Capitolo 7

Codifica convoluzionale*

[Non in programma per l'anno 2003/04]

Nell'ambito delle comunicazioni digitali esistono due grandi classi di codici: i codici a blocchi e i codici convoluzionali.

La teoria dei codici a blocchi è ben sviluppata, come documentano anche numerose monografie ad essi dedicate, alcune delle quali sono riportate in bibliografia. I tipi più importanti di codici a blocchi sono costruiti sulla base di una teoria di carattere algebrico, che fornisce anche gli strumenti per analizzare le loro principali proprietà (quali ad esempio le distanze minime) e per derivare gli algoritmi di decodifica.

La teoria dei codici convoluzionali è più recente e meno ricca di risultati. I codici convoluzionali sono ottenuti tipicamente con procedimenti di ricerca più o meno esaustiva per determinare quelli con migliori proprietà di distanza. Anche gli algoritmi di decodifica (ed. es. l'algoritmo di Viterbi) si basano essenzialmente su procedure di ricerca. Cionondimeno i codici convoluzionali si dimostrano in molte applicazioni migliori di quelli a blocchi, nel senso che offrono, rispetto ai codici a blocchi, un migliore rapporto prestazioni/complessità.

A partire dall'inizio degli anni settanta, grazie ad alcuni fondamentali lavori di D.Forney, e con rinnovato interesse dalla fine degli anni ottanta, anche grazie all'introduzione dell'approccio "behaviors", la teoria dei codici convoluzionali sta raggiungendo un certo livello di completezza. Come vedremo, essa costituisce per molti aspetti un settore di indagine vicino a quello dei sistemi lineari; in particolare, i metodi delle matrici polinomiali e razionali, delle serie formali, dei polinomi di Laurent descritti nei capitoli precedenti forniscono gli strumenti per l'analisi, la sintesi e il controllo dei sistemi dinamici, ma anche per lo studio dei codici convoluzionali e per l'implementazione di codificatori e decodificatori.

Va anche ricordato che svariati concetti e algoritmi, una volta introdotti in

ambito sistemistico, sono stati poi utilizzati per la codifica convoluzionale e viceversa. In qualche caso l'introduzione è avvenuta simultaneamente e indipendentemente nei due contesti, e purtroppo non sempre la nomenclatura è risultata uniforme. A questo proposito, cercheremo qui di seguire notazione e nomenclatura congruenti con quelle utilizzate nel resto della dispensa, e tipiche della letteratura sistemistica. Avvertiamo il lettore che nella letteratura sui codici convoluzionali di solito

- si usano vettori riga, anzichè vettori colonna, per rappresentare ingressi, stati e uscite con più componenti;
- le trasformazioni lineari sono rappresentate da matrici applicate a destra del vettore riga (anziché a sinistra del vettore colonna);
- le lettere utilizzate per denotare ingressi, stati e uscite e il numero delle componenti sono diverse da quelle dell'ambiente sistemistico (gli ingressi sono denotati talvolta con $\mathbf{x}$ e il loro numero con k, il numero delle uscite con n, etc.).

7.1 Il sistema di trasmissione

I sistemi per la trasmissione e per la memorizzazione dei dati pongono spesso stringenti richieste di efficienza e di affidabilità. In particolare, si richiede che sia possibile controllare gli effetti del rumore introdotto nei canali utilizzati per trasmettere (o nei supporti utilizzati per immagazzinare) l'informazione, così da riottenere correttamente i dati originali.

In un lavoro del 1948, Shannon dimostrò che gli errori indotti dal rumore in un canale di trasmissione (o in un supporto per memorizzazione) possono essere ridotti al di sotto di qualsiasi livello prescelto, senza sacrificare la velocità di trasmissione del canale (o le capacità di immagazzinamento del mezzo), pur di ricorrere ad un'appropriata *codifica* del segnale che reca l'informazione. Il risultato di Shannon dimostrava *l'esistenza* di metodi di codifica e di decodifica di efficienza comunque buona, ma *non li forniva costruttivamente*. Negli anni seguenti, lo sforzo per ottenere algoritmi di codifica e decodifica efficienti non ha conosciuto soste, ed oggi si dispone di una larga messe di risultati.

Un tipico sistema di trasmissione (o di memorizzazione) può essere rappresentato dal diagramma a blocchi di fig.7.1.

La *sorgente di informazione* produce un segnale $v(\cdot)$, da inviare a destinazione, che può essere continuo o discreto. Il *codificatore di sorgente* trasforma $v(\cdot)$ in una sequenza $u(\cdot)$ di simboli, appartenenti a un particolare alfabeto W. In moltissimi

casi W consiste di due soli simboli (0 e 1) o degli elementi di qualche altro campo finito $\mathbb{F}$. Se la sorgente di informazione produce un segnale continuo, la codifica di sorgente coinvolge anche un processo di conversione analogica/digitale; in ogni caso, essa deve produrre una sequenza $u(\cdot)$ contenente il numero minimo di bit per unità di tempo (minimizzazione della *ridondanza*) ma dalla quale si possa ricostruire senza ambiguità $v(\cdot)$. Non ci occuperemo oltre della codifica di sorgente: nei discorsi a venire, supporremo sempre che la *sequenza di informazione* $u(\cdot)$ sia disponibile, e la assumeremo come dato di partenza.

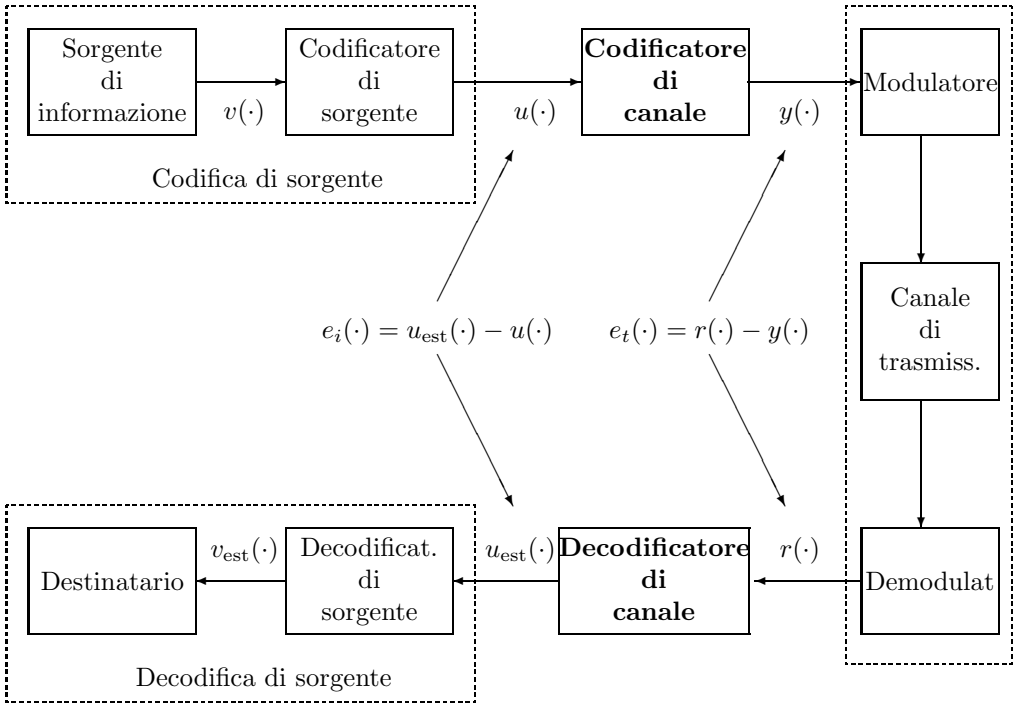

Fig. 7.1

Prima di trasmettere $u(\cdot)$ su un canale rumoroso, conviene ricorrere alla *codifica di canale*, che ha lo scopo di minimizzare il tasso di errore in sede di ricezione. Sulla base dei risultati di Shannon, infatti, dalle proprietà di un canale di comunicazione (larghezza di banda, potenza di segnale, livello di rumore) si può determinare la *capacità del canale* c, e finchè il tasso di trasmissione dell'

informazione è inferiore a c esiste una procedura di codifica di $u(\cdot)$ che permette di conseguire un'arbitraria accuratezza nell'informazione ricevuta.

Il *codificatore di canale* o, visto che non ci occuperemo di altre codifiche, semplicemente il *codificatore*, trasforma la sequenza di informazione in un'altra, $y(\cdot)$, che chiameremo la sequenza codificata o la *parola di codice*, appartenente ad un particolare insieme di sequenze, che chiameremo *codice*. Dal punto di vista realizzativo, i simboli discreti non sono adatti a essere trasmessi come tali su un canale fisico ed è pertanto necessario introdurre anche un *modulatore*, che trasformi ciascun simbolo di $u(\cdot)$ in una forma d'onda di durata T, adatta a essere immessa sul canale.

Durante la trasmissione, il segnale viene corrotto dal rumore e in sede di ricezione un *demodulatore* elabora l'uscita rumorosa del canale di trasmissione, riconvertendo ogni forma d'onda di durata T in un simbolo e quindi l'intero segnale analogico in una sequenza di simboli, la *sequenza ricevuta* $r(\cdot)$.

La sequenza ricevuta è in generale diversa da $y(\cdot)$, ovvero in generale non è nullo l'*errore di trasmissione*

$$e_t(\cdot) := r(\cdot) - y(\cdot)$$

La $r(\cdot)$ può essere ancora una parola di codice, diversa dalla parola di codice trasmessa $y(\cdot)$, oppure una sequenza non contenuta nel codice. Basandosi sulla conoscenza delle caratteristiche di rumore del canale e sulla struttura del codice, si implementa una procedura di stima per determinare dalla sequenza ricevuta $r(\cdot)$ una *stima* $y_{\text{est}}(\cdot)$ di $y(\cdot)$, che appartiene al codice e coincide con $r(\cdot)$ nel caso in cui essa già sia una parola di codice. Dalla $y_{\text{est}}(\cdot)$ si determina infine, con un procedimento di *decodifica*, la sequenza di informazione $u_{\text{est}}(\cdot)$ codificata da a $y_{\text{est}}(\cdot)$ e che idealmente dovrebbe costituire una replica della sequenza originale $u(\cdot)$. In realtà, se il rumore è abbastanza elevato, la stima $y_{\text{est}}(\cdot)$ sarà una parola di codice diversa da $y(\cdot)$ e conseguentemente non sarà nullo l'*errore di informazione*

$$e_i(\cdot) := u_{\text{est}}(\cdot) - u(\cdot).$$

Poichè la procedura di stima e quella di decodifica sono spesso inestricabilmente connesse, per semplicità chiameremo *decodificatore (di canale)* il dispositivo (o l'insieme dei dispositivi) che associano alla sequenza $r(\cdot)$ la $u_{\text{est}}(\cdot)$.

Per completare la descrizione del sistema, accenniamo al successivo *decodificatore di sorgente* che trasforma $u_{\text{est}}(\cdot)$ in una stima $v_{\text{est}}(\cdot)$ della sequenza originalmente prodotta dalla sorgente, introducendo, se del caso, una conversione digitale/analogica. Ma, nell'ottica in cui ci siamo posti, in questo capitolo non ci occuperemo della decodifica di sorgente.

7.2 Codici a blocchi

Come accennato nell'introduzione, oggi sono comunemente in uso due tipi di codici: i codici a blocchi e quelli convoluzionali. Anche se questo capitolo è dedicato ai codici convoluzionali, discuteremo prima succintamente quelli a blocchi, perché le definizioni e i concetti risultano formalmente piú semplici.

7.2.1 Struttura dei codici a blocchi

Nei codici a blocchi, il codificatore segmenta preliminarmente la sequenza di informazione in *blocchi* di lunghezza m, ciascuno comprendente m termini successivi della sequenza $u(\cdot)$. Il singolo blocco è un un vettore (o, più propriamente, una stringa quando le componenti non prendono valori in un campo) ad m componenti

$$\mathbf{u} = \begin{bmatrix} u_1 \\ \vdots \\ u_m \end{bmatrix},$$

che chiameremo *messaggio*. Se, come qui supporremo, le componenti del vettore prendono valori in un campo $\mathbb{F}$ con a elementi (e il caso di gran lunga più comune è quello in cui $a = 2$), sono possibili a^m messaggi distinti. A seguito di questa operazione di "compattazione" in blocchi, la sequenza di informazione si trasforma in una sequenza di messaggi vettoriali a m componenti (o equivalentemente nelle m sequenze "scalari" ottenibili da $u(\cdot)$ campionandone un campione ogni m).
La successiva operazione del codificatore è quella di trasformare ciascun messaggio $\mathbf{u} \in \mathbb{F}^m$, *indipendentemente da tutti gli altri che lo precedono o lo seguono*, in un vettore

$$\mathbf{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_p \end{bmatrix}$$

di $\mathbb{F}^p$, con $p \geq m$, che chiameremo *vettore di codice*. Perciò, a fronte degli a^m messaggi distinti, dobbiamo scegliere a^m distinti vettori di codice fra gli a^p vettori di $\mathbb{F}^p$ e specificare una *mappa di codifica* χ che associ iniettivamente a ciascun messaggio un vettore di codice. L' insieme $\mathbf{C}$ degli a^m vettori di codice è chiamato un *codice a blocchi* $[p, m]$ e il suo codificatore può essere implementato con un sistema senza memoria, i.e. con un circuito logico combinatorio, perché ogni vettore $\mathbf{y} \in \mathbf{C}$ è determinato da un singolo messaggio $\mathbf{u} \in \mathbb{F}^m$, e non anche dagli altri messaggi in cui la sequenza di informazione è stata suddivisa.

Il rapporto $R = m/p$, non può essere superiore a 1 per garantire che messaggi distinti possano essere codificati da vettori di codice distinti, ed è detto *rapporto*

del codice (code rate). Esso può essere interpretato come la frazione di bit di informazione entrante nel codificatore in corrispondenza a ciascun bit trasmesso in uscita. In realtà, perchè la codifica sia di una qualche utilità, si deve avere $p > m$, cosicché ciascun vettore di codice contiene $p - m$ simboli (nel caso $a = 2$, bit) in più rispetto al messaggio che esso codifica. Tale *ridondanza* attribuisce al codice la capacità di contrastare gli effetti introdotti dal rumore sul canale, correggendo gli errori eventualmente provocati.
Si noti che, per un fissato valore di R, i simboli ridondanti in ciascun vettore di codice possono essere accresciuti incrementando m, ovvere segmentando la sequenza di informazione in messaggi più lunghi. È intuibile, peraltro, che al crescere di m la complessità del codificatore possa divenire proibitiva se non si introducono opportune ipotesi strutturali sul codice e sulla mappa di codifica, perché si dovranno immagazzinare gli a^m vettori di codice sotto forma di dizionario. La più semplice condizione che usualmente si impone è quella che il codice $\mathbf{C}$ sia un sottospazio lineare, di dimensione m, di $\mathbb{F}^p$ e che la mappa di codifica χ sia lineare.
Per specificare un arbitrario codice lineare $\mathbf{C}$ di dimensione m entro $\mathbb{F}^p$ è sufficiente scegliere m vettori linearmente indipendenti $\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(m)}$ in $\mathbb{F}^p$ e considerare lo spazio da essi generato, ovvero lo spazio immagine della *matrice generatrice*

$$\mathbf{G} := [\, \mathbf{g}^{(1)} \quad \ldots \quad \mathbf{g}^{(m)} \,]$$

La mappa di codifica $\chi : \mathbb{F}^m \to \mathbf{C}$ associa a ciascun messaggio $\mathbf{e}^{(j)}$ della base canonica di $\mathbb{F}^m$ un vettore del codice $\mathbf{C}$, esprimibile come

$$\chi(\mathbf{e}^{(j)}) = \sum_{i=1}^{m} \mathbf{g}^{(i)} t_{ij} = \mathbf{G} \begin{bmatrix} t_{1j} \\ \vdots \\ t_{mj} \end{bmatrix}$$

Per linearità la mappa χ è allora completamente determinata: al generico messaggio $\mathbf{u} = \sum_{j=1}^{m} \mathbf{e}^{(j)} u_j$ corrisponderà il vettore di codice

$$\chi(\mathbf{u}) = \sum_{j=1}^{m} \mathbf{G} \begin{bmatrix} t_{1j} \\ \vdots \\ t_{mj} \end{bmatrix} u_j = \mathbf{G}T \begin{bmatrix} u_1 \\ \vdots \\ u_m \end{bmatrix}$$

dove $T := [t_{ij}]$ è una matrice invertibile perchè χ, essendo iniettiva, applica vettori linearmente indipendenti $\mathbf{e}^{(j)}$ in vettori $\chi(\mathbf{e}^{(j)})$ indipendenti. Ma allora

$$\hat{\mathbf{G}} := \mathbf{G}T$$

è ancora una matrice generatrice di $\mathbf{C}$, le cui colonne sono i vettori (indipendenti) di codice corrispondenti ai messaggi $\mathbf{e}^{(j)}$, e l'operazione eseguita dal codificatore è

quella di combinare linearmente le colonne di $\hat{\mathbf{G}}$ con le componenti del messaggio $\mathbf{u}$:

$$\mathbf{y} = \hat{\mathbf{G}}\mathbf{u}. \tag{7.1}$$

Nel seguito supporremo sempre che la base di $\mathbf{C}$ sia stata scelta in modo che valga la (7.1).

