Parte III - Automi

17. Teoria degli automi

Il primo lavoro completo che si conosce su questo argomento è del 1961:

V.M. Glushkov - The abstract theory of automata (testo in russo).

Successivamente sono stati pubblicati altri lavori:

S. Ginsburg - An introduction to mathematical machine thery (1962)

M.A.Arbib - Theory of abstract automata (1969)

Deusseu F - Halbgruppeu und automaten (1971)

Vi sono poi lavori più recenti.

In genere, quando si parla di automa si intende parlare di un "sistema" in cui si possono immettere informazioni, segnali, ecc. che modificano lo stato del sistema, da cui, intanto, vengono emesse informazioni trasformate, segnali, dati ecc.

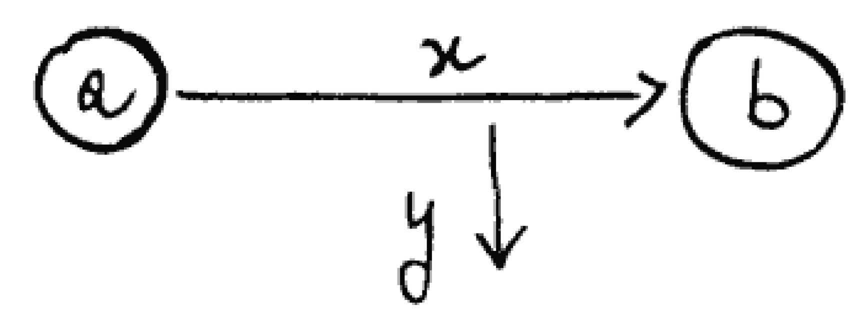
Da un punto di vista assiomatico intendiamo per automa (Automa MEALY) una 5-pla

$$\mathfrak{A} = (A, X, Y, \delta, \lambda)$$

dove A è l'insieme degli stati del sistema, X l'insieme dei segnali di entrata e Y l'insieme di quelli di uscita; δ e λ sono funzioni:

$$\delta: A \times X \longrightarrow A \quad , \quad \lambda: A \times X \longrightarrow Y$$

Ad esempio, se a e b indicano due stati di un sistema e x,y un segnale di entrata ed uno di uscita, $\delta(a,x) = b$ e $\lambda(a,x) = y$, si ha lo schema in figura.

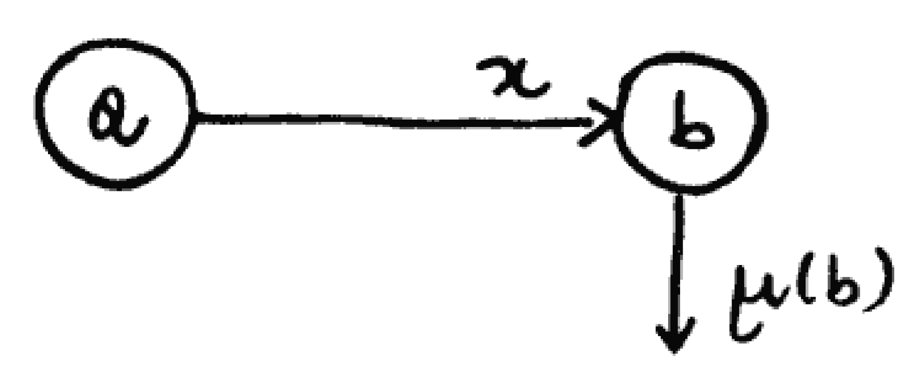


Un automa lo diremo definito perfettamente quando $\delta(a,x)$ è definito per ogni (a,x) e lo diremo deterministico se δ e λ sono funzioni univoche. Parleremo poi di automa stocastico se è possibile dare una funzione di probabilità condizionata $P(a',y \mid a,x)$, che esprime la probabilità che l'automa assuma lo stato a' dopo il segnale y nell'ipotesi che sia nello stato a dopo il segnale x.

