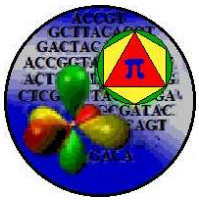
Università degli Studi di Palermo

Facoltà di Scienze MM. FF. NN.
Corso di Laurea Specialistica in Matematica



Codici bifissi ed insiemi Sturmiani

Studente
Francesco Dolce

Relatore
Prof. Antonio Restivo

Anno Accademico 2010/2011

Für die Entwicklung der logischen Wissenschaften wird es, ohne Rücksicht auf etwaige Anwendungen, von Bedeutung sein, ausgedehnte Felder für Spekulation über schwierige Probleme zu finden.

Per lo sviluppo delle scienze logiche è importante trovare, senza alcun riguardo sulle possibili applicazioni, ampî campi di speculazione su problemi difficili.

Alex Thue

Wir müssen wissen, wir werden wissen.

David Hilbert

Indice

Introduzione

Tale tesi prende spunto dal lavoro di J. Berstel, C. De Felice, D. Perrin, C. Reutenaur e G. Rindone riguardante lo studio dei codici bifissi in insiemi Sturmiani in [1] e dai risulati proposti da alcuni degli stessi autori nello studio dei gruppi sintattici in [12] e in [3] (nonché in [2] per una panoramica d'insieme).

L'elaborato è così suddiviso.

Nel Capitolo 1 sono contenute le nozioni preliminari. I tre macroargomenti che vengono affrontati sono l'Algebra (Sezione 1.1), la Combinatoria delle Parole (Sezione 1.2) e la Teoria degli Automi (Sezione 1.3). Sono qui presentati (ovviamente in maniera non esaustiva) tutti gli argomenti, e soprattutto tutte le notazioni, utili per sviluppare le nozioni dei Capitoli successivi.

Nel Capitolo 2 si introducono i concetti di parole Sturmiane, parole su un alfabeto binario non periodiche di complessità minima, e le parole episturmiane, estensione al caso di alfabeti finiti di cardinalità arbitraria. Si riprendono anche i concetti di insiemi chiusi per prefissi e fattoriali e si introducono quelli di insiemi ricorrenti, uniformemente ricorrenti e Sturmiani. Questi formano una gerarchia discendente. Si affronta, quindi, lo studio insiemi prefissi contenuti dentro un insieme fattoriale (Sezione 2.3) ed infine ci si concentra al caso di insiemi bifissi contenuti dentro insiemi ricorrenti (Sezione 2.4).

Il Capitolo 3 specializza ancor di più i risultati del Capitolo precedente studiando i codici bifissi dentro insiemi Sturmiani. Qui sono presenti i principali risultati dell'elaborato, ovvero il Teorema della Cardinalità (Teorema 3.1.3) ed il Teorema della Base Sturmiana (Teorema 3.4.4) che caratterizza in termini di codici bifissi in insiemi Sturmiani le basi dei sottogruppi del gruppo libero.

Infine il Capitolo 4 è dedicato ai gruppi sintattici. Alcuni dei risultati presenti riguardano il grado di un gruppo sintattico e sono ricavati da quanto dimostrato nel Capitolo precedente. Vi è poi un altro gruppo di risultati, riguardante i codici sintattici di codici con nucleo vuoto, che sfrutta le interpretazioni viste nel primo Capitolo.

Una Congettura proposta in forma privata da C. Reutenaur nel 2010, e postami indipendentemente dal Prof. A. Restivo, affermava che il Teorema della Cardinalità (Teorema 3.1.3) fosse in un qualche senso invertibile, ovvero che fosse possibile dare una caratterizzazione delle parole Sturmiane più generale di quella nota.

Il contro-esempio 3.1.6 qui presentato (originale, con una semplificazione suggerita da D. Perrin) confuta tale Congettura, lasciando però il problema aperto rispetto a formulazioni più restrittive.

Ringraziamenti. Mi è d'obbligo un ringraziamento al Prof. Antonio Restivo, relatore della tesi, non solo per avermi indirizzato verso gli argomenti della tesi, ma soprattutto per gli spunti di riflessione e i "compiti per casa" su congetture da dimostrare o confutare. Un ringraziamento va anche a M. Dominique Perrin per i suoi suggerimenti semplificatori e per avermi ricordato che a un matematico non serve costruire esplicitamente qualcosa, basta dimostrarne l'esistenza.

Grazie a M. Jean-Éric Pin per la sua disponbilità e celerità nel rispondere alle mie richieste di aiuto virtuale.

La stesura di una tesi prevede un "lavoro sporco" di scrittura e correzione. Per tale ragione ringrazio Laura Giambruno per i suggerimenti in GasTeXese ed Astrid Denaro per i consigli "estetici" sulla formattazione del documento. Infine un ringraziamento caloroso va a Roberto Signorello che mi ha aiutato a scovare errori/orrori tipografici in giro per queste pagine.

Va da sé che qualsiasi eventuale errore, sia di contenuto che di forma, è da imputare esclusivamente a me.

Francesco Dolce
Palermo, Marzo 2012

Capitolo 1

Nozioni preliminari

Questo Capitolo è dedicato alle nozioni basilari di Algebra (Sezione 1.1), Combinatoria delle Parole (Sezione 1.2) e Teoria degli Automi (Sezione 1.3).

La maggior parte degli argomenti sono di livello elementare e sono qui riportati, oltre che per un utile ripasso, soprattutto per fissare la notazione.

Per uno studio più approfondito degli argomenti si rimanda a [10], [4] e [14].

1.1 Richiami algebrici

In questa Sezione si introducono le strutture algebriche usate nella tesi – semigruppi, monoidi, gruppi, semianelli – ed altre definizioni basilari ad esse legate. Di fondamentale importanza risulteranno le nozioni di permutazione introdotte nella Sottosezione 1.1.5 e quella di monoide e gruppo libero, nella Sottosezione 1.1.6.

1.1.1 Semigruppi, monoidi, gruppi, semianelli

Sia S un insieme. Un'*operazione binaria* su S è una funzione da $S \times S$ in S. L'immagine della coppia (x, y) tramite questa funzione si dirà *prodotto* di x ed y e si denoterà come $x \cdot y$ o, più spesso, come xy. Seguendo tale notazione l'operazione binaria sarà detta *moltiplicazione*.

In alcuni casi si userà la notazione additiva chiamando *somma* l'immagine della coppia (x, y) e denotandola $x + y$.

Un'operazione su S si dirà *associativa* se per ogni $x, y, z \in S$ si ha $(xy)z = x(yz)$. Sarà detta invece *commutativa* se per ogni $x, y \in S$ si ha $xy = yx$.

Una coppia $(S, \cdot)$ è detta *semigruppo* se S è un insieme e $\cdot$ è un'operazione binaria su S. Quando non sussistono ambiguità sull'operazione si dirà semplicemente che "S è un semigruppo".

Esempio 1.1.1.

- $(\mathbb{N}_+, +)$ è il semigruppo degli interi positivi con operazione l'usuale somma di interi.

- $(\mathbb{N}_+ \setminus \{1\}, \cdot)$ è il semigruppo degli interi maggiori di 1 con operazione l'usuale prodotto di interi.

All'interno di un semigruppo vi sono degli elementi che godono di proprietà particolari.

Un elmento 1 di S è detto *elemento neutro*, o *identità*, dell'operazione se per ogni $x \in S$ risulta $x \cdot 1 = 1 \cdot x = x$. È facile dimostrare che se tale elemento neutro esiste esso sarà unico.

Chiameremo *monoide* una tripla $(M, \cdot, 1)$ dove $(M, \cdot)$ è un semigruppo ed 1 è l'elemento neutro per la sua operazione. Anche in questo caso, quando non ci saranno ambiguità sull'operazione e sull'identità, diremo che "M è un monoide".

Esempio 1.1.2.

- $(\mathbb{N}, +)$ è il monoide degli interi non negativi con operazione l'usuale somma di interi ed elemento neutro 0.

- $(\mathbb{N}_+, \cdot)$ è il monoide degli interi non negativi con operazione l'usuale prodotto di interi ed elemento neutro 1.

Esempio 1.1.3. Preso un monoide M, l'insieme $\mathcal{P}(M)$ di tutti i sottoinsiemi di M può essere dotato esso stesso della struttura di monoide definendo come prodotto di due elementi $X, Y \subseteq M$

$$XY = \{xy \mid x \in X, y \in Y\}.$$

In tal caso l'elemento neutro sarà il singleton $\{1\}$.

Se S è un semigruppo, si indicherà con S^1 il monoide dato da:

- S, nel caso S sia già un monoide;

- $S \cup \{1\}$, con $1 \notin S$, se S non è un monoide, ed in tal caso l'operazione di S si estenderà ad S^1 definendo $1 \cdot s = s \cdot 1 = s \quad \forall\, s \in S^1$.

Esempio 1.1.4. Il monoide additivo $\mathbb{N}_+^1$, ha come supporto $\mathbb{N}_+ \cup \{0\}$.

Esempio 1.1.5. Consideriamo B_2 il semigruppo dato delle matrici 2×2 con elementi in $\{0, 1\}$ ed al più un 1.

Il monoide B_2^1 ottenuto considerando anche l'identità sarà:

$$B_2^1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Ponendo 1 la matrice identica, 0 la matrice nulla, $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ e $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, si ottiene $ab = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ e $ba = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Il monoide può dunque essere riscritto come

$$B_2^1 = \{1, a, b, ab, ba, 0\} .$$

Moltiplicando gli elementi tra loro si ottengono le relazioni $aa = bb = 0$, $aba = a$ e $bab = b$.

Un elemento e di S è detto *identità destra* (risp. *identità sinistra*) di S se per ogni $s \in S$ risulta $se = s$ (risp. $es = s$).

Un elemento e di S è detto *idempotente* se $e^2 = e$. L'insieme degli idempotenti di S di denota $E(S)$.

Osservazione 1.1.6. Un elemento è un'identità se e solo se è contemporaneamente identità destra e sinistra. Inoltre un'identità destra (risp. sinistra) è necessariamente un idempotente.

Un elemento $0 \in S$ è detto *zero* se per ogni $s \in S$ si ha $0 \cdot s = s \cdot 0 = 0$. Anche in questo caso è facile dimostrare che se un semigruppo possiede uno zero questo è unico.

Inoltre è possibile dare la nozione di *zero destro* (risp. *zero sinistro*) per un elemento $e \in S$ tale che $se = e$ (risp. $es = e$).

Se S è un semigruppo, si indicherà con S^0 il semigruppo dato da:

- S, nel caso S possegga già uno zero;
- $S \cup \{0\}$, con $0 \notin S$, se S non ha zeri, ed in tal caso l'operazione di S si estenderà ad S^0 definendo $0 \cdot s = s \cdot 0 = 0 \quad \forall\, s \in S^0$.

Esempio 1.1.7. Il monoide moltiplicativo $\mathbb{N}_+^0$, ha come supporto $\mathbb{N}_+ \cup \{0\}$.

Un semigruppo sarà detto *nullo* se possiede uno zero ed il prodotto di due qualsiasi suoi elementi è zero.

Per definire gli inversi bisognerà porre particolare attenzione. Vi sono infatti due diverse definizioni di inverso: una "classica" ed un'altra "debole" usata in teoria dei Semigruppi.

Sia M un monoide. Dato un elemento $x \in M$, un elemento x' di M si dirà *inverso destro* (risp. *inverso sinistro*) di x se $xx' = 1$ (risp. $x'x = 1$).

Un *inverso* di x è un elemento x' che è contemporaneamente inverso destro ed inverso sinistro.

Dato un elemento x di un semigruppo S, un elemento $x' \in S$ si dirà *inverso debole* di x se $xx'x = x$ e $x'xx' = x'$.

Chiaramente ogni inverso è un inverso debole, mentre il viceversa non sempre è verificato. Ad esempio, nel caso di un monoide finito si può dimostrare che ogni elemento ha al più un solo inverso ma può avere diversi inversi deboli.

Un monoide $(G, \cdot, 1)$, o semplicemente G quando saranno chiari operazione ed elemento neutro, tale che ogni suo elemento possiede un inverso è detto *gruppo*.

In effetti è possibile dare una definizione equivalente più debole, in quanto è facile vedere che un monoide è un gruppo se e solo se ogni suo elemento ha un inverso destro ed un inverso sinistro. Nel caso di monoidi finiti la condizione si riduce all'esistenza del solo inverso destro (o del solo inverso sinistro).

Si dimostra facilmente che in un gruppo ogni elemento x ha un unico inverso, che sarà denotato come x^{-1}.

Esempio 1.1.8.

- $(\mathbb{Z}, +)$ è il gruppo degli interi con operazione l'usuale somma di interi ed elemento neutro 0.
- $(\mathbb{Q}_+, \cdot)$ è il gruppo dei razionali positivi con operazione l'usuale prodotto di interi ed elemento neutro 1.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ è il gruppo degli interi modulo n.

Il numero di elementi in un semigruppo (risp. monoide, gruppo) è detto *ordine* del semigruppo (risp. del monoide, del gruppo).

Esempio 1.1.9. L'ordine del gruppo $\mathbb{Z}/n\mathbb{Z}$ è n.

Un semigruppo (risp. monoide, gruppo) è detto *commutativo* o *Abeliano* se la sua operazione è commutativa.

Esempio 1.1.10. I semigruppi $\mathbb{N}_+$ e $\mathbb{N}_+ \setminus \{1\}$, i monoidi $\mathbb{N}$ e $\mathbb{N}_+$, e i gruppi $\mathbb{Z}$ e $\mathbb{Q}_+$ sopra definiti sono tutti Abeliani.

Il monoide $\mathcal{P}(M)$, con M monoide, invece, non è commutativo.

Un semigruppo S (risp. monoide) dotato di una relazione d'ordine $\leq$ su S compatibile col prodotto, ovvero tale che per ogni $x, y \in S$ e per ogni $u, v \in S^1$ si ha l'implicazione

$$x \leq y \;\Rightarrow\; uxv \leq uyv$$

è detto *semigruppo* (risp. *monoide*) *ordinato*.

Per enfatizzare il ruolo di una relazione d'ordine $\leq$ in una struttura algebrica S si userà la notazione $(S, \leq)$.

Esempio 1.1.11. L'ordine naturale degli interi non negativi è compatibile con l'addizione, quindi $\mathbb{N}$ è un monoide ordinato.

Fin'ora abbiamo studiato strutture algebriche con una sola operazione. Consideriamo adesso il caso in cui le operazioni presenti siano due. Un *semianello* è una quadrupla $(T, +, \cdot, 0)$ tale che:

- $(T, +, 0)$ è un monoide commutativo;
- $(T, \cdot)$ è un semigruppo;
- la moltiplicazione è distributiva rispetto all'addizione, ossia per ogni $s, t_1, t_2 \in T$ si ha $s(t_1 + t_2) = st_1 + st_2$ e $(t_1 + t_2)s = t_1 s + t_2 s$;
- per ogni $s \in T$ si ha $0s = s0 = 0$.

Anche in questo caso, quando non vi saranno ambiguità sulle operazioni, diremo che "T è un semianello".

Nel caso in cui $(T, +, 0)$ sia un gruppo Abeliano, T sarà detto *anello*.

Nel caso anche la moltiplicazione ammetta un'elemento neutro 1, e dunque $(T, \cdot 1)$ sia un monoide, il semianello (risp. anello) sarà detto *unitario* o *con unità*.

Un semianello (risp. anello) è detto *commutativo* se anche la moltiplicazione è commutativa.

Esempio 1.1.12. Preso un insieme X consideriamo l'insieme dei suoi sottoinsiemi $\mathcal{P}(X)$. Chiaramente $(\mathcal{P}(X), \cup, \emptyset)$ ha una struttura di monoide commutativo. Inoltre, seguendo quanto visto nell'Esempio 1.1.3, $\mathcal{P}(X)$ può essere dotato della struttura di monoide con operazione il prodotto di insiemi. Tale prodotto è distributivo rispetto all'unione, ossia presi tre elementi $L, L_1, L_2 \in \mathcal{P}(X)$ si ha:

$$L(L_1 \cup L_2) = LL_1 \cup LL_2 \qquad \text{e} \qquad (L_1 \cup L_2)L = L_1 L \cup L_2 L$$

Dunque $\mathcal{P}(X)$ è un semianello unitario.

1.1.2 Morfismi

Una funzione tra due strutture algebriche dello stesso tipo che preserva le operazioni è detta *omomorfismo* o, più semplicemente, *morfismo*.

In particolare un *morfismo di semigruppi* è una mappa φ da un semigruppo S ad un semigruppo T tale che, per ogni $s_1, s_2 \in S$ si abbia

$$\varphi(s_1 s_2) = \varphi(s_1)\varphi(s_2).$$

Similmente un *morfismo di monoidi* è una morfismo di semigruppi φ da un monoide M ad un monoide N tale che

$$\varphi(1_M) = 1_N.$$

Analogamente un *morfismo di monoidi ordinati* è un morfismo di monoidi φ che, in più, preserva l'ordine, ovvero per cui si abbia l'implicazione

$$s_1 \leq s_2 \ \Rightarrow \ \varphi(s_1) \leq \varphi(s_2).$$

Infine un *morfismo di gruppi* è un morfismo di monoidi φ da un gruppo G ad un gruppo H tale che per ogni $s \in G$ si abbia

$$\varphi(s^{-1}) = \varphi(s)^{-1}.$$

Si dimostra facilmente che ogni morfismo di semigruppi da un gruppo G ad un gruppo H è anche un morfismo di gruppi.

Un morfismo $\varphi : S \to T$ è detto *isomorfismo* se esiste un morfismo $\psi : T \to S$ tale che $\varphi \circ \psi = id_T$ e $\psi \circ \varphi = id_S$.

È noto che gli isomorfismo di sottogruppi (risp. monoidi, gruppi) sono tutti e soli i morfismi biettivi.

Osservazione 1.1.13. Quanto appena detto non vale per i morfismi di monoidi ordinati. Considerariamo infatti due relazioni d'ordine distinte $\leq$ e $\preceq$ su uno stesso monoide M. L'identità id_M è un morfismo biettivo da $(M, \leq)$ a $(M, \preceq)$ pur non essendo un isomorfismo.

In effetti, un morfismo di monoidi ordinati $\varphi : M \to N$ è un isomorfismo se e solo se è un morfismo biettivo e per ogni $x, y \in M$ si ha l'equivalenza tra $x \leq y$ e $\varphi(x) \leq \varphi(y)$.

Due semigruppi (risp. monoidi, gruppi, monoidi ordinati) sono detti *isomorfi* se esistono due isomorfismi dall'uno all'altro.

Un morfismo che va da un semigruppo (risp. monoide, gruppo, monoide ordinato) in se stesso sarà detto *endomorfismo*. Un endomorfismo che è anche isomorfismo sarà detto *automorfismo*.

1.1.3 Sottostrutture, quozienti, ideali

Alcuni sottoinsiemi di una struttura possono essere essi stessi dotati di struttra algebrica.

Un sottoinsieme T di S è detto *sottosemigruppo* se è chiuso rispetto all'operazione, ovvero se per ogni $s_1, s_2 \in T$ si ha $s_1 s_2 \in T$. Tale fatto è esprimibile anche dall'espressione

$$TT \subseteq T.$$

Un sottoinsieme $N \subseteq M$ di un monoide M sarà detto *sottomonoide* se è un suo sottosemigruppo e in più contiene l'identità.

Analogamente un *sottogruppo* di un gruppo è un sottomonoide che contiene gli inversi di tutti i suoi elementi.

Nel caso di sottogruppi useremo la notazione $H \leq G$ per indicare che H è un sottogruppo del gruppo G.

Esempio 1.1.14. L'insieme degli interi pari $2\mathbb{Z}$ è un sottogruppo del gruppo additivo $\mathbb{Z}$, ovvero $2\mathbb{Z} \leq \mathbb{Z}$

Osservazione 1.1.15. Esistono monoidi contenuti in M che non sono suoi sottomonoidi, ovvero può capitare che $N \subseteq M$ verifichi $NN \subseteq N$ ma che si abbia $1_M \neq 1_N$.

Esempio 1.1.16. Consideriamo il monoide $M_2(\mathbb{N})$ delle matrici 2×2 ad elementi in $\mathbb{N}$, dotato dell'usuale moltiplicazione riga per colonne, ed il suo sottoinsieme

$$N = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{N} \right\}.$$

N è un monoide con identità

$$1_N = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_M.$$

Dunque N è un monoide pur non essendo un sottomonoide di M.

Per ogni idempotente e di un monoide M, l'insieme eMe è un monoide contenuto in M. Esso è detto *monoide localizzato* in e ed è il più grande monoide contenuto in M ad avere e come elemento neutro.

Alcuni sottoinsiemi di una struttura possono avere una struttura più ricca.

Dato un monoide M, l'insieme degli elementi invertibili di M è un gruppo detto *gruppo delle unità* di M.

In generale un sottosemigruppo G di un semigruppo (risp. monoide) S è detto un *gruppo in* S se vi è un idempotente $e \in G$ tale che G dotato dell'operazione di S risulti un gruppo con identità e.

Esempio 1.1.17. Il singleton $\{1\}$ formato dalla sola identità è banalmente un gruppo in S per ogni semigruppo (risp. monoide) S.

Il seguente risultato è una proprietà classica dei gruppi in un monoide.

Proposizione 1.1.18. *Siano M un monoide, G un gruppo in M ed $m, n \in M$ due elementi tali che $mn \in G$. Allora nGm è isomorfo a G.*

Dimostrazione. Da $mn \in G$ ricaviamo l'inclusione $nGmnGm \subseteq nGm$. L'elemento $e = n\,(mn)^{-1}\,m \in nGm$ è chiaramente un idempotente e nGm è un monoide con e come elemento neutro. Inoltre, per ogni $g \in G$, l'elemento $h = n((mn)^{-1}\,g^{-1}\,(mn)^{-1})m$ è l'inverso di ngm. Dunque nGm è un gruppo.

Si verifica facilmente che la mappa $f : G \to nGm$ data da $f(g) = n\,(mn)^{-1}\,gm$ è un isomorfismo tra i due gruppi. □

Riprenderemo nel Capitolo 4 lo studio dei gruppi all'interno di un monoide.

Osservazione 1.1.19. Nel caso di gruppi finiti le strutture di sottosemigruppi e sottogruppi coincidono, ovvero ogni sottosemigruppo di un gruppo finito è un sottogruppo.

È noto che i morfismi e gli inversi dei morfismi preservano le sottostrutture dei sottogruppi (risp. sottomonoidi, sottogruppi), ovvero se $\varphi : S \to T$ è un morfismo di semigruppi (risp. monoidi, gruppi) ed S' e T' sono sottosemigruppi (risp. sottomonoidi, sottogruppi) rispettivamente di S e T, allora $\varphi(S')$ e $\varphi^{-1}(T')$ sono rispettivamente sottosemigruppi (risp. sottomonoidi, sottogruppi) di T e di S.

Un sottomonoide N di un monoide M sarà detto *unitario a destra* se è tale che $u, uv \in M \ \Rightarrow \ v \in M$. Analogamente si definisce la nozione di *unitario a sinistra* se $u, uv \in M \ \Rightarrow \ u \in M$.

Un sottomonoide N di un monoide M sarà, invece, detto *stabile* se, per ogni $u, v, w \in M$ si ha $u, v, uw, wv \in N \ \Rightarrow \ w \in N$.

Dato un grupppo G ed un suo sottogruppo $H \leq G$ chiameremo *classi laterali destre* (risp. *classi laterali sinistre*) di H gli insiemi della forma $Hg = \{hg \,|\, h \in H\}$ (risp. $gH = \{gh \,|\, h \in H\}$) al variare di $g \in G$. Si mostra facilmente che due classi laterali o sono disgiunte o coincidono.

L'*indice* $[G : H]$ di un sottogruppo $H \leq G$ di un gruppo G è il numero delle classi laterali destre disgiunte.

Se $K \leq H \leq G$ vale la formula

$$[G : K] = [G : H][H : K]. \tag{1.1}$$

Dunque se $H, K \leq G$ sono due sottogruppi di indice d dello stesso gruppo e $H \subset K$ allora $H = K$.

Siano S e T due semigruppi (risp. monoidi, gruppi, monoidi ordinati). T è detto essere un *quoziente* di S se esiste un morfismo suriettivo da S in T.

Altri sottoinsiemi notevoli di una struttura sono gli ideali. Sia S un semigruppo (risp. monoide). Un sottoinsieme R di S è detto *ideale destro* se $RS \subseteq R$, ovvero se per ogni $r \in R$ e per ogni $s \in S$ risulta $rs \in R$. Simmetricamente, un *ideale sinistro* è un sottoinsieme L di S tale che $SL \ \subseteq \ L$. Un *ideale* I è un sottoinsieme di S che è contemporaneamente ideale destro e sinistro.

Osservazione 1.1.20. Equivalentemente si può definire ideale di un semigruppo (risp. monoide) S un sottoinsieme I tale che per ogni $s \in I$ e per ogni $x, y \in S^1$ si abbia $xsy \in I$, ovvero se $SIS \subseteq I$.

Osservazione 1.1.21. Ogni intersezione di ideali (risp. ideali destri, ideali sinistri) è ancora un ideale.

L'ideale (risp. ideale destro, ideale sinistro) *generato* da un sottoinsieme R di un semigruppo (risp. monoide) S è il più piccolo ideale (risp. ideale

destro, ideale sinistro) di S contenente R; questo è dato da S^1RS^1 (risp. RS^1, S^1R).

Un ideale è detto *principale* se è generato da un solo elemento.

Osservazione 1.1.22. L'ideale (risp. ideale destro, ideale sinistro) generato da un idempotente e è uguale SeS (risp. eS, Se) anche se S non è un monoide. Infatti da $e = eee$ si ottiene $S^1eS^1 = SeS$.

È noto che i morfismi suriettivi e gli inversi dei morfismi preservano la struttura di ideale (risp. ideale destro, ideale sinistro).

Un ideale I di un semigruppo S è detto *minimale* se per ogni ideale non vuoto J di S si ha l'implicazione $J \subseteq I \Rightarrow J = I$.

Un semigruppo ha al più un ideale minimale. Infatti siano I_1 ed I_2 due ideali minimali di un semigruppo S. Per l'Osservazione 1.1.22 $I_1 \cup I_2$ è anch'esso un ideale e banalmente $I_1 \cup I_2 \subseteq I_1$. Dalla minimalità di I_1 si ricava $I_1 \cup I_2 = I_1$. Analogamente si ottiene $I_1 \cup I_2 = I_2$ e dunque $I_1 = I_2$.

Vi sono due casi notevoli in cui sicuramente esiste un ideale minimale: quando S è finito e quando S possiede uno zero. In quest'ultimo caso un ideale non vuoto $I \neq 0$ tale che per ogni ideale $J \subseteq I$ di S si abbia $J = 0$ o $J = I$ è detto *ideale* 0-*minimale*.

Osservazione 1.1.23. Mentre l'ideale minimale se esiste è unico, un semigruppo (risp. monoide) può avere più ideali 0-minimali.

Esempio 1.1.24. Sia $S = \{0, a, b\}$ il semigruppo con operazione $xy = 0$ per ogni $x, y \in S$. L'ideale minimale di S è $\{0\}$, mentre sia $\{0, a\}$ che $\{0, b\}$ sono due ideali 0-minimali.

Un gruppo in un monoide è contenuto in un unico ideale, ovvero dati un monoide M, un suo ideale I ed un gruppo G contenuto in M si ha $G \cap I = \emptyset$ o $G \subseteq I$. Infatti, se $x \in G \cap I$, allora per ogni $g \in G$ si ha $g = x^{-1}xg \in I$.

1.1.4 Relazioni e congruenze

Sia S un semigruppo (risp. monoide, gruppo). Una *congruenza* su S è una relazione di equivalenza $\sim$ stabile su S, ovvero per ogni $s, t \in S$ e per ogni $u, v \in S^1$, si ha l'implicazione

$$s \sim t \quad \Longrightarrow \quad usv \sim utv.$$

Si può dotare l'insieme delle classi di equivalenza $S/\sim$ di una struttura naturale di semigruppo (risp. monoide, gruppo) e la funzione che manda ogni elemento $s \in S$ nella sua classe di equivalenza $[s]$ è detta *proiezione canonica* ed è un morfismo da S in $S/\sim$.

Diamo di seguito due importanti esempi di congruenze.

Esempio 1.1.25. Sia $C \subseteq S$ un sottoinsieme di un semigruppo (risp. monoide) S. La relazione di equivalenza $\sim_C$ su S per cui $s \sim_C t$ se e solo se per ogni $x, y \in S^1$ si abbia

$$xsy \in C \iff xty \in C$$

è una congruenza.

La congruenza definita nell'Esempio 1.1.25 è detta *congruenza sintattica* di C ed il semigruppo (risp. monoide) quoziente $S/\sim_C$ è detto *semigruppo sintattico* di C.

Nel caso in cui $C = S$ si ometterà la dizione "di C".

Esempio 1.1.26. Sia $\varphi : S \to T$ un morfismo di semigruppi (risp. monoidi). L'equivalenza $\sim_\varphi$ su S definita da

$$s \sim_\varphi t \iff \varphi(s) = \varphi(t)$$

è una congruenza.

La congruenza definita nell'Esempio 1.1.26 è detta *congruenza nucleare* di φ e gode della seguente ben noto proprietà.

Proposizione 1.1.27 (Primo Teorema d'Isomorfismo)**.** *Sia $\varphi : S \to T$ un morfismo di semigruppi (risp. monoidi, gruppi) e sia $\pi : S \to S/\sim_\varphi$ la proiezione canonica. Esiste un unico morfismo di semigruppi (risp. monoidi, gruppi) $\widetilde{\varphi} : S/\sim_\varphi \to T$ tale che $\varphi = \widetilde{\varphi} \circ \pi$. Inoltre $\widetilde{\varphi}$ è un isomorfismo tra $S/\sim_\varphi$ e $\varphi(S)$.*

1.1.5 Trasformazioni, azioni

Una *trasformazione* (risp. *trasformazione parziale*) su un insieme Q è una funzione (risp. *funzione parziale*) da Q in se stesso. Una trasformazione biettiva è detta *permutazione*.

Per indicare una trasformazione s su un insieme Q di cardinalità n si userà una matrice $2 \times n$ in cui in ogni colonna compaiono nelle due righe rispettivamente gli elementi di Q e le immagini attraverso s. Nel caso di trasformazioni parziali useremo il simbolo $-$ nella seconda riga nel caso l'immagine dell'elemento corrispondente sia l'insieme vuoto.

Esempio 1.1.28. Sia $Q = \{a, b, c, d, e\}$.

- La funzione
$$\begin{pmatrix} a & b & c & d & e \\ b & a & b & e & d \end{pmatrix}$$
è una trasformazione totale su Q.

- La funzione
$$\begin{pmatrix} a & b & c & d & e \\ e & - & a & d & d \end{pmatrix}$$
è una trasformazione parziale su Q.

- La funzione
$$\begin{pmatrix} a & b & c & d & e \\ c & b & a & e & d \end{pmatrix}$$
è una permutazione su Q.

Se l'insieme Q è ordinato e qualora non sussista ambiguità si scriverà soltanto la seconda riga.

Esempio 1.1.29. Ordinando l'insieme Q dell'Esempio 1.1.28 ponendo $a < b < c < d < e$ possiamo riscrivere le tre trasformazioni rispettivamente come $(b\,a\,b\,e\,d)$, $(e\ -\ a\,d\,d)$ e $(c\,b\,a\,e\,d)$.

Sia Q un insieme e sia S un semigruppo (risp. monoide, gruppo). Un'*azione destra* di S su Q è una funzione $Q \times S \to Q$, denotata $(q, s) \mapsto q \cdot s$, tale che per ogni $s, t \in S$ e per ogni $q \in Q$ si abbia $(q \cdot s) \cdot t = q \cdot (st)$.

Un'azione sarà detta *fedele* se

$$q \cdot s = q \cdot t \ \ \forall\, q \in Q \quad \Longrightarrow \quad s = t.$$

Un *semigruppo di trasformazioni* (risp. *monoide di trasformazioni*, *gruppo di trasformazioni*) su Q è un semigruppo S dotato di un'azione fedele di S su Q.

Un monoide (risp. gruppo) di trasformazioni S su Q si dirà *transitivo* se per ogni $p, q \in Q$ esiste un $g \in S$ tale che $p \cdot g = S$.

Dato S un semigruppo (risp. monoide) di trasformazione su Q, la relazione di equivalenza

$$s \sim t \quad \Longrightarrow \quad q \cdot s = q \cdot t \ \ \forall\, q \in Q$$

è una congruenza su S. Tale azione induce un'azione fedele sul semigruppo (risp. monoide) quoziente $S/\sim$.

Il risultante semigruppo (risp. monoide) di trasformazione $(Q, S/\sim)$ è detto semigruppo (risp. monoide) di trasformazione *indotto dall'azione* $\sim$ di S su Q.

Esempio 1.1.30. Ogni semigruppo S definisce banalmente un semigruppo di trasformazioni (S^1, S) dato dall'azione fedele $q \cdot s = qs$.

Il semigruppo di tutte le trasformazioni su un insieme Q si denota con $\mathcal{T}(Q)$, quello di tutte le trasformazioni parziali con $\mathcal{F}(Q)$ e quello delle permutazioni su Q con $\mathcal{S}(Q)$. Quest'ultimo è, in effetti, un gruppo ed è chiamato *gruppo simmetrico* dell'insieme Q.

Nel caso particolare $Q = \{1, 2, \dots n\}$ vengono usate anche le notazioni $\mathcal{T}_n, \mathcal{F}_n$ ed $\mathcal{S}_n$.

Tali semigruppi di trasformazioni sono di fondamentale importanza nello studio dei semigruppi. Vale infatti il seguente risultato.

Proposizione 1.1.31. *Ogni semigruppo S è isomorfo ad un sottosemigruppo di $\mathcal{T}(S^1)$. In particolare, ogni semigruppo finito è isomorfo ad un sottosemigruppo di $\mathcal{T}_n$ per qualche n.*

Cayley ha dimostrato un simile risultato per i gruppi.

Teorema 1.1.32 (Teorema di Cayley)**.** *Ogni gruppo G è isomorfo ad un sottogruppo di $\mathcal{S}(G)$. In particolare ogni gruppo finito è isomorfo ad un sottogruppo di $\mathcal{S}_n$ per qualche n.*

Dato G un gruppo di permutazioni su un insieme Q si definisce *grado* di G la cardinalità di Q.

Proposizione 1.1.33. *Siano G un gruppo di permutazioni transitivo su un insieme Q e $p \in Q$. Il sottogruppo $H \leq G$ di permutazioni che fissano p ha indice Card (Q).*

Dimostrazione. Per ogni $q \in Q$ esisterà, essendo G transitivo, un elemento $g_q \in G$ tale che $p \cdot g_q = q$. Per ogni altro $g \in G$ tale che $p \cdot g = q$ si avrà $p \cdot g g_q^{-1} = p$ il che implica $g g_q^{-1} \in H$ da cui $g \in H_{g_q}$. Dunque ogni $g \in G$ è in una classe laterale H_{g_q} con $q \in Q$. Essendo tali classi laterali a due a due disgiunte il loro numero è esattamente Card (Q). □

Due gruppi di permutazioni G su un insieme R ed H su un insieme S saranno detti *equivalenti* se esiste una biezione $\beta : R \to S$ ed un isomorfismo $\sigma : G \to H$ tale che

$$\beta(rg) = \beta(r)\sigma(g) \quad \forall\, g \in G, r \in R, \tag{1.2}$$

ovvero se il diagramma in Figura 1.1 è commutativo per ogni $g \in G$.

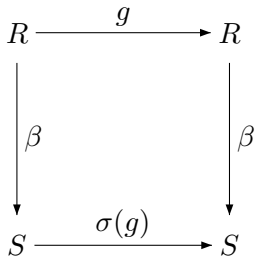


Figura 1.1: G ed H, gruppi di permutazioni rispettivamente su R e su S, sono equivalenti.

Un gruppo di permutazioni G sarà detto *regolare* se tutti gli elementi $g \in G \setminus \{1_G\}$ sono privi di punto fisso, ovvero se

$$q \cdot g = q \text{ per qualche } q \in Q \quad \Longrightarrow \quad g = 1_G.$$

Proposizione 1.1.34. *Un gruppo di permutazioni transitivo e Abeliano è regolare.*

Dimostrazione. Sia $g \in G$ un elemento avente un punto fisso $p \in Q$, ovvero tale che $pg = p$. Mostriamo che $g = 1_G$, ovvero che per ogni $q \in Q$ si ha $qg = q$.

Poiché G transitivo esisterà un $h \in G$ tale che $p = qh$. Dall'Abelianità di G ricaviamo $q(hg) = q(gh) = (qg)h = qh$ ed essendo h è una permutazione ciò implica $qg = q$. □

1.1.6 Generatori, grafo di Cayley

Dato un sottoinsieme A di un semigruppo S, il sottosemigruppo di S *generato* da A è il più piccolo semigruppo di S contenente A. Esso si denota con $\langle A \rangle$ ed è ottenuto intersecando tutti i sottogruppi di S contenenti A, ovvero considerando tutti i possibili prodotti $a_1 a_2 \cdots a_n$ di elementi di A.

In maniera simile, dato un monoide M ed un suo sottoinsieme A si definisce *sottomonoide generato* da X il sottosemigruppo generato da A con l'aggiunta dell'identità 1_S.