Un codificatore è detto *sistematico* quando, a meno di una permutazione delle sue righe, ha la struttura

$$\mathbf{G} = \begin{bmatrix} \mathbf{I}_m \\ \mathbf{P} \end{bmatrix} \tag{7.2}$$

ovvero quando la codifica di un messaggio $\mathbf{u}$ dà luogo ad un vettore di codice

$$\mathbf{y} = \begin{bmatrix} \mathbf{u} \\ \mathbf{P}\mathbf{u} \end{bmatrix} \tag{7.3}$$

le cui (prime) m componenti riproducono esattamente il messaggio stesso. Ciascuna delle ultime $p-m$ componenti è una combinazione lineare delle componenti di $\mathbf{u}$, e quindi l'immagine di un funzionale lineare sullo spazio $\mathbb{F}^m$ dei messaggi.

- **Esercizio 7.2.1** Si verifichi che per ogni codice $[p, m]$ lineare $\mathbf{C} \subset \mathbb{F}^p$ esiste un codificatore sistematico.

7.2.2 Dualita' e formazione della sindrome

Com'è noto, ad ogni sottospazio $\mathbf{C}$ di dimensione m in $\mathbb{F}^p$ può essere associato in modo unico il sottospazio ortogonale, di dimensione $p - m$,

$$\mathbf{C}^\perp := \{\tilde{\mathbf{y}} \in \mathbb{F}^p : \tilde{\mathbf{y}}^T\mathbf{y} = 0, \forall \mathbf{y} \in \mathbf{C}\}. \tag{7.4}$$

$\mathbf{C}^\perp$ può essere considerato a sua volta un codice lineare a blocchi $[p, p - m]$, e sarà detto il *codice duale* di $\mathbf{C}$. Esso ammette come matrice generatrice qualsiasi matrice in $\mathbb{F}^{p\times(p-m)}$ le cui colonne costituiscano una base per lo spazio ortogonale a quello generato dalle colonne di un codificatore $\mathbf{G}$ del codice $\mathbf{C}$.

Si osservi che codice $\mathbf{C}$ non solo determina univocamente il suo duale $\mathbf{C}^\perp$ ma, viceversa, ne è anche univocamente determinato, dal momento che $\mathbf{y} \in \mathbb{F}^p$ è un vettore del codice $\mathbf{C}$ se e solo se $\mathbf{y}$ risulta ortogonale a (una base di) $\mathbf{C}^\perp$, ovvero se, detta $\mathbf{S} \in \mathbb{F}^{p\times(p-m)}$ una matrice generatrice di $\mathbf{C}^\perp$, risulta

$$\mathbf{S}^T\mathbf{y} = \mathbf{0} \tag{7.5}$$

La matrice $\mathbf{S}^T$, trasposta di una generatrice del codice duale, si dice matrice dei *check di parità* o *formatore di sindrome* di $\mathbf{C}$. Essa associa ad ogni vettore $\mathbf{v} \in \mathbb{F}^p$ il vettore

$$\mathbf{s} = \mathbf{S}^T\mathbf{v} \in \mathbb{F}^{p-m} \tag{7.6}$$

detto la sindrome di $\mathbf{v}$. Per la (7.5), $\mathbf{v}$ è un vettore del codice $\mathbf{C}$ se e solo se la sua sindrome è nulla.

- **Esercizio 7.2.2** (*i*) Se $\mathbf{L} \in \mathbb{F}^{p\times(p-m)}$ è tale che $[\,\mathbf{G} \quad \mathbf{L}\,]$ sia invertibile, si individui nella matrice inversa una sottomatrice di check di parità per il codice generato da $\mathbf{G}$.

  (*ii*) Se $\mathbf{G} = \begin{bmatrix} \mathbf{I}_m \\ \mathbf{P} \end{bmatrix}$ è un codificatore sistematico, una matrice di check di parità per il codice generato da $\mathbf{G}$ è data da $\mathbf{S}^T = \begin{bmatrix} -\mathbf{P}^T \\ \mathbf{I}_m \end{bmatrix}$.

Se $\mathbf{y}$ è il vettore di codice trasmesso attraverso un canale rumoroso e se il vettore corrispondentemente ricevuto $\mathbf{r}$ è diverso da $\mathbf{y}$, l'*errore di trasmissione*

$$\mathbf{e}_t := \mathbf{r} - \mathbf{y} \tag{7.7}$$

risulterà non nullo. Essendo incogniti in sede di ricezione sia $\mathbf{e}_t$ che $\mathbf{y}$, il dispositivo di decodifica dovrà stabilire anzitutto se il vettore ricevuto $\mathbf{r}$ contiene errori di trasmissione, per procedere poi alla loro correzione o, eventualmente, alla richiesta di una nuova trasmissione del vettore $\mathbf{y}$.
A tale scopo, il formatore di sindrome $\mathbf{S}^T$ determina la sindrome

$$\mathbf{s} = \mathbf{S}^T\mathbf{r} = \mathbf{S}^T[\mathbf{e}_t + \mathbf{y}] = \mathbf{S}^T\mathbf{e}_t \tag{7.8}$$

del vettore ricevuto, ovvero la sindrome dell'errore di trasmissione. Si noti che $\mathbf{s}$ è nulla se e solo se il vettore ricevuto, o equivalentemente l'errore di trasmissione, è un vettore di $\mathbf{C}$. L'annullarsi della sindrome è condizione necessaria, ma non sufficiente, perchè $\mathbf{r}$ sia esente da errori di trasmissione: se $\mathbf{e}_t$ non è nullo, ma è una parola di codice, l'errore non può essere rivelato, né tanto meno corretto. Gli errori di trasmissione non rivelabili sono in numero di $a^m - 1$, tanti quanti i vettori di codice non nulli, e la loro presenza dà comunque luogo ad un *errore di decodifica*.
La situazione può essere illustrata più completamente considerando la "mappa di sindrome"

$$\mathcal{S} : \mathbb{F}^p \to \mathbb{F}^{p-m} : \mathbf{r} \mapsto \mathbf{S}^T\mathbf{r} = \mathbf{s}. \tag{7.9}$$

Essa è suriettiva ed ha per nucleo il codice $\mathbf{C}$, quindi può essere fattorizzata come segue

$$\begin{array}{ccc} \mathbb{F}^p & \xrightarrow{\mathcal{S}} & \mathbb{F}^{p-m} \\ & \pi \searrow \quad \nearrow \bar{\mathcal{S}} & \\ & \mathbb{F}^p/\mathbf{C} & \end{array}$$

con π proiezione canonica dello spazio $\mathbb{F}^p$ sul quoziente $\mathbb{F}^p/\mathbf{C}$ e $\bar{\mathcal{S}}$ un isomorfismo che applica la classe $\mathbf{r}+\mathbf{C}$ in $\mathbf{S}^T\mathbf{r}$. Ciascuna classe di equivalenza del quoziente contiene tutti i vettori ricevuti $\mathbf{r}\in\mathbb{F}^p$, e quindi (tenendo conto che le parole di codice producono sindrome nulla) tutti gli errori di trasmissione che inducono una medesima sindrome; in particolare, la classe $\mathbf{0}+\mathbf{C}$ contiene gli errori di trasmissione che inducono sindrome nulla, ovvero i vettori di codice. Ogni classe di equivalenza comprende a^m elementi.

Nota la sindrome $\mathbf{s}$ del vettore $\mathbf{r}$, i possibili errori di trasmissione sono *tutti e soli* quelli della classe di equivalenza $\bar{\mathcal{S}}^{-1}\mathbf{s}$ e un vettore di codice può essere ricavato da $\mathbf{r}$ se e solo se ad $\mathbf{r}$ si sottrae un elemento *qualsiasi* della classe di equivalenza. A questo punto si rende necessario introdurre un criterio per stimare qual è la parola di codice effettivamente trasmessa: dalla sindrome infatti siamo risaliti alla classe $\bar{\mathcal{S}}^{-1}\mathbf{s}$ dei possibili errori di trasmissione, ma ogni scelta di un errore entro la classe (e la sua sottrazione al vettore ricevuto) è formalmente compatibile con i dati a disposizione e con la sindrome prodotta.

Si noti che se $L\in\mathbb{F}^{p\times(p-m)}$ è un'arbitraria matrice inversa destra del formatore di sindrome $\mathbf{S}^T$, ovvero una matrice soddisfacente le condizione $\mathbf{S}^TL=I_{p-m}$, si ha

$$\bar{\mathcal{S}}[(L\mathbf{s})+\mathbf{C}]=\mathbf{S}^T(L\mathbf{s})=\mathbf{s}.$$

Quindi la classe di equivalenza $\bar{\mathcal{S}}^{-1}\mathbf{s}$ si esprime più concretamente come $(L\mathbf{s})+\mathbf{C}$ e potremmo pensare di scegliere il *rappresentante* $L\mathbf{s}$ della classe di equivalenza come termine correttivo da applicare a $\mathbf{r}$. Tale procedimento è soggetto ad una grave obiezione, che deriva dai fatti seguenti:

(i) sotto ipotesi abbastanza generali, si può provare che, quando $\mathbf{r}$ è il vettore ricevuto, gli errori di trasmissione più probabilmente intervenuti sono gli elementi della classe di equivalenza con minor numero di componenti non nulle;

(ii) il rappresentante $(L\mathbf{s})$ può avere un numero di componenti non nulle più elevato di altri vettori nella sua classe di equivalenza, e indurre quindi una correzione di $\mathbf{r}$ che coinvolge un numero di componenti più elevato di quello che si avrebbe utilizzando altri vettori nella classe.

Si rende quindi necessario un approccio più articolato (e complesso) al problema della decodifica, e, di riflesso, al problema di scegliere i codificatori. Accenneremo in proposito solo ad alcune definizioni e concetti elementari, che saranno ripresi in ambito convoluzionale.

7.2.3 Rivelazione e correzione degli errori di trasmissione

Definizione 7.2.1 *Se* $\mathbf{v}$ *è un vettore in* $\mathbb{F}^p$*, il peso di Hamming di* $\mathbf{v}$ *è il numero delle sue componenti non nulle , ovvero*

$$w_H(\mathbf{v}) = \text{card}\{i : i \in \{1, 2, \ldots, p\}, v_i \neq 0\}.$$

Se $\mathbf{v}$ *e* $\mathbf{u}$ *sono due vettori in* $\mathbb{F}^p$*, la loro distanza di Hamming è il numero delle componenti in cui i due vettori differiscono l'uno dall'altro, ovvero*

$$d_H(\mathbf{v}, \mathbf{u}) = \text{card}\{i : i \in \{1, 2, \ldots, p\}, v_i \neq u_i\}.$$

Verificando la diseguaglianza triangolare

$$d_H(\mathbf{v}, \mathbf{u}) \leq d_H(\mathbf{v}, \mathbf{w}) + d_H(\mathbf{w}, \mathbf{u}), \qquad \forall \mathbf{v}, \mathbf{u}, \mathbf{w} \in \mathbb{F}^p$$

è facile concludere che d_H è una metrica su $\mathbb{F}^p$. Poiché risulta, per ogni $\mathbf{x} \in \mathbb{F}^p$ e per ogni α non nullo in $\mathbb{F}$,

$$\begin{aligned} d_H(\mathbf{v}, \mathbf{u}) &= d_H(\mathbf{v} + \mathbf{x}, \mathbf{u} + \mathbf{x}) \\ d_H(\alpha\mathbf{v}, \alpha\mathbf{u}) &= d_H(\mathbf{v}, \mathbf{u}) \end{aligned} \tag{7.10}$$

si ha, per ogni α non nullo in $\mathbb{F}$,

$$d_H(\alpha\mathbf{v}, \alpha\mathbf{u}) = d_H(\mathbf{v} - \mathbf{u}, \mathbf{0}) = w_H(\mathbf{v} - \mathbf{u})$$

Dato un codice a blocchi $\mathbf{C} \subset \mathbb{F}^p$, la *minima distanza del codice* si definisce come la più piccola distanza fra due distinti vettori di $\mathbf{C}$:

$$d_{\min} = \min\{d_H(\mathbf{v}, \mathbf{u}),\ \mathbf{v}, \mathbf{u} \in \mathbf{C},\ \mathbf{v} \neq \mathbf{u}\} \tag{7.11}$$

Quando $\mathbf{C}$ è lineare, $\mathbf{v} - \mathbf{u}$ è ancora un vettore di $\mathbf{C}$ e la (7.26) può essere riscritta nella forma

$$d_{\min} = \min\{d_H(\mathbf{v}, \mathbf{0}),\ \mathbf{v} \in \mathbf{C}, \mathbf{v} \neq \mathbf{0}\} = \min\{w_H(\mathbf{v}),\ \mathbf{v} \in \mathbf{C}, \mathbf{v} \neq \mathbf{0}\} \tag{7.12}$$

ovvero $d_{\min}$ rappresenta il minimo fra i pesi di Hamming dei vettori non nulli del codice.

Proposizione 7.2.2 *Siano* $\mathbf{C}$ *un codice* $[p, m]$ *lineare a blocchi sul campo* $\mathbb{F}$ *e* $\mathbf{S}^T$ *un formatore di sindrome per* $\mathbf{C}$*.*

(i) per ogni $\ell \leq p$ *esistono* ℓ *colonne linearmente dipendenti in* $\mathbf{S}^T$ *se e solo se esiste un vettore non nullo con peso di Hamming minore o eguale a* ℓ *in* $\mathbf{C}$*;*

(ii) il numero minimo $\bar{\ell}$ di colonne linearmente dipendenti che si possono estrarre da $\mathbf{S}^T$ coincide con la minima distanza $d_{\min}$ del codice $\mathbf{C}$.

DIMOSTRAZIONE (i) Se il vettore $\mathbf{v} \in \mathbf{C}$ ha peso ℓ, ha esattamente ℓ componenti non nulle, in posizione $\nu_1, \nu_2, \ldots, \nu_\ell$. Dalla relazione

$$\mathbf{S}^T\mathbf{v} = 0$$

si ricava immediatamente che le ℓ colonne di indici $\nu_1, \nu_2, \ldots, \nu_\ell$ in $\mathbf{S}^T$ sono linearmente dipendenti.

D'altra parte, se nella matrice $\mathbf{S}^T$ le colonne $\mathbf{s}_{\mu_1}, \mathbf{s}_{\mu_2}, \ldots, \mathbf{s}_{\mu_\ell}$ sono linearmente dipendenti, esistono in $\mathbb{F}$ combinatori $\alpha_{\mu_1}, \alpha_{\mu_2}, \ldots, \alpha_{\mu_\ell}$, non tutti nulli, tali che

$$\alpha_{\mu_1}\mathbf{s}_{\mu_1} + \alpha_{\mu_2}\mathbf{s}_{\mu_2} + \ldots + \alpha_{\mu_\ell}\mathbf{s}_{\mu_\ell} = 0$$

e il codice contiene il vettore $\mathbf{v}$, con

$$v_i = \begin{cases} \alpha_i, & \text{se } i \in \{\mu_1, \mu_2, \ldots, \mu_\ell\} \\ 0, & \text{negli altri casi,} \end{cases}$$

ovvero un vettore con peso di Hamming al più ℓ.

