup_{j=1}^{t} B_j$ (se $t = 0$, poniamo $B = \emptyset$), allora

$$P\{(X,Y) \in A\} = \sum_x p(x) \left(\sum_{y \in B \cap A_x} p(y|x) \right) + \sum_x p(x) \left(\sum_{y \in B^C \cap A_x} p(y|x) \right). \tag{1.1}$$

Dal momento che $B \cap A_x \subset B$, il primo termine della somma sopra è minore o uguale di

$$\sum_x p(x) \sum_{y \in B} p(x \mid y) = P\{Y \in B\}$$

ma d'altro canto, poiché $B_i \subset A_{x^{(i)}}$,

$$P\{Y \in B\} = \sum_{i=1}^{t} P\{Y \in B_i\} \leq \sum_{i=1}^{t} P\{Y \in A_{x^{(i)}}\}.$$

Preso $y \in A_{x^{(i)}}$, $x^{(i)}, y$ appartiene ad A e quindi

$$\log \frac{p\left(y \mid x^{(i)}\right)}{p(y)} > a$$

che equivale a dire (poiché la base del logaritmo è 2)

$$p(y) < p\left(y \mid x^{(i)}\right) 2^{-a}.$$

Ne segue che

$$P\left\{Y \in A_{x^{(i)}}\right\} = \sum_{y \in A_{x^{(i)}}} p(y) \leq 2^{-a} \sum_{y \in A_{x^{(i)}}} p\left(y \mid x^{(i)}\right) \leq 2^{-a}$$

e quindi il primo termine di (1.1) è minore o uguale di $t/2^a$.
Per stimare il secondo termine, iniziamo coll'osservare che $B^C \cap A_x = \emptyset$ se x è una codeword $x^{(k)}$. Per verificarlo, diciamo che se una sequenza y appartiene a $A_{x^{(k)}}$, y appartiene a B, infatti sappiamo che $B_k = A_{x^k} - \bigcup_{i=1}^{k-1} B_i$, quindi se y non appartiene a $\bigcup_{i=1}^{k-1} B_i$, allora y appartiene a B_k e, viceversa, se y appartiene a $\bigcup_{i=1}^{k-1} B_i$, y appartiene a B.
Osserviamo che se $x = x^{(1)}, \ldots, x^{(t)}$,

$$\sum_{y \in B^C \cap A_x} p(y \mid x) < 1 - \epsilon.$$

Se x non è uguale a nessun $x^{(i)}$ e se per assurdo $P\{Y \in B^C \cap A_x \mid X = x\} \geq 1 - \epsilon$, allora poichè $B^c \cap A = A_x - \bigcup_{i=1}^{t} B_i$, potremmo aumentare la dimensione del codice aggiungendo la sequenza $x^{(t+1)}$ e l'insieme $B_{t+1} = B^C \cap A_{x^{(t+1)}}$, contraddicendo l'ipotesi che il processo termini dopo t passi. Quindi

$$\sum_{y \in B^C \cap A_x} p(y \mid x) < 1 - \epsilon \quad \text{per ogni sequenza di input } x$$

e il secondo termine di (1.1) è minore o uguale a $1 - \epsilon$. Ma allora

$$P\{(X,Y) \in A\} \leq \frac{t}{2^a} + 1 - \epsilon,$$

$$\epsilon \leq \frac{t}{2^a} + P\{(X,Y) \notin A\}$$

e la dimostrazione del lemma è conclusa.

□

Adesso possiamo dimostrare il teorema fondamentale.

Dimostrazione. Sia n un intero positivo e $p_0(\alpha)$ una distribuzione di input che raggiunge la capacità di canale. Applichiamo il Lemma 1.27 con $s = [2^{nR}]$, $a = n[(R + C)/2] < nC$ e $p(x)$ scelta prendendo $X_1, \ldots, X_n$ indipendenti tra loro, ciascuna avente distribuzione $p_0(\alpha)$, quindi per $x = (\alpha_1, \ldots, \alpha_n)$, abbiamo

$$p(x) = p(\alpha_1, \ldots, \alpha_n) = \prod_{i=1}^{n} p_0(\alpha_i).$$

Per il Lemma 1.27, esiste un codice $\left([2^{nR}], n, \lambda_n\right)$ tale che

$$\lambda_n \leq [2^{nR}] 2^{-\frac{1}{2}n(R+C)} + P\{(X,Y) \notin A\}. \tag{1.2}$$

Poiché R è minore di C, il primo termine di (1.2) tende a 0 quando n tende a infinito. Per quanto riguarda il termine

$$P\{(X,Y) \notin A\} = P\left\{(x,y) \middle| \log \frac{p(y \mid x)}{p(y)} \leq a\right\},$$

notiamo che poiché $X_1, \ldots . X_n$ sono indipendenti, lo sono anche $Y_1, \ldots, Y_n$. Osserviamo che

$$P\{Y_1 = \beta_1, \ldots, Y_n = \beta_n\} =$$

$$\sum_{\alpha_1,\ldots,\alpha_n} P\{X_1 = \alpha_1, \ldots, X_n = \alpha_n\} P\{Y_1 = \beta_1, \ldots, Y_n = \beta_n | X_1 = \alpha_1, \ldots, X_n = \alpha_n\} =$$

$$\sum_{\alpha_1,\ldots,\alpha_n} p_0(\alpha_1) \ldots p_0(\alpha_n) p(\beta_1 \mid \alpha_1) \ldots p(\beta_n \mid \alpha_n) =$$

$$\prod_{i=1}^{n} \left(\sum_{\alpha_i} p_0(\alpha_i) p(\beta_i \mid \alpha_i) \right) = \prod_{i=1}^{n} P\{Y_i = \beta_i\}.$$

Questo implica che

$$\begin{aligned} P\{(X,Y) \notin A\} &= P\left\{ (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n) \Big| \log \left(\prod_{i=1}^{n} \frac{p(\beta_i \mid \alpha_i)}{p(\beta_i)} \right) \leq a \right\} \\ &= P\left\{ (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n) \Big| \frac{1}{n} \sum_{i=1}^{n} \log \frac{p(\beta_i \mid \alpha_i)}{p(\beta_i)} \leq \frac{R+C}{2} \right\}. \end{aligned}$$

Per ogni $k = 1, 2, \ldots, n$ definiamo una variabile aleatoria $U(X_k, Y_k)$ come segue:

$$U(X_k, Y_k) = \log \frac{p(\beta_k \mid \alpha_k)}{p(\beta_k)} \quad \text{se } X_k = \alpha_k, Y_k = \beta_k.$$

Le variabili aleatorie $U(X_1, Y_1), \ldots, U(X_n, Y_n)$ sono indipendenti, identicamente distribuite e hanno valore atteso

$$\sum_{\alpha_k, \beta_k} p(\alpha_k, \beta_k) \log \frac{p(\beta_k \mid \alpha_k)}{p(\beta_k)} = H(Y_k) - H(Y_k \mid X_k) + C$$

quindi possiamo scrivere

$$P\{(X,Y) \notin A\} = P\left\{ \frac{1}{n} \sum_{i=1}^{n} U(X_i, Y_i) \leq \frac{R+C}{2} \right\}$$

e, per la legge debole dei grandi numeri, $\frac{1}{n} \sum_{i=1}^{n} U(X_i, Y_i)$ converge a C. Poiché $\frac{1}{2}(R+C)$ è minore di C,

$$P\{(X,Y) \notin A\} \to 0 \quad n \to \infty$$

e la dimostrazione è completa. □

1.6 Inverso debole del teorema fondamentale

In questa sezione dimostriamo un risultato che può essere considerato l'inverso debole del teorema fondamentale.
Prima, enunciamo e dimostriamo un teorema che mette in relazione la probabilità di errore di

un codice con l'entropia.

Teorema 1.28. *Supponiamo di avere un codice (s, n) composto dalle codewords $x^{(1)}, \dots, x^{(s)}$ e $X = (X_1, \dots, X_n)$ una variabile aleatoria tale che X_i assuma il valore $x^{(i)}$ con probabilità $p(x^{(i)})$, $i = 1, 2, \dots, s$, dove $\sum_{i=1}^{s} p(x^{(i)}) = 1$. Sia $Y = (Y_1, \dots, Y_n)$ la corrispondente sequenza di output, se $p(e)$ è la probabilità di errore del codice, allora*

$$H(X \mid Y) \leq H(p(e), 1 - p(e)) + p(e) \log(s - 1).$$

Dimostrazione. Sia y una sequenza di output qualunque e $g(y)$ l'input scelto dal decoder in modo che, se y è ricevuto, si verifica un errore se e solo se la sequenza trasmessa è diversa da $g(y)$.
Possiamo dividere X in due gruppi,

$$X = \{g(y)\} \cup \{x \mid x \neq g(y)\}$$

e otteniamo

$$H(X \mid Y = y) = H(q, 1 - q) + qH(1) + (1 - q)H(q_1, \dots, q_{s-1})$$

dove $q = P\{X = g(y) \mid Y = y\}$ e $q_1, \dots, q_{s-1}$ sono della forma

$$\frac{p(x \mid y)}{\sum_{x \neq g(y)} p(x \mid y)}$$

con x che varia tra tutte le codewords tranne $g(y)$.
Poiché $H(q_1, \dots, q_{s-1}) \leq \log(s - 1)$,

$$H(X \mid Y = y) \leq H(p(e \mid y), 1 - p(e \mid y)) + p(e \mid y) \log(s - 1) \tag{1.3}$$

e, per la convessità di H,

$$\begin{aligned} H(p(e), 1 - p(e)) &= H\left(\sum_y p(y)p(e \mid y), 1 - \sum_y p(y)p(e \mid y)\right) \\ &= H\left(\sum_y p(y)p(e \mid y), \sum_y p(y)(1 - p(e \mid y))\right) \\ &\geq \sum_y p(y) H\left(p(e \mid y), 1 - p(e \mid y)\right). \end{aligned}$$

Allora, se moltiplichiamo (1.3) per $p(y)$ e sommiamo su y, usando la formula sopra, troviamo che

$$H(X \mid Y) \leq H(p(e), 1 - p(e)) + p(e) \log(s - 1),$$

come volevamo. □

Ci serve adesso un lemma.

Lemma 1.29. *Sia $X_1, \dots, X_n$ una sequenza di input di un canale discreto privo di memoria (DMC) e sia $Y_1, \dots, Y_n$ l'output corrispondente. Allora*

$$I(X_1, \dots, X_n \mid Y_1, \dots, Y_n) \leq \sum_{i=1}^{n} I(X_i \mid Y_i)$$

e vale l'uguaglianza se e solo se $Y_1, \dots, Y_n$ sono indipendenti.

Dimostrazione. La formula

$$H(X_1, \dots, X_n \mid Y_1, \dots, Y_n) = \sum_{(x,y)} p(x,y) \log p(x,y)$$

con $x = (\alpha_1, \dots, \alpha_n)$, $y = (\beta_1, \dots, \beta_n)$ e $p(x \mid y) = p(\beta_1 \mid \alpha_1) \dots p(\beta_n \mid \alpha_n)$ diventa

$$\begin{aligned} H(Y_1, \dots, Y_n \mid X_1, \dots, X_n) &= -\sum_{(x,y)} p(x,y) \left(\sum_{i=1}^{n} \log p(\beta_i \mid \alpha_i) \right) \\ &= \sum_{i=1}^{n} H(Y_i \mid X_i). \end{aligned}$$

Abbiamo già visto che

$$H(Y_1, \dots, Y_n) \leq \sum_{i=1}^{n} H(Y_i)$$

e che vale l'uguaglianza se e solo se $Y_1, \dots, Y_n$ sono indipendenti, quindi il lemma è dimostrato. □

A questo punto, possiamo dimostrare l'inverso debole del teorema fondamentale.

Teorema 1.30 (Inverso debole del teorema fondamentale)**.** *La probabilità media di errore $\overline{p(e)}$ di un (s, n) codice deve soddisfare*

$$\log s \leq \frac{nC + \log 2}{1 - \overline{p(e)}}$$

dove C è la capacità del canale. Quindi se $s \geq 2^{n(C+\delta)}$, dove $\delta > 0$, allora

$$n(C + \delta) \leq \frac{nC + 1}{1 - \overline{p(e)}} \qquad \textit{oppure}$$

$$\overline{p(e)} \geq 1 - \frac{C + 1/n}{C + \delta} \longrightarrow 1 - \frac{C}{C + \delta} > 0.$$

Quindi, se $R < C$, nessuna successione di $(2^{nR}, n)$ codici può avere $\overline{p(e)} \to 0$ per $n \to \infty$, quindi non esiste nessuna sequenza di $(2^{nR}, n, \lambda_n)$ codici con $\lim_{n\to\infty} \lambda_n = 0$.

Dimostrazione. Siano $x^{(i)}$, $i = 1, \dots, s$ le codewords del codice (s, n) con $p(x^{(i)}) = 1/s$ per ogni i e scegliamo una codeword arbitraria X con output Y come nel Teorema 1.28. Allora $H(X) = \log s$ e

$$I(X \mid Y) = \log s - H(X \mid Y).$$

Per il Lemma 1.29,

$$I(X \mid Y) \leq \sum_{i=1}^{n} I(X_i \mid Y_i)$$

e, poiché $I(X_i \mid Y_i) \leq C$ per definizione di capacità,

$$\log s - H(X \mid Y) \leq nC. \tag{1.4}$$

Per il Teorema 1.28,

$$H(X \mid Y) \leq H(\overline{p(e)}, 1 - \overline{p(e)}) + \overline{p(e)} \log(s-1), \tag{1.5}$$

quindi

$$H(X \mid Y) \leq \log 2 + \overline{p(e)} \log s \tag{1.6}$$

e la dimostrazione segue da (1.4) e (1.6). □

1.7 Inverso forte del teorema fondamentale nel caso del canale simmetrico

Mostriamo, nel caso particolare del canale binario simmetrico, che se il tasso di trasmissione viene mantenuto al di sotto della capacità del canale, la probabilità di errore si avvicina a 1 con l'aumentare della lunghezza delle codewords.

Teorema 1.31. *Dato un canale binario simmetrico con capacità C, sia ϵ reale positivo e λ reale, $0 \leq \lambda < 1$, allora, per n sufficientemente grande, ogni (s, n, λ) codice deve soddisfare*

$$s < 2^{n(C+\epsilon)}.$$

In particolare, per ogni successione di $(2^{nR}, n, \lambda_n)$ codici con $R > C$,

$$\lambda_n \to 1 \quad \textit{per} \quad n \to \infty.$$

Dimostrazione. L'idea della dimostrazione è di stimare il numero di sequenze in ciascun insieme di decodifica e di provare che questo numero è abbastanza alto da rendere la probabilità di corretta trasmissione almeno $1 - \lambda$.
Supponiamo di avere un codice $(s, n\lambda)$ con $0 \leq \lambda < 1$ e sia r il più piccolo intero tale che

$$\sum_{j=0}^{r} \binom{n}{j} \beta^j (1-\beta)^{n-j} \geq 1 - \lambda. \tag{1.7}$$

Mostriamo che ogni insieme di decodifica ha almeno $\sum_{j=0}^{r-1} \binom{n}{j}$ sequenze. Sia B l'insieme di decodifica associato alla codeword w e supponiamo che B abbia $\sum_{j=0}^{r-1} \binom{n}{j}$ sequenze, allora $p(e \mid w)$ è minima se gli errori correggibili sono gli elementi di B che hanno fino ad $r-1$ errori.

In questo caso la probabilità di corretta trasmissione quando w è trasmessa è

$$p(e' \mid w) = \sum_{j=0}^{r-1} \binom{n}{j} \beta^j (1-\beta)^{n-j} < 1$$

e poiché il numero di sequenze di B è al più $\sum_{j=0}^{r-1} \binom{n}{j}$, si ha sempre $p(e' \mid w) < 1 - \lambda$, contraddicendo il fatto che abbiamo assunto che la massima probabilità d'errore sia λ. Dal momento che gli insiemi di decodifica sono s e il numero di sequenze totali è 2^n,

$$s \sum_{j=0}^{r-1} \binom{n}{j} \beta^j (1-\beta)^{n-j} < 2^n. \tag{1.8}$$

Se denotiamo con N il numero di errori nella trasmissione,

$$P\{N \leq r\} = \sum_{j=0}^{r} \binom{n}{j} \beta^j (1-\beta)^{n-j} \geq 1 - \lambda$$

per definizione di r. Poiché N/n converge in probabilità a β quando $n \to \infty$ per la legge debole dei grandi numeri, allora per ogni $\delta > 0$ fissato,

$$P\{N \leq n(\beta - \delta)\} \to 0 \quad \text{per } n \to \infty.$$

In particolare, per n abbastanza grande,

$$P\{N \leq n(\beta - \delta)\} < 1 - \lambda$$

e quindi, sempre per n abbastanza grande,

$$r \geq n(\beta - \delta). \tag{1.9}$$

Le disuguaglianze (1.8) e (1.9) implicano

$$s \sum_{j=0}^{n(\beta-\delta)-1} \binom{n}{j} < 2^n$$

e possiamo scrivere $n(\beta - \delta) - 1 = n(\beta - \delta')$ se $\delta' \to \delta$ per $n \to \infty$.

Introduciamo un risultato dimostrato in [8].

Lemma 1.32. *Sia $\Psi_p(n, \lambda)$ la coda di una distribuzione binomiale, ovvero*

$$\Psi_p(n, \lambda) = \sum_{k=\lambda n}^{n} \binom{n}{k} p^k q^{n-k}$$

dove $n\lambda$ è un intero e $0 < p < \lambda < 1$. Allora

$$(8n\lambda(1-\lambda))^{-1/2} \, 2^{-nB(\lambda,p)} \leq \Psi_p(n, \lambda) \leq 2^{-nB(\lambda,p)}$$

dove

$$\begin{aligned} B(\lambda, p) &= -H(\lambda, 1-\lambda) - \lambda \log p - (1-\lambda)\log q \\ &= \lambda \log \frac{\lambda}{p} + (1-\lambda)\log \frac{1-\lambda}{q}. \end{aligned}$$

Questo implica che

$$\lim_{n\to\infty} \left(-\frac{1}{n} \log \Psi_p(n, \lambda_n) \right) = B(\lambda, p)$$

per $n\lambda_n$ intero e $\lambda_n \to \lambda$.
In particolare se $p = q = 1/2$, otteniamo

$$\frac{2^{nH(\lambda,1-\lambda)}}{\sqrt{8n\lambda(1-\lambda)}} \leq \sum_{k=\lambda n}^{n} \binom{n}{k} \leq 2^{nH(\lambda,1-\lambda)} \quad \lambda > \frac{1}{2}$$

e quindi

$$\lim_{n\to\infty} \left(-\frac{1}{n} \log \left(\sum_{k=\lambda n}^{n} \binom{n}{k} \right) \right) = H(\lambda, 1-\lambda) \quad \textit{se } \lambda_n \to \lambda.$$

Per il Lemma 1.32,

$$s \frac{2^{nH(\beta-\delta', 1-(\beta-\delta'))}}{\left(8n(\beta-\delta')(1-(\beta-\delta'))\right)^{-1/2}} < 2^n$$

o, equivalentemente,

$$s < 2^{n\left(1-H(\beta-\delta', 1-(\beta-\delta'))+(1/2n)\log\left(8n(\beta-\delta')(1-(\beta-\delta'))\right)\right)}$$

e, poiché $C = 1 - H(\beta, 1-\beta)$ e δ' possono essere scelti arbitrariamente piccoli, abbiamo dimostrato il teorema. □

2 | Polarizzazione dei canali binari

In questo capitolo trattiamo il metodo di *polarizzazione dei canali* che parte da un arbitrario canale B-DMC e crea dei canali *polarizzati*, dove con questo termine si intende che asintoticamente tali canali si dividono tra canali con mutua informazione massima e canali con mutua informazione minima.

La polarizzazione si può applicare ad un arbitrario canale DMC $W : \mathcal{X} \to \mathcal{Y}$ con alfabeto di input $\mathcal{X} = \{0, 1\}$, alfabeto di output $\mathcal{Y}$. Denotiamo con

$$W(y \mid x) \quad x \in \mathcal{X}, y \in \mathcal{Y}$$

la *probabilità di trasmissione* di y, ovvero la probabilità che, inviato x, y sia ricevuto.
Denotiamo con W^N il canale generato da N copie indipendenti di W, ovvero $W^N : \mathcal{X}^N \to \mathcal{Y}^N$ con probabilità

$$W^N(y \mid x) = \prod_{i=1}^{N} W(y_i \mid x_i)$$

dove $y = (y_1, \ldots, y_N) \in \mathcal{Y}^N$ e $x = (x_1, \ldots, x_N) \in \mathcal{X}^N$.

Per un canale W B-DMC, introduciamo due parametri che saranno utili nella trattazione successiva. Il primo lo conosciamo già ed è

$$I(W) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \frac{1}{2} W(y \mid x) \log_2 \frac{W(y \mid x)}{\sum_{x' \in \mathcal{X}} \frac{1}{2} W(y \mid x')},$$

la mutua informazione tra input e output. Il secondo parametro, il parametro di Bhattacharya, è a sua volta un parametro a valori in $[0, 1]$, è definito da:

$$Z(W) = \sum_{y \in \mathcal{Y}} \sqrt{W(y \mid 0) W(y \mid 1)}$$

e prende il nome di *affidabilità* del canale.

La capacità di un canale DMC $W : \mathcal{X} \to \mathcal{Y}$ è data da $C(W) = \max_Q I(X; Y)$, dove $P_{X,Y}(x, y) =$

$Q(x)W(y|x)$ per $(x,y) \in \mathcal{X} \times \mathcal{Y}$ e Q è una probabilità su $\mathcal{X}$. La capacità simmetrica è $I(W) = I(X;Y)$, con Q probabilità uniforme su $\mathcal{X}$.

Ricordiamo che un canale B-DMC $W : \mathcal{X} \to \mathcal{Y}$ è un canale BEC se, comunque scelto un output $y \in \mathcal{Y}$, una tra le seguenti è verificata:

- $W(y|0)\,W(y|1) = 0$;
- $W(y|0) = W(y|1)$.

Nel secondo caso y è il simbolo di erasure e $W(y|0) = W(y|1)$ la probabilità di erasure.

Mostriamo adesso due risultati che saranno utili in seguito.

Proposizione 2.1. *Sia W un canale B-DMC, allora valgono le seguenti disuguaglianze:*

$$I(W) \geq \log \frac{2}{1+Z(X)}, \tag{2.1}$$

$$I(W) \leq \sqrt{1-Z(X)^2}. \tag{2.2}$$

Dimostrazione. La quantità $\log \frac{2}{1+Z(X)}$ equivale al parametro di canale $E_0(1,Q)$ che prende il nome di *tasso di cutoff simmetrico* come definito da Gallager ([13], Sezione 5.6), dove Q è la distribuzione uniforme. Sempre in [13] è dimostrato che

$$I(W) \geq E_0(1,Q)$$

e quindi abbiamo provato (2.1).

Per provare (2.2), definiamo

$$d(W) := \frac{1}{2}\sum_{y\in\mathcal{Y}} |W(y \mid 0) - W(y \mid 1)|$$

e dimostriamo due risultati che rendono immediata la dimostrazione di (2.2).

Lemma 2.2. *Sia W un canale B-DMC, allora $I(W) \leq d(W)$.*

Dimostrazione. Sia W un arbitrario canale B-DMC con alfabeto di output $\mathcal{Y} = \{1,\dots,n\}$ e siano $P_i = W(i \mid 0)$, $Q_i = W(i \mid 1)$, $i = 1,\dots,n$. Per definizione

$$I(W) = \sum_{i=1}^{n} \frac{1}{2}\left(P_i \log \frac{P_i}{\frac{1}{2}P_i + \frac{1}{2}Q_i} + Q_i \log \frac{Q_i}{\frac{1}{2}P_i + \frac{1}{2}Q_i}\right)$$

e l'i-simo termine è

$$f(x) := x \log \frac{x}{x+\delta} + (x+2\delta)\log \frac{x+2\delta}{x+\delta}$$

dove $x = \min\{P_i, Q_i\}$ e $\delta = \frac{1}{2}|P_i - Q_i|$.
Il massimo di $f(x)$ per $0 \leq x \leq 1 - 2\delta$ è in $x = 0$, quindi $f(x) \leq 2\delta$.
Se usiamo questo risultato nell'espressione per $I(W)$, otteniamo $I(W) \leq d(W)$. □

Lemma 2.3. *Sia W un canale B-DMC, allora $d(W) \leq \sqrt{1 - Z(W)^2}$.*

Dimostrazione. Sia W un arbitrario canale B-DMC con alfabeto di output $\mathcal{Y} = \{1, \ldots, n\}$ e siano $P_i = W(i \mid 0)$, $Q_i = W(i \mid 1)$, $i = 1, \ldots, n$.
Definiamo:

- $\delta_i := \frac{1}{2}|P_i - Q_i|$,
- $\delta := d(W)$,
- $R_i := \frac{P_i + Q_i}{2}$.

Con questa notazione, $Z(W) = \sum_{i=1}^{n} \sqrt{(R_i - \delta_i)(R_i + \delta_i)} = \sum_{i=1}^{n} \sqrt{R_i^2 - \delta_i^2}$.
Il massimo di $\sum_{i=1}^{n} \sqrt{R_i^2 - \delta_i^2}$ per $0 \leq \delta_i \leq R_i$ e $\delta = \sum_{i=1}^{n} \delta_i$ si trova in $\delta_i = \delta R_i$ e per questo valore $Z(W)$ vale $\sqrt{1 - \delta_i}$. Quindi $Z(W) \leq \sqrt{1 - d(W)^2}$, che è equivalente a $d(W) \leq \sqrt{1 - Z(W)^2}$.

□

E questo completa la dimostrazione della Proposizione 2.1. □

Il secondo risultato utile è la seguente proposizione.

Proposizione 2.4. *Siano $W_j : \mathcal{X} \to \mathcal{Y}$, $j \in \mathcal{J}$, canali B-DMC e sia Q una distribuzione di probabilità su $\mathcal{J}$; definiamo $W : \mathcal{X} \to \mathcal{Y}$ come il canale con probabilità $W(y|x) = \sum_{j \in \mathcal{J}} Q(j) W_j(y|x)$. Allora*

$$\sum_{j \in \mathcal{J}} Q(j) Z(W_j) \leq Z(W).$$

Dimostrazione. Possiamo riscrivere $Z(W)$ come segue

$$Z(W) = \sum_{y} \sqrt{W(y \mid 0) W(y \mid 1)} = -1 + \frac{1}{2} \sum_{y} \left(\sum_{x} \sqrt{W(y \mid x)} \right)^2$$

e, per la disuguaglianza di Minkowsky,

$$\begin{aligned} Z(W) &= -1 + \frac{1}{2}\sum_{y}\left(\sum_{x}\sqrt{W(y \mid x)}\right)^2 \\ &\geq -1 + \frac{1}{2}\sum_{y}\sum_{j\in\mathcal{J}} Q(j)\left(\sum_{x}\sqrt{W_j(y \mid x)}\right)^2 \\ &= \sum_{j\in\mathcal{J}} Q(j) Z(W_j). \end{aligned}$$

□

2.1 Polarizzazione

La polarizzazione di un canale è un metodo che passa da due fasi, combinazione e separazione. Prima di illustrare queste due fasi, denotiamo con:

- a_1^N il vettore riga $(a_1, \ldots, a_N)$
- a_1^i il sottovettore $(a_1, \ldots a_i)$, $1 \leq i \leq N$;
- $a_{1,o}^j$ il sottovettore $(a_k \;\; 1 \leq k \leq j$ e k dispari) (la lettera "o" viene dall'inglese *odd*);
- $a_{1,e}^j$ il sottovettore $(a_k \;\; 1 \leq k \leq j$ e k pari) (la lettera "e" viene dall'inglese *even*);
- $a_{\mathcal{A}}$ il sottovettore $(a_i |\; i \in \mathcal{A})$, dove $\mathcal{A} \subset \{1, \ldots, N\}$.

Combinazione

La prima fase della combinazione si basa sulla definizione di una mappa $F : \mathcal{X}^2 \to \mathcal{X}^2$ chiamata *kernel* tale che $F : (u_1, u_2) \mapsto (u_1 \oplus u_2, u_2)$, dove con il simbolo $\oplus$ indichiamo la somma modulo 2. Usiamo F per combinare due copie indipendenti di W e costruire il canale $W_2 : \mathcal{X}^2 \to \mathcal{Y}^2$, mostrato in Figura 2.1, la cui probabilità è

$$W_2\left(y_1 y_2 \mid u_1 u_2\right) = W\left(y_1 \mid u_1 \oplus u_2\right) W\left(y_2 \mid u_2\right).$$

Il processo di combinazione dei canali è un processo ricorsivo, il cui passo successivo è mostrato in Figura 2.2, dove due copie indipendenti di W_2 sono combinate tra loro tramite il kernel F e la permutazione R_4 che manda (s_1, s_2, s_3, s_4) in $v_1^4 := (s_1, s_3, s_2, s_4)$. Il canale risultante è il canale $W_4 : \mathcal{X}^4 \to \mathcal{Y}^4$ la cui probabilità è

$$W_4\left(y_1^4 \mid u_1^4\right) = W_2\left(y_1^2 \mid u_1 \oplus u_2, u_3 \oplus u_4\right) W_2\left(y_3^4 \mid u_2, u_4\right).$$

Il caso generale della ricorsione è mostrato in Figura 2.3, dove due copie indipendenti di $W_{N/2}$ sono combinate tra loro per generare il canale $W_N : \mathcal{X}^N \to \mathcal{Y}^N$:

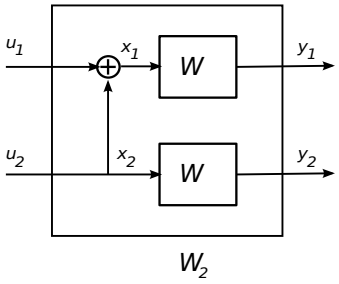

Figura 2.1: Il canale W_2.

