Sulla fattorizzazione dei codici

CHRISTOPHE REUTENAUER (*)

Introduzione

In questo articolo sarà dimostrata una proprietà di fattorizzazione dei codici.

Un *codice* X è la base d'un sottomonoide libero del monoide libero A^* (generato dall'alfabeto A). Una congettura di Schützenberger afferma che se X è massimale (come codice) e finito, allora A^* è unione finita e disgiunta d'insiemi della forma sX^*p, dove s, p sono delle parole (i.e. elemento di A^*). Equivalentemente questo si esprime nell'algebra $\mathbb{Z}\langle A\rangle$ dei polinomi non commutativi su A a coefficienti in $\mathbb{Z}$, mediante l'uguaglianza

$$\underline{X} - 1 = P(\underline{A} - 1)S \tag{1}$$

dove P ed S sono dei polinomi di $\mathbb{Z}\langle A\rangle$ a coefficienti non negativi e dove $\underline{L}$ denota il polinomio caratteristico della della parte finita L di A^*.

Il risultato principale di questo articolo è che esiste una fattorizzazione del tipo (1), ma con dei polinomi P, S a coefficienti in Z (teorema 1). Noi proviamo anche un teorema inverso: se X è una parte finita di A^* che verifica una relazione del tipo (1), allora X è un codice massimale e finito (teorema 2).

Una versione preliminare di questi risultati si trova in [4].

Questo articolo è il contenuto di una serie di conferenze tenute presso l'Università di Napoli. Voglio ringraziare il professore Aldo de Luca per avermi dato l'occasione di tenere questi seminari; e Clelia de Felice, che ha riletto con attenzione tutto l'articolo e senza l'aiuto della quale esso sarebbe stato incomprensibile.

(*) Institut de Programmation - 4 place Jussieu - 75005 Paris (France)

Sia A un alfabeto finito e A^* il monoide libero generato da A. Denotiamo con $\mathbb{Q}$ il corpo dei numeri razionali, con $\mathbb{Z}$ l'anello dei numeri interi e con $\mathbb{N}$ l'insieme degli interi naturali.

Una *serie formale* è un'applicazione $S: A^* \to \mathbb{Q}$. Il valore di S su una parola $w \in A^*$ si denota con (S, w). La somma di due serie S e T si definisce al seguente modo

$$(S + T, w) = (S, w) + (T, w)$$

Il prodotto esterno di $\alpha \in \mathbb{Q}$ per la serie S si definisce come

$$(\alpha S, w) = \alpha (S, w)$$

Il prodotto di due serie S e T è

$$(ST, w) = \sum_{uv=w} (S, u)(T, v)$$

(Questa somma è naturalmente finita).

L'insieme $\mathbb{Q}\langle\langle A \rangle\rangle$ delle serie formali è un'algebra su $\mathbb{Q}$.

Una *famiglia localmente finita* di serie è una famiglia $(S_i)_{i \in I}$ di serie S_i tale che per ogni parola $w \in A^*$, l'insieme $\{i \in I, (S_i, w) \neq 0\}$ è finito. Allora, si può definire la somma $\sum_{i \in I} S_i$ di questa famiglia come

$$\left(\sum_{i \in I} S_i, w\right) = \sum_{i \in I} (S_i, w)$$

Sia w una parola: denotiamo ancora con w la serie S definita al seguente modo:

$$\begin{cases} (S, w) = 1 \\ (S, u) = 0 \quad \text{per ogni parola} \quad u \neq w \end{cases}$$

Si vede subito che se S è una serie, allora la famiglia di serie $((S, w)\, w)_{w \in A^*}$ è localmente finita e che la sua somma è S. Da ciò segue la notazione

$$S = \sum_{w \in A^*} (S, w)\, w$$

Ora, sia S una serie tale che $(S, 1) = 0$ ($(S, 1)$ si chiama il *termine costante* di S). Allora la famiglia $(S^n)_{n \in \mathbb{N}}$ è localmente finita. La sua somma si denota con S^*:

$$S^* = \sum_{n \geq 0} S^n$$

e risulta

$$S^* = 1 + S S^* = 1 + S^* S$$

Questo implica che S^* è l'inverso di $1 - S$. Una conseguenza di ciò è che una serie è invertibile se e solo se il suo termine costante è $\neq 0$.

Il supporto d'una serie S è il linguaggio

$$\text{supp}(S) = \{w \in A^*, (S, w) \neq 0\}$$

Un polinomio è una serie si supporto finito. L'insieme dei polinomi si denota con $\mathbb{Q}\langle A \rangle$ ed è una sottoalgebra di $\mathbb{Q}\langle\langle A \rangle\rangle$. Il *grado* grad (P) d'un polinomio P è la lunghezza massimale delle parole nel suo supporto.

Sia $L \subset A^*$ un linguaggio: la sua *serie caratteristica* è la serie $\underline{L}$ definita al seguente modo:

$$\begin{cases} (\underline{L}, w) = 1 & \text{se} \quad w \in , L \\ (\underline{L}, w) = 0 & \text{altrimente} \end{cases}$$

Si può anche definire $\underline{L}$ come la somma

$$\underline{L} = \sum_{w \in L} w$$

Qualora ciò non dia luogo ad ambiguità, scriveremo anche L invece di $\underline{L}$.