(ii) Dalla definizione di $\bar{\ell}$ e per il ragionamento svolto al punto (i), in $\mathbf{C}$ esistono vettori non nulli con al più $\bar{\ell}$ componenti diverse da zero e quindi con peso di Hamming non superiore a $\bar{\ell}$. D'altra parte, se esistesse un vettore non nullo $\mathbf{v} \in \mathbf{C}$ con $w_H(\mathbf{v}) < \bar{\ell}$, da $\mathbf{S}^T$ si potrebbero estrarre $w_H(\mathbf{v}) < \bar{\ell}$ colonne linearmente dipendenti, contro la definizione di $\bar{\ell}$. Allora $\bar{\ell}$ è il minimo fra i pesi di Hamming dei vettori non nulli di $\mathbf{C}$, e coincide con $d_{\min}$. ■

- **Esercizio 7.2.3** Se $\mathbf{C}$ è un codice lineare sul campo $\mathbb{F}$ a due elementi

  (i) un vettore $\mathbf{v} \in \mathbb{F}^p$, con componenti unitarie in posizione i_1, i_2, i_r appartiene al codice lineare $\mathbf{C}$ se e solo se è nulla la somma delle colonne $\mathbf{s}_{i_1}, \mathbf{s}_{i_2}, \ldots, \mathbf{s}_{i_r}$ di $\mathbf{S}^T$.

  (ii) la distanza minima del codice coincide con il piu' piccolo numero di colonne a somma zero estraibili da $\mathbf{S}^T$.

  (ii) se nessuna k-upla di colonne di $\mathbf{S}^T$ ha somma zero, possiamo concludere che $d_{\min} > k$? (Suggerimento: si supponga che $\mathbf{S}^T$ abbia una sola colonna nulla e si ponga $k = 2$)

Quando la distanza minima di un codice $\mathbf{C}$ è $d_{\min}$, nessun errore di trasmissione $\mathbf{e}_t \neq \mathbf{0}$ con peso inferiore a $d_{\min}$ può cambiare un vettore di codice in un altro vettore di codice. Quindi, se la trasmissione di $\mathbf{v} \in \mathbf{C}$ sul canale rumoroso altera $\mathbf{v}$ in meno di $d_{\min}$ posizioni, il vettore ricevuto non sarà mai un vettore di $\mathbf{C}$, nel caso lineare la sua sindrome non sara' nulla, e comunque in ricezione sarà possibile *rivelare* la presenza di un errore di trasmissione. In altre parole, un codice a blocchi con distanza minima $d_{\min}$ permette la rivelazione di *ogni* errore di trasmissione che alteri il vettore trasmesso in non più di $d_{\min} - 1$ posizioni.

- **Esercizio 7.2.4** Si verifichi che gli errori di trasmissione con peso inferiore a $d_{\min}$ in un codice a blocchi $[p, m]$ su un campo di Galois con a elementi sono in numero pari a

$$\binom{p}{1}(a-1) + \binom{p}{2}(a-1)^2 + \cdots + \binom{p}{d_{\min}-1}(a-1)^{d_{\min}-1}$$

Il fatto che un codice a blocchi con distanza minima $d_{\min}$ permetta di rivelare *tutti* gli errori con peso inferiore a $d_{\min}$ non significa che esso non sia in grado di rivelarne altri, di peso maggiore o eguale a $d_{\min}$. Il punto è che, quando il peso dell'errore può essere maggiore o eguale a $d_{\min}$, qualche errore $\mathbf{e}_t$ non è più rivelabile. Per questo motivo , si dice che il codice ha *capacità di rivelazione di errore* pari a $d_{\min} - 1$.
Limitandoci a codici lineari, in un codice a blocchi $[p, m]$ su un campo di Galois con a elementi sono rivelabili tutti gli errori che non sono parole di codice (infatti essi inducono una sindrome diversa da zero). Il loro numero, pari a $a^p - a^m$, è in genere molto più grande di quello degli errori con peso inferiore a $d_{\min}$. Non sono invece rivelabili gli $a^m - 1$ errori non nulli che sono vettori del codice: se il rapporto di codice $R = m/p$ è mantenuto costante, al crescere di p il tasso degli errori non rivelabili diventa trascurabile. Esso è infatti

$$\frac{a^m - 1}{a^p - a^m} \simeq \frac{a^m}{a^p - a^m} \simeq a^{m-p} = a^{-p(1-R)}.$$

- **Esercizio 7.2.5** Si consideri il codice (non lineare) sul campo $\mathbb{F}$ a due elementi, costituito dai tre vettori di $\mathbb{F}^4$

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

Si determinino

(i) un vettore di errore appartenente a $\mathbf{C}$, ma la cui somma con qualche vettore di codice non appartenga a $\mathbf{C}$;

(ii) un vettore di errore non appartenente a $\mathbf{C}$, ma la cui somma con qualche vettore di codice appartenga a $\mathbf{C}$

Per quanto attiene alla *decodifica* di un codice lineare $[p, m]$ a blocchi $\mathbf{C}$, le varie strategie adottabili si riconducono al seguente schema di principio: poiché i vettori del codice sono a^m e i vettori che possono presentarsi in ricezione sono tutti gli a^p elementi di $\mathbb{F}^p$,

(i) a ciascun vettore $\mathbf{y}$ del codice si associa un sottoinsieme $D_{\mathbf{y}}$ di $\mathbb{F}^p$ contenente $\mathbf{y}$, in modo tale che la famiglia di sottoinsiemi $\{D_{\mathbf{y}}, \mathbf{y} \in \mathbf{C}\}$ costituisca una partizione di $\mathbb{F}^p$ in 2^m classi disgiunte ;

(ii) si decodifica un vettore $\mathbf{r} \in \mathbb{F}^p$ facendogli corrispondere l'unico vettore di codice $\mathbf{y}$ della classe $D_{\mathbf{y}}$ alla quale $\mathbf{r}$ appartiene.

Il problema sta evidentemente nel caratterizzare al meglio le classi $D_{\mathbf{y}}$ o, equivalentemente, la strategia che associa ad ogni vettore di $\mathbb{F}^p$ un vettore del codice.

Se α è un numero reale, denotiamo con $\lfloor \alpha \rfloor$ la *parte intera* di α, ovvero il più grande intero che non supera α, e per ogni $\mathbf{v} \in \mathbb{F}^p$ denotiamo con

$$S_H(\mathbf{v}, \alpha) := \{\mathbf{w} \in \mathbb{F}^p : d_H(\mathbf{v}, \mathbf{w}) \leq \alpha\}$$

la sfera di Hamming di raggio α e centro $\mathbf{v}$.
Per il codice lineare $\mathbf{C}$ introduciamo il parametro

$$\tau := \lfloor (d_{\min} - 1)/2 \rfloor, \tag{7.13}$$

che chiamiamo *capacità di correzione d'errore (casuale)* del codice.

Proposizione 7.2.3 *Se in un codice lineare a blocchi* $\mathbf{C}$ *l'errore di trasmissione* $\mathbf{e}_t$ *del vettore di codice* $\mathbf{y}$ *ha peso di Hamming minore o eguale a* τ*, allora il vettore ricevuto* $\mathbf{r} := \mathbf{y} + \mathbf{e}_t$ *appartiene alla sfera di Hamming*

$$S_H(\mathbf{y}, \tau) \tag{7.14}$$

e non appartiene a nessun altra sfera di Hamming di raggio τ *e centro in un vettore di codice diverso da* $\mathbf{y}$*.*

DIMOSTRAZIONE La prima parte è conseguenza della definizione della sfera (7.14), che è l' insieme di tutti i vettori di $\mathbb{F}^p$ che hanno distanza da $\mathbf{v}$ non superiore a τ.
Se $\mathbf{r}$ appartenesse anche alla sfera $S_H(\mathbf{y}', \tau)$, con $\mathbf{y} \neq \mathbf{y}' \in \mathbf{C}$, sarebbe

$$d_H(\mathbf{y}, \mathbf{y}') \leq d_H(\mathbf{y}, \mathbf{r}) + d_H(\mathbf{r}, \mathbf{y}') \leq 2\tau < d_{\min}, \tag{7.15}$$

e avremmo due vettori distinti di $\mathbf{C}$ con distanza inferiore alla minima del codice. ■

La proposizione precedente afferma che, quando l'errore di trasmissione $\mathbf{e}_t$ ha peso non superiore a τ, il vettore ricevuto $\mathbf{r} = \mathbf{y} + \mathbf{e}_t$ è più vicino al vettore $\mathbf{y}$ inizialmente trasmesso piuttosto che ad ogni altro vettore di $\mathbf{C}$. Ovviamente, in ricezione si ha a disposizione soltanto il vettore $\mathbf{r}$ e non si sa quale sia il peso dell'errore $\mathbf{e}_t$ e meno ancora quale sia il corretto vettore di codice . Tuttavia, quando $\mathbf{r}$ appartiene ad una sfera di Hamming (7.14) centrata in qualche vettore di codice $\mathbf{y}$ e il canale è binario e simmetrico, allora la probabilità che il vettore di codice originariamente trasmesso sia proprio il centro sfera $\mathbf{y}$ supera quella che esso sia ogni altro vettore $\mathbf{y}'$ di $\mathbf{C}$.

E' chiaro allora che per ogni $\mathbf{y} \in \mathbf{C}$ la classe $D_{\mathbf{y}}$ deve contenere la sfera di Hamming (7.14) centrata nel vettore di codice $\mathbf{y}$. Per ottenere questo risultato, possiamo enumerare gli a^m vettori di codice:

$$\mathbf{0} = \mathbf{y}_1, \quad \mathbf{y}_2, \quad \mathbf{y}_3, \quad \ldots, \quad \mathbf{y}_{a^m}$$

e i q vettori contenuti nella sfera di Hamming $S_H(\mathbf{0}, \tau)$:

$$\mathbf{0} = \mathbf{e}_1, \quad \mathbf{e}_2, \quad \mathbf{e}_3, \quad \ldots, \quad \mathbf{e}_q$$

Si costruiscono poi le q righe della seguente tabella:

$$\begin{array}{ccccc} \mathbf{0} = \mathbf{y}_1 & \mathbf{y}_2 & \mathbf{y}_3 & \ldots & \mathbf{y}_{a^m} \\ \mathbf{e}_2 & \mathbf{y}_2 + \mathbf{e}_2 & \mathbf{y}_3 + \mathbf{e}_2 & \ldots & \mathbf{y}_{a^m} + \mathbf{e}_2 \\ \mathbf{e}_3 & \mathbf{y}_2 + \mathbf{e}_3 & \mathbf{y}_3 + \mathbf{e}_3 & \ldots & \mathbf{y}_{a^m} + \mathbf{e}_3 \\ & \ldots & \ldots & \ldots & \\ \mathbf{e}_q & \mathbf{y}_2 + \mathbf{e}_q & \mathbf{y}_3 + \mathbf{e}_q & \ldots & \mathbf{y}_{a^m} + \mathbf{e}_q \end{array}$$

nella quale nessun vettore di $\mathbb{F}^q$ figura due o più volte, grazie alla proposizione precedente. In generale, i vettori della tabella non esauriscono $\mathbb{F}^q$, ovvero le sfere di Hamming con raggio pari alla capacita' di correzione d'errore τ non costituiscono una copertura di $\mathbb{F}^q$. Si può allora completare la tabella scegliendo un vettore $\mathbf{e}_{q+1}$ *non presente nelle righe già completate*,costruire la riga $(q+1)$-esima

$$\mathbf{e}_{q+1} \quad \mathbf{y}_2 + \mathbf{e}_{q+1} \quad \mathbf{y}_3 + \mathbf{e}_{q+1} \quad \ldots \quad \mathbf{y}_{a^m} + \mathbf{e}_{q+1},$$

e così via, fino ad esaurire lo spazio $\mathbb{F}^q$. Anche in questa fase nessun vettore viene ripetuto nella lista: se un vettore $\mathbf{r}$ soddisfacesse le eguaglianze

$$\mathbf{r} = \mathbf{y}_i + \mathbf{e}_h = \mathbf{y}_j + \mathbf{e}_k$$

dovrebbe essere $h \neq k$, perché i vettori di una stessa riga della tabella sono tutti distinti; supponendo p.es. che k sia maggiore di h, si avrebbe

$$\mathbf{e}_k = (\mathbf{y}_i - \mathbf{y}_j) + \mathbf{e}_h$$

Ma ciò è assurdo: $\mathbf{y}_i - \mathbf{y}_j$ è un vettore di codice e quindi $(\mathbf{y}_i - \mathbf{y}_j) + \mathbf{e}_h$, figurando già nella h-esima riga della tabella, non sarebbe stato scelto come iniziale di un'ulteriore riga. Lo stesso ragionamento (o un ragionamento di cardinalità) mostra anche che l'ultima riga della tabella, la a^{p-m}-esima, e' una riga completa:

$$\begin{array}{ccccc} \mathbf{0} = \mathbf{y}_1 & \mathbf{y}_2 & \mathbf{y}_3 & \ldots & \mathbf{y}_{a^m} \\ \mathbf{e}_2 & \mathbf{y}_2 + \mathbf{e}_2 & \mathbf{y}_3 + \mathbf{e}_2 & \ldots & \mathbf{y}_{a^m} + \mathbf{e}_2 \\ \mathbf{e}_3 & \mathbf{y}_2 + \mathbf{e}_3 & \mathbf{y}_3 + \mathbf{e}_3 & \ldots & \mathbf{y}_{a^m} + \mathbf{e}_3 \\ & \ldots & \ldots & \ldots & \\ \mathbf{e}_{a^{p-m}} & \mathbf{y}_2 + \mathbf{e}_{a^{p-m}} & \mathbf{y}_3 + \mathbf{e}_{a^{p-m}} & \ldots & \mathbf{y}_{a^m} + \mathbf{e}_{a^{p-m}} \end{array} \tag{7.16}$$

Alla tabella (7.16) così ottenuta corrispondono due partizioni di $\mathbb{F}^p$, a seconda che la si guardi per righe o per colonne.

Le a^{p-m} classi che hanno per elementi i vettori di una stessa riga sono le classi di equivalenza del quoziente $\mathbb{F}^p/\mathbf{C}$ e corrispondono biunivocamente alle sindromi del codice: per ogni classe di equivalenza, la prima colonna fornisce un rappresentante (detto anche, in questo contesto, *leader*), che nel processo di decodifica sarà interpretato come la correzione da apportare al vettore ricevuto per ottenere il vettore di codice.

D'altra parte, se per $i = 1, 2, \ldots, a^m$ denotiamo con $D_{\mathbf{y}_i}$ l' insieme costituito dagli elementi che figurano nelle colonna avente $\mathbf{y}_i$ come primo elemento, otteniamo una diversa partizione di $\mathbb{F}^p$, in a^m classi, ciascuna contenente un solo vettore di $\mathbf{C}$. Il criterio di decodifica associato a quest'ultima partizione è quello sostituire il vettore $\mathbf{y}_i$ iniziale di colonna a tutti i vettori contenuti in $D_{\mathbf{y}_i}$.

- **Esercizio 7.2.6** Nello spazio quoziente $\mathbb{F}^p/\mathbf{C}$ si scelga una base $\mathbf{r}_1+\mathbf{C}, \mathbf{r}_2+\mathbf{C}, \ldots, \mathbf{r}_{p-m}+\mathbf{C}$ e si consideri il sottospazio $\mathbf{D} := \langle \mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{p-m} \rangle$ di $\mathbb{F}^p$ generato dai rappresentanti delle classi di equivalenza.

  (i) Ogni classe di equivalenza in $\mathbb{F}^p/\mathbf{C}$ è esprimibile nella forma $d_j + \mathbf{C}$, dove d_j è un elemento univocamente individuato di $\mathbf{D}$.

  (ii) Se $\mathbf{D}$ è un arbitrario sottospazio di $\mathbb{F}^p$ soddisfacente $F^p = \mathbf{C} \oplus \mathbf{D}$ e se $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{p-m}$ è una base di $\mathbf{D}$, allora $\mathbf{r}_1 + \mathbf{C}, \mathbf{r}_2 + \mathbf{C}, \ldots, \mathbf{r}_{p-m} + \mathbf{C}$ è una base del quoziente $\mathbb{F}^p/\mathbf{C}$ e $\mathbf{D}$ è un insieme di rappresentanti (leaders) delle classi di equivalenza.

  (ii) quali potrabbero essere gli inconvenienti a scegliere $\mathbf{D}$ come insieme di leaders , invece dell'insieme $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \ldots, \mathbf{e}_{a^{p-m}}$ utilizzato nella tabella (7.16)?