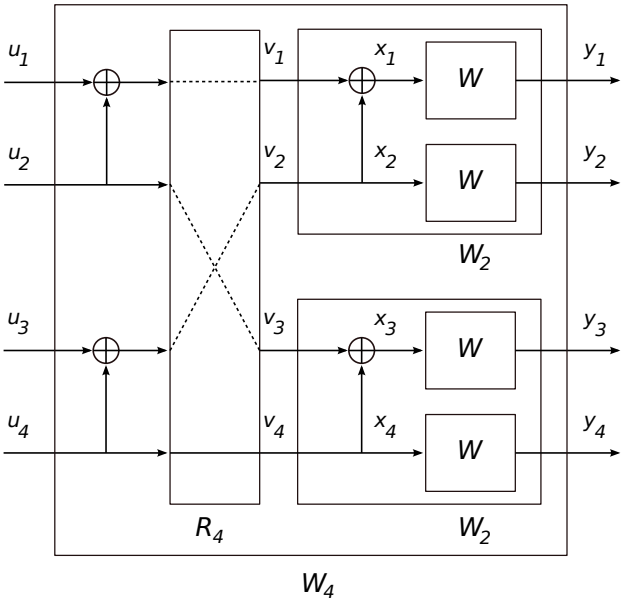

Figura 2.2: Il canale W_4.

- il vettore di input u_1^N è trasformato in $s_1^N = \begin{cases} s_{2i-1} = u_{2i-1} \oplus u_{2i} \\ s_{2i} = u_{2i} \end{cases} \qquad 1 \leq i \leq N/2;$

- l'operatore R_N è la permutazione, chiamata *reverse shuffle*, che manda s_1^N nel vettore

$$v_1^N := (s_1, s_3, \ldots, s_{N-1}, s_2, s_4, \ldots, s_N)\,;$$

- la sequenza v_1^N diventa l'input delle due copie di $W_{N/2}$ come mostrato in figura.

Relazione con W^N

Se guardiamo la Figura 2.2, possiamo osservare che la trasformazione degli input u_1^4 del canale W_4 negli input x_1^4 del canale W^4 può essere pensata come $x_1^4 = u_1^4 G_4$, dove G_4 prende il nome

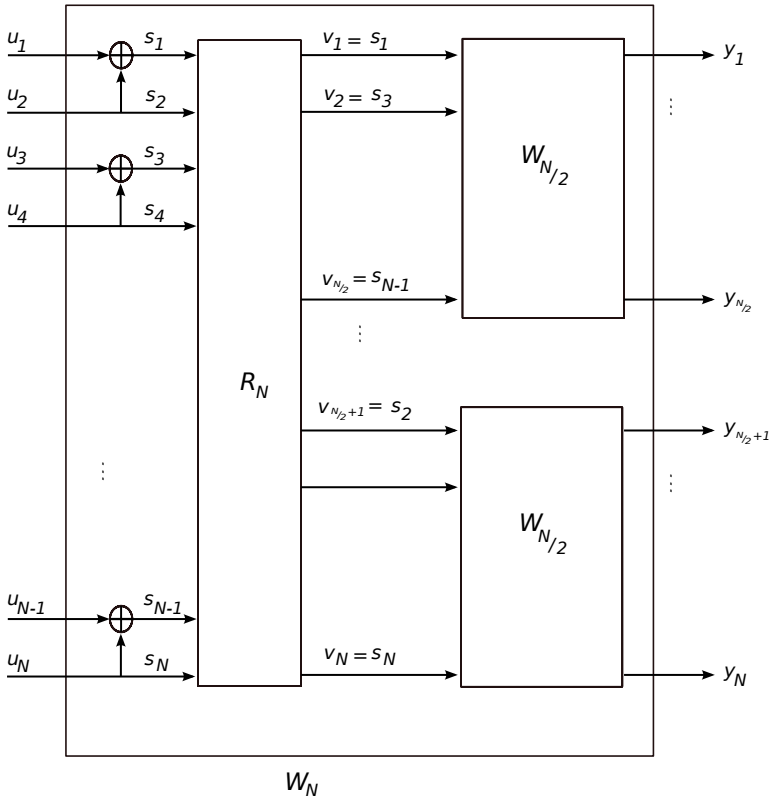

Figura 2.3: Il canale W_N.

di *matrice generatrice* di dimensione 4 ed è la matrice

$$G_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Detto questo, possiamo esprimere una relazione tra le probabilità del canale W_4 e quelle di W^4:

$$W_4\left(y_1^4 \mid x_1^4\right) = W^4\left(y_1^4 \mid u_1^4 G_4\right).$$

Analogamente, nel caso generale possiamo definire una matrice G_N, chiamata *matrice generatrice* di dimensione N, che descrive la trasformazione dell'input u_1^N del canale W_N nell'input x_1^N del canale W^N e le probabilità sono relazionate da

$$W_N\left(y_1^N \mid u_1^N\right) = W^N\left(y_1^N \mid u_1^N G_N\right).$$

Un descrizione più esplicita di G_N verrà data nel prossimo capitolo quando parleremo di codifica.

Spezzamento

Il passo successivo consiste nello spezzare W_N in un insieme di N canali binari:

$$\begin{aligned} W_N^{(i)} : \mathcal{X} &\to \mathcal{Y}^N \times \mathcal{X}^{i-1} \\ u_i &\mapsto \left(y_1^N, u_1^{i-1}\right) \end{aligned}$$

per ogni i, $1 \leq i \leq N$, definiti dalle probabilità di transizione

$$W_N^{(i)}\left(y_1^N, u_1^{i-1} \mid u_i\right) := \sum_{u_{i+1}^N \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N\left(y_1^N \mid u_1^N\right). \tag{2.3}$$

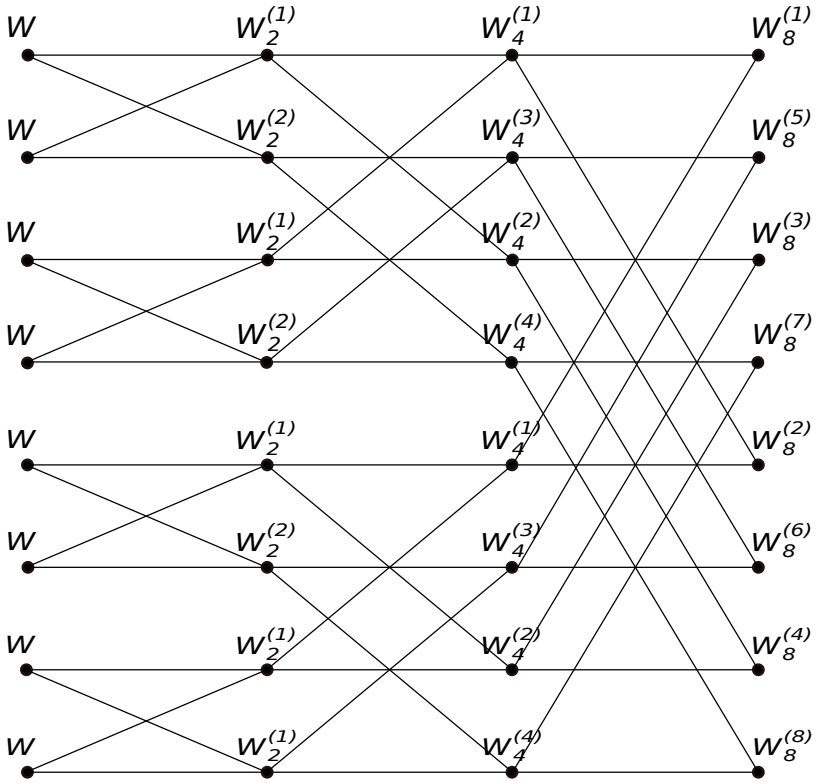

Figura 2.4: Il processo di trasformazione con $N = 8$ canali.

I canali $W_N^{(i)}$ mostrano un effetto di *polarizzazione* nel senso che, per ogni $\delta \in (0, 1)$, al crescere di N:

- $I\left(W_N^{(i)}\right) \to I(W)$ per ogni i tale che $I\left(W_N^{(i)}\right) \in (1-\delta, \delta]$;
- $I\left(W_N^{(i)}\right) \to 1 - I(W)$ per ogni i tale che $I\left(W_N^{(i)}\right) \in [0, \delta)$.

Consideriamo il parametro Z in questo caso,

$$Z\left(W_N^{(i)}\right) = \sum_{u_1^{i-1} \in \mathcal{X}^{i-1}} \sum_{y_1^N \in \mathcal{Y}^N} \sqrt{W_N^{(i)}\left(y_1^N, u_1^{i-1}|0\right) W_N^{(i)}\left(y_1^N, u_1^{i-1}|1\right)}.$$

Alla fine del capitolo dimostreremo il seguente risultato su $Z\left(W_N^{(i)}\right)$.

Teorema 2.5. *Per ogni B-DMC W con $I(W) > 0$ e ogni R fissato, $R < I(W)$, esiste una sequenza di insiemi $\mathcal{A}_N \subset \{1, \ldots, N\}$, con $N = 2^n$, per un certo $n \in \mathbb{N}$ tale che*

$$|\mathcal{A}_N| \geq NR \quad e \quad Z\left(W_N^{(i)}\right) \leq O\left(N^{-5/4}\right) \quad \forall i \in \mathcal{A}_N\,.$$

2.2 Struttura ricorsiva di $W_N^{(i)}$

Le operazioni di combinazione e spezzamento possono essere riassunte dalla notazione:

$$W^N \mapsto \left(W_N^{(1)}, \ldots, W_N^{(N)}\right).$$

In questa sezione analizziamo la struttura ricorsiva di $W_N^{(i)}$.

Proposizione 2.6. *Per ogni $n \geq 1$, $N = 2^n$, $1 \leq i \leq N$,*

$$W_N^{(i-1)}\left(y_1^N, u_1^{i-2} \mid u_{i-1}\right) = \sum_{u_i \in \mathcal{X}} W_N^{(i)}\left(y_1^n, u_1^{i-1} \mid u_i\right).$$

Dimostrazione. Segue direttamente dalla definizione 2.3. □

Prima di arrivare alla definizione ricorsiva più significativa, notiamo che:

$$W_2^{(1)}\left(y_1^2 \mid u_1\right) = \sum_{u_2 \in \mathcal{X}} \frac{1}{2} W_2\left(y_1^2 \mid u_1^2\right) = \sum_{u_2 \in \mathcal{X}} \frac{1}{2} W\left(y_1 \mid u_1 \oplus u_2\right) W\left(y_2 \mid u_2\right) \tag{2.4}$$

$$W_2^{(2)}\left(y_1^2, u_1 \mid u_2\right) = \frac{1}{2} W_2\left(y_1^2 \mid u_1^2\right) = \frac{1}{2} W\left(y_1 \mid u_1 \oplus u_2\right) W\left(y_2 \mid u_2\right). \tag{2.5}$$

Queste formule si generalizzano come segue.

Proposizione 2.7. *Per ogni $n \geq 0$, $N = 2^n$, $1 \leq i \leq N$,*

$$W_{2N}^{(2i-1)}\left(y_1^{2N}, u_1^{2i-2} | u_{2i-1}\right) = \sum_{u_{2i} \in \mathcal{X}} \frac{1}{2} W_N^{(i)}\left(y_1^N, u_{1,e}^{2i-2} \oplus u_{1,o}^{2i-2} | u_{2i-1} \oplus u_{2i}\right) W_N^{(i)}\left(y_{N+1}^{2N}, u_{1,e}^{2i-2} | u_{2i}\right) \tag{2.6}$$

$$W_{2N}^{(2i)}\left(y_1^{2N}, u_1^{2i-1} \mid u_{2i}\right) = \frac{1}{2} W_N^{(i)}\left(y_1^N, u_{1,e}^{2i-2} \oplus u_{1,o}^{2i-2} \mid u_{2i-1} \oplus u_{2i}\right) W_N^{(i)}\left(y_{N+1}^{2N}, u_{1,e}^{2i-2} \mid u_{2i}\right) \tag{2.7}$$

Dimostrazione. Per dimostrare (2.6), scriviamo:

$$\begin{aligned} W_{2N}^{(2i-1)}\left(y_1^{2N}, u_1^{2i-1} \mid u_{2i-1}\right) &= \sum_{u_{2i}^{2N} \in \mathcal{X}^{2N-2i+1}} \frac{1}{2^{2N-1}} W_{2N}\left(y_1^{2N} \mid u_1^{2N}\right) \\ &= \sum_{u_{2i,e}^{2N}, u_{2i,o}^{2N} \in \mathcal{X}^{N-i+1}} \frac{1}{2^{2N-1}} W_N\left(y_1^N \mid u_{1,o}^{2N} \oplus u_{1,e}^{2N}\right) W_N\left(y_{N+1}^{2N} \mid u_{1,e}^{2N}\right) \\ &= \sum_{u_{2i} \in \mathcal{X}} \frac{1}{2} \sum_{u_{2i+1,e}^{2N} \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N\left(y_{N+1}^{2N} | u_{1,e}^{2N}\right) \sum_{u_{2i+1,o}^{2N} \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N\left(y_1^N | u_{1,o}^{2N} \oplus u_{1,e}^{2N}\right). \end{aligned}$$

E, per la definizione (2.3),

$$\sum_{u_{2i+1,o}^{2N} \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N\left(y_1^N | u_{1,o}^{2N} \oplus u_{1,e}^{2N}\right) = W_N^{(i)}\left(y_1^N, u_{1,e}^{2i-2} \oplus u_{1,o}^{2i-2} \mid u_{2i-1} \oplus u_{2i}\right)$$

dal momento che, per ogni $u_{1,e}^{2N}$ fissato, se $u_{2i+1,o}^{2N}$ varia in $\mathcal{X}^{N-i}$, $u_{2i+1,o}^{2N} \oplus u_{2i+1,e}^{2N}$ varia nello stesso insieme. Per quanto riguarda l'altro termine, possiamo scrivere

$$\sum_{u_{2i+1,e}^{2N} \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N\left(y_{N+1}^{2N} | u_{1,e}^{2N}\right) = W_N^{(i)}\left(y_{N+1}^{2N}, u_{1,e}^{2i-2} \mid u_{2i}\right)$$

e questo prova (2.6).
La dimostrazione di (2.7) è analoga. Innanzitutto scriviamo

$$\begin{aligned} W_{2N}^{(2i)}\left(y_1^{2N}, u_1^{2i-1} \mid u_{2i}\right) &= \sum_{u_{2i+1}^{2N} \in \mathcal{X}^{2N-2i}} \frac{1}{2^{2N-1}} W_{2N}\left(y_1^{2N} \mid u_1^{2N}\right) \\ = \frac{1}{2} \sum_{u_{2i+1,e}^{2N} \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N\left(y_{N+1}^{2N} \mid u_{1,e}^{2N}\right) &\sum_{u_{2i+1,o}^{2N} \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N\left(y_1^N \mid u_{1,o}^{2N} \oplus u_{1,e}^{2N}\right) \end{aligned}$$

e i termini di questa somma possono essere calcolati analogamente a sopra per ottenere 2.7, come voluto.

□

Osservazione 2.8. La struttura ricorsiva ci permette di intrudurre un'ulteriore notazione. Sia W il canale B-DMC, chiamiamo:

$$W^-(y_1, y_2 \mid u_1) := W_2^{(1)}(y_1, y_2 \mid u_1), \tag{2.8}$$

$$W^+(y_1, y_2, u_1 \mid u_2) := W_2^{(2)}(y_1, y_2, u_1 \mid u_2). \tag{2.9}$$

Al passo successivo otteniamo i quattro canali:

$$W^{--} := (W^-)^- \quad W^{-+} := (W^-)^+ \quad W^{++} := (W^+)^+ \quad W^{+-} := (W^+)^-$$

e all'n-simo passo otteniamo 2^n canali $W^{-\cdots-}, \ldots, W^{+\cdots+}$.

Possiamo generalizzare la combinazione e lo spezzamento di canali come segue.

Combinazione

Supponiamo di avere due copie indipendenti di un arbitrario canale B-DMC $W : \mathcal{X} \to \mathcal{Y}$ e di combinarle per ottenere una canale $W_2 : \mathcal{X}^2 \to \widetilde{\mathcal{Y}}$, dove la differenza rispetto al canale mostrato nella Figura 2.1 consiste nell'aver aggiunto una funzione invertibile $f : \mathcal{Y}^2 \to \widetilde{\mathcal{Y}}$ che chiamiamo *blocco di post-processore*.

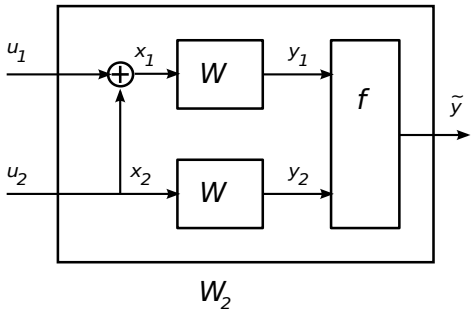

Figura 2.5: Forma generale di combinazione dei canali

Osservazione 2.9. L'invertibilità di f implica che $\widetilde{\mathcal{Y}}$ deve avere lo stesso numero di elementi di $\mathcal{Y}^2$ ma, al di là di questa limitazione, l'alfabeto di $\widetilde{\mathcal{Y}}$ può essere scelto a piacere.

Spezzamento

Possiamo adesso spezzare il canale W_2 in due canali $W_2^{(1)}$ e $W_2^{(2)}$,

$$W_2^{(1)} : \mathcal{X} \to \widetilde{\mathcal{Y}},$$

$$W_2^{(2)} : \mathcal{X} \to \widetilde{\mathcal{Y}} \times \mathcal{X}$$

in modo analogo a prima, sarebbe a dire

$$W_2^{(1)}\left(\tilde{y} \mid u_1\right) = \sum_{u_2} \frac{1}{2} W_2\left(f^{-1}\left(\tilde{y}\right) \mid u_1, u_2\right)$$

$$W_2^{(2)}\left(\tilde{y}, u_1 \mid u_2\right) = \frac{1}{2} W_2\left(f^{-1}\left(\tilde{y}\right) \mid u_1, u_2\right);$$

scriviamo $(W, W) \mapsto \left(W_2^{(1)}, W_2^{(2)}\right)$ per indicare che la coppia di canali $\left(W_2^{(1)}, W_2^{(2)}\right)$ è ottenuta da due copie indipendenti di W attraverso l'operazione descritta sopra, avendo fissato la scelta di una funzione f.

Proposizione 2.10. *Sia $W_N^{(i)}$ un canale definito ricorsivamente, possiamo ottenere i canali $W_{2N}^{(2i-1)}$ e $W_{2N}^{(2i)}$ dal canale $W_N^{(i)}$ come definito sopra:*

$$\left(W_N^{(i)}, W_N^{(i)}\right) \mapsto \left(W_{2N}^{(2i-1)}, W_{2N}^{(2i)}\right) \tag{2.10}$$

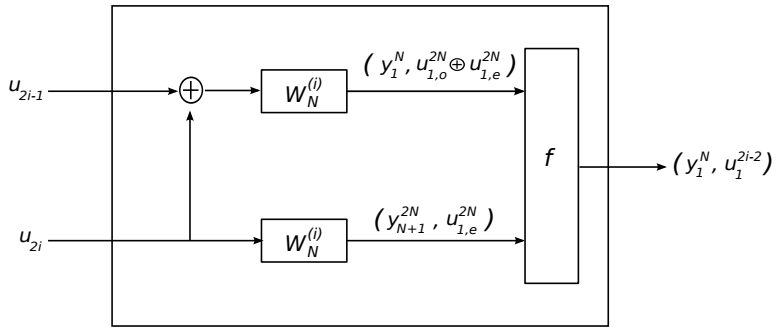

Figura 2.6: Relazione tra $W_N^{(i)}$ e $\left(W_{2N}^{(2i-2)}, W_{2N}^{(2i)}\right)$.

Dimostrazione. Usiamo le formule ricorsive (2.6) e (2.7) con la scelta della funzione f

$$f\left(\left(y_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2}\right), \left(y_{N+1}^{2N}, u_{1,e}^{2i-2}\right)\right) = \left(y_1^{2N}, u_1^{2i-2}\right)$$

dove $\widetilde{\mathcal{Y}} = \mathcal{Y}^{2N} \times \mathcal{X}^{2i-2}$. □

2.3 Trasformazione di $I\left(W_N^{(i)}\right)$ e $Z\left(W_N^{(i)}\right)$

Vogliamo studiare come cambiano i parametri $I\left(W_N^{(i)}\right)$ e $Z\left(W_N^{(i)}\right)$ tramite la trasformazione descritta da (2.10). Per la struttura ricorsiva del canale, ci basta studiare il caso $(W, W) \mapsto \left(W_2^{(1)}, W_2^{(2)}\right)$ del quale (2.10) è un caso particolare.

Proposizione 2.11. *Sia $W : \mathcal{X} \to \mathcal{Y}$ un arbitrario canale B-DMC, siano $W_2^{(1)}$ e $W_2^{(2)}$ ottenuti tramite la trasformazione $(W, W) \mapsto \left(W_2^{(1)}, W_2^{(2)}\right)$ con una funzione arbitraria $f : \mathcal{Y}^2 \to \widetilde{\mathcal{Y}}$, allora*

$$I\left(W_2^{(1)}\right) + I\left(W_2^{(2)}\right) = 2I\left(W\right) \tag{2.11}$$

$$I\left(W_2^{(1)}\right) \leq I\left(W_2^{(2)}\right) \tag{2.12}$$

e si ha l'uguaglianza se e solo se $I\left(W\right)$ vale 0 o 1.

Dimostrazione. Iniziamo la dimostrazione col definire alcune variabili aleatorie:

- U_1, U_2 tali che la coppia (U_1, U_2) sia distribuita uniformemente su $\mathcal{X}^2$;
- X_1, X_2 tali che $(X_1, X_2) = (U_1 \oplus U_2, U_2)$;

- Y_1, Y_2 con probabilità $P_{Y_1,Y_2|X_1,X_2}(y_1,y_2 \mid x_1,x_2) = W(y_1 \mid x_1)\,W(y_2 \mid x_2)$;

- $\widetilde{Y} = f(Y_1,Y_2)$.

Queste variabili aleatorie possono essere interpretate come input e output del canale mostrato nella Figura 2.5.
Per questo spazio di probabilità, la probabilità $W_2^{(1)}(\tilde{y} \mid u_1)$ può essere vista come la probabilità $P_{\widetilde{Y}|U_1}(\tilde{y} \mid u_1)$ e $W_2^{(2)}(\tilde{y},u_1 \mid u_2)$ come $P_{\widetilde{Y},U_1|U_2}(\tilde{y},u_1 \mid u_2)$.
Poichè la funzione $f : (Y_1,Y_2) \mapsto \widetilde{Y}$ è invertibile, abbiamo $I\left(W_2^{(1)}\right) = I(U_1;Y_1,Y_2)$ e $I\left(W_2^{(2)}\right) = I(U_2;Y_1,Y_2,U_1)$.
La dimostrazione di (2.11) segue da:

$$\begin{aligned} I\left(W_2^{(1)}\right) + I\left(W_2^{(2)}\right) &= I(U_1;Y_1,Y_2) + I(U_2;Y_1,Y_2 \mid U_1) && U_1,U_2 \text{ indipendenti} \\ &= I(U_1,U_2;Y_1,Y_2) && \text{per le proprietà di } I \\ &= I(X_1,X_2;Y_1,Y_2) && (X_1,X_2) \leftrightarrow (U_1,U_2) \\ &= 2I(W) \end{aligned}$$

Per dimostrare (2.12), proviamo le due disuguaglianze $I\left(W_2^{(2)}\right) \geq I(W)$ e $I(W) \geq I\left(W_2^{(1)}\right)$.
Per dimostrare la prima disuguaglianza, consideriamo $I\left(W_2^{(2)}\right)$:

$$\begin{aligned} I\left(W_2^{(2)}\right) &= I(U_2;Y_1,Y_2,U_1) \\ &= I(U_2;Y_2) + I(U_2;Y_1,U_1 \mid Y_2) \\ &= I(W) + I(U_2;Y_1,U_1 \mid Y_2). \end{aligned}$$

E questo mostra che $I\left(W_2^{(2)}\right) \geq I(W)$.

Poichè $I\left(W_2^{(2)}\right) \geq I(W)$,

$$I\left(W_2^{(1)}\right) + I\left(W_2^{(2)}\right) = 2I(W) \leq I(W) + I\left(W_2^{(2)}\right) \text{ e quindi } I\left(W_2^{(1)}\right) \leq I(W).$$

Resta da dimostrare che la disuguaglianza (2.12) è un'uguaglianza se e solo se $I(W)$ vale 0 o 1. La dimostrazione che abbiamo dato per (2.12) mostra come la disuguaglianza diventa un'uguaglianza se e solo se $I(U_2;Y_1,U_1 \mid Y_2)$ è nullo, o equivalentemente

$$P(u_1,u_2,y_1|y_2) = P(u_1,y_1|y_2)\,P(u_2|y_2)$$

per tutte le quaterne (u_1,u_2,y_1,y_2) tali che $P(y_2) > 0$ o, ancora equivalentemente,

$$P(y_1,y_2|u_1,u_2)\,P(y_2) = P(y_1,y_2|u_1)\,P(y_2|u_2)$$

per tutte le quaterne (u_1,u_2,y_1,y_2). Poichè $P(y_1,y_2|u_1,u_2) = W(y_1|u_1 \oplus u_2)\,W(y_2|u_2)$, pos-

siamo riscrivere la formula sopra

$$W\left(y_2|u_2\right)\left(W\left(y_1|u_1\oplus u_2\right)P\left(y_2\right)-P\left(y_1,y_2|u_1\right)\right)=0.$$

Sostituiamo $P\left(y_2\right)=\frac{1}{2}W\left(y_2|u_2\right)+\frac{1}{2}W\left(y_2|u_2\oplus 1\right)$ e

$$P\left(y_1,y_2|u_1\right)=\frac{1}{2}W\left(y_1|u_1\oplus u_2\right)W\left(y_2|u_2\right)+\frac{1}{2}W\left(y_1|u_1\oplus u_2\oplus 1\right)W\left(y_2|u_2\oplus 1\right)$$

e otteniamo

$$W\left(y_2|u_2\right)W\left(y_2|u_2\oplus 1\right)\left(W\left(y_1|u_1\oplus u_2\right)-W\left(y_1|u_1\oplus u_2\oplus 1\right)\right)=0$$

che, per tutte e quattro le possibili scelte di (u_1,u_2) è equivalente a

$$W\left(y_2|0\right)W\left(y_2|1\right)\left(W\left(y_1|0\right)-W\left(y_1|1\right)\right)=0.$$

Quindi, o non esiste alcun y_2 tale che $W\left(y_2|0\right)W\left(y_2|1\right)>0$, e in tal caso $I\left(W\right)$ è uguale a 1, oppure $W\left(y_1|0\right)=W\left(y_1|1\right)$ per ogni scelta di y_1 e $I\left(W\right)$ è uguale a 0. □

Proposizione 2.12. *Sia $W:\mathcal{X}\to\mathcal{Y}$ un arbitrario canale B-DMC. Siano $W_2^{(1)}$ e $W_2^{(2)}$ due canali ottenuti dalla trasformazione $(W,W)\mapsto\left(W_2^{(1)},W_2^{(2)}\right)$ con $f:\mathcal{Y}^2\to\widetilde{\mathcal{Y}}$, allora*

$$Z\left(W_2^{(2)}\right)=Z\left(W\right)^2 \tag{2.13}$$

$$Z\left(W_2^{(1)}\right)\leq 2Z\left(W\right)-Z\left(W\right)^2 \tag{2.14}$$

$$Z\left(W_2^{(2)}\right)\leq Z\left(W\right)\leq Z\left(W_2^{(1)}\right). \tag{2.15}$$

La disuguaglianza (2.14) *è un'uguaglianza se e solo se W è un canale BEC.*
Per quanto riguarda (2.15), *$Z\left(W_2^{(1)}\right)=Z\left(W_2^{(2)}\right)$ se e solo se $Z\left(W\right)$ vale 0 o 1 o, equivalentemente, se $I\left(W\right)$ vale 0 o 1.*

Dimostrazione. Incominciamo col dimostrare (2.13). Si ha

$$\begin{aligned}Z\left(W_2^{(2)}\right)&=\sum_{y_1^2,u_1}\sqrt{W_2^{(2)}\left(f\left(y_1,y_2\right),u_1|0\right)W_2^{(2)}\left(f\left(y_1,y_2\right),u_1|1\right)}\\&=\sum_{y_1^2,u_1}\frac{1}{2}\sqrt{W\left(y_1|u_1\right)W\left(y_2|0\right)W\left(y_1|u_1\oplus 1\right)W\left(y_2|1\right)}\\&=\sum_{y_2}\sqrt{W\left(y_2|0\right)W\left(y_2|1\right)}\sum_{u_1}\frac{1}{2}\sum_{y_1}\sqrt{W\left(y_1|u_1\right)W\left(y_1|u_1\oplus 1\right)}\end{aligned}$$

e vediamo che quest'ultimo termine altro non è che $Z\left(W\right)^2$.
Infatti, sia $\mathcal{Y}$ alfabeto di output, $\mathcal{Y}=\{s,t\}$:

- $\sum_{y_1}\sqrt{W\left(y_1|u_1\right)W\left(y_1|u_1\oplus 1\right)}=\sqrt{W\left(s|u_1\right)W\left(s|u_1\oplus 1\right)}+\sqrt{W\left(t|u_1\right)W\left(t|u_1\oplus 1\right)}$;
- questo termine sommato su u_1 vale $2\left(\sqrt{W\left(s|0\right)W\left(s|1\right)}+\sqrt{W\left(t|0\right)W\left(t|1\right)}\right)$;

- la somma su y_2 ha come risultato

$$W(s|0)\,W(s|1) + W(t|0)\,W(t|1) + 2\sqrt{W(s|0)\,W(s|1)\,W(t|0)\,W(t|1)} = Z(W)^2.$$

Dimostriamo ora (2.14):

$$\begin{aligned}
&Z\left(W_2^{(1)}\right) = \sum_{y_1^2} \sqrt{W_2^{(1)}(f(y_1,y_2)|0)\,W_2^{(1)}(f(y_1,y_2)|1)} \\
&= \sum_{y_1^2} \frac{1}{2}\sqrt{(W(y_1|0)\,W(y_2|0) + W(y_2|1)\,W(y_1|1))\,(W(y_1|0)\,W(y_2|1) + W(y_2|0)\,W(y_1|1))} \\
&\leq \sum_{y_1^2} \frac{1}{2}\left(\sqrt{W(y_1|0)\,W(y_2|0)} + \sqrt{W(y_2|1)\,W(y_1|1)}\right)\left(\sqrt{W(y_1|0)\,W(y_2|1)} + \sqrt{W(y_2|0)\,W(y_1|1)}\right) \\
&- \sum_{y_1^2} \sqrt{W(y_1|0)\,W(y_2|0)\,W(y_2|1)\,W(y_1|1)},
\end{aligned}$$

dove la disuguaglianza segue dal fatto che, se consideriamo l'identità

$$(ab+cd)(ac+bd) + 2\sqrt{abcd}\left(\sqrt{a}-\sqrt{d}\right)^2\left(\sqrt{b}-\sqrt{c}\right)^2 = \left(\left(\sqrt{ab}+\sqrt{cd}\right)\left(\sqrt{ac}+\sqrt{bd}\right) - 2\sqrt{abcd}\right)^2$$

possiamo ricavarne la disuguaglianza

$$\left(\sqrt{(ab+cd)(ac+bd)}\right)^2 = (ab+cd)(ac+bd) \leq \left(\left(\sqrt{ab}+\sqrt{cd}\right)\left(\sqrt{ac}+\sqrt{bd}\right) - 2\sqrt{abcd}\right)^2.$$

Concludiamo la dimostrazione di (2.14) osservando che:

- $$\begin{aligned}
\sum_{y_1^2} &W(y_1 \mid 0)\sqrt{W(y_2 \mid 0)\,W(y_2 \mid 1)} = \\
&= W(s \mid 0)\sqrt{W(s \mid 0)\,W(s \mid 1)} + W(t \mid 0)\sqrt{W(s \mid 0)\,W(s \mid 1)} + \\
&\quad W(s \mid 0)\sqrt{W(t \mid 0)\,W(t \mid 1)} + W(t \mid 0)\sqrt{W(t \mid 0)\,W(t \mid 1)}
\end{aligned}$$

  Ora, poiché se $W(s \mid 0) = p$, allora $W(t \mid 0) = 1-p$, la somma sopra diventa $\sqrt{W(t \mid 0)\,W(t \mid 1)} + \sqrt{W(s \mid 0)\,W(s \mid 1)} = Z(W)$.