Un *codice* X è una parte di A^* tale che comunque si scelgono le parole $u_1, \ldots, u_n, v_1, \ldots, v_p$ in X, la relazione

$$u_1 \ldots u_n = v_1 \ldots v_p$$

implica che $n = p$ e $u_i = v_i$ per ogni i.

Una parte X di A^* è un codice se e solo se il sottomonoide X^* generato da X è libero con base X (questa base è allora unica).

Sia $X \subset A^*$ tale che $1 \notin X$. Allora la sua serie caratteristica $\underline{X}$ verifica $(\underline{X}, 1) = 0$. Dunque si può considerare $\underline{X}^* = (1 - \underline{X})^{-1}$. Allora

$$X \text{ codice} \Leftrightarrow \text{i coefficienti di } \underline{X}^* \text{ sono 0 o 1}$$

$$\Leftrightarrow \underline{X}^* = \underline{X^*}$$

In particolare A è un codice, dunque

$$\underline{A}^* = (1 - \underline{A})^{-1} = \underline{A^*}$$

Una parte X di A^* è *prefissa* se comunque si scelgono le parole u, v

$$u, uv \in X \Rightarrow v = 1$$

In altri termini, nessuna parola di X è prefisso di un'altra parola di X.

Simmetricamente, X è *suffissa* se

$$v, uv \in X \Rightarrow u = 1$$

Si vede facilmente che una parte prefissa X tale che $1 \notin X$ è un codice: un tale codice si dirà un *codice prefisso*.

Un codice X è massimale se per ogni codice X' che contiene X si ha $X = X'$.

Siano K, L due linguaggi: allora il prodotto KL è *non ambiguo* se per tutte le parole $u, u' \in K, v, v' \in L$ la relazione $uv = u'v'$ implica che $u = u'$ e $v = v'$.

Il prodotto KL è non ambiguo se è solo se

$$\underline{KL} = \underline{K}\,\underline{L}$$

Sussiste la seguente congettura dovuta a Schützenberger: *Congettura della fattorizzazione.*

Sia X un codice finito e massimale. Allora, esistono due parti finite S e P di A^* tali che

$$A^* = S X^* P \tag{1}$$

dove il prodotto è non ambiguo.

Quando si ha la (1), allora $\underline{A}^* = \underline{S}\,\underline{X}^*\,\underline{P}$. Dunque $\underline{S}$ e $\underline{P}$ sono invertibili in $\mathbb{Q}\langle\langle A\rangle\rangle$ e risulta $1 - \underline{A} = \underline{P}^{-1}(1 - \underline{X})^{-1}\,\underline{S}^{-1}$ da cui

$$\underline{X} - 1 = \underline{P}\,(\underline{A} - 1)\,\underline{S} \tag{2}$$

In effetti, (1) e (2) sono equivalenti: perciò la congettura si formula anche sostituendo alla (1) la (2).

Dimostreremo il teorema seguente:

TEOREMA 1 - *Sia* X *un codice finito e massimale. Allora esistono polinomi* $P, S \in \mathbb{Z}\langle A\rangle$ *tali che* $\underline{X} - 1 = P\,(\underline{A} - 1)\,S$.

La differenza tra questo teorema e la congettura è che quest'ultima richiede che P, S siano a coefficienti 0,1. Il teorema precedente ammette un inverso.

TEOREMA 2 - *Sia* $Y \in \mathbb{N}\langle A\rangle$ *tale che* $(\underline{Y}, 1) = 0$ *e* P, S *due polinomi in* $\mathbb{Q}\langle A\rangle$ *tali che* $Y - 1 = P(\underline{A} - 1)S$. *Allora esiste un codice massimale e finito* X *tale che* $Y = \underline{X}$. *Se in più* $S \in \mathbb{Q}$ (*risp.* $P \in \mathbb{Q}$) *allora* X *è prefisso (risp. suffisso).*

Una conseguenza di ciò è il

COROLLARIO - *Sia* X *una parte finita di* A^*, $1 \notin X$. *Le due condizioni sono equivalenti:*

(i) X *è un codice finito e massimale.*

(ii) *Esistono due polinomi* $P, S \in \mathbb{Z}\langle A\rangle$ *tali che* $\underline{X} - 1 = P(\underline{A} - 1)S$.

Dimostriamo prima il Teorema 2. Per fare ciò, introduciamo alcune notazioni. Sia

$$\pi : \mathbb{Q}\langle A\rangle \to \mathbb{Q}$$

l'omomorfismo di $\mathbb{Q}$-algebre tale che

$$\pi(a) = 1/|A|$$

per ogni lettera $a \in A$. Dunque

$$\pi(P) = \sum_{w \in A^*} (P, w)\,|A|^{-|w|}$$

per ogni polinomio P.