7.3 Codici e codificatori convoluzionali

Condideriamo dapprima un codice lineare a blocchi $[p, m]$, con matrice generatrice $\mathbf{G} \in \mathbb{F}^{p \times m}$, e associamo alla successione dei vettori di informazione

$$\ldots, \mathbf{u}(-k), \mathbf{u}(-k+1), \ldots, \mathbf{u}(0), \mathbf{u}(1), \ldots \tag{7.17}$$

(che supporremo sempre compatta a sinistra) la serie formale nell'operatore di ritardo d

$$\hat{\mathbf{u}}(d) = \sum_t \mathbf{u}(t) d^t$$

Essa è un elemento dell' $\mathbb{F}$-spazio $\mathbb{F}^m((d))$ delle serie formali a coefficienti in $\mathbb{F}^m$, ma può essere considerata anche un vettore dello spazio vettoriale $\mathbb{F}((d))^m$ sul

campo $\mathbb{F}((d))$ ponendo

$$\hat{\mathbf{u}}(d) = \begin{bmatrix} \sum_t u_1(t)d^t \\ \sum_t u_2(t)d^t \\ \vdots \\ \sum_t u_m(t)d^t \end{bmatrix}$$

La corrispondente successione dei vettori di codice

$$\ldots, \mathbf{y}(-k), \mathbf{y}(-k+1), \ldots, \mathbf{y}(0), \mathbf{y}(1), \ldots,$$

ovvero, in notazione seriale, la serie

$$\hat{\mathbf{y}}(d) = \begin{bmatrix} \sum_t y_1(t)d^t \\ \sum_t y_2(t)d^t \\ \vdots \\ \sum_t y_p(t)d^t \end{bmatrix} \in \mathbb{F}((d))^p$$

è la *parola di codice* che codifica la successione (7.17). Il legame fra $\hat{\mathbf{u}}(d)$ e $\hat{\mathbf{y}}(d)$ è dato da

$$\hat{\mathbf{y}}(d) = \mathbf{G}\hat{\mathbf{u}}(d),$$

e, al variare di $\hat{\mathbf{u}}(d)$ in $\mathbb{F}((d))^m$, le parole di codice $\mathbf{G}\hat{\mathbf{u}}(d)$ descrivono un $\mathbb{F}((d))$-sottospazio di $\mathbb{F}((d))^p$, di dimensione m, che fornisce un primo, banale, esempio di codice convoluzionale. Diciamo "banale" perché. come vedremo, esso corrisponde al caso limite in cui ciascun vettore $\mathbf{y}(t)$ nella parola di codice $\hat{\mathbf{y}}(d)$ dipende unicamente dal contemporaneo vettore di informazione $\mathbf{u}(t)$ nella serie $\hat{\mathbf{u}}(d)$. In questo caso, la trasformazione lineare (il "codificatore") che mappa la serie di informazione $\hat{\mathbf{u}}(d)$ nella parola di codice $\hat{\mathbf{y}}(d)$ è rappresentata da una matrice $\mathbf{G}$ a coefficienti in $\mathbb{F}$, e il codice convoluzionale è un sottospazio di $\mathbb{F}((d))^p$ con una base (le colonne di $\mathbf{G}$) costituita da vettori di $\mathbb{F}^p$.
Veniamo ora alla definizione generale di codice convoluzionale:

Definizione 7.3.1 *Un codice convoluzionale $[p, m]$ sul campo $\mathbb{F}$ è un $\mathbb{F}((d))$-sottospazio $\mathcal{C}$ di $\mathbb{F}((d))^p$, di dimensione m e avente una base di vettori appartenenti a $\mathbb{F}(d)^p$.*

In altri termini, le parole di un codice convoluzionele $[p, m]$ si ottengono combinando con arbitrarie serie formali m colonne razionali $\hat{\mathbf{g}}_1(d), \hat{\mathbf{g}}_2(d), \ldots, \hat{\mathbf{g}}_m(d)$ a p componenti, linearmente indipendenti rispetto al campo $\mathbb{F}(d)$ (o, equivalentemente, indipendenti rispetto al campo $\mathbb{F}((d))$). Se giustapponiamo in una matrice $G(d)$ le colonne $\hat{\mathbf{g}}_i(d)$ che formano una base per $\mathcal{C}$, gli elementi del codice (le "parole" del codice) sono gli elementi dello spazio immagine di $G(d)$, quando la matrice opera sullo spazio $\mathbb{F}((d))^m$.

Definizione 7.3.2 *Ogni matrice $G(d) \in \mathbb{F}(d)^{p\times m}$ di rango m le cui colonne sono una base per il codice convoluzionale $\mathcal{C}$ si dice* codificatore *o* matrice generatrice *di $\mathcal{C}$.*
Due matrici razionali $\tilde{G}(d)$ e $G(d)$ in $\mathbb{F}(d)^{p\times m}$ sono codificatori equivalenti *se sono codificatori del medesimo codice convoluzionale.*

- **Esercizio 7.3.1** Si considerino gli $\mathbb{F}((d))$- spazi immagine delle seguenti matrici

$$G_1(d) = \begin{bmatrix} de^d \\ e^d \end{bmatrix}, \quad G_2(d) = \begin{bmatrix} de^d \\ d \end{bmatrix}, \quad G_3(d) = \begin{bmatrix} \sin(d) \\ \cos(d) \end{bmatrix}$$

  Quali fra essi sono codici convoluzionali?

Riuniamo nella seguente proposizione alcuni semplici fatti riguardanti la famiglia dei codificatori di un medesimo codice convoluzionale $[p, m]$.

Proposizione 7.3.3 *Sia $\mathcal{C}$ un codice convoluzionale $[p, m]$ e sia $G(d) \in \mathbb{F}(d)^{p\times m}$ un suo codificatore.*
(i) Sono codificatori equivalenti di $\mathcal{C}$ tutte e sole le matrici

$$G'(d) = G(d)T(d), \tag{7.18}$$

al variare di $T(d)$ nel gruppo delle matrici $m \times m$ invertibili a elementi in $\mathbb{F}(d)$;
(ii) fra i codificatori di $\mathcal{C}$, ne esistono sempre di propri (o causali*);*
(iii) Fra i codificatori propri di $\mathcal{C}$, ne esistono sempre di polinomiali;
*(iv) Fra i codificatori polinomiali di $\mathcal{C}$, ne esistono sempre di primi a destra (*codificatori basici*);*
*(v) Fra i codificatori polinomiali di $\mathcal{C}$, ne esistono sempre di ridotti per colonne (*codificatori ridotti*);*
(vi) Il numeratore $N(d)$ di ogni RMF destra $N(d)D(d)^{-1}$ di $G(d)$ è ancora un codificatore di $\mathcal{C}$.

Dimostrazione (i) Se vale la (7.18) e se $\hat{\mathbf{y}}(d)$ è una parola di $\mathcal{C}$, esiste una serie di informazione $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$ tale che $\hat{\mathbf{y}}(d) = G(d)\hat{\mathbf{u}}(d)$. Ponendo $\hat{\mathbf{u}}'(d) := T(d)^{-1}\hat{\mathbf{u}}(d)$ si ricava $\hat{\mathbf{y}}(d) = G'(d)\hat{\mathbf{u}}'(d)$ e quindi ogni parola di codice è generabile da $G'(d)$. Viceversa ogni serie nell'immagine di $G'(d)$ è generabile da $G(d)$ e pertanto è una parola di codice. Ma allora tutte le matrici fornite da (7.18) sono codificatori di $\mathcal{C}$.
Supponiamo ora che $G'(d)$ sia un codificatore equivalente a $G(d)$ e proviamo che esiste una matrice razionale invertibile $T(d)$ che soddisfa (7.18). È chiaro che (gli sviluppi in serie del)le colonne di $G'(d)$ sono parole di $\mathcal{C}$ e quindi esiste una matrice $\tilde{T}(d)$, $m \times m$, a elementi in $\mathbb{F}((d))$ per cui risulta

$$G'(d) = G(d)\tilde{T}(d) \tag{7.19}$$

La matrice $G(d)$, razionale e con rango di colonna pieno m, ammette un'inversa sinistra razionale, ovvero esiste $L(d) \in \mathbb{F}(d)^{m\times p}$ soddisfacente $L(d)G(d) = I_m$. Basta allora premoltiplicare entrambi i membri di (7.19) per $L(d)$ e si conclude che $\tilde{T}(d)$ è razionale. Similmente, $G'(d)$ ammette un'inversa sinistra razionale $L'(d)$, e premoltiplicando entrambi i membri di (7.19) per $L'(d)$ si conclude che $\tilde{T}(d)$ è invertibile.

(ii) e (iii) Si esprime $G(d)$ come frazione matriciale destra $G(d) = N(d)D(d)^{-1}$ e in (7.18) si sceglie $T(d) = D(d)$. Si ottiene così un codificatore polinomiale e quindi, in particolare, razionale proprio.

(iv) Se $G(d)$ è polinomiale, ma non prima a destra, la si fattorizza nella forma

$$G(d) = \bar{G}(d)\Delta(d)$$

con $\Delta(d)$ quadrata polinomiale di rango pieno e con $\bar{G}(d)$ prima a destra. È chiaro che $\bar{G}(d) = G(d)\Delta(d)^{-1}$ è ancora un codificatore di $\mathcal{C}$, ed ha le proprietà volute.

(v) Se $G(d)$ è polinomiale, esiste una matrice unimodulare $U(d)$ tale che $\tilde{G}(d) = G(d)U(d)$ sia ridotta per colonne.

(vi) Ovvio. ■

- **Esercizio 7.3.2** Se $N(d)$ è un codificatore polinomiale primo a destra, ogni codificatore equivalente ha una RMF destra $\tilde{N}(d)\tilde{D}(d)^{-1}$ con $\tilde{N}(d) = N(d)\Delta(d)$ e $\Delta(d)$ polinomiale di rango m (Suggerimento: deve essere $\tilde{N}(d)\tilde{D}(d)^{-1} = N(d)T(d)$ con $T(d)$ razionale; allora in $\tilde{N}(d) = N(d)[T(d)\tilde{D}(d)]$ la matrice $[T(d)\tilde{D}(d)]$ è polinomiale).

7.4 Codificatori polinomiali

I *codificatori basici* del codice convoluzionale $\mathcal{C}$ sono quelli rappresentati da matrici polinomiali prime a destra. Per essi valgono quindi tutte le caratterizzazioni riportate nella Proposizione 3.3.3.

È naturale chiedersi quale relazione intercorra fra due codificatori basici del medesimo codice $\mathcal{C}$. La risposta, forse non inaspettata, è la seguente:

Proposizione 7.4.1 *Le matrici polinomiali prime a destra $G_1(d)$ e $G_2(d)$ sono codificatori basici del medesimo codice convoluzionale $\mathcal{C}$ se e solo se differiscono per un fattore destro unimodulare. Quindi i codificatori basici di $\mathcal{C}$ hanno tutti il medesimo grado interno.*

DIMOSTRAZIONE Se $U(d) \in \mathbb{F}[d]^{m\times m}$ è unimodulare e

$$G_2(d) = G_1(d)U(d),$$

è evidente l'equivalenza dei codificatori.
Viceversa, se $G_1(d)$ e $G_2(d)$ sono basici ed equivalenti, esiste $T(d)$ razionale di rango m per cui vale

$$G_2(d) = G_1(d)T(d) \tag{7.20}$$

Poiché $G_1(d)$ è prima a destra e $G_2(d)$ è polinomiale, anche $T(d)$ è polinomiale. Ma allora dalla primalità di $G_2(d)$ segue che in (7.20) il fattore destro $T(d)$ è unimodulare. ■

Un *codificatore ridotto* $G(d)$ del codice $\mathcal{C}$ è una matrice polinomiale (non necessariamente prima a destra) ridotta per colonne. Per esso valgono allora le caratterizzazioni delle Proposizioni 3.5.5 (rango pieno di G_{hc}) e 3.5.7 (predicibilità del grado). Un codificatore ridotto $G(d)$ ha somma dei gradi di colonna (i.e. il grado esterno) non superiore a quello di ogni altro codificatore del tipo $G(d)U(d)$, al variare di $U(d)$ nel gruppo delle matrici unimodulari $m \times m$, e coincidente con il grado interno di $G(d)$, ovvero con il grado massimo dei suoi minori di ordine m.
Si noti che i codificatori ridotti di $\mathcal{C}$ non hanno tutti il medesimo grado esterno: per convincersene, basta prendere due codificatori polinomiali $G_1(d)$ e $G_2(d)$ con gradi interni n_1 e n_2 diversi (p.es. uno primo a destra e l'altro no) e ridurli per colonne applicando alla loro destra opportune matrici unimodulari $U_1(d)$ e $U_2(d)$. Poiché

$$\tilde{G}_1(d) = G_1(d)U_1(d) \quad \text{e} \quad \tilde{G}_2(d) = G_2(d)U_2(d)$$

hanno gradi interni n_1 e n_2 coincidenti con gli esterni, i codificatori ridotti $\tilde{G}_1(d)$ e $\tilde{G}_1(d)$ hanno gradi esterni diversi.
Fra i codificatori polinomiali di $\mathcal{C}$, quelli per cui è minimo il grado esterno vengono chiamati *codificatori canonici*.

Proposizione 7.4.2 *Siano $\mathcal{C}$ un codice convoluzionale $[p, m]$ e $G(d)$ un suo codificatore polinomiale. Si equivalgono i seguenti fatti:*

(i) $G(d)$ è canonico, ovvero ha grado esterno minimo fra tutti i codificatori polinomiali di $\mathcal{C}$,

(ii) $G(d)$ è un codificatore basico e ridotto

Inoltre tutti i codificatori canonici di $\mathcal{C}$ hanno il medesimo insieme di gradi di colonna.

DIMOSTRAZIONE $(i) \Rightarrow (ii)$ Se $G(d)$ è canonico, deve essere ridotto, ovvero deve essere $\text{intdeg}G = \text{extdeg}G$, altrimenti si potrebbe diminuirne il grado esterno postmoltiplicando $G(d)$ per una opportuna matrice unimodulare. Ma deve

essere anche basico, sennò si potrebbe fattorizzarlo come $G(d) = G_1(d)\Delta(d)$ con $\deg\det\Delta > 0$ e ridurre per colonne $G_1(d)$, ottenendo il nuovo codificatore

$$G_2(d) = G_1(d)U(d)$$

con

$$\text{extdeg}G_2 = \text{intdeg}G_2 = \text{intdeg}G_1 < \text{intdeg}G = \text{extdeg}G$$

e ciò contro l'ipotizzata minimalità del grado esterno di $G(d)$ fra tutti i codificatori polinomiali di $\mathcal{C}$.
$(ii) \Rightarrow (i)$ Se $G(d)$ è basico e ridotto e $\tilde{G}(d)$ è un arbitrario codificatore polinomiale, esiste una matrice razionale $T(d)$ per cui risulta

$$\tilde{G}(d) = G(d)T(d),$$

e la primalità a destra di $G(d)$ implica che $T(d)$ è polinomiale. Risulta allora

$$\text{extdeg}\tilde{G} \geq \text{intdeg}\tilde{G} = \text{intdeg}G + \deg\det T \geq \text{intdeg}G = \text{extdeg}G$$

e il grado esterno di $G(d)$ è il minimo fra quelli dei codificatori polinomiali di $\mathcal{C}$.

Infine, se $G_1(d)$ e $G_2(d)$ sono codificatori canonici di $\mathcal{C}$, differiscono per un fattore unimodulare perché sono basici. Basta allora applicare la Proposizione 3.5.10 per concludere che i gradi di colonna dei due codificatori sono gli stessi, a meno di una permutazione. ■

Definizione 7.4.3 *Sia $\mathcal{C}$ un codice convoluzionale $[p, m]$. Il grado (interno ed esterno) di un arbitrario codificatore canonico di $\mathcal{C}$ si dice* grado del codice *e si denota con* deg$\mathcal{C}$.
I gradi di colonna di un codificatore canonico si chiamano indici di Forney *del codice.*
Il massimo indice di Forney si dice memoria *del codice.*

Si noti che il grado del codice e gli indici di Forney, qui definiti con riferimento a un codificatore (canonico), sono parametri propri del codice. Vedremo nel seguito qual è il loro significato intrinseco.

In generale deg$\mathcal{C}$ sarà denotato con la lettera n, e ci riferiremo a un codice convoluzionale $[p, m]$ di grado n coma a un codice $[p, m, n]$.