- ciascun termine di $\left(\sqrt{ab}+\sqrt{cd}\right)\left(\sqrt{ac}+\sqrt{bd}\right)$ equivale a $Z(W)$;

- $\sum_{y_1^2} \sqrt{W(y_1|0)\,W(y_2|0)\,W(y_2|1)\,W(y_1|1)} = Z(W)^2$.

Si ha l'uguaglianza in (2.14) se e solo se, per ogni scelta di y_1^2 è verificata una delle seguenti:

a. $W(y_1|0)\,W(y_2|0)\,W(y_2|1)\,W(y_1|1) = 0$;

b. $W(y_1|0) = W(y_1|1)$;

c. $W(y_2|0) = W(y_2|1)$.

Se W è un canale BEC, queste condizioni sono soddisfatte. Viceversa, se scegliamo $y_1 = y_2$, vediamo che per ottenere l'uguaglianza in (2.14) dobbiamo avere $W(y_1|0)W(y_1|1) = 0$ o $W(y_2|0)W(y_2|1) = 0$, che equivale a dire che W è un BEC.

Per dimostrare (2.15), riscriviamo $W_2^{(1)}$ come

$$W_2^{(1)}\left(y_1^2|u_1\right) = \frac{1}{2}\left(W(y_1|u_1)W(y_2|0) + W(y_1|u_1 \oplus 1)W(y_2|1)\right)$$

e applichiamo la Proposizione 2.4 per ottenere la disuguaglianza:

$$Z\left(W_2^{(1)}\right) \geq \frac{1}{2}\left(Z\left(W(y_1|u_1)W(y_2|0)\right) + Z\left(W(y_1|u_1 \oplus 1)W(y_2|1)\right)\right) = Z(W).$$

Per completare la dimostrazione ci basta osservare che $0 \leq Z(W) \leq 1$ e $Z\left(W_2^{(2)}\right) = Z(W)^2$ implicano $Z(W) \leq Z\left(W_2^{(2)}\right)$ con $Z(W) = Z\left(W_2^{(2)}\right)$ se e solo se $Z(W)$ vale 0 o 1 e questo, per la Proposizione 2.1, equivale a dire che $I(W)$ vale 0 o 1. □

I due risultati precedenti possono essere riassunti dalla seguente proposizione.

Proposizione 2.13. *Sia $N = 2^n$, $n \geq 0$, $1 \leq i \leq N$, la trasformazione*

$$\left(W_N^{(i)}, W_N^{(i)}\right) \mapsto \left(W_{2N}^{(2i-1)}, W_{2N}^{(2i)}\right)$$

preserva la mutua informazione e migliora l'affidabilità nel senso che

$$I\left(W_{2N}^{(2i-1)}\right) + I\left(W_{2N}^{(2i)}\right) = 2I\left(W_N^{(i)}\right)$$

$$Z\left(W_{2N}^{(2i-1)}\right) + Z\left(W_{2N}^{(2i)}\right) \leq 2Z\left(W_N^{(i)}\right)$$

e l'ultima è un'uguaglianza se e solo se $W_N^{(i)}$ è un canale BEC. Lo spezzamento allontana dal centro mutua informazione e affidabilità nel senso che

$$I\left(W_{2N}^{(2i-1)}\right) \leq I\left(W_N^{(i)}\right) \leq I\left(W_{2N}^{(2i)}\right)$$

$$Z\left(W_{2N}^{(2i)}\right) \leq Z\left(W_N^{(i)}\right) \leq Z\left(W_{2N}^{(2i-1)}\right)$$

e valgono tutte le uguaglianze se e solo se $I\left(W_N^{(i)}\right)$ vale 0 o 1. Il termine di affidabilità soddisfa anche

$$Z\left(W_N^{(i)}\right) \leq Z\left(W_{2N}^{(2i-1)}\right) \leq 2Z\left(W_N^{(i)}\right) - Z\left(W_N^{(i)}\right)^2$$

$$Z\left(W_N^{(i)}\right)^2 = Z\left(W_{2N}^{(2i)}\right) \leq Z\left(W_N^{(i)}\right).$$

Se consideriamo la trasformazione $W^N \mapsto \left(W_N^{(1)}, \ldots, W_N^{(N)}\right)$, mutua informazione e affidabilità

soddisfano

$$\sum_{i=1}^{N} I\left(W_N^{(i)}\right) = NI\left(W\right)$$

$$\sum_{i=1}^{N} Z\left(W_N^{(i)}\right) \leq NZ\left(W\right)$$

e l'ultima è un'uguaglianza se e solo se W è un canale BEC.

Dal momento che i canali BEC hanno rilevanza significativa in questo contesto, viene spontaneo chiedersi se la trasformazione di un canale conservi la proprietà di essere un canale a erasure. La risposta è nella seguente proposizione.

Proposizione 2.14. *Sia W un BEC con probabilità di erasure ϵ, allora i canali $W_2^{(1)}$ e $W_2^{(2)}$ sono BEC con probabilità di erasure $2\epsilon - \epsilon^2$ e ϵ^2 rispettivamente. Viceversa, se uno tra $W_2^{(1)}$ e $W_2^{(2)}$ è un BEC, W è un BEC.*

2.4 Convergenza di $I\left(W_N^{(i)}\right)$ e $Z\left(W_N^{(i)}\right)$

In questa sezione ci è più utile immaginarci il rapporto tra i canali $W_N^{(i)}$ come un albero binario come in Figura 2.7 e introdurre una nuova nuova notazione $W_{b_1 b_2 \dots b_n}$, $b_i \in \{0,1\}$ dove n indica che il canale è stato creato al livello n e $b_i = 0$ se all'i-simo livello si va verso l'alto, $b_i = 1$ se si va verso il basso.
Data questa descrizione, il canale $W_{2^n}^{(i)}$ è associato a $W_{b_1 b_2 \dots b_n}$, dove $i = 1 + \sum_{j=1}^{n} b_j 2^{n-j}$.

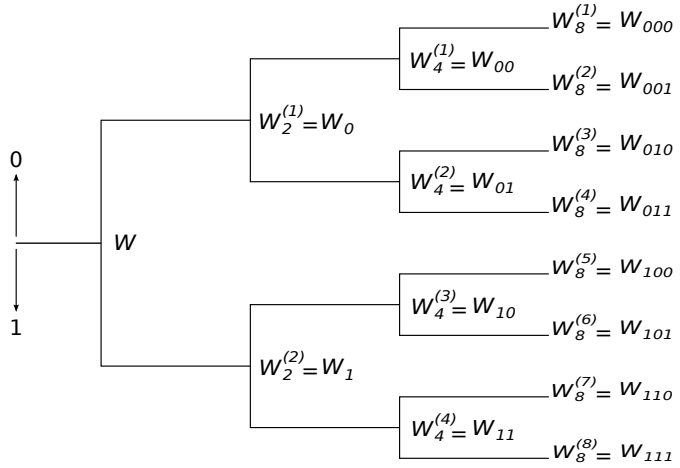

Figura 2.7: Albero che rappresenta la costruzione ricorsiva

Consideriamo lo spazio di probabilità $(\Omega, \mathcal{F}, P)$, dove:

- $\Omega = \{0,1\}^{\infty}$;

- $\mathcal{F}$ è l'algebra di Borel generata dagli $S(b_1, \ldots, b_n) := \{\omega \in \Omega \mid \omega_1 = b_1, \ldots \omega_n = b_n\}$;
- P è la probabilità definita su $\mathcal{F}$ tale che $P(S(b_1, \ldots, b_n)) = \frac{1}{2^n}$.

Per ogni $n \geq 1$, definiamo $\mathcal{F}_n$ come l'algebra di Borel generata dagli insiemi $S(b_1, \ldots, b_i)$, $1 \leq i \leq n$ e definiamo $\mathcal{F}_0$ come l'algebra di Borel generata dall'insieme vuoto e da Ω. Ovviamente, $\mathcal{F}_0 \subset \mathcal{F}_1 \subset \ldots \subset \mathcal{F}$.
Possiamo adesso definire un processo stocastico, che denotiamo con $\{K_n(\omega) \mid n \geq 0\}$ per $\omega \in \Omega$, legato alla costruzione dei canali:

- $K_0 = W$;
- se $K_n(\omega) = W_{\omega_1\omega_2\ldots\omega_n}$, $\quad K_{n+1} = \begin{cases} W_{\omega_1\omega_2\ldots\omega_n 0} & \text{con probabilità } \frac{1}{2} \\ W_{\omega_1\omega_2\ldots\omega_n 1} & \text{con probabilità } \frac{1}{2} \end{cases}$.

Quindi possiamo definire una sequenza di variabili aleatorie di Bernoulli $\{B_n(\omega) \mid n \geq 1\}$ dove $B_n(\omega) = \omega_n$ rappresenta la decisione al nodo n-simo e può assumere valori 0 e 1 con probabilità $1/2$, così che, se $B_1(\omega), \ldots, B_n(\omega)$ sono $\omega_1, \ldots, \omega_n$ rispettivamente, $K_n(\omega)$ è $W_{\omega_1\omega_2\ldots\omega_n}$. Definiamo

$$I_n(\omega) := I(K_n(\omega)), \tag{2.16}$$

$$Z_n(\omega) := Z(K_n(\omega)). \tag{2.17}$$

Per ogni $n \geq 0$ fissato, le variabili aleatorie B_n, K_n, I_n e Z_n sono misurabili rispetto all'algebra di Borel $\mathcal{F}_n$.

Adesso possiamo dimostrare alcuni risultati di convergenza per I_n e Z_n.

Proposizione 2.15. *La successione $\{I_n, \mathcal{F}_n \mid n \geq 0\}$ è una martingala, ovvero:*

$$\begin{aligned} &\mathcal{F}_n \subset \mathcal{F}_{n+1} \quad \text{ e } I_n \text{ è } \mathcal{F}_n\text{-misurabile} \\ &E[I_n] < \infty \\ &I_n = E[I_{n+1} \mid \mathcal{F}_n]. \end{aligned}$$

Inoltre, $\{I_n \mid n \geq 0\}$ converge q.o. ad una variabile aleatoria I_∞ tale che $E[I_\infty] = I_0$.

Dimostrazione. La prima condizione è vera per costruzione, mentre la seconda è vera perchè $0 < I_n < 1$. Per dimostrare che $I_n = E[I_{n+1} \mid \mathcal{F}_n]$, consideriamo $S(b_1, \ldots, b_n) \in \mathcal{F}_n$ e usiamo la Proposizione 2.13 per calcolare

$$\begin{aligned} E[I_n \mid S(b_1, \ldots, b_n)] &= \frac{1}{2} I(W_{b_1\ldots b_n 0}) + \frac{1}{2} I(W_{b_1\ldots b_n 1}) \\ &= I(W_{b_1\ldots b_n}) \end{aligned}$$

che equivale a I_n su $S(b_1, \ldots, b_n)$, quindi $\{I_n, \mathcal{F}_n\}$ è una martingala.
Osserviamo che $\{I_n, \mathcal{F}_n\}$ è una successione uniformemente integrabile, per concludere la dimostrazione ci serviamo di un risultato sulle martingale dimostrato in [11].

Teorema 2.16. *Sia $\{X_n, \mathcal{F}_n\}$ una martingala, le seguenti condizioni sono equivalenti:*

(a) $\{X_n, \mathcal{F}_n\}$ è una successione uniformemente integrabile;

(b) $\{X_n, \mathcal{F}_n\}$ converge in $\mathcal{L}^1$;

(c) $\{X_n, \mathcal{F}_n\}$ converge quasi ovunque ad una variabile aleatoria integrabile X_∞;

(d) esiste una variabile aleatoria integrabile tale che $X_n = E[Y \mid \mathcal{F}_n]$ per ogni $n \in \mathbb{N}$.

□

Proposizione 2.17. *La successione $\{Z_n, \mathcal{F}_n \mid n \geq 0\}$ è una supermartingala, ovvero:*

$$\begin{aligned} &\mathcal{F}_n \subset \mathcal{F}_{n+1} \quad \text{e } Z_n \text{ è } \mathcal{F}_n\text{-misurabile} \\ &E[Z_n] < \infty \\ &Z_n \geq E[Z_{n+1} \mid \mathcal{F}_n]. \end{aligned}$$

Inoltre, $\{Z_n \mid n \geq 0\}$ converge q.o. ad una v.a. Z_∞ che assume q.o. valori 0 o 1.

Dimostrazione. Le prime due condizioni sono ovvie. Per verificare che $Z_n \geq E[Z_{n+1} \mid \mathcal{F}_n]$, consideriamo $S(b_1, \ldots, b_n) \in \mathcal{F}_n$ e, per la Proposizione 2.13,

$$\begin{aligned} E[Z_{n+1} \mid S(b_1, \ldots, b_n)] &= \frac{1}{2} Z(W_{b_1,\ldots,b_n,0}) + \frac{1}{2} Z(W_{b_1,\ldots,b_n,1}) \\ &\leq Z(W_{b_1,\ldots,b_n}). \end{aligned}$$

Poichè $Z(W_{b_1,\ldots,b_n})$ è il valore di Z_n su $S(b_1, \ldots, b_n)$,

$$E[Z_{n+1} \mid \mathcal{F}_n] \leq Z_n$$

e $\{Z_n, \mathcal{F}_n \mid n \geq 0\}$ è una supermartingala. Poichè $\{Z_n, \mathcal{F}_n \mid n \geq 0\}$ è una successione uniformemente integrabile, possiamo applicare il seguente teorema dimostrato in [11].

Teorema 2.18. *Sia $\{X_n, \mathcal{F}_n\}$ una supermartingala, le seguenti condizioni sono equivalenti:*

(a) $\{X_n, \mathcal{F}_n\}$ è una successione uniformemente integrabile;

(b) $\{X_n, \mathcal{F}_n\}$ converge in $\mathcal{L}^1$;

(c) $\{X_n, \mathcal{F}_n\}$ converge quasi ovunque ad una variabile aleatoria integrabile X_∞ tale che

$$E[|X_n - X_\infty|] \to 0.$$

Quindi $\{Z_n, \mathcal{F}_n\}$ converge quasi ovunque a Z_∞ tale che $E[|Z_n - Z_\infty|] \to 0$.
Ne segue che $E[|Z_{n+1} - Z_n|] \to 0$ ma, per la Proposizione 2.13, $Z_{n+1} = Z_n^2$ con probabilità $1/2$ e quindi $E[|Z_{n+1} - Z_n|] \geq \frac{1}{2} E[Z_n(1 - Z_n)] \geq 0$. Ma allora $E[Z_n(1 - Z_n)] \to 0$ e questo implica $E[Z_\infty(1 - Z_\infty)] = 0$. Quindi Z_∞ assume q.o. valori 0 o 1.

□

Il prossimo risultato mostra come 0 e 1 siano gli unici punti fissi della capacità simmetrica di canale tramite le operazioni di trasformazione e in questo senso diciamo che le trasformazioni *polarizzano*.

Proposizione 2.19. *Siano I_∞ e Z_∞ come definite prima,*

$$I_\infty = 1 - Z_\infty$$

quasi ovunque con $P(I_\infty = 1) = I_0$ e $P(I_\infty = 0) = 1 - I_0$.

Dimostrazione. La Proposizione 2.1 e il risultato precedente implicano che $I_\infty = 1 - Z_\infty$ quasi ovunque. Il fatto che $E[I_\infty] = I_0$ ci permette di concludere la dimostrazione. □

Proposizione 2.20. *Sia W un canale B-DMC, allora*

$$I(W) + Z(W) \geq 1$$

e vale l'uguaglianza se e solo se W è un canale BEC.

Dimostrazione. Siano W e W' due canali tali che $Z(W) = Z(W') = z_0$. Supponiamo anche che W' sia un BEC, con probabilità di erasure z_0. Allora $I(W') = 1 - z_0$. Se consideriamo i processi stocastici $\{Z_n\}$ e $\{Z'_n\}$, grazie alla Proposizione 2.13, $P(Z_n \leq z) \geq P(Z'_n \leq z)$ per ogni $n \geq 1$, $0 \leq z \leq 1$. Quindi la probabilità che $\{Z_n\}$ converga a 0 è limitata dal basso dalla probabilità che $\{Z'_n\}$ converga a 0 e $I(W) \geq I(W')$. Questo implica che $I(W) + Z(W) \geq 1$. □

Adesso possiamo dimostrare il Teorema 2.5.

Dimostrazione. Sia $(\Omega, \mathcal{F}, P)$ uno spazio di probabilità e sia $\omega \in \Omega$, scriviamo la successione di parametri di affidabilità per $i \geq 0$ come definiti in (2.17):

$$Z_{i+1}(\omega) = Z_i^2 \quad \text{se } B_{i+1}(\omega) = 1,$$

$$Z_{i+i} \leq 2Z_i(\omega) - Z_i(\omega)^2 \leq 2Z_i(\omega) \quad \text{se } B_{i+1}(\omega) = 0.$$

Sia adesso $0 \leq \zeta \leq 1$ e $m \geq 0$, definiamo $T_m(\zeta) := \{\omega \in \Omega \mid Z_i(\omega) \leq \zeta \quad \forall i \geq m\}$. Per $\omega \in T_m(\omega)$ e $i \geq m$,

$$\frac{Z_{i+1}(\omega)}{Z_i(\omega)} \leq \begin{cases} 2 & \text{se } B_{i+1}(\omega) = 0, \\ \zeta & \text{se } B_{i+1}(\omega) = 1 \end{cases}$$

e quindi per ogni $n > m$

$$Z_n(\omega) \leq \zeta\, 2^{n-m} \prod_{i=m+1}^{n} \left(\frac{\zeta}{2}\right)^{B_i(\omega)}.$$

Siano $n > m \geq 0$ e $0 < \eta < 1/2$, definiamo l'evento

$$\mathcal{U}_{m,n}(\eta) := \left\{ \omega \in \Omega \;\middle|\; \sum_{i=m+1}^{n} B_i(\omega) > (1/2 - \eta)(n - m) \right\}.$$

Se prendiamo $\omega \in T_m(\zeta) \cap \mathcal{U}_{m,n}(\eta)$,

$$Z_n(\omega) \leq \zeta \left(2^{(1/2+\eta)}\zeta^{(1/2-\eta)}\right)^{n-m}$$

che per $\zeta = \zeta_0 = 1/2^4$ e $\eta = \eta_0 = 1/20$ diventa

$$Z_n(\omega) \leq 2^{-4-\frac{5(n-m)}{4}}. \tag{2.18}$$

Adesso vorremmo dimostrare che la relazione (2.18) ha probabilità abbastanza alta di verificarsi. Come prima cosa, enunciamo un risultato che dimostreremo più avanti.

Lemma 2.21. *Per ogni $\zeta,\ \epsilon > 0$, esiste $m_0(\zeta, \epsilon)$ intero positivo tale che*

$$P(T_{m_0}(\zeta)) \geq I_0 - \epsilon.$$

Per la disuguaglianza di Chernoff, possiamo scrivere

$$P(\mathcal{U}_{m,n}(\eta)) \geq 1 - 2^{-(n-m)(1-H(1/2-\eta))}$$

dove H rappresenta la funzione di entropia binaria. Sia $n_0(m, \eta, \epsilon)$ il più piccolo n tale che

$$1 - 2^{-(n_0(m,\eta,\epsilon)-m)(1-H(1/2-\eta))} \leq 1 - \epsilon.$$

Osserviamo che, se poniamo

$$m_1 = m_1(\delta) := m_0(\zeta_0, \delta)$$

$$n_1 = n_1(\delta) := n_0(m_1, \eta_0, \delta)$$

otteniamo

$$P\left(T_{m_1}(\zeta_0) \cap \mathcal{U}_{m_1,n}(\eta_0)\right) \geq I_0 - \delta \qquad n \geq n_1.$$

Se definiamo

$$c := 2^{-4+5m_1/4}$$

$$\mathcal{V}_n := \{\omega \in \Omega \mid Z_n(\omega) \leq c2^{-5n/4}\} \qquad n \geq 0$$

e, poiché

$$T_{m_1}(\zeta_0) \cap \mathcal{U}_{m_1,n}(\eta_0) \subset \mathcal{V}_n \qquad n \geq n_1,$$

allora $P(\mathcal{V}_n) \geq I_0 - \delta$ per $n \geq n_1$. D'altro canto,

$$P(\mathcal{V}_n) = \sum_{\omega_1^n \in \mathcal{X}^n} \frac{1}{2^n} 1_{|\{Z(W_{\omega_1^n}) \leq c2^{-5n/4}\}} = \frac{1}{2^n}|\mathcal{A}_n|,$$

dove definiamo $\mathcal{A}_n := \left\{i \in \{1, \ldots, N\} \;\middle|\; Z\left(W_{2^n}^{(i)}\right) \leq cN^{-5/4}\right\}$. Questo ci permette di concludere che, per $n \geq n_1(\delta)$, $|\mathcal{A}_n| \geq 2^n(I_0 - \delta)$ e il Teorema 2.5 è dimostrato. □

Dimostriamo il Lemma 2.21.

Dimostrazione. La dimostrazione ricalca quella di un risultato analogo di Chung ([11], Teorema 4.1.1).
Sia $\zeta > 0$ e

$$\Omega_0 := \{\omega \in \Omega \mid \lim_{n\to\infty} Z_n(\omega) = 0\},$$

per la Proposizione 2.19, $P(\Omega_0) = I_0$. Sia $\omega \in \Omega_0$ fissato, il fatto che $Z_n(\omega)$ converge a 0 implica che esiste $n_0(\omega, \zeta)$ tale che

$$n \geq n_0(\omega, \zeta) \quad \Rightarrow \quad Z_n(\omega) \leq \zeta.$$

Quindi esiste m tale che ω appartenga a $T_m(\zeta)$ e $\Omega_0 \subset \bigcup_{m=1}^{\infty} T_m(\zeta)$. Quindi

$$P\left(\bigcup_{m=1}^{\infty} T_m(\zeta)\right) \geq P(\Omega_0).$$

Dal momento che $T_m(\zeta) \to \bigcup_{m=1}^{\infty} T_m(\zeta)$, per la proprietà di convergenza monotona della misura,

$$\lim_{m\to\infty} P\left(T_m(\zeta)\right) = P\left(\bigcup_{m=1}^{\infty} T_m(\zeta)\right).$$

Quindi $\lim_{m\to\infty} P\left(T_m(\zeta)\right) \geq I_0$ e, per ogni $\zeta > 0$, $\delta > 0$, esiste finito $m_0 = m_0(\zeta, \delta)$ tale che, per ogni $m \geq m_0$, $P\left(T_m(\zeta)\right) \geq I_0 - \delta/2$. □

2.5 Caso del canale simmetrico

Sia $W : \mathcal{X} \to \mathcal{Y}$ un canale B-DMC simmetrico con $\mathcal{X} = \{0, 1\}$ e $\mathcal{Y}$ arbitrario. Poichè il canale è simmetrico, esiste una permutazione π_1 di $\mathcal{Y}$ tale che:

(i) $\pi_1 = \pi_1^{-1}$;

(ii) $W\left(y \mid 1\right) = W\left(\pi_1\left(y\right) \mid 0\right) \quad \forall y \in \mathcal{Y}$.

Chiamiamo π_0 la permutazione identità e, per semplicità di notazione, scriviamo $x \cdot y$ al posto di $\pi_x\left(y\right)$, dove $x \in \mathcal{X}$ e $y \in \mathcal{Y}$.

Osservazione 2.22. Le permutazioni $\{\pi_0, \pi_1\}$ formano un gruppo abeliano tramite l'azione di composizione.

Osservazione 2.23. Siano $x, a \in \mathcal{X}$, $y \in \mathcal{Y}$, osserviamo che

a. $W\left(y \mid x \oplus a\right) = W\left((x \oplus a) \cdot y \mid 0\right) = W\left(x \cdot (a \cdot y) \mid 0\right) = W\left(a \cdot y \mid x\right)$;

b. $W\left(y \mid x \oplus a\right) = W\left(x \cdot y \mid a\right)$ poich'e $\oplus$ è commutativa.

Consideriamo il canale prodotto $W^N : \mathcal{X}^N \to \mathcal{Y}^N$ per $N \geq 1$ e sia

$$x_1^N \cdot y_1^N := \left(x_1 \cdot y_1, \ldots, x_N \cdot y_N\right),$$

per ogni $x_1^N \in \mathcal{X}^N$, $y_1^N \in \mathcal{Y}^N$, la simmetria di W induce una simmetria nei canali W^N, W_N e $W_N^{(i)}$ come descritto dai risultati seguenti.

Proposizione 2.24. *Sia W un canale B-DMC simmetrico, allora il canale W^N verifica*

$$W^N\left(y_1^N \mid x_1^N \oplus a_1^N\right) = W^N\left(x_1^N \cdot y_1^N \mid a_1^N\right)$$

per ogni a_1^N, $x_1^N \in \mathcal{X}^N$, $y_1^N \in \mathcal{Y}^N$.

Dimostrazione. Segue in modo ovvio dai conti. □

Proposizione 2.25. *Sia W un canale B-DMC simmetrico, allora i canali W_N e $W_N^{(i)}$ verificano*

$$W_N\left(y_1^N \mid u_1^N\right) = W_N\left(a_1^N \cdot y_1^N \mid u_1^N \oplus a_1^N\right) \tag{2.19}$$

$$W_N^{(i)}\left(y_1^N, u_1^{i-1} \mid u_i\right) = W_N^{(i)}\left(a_1^N G_N \cdot y_1^N, u_1^{i-1} \oplus a_1^{i-1} \mid u_i \oplus a_i\right) \tag{2.20}$$

per ogni a_1^N, $u_1^N \in \mathcal{X}^N$, $y_1^N \in \mathcal{Y}^N$, $N = 2^n$, $n \geq 0$, $0 \leq i \leq N$.

Dimostrazione. Sia $u_1^N \in \mathcal{X}^N$ fissato e sia $x_1^N = u_1^N G_N$,

$$W_N(y_1^N|x_1^N) = \prod_{i=1}^N W(y_i|x_i) = \prod_{i=1}^N W(x_i \cdot y_i|0) = W_N(u_1^N \cdot y_1^N|0_1^N).$$

Analogamente,

$$W_N(u_1^N \cdot y_1^N|u_1^N \oplus a_1^N) = W_N((u_1^N \oplus a_1^N) \cdot (a_1^N \cdot y_1^N)|0_1^N) = W_N(u_1^N \cdot y_1^N|0_1^N)$$

e questo dimostra la prima parte della proposizione.
Per dimostrare la seconda, usiamo il risultato precedente:

$$\begin{aligned} W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) &= \sum_{u_{i+1}^N} \frac{1}{2^{N-1}} W_N(y_1^N|u_1^N) \\ &= \sum_{u_{i+1}^N} \frac{1}{2^{N-1}} W_N(a_1^N \cdot y_1^N|u_1^N \oplus a_1^N) \\ &= \sum_{v_{i+1}^N} \frac{1}{2^{N-1}} W_N(a_1^N \cdot y_1^N|(u_1^i \oplus a_1^i, v_{i+1}^N)) \\ &= W_N(a_1^N \cdot y_1^N, u_1^{i-1} \oplus a_1^{i-1}|u_i \oplus a_i) \end{aligned}$$

dove abbiamo posto $v_{i+1}^N := u_{i+1}^N \oplus a_{i+1}^N$. □

Osserviamo che la formula (2.20) vale per ogni scelta di a_1^N. Allora, se poniamo $a_1^i = u_1^i$, troviamo

$$W_N^{(i)}(y_1^N, u_1^{i-1} \mid u_i) = W_N^{(i)}(a_1^N G_N \cdot y_1^N, 0_1^{i-1} \mid 0). \tag{2.21}$$

Se definiamo $\mathcal{X}_{i+1}^N := \{a_1^N \in \mathcal{X}^N \mid a_1^i = 0_1^i\}$ per $1 \leq i \leq N$, per $a_1^N \in \mathcal{X}_{i+i}^N$ e $y_1^N \in \mathcal{Y}^N$, segue dall'equazione (2.21) con $u_1^i = 0_1^i$ che

$$W_N^{(i)}(y_1^N, 0_1^{i-1} \mid 0) = W_N^{(i)}(a_1^N G_N \cdot y_1^N, 0_1^{i-1} \mid 0). \tag{2.22}$$

A questo punto, possiamo definire

$$\mathcal{X}_{i+1}^N \cdot y_1^N := \{a_1^N G_N \cdot y_1^N \mid a_1^N \in \mathcal{X}_{i+1}^N\},$$

l'orbita di y_1^N tramite l'azione del gruppo $\mathcal{X}_{i+1}^N$ e chiamiamo $\mathcal{Y}_{i+1}^N$ l'insieme formato da un rappresentante per ciascuna classe di equivalenza. Per le simmetrie del canale, possiamo effettivamente dire che l'output del canale $W_N^{(i)}$ è rappresentato dall'insieme $\mathcal{Y}_{i+1}^N$.