Un automa è poi detto di MOORE quando da $\delta(a,x) = \delta(a',x')$ segue $\lambda(a,x) = \lambda(a',x')$. In questo caso il valore di λ dipende solo dallo stato finale $\delta(a,x)$, cioè

$\lambda(a,x) = \mu(\delta(a,x))$ e, ad esprimere ciò, si scrive:

$\mathfrak{A} = (A,X,Y,\delta,\mu)$



Continuiamo a dare altre definizioni.

Un automa lo diciamo iniziale quando uno dei suoi stati, a_0, è distinto dagli altri: $= (A,a_0,X,Y,\delta,\lambda)$; quando $\mathfrak{A} = (A,X,\delta)$, lo diciamo senza segnali di uscita; quando A è finito, $\mathfrak{A}$ si dice A-finito; quando sono finiti anche X e Y, $\mathfrak{A}$ si dice finito.

Un automa $\mathfrak{A}$ con stato iniziale a_0 lo diciamo di <u>ROBIN-SCOTT</u> quando esiste $F \subset A$, $F \not\ni a_0$, i cui elementi sono <u>privilegiati</u> rispetto agli altri stati del sistema.

Un automa finito può essere descritto con una tabella del tipo delle tabelle di Cayley:

$\mathfrak{A}$	a	b	c	...
x				
y				
z			$(\delta(c,z), \lambda(c,z))$	
⋮				

nel punto d'incontro tra la riga z e la colonna c è riportato la coppia di valori $(\delta(c,z),\ \lambda(c,z))$: se l'automa è senza segnale d'uscita va riportato solo il valore $\delta(c,z)$.

Quando l'automa è di Moore si mette in evidenza la funzione μ, come si vede nella tabella seguente.

	μ			
$\mathfrak{A}$	a	b	c	...
x				
y				
z			$\delta(c,z)$	
⋮				

Un automa può essere descritto anche mediante un grafo, come vedremo in qualche esempio.

Prima di dare altre definizioni, richiamiamo il concetto di semigruppo libero.

Se X *è un insieme, indichiamo con* $F(X)$ *l'insieme delle "parole" formali, o sequenze finite, costituite da elementi di* X. *Se*

$p = x_1 x_2 \ldots\ldots x_k \quad , \quad x_i \in X \quad (1 \leq i \leq k)$

$q = y_1 y_2 \ldots\ldots y_\ell \quad , \quad y_i \in X \quad (1 \leq i \leq \ell)$

sono due parole, definiamo il prodotto pq *come segue:*

$pq = x_1 x_2 \ldots\ldots x_k y_1 y_2 \ldots\ldots y_\ell$

Il prodotto è associativo e quindi $F(X)$ *è un semigruppo (*<u>*semigruppo libero con base*</u> X*). Si può aggiungere la "parola vuota",* e *, e si ha allora l'elemento neutro.*

Ora, se $\mathfrak{A} = (A, X, Y, \delta, \lambda)$ *è un automa, possiamo considerare* $F(A)$, $F(X)$, $F(Y)$, *insiemi delle parole di stati, parole di entrata e parole di uscita, rispettivamente. Vogliamo prolungare* δ *e* λ *a* $\bar{\delta}$, $\bar{\lambda}$ *in modo che:*

$\bar{\delta} : A \times F(X) \longrightarrow F(A) \quad \ni' \quad \bar{\delta}(a,e) = a$

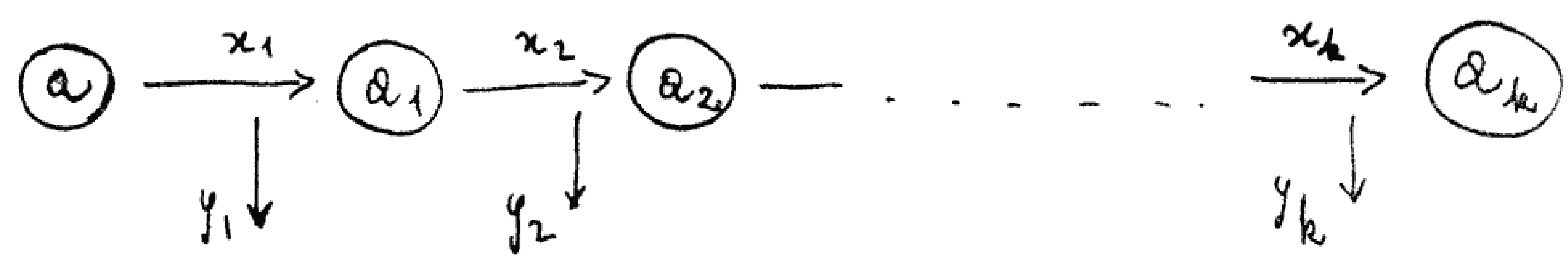
$\bar{\lambda} : A \times F(X) \longrightarrow F(y) \quad \ni' \quad \bar{\lambda}(a,e) = e$