Nel caso di un gruppo G, il *sottogruppo generato* da $A \subseteq G$ è definito analgomente ed è formato da tutti i prodotti $a_1 a_2 \cdots a_n$ dove gli a_i sono o elementi di A o inversi di elementi di A.

Un semigruppo (risp. monoide, gruppo) generato da un insieme A sarà detto *A-generato*.

Dato un monoide (risp. gruppo) A-generato M, si definisce *grafo di Cayley destro* di M il grafo che ha per vertici gli elementi di M e per lati le triple (m, a, ma) con $m \in M$ e $a \in A$.

In maniera analoga si definisce *grafo di Cayley sinistro* di M il grafo che ha per vertici gli elementi di M e per lati le triple (m, a, am) con $m \in M$ e $a \in A$.

In Figura 1.2 è rappresentato il grafo di Cayley destro del monoide B_2^1 visto nell'Esempio 1.1.5

Un semigruppo (risp. monoide, gruppo) generato da un solo elemento è detto *semigruppo ciclico* (risp. *monoide ciclico*, *gruppo ciclico*). Ovvero S è ciclico se è della forma

$$S = \{a^n \mid n \in \mathbb{N}\}$$

con, nel caso S possegga un'identità, $a^0 = 1$.

Se S è un semigruppo ciclico infinito (risp. monoide ciclico infinito, gruppo ciclico infinito) allora esso è isomorfo al semigruppo additivo $\mathbb{N}_+$ (risp. al monoide additivo $\mathbb{N}$, al gruppo additivo $\mathbb{Z}$).

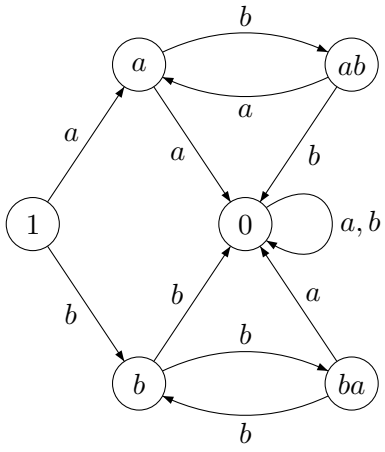


Figura 1.2: Grafo di Cayley destro di B_2^1.

Nel caso S sia invece un gruppo ciclico finito, si chiamano *indice* e *periodo* di S i più piccoli interi positivi i e p tali che $a^{i+p} = a^i$.

In tal caso il semigruppo S avrà $i + p - 1$ elementi e sarà della forma

$$S = S_{i,p} = \{a, a^2, \ldots, a^{i-1}, a^i, \ldots, a^{i+p-1}\}.$$

Il grafo destro di Cayley del monoide $M_{i,p} = S_{i,p}^1$, con $i + p$ elementi è rappresentato in Figura 1.3.

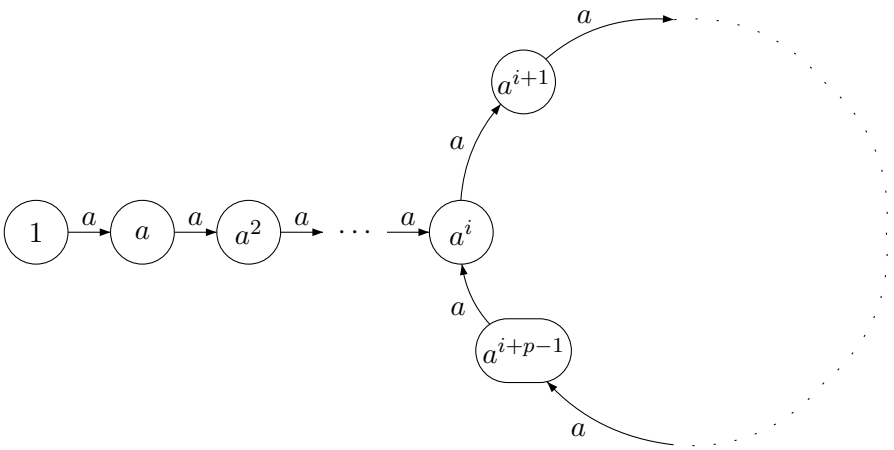


Figura 1.3: Grafo di Cayley destro di $M_{i,p}$.

Una struttura fondamentale nel nostro studio è quella del monoide libero. Dato un insieme A, detto *base* del semigruppo, il *semigruppo libero* è il

semigruppo A^+ ottenuto considerando tutte le possibili concatenazioni non vuote di elementi di A.

Il *monoide libero* A^* è il monoide $(A^+)^1$ con elemento neutro la parola vuota.

Il *gruppo libero* A° generato da A è definito come segue. Sia $\bar{A}$ un insieme in corrispondenza biunivoca con A e tale che $A \cap \bar{A} = \emptyset$. Denotiamo con $^-\colon A \to \bar{A}$ tale corrispondenza e con $\bar{a}$ l'immagine di a; possiamo estendere la funzione $^-$ ad $a \in A \cup \bar{A}$ ponendo $\bar{\bar{a}} = a$.

Sia $\sim_\delta$ la relazione di equivalenza su $\left(A \cup \bar{A}\right)^*$ definita da

$$ua\bar{a}v \sim_\delta uv \quad \forall\, u, v \in \left(A \cup \bar{A}\right)^* \; a \in A \cup \bar{A}.$$

Sia $\sim_\rho$ la chiusura riflessiva e transitiva di $\sim_\delta$. La relazione $\sim_\rho$ è una congruenza ed il monoide quoziente $A^\circ = \left(A \cup \bar{A}\right)^* / \sim_\rho$ è un gruppo. Infatti, per ogni $a \in A \cup \bar{A}$ si ha

$$a\bar{a} \sim_\rho 1.$$

Ciò mostra che le immagini dei generatori, e dunque tutti gli elementi di A°, sono invertibili.

Ogni elemento di A° è una classe di equivalenza di elementi di $\left(A \cup \bar{A}\right)^*$. Chiameremo *ridotto* il rappresentante di lunghezza minima di una classe di equivalenza. Esso è unico ed è caratterizzato dal non contenere come fattore $a\bar{a}$ per $a \in A \cup \bar{A}$. Ovvero $w = a_1 a_2 \dots a_{n+1}$ è ridotto se $a_{i+1} \neq \bar{a_i}$ per ogni $1 \leq i \leq n$.

Anche gli elementi del monoide libero A^* possono esser visti come elementi ridotti di A° poiché non contengono lettere di $\bar{A}$. Dunque A^* può essere pensato come sottomonoide di A°.

Chiameremo *rango* di A° il numero di elementi $\mathrm{Card}\,(A)$ dell'insieme A.

Tutti gli insiemi generanti un gruppo libero di rango k hanno almeno k elementi. In tale ambito useremo il termine *base* per indicare un insieme minimale di generatori per il gruppo. Si dimostra che tutte le basi di un gruppo libero di rango k hanno esattamente k elementi.

Sia H un sottogruppo di rango n e di indice d del gruppo libero di rango k. Allora vale la seguente formula detta *formula di Schreier*

$$n = d(k-1) + 1. \tag{1.3}$$

Nel caso di un gruppo generico G chiameremo *rango minimo* di G la cardinalità di un insieme minimale di generatori per G. Dunque nel caso di gruppi liberi le nozioni di rango e di rango minimo coincideranno.

1.1.7 Residuali, fattori

Sia M un monoide e siano $x, y \in M$. Si definiscono gli insiemi

$$x^{-1}y = \{z \in M \mid xz = y\} \qquad \text{e} \qquad xy^{-1} = \{z \in M \mid x = zy\}.$$

Tale notazione è estesa anche ai sottoinsiemi $X, Y \subseteq M$

$$X^{-1}Y = \bigcup_{x \in X} \bigcup_{y \in Y} x^{-1}y \qquad \text{e} \qquad XY^{-1} = \bigcup_{x \in X} \bigcup_{y \in Y} xy^{-1}.$$

L'insieme $X^{-1}Y$ è detto *residuale sinistro di* Y, mentre XY^{-1} è il *residuale destro* di X.

Dati tre sottoinsiemi $X, Y, X \subseteq M$, valgono le seguenti identità

$$(XY)^{-1} Z = Y^{-1} \left(X^{-1} Z\right) \qquad \text{e} \qquad X^{-1} \left(Y Z^{-1}\right) = \left(X^{-1} Y\right) Z^{-1}.$$

Di seguito useremo le più sintetiche notazioni XA^{-} ed $A^{-}X$ al posto rispettiamente di $X\left(A^{+}\right)^{-1}$ e $\left(A^{+}\right)^{-1}X$.

Dato un sottoinsieme X di un monoide M si definisce l'insieme dei *fattori* degli elementi di X, o più sinteticamente l'insieme dei fattori di X

$$F(X) = \{m \in M \mid \exists\, u, v \in M \ : \ umv \in X\},$$

ovvero l'insieme $F(X) = M^{-1}XM^{-1}$. Il complementare $M \setminus F(X)$ è spesso denotato come $\bar{F}(X)$ o $F(X)^c$.

1.1.8 Serie formali

Uno strumento molto utile in teoria dei codici è lo studio delle serie formali (si veda [4]).

Siano A un insieme e K un semianello. Una *serie formale*, o semplicemente *serie*, su A a coefficienti in K è una funzione $\sigma : A^* \to K$. Per lo studio delle serie useremo la notazione (σ, w) al posto di $\sigma(w)$. In tale ambito, il valore $\sigma(w)$ viene denotato con (σ, w).

L'insieme di tutte le serie formali su A sarà indicato con $K\langle\langle A \rangle\rangle$. Il *supporto* di una serie sarà l'insieme

$$\operatorname{supp}(\sigma) = \{w \in A^* \mid (\sigma, w) \neq 0\}.$$

Denoteremo con $K\langle A \rangle$ l'insieme delle serie $\sigma \in K\langle\langle A \rangle\rangle$ a supporto finito.

Un elemento p di $K\langle A \rangle$ sarà chiamato *polinomio*. Se $p \neq 0$, si definisce il *grado* di p, e lo si denota con $\deg(p)$, la lunghezza massima delle parole in $\operatorname{supp}(p)$. Il grado del polinomio nullo lo si pone pari a $-\infty$.

Date due serie $\sigma, \tau \in K\langle\langle A \rangle\rangle$ e dato $k \in K$, è possibile definire le serie $\sigma + \tau$, $\sigma\tau$ e $k\sigma$ ponendo:

$$(\sigma + \tau, w) = (\sigma, w) + (\tau, w),$$

$$(\sigma\tau, w) = \sum_{uv = w} (\sigma, u)(\tau, w),$$

$$(k\sigma, w) = k(\sigma, w).$$

Nella seconda equazione la somma è finita, poiché scorre tra le $1+|w|$ coppie (u, v) tali che $w = uv$.

$K\langle\langle A\rangle\rangle$ contiene due serie importanti, denotati con 0 e 1 e definite come

$$(0, w) = 0 \ \forall w \in A^* \qquad (1, w) = \begin{cases} 1 & \text{se } w = 1, \\ 0 & \text{altrimenti.} \end{cases}$$

Si userà la scrittura compatta σ^n per indicare il prodotto $\sigma\sigma\cdots\sigma$ (n volte) e si porrà $\sigma^0 = 1$.

Con le operazioni su definite l'insieme $K\langle\langle A\rangle\rangle$ risulta essere un semianello.

L'elemento $(\sigma, 1)$ sarà detto *termine costante* della serie σ.

Denoteremo con σ^* e σ^+ le serie

$$\sigma^* = \sum_{n\geq 0} \sigma^n \qquad \text{e} \qquad \sigma^+ = \sum_{n>0} \sigma^n.$$

Notiamo che $\sigma^* = 1 + \sigma^+$ e che $\sigma^+ = \sigma\sigma^* = \sigma^*\sigma$.

Proposizione 1.1.35. *Sia K un anello con unità e sia $\sigma \in K\langle\langle A\rangle\rangle$ una serie con termine costante nullo. Allora $1-\sigma$ è invertibile e $\sigma^* = (1-\sigma)^{-1}$.*

Dimostrazione. Per quanto visto sopra si ha

$$1 = \sigma^* - \sigma^+ = \sigma^* - \sigma^*\sigma = \sigma^*(1-\sigma).$$

Simmetricamente si ha $1 = (1-\sigma)\sigma^*$, da cui la tesi. □

Dato un insieme $X \subseteq A^*$ si definisce la *serie caratteristica* di X, e la si denota con $\underline{X}$, la serie data da

$$(\underline{X}, x) = \begin{cases} 1 & \text{se } x \in X \\ 0 & \text{altrimenti} \end{cases}.$$

Quando l'insieme $X = \{x\}$ è un singleton, si scriverà semplicemente x al posto di $\underline{x}$. Data questa notazione è possibile scrivere

$$\underline{X} = \sum_{x\in X} x.$$

Vediamo di seguito alcune proprietà delle serie caratteristiche

Proposizione 1.1.36. *Siano $X, Y \subseteq A^*$. Allora*

$$(\underline{X} + \underline{Y}, w) = \begin{cases} 0 & \textit{se } w \notin X \cup Y \\ 1 & \textit{se } w \in (X \cup Y) \setminus (X \cap Y) \\ 2 & \textit{se } w \in X \cap Y \end{cases}$$

Dalla Proposizione 1.1.36 si deduce, in particolare, che se $Z = X \cup Y$ allora

$$\underline{X} + \underline{Y} = \underline{Z} \qquad \Longleftrightarrow \qquad X \cap Y = \emptyset.$$

Dati due insiemi $X, Y \subseteq A^*$, il prodotto XY è detto *non ambiguo* se ogni parola $w \in XY$ può essere scritta come $w = xy$ con $x \in X$ e $y \in Y$.

Proposizione 1.1.37. *Siano $X, Y \subseteq A^*$. Allora*

$$(\underline{XY}, w) = \mathit{Card}\{(x, y) \in X \times Y | w = xy\}.$$

In particolare, dalla Proposizione 1.1.37 si deduce che, dato $Z = XY$ si ha

$$\underline{Z} = \underline{XY} \quad \Longleftrightarrow \quad XY \text{ è non ambiguo.}$$

Dalle proposizioni viste si ricava il seguente fondamentale risultato.

Proposizione 1.1.38. *Sia $X \subseteq A^+$. Allora*

$$((\underline{X})^*, w) = \mathit{Card}\{(x_1, \ldots, x_n) \,|\, n \geq 0,\, x_i \in X,\, w = x_1 x_2 \cdots x_n\}.$$

Dimostrazione. Per la definizione di $(\underline{X})^*$, si ha

$$((\underline{X})^*, w) = \sum_{k \geq 0} ((\underline{X})^k, w).$$

Applicando la Proposizione 1.1.37 si ottiene

$$((\underline{X})^k, w) = \mathrm{Card}\{(x_1, \ldots, x_k) \,|\, x_i \in X,\, w = x_1 x_2 \cdots x_k\},$$

da cui la tesi. □

1.2 Parole, Linguaggi, Codici

In questa Sezione riprenderemo il concetto di monoide libero definito nella Sottosezione 1.1.6 che qui sarà definito monoide delle parole finite. Nella Sottosezione 1.2.2 vedremo varie possibilità per rendere tale monoide ordinato. Nella Sottosezione 1.2.3 estenderemo le nozioni viste al caso infinito (a destra) e nella Sottosezione 1.2.4 consideremo una classe particolare di parole. Il concetto di fattorizzazione sarà introdotto nella Sottosezione 1.2.5. Dopo aver introdotto nella Sottosezione 1.2.6 i linguaggi, ossia degli insiemi di parole, ci concentreremo nella Sottosezione 1.2.7 su una particolare classe di essi, i codici, definiti dal fatto che ogni parola ha un'unica fattorizzazione in termini di suoi elementi. Infine nella Sottosezione 1.2.8 ci concentreremo sui parse e sulle interpretazioni, argomenti che svilupperemo poi nei Capitolo 2 e 4.

1.2.1 Parole

Sia A un insieme detto *alfabeto* i cui elementi sono chiamati *lettere*. Una *parola finita* w nell'alfabeto A è una sequenza finita di elementi di A della forma $(a_1, a_2, \ldots, a_n)$ con $a_i \in A$ ed $n \in \mathbb{N}$.

Prese due parole $u = (a_1, a_2, \ldots a_n)$ e $v = (b_1, b_2, \ldots b_m)$ il *prodotto*, o *concatenazione*, di u e v è la parola

$$uv = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots b_m).$$

Tale prodotto ha come identità la *parola vuota* 1, o ε, corrispondente alla sequenza vuota. Esso è inoltre associativo. Per tale ragione si possono indicare le parole tramite semplice giustapposizione di lettere, ossia nella forma $w = a_1 a_2 \ldots a_n$.

Come già visto nella Sezione precedente (Sottosezione 1.1.6), l'insieme di tutte le parole non vuote, denotato A^+, dotato dell'operazione di concatenazione è un semigruppo detto semigruppo libero. Aggiungendo la parola vuota come elemento neutro, otteniamo il monoide libero A^*. Tale monoide sarà detto, appunto, *monoide delle parole (finite)*.

Data una parola $w = a_1 a_2 \ldots a_n$ con $a_i \in A$, si definisce *lunghezza* di w, e la si denota con $|w|$, il numero n di lettere in w. Per definizione la lunghezza della parola vuota 1 è 0. La funzione $\ell : A^* \to \mathbb{N}$ che associa $w \mapsto |w|$ è un morfismo di monoidi. Il sottoinsieme di A^* dato dalle parole di lunghezza n è denotato A^n, ovvero $A^n = \{w \in A^* \mid |w| = n\}$.

Data una parola $w = a_1 a_2 \ldots a_n$, l'intero i è detto *occorrenza* della lettera a in w se $a_i = a$.

Il numero di occorrenze di una lettera a in una parola w si denota $|w|_a$. Sussiste, chiaramente, la relazione

$$|w| = \sum_{a \in A} |w|_a.$$

L'insieme delle lettere che compaiono in una parola w si indica con $\mathrm{alph}(w)$, ovvero $\mathrm{alph}(w) = \{a \in A \mid |w|_a > 0\}$. Tale notazione si estende ai sottoinsiemi X di A^* ponendo

$$\mathrm{alph}(X) = \bigcup_{x \in X} \mathrm{alph}(x).$$

Esempio 1.2.1. Consideriamo la parola $w = abbab$ nell'alfabeto $A = \{a, b, c, \}$. Si ha $|w|_a = 2$, $|w|_b = 3$ e $|w|_c = 0$. La lunghezza della parola è $|w| = 5$ mentre $\mathrm{alph}(w) = \{a, b\}$.

Data una parola $w = a_1 a_2 \cdots a_n$, un intero $p \geq 1$ è detto *periodo* di w se $a_i = a_{i+p}$ per ogni $i = 1, \ldots n - p$. Il più piccolo periodo di w è detto *il* periodo di w.

Una parola $w \in A^+$ è detta *primitiva* se non è potenza di alcuna altra parola di A^+, ovvero se si ha l'implicazione

$$w = u^n \text{ con } u \in A^+ \quad \Longrightarrow \quad n = 1 \text{ e } w = u.$$

1.2.2 Ordine delle parole

Nell'insieme delle parole è possibile definire delle relazioni d'ordine, sia parziali che totali.

La prima e più semplice relazione d'ordine totale che si può dare su A^* è quella data delle lunghezze, ponendo $u \leq v$ se e solo se $|u| \leq |v|$.

Sia $w = a_1 a_2 \dots a_n \in A^*$. La parola u è detta *fattore* di w se $u = a_i a_{i+1} \dots a_j$ per $1 \leq i \leq j \leq n$. Ovvero u è un fattore di w se esistono due parole $v, v' \in A^*$ tali che $w = vuv'$. Nel caso $u \neq w$, ovvero se $w = vuv'$ con v e v' non entrambi uguali alla parola vuota, si dirà che u è un *fattore proprio* di w. In particolare se $w = vuv'$ con $v, v' \in A^+$, allora u sarà detto *fattore interno* di w.

La relazione "essere fattore di" è una relazione d'ordine parziale su A^* (totale se $|A| = 1$).

L'insieme di tutti i fattori di una parola w è denotato con $F(w)$. La notazione si estende ad un insieme $X \subseteq A^*$ denotando con $F(X) = \bigcup_{x \in X} F(x)$.

Una parola u sarà detta *prefisso* di w se u è un *fattore sinistro* di w, ovvero se esiste una $v \in A^*$ tale che $w = uv$; nel caso $v \in A^+$, u sarà detto prefisso *proprio* di w.

Analogamente si definisce *suffisso* (risp. suffisso *proprio*), o *fattore destro* di w una parola u per cui esiste una $v \in A^*$ (risp. A^+) tale che $w = vu$.

Anche le relazioni "essere prefisso di" ed "essere suffisso di" sono relazioni d'ordine parziali su A^* (totale se $|A| = 1$). In particolare riferendoci all'*ordine prefisso* scriveremo $u \leq v$ quando u è un prefisso di v e $u < v$ quando $u \leq v$ e $u \neq v$.

Osservazione 1.2.2. Se due parole w e w' sono entrambe prefisse di una parola u allora w e w' sono comparabili, ovvero si ha $w \leq w'$ o $w' \leq w$.

Dato un insieme X diremo che una parola w è un *prefisso per* X se essa è prefissa di una parola $x \in X$.

Un insieme $P \subset A^*$ sarà detto *chiuso per fattori* (risp. *chiuso per prefissi*, *chiuso per suffissi*) se contiene tutti i fattori (risp. prefissi, suffissi) dei suoi elementi, ovvero se $uwv \in P \Rightarrow w \in P$ (risp. $uv \in P \Rightarrow u \in P$, $uv \in P \Rightarrow v \in P$).

Data una parola $x \in A^*$, indicheremo con $F(x)$ l'insieme di tutti i fattori di x.

Due relazioni d'ordine totali di fondamentale impotanza sono l'ordine lessicografico, ossia quello dei vocabolari, e quello militare. In entrambi i casi supponiamo di avere un ordine totale sull'alfabeto A.

L'*ordine lessicografico*, o *alfabetico*, è definito ponendo $u \prec v$ se u è un prefisso proprio di v oppure se $u = ras, v = rbt$, con $a, b \in A$, $r, s, t \in A^*$ e $a < b$. Chiaramente si userà la notazione $u \preceq v$ se $u \prec v$ o $u = v$.

Osservazione 1.2.3. L'ordine lessicografico è stabile a sinistra, ovvero $u \preceq v \iff wu \preceq wv$.

L'ordine *militare*, o *metrico-lessicale*, ordina le parole prima in base alla lunghezza e poi in base all'ordine lessicografico, ovvero lo si definisce ponendo $u < v$ se $|u| < |v|$ o se $|u| = |v|$ e $u \prec v$.

Osservazione 1.2.4. L'ordine militare è stabile sia a sinistra che a destra, ovvero se $u \leq v$ allora $xuy \leq xvy$ per ogni $x, y \in A^*$.

1.2.3 Parole infinite

Molti dei concetti e delle definizioni espresse sin d'ora (e molte di quelle che esprimeremo in seguito) sono estendibili alla classe delle parole infinite.

Così come le parole finite sono state definite come sequenze finite di lettere, è possibile definire le parole *infinite* (a destra) come le sequenze di lettere in A con indice in $\mathbb{N}$. L'insieme di tutte le parole infinite lo si denota con $A^{\mathbb{N}}$ o A^ω. L'insieme di tutte le parole finite ed infinite (a destra) è denotato con $A^\infty = A^* \cup A^\omega$.

Esempio 1.2.5. Sia $a \in A$. La parola infinita a^ω è la sequenza infinita $(a, a, \ldots)$.

Il prodotto uv è definito per ogni $u \in A^*$ e $v \in A^\omega$. Una parola finita w è detta fattore di una parola infinita u se $u = xwy$ con $x \in A^*$ e $y \in A^\omega$. Anche in questo caso l'insieme $F(w)$ sarà l'insieme di tutti i fattori della parola w. Un prefisso (risp. suffisso) di una parola $w \in A^\omega$ è una parola $u \in A^*$ (risp. $v \in A^\omega$) tale che esiste $v \in A^\omega$ (risp. $u \in A^*$) per cui si abbia $w = uv$.

Anche l'ordine lessicogafico si può estendere al caso infinito, ponendo $u < v$ se e soltanto se $u = wau', v = wbv'$ per qualche $w \in A^*$, $a, b \in A$, con $a < b$ è $u', v' \in A^\omega$.

Una parola infinita $x = a_1 a_2 \cdots$ con $a_i \in A$ è detta *periodica* se esiste un intero $n \geq 1$ tale che $a_{i+n} = a_i$ per ogni $i \geq 1$. Sarà detta *definitivamente periodica* se da un certo punto in poi tutti i suoi suffissi sono periodici, ovvero se $x = uy$ con $u \in A^*$ e y una parola infinita periodica. Il seguente risultato, dovuto a Coven e Hedlund, è ben noto (si veda [10, Teorema 1.3.13]).

Teorema 1.2.6 (Coven e Hedlund, 1973)**.** *Sia $x \in A^\omega$ una parola infinita su un alfabeto A di k lettere. x è definitivamente periodica se e solo se esiste un intero $d \geq 1$ tale che x ha al più $d + k - 2$ fattori di lunghezza d.*

Nella Sezione 3.2 generalizzeremo tale risultato.

1.2.4 Palindrome

Il *rovescio* di una parola $w = a_1 a_2 \dots a_n$ è la parola $\widetilde{w} = a_n a_{n-1} \dots a_1$ ottenuta leggendo w da destra verso sinistra. In particolare il rovescio della parola vuota sarà la parola vuota.

Osservazione 1.2.7. Per ogni coppia di parole $u, v \in A^*$ si ha $\widetilde{uv} = \widetilde{v}\,\widetilde{u}$.

Un insieme X di parole è detto *chiuso per rovescio* se contiene i rovesci di tutti i suoi elementi, ovvero se $x \in X \;\Rightarrow\; \widetilde{x} \in X$.

Una *parola palindroma* è una parola w che coincide col proprio rovescio $\widetilde{w}$. Se $|w|$ è pari, allora w è palindroma se e solo se è della forma $w = x\widetilde{x}$ per $x \in A^*$; se invece la sua lunghezza è dispari la condizione necessaria e sufficiente è $w = xa\widetilde{x}$ per $x \in A^*$ e $a \in A$.

La *chiusura palindromica* di una parola w è la più piccola parola palindroma che ha w come prefisso ed è denotata come $w^{(+)}$. La *chiusura palindromica iterata* di una parola w è la parola Pal(w) definita ricorsivamente come

- $\mathrm{Pal}(1) = 1$;
- $\mathrm{Pal}(ua) = (\mathrm{Pal}(u)a)^{(+)} \quad \forall\, u \in A^*\ a \in A$.

Essendo $\mathrm{Pal}(u)$ un prefisso proprio di $\mathrm{Pal}(ua)$, ha senso definire la chiusura palindromica iterata di una parola infinita x come il limitie delle chiusure palindromiche iterate dei prefissi di x.

Definiamo adesso, per ogni lettera $a \in A$, il morfismo ψ_a da A^* in se stesso, detto *morfismo elementare*, come

$$\psi_a(b) = \begin{cases} ab & \text{se } b \neq a \\ a & \text{altrimenti.} \end{cases}$$

Tale notazione si estende anche alle parole $u \in A^*$ definendo $\psi_u = \psi(u)$ dove $\psi : A^* \to \mathrm{End}(A^*)$ è il morfismo da A^* nel monoide degli endomorfismi di A^* definito da $\psi(a) = \psi_a$ per ogni $a \in A$. Dunque date tre parole u, v, w in A^* si ha la relazione

$$\psi_{uv}(w) = \psi_u(\psi_v(w)).$$

Si può dimostrare che tali morfismi elementari, che nel caso del monoide A^* sono degli endomorfismi, definiscono degli automorfismi nel gruppo libero A°.

Usando i morfismi elementari è possibile dare una forma elegante per la chiusura palindromica di un prodotto di due parole. La *formula di Justin* è la seguente:

$$\mathrm{Pal}(uv) = \psi_u\left(\mathrm{Pal}(v)\right)\mathrm{Pal}(u).$$

Tale formula può essere estesa al caso in cui u sia una parola in A^* e v sia una parola infinita, ottenendo

$$\mathrm{Pal}(uv) = \psi_u\left(\mathrm{Pal}(v)\right).$$

1.2.5 Fattorizzazioni

Definiamo *fattorizzazione* di una parola $w \in A^*$ una sequenza $(u_1, u_2, \ldots, u_n)$ con $n \geq 1$, $u_i \in A^+$ per $2 \leq i \leq n-1$ e $u_1, u_n \in A^*$ tali che $w = u_1 u_2 \cdots u_n$.

Il *contenuto* di una sequenza $\alpha = (u_1, u_2, \ldots u_n)$ di parole $u_i \in A^*$ è la parola $c(\alpha) = u_1 u_2 \cdots u_n$.

Data una fattorizzazione $\alpha = (u_1, u_2, \ldots, u_n)$ denotiamo con

$$P(\alpha) = \{u_1, u_1u_2, \ldots, u_1u_2 \cdots u_{n-1}\}.$$

Date due fattorizzazioni α, β di $w \in A^*$ diremo che β è più *fine* di α, e scriveremo $\alpha < \beta$, se $P(\alpha) \subseteq P(\beta)$. La relazione "essere più fine di" è una relazione d'ordine parziale. Il *supremum* di due fattorizzazioni $\alpha = (u_1,\ u_2,\ \ldots\ u_n)$ e $\beta = (v_1, v_2, \ldots v_m)$ di una parola w, denotato con $\alpha \vee \beta$, è l'unica fattorizzazione $\gamma = (w_1, w_2, \ldots w_p)$ di w tale che $P(\gamma) = P(\alpha) \cup P(\beta)$.

Esempio 1.2.8. La parola ab ha 8 fattorizzazioni distinte rappresentate in Figura 1.4 ordinate verticamente per finezza.

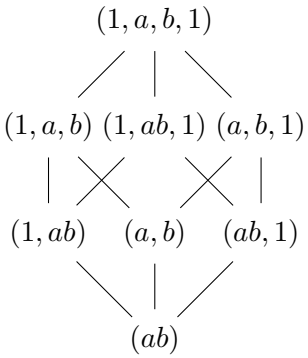


Figura 1.4: Fattorizzazioni della parola ab.

Due fattorizzazioni $\alpha = (u_1, u_2, \ldots u_n)$ e $\beta = (v_1, v_2, \ldots v_m)$ di una parola w sono dette *adiacenti*, se $u_1u_2 \cdots u_i = v_1v_2 \cdots v_j$ (e dunque $u_{i+1}u_{i+2} \cdots u_n = v_{j+1}v_{j+2} \cdots v_m$) per opportuni i, j con $1 \leq i \leq n-1$ e $1 \leq j \leq m-1$. Ovvero α e β sono adiacenti se $P(\alpha) \cap P(\beta) \neq \emptyset$. Due fattorizzazioni non adiacenti sono dette *disgiunte*.

Diremo che una fattorizzazione $\alpha = (u_1, u_2, \ldots, u_m)$ è *n-periodica* rispetto ad un codice X se e solo se il numero di fattori non vuoti consecutivi u_i con $2 \leq i \leq m-1$ il cui prodotto è in X è costante ed è pari ad n.

Formalmente α sarà n-periodica rispetto ad X se dati r, ℓ con $1 \leq \ell \leq r \leq m-1$ si ha

$$u_{\ell+1}u_{\ell+2}\cdots u_r \in X \quad \Longleftrightarrow \quad r - \ell = n.$$

Qualora non sussistano ambiguità si indicherà una fattorizzazione $\alpha = (u_1u_2\cdots u_n)$ di w semplicemente con $w = u_1u_2\cdots u_n$.

1.2.6 Linguaggi

Dato un alfabeto finito A, un sottoinsieme L di A^* è detto *linguaggio*. In altre termini un linguaggio è una collezione, finita o infinita, di parole su un certo alfabeto.

Esempio 1.2.9. Sia $A = \{0, 1\}$. L'insieme $\{0^n10^m \mid n, m \geq 0\}$ è il linguaggio delle parole in A contenenti un solo 1.

Sui linguaggi è possibile definire diverse operazioni. Oltre alle classiche *operazioni Booleane* – ossia *unione*, *intersezione*, *complemento* rispetto ad A^*, *differenza* e *differenza divisa* – si può definire il *prodotto* di linguaggi come già definito per gli insiemi nell'Esempio 1.1.3.

Per quanto visto nell'Esempio 1.1.12 l'insieme dei linguaggi ha una struttura di semianello. Per tale ragione spesso si usa il simbolo + al posto di $\cup$ e si denota il linguaggio vuoto $\emptyset$ con 0 ed il linguaggio $\{1\}$ con 1. Un'altra convenzione è quella di denotare il singleton $\{w\}$ semplicemente con w.

Osservazione 1.2.10. Se l'alfabeto A contiene almeno due lettere, allora il semianello dei linguaggi non è commutativo.

Dato un linguaggio L, si definisce la sua *potenza n-sima* L^n come il prodotto di L per se stesso n volte, ovvero

$$L^0 = 1, \qquad L^n = L^{n-1}L$$

Osservazione 1.2.11. Nonostante la notazione uguale bisogna stare attenti a non confondere le potenze dei linguaggi L^0 ed L^1 con i semigruppi e monoidi dotati di zero ed identità definiti nella sezione 1.1.1.

La *star* di un linguaggio L, denotata con L^* è l'unione, denotata come somma, di tutte le potenze di L, ossia $L^* = \sum_{n\geq 0} L^n$. L'operatore *più* di un liguaggio L è definito considerando l'unione delle potenze non negative di L, ovvero $L^+ = \sum_{n>0} L^n$. Ovviamente si ha l'uguaglianza $L^* = L^+ \cup 1$.

Secondo quanto appena definito si hanno le seguenti formule:

$$0^* = 1^* = 1 \qquad \text{mentre} \qquad 0^+ = 0 \ \text{ e } \ 1^+ = 1.$$

Un linguaggio è detto *razionale*, o *regolare*, se è possibile ottenerlo a partire dai linguaggi 0 e a con $a \in A$ usando un numero finito di volte le operazioni unione, prodotto e star.

Esempio 1.2.12. Sia $A = \{a, b\}$. Il linguaggio $L = (a + ab + ba)^*$ è razionale.

Si dimostra che i linguaggi razionali sono stabili per morfismi, ossia se $\varphi : A^* \to B^*$ è un morfismo ed L è un linguaggio razionale di A^* allora $\varphi(L)$ sarà un linguaggio razionale di B^*.

1.2.7 Codici

Se prendiamo un linguaggio L ed una parola $w \in L^*$, per definizione esisteranno delle parole $u_1, u_2, \dots u_n \in L$ tali che $w = u_1 u_2 \dots u_n$. Tale fattorizzazione $(u_1, u_2, \dots u_n)$ di w sarà detta essere una *L-fattorizzazione*. È utile spesso rappresentare una L-fattorizzazione come in Figura 1.5

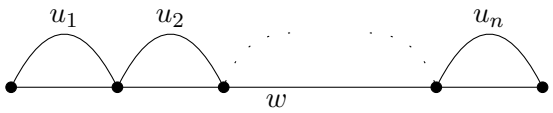


Figura 1.5: Una L-fattorizzazione di w

Un sottoinsieme X di A^* è un *codice* su A se per ogni $n, m \geq 0$ e per ogni $x_1, x_2, \dots, x_n$, $y_1, y_2, \dots, y_m \in X$ si ha l'implicazione:

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \quad \Longrightarrow \quad n = m \text{ e } x_i = y_i \, \forall \, i = 1, \dots n.$$

Ovvero X è un codice se ogni parola di X^* ha un'unica X-fattorizzazione.

Osservazione 1.2.13. Chiaramente un codice non conterrà mai la parola 1. Inoltre ogni sottoinsieme di un codice è esso stesso un codice. In particolare l'insieme vuoto è un codice.

Esempio 1.2.14. Per ogni alfabeto A, l'insieme $X = A$ è un codice. Più in generale, per ogni $n \in \mathbb{N}$, l'insieme $X = A^n$ è un codice, detto il *codice uniforme* su A delle parole di lunghezza n.

Si dimostra, inoltre, che se $X \subset A^*$ è un codice allora sarà un codice anche X^n al variare di $n > 0$.

Esempio 1.2.15. L'insieme $X = \{a, ab, ba\}$ non è un codice poiché, ad esempio, la parola $w = aba$ ha due X-fattorizzazione distinte: $w = (a)(ba) = (ab)(a)$.

Un sottoinsieme X di A^* sarà detto *prefisso* se nessun elemento di X è prefisso di un altro elemento di X, ovvero se dati due elementi $x, x' \in X$ si ha l'implicazione

$$x \leq x' \Rightarrow x = x'.$$

Analogamente si definisce *suffisso* un sottoinsieme X di A^* tale che nessun elemento di X è suffisso di un altro elemento di X.

Un insieme sarà detto *bifisso* se è sia prefisso che suffisso.

È facile dimostrare che ogni insieme $X \neq \{1\}$ prefisso (risp. suffisso, bifisso) è un codice. Per tale ragione ogni insieme prefisso (risp. suffisso, bifisso) $X \neq \{1\}$ sarà detto *codice prefisso* (risp. *suffisso*, *bifisso*).

Esempio 1.2.16. I codici uniformi sono bifissi.