Esempio 2.26. Sia W un BSC con $\mathcal{Y} = \{0, 1\}$, allora:

- ogni orbita $\mathcal{X}_{i+1}^N \cdot y_1^N$ ha 2^{N-i} elementi;
- ci sono 2^i orbite;
- il canale $W_N^{(1)}$ ha due output e, essendo a sua volta simmetrico, deve essere a sua volta un BSC;
- il canale $W_N^{(i)}$ dovrebbe avere un alfabeto di output di dimensione 2^{N+i-1} che per ragioni di simmetria si riducono ad essere 2^i.

Le proprietà di simmetria di $W_N^{(i)}$ semplificano il calcolo dei parametri del canale.

Proposizione 2.27. *Sia W un canale B-DMC simmetrico, allora*

$$Z\left(W_N^{(i)}\right) = 2^{i-1} \sum_{y_1^N \in \mathcal{Y}_{i+1}^N} \#\{\mathcal{X}_{i+1}^N \cdot y_1^N\} \sqrt{W_N^{(i)}\left(y_1^N, 0_1^{i-1} \mid 0\right) W_N^{(i)}\left(y_1^N, 0_1^{i-1} \mid 1\right)}.$$

Dimostrazione. Sia

$$Z\left(W_N^{(i)}\right) = \sum_{u_1^{i-1} \in \mathcal{X}^{i-1}} \sum_{y_1^N \in \mathcal{Y}^N} \sqrt{W_N^{(i)}\left(y_1^N, u_1^{i-1}|0\right) W_N^{(i)}\left(y_1^N, u_1^{i-1}|1\right)},$$

notiamo che nel caso del canale simmetrico la somma più interna è indipendente da u_1^{i-1} e quindi possiamo riscriverla come somma sui rappresentanti delle classi di equivalenza.

□

Esempio 2.28. Nel caso di un canale binario simmetrico BSC, la formula sopra diventa:

$$Z\left(W_N^{(i)}\right) = 2^{N-1} \sum_{y_1^N \in \mathcal{Y}_{i+1}^N} \sqrt{W_N^{(i)}\left(y_1^N, 0_1^{i-1} \mid 0\right) W_N^{(i)}\left(y_1^N, 0_1^{i-1} \mid 1\right)}$$

ed è una somma di 2^i termini.

3 | Polar Codes per canali binari

L'idea base dei polar codes è di creare un metodo di codifica tale che si possa accedere a ciascun canale $W_N^{(i)}$ separatamente e inviare dati solo attraverso i canali per i quali $Z\left(W_N^{(i)}\right)$ si avvicina a 0 o, equivalentemente, $I\left(W_N^{(i)}\right)$ si avvicina a 1.

3.1 Codifica

Trattiamo i polar codes come membri di una più ampia classe di codice a blocchi, ovvero codici senza memoria il cui nome deriva dal fatto che le parole di codice, di N cifre, dipendono solo dal corrispondente blocco di K bit generato dalla sorgente: dato $\mathcal{C}$ un (s, N) codice, scriviamo la matrice $s \times N$ formata dalle code words $w_1, \ldots, w_s$,

$$M = \begin{pmatrix} w_1 \\ \vdots \\ w_s \end{pmatrix}.$$

Se il rango di M è uguale a K, possiamo trovare tra le parole del codice un insieme di generatori linearmente indipendenti e il codice $\mathcal{C}$ è un sottospazio vettoriale di dimensione K dello spazio vettoriale delle N-uple a coefficienti in $\mathbb{Z}/2\,\mathbb{Z}$.

Definizione 3.1. Il codice (N, K) prende il nome di codice a blocchi lineare con k digits di informazione.

Dato un codice a blocchi di lunghezza N, ogni codice in questa classe ha una struttura che manda un input $u_1^N \in \mathcal{X}^N$ in una codeword $x_1^N \in \mathcal{X}^N$ attraverso

$$x_1^N = u_1^N G_N.$$

Sia adesso $\mathcal{A}$ un arbitrario sottoinsieme di $\{1, \ldots, N\}$, denotiamo con $G_N(\mathcal{A})$ la sottomatrice

di G_N formata dalle righe con indici in $\mathcal{A}$. Possiamo riscrivere $x_1^N = u_1^N G_N$ come

$$x_1^N = u_{\mathcal{A}} G(\mathcal{A}) \oplus u_{\mathcal{A}^c} G(\mathcal{A}^c).$$

Possiamo ottenere i codici opportuni nel modo seguente:

- scegliamo l'*insieme d'informazione* $\mathcal{A} \subset \{1, \dots, N\}$;
- scegliamo il *vettore congelato* o *vettore dei frozen bit* $u_{\mathcal{A}^c} \in \mathcal{X}^{N-K}$, dove K denota la cardinalità di $\mathcal{A}$;
- il *vettore dati* $u_{\mathcal{A}}$ è libero di assumere qualunque valore in $\mathcal{X}^K$.

Il codice risultante avrà rate $R = K/N$ e sarà chiamato codice $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$

Esempio 3.2. Consideriamo un codice $(4, 2, \{2, 4\}, (0, 1))$. La mappa di codifica è data da

$$x_1^4 = u_1^4 G_4 = (u_2, u_4) \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} + (0, 1) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix},$$

dove G_4 è definita come in precedenza:

$$G_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Per $(u_2, u_4) = (1, 1)$, otteniamo $x_1^4 = (1, 1, 0, 1)$.

3.1.1 Costruzione di G_N

Soffermiamoci un attimo sulla costruzione ricorsiva di G_N. Per farlo ci serve innanzitutto una definizione.

Definizione 3.3. Sia A una matrice $m \times n$ e B una matrice $p \times q$, il prodotto di Kronecker $A \otimes B$ è una matrice $mp \times nq$ definita a blocchi nel modo seguente:

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix}.$$

Possiamo definire ricorsivamente la potenza di Kronecker della matrice A:

- $A^{\otimes 1} = A$;
- $A^{\otimes n} = A \otimes A^{\otimes n-1}$ per $n \geq 2$.

Proprietà:

- il prodotto di Kronecker è un caso speciale di prodotto tensoriale, dunque è bilineare e associativo;
- il prodotto misto segue la regola $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

Tornando alla costruzione di G_N, sia adesso G_2 la matrice associata al kernel F,

$$G_2 = F := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

e, osservando la Figura 2.3, possiamo scrivere la seguente formula ricorsiva

$$G_N = \left(I_{N/2} \otimes F\right) R_N \left(I_2 \otimes G_{N/2}\right), \tag{3.1}$$

dove I_n è la matrice identità $n \times n$.

Consideriamo una costruzione alternativa, ma equivalente, per W_N, sempre ricorsiva, definita come mostrato nella Figura 3.1.

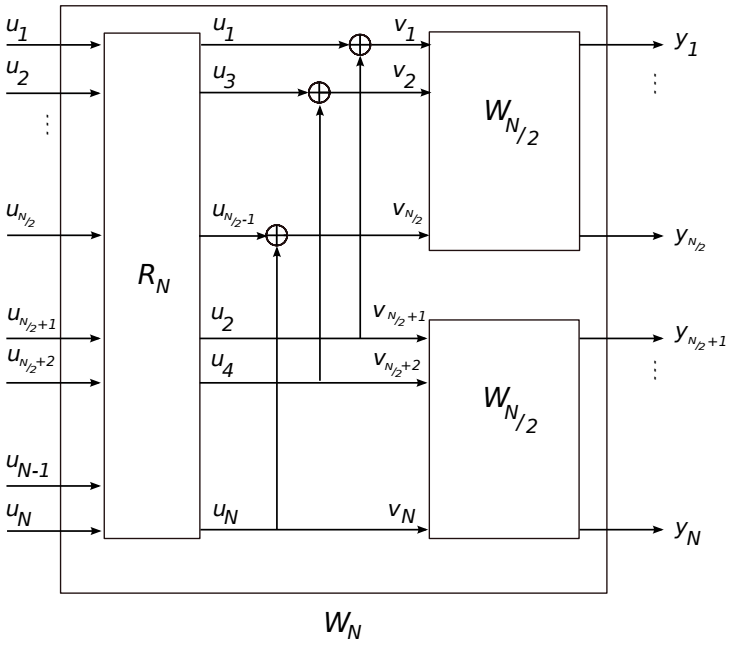

Figura 3.1: Costruzione alternativa di W_N

Con la nuova costruzione otteniamo un'altra formula ricorsiva per la matrice generatrice, ovvero

$$G_N = R_N \left(F \otimes G_{N/2}\right).$$

Dal momento che $G_{N/2}$ è a sua volta uguale a $R_{N/2}\left(F \otimes G_{N/4}\right)$, possiamo scrivere

$$G_N = R_N\left(F \otimes \left(R_{N/2}\left(F \otimes G_{N/4}\right)\right)\right)$$

$$= R_N\left(I_2 \otimes R_{N/2}\right)\left(F^{\otimes 2} \otimes G_{N/4}\right),$$

usando il fatto che $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.
Ripetendo il ragionamento, otteniamo

$$G_N = B_N F^{\otimes \log N} \tag{3.2}$$

dove $B_N := R_N\left(I_2 \otimes R_{N/2}\right)\left(I_4 \otimes R_{N/4}\right)\ldots\left(I_{N/2} \otimes R_2\right)$ è l'operatore di *inversione di bit*.

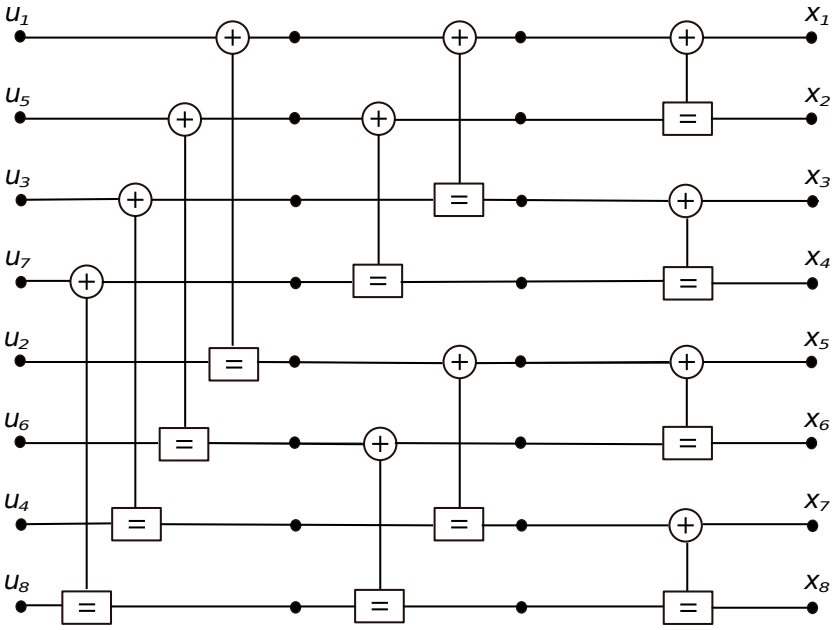

Figura 3.2: Il grafo rappresenta la trasformazione $F^{\otimes 3}$.

Bit-indexing

Per continuare ad analizzare l'operazione di codifica, ci conviene indicizzare vettori e matrici con sequenze di bit.
Sia a_1^N il vettore di lunghezza $N = 2^n$, $n > 0$, e sia a_i l'elemento di posto i di a_1^N, denotiamo a_i con

$$a_{b_1 \ldots b_n},$$

dove i $b_1, \ldots, b_n$ sono i coefficienti dell'espansione binaria di $i - i$, ovvero

$$i - 1 = \sum_{j=1}^{n} b_j 2^{n-j}.$$

Analogamente, denotiamo l'elemento $A_{i,j}$ di posto (i,j) della matrice $N \times N$ A con

$$A_{b_1 \dots b_n, b'_1 \dots b'_n},$$

dove $b_1 \dots b_n$ e $b'_1 \dots b'_n$ sono rispettivamente l'espansione binaria di $i-1$ e $j-1$.

Usando questa notazione, sia A una matrice $2^n \times 2^n$ e B una matrice $2^m \times 2^m$; la matrice prodotto $C = A \otimes B$ ha elementi

$$C_{b_1 \dots b_{n+m}, b'_1 \dots b'_{n+m}} = A_{b_1 \dots b_n, b'_1 \dots b'_n} B_{b_{n+1} \dots b_{n+m}, b'_{n+1} \dots b'_{n+m}}.$$

Consideriamo l'operazione di codifica con questa notazione:

- la matrice F in questa forma è data da elementi

$$F_{b,b'} = 1 \oplus b' \oplus bb' \quad b, b' \in \{0,1\}$$

  quindi $F^{\otimes n}$ ha elementi

$$F^{\otimes n}_{b_1 \dots b_n, b'_1 \dots b'_n} = \prod_{i=1}^{n} F_{b_i, b'_i} = \prod_{i=1}^{n} (1 \oplus b'_i \oplus b_i b'_i); \tag{3.3}$$

- l'operatore R_N agisce sul vettore riga u_1^N scambiando l'elemento indicizzato con $b_1 \dots b_n$ con quello di indice $b_2 \dots b_n b_1$, ovvero R_N ruota ciclicamente gli indici spostandoli a destra di una posizione, quindi se $v_1^N = u_1^N R_N$, allora

$$v_{b_1 \dots b_n} = u_{b_2 \dots b_n b_1} \quad b_i \in \{0,1\};$$

- la matrice B_N che compare in 3.2 può essere interpretata come la matrice di inversione di bit, quindi se $v_1^N = u_1^N B_N$, allora

$$v_{b_1 \dots b_n} = u_{b_n \dots b_1} \quad b_i \in \{0,1\}.$$

Lemma 3.4. *La matrice B_N è un operatore di inversione di bit.*

Dimostrazione. Mostriamo l'idea della dimostrazione con un esempio.
Supponiamo che B_4 sia un operatore di inversione di bit, dimostriamo che lo è anche B_8.
Sia u_1^8 un vettore qualsiasi, usando la notazione di bit-indexing possiamo scrivere

$$u_1^8 = (u_{000}, u_{001}, u_{010}, u_{011}, u_{100}, u_{101}, u_{110}, u_{111}).$$

Dal momento che $u_1^8 B_8 = u_1^8 R_8 (I_2 \otimes B_4)$, consideriamo l'azione di R_8 su u_1^8,

$$u_1^8 R_8 = (u_{000}, u_{010}, u_{100}, u_{110}, u_{001}, u_{011}, u_{101}, u_{111}).$$

Denotiamo con c_1^4 e d_1^4 la metà sinistra e destra di $u_1^8 R_8$ rispettivamente:

$$c_1^4 := (u_{000}, u_{010}, u_{100}, u_{110})$$
$$d_1^4 := (u_{001}, u_{011}, u_{101}, u_{111})$$

e osserviamo che

$$c_{b_1 b_2} = u_{b_1 b_2 0} \quad \text{e} \quad d_{b_1 b_2} = u_{b_1 b_2 1} \quad \forall b_1, b_2 \in \{0, 1\}.$$

Adesso consideriamo l'azione di $I_2 \otimes B_4$ su (c_1^4, d_1^4),

$$\begin{aligned}(c_1^4 B_4, d_1^4 B_4) &= (c_{00}, c_{10}, c_{01}, c_{11}, d_{00}, d_{10}, d_{01}, d_{11}) \\ &= (u_{000}, u_{100}, u_{010}, u_{110}, u_{001}, u_{011}, u_{101}, u_{111})\end{aligned}$$

quindi B_8 è un operatore di inversione di bit.
Il caso generale è analogo.

□

- la matrice G_N con queste notazioni ha la forma mostrata dal seguente risultato.

Proposizione 3.5. *Sia $N = 2^n$, $n > 1$, la matrice generatrice G_N è data da*

$$G_N = B_N F^{\otimes n} = F^{\otimes n} B_N. \tag{3.4}$$

La matrice G_N è invariante rispetto all'inversione di bit e ha elementi

$$(G_N)_{b_1 \dots b_n, b'_1 \dots b'_n} = \prod_{i=1}^{n} (1 \oplus b'_i \oplus b_{n-i} b'_i). \tag{3.5}$$

Dimostrazione. Osserviamo che, per ogni matrice A di dimensione $N \times N$, il prodotto $C = B_N^T A B_N$ ha elementi

$$C_{b_1 \dots b_n, b'_1 \dots b'_n} = A_{b_n \dots b_1, b'_n \dots b'_1}.$$

Quindi se A è invariante rispetto alla permutazione di bit, ovvero se

$$A_{b_1 \dots b_n, b'_1 \dots b'_n} = A_{b_n \dots b_1, b'_n \dots b'_1},$$

si ha $A = B_N^T A B_N$. Poiché B_N è simmetrica ed è una permutazione, $B_N^{-1} = B_N$ e

$$B_N A = A B_N$$

per ogni matrice A invariante rispetto alla permutazione di bit.
Segue da 3.3 che la matrice $F^{\otimes n}$ è invariante rispetto alla permutazione di bit, quindi commuta con B_N e, poiché sapevamo già che $G_N = B_N F^{\otimes n}$, abbiamo dimostrato anche

che $G_N = F^{\otimes n} B_N$.
La formula 3.5 segue dall'aver applicato l'inversione di bit a 3.3. □

Prima di dimostrare l'ultimo risultato di questa sezione, definiamo la distanza tra due sequenze binarie.

Definizione 3.6. Siano $v_1 = (v_1^1, \dots, v_1^n)$ e $v_2 = (v_2^1, \dots, v_2^n)$ due n-sequenze binarie, la distanza di Hamming tra v_1 e v_2 è

$$d(v_1, v_2) = \#\{i \mid v_1^i \neq v_2^i\}.$$

Proposizione 3.7. *La distanza di Hamming è una vera distanza, ovvero verifica:*

- $d(v_1, v_2) \geq 0 \quad e \quad d(v_1, v_2) = 0$ *se e solo se* $v_1 = v_2$*;*
- $d(v_1, v_2) = d(v_2, v_1)$*;*
- $d(v_1, v_3) \leq d(v_1, v_2) + d(v_2, v_3)$.

Definizione 3.8. Il peso di Hamming di una sequenza v è

$$w_H(v) = d(v, 0),$$

la distanza di Hamming di v dalla sequenza nulla.

Proposizione 3.9. *Sia* $N = 2^n$*,* $n > 0$*, e siano* $b_1, \dots, b_n \in \{0, 1\}$*, le righe di* G_N *e di* $F^{\otimes n}$ *di indice* $b_1 \dots b_n$ *hanno peso di Hamming* $2^{w_H(b_1,\dots,b_n)}$ *dove*

$$w_H(b_1, \dots, b_n) := \sum_{i=1}^{n} b_i \tag{3.6}$$

Dimostrazione. Per ogni $b_1, \dots, b_n$, la somma in $\mathbb{Z}$ dei termini di $(G_N)_{b_1 \dots b_n, b'_1 \dots b'_n}$ al variare di $b'_1, \dots, b'_n$ equivale al peso di Hamming della riga di G_N di indice $b_1 \dots b_n$. Poiché abbiamo dimostrato nella Proposizione 3.5 che $(G_N)_{b_1 \dots b_n, b'_1 \dots b'_n} = \prod_{i=1}^{n} (1 \oplus b'_i \oplus b_{n-i} b'_i)$, si vede facilmente che questa somma è proprio

$$2^{w_H(b_1,\dots,b_n)}.$$

La dimostrazione per $F^{\otimes n}$ è analoga. □

Complessità computazionale

Chiamiamo $\chi_E(N)$ la più alta complessità di codifica tra tutti i codici avente lunghezza di blocco N. Se consideriamo come unità la complessità dell'addizione modulo 2 e la complessità dell'operazione di permutazione R_N come N unità, allora vediamo dalla Figura 2.3 che

$$\chi_E(N) \leq \frac{N}{2} + N + 2\chi_E\left(\frac{N}{2}\right).$$

Poiché $\chi_E(2) = 1$, otteniamo $\chi_E(N) = \frac{3}{2} N \log N$ e quindi la codifica ha complessità $O(N \log N)$.

3.1.2 Scelta di $\mathcal{A}$

Denotiamo con $P_e(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ la probabilità di errori di blocco per un codice $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$, assumendo che ciascun vettore $u_{\mathcal{A}}$ sia inviato con probabilità $\frac{1}{2^K}$ e la decodifica sia effettuata attraverso l'SC decoder descritto nel paragrafo precedente. Denotiamo invece con $P_e(N, K, \mathcal{A})$ la probabilità di errori di blocco attraverso un SC decoder pesata su tutti i codici $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ aventi uguale probabilità per ogni scelta di $u_{\mathcal{A}^c} \in \mathcal{X}^{N-K}$, ovvero

$$P_e(N, K, \mathcal{A}) := \sum_{u_{\mathcal{A}^c}} \frac{1}{2^{N-K}} P_e(N, K, \mathcal{A}, u_{\mathcal{A}^c}).$$

Proposizione 3.10. *Sia W un canale B-DMC, per ogni insieme $(N, K, \mathcal{A})$ di codici, la probabilità di errore di blocco soddisfa*

$$P_e(N, K, \mathcal{A}) \leq \sum_{i \in \mathcal{A}} Z\left(W_N^{(i)}\right).$$

La disuguaglianza suggerisce di scegliere $\mathcal{A}$ tra tutti i possibili sottoinsiemi di $\{1, \ldots, K\}$ in modo tale da minimizzare la sommatoria a destra. Quest'idea ci permette di dare, finalmente, la definizione di *polar code*.

Definizione 3.11. Sia W un canale B-DMC, un codice $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ è detto polar code se l'insieme $\mathcal{A}$ ha la seguente proprietà: ogni $i \in \mathcal{A}$ è scelto in modo che $Z\left(W_N^{(i)}\right)$ sia tra i K valori inferiori di $\left\{ Z\left(W_N^{(j)}\right) \,\middle|\, j = 1, \ldots, N \right\}$.

Osservazione 3.12. Notiamo che la definizione di polar code dipende dalla caratteristiche specifiche del canale. Infatti, un codice può essere un polar code per un canale e non esserlo per un altro.

Complessità computazionale

L'algoritmo di costruzione di un polar code ha bisogno di tre input:

- il canale B-DMC $W : \mathcal{X} \to \mathcal{Y}$;
- la lunghezza del blocco N;
- la dimensione del codice K.

L'output è un insieme d'informazione $\mathcal{A} \subset \{1, \ldots, N\}$ di dimensione K tale che sia minima la somma $\sum_{i \in \mathcal{A}} Z\left(W_N^{(i)}\right)$.
In linea di principio, per costruire il codice basta calcolare il valore di $Z\left(W_N^{(i)}\right)$ per ogni i e ordinarli, ma poiché non abbiamo un algoritmo efficiente per questo metodo, quel che facciamo è cercare costruzioni approssimate basate sulla stima dei parametri $Z\left(W_N^{(i)}\right)$.
La costruzione dei polar codes ha una formula semplice per i canali BEC, per i quali

$$\begin{cases} Z\left(W_2^{(2)}\right) = Z\left(W\right)^2 ; \\ Z\left(W_2^{(1)}\right) = 2Z\left(W\right) - Z\left(W\right)^2 . \end{cases}$$

Calcoliamo ricorsivamente il vettore $z_N = (z_{N,1}, \ldots, z_{N,N})$ tramite

$$z_{2k,j} = \begin{cases} 2z_{k,j} - z_{k,j}^2 & 1 \leq j \leq k \\ z_{k,j-k}^2 & k+1 \leq j \leq 2k \end{cases}$$

per $k = 1, 2, 2^2, \ldots, 2^{n-1}$ e con valore iniziale $k_{1,1} = p_e$ uguale alla probabilità di erasure.
Dato il vettore z_N e scelti i K elementi più piccoli del vettore, l'insieme d'informazione $\mathcal{A}$ è costituito dagli indici di tali elementi. Si verifica facilmente che il costo computazione è $O(N \log N)$.
Sfortunatamente, la costruzione esatta del codice per canali arbitrari è molto più complessa e per questa ragione, dato un canale binario arbitrario con capacità C, Arıkan suggerisce in [6] di costruire il polar code per il canale BEC con la stessa capacità e con probabilità di erasure $p_e = 1 - C$.

3.2 Decodifica

Supponiamo di avere un codice $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$. Sia u_1^N la sequenza codificata nella codeword x_1^N, inviamo x_1^N tramite il canale W^N e denotiamo la sequenza ricevuta con y_1^N. Lo scopo della decodifica è generare un vettore $\widehat{u}_1^N$ che stimi u_1^N conoscendo $\mathcal{A}$ e $u_{\mathcal{A}^c}$.
La decodifica stima sempre correttamente la parte di vettore congelato ponendo $\widehat{u}_{\mathcal{A}^c} = u_{\mathcal{A}^c}$, quindi la vera difficoltà è stimare $\widehat{u}_{\mathcal{A}}$.
Diremo che si è verificato un *errore di blocco* se $\widehat{u}_1^N \neq u_1^N$ o equivalentemente se $\widehat{u}_{\mathcal{A}^c} \neq u_{\mathcal{A}^c}$.

Consideriamo una decodifica a cancellazione successiva (SC decoder), che calcoli $\widehat{u}_i$. A questo scopo dobbiamo prima dare una definizione.

Definizione 3.13. Sia $h_i : \mathcal{Y}^N \times \mathcal{X}^{i-1} \to \mathcal{X}$; h_i prende il nome di funzione di decisione se è la mappa definita da

$$h_i(y_1^N, u_1^{i-1}) := \begin{cases} 0 & \text{se } W_N^{(i)}(y_1^N, u_1^{i-1} \mid 0) \geq W_N^{(i)}(y_1^N, u_1^{i-1} \mid 1) \\ 1 & \text{altrimenti} \end{cases}$$

per ogni $y_1^N \in \mathcal{Y}^N$, $u_1^{i-1} \in \mathcal{X}^{i-1}$.

Detto questo, possiamo calcolare l'intero vettore $\widehat{u}_1^N$ ponendo

$$\widehat{u}_i = \begin{cases} u_1 & i \in \mathcal{A}^c \\ h_i(y_1^N, \widehat{u}_1^{i-1}) & i \in \mathcal{A} \end{cases} .$$

3.2.1 Un primo algoritmo di decodifica

Un SC decoder per un arbitrario codice $(N, K, \mathcal{A}, u_{\mathcal{A}})$ osserva $(y_1^N, u_{\mathcal{A}^c})$ e genera una stima $\widehat{u}_1^N$ di u_1^N. Possiamo vedere il decoder come consistente di N elementi di decisione, uno per

ciascun u_i. Come abbiamo già detto, se $i \in \mathcal{A}^c$, l'elemento u_i è noto; se invece $i \in \mathcal{A}$, il decoder calcola il *rapporto di verosimiglianza* LR (dall'inglese *likelihood ratio*)

$$L_N^{(i)} := \frac{W_N^{(i)}\left(y_1^N, \widehat{u}_1^{i-1} \mid 0\right)}{W_N^{(i)}\left(y_1^N, \widehat{u}_1^{i-1} \mid 1\right)}$$

e genera la decisione

$$\widehat{u}_i = \begin{cases} 0 & \text{se } L_N^{(i)} \geq 1 \\ 1 & \text{altrimenti} \end{cases}.$$

Se usiamo le formule ricorsive (2.6) e (2.7), per trovare $L_N^{(i)}$ calcoliamo:

$$L_N^{(2i-1)}\left(y_1^N, \widehat{u}_1^{2i-2}\right) = \frac{L_{N/2}^{(i)}\left(y_1^{N/2}, \widehat{u}_{1,e}^{2i-2} \oplus \widehat{u}_{1,o}^{2i-2}\right) L_{N/2}^{(i)}\left(y_{N/2+1}^N, \widehat{u}_{1,e}^{2i-2}\right) + 1}{L_{N/2}^{(i)}\left(y_1^{N/2}, \widehat{u}_{1,e}^{2i-2} \oplus \widehat{u}_{1,o}^{2i-2}\right) + L_{N/2}^{(i)}\left(y_{N/2+1}^N, \widehat{u}_{1,e}^{2i-2}\right)}$$

$$L_N^{(2i)}(y_1^N, \widehat{u}_1^{2i-1}) = \begin{cases} L_{N/2}^{(i)}\left(y_1^{N/2}, \widehat{u}_{1,e}^{2i-2} \oplus \widehat{u}_{1,o}^{2i-2}\right) L_{N/2}^{(i)}\left(y_{N/2+1}^N, \widehat{u}_{1,e}^{2i-2}\right) & \widehat{u}_{2i-1} = 0 \\ L_{N/2}^{(i)}\left(y_{N/2+1}^N, \widehat{u}_{1,e}^{2i-2}\right) / L_{N/2}^{(i)}\left(y_1^{N/2}, \widehat{u}_{1,e}^{2i-2} \oplus \widehat{u}_{1,o}^{2i-2}\right) & \widehat{u}_{2i-1} = 1 \end{cases}.$$

Quindi il calcolo di $L_N^{(i)}$ si è ridotto al calcolo di due LR di lunghezza $N/2$ che a loro volta possono essere ottenuti tramite calcoli di LR di lunghezza $N/4$ e così via.