Se $P = \underline{L}$ è la serie caratteristica d'un linguaggio finito, scriveremo anche $\pi(L)$ per $\pi(P)$.

Una parte X di A^* è *completa* se X^* interseca ogni ideale di A^*. In altri termini, ogni parola in A^* è fattore di qualche parola in X^*.

Sussiste il seguente:

TEOREMA (*Schützenberger*) - *Sia* X *un codice finito.*

(i) X *è massimale se e solo se* X *è completo.*

(ii) *Se* X^* *interseca ogni ideale destro di* A, *allora* X *è prefisso.*

Useremo anche il seguente

TEOREMA (*Boë, de Luca, Restivo*) - *Sia* X *una parte finita di* A^*.

(i) *Se* X *è completo, allora* $\pi(X) \geq 1$.

(ii) *Delle tre condizioni seguenti, la validità simultanea di due implica la terza:*

1. X *è completo.*
2. X *è un codice.*
3. $\pi(X) = 1$.

Dimostriamo prima un lemma.

LEMMA 1 - (i) *Siano* S, T *due serie. Allora*

$$\text{supp}(ST) \subset \text{supp}(S)\,\text{supp}(T)$$

(ii) *Sia* S *una serie tale che* $(S, 1) = 0$. *Allora*

$$\text{supp}(S^*) \subset \text{supp}(S)^*$$

Prova (1) Sia $w \in \text{supp}(ST)$. Allora

$$0 \neq (ST, w) = \sum_{uv=w} (S, u)(T, v)$$

Dunque, esistono u, v tali che $(S, u)(T, v) \neq 0$ e $uv = w$. Allora $u \in \text{supp}(S)$, $v \in \text{supp}(T)$ e finalmente:

$$w = uv \in \text{supp}(S)\,\text{supp}(T) .$$

(ii) Per induzione e dalla (i), si ha $\text{supp}(S^n) \subset \text{supp}(S)^n$.

Sia $w \in \text{supp}(S^*)$. Allora $0 \neq (S^*, w) = \sum_{n \geq 0} (S^n, w)$.

Dunque esiste n tale che $(S^n, w) \neq 0$, i.e. $w \in \text{supp}(S^n)$.

Allora $w \in \text{supp}(S)^n$. Finalmente

$$\text{supp}(S^*) \subset \bigcup_{n \geq 0} \text{supp}(S)^n = \text{supp}(S)^*. \quad \square$$

Prova del teorema 2.

Sia $X = \text{supp}(Y)$. Perché $Y - 1$ è invertibile in $\mathbb{Q}\langle\langle A \rangle\rangle$, lo sono anche P e S. Allora $(1 - Y)^{-1} = S^{-1}(1 - \underline{A})^{-1} P^{-1}$ e $\underline{A}^* = S\,Y^*\,P$.

Siccome $\text{supp}(\underline{A}^*) = A^*$, per il lemma 1, si ha

$$A^* \subset \text{supp}(S)\; X^*\; \text{supp}(P) \tag{3}$$

Sia u una parola tale che $|u| > \text{grad}(P), \text{grad}(S)$.

Per ogni parola w, la (3) implica l'esistenza di parole $p \in \mathrm{supp}\,(P)$, $m \in X^*$, $s \in \mathrm{supp}\,(S)$ tali che

$$uwu = smp$$

Perché $|u| > |p|, |s|$ si ha che w è fattore di m.

Ciò mostra che X è completo. In particolare $\pi(X) \geq 1$ (teorema di Boë et al.). Adesso, la relazione $Y - 1 = P(\underline{A} - 1)S$ implica $\pi(Y) - 1 = \pi(P)(\pi(A) - 1)\pi(S) = 0$ poiché $\pi(A) = 1$. Dunque $\pi(Y) = 1$.

Poiché $Y \in \mathbb{N}\langle A \rangle$, si ha $Y = \underline{X} + Y'$ per qualche $Y' \in \mathbb{N}\langle A \rangle$. Allora

$$1 \leq \pi(X) \leq \pi(X) + \pi(Y') = \pi(Y) = 1 \ .$$

Dunque $\pi(X) = 1$, $\pi(Y') = 0$ e $Y' = 0$ (perché i coefficienti di Y' sono non negativi).

Allora $Y = \underline{X}$ ed X è un codice (teorema di Boë et al.).

Poiché $\pi(X) = 1$ ed X è completo, X è quindi un codice massimale e finito (teorema di Schützenberger).

Se in più $S \in \mathfrak{Q}$, allora $S \neq 0$ (altrimenti $Y = 1$ e $(Y, 1) \neq 0$) e la (3) si scrive

$$A^* \subset X^* \,\mathrm{supp}\,(P)$$

Un ragionamento analogo al precedente mostra allora che X^* interseca tutti gli ideali destri di A^*, dunque X è un codice prefisso (teorema di Schutzenberger). □

Ora, cominciamo la prova del teorema 1.