7.5 Codificatori catastrofici

Riprendiamo in esame la procedura che abbiamo descritto nel primo paragrafo, per passare dalla sequenza $\mathbf{r}(\cdot)$ ricevuta in uscita dal canale di trasmissione alla stima della sequenza di informazione $\mathbf{u}_{\text{est}}(\cdot)$. Concettualmente i passi da compiere sono due:

il primo richiede di valutare la parola di codice che, corrotta dal rumore di canale, ha dato luogo a $\mathbf{r}(\cdot)$; si deve cioè ottenere dalla serie $\hat{\mathbf{r}}(d)$, associata alla sequenza ricevuta, una serie $\hat{\mathbf{y}}_{\text{est}}(d)$ che appartenga al codice $\mathcal{C}$ e che costituisca, in base a criteri statistici di cui ora non ci occuperemo, una buona stima di $\hat{\mathbf{y}}(d)$, la parola di codice che è stata immessa sul canale;

il secondo richiede di applicare alla stima $\hat{\mathbf{y}}_{\text{est}}(d)$ la mappa inversa di quella di codifica, ottenendo una stima $\hat{\mathbf{u}}_{\text{est}}(d)$ di $\hat{\mathbf{u}}(d)$.

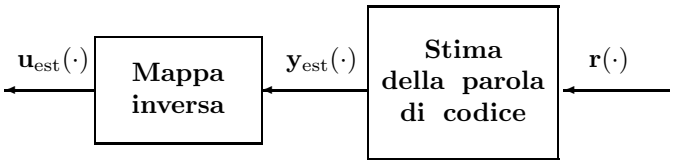

Fig. 7.2

Dal punto di vista formale, la determinazione della mappa inversa non comporta difficoltà: se $G(d) \in \mathbb{F}(d)^{p\times m}$ è il codificatore, di rango m, ogni matrice razionale $L(d) \in \mathbb{F}(d)^{m\times p}$, inversa sinistra di $G(d)$, i.e. soddisfacente

$$L(d)G(d) = I_m \tag{7.21}$$

soddisfa allo scopo.
Se la stima $\hat{\mathbf{y}}_{\text{est}}(d)$ coincide con la parola di codice $\hat{\mathbf{y}}(d)$, ovvero se l'*errore sulla parola di codice stimata*

$$\hat{\mathbf{e}}_c(d) := \hat{\mathbf{y}}_{\text{est}}(d) - \hat{\mathbf{y}}(d)$$

è nullo, allora è nullo anche l'*errore di informazione*

$$\hat{\mathbf{e}}_i(d) := \hat{\mathbf{u}}_{\text{est}}(d) - \hat{\mathbf{u}}(d)$$

Se $\hat{\mathbf{e}}_c(d)$ non è nullo, esso è una parola di codice (in quanto differenza di due parole di codice) e l'errore di informazione $\hat{\mathbf{e}}_i(d)$ corrispondente è la sequenza di informazione che il codificatore $G(d)$ codifica in $\hat{\mathbf{e}}_c(d)$. Risulta infatti

$$\hat{\mathbf{e}}_i(d) = \hat{\mathbf{u}}_{\text{est}}(d) - \hat{\mathbf{u}}(d) = L(d)(\hat{\mathbf{y}}_{\text{est}}(d) - \hat{\mathbf{y}}(d)) = L(d)\hat{\mathbf{e}}_c(d)$$

e quindi

$$G(d)\hat{\mathbf{e}}_i(d) - \hat{\mathbf{e}}_c(d) = [G(d)L(d) - I_p]\hat{\mathbf{e}}_c(d). \tag{7.22}$$

Poiché $\hat{\mathbf{e}}_c(d)$ è una parola di codice e quindi esprimibile come $G(d)\hat{\mathbf{v}}(d)$, da (7.22) e da (7.21) si ricava

$$G(d)\hat{\mathbf{e}}_i(d) - \hat{\mathbf{e}}_c(d) = [G(d)L(d) - I_p]G(d)\hat{\mathbf{v}}(d) = [G(d)[L(d)G(d)] - G(d)]\hat{\mathbf{v}}(d) = 0,$$

ovvero l'errore sulla parola di codice $\hat{\mathbf{e}}_c(d)$ coincide con la codifica dell'errore $G(d)\hat{\mathbf{e}}_i(d)$ di informazione risultante.
Se la parola di codice $\mathbf{e}_c(\cdot)$ ha supporto finito (i.e. se $\hat{\mathbf{e}}_c(d)$ è un polinomio di Laurent), ma la sequenza di informazione $\mathbf{e}_i(\cdot)$ che viene codificata in $\mathbf{e}_c(\cdot)$ ha supporto infinito (i.e. se la serie $\hat{\mathbf{e}}_i(d)$ ha infiniti coefficienti non nulli), diremo che si è verificata una *decodifica catastrofica*: un errore di stima che, a livello di codice, riguarda un numero finito di campioni, dà luogo ad un errore di informazione contenente infiniti campioni e quindi di durata infinita.

Una tale eventualità può presentarsi se e solo se il codificatore $G(d)$ è in grado di codificare qualche sequenza a supporto infinito (rappresentata quindi da una serie formale $\hat{\mathbf{u}}(d)$ non polinomiale) in una parola di codice a supporto finito (rappresentata da $\hat{\mathbf{y}}(d) = G(d)\hat{\mathbf{u}}(d)$ polinomiale di Laurent).
I codificatori polinomiali, eventualmente di Laurent, non sono catastrofici se e solo se sono primi a destra, e ogni codice ammette codificatori siffatti, per quanto si è visto nella Proposizione 7.3.3 . Esistono tuttavia codificatori non catastrofici che non sono polinomiali, come indicato nella proposizione seguente.

Proposizione 7.5.1 *Sia $G(d) \in \mathbb{F}(d)^{p\times m}$ un codificatore del codice convoluzionale $\mathcal{C}$. Sono allora fatti equivalenti :*

1. [non catastroficità di $G(d)$] *Se $G(d)\hat{\mathbf{u}}(d)$ è polinomiale di Laurent, anche $\hat{\mathbf{u}}(d)$ lo è.*
2. *In ogni RMF destra irriducibile su $\mathbb{F}[d, d^{-1}]$ del codificatore*
$$G(d) = N(d, d^{-1})D(d, d^{-1})^{-1}$$
la matrice numeratore $N(d, d^{-1})$ è prima a destra.
3. *$G(d)$ ammette un'inversa sinistra $L(d, d^{-1})$ polinomiale di Laurent.*
4. *Nella forma canonica di Smith McMillan di $G(d)$ i polinomi $\varepsilon_i(d)$ sono potenze di d.*

Dimostrazione $(i) \Rightarrow (ii)$ Se $N(d, d^{-1})$ non fosse prima a destra, esisterebbe una serie a supporto non finito $\hat{\mathbf{u}}'(d)$ tale che $N(d, d^{-1})\hat{\mathbf{u}}'(d)$ sia polinomiale di Laurent. Posto allora
$$\hat{\mathbf{u}}(d) := D(d, d^{-1})\hat{\mathbf{u}}'(d),$$

osserviamo che

$$G(d)\hat{\mathbf{u}}(d) = N(d,d^{-1})D(d,d^{-1})^{-1}\hat{\mathbf{u}}(d) = N(d,d^{-1})\hat{\mathbf{u}'}(d) \tag{7.23}$$

è polinomiale di Laurent. D'altra parte, dato che $\begin{bmatrix} D \\ N \end{bmatrix}$ è prima a destra e $\hat{\mathbf{u}'}(d)$ ha supporto infinito, non può essere polinomiale il vettore

$$\begin{bmatrix} D(d,d^{-1}) \\ N(d,d^{-1}) \end{bmatrix} \hat{\mathbf{u}'}(d) = \begin{bmatrix} \hat{\mathbf{u}}(d) \\ N(d,d^{-1})\hat{\mathbf{u}'}(d) \end{bmatrix}$$

e quindi non può esserlo il vettore $\hat{\mathbf{u}}(d)$. Ma allora in (7.23) avremmo un segnale a supporto infinito, $\hat{\mathbf{u}}(d)$, che $G(d)$ trasforma in un altro a supporto finito, contro l'ipotesi di non catastroficità del codificatore.

(ii) $\Rightarrow$ *(iii)* Essendo prima a destra, $N(d,d^{-1})$ ammette un' inversa sinistra polinomiale di Laurent $L(d,d^{-1})$ e $N(d,d^{-1})D(d,d^{-1})^{-1}$ ha come inversa la matrice polinomiale di Laurent $D(d,d^{-1})L(d,d^{-1})$.

(iii) $\Rightarrow$ *(iv)* Basandoci sulle considerazioni svolte nel par.4.3 e con il medesimo significato di $\mathcal{E}$ e di Ψ, rappresentiamo il codificatore nella forma

$$G(d) = U(d)\mathcal{E}(d)[V(d)\Psi(d)]^{-1} \tag{7.24}$$

Se $L(d,d^{-1})$ ne è un'inversa sinistra polinomiale di Laurent, è facile ottenere

$$[V^{-1}(d)L(d,d^{-1})U(d)][\mathcal{E}(d)\Psi(d)^{-1}] = I_m \tag{7.25}$$

o anche, denotando con $\tilde{L}_1(d,d^{-1}) \in \mathbb{F}[d,d^{-1}]^{m\times m}$ la sottomatrice formata dalle prime m colonne di $V^{-1}(d)N(d,d^{-1})U(d)$,

$$\tilde{L}_1(d,d^{-1})\mathrm{diag}\{\varepsilon_1(d)/\psi_1(d), \varepsilon_2(d)/\psi_2(d), \ldots, \varepsilon_m(d)/\psi_m(d)\}_{m\times m} = I_m,$$

da cui

$$\tilde{L}_1(d,d^{-1}) = \mathrm{diag}\{\psi_1(d)/\varepsilon_1(d), \psi_2(d)\varepsilon_2(d), \ldots, \psi_m(d)/\varepsilon_m(d)\}_{m\times m}$$

Poiché $\varepsilon_i(d)/\psi_i(d)$ sono rappresentazioni irriducibili, i polinomi $\varepsilon_i(d)$ possono solo essere potenze di d.

(iv) $\Rightarrow$ *(i)* Rappresentiamo $G(d)$ come in (7.24) e supponiamo che il prodotto $G(d)\hat{\mathbf{u}}(d) = U(d)\mathcal{E}(d)[V(d)\Psi(d)]^{-1}\hat{\mathbf{u}}(d) = \hat{\mathbf{y}}(d)$ sia polinomiale di Laurent. La matrice

$$\mathcal{E}(d) = \mathrm{diag}\{d^{\nu_1}, d^{\nu_2}, \ldots, d^{\nu_m}\}_{p\times m}$$

ha un'inversa sinistra di Laurent

$$\mathcal{L}(d) = \mathrm{diag}\{d^{-\nu_1}, d^{-\nu_2}, \ldots, d^{-\nu_m}\}_{m\times p}$$

e quindi

$$\hat{\mathbf{u}}(d) = V(d)\Psi(d)\mathcal{L}(d)U(d)^{-1}\hat{\mathbf{y}}(d)$$

è polinomiale di Laurent. ■

Un codificatore $G(d)$ è *sistematico* se, come già per i codici a blocchi, ha come sottomatrice la matrice identità $m \times m$, ovvero se, a meno di una permutazione delle righe

$$G(d) = \begin{bmatrix} I_m \\ G_2(d) \end{bmatrix} \tag{7.26}$$

con $G_2(d) \in \mathbb{F}(d)^{(p-m)\times m}$ Un codificatore sistematico non é mai catastrofico, perché non può codificare una sequenza di informazione di durata infinita in una parola di codice a supporto finito (o, equivalentemente, perché ha come inversa sinistra la matrice costante $[\, I_m \quad 0\,]$)

- **Esercizio 7.5.1** (i) Se il codificatore sistematico $G(d)$ ha l'espressione (7.26) e se $N_2(d, d^{-1})D_2(d, d^{-1})^{-1}$ è una RMF irriducibile di $G_2(d)$, allora

$$\begin{bmatrix} D_2(d, d^{-1}) \\ N_2(d, d^{-1}) \end{bmatrix}$$

è un codificatore non catastrofico del medesimo codice.

(ii) Un codificatore $G(d, d^{-1}) \in \mathbb{F}[d, d^{-1}]^{p\times m}$ è equivalente a un codificatore sistematico polinomiale di Laurent se e solo se nella fattorizzazione

$$G(d, d^{-1}) = \bar{G}(d, d^{-1})\Delta(d, d^{-1})$$

la matrice prima a destra $\bar{G}(d, d^{-1})$ contiene una sottomatrice $m \times m$ unimodulare.

(iii) Se un codificatore sistematico di $\mathcal{C}$ è polinomiale di Laurent, sono tali tutti i codificatori sistematici di $\mathcal{C}$? (Suggerimento: si consideri $G(d, d^{-1}) = \begin{bmatrix} I_m \\ P(d, d^{-1}) \end{bmatrix}$, con $P(d, d^{-1})$ matrice $m \times m$ di rango m e con $\det P$ polinomio di Laurent non invertibile).

Proposizione 7.5.2 *Ogni codice convoluzionale $\mathcal{C}$ ammette codificatori sistematici.*
Sono fatti equivalenti:

1. *$\mathcal{C}$ ammette un codificatore sistematico polinomiale di Laurent;*
2. *ogni codificatore basico di $\mathcal{C}$ ha almeno un minore di ordine m che è un monomio non nullo di $\mathbb{F}[d]$;*
3. *per opportuni $i_1, i_2, \ldots i_m \in \{1, 2, \ldots p\}$, ogni parola di codice $\mathbf{y}(\cdot)$ nella quale hanno supporto finito le componenti $y_{i_1}, y_{i_2}, \ldots, y_{i_m}$, ha supporto finito.*

DIMOSTRAZIONE Se $G(d)$ è un codificatore polinomiale del codice, esso ha rango m e perciò esiste una matrice $D(d)$ di rango m formata da m opportune righe di $G(d)$. È chiaro che $G(d)D(d)^{-1}$ è un codificatore sistematico.

Per quanto attiene alle equivalenze:

(1) $\Rightarrow$ (2) A meno di una permutazione delle componenti del codice, o equivalentemente delle righe dei codificatori del codice, possiamo supporre che il codificatore sistematico polinomiale di Laurent di $\mathcal{C}$ sia

$$G(d, d^{-1}) = \begin{bmatrix} I_m \\ P(d, d^{-1}) \end{bmatrix}. \tag{7.27}$$

Moltiplicandone le colonne per opportune potenze di d, si perviene a un codificatore polinomiale (non di Laurent) equivalente

$$\tilde{G}(d) = \begin{bmatrix} d^{\nu_1} & & & \\ & d^{\nu_2} & & \\ & & \ddots & \\ & & & d^{\nu_m} \\ & M(d) & & \end{bmatrix} \tag{7.28}$$

Se da (7.28) si estrae un fattore polinomiale destro massimale, si ricava un codificatore basico in cui un minore di ordine massimo (quello associato alle prime m righe della matrice) è un monomio non nullo di $\mathbb{F}[d]$; basta allora applicare la Proposizione 7.4.1 per concludere che ogni codificatore basico ha la medesima proprietà.