Un codice X sarà detto *massimale* su A se non è contenuto propriamente in nessun altro codice su A, ovvero se

$$X \subset X' \text{ con } X' \text{ codice} \quad \Longrightarrow \quad X = X'.$$

Si dimostra (si veda, ad esempio, [4, Proposizione 2.1.14]) che ogni codice X su un alfabeto A è contenuto in un codice massimale su A.

Un codice X sarà detto *massimale prefisso* (risp. *massimale suffisso*, *massimale bifisso*) su A se non è contenuto propriamente in alcun altro codice prefisso (risp. suffisso, bifisso) su A.

Esempio 1.2.17. I codici uniformi A^n, con $n \in \mathbb{N}$ sono codici massimali bifissi.

Sia X un codice prefisso (risp. suffisso). Il sottomonoide $M = X^*$ generato da X è unitario a destra (risp. a sinistra). Viceversa, ogni sottomonoide unitario a destra (risp. a sinistra) di A^* è generato da un codice prefisso (risp. suffisso) (si veda [4]).

Dato un sottogruppo $H \leq A^\circ$ del gruppo libero, il sottomonoide $H \cap A^*$ è unitario a destra e a sinistra e quindi, per quanto appena visto, generato da un codice bifisso.

Un sottogruppo $H \leq A^\circ$ di A° è detto *positivamente generato* se esiste un insieme $X \subseteq A^*$ che genera H.

Proposizione 1.2.18. *Sia $H \leq A^\circ$ un sottogruppo positivamente generato del gruppo libero A°. Allora esiste un codice bifisso X che genera H.*

Dimostrazione. Se H è positivamente generato allora un insieme che lo genera è proprio $H \cap A^*$. Tale $H \cap A^*$ è, per quanto già visto, generato da un opportuno codice bifisso X. Dunque X genera il sottogruppo H. □

Importante nello studio algebrico dei codici è lo studio della *serie caratteristica* $\underline{X}$ di un insieme $X \subset A^*$ (si veda Sottosezione 1.1.8). Ad esempio, si vede facilmente che $X \subseteq A^*$ è un codice se e solo se $((\underline{X})^*, w) \leq 1$ per ogni $w \in A^*$.

Il seguente risultato è in [4, Proposizione 3.1.6]

Proposizione 1.2.19. *Sia X un codice prefisso su A e sia $P = A^* \setminus XA^*$. Allora*

$$\underline{X} - 1 = \underline{P}(\underline{A} - 1) \quad e \quad \underline{A}^* = \underline{X}^*\underline{P}$$

In particolare la seconda equazione della Proposizione precedente ci dice che, se X è un codice prefisso, ogni parola può essere scritta in un'unica maniera come composizione di parole di X e di una parola incomparabile per prefissi con X.

Un risultato duale rispetto alla Proposizione 1.2.19 vale nel caso X sia un codice suffisso ed $S = A^* \setminus A^*X$. in tal caso si avrà $\underline{A}^* = \underline{SX}^*$ e $\underline{X} - 1 = (\underline{A} - 1)\underline{S}$.

1.2.8 Parse ed interpretazioni

Sia $X \subseteq A^*$ un insieme. Un *parse* di una parola w rispetto ad X è una tripla (u, x, v) tale che u non ha suffissi in X, x è una concatenazione di parole di X, v non ha prefissi in X e uxv sia una fattorizzazione di w (Figura 1.6). Formalmente (u, x, v) è un parse se si ha $w = uxv$ con $u \in A^* \setminus A^*X$, $x \in X^*$ e $v \in A^* \setminus XA^*$.

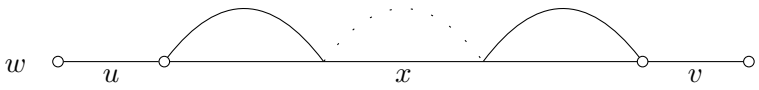


Figura 1.6: Un parse di w rispetto ad X.

Consideriamo adesso il caso in cui $X \subseteq A^+$ sia un codice. Siano $P = XA^-$ ed $S = A^-X$ gli insiemi rispettivamente dei prefissi propri e dei suffissi propri di X. Una *interpretazione* di una parola $w \in A^*$ rispetto ad X è una fattorizzazione $w = uxv$ con $u \in S$, $x \in X^*$ e $v \in P$.

Osservazione 1.2.20. Se X è un codice bifisso, ogni interpretazione di una parola w rispetto ad X è anche un parse di w rispetto ad X. Infatti in tal caso si avrebbe

$$A^-X \subseteq A^* \setminus A^*X \quad \text{e} \quad XA^- \subseteq A^* \setminus XA^*.$$

Ricorrendo alla notazione della Sottosezione 1.2.5, chiameremo interpretazione rispetto al codice X una fattorizzazione $\alpha = (u, x_1, x_2, \ldots, x_n, v)$ di w tale che $u \in S$, $n \geq 0$, $x_i \in X$ e $v \in P$.

Dunque un'interpretazione α è una fattorizzazione con almeno due termini: uno iniziale, che indicheremo con s_α, suffisso proprio di X ed uno finale, che indicheremo con p_α. Come termine intermedio tra i due vi è una sequenza $(x_1, x_2, \ldots, x_n)$, eventualmente vuota, di parole di X che denoteremo con f_α.

Due interpretazioni di una parola w saranno dette *adiacenti* se le fattorizzazioni corrispondenti sono adiacenti (si veda Figura 1.7). Analogamente si definisce il concetto di interpretazioni *disgiunte*.

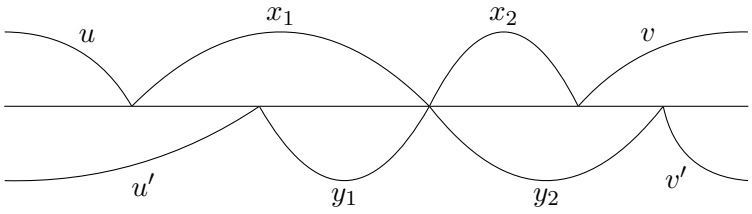


Figura 1.7: Due interpretazioni adiacenti.

Due interpetazioni α, β di una stessa parola w sono dette *connesse* se $w = uxv$ con $u, v \in A^*$ e $x \in X^*$ tali che $u \in P(\alpha)$ e $ux \in P(\beta)$.

Due interpretazioni α, β di w sono dunque connesse se e solo se esiste un'interpretazione γ di w adiacente sia ad α che a β (si veda Figura 1.8).

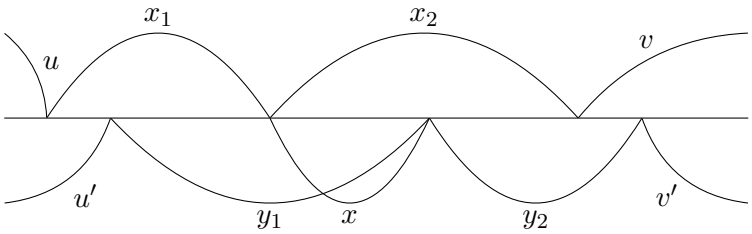


Figura 1.8: Due interpretazioni connesse.

Due interpretazioni adiacenti sono sempre connesse. In generale, però, non vale il viceversa, come mostrato nel seguente Esempio.

Esempio 1.2.21. Siano $A = \{a, b\}$ ed $X = \{aab, aabbb, baa, bba, bbb\}$. La parola $w = aabbba$ ha due interpretazioni disgiunte, ovvero $\alpha = (aa, bbb, a)$ e $\beta = (1, aab, bba, 1)$. Entrambe sono però adiacenti all'interpretazione $\gamma = (1, aabbb, a)$, quindi connesse tra loro.

Due interpretazioni di una stessa parola che non risultano connesse saranno dette *indipendenti*.

Poiché per quanto visto ogni interpretazione è una fattorizzazione, dato un insieme J di interpretazioni di una parola w è possibile considerare il supremum di J. Esso sarà della forma $(u_1, u_2, \dots u_m)$ e sarà tale che per ogni k con $1 \leq k \leq m-1$ esisterà un elemento di J che raffina la fattorizzazione $(u_1 \cdots u_k, u_{k+1} \cdots u_m)$.

Abbiamo già definito nella Sottosezione 1.1.7 il concetto di residuale di un insieme X. Nel caso di un insieme formato da una sola parola $X = \{w\} \subseteq A^*$ sarà equivalente scrivere $u^{-1}\{w\}$ o $u^{-1}w$. Esso sarà un sottoinsieme di A^*

di cardinalità al più 1. Nel caso $u^{-1}w$ sia non vuoto identificheremo tale insieme con la parola v tale che $w = uv$.

Trasportando il concetto di residuale di un insieme alle sequenze, definiremo per ogni lettera $a \in A$ ed ogni sequenza $\alpha = (u_1, u_2, \dots u_n)$ di parole $u_i \in A^*$ con $n \geq 1$ la seguenza $a^{-1}\alpha$ data da

$$a^{-1}\alpha = \begin{cases} a^{-1}(u_2, u_3, \dots u_n) & \text{se } u_1 = 1, \\ (a^{-1}u_1, u_2, \dots u_n) & \text{se } u_1 \in aA^*, \\ \emptyset & \text{altrimenti.} \end{cases}$$

Data una lettera $a \in A$ ed una fattorizzazione α di una parola $w \in A^+$ si ha che $a^{-1}\alpha$ ed $a^{-1}w$ sono non vuote se e solo se $w \in aA^*$. In tal caso $a^{-1}\alpha$ sarà una fattorizzazione di $a^{-1}w$.

Esempio 1.2.22. Abbiamo già visto nell'Esempio 1.2.8 che la parola $w = ab$ ha 8 fattorizzazioni distinte (si veda Figura 1.4). La 4 fattorizzazioni distinte della parola $a^{-1}w$ sono rappresentate in Figura 1.9.

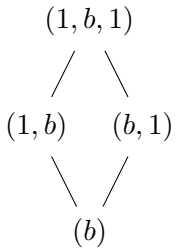


Figura 1.9: Fattorizzazioni della parola $a^{-1}(ab) = b$.

Interpretazioni e residuali sono legati dai due seguenti risultati.

Proposizione 1.2.23. *Siano $a \in A$, $w \in aA^*$ una parola non vuota iniziante per a ed α un'interpretazione di w rispetto ad un codice X. Se $s_\alpha \neq 1$ o f_α è non vuoto, allora $a^{-1}\alpha$ è un'interpretazione di $a^{-1}w$.*

Dimostrazione. Sia $\alpha = (s, x_1, x_2, \dots x_n, p)$ con $s \in A^-X$, $n \geq 0$, $x_i \in X$ e $p \in XA^-$.

- Se $s \neq 1$ allora $a^{-1}\alpha = (a^{-1}s, x_1, x_2, \dots, x_n, p)$.
- Se $s = q$ ed $n \geq 1$ allora $a^{-1}\alpha = (a^{-1}x_1, x_2, \dots, x_n, p)$.

In entrambi i casi la tesi è verificata. □

Proposizione 1.2.24. *Siano $a \in A$, $w \in aA^*$ una parola non vuota iniziante per a ed α, β due interpretazioni indipendenti di w rispetto ad un codice X. Se $s_\alpha \neq 1$ o f_α è non vuoto, allora $a^{-1}\alpha$ ed $a^{-1}\beta$ sono due interpretazioni indipendenti di $a^{-1}w$*

Dimostrazione. Per la Proposizione 1.2.23 sappiamo che $a^{-1}\alpha$ ed $a^{-1}\beta$ sono entrambe interpretazioni di $a^{-1}w$.

Supponiamo, per assurdo, che $a^{-1}\alpha$ ed $a^{-1}\beta$ siano connesse. Allora esisterebbero $u, v \in A^*$ ed $x \in X^*$ tali che $a^{-1}w = uxv$ con $u \in P(a^{-1}\alpha)$ ed $ux \in P(a^{-1}\beta)$. Dunque si avrebbe $w = auxv$ con $au \in P(\alpha)$ ed $aux \in P(\beta)$, contraddicendo l'indipendenza di α e β. □

Consideriamo adesso un insieme J di n interpretazioni di una parola w rispetto ad un codice X. Sia $\sigma = (u_1, u_2, \dots u_m)$ il supremum di J. Per ogni $\alpha \in J$ avremo $w = sxp$ con $s = s_\alpha$, $x = c(f_\alpha)$ e $p = p_\alpha$.

Per quanto visto in precedenza esisteranno (e saranno unici) degli interi i, j con $1 \leq i \leq n$ e $i \leq j \leq m-1$ tali che

$$s = u_1 u_2 \cdots u_i, \quad x = u_{i+1} u_{i+2} \cdots u_j, \quad p = u_{j+1} u_{j+2} \cdots u_m. \tag{1.4}$$

Definiamo le seguenti quantità

$$\lambda(\alpha, J) = i - 1, \quad \mu(\alpha, J) = j - 1, \quad \nu(\alpha, J) = m - j - 1. \tag{1.5}$$

Dunque $\lambda(\alpha, J), \mu(\alpha, J)$ e $\nu(\alpha, J)$ rappresentano il numero di parole u_k che compongono ciascuno dei tre termini dell'interpretazione, non contando le due parole estremali (eventualmente vuote).

Un insieme J di n interpretazioni di una parola w rispetto ad un codice X sarà detto *ciclico* se il suo supremum $(u_1, u_2, \dots u_m)$ è n-periodico rispetto ad X.

Proposizione 1.2.25. *Sia J un insieme ciclico di n interpretazioni di una parola w rispetto ad un codice X. Allora per ogni $\alpha \in J$ si avrà $\mu(\alpha, J) \equiv 0 \pmod n$.*

Dimostrazione. Sia $\sigma = (u_1, u_2, \dots u_m)$ il supremum di J. Essendo J ciclico, σ, vista come fattorizzazione, è n-periodica. Dunque, ogni parola di X che appare in $c(f_\alpha)$ è un prodotto di n elemento consecutivi non vuoti di σ. □

Proposizione 1.2.26. *Sia J un insieme ciclico di n interpretazioni di una parola w rispetto ad un codice X. Allora gli elementi di J sono a due a due disgiunti.*

Dimostrazione. Siano $\sigma = (u_1, u_2, \dots u_m)$ il supremum di J ed $\alpha, \beta \in J$ due interpretazioni connesse.

Poiché α è un elemento di J avremo $s_\alpha = u_1 u_2 \cdots u_i$ per un opportuno $1 \leq i \leq n-1$. Dalla Proposizione 1.2.25 ricaviamo che per ogni r tale che $i \leq r \leq m-1$ si ha

$$u_1 u_2 \cdots u_r \in P(\alpha) \Rightarrow u_{i+1} u_{i+2} \cdots u_r \in X^* \Rightarrow r \equiv i \pmod n,$$

da cui, sottraendo 1 ad entrambi i membri, otteniamo

$$u_1 u_2 \cdots u_r \in P(\alpha) \Rightarrow r - 1 \equiv \lambda(\alpha, J) \pmod n.$$

Essendo α, β connessi, per definizione, esisteranno $u, v \in A^*$ e $x \in X^*$ tali che $w = uxv$ con $u \in P(\alpha)$ e $ux \in P(\beta)$. Possiamo scrivere $u = u_1u_2 \cdots u_\ell$ e $x = u_{\ell+1}u_{\ell+2} \cdots u_r$ per opportuni ℓ, r.

Per quanto visto sopra si ha, dunque, $\lambda(\alpha, J) \equiv \ell - 1 \pmod{n}$ e $\lambda(\beta, J) \equiv r - 1 \pmod{n}$. Essendo $x \in X^*$ si ha anche, per la Proposizione 1.2.25, $r - \ell \equiv 0 \pmod{n}$. Dunque otteniamo $\lambda(\alpha, J) \equiv \lambda(\beta, J) \pmod{n}$ e da ciò $\lambda(\alpha, J) = \lambda(\beta, J)$.

Analogamente si dimostra che $\nu(\alpha, J) = \nu(\beta, J)$. Quindi $\alpha = \beta$. □

Esempio 1.2.27. Siano $A = \{a, b\}$ un alfabeto, $X = \{aab, abaa, abab, baba\}$ un codice su A e $w = ababaababa$ una parola di A^*.

L'insieme $J = \{(1, abab, aab, aba), (a, baba, abab, a), (ab, abaa, baba, 1)\}$ è un insieme di interpretazioni per w. J è ciclico, infatti il suo supremum è la fattorizzazione 3-periodica $(1, a, b, ab, a, a, b, ab, a, 1)$ di w con $m = 10$ fattori.

1.3 Automi

In questa Sezione introdurremo gli automi, uno degli argomenti principali dell'informatica teorica nonché uno strumento importantissimo in combinatoria delle parole. Le nozioni basilari compariranno nella Sottosezione 1.3.1, mentre nelle Sottosezioni 1.3.2 e 1.3.3 si definiranno delle particolari famiglie di automi, ossia gli automi deterministici, gli automi non ambigui, gli automi completi, gli automi trim e quelli semplici.

Nella Sottosezione 1.3.4 parleremo del concetto fondamentale di monoide sintattico. Infine, nell'ultima Sottosezione definiremo gli automi di gruppi che sfrutteremo poi nel Capitolo 4.

1.3.1 Automi, cammini, linguaggi riconosciuti

Un *automa* (finito) è una quintupla $\mathcal{A} = (Q, A, E, I, T)$ dove Q è un insieme (finito) chiamato insieme degli *stati*, A è un alfabeto, $E \subseteq Q \times A \times Q$ è l'insieme dei *lati* o *transizioni* ed I e T sono sottoinsiemi di Q detti rispettivamente insiemi degli stati *iniziali* e *finali*.

Quando non sussistono ambiguità sull'alfabeto e sull'insieme delle transizioni, si scriverà più semplicemente $\mathcal{A} = (Q, I, T)$.

Graficamente un automa viene rappresentato tramite un grafo etichettato e orientato con vertici gli stati ed archi le transizioni. Gli stati iniziali sono indicati tramite frecce entranti mentre quelli finali con un doppio bordo.

Esempio 1.3.1. L'automa rappresentato in Figura 1.10 ha come insieme degli stati $\{1, 2\}$ e come transizioni le triple $(1, a, 2), (1, b, 1), (2, a, 1), (2, b, 2)$. Lo stato 1 è sia iniziale che finale.

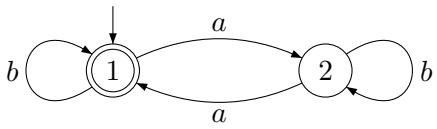


Figura 1.10: Un automa.

Due transizioni $f_1 = (p_1, a_1, q_1)$ ed $f_2 = (p_2, a_2, q_2)$ sono dette *consecutive* se $q_1 = p_2$. Un *cammino* (finito) nell'automa $\mathcal{A}$ è una sequenza (finita) $c = (f_1, f_2, \dots f_n)$ di transizioni consecutive $f_i = (q_i, a_i, q_{i+1})$ con $1 \leq i \leq n$. L'intero n è detto *lunghezza* del cammino c, la parola $w = a_1 a_2 \cdots a_n$ è l'*etichetta* del cammino c mentre gli stati q_1 e q_{n+1} sono detti rispettivamente *origine* e *fine* del cammino.

Per indicare un cammino c con origine p, fine q ed etichetta w useremo la notazione

$$c : p \xrightarrow{w} q$$

o, più semplicemente, scriveremo $p \cdot w = q$. Quando non esiste alcun cammino con origine p ed etichetta w scriveremo $p \cdot w = \emptyset$.

Per convenzione si considera, per ogni stato $q \in Q$ un cammino, detto *cammino nullo*, di lunghezza 0 da q in se stesso con etichetta la parola vuota 1, ovvero si pone $q \cdot 1 = q$.

Un automa può esser visto come un multigrafo etichettato dotato di due particolari sottoinsiemi di vertici, gli stati iniziali e quelli finali. Il multigrafo avente come vertici gli stati $q \in Q$ e come insieme di lati E è detto *grafo sottostante* l'automa. Un automa è detto *fortemente connesso* se il suo grafo sottostante è fortemente connesso, ovvero se per ogni $p, q \in Q$ esiste un cammino c avente origine in p e fine in q.

Un cammino $c : i \longrightarrow t$ da uno stato iniziale $i \in I$ ad uno stato finale $t \in T$ è detto *accettato*. L'insieme delle etichette dei cammini accettati da un automa $\mathcal{A}$ è un linguaggio su A detto linguaggio *riconosciuto* da $\mathcal{A}$ ed è indicato con $L(\mathcal{A})$. Dunque $L(\mathcal{A}) = \{w \in A^* \mid i \cdot w \in T \text{ per qualche } i \in I\}$.

Due automi che riconoscono lo stesso linguaggio sono detti *equivalenti*.

Un linguaggio $L \subseteq A^*$ è detto *riconoscibile* se è riconosciuto da un automa finito, ovvero se esiste un automa finito $\mathcal{A}$ tale che $L = L(\mathcal{A})$.

Una generalizzazione degli automi è data dai transduttori, in cui ad ogni cammino è associata una doppia etichetta. Formalmente un *transduttore* (finito) è una sestupla $\mathcal{T} = (Q, A, B, E, I, T)$ dove Q è un insieme detto degli *stati*, $I, T \subseteq Q$ due suoi sottoinsiemi detti rispettivamente degli stati *iniziali* e *finali*, A, B due alfabeti detti rispettivamente di *input* e di *output* ed $E \subseteq Q \times A \times B \times Q$ l'insieme delle *transizioni*.

Estendendo la notazione degli automi indicheremo un *cammino*, ovvero una sequenza di transizioni consecutive, tramite la notazione $c : p \xrightarrow{u|v} q$ con $p, q \in Q$ stati rispettivamente *iniziale* e *finale*, $u \in A^*$ e $v \in B^*$ etichette rispettivamente di *input* e di *output*.

Analogamente si estenderanno i concetti di *lunghezza* di un cammino, cammino *accettato*, etc.

Un transduttore sarà detto *ad input semplice* se si ha l'implicazione

$$(p, u, v, q), (p, u, v', q) \in E \quad \Rightarrow \quad v = v'.$$

Un transduttore ad input semplice definisce in maniera naturale un automa sull'alfabeto di input chiamato *automa di input*, ottenuto considerando solo le etichette di input.

Un esempio di transduttore è mostrato in Figura 1.11

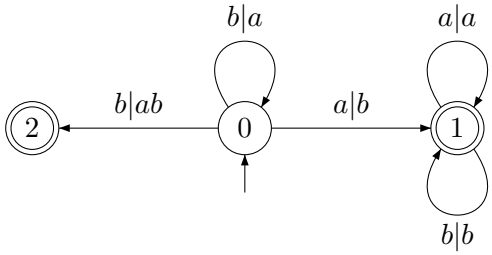


Figura 1.11: Un transduttore.

1.3.2 Automi deterministici ed automi completi

Un automa $\mathcal{A} = (Q, I, T)$ è detto *deterministico* se $I = \{i\}$ è un singleton di Q e se per ogni stato $p \in Q$ e per ogni lettera $a \in A$ esiste al più un unico $q \in Q$ tale che (p, a, q) è una transizione di $\mathcal{A}$, ovvero se

$$(p, a, q), (p, a, q') \in E \quad \Rightarrow \quad q = q'.$$

Nel caso l'automa abbia come unico stato iniziale i useremo la notazione $\mathcal{A} = (Q, i, T)$ invece di $\mathcal{A} = (Q, \{i\}, T)$.

Esempio 1.3.2. L'automa rappresentato in Figura 1.12 è deterministico.

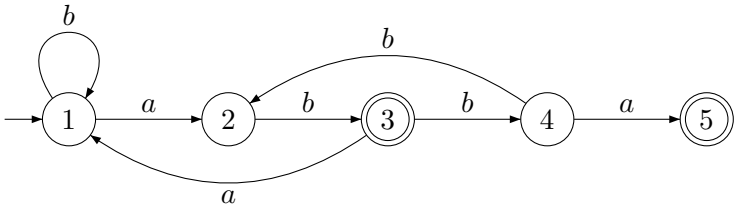


Figura 1.12: Un automa deterministico.

Proposizione 1.3.3. *Ogni automa finito è equivalente ad un automa deterministico.*

La Proposizione 1.3.3 è ben nota e la sua dimostrazione si basa sulla cosiddetta *costruzione dei sottoinsiemi* (si veda [14]). Essa trasforma un automa $\mathcal{A} = (Q, I, T)$ nell'automa $D(\mathcal{A}) = (\mathcal{P}(Q), I, \mathcal{F})$ dove $\mathcal{P}(Q)$ è l'insieme delle parti di Q, $\mathcal{F} = \{P \subseteq Q \mid P \cap F \neq \emptyset\}$ e le transizioni sono date da

$$P \cdot a = \{q \in Q \mid p \cdot a = q \text{ per qualche } p \in P\}.$$

Tale costruzione converte un automa non deterministico avente n stati in un automa deterministico con al più 2^n stati.

Un automa $\mathcal{A} = (Q, I, T)$ è detto *non ambiguo* se per ogni $w \in A^*$ vi è al più un cammino da p in q etichettato con w. Chiaramente un automa deterministico è non ambiguo.

Un automa $\mathcal{A} = (Q, i, T)$ è detto *completo* se per ogni stato $p \in Q$ e per ogni lettera $a \in A$ esiste almeno uno stato $q \in Q$ tale che (p, a, q) è una transizione di $\mathcal{A}$, ovvero se $\forall\, p \in Q\,, a \in A$ si ha $p \cdot a \neq \emptyset$.

Esempio 1.3.4. L'automa rappresentato in Figura 1.10 è sia deterministico che completo.

1.3.3 Automi trim ed automi semplici

Uno stato $q \in Q$ è detto *accessibile* (risp. *coaccessibile*) se esiste un cammino $c : i \longrightarrow q$ con $i \in I$ (risp. $c : q \longrightarrow t$ con $t \in T$) ovvero se esiste un $w \in A^*$ tale che $i \cdot w = q$ per qualche $i \in I$ (risp. $q \cdot w = t$ per qualche $t \in T$). Un automa in cui ogni stato è sia accessibile che coaccessibile è detto *trim*.

Dato un automa $\mathcal{A}$ la *parte trim* di $\mathcal{A}$ è l'automa $\mathcal{A}' = (P,\ P \cup I,\ P \cup T)$ dove P è l'insieme degli stati di $\mathcal{A}$ contemporaneamente accessibili e coaccessibili.

Si può dimostrare che ogni automa deterministico è equivalente ad un automa trim.

Proposizione 1.3.5. *Per ogni codice $X \subseteq A^+$ esiste un automa semplice non ambiguo che riconosce X^*.*

Dimostrazione. Siano $\mathcal{A} = (Q, I, T)$ un automa trim e non ambiguo tale da riconoscere X ed E il suo insieme delle tranzizioni. Consideriamo l'automa $\mathcal{B} = (Q \cup \omega, \omega, \omega)$, con $\omega \notin Q$ un nuovo stato, con transizioni quelle di E più le triple (ω, a, q) tali che $(i, a, q) \in E$ per qualche $i \in I$, le triple (p, a, ω) tali che $(p, a, t) \in E$ per qualche $t \in T$ e le triple (ω, a, ω) tali che $(i, a, t) \in E$ per qualche $i \in I$ e $t \in T$.

Si vede facilmente che la parte trim di $\mathcal{B}$, che denoteremo con $\mathcal{A}^*$, è un automa semplice e non ambiguo che riconosce X^*. □

Osservazione 1.3.6. L'insieme delle etichette dei cammini semplici in $\mathcal{A}^*$ è esattamente X.

Un automa sarà detto *semplice* se è trim e se ha un unico stato iniziale, un'unico stato finale e questi due coincidono.

Sia $\mathcal{A} = (Q, i, i)$ un automa semplice. Un cammino $p \xrightarrow{w} q$ è detto *semplice* se esso non è il cammino nullo e se esso non passa per lo stato iniziale. Ovvero, se $w \neq 1$ e se per ogni fattorizzazione $w = uv$ si ha $p \xrightarrow{u} r \xrightarrow{v} q$ con $r \neq i$.

1.3.4 Automi minimali, monoide sintattico

In maniera analoga a quanto visto nella sottosezione 1.1.7 definiamo per ogni $u \in A^*$ gli insiemi non vuoti

$$u^{-1}X = \{v \in A^* \mid uv \in X\}$$

Per ogni insieme $X \subseteq A^*$ si dirà *automa minimale* di X l'automa $\mathcal{A}(X) = \{ Q, X, T \}$ che ha come insieme degli stati $Q = \{u^{-1}X \mid u \in A^*\}$, come stato iniziale X, come insieme degli stati finali $T = \{u^{-1}X \mid u \in X\}$ e come transizioni le triple $(u^{-1}X, a, (ua)^{-1}X)$ con $a \in A$. L'automa minimale $\mathcal{A}(X)$ è trim e riconosce l'insieme X.

Sia $\mathcal{A} = (Q, i, T)$ un automa. Denotiamo con $\varphi_{\mathcal{A}}$ il morfismo da A^* nel monoide $\mathcal{T}(Q)$ delle trasformazioni parziali da Q in Q definito da $p\varphi_{\mathcal{A}}(w) = q$ per ogni $q \in Q$ tale che $p \cdot w = q$. Il monoide $M = \varphi_{\mathcal{A}}(A^*)$ è detto *monoide di transizione* dell'automa $\mathcal{A}$.

Esempio 1.3.7. Il monoide di transizione dell'automa dell'Esempio 1.3.4 ha due elementi, immagini rispettivamente di a e b. Esso è il gruppo ciclico $\mathbb{Z}/2\mathbb{Z}$.

Un automa è fortemente connesso se e solo se il suo monoide di transizione è transitivo.

Il monoide di transizione dell'automa minimale $\mathcal{A}(X)$ è detto *monoide sintattico* di X (si veda anche Esempio 1.1.25).

Sia $X \subseteq A^+$ un codice prefisso. L'automa minimale di X^* è un automa semplice tale da riconoscere X^*. Viceversa si dimostra che ogni insieme riconosciuto da un automa semplice è un sottomonoide di A^* generato da un codice prefisso.

Siano $X \subseteq A^+$ un codice prefisso e $P = XA^-$ l'insieme dei suoi prefissi propri. L'*automa letterale* di X^* è l'automa semplice $\mathcal{A} = (P, 1, 1)$ con transizioni definite per $p \in P$ ed $a \in A$ da

$$p \cdot a = \begin{cases} pa & \text{se } pa \in P, \\ 1 & \text{se } pa \in X, \\ \emptyset & \text{altrimenti.} \end{cases}$$

Si può verificare che tale automa riconosce X^*.

1.3.5 Automi invertibili, automi di gruppo

Un automa semplice $\mathcal{A} = (Q, i, i)$ è detto *invertibile* se per ogni $a \in A$ la trasformazione parziale $\varphi_{\mathcal{A}} : p \to p \cdot a$ definita nella Sottosezione precedente è iniettiva. Sotto tale ipotesi è possibile costruire l'*inverso* dell'automa $\mathcal{A}$ come l'automa $\mathcal{A}^{-1} = (Q, i, i)$ avente lo stesso insieme degli stati, lo stesso stato iniziale e finale e come transizioni $q \cdot a = p$ per ogni transizione $p \cdot a = q$ di $\mathcal{A}$.

Ogni automa invertibile è minimale (si veda [13]). L'insieme riconosciuto da un automa invertibile è unitario sia a destra che a sinistra e, dunque, per quanto visto nella Sottosezione 1.2.7, è generato da un codice bifisso.

Vi è un collegamento tra i codici bifissi e gli automi invertibili, come mostrato nella seguente Proposizione (si veda [13]).

Proposizione 1.3.8. *Sia $X \subseteq A^+$ un codice bifisso. Le seguenti condizioni sono equivalenti:*

(*i*) $X^* = \langle X \rangle \cap A^*$;

(*ii*) *l'automa minimale di X^* è invertibile.*

Un automa $\mathcal{A} = (Q, i, i)$ tale che per ogni $a \in A$ la funzione $\varphi_{\mathcal{A}}(a) : p \mapsto p \cdot a$ è una permutazione su Q è detto *automa di gruppo*.

Esempio 1.3.9. L'automa dell'Esempio 1.3.4 è un automa di gruppo poiché $\varphi_{\mathcal{A}}(w)$ è una permutazione per ogni $w \in A^*$, essendo $\varphi_{\mathcal{A}}(a)$ e $\varphi_{\mathcal{A}}(b)$ permutazioni e la composizione di permutazioni ancora una permutazione.

Si dimostra che, se Q è un insieme finito, un automa di gruppo è sia invertibile sia completo.

Il monoide di transizione di un automa di gruppo è un gruppo di permutazioni su Q di grado $\mathrm{Card}\,(Q)$. Poiché l'automa è trim, tale gruppo sarà transitivo.

Il seguente risultato è presente in [1, Proposizione 6.1.5].

Proposizione 1.3.10. *Sia M un sottomonoide di A^*. Le seguenti condizioni sono equivalenti:*

(*i*) *M è riconosciuto da un automa di gruppo con d stati;*

(*ii*) *$M = \varphi^{-1}(H)$ con $H \leq G$ un sottogruppo di indice d di un gruppo G e $\varphi : A^* \to G$ un morfismo surgettivo;*

(*iii*) *$M = H \cap A^*$ con $H \leq A^\circ$ un sottogruppo di indice d del gruppo libero A°.*

Un codice bifisso Z tale che Z^* verifica una delle condizioni equivalenti della Proposizione 1.3.10 è detto *codice di gruppo* e l'intero d è detto il suo *grado*. Il monoide di transizione dell'automa minimale di Z^* è detto il *gruppo* di Z ed è denotato con $G(Z)$.

Osservazione 1.3.11. Poiché un automa di gruppo è minimale, l'automa di gruppo che riconosce Z^* è unico. Inoltre il grado di Z è uguale sia al grado del gruppo di permutazioni $G(Z)$ sia all'indice $[A^\circ : \langle Z \rangle]$.

Esempio 1.3.12. L'insieme $X = a \cup ba^*b$ è un codice di gruppo di grado 2. Il sottomonoide X^*, formato dalle parole in $\{a, b\}$ con un numero pari di b, è infatti riconosciuto dall'automa di gruppo dell'Esempio 1.3.4.

Sia $\mathcal{A} = (Q, i, T)$ un automa deterministico. Un *cammino generalizzato* è una sequenza $(p_0, a_1, p_1, a_2, \ldots, p_{n-1}, a_n, p_n)$ con $a_i \in A \cup \bar{A}$ e $p_i \in Q$ tale che per ogni $1 \leq i \leq n$ si abbia

$$p_{i-1} \cdot a_i = p_i \text{ se } a_i \in A \qquad \text{e} \qquad p_i \cdot \bar{a_i} = p_{i-1} \text{ se } a_i \in \bar{A}.$$

L'*etichetta* del cammino generalizzato è l'elemento $a_1 a_2 \cdots a_n \in A^\circ$. Un cammino in un automa può esser visto come un particolare cammino generalizzato.

Dato un automa $\mathcal{A} = (Q, 1, 1)$, l'insieme delle etichette dei suoi cammini generalizzati da 1 in 1 è un sottogruppo di A°. Esso è detto *sottogruppo descritto* da $\mathcal{A}$. In tal caso il sottomonoide di A^* riconosciuto da $\mathcal{A}$ è contenuto nel sottogruppo di A° descritto da $\mathcal{A}$.

Esempio 1.3.13. Sia $\mathcal{A} = (Q, 1, 1)$ l'automa con insieme di stati $Q = \{1, 2\}$ e transizioni $1 \cdot a = 1 \cdot b = 2$ e $2 \cdot a = 2 \cdot b = \emptyset$. Il sottomonoide riconosciuto da $\mathcal{A}$ è $\{1\}$ mentre il sottogruppo descritto da $\mathcal{A}$ è il gruppo ciclico generato da ab^{-1}.

Si può dimostrare che per ogni sottogruppo positivamente generato H di A°, esiste un unico automa invertibile $\mathcal{A}$ tale che H è il sottogruppo descritto da $\mathcal{A}$ (vedi [1, Proposizione 6.1.4]).

L'automa invertibile $\mathcal{A}$ tale che H è il sottogruppo descritto da $\mathcal{A}$ è detto *automa di Stallings* del sottogruppo H.

Capitolo 2

Insiemi fattoriali

In questo Capitolo riprenderemo il concetto di insieme fattoriale ed introdurremo quelli di insieme ricorrente, uniformemente ricorrente (Sezione 2.1) e Sturmiano (Sezione 2.2).

Nella Sezione 2.3 ci si occuperà di codici prefissi contenuti dentro un insieme fattoriale. La maggior parte dei risultati di tale Sezione sono estensioni di nozioni ben note nel caso generale.

Infine nella Sezione 2.4 specializzeremo tali risultati al caso di codici bifissi all'interno di insiemi ricorrenti.

2.1 Insiemi ricorrenti e parole ricorrenti

Di seguito studieremo una famiglia particolare di insiemi fattoriali: gli insiemi ricorrenti. Essi sono tali che per ogni coppia di parole u, v che vi appartengono ne esiste una terza w per cui anche uwv vi appartiene.

Anche per le parole esiste una nozione di ricorrenza. Una parola è ricorrente se ogni suo fattore compare infinite volte.

Vi è una profonda relazione tra insiemi e parole ricorrenti. La Proposizione 2.1.4 ci mostrerà, infatti, che gli insiemi ricorrenti sono tutti e soli gli insiemi dei fattori di una parola ricorrente.