Complessità computazionale

Per ogni $k \in \{N, N/2, N/4, \ldots, 2, 1\}$, chiamiamo $\chi_L(k)$ la più alta complessità possibile per $L_k^{(i)}\left(y_1^N, v_1^{i-1}\right)$ per $1 \leq i \leq k$ e $(y_1^N, v_1^{i-1}) \in \mathcal{Y}^k \times \mathcal{X}^{i-1}$. Grazie alle formule ricorsive, possiamo scrivere

$$\chi_L(k) \leq 2\chi_L\left(\frac{k}{2}\right) + a$$

dove a è la complessità data dall'assemblare i due LR di lunghezza $k/2$. Prendendo come unità $\chi_L^{(i)}$, otteniamo

$$\chi_L(N) \leq (1+a)N = O(N).$$

La complessità totale può essere limitata da

$$\chi_D(N) \leq K\chi_L(N) \leq N\chi_L(N) = O(N^2).$$

3.2.2 Implementazione dell'algoritmo di decodifica

Osserviamo che

$$L_N^{(2i-1)}\left(y_1^N, \widehat{u}_1^{2i-2}\right) \quad \text{e} \quad L_N^{(2i)}\left(y_1^N, \widehat{u}_1^{2i-1}\right),$$

entrambi di lunghezza N, sono calcolati usando la stessa coppia di LR,

$$L_{N/2}^{(i)}\left(y_{N/2+1}^{N}, \widehat{u}_{1,e}^{2i-2}\right) \quad \text{e} \quad L_{N/2}^{(i)}\left(y_{1}^{N/2}, \widehat{u}_{1,e}^{2i-2} \oplus \widehat{u}_{1,o}^{2i-2}\right)$$

di lunghezza $N/2$. Quindi, tutti gli N valori di LR di lunghezza N possono essere calcolati usando N valori di LR di lunghezza $N/2$.
Possiamo dividere gli N valori di LR di lunghezza $N/2$ in due classi disgiunte:

- $\left\{L_{N/2}^{(i)}\left(y_{N/2+1}^{N}, \widehat{u}_{1,e}^{2i-2}\right) \mid 1 \leq i \leq N/2\right\}$;
- $\left\{L_{N/2}^{(i)}\left(y_{1}^{N/2}, \widehat{u}_{1,e}^{2i-2} \oplus \widehat{u}_{1,o}^{2i-2}\right) \mid 1 \leq i \leq N/2\right\}$.

Analogamente, ciascuna di queste classi richiede il calcolo di $N/2$ valori di LR ciascuno di lunghezza $N/4$. Sia $v_1^{N/2} := \widehat{u}_{1,e}^{N/2} \oplus \widehat{u}_{1,o}^{N/2}$, possiamo a loro volta dividere i valori di LR di lunghezza $N/4$ in due classi:

- $\left\{L_{N/4}^{(i)}\left(y_{N/4+1}^{N/2}, v_{1,e}^{2i-2}\right) \mid 1 \leq i \leq N/4\right\}$;
- $\left\{L_{N/4}^{(i)}\left(y_{1}^{N/4}, v_{1,e}^{2i-2} \oplus v_{1,o}^{2i-2}\right) \mid 1 \leq i \leq N/4\right\}$.

Ripetendo il ragionamento visto sopra induttivamente, vediamo che ad ogni passaggio la lunghezza del blocco si dimezza e sono richiesti N calcoli di LR, per un totale di $(1+N)\log N$ calcoli.

Per spiegare il ragionamento più nel dettaglio, studiamo ad esempio un codice

$$(N, K, \mathcal{A}, u_{\mathcal{A}^c}) = (8, 5, \{3, 5, 6, 7, 8\}, (0, 0, 0)).$$

La decodifica è descritta nel grafo della Figura 3.3:

- il grafo ha $N(\log N + 1) = 32$ nodi, ciascuno corrispondente ad un calcolo di LR, ed ha N righe e $\log N + 1$ colonne;
- la prima colonna da sinistra rappresenta il calcolo di LR di lunghezza 8;
- la seconda il calcolo di lunghezza 4;
- la terza di lunghezza 2;
- la quarta di lunghezza 1 (livello del canale).

Ciascun nodo ha due etichette, una che designa l'odine in cui avvengono i calcoli e l'altra con l'argomento del calcolo di ciascun LR. Possiamo immaginarci il decoder come N elementi di decisione (DE) all'estrema sinistra del grafo.
Notiamo che il grafo, se letto da destra a sinistra, è lo stesso della Figura 2.4, infatti il processo di decodifica avviene a posteriori.

La decodifica inizia al nodo 1 col calcolo di $L_8^{(1)}\left(y_1^8\right)$:

- il nodo 1 chiama il nodo 2 per il calcolo di $L_4^{(1)}\left(y_1^4\right)$, il programma passa al nodo 2 e il nodo 1 aspetta finché il nodo 2 non risponde con il calcolo di LR richiesto;
- il nodo 2 chiama il nodo 3;
- il nodo 3 chiama il nodo 4, che è un nodo al livello del canale, quindi calcola $L_1^{(1)}(y_1)$ e lo manda al nodo 3;
- il nodo 3 ha bisogno di ulteriori informazioni e chiama il nodo 5 che manda $L_1^{(1)}(y_2)$ al nodo 3
- il nodo 3 assembla i risultati ottenuti dai nodi 4 e 5 e invia il risultato ottenuto al nodo 2;
- il nodo 2 chiama il nodo 6, che a sua volta chiama i nodi 7 e 8 e manda il risultato al nodo 2;
- il nodo 2 calcola $L_4^{(1)}\left(y_1^4\right)$ e lo manda al nodo 1;
- il nodo 1 ora chiama il nodo 9 e il processo si ripete come nella figura;
- il nodo 1 assembla i risultati ottenuti, ottiene $L_8^{(1)}\left(y_1^8\right)$ e lo invia a DE 1.

Poiché u_1 è un nodo congelato, DE 1 ignora il riultato ottenuto, dichiara $\widehat{u}_1 = 0$ e passa a controllare DE 2, ovvero il nodo 16.
Per trovare $L_8^{(2)}\left(y_1^8, \widehat{u}\right)$ al nodo 16 servono i valori dei nodi 2 e 9, già calcolati e solo da assemblare.
I procedimenti per DE 3, DE 4. DE 5, DE 6, DE 7 e DE 8 sono analoghi.

Possiamo implementare ulteriormente la decodifica. Per spiegarlo, osserviamo la Figura 3.4 (il grafo è lo stesso di prima ma abbiamo cambiato l'etichetta dei nodi):

- i nodi a livello del canale (1, 2, 3, 4, 5, 6, 7 e 8) calcolano i loro valori LR $L_N^{(i)}(y_i)$ e inviano i valori ottenuti alla loro sinistra;
- al secondo passo i nodi 9, 11, 13 e 15 calcolano i loro valori LR (mentre il nodo 10, ad esempio, deve aspettare il calcolo di $\widehat{u}_i \quad i = 1, \ldots, 4$);
- al terzo passo i nodi 17 e 21 calcolano i valori LR;
- il processo si ripete come mostrato in Figura 3.4 fino al 15-simo passo, quando il nodo 32 calcola $\widehat{u}_8$.

In generale, se la lunghezza di blocco è N, serviranno $2N - 1$ passaggi.

La numerazione dei nodi ha a che fare con l'ordine con cui vengono chiamati. Quest'ordine lo possiamo pensare come un albero binario, come in figura 3.5. Al primo passo, corrispondente alla colonna più a destra del grafo della Figura 3.4, vengono calcolati tutti i valori $L_N^{(i)}(y_i)$. Al secondo passo si calcolano i valori di LR dei nodi della seconda colonna con etichette congrue

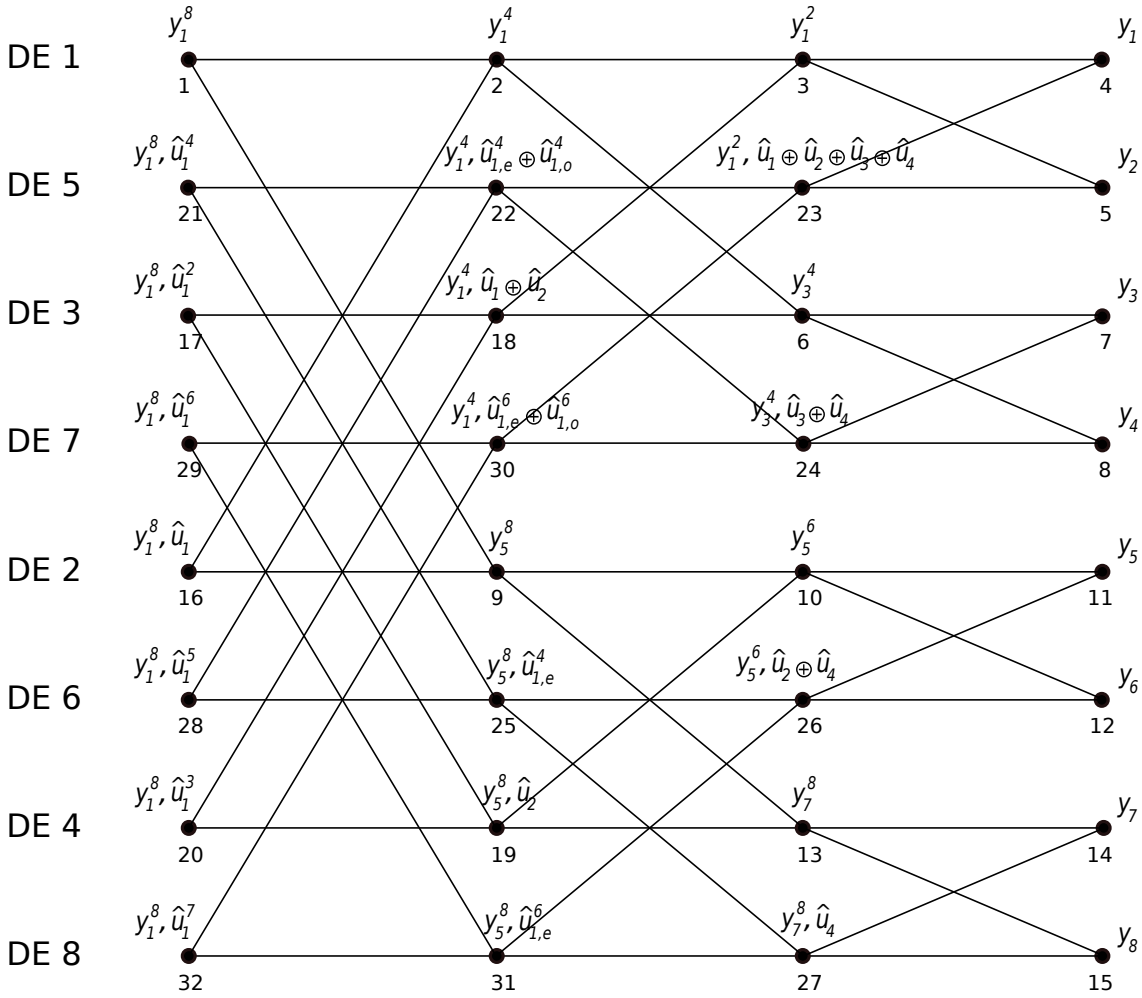

Figura 3.3: Implementazione di un SC decoder con $N = 8$.

a 1 modulo 2, al terzo passo i nodi della terza colonna di etichette congrue a 1 modulo 2^2, al quarto i nodi della quarta colonna di etichette congrue a 1 modulo 2^3. Arrivati a questo punto si calcola $L_8^{(1)}\left(y_1^8\right)$ e $\widehat{u}_1$ e si passa al sottoalbero che calcola il valore di LR del nodo di etichetta congrua a $1 + 2^2 = 5$.
Fatto questo si passa al sottoalbero che calcola i valori di LR della terza colonna di etichette congrue a 3 modulo 2^3.
L'albero si può generalizzare osservando che, se abbiamo calcolato i valori LR dei nodi del grafo della Figura 3.4 della colonna i che hanno etichette congrue a k modulo 2^{i-1}, questo nella figura 3.5 si traduce nel trovarsi in un nodo dal quale partono due sottoalberi, quello in alto che chiamerà i nodi della colonna $i+1$ che hanno etichette congrue a k modulo 2^i e quello in basso che chiamerà i nodi della colonna $i+1$ che hanno etichette congrue a $k+2^{i-1}$ modulo 2^i.

Un'alternativa a questa forma di decodifica, che usa ricorsivamente moltiplicazione e divisione, è passare ai logaritmi delle funzioni LR. Il metodo usato finora prevedeva che a ciascun

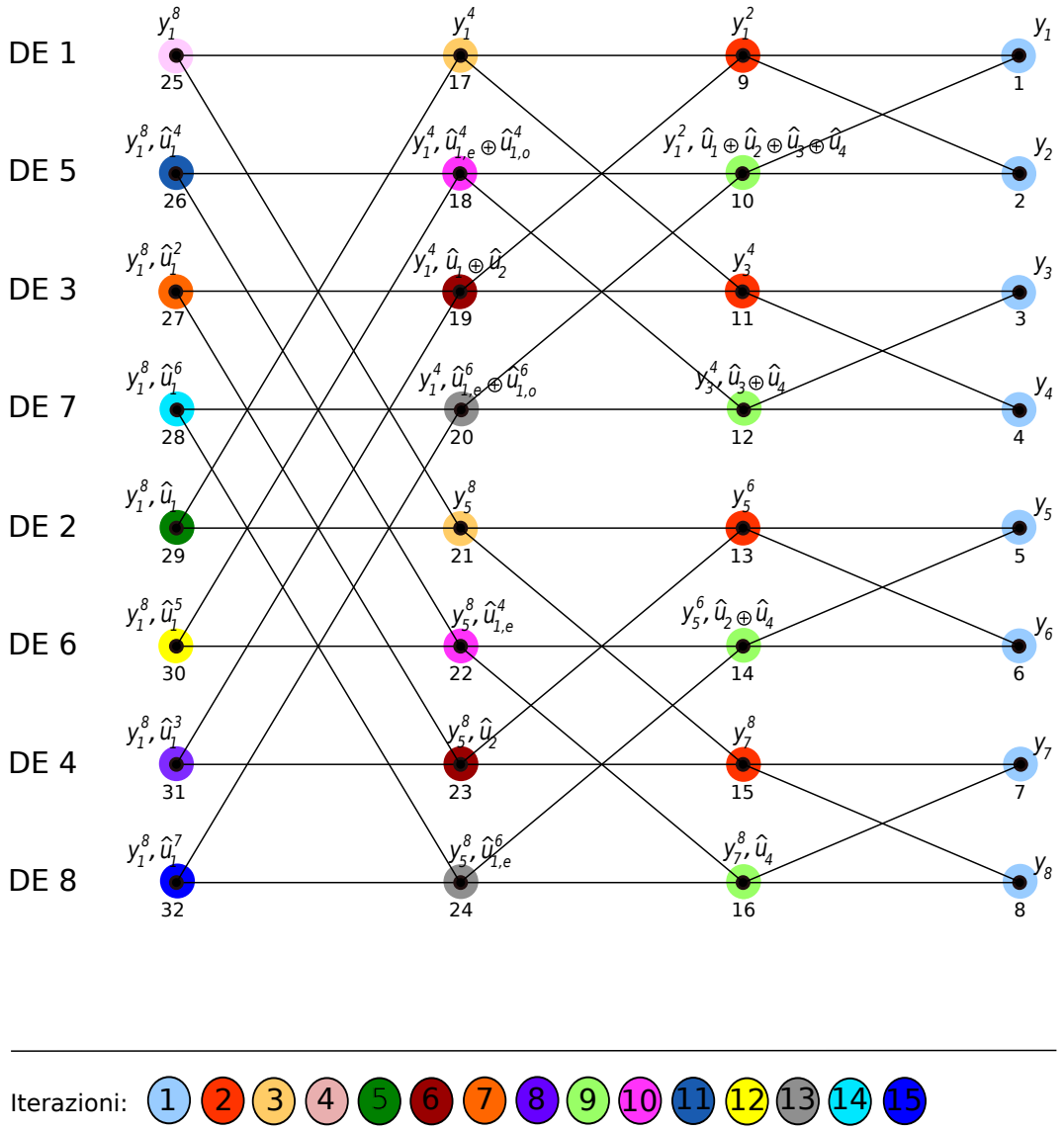

Figura 3.4: Implementazione in parallelo

nodo avvenisse una delle seguenti operazioni:

- $(ab+1)/(a+b)$ se il vettore $\widehat{u}$ di riferimento ha dimensione dispari,
- ab se il vettore $\widehat{u}$ di riferimento ha dimensione pari e ultimo ingresso 0,
- b/a se il vettore $\widehat{u}$ di riferimento ha dimensione pari e ultimo ingresso 1,

dove a e b sono i valori di LR calcolati al passo precedente.

Consideriamo ora le funzioni LLR (log-likelihood ratio), ovvero i logaritmi delle funzioni LR. In ciascun nodo le operazioni diventano:

- $2\tanh^{-1}\left(\tanh\left(\frac{L_a}{2}\right)\tanh\left(\frac{L_b}{2}\right)\right)$ se il vettore $\widehat{u}$ di riferimento ha dimensione dispari,
- $L_b + L_a$ se il vettore $\widehat{u}$ di riferimento ha dimensione pari e ultimo ingresso 0,
- $L_b - L_a$ se il vettore $\widehat{u}$ di riferimento ha dimensione pari e ultimo ingresso 1,

dove L_a e L_b sono i valori di LLR calcolati al passo precedente.

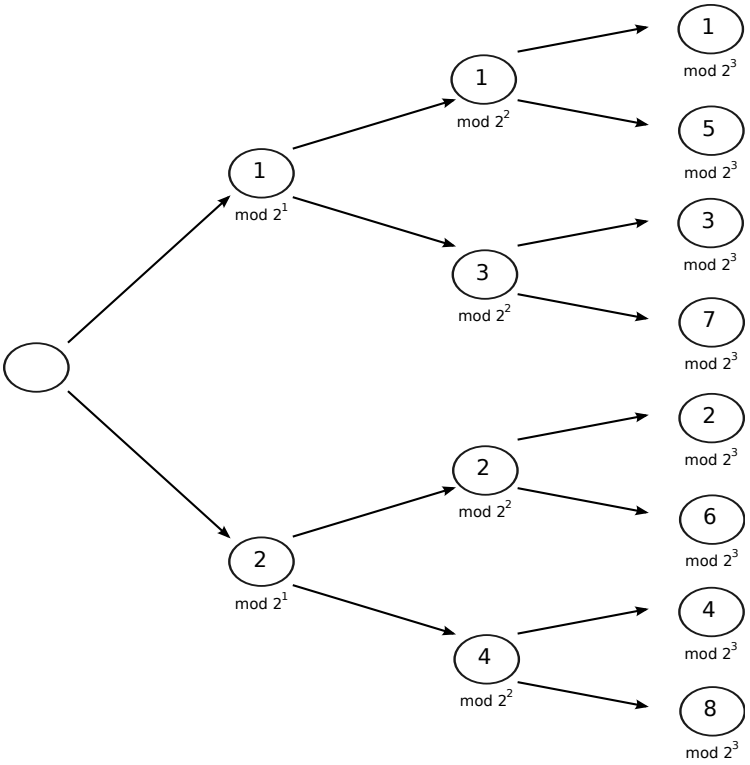

Figura 3.5: Grafo che rappresenta l'ordine di chiamata dei nodi

Caso del canale BEC

Se si usa un canale BEC, la situazione si semplifica notevolmente. In questo caso, infatti, se il valore ricevuto è 0 o 1, si conosce il simbolo inviato:

$$P\{x = 0|y = 0\} = 1,$$
$$P\{x = 1|y = 0\} = 0,$$
$$P\{x = 0|y = 1\} = 0,$$
$$P\{x = 1|y = 1\} = 1.$$

D'altro canto, se il canale ha cancellato il bit trasmesso (e si riceve quindi il simbolo di erasure ϵ):

$$P\{x = 0|y = \epsilon\} = \frac{1}{2},$$
$$P\{x = 1|y = \epsilon\} = \frac{1}{2}.$$

Quindi, per questo canale i parametri LLR sono:

$$LLR(x_i|y_i) = \log \frac{P\{x_i = 0|y_i\}}{P\{x_i = 1|y_i\}} = \begin{cases} \log \frac{0}{1} = -\infty & \text{se } y_i = 1, \\ \log \frac{1}{0} = +\infty & \text{se } y_i = 0, \\ \log \frac{1/2}{1/2} = 0 & \text{se } y_i = \epsilon. \end{cases}$$

Chiaramente, nell'implementare un algoritmo non vorremmo avere a che fare con degli infiniti, quindi stabiliamo per convenzione che

$$-\infty \to -1$$
$$+\infty \to 1$$

e ridefiniamo i valori di LLR nel modo seguente:

$$LLR(x_i|y_i) = \begin{cases} \log \frac{0}{1} = -1 & \text{se } y_i = 1, \\ \log \frac{1}{0} = 1 & \text{se } y_i = 0, \\ \log \frac{1/2}{1/2} = 0 & \text{se } y_i = \epsilon. \end{cases}$$

Se percorriamo come prima lo schema di decodifica, poiché ciascun canale $W_N^{(i)}$ è a sua volta un canale BEC, si trova con facilità il valore di LLR distinguendo tre casi:

- il vettore $\widehat{u}$ di riferimento ha dimensione dispari, LLR = $L_a L_b$;
- il vettore $\widehat{u}$ di riferimento ha dimensione pari e ultimo ingresso 0, allora
  - se $L_a = 1$, per ogni valore di L_b, LLR= 1,
  - se $L_a = 0$, LLR = L_b,
  - se $L_a = -1$ per ogni valore di L_b, LLR= -1,
- il vettore $\widehat{u}$ di riferimento ha dimensione pari e ultimo ingresso 1, allora
  - se $L_a = 1$, per ogni valore di L_b, LLR=-1,
  - se $L_a = 0$, LLR = L_b,
  - se $L_a = -1$ per ogni valore di L_b, LLR= 1,

dove L_a e L_b sono i valori di LLR calcolati al passo precedente.

Complessità computazionale

Osserviamo che, qualora i sottoalberi non abbiano nodi in comune, i calcoli possono avvenire in parallelo.
La seconda osservazione che possiamo fare è che il grafo presenta alcune *farfalle* che legano tra loro 4 nodi a livelli adiacenti tra loro (ad esempio i nodi 9,10,19 e 13 formano una farfalla) e, all'interno della farfalla, i nodi a destra possono essere chiamati in parallelo, quello a sinistra in basso si limita ad assemblare i risultati che ottiene da destra e quello in alto a sinistra assembla i valori sfruttando le formule ricorsive. Questo spiega come si può evitare di ripetere gli stessi calcoli e abbassare la complessità a $O(N \log N)$.

Quest'osservazione, affiancata da quanto visto per la codifica, permette di formulare il seguente teorema.

Teorema 3.14. *Sia W un canale B-DMC. Per ogni rate R, $0 \leq R \leq 1$, le operazioni di codifica e decodifica tramite SC decoder per i polar codes, viste come funzioni della lunghezza del blocco N, hanno entrambe complessità $O(N \log N)$.*

3.3 Errori di blocco

Denotiamo con $P_e(N, R)$ la probabilità di errori di blocco tramite un SC decoder per un polar code con lunghezza di blocco N e rate R, pesata su tutti i codici $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ aventi uguale probabilità per ogni scelta di $u_{\mathcal{A}^c} \in \mathcal{X}^{N-K}$.

Teorema 3.15. *Sia W un canale B-DMC, $P_e(N, R)$ soddisfa per ogni R fissato, $R < I(W)$:*

$$P_e(N, R) = O\left(N^{-\frac{1}{4}}\right).$$

Teorema 3.16. *Sia W un canale B-DMC simmetrico e sia R un rate fissato, $R < C(W)$. Per ogni sequenza di codici $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$ con $N = 2^n$, dove $n \in \mathbb{N}$, $K = [NR]$, $\mathcal{A}$ scelto in modo che i codici siano polar codes e $u_{\mathcal{A}^c}$ qualsiasi, la probabilità di errore di blocco soddisfa*

$$P_e(N, K, \mathcal{A}, u_{\mathcal{A}^c}) = O\left(N^{-\frac{1}{4}}\right).$$

Il Teorema 3.15 può essere migliorato dal seguente risultato.

Teorema 3.17. *Sia W un canale B-DMC con $I(W) > 0$ e siano $R < I(W)$ e $\beta < \frac{1}{2}$ fissati. Allora per ogni $N = 2^n$, $n \geq 0$, la migliore la probabilità di errore di blocco per dei polar codes tramite un SC decoder soddisfa*

$$P_e(N, R) = O\left(2^{-N^{\beta}}\right).$$

Dimostrazione del Teorema 3.15

Per dimostrare il teorema, dobbiamo prima introdurre uno spazio di probabilità $\left(\mathcal{X}^N \times \mathcal{Y}^N, P\right)$ dove

$$P\left(\{\left(u_1^N, y_1^N\right)\}\right) := \frac{1}{2^N} W_N\left(y_1^N \mid u_1^N\right)$$

per ogni $\left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N$. Su questo spazio di probabilità definiamo la quaterna

$$\left(U_1^N, X_1^N, y_1^N, \widehat{U}_1^N\right)$$

di variabili aleatorie tali che per ogni coppia di punti $\left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N$:

- $U_1^N\left(u_1^N, y_1^N\right) = u_1^N$ rappresenta l'input del canale W_N;
- $X_1^N\left(u_1^N, y_1^N\right) = u_1^N G_N$ rappresenta l'input di W^N;
- $y_1^N\left(u_1^N, y_1^N\right) = y_1^N$ rappresenta l'output di W_N e W^N;
- $\widehat{U}_1^N$ rappresenta la decisione del decoder ed è definita ricorsivamente da

$$\widehat{U}_i\left(u_1^N, y_1^N\right) = \begin{cases} u_i & i \in \mathcal{A}^c \\ h_i\left(y_1^N, \widehat{U}_1^{i-1}(u_1^N, y_1^N)\right) & i \in \mathcal{A} \end{cases} .$$

L'evento errore di blocco tramite SC decoder è definito da

$$\mathcal{E} := \left\{\left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N \,\middle|\, \widehat{U}_{\mathcal{A}}\left(u_1^N, y_1^N\right) \neq u_{\mathcal{A}}\right\}$$

e con questa notazione

$$\begin{aligned} P_e(N, K, \mathcal{A}) &:= P\left(\mathcal{E}\right) \\ P_e(N, K, \mathcal{A}, u_{\mathcal{A}^c}) &:= P\left(\mathcal{E} \mid \{U_{\mathcal{A}^c} = u_{\mathcal{A}^c}\}\right) \end{aligned}$$

dove $\{U_{\mathcal{A}^c} = u_{\mathcal{A}^c}\}$ rappresenta l'evento $\left\{\left(\widetilde{u}_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N \,\middle|\, \widetilde{u}_{\mathcal{A}^c} = u_{\mathcal{A}^c}\right\}$.

Possiamo riscrivere $\mathcal{E} = \bigcup_{i \in \mathcal{A}} \mathcal{B}_i$,

$$\mathcal{B}_i := \left\{\left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N \,\middle|\, \widehat{U}_1^{i-1}\left(u_1^N, y_1^N\right) = u_1^{i-1},\ \widehat{U}_i\left(u_1^N, y_1^N\right) \neq u_i\right\}$$

è l'evento che il primo errore dell'SC decoder avvenga all'i-sima posizione. Notiamo che

$$\begin{aligned} \mathcal{B}_i &= \left\{\left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N \mid \widehat{U}_1^{i-1}(u_1^N, y_1^N) = u_1^{i-1},\ h_i\left(y_1^N, \widehat{U}_1^{i-1}(u_1^N, y_1^N)\right) \neq u_i\right\} \\ &= \left\{\left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N \mid \widehat{U}_1^{i-1}(u_1^N, y_1^N) = u_1^{i-1},\ h_i\left(y_1^N, u_1^{i-1}\right) \neq u_i\right\} \\ &\subset \left\{\left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N \mid h_i\left(y_1^N, u_1^{i-1}\right) \neq u_i\right\} \\ &\subset \left\{\left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N \mid W_N^{(i-1)}(y_1^N, u_1^{i-1} | u_i) \leq W_N^{(i-1)}(y_1^N, u_1^{i-1} | u_i \oplus 1)\right\}. \end{aligned}$$

Se chiamiamo

$$\mathcal{E}_i := \left\{ \left(u_1^N, y_1^N\right) \in \mathcal{X}^N \times \mathcal{Y}^N \mid W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i) \leq W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i \oplus 1) \right\},$$

abbiamo $\mathcal{E} \subset \bigcup_{i \in \mathcal{A}} \mathcal{E}_i$ e $P(\mathcal{E}) \leq \sum_{i \in \mathcal{A}} P(\mathcal{E}_i)$.

Consideriamo adesso la funzione indicatrice di $\mathcal{E}_i$, che denotiamo con $1_{\mathcal{E}_i}$.
Osserviamo che:

- se $(u_1^N, y_1^N) \notin \mathcal{E}_i$, allora

$$1_{\mathcal{E}_i}(u_1^N, y_1^N) = 0 \quad \text{e} \quad 0 < \frac{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i \oplus 1)}{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i)} < 1;$$

- se $(u_1^N, y_1^N) \in \mathcal{E}_i$, allora $1_{\mathcal{E}_i}(u_1^N, y_1^N) = 1 \quad \text{e} \quad \frac{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i \oplus 1)}{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i)} \geq 1.$

E quindi si ha la disuguaglianza

$$1_{\mathcal{E}_i}(u_1^N, y_1^N) \leq \sqrt{\frac{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i \oplus 1)}{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i)}}$$

che ci permette di ottenere la seguente limitazione seguente su $P(\mathcal{E}_i)$:

$$\begin{aligned}
P(\mathcal{E}_i) &= \sum_{u_1^N \in \mathcal{X}^N} \sum_{y_1^N \in \mathcal{Y}^N} \frac{1}{2^N} W_N\left(y_1^N \mid u_1^N\right) 1_{\mathcal{E}_i}(u_1^N, y_1^N) \\
&\leq \sum_{u_1^N \in \mathcal{X}^N} \sum_{y_1^N \in \mathcal{Y}^N} \frac{1}{2^N} W_N\left(y_1^N \mid u_1^N\right) \sqrt{\frac{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i \oplus 1)}{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i)}} \\
&= \sum_{u_1^i \in \mathcal{X}^i} \sum_{y_1^N \in \mathcal{Y}^N} \frac{1}{2}\left(y_1^N, u_1^{i-1} \mid u_i\right) \sqrt{\frac{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i \oplus 1)}{W_N^{(i-1)}(y_1^N, u_1^{i-1}|u_i)}} \\
&= Z\left(W_N^{(i)}\right).
\end{aligned}$$

Questo risultato prova la Proposizione 3.10.

Per concludere la dimostrazione, ci basta ricordare che il Teorema 2.5 assicura l'esistenza di una successione di insiemi $\mathcal{A}_N$ con cardinalità $|\mathcal{A}_N| > NR$ tali che $Z\left(W_N^{(i)}\right) = O\left(N^{-\frac{5}{4}}\right)$ e che

$$\sum_{i \in \mathcal{A}_N} Z\left(W_N^{(i)}\right) \leq N \max\left\{ Z\left(W_N^{(i)}\right) \,\middle|\, i \in \mathcal{A}_N \right\} = O\left(N^{-\frac{1}{4}}\right).$$

Dimostrazione del Teorema 3.16

Per dimostrare il teorema mostriamo prima di tutto un risultato di simmetria.