(2) $\Rightarrow$ (3) Permutando, se necessario, le righe del codificatore, supponiamo che esso abbia la forma

$$G(d) = \begin{bmatrix} V(d) \\ M(d) \end{bmatrix} \tag{7.29}$$

con $V(d) \in \mathbb{F}[d]^{m\times m}$ unimodulare su $\mathbb{F}[d, d^{-1}]$ e $M(d) \in \mathbb{F}[d]^{(p-m)\times m}$. Se partizioniamo una parola di codice $\hat{\mathbf{y}}(d) = G(d)\hat{\mathbf{u}}(d)$ conformemente alla partizione di $G(d)$

$$\hat{\mathbf{y}}(d) = \begin{bmatrix} \hat{\mathbf{y}}_1(d) \\ \hat{\mathbf{y}}_2(d) \end{bmatrix} \begin{matrix} m \\ p-m \end{matrix}$$

e se $\hat{\mathbf{y}}_1(d)$ ha supporto finito, lo ha pure $\hat{\mathbf{u}}(d) = V(d)^{-1}\hat{\mathbf{y}}_1(d)$, e con essa

$$\hat{\mathbf{y}}(d) = \begin{bmatrix} \hat{\mathbf{y}}_1(d) \\ M(d)V(d)^{-1}\hat{\mathbf{y}}_1(d) \end{bmatrix}$$

(3) $\Rightarrow$ (1) Supponiamo che $i_1, i_2, \ldots i_m$ coincidano con $1, 2, \ldots, m$, e sia

$$G(d) = \begin{bmatrix} A(d) \\ B(d) \end{bmatrix} \begin{matrix} m \\ p-m \end{matrix} \tag{7.30}$$

un codificatore basico di $\mathcal{C}$. Allora $A(d)$ ha rango m ed è unimodulare di Laurent. In caso contrario, esisterebbe un segnale di informazione $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$ con supporto infinito, tale che $\hat{\mathbf{y}}_1(d) := A(d)\hat{\mathbf{u}}(d)$ abbia supporto finito (ed eventualmente vuoto). Ma allora $\hat{\mathbf{y}}_2(d) := B(d)\hat{\mathbf{u}}(d)$ avrebbe supporto infinito, per la primalità a destra del codificatore, e

$$\begin{bmatrix} \hat{\mathbf{y}}_1(d) \\ \hat{\mathbf{y}}_2(d) \end{bmatrix}$$

sarebbe una parola di codice che non soddisfa la condizione (3). Il codificatore sistematico

$$\hat{G}(d) = \begin{bmatrix} I_m \\ B(d)A(d)^{-1} \end{bmatrix} \begin{matrix} m \\ p-m \end{matrix} \tag{7.31}$$

ha le proprietà volute. ■

7.6 Codificatori causali

Nello studio dei codificatori di un codice convoluzionale, finora abbiamo toccato solo marginalmente l'argomento importante della causalità della mappa che essi inducono e quindi della loro effettiva realizzabilità mediante un sistema lineare sul campo $\mathbb{F}$. Consideriamo la *mappa di codifica* χ indotta da un codificatore $G(d) \in \mathbb{F}(d)^{p\times m}$

$$\chi : \mathbb{F}((d))^m \to \mathbb{F}((d))^p : \hat{\mathbf{u}}(d) \mapsto \hat{\mathbf{y}}(d) = G(d)\hat{\mathbf{u}}(d) \tag{7.32}$$

Ovviamente χ è $\mathbb{F}((d))$-*lineare* e *invariante* per traslazioni, nel senso che $G(d)[d^k\hat{\mathbf{u}}(d)] = d^k[G(d)\hat{\mathbf{u}}(d)]$ per ogni $k \in \mathbb{Z}$.

Per precisare che cosa intendiamo per mappa causale, conviene introdurre l'operatore di troncamento all'istante $T \in \mathbb{Z}$:

$$\mathcal{P}_T : \mathbb{F}((d))^m \to d^{T-1}\mathbb{F}[d^{-1}]^m : \sum_t u(t)d^t \mapsto \sum_{t<T} u(t)d^t \tag{7.33}$$

Definizione 7.6.1 *χ è una mappa causale se per ogni $T \in \mathbb{Z}$ e per ogni $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$*

$$\mathcal{P}_T[\chi(\hat{\mathbf{u}}(d))] = \mathcal{P}_T[\chi(\mathcal{P}_T\hat{\mathbf{u}}(d))], \tag{7.34}$$

ovvero se i campioni della parola di codice precedenti l'istante T dipendono solo dai campioni della sequenza di informazione precedenti l'istante T.

La seguente proposizione riporta varie condizioni equivalenti per la causalità di una mappa di codifica. Alcune delle condizioni sono note dal cap.4, e vengono qui inserite per completezza.

Proposizione 7.6.2 *Sia $G(d)$ un codificatore per il codice convoluzionale $[p, m]$ $\mathcal{C}$ e sia $W(z) := G(z^{-1})$. Sono fatti equivalenti*

(i) *$G(d)$ induce una mappa di codifica χ causale;*

(ii) *per ogni $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$*

$$\mathcal{P}_0[\chi(\hat{\mathbf{u}}(d))] = \mathcal{P}_0[\chi(\mathcal{P}_0\hat{\mathbf{u}}(d))]; \tag{7.35}$$

(iii) *$G(d)$ ammette uno sviluppo in serie con elementi in $\mathbb{F}[[d]]$;*

(iv) *Se $G(d) = N(d)D(d)^{-1}$ è una RMF destra irriducibile, $D(0)$ è invertibile;*

(v) *Nella forma canonica di Smith McMillan di $G(d)$ i polinomi $\psi_i(d)$ non sono multipli di d;*

(vi) *$W(z)$ ammette uno sviluppo in serie con elementi in $\mathbb{F}[[z^{-1}]]$;*

(vii) *$W(z)$ è una matrice razionale propria*

(viii) *Se $W(z) = \tilde{N}(z)\tilde{D}(z)^{-1}$ è una RMF destra con il denominatore $D(z)$ ridotto per colonne, allora*

$$\deg \operatorname{col}_i D(z) \geq \deg \operatorname{col}_i N(z), \quad i = 1, 2, \ldots, m$$

DIMOSTRAZIONE $(i) \Leftrightarrow (ii)$ In un verso l'implicazione è ovvia, perchè ottenuta dalla (7.34) particolarizzando in 0 il valore dell'indice T.
Per l'altro, tenendo conto dell'invarianza di χ e dell'identità

$$\mathcal{P}_T\hat{\mathbf{u}}(d) = d^T\mathcal{P}_0(d^{-T}\hat{\mathbf{u}}(d)),$$

si ricava facilmente

$$\begin{aligned}
\mathcal{P}_T\chi\hat{\mathbf{u}} &= d^T\mathcal{P}_0d^{-T}(\chi\hat{\mathbf{u}}) = d^T\mathcal{P}_0\chi(d^{-T}\hat{\mathbf{u}}) \\
\mathcal{P}_T\chi(\mathcal{P}_T\hat{\mathbf{u}}) &= d^T\mathcal{P}_0d^{-T}\chi(\mathcal{P}_T\hat{\mathbf{u}}) = d^T\mathcal{P}_0\chi[d^{-T}(d^T\mathcal{P}_0d^{-T}\hat{\mathbf{u}})] \\
&= d^T\mathcal{P}_0\chi[\mathcal{P}_0(d^{-T}\hat{\mathbf{u}})] = d^T\mathcal{P}_0\chi(d^{-T}\hat{\mathbf{u}})
\end{aligned}$$

per cui χ è causale se e solo se la (7.34) vale per ogni $\hat{\mathbf{u}}(d)$ e per $T = 0$.

$(ii) \Rightarrow (iii)$ Supponiamo che per qualche $j \in \{1, 2, \dots m\}$ la colonna $\hat{\mathbf{g}}_j(d)$ di $G(d)$ abbia uno sviluppo in serie che include potenze negative di d:

$$\hat{\mathbf{g}}_j(d) = \sum_{t=-\nu}^{+\infty} \mathbf{g}_j(t) d^t, \quad -\nu < 0, \quad \mathbf{g}_j(-\nu) \neq 0$$

e consideriamo l'ingresso

$$\hat{\mathbf{u}}(d) = \mathbf{e}_j d^{\nu-1},$$

dove $\mathbf{e}_j$ è lo j-esimo vettore della base canonica di $\mathbb{F}^m$. Allora risulta

$$\mathcal{P}_0[\chi(\hat{\mathbf{u}}(d))] = \mathcal{P}_0[\sum_{t=-\nu}^{+\infty} \mathbf{g}_j(t) d^{t+\nu-1}] = \mathcal{P}_0[\sum_{\tau=-1}^{+\infty} \mathbf{g}_j(\tau - \nu + 1) d^{\tau}] = \mathbf{g}_j(-\nu) d^{-1} \neq \mathbf{0}, \tag{7.36}$$

mentre

$$\mathcal{P}_0[\chi(\mathcal{P}_0 \hat{\mathbf{u}}(d))] = \mathcal{P}_0[G(d)\mathbf{0}] = \mathbf{0}. \tag{7.37}$$

$(iii) \Rightarrow (iv)$ Per la irriducibilità di $N(d)D(d)^{-1}$, è risolubile polinomialmente l'equazione di Bézout

$$X(d)N(d) + Y(d)D(d) = I_m, \tag{7.38}$$

mentre per l'ipotesi (ii) $N(d)D(d)^{-1}$ ammette uno sviluppo in serie

$$N(d)D(d)^{-1} = \sum_{t=0}^{+\infty} G_t d^t. \tag{7.39}$$

Da (7.38) e (7.39) segue

$$[X(d) \sum_{t=0}^{+\infty} G_t d^t + Y(d)]D(d) = I_m \tag{7.40}$$

e il termine di grado 0 di $D(d)$ è invertibile, avendo per inverso il termine di grado 0 della serie in $\mathbb{F}[[d]]^m$ fra parentesi quadra.

$(iv) \Rightarrow (ii)$ Basta verificare che, per ogni $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$,

$$\mathcal{P}_0\Big(N(d)D(d)^{-1}[\hat{\mathbf{u}}(d) - \mathcal{P}_0(\hat{\mathbf{u}}(d))]\Big) = \mathbf{0}. \tag{7.41}$$

Ma questo è ovvio, perché $\hat{\mathbf{u}}(d) - \mathcal{P}_0(\hat{\mathbf{u}}(d)) \in \mathbb{F}[[d]]^m$ viene mappata da $D(d)^{-1}$ in una serie di $\mathbb{F}[[d]]^m$ e quindi da $N(d)$ in una serie di $\mathbb{F}[[d]]^p$, che l'operatore $\mathcal{P}_0$ annulla.

$(iv) \Leftrightarrow (v)$ Nella rappresentazione irriducibile $N(d)D(d)^{-1}$ il denominatore è esprimibile nella forma $D(d) = V(d)\Psi(d)W(d)$, con $V(d)$ e $W(d)$ unimodulari, e la condizione che $D(0)$ sia invertibile equivale a quella che lo sia $\Psi(0)$.

$(iii) \Leftrightarrow (vi)$ Ovvio, dal momento che $W(z)$ si ottiene formalmente da $G(d)$ ponendovi $d = z^{-1}$.

$(vi) \Rightarrow (vii) \Rightarrow (viii) \Rightarrow (vi)$ Si vedano l'esercizio 1.6.3 e il paragrafo 4.5.1. ■

Nel capitolo 5, abbiamo visto come la dimensione minima di realizzazione di una matrice razionale propria $W(z)$ possa essere "letta" sulla matrice denominatore di una rappresentazione matriciale destra irriducibile, $\tilde{N}(z)\tilde{D}(z)^{-1}$ considerando il grado del suo determinante. Quando, inoltre, $\tilde{D}(z)$ sia ridotta per colonne, la dimensione minima è semplicemente la somma dei gradi delle sue colonne. È naturale domandarsi come tale informazione posa essere estratta da una RMF nella variabile $d = z^{-1}$ Per rispondere, premettiamo un lemma, che pone in relazione le rappresentazioni matriciali fratte di un codificatore convoluzionale causale $G(d)$ con quelle della matrice di trasferimento $W(z) := G(z^{-1})$

Lemma 7.6.3 *Se $N(d)D(d)^{-1}$ è una rappresentazione irriducibile di $G(d)$, con*

(i) $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ *ridotta per colonne e gradi di colonna $K_1, K_2, \ldots K_m$*

(ii) $D(0)$ *invertibile*

e poniamo

$$\begin{bmatrix} \tilde{N}(z) \\ \tilde{D}(z) \end{bmatrix} := \begin{bmatrix} N(d) \\ D(d) \end{bmatrix} \begin{bmatrix} d^{-K_1} & & & \\ & d^{-K_2} & & \\ & & \ddots & \\ & & & d^{-K_m} \end{bmatrix} \Big|_{z=d^{-1}} \tag{7.42}$$

allora $\tilde{N}(z)\tilde{D}(z)^{-1}$ è una rappresentazione irriducibile di $W(z) := G(z^{-1})$, con

(iii) $\tilde{D}(z)$ *ridotta per colonne e gradi di colonna $K_1, K_2, \ldots K_m$*

(iv) $\deg \mathrm{col}_i \tilde{N} \leq \deg \mathrm{col}_i \tilde{D}$

Viceversa, se $\tilde{N}(z)\tilde{D}(z)^{-1}$ è una rappresentazione irriducibile di $W(z)$ soddisfacente (iii) e (iv) e poniamo

$$\begin{bmatrix} N(d) \\ D(d) \end{bmatrix} := \begin{bmatrix} \tilde{N}(z) \\ \tilde{D}(z) \end{bmatrix} \begin{bmatrix} z^{-K_1} & & & \\ & z^{-K_2} & & \\ & & \ddots & \\ & & & z^{-K_m} \end{bmatrix} \Big|_{d=z^{-1}} \tag{7.43}$$

allora $N(d)D(d)^{-1}$ è una rappresentazione irriducibile di $G(d) := W(d^{-1})$ soddisfacente (i) e (ii).

DIMOSTRAZIONE Tenendo conto di (7.42), si vede che la matrice dei coefficienti dei termini di grado massimo per colonna $\tilde{D}_{\text{hc}}$ in $\tilde{D}(z)$ coincide con la matrice delle costanti $D(0)$ in $D(d)$ e quindi $\tilde{D}(z)$ è ridotta per colonne con gradi di colonna $K_1, K_2, \ldots, K_m$. Risulta inoltre $\deg \text{col}_i \tilde{N} \leq K_i$ (dove l'uguaglianza vale se la colonna K_i-esima di $N(d)$ contiene delle costanti). Infine, da (7.42) è chiaro che $\begin{bmatrix} \tilde{N}(z) \\ \tilde{D}(z) \end{bmatrix}$ ha rango pieno per ogni valore non nullo della variabile z in $\bar{\mathbb{F}}$, la chiusura algebrica di $\mathbb{F}$, mentre per $z = 0$

$$\begin{bmatrix} \tilde{N}(0) \\ \tilde{D}(0) \end{bmatrix} = \begin{bmatrix} N \\ D \end{bmatrix}_{\text{hc}} \tag{7.44}$$

ha rango pieno perché $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ è ridotta per colonne. Si conclude che $\tilde{N}(z)\tilde{D}(z)^{-1}$ è irriducibile.
Viceversa, da (iii) e da (7.43) segue che $D(0) = \tilde{D}_{\text{hc}}$ è invertibile. Inoltre

$$\begin{bmatrix} N \\ D \end{bmatrix}_{\text{hc}} = \begin{bmatrix} \tilde{N}(0) \\ \tilde{D}(0) \end{bmatrix}$$

ha rango pieno per l'irriducibilità di $\tilde{N}(z)\tilde{D}(z)^{-1}$ e quindi $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ è ridotta per colonne.
Infine, da (7.43) è chiaro che $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ ha rango pieno per ogni valore non nullo della variabile d in $\bar{\mathbb{F}}$, la chiusura algebrica di $\mathbb{F}$, mentre per $d = 0$

$$\begin{bmatrix} N(0) \\ D(0) \end{bmatrix} = \begin{bmatrix} \tilde{N} \\ \tilde{D} \end{bmatrix}_{\text{hc}} \tag{7.45}$$

ha rango pieno perché $\tilde{D}(z)$ è ridotta per colonne, con gli stessi gradi di colonna di $\begin{bmatrix} \tilde{N}(z) \\ \tilde{D}(z) \end{bmatrix}$. Quindi $N(d)D(d)^{-1}$ è irriducibile. ■

Proposizione 7.6.4 *Sia $G(d)$ un codificatore causale del codice convoluzionale $\mathcal{C}$ e siano $N(d)D(d)^{-1}$ e $\tilde{N}(z)\tilde{D}(z)^{-1}$ due sue RMF destre irriducibili, rispettivamente nelle indeterminate d e $z = d^{-1}$, con*

$$\begin{bmatrix} N(d) \\ D(d) \end{bmatrix} \quad \text{e} \quad \tilde{D}(z) \tag{7.46}$$

ridotte per colonna. Allora i gradi di colonna $K_1, K_2, \ldots, K_m$ delle due matrici in (7.46) coincidono a meno dell'ordine, e $\sum_{i=1}^{m} K_i$ fornisce la dimensione di realizzazione minima di $G(d)$.

La dimostrazione è immediata: poiché $\tilde{D}(d^{-1})$ è ridotta per colonne e $\tilde{N}(d^{-1})\tilde{D}(d^{-1})$ è irriducibile, la somma dei gradi di colonna K_i del denominatore fornisce la dimensione minima di realizzazione, per la Proposizione 5.2.2. D'altra parte, per il lemma precedente, i gradi di colonna di $\tilde{D}(d^{-1})$ coincidono con quelli di $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$, e quindi la dimensione minima di realizzazione si "legge" anche sulla rappresentazione irriducibile $N(d)D(d)^{-1}$ quando $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ sia ridotto per colonne.

- **Esercizio 7.6.1** Sia $G_c(d)$ un codificatore canonico del codice $\mathcal{C}$, con indici di Forney $k_1, k_2, \ldots, k_m$.