Una proprietà più forte della ricorrenza è l'uniforme ricorrenza. Un insieme sarà detto uniformemente ricorrente se ogni suo elemento appare come fattore di tutti gli elementi di lunghezza opportuna. Analogamente, una parola sarà detta uniformemente ricorrente se il suo insieme dei fattori è uniformemente ricorrente.

2.1.1 Insiemi ricorrenti ed uniformemente ricorrenti

Dato un insieme $F \subseteq A^*$, l'*ordine destro* (risp. *sinistro*) di una parola w rispetto ad F è il numero delle lettere $a \in A$ tali che $wa \in F$ (risp. $aw \in F$).

Un insieme F è detto *essenzialmente destro* (risp. *sinistro*) se è chiuso per prefissi (risp. per suffissi) ed ogni parola $w \in F$ ha ordine destro (risp. sinistro) positivo. Chiaramente se F è essenzialmente destro (risp. sinistro), allora per ogni $u \in F$ e per ogni intero $n \geq 1$ esisterà una parola v di lunghezza n tale che $uv \in F$ (risp. $vu \in F$).

Una parola $u \in F$ sarà detta *speciale a destra* (risp. *a sinistra*) se il suo ordine destro (risp. sinistro) è almeno 2. Una parola speciale a destra sarà *stretta* se il suo ordine è esattamente pari al numero $\mathrm{Card}\,(A)$ delle lettere dell'alfabeto A.

Ricordiamo che un insieme F è detto *fattoriale* se contiene i fattori di tutti i suoi elementi. Un insieme F è detto essere *ricorrente* se è fattoriale e se per ogni $u, v \in F$ esiste una parola $w \in F$ tale che $uwv \in F$. Un insieme ricorrente $F \neq \{1\}$ è sia essenzialmente destro che essenzialmente sinistro.

Esempio 2.1.1. Sia $A = \{a, b\}$ e consideriamo F l'insieme delle parole in A che non presentino come fattore bb. Dunque $F = A^* \setminus A^*bbA^*$. Tale insieme è ricorrente poiché, dati $u, v \in F$, sicuramente anche $uav \in F$.

Un insieme F è detto essere *uniformemente ricorrente* se è fattoriale, essenzialmente destro e se per ogni $u \in F$ esiste un intero $n \geq 1$ tale che u è un fattore di ogni parola in F di lunghezza n, ovvero se u è fattore di ogni parola $w \in F \cap A^n$ per un opportuno n.

Proposizione 2.1.2. *Un insieme uniformemente ricorrente è ricorrente.*

Dimostrazione. Siano $u, v \in F$ e sia n l'intero tale che v è un fattore di ogni parola in $F \cap A^n$. Poiché F è essenzialmente destro, esiste una parola w di lunghezza n tale che $uw \in F$. Dunque v è fattore di w, ovvero si ha $w = rvs$ per opportune parole r, s. Da cui si ricava che $urw \in F$. □

L'implicazione inversa della Proposizione 2.1.2 non vale, come mostrato nel seguente Esempio.

Esempio 2.1.3. L'insieme $F = A^*$, con $A = \{a, b\}$, è banalmente ricorrente ma non è uniformemente ricorrente in quanto $b \in F$ ma, per ogni $n \geq 1$, b non è fattore di $a^n \in F$.

2.1.2 Parole ricorrenti ed uniformemente ricorrenti

L'insieme $F(x)$ dei fattori di una parola infinita $x \in A^\omega$ è un insieme fattoriale ed essenzialmente destro.

Una parola infinita $x \in A^\omega$ è detta *ricorrente* se ogni suo fattore ha un infinito numero di occorrenze in x, ovvero se per ogni $u \in F(x)$ esiste una $v \in F(x)$ tale che $uvu \in F(x)$.

Le nozioni di insieme ricorrente e di parola ricorrente sono strettamente correlate come afferma la seguente Proposizione.

Proposizione 2.1.4. *Gli insiemi ricorrenti sono tutti e soli della forma $F(x)$ per un'opportuna parola infinita x ricorrente.*

Dimostrazione. Consideriamo un insieme ricorrente $F = \{u_1, u_2, \ldots\}$. Essendo F ricorrente, presi $u_1, u_2 \in F$ esisterà una parola $v_1 \in F$ tale che $u_1 v_1 u_2 \in F$. Inoltre, presi $u_1 v_1 u_2, u_3 \in F$ esisterà una parola $v_2 \in F$ tale che $u_1 v_1 u_2 v_2 u_3 \in F$. Procedendo in tal modo otterremo una parola infinita $x = u_1 v_1 u_2 v_2 \cdots$ tale che $F(x) = F$. Tale x è ricorrente, infatti per ogni $u \in F = F(x)$ esisterà una $v \in F$ tale che $uvu \in F$.

Supponiamo adesso che x sia una parola ricorrente. L'insieme $F = F(x)$ è ricorrente. Siano, infatti, $u, v \in F(x)$. Vi è dunque una fattorizzazione $x = puy$ per opportuni $p \in F$ e $y \in A^\omega$. Essendo x ricorrente, v sarà un fattore anche di y, ovvero possiamo fattorizzare $y = qvz$ per opportuni $q \in F$ e $z \in A^\omega$. Dunque si ha $x = puqvz$, ovvero $uqv \in F$, da cui la tesi. □

Similmente a quanto visto sopra, una parola infinita $x \in A^\omega$ sarà detta *uniformemente ricorrente* se l'insieme $F(x)$ è uniformemente ricorrente. Anche in questo caso esistono parole infinite ricorrenti che non sono uniformemente ricorrenti, come mostrato nel seguente Esempio.

Esempio 2.1.5. Consideriamo la parola infinita x ottenuta concatenando tutte le parole in $A = \{a, b\}$ seguendo l'ordine metrico-lessicale. Dunque x è la parola

$$x = a\,b\,aa\,ab\,ba\,bb\,aaa\,aab\,aba\,abb\,baa\,bab\,bba\,bbb\,aaaa\,aaab\cdots$$

Tale parola, detta di *Champernowne*, è ricorrente poiché ogni fattore appare infinite volte. Essa non è però uniformemente ricorrente poiché, essendo a^n un fattore di x per ogni $n \geq 1$, si possono trovare due occorrenze consecutive della lettera b a distanza arbitraria.

2.2 Insiemi Sturmiani

Di seguito introdurremo una particolare famiglia di parole su un alfabeto binario, le parole Sturmiane, e la loro estensione ad alfabeti con cardinalità arbitraria, le parole episturmiane. Esse sono le parole non periodiche di complessità minima.

Una caratterizzazione degli insiemi di fattori di una parola episturmiana stretta, detto insieme Sturmiano, sarà data nella Proposizione 2.2.7.

2.2.1 Parole episturmiane

Di seguito chiameremo *sostituzione* un morfismo di monoidi da A^* in se stesso.

Sia $f : A^* \to A^*$ una sostituzione tale che vi sia una lettera $a \in A$ che venga mandata in una parola che abbia come prefisso proprio a, ovvero tale

che $f(a) \in aA^+$. Da tale ipotesi segue che le parole $f^n(a)$ per $n \geq 1$ sono ognuna un prefisso proprio della successiva e che $|f^n(a)| \to \infty$. Denotiamo con $f^\omega(a)$ la parola infinita avente $f^n(a)$, al variare di $n \in \mathbb{N}$, come prefissi. Essa sarà detta un *punto fisso* di f.

Esempio 2.2.1. Sia $A = \{a, b\}$. Il *morfismo di Thue-Morse* è la sostituzione $f : A^* \to A^*$ tale che $f(a) = ab$ e $f(b) = ba$. Il punto fisso $f^\omega(a)$ di f è la parola

$$x = abbabaabbaababbabaababba\cdots$$

Tale parola, detta *parola di Thue-Morse*, è uniformemente ricorrente. Infatti, né aaa né bbb sono fattori di x, dunque due occorrenze successive di a, o di b, sono separate al più da due simboli. Ciò implica che anche due occorrenze del blocco $f^n(a)$, o di $f^n(b)$, con $n \geq 1$, sono separati da al più due blocchi. Poiché ogni fattore di x appare in $f^k(a)$ o in $f^k(b)$ per un opportuno k, segue che tale fattore riapparirà in x dopo una distanza limitata.

L'insieme dei fattori di x è detto *insieme di Thue-Morse*.

Una parola infinita w nell'alfabeto $A = \{a, b\}$ sarà detta *parola Sturmiana* se per ogni $n \geq 0$ vi sono esattamente $n + 1$ fattori di w di lunghezza n, ovvero se $\forall\, n \geq 0$ si ha $\mathrm{Card}\,(F(x) \cap A^n) = n + 1$.

Esempio 2.2.2. Il *morfismo di Fibonacci* sull'alfabeto $A = \{a, b\}$ è la sostituzione $\varphi : A^* \to A^*$ definita da $\varphi(a) = ab$ e $\varphi(b) = a$. La *parola di Fibonacci*

$$f = abaababaabaababaababaabaababaabaab\cdots$$

è il punto fisso $f = \varphi^\omega(a)$ di φ. Per dimostrare che f è Sturmiana introduciamo le *parole finite di Fibonacci* $f_{-1} = b$, $f_i = \varphi^i(a)$ per $i \geq 0$.

Poiché $f = \varphi(f)$, essa sarà un prodotto di vari ab e a. Quindi la parola bb non sarà mai un fattore di f. Dunque i fattori di lunghezza 2 sono esattamente 3. Inoltre la parola aaa non è mai un fattore di $f = \varphi(f)$ in quanto, altrimenti, questa sarebbe un prefisso di un qualche $\varphi(x)$ con x un fattore di f e ciò implicherebbe che x inizi con bb. Dunque i fattori di lunghezza 3 sono esattamente 4.

Mostriamo adesso che f ha esattamente un fattore speciale a destra di lunghezza n per ogni $n \geq 0$.

Per prima cosa notiamo che data una parola x, axa e bxb non possono essere contemporaneamente in $F(f)$. Dimostriamolo per induzione sulla lunghezza di x. Abbiamo già visto la validità nel caso in cui consideriamo la parola vuota. Supponiamo adesso, per assurdo, che vi sia una parola x tale che sia axa che bxb siano fattori di f. Non essendo bb in $F(f)$ sicuramente x inizierà e terminerà con a, ovvero sarà della forma $x = aya$ per un'opportuna $y \in F(f)$. Dunque sia $aayaa$ che $bayab$ saranno fattori di $\varphi(f)$. Da ciò ricaviamo che esisterà una parola $z \in F(f)$ tale che $\varphi(z) = ay$. Quindi avremo $aaya = \varphi(bzb) \in F(f)$; inoltre, poiché f non inizia con b e $bb \notin F(f)$

avremo anche $abayab = \varphi(aza) \in F(f)$. Ovvero $aza, bzb \in F(f)$ con $|z| \leq \varphi(z) < |x|$, contraddicendo l'ipotesi induttiva.

La parola f ha al più un fattore speciale a destra per ogni lunghezza. Infatti supponiamo, per assurdo, che esistano due parole distinte $u,\ v \in F(f)$ entrambe fattori speciali a destra di f della stessa lunghezza e sia x il più lungo suffisso comune ad u e v. Dunque $axa, axb, bxa, bxb \in F(f)$ contraddicendo quanto osservato prima.

Per dimostrare che f ha almeno un fattore speciale a destra per ogni lunghezza usiamo la seguente relazione.

$$f_{n+2} = g_n \widetilde{f_n}\,\widetilde{f_n}\, t_n \qquad (n \geq 2) \tag{2.1}$$

dove $g_2 = 1$ e per $n \geq 3$ si ha

$$g_n = f_{n-3} \cdots f_1 f_0 \quad \text{e} \quad t_n = \begin{cases} ab & \text{se } n \text{ è dispari,} \\ ba & \text{se } n \text{ è pari.} \end{cases}$$

L'Equazione 2.1 può essere dimostrata per induzione. Infatti $f_{2+2} = f_4 = 1\ (aba)(aba)ba$ e $f_{3+2} = f_5 = a(baaba)(baaba)ab$. Si può poi dimostrare per induzione che $\varphi(\widetilde{u})a = a\widetilde{\varphi(u)}$ per ogni u e dunque che $\varphi(\widetilde{f_n}t_n) = a\widetilde{f_{n+1}}t_{n+1}$. Da ciò e dal fatto che $\varphi(g_n)a = g_{n+1}$ si ottiene la formula dell'Equazione 2.1.

Poiché la prima lettera di $\widetilde{f_n}$ è l'opposta della prima lettera di t_n, il fattore $\widetilde{f_n}$ è speciale a destra per ogni $n \geq 2$. Essendo un suffisso di una parola speciale a destra anch'esso sarà speciale a destra, ciò prova l'esistenza di fattori speciali a destra per ogni lunghezza.

Chiameremo *insieme di Fibonacci* l'insieme dei fattori di f.

Le *parole episturmiane* sono un'estensione delle parole Sturmiane per alfabeti finiti con un numero arbitrario di lettere.

Per definizione, una parola infinita x è *episturmiana* se $F(x)$ è chiuso per rovesci e se, per ogni $n \geq 1$, $F(x)$ contiene al più una parola di lunghezza n speciale a destra.

Dalla proprietà di chiusura per rovescio si ottiene che il rovescio della parola speciale a destra è anche l'unica parola speciale a sinistra di lunghezza n di x. Ricordiamo inoltre che un suffisso (risp. prefisso) di un fattore speciale a destra (risp. a sinistra) è ancora speciale a destra (risp. a sinistra).

Diremo che una parola episturmiana x è *stretta* se x ha esattamente un fattore speciale a destra di lunghezza n, per ogni $n \geq 1$ e se tale fattore u è stretto, ovvero se $uA \subset F(x)$.

Si vede facilmente che, nel caso di una parola episturmiana stretta su un alfabeto A di k lettere, l'insieme $F(x) \cap A^n$ ha esattamente $(k-1)n+1$ elementi per ogni n. Dunque, nel caso di alfabeti binari, le parole episturmiane strette sono proprio le parole Sturmiane.

Una parola episturmiana x è detta *standard* se tutti i suoi fattori speciali a sinistra sono prefissi di x. Per ogni parola episturmiana x esiste una parola episturmiana standard y tale che $F(x) = F(y)$ (si veda [5]).

Esempio 2.2.3. Consideriamo l'estensione della parola di Fibonacci, vista nell'Esempio 2.2.2, ad un alfabeto ternario $A = \{a, b, c\}$. Consideriamo il morfismo $\varphi : A^* \to A^*$ definito da $\varphi(a) = ab$, $\varphi(b) = ac$ e $\varphi(c) = a$. La *parola di Tribonacci* è il punto fisso

$$\varphi^\omega(a) = abacabaabacababacabaabacabacabaabacab\cdots$$

Essa è una parola episturmiana standard, come dimostrato in [8].

Una parola episturmiana è uniformemente ricorrente (si veda [5]).

Esempio 2.2.4. La parola di Thue-Morse, vista nell'Esempio 2.2.1, non è episturmiana. Infatti essa ha quattro fattori di lunghezza 2.

Per le parole episturmiane standard vi è una descrizione combinatoria ben precisa (si vedano, ad esempio, [8] e [6]).

Teorema 2.2.5. *Una parola infinita w è episturmiana standard se e solo se esiste una parola infinita $\Delta = a_0a_1, \ldots$, con $a_i \in A$, tale che*

$$w = \lim_{n\to\infty} u_n,$$

dove la sequenza (u_n) è definita da $u_n = Pal(a_0a_1\cdots a_{n-1})$.

Inoltre, w è episturmiana stretta se e solo se ogni lettera appare in Δ infinite volte.

La parola infinita Δ del Teorema precedente è detta *parola direttiva* della parola standard w. Il Teorema 2.2.5 può essere riassunto dall'equazione

$$w = \mathrm{Pal}(\Delta).$$

Come caso particolare della formula di Justin, si ha

$$u_{n+1} = \psi_{a_0\cdots a_{n-1}}(a_n)u_n.$$

Le parole u_n sono i soli prefissi di w palindromi.

Esempio 2.2.6. La parola di Fibonacci x dell'Esempio 2.2.2 è una parola episturmiana standard con parola direttiva $(ab)^\omega$, ovvero $x = \mathrm{Pal}((ab)^\omega)$ (si veda [6]). Quella di Tribonacci dell'Esempio 2.2.3 ha, invece, come parola direttiva $(abc)^\omega$ (si veda [8]).

2.2.2 Insiemi Sturmiani

Un insieme F è detto *Sturmiano* se è l'insieme dei fattori $F(x)$ di una parola episturmiana stretta x. Per quanto visto nella Sottosezione 2.2.1, una parola episturmiana è uniformemente ricorrente, dunque un insieme Sturmiano è un insieme uniformemente ricorrente. Inoltre ogni parola speciale a destra (risp. speciale a sinistra) in F è stretta.

Una caratterizzazione degli insiemi Sturmiani è data dalla seguente Proposizione.

Proposizione 2.2.7. *Un insieme F è Sturmiano se e solo se è uniformemente ricorrente e verifica le due condizioni*

(*i*) *è chiuso per rovescio,*

(*ii*) *per ogni $n \geq 0$ esiste esattamente una parola speciale a destra in F di lunghezza n e questa è stretta.*

Dimostrazione.

($\Rightarrow$) Sia $F = F(x)$ per qualche parola episturmiana stretta x. Allora le condizioni sono verificate per quanto visto nella Sottosezione precedente.

($\Leftarrow$) Sia F un insieme uniformemente ricorrente verificante le condizioni (*i*) e (*ii*). Per ogni $n \geq 0$ il rovescio $\widetilde{u_n}$ dell'unica parola speciale a destra u_n di lunghezza n è una parola speciale a sinistra. Essendo tali $\widetilde{u_n}$ una successione di parole ognuna prefissa del successivo, esisterà una parola infinita x avente le $\widetilde{u_n}$ come prefissi. Chiaramente $F(x) \subseteq F$.

Per mostrare che x è episturmiana stretta verifichiamo che $F(x)$ è chiuso per rovescio. Sia $v \in F(x) \subset F$. Essendo F uniformemente ricorrente, esiste un intero m tale che v è fattore di tutte le parole di lunghezza m in F. In particolare v sarà fattore di u_m. Dunque anche $\widetilde{v}$ sarà un fattore di $\widetilde{u_m}$ e dunque $\widetilde{v} \in F(x)$.

Infine sia $v \in F$. Essendo F uniformemente ricorrente, esisterà un intero m tale che v è fattore di tutte le parole di lunghezza m in F. In particolare v sarà fattore di $\widetilde{u_m} \in F(x)$. Dunque anche $v \in F(x)$, ovvero si ha $F \subseteq F(x)$, da cui la tesi.

□

2.3 Codici prefissi in insiemi fattoriali

In questa Sezione studieremo i codici prefissi all'interno di un insieme fattoriale.

Come già visto nella Sottosezione 1.2.7, un codice prefisso è un insieme non vuoto $X \subseteq A^+$ tale che i suoi elementi siano a due a due incomparabili per l'ordine prefisso. Esso è inoltre un codice, ovvero ogni parola in X^* ammette un'unica fattorizzazione in elementi di X.

Sia $F \subseteq A^*$ un sottoinsieme di A^*. Un insieme $X \subseteq A^*$ si dirà *denso a destra* in F o *F-denso a destra*, se ogni $u \in F$ è un prefisso di X. Un insieme $X \subseteq F$ si dirà *completo a destra* in F, o *F-completo a destra*, se X^* è denso a destra in F, ovvero se ogni $u \in F$ è un prefisso di X^*.

Un codice prefisso $X \subseteq F$ sarà detto *massimale prefisso* in F, o *F-prefisso massimale*, se non è propriamente contenuto in alcun altro codice prefisso $Y \subseteq F$. Analogamente si definisce la nozione di *F-massimale suffisso*.

Alcuni dei risultati classici per i prefissi massimali in A^* possono essere estesi al caso di codici F-massimali.

Proposizione 2.3.1. *Siano $F \subseteq A^*$ un sottoinsieme fattoriale di parole ed $X \subseteq F$ un codice prefisso in F. Le seguenti condizioni sono equivalenti:*

(i) ogni elemento di F è comparabile per prefisso con qualche elemento di X;

(ii) X è un codice F-massimale prefisso;

(iii) XA^* è F-denso a destra;

(iv) X è F-completo a destra.

Dimostrazione. Mostriamo che (i) vale se e solo se vale (ii).

$((i) \Rightarrow (ii))$ Supponiamo, per assurdo, esista $Y \supsetneq X$ codice prefisso contenuto in F. Preso un elemento $u \in Y \setminus X$ l'insieme $X \cup u$ sarà prefisso e dunque x non sarà comparabile per prefisso con alcun elemento di x.

$((ii) \Rightarrow (i))$ Viceversa se, per assurdo, vi fosse un elemento $u \in F$ non comparabile per prefisso con ogni parola di X, allora $X \cup u$ sarebbe un codice prefisso, contraddicendo la F-massimalità di X.

Notiamo che in questa doppia implicazione non abbiamo usato come ipotesi dell'essere chiuso per fattori di F.

Mostriamo adesso l'equivalenza tra le prime due condizioni e le ultime due. Per far ciò sarà superflua l'ipotesi che X sia un codice bifisso e basterà il suo essere non vuoto e contenuto in F.

$((i) \Rightarrow (iii))$ Sia $u \in F$. Per ipotesi esiste un elemento $x \in X$ comparabile per prefisso con u, ovvero tale che $uv = xw$ per opportuni $v, w \in A^*$. Dunque XA^* è F-denso a destra.

$((iii) \Rightarrow (iv))$ Sia $u \in F$ e dimostriamo per induzione. Se $|u| = 1$ banalmente si ha $u = 1$ prefisso di ogni parola di X^*. Supponiamo adesso $|u| > 1$. Essendo XA^* F-denso a destra, si ha $uv = xw$ per opportuni $x \in X$ e $v, w \in A^*$. Se u è un prefisso di $X \subseteq X^*$ allora non c'è niente da provare. Altrimenti, se x è un prefisso proprio di u, si ha $u = xu'$ per un opportuno $u' \in A^*$. Essendo F fattoriale si ha $u' \in F$ e poiché $x \neq 1$ risulta $|u'| < |u|$. Dunque, per ipotesi induttiva, u' è un prefisso di X^*, da cui si ricava che anche u è un prefisso di X^*. Dunque X^* è F-denso a destra, ovvero X è F-completo a destra.

$((iv) \Rightarrow (i))$ Sia $u \in F$. Per ipotesi u è un prefisso di X^* dunque u è comparabile per prefisso con qualche parola di X.

□

La Proposizione 2.3.1 ammette una formulazione duale sostituendo "prefisso" con "suffisso", "destro" con "sinistro" e "XA^*" con "A^*X".

Esempio 2.3.2. L'insieme $X = \{a, ba\}$ è un codice prefisso massimale nell'insieme di Fibonacci poiché XA^* è F-denso a destra.

2.4 Codici bifissi in insiemi ricorrenti

Di seguito specializzeremo quanto visto nella Sezione precedente, studiando il caso di codici bifissi all'interno di insiemi ricorrenti.

Con il Teorema 2.4.32 vedremo che quando F è un insieme ricorrente, contrariamente al caso generale, vi è solo un numero finito di codici massimali bifissi in F.

2.4.1 Parse

Abbiamo introdotto nella Sottosezione 1.2.8 la nozione di parse di una parola rispetto ad un insieme $X \subseteq A^*$. Mostriamo adesso che, nel caso di codici bifissi, ad ogni fattorizzazione corrisponde un parse.

Proposizione 2.4.1. *Siano F un insieme fattoriale ed $X \subseteq F$ un codice bifisso. Per ogni fattorizzazione $w = uv$ di una parola $w \in F$ esiste un parse (s, yz, p) di w con $y, z \in X^*$, $u = sy$ e $v = zp$.*

Dimostrazione. Abbiamo visto nella Proposizione 1.2.19 che possiamo scrivere $v = zp$ per opportuni $z \in X^*$ e $p \in P = A^* \setminus XA^*$. Analogalmente, dal duale della stessa Proposizione, si ha $u = sy$ per opportuni $y \in X^*$ ed $s \in S = A^* \setminus A^*X$. Dunque (s, yz, p) è un parse di w che soddisfa le condizioni dell'enunciato. □

Esempio 2.4.2. L'insieme $X = \{a, bab\}$ è un codice bifisso. La parola bab ammette due parse: $(1, bab, 1)$ e (b, a, b).

Data una parola $w \in A^*$ denotiano con $\delta_X(w)$ il numero di parse di questa rispetto ad un insieme X. La funzione $\delta_X : A^* \to \mathbb{N}$ è detta *enumeratore di parse* rispetto ad X. La serie L_X definita da $(L_X, w) = \delta_X(w)$, per $w \in A^*$, è detta *indicatore* dell'insieme X.

Esempio 2.4.3. Sia $X = A^*$. Allora $\delta_X(w) = 1$.

Esempio 2.4.4. Sia $X = \emptyset$. Allora $\delta_X(w) = |w| + 1$.

Osservazione 2.4.5. Possiamo esprimere la serie L_X in termini di serie caratteristiche. Infatti, ponendo $P = A^* \setminus XA^*$ ed $S = A^* \setminus A^*X$, si ottiene la formula

$$L_X = \underline{S}\,\underline{X}^*\,\underline{P}.$$

Un'importante caratterizzazione per l'enumeratore di parse nel caso di codici prefissi all'interno di insiemi fattoriali è data dalla seguente Proposizione.

Proposizione 2.4.6. *Siano F un insieme fattoriale ed $X \subseteq F$ un codice prefisso. Per ogni parola $w \in F$, il valore $\delta_X(w)$ è pari al numero di prefissi di w privi di suffissi in X.*

Dimostrazione. Sia $u \in A^* \setminus A^*X$ tale che $w = uw'$. Essendo X un codice prefisso, possiamo fattorizzare $w' = xv$ per opportuni $x \in X^*$ e $v \in A^* \setminus XA^*$. Otteniamo dunque il parse di w (u, x, v). Poiché ogni parse si ottiene in questa maniera, l'enunciato è verificato. □

La Proposizione 2.4.6 ammette un enunciato duale per i codici suffissi.

Un Corollario immediato della Proposizione è il seguente (si veda anche Figura 2.1).

Corollario 2.4.7. *Sia X un codice prefisso. Per ogni $w \in A^*$ e $a \in A$, si ha*

$$\delta_X(wa) = \begin{cases} \delta_X(w) & \text{se } wa \in A^*X \\ \delta_X(w) + 1 & \text{altrimenti} \end{cases} \tag{2.2}$$

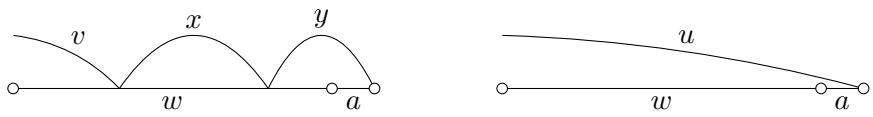


Figura 2.1: La funzione δ_X determina X.

Siano X, Y due codici prefissi. Se $X \subseteq Y$ allora una parola priva di suffissi in Y sarà priva di suffissi anche in X. Dunque per ogni w si avrà

$$X \subseteq Y \quad \Rightarrow \quad \delta_Y(w) \leq \delta_X(w). \tag{2.3}$$

Osservazione 2.4.8. Il risultato della Proposizione 2.4.6 lo si può ottenere anche dalla Proposizione 1.2.19. Infatti per l'Osservazione 2.4.5 si ha $L_X = \underline{S}\ \underline{X}^*\ \underline{P}$, con $P = A^* \setminus XA^*$ ed X codice prefisso. Dunque $\underline{X}^*\underline{P} = \underline{A}^*$, da cui

$$L_X = \underline{S}\,\underline{A}^* \tag{2.4}$$

Proposizione 2.4.9. *Sia X un codice bifisso ed L_X l'indicatore di X. Allora si ha*

$$1 - \underline{X} = (1 - \underline{A})\, L_X\, (1 - \underline{A}). \tag{2.5}$$

Dimostrazione. Essendo X un codice prefisso si ha, per l'Equazione 2.4, $L_X = \underline{S}\,\underline{A}^*$. Moltiplicando su entrambi a destra per $(1 - \underline{A})$ otteniamo, per la Proposizione 1.1.35,

$$L_X(1 - \underline{A}) = \underline{S}.$$

Essendo X un codice suffisso si ha, per il duale della Proposizione 1.2.19, $1 - \underline{X} = (1 - \underline{A})\underline{S}$. Da cui, per quanto appena visto,

$$1 - \underline{X} = (1 - \underline{A})\, L_X\, (1 - \underline{A}).$$

□

La Proposizione 2.4.9 ci dice che un codice bifisso X è determinato dal suo indicatore L_X e dunque dalla funzione δ_X. Viceversa, essendo la formula 2.5 equivalente a $L_X = \underline{A}^*\,(1 - \underline{X})\,\underline{A}^*$, l'indicatore L_X, e dunque la funzione δ_X, sono determinati dall'insieme X.

Nel caso di codici bifissi, i due Esempi 2.4.3 e 2.4.4 sono estremali. Infatti vale il seguente risultato (si veda [4, Proposizione 6.1.8]).

Proposizione 2.4.10. *Sia $X \subset A^+$ un codice bifisso. Allora per ogni $w \in A^*$ si ha*

$$1 \leq \delta_X(w) \leq |w| + 1.$$

In particolare, $\delta_X(1) = 1$ e per ogni $u, v, w \in A^*$

$$\delta_X(v) \leq \delta_X(uvw). \tag{2.6}$$

Osservazione 2.4.11. Se, nella Proposizione precedente, $u, v \in A^+$ sono parole non vuote, allora la disuguaglianza è stretta, ovvero $\delta_X(v) < \delta_X(uvw)$.

Diamo adesso una caratterizzazione dell'enumeratore di parse per i codici bifissi (si veda [4, Proposizione 6.1.11]).

Proposizione 2.4.12. *Una funzione $\delta : A^* \to \mathbb{N}$ è l'enumeratore di parse di un qualche codice bifisso se e solo se sono verificate le seguenti condizioni.*

(i) Per ogni $a \in A$ e $w \in A^*$

$$0 \leq \delta(aw) - \delta(w) \leq 1. \tag{2.7}$$

$$0 \leq \delta(wa) - \delta(w) \leq 1. \tag{2.8}$$

(ii) Per ogni $a, b \in A$ e $w \in A^*$

$$\delta(aw) + \delta(wb) \geq \delta(w) + \delta(awb). \tag{2.9}$$

(iii) $\delta(1) = 1$.

2.4.2 Codici F-thin

Sia $F \subseteq A^*$. Un insieme $X \subseteq F$ è detto *thin* in F, o F-*thin*, se esiste una parola di F che non è fattore di alcuna parola di X.

Esempio 2.4.13. Sia $F = A^*$. L'insieme $X = \{a^n b^n \mid n \geq 1\}$ è thin in A^* poichè, ad esempio, ba non è fattore di alcuna parola di X.

Osservazione 2.4.14. Se F è un insieme infinito ogni insieme finito $X \subset F$ è F-thin.

Come già visto nella Sottosezione 1.2.2, un fattore interno di una parola x è una parola v tale che $x = uvw$ per opportune parole non vuote $u,\ w \in A^+$. Nel caso di un insieme $X \subseteq F$ con F un insieme fattoriale di parole, denoteremo l'insieme dei fattori interni di parole in X come

$$H(X) = A^- X A^- = \left\{ w \in A^* \mid A^+ w A^+ \cap X \neq \emptyset \right\}.$$

I fattori interni di una parola sono, chiaramente, fattori della stessa.

Proposizione 2.4.15. *Sia F un insieme fattoriale essenzialmente destro ed essenzialmente sinistro. Un insieme $X \subseteq F$ è F-thin se e solo se $F \setminus H(X) \neq \emptyset$.*

Dimostrazione.

($\Rightarrow$) Se X è F-thin esisterà una parola $w \in F$ che non sarà fattore di alcuna parola di X. Dunque, in particolare, essa non sarà in $H(X)$.

($\Leftarrow$) Sia $w \in F \setminus H(X)$ e siano $a, b \in A$ tali che $awb \in F$. Per costruzione awb non sarà fattore di alcuna parola di X. Dunque X è F-thin.

□

Un codice bifisso $X \subseteq F$ sarà detto *massimale bifisso* in F, o F-*massimale bifisso*, se non è contenuto propriamente in alcun altro codice bifisso $Y \subseteq F$.

Esempio 2.4.16. Siano $A = \{a, b\}$ ed $F = A^* \setminus A^*(bb)A^*$ l'insieme delle parole senza il fattore bb. L'insieme $X = \{aaa, aaba, ab, baa, baba\}$ è un codice F-massimale, come si può evincere dalla Figura 2.2.

Una caratterizzazione dei codici F-massimali bifissi che siano anche F-thin è data dal seguente risultato (si veda [1, Teorema 4.2.2]).

Teorema 2.4.17. *Siano F un insieme ricorrente ed $X \subseteq F$ un insieme F-thin. Le seguenti condizioni sono equivalenti:*

(i) X è un codice F-massimale bifisso;

(ii) X è un codice prefisso F-completo a sinistra;

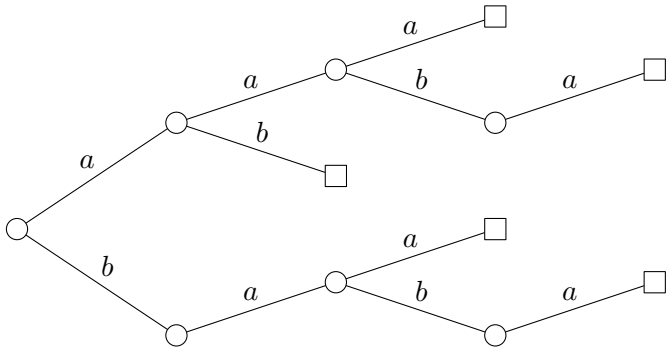


Figura 2.2: Rappresentazione del codice F-massimale $X = \{aaa, aaba, ab, baa, baba\}$.

(iii) X *è un codice suffisso* F*-completo a destra;*

(iv) X *è un codice* F*-massimale prefisso ed* F*-massimale suffisso.*

Il caso $F = A^*$ è stato studiato da Schützenberger nel 1961 (si veda [15]). Egli dimostrò che per gli insiemi thin (in A^*) l'essere massimale bifisso equivaleva ad essere massimale prefisso e massimale suffisso.

Esempio 2.4.18. Sia $F = a^*b^*$. L'insieme $X = \{aa, ab, b\}$ è un codice F-massimale prefisso ed F-completo a sinistra. Esso non è però suffisso.

Sia $F \subseteq A^*$ un insieme fattoriale. L'F*-grado* di un insieme $X \subseteq A^*$, denotato con $d_F(X)$, è il numero massimo di parse rispetto ad X di parole di F, ovvero

$$d_F(X) = \max_{w \in F}\{\delta_X(w)\}.$$

Esso può essere finito o infinito. L'A^*-grado di un insieme X si chiamerà semplicemente *grado* di X, denotandolo con $d(X)$.

Osservazione 2.4.19. Si osservi che $d_F(X) = d_F(X \cap F)$. Inoltre si avrà $d_F(X) \leq d(X)$.

La nozione di grado di un insieme ci permette, nel caso di codici bifissi all'interno di insiemi ricorrenti, di caratterizzare i codici F-thin ed F-massimali bifissi. Il seguente risultato è in [1, Teorema 4.2.8].

Teorema 2.4.20. *Siano* F *un insieme ricorrente ed* $X \subseteq F$ *un codice bifisso. L'insieme* X *è* F*-thin ed* F*-massimale bifisso se e solo se il suo* F*-grado* $d_F(X)$ *è finito. In tale caso le parole di grado massimo sono quelle che non risultano fattori interni di* X*, ovvero*

$$H(X) = \{w \in F \mid \delta_X(w) < d_F(X)\}.$$

Esempio 2.4.21. Sia F l'insieme di Fibonacci. L'insieme $X = \{a, bab, baab\}$ è un codice F-thin (poiché finito) ed F-massimale bifisso. Il grado di X è $d_F(X) = 2$, infatti bab non è un fattore interno di X ed esso ha due parse: $(1, bab, 1)$ e (b, a, b).

Esempio 2.4.22. Sia F l'insieme di Fibonacci. L'insieme $X = \{aaba, ab, baa, baba\}$ è un codice F-massimale bifisso di F-grado 3. Infatti la parola $aaba$ ha tre parse, ovvero $(1, aaba, a)$, (a, ab, a) e $(aa, 1, ba)$, e $aaba \in F \setminus H(X)$.

Dal Teorema 2.4.20 segue un'importante relazione tra i codici bifissi massimali e quelli F-massimali.

Corollario 2.4.23. *Siano F un insieme ricorrente ed $X \subseteq A^+$ un codice massimale bifisso di grado d. Allora l'insieme $Y = X \cap F$ è F-thin ed F-massimale bifisso. Inoltre $d_F(Y) \leq d$ con uguaglianza nel caso X sia finito.*

Dimostrazione. Dall'Osservazione 2.4.19 otteniamo

$$d_F(Y) = d_F(X \cap F) = d_F(X) \leq d(X) = d.$$

Dunque, avendo Y F-grado finito, per il Teorema 2.4.20, X è F-thin ed F-massimale bifisso.

Inoltre, essendo X finito, sarà possibile trovare una parola $w \in F \setminus H(X)$ (basta sceglierne una di lunghezza maggiore di quella della parola più lunga di X). Tale parola avrà d parse, da cui si ottiene $d_F(Y) = d_F(X) = d$. □

Esempio 2.4.24. L'insieme $X = a \cup ba^*b$ è un codice massimale bifisso di grado 2, poiché $bb \notin H(X)$ ha due parse: $(1, bb, 1)$ e $(b, 1, b)$.