Se $p = x_1 x_2 \ldots\ldots x_k$, *definiamo* $\bar{\delta}(a,p) = a_1 a_2 \ldots\ldots a_k$ *e*

$\bar{\lambda}(a,p) = y_1 y_2 \ldots\ldots y_k$ *dove:*

$a_1 = \delta(a, x_1),\ a_2 = \delta(a_1, x_2),\ \ldots\ldots,\ a_k = \delta(a_{k-1}, x_k)$

$y_1 = \lambda(a, x_1),\ y_2 = \lambda(a_1, x_2),\ \ldots\ldots,\ y_k = \lambda(a_{k-1}, x_k)$



Per brevità indicheremo spesso con ap lo stato finale.

Tale automa si dice <u>sequenziale</u>.

Si dice che un automa ha un <u>sistema B di generatori per A</u> $(B \subset A)$ quando per ogni stato $a \in A$ è : $a = bp$ con b e p opportuni elementi di B e $F(X)$ rispettivamente.

$\mathfrak{A}$ si dice <u>ciclico</u> quando esiste un sistema di generatori costituito da un solo elemento. Un automa iniziale si dice <u>connesso inizialmente</u> quando lo stato iniziale a_0 genera A. Un automa ciclico si dice <u>connesso fortemente</u> quando ogni stato genera A.

Un automa $\mathfrak{A} = (A,F,\delta)$, con F semigruppo, si dice <u>quasi-automa</u> quando :

$$\delta(a,fg) = \delta\big(\delta(af),g\big) \qquad \text{per ogni} \quad a \in A \quad \text{e} \quad f,g \in F$$