Proposizione 3.18. *Sia W un canale B-DMC simmetrico, gli eventi $\mathcal{E}_i$ hanno la proprietà seguente:*

$$(u_1^N, y_1^N) \in \mathcal{E}_i \iff (a_1^N \oplus u_1^N, a_1^N \cdot y_1^N) \in \mathcal{E}_i$$

per ogni $(u_1^N, y_1^N) \in \mathcal{X}^N \times \mathcal{Y}^N$, $a_1^N \in \mathcal{X}^N$, $1 \leq i \leq N$.

Dimostrazione. Segue direttamente dalla definizione di $\mathcal{E}_i$ e dalle proprietà di simmetria del canale. □

Consideriamo adesso l'evento $\{U_1^N = u_1^N\}$, ovvero la trasmissione di uno specifico vettore $u_{\mathcal{A}}$ e di un vettore congelato $u_{\mathcal{A}^c}$ che insieme formano u_1^N, input del canale W_N.

Corollario 3.19. *Sia W un canale B-DMC simmetrico, per ogni $1 \leq i \leq N$ e per ogni $u_1^N \in \mathcal{X}^N$, gli eventi $\mathcal{E}_i$ e $\{U_1^N = u_1^N\}$ sono indipendenti.*

Dimostrazione. Consideriamo $P\left(\mathcal{E}_i \mid \{U_1^N = u_1^N\}\right) = \sum_{y_1^N \in \mathcal{Y}^N} W_N(y_1^N, u_1^N) 1_{\mathcal{E}_i}\left(u_1^N, y_1^N\right)$.
Per il risultato precedente e poiché $W_N\left(y_1^N \mid u_1^N\right) = W_N\left(a_1^N \cdot y_1^N \mid u_1^N \oplus a_1^N\right)$, prendendo $a_1^N = u_1^N$,

$$\begin{aligned}\sum_{y_1^N \in \mathcal{Y}^N} W_N(y_1^N, u_1^N) 1_{\mathcal{E}_i}\left(u_1^N, y_1^N\right) &= \sum_{y_1^N \in \mathcal{Y}^N} W_N(u_1^N \cdot y_1^N \mid 0_1^N) 1_{\mathcal{E}_i}\left(0_1^N, u_1^N, y_1^N\right) \\ &= P\left(\mathcal{E}_i \mid \{U_1^N = 0_1^N\}\right)\end{aligned}$$

poiché $\{u_1^N \cdot y_1^N \mid y_1^N \in \mathcal{Y}^N\} = \mathcal{Y}^N$. Questo mostra che $P(\mathcal{E}_i) = P\left(\mathcal{E}_i \mid \{U_1^N = u_1^N\}\right)$ e prova il corollario. □

Per ogni $u_1^N \in \mathcal{X}^N$, $P\left(\mathcal{E}_i \mid \{U_1^N = u_1^N\}\right) = P(\mathcal{E}_i) \leq Z\left(W_N^{(i)}\right)$ e, dal momento che $\mathcal{E} \subset \bigcup_{i \in \mathcal{A}} \mathcal{E}_i$,

$$P\left(\mathcal{E} \mid \{U_1^N = u_1^N\}\right) \leq \sum_{i \in \mathcal{A}} P\left(\mathcal{E}_i \mid \{U_1^N = u_1^N\}\right) \leq \sum_{i \in \mathcal{A}} Z\left(W_N^{(i)}\right).$$

Questo implica che, per ogni codice $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$,

$$P_e(N, K, \mathcal{A}, u_{\mathcal{A}^c}) = \sum_{u_{\mathcal{A}} \in \mathcal{X}^K} \frac{1}{2^K} P\left(\mathcal{E} \mid \{U_1^N = u_1^N\}\right) \leq \sum_{i \in \mathcal{A}} Z\left(W_N^{(i)}\right)$$

e la tesi segue dalla stessa argomentazione del Teorema 3.15.

Dimostrazione del Teorema 3.17

Abbiamo già visto che, per ogni canale W, per ogni n e per ogni $\gamma \in [0,1]$, esiste un polar code con lunghezza di blocco $N = 2^n$, il cui rate e la cui probabilità di errore di blocco soddisfano:

$$R \geq P(Z_n \leq \gamma)$$

$$P_e \leq N\gamma.$$

Il Teorema 3.17 segue come corollario dalla prima metà del seguente teorema.

Teorema 3.20. *Sia W un canale B-DMC, per ogni $\beta < \frac{1}{2}$ fissato,*

$$\liminf_{n\to\infty} P\left(Z_n \leq 2^{-N^\beta}\right) = I(W). \tag{3.7}$$

Viceversa, se $I(W) < 1$, per ogni $\beta > \frac{1}{2}$ fissato,

$$\liminf_{n\to\infty} P\left(Z_n \geq 2^{-N^\beta}\right) = 1. \tag{3.8}$$

Per dimostrare il Teorema 3.20 riformuliamo il problema in termini più generali. Sia $(\Omega, \mathcal{F}, P)$ lo spazio di probabilità, $\{B_n \mid n \geq 1\}$ la successione di variabili aleatorie indipendenti e identicamente distribuite con

$$P(B_i = 0) = P(B_i = 1) = \frac{1}{2}$$

e per ogni $n \geq 1$ $\mathcal{F}_n$ la σ-algebra generata da $(B_1, \ldots, B_n)$, $\mathcal{F} = \bigcup_{n=1}^{\infty} \mathcal{F}_n$.

Definizione 3.21. Per ogni $z_0 \in (0,1)$, definiamo $\mathcal{Z}_{z_0}$ come la classe dei processi stocastici $\{Z_n \mid n \geq 0\}$ tali che per $n \geq 1$:

- $Z_0 = z_0$;
- Z_n è misurabile rispetto a $\mathcal{F}_n$;
- $Z_n = Z_{n-1}^2$ se $B_n = 1$;
- $Z_{n-1} \leq Z_n \leq 2Z_{n-1} - Z_{n-1}^2$ se $B_n = 0$.

Definiamo $\mathcal{Z} = \bigcup_{z_0 \in (0,1)} \mathcal{Z}_{z_0}$.

Osservazione 3.22. I processi Z_n definiti in (2.17) appartengono alla classe $\mathcal{Z}$.

Osservazione 3.23. La proprietà dei processi definiti in (2.17) valgono anche in questo contesto più ampio, ovvero per ogni $\{Z_n\} \in \mathcal{Z}$:

(i) $Z_n \in (0,1)$ per ogni $n \geq 0$;

(ii) $\{(Z_n, \mathcal{F}_n)\}$ è una supermartingala limitata;

(iii) $\{Z_n\}$ converge q.o. ad una variabile aleatoria Z_∞ che assume q.o valori 0 o 1.

Per dimostrare il Teorema 3.20, dimostriamo il seguente risultato equivalente.

Teorema 3.24. *Per ogni $\{Z_n\} \in \mathcal{Z}$ e per ogni $\beta < \frac{1}{2}$,*

$$\liminf_{n\to\infty} P\left(Z_n \leq 2^{-2^{\beta n}}\right) \geq P\left(Z_\infty = 0\right). \tag{3.9}$$

Viceversa, per ogni $\beta > \frac{1}{2}$,

$$\liminf_{n\to\infty} P\left(Z_n \geq 2^{-2^{\beta n}}\right) = 1. \tag{3.10}$$

Dimostrazione. Iniziamo col dimostrare (3.10). Sia $\delta_n(\beta) := 2^{-2^{\beta n}}$ e $\{\widetilde{Z}_i\}$ il processo stocastico definito da:

$$\widetilde{Z} = Z_0 \quad \text{e} \quad \widetilde{Z}_{i+1} = \begin{cases} \widetilde{Z}_i^2 & \text{se } B_{i+1} = 1 \\ \widetilde{Z}_i & \text{se } B_{i+1} = 0 \end{cases}.$$

Il processo $\{\widetilde{Z}_i\}$ è dominato da $\{Z_i\}$ e quindi

$$P\left(Z_n \geq \delta_n\right) \geq P\left(\widetilde{Z}_n \geq \delta_n\right).$$

Osserviamo che, se poniamo $L = \sum_{i=1}^{n} B_i$, possiamo scrivere $\widetilde{Z}_n = Z_0^{(2^L)}$. Allora,

$$P\left(Z_n \geq \delta_n\right) = P\left(L + \log_2 \log_2 \frac{1}{Z_0} \leq n\beta\right)$$

che tende a 1 per n che tende all'infinito e questo prova (3.10).

Dimostriamo (3.9). Cominciamo col dare alcune definizioni.

Definizione 3.25. Sia $\{Z_n\} \in \mathcal{Z}$ e $\{f_n\} \in [0,1]$ una successione di reali che converge a 0, $\{f_n\}$ è asintoticamente dominante (a.d.) per $\{Z_n\}$ e scriviamo $Z_n \prec f_n$ se

$$\liminf_{n\to\infty} P(Z_n \leq f_n) \geq P(Z_\infty = 0).$$

La successione $\{f_n\}$ è universalmente dominante (u.d.) se, per ogni $k \geq 0$, $\{f_{n+k}\}$ è asintoticamente dominante (a.d.) per $\{Z_n\}$.

Definizione 3.26. Un processo stocastico $\{Z_n\} \in \mathcal{Z}$ è detto estremale se

$$Z_{n+1} = \begin{cases} Z_n^2 & \text{se } B_{n+1} = 0, \\ 2Z_n - Z_n^2 & \text{se } B_{n+1} = 1. \end{cases} \tag{3.11}$$

Il processo estremale in $\mathcal{Z}_{z_0}$ sarà denotato con $\{Z_n^{(z_0)}\}$.

Osserviamo che i processi estremali verificano

$$Z_{n+1} = Z_n^2 \quad \text{se } B_{n+1} = 1,$$

$$(1 - Z_{n+1}) = (1 - Z_n)^2 \quad \text{se } B_{n+1} = 0.$$

Dall'Osservazione 3.23 derivano alcune proprietà dei processi estremali. Sia $\{Z_n\}$ un tale processo, allora:

(i) $\{Z_n\}$ è un processo di Markov;

(ii) $\{Z_n\}$ è una martingala limitata;

(iii) $P(Z_\infty = 0) = 1 - Z_0, \quad P(Z_\infty = 1) = Z_0.$

Il termine *estremale* è giustificato dal fatto che:

(i) un qualunque processo $\{Z_n\} \in \mathcal{Z}_{z_0}$ è dominato da $\left\{Z_n^{(z_0)}\right\}$, ovvero $Z_n \leq Z_n^{(z_0)}$;

(ii) il processo estremale $\left\{Z_n^{(\alpha)}\right\}$ è dominato da $\left\{Z_n^{(\beta)}\right\}$ per ogni $0 < \alpha \leq \beta < 1$.

Dimostreremo (3.9) in tre passi:

1. mostriamo che una successione è a.d. per la classe $\mathcal{Z}$ se è u.d. per la sottoclasse dei processi estremali;

2. dimostriamo che $\{\rho^n\}$, con $\rho \in (3/4, 1)$, è a.d. per ogni processo estremale;

3. usiamo il risultato precedente per dimostrare che, per ogni $\beta < 1/2$ fissato, la successione $\left\{2^{-2^{n\beta}}\right\}$ è u.d. per i processi estremali.

Dimostrazione di 1.

Proposizione 3.27. *Se $\{f_n\}$ è una successione u.d. per la classe di processi estremali in $\mathcal{Z}$, allora $\{f_n\}$ è a.d. per la classe $\mathcal{Z}$.*

Dimostrazione. Sia $\{Z_n\} \in \mathcal{Z}$ e sia $\{f_n\}$ una sequenza u.d. per la classe dei processi estremali. Per ogni $k \geq 0$, $n \geq 0$ e $\delta \in (0, 1)$ si ha

$$P(Z_{n+k} \leq f_{n+k}) \geq P(Z_{n+k} \leq f_{n+k} \mid Z_k \leq \delta) P(Z_k \leq \delta).$$

Questo, insieme al fatto che

$$P(Z_{n+k} \leq f_{n+k} \mid Z_k \leq \delta) \geq P(Z_n^\delta \leq f_{n+k}) \quad \text{e}$$

$$\liminf_{n\to\infty} P(Z_n^\delta \leq f_{n+k}) \geq (1 - \delta)$$

ci dice che per ogni $k \geq 0$,

$$\begin{aligned} \liminf_{n\to\infty} P(Z_n \leq f_n) &= \liminf_{n\to\infty} P(Z_{n+k} \leq f_{n+k}) \\ &\geq (1 - \delta) P(Z_k \leq \delta). \end{aligned}$$

Poiché è vero per ogni scelta di k, otteniamo

$$\begin{aligned} \liminf_{n\to\infty} P(Z_n \le f_n) &\ge (1-\delta)\liminf_{k\to\infty} P(Z_k \le \delta) \\ &\ge (1-\delta)P(\liminf_{k\to\infty} Z_k \le \delta) && \text{per il Lemma di Fatou} \\ &= (1-\delta)P(Z_\infty = 0) && \text{perchè } \{Z_k\} \to Z_\infty \end{aligned}$$

e, facendo tendere δ a 0^+, si ha

$$\liminf_{n\to\infty} P(Z_n \le f_n) \ge P(Z_\infty = 0)$$

che conclude la dimostrazione. □

Dimostrazione di 2.

Proposizione 3.28. *Per ogni $\rho \in (3/4, 1)$, la successione $\{\rho^n\}$ è a.d. per la classe dei processi estremali.*

Dimostrazione. Sia $\{Z_n\}$ un processo estremale in $\mathcal{Z}$ con $Z_0 = z_0$, $z_0 \in (0,1)$ e definiamo $Q_n := Z_n(1-Z_n)$. Allora Q_n è in $(0, 1/4]$ e

$$Q_{n+1} = \begin{cases} Z_n^2(1-Z_n^2) & \text{se } B_{n+1} = 1 \\ (2Z_n - Z_n^2)(1-2Z_n+Z_n^2) & \text{se } B_{n+1} = 0 \end{cases}$$

o, equivalentemente,

$$Q_{n+1} = Q_n \cdot \begin{cases} Z_n(1+Z_n) & \text{se } B_{n+1} = 1 \\ (1-Z_n)(2-Z_n) & \text{se } B_{n+1} = 0 \end{cases} . \tag{3.12}$$

Lemma 3.29. *Sia $\{Q_n\}$ definito come sopra, $E\left[Q_n^{1/2}\right] \le \frac{1}{2}\left(\frac{3}{4}\right)^{n/2}$.*

Dimostrazione. Osserviamo che $\sqrt{z(1+z)} + \sqrt{(1-z)(2-z)} \le \sqrt{3}$ per $z \in [0,1]$. Allora, per (3.12),

$$E\left[Q_{n+1}^2 \mid Q_n\right] \le Q_n^{1/2}\left(\frac{3}{4}\right)^{1/2}.$$

Quindi

$$E\left[Q_n^{1/2}\right] \le E\left[Q_0^{1/2}\right]\left(\frac{3}{4}\right)^{n/2} \le \frac{1}{2}\left(\frac{3}{4}\right)^{n/2}.$$

□

Corollario 3.30. $P\left(Q_n \ge \rho^n\right) \le \frac{1}{2}\left(\frac{3}{4\rho}\right)^{n/2}$ *per ogni $\rho > 0$.*

Dimostrazione. Per la disuguaglianza di Markov, sia X una variabile aleatoria non negativa,

$$P(X > \alpha) \le \frac{E[X]}{\alpha}.$$

Il risultato segue immediatamente dal Lemma 3.29. □

Adesso ci serviamo di un lemma che trasforma la limitazione appena trovata in una limitazione su Z_n.

Lemma 3.31. *Sia $f_n : \mathbb{R} \to \mathbb{R}$ la funzione definita da:*

$$f_n(\rho) := \begin{cases} \frac{1-\sqrt{1-4\rho^n}}{2} & \text{se } 1-4\rho^n > 0 \\ 1 & \text{altrimenti} \end{cases}$$

allora $Z_n \prec f_n(\rho)$ per ogni $\rho \in (3/4, 1)$.

Dimostrazione. Sia $\rho \in (3/4, 1)$; per n abbastanza grande tale che $1 - 4\rho^n > 0$, possiamo scomporre $\{Q_n \leq \rho^n\}$ in due insiemi disgiunti,

$$\{Q_n \leq \rho^n\} = \{Z_n \leq f_n(\rho)\} \cup \{Z_n \geq 1 - f_n(\rho)\}$$

e quindi

$$P\left(Q_n \leq \rho^n\right) = P\left(Z_n \leq f_n(\rho)\right) + P\left(Z_n \geq 1 - f_n(\rho)\right)$$

che implica

$$\liminf_{n\to\infty} P\left(Q_n \leq \rho^n\right) = \liminf_{n\to\infty} P\left(Z_n \leq f_n(\rho)\right) + \liminf_{n\to\infty} P\left(Z_n \geq 1 - f_n(\rho)\right).$$

Dal momento che $\rho \geq 3/4$, per il Corollario 3.30

$$\liminf_{n\to\infty} P(Q_n \leq \rho^n) = 1.$$

Poiché la successione di funzioni $\{f_k\}$ è monotona decrescente,

$$\liminf_{n\to\infty} P\left(Z_n \geq 1 - f_n(\rho)\right) \leq \liminf_{n\to\infty} P\left(Z_n \geq 1 - f_k(\rho)\right)$$

per ogni $k \geq 1$. Ma $\liminf_{n\to\infty} P\left(Z_n \geq 1 - f_k(\rho)\right) = z_0$, quindi

$$\liminf_{n\to\infty} P\left(Z_n \leq f_n(\rho)\right) \geq 1 - z_0$$

e $Z_n \prec f_n(\rho)$ come volevamo.

□

Per concludere la dimostrazione della Proposizione 3.28 ci basta dimostrare che per ogni $\rho \in (3/4, 1)$, esiste $\widetilde{\rho} \in (3/4, 1)$ tale che $f_n(\widetilde{\rho}) \leq \rho^n$ per n sufficientemente grande, ma è immediato vedere che questo vale per ogni $\widetilde{\rho} \in (\rho, 1)$.

□

Dimostrazione di 3.

Proposizione 3.32. *Per ogni $\beta < 1/2$, la successione $\left\{2^{-2^{n\beta}}\right\}$ è u.d. per la classe dei processi estremali.*

Dimostrazione. Sia $\beta < 1/2$ fissato. Osserviamo che, per ogni $k > 0$ fissato, $2^{-2^{(n+k)\beta}}$ si comporta asintoticamente come $2^{-2^{n\beta}}$, quindi ci basta dimostrare che $\left\{2^{-2^{n\beta}}\right\}$ è una successione asintoticamente dominante.
Sia $\{Z_n\}$ un processo estremale, vorremmo provare che $Z_n \prec 2^{-2^{n\beta}}$.
Sia $\left\{\widetilde{Z}_i\right\}$ definito scegliendo $n \geq 1$ e $m \in \{0, \dots, n\}$ e ponendo

$$\widetilde{Z}_i = Z_i, \quad i = 0, \dots, m, \qquad \widetilde{Z}_{i+1} = \begin{cases} \widetilde{Z}_i^2 & \text{se } B_{i+1} = 1 \\ 2\widetilde{Z}_i & \text{se } B_{i+1} = 0 \end{cases}, \quad i \geq m.$$

Segue dalla definizione di processo estremale che $Z_i < \widetilde{Z}_i$ per ogni $i \geq 1$.
Sia $a_n = \sqrt{n}$ fissato e suddividiamo l'insieme $\{m, \dots, n-1\}$ in $k = (n-m)/a_n$ intervalli consecutivi $J_1, \dots, J_k$ di dimensione a_n:

$$J_j = \{m + (j-1)a_n, \dots, m + ja_n - 1\}.$$

Chiamiamo E_j l'evento $\sum_{i \in J_j} B_i < a_n\beta$. Osserviamo che

$$P(E_j) \leq 2^{-a_n(1-H(\beta))}$$

dove $H(\beta) = -\beta \log_2(\beta) - (1-\beta)\log_2(1-\beta)$ é la funzione di entropia binaria.

L'evento $G := \bigcap_j E_j^C$ ha probabilità maggiore o uguale di $1 - k2^{-a_n(1-H(\beta))}$.
Supponendo che si verifichi l'evento G, su ogni intervallo J_j il valore di $\widetilde{Z}$ appare al quadrato almeno $a_n\beta$ volte e raddoppiato almeno $a_n(1-\beta)$ volte, quindi

$$\log_2 \widetilde{Z}_{m+(j+1)a_n} \leq 2^{a_n\beta}\left(\log_2 \widetilde{Z}_{m+ja_n} + a_n(1-\beta)\right)$$

e dunque

$$\begin{aligned} \log_2 Z_n &\leq \log_2 \widetilde{Z}_n \\ &\leq 2^{(n-m)\beta} \log_2 Z_m + a_n(1-\beta) \sum_{j=1}^{k} 2^{ja_n\beta} \\ &\leq 2^{(n-m)\beta} \log_2 Z_m + a_n(1-\beta) 2^{(n-m)\beta} \left(1 - 2^{-a_n\beta}\right)^{-1} \\ &\leq 2^{(n-m)\beta} \left(\log_2 Z_m + a_n\right) \quad \text{per } n \text{ abbastanza grande.} \end{aligned}$$

Ora consideriamo

$$m = n^{3/4}, \quad \rho = 7/8 \quad \text{e} \quad \widetilde{G} = \left\{ Z_m \leq \left(\frac{7}{8}\right)^m \right\} \cap G.$$

Per n abbastanza grande, se si verifica l'evento $\widetilde{G}$, abbiamo

$$\log_2 Z_m \leq -n^{3/4} \log_2(8/7)$$

e dunque

$$\log_2 Z_n \leq 2^{(n-m)\beta} \left(-n^{3/4} \log_2(8/7) + n^{1/2} \right) \leq -2^{n\beta} o(1).$$

Poiché la probabilitá che si verifichi l'evento G tende a 1, per il Lemma 3.31 la probabilitá che si verifichi $\widetilde{G}$ tende a $1 - z_0$ e questo mostra che $Z_n \prec 2^{-2^{\beta n}}$ per ogni $\beta < 1/2$ fissato.

□

Abbiamo dimostrato i tre passi, qundi abbiamo dimostrato il teorema. □

3.4 Costruzione di Polar Codes dai codici RM

I codici di Reed-Muller (RM) sono una classe di codici a correzione d'errore lineari e si costruiscono come segue.
Sia $\mathbb{F}_{2^m}$ un campo finito, denotiamo con $n = 2^m$ e consideriamo il prodotto wedge in $\mathbb{F}_{2^m}$

$$w \wedge z = (w_1 \cdot z_1, \ldots, w_n \cdot z_n)$$

dove $'\cdot'$ è l'usuale prodotto in $\mathbb{F}_2$. Definiamo i vettori di lunghezza n:

- $v_0 = (1, \ldots, 1)$;
- $v_i = 1_{H_i}$, dove gli H_i sono gli iperpiani $H_i = \{y \in \mathbb{F}_{2^m} \mid y_i = 0\}$.

Il codice di Reed-Muller $RM(r, m)$ di ordine r e lunghezza $n = 2^m$ è il codice generato da tutti i prodotti wedge dei $v_0, \ldots, v_m$:

$$v_0, v_1, \ldots, v_d, \ldots, (v_i \wedge v_j), \ldots, (v_i \wedge v_j \ldots \wedge v_m).$$

Osservazione 3.33. I vettori $v_0, v_1, \ldots, v_d, \ldots, (v_i \wedge v_j), \ldots, (v_i \wedge v_j \ldots \wedge v_m)$ sono le righe della matrice generatrice del codice $RM(r, m)$.

Osservazione 3.34. La minima distanza del codice $RM(r, m)$ è $d = 2^{m-r}$.

Esempio 3.35. Il codice $RM(2, 3)$ è generato dai vettori

$$\{v_0, v_1, v_2, v_3, v_1 \wedge v_2, v_1 \wedge v_3, v_2 \wedge v_3\}$$

e la matrice generatrice è

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Costruzione di Plotkin per i codici RM

La *costruzione di Plotkin* è un metodo per concatenare due codici di lunghezza n e ottenere un nuovo codice di lunghezza $2n$.
Siano $C_u(n, k_u, d_u)$ e $C_v(n, k_v, d_v)$ due codici binari, il nuovo codice è

$$C := \{u, u \oplus v \mid u \in C_u,\ v \in C_v\},$$

dove $'\oplus'$ è la sommma modulo 2 componente per componente.
Il codice C ha lunghezza $2n$, il numero di bit d'informazione è $k_u + k_v$ e la distanza minima è $d = \min\{2d_u, d_v\}$, quindi abbiamo costruito un codice

$$C(2n, k_u + k_v, d).$$

La matrice generatrice del codice è

$$G = \begin{pmatrix} G_u & G_u \\ 0 & G_v \end{pmatrix}.$$

Osservazione 3.36. La decodifica di un codice creato attraverso la costruzione di Plotkin può essere effettuata combinando la decodifica sulle componenti.

Possiamo usare questo metodo per costruire codici RM di dimensione sempre maggiore. Siano

$$C_u = R(r + 1, m),$$

$$C_v = R(r, m)$$

con $n_u = n_v = 2^m$, con la costruzione di Plotkin costruiamo un codice

$$C = \{u, u \oplus v \mid u \in C_u = R(r + 1.m),\ v \in R(r, m)\}$$

di lunghezza $n = n_u + n_v = 2n_u = 2^{m+1}$, dimensione

$$k = k_u + k_v = \sum_{i=0}^{r+1} \binom{m}{i} + \sum_{i=0}^{r} \binom{m}{i} = \sum_{i=0}^{r+1} \binom{m+1}{i}$$

e distanza minima $d = \min\{2d_u, d_v\} = \min\{2 \cdot 2^{m-(r+1)}, 2^{m-r}\} = 2^{m-r}$.

Iterando questa costruzione possiamo costruire qualunque codice $R(r, m)$ a partire da codici RM di ordine $r = 0$, equivalenti a codici a ripetizione (codici in cui un unico bit viene trasmesso un numero dispari di volte e il ricevente sceglie il bit ricevuto con più frequenza), e codici RM di ordine $r = m - 1$, equivalenti a parity check codes. La costruzione ricorsiva è illustrata in Figura 3.6.

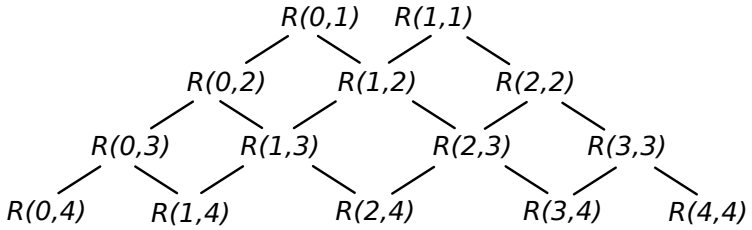

Figura 3.6: Struttura dei codici di Reed-Muller

Denotiamo con $G_{RM}(n, n)$ la matrice generatrice di un codice $RM(n, n)$ di ordine n e dimensione di blocco $N = 2^n$. Se usiamo la costruzione di Plotkin, si dimostra che

$$G_{RM}(n, n) = F^{\otimes n}$$

dove $F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, l'$n$-sima potenza di Kronecker di F.

Il codice $RM(r, n)$ può essere definito come il codice lineare di matrice generatrice $G_{RM}(r, n)$, ottenuta considerando le righe di $G_{RM}(n, n)$ aventi peso di Hamming maggiore o uguale di 2^{n-r}.

Esempio 3.37. La matrice generatrice del codice $RM(3, 3)$ è

$$G_{RM}(3,3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

e il codice $RM(1,3)$ è il codice con matrice generatrice

$$G_{RM}(1,3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Per ogni $N = 2^n$, $n \geq 1$ e $1 < K < N$, un (N, K) polar code è un codice a blocchi la cui matrice generatrice, che in questo contesto denotiamo con $G_P(N, K)$, è una sottomatrice di $F^{\otimes n}$ di dimensione $K \times N$ costruita nel modo seguente:

- definiamo ricorsivamente il vettore $z_N = (z_{N,1}, \ldots, z_{N,N})$ dove

$$z_{2k,j} = \begin{cases} 2z_{k,j} - z_{k,j}^2 & \text{per } 1 \leq j \leq k \\ z_{k,j-k}^2 & \text{per } k+1 \leq j \leq 2k \end{cases}$$

  per $k = 1, 2, 2^2 \ldots, 2^{n-1}$ e $z_{1,1} = 1/2$;

- consideriamo la permutazione $\pi_N = (i_1, \ldots, i_N)$ di $(1, \ldots, N)$ tale che per ogni $1 \leq j < k \leq N$ valga la disuguaglianza $z_{N,i_j} \leq z_{N,i_k}$;

- la matrice $G_P(N, K)$ è la sottomatrice di $F^{\otimes n}$ ottenuta considerando le righe di $F^{\otimes n}$ di indici $i_1, \ldots, i_K$.

Esempio 3.38. Nel caso $n = 3$:

- $z_8 = (0.096, 0.684, 0.809, 0.121, 0.879, 0.191, 0.316, 0.004)$;
- $\pi_8 = (8, 4, 6, 7, 2, 3, 5, 1)$;
- il polar code $(8, 5)$ ha matrice generatrice

$$G_P(8,5) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Lemma 3.39 ([14]). *Un codice $RM(n, r)$ è un polar code di lunghezza 2^n con*

$$\mathcal{A}^c = \{i \mid wt(i) < r\},$$

dove $wt(i)$ è il numero di 1 nell'espansione binaria di i, ovvero il peso di Hamming di i.

Questo metodo, che consiste nel scegliere l'insieme d'informazione $\mathcal{A}$ in base al peso di Hamming, si chiama *RM rule*.

Il seguente lemma caratterizza la distanza minima di un polar code.