Sia F l'insieme di Fibonacci. Allora $X \cap F = \{a, baab, bab\}$ è un codice F-massimale bifisso di F-grado 2.

Un Esempio che mostra come nel caso di insiemi infiniti la disuguaglianza sia stretta è il seguente.

Esempio 2.4.25. Siano $A = \{a, b\}$ ed $F = a^*$ un insieme ricorrente. L'insieme $X = a \cup ba^*b$ è un codice bifisso di grado 2 per quanto visto nell'Esempio precedente. L'intersezione $Y = X \cap F = \{a\}$ ha però F-grado 1.

2.4.3 Nucleo, codice derivato

Dato un insieme X definiamo il suo *nucleo* $K(X)$ l'insieme delle parole di X che sono fattori interi di parole di X, ovvero $K(X) = H(X) \cap X$.

Il seguente risultato è in [1, Teorema 4.3.1].

Teorema 2.4.26. *Siano F un insieme ricorente ed $X \subseteq F$ un codice bifisso di F-grado finito $d \geq 2$. Poniamo $H = H(X)$, $K = K(X)$, $G = (HA \cap F) \setminus H$ e $D = (AH \cap F) \setminus H$.*

L'insieme $X' = K \cup (G \cap D)$ è un codice bifisso di F-grado $d-1$.

Il codice X' definito nel Teorema 2.4.26 è detto codice *derivato* di X rispetto ad F, o F*-derivato*.

Esempio 2.4.27. Siano F l'insieme di Fibonacci ed $X = \{a, bab, baab\}$ il codice bifisso di F-grado 2 dell'Esempio 2.4.21. Abbiamo

$$K = \{a\}, \qquad H = \{1, a, aa\},$$

$$G = \{a, b, aa, ab, aab\} \setminus \{1, a, aa\} = \{b, ab, aab\},$$

$$D = \{a, b, aa, ba, baa\} \setminus \{1, a, aa\} = \{b, ba, baa\}.$$

Dunque il codice derivato è

$$X' = \{a\} \cup (\{b, ab, aab\} \cap \{b, ba, baa\}) = \{a, b\}.$$

Mostriamo adesso come un codice F-thin ed F-massimale bifisso sia determinato dal suo F-grado e dal suo nucleo.

Lemma 2.4.28. *Siano F un insieme ricorrente ed $X \subseteq F$ un codice bifisso di F-grado finito d. Sia Y un insieme tale che $K(X) \subseteq Y \subset X$. Allora per ogni $w \in H(X) \cup Y$,*

$$\delta_Y(w) = \delta_X(w). \tag{2.10}$$

Inoltre, per ogni $w \in F$,

$$\delta_X(w) = \min\{d, \delta_Y(w)\}. \tag{2.11}$$

Dimostrazione. Per quanto visto nella Sottosezione 2.4.1 $L_X = \underline{A}^*(1-\underline{X})\underline{A}^*$. Dunque per provare la 2.10 è sufficiente far vedere che per ogni $w \in H(X) \cup Y$ si ha $F(w) \cap X = F(w) \cap Y$, dove $F(w)$ è l'insieme dei fattori di w.

L'inclusione $F(w) \cap Y \subseteq F(w) \cap X$ è banale.

Mostriamo l'inclusione inversa. Certamente si avrà $F(w) \cap X \subseteq F(w)$. Se $w \in H(X)$ allora $F(w) \cap X \subset K(X) \subset Y$ e dunque l'inclusione è verificata. Se $w \in Y \subseteq X$ allora nessun prefisso proprio o suffisso proprio di w sarà in X poiché X è un codice bifisso. Dunque tutte le parole in $(F(w) \cap X) \setminus \{w\}$ saranno in $K(X)$, ovvero, si avrà

$$F(w) \cap X = \{w\} \cup \left(A^- w A^- \cap X\right) \subseteq \{w\} \cup K(X) \subseteq Y,$$

e quindi anche in questo caso l'inclusione è verificata.

Dall'Equazione 2.10 ricaviamo che per ogni $w \in F$ si ha $\delta_X(w) \leq \delta_Y(w)$. Se $w \in F \setminus H(X)$, si ha $\delta_X(w) = d$ per il Teorema 2.4.20 e dunque l'Equazione è verificata. Se invece $w \in H(X)$ allora, $\delta_X(w) < d$ per il Teorema 2.4.20 e, per l'Equazione 2.10, $\delta_X(w) = \delta_Y(w)$. Ciò prova 2.11. □

Teorema 2.4.29. *Siano F un insieme ricorrente ed $X \subseteq F$ un codice bifisso di F-grado finito d. Per ogni $w \in F$ si ha*

$$\delta_X(w) = \min\{d, \delta_{K(X)}(w)\}.$$

Dimostrazione. La formula segue immediatamente da 2.11 scegliendo $Y = K(X)$ nel Lemma 2.4.28. □

Per quanto visto nella Sottosezione 2.4.1, il Teorema precedente afferma che un codice bifisso X all'interno di un insieme F ricorrente e di F-grado finito è determinato dal suo F-grado e dal suo nucleo.

Diamo adesso una caratterizzazione dei nuclei dei codici bifissi di F-grado finito.

Teorema 2.4.30. *Sia F un insieme ricorrente. Un codice bifisso $Y \subseteq F$ è il nucleo di un qualche codice bifisso di F-grado finito d se e solo se sono verificate le due condizioni*

(i) *Y non è un codice F-massimale bifisso;*

(ii) $\max\{\delta_Y(w) \mid w \in Y\} \leq d - 1$.

Dimostrazione.

($\Rightarrow$) Sia X un codice F-thin ed F-massimale biffiso di F-grado d tale che $Y = K(X)$ sia il suo nucleo. La condizione (i) è verificata poiché $Y \subsetneq X$, avendo i due insiemi F-grado diversi. Anche la condizione (ii) è verificata poiché, per l'equazione 2.10, $\delta_X(w) = \delta_Y(w)$ per ogni $w \in Y$ e, essendo $Y = K(X) \subseteq H(X)$, per il Teorema 2.4.20, $\delta_X(w) \leq d - 1$.

($\Leftarrow$) Sia $Y \subseteq F$ un codice bifisso soddisfacente le condizioni (i) e (ii). Consideriamo la funzione $\delta : A^* \to \mathbb{N}$ definita da

$$\delta(w) = \min\{d, \delta_Y(w)\}.$$

Si può verificare che tale funzione verifica le condizioni $(i) - (iii)$ della Proposizione 2.4.12 e dunque che esiste un codice bifisso Z tale che δ sia il suo enumeratore di parse.

Sia $X = Z \cap F$. La funzione δ_X è limitata su F poiché lo è δ, dunque, per il Teorema 2.4.20, X è un codice F-thin ed F-massimale bifisso. Essendo Y un codice non F-massimale bifisso, invece, la funzione δ_Y diverge e dunque $\max\{\delta(w) \mid w \in F\} = d$, mostrando che X ha F - grado d.

Mostriamo, infine, che il nucleo di X è proprio Y.

Dalla condizione (ii) e dal Teorema 2.4.20 ricaviamo $Y \subseteq H(X)$. Consideriamo una parola $w \in H(X)$. Sempre dal Teorema 2.4.20 ricaviamo che $\delta_X(w) = \delta_Y(w)$. Per quanto visto nella sottosezione 2.4.1, questo implica che per ogni $w \in H(X)$ si ha $(\underline{X}, w) = (\underline{Y}, w)$, ovvero che i fattori interni di X stanno in X se e solo se stanno in Y. Quindi $K(X) = H(X) \cap X = H(X) \cap Y = Y$.

□

Esempio 2.4.31. Sia F l'insieme di Fibonacci. I codici F-massimali bifissi di F-grado 2 sono soltanto tre (Figura 2.3). Infatti, per il Teorema 2.4.30, i possibili nuclei sono $\emptyset, \{a\}$ e $\{b\}$.

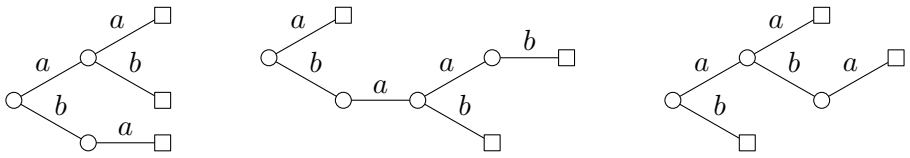


Figura 2.3: I tre codici F-massimali bifissi di F-grado 2, con F l'insieme di Fibonacci.

2.4.4 Codici F-massimali bifissi finiti

Nel caso di insiemi ricorrenti, il numero di codici F-massimali bifissi finiti di F-grado dato è limitato, come mostrato nel seguente Teorema.

Teorema 2.4.32. *Siano F un insieme ricorrente e $d \geq 1$. Vi è solo un numero finito di codici F-massimali bifissi finiti $X \subseteq F$ di F-grado d.*

Dimostrazione. Procediamo per induzione sull'F-grado.

- Il caso $d = 1$ è banale poiché vi è un solo codice F-massimale bifisso di F-grado 1, ovvero $F \cap A$.
- Supponiamo adesso che i codici F-massimali bifissi finiti di F-grado d siano in numero finito. Ogni codice F-massimale bifisso finito $X \subseteq F$ di F-grado $d+1$ è determinato dal suo nucleo che è un sottoinsieme del suo codice derivato X'. Poiché X' è un codice F-massimale bifisso finito di F-grado d, per ipotesi induttiva vi saranno solo un numero finito di nuclei, da cui la tesi.

□

Il numero dei codici F-massimali bifissi di F-grado d nel caso F sia l'insieme di Fibonacci è mostrato nella tabella 2.4.4 per $d \leq 8$.

d	1	2	3	4	5	6	7	8
	1	3	13	71	461	3447	29092	273343

Mentre nel caso classico $F = A^*$, se $\mathrm{Card}\,(A) \geq 2$, esistono codici massimali bifissi infiniti per ogni grado fissato (si veda [4, Teorema 6.4.6 ed Esempio 6.4.7]), nel caso di insiemi uniformemente ricorrenti vale il seguente risultato.

Teorema 2.4.33. *Sia F un insieme uniformemente ricorrente. Ogni codice bifisso F-thin $X \subseteq F$ è finito. Inoltre ogni codice bifisso finito è contenuto in un codice F-massimale bifisso finito.*

Dimostrazione. Sia X un codice bifisso F-thin. Essendo X F-thin, esisterà una parola $w \in F \setminus H(X)$ e, poiché F è uniformemente ricorrente, esisterà un intero r tale che w è un fattore per ogni parola di $F_r = F \cap A^r$. Le parole di X hanno lunghezza al più $r + 1$. Infatti supponiamo per assurdo che esista un $k \geq r + 2$ tale che $F_k \cap X \neq \emptyset$ e sia $x \in F_k \cap X$. Possiamo fattorizzare $x = pus$ con $u \in F_r \cap H(X)$ e p, s parole non vuote. Essendo w un fattore di u, avremo $w \in H(X)$, ottenendo una contraddizione. Dunque, poichè X ha parole di lunghezza limita, esso è finito.

Sia $X \subseteq F$ un codice bifisso non F-massimale e sia $d = \max_{x \in X}\{\delta_X(x)\}$. Per il Teorema 2.4.30 X è il nucleo di un codice Z di F-grado $d + 1$, F-massimale bifisso ed F-thin e dunque, per quanto appena visto, finito. □

2.4.5 Immagine e rango di una parola

Diamo infine alcuni risultati che sfrutteremo nel Capitolo 4.

Siano F un insieme ricorrente ed $X \subseteq F$ un codice bifisso di F-grado d. Sia $\mathcal{A} = (Q, 1, 1)$ un automa semplice tale da riconoscere X^*. Per ogni parola $w \in A^*$ denotiamo con $\Im(w)$ l'*immagine* di w rispetto ad $\mathcal{A}$, ovvvero l'insieme $\Im(w) = \{p \cdot w \,|\, p \in Q\}$. Chiameremo *rango* di w (rispetto all'automa $\mathcal{A}$) il numero $\mathrm{rank}(w) = \mathrm{Card}\,(\Im(w))$.

Osservazione 2.4.34. Data una parola w, l'immagine $\Im(w)$ ed il rango $\mathrm{rank}(w)$ sono uguali all'immagine ed al rango (ovvero alla cardinalità dell'immagine) della funzione $\varphi_{\mathcal{A}}(w)$.

Osservazione 2.4.35. Date tre parole $u, v, w \in A^*$ si ha

$$\mathrm{rank}(uwv) \leq \mathrm{rank}(w).$$

Il seguente Lemma ci da una caratterizzazione di $\Im(w)$ per una parola $w \in F$ con d parse rispetto ad X.

Lemma 2.4.36. *Siano F, X, $\mathcal{A}$ come sopra e $w \in F$ una parola con $\delta_X(w) = d$. Allora rank$(w) = d$. Inoltre $\Im(w)$ è l'insieme degli stati $1 \cdot p$ tali che (s, x, p) è un parse di w, ovvero*

$$\Im(w) = \{1 \cdot p \,|\, (s, x, p) \text{ è un parse di } w, \text{ per un opportuno } s\}.$$

Per ogni $r \in \Im(w)$ vi è un unico prefisso proprio p di X che è suffisso di w e tale che $r = 1 \cdot p$.

Dimostrazione. Per ogni $r \in \Im(w)$ esiste un unico $p \in XA^-$ suffisso di w tale che $r = 1 \cdot p$. Infatti.

- Siano $r \in \Im(w)$ e $q \in Q$ tale che $q \cdot w = r$. Essendo $\mathcal{A}$ trim, in quanto semplice, esisteranno due parole $u, v \in A^*$ tali che $1 \cdot u = q$ e $r \cdot v = 1$. Dunque $uwv \in X^*$. Essendo $\delta_X(w) = d$, per il Teorema 2.4.20, $w \notin H(X)$. Dunque esisterà un parse (s, x, p) di w tale che $us, pv \in X^*$. In particolare, quindi, $r = 1 \cdot p$ con $p \in XA^-$ suffisso di w.

- Tale scelta di p è unica, ovvero che la relazione $r \mapsto (s, x, p)$ è una funzione. Supponiamo infatti che esistano due parse di w (s, x, p) e (s', x', p') con $1 \cdot p = 1 \cdot p'$. Allora esisterà una parola $v \in A^*$ tale che $pv, p'v \in X^*$. Tali p e p' sono entrambi suffissi di w e quindi comparabili per suffissi. Ma, essendo X un codice bifisso, ciò implica $p = p'$ e dunque $(s, x, p) = (s', x', p')$.

Per dimostrare che $\Im(w) = \{1 \cdot p \,|\, (s, x, p) \text{ è un parse di } w\}$ verifichiamo che la funzione $r \mapsto (s, x, p)$ è biettiva.

- L'iniettività è verificata poiché $\mathcal{A}$ è un automa deterministico.

- Sia (s, x, p) un parse di w. Essendo X un codice F-massimale bifisso, per il Teorema 2.4.17, esisteranno due parole $u, v \in A^*$ tali che $us,\ pv \in X^*$ e quindi tali che $1 \cdot us = 1 \cdot x = 1 \cdot pv = 1$. Dunque

$$(1 \cdot u) \cdot w = 1 \cdot usxp = 1 \cdot xp = 1 \cdot p.$$

  da cui $r = 1 \cdot p \in \Im(w)$.

Per quanto appena visto si ha, in particolare,

$$\text{rank}(w) = \text{Card}\,(\Im(w)) = \delta_X(w) = d.$$

□

Dal Lemma precedente ricaviamo il seguente risultato.

Proposizione 2.4.37. *Siano F, X, $\mathcal{A}$ come sopra e $u \in F$ una parola con rank$(u) = d$. Allora rank$(uv) = d$ per ogni $v \in u^{-1}F$.*

Dimostrazione. Per il Teorema 2.4.20, X è F-thin, dunque esisterà una parola $w \in F \setminus F(X) \subseteq F \setminus H(X)$ e, sempre per il Teorema 2.4.20, si avrà $\delta_X(w)$. Sia v tale che $uv \in F$. Allora, essendo F ricorrente, esisterà una parola $t \in F$ tale che $uvtw \in F$. Anche $uvtw$ avrà d parse e, per il Lemma 2.4.36, cià implica che rank$(uvtw) = d$. Dunque, $d = \text{rank}(uvtw) \leq \text{rank}(u) = d$, da cui la tesi. □

Capitolo 3

Codici bifissi in insiemi Sturmiani

Il risultato principale della Sezione 3.1 è il Teorema 3.1.3 che ci permette di stabilire la cardinalità di un codice F-massimale bifisso nel caso F sia un insieme Sturmiano. La Sezione termina con un esempio sulla non invertibilità del Teorema.

Nella Sezione 3.2 è data una condizione sufficiente affinché una parola x sia definitivamente periodica (Teorema 3.2.5). La dimostrazione sfrutta il Teorema della Fattorizzazione Critica (Teorema 3.2.2).

Nella Sezione 3.3 sono definite le parole di ritorno, una base del gruppo libero (Corollario 3.3.3). Queste sono usate per dimostrarare il Teorema della Base Sturmiana (Teorema 3.4.4) che caratterizza i codici F-massimali bifissi di grado d, per un insieme Sturmiano F come tutte e sole le basi di un sottogruppo di indice d del gruppo libero. Da questo si ricava, tra le altre cose, che per ogni insieme F Sturmiano, $F \cap A^d$ è una base del sottogruppo $\langle A^d \rangle$. Infine viene fornita una formula (Corollario 3.4.8) per contare il numero di codici F-massimali bifissi finiti di F-grado d, quando F è Sturmiano.

3.1 Cardinalità

Nella Sottosezione 2.4.4 abbiamo studiato i codici F-massimali bifissi finiti nel caso in cui F sia un insieme ricorrente. Vedremo adesso che nel caso l'insieme F sia Sturmiano è possibile dare informazioni più precise sulla cardinalità dei codici.

Diamo due risultati preliminari.

Lemma 3.1.1. *Siano F un insieme Sturmiano, $X \subseteq F$ un codice bifisso finito di F-grado d e $P = XA^- \setminus$ l'insieme dei prefissi propri di X. Esiste una parola $u \in F$ speciale a destra tale che $\delta_X(u) = d$. Inoltre i d suffissi di u che sono in P sono tutte e sole le parole speciali a destra in P.*

Dimostrazione. Poiché X è un insieme finito esisterà un intero $n \geq 1$ maggiore delle lunghezze delle parole di X. Per la Proposizione 2.2.7 vi sarà una parola u di lunghezza n speciale a destra. Questa sicuramente non apparterrà ad $H(X)$ e dunque, per il Teorema 2.4.20 si avrà $\delta_X(u) = d$.

Dal duale della Proposizione 2.4.6 sappiamo che u ha esattamente $d_F(X)$ suffissi in P. Essendo u una parola speciale a destra anche tali suffissi saranno speciali a destra.

Inoltre, essi sono i soli ad avere questa proprietà poiché, per la Proposizione 2.2.7, per ogni n esiste un'unica parola speciale a destra di lunghezza n e questa è proprio il suffisso di lunghezza n di u. □

Lemma 3.1.2. *Siano A un alfabeto di k lettere, $X \subset A^+$ un codice prefisso finito oppure $X = \{1\}$ e $P = XA^-$ l'insieme dei prefissi propri di X. Se ogni parola $p \in P$ ha grado $d(p) = k$ o 1 allora $Card\,(X) = (k-1)\,Card\,(Q_X) + 1$, dove $Q_X = \{p \in P \mid d(p) = k\}$.*

Dimostrazione. Procediamo per induzione sulla lunghezza massima n delle parole di X.

Se $n = 0$ la proprietà vale poiché siamo nel caso $X = \{1\}$ e $P = Q_X = \emptyset$.

Supponiamo adesso $n > 0$. Distinguiamo due casi.

- Se $1 \notin Q_X$, allora tutte le parole di X cominciano con la stessa lettera $a \in A$, ovvero $X = aY$. Tale insieme Y sarà o un codice prefisso finito oppure l'insieme $\{1\}$. In entrambi i casi si avrà $\mathrm{Card}\,(Q_X) = \mathrm{Card}\,(Q_Y)$. Per ipotesi induttiva, dunque, $\mathrm{Card}\,(X) = \mathrm{Card}\,(Y) = (k-1)\mathrm{Card}\,(Q_Y) + 1 = (k-1)\mathrm{Card}\,(Q_X) + 1$.

- Se $1 \in Q_X$, potremo scrivere $X = \cup_{a \in A} X_a$. Ponendo $t_a = \mathrm{Card}\,(Q_{X_a})$ si ha
$$\mathrm{Card}\,(Q_X) = 1 + \sum_{a \in A} t_a,$$
da cui
$$\sum_{a \in A} t_a = \mathrm{Card}\,(Q_X) - 1.$$
Per ipotesi induttiva abbiamo $\mathrm{Card}\,(Q_{X_a}) = (k-1)t_a + 1$. Dunque
$$\begin{aligned} \mathrm{Card}\,(X) &= \sum_{a \in A} \mathrm{Card}\,(X_a) \\ &= \sum_{a \in A} (k-1)t_a + k \\ &= (k-1)\mathrm{Card}\,(Q_X) - (k-1) + k \\ &= (k-1)\mathrm{Card}\,(Q_X) + 1 \end{aligned}$$

□

Teorema 3.1.3 (Teorema della Cardinalità)**.** *Siano F un insieme Sturmiano su un alfabeto di k lettere ed $X \subseteq F$ un codice F-massimale bifisso finito. Allora $Card(X) = (k-1)d_F(X) + 1$.*

Dimostrazione. Sia $P = XA^- \setminus X$ l'insieme dei prefissi propri di X. Un elemento $p \in P$ verifica $pA \subseteq P \cup X$ se e solo se è speciale a destra. Per il Lemma 3.1.1 tali parole sono esattamente $d_F(X)$ e dal Lemma 3.1.2 segue immediatamente la tesi. □

Esempio 3.1.4. Tutti i codici F-massimali bifissi finiti di F-grado 2 nel caso F sia l'insieme di Fibonacci hanno cardinalità 3.

Abbiamo definito le parole Sturmiane come le parole infinite aventi, per ogni n, esattamente $n+1$ fattori di lunghezza $n+1$, ovvero tali che $\mathrm{Card}\,(A^n \cap F(x)) = n+1 \ \forall\, n \geq 0$. Il seguente Corollario permette di generalizzare tale risultato non solo ad A^n ma anche a qualsiasi altro codice massimale bifisso finito di grado n.

Corollario 3.1.5. *Siano x una parola Sturmiana su $A = \{a, b\}$ ed $X \subseteq A^+$ un codice massimale bifisso finito di grado d. Allora $Card\,(X \cap F(x)) = d+1$.*

Dimostrazione. Essendo X un codice massimale bifisso finito, per il Corollario 2.4.23 si ha $d = d_{F(x)}(X \cap F(x))$. Dal Teorema 3.1.3 si ricava dunque $\mathrm{Card}\,(X \cap F(x)) = (2-1)d_{F(x)}(X) + 1 = d + 1$. □

Il seguente Esempio mostra che non è possibile invertire il Corollario 3.1.5 e dunque neanche il Teorema 3.1.3.

Esempio 3.1.6. Sia $x = babf$ con f la parola di Fibonacci definita nell'Esempio 2.2.2. Ovvero

$$x = bababaabaababaabababaabaababaabab \cdots .$$

Tale parola non è Sturmiana poiché ha 7 fattori di lunghezza 5.

Poiché $babab \notin F(f)$, si ha $z \in F(x) \setminus F(f)$ per ogni prefisso z di x di lunghezza $|z| > 4$. D'altra parte se z non è un prefisso di x oppure ha lunghezza $|z| \leq 4$ allora esso è un fattore di f. Ovvero

$$F(x) \setminus babaA^+ \subseteq F(f). \tag{3.1}$$

Essendo $F(f) \subseteq F(bf) \subseteq F(abf)$, per dimostrare l'Equazione 3.1 è sufficiente provare che $F(abf) = F(f)$. Sia $z \in F(abf)$. Se z non è un prefisso di abf o di bf, allora chiaramente si avrà $z \in F(f)$. È noto che ogni prefisso della parola di Fibonacci è speciale a sinistra. Dunque $bg \in F(f)$ per ogni prefisso g di f. Supponiamo, infine, che $z = abg$ per qualche prefisso g di f. Per quanto appena visto e poiché $F(x)$ è chiuso per rovescio, si ha $\widetilde{g}b \in F(f)$. Essendo $F(f)$ essenzialmente destro, ogni parola di $F(f)$

ha ordine destro almeno 1, e poiché $bb \notin F(f)$, si ha $\widetilde{g}ba \in F(f)$, da cui $z \in F(f)$.

Mostriamo adesso che esiste una famiglia $\{X_d\}_{d>0}$ di codici massimali bifissi finiti con $\deg X_d = d$, tali che $\mathrm{Card}\,(F(x) \cap X_d) = d+1$ per ogni $d > 0$.

Sia $X_d = A^d$ per $d \leq 4$. Per il Teorema 2.4.30 ed il Teorema 2.4.29 sappiamo che esiste ed è unico il codice massimale bifisso finito di grado d e nucleo $\{baba\}$. Sia esso X_d per ogni $d > 4$. I codici così costruiti sono tali che $X_d \cap babaA^+ = \emptyset$ per ogni $d > 0$.

Dall'Equazione 3.1 e dal Teorema 3.1.3 ricaviamo, per ogni $d > 0$,

$$\mathrm{Card}\,(F(x) \cap X_d) = \mathrm{Card}\,(F(f) \cap X_d) = d+1.$$

Osservazione 3.1.7. La parola x dell'Esempio 3.1.6 non è neanche ricorrente. Infatti se esistesse una parola $v \in A^*$ tale che $(babab)v(babab) \in F(x)$, si avrebbe $babab \in F(f)$.

Dunque esiste una parola non ricorrente ed una famiglia $\{X_d\}_{d>0}$ di codici massimali bifissi con $\deg X_d = d$, tali che x ha esattamente $d+1$ fattori di lunghezza d in X_d per ogni $d > 0$.

Non si conosce se il Corollario 3.1.5 sia invece invertibile aggiungendo l'ipotesi aggiuntiva che la parola sia ricorrente.

Congettura 1. *Siano x una parola ricorrente ed $\{X_d\}_{d>0}$ una famiglia di codici massimali bifissi finiti con* $\deg X_d = d$ *e* $\mathrm{Card}\,(F(x) \cap X_d) = d+1$ *per ogni $d > 0$. Allora x è Sturmiana.*

3.2 Periodicità

Nella Sezione 1.2.3 abbiamo dato la nozione di parola definitivamente periodica. Abbiamo visto, inoltre, che se una parola infinita $x \in A^\omega$, con A un alfabeto di k caratteri, è tale che $\mathrm{Card}\left(A^d \cap F(x)\right) \leq d+k-2$ per un opportuno $d \geq 1$ allora essa è definitivamente periodica (Teorema 1.2.6). Vediamo adesso una generalizzazione di tale risultato.

Siano $x \in A^\omega$ ed X un codice thin massimale bifisso. Per ogni suffisso infinito y di x si ha $F(y) \subseteq F(x)$ e dunque, per l'Equazione 2.3, $d_{F(y)}(X) \leq d_{F(x)}(X)$.

Una parola x è detta *X-stabile* se $d_{F(y)}(X) = d_{F(x)}(X)$ per tutti i suffissi y di x. Data una parola $x \in A^\omega$, il suffisso y di x tale che $d_{F(y)}(X)$ sia minimale è una parola X-stabile.

Esempio 3.2.1. Siano $X = a \cup ba^*b$ ed $x = ba^\omega$. Il suffisso a^ω di x è una parola X-stabile.

Prima di proseguire enunciamo il Teorema della Fattorizzazione Critica (si veda [9]).

Data una coppia di parole finite non entrambe vuote $(u, v) \neq (1, 1)$ consideriamo l'insieme $R(u, v)$ delle parole non vuote comparabili per prefissi con v e comparabili per suffissi con u, ossia l'insieme

$$R(u, v) = \left\{ r \in A^+ \mid A^*u \cap A^*r \neq \emptyset \neq vA^* \cap rA^* \right\}.$$

Tale insieme è non vuoto poiché vi appartiene la parola $r = vu$. Chiamiamo *ripetizione* della coppia (u, v) la minima lunghezza $\mathrm{rep}(u, v)$ delle parole di $R(u, v)$.

Teorema 3.2.2 (Teorema della Fattorizzazione Critica)**.** *Per ogni parola $w \in A^+$, il valore massimo di $\mathrm{rep}(p, s)$, per ogni possibile fattorizzazione $w = ps$ con $p, s \in A^+$, è il periodo di w.*

Una fattorizzazione (p, s) di una parola w tale che $\mathrm{rep}(p, s)$ è il periodo di w è detta *critica*. Il Teorema 3.2.2 afferma, dunque, che ogni parola ha una fattorizzazione critica.

Di seguito ci saranno utile anche i seguente risultati.

Lemma 3.2.3. *Siano X un codice thin massimale bifisso ed x una parola X-stabile. La parola x ha un numero infinito di fattori con $d_{F(x)}(X)$ parse rispetto ad X. Inoltre tali fattori di x potranno essere scelti prefissi.*

Dimostrazione. Per ogni fattorizzazione $x = uy$ con $u \in A^*$ e $y \in A^\omega$ avremo y X-stabile, ovvero $d_{F(y)}(X) = d$, quindi y avrà un fattore $w \in F(y) \subseteq F(x)$ con d parse. Inoltre scegliendo tale w come prefisso di y avremo che uw è un prefisso di x con d parse. □

Lemma 3.2.4. *Siano $x \in A^\omega$ una parola infinita ed $n \geq 1$ un intero tale che il periodo di un numero infinito di prefissi di x sia al più n. Allora x è periodica.*

Dimostrazione. Sia $x = a_0 a_1 \cdots$ con $a_i \in A$. Avendo un numero infinito di prefissi di x periodo al più n ve ne sarà un'infinità di essi che avranno periodo uguale, sia esso p. Per ogni $i \geq 0$ vi è un prefisso di x di lunghezza maggiore di $i + p$ di periodo p. Dunque $a_i = a_{i+p}$, da cui la tesi. □

Siamo adesso pronti per dimostrare la generalizzazione annunciata prima.

Teorema 3.2.5. *Siano X un codice thin massimale bifisso ed $x \in A^\omega$ una parola X-stabile. Se $\mathrm{Card}(X \cap F(x)) \leq d_{F(x)}(X)$, allora x è definitivamente periodica.*

Dimostrazione. Siano $P = A^* \setminus XA^*$ ed $S = A^* \setminus A^*X$ e poniamo $d = d_{F(x)}(X)$.

L'insieme $X \cap F(x)$ è finito poiché, per ipotesi e per l'Osservazione 2.4.19, $\mathrm{Card}\,(X \cap F(x)) \leq d \leq d(X)$. Sia n la massima lunghezza delle parole in $X \cap F(x)$.

Consideriamo una fattorizzazione $x = uwvz$ con $u, w, v \in A^+$, $z \in A^\omega$ tali che $|u|, |v| > n$ e $\delta_X(u) = \delta_X(v) = d$. Tale scelta è possibile perché, essendo x e vz parole X-stabili, per il Lemma 3.2.3, esse avranno un numero infinito di prefissi con d parse rispetto ad X.

Mostriamo adesso che, per ogni fattorizzazione $w = ps$, si ha $\mathrm{rep}(p, s) \leq n$.

Dall'Equazione 2.6 sappiamo che $\delta_X(up) = \delta_X(sv) = d$, dunque vi sono d suffissi $p_1 = 1, p_2, \ldots, p_d$ di up che sono in P e d prefissi $s_1 = 1, s_2, \ldots, s_d$ di sv che sono in S.

Poichè anche $upsv$ ha d parse, per ogni $2 \leq i \leq d$ vi è esattamente un $2 \leq j \leq d$ tale che $p_i s_j \in X$. Infatti per ogni p_i vi è, per costruzione, un prefisso s' di sv tale che $p_i s' \in X$. Ma tale s' è appunto uno degli s_j. Possiamo dunque rinumerare gli s_j in modo che $s_1 = 1$ e per $2 \leq i \leq d$ si abbia $x_i = p_i s_i \in S$. Essendo X un codice massimale bifisso ed up, sv parole sufficientemente lunghe, esistono $x_0, x_1 \in X$ rispettivamente un suffisso di up ed un prefisso di sv (Figura 3.1).

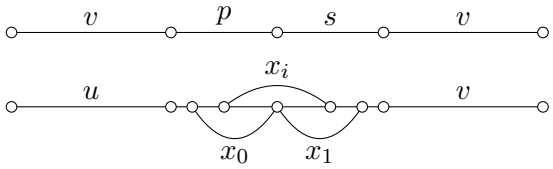


Figura 3.1: Le $d + 1$ parole $x_0, x_1, \ldots, x_d$.

Poiché $\mathrm{Card}\,(X \cap F(x)) \geq d$, due delle $d+1$ parole $x_0, x_1, \ldots x_d$ saranno uguali.

- Se $x_0 = x_1$ allora proprio $x_0 = x_1 \in X \cap F(x)$ sarà una ripetizione di (p, s) di lunghezza al più n per costruzione. Dunque $\mathrm{rep}(p, s) \leq n$.
- Se $x_0 = x_i$ con $2 \leq i \leq d$ allora s_i sia prefisso di sv sia suffisso di x_0 e quindi di up. Dunque $\mathrm{rep}(p, s) \leq |s_i| \leq |p_i s_i| = |x_i| \leq n$.
- Se $x_i = x_1$ con $2 \leq i \leq d$ vale un ragionamento analogo a quello appena mostrato.
- Se $x_i = x_j$ con $2 \leq i < j \leq d$ supponiamo $|p_i| < |p_j|$. Si avrà $p_j = p_i t$ e $t s_j = s_i$ per un opportuno $t \in A^+$. Tale t sarà sia suffisso di p_j e quindi di up, sia prefisso di s_i e quindi di sv. Dunque $\mathrm{rep}(p, s) \leq |t| \leq n$.

Riassumendo, per ogni fattorizzazione $w = ps$ si ha $\mathrm{rep}(p, s) \leq n$. Per il Teorema della Fattorizzazione Critica il periodo di w sarà al più n. Quindi un numero infinito di prefissi di y hanno periodo al più n. Per il Lemma 3.2.4 y è periodica, da cui la tesi. □

Corollario 3.2.6. *Sia $x \in A^\omega$ una parola infinita. Se esiste un codice X massimale bifisso finito di grado d tale che $Card\,(X \cap F(x)) \leq d$, allora x è definitivamente periodico.*

Dimostrazione. Ogni parola sufficientemente lunga di X ha d parse, quindi $d_{F(x)}(X) = d$ ed x è X-stabile. Dall'ipotesi $\mathrm{Card}\,(X \cap F(x)) \leq d$ segue, per il Teorema 3.2.5, la tesi. □

Osservazione 3.2.7. A^d è un codice massimale bifisso di grado d. Quindi il caso $k = 2$ del Teorema 1.2.6 segue dal Corollario 3.2.6.

Esempio 3.2.8. Sia $X = \{a^3, a^2ba, a^2b^2, ab, ba^2, baba, bab^2, b^2a, b^3\}$ il codice massimale bifisso finito mostrato in Figura 3.2. Sia $x \in A^\omega$ tale che $X \cap F(x) = \{a^2ba, ab, baba\}$ (i nodi in neretto in Figura 3.2).

Essendo ba un fattore di x potremo scrivere $x = ubay$ per opportuni $u \in A^*$ e $y \in A^\omega$. La prima lettera di y è b poiché, altrimenti, si avrebbe $ba^2 \in X \cap F(x)$; la seconda lettera di y è a poichè, altrimenti, si avrebbe $bab^2 \in X \cap F$. Da quest'argomento ricaviamo che $x = u\,(ba)^\omega$ per un'opportuna parola $u \in A^*$.

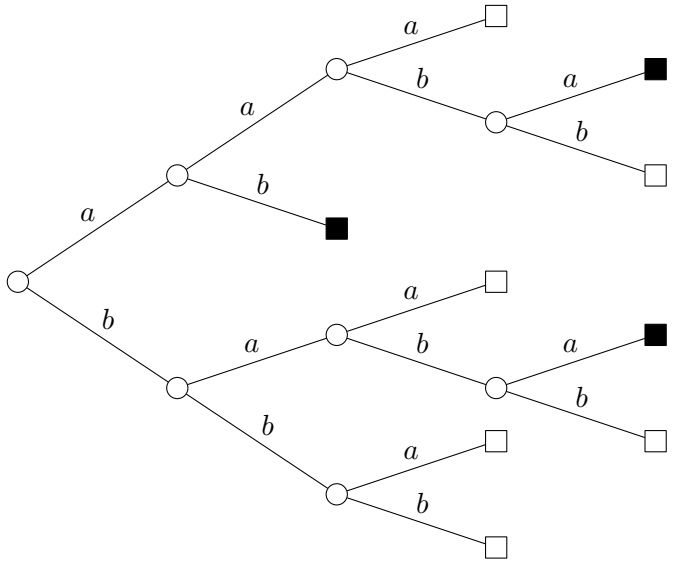


Figura 3.2: Rappresentazione del codice massimale bifisso $X = \{a^3, a^2ba, a^2b^2, ab, ba^2, baba, bab^2, b^2a, b^3\}$. In neretto $X \cap F(x)$.

