TEOREMA DI POST

Non esiste alcun algoritmo per determinare se un arbitrario sistema di corrispondenza di Post dato ammetta o no una soluzione.

Dimostrazione

Metodo usato:

Ricondurremo la soluzione di un sistema di corrispondenza di Post a quella di un problema che sappiamo essere insolubile algoritmicamente.

Più precisamente, costruiremo un sistema di Post $P_{u,v}$ e mostreremo che $P_{u,v}$ ammette una soluzione se e solo se $u \overset{*}{\underset{\Pi}{\Rightarrow}} v$, cioè se e solo se v è derivabile da u, mediante un processo di Semi-Thue il cui problema della parola è insolubile.

Ricordiamo che:

- Il problema della parola per un processo di Semi-Thue Π è il problema di determinare, per ogni coppia di parole data, u, v, sull'alfabeto di Π, se $u \overset{*}{\underset{\Pi}{\Rightarrow}} v$.
- Sappiamo, per averlo dimostrato, che esiste un processo di Semi-Thue su un alfabeto $\{a, b\}$ di due simboli il cui problema della parola è insolubile.

Consideriamo un processo di semi-Thue Π su $\{a, b\}$ il cui problema della parola è insolubile ed aggiungiamo alle regole di riscrittura di Π le due seguenti:

$$a \to a \,, \quad b \to b \,.$$

Esse, ovviamente, non modificano il processo, ma ci permettono di aumentare la lunghezza della derivazione qualora ciò (come accadrà) ci dovesse servire.

Costruiamo adesso il nostro sistema di Post $P_{u,v}$.

- SIANO $g_i \to h_i$, $i=1,2,\dots,n$ LE REGOLE DI RISCRITTURA DI Π COMPRESE LE ULTIME AGGIUNTE

- L'ALFABETO DI $P_{u,v}$ SIA FORMATO DAI SIMBOLI SEGUENTI

$$a,\ b,\ \tilde{a},\ \tilde{b},\ [\,,\ ]\,,\ *\,,\ \tilde{*}$$

- PER OGNI PAROLA $w \in \{a, b\}^*$ SIA $\tilde{w} \in \{\tilde{a}, \tilde{b}\}^*$ LA PAROLA OTTENUTA DA w SOSTITUENDO AD a, $\tilde{a}$ E A b, $\tilde{b}$.

- $P_{u,v}$ CONSISTA DELLE SEGUENTI $2n+4$ TESSERE

$$\boxed{\frac{[u*}{[}} \quad \boxed{\frac{*}{\tilde{*}}} \quad \boxed{\frac{\tilde{*}}{*}} \quad \boxed{\frac{]}{\tilde{*}v]}} \quad \boxed{\frac{h_i}{\tilde{g}_i}} \quad \boxed{\frac{\tilde{h}_i}{g_i}}$$

$$i = 1, 2, \dots, n$$

Osserviamo che, poiché tra le produzioni di Π vi sono $a \to a$ e $b \to b$, tra le tessere di $P_{u,v}$ vi saranno anche le seguenti:

$$\begin{array}{|c|}\hline a \\ \hline \tilde{a} \\ \hline\end{array} \quad \begin{array}{|c|}\hline \tilde{a} \\ \hline a \\ \hline\end{array} \quad \begin{array}{|c|}\hline b \\ \hline \tilde{b} \\ \hline\end{array} \quad \begin{array}{|c|}\hline \tilde{b} \\ \hline b \\ \hline\end{array}$$

e allora per compendiare un uso ripetuto della seconda e quarta tessera e della prima e terza tessera, rispettivamente, potremo usare tessere del tipo:

$$\begin{array}{|c|}\hline \tilde{p} \\ \hline p \\ \hline\end{array} \quad \begin{array}{|c|}\hline p \\ \hline \tilde{p} \\ \hline\end{array} \qquad \text{essendo } p \in \{a,b\}^*$$

Supponiamo adesso che sia $u \underset{\Pi}{\overset{*}{\Rightarrow}} v$

e mostriamo che $P_{u,v}$ ammette una soluzione.

La derivazione $u \underset{\Pi}{\overset{*}{\Rightarrow}} v$ può essere decomposta nei suoi passi elementari:

$$u = u_1 \underset{\Pi}{\Rightarrow} u_2 \underset{\Pi}{\Rightarrow} \dots \underset{\Pi}{\Rightarrow} u_m = v$$

con m dispari grazie alla presenza in Π di $a \to a$ e $b \to b$

per ogni i, $1 \le i < m$ possiamo scrivere

$$u_i = p_i g_{j_i} q_i \quad \text{e} \quad u_{i+1} = p_i h_{j_i} q_i$$

essendo $p_i, q_i \in \{a,b\}^*$ e $g_{j_i} \to h_{j_i}$ la j_i-esima produzione

Scriviamo adesso la stringa

$$[\; u_1 * \tilde{u}_2 \,\tilde{*}\, u_3 * \ldots * \tilde{u}_{m-1} \,\tilde{*}\, u_m \;]$$