Lemma 3.40. *Sia $\mathcal{A}$ l'insieme d'informazione di un polar code C, la distanza minima del codice è*

$$d(C) = \min_{i \in \mathcal{A}} 2^{wt(i)}.$$

Dimostrazione. Poniamo $w_{\min} := \min_{i \in \mathcal{A}} wt(i)$. Dal momento che d non può essere più grande del minimo peso di Hamming delle righe della matrice generatrice, $d \leq 2^{w_{\min}}$.
D'altro canto, poiché aggiungere righe alla matrice generatrice non aumenta la distanza minima, possiamo aggiungere le righe di $F^{\otimes n}$ con peso di Hamming almeno $2^{w_{\min}}$. Il codice risultante è un codice $RM(nn - w_{\min})$ e la distanza minima di un codice $RM(n,r)$ è $d\left(RM(n,r)\right) = 2^{n-r}$, quindi $d \geq d\left(RM(nn - w_{\min})\right) = 2^{w_{\min}}$. □

3.5 Simulazioni

Abbiamo scritto un programma in matlab che simula la *bit error rate* (BER) dei Polar Codes, ovvero il rapporto tra i bit non decodificati correttamente e il numero di bit totali inviati.

Gli algoritmi di codifica e decodifica impiegati sono quelli descritti nei paragrafi precedenti. La Figura 3.7 rappresenta il rapporto tra la probabilità di erasure di un canale BEC (in ascissa) e la BER (in ordinata). Abbiamo scelto $N = 2^{10}$ e rate $R = 1/2$. Osserviamo che, quando la probabilità di erasure è circa $\frac{1}{10}$, la BER è inferiore a $\frac{1}{1000}$, quindi abbiamo ottenuto un significativo miglioramento.

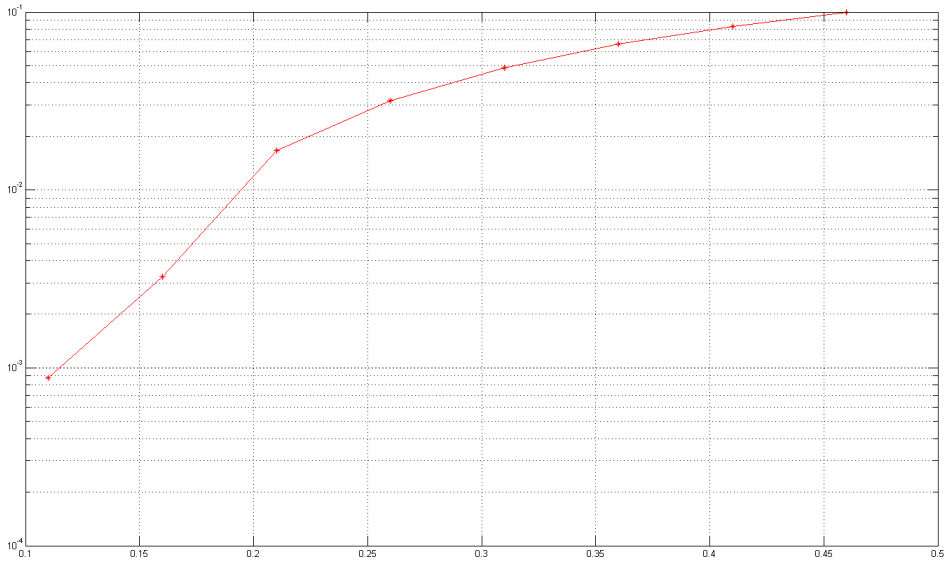

Figura 3.7: Polar Codes con canale BEC

4 Polarizzazione come fenomeno più generale

La polarizzazione dei canali è un metodo introdotto in [3] per canali binari, discreti e privi di memoria. In questo capitolo abbiamo studiato due generalizzazioni del metodo: la polarizzazione nel caso in cui l'alfabeto di input non sia binario e la polarizzazione in caso di canale B-DMC e matrice generatrice qualunque.

4.1 Alfabeto di input arbitrario

Sia $W : \mathcal{X} \to \mathcal{Y}$ un canale DMC, la polarizzazione avviene iterando il processo $W \mapsto (W^-, W^+)$ ottenendo i canali $W^{-\cdots-}, \ldots, W^{+\cdots+}$ come definiti nell'Osservazione 2.8 e questi canali polarizzano nel senso del risultato seguente.

Proposizione 4.1. *Per ogni $\delta > 0$,*

$$\lim_{n\to\infty} \frac{\#\{s \in \{+,-\}^n \mid I(W^s) \in (\delta, 1-\delta)\}}{2^n} = 0.$$

Per dimostrare la Proposizione 4.1 nel caso l'alfabeto di input non sia binario, ma bensì

$$\mathcal{X} = \{0, 1, \ldots, q-1\}, \quad q \geq 2,$$

ci serviamo di un lemma.

Lemma 4.2. *Sia $\{B_i \mid i \geq 1\}$ una sequenza di variabili aleatorie indipendenti e identicamente distribuite (i.i.d.) a valori in $\{+,-\}$ con*

$$P(B_i = +) = P(B_i = -) = \frac{1}{2}$$

e definite sullo spazio di probabilità $(\Omega, \mathcal{F}, P)$.
Sia $\mathcal{F}_0$ la σ-algebra banale e definiamo $\mathcal{F}_n$, $n \geq 1$, la σ-algebra generata da $(B_1, \ldots, B_n)$.
Supponiamo di avere due processi stocastici $\{I_n \mid n \geq 0\}$ e $\{T_n \mid n \geq 0\}$, definiti sullo stesso spazio di probabilità, con le seguenti proprietà:

(i) I_n *è a valori in* $[0,1]$ *ed è misurabile rispetto a* $\mathcal{F}_n$*, ovvero* I_0 *è costante e* I_n *è una funzione di* $B_1, \dots, B_n$*;*

(ii) $\{(I_n, \mathcal{F}_n) \mid n \geq 0\}$ *è una martingala;*

(iii) T_n *è a valori in* $[0,1]$ *ed è misurabile rispetto a* $\mathcal{F}_n$*;*

(iv) $T_{n+1} = T_n^2$ *se* $B_{n+1} = +$*;*

(v) $\forall \epsilon > 0\ \exists \delta > 0$ *tale che* $I_n \in (\epsilon, 1-\epsilon)$ *implica* $T_n \in (\delta, 1-\delta)$.

Allora $I_\infty := \lim_{n\to\infty} I_n$ *esiste con probabilità 1,* I_∞ *è a valori in* $\{0,1\}$ *e* $P(I_\infty = 1) = I_0$.

Dimostrazione. La convergenza quasi ovunque di I_n segue dal fatto che $\{I_n\}$ è una martingala limitata. Se supponiamo di aver dimostrato che I_∞ è a valori in $\{0,1\}$, segue dalle proprietà di martingala che

$$P(I_\infty = 1) = E[I_\infty] = I_0.$$

Ci rimane da provare che I_∞ è a valori in $\{0,1\}$. Questo è equivalente a dire che, per ogni $\eta > 0$,

$$P(I_\infty \in (\eta, 1-\eta)) = 0.$$

Per ogni $0 < \epsilon < \eta$, l'evento $\{I_\infty \in (\eta, 1-\eta)\}$ è incluso nell'evento

$$J_\epsilon = \{\omega \mid \exists m \text{ tale che } \forall n \geq m,\ I_n \in (\epsilon, 1-\epsilon)\}$$

detto poi

$$K_\delta = \{\omega \mid \exists m \text{ tale che } \forall n \geq m,\ T_n \in (\delta, 1-\delta)\},$$

per la proprietà (v) esiste $\delta > 0$ tale che $J_\epsilon \subset K_\delta$, quindi ci basta dimostrare che $P(K_\delta) = 0$ per ogni $\delta > 0$.
Se $\delta \geq 1/2$ ciò è banalmente vero, quindi dobbiamo dimostrarlo per $0 < \delta < 1/2$.
Sia quindi $0 < \delta < 1/2$, consideriamo un intero positivo k tale che $(1-\delta)^{2^k} < \delta$.
Sia $n \geq 1$, definiamo E_n l'evento tale che $B_n = B_{n+1} = \ldots = B_{n+k-1} = +$, allora $P(E_n) \geq 2^{-k}$ e $\{E_{mk} \mid m \geq 1\}$ è un insieme di eventi indipendenti tra loro. Per il Lemma di Borel-Cantelli, l'evento

$$\begin{aligned} E &= \{E_n \text{ ha infinite occorrenze }\} \\ &= \{\omega \mid \forall m \quad \exists n \geq m \text{ tale che } \omega \in E_n\} \end{aligned}$$

ha probabilità 1 e quindi $P(K_\delta) = P(E \cap K_\delta)$.
Sia adesso $\omega \in E \cap K_\delta$. Poiché $\omega \in K_\delta$, esite m tale che $T_n(\omega) \in (\delta, 1-\delta)$ per ogni n maggiore o uguale ad m. Ma ω appartiente a E, quindi esiste $n_0 \geq m$ tale che $B_{n_0+1} = \ldots = B_{n_0+k-1} = +$ e dunque $T_{n_0+k}(\omega) = T_{n_0}(\omega)^{2^k} \leq (1-\delta)^{2^k} < \delta$, in contraddizione col fatto che $T_{n_0+k}(\omega) \in (\delta, 1-\delta)$. Quindi l'intersezione $E \cap K_\delta$ è vuota e $P(K_\delta) = 0$. □

Enunciamo con queste notazioni un lemma, la cui dimostrazione è sostanzialmente la stessa del Teorema 3.20.

Lemma 4.3. *Siano $\{B_n\}$, $\{I_n\}$ e $\{T_n\}$ processi che verificano le condizioni (i)-(v) del risultato precedente. Supponiamo anche che:*

(i) esista una costante k tale che $T_{n+1} \leq kT_n$ se $B_{n+1} = -$;

(ii) per ogni $\epsilon > 0$ esista $\delta > 0$ tale che $I_n > 1 - \delta$ implichi $T_n < \epsilon$.

Allora, per ogni $0 < \beta < 1/2$,

$$\lim_{n\to\infty} P\left(T_n \leq 2^{-2^{\beta n}}\right) = I_0.$$

Caso generale: q arbitrario

Sia q la cardinalità dell'alfabeto di input $\mathcal{X}$, definiamo

$$I(W) := \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \frac{1}{q} W(y \mid x) \log \frac{W(y \mid x)}{\sum_{x'\in\mathcal{X}} \frac{1}{q} W(y \mid x')}$$

dove il logaritmo è inteso in base q in modo che $I(W)$ sia compreso tra 0 e 1.
Per ogni coppia $x, x' \in \mathcal{X}$, definiamo la distanza di Bhattacharya tra x e x' come

$$Z\left(W_{\{x,x'\}}\right) := \sum_{y\in\mathcal{Y}} \sqrt{W(y \mid x) W(y \mid x')}$$

e la distanza media di Bhattacharya di W come

$$Z(W) := \sum_{x,x'\in\mathcal{X}, x\neq x'} \frac{1}{q(q-1)} Z\left(W_{\{x,x'\}}\right).$$

Proposizione 4.4. *Sia W un canale con alfabeto di input q-ario e sia P_e la probabilità di errore del decoder di massima verosimiglianza per un singolo uso del canale. Allora*

$$P_e \leq (q-1) Z(W).$$

Dimostrazione. Se denotiamo con $P_{e,x}$ la probabilità P_e quando $x \in \mathcal{X}$ è inviato, abbiamo

$$\begin{aligned} P_{e,x} &\leq P\left(y \text{ tale che } W(y \mid x') \geq W(y \mid x) \text{ per un certo } x' \neq x \mid x \text{ inviato}\right) \\ &= \sum_{\substack{y \mid \exists x' \neq x \\ W(y\mid x') \geq W(y\mid x)}} W(y \mid x) \leq \sum_{y} \sum_{\substack{x' \mid x' \neq x \\ W(y\mid x') \geq W(y\mid x)}} W(y \mid x) \leq \sum_{y} \sum_{x' \mid x' \neq x} \sqrt{W(y \mid x) W(y \mid x')}. \end{aligned}$$

Quindi P_e è limitato come segue:

$$P_e = \frac{1}{q} \sum_{x\in\mathcal{X}} P_{e,x} \leq \frac{1}{q} \sum_{x\in\mathcal{X}} \sum_{x'\neq x} \sum_{y} \sqrt{W(y \mid x) W(y \mid x')} = (q-1) Z(W).$$

□

Proposizione 4.5. *Sia W un canale con alfabeto di input q-ario, allora*

$$I(W) \geq \log \frac{q}{1+(q-1)Z(W)} \tag{4.1}$$

$$I(W) \leq \log\left(\frac{q}{2}\right) + (\log 2)\sqrt{1-Z(W)^2} \tag{4.2}$$

$$I(W) \leq 2(q-1)(\log e)\sqrt{1-Z(W)^2}. \tag{4.3}$$

Dimostrazione. Dimostriamo separatamente le tre disuguaglianze:

(4.1) Analogamente al caso binario, $\log \frac{q}{1+(q-1)Z(W)}$ equivale alla funzione $E_0(1,Q)$ come definita in [13] ed è dimostrato in [13] che

$$I(W) \geq E_0(1,Q).$$

(4.2) Possiamo servirci del seguente lemma.

Lemma 4.6. *Sia $W : \mathcal{X} \to \mathcal{Y}$ un canale di input q-ario, allora*

$$I(W) \leq \log\left(\frac{q}{2}\right) + \sum_{\substack{x_1,x_2\in\mathcal{X}\\ x_1\neq x_2}} \frac{1}{q(q-1)} I\left(W_{\{x_1,x_2\}}\right).$$

Osserviamo che

$$\sum_{\substack{x_1,x_2\in\mathcal{X}\\ x_1\neq x_2}} \frac{1}{q(q-1)} I\left(W_{\{x_1,x_2\}}\right) = E\left[I\left(W_{\{x_1,x_2\}}\right)\right]$$

dove (X_1, X_2) varia tra le coppie di $\mathcal{X}$ con uguale probabilità. Se applichiamo la Proposizione 2.1, possiamo scrivere

$$E\left[I\left(W_{\{x_1,x_2\}}\right)\right] \leq \log 2 E\left[\sqrt{1-Z\left(W_{\{x_1,x_2\}}\right)^2}\right].$$

Per la disuguaglianza di Jensen,

$$E\left[\sqrt{1-Z\left(W_{\{x_1,x_2\}}\right)^2}\right] \leq \sqrt{1-E\left[Z\left(W_{\{x_1,x_2\}}\right)\right]^2}$$

e, dal momento che $Z(W) = E\left[Z\left(W_{\{x_1,x_2\}}\right)\right]$, abbiamo concluso.

(4.3) Se denotiamo con $W_x(\cdot) := W(\cdot|x)$, possiamo scrivere

$$I(W) = \frac{1}{q}\sum_{x\in\mathcal{X}} D\left(W_x \middle\| \frac{1}{q}\sum_{x'} W_{x'}\right)$$

dove $D(\cdot\|\cdot)$ è la divergenza di Kullback-Leibler. Ciascun termine della somma può essere maggiorato nel modo seguente:

$$\begin{aligned} D\left(W_x \middle\| \frac{1}{q}\sum_{x'} W_{x'}\right) &= \sum_y W_x(y) \log \frac{W_x(y)}{\frac{1}{q}\sum_{x'} W_{x'}(y)} \\ &\leq \log e \sum_y W_x(y) \left(\frac{W_x(y) - \frac{1}{q}\sum_{x'} W_{x'}(y)}{\frac{1}{q}\sum_{x'} W_{x'}(y)}\right) \\ &\leq q \log e \sum_y \left| W_x(y) - \frac{1}{q}\sum_{x'} W_{x'}(y) \right| \\ &= q \log e \left\| W_x - \frac{1}{q}\sum_{x'} W_{x'} \right\|_1 \end{aligned}$$

dove la prima disuguaglianza segue dal fatto che $\log z \leq z - 1$ e la seconda dal fatto che $W_x(y) \leq \sum_{x'} W_{x'}(y)$. Per la disuguaglianza triangolare,

$$\left\| W_x - \frac{1}{q}\sum_{x'} W_{x'} \right\|_1 \leq \frac{1}{q} \sum_{x' \in \mathcal{X}} \|W_x - W_{x'}\|_1$$

e, come dimostrato nel Lemma 2.3,

$$\|W_x - W_{x'}\|_1 \leq 2\sqrt{1 - Z\left(W_{\{x,x'\}}\right)^2}.$$

Quindi

$$I(W) \leq \frac{2\log e}{q} \sum_{\substack{x,x' \in \mathcal{X} \\ x \neq x'}} \sqrt{1 - Z\left(W_{\{x,x'\}}\right)^2} \leq 2(q-1)\log e \sqrt{1 - Z(W)^2},$$

dove l'ultimo passaggio discende dalla concavità della funzione $x \mapsto \sqrt{1-x^2}$ per $0 \leq x \leq 1$.

□

Consideriamo adesso una permutazione di $\mathcal{X}$ fissata π e

$$\begin{aligned} x_1 &= u_1 + u_2, \\ x_2 &= \pi(u_2), \end{aligned}$$

dove denotiamo con $+$ la somma modulo q. In questo caso si calcola facilmente

$$Z\left(W^+\right) = \frac{1}{q(q-1)} \sum_{x \neq x'} Z\left(W_{\pi(x),\pi(x')}\right) \frac{1}{q} \sum_u Z\left(W_{x+u,x'+u}\right).$$

Sia adesso Π scelta uniformemente dall'insieme $\mathcal{P}_\mathcal{X}$ di permutazioni su $\mathcal{X}$ e rivelata al ricevente. Siano X_1, X_2 e U_1, U_2 variabili aleatorie, U_1, U_2 indipendenti e uniformemente distrubuite che rappresentano gli input, poniamo

$$(X_1, X_2) = (U_1 + U_2, \Pi(U_2)) . \tag{4.4}$$

Osserviamo che $I(U_1, U_2; Y_1, Y_2, \Pi) = 2I(W) = I(U_1; Y_1, Y_2, \Pi) + I(U_2; Y_1, Y_2, U_1, \Pi)$
e definiamo i canali $W^- : \mathcal{X} \to \mathcal{Y}^2 \times \mathcal{P}_\mathcal{X}$ e $W^+ : \mathcal{X} \to \mathcal{Y}^2 \times \mathcal{X} \times \mathcal{P}_\mathcal{X}$

$$W^-(y_1, y_2, \pi \mid u_1) = \sum_{u_2 \in \mathcal{X}} \frac{1}{q \cdot q!} W_2(y_1, y_2 \mid u_1, u_2)$$

$$W^+(y_1, y_2, u_1, \pi \mid u_2) = \frac{1}{q \cdot q!} W_2(y_1, y_2 \mid u_1, u_2),$$

dove $W_2(y_1, y_2 \mid u_1, u_2) := W(y_1 \mid u_1 + u_2) W(y_2 \mid \pi(u_2))$, in modo che

$$I\left(W^-\right) = I(U_1; Y_1, Y_2, \Pi) ,$$
$$I\left(W^+\right) = I(U_2; Y_1, Y_2, U_1, \Pi) .$$

Teorema 4.7. *Le trasformazioni descritte sopra polarizzano tutti i canali discreti senza memoria W nel senso della Proposizione 4.1.*

Dimostrazione. Come nel caso binario, definiamo $B_1, B_2, \ldots$ variabili aleatorie indipendenti e identicamente distribuite a valori in $\{+, -\}$ equidistribuite e poniamo

$$I_n := I_n(B_1, \ldots, B_n) = I(W^{B_1, \ldots, B_n}),$$

$$T_n := T_n(B_1, \ldots, B_n) = Z(W^{B_1, \ldots, B_n}),$$

con $I_0 = I(W)$ e $T_0 = Z(W)$. Vogliamo mostrare che i processi $\{I_n\}$ e $\{T_n\}$ soddisfano le condizioni del Lemma 4.2.
Le condizioni (i), (ii) e (iii) sono verificate e la condizione (v) è una conseguenza delle disuguaglianze (4.1) e (4.3) della Proposizione 4.5. Ci resta da verificare la condizione (iv). Osserviamo che

$$Z(W^+) = \frac{1}{q(q-1)} \sum_{\substack{x, x' \\ x \neq x'}} \frac{1}{q!} \sum_{\pi} Z\left(W_{\pi(x), \pi(x')}\right) \frac{1}{q} \sum_{u} Z\left(W_{u+x, u+x'}\right) .$$

Per ogni scelta di x, x', il valore di $\frac{1}{q!} \sum_\pi Z\left(W_{\pi(x), \pi(x')}\right)$ è uguale a $Z(W)$, quindi $Z(W^+) = Z(W)^2$.
Poiché, come dimostrato nella Proposizione 4.4, $Z(W)$ limita dall'alto la probabilità di errore, ci basta mostrare che valgono le ipotesi del Lemma 4.3. La condizione (ii) è implicata dalla disuguaglianza (4.2) della Proposizione 4.5, quindi ci resta da verificare la condizione (i) con la seguente proposizione. □

Proposizione 4.8. *Le trasformazioni descritte sopra verificano*

$$Z(W) \leq Z(W^-) \leq \min\{qZ(W), 2Z(W) + (q-1)Z(W)^2\}.$$

Dimostrazione. Definiamo il canale $W^{(\pi u)}$

$$W^{(\pi u)}(y_1, y_2 \mid x) = W(y_1 \mid x+u)W(y_2 \mid \pi(u))$$

e sia

$$W^{(\pi)} = \frac{1}{q}\sum_{u\in\mathcal{X}} W^{(\pi u)}.$$

Osserviamo che, se la permutazione scelta nel corso dalla trasformazione $W \mapsto (W^-, W^+)$ è π, allora $W^- = W^{(\pi)}$. Se mostriamo che

$$Z(W) \le Z\left(W^{(\pi)}\right) \le \min\{qZ(W), 2Z(W) + (q-1)Z(W)^2\}$$

per ogni scelta di π, abbiamo dimostrato la proposizione poiché $Z(W^-) = \frac{1}{q!}\sum_{\pi} Z\left(W^{(\pi)}\right)$.

Per dimostrare la maggiorazione su $Z\left(W^{(\pi)}\right)$, scriviamo

$$\begin{aligned}
Z\left(W^{(\pi)}\right) &= \frac{1}{q(q-1)} \sum_{\substack{x,x'\in\mathcal{X}\\ x\neq x'}} \sum_{y_1,y_2\in\mathcal{Y}} \frac{1}{q}\sqrt{\sum_{u\in\mathcal{X}} W(y_2|\pi(u))W(y_1|x+u)}\sqrt{\sum_{v\in\mathcal{X}} W(y_2|\pi(v))W(y_1|x'+v)} \\
&\le \frac{1}{q(q-1)} \sum_{\substack{x,x'\\ x\neq x'}} \sum_{y_1,y_2} \frac{1}{q}\sum_{u} \sqrt{W(y_2|\pi(u))W(y_1|x+u)}\sum_{v} \sqrt{W(y_2|\pi(v))W(y_1|x'+v)} \\
&= \frac{1}{q}\sum_{u} \frac{1}{q(q-1)} \sum_{\substack{x,x'\\ x\neq x'}} \sum_{y_2} W(y_2|\pi(u)) \sum_{y_1} \sqrt{W(y_1|x+u)W(y_1|x'+u)} \\
&\quad + \frac{1}{q^2(q-1)} \sum_{\substack{u,v\\ u\neq v}} \sum_{y_2} \sqrt{W(y_2|\pi(u))W(y_2|\pi(v))} \sum_{\substack{x,x'\\ x\neq x'}} \sum_{y_1} \sqrt{W(y_1|x+u)W(y_1|x'+v)}.
\end{aligned}$$

Chiamiamo

$$A := \frac{1}{q}\sum_{u} \frac{1}{q(q-1)} \sum_{\substack{x,x'\\ x\neq x'}} \sum_{y_2} W(y_2|\pi(u)) \sum_{y_1} \sqrt{W(y_1|x+u)W(y_1|x'+u)},$$

$$B := \frac{1}{q^2(q-1)} \sum_{\substack{u,v\\ u\neq v}} \sum_{y_2} \sqrt{W(y_2|\pi(u))W(y_2|\pi(v))} \sum_{\substack{x,x'\\ x\neq x'}} \sum_{y_1} \sqrt{W(y_1|x+u)W(y_1|x'+v)}.$$

Osserviamo che per ogni $u \in \mathcal{X}$,

$$\sum_{y_2} W(y_2|\pi(u)) \sum_{y_1} \sqrt{W(y_1|x+u)W(y_1|x'+u)} = Z\left(W_{\{x+u,x'+u\}}\right)$$

e quindi $A = Z(W)$.

Poiché $\sum_{y_1} \sqrt{W(y_1|x+u)W(y_1|x'+v)} \leq 1$, si ha $B \leq (q-1)Z(W)$.
D'altro canto, per ogni $u \neq v$ fissato,

$$\sum_{\substack{x,x' \\ x \neq x'}} \sum_{y_1} \sqrt{W(y_1|x+u)W(y_1|x'+v)} = q + \left(\sum_{\substack{x \neq x' \\ x+u \neq x' \neq v}} \sqrt{W(y_1|x+u)W(y_1|x'+v)} \right)$$
$$\leq q + (q-1)Z(W)$$

e quindi $B \leq Z(W) + (q-1)Z(W)^2$.
Questo dimostra che

$$Z\left(W^{(\pi)}\right) \leq A + B \leq \min\{qZ(W), 2Z(W) + (q-1)Z(W)^2\}.$$

L'altra disuguaglianza segue dal fatto che

$$\begin{aligned}
Z\left(W^{(\pi)}\right) &= \frac{1}{q(q-1)} \sum_{x \neq x'} Z\left(W^{(\pi)}_{\{x,x'\}}\right) \\
&\leq \frac{1}{q(q-1)} \sum_{x \neq x'} \frac{1}{q} \sum_{u} Z\left(W^{(\pi u)}_{\{x,x'\}}\right) \\
&= \frac{1}{q} \sum_{u} \frac{1}{q(q-1)} \sum_{x \neq x'} \sum_{y_1,y_2} \sqrt{W(y_1|x+u)W(y_1|x'+u)W(y_2|\pi(u))W(y_2|\pi(u))} \\
&= \frac{1}{q} \sum_{u} \frac{1}{q(q-1)} \sum_{x \neq x'} Z\left(W_{\{x+u,x'+u\}}\right) \\
&= Z(W).
\end{aligned}$$

□

Teorema 4.9. *Se la permutazione* Π *definita sopra è scelta tra le permutazioni per cui* 0 *è un punto fisso, la trasformazione dà* $Z(W^+) = Z(W)$ *e quindi polarizza.*

Caso particolare: q primo

Supponiamo di avere un canale $W : \mathcal{X} \to \mathcal{Y}$ DMC e $\mathcal{X} = \{0, \ldots, q-1\}$ con q numero primo. Come nel caso binario, combiniamo due copie indipendenti di W, scegliendo come input dei due canali

$$x_1 = u_1 + u_2,$$
$$x_2 = u_2$$

e definiamo i canali W^- e W^+

$$W^-(y_1, y_2 \mid u_1) = \sum_{u_2 \in \mathcal{X}} \frac{1}{q} W_2(y_1, y_2 \mid u_1, u_2)$$
$$W^+(y_1, y_2, u_1 \mid u_2) = \frac{1}{q} W_2(y_1, y_2 \mid u_1, u_2)$$

dove, come prima, $W_2(y_1, y_2 \mid u_1, u_2) = W(y_1 \mid u_1 + u_2)W(y_2 \mid u_2)$.

Il risultato più importante di questa sezione è il seguente Teorema.

Teorema 4.10. *Se q è un numero primo, le trasformazioni descritte sopra polarizzano i canali q-ari nel senso della Proposizione 4.1 e la probabilità dell'errore di blocco soddisfa*

$$P_e \leq 2^{-N^\beta} \quad \forall \beta < 1/2.$$

Come prima cosa, riscriviamo il parametro $Z(W)$ nel modo seguente:

$$Z(W) = \frac{1}{q-1} \sum_{d \neq 0} Z_d(W)$$

dove $Z_d(W)$ è definito come

$$Z_d(W) := \frac{1}{q} \sum_{x \in \mathcal{X}} Z(W_{\{x, x+d\}}), \quad d \neq 0.$$

Definiamo anche

$$Z_{\max}(W) := \max_{d \neq 0} Z_d(W).$$

Per dimostrare il Teorema 4.10 ci serviremo di un lemma.

Lemma 4.11. *Sia W un canale il cui alfabeto di input sia di dimensione q, q primo. Se $Z_{\max}(W) \geq 1 - \delta$, allora per ogni $\delta > 0$*

$$Z(W) \geq 1 - q(q-1)^2\delta.$$

Dimostrazione. Sia d tale che $Z_{\max}(W) = Z_d(W)$. La disequazione $Z_d(W) \geq 1 - \delta$ implica

$$1 - Z(W_{\{x, x+d\}}) \leq q\delta \quad \forall x \in \mathcal{X}\,.$$

Per un $x \in \mathcal{X}$ fissato, definiamo per ogni $y \in \mathcal{Y}$:

$$a_y = \sqrt{W(y \mid x)} - \sqrt{W(y \mid x+d)},$$
$$b_y = \sqrt{W(y \mid x+d)} - \sqrt{W(y \mid x+d+d)}.$$

Per la disuguaglianza triangolare,

$$\left(\sum_y (a_y + b_y)^2\right)^{1/2} \leq \left(\sum_y a_y^2\right)^{1/2} + \left(\sum_y + b_y^2\right)^{1/2}$$

$$\sqrt{1 - Z(W_{\{x,x+d+d\}})} \leq \sqrt{1 - Z(W_{\{x,x+d\}})} + \sqrt{1 - Z(W_{\{x+d,x+d+d\}})} \leq 2\sqrt{q\delta}.$$

Osserviamo che, poiché q è primo, possiamo riscrivere l'alfabeto di input come

$$\mathcal{X} = \{x, x + d, x + d + d, \ldots, x + (q - 1)d\}$$

per $x \in \mathcal{X}$ e $d \neq 0$. Quindi per ogni $x, x' \in \mathcal{X}$

$$\sqrt{1 - Z(W_{\{x,x'\}})} \leq (q - 1)\sqrt{q\delta}$$

che implica

$$Z(W) = \frac{1}{q(q-1)} \sum_{\substack{x,x' \\ x \neq x'}} Z(W_{\{x,x'\}}) \geq 1 - q(q-1)^2\delta.$$

□

A questo punto possiamo dimostrare il Teorema 4.10.