Sia X un codice massimale e finito. Per il teorema di Kleene, X^* è un linguaggio *riconoscibile*, i.e. esiste un monoide finito M, un omomorfismo di monoidi $\mu: A^* \to M$ e una parte M' di M tali che $X^* = \mu^{-1}(M')$. Si può supporre che $\mu(A^*) = M$. Allora $M' = \mu(X^*)$ è un sottomonoide di M. Sia $\mathfrak{I}$ l'ideale minimale di M (i.e. l'intersezione di tutti gli ideali di M: questa è non vuota perché M è finito). Useremo il:

TEOREMA (*Suschkewitsch*) - *Sia* M *un monoide finito e* $\mathfrak{I}$ *il suo ideale minimale. Allora* $\mathfrak{I}$ *è l'unione dusgiunta degli ideali destri minimali (risp. sinistri minimali) di* M. *Per ogni ideale destro (risp. sinistro) minimale* R (*risp.* L), *l'intersezione* $R \cap L$ *è un gruppo finito.*

PROPOSIZIONE - *Sia* X *un codice massimale e finito. Allora esistono tre parti finite* P, S, F *di* A^* *tali che*:

$$\underline{A}^* = S\underline{X}^*\underline{P} + \underline{F} \tag{4}$$

e $1 \notin F$.

In altre parole, A^* è l'unione disgiunta di $S X^* P$ e di F, e il prodotto $S X^* P$ è non ambiguo. Questa proposizione è un'altra forma debole della congettura della fattorizzazione.

Prova 1. Siano M un monoide finito, M' un sottomonoide di M e $\mu : A^* \to M$ un omomorfismo di monoidi tale che $X^* = \mu^{-1}(M')$. Sia $\mathfrak{J}$ l'ideale minimale di M. Dal teorema di Schützenberger, X^* interseca ogni ideale di A^*, in particolare l'ideale $\mu^{-1}(\mathfrak{J})$. Poiché μ è surgettivo, si ha $M' = \mu(X^*)$ e $\mathfrak{J} = \mu\mu^{-1}(\mathfrak{J})$, dunque M' interseca $\mathfrak{J}$. Dal teorema di Suschkewitsch, esistono un ideale destro minimale R e un ideale sinistro minimale L tali che M' interseca il gruppo finito G. Sia $H = M' \cap G$. Allora H è un sottosemigruppo d'un gruppo finito, dunque un sottogruppo di G.

Sia $d = [G : H]$. Siano $g_1, \ldots, g_d$, $h_1, \ldots, h_d$ elementi di G tali che $g_1 H, \ldots, g_d H$ (risp. $H h_1, \ldots, H h_d$) siano i d laterali destri (risp. sinistri) di H in G.

È possibile scegliere $h_1 = g_1 = e$ (l'elemento neutro di G) e supporre che g_i è l'inverso di h_i in G.

Siano $x_1, \ldots, x_d$, $y_1, \ldots, y_d$ parole tali che $\mu(x_i) = h_i$ e $\mu(y_j) = g_j$.

Proviamo che per ogni parola w, esiste un unico j tale che

$$x_1 w y_j \in X^* \tag{5}$$

Infatti, $\mu(x_1 w x_1) = e\mu w$ e appartiene a G (perché $e \in R$, $e \in L \Rightarrow$ $\Rightarrow e\mu w e \in R \cap L$); dunque esiste un j tale che $e\mu w e \in H h_j$; allora $e\mu w g_j = e\mu w e g_j \in H h_j g_j = H$; dunque $\mu(x_1 w y_j) = e\mu w g_j \in H \subset M' \Rightarrow$ $\Rightarrow x_1 w y_j \in \mu^{-1}(M') = X^*$.

Per mostrare l'unicità di j, il ragionamento è analogo (si mostra che $x_1 w y_j \in X^* \Rightarrow e\mu w e \in H h_j$, dunque j è unico).

La relazione (5) mostra che

$$A^* = \bigcup_{1 \le j \le d} L(x_1, y_j)$$

dove l'unione è disgiunta e dove $L(x, y) = \{w \in A^*, xwy \in X^*\}$. Ciò si puó scrivere

$$\underline{A}^* = \sum_{1 \le j \le d} \underline{L}(x_1, y_j) \tag{6}$$

La proposizione è allora conseguenza del seguente:

LEMMA 2 - *Sia* X *un codice finito e per ogni* $x, y \in A^*$, *sia* $L(x, y) = \{w \in A^*, xwy \in X^*\}$. *Esistono due applicazioni* $x \mapsto S_x$, $y \mapsto P_y$ *di* A^* *nell'insieme* $2^{(A^*)}$ *delle parti finite di* A^* *e un'applicazione* $(x, y) \mapsto F(x, y)$ *di*

$A^* \times A^*$ *in* $2^{(A^*)}$ *tali che: per tutte le parole* x, y *si ha*

$$\underline{L}(x,y) = \underline{S}_x \underline{X}^* \underline{P}_y + \underline{F}(x,y)$$

Inoltre, se $x, y \in X^*$, *allora* $1 \in S_x \cap P_y$.