  (i) Se $T(d) \in \mathbb{F}(d)^{m\times m}$ è una matrice causale di rango m, $G_c(d)T(d)$ è un codificatore causale di $\mathcal{C}$.

  (ii) Se $G(d)$ è un codificatore causale di $\mathcal{C}$, esiste una matrice causale di rango m $T(d) \in \mathbb{F}(d)^{m\times m}$, tale che $G(d) = G_c(d)T(d)$ (Suggerimento: l'esistenza di una matrice razionale e di rango m è stata provata. Se $T(d)$ non fosse causale, lo sviluppo in serie di $G(d)$ conterrebbe termini con esponente negativo).

  (iii) Se $G(d)$ è un arbitrario codificatore polinomiale del codice $\mathcal{C}$ con gradi di colonna $h_1, h_2, \ldots, h_m$, esiste una permutazione $(p_1, p_2, \ldots, p_m)$ di $(1, 2, \ldots, m)$ tale che $k_{p_i} \leq h_i,\ i = 1, 2 \ldots, m$ (Suggerimento: $G(d) = G_c(d)T(d)$ con $T(d)$ matrice polinomiale: si applichi l'esercizio 3.5.5).

  (iv) Se $G(d) = N(d)D(d)^{-1}$ è un arbitrario codificatore causale del codice $\mathcal{C}$ e se $h_1, h_2, \ldots, h_m$ sono i gradi di colonna di $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$, esiste una permutazione $(p_1, p_2, \ldots, p_m)$ di $(1, 2, \ldots, m)$ tale che $k_{p_i} \leq h_i,\ i = 1, 2 \ldots, m$ (Suggerimento: $N(d)$ è un codificatore di $\mathcal{C}$).

  (v) Se $W(z) = \tilde{N}(z)\tilde{D}(z)^{-1}$ è un arbitrario codificatore causale del codice $\mathcal{C}$ e se $h_1, h_2, \ldots, h_m$ sono i gradi di colonna di $\tilde{D}(z)$, esiste una permutazione $(p_1, p_2, \ldots, p_m)$ di $(1, 2, \ldots, m)$ tale che $k_{p_i} \leq h_i,\ i = 1, 2 \ldots, m$ (Suggerimento: se $\tilde{N}(z)\tilde{D}(z)^{-1}$ è irriducibile e con il denominatore ridotto per colonne e se $N(d)D(d)^{-1}$ è data da (7.43), allora i gradi di colonna di $D(z)$ coincidono con quelle di $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$: basta applicare allora il punto precedente. Altrimenti, basta fornire di $W(z)$ una RMF destra irriducibile e con il denominatore ridotto per colonne e applicare l'esercizio 3.5.5).

7.7 Codificatori minimali

Basandoci sui risultati appena ottenuti, vogliamo ora studiare i codificatori causali di un codice convoluzionale $\mathcal{C}$ dal punto di vista del loro grado di McMillan, ovvero della dimensione minima in cui ciascuno di essi può essere realizzato con un modello di stato, e determinare quali codificatori causali di $\mathcal{C}$ hanno grado di McMillan minimo.

Definizione *Un codificatore causale $G(d)$ del codice convoluzionale $\mathcal{C}$ si dice* minimale *se per ogni altro codificatore causale $\tilde{G}(d)$ risulta*

$$\mu(G) \leq \mu(\tilde{G}) \tag{7.47}$$

Cominciamo con alcune semplici considerazioni, che metteranno in luce come i codificatori canonici siano sempre minimali.

1. Se $G_c(d)$ è un codificatore canonico, con indici di Forney $k_1, k_2, \ldots, k_m$, il suo grado di McMillan è
$$\mu(G_c) = \sum_{i=1}^{m} k_i$$
Infatti $G_c(d) = G_c(d)[I_m]^{-1}$ è una RMF destra irriducibile, con denominatore invertibile per $d = 0$ e con $\begin{bmatrix} G_c(d) \\ I_m \end{bmatrix}$ ridotta per colonne e gradi di colonna $k_1, k_2, \ldots, k_m$. Si applica allora la Proposizione 7.6.4.

2. Se $G_b(d)$ è un codificatore basico - ma non canonico - e $G_c(d)$ è un codificatore canonico, per la Proposizione 7.4.1 esiste una matrice unimodulare $U(d)$ tale da aversi
$$G_b(d) = G_c(d)U(d)^{-1} \tag{7.48}$$
Ovviamente la RMF destra (7.48) è irriducibile e $U(0)$ è invertibile. Se $\begin{bmatrix} G_c(d) \\ U(d) \end{bmatrix}$ non è ridotta per colonne, si può determinare una matrice unimodulare $V(d)$, in modo che
$$\begin{bmatrix} \bar{G}(d) \\ \bar{U}(d) \end{bmatrix} = \begin{bmatrix} G_c(d) \\ U(d) \end{bmatrix} V(d)$$
sia ridotta per colonne, con gradi di colonna $K_1, K_2, \ldots K_m$. La RMF destra
$$G_b(d) = \bar{G}(d)V(d)^{-1}U(d)^{-1} = \bar{G}(d)\bar{U}(d)^{-1}$$

soddisfa ora le condizioni della Proposizione 7.6.4. Poichè $\bar{G}(d) = G_c(d)V(d)$ è un codificatore polinomiale, la somma dei suoi gradi di colonna non può essere inferiore a $\sum_{i=1}^{m} k_i$, e quindi, a maggior ragione, non può esserlo la somma dei gradi di colonna K_i di $\begin{bmatrix} \bar{G}(d) \\ \bar{U}(d) \end{bmatrix}$. Pertanto

$$\mu(G_b) = \sum_{i=1}^{m} K_i \geq \sum_{i=1}^{m} k_i = \mu(G_c)$$

3. Se $G_r(d)$ è un arbitrario codificatore razionale causale, esso ha una RMF destra irriducibile del tipo $G_r(d) = [G_c(d)\Delta(d)]D(d)^{-1}$ con $D(0)$ invertibile. La matrice prima a destra

$$\begin{bmatrix} G_c(d)\Delta(d) \\ D(d) \end{bmatrix}$$

può non essere ridotta per colonne. In tal caso la si postmoltiplica per un'opportuna matrice unimodulare $V(d)$, pervenendo a una matrice

$$\begin{bmatrix} \bar{G}(d) \\ \bar{D}(d) \end{bmatrix} = \begin{bmatrix} G_c(d)\Delta(d)V(d) \\ D(d)V(d) \end{bmatrix}$$

ridotta, con gradi di colonna $K_1, K_2, \ldots, K_m$ e tale che $G_r(d) = \bar{G}(d)\bar{D}(d)^{-1}$. Si ha così

$$\begin{aligned} \mu(G_r) &= \sum_{i=1}^{m} K_i = \text{extdeg} \begin{bmatrix} \bar{G} \\ \bar{U} \end{bmatrix} \geq \text{extdeg}(G_c\Delta V) \\ &\geq \text{intdeg}(G_c\Delta) \geq \text{intdeg}G_c = \text{extdeg}G_c = \sum_{i=1}^{m} k_i \end{aligned} \quad (7.49)$$

Possiamo riassume la discussione nella seguente

Proposizione 7.7.1 *Il grado* $\deg\mathcal{C} = \sum_{i=1}^{m} k_i$ *di un codice convoluzionale* $\mathcal{C}$ *fornisce il minimo grado di McMillan dei suoi codificatori causali, siano essi polinomiali o razionali. Quindi un codificatore causale* $G(d)$ *di* $\mathcal{C}$ *è minimale se e solo se*

$$\mu(G) = \deg\mathcal{C}$$

Esempio 7.7.1 [codificatore non canonico minimale] Si considerino il codificatore canonico

$$G_c(d) = \begin{bmatrix} d^4+1 & d^3 \\ d^4 & 1 \\ d & d+1 \end{bmatrix},$$

con grado di McMillan 7, e la matrice unimodulare

$$U(d) = \begin{bmatrix} d^2+1 & d^2 \\ d^2 & d^2-1 \end{bmatrix}$$

Allora

$$\begin{aligned} G_b(d) = G_c(d)U(d)^{-1} &= \begin{bmatrix} d^4+1 & d^3 \\ d^4 & 1 \\ d & d+1 \end{bmatrix} \begin{bmatrix} -d^2+1 & d^2 \\ d^2 & -d^2-1 \end{bmatrix} \\ &= \begin{bmatrix} -d^6+d^5+d^4-d^2+1 & d^6-d^5-d^3+d^2 \\ -d^6+d^4+d & d^6-d^2-1 \\ d^2+d & -d^2-d-1 \end{bmatrix} \end{aligned} \quad (7.50)$$

è un codificatore basico, non ridotto per colonne, ma con il medesimo grado di McMillan di $G_c(d)$, dato che $\begin{bmatrix} G_c(d) \\ U(d) \end{bmatrix}$ è ridotta per colonne, con gli stessi gradi di colonna di $G_c(d)$.

Esempio 7.7.2 [codificatore basico non minimale] Si consideri il codificatore canonico

$$G_c(d) = \begin{bmatrix} d+1 & 1 \\ d & 1 \\ d & d+1 \end{bmatrix}$$

con grado di McMillan 2, e utilizzando la medesima $U(d)$ dell'esercizio precedente poniamo

$$G_b(d) = G_c(d)U(d)^{-1}.$$

Il codificatore così ottenuto

$$G_b(d) = \begin{bmatrix} -d^3-d^2+d+1 & d^3-1 \\ -d^3+d^2+d & d^3-d^2-1 \\ d^2+d & -d^2-d-1 \end{bmatrix}, \quad (7.51)$$

è basico e non ridotto per colonne . La matrice $\begin{bmatrix} G_c(d) \\ U(d) \end{bmatrix}$ non è ridotta per colonne; per ridurla si può postmoltiplicarla per

$$V(d) = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix},$$

ottenendo

$$\begin{bmatrix} \bar{G}(d) \\ \bar{U}(d) \end{bmatrix} = \begin{bmatrix} G_c(d) \\ U(d) \end{bmatrix} V(d) = \begin{bmatrix} d+1 & -d \\ d & 1-d \\ d & 1 \\ d^2+1 & -1 \\ d^2 & -1 \end{bmatrix} \quad (7.52)$$

ridotta per colonne con gradi di colonna $K_1 = 2$ e $K_2 = 1$. Quindi il grado di McMillan di $G_b(d)$ è 3.

Proposizione 7.7.2 *Sia $G(d) \in \mathbb{F}(d)^{p\times m}$ un codificatore causale del codice convoluzionale $\mathcal{C}$. Sono fatti equivalenti:*

(i) $G(d)$ è minimale;

(ii) $G(d)$ *è esprimibile nella forma*

$$G(d) = G_c(d)D(d)^{-1} \tag{7.53}$$

dove $G_c(d)$ *è un codificatore canonico e ogni colonna di* $D(d)$ *ha grado non superiore a quello della colonna corrispondente in* $G_c(d)$*;*

(iii) la matrice $G(d)$ *ammette un'inversa sinistra polinomiale* $X(d) \in \mathbb{F}[d]^{m\times p}$ *e un'inversa sinistra polinomiale* $Y(d^{-1}) \in \mathbb{F}[d^{-1}]^{m\times p}$*.*

DIMOSTRAZIONE $(i) \Rightarrow (ii)$ Se il codificatore causale $G(d)$ è minimale, soddisfa la condizione

$$\mu(G) = \deg\mathcal{C} = \sum_{i=1}^{m} k_i.$$

Rappresentiamolo nella forma irriducibile

$$G(d) = \bar{G}(d)\bar{D}(d)^{-1}$$

con

$$\begin{bmatrix} \bar{G}(d) \\ \bar{D}(d) \end{bmatrix} \tag{7.54}$$

prima a destra, ridotta per colonne e con $\bar{D}(0)$ invertibile. Poichè $\bar{G}(d)$ è un codificatore polinomiale di $\mathcal{C}$, esso non può avere somma dei gradi di colonna inferiore a $\sum_{i=1}^{m} k_i$ (che è la somma dei gradi di colonna di un codificatore canonico). Ma non può neppure averla superiore, altrimenti la dimensione di realizzazione minima di $G(d)$, data per la Proposizione 7.6.4 dalla somma dei gradi di colonna di (7.54), supererebbe il grado del codice $\sum_i k_i$. Quindi $\bar{G}(d)$ è un codificatore canonico.
Inoltre $\bar{D}(d)$ non può avere alcun grado di colonna superiore a quello corrispondente nel codificatore canonico $\bar{G}(d)$, altrimenti la somma dei gradi di colonna di (7.54), e e quindi il grado di McMillan $\mu(G)$, eccederebbe il grado del codice.

$(ii) \Rightarrow (iii)$ Poiché $G_c(d)$ è una matrice polinomiale prima a destra, ammette un'inversa sinistra $L(d) \in \mathbb{F}[d]^{m\times p}$ e basta porre

$$X(d) = D(d)L(d).$$

Se $k_1, k_2, \ldots, k_m$ sono i gradi di colonna di $G_c(d)$, poniamo

$$\begin{aligned} G(d) &= \left[G_c(d)\mathrm{diag}\{d^{-k_1}, d^{-k_2}, \ldots, d^{-k_m}\}\right]\left[D(d)\mathrm{diag}\{d^{-k_1}, d^{-k_2}, \ldots, d^{-k_m}\}\right]^{-1} \\ &=: \tilde{N}(d^{-1})\tilde{D}(d^{-1})^{-1} \end{aligned} \tag{7.55}$$

ottenendo una RMF destra sull'anello $\mathbb{F}[d^{-1}]$.
E' facile vedere che $\tilde{N}(d^{-1})$ è prima a destra: infatti per ogni valore non nullo di $d^{-1} \in \bar{\mathbb{F}}$ essa ha rango pieno perchè ha rango pieno $G_c(d)$, mentre $\tilde{N}(0) = (G_c)_{\rm hc}$ ha rango pieno perché $G_c(d)$ è ridotta per colonne.
Ma allora $\tilde{N}(d^{-1})$ ha un'inversa sinistra $\tilde{L}(d^{-1}) \in \mathbb{F}[d^{-1}]^{m\times p}$ e basta porre

$$Y(d^{-1}) = \tilde{D}(d^{-1})\tilde{L}(d^{-1})$$

$(iii) \Rightarrow (i)$ Si considerino una rappresentazione irriducibile $N(d)D(d)^{-1}$ di $G(d)$, soddisfacente le condizioni (i) e (ii) del Lemma 7.6.3, e la corrispondente rappresentazione irriducibile $\tilde{N}(d^{-1})\tilde{D}(d^{-1})^{-1}$ data da (7.42).
Da $X(d)N(d)D(d)^{-1} = I$ si ricava $X(d)N(d) = D(d)$ e per l'irriducibilita' di $N(d)D(d)^{-1}$ esiste una matrice polinomiale $M(d)$ soddisfacente

$$I = M(d)\begin{bmatrix} N(d) \\ D(d) \end{bmatrix} = M(d)\begin{bmatrix} N(d) \\ X(d)N(d) \end{bmatrix} = M(d)\begin{bmatrix} I \\ X(d) \end{bmatrix} N(d). \qquad (7.56)$$

Quindi $N(d)$, ammettendo un'inversa polinomiale sinistra , è prima a destra.
Con il medesimo ragionamento si prova che $\tilde{N}(d^{-1})$, matrice polinomiale nell'indeterminata d^{-1}, è prima a destra, e di conseguenza $\tilde{N}(0)$ ha rango pieno m. In base a (7.43), risulta $N_{\rm hc} = \tilde{N}(0)$ e perciò $N(d)$ è ridotta per colonne mentre $D(d)$ ha gradi di colonna non superiori ai corrispondenti di $N(d)$.
Il grado di McMillan di $G(d)$, che in base al Lemma 7.6.3 coincide con la somma dei gradi di colonna di $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$, coincide allora con la somma dei gradi di colonna di $N(d)$. Ma $N(d)$, ridotta per colonne e prima a destra, è un codificatore canonico e ha per gradi di colonna gli indici di Forney k_i. Concludendo, $\mu(G) = \sum_i k_i$ e $G(d)$ è codificatore minimale. ■

Dal punto (iii) della Proposizione 7.7.2 segue immediatamente:

Corollario 7.7.3 *Ogni codificatore causale e sistematico è minimale.*

Il risultato della Proposizione 7.7.2 può essere raffinato, fornendo una parametrizzazione di tutti i codificatori causali minimali di un codice convoluzionale $[p, m]$ $\mathcal{C}$: basta *fissare* un suo particolare codificatore canonico $G_c(d)$ e considerare i codificatori $G_c(d)D(d)^{-1}$, al variare di $D(d)$ sulle matrici polinomiali $m \times m$, invertibili, con $D(0)$ invertibile, e con gradi di colonna non superiori a quelli di $G_c(d)$. Per provarlo, premettiamo il seguente

Lemma 7.7.4 *Se la matrice polinomiale* $\begin{bmatrix} N_1(d) \\ D_1(d) \end{bmatrix}$ *e il suo blocco* $N_1(d)$ *sono ridotti per colonne, con i medesimi gradi di colonna* $k_1, k_2, \ldots, k_m$. *e se in*

$$\begin{bmatrix} N_2(d) \\ D_2(d) \end{bmatrix} = \begin{bmatrix} N_1(d) \\ D_1(d) \end{bmatrix} V(d) \tag{7.57}$$

la matrice $V(d)$ *è unimodulare e il blocco* $N_2(d)$ *è ridotto per colonne, allora è ridotta anche* $\begin{bmatrix} N_2(d) \\ D_2(d) \end{bmatrix}$ *e i gradi di colonna di entrambe le matrici sono, a parte l'ordine,* $k_1, k_2, \ldots, k_m$.