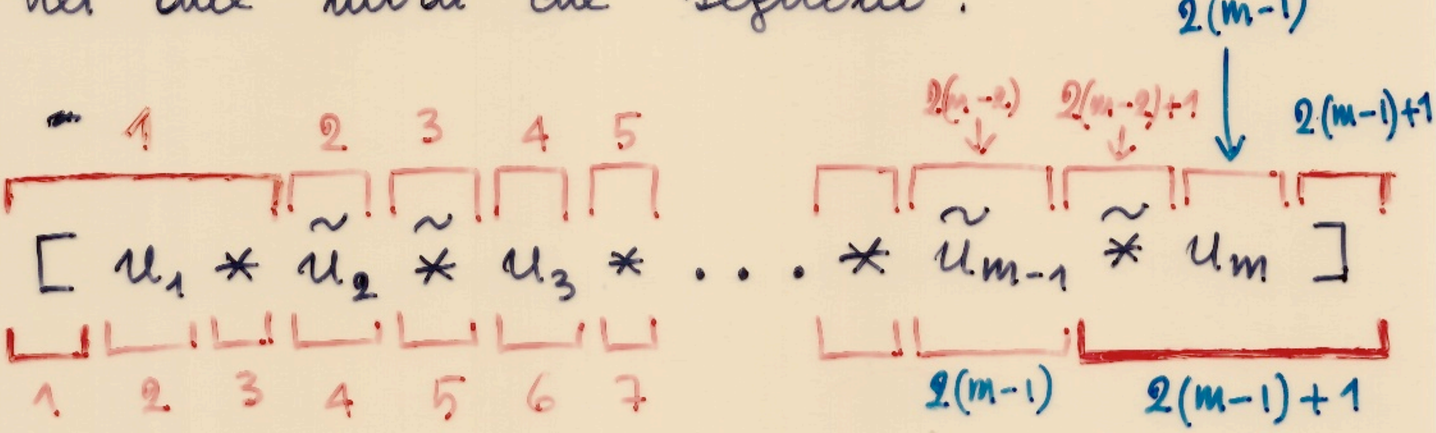
la cui regola di formazione è evidente dalle separazioni indicate in rosso sotto la stringa stessa e cioè:

- iniziamo con [
- concateniamo la prima parola u_1 della deduzione seguita dal simbolo di separ. $*$
- concateniamo l'immagine in $\{\tilde{a}, \tilde{b}\}^*$ della seconda parola u_2 della deduzione seguita dal simbolo di separazione $\tilde{*}$.
- continuiamo in questo modo alternando parole in $\{a, b\}$ ed in $\{\tilde{a}, \tilde{b}\}$
- dopo l'ultima parola u_m non mettiamo alcun simbolo di separazione
- chiudiamo concatenando il simbolo].

IL FATTO CHE m SIA DISPARI CI ASSICURA CHE u_m COMPARIRÀ IN QUANTO TALE E NON NELLA FORMA $\tilde{u}_m$.

La presenza delle tessere $\boxed{\dfrac{[u*}{[}}$ e $\boxed{\dfrac{]}{\tilde{*}\, v]}}$

ci permette di iniziare a decomporre, dall'inizio e dalla fine, la nostra stringa nei due modi che seguono:



Sia sopra sia sotto vi sono $2(m-1)+1$ separazioni; numeriamole.

Costruiamo adesso le tessere che hanno come parole superiore ed inferiore rispettivamente quelle di numero corrispondente nelle separazioni superiore ed inferiore.

Mostriamo adesso che tutte queste tessere appartengono a $P_{u,v}$.

Si ha che:

la prima tessera $\boxed{\dfrac{[u_1*}{[}}$ e l'ultima tessera $\boxed{\dfrac{]}{\tilde{*}\, u_m]}}$

appartengono a $P_{u,v}$.

Per tutte le altre tessere intermedie che abbiamo costruito si ha che sono di uno dei due tipi seguenti:

$$\underbrace{\left[\frac{\tilde{u}_{i+1}}{u_i}\right], \left[\frac{u_{i+1}}{\tilde{u}_i}\right]}\qquad \underbrace{\left[\frac{\tilde{*}}{*}\right], \left[\frac{*}{\tilde{*}}\right]}.$$

Le ultime due appartengono a $P_{u,v}$.
Per quelle del primo tipo osserviamo che: poiché $u_i = p_i\, g_{j_i}\, q_i$ e $u_{i+1} = p_i\, h_{j_i}\, q_i$ si possono decomporre nel modo seguente:

$$\left[\frac{\tilde{u}_{i+1}}{u_i}\right] = \left[\frac{\tilde{p}_i}{p_i}\right]\left[\frac{\tilde{h}_{j_i}}{g_{j_i}}\right]\left[\frac{\tilde{q}_i}{q_i}\right] \quad \text{e} \quad \left[\frac{u_{i+1}}{\tilde{u}_i}\right] = \left[\frac{p_i}{\tilde{p}_i}\right]\left[\frac{h_{j_i}}{\tilde{g}_{j_i}}\right]\left[\frac{q_i}{\tilde{q}_i}\right]$$

La prima e la terza di entrambe le decomposizioni si ottengono, come già osservato, a partire dalle tessere $\left[\frac{a}{\tilde{a}}\right]$, $\left[\frac{\tilde{a}}{a}\right]$, $\left[\frac{b}{\tilde{b}}\right]$, $\left[\frac{\tilde{b}}{b}\right]$, quelle centrali sono già in $P_{u,v}$.