Prima di dimostrare il lemma, facciamo vedere che da esso segue la proposizione. Dal lemma e dalla (6), abbiamo

$$\underline{A}^* = \sum_j \underline{S}_{x_1} \underline{X}^* \underline{P}_{y_j} + \sum_j \underline{F}(x_1, y_j)$$

$$= \underline{S}_{x_1} \underline{X}^* \left(\sum_j \underline{P}_{y_j} \right) + \sum_j \underline{F}(x_1, y_j)$$

Siccome $\underline{A}^*$ è una serie caratteristica, anche le serie $\sum_j \underline{P}_{y_j}$ e $\sum_j \underline{F}(x_1, y_j)$ sono caratteristiche: esistono parti finite S, P, F di A^* tali che $\underline{S}_{x_1} = \underline{S}$, $\sum_j \underline{P}_{y_j} = \underline{P}$ e $\sum_j \underline{F}(x_1, y_j) = \underline{F}$. Allora

$$\underline{A}^* = \underline{S}\,\underline{X}^*\,\underline{P} + \underline{F}$$

e $x_1, y_1 \in X^*$ implica $1 \in S \cap P$; dunque $1 \notin F$ (altrimenti $(\underline{A}^*, 1) = (\underline{S}\,\underline{X}^*\,\underline{P}, 1) + (\underline{F}, 1) \geq 2$).

Prova del lemma.

Siano

$$S'_x = \{u, xu \in X^*\}$$

$$P'_x = \{v, vx \in X^*\}$$

Ora, siano

$$S_x = S'_x \setminus S'_x X^+$$

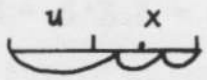
$$P_x = P'_x \setminus X^+ P'_x$$

dove $X^+ = X^* \setminus 1$.

Allora S_x e P_x sono finiti: infatti, se $u \in P'_x$ si ha lo schema seguente

dove ogni arco rappresenta un elemento del codice X.

Ma nel caso di questo schema, si ha $u \in X^+ P'_x$; dunque, se $u \in P_x$, allora si ha



dunque u è fattore sinistro di qualche parola in X. Poiché X è finito, lo è anche P_x.

Mostriamo che il prodotto

$$S_x X^* P_y$$

è non ambiguo. Siano $s, s' \in S_x$, $m, m' \in X^*$ e $p, p' \in P_y$ tali che $smp = s'm'p'$. Allora

$$w = xsmpy = xs'm'p'y \in X^*$$

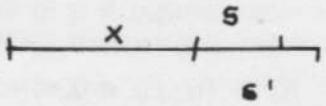
perché $xs, xs', py, p'y \in X^*$. Allora

$$w = x_1 \dots x_n, \; x_i \in X$$

e perché X è un codice

$$xs = x_1 \dots x_i \quad \text{e} \quad xs' = x_1 \dots x_j$$

Ma se $j > i$ si ha lo schema



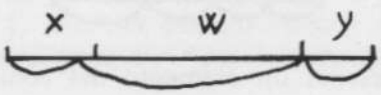
e dunque $s' = sx_{i+1} \dots x_j \in S'_x X^+$: contraddizione. Similmente, $i < j$ è impossibile, dunque $i = j$ e $s = s'$. Un ragionamento simmetrico mostra che $p = p'$. Finalmente $m = m'$. Sia

$$F(x, y) = L(x, y) \setminus S_x X^* P_y$$

Sia $w \in L(x, y)$. Allora si possono presentare due casi:

1)

2)



Nel primo caso, si vede che $w \in S_x X^* P_y$. Dunque, se $w \in F(x,y)$ allora siamo nel caso 2, e allora w è fattore di qualche parola in X. Quindi, $F(x,y)$ è finito.

Si vede subito che $S_x X^* P_y \subset L(x,y)$. Dunque

$$\underline{L}(x,y) = \underline{S}_x \underline{X}^* \underline{P}_y + \underline{F}(x,y)$$

Se in più, $x, y \in X^*$, allora $1 \in S'_x \cap P'_y$, dunque $1 \in S_x \cap P_y$. □

Torniamo alla relazione (4):

$$\underline{A}^* = \underline{S}\,\underline{X}^*\,\underline{P} + \underline{F} \tag{4}$$

con $1 \notin F$.

La serie $\underline{A}^* - \underline{F}$ è invertibile in $\mathbb{Q}\langle\langle A\rangle\rangle$ perché il suo termine costante è 1. Si ha

$$\underline{A}^* - F = (1-\underline{A})^{-1} - \underline{F} = (1-\underline{A})^{-1}(1-(1-\underline{A})\underline{F})$$

e $1 \notin F$ implica che $1-(1-\underline{A})\underline{F}$ è invertibile. Dunque la (4) implica che

$$1 - \underline{X} = \underline{P}(1-(1-\underline{A})\underline{F})^{-1}(1-\underline{A})\,\underline{S} \tag{7}$$

Ora, dobbiamo eliminare il fattore in più $(1-(1-\underline{A})\underline{F})^{-1}$ per ottenere il teorema 1. Per questo, useremo il

LEMMA 3 (Cohn) - Siano P_1, P_2, P_3 tre polinomi tali che P_2 è invertibile in $\mathbb{Q}\langle\langle A\rangle\rangle$ e che $P_1 P_2^{-1} P_3$ è un polinomio. Allora esistono polinomi Q, R, S, T tali che $P_1 = QR$, $P_2 = SR$, $P_3 = ST$ (dunque $P_1 P_2^{-1} P_3 = QT$).