3.3 Parole di ritorno

Siano F un insieme fattoriale ed $u \in F$. Definiamo gli insiemi

$$R_F(u) = \Gamma_F(u) \setminus \Gamma_F(u)A^+, \qquad \text{e} \qquad R'_F(u) = \Gamma'_F(u) \setminus A^+\Gamma'_F(u),$$

dove

$$\Gamma_F(u) = \{z \in F \mid uz \in A^+u \cap F\} \qquad \text{e} \qquad \Gamma'_F(u) = \{z \in F \mid zu \in uA^+ \cap F\}.$$

Nel caso $F = F(x)$ sia l'insieme dei fattori di una parola infinita x, gli insiemi $\Gamma_F(u)$ e $R_F(u)$ sono detti rispettivamente l'insieme delle *parole di ritorno destre* e l'insieme delle *parole di primo ritorno destre* di u in x. Analogamente $\Gamma'_F(u)$ e $R'_F(u)$ sono rispettivamente gli insiemi delle *parole di ritorno sinistre* e delle *parole di primo ritorno sinistre* di u in x.

Si ha una semplice relazione tra $R_F(u)$ e $R'_F u$, ossia

$$uR_F(u) = R'_F(u)u. \tag{3.2}$$

Le parole nell'insieme definito nell'Equazione 3.2 sono dette *parole di ritorno complete* (si veda [8]).

Esempio 3.3.1. Sia F l'insieme di Fibonacci. Gli insiemi delle parole di primo ritorno destre e sinistre sono date nella Tabella 3.3.

u	1	a	b	aa	ab	ba	aab	...
$R_F(u)$	a b	a ba	ab aab	baa $babaa$	ab aab	ba aba	aab $abaab$	...
$R'_F(u)$	a b	a ab	ba baa	aab $aabab$	ab aba	ba baa	aab $aabab$	...

Una parola x è Sturmiana se e solo se per ogni $u \in F(x)$ si ha Card $(R'_F(u)) = 2$ (si veda [8]). Inoltre vale il seguente risultato (si veda [8]) che lega il Teorema 2.2.5 e le parole di ritorno.

Proposizione 3.3.2. *Siano s una parola episturmiana standard su A, $\Delta = a_0a_1\cdots$ la sua parola direttiva e (u_n) la sequenza dei suoi prefissi palindromi. Allora*

(i) Le parole di primo ritorno sinistro di u_n sono le parole $\psi_{a_0\cdots a_{n-1}}(a)$ con $a \in A$.

(ii) Per ogni $u \in F(s)$ esistono $n \geq 0$ e $z \in A^*$ tali che le parole di primo ritorno sinistro di u sono le parole zyz^{-1} al variare di $y \in R'_F(u_n)$.

Da questa Proposizione segue il seguente Corollario.

Corollario 3.3.3. *Sia F un insieme Sturmiano. Per ogni $u \in F$, gli insiemi $R_F(u)$ sono una base del gruppo libero A°.*

Dimostrazione. Sia s una parola episturmiana stretta standard tale che $F = F(s)$. Dal punto (i) della Proposizione 3.3.2 sappiamo che $R'_F(u_n)$ è l'immagine di A tramite l'automorfismo $\psi_{a_0 \cdots a_{n-1}}$ e dunque una base del gruppo libero su A. Dal punto (ii) della stessa Proposizione ricaviamo che anche $R_F(u)$ è una base, in quanto immagine tramite l'automorfismo di coniugazione per z di $R'_F(u_n)$ per opportuni $z \in A^*$ e $n \geq 0$. □

Quanto mostrato nel Corollario 3.3.3 vale anche per gli insiemi $R'_F(u)$. Infatti per l'Equazione 3.2 gli insiemi $R_F(u)$ e $R'_F(u)$ sono coniugati nel gruppo libero, ovvero esiste un automorfismo, la coniugazione tramite u, che manda il primo nel secondo.

3.4 Basi di sottogruppi

Prima di proseguire abbiamo bisogno di alcuni risultati preliminari. Il seguente Lemma è dimostrato in [1, Proposizione 6.6.1].

Lemma 3.4.1. *Siano F un insieme Sturmiano ed $X \subseteq F$ un codice F-massimale bifisso finito. Allora $\langle X \rangle \cap F = X^* \cap F$.*

Lemma 3.4.2. *Siano F un insieme Sturmiano ed $X \subseteq F$ un codice F-massimale bifisso finito. Ogni classe laterale destra del sottogruppo H generato da X contiene al più un prefisso proprio di X speciale a destra.*

Dimostrazione. Sia Q l'insieme dei prefissi propri di X che sono speciali a destra e siano $p, q \in Q$ tali che $Hp = Hq$. Da $p \in Hq$ ricaviamo che esisterà una parola $u \in F$ tale che $p = uq$. Dunque $Huq = Hq$, da cui $Hu = H$, ovvero $u \in H$. Per il Lemma 3.4.1 si ha $u \in \langle X \rangle \cap F = X^* \cap F \subseteq X^*$. Essendo p un prefisso proprio di X si ha necessariamente $u = 1$, da cui $p = q$. □

Lemma 3.4.3. *Siano F un insieme Sturmiano, $d \geq 1$ un intero ed $X \subseteq F$ un codice F-massimale bifisso di F-grado d. Siano P l'insieme dei prefissi propri di X, $Q \subseteq P$ l'insieme delle parole in P che sono speciali a destra ed H il sottogruppo generato da X. Allora l'insieme*

$$V = \{v \in A^\circ \mid Qv \subseteq HQ\}$$

è un sottogruppo di A°.

Dimostrazione. Chiaramente $1 \in V$.

Ogni $v \in V$ definisce una permutazione su Q, ovvero possiamo pensare $V \subseteq \mathcal{S}(Q)$. Infatti se $p, q \in Q$ sono tali che $pv, qv \in Hr$ per un'opportuna parola $r \in Q$, allora $rv^{-1} \in Hp \cap Hq$. Per quanto visto nella Sottosezione 1.1.3 ciò implica $Hp = Hq$ e dunque, per il Lemma 3.4.2, $p = q$.

Gli inversi di elementi di V stanno ancora in V. Infatti, poiché ogni $v \in V$ definisce una permutazione su Q, per ogni $q \in Q$ esiste un $p \in Q$ tale che $pv \in Hq$. Dunque $qv^{-1} \in Hp$, ovvero anche $v^{-1} \in V$

Infine V è chiuso rispetto al prodotto. Infatti dati $v, w \in V$ si ha la catena di inclusioni $Qvw \subseteq HQw \subseteq HQ$ e dunque $vw \in V$. □

Siamo adesso in grado di provare il seguente risultato

Teorema 3.4.4 (Teorema dalla Base Sturmiana)**.** *Siano F un insieme Sturmiano e $d \geq 1$ un intero. Un codice bifisso $X \subseteq F$ è una base di un sottogruppo di indice d di A° se e solo se esso è F-massimale bifisso finito di F-grado d.*

Dimostrazione.

(⇐) Siano X un codice F-massimale bifisso di F-grado d e P, Q, H e V come nel Lemma 3.4.3. Dunque $V \leq A^\circ$.

Per il Lemma 3.1.1 esiste una parola u speciale a destra tale che $\delta_X(u) = d$ e i cui d suffissi che sono in P sono in Q. Per il Teorema 2.4.20, tale parola u non sarà in $H(X)$.

Mostriamo che l'insieme $R_F(u)$ delle parole di primo ritorno di u è contenuto in V. Infatti, siano $q \in Q$ ed $y \in R_F(u)$. Per definizione di $R_F(u)$ si avrà $uy \in F$. Poiché q è un suffisso di u, qy sarà un suffisso di uy e dunque anche $qy \in F$. Allora, essendo X un codice F-massimale, esisterà una parola $r \in P$ tale che $qy \in X^*r$. Tale r è un elemento di Q. Infatti, per la Formula 3.2 esisterà una parola y' tale che $uy = y'u$. Per cui r è suffisso di $y'u$ e se, per assurdo, si avesse $|r| > |u|$ si avrebbe $u \in H(X)$, in contraddizione con quanto detto sopra (Figura 3.3). Dunque r è un suffisso di u e quindi $r \in Q$

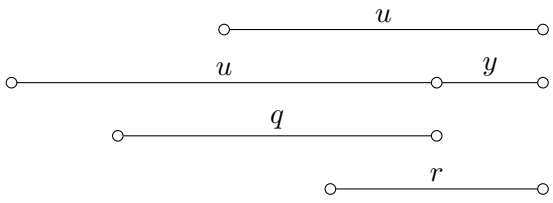


Figura 3.3: Una parola $y \in R_F(u)$.

Essendo $X^* \subseteq Q$ per ipotesi, si ha $qy \in X^*r \in HQ$. Ovvero $y \in V$, da cui $R_F(u) \subseteq V$.

V è un sottogruppo di A° (per il Lemma 3.4.3) che contiene $R_F(u)$ e poiché, per il Corollario 3.3.3, il gruppo generato da $R_F(u)$ è A°, abbiamo $V = A^\circ$.

Dunque per ogni $w \in A^\circ$ si ha $Qw \subseteq HQ$. In particolare, essendo $1 \in Q$, si ha $w \in HQ$ per ogni $w \in A^\circ$, ovvero $A^\circ = HQ$. Dal fatto che $\mathrm{Card}\,(Q) = d$ e che le classi laterali Hq al variare di $q \in Q$ sono a due a due disgiunte, ricaviamo che H è un sottogruppo di indice d di A°, ovvero che $[A^\circ : \langle X \rangle] = d$. Dalla Formula di Schreier 1.3 e dal Teorema della Cardinalità (Teorema 3.1.3) ricaviamo che una base di $\langle X \rangle$ è proprio X.

($\Rightarrow$) Sia $X \subseteq F$ un codice bifisso base del gruppo $H = \langle X \rangle \leq A^\circ$ con indice $[A^\circ : H] = d$. Dalla Formula di Schreier 1.3 si ha $\mathrm{Card}\,(X) = (k-1)d + 1$ con $k = \mathrm{Card}\,(A)$. Il caso $k = 1$ è banale; supponiamo quindi $k \geq 2$. Per il Teorema 2.4.33 esisteranno un intero $d' \geq 0$ ed un codice Y F-massimale bifisso di F-grado d' con $X \subseteq Y$.

Dalla prima parte della dimostrazione sappiamo che Y è una base di un sottogruppo $K = \langle Y \rangle \leq A^\circ$ con indice $[A^\circ : K] = d'$. Da $X \subseteq Y$ otterremo $H \leq K$, da cui ricaviamo, per la Formula 1.1 che d è un multiplo di d'.

Per il Teorema della Cardinalità (Teorema 3.1.3) si ha $\mathrm{Card}\,(Y) = (k-1)d' + 1$ e dunque, essendo $X \subseteq Y$, $(k-1)d + 1 \leq (k-1)d' + 1$, ovvero $d' \leq d$.

Quindi d è un multiplo di d' con $d' \leq d$, ovvero $d = e$ e, dunque, $X = Y$.

□

Osservazione 3.4.5. Dal Teorema della Base Sturmiana discende, in particolare, il Teorema della Cardinalità già visto nella sezione 3.1. Infatti siano F un insieme Sturmiano su un alfabeto A di k lettere ed X un codice F-massimale bifisso finito di F-grado d. Per il Teorema 3.4.4, il sottogruppo $\langle X \rangle$ del gruppo libero A° ha rango $\mathrm{Card}\,(X)$ ed indice d. Dunque per la Formula di Schreier 1.3 si ha $\mathrm{Card}\,(X) = (\mathrm{Card}\,(A) - 1) + 1$.

Corollario 3.4.6. *Siano F un insieme Sturmiano e $d \geq 1$ un intero. L'insieme di parole in $F \cap A^d$ è una base del sottogruppo $\langle A^d \rangle$ di A°.*

Dimostrazione. L'insieme A^d è un codice massimale bifisso, l'insieme $F \cap A^d$ è un codice bifisso finito e, per il Corollario 2.4.23, F-massimale bifisso di F-grado d. Dunque $\langle F \cap A^d \rangle$ è, per il Teorema 3.4.4 una base del sottogruppo $\langle A^d \rangle$. □

Nella Sottosezione 1.3.5 si è definito il concetto di codice di gruppo. Un codice di gruppo Z, ossia un sottomonoide tale che $Z^* = H \cap A^*$ per qualche sottogruppo $H \leq A^\circ$ di indice d del gruppo libero, è un codice massimale bifisso di grado d (si veda [1, Proposizione 6.1.5]).

Il seguente Corollario mostra che ogni sottogruppo di A° di indice finito ha una base contenuta in ogni insieme Sturmiano F.

Corollario 3.4.7. *Sia F un insieme Sturmiano e consideriamo la funzione che manda i sottoinsiemi $X \subseteq F$ nei sottogruppi $\langle X \rangle \leq A^\circ$. Vi è una biezione tra l'insieme dei codici F-massimali bifissi di F-grado d e quello dei sottogruppi di A° di indice d. In particolare il sottogruppo $\langle X \rangle$ avrà come base proprio il codice bifisso X. La biezione inversa associa ad ogni sottogruppo $H \leq A^\circ$ del gruppo libero l'insieme $Z \cap F$ con Z il codice di gruppo che è generatore minimale del sottomonoide $H \cap A^*$ di A^*.*

Dimostrazione. Sia X un codice F-massimale bifisso di F-gado d. Se X è finito allora, per il Teorema 3.4.4, si ha $\langle X \rangle \leq A^\circ$ sottogruppo di indice d.

Viceversa, siano $H \leq A^\circ$ è un sottogruppo di indice d e Z il codice di gruppo tale che $Z^* = H \cap A^*$. Per il Corollario 2.4.23, l'insieme $X = Z \cap F$ è un codice F-thin ed F-massimale bifisso di F-grado $d' < d$. Inoltre per il Teorema 2.4.33 X è finito. Dunque, dal Teorema 3.4.4 ricaviamo che $\langle X \rangle$ è un sottogruppo di A° di indice d'.

Dalla catena di inclusioni $X = Z \cap F \subseteq Z \subseteq Z^* = H \cap A^* \subseteq H$ ricaviamo che $\langle X \rangle$ è un sottogruppo di H e, per la Formula 1.1, si ha che d' è un multiplo di d. Dunque $d' = d$ ed $\langle X \rangle = H$.

Sia, infine, X un codice F-massimale bifisso di F-grado d. Per il Teorema 3.4.4, $H = \langle X \rangle$ è un sottogruppo di indice d di A°. Siano Z il codice di gruppo tale che $Z^* = H \cap A^*$ ed $Y = Z \cap F$. Allora $X \subseteq Y$ poiché Z un codice massimale bifisso si ha $X \subseteq Z$ e per costruzione $X \subset F$. Ma allora $X = Y$, essendo X F-massimale bifisso. Dunque le due funzioni sono l'una l'inversa dell'altra. □

Dal Corollario 3.4.7 ricaviamo, in particolare, che ogni sottogruppo di A° di indice finito è positivamente generato.

Il Teorema della Base Sturmiana ci permette, inoltre, dato un insieme Sturmiano, di contare i codici F-massimali bifissi finiti. Infatti Hall ha dato una formula per il numero di sottogruppi di indice d nel gruppo libero di rango k (si veda [7, Teorema 5.2]).

Corollario 3.4.8. *Sia F un insieme Sturmiano su un alfabeto di k lettere. Il numero $N_{d,k}$ di codici $X \subseteq F$ F-massimali bifissi finiti di F-grado d è dato ricorsivamente da $N_{1,k} = 1$ e*

$$N_{d,k} = d\,(d!)^{k-1} - \sum_{i=1}^{d-1} ((d-1)!)^{k-1}\, N_{i,k}.$$

Nel caso $k = 2$, ad esempio, la formula è

$$N_{d,2} = d\,d! - \sum_{i=1}^{d-1} (d-1)!\, N_{i,2}.$$

Capitolo 4

Gruppi Sintattici

Un ruolo fondamentale nella descrizione di monoidi finiti è data dallo studio dei gruppi contenuti dentro questi (si veda Sottosezione 1.1.3). Una parte importante della teoria degli automi è relativa proprio allo studio dei gruppi contenuti nel monoide sintattico. Dato un monoide di trasformazioni M su un insieme finito Q, definito da un insieme finito di generatori, è in generale non banale lo studio dei gruppi contenuti in M.

Di seguito considereremo il caso in cui i monoidi di trasformazioni sono particolari monoidi sintattici (si veda la Sottosezione 1.3.4), ovvero monoidi di transizione di automi minimali che riconoscono il sottomonoide generato da un codice prefisso X. Nella Sezione 4.1 si definiranno i gruppi di olonomia ed i gruppi sintattici e si esporranno due diversi metodi per calcolare l'insieme di generatori di un gruppo di olonomia.

Nella Sezione 4.2 studieremo le relazioni di Green, uno strumento fondamentale in Teoria dei Semigruppi.

Nella Sezione 4.4 si enuncierà la Congettura del rango (Congettura 2) proposta da D. Perrin e mostriamo sia che essa è valida nel caso di alfabeti binari (Teorema 4.4.1) sia che essa non può esser migliorata (Teorema 4.4.5).

Infine nella Sezione 4.5 mostreremo come per una particolare classe di codici prefissi tutti i gruppi sintattici propri sono ciclici, finiti e regolari.

4.1 Gruppi di olonomia

Siano Q un insieme finito ed M un monoide di trasformazioni su Q. Per ogni sottoinsieme $I \subseteq Q$ definiamo lo *stabilizzatore* di I come l'insieme

$$\mathrm{Stab}(I) = \{m \in M \mid mI = I\}.$$

La restrizione di $\mathrm{Stab}(I)$ all'insieme I, che indicheremo con $\mathrm{Stab}(I)|_I$, è un gruppo di permutazioni detto *gruppo di olonomia* di M relativo ad I. Esso sarà denotato con $\mathrm{Group}(I)$.

Ricordiamo la definizione data nella Sottosezione 1.1.3 di gruppo in un monoide. Sia M un monoide. Un gruppo in M è un sottosemigruppo di M che è isomorfo ad un gruppo. In generale l'elemento neutro di un gruppo in M non è 1_M, ma solo un idempotente del monoide.

Diremo che un gruppo in M è *massimale* se non è contenuto propriamente in alcun altro gruppo in M. Per ogni idempotente $e \in M$ vi è un unico gruppo massimale in M contenente e. Esso è denotato con $G(e)$.

Proposizione 4.1.1. *Siano M un monoide di trasformazioni su Q e G un gruppo in M. Tutti gli elementi di G hanno la stessa immagine I. La restrizione degli elementi di G alla loro immagine comune è una rappresentazione fedele di G come gruppo di permutazioni su I.*

Dimostrazione. Siano $g, h \in G$. Mostriamo che essi hanno la stessa immagine. Sia k l'inverso di g in G. Allora $h = hkg$, da cui ricaviamo che $h = (1 \cdot (hk)) \cdot g \in Mg$. Analogamente si ottiene $g \in Mh$. Dunque $Mg = Mh$. Chiamiamo I l'immagine comune degli elementi di G.

G è un gruppo di permutazioni su I. Infatti sia e l'elemento neutro di G. Per ogni $p \in I$ sia $q \in Q$ tale che $qe = p$. Allora $pe = qe^2 = qe = p$. Dunque e è l'identità anche su I. Inoltre ogni $g \in G$ possiede un inverso k e tale elemento è tale che $gk = kg = e$. Dunque g è una permutazione su I per ogni $g \in G$.

Infine mostriamo che la rappresentazione di G come gruppo di permutazioni su I è fedele. Siano $g, g' \in G$ tali che la loro restrizione su I è la stessa, ossia $g|_I = g'|_I$. Allora per ogni $p \in Q$ si ha $pg = p(eg) = (pe)g = pg' = (pe)g' = p(eg') = pg'$, poiché $pe \in I$. Dunque $g = g'$. □

Il gruppo di permutazioni formato dalle restrizioni delle funzioni di G rispetto all'immagine comune è detta *rappresentazione canonica* di G. La rappresentazione canonica del gruppo $G(e)$ è denotata con G_e. Tale rappresentazione è fedele per la Proposizione 4.1.1.

Per ogni insieme $I \subseteq Q$ esiste un idempotente $e \in M$ tale che $I \subseteq Qe$, infatti basta scegliere $e = 1_M$. Diremo che un idempotente $e \in M$ *ricopre esattamente* l'insieme I se $I \subseteq Qe$ e qe è minimale per tale proprietà.

Osservazione 4.1.2. Ogni idempotente e ricopre esattamente l'insieme Qe.

Osservazione 4.1.3. Sia e un idempotente che ricopre esattamente un insieme I. Allora $e \in \mathrm{Stab}(I)$. Infatti, essendo $I \subseteq Qe$, possiamo scrivere ogni $i \in I$ come $i = qe$ per un opportuno $q \in Q$. Dunque $ie = qe^2 = qe = i$, da cui, in particolare, $Ie = I$.

Il seguente Lemma mostra come per ogni insieme I il gruppo di olonomia di M relativo ad I si ottiene come restrizione ad I di un gruppo in M.

Lemma 4.1.4. *Siano Q un insieme finito, M un monoide di trasformazioni su Q, $I \subset Q$ ed $e \in M$ un idempotente che ricopre esattamente I. Allora $Group(I)$ è la restrizione ad I del gruppo $H = G(e) \cap Stab(I)$.*

Dimostrazione. Dato un elemento di $H \subseteq \mathrm{Stab}(I)$, la sua restrizione ad I è, per costruzione, in $\mathrm{Group}(I)$.

Viceversa mostriamo che ogni elemento di $\mathrm{Group}(I)$ è ottenuto come restrizione ad I di un elemento di H. Siano $m \in \mathrm{Stab}(I)$ e consideriamo l'elemento $g = eme$. Essendo M finito esisterà un intero n tale che $h = g^n$ è un idempotente. Esso appartiene a $\mathrm{Stab}(I)$, poiché per l'Osservazione 4.1.3 $e \in \mathrm{Stab}(I)$ e quindi anche $g = eme$ ed $h = g^n$ sono elementi di $\mathrm{Stab}(I)$. Dunque $I \subseteq Qh$. D'altra parte, però, $h \in Me$ da cui $Qh \subseteq Qe$. Dalla minimalità di Qe ricaviamo $Qh = Qe$ e quindi $h = e$.

Il sottomonoide generato da g è perciò un gruppo ciclico contenente e, il che implica che $g \in G(e)$ e dunque $g \in H$. Ciò mostra che $m|_I = g|_I$, da cui la tesi. □

La seguente Proposizione ci mostra che, dato un monoide M, ogni gruppo di olonomia relativo all'immagine di un idempotente è isomorfo ad un gruppo massimale in M.

Proposizione 4.1.5. *Siano Q un insieme finito, M un monoide di trasformazioni su Q, $e \in M$ un idempotente ed $I = Qe$. allora $Group(I) = G_e$.*

Dimostrazione. Dato un $g \in G(e)$ si ha, per la Proposizione 4.1.1, $Ig = Ie = Qe^2 = Qe = I$, ovvero $G(e) \subseteq \mathrm{Stab}(I)$.

Per il Lemma 4.1.4 $\mathrm{Group}(I) = (G(e) \cap \mathrm{Stab}(I))\,|_I = G(e)|_I$, che è, per definizione, G_e. □

Dato un automa $\mathcal{A}$ definiamo un *gruppo di olonomia* di $\mathcal{A}$ un gruppo di olonomia del monoide di transizione $\varphi_{\mathcal{A}}(A^*)$.

Siano $\mathcal{A}$ un automa, $I \subseteq Q$ e $w \in A^*$ tale che $\varphi_{\mathcal{A}}(w) \in \mathrm{Stab}(I)$. Allora $\varphi_{\mathcal{A}}(w)|_I$ è una permutazione appartenente a $\mathrm{Group}(I)$. Essa sarà detta permutazione su I *definita da* w.

Esempio 4.1.6. Sia $\mathcal{A} = (\{1, \dots 5\}, 1, 1)$ l'automa rappresentato in Figura 4.1. L'elemento $\varphi_{\mathcal{A}}(a^3)$ è un idempotente che ricopre esattamente l'insieme $I = \{1, 2, 3\}$. Come si può vedere anche dalla Figura 4.2 i due elementi $\varphi_{\mathcal{A}}(a)$ e $\varphi_{\mathcal{A}}(baa)$ sono entrambi in $\mathrm{Stab}(I)$. $\mathrm{Group}(I)$ contiene le permutazioni (123) e (23) definite rispettivamente da a e baa. Dunque $\mathrm{Group}(I) = \mathcal{S}_3$.

Siano X un codice prefisso, $\mathcal{A} = \mathcal{A}(X^*)$ l'automa minimale di X^* ed $M = \varphi_{\mathcal{A}}(A^*)$ il monoide di transizione di $\mathcal{A}$. Un *gruppo sintattico* di X è un gruppo di olonomia di M relativo all'immagine di un idempotente di M.

Dunque, per la Proposizione 4.1.5, un gruppo sintattico di X sarà del tipo $\mathrm{Group}(I)$ con $I = Qe$, dove Q è l'insieme degli stati di $\mathcal{A}$ ed e è un idempotente di M.

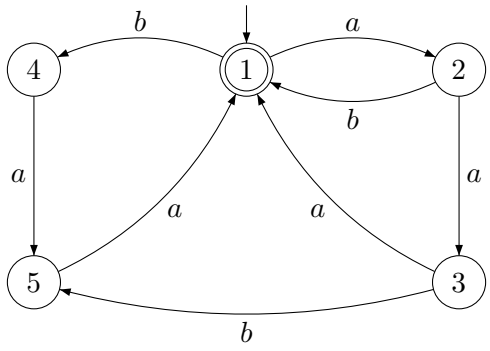


Figura 4.1: Un automa con gruppo d'olonomia S_3.

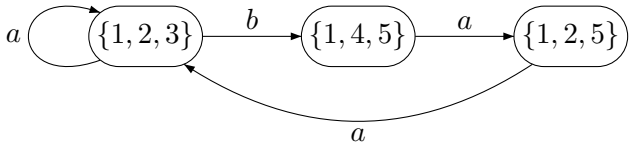


Figura 4.2: Azione delle lettere sui 3-sottoinsiemi di Q.

Di seguito esponiamo due diversi metodi per calcolare l'insieme di generatori di un gruppo d'olonomia, e quindi in particolare di un gruppo sintattico. Il primo consiste nel calcolare la rappresenzatione si Schützenberger del monoide di trasformazione. La seconda usa il concetto di gruppo fondamentale.

4.1.1 Rappresentazione di Schützenberger

Siano Q un insieme finito, M un monoide di trasformazioni su Q, $e \in M$ un idempotente ed $I = Qe$. Consideriamo la famiglia di sottoinsiemi di Q

$$\mathcal{I} = \{J \subseteq Q \mid Im = J,\ Jm = I \text{ per opportuni } m, n \in M\}.$$

Per ogni $J \in \mathcal{I}$ poniamo m_J, m'_J gli elementi di M tali che

$$Im_J = J, \quad Jm'_J = I, \quad \text{con} \quad em_Jm'_J = e,$$

e ponendo, in particolare, $m_I = m'_I = e$.

Si dimostra che è sempre possibile scegliere degli m_J, m'_J di tal sorta.

Osservazione 4.1.7. Per ogni $J \in \mathcal{I}$ si ha $Jm'_Jm_J = J$. In effetti vale un risultato più forte: la restrizione di m'_Jm_J a J è l'identità su J. Infatti per ogni $j \in J$ esisterà un $i \in I$ tale che $j = im_J$. Dunque

$$jm'_Jm_J = im_Jm'_Jm_J = iem_Jm'_Jm_J = iem_J = im_J = j.$$

Per ogni $J, K \in \mathcal{I}$ ed $m \in M$ tali che $Jm = K$ consideriamo la restrizione $(m_J m m'_K)|_I$. Tale elemento sarà, per costruzione, in Group(G) e verrà denotato (J, m, K).

Dati $J, K, L \subseteq \mathcal{I}$ e $m, n \in M$ tali che $Jm = K$ e $Kn = L$ allora vale la formula

$$(J, m, K)(K, n, L) = (J, mn, L).$$

Infatti, per ogni $i \in I$ si ha

$$i(J, m, K)(K, n, L) = im_J m m'_K m_K n m'_L = im_J mnm'_L = i(J, mn, L).$$

La seguente Proposizione è un caso particolare di un risultato noto (si veda [4, Proposizione 9.2.1]).

Proposizione 4.1.8. *Siano Q un insieme finito, $I \subseteq Q$ un suo sottoinsieme, M un monoide di trasformazioni su Q ed S un insieme di generatori di M. Le permutazioni $(J, m, K) = m_J m m'_K|_I$ al variare di $m \in S$, e $J, K \in \mathcal{I}$ tali che $Jm = K$, formano un insieme di generatori del gruppo Group(I).*

Dato un monoide di trasformazioni M ed un suo idempotente $e \in M$ definiamo la *rappresentazione di Schützenberger* di M relativa ad e la funzione $\mu : M \to \mathrm{Mat}(\mathcal{I}, \mathcal{I})$ che associa ad un elemento $m \in M$ la matrice quadrata con elementi in Group$(I) \cup 0$ definita da

$$\mu(m)_{J,K} = \begin{cases} (J, m, K) & \text{se } Jm = K \\ 0 & \text{altrimenti.} \end{cases}$$

Quando M è il monoide di transizione di un automa $\mathcal{A}$, la rappresentazione di Schützenberger può essere vista come un transduttore, come mostrato nel seguente Esempio.

Esempio 4.1.9. Sia $\mathcal{A}$ l'automa dell'Esempio 4.1.6. Come già visto l'elemento $\varphi_{\mathcal{A}}(a^3)$ è un idempotente che ricopre esattamente l'insieme $I = \{1, 2, 3\}$.

L'insieme $\mathcal{I}$ è composto dai tre elementi I, $J = \{1, 4, 5\}$ e $K = \{1, 2, 5\}$. Notiamo che

$$Ib = J, \qquad Ja^2ba^2 = I \quad \text{e} \quad (a^2ba^2)(b)|_J = 1_J$$

e

$$Iba = K, \qquad Kaba^2 = I \quad \text{e} \quad (aba^2)(ba)|_K = 1_K.$$

Possiamo dunque scegliere $m_J = \varphi_{\mathcal{A}}(b), m'_J = \varphi_{\mathcal{A}}(a^2ba^2), m_K = \varphi_{\mathcal{A}}(ba)$ e $m'_K = \varphi_{\mathcal{A}}(aba^2)$.

La rappresentazione di Schützenberger di $\varphi_{\mathcal{A}}(A^*)$ relativa all'idempotente $\varphi_{\mathcal{A}}(a^3)$ può esser rappresentata tramite il transduttore della Figura 4.3.

Per la Proposizione 4.1.8, un insieme di generatori di $\varphi_{\mathcal{A}}(A^*)$ è dato da $(123), (23)$. Infatti $(I, a, I) = a^3aa^3|_I = (123)$, $(I, b, J) = a^3ba^2ba^2|_I = (1)$, $(J, a, K) = baaba^2|_I = (1)$, e $(K, a, I) = baaa^3|_I = (23)$. Ciò è coerente con quanto già visto nell'Esempio 4.1.6.

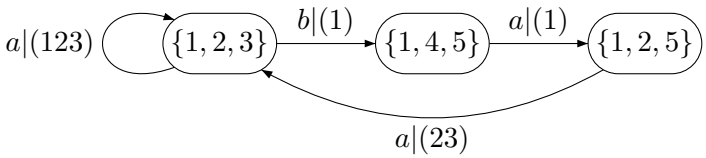


Figura 4.3: Rappresentazione di Schützenberger di $\varphi_{\mathcal{A}^*}$ relativa all'idempotente $\varphi_{\mathcal{A}}(a^3)$.

4.1.2 Gruppo fondamentale

Siano $\mathcal{A}$ un automa su un insieme finito Q di stati, M il monoide di transizione di $\mathcal{A}$, $e \in M$ un idempotente, $I = Qe$ ed $\mathcal{I} = \{J \subseteq Q \mid Im = J,\ Jm = I \text{ per opportuni } m, n \in M\}$. Sia $\mathcal{G}$ il grafo etichettato con vertici gli elementi di $\mathcal{I}$ e lati elementi dell'insieme $E = \{(J, a, K) \mid J, K \in \mathcal{I}, a \in A \text{ con } Ja = K\}$.

Osservazione 4.1.10. Il grafo $\mathcal{G}$ così definito è un grafo fortemente connesso.

Se $f = (J, a, K)$ è un lato di $\mathcal{G}$, chiameremo *lato inverso* di f, il lato $f^{-1} = (K, \bar{a}, J)$. Il grafo avente gli stessi vertici di $\mathcal{G}$ e per lati i lati inversi di quelli di $\mathcal{G}$ sarà detto *grafo inverso* di $\mathcal{G}$.

Analogamente a quanto già visto nella Sottosezione 1.3.5, definiamo *cammino generalizzato* in $\mathcal{G}$ una sequenza di lati consecutivi con etichette in $A \cup \bar{A}$. Le etichette dei cammini generalizzati saranno elementi del gruppo libero A°, ossia classi di equivalenza di cammini generalizzati con rappresentante minimale un cammino *semplificato*, cioè la cui etichetta non contiene fattori del tipo $a\bar{a}$ con $a \in A \cup \bar{A}$.

I cammini generalizzati da I ad I vengono detti anche *lacci* con base in I. Generalizzando la nozione di sottogruppo descritto dall'automa della Sottosezione 1.3.5, definiamo *gruppo fondamentale* rispetto al punto I l'insieme H dei lacci con base in I. È ben noto che H è un gruppo libero e che una sua base può essere ottenuta come segue.

Consideriamo $T \subseteq E$ uno spanning tree del grafo $\mathcal{G}$ con radice I. Essendo $\mathcal{G}$ fortemente connesso, per ogni $J \in \mathcal{I}$ vi sarà un unico cammino p_J in T da I a J. È ben noto che l'insieme

$$X = \{p_J f p_K^{-1} \mid f = (J, a, K) \in E \setminus T\}.$$

è una base di H, chiamata la *base di Schreier* relativa a T.

Analogamente consideriamo $S \subseteq E$ tale che S^{-1} sia uno spanning tree del grafo inverso a $\mathcal{G}$ con radice I. Per ogni $J \in \mathcal{G}$ vi sarà un unico cammino q_J in S da J in I.

Fissiamo T ed S e poniamo p_J e q_J al variare di $J \in \mathcal{I}$ come sopra.

Lemma 4.1.11. *Siano* $Y = \{p_J f q_K \mid (J, a, K) \in E \setminus T\}$ *ed* $Y' = \{p_J f q_K \mid (J, a, K) \in E\}$. *Allora* $Y = Y'$.

Dimostrazione. Chiaramente $Y \subseteq Y'$.

Dimostriamo l'inclusione inversa mostrando, per induzione sulla lunghezza di q_K, che $p_J f q_K \in Y$ anche quando $f = (J, a, K) \in T$. Essendo T un albero, sicuramente $K \neq I$ e dunque q_K è un cammino non vuoto. Sia $g = (K, b, L)$ il primo lato di q_K. L'insieme dei cammini in S è chiuso per suffissi, quindi potremo scrivere $q_K = q q_L$. Analogamente, essendo T un albero, si avrà $p_K = p_J f$. Per ipotesi induttiva $p_K q q_L \in Y$, e poiché $p_J f q_K = p_K q g_L$ la tesi è dimostrata. □

Proposizione 4.1.12. *L'insieme* $Y = \{p_J f q_K \mid f = (J, a, K) \in E \setminus T\}$ *è una base di* H.

Dimostrazione. Sia X la base di Schreier di H relativa a T. Chiaramente $Y \subseteq H = \langle X \rangle$. Proviamo che $X \subseteq \langle Y \rangle$. Per far ciò mostriamo che per ciascun $f = (J, a, K) \in E \setminus T$ si ha $p_J f p_K^{-1} \in \langle Y \rangle$.

Ciò è vero se q_K è vuoto, poiché $p_J f \in X \cap Y$. Altrimenti, essendo S chiuso per prefissi, possiamo scrivere $q_K = g q_L$ con $g = (K, b, L)$. Dunque $p_J f q_K = p_J f (p_K^{-1} p_K) g q_L = (p_J f p_K^{-1})(p_K g q_L)$, da cui $p_J f p_K^{-1} = (p_J f q_K)\,(p_K g q_L)^{-1} \in \langle Y \rangle$ poiché $p_J f q_K \in Y$ per definizione e $p_K g q_L \in Y$ per il Lemma 4.1.11. □

Dalla Proposizione 4.1.12 segue che per ogni scelta della coppia (T, S), Y è un insieme di generatori per Group(I), come mostrato nel seguente Corollario.

Corollario 4.1.13. *Le restrizioni ad* I *delle etichette degli elementi di* Y *generano Group*(I).

Dimostrazione. Per quanto visto nella Proposizione 4.1.12, le etichette degli elementi di Y formano il sottomonoide Stab(I). Dunque la loro restrizione ad I forma il gruppo Group(I). □

Osservazione 4.1.14. Per come abbiamo definito Y ogni elemento appare una sola volta. Infatti supponiamo esistano due lati $f = (J, a, K)$ ed $f' = (J', a', K')$ con $p_J f q_K = p_{J'} f' q_{K'}$ e p_J prefisso proprio di $p_{J'}$. Allora f sarà un lato del cammino $p_{J'}$ e dunque sarà in T contraddicendo la scelta di $f \in E \setminus T$.