DIMOSTRAZIONE Poiché $N_1(d)$ e $N_2(d)$ sono entrambe ridotte e differiscono per operazioni elementari di colonna, in base alla Proposizione 3.5.10 i loro gradi di colonna coincidono, salvo per l'ordine. Applicando la predicibilita' del grado, da $N_2(d) = N_1(d)V(d)$ segue che la i-esima colonna di $N_2(d)$ ha grado definito da

$$\tilde{k}_i = \max_{j:v_{ij}(d)\neq 0} \{k_j + \deg v_{ij}\}. \tag{7.58}$$

Ma la i-esima colonna di $D_2(d)$ non può possedere un grado più elevato di $\tilde{k}_i$: infatti da $D_2(d) = D_1(d)V(d)$ e dal fatto che la j-esima colonna di $D_1(d)$ ha grado minore o eguale a k_j , $j = 1, 2, \ldots, m$ segue

$$\deg \mathrm{col}_i D_2 \leq \max_{j:v_{ij}(d)\neq 0} \{k_j + \deg v_{ij}\}. \tag{7.59}$$

Proposizione 7.7.5 *Se* $G_c(d)$ *è un particolare codificatore canonico del codice* $[p, m]$ $\mathcal{C}$, *tutti i codificatori causali a grado di McMillan minimo si ottengono dall'espressione*

$$G(d) = G_c(d)D(d)^{-1} \tag{7.60}$$

al variare di $D(d)$ *sull'insieme delle matrici polinomiali* $m \times m$, *invertibili, con* $D(0)$ *invertibile, e con gradi di colonna non superiori a quelli di* $G_c(d)$
In particolare, i codificatori polinomiali a grado di McMillan minimo si ottengono scegliendo la matrice $D(d)$ *unimodulare e soddisfacente i medesimi vincoli sui gradi di colonna*

DIMOSTRAZIONE Per la Proposizione 7.7.4, un arbitrario codificatore causale a grado di McMillan minimo è esprimibile nella forma $G(d) = \bar{G}_c(d)\bar{D}(d)^{-1}$, dove $\bar{G}_c(d)$ è un codificatore canonico, $\bar{D}(d)$ ha gradi di colonna non superiori agli indici di Forney delle colonne di $\bar{G}_c(d)$ e $\det \bar{D}(0) \neq 0$

Sia $V(d)$ una matrice unimodulare tale da aversi $\bar{G}_c(d)V(d) = G_c(d)$ e poniamo $D(d) := \bar{D}(d)V(d)$. Chiaramente si ha $G(d) = G_c(d)D(d)^{-1}$, e basta applicare il lemma precedente per concludere che $\begin{bmatrix} G_c(d) \\ D(d) \end{bmatrix}$ è ridotta per colonne e i gradi di colonna di $D(d)$ non superano quelli corrispondenti in $G_c(d)$.
Affinchè il codificatore (7.60) sia polinomiale basta e occorre (si applichi la Proposizione 3.3.3) che $D(d)^{-1}$ sia polinomiale e quindi $D(d)$ unimodulare. Al variare di $D(d)$ sulle matrici unimodulari con gradi di colonna non superiori a quelli di $G_c(d)$ si ottengono allora tutti i codificatori polimomiali a minimo grado di McMillan. ■

- **Esercizio 7.7.1** Sia $\mathcal{C}$ un codice con indici di Forney $k_1, k_2, \ldots, k_m$. Si dimostri che un codificatore polinomiale $G(d)$ con grado di McMillan pari a $\sum_{i=1}^{m} k_i$ è basico (Suggerimento: una RMF destra irriducibile del codificatore ha la forma (7.53), e per la polinomialità di $G(d)$ la matrice $D(d)$ deve essere unimodulare. Si applichi la Prop. 7.4.1)

Si vede facilmente che tutti i codificatori causali minimali sono non catastrofici. Infatti per la Proposizione 7.7.2 sono dotati di un'inversa sinistra polinomiale.

Esistono tuttavia codificatori causali non catastrofici e non minimali. Basta in proposito notare che se $N(d)$ è un codificatore basico di $\mathcal{C}$ e $D(d)$ una arbitraria matrice polinomiale $m \times m$ con $D(0)$ a rango pieno, la RMF destra $N(d)D(d)^{-1}$ è un codificatore causale non catastrofico di $\mathcal{C}$.
Utilizzando matrici $D(d)$ ridotte per colonna e con gradi di colonna opportunamente elevati, si possono costruire codificatori non catastrofici con grado di McMillan arbitrariamente grande.

7.8 Codificatori e retroazione

In questo paragrafo vogliamo studiare l'effetto della retroazione dallo stato sulla realizzazione di un codificatore causale del codice convoluzionale $\mathcal{C}$.
Consideriamo dapprima un codificatore **canonico** $G_c(d) \in \mathbb{F}[d]^{p \times m}$, e quindi con indici di Forney $k_1, k_2, \ldots, k_m$ **tutti strettamente positivi**.

- L'ipotesi di positività degli indici equivale ad assumere che il codice convoluzionale **non contenga parole di lunghezza 0**. Infatti, essendo $G(d)$ prima a destra, eventuali parole di codice $\hat{\mathbf{y}}(d)$ di durata finita sono immagine di sequenze di informazione $\hat{\mathbf{u}}(d)$ di durata finita, e se gli indici di Forney sono strettamente positivi la proprietà di predicibilità del grado implica che ogni $\hat{\mathbf{u}}(d)$ di durata finita produca una $\hat{\mathbf{y}}(d) = G(d)\hat{\mathbf{u}}(d)$ di durata strettamente più grande.

Viceversa, se $G(d)$ ha una colonna costante, è chiaro che $\mathcal{C}$ contiene parole di lunghezza 0.

- Dal punto di vista dei modelli di stato, l'ipotesi equivale ad assumere che in **ogni** realizzazione (F, G, H, J) di **qualsiasi** codificatore causale di $\mathcal{C}$ la matrice G abbia **rango di colonna** m. Sia infatti $\tilde{N}(z)\tilde{D}(z)^{-1}$ una RMF irriducibile di un codificatore causale di $\mathcal{C}$, con $D(z)$ ridotto per colonne e gradi di colonna $h_1, h_2, \ldots, h_m$. Per la Proposizione 7.6.4, se $N(d)D(d)^{-1}$ è una RMF irriducibile del codificatore nella indeterminata $d = z^{-1}$ e se

$$\begin{bmatrix} N(d) \\ D(d) \end{bmatrix} \tag{7.61}$$

è ridotta per colonne, i gradi di colonna di $\tilde{D}(z)$ e di (7.61) coincidono, a meno dell'ordine. Il codificatore $N(d)$ di $\mathcal{C}$ ha gradi di colonna non superiori a quelli di (7.61) e, per l'esercizio 7.6.4.(iii), i gradi di $G_c(d)$, opportunamente ordinati, sono a loro volta non superiori a quelli di $G_c(d)$. Perciò esiste una permutazione $(p_1, p_2, \ldots, p_m)$ di $(1, 2, \ldots, m)$ tale che $k_i \leq h_{p_i},\ i = 1, 2 \ldots, m$. Ne consegue che, se gli indici di Forney k_i sono strettamente positivi, tali sono i gradi di colonna h_i, ovvero gli indici di Kronecker della coppia (F, G) in ogni realizzazione minima $\Sigma_m = (F, G, H, J)$ di $W(z)$. Allora ha rango m la matrice G di Σ_m e quindi la matrice G in ogni altra realizzazione di $W(z)$.

Viceversa, se una realizzazione minima $\Sigma_m = (F, G, H, J)$ del codificatore canonico $G_c(d)$ ha la matrice G con rango m, sono strettamente positivi gli indici di Kronecker della coppia (F, G), ovvero i gradi di colonna del denominatore ridotto per colonne nella RMF irriducibile di $G_c(z^{-1})$. Per la Prop.7.6.4 essi coincidono con i gradi di colonna di $\begin{bmatrix} G_c(d) \\ I_m \end{bmatrix}$ e quindi con i gradi di colonna di $G_c(d)$.

Poniamo $W(z) = G_c(z^{-1})$ e denotiamo con $\tilde{N}(z)$ la matrice

$$[G_c(z^{-1}) - G_c(0)]\text{diag}\{z^{k_1}, z^{k_2}, \ldots, z^{k_m}\}_{m\times m},$$

con gradi di colonna non superiori a $k_1-1, k_2-1, \ldots, k_m-1$. Allora il codificatore può essere rappresentato come

$$W(z) = G_c(0) + \tilde{N}(z)\text{diag}\{z^{k_1}, z^{k_2}, \ldots, z^{k_m}\}^{-1}_{m\times m} \tag{7.62}$$

e la parte strettamente propria è una RMF irriducibile e con denominatore ridotto per colonne.

Se $S(z)$ denota la stessa matrice del par. 5.4.2 e poniamo $\tilde{N}(z) = H_c S(z)$, per ottenere una realizzazione minima di $W(z)$ basta assumere come matrici F_c e G_c della forma canonica di controllo multivariabile quelle le cui righe di indice $k_1, k_1 + k_2, \ldots, k_1 + k_2 + \ldots + k_m$ formano rispettivamente la matrice $0_{m\times n}$ e la matrice identità I_m, e come matrice J la matrice $G_c(0)$.

La **matrice di trasferimento ingresso-stato** è data da

$$W_{\text{is}}(z) = S(z)\text{diag}\{z^{k_1}, z^{k_2}, \ldots, z^{k_m}\}^{-1}_{m\times m}$$

ovvero, nella variabile d, da

$$P_{\text{is}}(d) = \begin{bmatrix} d^{k_1} & & & \\ d^{k_1-1} & & & \\ \vdots & & & \\ d & & & \\ & d^{k_2} & & \\ & d^{k_2-1} & & \\ & \vdots & & \\ & d & & \\ & & \ddots & \\ & & & d^{k_m} \\ & & & d^{k_m-1} \\ & & & \vdots \\ & & & d \end{bmatrix} \tag{7.63}$$

Applicando una retroazione K dallo stato, la matrice ingresso-stato (7.63) si modifica in $P_{\text{is}}(d)[I_m - KP_{\text{is}}(d)]^{-1}$, nella cui matrice denominatore $[I_m - KP_{\text{is}}(d)]$ la i-esima colonna descrive al variare di K la totalità dei vettori polinomiali di grado non superiore a k_i e che valgono $\mathbf{e}_i$ in $d = 0$.

La **matrice di trasferimento ingresso-uscita** nella variabile d, data in assenza di retroazione dalla matrice polinomiale $G_c(d) = [J + H_c P_{\text{is}}(d)]$ con gradi di colonna $k_1, k_2, \ldots, k_m$, per effetto della retroazione si trasforma in

$$G^{(K)}(d) = [J + H_c P_{\text{is}}(d)][I_m - KP_{\text{is}}(d)]^{-1} = G_c(d)[I_m - KP_{\text{is}}(d)]^{-1} \tag{7.64}$$

Se supponiamo di introdurre anche all'ingresso del codificatore un precompensatore statico, rappresentato da una matrice invertibile $M \in \mathbb{F}^{m\times m}$, e poniamo $\tilde{K} = M^{-1}K$, il sistema cui si perviene ha matrice di trasferimento

$$G^{(K,M)}(d) \quad = \quad [J + H_c P_{\text{is}}(d)][I_m - KP_{\text{is}}(d)]^{-1} M$$

$$\begin{aligned} &= G_c(d)[M^{-1} - M^{-1}KP_{\rm is}(d)]^{-1} \\ &= G_c(d)[M^{-1} - \tilde{K}P_{\rm is}(d)]^{-1} \end{aligned} \tag{7.65}$$

Comunque si scelga una matrice $D(d) \in \mathbb{F}[d]^{m\times m}$, con $D(0)$ invertibile e gradi di colonna non superiori a $k_1, k_2, \ldots, k_m$, e' possibile determinare immediatamente il precompensatore $M = D(0)^{-1}$ e la matrice $\tilde{K}$ in modo che valga l'identità $D(d) = M^{-1} - \tilde{K}P_{\rm is}(d)$. La matrice di retroazione K si ricava allora ponendo $K = D(0)^{-1}\tilde{K}$. Come conseguenza della Proposizione 7.7.7, abbiamo così dimostrato la seguente

Proposizione 7.8.1 *Sia (F, G, H, J) una realizzazione minima, di ordine n, del codificatore canonico $G_c(d)$ del codice $\mathcal{C}$. Se $M \in \mathbb{F}^{m\times m}$ è una matrice di precompensazione e $K \in \mathbb{F}^{m\times n}$ è una matrice di reazione dallo stato, al variare di M e K è possibile ottenere tutti (e soli) i codificatori minimali del codice. Essi avranno realizzazioni minime date da $(F + GK, GM, H + JK, JM)$.*

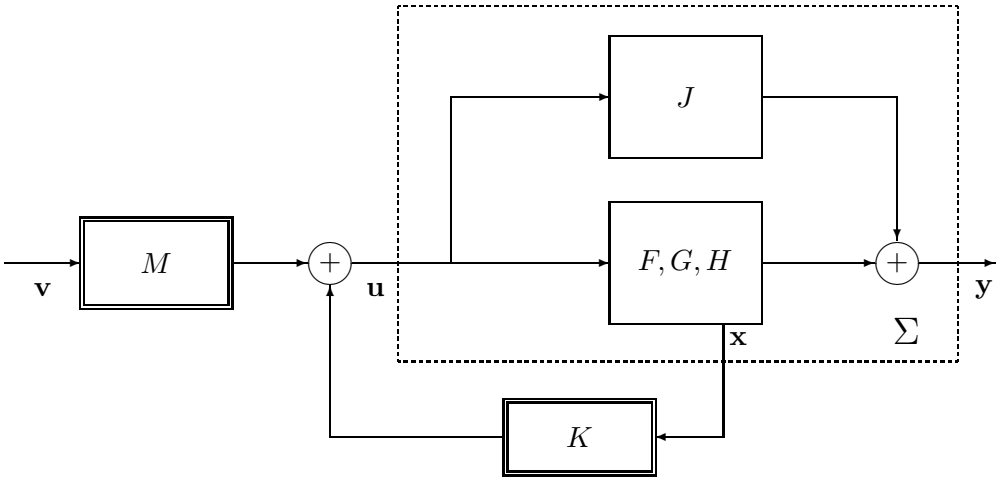

Fig. 7.3

- **Esercizio 7.8.1** Applicando un opportuno precompensatore statico e un'opportuna retroazione statica dallo stato, si possono ottenere tutti i codificatori minimali a partire da uno minimale arbitrario (i.e. non necessariamente canonico).

- **Esercizio 7.8.2** Se (F_c, G_c, H_c, J) è una realizzazione minima in forma canonica di controllo del codificatore canonico $G_c(d)$, con indici di Forney positivi k_i, le colonne di H_c di indice $1, 1+k_1, 1+k_1+k_2, \ldots, 1+k_1+\ldots+k_{m-1}$ formano una matrice di rango m (Suggerimento: in $G_c(d)$ un minore di ordine m ha grado $\sum_i k_i$. Esso può provenire solo dal prodotto di una opportuna sottomatrice H_c' di H_c, di dimensioni $m \times n$, per la matrice $P_{\rm is}(d)$. Si applichi a $H_c'P_{\rm is}(d)$ il teorema di Binet Cauchy e si tenga conto della struttura di $P_{\rm is}(d)$).