Prova 1. Supponiamo prima che P_1 e P_2 hanno un divisore comune non scalare a destra: $P_1 = P'_1 U$ e $P_2 = P'_2 U$. Allora P'_2 è invertibile in $\mathbb{Q}\langle\langle A\rangle\rangle$ e $P_1 P_2^{-1} P_3 = P'_1 P'^{-1}_2 P_3$. Ma allora $\operatorname{grad}(P'_2) < \operatorname{grad}(P_2)$ e per induzione $P'_1 = QR$, $P'_2 = SR$, $P_3 = ST$. Dunque $P_1 = Q(RU)$, $P_2 = S(RU)$, $P_3 = ST$.

2. Simmetricamente, se P_2 e P_3 hanno un divisore comune non scalare a sinistra, si prova l'asserto.

3. Mostriamo che siamo sempre nel caso 1 o 2. È possibile supporre che $P_2 \notin \mathbb{Q}$ e che $(P_2, 1) = 1$. Allora $P_2 = 1 - T$, $T \in \mathbb{Q}\langle A\rangle$ e $(T, 1) = 0$. Dunque l'ipotesi diviene

$$P_1 T^* P_3 \in \mathbb{Q}\langle A\rangle$$

Sia E l'insieme dei polinomi P tale che $P_1 T^* P \in \mathbb{Q}\langle A\rangle$. Allora, E è un sottospazio di $\mathbb{Q}\langle A\rangle$ e contiene P_3 e $1-T$.

Sia P_0 un polinomio in $E \setminus 0$ ($E \setminus 0$ è non vuoto perché $1 - T \neq 0$) di grado minimale. Se P_0 è uno scalare, allora $P_1 T^*$ è un polinomio, dunque $P_1 = P_1'(1-T)$ e siamo nel caso 1.

Se P_0 non è uno scalare, mostreremo che P_2 e P_3 hanno P_0 come divisore sinistro riportandosi così al caso 2.

4. Per una serie formale S è una lettera a, si definisce la serie Sa^{-1} come $(Sa^{-1}, w) = (S, wa)$ per ogni parola w.

LEMMA 4 - 1. *Siano* S_1, S_2 *due serie e a una lettera. Allora*

$$(S_1 S_2) a^{-1} = S_1 (S_2 a^{-1}) + (S_2, 1) S_1 a^{-1}$$

2. *Sia* T *una serie tale che* $(T, 1) = 0$. *Allora*

$$(T^*) a^{-1} = T^* (T a^{-1})$$

Prova 1. Si verifica immediatamente quando S_1 e S_2 sono parole, e si estende per linearità alle serie.

2. E una conseguenza di 1. e della formula

$$T^* = 1 + T^* T \quad \square$$

LEMMA 5 - *Per ogni polinomio* P, Pa^{-1} *è un polinomio di grado* $<$ grad (P) *se* $P \neq 0$, *e si ha*

$$P = (P, 1) + \sum_{a \in A} (Pa^{-1}) a \tag{8}$$

In particolare, $P \notin \mathbb{Q}$ *se e solo se esiste una lettera* $a \in A$ *tale che* $Pa^{-1} \neq 0$.

Prova. La formula è evidente quando P è una parola e si estende per linearità. $\square$

5. Ora sia $P \in E$. Allora $P_1 T^* P$ è un polinomio, dunque anche $(P_1 T^* P) a^{-1}$ è un polinomio. Ma del lemma 4

$$\begin{aligned}(P_1 T^* P) a^{-1} &= (P_1 T^*) P a^{-1} + (P, 1) (P_1 T^*) a^{-1} \\ &= (P_1 T^*) P a^{-1} + (P, 1) P_1 (T^* a^{-1}) + (P, 1) (T^*, 1) P_1 a^{-1} \\ &= (P_1 T^*) P a^{-1} + (P, 1) P_1 T^* T a^{-1} + (P, 1) P_1 a^{-1}\end{aligned}$$

Poiché $P_1 a^{-1} \in \mathbb{Q}$

$$P_1 T$$

Dunque

(9) P

Sia $P \in E$ di grad
fatti $P \neq 0$ e $(P, 1) =$
$Pa^{-1} \neq 0$. Si ha Pa^{-1}
traddice la minimalità
Una prima conseg
$(P_0, 1) = 1$.
Un'altra conseguc
$\leq$ grad (P_0), si ha
grad (R) $\leq$ grad (P_0) e
Ora, mostriamo c
$P_3, 1 - T \in E$).
Sia $P \in E$: l'asser
supporre che grad (P)
$(R, 1) = 0$, grad (R) $\leq$
grad $(Ra^{-1}) <$ grad (R)
Dalla (8) segue che
$P \in P_0 \mathbb{Q}\langle A\rangle$. $\square$