Esempio 4.1.15. Consideriamo l'automa dell'Esempio 4.1.6, l'idempotente $\varphi_{\mathcal{A}}(a^3)$ e l'insieme $I = \{1, 2, 3\}$ da esso ricoperto. Il gruppo H è generato da

$$H = \langle (I, a, I), (I, baa, I) \rangle.$$

Il gruppo Group(I) è generato da $\varphi_{\mathcal{A}}(a)|_I = (123)$ e $\varphi_{\mathcal{A}}(baa)|_I = (23)$.

4.2 Relazioni di Green

Definiamo di seguito le relazioni di Green per un monoide M (si vedano [4] e [14]). Esse furono introdotte da J.A. Green nel 1951 e rappresentano una generalizzazione della naturale divisione tra interi al caso non commutativo dei semigruppi (e dunque dei monoidi).

Ricordiamo che una relazione sarà detta *preordine* se essa è riflessiva e transitiva, un *ordine* (*parziale*) se è un preordine antisimmetrico ed un'*equivalenza* se è un preordine simmetrico. Se $\leq_{\mathcal{K}}$ è un preordine, la relazione $\sim_{\mathcal{K}}$, o $\mathcal{K}$, definita da $x \sim_{\mathcal{K}} y \Leftrightarrow x \leq_{\mathcal{K}} y$ e $y \leq_{\mathcal{K}} x$ è un'equivalenza detta *relazione di equivalenza associata* ad $\leq_{\mathcal{K}}$.

Sia, di seguito, M un monoide. Definiamo le quattro relazioni di preordine $\leq_{\mathcal{R}}$, $\leq_{\mathcal{L}}$, $\leq_{\mathcal{J}}$ e $\leq_{\mathcal{H}}$ come segue

$$\begin{aligned} m \leq_{\mathcal{R}} n &\iff m = nu \text{ per qualche } u \in M, \\ m \leq_{\mathcal{L}} n &\iff m = un \text{ per qualche } u \in M, \\ m \leq_{\mathcal{J}} n &\iff m = unv \text{ per qualche } u, v \in M, \\ m \leq_{\mathcal{H}} n &\iff m \leq_{\mathcal{R}} n \text{ e } m \leq_{\mathcal{L}} n. \end{aligned}$$

Come già detto, tali relazioni possono essere considerate come una generalizzazione non commutativa della nozione di prodotto tra interi. Ad esempio, si avrà $m \leq_{\mathcal{R}} n$ se m è un *multiplo destro* di n, nel senso che si può ottenere m moltiplicando n a destra per un opportuno elemento di M.

Si possono riformulare le definizioni date in termini di ideali. Ovvero

$$\begin{aligned} m \leq_{\mathcal{R}} n &\iff mM \subseteq nM, \\ m \leq_{\mathcal{L}} n &\iff Mm \subseteq Mn, \\ m \leq_{\mathcal{J}} n &\iff MmM \subseteq MnM, \\ m \leq_{\mathcal{H}} n &\iff mM \subseteq nM \text{ e } Mm \subseteq Mn. \end{aligned}$$

La connessione tra i quattro preordini è rappresentata nel diagramma in Figura 4.4.

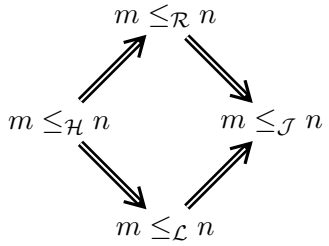


Figura 4.4: Connessione tra i preordini $\leq_{\mathcal{R}}$, $\leq_{\mathcal{L}}$, $\leq_{\mathcal{J}}$ e $\leq_{\mathcal{H}}$.

Le equivalenze associate alle quattro relazioni di preordine sopra definite sono dette *relazioni di Green* e sono denotate rispettivamente con $\mathcal{R}$, $\mathcal{L}$, $\mathcal{J}$ e $\mathcal{H}$. Dunque si ha

$$\begin{aligned} m\mathcal{R}n &\iff mM = nM, \\ m\mathcal{L}n &\iff Mm = Mn, \\ m\mathcal{J}n &\iff MmM = MnM, \\ m\mathcal{H}n &\iff mM = nM \text{ e } Mm = Mn. \end{aligned}$$

Osservazione 4.2.1. Analogamente a quanto visto nel diagramma in Figura 4.4, si ha, vedendo le relazioni come sottoinsiemi di $M \times M$,

$$\mathcal{R} \subseteq \mathcal{J}, \qquad \mathcal{L} \subseteq \mathcal{J} \quad \text{e} \quad \mathcal{H} = \mathcal{R} \cap \mathcal{L}.$$

Proposizione 4.2.2. *Le due relazioni di equivalenza $\mathcal{R}$ e $\mathcal{L}$ commutano, ovvero $\mathcal{RL} = \mathcal{LR}$.*

Dimostrazione. Dimostriamo che dati $m, n \in M$ tali che $m\mathcal{RL}n$ allora si avrà $m\mathcal{LR}n$. L'implicazione inversa sarà simmetrica.

Sia $p \in M$ tale che $m\mathcal{R}p$ e $p\mathcal{L}n$. Allora, per definizione, esisteranno $u, u', v, v' \in M$ tali che $p = mu$, $m = pu'$, $n = vp$ e $p = v'n$. Sia $q = vm$. Allora $q\mathcal{R}n$, infatti

$$q = vm = v(pu') = (vp)u' = nu' \quad \text{e} \quad n = vp = v(mu) = (vm)u = qu.$$

Inoltre $m\mathcal{L}q$, infatti

$$m = pu' = (v'n)u' = v'(nu') = v'q \quad \text{e} \quad q = vm \text{ per definizione.}$$

Dunque $m\mathcal{L}q\mathcal{R}n$, da cui la tesi. □

Poichè per la Proposizione 4.2.2 le due relazioni $\mathcal{R}$ e $\mathcal{L}$ commutano, possiamo definire la relazione di equivalenza $\mathcal{D} = \mathcal{RL} = \mathcal{LR}$.

Osservazione 4.2.3. Vedendo le relazioni come sottoinsiemi di $M \times M$ si ha

$$\mathcal{H} \subseteq \mathcal{R}, \mathcal{L} \subseteq \mathcal{D} \subseteq \mathcal{J}.$$

Possiamo rappresentare la connessione tra le cinque relazioni di Green tramite il diagramma in Figura 4.5

Si può dimostrare che, nel caso di monoidi finiti, $\mathcal{D} = \mathcal{J}$.

Le $\mathcal{D}$-classi possono essere rappresentate tramite uno schema detto "scatola delle uova" come in Figura 4.6. Le $\mathcal{R}$-classi contenute dentro la $\mathcal{D}$-classe sono rappresentate tramite le righe, mentre le $\mathcal{L}$-classi tramite le colonne. I quadrati ottenuti dalle intersezioni tra $\mathcal{R}$-classi ed $\mathcal{L}$-classi sono le $\mathcal{H}$-classi. La presenza di un idempotente all'interno di una $\mathcal{H}$-classe è indicata tramite un asterisco.

La forma regolare delle $\mathcal{H}$-classi nella Figura 4.6 è data dalla seguente Proposizione (si veda [4, Proposizione 1.12.3]).

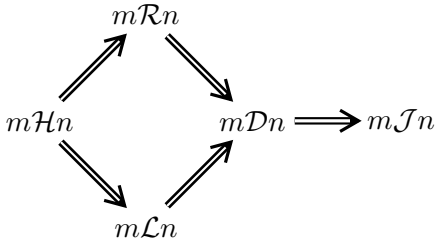


Figura 4.5: Connessioni tra le relazioni $\mathcal{R}, \mathcal{L}, \mathcal{J}, \mathcal{D}$ e $\mathcal{D}$.

	L_1	L_2	L_3	L_4	L_5	L_6
R_1	$*$					$*$
R_2			$*$			
R_3					$*$	
R_4		$*$		$*$		

Figura 4.6: Una $\mathcal{D}$-classe contenente alcuni idempotenti.

Proposizione 4.2.4. *Data una $\mathcal{D}$-classe, le $\mathcal{H}$-classi contenute in esse hanno tutte la stessa cardinalità.*

Denoteremo con $L(m)$ (risp. $R(m)$, $D(m)$, $H(m)$) la $\mathcal{L}$-classe (risp. $\mathcal{R}$-classe, $\mathcal{D}$-classe, $\mathcal{H}$-classe) dell'elemento $m \in M$. Con tale notazione si avrà

$$H(m) = R(m) \cap L(m) \quad \text{e} \quad R(m), L(m) \subseteq D(m).$$

Lemma 4.2.5. *Siano M un monoide ed $e \in M$ un idempotente. Allora $H(e)$ è il gruppo delle unità del monoide eMe.*

Dimostrazione.

($\subseteq$) Sia $m \in H(e)$. Esisteranno degli elementi $u, u', v, v' \in M$ tali che

$$e = mu, \quad m = eu', \quad e = vm, \quad m = v'e.$$

Allora $m = eu' = e^2u' = e(eu') = em = e(v'e) = (ev')e^2 = e(v'e)e = eme \in eMe$ e, in particolare, $me = em = m$. Inoltre m è invertibile sia a destra che a sinistra in M, infatti

$$m(eue) = (me)(ue) = mue = (mu)e = e^2 = e$$

e

$$(eve)m = (ev)(em) = evm = e^2 = e.$$

Dunque m appartiene al gruppo delle unità di eMe.

($\supseteq$) Sia $m \in eMe$ un elmento invertibile sia a destra che a sinistra in M. Allora esisteranno $u, v \in M$ tali che $mu = vm = e$. Essendo $eMe \subseteq M$ si ha, per quanto visto prima, $me = em = e$. Dunque $m\mathcal{H}e$.

□

Il monoide eMe è chiamato *monoide localizzato* in e. Esso è il più grande monoide contenuto in M avente e come elemento neutro.

Il Lemma precedente permette di ricavare un'importante proprietà sulle $\mathcal{H}$-classi.

Proposizione 4.2.6. *Un'$\mathcal{H}$-classe di un monoide M è un gruppo se e solo se essa contiene un idempotente.*

Dimostrazione. In ogni gruppo l'identità è, banalmente, un idempotente. Viceversa, se H è una $\mathcal{H}$-classe contenente un idempotente e, allora $H = H(e)$ è un gruppo per quanto visto nel Lemma 4.2.5. □

Per ogni idempotente $e \in M$, dunque $H(e)$ è un gruppo. La seguente Proposizione mostra che $H(e) = G(e)$, ovvero che $H(e)$ è l'unico gruppo massimale in M contenente e.

Proposizione 4.2.7. *Ogni gruppo G in M è contenuto in una $\mathcal{H}$-classe.*

Dimostrazione. Sia $G \subseteq M$ un gruppo con identità e. Per ogni $s \in G$ esisterà un elmento $t \in G$ inverso di s. Dunque si avrà

$$s = se, \quad e = st, \quad \text{ed} \quad s = es, \quad e = ts.$$

Dunque $s\mathcal{H}e$ per ogni $s \in G$, da cui $G \subseteq H(e)$. □

Si può dimostrare che tutti i gruppi massimali in M contenuti in una $\mathcal{D}$-classe, che per quanto appena visto sono della forma $H(e)$ con $e \in D$ un idempotente, sono tra loro isomorfi (si veda [14]). Ognuno di essi è detto *gruppo di Schützenberger* di D.

Il seguente risultato è noto come Lemma di Clifford e Miller (si veda [4, Proposizione 1.12.6]).

Lemma 4.2.8 (Clifford e Miller)**.** *Siano M un monoide ed $m, n \in M$. Allora $mn \in R(m) \cap L(n) \iff R(n) \cap L(m)$ contiene un idempotente.*

Studiamo adesso un'importante famiglia di $\mathcal{D}$-classi.

Proposizione 4.2.9. *Siano M un monoide e D una sua $\mathcal{D}$-classe. Allora le seguenti condizioni sono equivalenti:*

(*i*) *D contiene un idempotente;*

(*ii*) *ogni $\mathcal{R}$-classe di D contiene un idempotente;*

(*iii*) *ogni $\mathcal{L}$-classe di D contiene un idempotente.*

Dimostrazione. Le implicazioni $(ii) \Rightarrow (i)$ e $(iii) \Rightarrow (i)$ sono banali. Dimostriamo soltanto l'implicazione $(i) \Rightarrow (ii)$. L'implicazione $(i) \Rightarrow (iii)$ sarà analoga.

Siano $e \in D$ un idempotente ed R una $\mathcal{R}$-classe di D. La $\mathcal{H}$-classe $H = L(e) \cap R$ è non vuota poiché, per la Proposizione 4.2.4, $\mathrm{Card}\,(H) = \mathrm{Card}\,(R(e) \cap H(e)) \geq 1$. Preso un elemento $n \in H$, si ha, essendo $H \subseteq L(e)$, $n\mathcal{L}e$ e dunque

$$n = ve \quad \text{e} \quad e = v'n$$

per opportuni $v, v' \in M$.

Sia $m = ev'$. Allora $mn = e$, infatti

$$mn = (ev')n = e(v'n) = e^2 = e.$$

Quindi, essendo $e = mn$ e $m = ev'$ si ha $m\mathcal{R}e$. Da ciò ricaviamo che $e = mn \in R(m) \cap L(n)$ e dunque, per il Lemma di Clifford e Miller, che $R(n) \cap L(m)$ contiene un idempotente. Dall'inclusione $R(n) \cap L(m) \subseteq R(n) = R$ otteniamo la tesi. □

Una $\mathcal{D}$-classe soddisfacente una delle condizioni equivalenti della Proposizione 4.2.9 è detta *regolare*.

Consideriamo adesso il caso in cui M sia un monoide di trasformazioni su un insieme finito Q. In tal caso le rappresentazioni canoniche dei gruppi $H(e)$ sono dei gruppi di permutazioni equivalenti (si veda [4, Proposizione 9.1.9]). Anche i gruppi di Schützenberger potranno esser visti come gruppi di permutazioni.

Ricordiamo che data una funzione parziale $m \in M$, l'equivalenza nucleare $\sim_m$ è l'equivalenza parziale definita per $p, q \in Q$ da $p \sim_m q \iff pm = qm$ (si veda Esempio 1.1.26).

Se $m\mathcal{L}n$ allora m ed n hanno la stessa immagine. Se $m\mathcal{R}n$ allora m ed n hanno la stessa equivalenza nucleare. Se $m\mathcal{H}n$ allora m ed n hanno la stessa immagine la stessa equivalenza nucleare. Il viceversa in generale non è vero ma vale nel seguente caso notevole.

Proposizione 4.2.10. *Siano Q un insieme finito, M un monoide di trasformazioni su Q ed $e, m \in M$ con e idempotente. Allora $H(e) = H(m) \iff e$ ed m hanno la stessa immagine e la stessa equivalenza nucleare.*

Dimostrazione.

($\Leftarrow$) Se e ed m sono $\mathcal{H}$-equivalenti allora essi hanno la stessa immagine I e la stessa equivalenza nucleare $\sim_\rho$.

($\Rightarrow$) Siano $Qe = Qm = I$ e $\sim_\rho$ l'equivalenza nucleare di e ed m. Mostriamo che m ed e sono $\mathcal{H}$-equivalenti. Essendo e l'identità su I si avrà $me =$

m. Per ogni $p \in Q$ si ha $pe^2 = pe$ e dunque $p \sim_\rho pe$. Ciò implica $pem = em \ \forall\, p \in Q$ e dunque, essendo l'azione fedele, $em = m$. La restrizione $m|_I$ è una permutazione, poiché se $p, q \in I$ sono tali che $pm = qm$ allora $p = pe = qe = q$. Esisterà dunque un intero $k > 0$ tale che $m^k|_i$ sarà l'identità su I. Si ha l'uguaglianza $m^k = e$. Infatti per ogni $p \in Q$ si ha

$$pe = (pe)m^k = p(em)m^{k-1} = pm^k.$$

Riassumendo si ha $m = me$, $e = m^{k-1}m$, $m = em$ ed $e = mm^{k-1}$, da cui la tesi.

□

4.3 Gruppo di un codice bifisso

Siano, di seguito, F un insieme ricorrente, $X \subseteq F$ un codice bifisso di F-grado d ed $\mathcal{A} = (Q, 1, 1)$ un automa semplice tale da riconoscere X^*.

Come già visto nella Sottosezione 2.4.5, data una parola $w \in A^*$, l'immagine ed il rango di w sono rispettivamente

$$\Im(w) = \{p \cdot w \,|\, p \in Q\} \quad \text{e} \quad \operatorname{rank}(w) = \operatorname{Card}(\Im(w)).$$

Proposizione 4.3.1. *L'insieme di elementi di $\varphi_{\mathcal{A}}(F)$ di rango d è contenuto in una $\mathcal{D}$-classe regolare del monoide di transizione $\varphi_{\mathcal{A}}(A^*)$ di $\mathcal{A}$.*

Dimostrazione. Siano $u, v \in F$ due parole di rango d. Essendo F ricorrente, esisterà una parola $w \in F$ tale che $uwv \in F$. Poniamo $m = \varphi_{\mathcal{A}}(u)$, $n = \varphi_{\mathcal{A}}(v)$, $p = \varphi_{\mathcal{A}}(wv)$ e $q = mp = \varphi_{\mathcal{A}}(uwv)$. Di seguito mostreremo che $D(m) = D(n)$ e che tale $\mathcal{D}$-classe è regolare.

- Per prima cosa dimostriamo che $m\mathcal{R}q$. Essendo F ricorrente esisterà un $t \in F$ tale che $uwvtu \in F$. Sia $z = wvtu$. Per la Proposizione 2.4.37, $\operatorname{rank}(uz) = d$ e poiché $\Im(uz) \subseteq \Im(z) \subseteq \Im(u)$ si avrà $\Im(uz) = \Im(z) = \Im(u)$, e quindi, in particolare, che $\varphi_{\mathcal{A}}(z)|_{\Im(u)}$ è una permutazione. Dunque, essendo $\Im(u)$ finito, esisterà un intero $k > 0$ tale che $e = \varphi_{\mathcal{A}}(z)^k$ è l'identità su $\Im(u)$. Allora $m\mathcal{R}q$, infatti

  $$m = me = \varphi_{\mathcal{A}}(u)\varphi_{\mathcal{A}}(z^k) = \varphi_{\mathcal{A}}(uwv)\varphi_{\mathcal{A}}(tuz^{k-1}) = q\varphi_{\mathcal{A}}(tuz^{k-1})$$

  e

  $$q = \varphi_{\mathcal{A}}(uwv) = \varphi_{\mathcal{A}}(u)\varphi_{\mathcal{A}}(wv) = mp.$$

- Analogamente mostriamo che $q\mathcal{L}n$. Sia $z' = tuwv$. e poiché $\Im(vz') \subseteq \Im(z') \subseteq \Im(v)$ si avrà $\Im(vz') = \Im(z') = \Im(v)$ e quindi, in particolare, che $\varphi_{\mathcal{A}}(z')|_{\Im(v)}$ è una permutazione. Dunque, essendo $\Im(u)$ finito,

esisterà un intero $k' > 0$ tale che $e' = \varphi_{\mathcal{A}}(z')^{k'}$ è l'identità su $\Im(v)$. Allora $q\mathcal{L}n$, infatti

$$n = ne' = \varphi_{\mathcal{A}}(v)\varphi_{\mathcal{A}}(z'^{k'}) = \varphi_{\mathcal{A}}(vz'^{k'-1}t)\varphi_{\mathcal{A}}(uwv) = \varphi_{\mathcal{A}}(vz'^{k'-1}t)q$$

e

$$q = \varphi_{\mathcal{A}}(uwv) = \varphi_{\mathcal{A}}(uw)\varphi_{\mathcal{A}}(v) = \varphi_{\mathcal{A}}(uw)n.$$

- Si ha inoltre $n\mathcal{L}p$, infatti

$$n = ne' = \varphi_{\mathcal{A}}(v)\varphi_{\mathcal{A}}(z'^{k'}) = \varphi_{\mathcal{A}}(vz'^{k'-1}tu)\varphi_{\mathcal{A}}(wv) = \varphi_{\mathcal{A}}(vz'^{k'-1}tu)p$$

e

$$p = \varphi_{\mathcal{A}}(wv) = \varphi_{\mathcal{A}}(w)\varphi_{\mathcal{A}}(v) = \varphi_{\mathcal{A}}(w)n$$

Riassumendo si ha $m\mathcal{R}q\mathcal{L}n$, ovvero $D(m) = D(n)$ e $q = mp \in R(m) \cap L(n) = R(m) \cap L(p)$. Dal Lemma 4.2.8 di Clifford e Miller ricaviamo che $R(p) \cap L(m)$ contiene un idempotente. Ovvero la $\mathcal{D}$-classe di $\varphi_{\mathcal{A}}(u)$ e $\varphi_{\mathcal{A}}(v)$ è regolare. □

Il gruppo di Schützenberger della $\mathcal{D}$-classe di $\varphi_{\mathcal{A}}(A^*)$ contenente gli elementi di $\varphi_{\mathcal{A}}(F)$ di rango d è un gruppo di permutazioni di rango d. Tale gruppo non dipende dalla scelta dell'automa semplice $\mathcal{A}$ tale da riconoscere X^* (si veda [4, Proposizione 9.5.1]). Esso è detto *F-gruppo* del codice X e lo si denota con $G_F(X)$.

Osservazione 4.3.2. Un F-gruppo di un codice $X \subseteq F$ è un gruppo sintattico di X.

Seguendo la notazione di [4] denoteremo il *gruppo del codice* X, per ogni codice X, il gruppo $G(X) = G_{A^*}(X)$. Si dimostra che, ponendo K la $\mathcal{D}$-classe degli elementi di rango d, i gruppi G_e sono, per ogni idempotente $e \in K$, gruppi di permutazioni equivalenti tra loro. Ognuno di essi sarà detto *gruppo di Suschkevitch* di $\varphi_{\mathcal{A}}(A^*)$.

4.4 Grado di un gruppo sintattico

Ricordiamo dalle Sottosezioni 1.1.1 e 1.1.5 che, dato un gruppo di permutazioni G su un insieme Q, l'ordine di G sarà la sua cardinalità, il grado di G la cardinalità dell'insieme Q e diremo che G è transitivo se per ogni $p, q \in Q$ esiste un elemento $g \in G$ tale che $pg = q$ e che G è regolare se l'identità è l'unico elemento del gruppo avente un punto fisso.

Il rango minimo di un gruppo G è, per quanto visto nella Sottosezione 1.1.6, la minima cardinalità di un insieme di generatori di G.

Dominique Perrin ha formulato nel 1981 la seguente Congettura (si veda [11]).

Congettura 2 (Congettura del rango)**.** *Siano X un codice bifisso finito e G un gruppo di permutazione transitivo di grado d e rango minimo k. Se G è un gruppo sintattico di X, allora $Card(X) \geq (k-1)d+1$.*

La disuguaglianza nella Congettura 2 è legata alla Formula di Schreier. Infatti se X è una base di un sottogruppo di indice d del gruppo libero A° con $\mathrm{Card}\,(A) = k$, allora, per la Formula 1.3 si ha $\mathrm{Card}\,(X) = (k-1)d+1$.

Lo stesso Perrin ha dimostrato nel 2003 con Giuseppina Rindone che la congettura vale nel caso $k = 2$. Per dimostrare tale risultato introduciamo il concetto di gruppo speciale (si veda [12]).

Dato un codice prefisso X su un alfabeto binario, un gruppo sintattico G di X sarà detto *speciale* se il sottomonoide $\varphi_{\mathcal{A}}^{-1}(G)$ è ciclico ovvero, per quanto visto nella Sottosezione 1.1.6, generato da un solo elemento. Un gruppo sintattico speciale è ciclico mentre non vale, in generale, il vicevera.

Teorema 4.4.1. *Siano $X \subseteq A^*$ un codice prefisso e G un gruppo sintattico di X non speciale di grado d. Allora $Card(X) \geq d+1$.*

Dimostrazione. Consideriamo l'insieme dei d-sottoinsiemi di Q

$$\mathcal{I} = \{I \subseteq Q \mid \mathrm{Card}\,(I) = d\}$$

e sia $I \in \mathcal{I}$ l'insieme fissato da G. Poiché $\varphi_{\mathcal{A}}^{-1}(G)$ non è ciclico, esisteranno due parole $u, v \in A^*$ tali da non essere potenze di una stessa parola e per cui si abbia $I \cdot u = I \cdot v = I$. Prendendo, se necessario, potenze appropriate di u e di v possiamo supporre che $\{u, v\}$ sia un codice prefisso. Sia $r \in A^*$ il prefisso comune più lungo di u e v. Si avrà dunque $u = ras, v = rbt$ per opportuni $a, b \in A$, $s, t \in A^*$ con $a \neq b$.

Consideriamo il d-sottoinsieme $J = I \cdot r$ (si veda Figura 4.7). Esso è tale che $J \cdot a, J \cdot b = I \in \mathcal{I}$. Dunque $\mathcal{I}$ è formato da insiemi di d stati p dell'automa sintattico tali da avere almeno due transizioni uscenti, $p \cdot a \neq p \cdot b$.

Quindi, l'insieme dei prefissi di X è rappresentabile da un albero avente almeno d nodi con almeno due figli. Ciò implica che esso avrà almeno $d+1$ foglie, ovvero $\mathrm{Card}\,(X) \geq d+1$. □

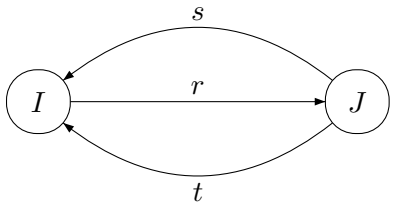


Figura 4.7: Azione sui d-sottoinsiemi di Q.

Osservazione 4.4.2. Una forma più debole del Teorema precedente, ossia $\mathrm{Card}\,(d) \geq d$, è stata provata per la prima volta da Schützenberger nel 1979 (si veda [16]) usando ipotesi più generali: prendendo un insieme X arbitrario non necessariamente codice prefisso.

Il grado di un gruppo sintattico speciale non è limitato in termini di cardinalità di X. Infatti per ogni $n \geq 1$ il codice $X = \{a^n\}$ ha come gruppo sintattico $\mathbb{Z}/n\mathbb{Z}$.

Nello stesso articolo in cui proponeva la congettura ([11]), Perrin ha dimostrato che ogni gruppo di permutazioni transitivo è un gruppo sintattico di un codice bifisso.

Di seguito mostreremo un risultato più forte: ogni gruppo di permutazioni transitivo di grado d e generato da k elementi è un gruppo sintattico di un particolare codice bifisso avente $(k-1)d+1$ elementi. Ciò implicherà che la disuguaglianza nella Congettura 2 non può essere migliorata.

Per far ciò abbiamo bisogno del seguente risultato preliminare.

Lemma 4.4.3. *Siano $Z \subseteq A^*$ un codice di gruppo di grado d ed F un insieme Sturmiano. Allora l'insieme $X = Z \cap F$ è un codice F-massimale bifisso di F-grado d e $G_F(X) = G(Z)$.*

Dimostrazione. Il fatto che X sia un codice F-massimale bifisso di F-grado segue direttamente dal Corollario 3.4.7.

Siano $\mathcal{A} = (Q, 1, 1)$ l'automa minimale di X^* ed $\Im(w)$ l'immagine di $\varphi_{\mathcal{A}}(w)$ l'immagine di w rispetto ad $\mathcal{A}$.

Siano $u \in F$ una parola tale che $\delta_X(u) = d$ ed $I = \Im(u)$. Per il Lemma 2.4.36 si ha $\mathrm{rank}(u) = d$ e dunque $\mathrm{Card}\,(I) = d$. Consideriamo l'insieme $Y = R_F(u)$ delle parole di primo ritorno di u. Esso è, per il Corollario 3.3.3, una base del gruppo libero A°.

Per ogni $y \in Y \subseteq \{z \in F \mid uz \in A^+u \cap F\}$, la restrizione $\varphi_{\mathcal{A}}(y)|_I$, che indicheremo con $\chi(y)$ è una permutazione di I. Infatti da $uy \in A^+u$ otteniamo $\Im(uy) \subseteq \Im(u) = I$ e da $uy \in F$ otteniamo, per la Proposizione 2.4.37, $\mathrm{Card}\,(\Im(uy)) = d$. Dunque $\Im(uy) = \Im(u) = I$.

Per ogni permutazione $\chi(y)$ esiste un intero $k > 0$ tale che $\chi(y)^k$ è l'identità su I. Sarà dunque possibile trovare un elemento $e \in \varphi_{\mathcal{A}}(Y^+)$ idempotente, tale che $\chi(e) = (1)|_I$.

Da ciò e dalla definizione di Y ricaviamo che ogni elemento sufficientemente lungo di $\varphi_{\mathcal{A}}^{-1}(e) \cap Y^*$ avrà u come suffisso. In particolare l'immagine di e è contenuta in I, ovvero $\varphi_{\mathcal{A}}(A^*)e \subseteq I$.

Per quanto appena visto si ha

$$\varphi_{\mathcal{A}}(u)e = \varphi_{\mathcal{A}}(u) \quad \text{e} \quad e \in \varphi_{\mathcal{A}}(A^*u),$$

ovvero $e\mathcal{L}\varphi_{\mathcal{A}}(u)$, e dunque $e\mathcal{D}\varphi_{\mathcal{A}}(u)$. Quindi e appartiene alla $\mathcal{D}$-classe di $\varphi_{\mathcal{A}}(A^*)$ contenente gli elementi di rango d in $\varphi_{\mathcal{A}}(F)$.

Sia $G' = H(e) = G(e)$ il gruppo massimale in $\varphi_{\mathcal{A}}(A^*)$ contenente e. Esso è per definizione, a meno di equivalenze, $G_F(X)$.

Estendendo la notazione possiamo indicare con $\chi(y)$ la restrizione di $\varphi_{\mathcal{A}}(y)$ all'insieme I per ogni $y \in Y^*$.

Per ogni $y \in Y^*$, $e\varphi_{\mathcal{A}}(y)e$ ed e hanno la stessa immagine e la stessa equivalenza nucleare, dunque, per la Proposizione 4.2.10, $H(e\varphi_{\mathcal{A}}e) = H(e)$, da cui, in particolare, $e\varphi_{\mathcal{A}}e \in G'$.

Dall'uguaglianza $\varphi_{\mathcal{A}}(y)|_I = (e\varphi_{\mathcal{A}}(y)e)|_I$ ricaviamo che $\chi : Y^* \to G'$ è un morfismo. Tale morfismo è surgettivo. Infatti, essendo Y una base del gruppo A° per il Corollario 3.3.3, per ogni $\varphi_{\mathcal{A}}(w)|_I \in G'$, possiamo scrivere $w = y_1^{\varepsilon_1} y_2^{\varepsilon_2} \cdots y_n^{\varepsilon_n}$ per opportuni $n \geq 0$, $y_i \in Y$ ed $\varepsilon_i \in \{-1, +1\}$. Essendo G' un gruppo finito, per ogni $y \in Y$ si avrà $\chi(y)^{-1} \in \chi(Y^*)$. Dunque $\chi(w) = \chi(y_1)^{\varepsilon_1}\chi(y_2)^{\varepsilon_2} \cdots \chi(y_n)^{\varepsilon_n} \in \chi(Y^*)$, per ogni $\varphi_{\mathcal{A}}(w) \in G'$, ovvero $G' = \chi(Y^*)$.

Siano $\mathcal{B} = (R, 1, 1)$ l'automa minimale di Z^* e $G = \varphi_{\mathcal{B}}(A^*)$. Allora G è un gruppo di permutazioni equivalente a $G(Z)$.

Per dimostrare la tesi sarà dunque sufficiente mostrare che G e G' sono gruppi di permutazioni equivalenti.

Per far ciò definiamo la funzione $\beta : I \to R$ come segue. Siano $P = XA^-$ l'insieme dei prefissi propri di X ed S l'insieme degli elementi di P che sono suffissi di u. Per il Lemma 2.4.36, per ogni $i \in I$ esisterà un unico $q \in S$ tale che $i = 1 \cdot q$. Poniamo $\beta(i) = 1\varphi_{\mathcal{B}}(q)$. Mostriamo che tale funzione è biettiva.

- Siano $q, t \in S$ tali che $1\varphi_{\mathcal{B}}(q) = 1\varphi_{\mathcal{B}}(t)$ e supponiamo $|q| \leq |t|$. Essendo q, t comparabili per suffissi avremo $t = vq$ per un opportuno $v \in F$. Da $1\varphi_{\mathcal{B}}(t) = 1\varphi_{\mathcal{B}}(v)\varphi_{\mathcal{B}}(q) = 1\varphi_{\mathcal{B}}(q)$ e dal fatto che $\varphi_{\mathcal{B}}(q)$ è una permutazione ricaviamo $1\varphi_{\mathcal{B}}(v) = 1$, ovvero $v \in Z^*$. Riassumendo $v \in Z^* \cap F \subseteq X^*$ e dunque $v = 1$ e $q = t$. Dunque β è iniettiva.

- Poiché $\mathrm{Card}\,(R) = \mathrm{Card}\,(I) = d$, la funzione è anche suriettiva, dunque biettiva.

Verifichiamo adesso che per ogni $i, j \in I$ e per ogni $y \in Y^*$ vale la doppia implicazione

$$i\varphi_{\mathcal{A}}(y) = j \quad \Longleftrightarrow \quad \beta(i)\varphi_{\mathcal{B}}(y) = \beta(j) \tag{4.1}$$

- Proviamo per prima cosa la validità di 4.1 per $y \in Y$. Dal Lemma 2.4.36 sappiamo che $i = 1 \cdot q$ e $j = 1 \cdot t$ per oppportuni $q, t \in S$. Allora

$$i\varphi_{\mathcal{A}}(y) = j \quad \Longleftrightarrow \quad 1\varphi_{\mathcal{A}}(qy) = 1\varphi_{\mathcal{A}}(t) \quad \Longleftrightarrow \quad qy \in X^*t.$$

  Inoltre qy, in quanto suffisso di uy con $y \in R_F(u)$ è un elemento di F. Dunque

$$qy \in X^*t \quad \Longleftrightarrow \quad qy \in Z^*t$$

  e analogamente a quanto visto sopra

$$qy \in Z^*t \quad \Longleftrightarrow \quad \beta(i)\varphi_{\mathcal{B}}(y) = \beta(j).$$

Mettendo insieme le doppie implicazioni precedenti otteniamo proprio la Formula 4.1.

- Mostriamo adesso che se $y, z \in Y^*$ verificano 4.1 per ogni $i, j \in I$, allora anche yz verifica la doppia implicazione.

  ($\Rightarrow$) Supponiamo che dati $i, j \in I$ si abbia $i\varphi_{\mathcal{A}}(yz) = j$. Essendo $\varphi_{\mathcal{A}}(y)|_I, \varphi_{\mathcal{A}}(z)|_I$ permutazioni esisterà un unico $k \in I$ tale che $i\varphi_{\mathcal{A}}(y) = k$ e $k\varphi_{\mathcal{A}}(z) = j$. Poiché y e z verificano la Formula 4.1, avremo $\beta(i)\varphi_{\mathcal{B}}(y) = \beta(k)$ e $\beta(k)\varphi_{\mathcal{B}}(z) = \beta(j)$, da cui $\beta(i)\varphi_{\mathcal{B}}(yz) = \beta(j)$.

  ($\Leftarrow$) Viceversa, supponiamo che $\beta(i)\varphi_{\mathcal{B}}(yz) = \beta(j)$. Essendo β una biezione tra I ed R, esisterà un unico $k \in I$ tale che $\beta(k) = \beta(i)\varphi_{\mathcal{B}}(y)$. Tale k sarà dunque tale che $\beta(k)\varphi_{\mathcal{B}}(z) = \beta(j)$. Per la Formula 4.1 si avrà, quindi, $i\varphi_{\mathcal{A}}(y) = k$ e $k\varphi_{\mathcal{A}}(z) = j$, da cui $i\varphi_{\mathcal{A}}(yz) = j$.

Dalla Formula 4.1 ricaviamo che è possibile definire un morfismo $\alpha : G' \to G$ tale che $\alpha : g \mapsto \varphi_{\mathcal{B}}(y)$ dove $y \in Y^*$ è tale che $g = \chi(y) = \varphi_{\mathcal{A}}(y)|_I$. Mostriamo che tale morfismo è biettivo.

- Il morfismo α è iniettivo. Infatti se $\alpha(g) = \alpha(g')$, siano $y, y' \in Y^*$ tali che $g = \chi(y)$ e $g' = \chi(y')$. Allora si avrà $\varphi_{\mathcal{B}}(y) = \varphi_{\mathcal{B}}(y')$ e per la 4.1 ciò implicherà $\chi(y) = \chi(y')$, ovvero $g = g'$.

- Il morfismo α è suriettivo. Infatti, essendo Y una base del gruppo libero A° per il Corollario 3.3.3, per ogni $a \in A$, possiamo scrivere $a = y_1^{\varepsilon_1} y_2^{\varepsilon_2} \cdots y_n^{\varepsilon_n}$, per opportuni $n \geq 0$, $y_i \in Y$ ed $\varepsilon_i \in \{-1, +1\}$. Dunque $\varphi_{\mathcal{B}}(a) = \varphi_{\mathcal{B}}(y_1)^{\varepsilon_1}\varphi_{\mathcal{B}}(y_2)^{\varepsilon_2} \cdots \varphi_{\mathcal{B}}(y_n)^{\varepsilon_n} = \alpha(g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n})$ con $g_i = \chi(y_i)$. Essendo, banalmente, ogni elemento di G prodotto di lettere in A, segue che α è suriettivo.