ABBIAMO COSÌ MOSTRATO CHE SOTTO L'IPOTESI CHE $u \overset{*}{\underset{\Pi}{\Longrightarrow}} v$, $P_{u,v}$ AMMETTE SOLUZIONE

(Il "trucco" consiste nel costruire tessere mettendo sotto ogni parola u_{i+1} la parola u_i da cui viene derivata).

Viceversa, ammettiamo che $P_{u,v}$ ammetta una soluzione, vogliamo mostrare che è $u \overset{*}{\underset{\Pi}{\Rightarrow}} v$.

Andiamo ad esaminare le "tessere" a disposizione. Le uniche che hanno lo stesso simbolo sopra e sotto sono quelle con le parentesi. La soluzione, pertanto, deve necessariamente iniziare e terminare con:

$$\begin{array}{|c|}\hline [u* \\ \hline [\\ \hline\end{array} \;,\; \begin{array}{|c|}\hline] \\ \hline \tilde{*}v] \\ \hline\end{array}$$

Possiamo ancora supporre che la soluzione w non contenga al suo interno una sottoparola w' del tipo $[z]$ perché in questo caso w' sarebbe già una soluzione e potremmo partire da w' invece che da w.

Allora sarà

$$w = [u* \underbrace{\dots} \tilde{*} v]$$

Nella zona $\underbrace{\dots}$ avremo un certo numero di tessere appartenenti o al

tipo I: $\begin{array}{|c|}\hline h \\ \hline \tilde{g} \\ \hline\end{array}$ $\begin{array}{|c|}\hline \tilde{h} \\ \hline g \\ \hline\end{array}$ $\begin{array}{|c|}\hline * \\ \hline \tilde{*} \\ \hline\end{array}$ $\begin{array}{|c|}\hline \tilde{*} \\ \hline * \\ \hline\end{array}$ o al tipo II: $\begin{array}{|c|}\hline \tilde{p} \\ \hline p \\ \hline\end{array}$, $\begin{array}{|c|}\hline p \\ \hline \tilde{p} \\ \hline\end{array}$

Quale sarà un gruppo di tessere che può seguire la prima?

Un gruppo del tipo $\begin{array}{|c|}\hline \\ \hline g_{i_1} \\ \hline \end{array}\ \begin{array}{|c|}\hline \\ \hline g_{i_2} \\ \hline \end{array} \cdots \begin{array}{|c|}\hline \\ \hline g_{i_k} \\ \hline \end{array}\ \begin{array}{|c|}\hline \\ \hline * \\ \hline \end{array}$

con $g_{i_1} g_{i_2} \cdots g_{i_k} = u$

Nella parte superiore di tali tessere dovremo necessariamente avere stringhe del tipo $\tilde{s}$, per cui sarà:

$$\begin{array}{|c|}\hline \tilde{h}_{i_1} \\ \hline g_{i_1} \\ \hline \end{array}\ \begin{array}{|c|}\hline \tilde{h}_{i_2} \\ \hline g_{i_2} \\ \hline \end{array} \cdots \begin{array}{|c|}\hline \tilde{h}_{i_k} \\ \hline g_{i_k} \\ \hline \end{array}\ \begin{array}{|c|}\hline \tilde{*} \\ \hline * \\ \hline \end{array}$$

chiamiamo $u_1 = u = g_{i_1} g_{i_2} \cdots g_{i_k}$

e $u_2 = h_{i_1} h_{i_2} \cdots h_{i_k}$

allora sarà, necessariamente, $u_1 \underset{\pi}{\Rightarrow} u_2$

perché le tessere usate corrispondono o a trasformazioni $a \to a$, $b \to b$ oppure a regole di riscrittura.

Iterando il procedimento ci accorgiamo che deve essere

$$w = [u_1 * \tilde{u}_2 \tilde{*} u_3 * \ldots * \tilde{u}_{m-1} \tilde{*} u_m]$$

$$\text{con} \quad u_i \overset{*}{\Rightarrow} u_{i+1} \quad , \; i = 1, \ldots, m-1$$

e quindi abbiamo mostrato che

$$u \underset{\Pi}{\overset{*}{\Rightarrow}} v.$$

Poiché Π ha un problema della parola insolubile possiamo concludere che anche il problema di corrispondenza di Post non è solubile algoritmicamente.