Il lemma 3 non è
(7): perderemmo il fa

LEMMA 6 (*Divisio*
nulli tali che PQ = R

$$P = R$$

Prova 1. Definiamo per
al seguente modo

per ogni parola u. Si
Allora, per tutti

(10)

dove grad (P') $<$ grad
duzione, adoperando

Poiché $P_1 a^{-1} \in \mathbb{Q}\langle A\rangle$, abbiamo

$$P_1 T^* (P a^{-1} + (P, 1)\, T a^{-1}) \in \mathbb{Q}\langle A\rangle$$

Dunque

$$P \in E \Rightarrow P a^{-1} + (P, 1)\, T a^{-1} \in E \tag{9}$$

Sia $P \in E$ di grado $\leq \text{grad}(P_0)$. Allora, se $(P, 1) = 0$ si ha $P = 0$. Infatti $P \neq 0$ e $(P, 1) = 0$ implicano $P \notin \mathbb{Q}$ e dal lemma 5, esiste a tale che $P a^{-1} \neq 0$. Si ha $P a^{-1} \in E$ dalla (9), $\text{grad}(P a^{-1}) < \text{grad}(P_0)$; questo contraddice la minimalità di P_0.

Una prima conseguenza di ciò è che $(P_0, 1) \neq 0$: si può anche scegliere $(P_0, 1) = 1$.

Un'altra conseguenza è che per ogni $P \in E$ tale che $\text{grad}(P) \leq \text{grad}(P_0)$, si ha $P = (P, 1)\, P_0$. Infatti $R = P - (P, 1)\, P_0 \in E$, $\text{grad}(R) \leq \text{grad}(P_0)$ e $(R, 1) = 0$: dunque $R = 0$.

Ora, mostriamo che $E \subset P_0 \mathbb{Q}\langle A\rangle$ (e la prova sarà finita, perché $P_3, 1 - T \in E$).

Sia $P \in E$: l'asserto è vero se $\text{grad}(P) \leq \text{grad}(P_0)$ dunque possiamo supporre che $\text{grad}(P) > \text{grad}(P_0)$. Sia $R = P - (P, 1)\, P_0$. Allora $R \in E$, $(R, 1) = 0$, $\text{grad}(R) \leq \text{grad}(P)$, e dalla (9), $R a^{-1} \in E$ per ogni lettera a. Ma $\text{grad}(R a^{-1}) < \text{grad}(R) \leq \text{grad}(P)$, dunque per induzione, $R a^{-1} \in P_0 \mathbb{Q}\langle A\rangle$. Dalla (8) segue che $R \in P_0 \mathbb{Q}\langle A\rangle$ (perché $(R, 1) = 0$) e finalmente $P \in P_0 \mathbb{Q}\langle A\rangle$. □

Il lemma 3 non è sufficiente per dedurre il teorema 1 della relazione (7): perderemmo il fattore $1 - \underline{A}$. Dobbiamo ancora usare il

LEMMA 6 (*Divisione euclidea di Cohn*) - *Siano* P, Q, R, S *polinomi non nulli tali che* $PQ = RS$. *Allora esistono polinomi* T, U *tali che*

$$P = RT + U \quad \text{e} \quad \text{grad}(U) < \text{grad}(R)\ .$$

Prova 1. Definiamo per ogni polinomio P e ogni parola w il polinomio $P w^{-1}$ al seguente modo

$$(P w^{-1}, u) = (P, uw)$$

per ogni parola u. Si verifica facilmente che $P (uv)^{-1} = (P v^{-1})\, u^{-1}$.

Allora, per tutti i polinomi P, Q si ha

$$(PQ)\, w^{-1} = P\, (Q w^{-1}) + P' \tag{10}$$

dove $\text{grad}(P') < \text{grad}(P)$ o $P = P' = 0$. Questa formula si dimostra per induzione, adoperando i lemmi 4 e 5.

2. Ora, siano P, Q, R, S come nel lemma. Possiamo supporre che $\text{grad}(P) \geq \text{grad}(R)$: altrimenti si prende $T = 0$ e $U = P$. Sia w una parola nel supporto di Q di lunghezza massimale. Allora $\lambda = (Q, w) \neq 0$ e $Qw^{-1} = \lambda$. In più dalla (10)

$$(PQ)\,w^{-1} = P(Qw^{-1}) + P' = \lambda P + P',\ \text{grad}(P') < \text{grad}(P)$$