Infine si vede facilmente dal diagramma in Figura 4.8, che la biezione β e l'isomorfismo α verificano l'equazione 1.2. □

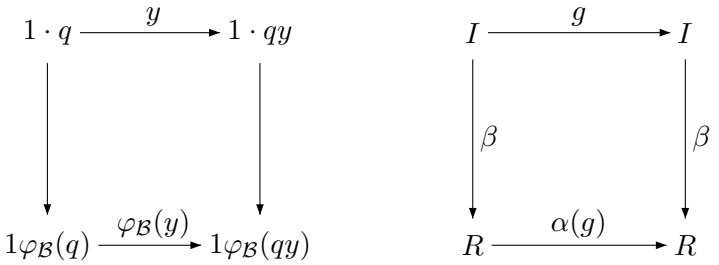


Figura 4.8: La biezione $\beta : I \to R$ e l'isomorfismo $\alpha : G' \to G$ del Lemma 4.4.3.

Illustriamo la dimostrazione del Lemma 4.4.3 tramite il seguente Esempio.

Esempio 4.4.4. Siano F l'insieme di Fibonacci e Z il codice di gruppo dato da $Z = \varphi^{-1}(0,0)$ con $\varphi : \{a,b\}^* \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ la funzione definita da $\varphi(a) = (1,0)$ e $\varphi(b) = (0,1)$. L'automa di gruppo che riconosce Z è rappresentato in Figura 4.9.

Intersecando Z con l'insieme di Fibonacci otteniamo il codice F-massimale $X = Z \cap F = \{a^2, aba^2ba, abab, ba^2b, baba\}$. L'automa minimale di X^* è rappresentato in Figura 4.10.

Sia $u = aba \in F$. Essa ha rango 4 e la sua immagine è $I = \Im(u) = \{1,2,4,8\}$. L'insieme delle parole di primo ritorno di u è $Y = \{aba, ba\}$ e le permutazioni ottenute per restrizione ad I sono $\chi(aba) = (14)(28)$ e $\chi(ba) = (18)(24)$.

La biezione β è definita da $\beta(1) = (0,0)$, $\beta(2) = (0,1)$, $\beta(3) = (1,0)$ e $\beta(4) = (1,1)$.

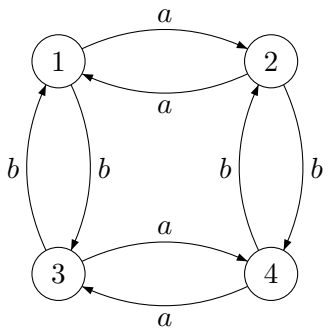


Figura 4.9: Un automa di gruppo.

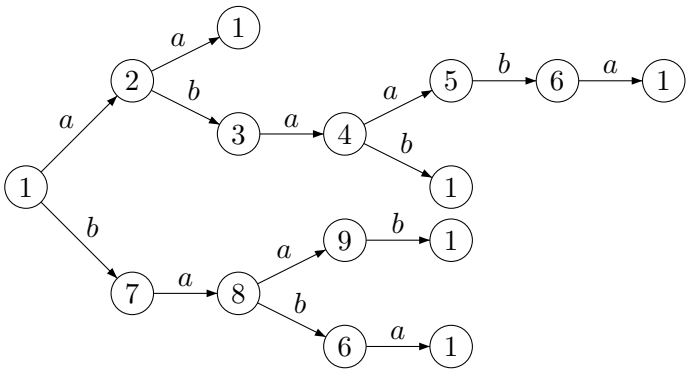


Figura 4.10: Automa minimale del codice F-massimale di F-grado 4 ottenuto dell'Esempio 4.4.4

Siamo adesso pronti ad enunciare il seguente risultato.

Teorema 4.4.5. *Ogni gruppo di permutazioni transitivo di grado d generato da k elementi è un gruppo sintattico di un codice bifisso avente $(k-1)d+1$ elementi.*

Dimostrazione. Sia G un gruppo di permutazioni transitivo di grado d e sia Z un codice di gruppo su un alfabeto di A di k lettere tale che $G(Z) = G$.

Siano $F \subseteq A^*$ un insieme Sturmiano ed $X = Z \cap F$. Per il Teorema della Cardinalità 3.1.3, tale insieme avrà cardinalità $\mathrm{Card}\,(X) = (k-1)d + 1$. Applicando il Lemma 4.4.3 otterremo proprio $G = G_F(X)$, ovvero la tesi. □

4.5 Codici con nucleo vuoto

In questa Sezione ci concentreremo sui gruppi sintattici di codici con nucleo vuoto. Vi sono due casi notevoli di codici prefissi con nucleo vuoto: i codici semaforo ed i codici infissi.

Un *codice semaforo* è un insieme della forma $X = A^*S \setminus A^*SA^+$ per un qualche insieme non vuoto $S \subseteq A^*$, detto *insieme dei semafori* per X.

La terminologia è giustificata dal fatto che una parola è in X se e solo se essa termina con un semaforo, ma nessuno dei suoi prefissi propri termina con un semaforo. Dunque, leggendo una parola da sinistra verso destra, l'apparire di un semaforo indicherà che è stata letta una parola del codice.

Esempio 4.5.1. Siano $A = \{a, b\}$ ed $S = a$. Allora l'insieme $X = A^*a \setminus A^*aA^+ = b^*a$ è un codice semaforo.

Un codice semaforo è un codice massimale prefisso (si veda [4, Proposizione 3.5.1]), dunque completo a destra. Viceversa si può dimostrare che un insieme $X \subseteq A^*$ è un codice semaforo se e solo se verifica una delle seguenti condizioni (si veda [4, Proposizione 3.5.4 e Proposizione 3.5.6]):

(*i*) X è prefisso e $A^*X \subseteq XA^*$;

(*ii*) X è completo a destra e $X \cap A^*XA^+ = \emptyset$.

Dalla condizione (*ii*) ricaviamo, in particolare, che i codici semaforo hanno nucleo vuoto. Infatti

$$K(X) = X \cap H(X) = X \cap A^+XA^+ \subseteq X \cap A^*XA^+ = \emptyset.$$

Chiameremo *codice infisso* un insieme $X \subseteq A^*$ tale che nessuna parola di X è fattore di un'altra parola di X. Un codice infisso è dunque, per costruzione, un codice bifisso e con nucleo vuoto.

Esempio 4.5.2. L'insieme $X = \{aaa, aab, abaa, abab, baba, babb, bba, bbb\}$ rappresentato in Figura 4.11 è un codice infisso.

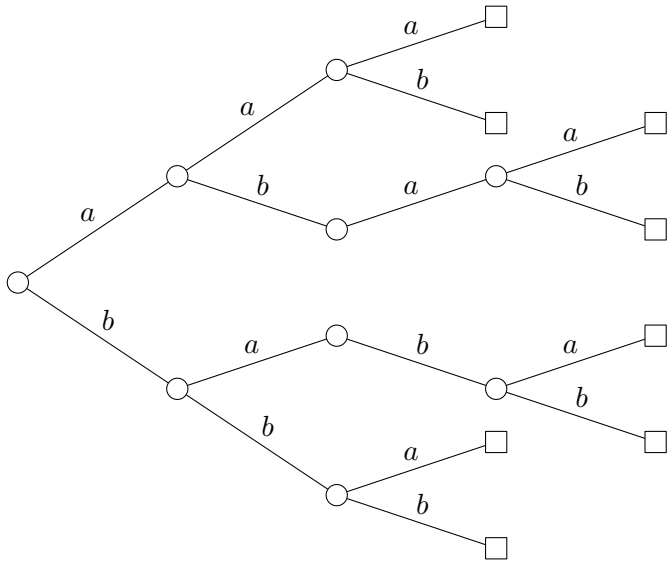


Figura 4.11: Il codice infisso $X = \{aaa, aab, abaa, abab, baba, babb, bba, bbb\}$.

Riprendiamo adesso la nozione di interpretazione vista nella Sottosezione 1.2.8.

Lemma 4.5.3. *Sia $X \subseteq A^+$ un codice con nucleo vuoto. Ogni insieme di interpretazioni indipendenti di una parola w rispetto ad X è ciclico.*

Dimostrazione. Dimostriamo il Lemma per induzione su $|w|$.

Il caso $|w| = 0$ è ovvio poiché la parola vuota ha al più un'interpretazione, ovvero $(1, 1)$, che verifica banalmente la proprietà.

Sia $w \neq 1$ e supponiamo che la proprietà sia verificata per tutte le parole di lunghezza al più $|w| - 1$. Sia $J = \{\alpha_0, \alpha_1, \dots \alpha_{n-1}\}$ l'insieme delle interpretazioni indipendenti di w ordinato in modo tale che s_{α_i} è un prefisso proprio di $s_{\alpha_{i+1}}$ per ogni $0 \leq i \leq n-2$. Consideriamo i tre possibili casi.

- Sia $s_{\alpha_0} \neq 1$. Sia a la prima lettera di w. Applicando la Proposizione 1.2.24 otteniamo che $J' = \{a^{-1}\alpha \,|\, \alpha \in J\}$ è un insieme di n interpretazioni indipendenti di $a^{-1}w$. Per l'ipotesi induttiva J' sarà ciclico ed il suo supremum $\mu = (u_1, u_2, \dots, u_m)$ sarà n-periodico. La sequenza $\nu = (au_1, u_2, \dots, u_m)$ è il supremum di J e poiché ν è n-periodico, J sarà ciclico.

- Siano $s_{\alpha_0} = 1$ e f_{α_0} non vuoto. Allora, analogamente al caso precedente, $J' = \{a^{-1}\alpha \,|\, \alpha \in J\}$ è un insieme ciclico di n interpretazioni indipendenti di $a^{-1}w$ con supremum $\mu = (u_1, u_2, \dots, u_m)$. La sequenza $\nu = (1, au_1, \dots, u_m)$ è il supremum di J. Verifichiamo che ν è n-periodico.

Essendo μ n-periodico si ha, per $1 \leq \ell \leq r \leq m-1$, la doppia implicazione $u_{\ell+1}u_{\ell+2}\cdots u_r \in X \Leftrightarrow r - l = n$. Rimane dunque da verificare solo il caso estremale, ossia che $au_1u_2\cdots u_r \in X \Leftrightarrow r = n$. È qui che useremo l'ipotesi del nucleo vuoto.

- ◇ Proviamo che se $au_1u_2\cdots u_r \in X$ allora $r \geq n$. Essendo X un codice con nucleo vuoto, nessuna parola $x \in X$ potrà essere un prefisso proprio, di $s_{\alpha_i} \in A^-X$ per $1 \leq i \leq n-1$. Dunque per $r \leq n-2$ si ha, tenendo conto dell'Equazione 1.4, $au_1u_2\cdots u_r = s_{\alpha_r} \notin X$. Anche il caso estremale è da escludere. Se infatti si avesse $au_1u_2\cdots u_{n-1} = s_{\alpha_{n-1}} \in X$, allora α_0 ed α_{n-1} sarebbero connesse in quanto entrambe adiacenti a $\gamma = (1, s_{\alpha_{n-1}}f_{\alpha_{n-1}}, p_{\alpha_{n-1}})$.
- ◇ Proviamo che se $au_1u_2\cdots u_r \in X$ allora $r \leq n$. Essendo J' ciclico si ha $u_2u_3\cdots u_{n-1} \in X$ e dunque $u_2u_3\cdots u_{n-1}$ è il primo termine di f_{α_1}. Inoltre, essendo μ una fattorizzazione, $u_i \neq 1$ per ogni $2 \leq i \leq m-1$. Il fatto che X abbia nucleo vuoto ci garantisce che se $au_1u_2\cdots u_r \in X$ sicuramente non si potrà avere $r > n+1$. Anche il caso $r = n+1$ è da escludere. Se infatti si avesse $au_1u_2\cdots u_{n+1} \in X$, allora α_0 ed α_{n-1} sarebbero connesse in quanto entrambe adiacenti a $\gamma = (1, s_{\alpha_1}f_{\alpha_1}, p_{\alpha_1})$. Il caso $r = n$ è, invece, possibile poiché $au_1u_2\cdots u_n$ è il primo termine di f_{α_0} e dunque è in X.

- ◦ Siano, infine, $s_{\alpha_0} = 1$ e f_{α_0} la sequenza vuota. Dunque $w = p_{\alpha_0}$. Inoltre le sequenze f_{α_j} sono vuote per ogni $1 \leq j \leq n-1$. Infatti, se così non fosse, i termini di f_{α_j}, al variare di j, sarebbero prefissi propri di $p_{\alpha_0}y$ per un'opportuna $y \in A^+$ tale che $p_{\alpha_0}y \in X$ e dunque in $K(X)$.

  Quindi le intepretazioni sono del tipo $\alpha_j = (s_{\alpha_j}, p_{\alpha_j})$, si ha $P_{\alpha_j} = \{s_{\alpha_j}\}$ per ogni $1 \leq j \leq n-1$ è il supremum di J è $(u_0, u_1, \ldots u_{n-1}, u_n)$ con $u_0u_1\cdots u_j = s_{\alpha_j}$ per $0 \leq j \leq n-1$ ed $u_n = p_{\alpha_{n-1}}$.

  Per provare che tale fattorizzazione è n-periodica mostriamo che $s_{\alpha_j} = u_0u_1\cdots u_{\alpha_j} \notin X$ per ogni $0 \leq j \leq n-1$.

  - ◇ Il caso $j = 0$ è banale poiché, per ipotesi, $s_{\alpha_0} = 1$.
  - ◇ Sia $1 \leq j \leq n-2$. Se, per assurdo, $s_{\alpha_j} \in X$ allora esso sarebbe un fattore proprio di $zs_{\alpha_{n-1}}$ per un'opportuna $z \in A^+$ tale che $zs_{\alpha_{n-1}} \in X$, contro l'ipotesi di $K(X) = \emptyset$.
  - ◇ Infine, se $s_{\alpha_{n-1}} = u_0u_1\cdots u_{n-1}$ fosse un elemento di X, allora α_0 ed α_{n-1} sarebbero entrambi adiacenti a $\gamma = (1, s_{\alpha_{n-1}}, p_{\alpha_{n-1}})$ e dunque connesse.

□

Sostituendo nel Lemma 4.5.3 l'ipotesi di indipendenza con la più debole ipotesi di disgiunzione tra le interpretazioni, la tesi non è più verificata, come mostrato nel seguente Esempio.

Esempio 4.5.4. Consideriamo il codice $X = \{aab, aabbb, baa, bba, bbb\}$ dell'Esempio 1.2.21. Esso ha nucleo $K(X) = \emptyset$. Come già visto, $J = \{(aa, bbb, a), (1, aab, bba, 1)\ \}$ è un insieme di interpretazioni disgiunte di $w = aabbba$. Il supremum di J è la fattorizzazione $(1, aa, b, bb, a, 1)$ che non è 2-periodica in quanto $aabbb \in X$ è un prodotto di tre termini di tale fattorizzazione.

Torniamo adesso allo studio dei gruppi sintattici.

Proposizione 4.5.5. *Siano $X \subseteq A^+$ un codice, $\mathcal{A}$ un automa semplice e non ambiguo che riconosce X^* e G un gruppo tale che $G \cap \varphi_{\mathcal{A}}(X^*) \neq \emptyset$. Allora $G \cap \varphi_{\mathcal{A}}(X^*)$ è un sottogruppo di G.*

Dimostrazione. È un risultato noto che il sottomonoide $\varphi_{\mathcal{A}}(X^*)$ è stabile. Siano $u \in G \cap \varphi_{\mathcal{A}}(X^*)$, 1_G l'elemento neutro di G e v l'inverso di u in G. Da $u1_G = 1_G u = u$ e da $uv = uv = 1_G$ ricaviamo rispettivamente che 1_G e v sono elementi di $\varphi_{\mathcal{A}}(X^*)$. Dunque $G \cap \varphi_{\mathcal{A}}(X^*) \leq G$. □

Siano X un codice ed $\mathcal{A}$ un automa semplice e non ambiguo tale da riconoscere X^*. Si può dimostrare che $\varphi_{\mathcal{A}}(A^* \setminus H(X))$ è un ideale. Da ciò si ricava che per ogni gruppo G contenuto in $\varphi_{\mathcal{A}}(A^*)$ si ha la doppia implicazione

$$G \subseteq \varphi_{\mathcal{A}}(A^* \setminus H(X)) \quad \Longleftrightarrow \quad G \cap \varphi_{\mathcal{A}}(A^* \setminus H(X)) \neq \emptyset.$$

Nel caso X sia un codice prefisso e G un gruppo sintattico di X, diremo che G è *proprio* se $G \subseteq \varphi_{\mathcal{A}}(A^* \setminus H(X))$ o equivalentemente, per quanto appena visto, se esiste una parola $w \in H(X)$ tale che $\varphi_{\mathcal{A}}(w) \in G$.

Osservazione 4.5.6. Un gruppo proprio non è, in generale, transitivo.

Di seguito ci sarà utile il seguente Lemma.

Lemma 4.5.7. *Siano $X \subseteq A^+$ un codice, $\mathcal{A} = (Q, 1, 1)$ un automa semplice e non ambiguo tale da riconoscere X^*, G un gruppo contenuto in $\varphi_{\mathcal{A}}(A^* \setminus H(X))$ ed I l'immagine comune degli elementi di G.*

Per ogni $g \in G$, $w \in \varphi_{\mathcal{A}}^{-1}(g) \setminus H(X)$ e $q \in I$ esiste un'unica interpretazione α_q di w tale che esistano dei cammini $q \xrightarrow{s_{\alpha_q}} 1$ e $1 \xrightarrow{p_{\alpha_q}} qg$ che siano semplici o nulli.

Inoltre l'insieme $J = \{\alpha_q \,|q \in I\}$ è formato da interpretazioni indipendenti.

Dimostrazione. Consideriamo un cammino $q \xrightarrow{w} qg$ con g, w, q come da ipotesi. Essendo $\mathcal{A}$ trim, esisteranno $f, h \in A^*$ tali che $1 \xrightarrow{f} f$ e $qg \xrightarrow{h} 1$.

Poiché $w \notin H(X)$, esisterà un'interpretazione α_q di w tale che $q \xrightarrow{s_{\alpha_q}} 1$ e $1 \xrightarrow{p_{\alpha_q}} qg$ sono o semplici o nulli. Tale interpretazione sarà unica.

Inoltre le interpretazioni α_q, al variare di $q \in I$, sono tra loro indipendenti. Supponiamo, infatti, vi siano due stati $p, q \in I$ tali che esistano $u, v \in A^*$ e $x \in X^*$ con $w = uxv$, $u \in P(\alpha_p)$ e $ux \in P(\alpha_q)$. Allora vi saranno due cammini $p \xrightarrow{u} 1 \xrightarrow{xv} pg$ e $q \xrightarrow{ux} 1 \xrightarrow{v} qg$ il che implica l'esistenza di un cammino $p \xrightarrow{u} 1 \xrightarrow{x} 1 \xrightarrow{v} qg$ (si veda Figura 4.12). Ovvero $pg = qg$. Essendo g una permutazione su I, ciò forza $p = q$. □

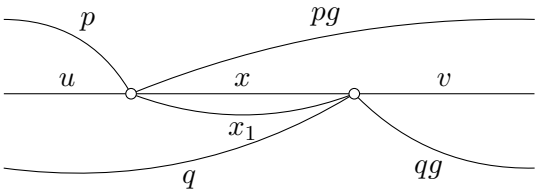


Figura 4.12: Le interpretazioni α_p ed α_q sono indipendenti.

Lemma 4.5.8. *Siano $X \subseteq A^+$ un codice con nucleo vuoto ed $\mathcal{A} = (Q, 1, 1)$ un automa semplice e non ambiguo che riconosce X^*. Ogni gruppo contenuto in $\varphi_{\mathcal{A}}(A^* \setminus H(X))$ è (a meno di isomorfismi) tale che la sua intersezione con $\varphi_{\mathcal{A}}(X^*)$ è non nulla.*

Dimostrazione. Sia $G \subseteq \varphi_{\mathcal{A}}(A^* \setminus H(X))$ un gruppo. Escludiamo il caso banale in cui G sia composto dalla sola relazione vuota, per cui non vi sarebbe nulla da provare. Consideriamo un elemento $w \in \varphi_{\mathcal{A}}^{-1}(1_G) \setminus H(X)$. Essendo 1_G diverso dalla relazione vuota, esso fisserà almeno un elemento $q \in Q$. Poiché $\mathcal{A}$ è trim, esisteranno delle parole $u, v \in A^*$ tali che $1 \xrightarrow{u} q$ e $q \xrightarrow{v} 1$, da cui ricaviamo $uwv \in X^*$. Non essendo w un fattore interno di X, esisteranno delle parole $t, z \in A^*$ tali che $w = tz$ con $ut, zv \in X^*$. Dunque si avranno i cammini $q \xrightarrow{t} 1$ e $1 \xrightarrow{z} q$, ovvero $zt \in X^*$.

Per la Proposizione 1.1.18, l'insieme $\varphi_{\mathcal{A}}(z)G\varphi_{\mathcal{A}}(t)$ è un gruppo isomorfo a G. Inoltre la sua intersezione con $\varphi_{\mathcal{A}}(X^*)$ è non vuota poiché $\varphi_{\mathcal{A}}(z)1_G\varphi_{\mathcal{A}}(t) = \varphi_{\mathcal{A}}(zt) \in \varphi_{\mathcal{A}}(z)G\varphi_{\mathcal{A}}(t) \cap \varphi_{\mathcal{A}}(X^*)$.

Dunque possiamo assumere che $G \cap \varphi_{\mathcal{A}}(X^*) \neq \emptyset$. □

Siamo adesso pronti a dare il seguente risultato.

Teorema 4.5.9. *Siano $X \subseteq A^+$ un codice con nucleo vuoto ed $\mathcal{A} = (Q, 1, 1)$ un automa semplice e non ambiguo che riconosce X^*. Ogni gruppo contenuto in $\varphi_{\mathcal{A}}(A^* \setminus H(X))$ è un gruppo ciclico finito e regolare.*

Dimostrazione. Sia $G \subseteq \varphi_{\mathcal{A}}(A^* \setminus H(X))$ un gruppo. Per il Lemma 4.5.8 possiamo supporre che $G \cap \varphi_{\mathcal{A}}(X^*) \neq \emptyset$.

Dalla Proposizione 4.5.5 ricaviamo che $G \cap \varphi_{\mathcal{A}}(X^*) \leq G$. Ciò implica, in particolare, che $1_G \in \varphi_{\mathcal{A}}(X^*)$ e dunque $1_G \in I$, con I l'immagine comune degli elementi di G.

Sia $w \in \varphi_{\mathcal{A}}(1_G) \setminus H(X)$. Per il Lemma 4.5.7, w ha un insieme $J = \{\alpha_q \,|q \in I\}$ di interpretazioni indipendenti tali che $q \xrightarrow{s_{\alpha_q}} 1$ e $1 \xrightarrow{p_{\alpha_q}} q$ siano cammini semplici o nulli.

Poniamo, per semplicità, $s_q = s_{\alpha_q}$, $f_q = f_{\alpha_q}$, $x_q = c(f_q)$ e $p_q = p_{\alpha_q}$ (si veda Figura 4.13).

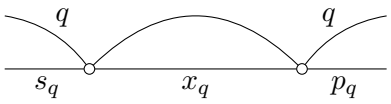


Figura 4.13: Le interpretazioni α_q con $q \in I$.

Essendo le interpretazioni a due a due disgiunte, la funzione $q \mapsto s_q$ è iniettiva. Dunque I è un insieme finito e così lo è G. Poniamo $I = \{1, 2, \ldots, n\}$ ed ordiniamo gli stati in modo che s_i sia un prefisso proprio di s_{i+1} per ogni $1 \leq i \leq n-1$. Per ogni $1 \leq i \leq n$ si avrà $w = s_i x_i p_i$, con $x_i = c(f_i)$.

Dimostriamo che tutti gli elementi di G sono potenze della permutazione $\sigma = (1\,2 \cdots n)$.

> Sia $\gamma = (v_1, v_2, \ldots, v_\ell)$ il supremum di J. Poiché $s_1 = p_1 = 1$ si ha $v_1 = v_\ell = 1$. Per ogni $1 \leq i \leq j \leq \ell - 1$ si ha
>
> $$s_i = v_1 v_2 \cdots v_i, \quad x_i = v_{i+1} v_{i+2} \cdots v_j, \quad p_i = v_{j+1} v_{j+2} \cdots v_\ell. \tag{4.2}$$
>
> Dal Lemma 4.5.3 ricaviamo che J è ciclico e dunque γ è n-periodico. Inoltre, per l'Equazione 1.5 e la Proposizione 1.2.25,
>
> $$j - 1 \equiv \ell - 2 \equiv 0 \,(\mathrm{mod}\, n). \tag{4.3}$$
>
> Consideriamo un elemento $g \in G$. Per ogni parola $z \in \varphi_{\mathcal{A}}^{-1}(g)$ si ha $\varphi_{\mathcal{A}}(wzw) = g$. Per il Lemma 4.5.7 la parola wzw ha un insieme $K = \{\beta_i \,|\, 1 \leq i \leq n\}$ di interpretazioni indipendenti tali che i cammini $i \xrightarrow{s_{\beta_i}} 1$ e $1 \xrightarrow{p_{\beta_i}} ig$ siano semplici o nulli. Possiamo dunque decomporre il cammino $i \xrightarrow{w} i \xrightarrow{z} ig \xrightarrow{w} ig$ come
>
> $$i \xrightarrow{s_1} 1 \xrightarrow{x_i} 1 \xrightarrow{p_i} i \xrightarrow{z} ig \xrightarrow{s_{ig}} 1 \xrightarrow{x_{ig}} 1 \xrightarrow{p_{ig}} ig.$$
>
> Dunque la sequenza $(s_i, x_i p_i z s_{ig} x_{ig}, p_{ig})$ è un'interpretazione di wzw.

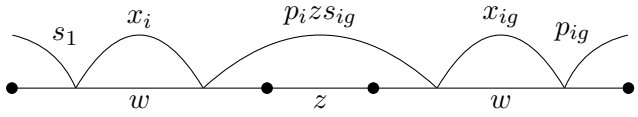


Figura 4.14: Un'interpretazione di wzw.

Dall'unicità di β_i e dal fatto che i cammini $i \xrightarrow{s_i} 1$ e $1 \xrightarrow{p_{ig}} ig$ siano semplici o nulli, otteniamo che $s_{\beta_i} = s_1$, $c(f_{\beta_i}) = x_i p_i z s_{ig} x_{ig}$ e $p_{\beta_i} = p_{ig}$ (si veda Figura 4.14).

In particolare si ha $p_i z s_{ig} \in X^*$ per ogni $i \in I$. Il supremum di K sarà della forma

$$\delta = (v_1, v_2, \ldots, v_{\ell-1}, u_1, u_2, \ldots, u_m, v_2, v_\ell)$$

per qualche $m > 0$ e qualche $u_i, u_2, \ldots, u_m \in A^+$ tali che $z = u_1 u_2 \cdots u_m$. Infatti i primi $\ell - 1$ termini di γ coincidono coi primi $\ell - 1$ termini di δ, mentre il termine di posto ℓ di γ è $1 \notin A^+$ e per questo non è presente in δ. Analogamente per gli ultimi $\ell - 1$ termini di γ che coincidono con gli ultimi $\ell - 1$ termini di δ mentre non appare $v_1 = 1$ a sinistra di v_2.

Per l'Equazione 4.2 si ha dunque, per ogni $1 \leq i \leq n$,

$$p_i z s_{ig} = v_{j+1} v_{j+2} \cdots v_{l-1} u_1 u_2 \cdots u_m v_2 v_3 \cdots v_{ig}.$$

Dunque, poiché $c(f_{\beta_i}) = x_i (p_i z s_{ig}) x_{ig}$, otteniamo

$$\mu(\beta_i, K) = \mu(\alpha_i, J) + \nu(\alpha_i, J) + m + \lambda(\alpha_{ig}, J) + \mu(\alpha_{ig}, J).$$

Essendo, per la Proposizione 1.2.25, $\mu(\alpha_i, J) \equiv \mu(\alpha_{ig}, J) \equiv 0 \,(\mathrm{mod}\, n)$, si ottiene

$$\mu(\beta_i, K) \equiv \ell - j - 1 + m + ig - 1 \,(\mathrm{mod}\, n).$$

Dalla n-periodicità di δ ricaviamo, inoltre, che $\ell - j - 1 + m + ig - 1 \equiv 0 \,(\mathrm{mod}\, n)$. Per quanto già visto nell'Equazione 4.3 si ha $\ell \equiv 2 \,(\mathrm{mod}\, 0)$ e $i \equiv j \,(\mathrm{mod}\, n)$, e quindi $-i + m + ig \equiv 0 \,(\mathrm{mod}\, n)$.

Dunque $ig \equiv i - m \,(\mathrm{mod}\, n)$. Poiché già vale per ogni $1 \leq i \leq n$, possiamo concludere che $g = \sigma^{-m}$.

Dunque G è incluso nel gruppo ciclico $\langle \sigma \rangle$. Poiché ogni sottogruppo di un gruppo ciclico e regolare è anch'esso ciclico e regolare, la tesi è verificata.

□

Dal Teorema precedente ricaviamo il seguente notevole risultato.

Corollario 4.5.10. *Siano $X \subseteq A^+$ un codice finito con nucleo vuoto ed $\mathcal{A}$ un automa semplice e non ambiguo tale da riconoscere X. Ogni gruppo in $\varphi_{\mathcal{A}}(A^*)$ è ciclico e regolare.*

Dimostrazione. Poiché X è finito, l'ideale $\varphi_{\mathcal{A}}(A^* \setminus H(X))$ contiene tutti i gruppi diversi da 1 e $\varphi_{\mathcal{A}}(A^*)$. La tesi segue dunque dal Teorema 4.5.9. □

Il Corollario 4.5.10 può essere riformulato, nel caso di codici prefissi, nel seguente Teorema.

Teorema 4.5.11. *Sia $X \subseteq A^+$ un codice prefisso con nucleo vuoto. Ogni gruppo sintattico proprio di X è un gruppo ciclico, finito e regolare.*

Esempio 4.5.12. L'insieme $X = \{aa, aba, bab, bb\}$ è un codice infisso. L'automa minimale $\mathcal{A}$ di X^* è rappresentato in Figura 4.15. Il monoide di transizione $\varphi_{\mathcal{A}}(A^*)$ contiene gruppi ciclici di ordine 1, 2 e 3. Ad esempio, $\varphi_{\mathcal{A}}(ab)$ contiene il ciclo $(1\,3\,4)$, mentre $\varphi_{\mathcal{A}}(a)$ contiene $(1\,2)$.

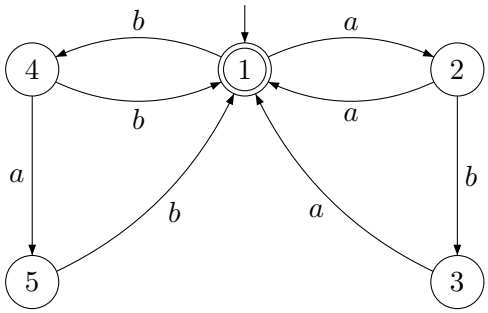


Figura 4.15: L'automa minimale $\mathcal{A}(X^*)$, con $X = \{aa, aba, bab, bb\}$.

Notiamo che per ogni parola $w \in (a \cup babb^*aba)$ si ha $\varphi_{\mathcal{A}}(w) \in \mathrm{Stab}(\{1,2\})$ e w definisce un gruppo ciclico di ordine 2 (si veda Figura 4.16). Ciò nonostante l'insieme $(a \cup babb^*aba)$ è un sottomonoide che non solo non è ciclico, ma non è neanche finitamente generato.

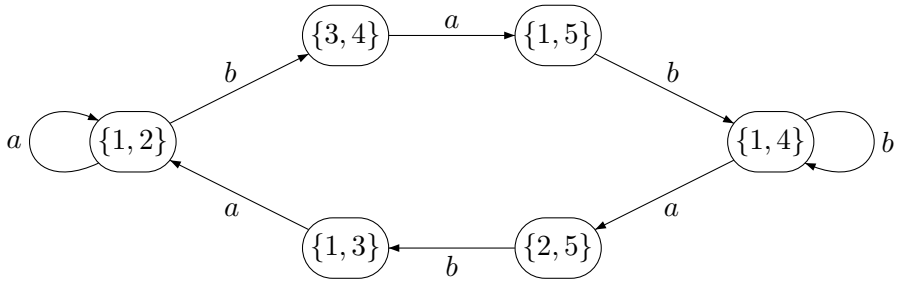


Figura 4.16: Azione di A^* sui 2-sottoinsiemi raggiungibili da $\{1, 2\}$.

Esempio 4.5.13. Il codice $X = \{aaa, aab, abaa, abab, baba, babb, bba, bbb\}$ dell'Esempio 4.5.2 è infisso. L'automa minimale di X^* è rappresentato in Figura 4.17. Il monoide di transizione $\varphi_{\mathcal{A}}(A^*)$ contiene gruppi ciclici di grado 1, 2, 3 e 4. Ad esempio, $\varphi_{\mathcal{A}}(a)$ contiene il ciclo $(1\,2\,3)$, mentre $\varphi_{\mathcal{A}}(ba)$ contiene la permutazione $(1\,6)(2\,3)$.

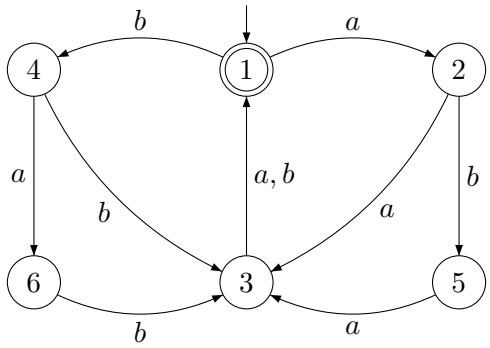


Figura 4.17: Un codice infisso di grado 4 ed ordine 2.

Consideriamo il gruppo G contenente $\varphi_{\mathcal{A}}(ba)$. Esso è un gruppo non transitivo di grado 4 ed ordine 2. Infatti, l'elemento neutro di G è $e = \varphi_{\mathcal{A}}(baba)$ ed il suo insieme di punti fissi è $\{1, 2, 3, 6\}$. G è composto dall'identità (1) e dalla permutazione $(1\,6)(2\,3)$.

Bibliografia

[1] Jean Berstel, Clelia De Felice, Dominique Perrin, Christophe Reutenauer, and Giuseppina Rindone. Bifix codes and sturmian words. http://arxiv.org/abs/1011.5369, 2011.

[2] Jean Berstel, Clelia De Felice, Dominique Perrin, Christophe Reutenauer, and Giuseppina Rindone. Recent results on syntactic groups of codes. 2011.

[3] Jean Berstel, Clelia De Felice, Dominique Perrin, and Giuseppina Rindone. On the groups of codes with empty kernel. *Semigroup Forum*, 80(3):351–374, 2010.

[4] Jean Berstel, Dominique Perrin, and Christophe Reutenauer. *Codes and Automata*. Cambridge University Press, 2009.

[5] Xavier Droubay, Jacques Justin, and Giuseppe Pirillo. Episturmian words and some constructions of de luca and rauzy. *Theoret. Comput. Sci.*, 255(1-2):539–553, 2001.

[6] Amy Glen and Jacques Justin. Episturmian words: a survey. *Theoret. Inform. Appl.*, 43:403–442, 2009.

[7] Marshall Hall. Subgroups of finite index in free groups. *Canadian J. Math.*, 1:187–190, 1949.

[8] Jacques Justin and Laurent Vuillon. Return words in sturmian and episturmian words. *Theoret. Inform. Appl.*, 34(5):343–356, 2000.

[9] M. Lothaire. *Combinatorics on words*. Cambridge University Press, seconda edition, 1997.

[10] M. Lothaire. *Algebraic combinatorics on words*. Cambridge University Press, 2002.

[11] Dominique Perrin. Sur les groupes dans les monoïdes finis. In *Quaderni de "La Ricerca Scientifica"*, volume 109 of *Non-commutative structures in algebra and geometric combinatorics (Napoli, 1978)*, pages 27–36. CNR, 1981.

[12] Dominique Perrin and Giuseppina Rindone. On syntactic groups. *Bull. Belg. Math. Soc. Simon Stevin*, 10(suppl.):749–759, 2003.

[13] Christophe Reutenauer. Une topologie du monoïde libre. *Semigoup Forum*, 18(1):33–49, 1979.

[14] Jean Éric Pin. Mathematical foundation of automata theory. http://www.liafa.jussieu.fr/∼jep/PDF/MPRI/MPRI.pdf, 2011.

[15] Marcel-Paul Schützenberger. On a family of submonoids. *Publ. Math. Inst. Hungar. Acad. Sci. Ser. A*, VI:381–391, 1961.

[16] Marcel-Paul Schützenberger. A property of finitely generated submonoids of free monoids. In *Colloquia Mathematica Societatis János Bolyai*, volume 20 of *Algebraic theory of semigroups (Proc. Sixth Algebraic Conf. Szeged, 1976)*, pages 545–576, 1979.