Dimostrazione. Siano $B_1, B_2 \ldots$ variabili aleatore i.i.d. a valori in $\{+, -\}$ con

$$P(B_i = -) = P(B_i = +) = \frac{1}{2}.$$

Definiamo i processi stocastici

$$I_n := I_n(B_1, \ldots B_n) = I(W^{B_1,\ldots,B_n}),$$

$$T_n := T_n(B_1, \ldots B_n) = Z_{\max}(W^{B_1,\ldots,B_n})$$

con $I_0 = I(W)$ e $T_0 = Z_{\max}(W)$. Per dimostrare il teorema ci basta verificare che $\{I_n\}$ e $\{T_n\}$ soddisfano le condizioni del Lemma 4.2 e del Lemma 4.3. Iniziamo col verificare le condizioni del Lemma 4.2:

- (i), (ii) e (iii) sono ovvie;
- per (iv), scriviamo

$$\begin{aligned} Z_d\left(W^+\right) &= \frac{1}{q} \sum_x Z\left(W^+_{\{x,x+d\}}\right) \\ &= \frac{1}{q} \sum_x \frac{1}{q} \sum_{y_1,y_2,u} \sqrt{W(y_1 \mid x+u)W(y_1 \mid x+d+u)}\sqrt{W(y_2 \mid x)W(y_2 \mid x+d)} \\ &= \frac{1}{q} \sum_x \left(W_{\{x,x+d\}}\right) \frac{1}{q} \sum_u Z\left(\left(W_{\{x+u,x+u+d\}}\right)\right) \\ &= Z_d(W)^2, \end{aligned}$$

quindi $Z_{\max}\left(W^+\right) = Z_{\max}(W)^2$ o, equivalentemente, $T_{n+1} = T_n^2$ quando $B_{n+1} = +$;

- per mostrare che vale (v), osserviamo che per le disuguaglianze (4.1) e (4.3) della Proposizione 4.5, per ogni $\epsilon > 0$ esiste $\delta > 0$ tale che

$$I(W) \in (\epsilon, 1-\epsilon) \text{ implica } Z(W) \in (\delta, 1-\delta)$$

e, segue dal Lemma 4.11 che, per ogni $\delta > 0$

$$Z(W) \in (\delta, 1-\delta) \text{ implica } Z_{\max}(W) \in \left(\delta, 1 - \frac{\delta}{q(q-1)^2}\right),$$

da cui segue (v).

Ci resta da verificare che i processi rispettano le condizioni del Lemma 4.3:

- per verificare (i), possiamo maggiorare $Z_d\left(W^-\right)$ come segue

$$\begin{aligned}
Z_d\left(W^-\right) &= \frac{1}{q}\sum_x Z\left(W^-_{\{x,x+d\}}\right) \\
&= \frac{1}{q}\sum_x \sum_{y_1,y_2} \frac{1}{q}\sqrt{\sum_u W(y_1 \mid x+u)W(y_2 \mid u)\sum_v W(y_1 \mid x+d+v)W(y_2 \mid v)} \\
&\leq \frac{1}{q}\sum_x \sum_{y_1,y_2}\sum_{u,v} \frac{1}{q}\sqrt{W(y_1 \mid x+u)W(y_2 \mid u)W(y_1 \mid x+d+v)W(y_2 \mid v)} \\
&= \frac{1}{q}\sum_u \frac{1}{q}\sum_x\sum_{y_1}\sqrt{W(y_1 \mid x+u)W(y_1 \mid x+d+u)} \\
&\quad + \frac{1}{q}\sum_{\substack{u,v\\ u\neq v}}\sum_{y_2}\sqrt{W(y_2 \mid u)W(y_2 \mid v)}\frac{1}{q}\sum_x\sum_{y_1}\sqrt{W(y_1 \mid x+u)W(y_1 \mid x+d+v)} \\
&= Z_d(W) + \left(\sum_{\Delta\neq 0}\frac{1}{q}\sum_u\sum_{y_2}\sqrt{W(y_2 \mid u)W(y_2 \mid u+\Delta)}\right)\cdot \\
&\qquad \left(\frac{1}{q}\sum_x\sum_{y_1}\sqrt{W(y_1 \mid x+u)W(y_1 \mid x+d+u+\Delta)}\right) \\
&= 2Z_d(W) + \sum_{\substack{\Delta\neq 0\\ d+\Delta\neq 0}} Z_\Delta(W)Z_{d+\Delta}(W) \\
&\leq 2Z_d(W) + (q-2)Z_{\max}(W)^2
\end{aligned}$$

e quindi $Z_{\max}(W^-) \leq 2Z_{\max}(W) + (q-2)Z_{\max}(W)^2 \leq qZ_{\max}(W)$, che implica (i);

- la condizione (ii) segue dalla disuguaglianza (4.2) della Proposizione 4.5 e dalla relazione

$$Z_{\max}(W) \leq qZ(W).$$

□

Un'altra definizione dei canali

Se diamo ad $\mathcal{X}$ una struttura di campo con le operazioni $(+, \cdot)$ e scegliamo R, noto al ricevente, un elemento di $\mathcal{X}_* = \mathcal{X} \setminus \{0\}$. Poniamo

$$(x_1, x_2) = (u_1 + u_2, R \cdot u_2).$$

Come prima, si ha

$$I(U_1, U_2; Y_1, Y_2, R) = 2I(W) = I(U_1; Y_1, Y_2, R) + I(U_2; Y_1, Y_2, U_1, R) = I\left(W^-\right) + I\left(W^+\right).$$

a meno di aver posto $\quad W^- : \mathcal{X} \to \mathcal{Y}^2 \times \mathcal{X}_* \quad$ e $\quad W^+ : \mathcal{X} \to \mathcal{Y}^2 \times \mathcal{X} \times \mathcal{X}_*$

$$W^-(y_1, y_2, r \mid u_1) = \sum_{u_2 \in \mathcal{X}} \frac{1}{q(q-1)} W(y_1 \mid u_1 + u_2) W(y_2 \mid r \cdot u_2),$$

$$W^+(y_1, y_2, u_1, r \mid u_2) = \frac{1}{q(q-1)} W(y_1 \mid u_1 + u_2) W(y_2 \mid r \cdot u_2).$$

Teorema 4.12. *Le trasformazioni descritte nel paragrafo precedente polarizzano tutti i canali nel senso della Proposizione 4.1.*

Osservazione 4.13. Se l'alfabeto di input non è primo, possiamo scomporre

$$q = \prod_{i=1}^{L} q_i,$$

dove q_i è primo per ogni i. Se X è la variabile aleatoria che rappresenta l'input, scriviamo $X = (U_1, \ldots, U_L)$ dove gli U_i sono indipendenti e uniformemente distribuite su $\mathcal{U}_i = \{0, \ldots, lq_i\}$ rispettivamente. Definiamo adesso i canali

$$W^{(i)} : \mathcal{U}_i \to \mathcal{Y} \times \mathcal{U}_1 \times \ldots \times \mathcal{U}_{i-1}$$

$$W^{(i)}(y, u_1^{i-1} \mid u_i) = \prod_{j \neq i} \frac{1}{q_j} \sum_{u_{i+1}^L} W(y \mid (u_1^L)).$$

Si vede facilmente che $I(W) = I(X;Y) = I(U_1^L; Y) = \sum_i I\left(W^{(i)}\right)$ e possiamo polarizzare ciascun canale $W^{(i)}$ separatamente.

4.2 Matrice di trasformazione dei canali

Abbiamo visto nei capitoli precedenti che la polarizzazione dei canali avviene attraverso una matrice

$$G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

In questa sezione consideriamo trasformazioni della forma $G^{\otimes n}$, dove G è una matrice $l \times l$ con $l \geq 3$, e cerchiamo le condizioni necessarie e sufficienti perché la matrice G polarizzi un canale B-DMC simmetrico.

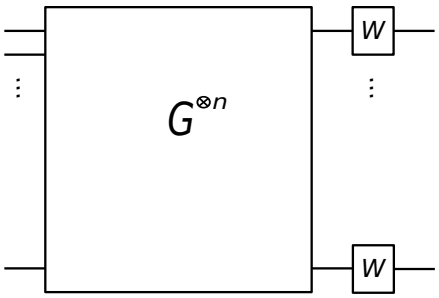

Figura 4.1: La matrice $G^{\otimes n}$ trasforma i vettori e li rende input dei canali W.

Consideriamo $W : \mathcal{X} \to \mathcal{Y}$, $\mathcal{X} = \{0,1\}$, un canale B-DMC simmetrico e, per $l \geq 3$ fissato, G una matrice $l \times l$ invertibile a valori in $\{0,1\}$. Sia U_1^l una variabile aleatorie uniformemente distribuita su $\{0,1\}^l$, chiamiamo $X_1^l := U_1^l G$. Se denotiamo con Y_1^l l'output di l usi del canale W con input X_1^l, il canale tra U_1^l e X_1^l ha probabilità di transizione

$$W_l(y_1^l \mid u_1^l) := \prod_{i=1}^{l} W(y_i \mid x_i) = \prod_{i=1}^{l} W(y_i \mid (u_1^l G)_i).$$

Definiamo $W^{(i)} : \mathcal{X} \to \mathcal{Y}^l \times \{0,1\}^{i-1}$ il canale con input u_i, output (y_1^l, u_1^{i-1}) e probabilità di transizione

$$W^{(i)}(y_1^l, u_1^{i-1} \mid u_i) = \frac{1}{2^{l-1}} \sum_{u_{i+1}^l} W_l(y_1^l \mid u_1^l)$$

denotiamo con $I^{(i)}$ la mutua informazione e con $Z^{(i)}$ il parametro di Bhattacharya di questo canale,

$$Z^{(i)} = \sum_{y_1^l, u_1^{i-1}} \sqrt{W^{(i)}(y_1^l, u_1^{i-1} \mid 0) W^{(i)}(y_1^l, u_1^{i-1} \mid 1)}.$$

Per $k \geq 1$ denotiamo con W^k il canale B-DMC $W^k : \mathcal{X} \to \mathcal{Y}^k$ con probabilità di transizione

$$W^k(y_1^k \mid x) = \prod_{j=1}^{k} W(y_j \mid x)$$

e con $\widetilde{W}^{(i)}$ il canale B-DMC $\widetilde{W}^{(i)} : \mathcal{X} \to \mathcal{Y}^l$ con probabilità di transizione

$$\widetilde{W}^{(i)}(y_1^l \mid u_i) = \frac{1}{2^{l-i}} \sum_{u_{i+1}^l} W_l(y_1^l \mid 0_1^{i-1}, u_i^l).$$

Osservazione 4.14. Dal momento che W è un canale simmetrico, i canali $W^{(i)}$ e $\widetilde{W}^{(i)}$ sono *equivalenti* nel senso che, per ogni u_1^{i-1} fissato, esiste una permutazione $\pi_{u_1^{i-1}} : \mathcal{Y}^l \to \mathcal{Y}^l$ tale

che

$$W^{(i)}(y_1^l, u_1^{i-1} \mid u_i) = \frac{1}{2^{i-1}} \widetilde{W}^{(i)}(\pi_{u_1^{i-1}}(y_1^l) \mid u_i).$$

Definizione 4.15. La matrice G è *polarizzante* se esiste $i \in \{1, \dots, l\}$ tale che

$$\widetilde{W}^{(i)}(y_1^l \mid u_i) = Q(y_{A^c}) \prod_{j \in A} W(y_j \mid u_i) \tag{4.5}$$

per $A \subset \{1, \dots, l\}$ e $|A| = k$, $k \geq 2$ e una distribuzione di probabilità $Q : \mathcal{Y}^{|A^c|} \to [0, 1]$.

Chiamiamo G *polarizzante* perché l'applicazione ripetuta di tale matrice polarizza il canale.

Per l'Osservazione 4.14, l'equazione (4.5) implica

$$W^{(i)}(y_1^l, u_1^{i-1} \mid u_i) = \frac{Q(y_{A^c})}{2^{i-1}} \prod_{j \in A} W\left((\pi_{u_1^{i-1}}(y_1^l))_j \mid u_i\right)$$

e denotiamo questa relazione con $W^{(i)} \equiv W^k$. Osserviamo che $W^{(i)} \equiv W^k$ implica $I^{(i)} = I(W^k)$ e $Z^{(i)} = Z(W^k)$.

Il seguente risultato dà una condizione necessaria e sufficiente affinché G sia polarizzante.

Lemma 4.16. *Sia W un canale simmetrico B-DMC, allora*

(i) *se G non è triangolare superiore, allora esiste un i per il quale $W^{(i)} \equiv W^k$ per un certo $k \geq 2$;*

(ii) *se G è triangolare superiore, allora $W^{(i)} \equiv W$ per ogni i, $1 \leq i \leq l$.*

Dimostrazione. Iniziamo con alcune osservazioni.

Osservazione 4.17. Poiché G è una matrice invertibile esiste una permutazione delle colonne di G tale che tutti gli elementi della diagonale della matrice permutata sono uguali ad 1.

Osservazione 4.18. Le probabilità di transizione che definiscono i canali $W^{(i)}$, a meno di permutare gli output y_1^l, sono invarianti rispetto alla permutazione delle colonne.

Possiamo quindi assumere senza perdita di generalità che G abbia tutti 1 sulla diagonale.

Sia k il numero di occorrenze di 1 nell'ultima riga di G. Chiaramente, $W^{(l)} \equiv W^k$. Se $k \geq 2$, allora G non è triangolare superiore e abbiamo provato la prima parte del lemma.
Se $k = 1$, allora $G_{lk} = 0 \quad 1 \leq k < l$.
In questo caso, possiamo scrivere:

$$
\begin{aligned}
W^{(l-i)}(y_1^l, u_1^{l-i-1} \mid u_{l-i}) &= \frac{1}{2^{l-1}} \sum_{u_{l-i+1}^l} W_l(y_1^l \mid u_1^l) \\
&= \frac{1}{2^{l-1}} \sum_{u_{l-i+1}^{l-1}, u_l} P(Y_1^{l-1} = y_1^{l-1} \mid U_1^l = u_1^l) P(Y_l = y_l \mid Y_1^{l-1} = y_1^{l-1}, U_1^l = u_1^l) \\
&= \frac{1}{2^{l-1}} \sum_{u_{l-i+1}^{l-1}, u_l} W_{l-1}(y_1^{l-1} \mid u_1^{l-1}) P(Y_l = y_l \mid Y_1^{l-1} = y_1^{l-1}, U_1^l = u_1^l) \\
&= \frac{1}{2^{l-1}} \sum_{u_{l-i+1}^{l-1}} W_{l-1}(y_1^{l-1} \mid u_1^{l-1}) \sum_{u_l} P(Y_l = y_l \mid Y_1^{l-1} = y_1^{l-1}, U_1^l = u_1^l) \\
&= \frac{1}{2^{l-1}} \left(W(y_l \mid 0) + W(y_l \mid 1)\right) \sum_{u_{l-i+1}^{l-1}} W_{l-1}(y_1^{l-1} \mid u_1^{l-1}).
\end{aligned}
$$

Quindi Y_l é indipendente dagli input dei canali $W^{(l-i)}$ per $i = 1, \ldots, l-1$. Questo è equivalente a dire che, se denotiamo con $G^{(l-i)}$ la matrice $(l-i) \times (l-i)$ ottenuta da G togliendo le ultime i righe e colonne, i canali $W^1, \ldots, W^{(l-1)}$ sono definiti dalla matrice $G^{(l-i)}$.
Possiamo ripetere lo stesso ragionamento per $G^{(l-i)}$ e vediamo che, se G è triangolare superiore, $W^{(i)} \equiv W$ per ogni i. Viceversa, se G non è triangolare superiore, esiste un indice i per il quale $W^{(l-i)}$ ha almeno due 1 nell'ultima riga e questo implica che $W^{(i)} \equiv W^k$ per $k \geq 2$.

□

Teorema 4.19. *Sia W un canale simmetrico B-DMC e G una matrice $l \times l$ fissata e siano $W^{(i)}$, per $i \in \{1, \ldots, l^n\}$, i canali definiti dalla trasformazione $A_n G^{\otimes n}$, dove $A_n : \{1, \ldots, l^n\} \to \{1, \ldots, l^n\}$ è una permutazione definita analogamente all'operazione in inversione di bit. Allora*

(i) *se G è polarizzante, per ogni $\delta > 0$*

$$\lim_{n \to \infty} \frac{\#\{i \in \{1, \ldots, l^n\} \mid I\left(W^{(i)}\right) \in (\delta, 1-\delta)\}}{l^n} = 0, \tag{4.6}$$

$$\lim_{n \to \infty} \frac{\#\{i \in \{1, \ldots, l^n\} \mid Z\left(W^{(i)}\right) \in (\delta, 1-\delta)\}}{l^n} = 0. \tag{4.7}$$

(ii) *se G non è polarizzante, per ogni n e per ogni $i \in \{1, \ldots, l^n\}$*

$$I\left(W^{(i)}\right) = I(W), \quad Z\left(W^{(i)}\right) = Z(W).$$

Dimostrazione. In modo analogo a quanto fatto nei capitoli precedenti, definiamo i processi $\{W_n \mid n \geq 0\}$:

$$W_0 = W$$

$$W_{n+1} = W_n^{(B_{n+1})}$$

dove $\{B_n \mid n \geq 1\}$ è una successione di variabili aleatorie i.i.d. definite su uno spazio di probabilità $(\Omega, \mathcal{F}, \mu)$ e uniformemente distribuite su $\{1, \ldots, l\}$. Anche in questo caso definiamo

la filtrazione $\mathcal{F}_n$ e i processi $\{I_n \mid n \geq 0\}$ e $\{Z_n \mid n \geq 0\}$. Si dimostra facilmente che questi processi verificano:

$$P(I_n \in (a,b)) = \frac{\#\{i \in \{1,\ldots,l^n\} \mid I_n \in (a,b)\}}{l^n} \tag{4.8}$$

$$P(Z_n \in (a,b)) = \frac{\#\{i \in \{1,\ldots,l^n\} \mid Z_n \in (a,b)\}}{l^n} \tag{4.9}$$

Osservazione 4.20. $\{I_n, \mathcal{F}_n)\}$ è una martingala limitata e converge in $\mathcal{L}^1$ probabilità 1 ad una variabile aleatoria I_∞.

Ci serve adesso un risultato.

Lemma 4.21. *Se G è polarizzante, allora*

$$I_\infty = \begin{cases} 1 & \textit{con probabilità } I(W) \\ 0 & \textit{con probabilità } 1 - I(W) \end{cases}$$

Osserviamo che per ogni $n \geq 0$,

$$\frac{\#\{i \in \{1,\ldots,l^n\} \mid I\left(W^{(i)}\right) \in (\delta, 1-\delta)\}}{l^n}$$

é uguale a $P(I_n \in (\delta, 1-\delta))$ e, per il Lemma 4.21 questo dimostra (4.6).
Per ogni canale W', siano $I(W')$ e $Z(W')$ che soddisfano 4.8 e 4.9,

$$I(W') + Z(W') \geq 1,$$

$$I(W')^2 + Z(W')^2 \leq 1.$$

Le disuguaglianze implicano che quando $I(W')$ assume i valori 0 o 1, $Z(W')$ assume i valori 1 e 0 rispettivamente. Dal Lemma 4.21 sappiamo che $\{I_n\}$ converge a I_∞ con probabilità 1 e $I_\infty \in \{0,1\}$. Questo implica che $\{Z_n\}$ converge con probabilità 1 ad una variabile aleatoria Z_∞

$$Z_\infty = \begin{cases} 0 & \text{con probabilità } I(W), \\ 1 & \text{con probabilità } 1 - I(W). \end{cases}$$

Abbiamo dimostrato la prima parte del teorema.
La seconda parte segue dal Lemma 4.16 (ii). □

Ci resta da dimostrare il Lemma 4.21.

Dimostrazione. Sia G una matrice polarizzante. Per il Lemma 4.16, esiste $i \in \{1, \dots, l\}$ e $k \geq 2$ tale che

$$I^{(i)} = I(W^k).$$

Questo implica che, per i processi definiti sopra,

$$I_{n+1} = I(W_n^k) \quad \text{con probabilità maggiore o uguale di } \frac{1}{l},$$

per un certo $k \geq 2$. La convergenza $\mathcal{L}^1$ di I_n implica che $E[|I_{n+1} - I_n|] \to 0$ per $n \to \infty$ e quindi

$$E[|I_{n+1} - I_n|] \geq \frac{1}{l} E[(I(W_n^k) - I(W_n))] \to 0. \tag{4.10}$$

Supponiamo di aver dimostrato il seguente risultato.

Lemma 4.22. *Sia W un canale B-DMC simmetrico e sia W^k il canale*

$$W^k(y_1^k \mid x) = \prod_{i=1}^{k} W(y_i \mid x).$$

Se $I(W) \in (\delta, 1-\delta)$ per un certo $\delta > 0$, allora esiste $\eta(\delta) > 0$ tale che $I(W^k) - I(W) > \eta(\delta)$.

Per il Lemma 4.22, la convergenza in (4.10) implica che I_∞ appartiene a $\{0, 1\}$ con probabilità 1. La distribuzione di I_∞ segue dalle proprietà di martingala di $\{I_n\}$. □

Dimostriamo adesso il Lemma 4.22.

Dimostrazione. La dimostrazione del lemma segue a sua volta dal seguente teorema, dimostrato in [21].

Teorema 4.23. *Siano $W_1, \dots, W_k$ k canali B-DMC simmetrici con capacità $I_1, \dots, I_k$ rispettivamente. Siano $W^{(k)}$ i canali con probabilità di transizione*

$$W^k(y_1^k \mid x) = \prod_{i=1}^{k} W_i(y_i \mid x)$$

e $W_{BSC}^{(k)}$ il canale con probabilità di transizione

$$W_{BSC}^{(k)}(y_1^k \mid x) = \prod_{i=1}^{k} W_{BSC(\epsilon_i)}(y_i \mid x),$$

dove $BSC(\epsilon_i)$ denota il canale BSC con probabilità di crossover $\epsilon_i \in [0, 1/2]$, $\epsilon_i = H^{-1}(1 - I_i)$, dove H é la funzione di entropia binaria. Allora, $I(W^{(k)}) \geq I(W_{BSC^{(k)}})$.

Nel nostro caso consideriamo $\epsilon \in [0, 1/2]$ la probabilità di crossover del canale BSC con capacità $I(W)$. Osserviamo che, per $k \geq 2$,

$$I(W^k) \geq I(W^2) \geq I(W).$$

Per il Teorema 4.23, $I\left(W^2\right) \geq I\left(W^2_{BSC(\epsilon)}\right)$ e si vede facilmente che

$$I\left(W^2_{BSC(\epsilon)}\right) = 1 + H(2\epsilon\bar{\epsilon}) - 2H(\epsilon).$$

Quindi possiamo scrivere

$$\begin{aligned} I(W^k) - I(W) &\geq I\left(W^2_{BSC(\epsilon)}\right) - I(W) \\ &= I\left(W^2_{BSC(\epsilon)}\right) - I\left(W_{BSC(\epsilon)}\right) \\ &= H(2\epsilon\bar{\epsilon}) - H(\epsilon). \end{aligned}$$

Poiché $I(W)$ appartiene a $(\delta, 1-\delta)$, ϵ appartiene a $(\phi(\delta), 1/2 - \phi(\delta))$, $\phi(\delta) > 0$, che a sua volta implica $H(2\epsilon\bar{\epsilon}) - H(\epsilon) > \eta(\delta)$ per un certo $\eta(\delta) > 0$.

□

Teorema 4.24. *Sia W un canale simmetrico B-DMC, G matrice polarizzante $l \times l$ e $\beta < \dfrac{\log_l 2}{l}$, allora*

$$\lim_{n\to\infty} P\left(Z_n \leq 2^{-l^{n\beta}}\right) = I(W).$$

Dimostrazione. Sia G una matrice polarizzante; è facile vedere che:

$$Z_{n+1} \leq Z_n^2 \quad \text{con probabilità maggiore o uguale di } \frac{1}{l},$$

$$Z_{n+1} \leq l Z_n \quad \text{con probabilità } 1.$$

La dimostrazione segue adattando quella del Teorema 3.20 a questo caso.

□

Definizione 4.25. Sia W un canale simmetrico B-DMC con $0 < I(W) < 1$, definiamo $E(G)$ il *tasso di polarizzazione* di una matrice G di dimensioni $l \times l$ se

(i) per ogni $\beta < E(G)$ fissato, $\liminf_{n\to\infty} P\left(Z_n \leq 2^{-l^{n\beta}}\right) = I(W)$;

(ii) per ogni $\beta > E(G)$ fissato, $\liminf_{n\to\infty} P\left(Z_n \geq 2^{-l^{n\beta}}\right) = 1$.

Fissiamo adesso R, $0 < R < 1$, e $\beta < E(G)$. La Definizione 4.25(i) implica che per n sufficientemente grande esiste un insieme $\mathcal{A}$ di cardinalità $l^n R$ tale che $\sum_{i\in\mathcal{A}} Z^{(i)} \leq 2^{-l^{n\beta}}$. Se usiamo $\mathcal{A}$ come l'insieme dei bit d'informazione, la probabilità di errore di blocco tramite SC decoder P_e è limitata nel modo seguente

$$P_e \leq 2^{-l^{n\beta}}.$$

Viceversa, se consideriamo $R > 0$ e $\beta > E(G)$, la Definizione 4.25(ii) implica che per n sufficientemente grande un arbitrario insieme $\mathcal{A}$ di cardinalità $l^n R$ soddisfa $\max_{i\in\mathcal{A}} Z^{(i)} > 2^{-l^{n\beta}}$ e, grazie all'osservazione seguente,

$$P_e \geq 2^{-l^{n\beta}}.$$

Osservazione 4.26. La probabilità di errore di blocco tramite SC decoder verifica

$$\max_{i\in\mathcal{A}} \frac{1}{2}\left(1-\sqrt{1-(Z^{(i)})^2}\right) \leq P_e \leq \sum_{i\in\mathcal{A}} Z^{(i)}.$$

Dimostrazione. La maggiorazione $P_e \leq \sum_{i\in\mathcal{A}} Z^{(i)}$ è già stata dimostrata. Ci rimane da provare che $P_e \geq \max_{i\in\mathcal{A}} \frac{1}{2}\left(1-\sqrt{1-(Z^{(i)})^2}\right)$. Sia W un canale B-DMC simmetrico, è una fatto noto di teoria dell'informazione che ciascun canale W con le caratteristiche appena descritte è equivalente alla combinazione convessa di un numero finito di canali BSC la cui forma è nota al ricevente ([20]) . Sia K la cardinalità di questi canali.

Denotiamo con $\widetilde{P}_e$ la probabilità di errore di bit del canale, $\{\epsilon_i\}_{i=1}^K$ la probabilità di errore di bit dei K canali e $\{Z_i\}_{i=1}^K$ i parametri di Bhattacharya dei K canali. Possiamo scrivere

$$\widetilde{P}_e(W) = \sum_{i=1}^K \alpha_i \epsilon_i, \qquad Z(W) = \sum_{i=1}^K \alpha_i Z_i$$

per determinati $\alpha_i > 0$, $\sum_{i=1}^K \alpha_i = 1$. Quindi,

$$\begin{aligned}
\widetilde{P}_e(W) &= \sum_{i=1}^K \alpha_i \frac{1}{2}\left(1-\sqrt{1-Z_i^2}\right) \\
&\geq \frac{1}{2}\left(1-\sqrt{1-\left(\sum_{i=1}^K \alpha_i Z_i\right)^2}\right) \\
&= \frac{1}{2}\left(1-\sqrt{1-Z(W)^2}\right)
\end{aligned}$$

dove la disuguaglianza segue dalla convessità della funzione $x \mapsto 1-\sqrt{1-x^2}$ per $x \in (0,1)$. La probabilità di errore di blocco tramite SC decoder è limitata dal basso da $\widetilde{P}_e(W)$ e quindi

$$\max_{i\in\mathcal{A}} \frac{1}{2}\left(1-\sqrt{1-(Z^{(i)})^2}\right) \leq P_e.$$

□

Bibliografia

[1] A-Y AMIN, R.K. FRANK : *A Simplified Successive-Cancellation Decoder for Polar Codes*, IEEE Communications Letters, vol 15 (2011).

[2] E. ARIKAN: *Channel combining and splitting for cutoff rate improvement*, IEEE Transactions on Information Theory (2006).

[3] E. ARIKAN: *Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels*, IEEE Transactions on Information Theory (2008).

[4] E. ARIKAN, E. ŞAŞOĞLU, E. TELATAR: *Polarization for arbitrary discrete memoryless channels*, arXiv:0908.0302 (2009).

[5] E. ARIKAN: *Source Polarizatione*, arXiv:1001.3087 (2010).

[6] E. ARIKAN: *A performance Comparison of Polar codes and Reed-Muller Codes*, IEEE Transactions on Information Theory (2008).

[7] E. ARIKAN, E. TELATAR: *On the rate of channel polarization*, IEEE International Symposium on Information Theory, Seul (2009).

[8] R.B. ASH: *Information Theory*, Dover Pubblications (1965).

[9] J.A. BONDY, U.S.R. MURTY: *Graph Theory*, Springer (2008).

[10] M. BOSSET: *Channel Coding*, Wiley (1999).

[11] K.L. CHUNG: *A Course in Probability Theory, 2nd ed.*, Academic (1974).

[12] D. COSTELLO, S. LIN: *Error Control Coding*, Pearson (2005).

[13] R.G. GALLAGER: *Information Theory and Reliable Communication*, Wiley (1968).

[14] N. HUSSAMI, S.B. KORADA, R. URBANKE: *Polar Codes for Channel and Source Coding*, IEEE International Symposium on Information Theory (2009).

[15] S.B. KORADA, E. ŞAŞOĞLU, R. URBANKE: *Polar Codes: Characterization of Exponent, Bounds, and Constructions*, IEEE Transactions on Information Theory (2010).

[16] C. LEROUX, I. TAL, A. VARDY, W.J. GROSS: *Hardware architectures for Successive Cancellation Decoding of Polar Codes*, IEEE International Conference on Acoustics, Speech and Signal Processing (2011).

[17] S. LIN, W.E. RYAN: *Channel Codes, Classical and Modern*, Cambridge University Press (2009).

[18] D.J.C. MACKAY: *Information Theory, Inference and Learning Algorithms*, Cambdridge University Press (2003).

[19] M. PLOTKIN: *Binary codes with specified minimum distance*, IEEE Transactions on Information Theory (1960).

[20] T. RICHARDSON, R. URBANKE: *Modern Coding Theory*, Cambdridge University Press (2008).

[21] S. SHAMAI, I. SUTSKOVER, J. ZIV: *Extremes of information combining*, IEEE Transactions on Information Theory (2005).

[22] C.E. SHANNON: *A mathematical Theory of Communication*, University of Illinois Press (1949).