e

$$(RS)\,w^{-1} = R(Sw^{-1}) + R',\ \text{grad}(R') < \text{grad}(R)\ .$$

Poiché $PQ = RS$ si ha

$$P(Qw^{-1}) + P' = R(Sw^{-1}) + R'$$

Dunque

$$P = -\lambda^{-1}P' + \lambda^{-1}R' + \lambda^{-1}R(Sw^{-1})$$

e

$$-\lambda^{-1}P'Q + \lambda^{-1}R'Q + \lambda^{-1}R(Sw^{-1})Q = PQ = RS$$

Quindi

$$\lambda^{-1}(-P' + R')Q = R(S - \lambda^{-1}R(Sw^{-1})Q) \tag{11}$$

Se $-P' + R' = 0$, allora $P = \lambda^{-1}R(Sw^{-1})$ e si ha l'asserto.
Altrimenti $-P' + R' \neq 0$, e perché $\text{grad}(R) \leq \text{grad}(P)$, si ha

$$\text{grad}(-P' + R') < \text{grad}(P)$$

Dalla (11) per induzione segue che

$$\lambda^{-1}(-P' + R') = RT + U$$

con $\text{grad}(U) < \text{grad}(R)$. Allora $P = R(\lambda^{-1}(Sw^{-1}) + T) + U$ come si voleva. □

Consideriamo ancora la (7)

$$\underline{X} - 1 = \underline{P}(1 - (1 - \underline{A})\,\underline{F})^{-1}(\underline{A} - 1)\,\underline{S}\ .$$

Poiché $\underline{X} - 1$ è un polinomio, dal lemma 3 esistono polinomi Q, R, T, U tali che:

$$\underline{P} = QR$$

$$1 - (1 - \underline{A})\,\underline{F} = TR \tag{12}$$

(13) $$(\underline{A} - 1)\,\underline{S} = TU$$

e dunque:

(14) $$\underline{X} - 1 = QU$$

Dalla (13) e dal lemma 6 segue l'esistenza di polinomi K e H tali che:

(15) $$T = (\underline{A} - 1)\,K + H \quad \text{e} \quad \text{grad}\,(H) < \text{grad}\,(\underline{A} - 1)$$

Dunque $H = h \in \mathbb{Q}$. Dalle (12) e (15) si ha:

$$1 - (1 - \underline{A})\,\underline{F} = (\underline{A} - 1)\,KR + hR$$

Allora $h \neq 0$ (altrimenti 1 sarebbe divisibile per $\underline{A} - 1$).
Dalle (13) e (15)

$$(\underline{A} - 1)\,\underline{S} = (\underline{A} - 1)\,KU + hU$$

dunque

$$U = (\underline{A} - 1)\,V$$

per qualche polinomio V (perché $h \neq 0$). Dalla (14), si ha allora

(16) $$\underline{X} - 1 = Q\,(\underline{A} - 1)\,V$$

Questa relazione è quasi il teorema 1: ma non abbiamo dimostrato che Q, V sono a coefficienti interi. Questa condizione sarà conseguenza d'una cosa più generale.

Diciamo come d'uso che un polinomio $P \in \mathbb{Z}\langle A\rangle \setminus 0$ è *primitivo* se i suoi coefficienti risultano primi tra loro.

LEMMA 7 (*lemma di Gauss*) - *Siano* P, Q *polinomi primitivi. Allora* PQ *è primitivo.*

Prova. Se PQ è non primitivo, allora esiste un numero primo p tale che p divide tutti i coefficienti di PQ. In altri termini, l'immagine $\underline{PQ}$ di PQ in $(\mathbb{Z}/p\mathbb{Z})\langle A\rangle$ è zero. Dall'ipotesi, le immagini $\underline{P}$ e $\underline{Q}$ di P e Q non sono zero. Questo è una contraddizione perché $\underline{PQ} = \underline{P}\,\underline{Q}$ ed essendo $\mathbb{Z}/p\mathbb{Z}$ un corpo, $(\mathbb{Z}/p\mathbb{Z})\langle A\rangle$ è integro. □

Per ogni polinomio $P \in \mathbb{Q}\langle A\rangle$, $P \neq 0$, sia $c(P)$ l'unico elemento di $\mathbb{Q}$ tale che $c(P) > 0$ e $P/c(P)$ è primitivo. Scriviamo

$$P = c(P)\,P'$$

dove P' è primitivo. Una conseguenza del lemma è che per tutti i polinomi P, Q si ha

$$c(PQ) = c(P)\,c(Q) \quad \text{e dunque} \quad (PQ)' = P'\,Q' .$$

Poiché $\underline{X} - 1$ e $\underline{A} - 1$ sono primitivi, si ha $c(\underline{X} - 1) = c(\underline{A} - 1) = 1$. Dunque, dalla (16)

$$\underline{X} - 1 = Q'\,(\underline{A} - 1)\,V'$$

Ciò conclude la prova del teorema 1. □

BIBLIOGRAFIA

[1] J. M. Boë, A. de Luca, A. Restivo, *Minimal complete sets of words*, Theor. Comp. Sci. *12* (1980), 325-332.
[2] P. M. Cohn, *Free rings and their relations*, Acad. Press (1971).
[3] G. Lallement, *Semigroups and combinatorial applications*, John Wiley (1979).
[4] C. Reutenauer, *Sur un théorème de Schützenberger*, Notes aux Comptes Rendus Acad. Sci. Paris *296* (1983) 619-621.

Pervenuto alla redazione il 16 Aprile 1983