<u>18. Esempi di automi</u>

1) Poniamo : $A = \{a,b,c,d\}$, $X = \{x,y\}$, $Y = \{u,v\}$

$\delta(b,x) = a$

$\delta(a,x) = \delta(c,x) = \delta(d,y) = b$

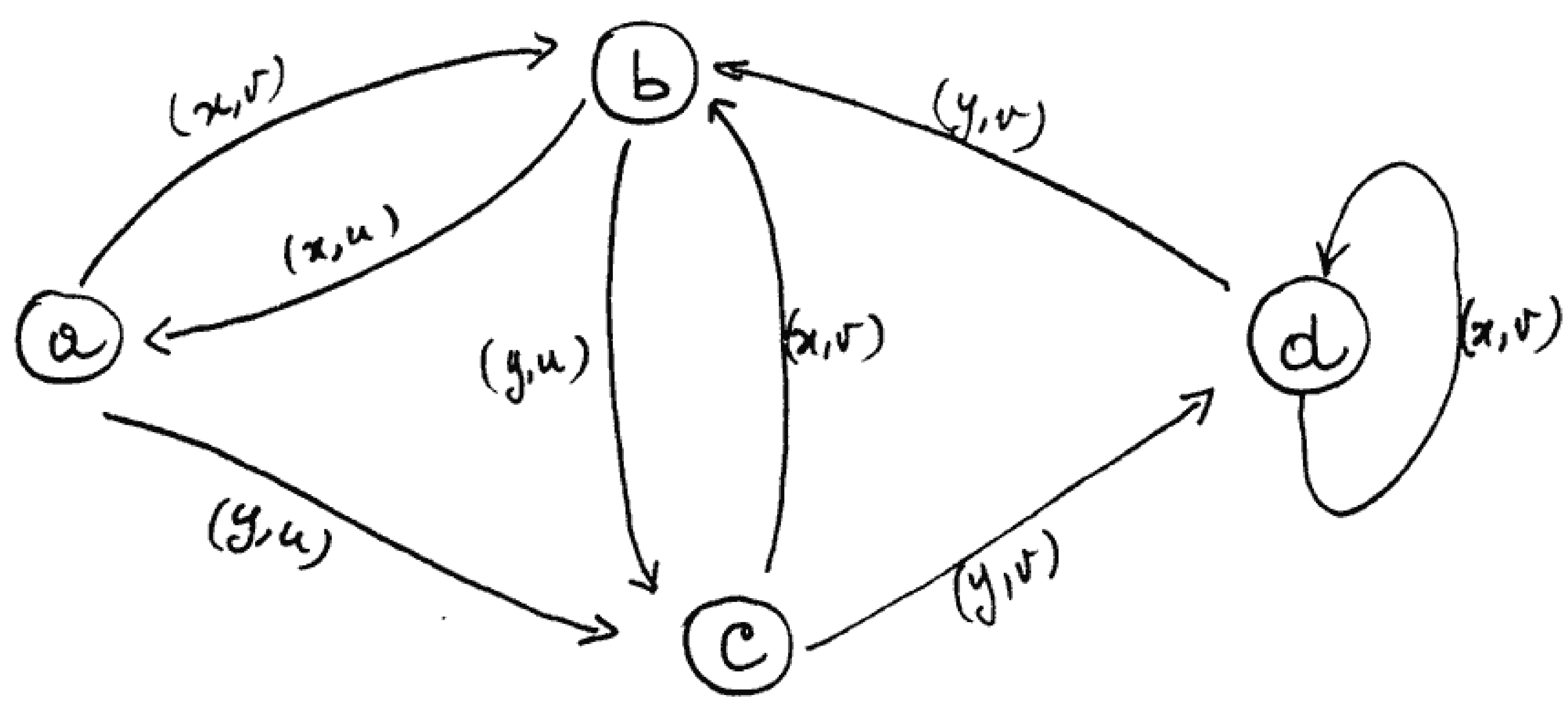
$$\delta(a,y) = \delta(b,y) = c$$

$$\delta(c,y) = \delta(d,x) = d$$

$$\lambda(a,y) = \lambda(b,x) = \lambda(b,y) = u$$

$$\lambda(a,x) = \lambda(c,x) = \lambda(c,y) = \lambda(d,x) = \lambda(d,y) = v$$

$\mathfrak{A} = (A,X,Y,\delta,\lambda)$ *è un automa di Moore il cui grafo è:*



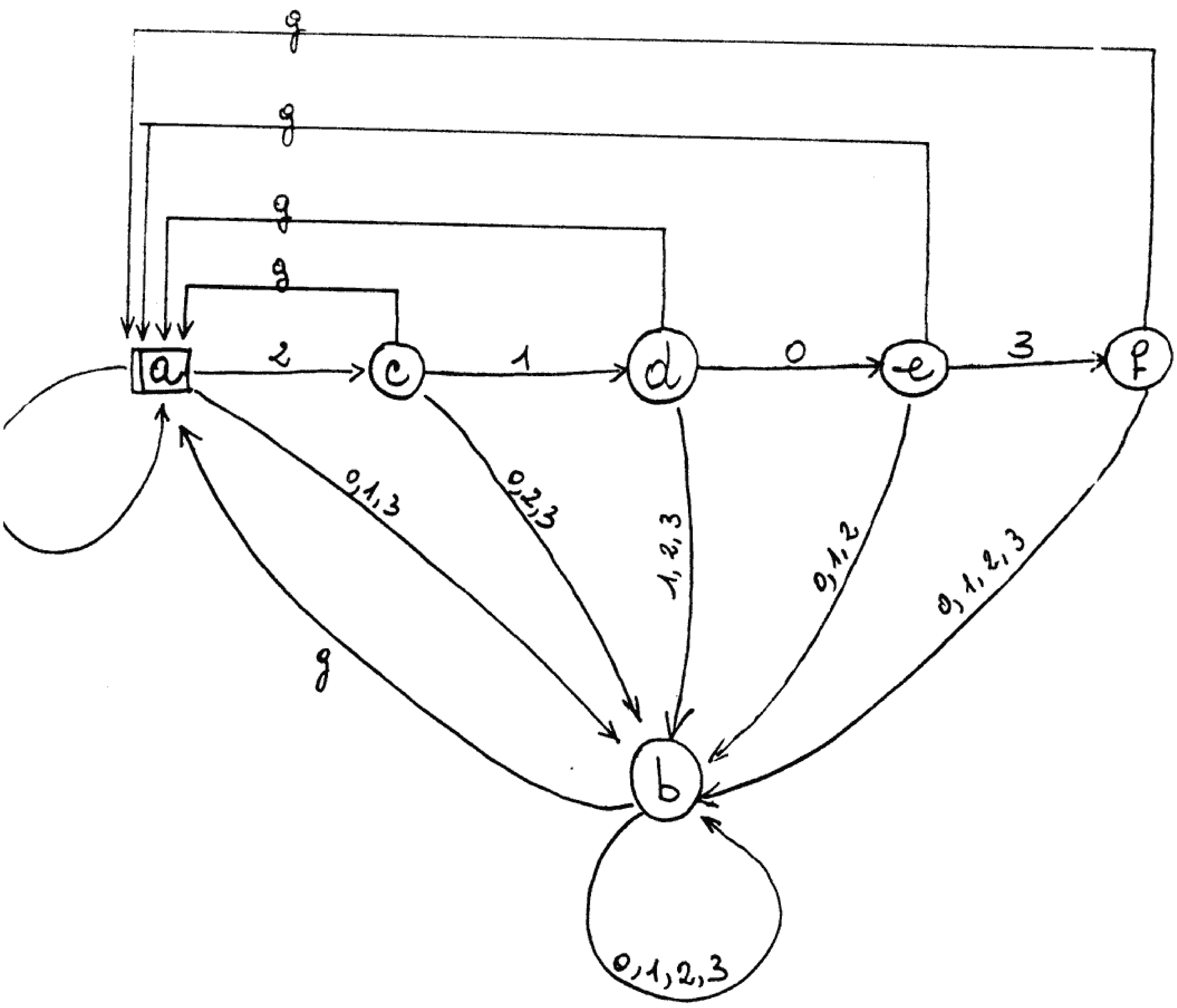
e la cui tabella è:

$\mathfrak{A}$	u	v	u	v
	a	b	c	d
x	b	a	b	d
y	c	c	d	b

2) Sia $A = \{a,b,c,d,e,f\}$, $X = \{0,1,2,3,g\}$, $F = \{f\}$

$\mathfrak{A} = (A,a,X,\delta;F)$, *in cui* δ *sarà definita mediante il grafo,*

è un automa di ***Robin-Scott***. *Il suo grafo è:*



Questo grafo rappresenta lo schema della serratura di sicurezza di una cassaforte per la quale f *è l'unico stato in cui la cassaforte può essere aperta; la combinazione che sblocca la serratura è* 2-1-0-3; g *rappresenta il segnale "premere il pulsante".*

3) *Sia* $B = \{b_1, b_2, \dots b_m\}$, $X = \{x_1, x_2, \dots x_n\}$ *ed* A *l'insieme delle espressioni formali del tipo:*

$b_i x_{i_1} x_{i_2} \dots\dots x_{i_k}$, $b_i \in B$, $x_{i_1}, \dots, x_{i_k} \in X$

Per queste espressioni supponiamo che:

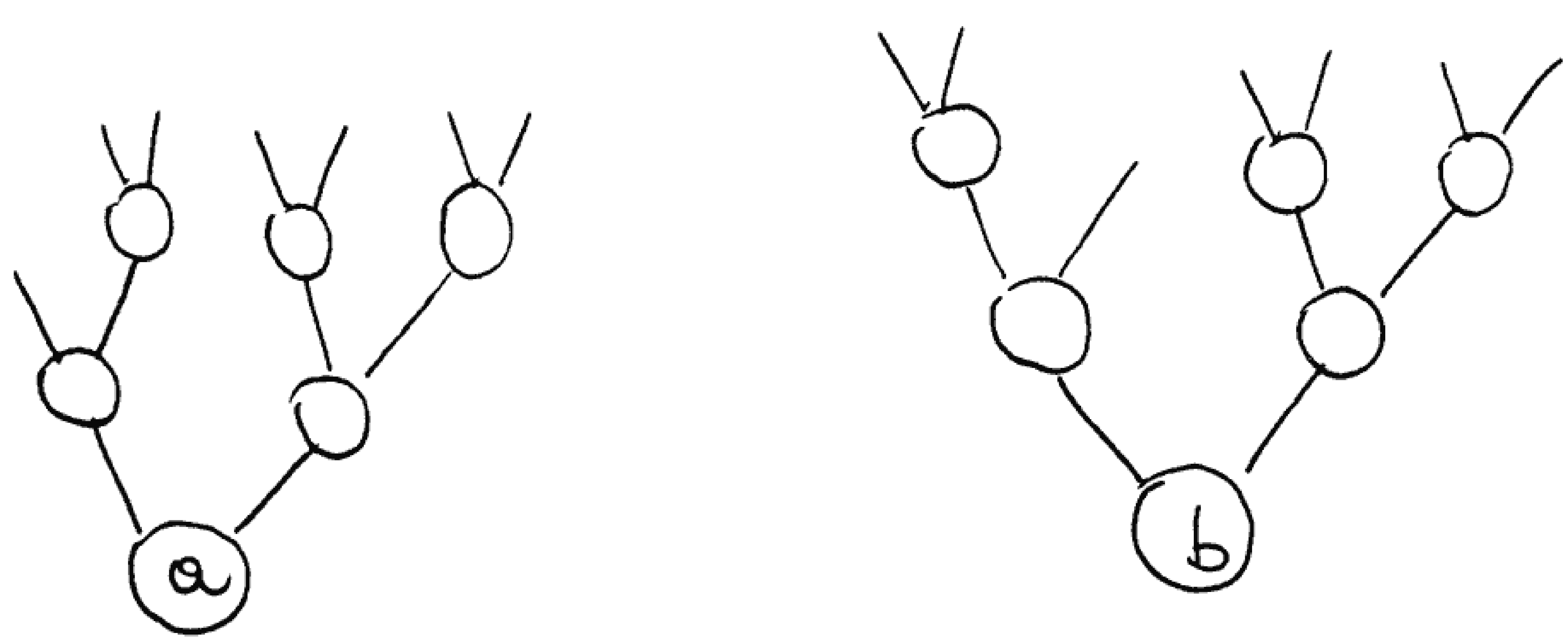
$$b_i x_{i_1} x_{i_2} \ldots\ldots x_{i_k} = b_j x_{j_1} x_{j_2} \ldots\ldots x_{j_\ell} \Leftrightarrow b_i = b_j,\ k = \ell\ ,\ x_{i_1} = x_{j_1},\ \ldots\ldots$$

Posto $\delta(b_i x_{i_1} x_{i_2},\ \ldots\ldots,\ x_{i_k},\ x_j) = b_j x_{i_1} \ldots\ldots x_{i_k} x_j$

si ha che:

$\mathfrak{A} = (A, X, \delta)$ *è un automa* (*automa libero*)

Se $B = \{a, b\}$ *e* $X = \{x, y\}$, *il grafo dell'automa è del tipo detto* *ad albero*:



19. *Sottoautomi, automi superiori, automi inferiori*

Per gli automi possono introdursi certi concetti usuali delle strutture algebriche.

Siano $\mathfrak{A} = (A, X, Y, \delta, \lambda)$ *e* $\mathfrak{A}' = (A', X', Y', \delta', \lambda')$ *due automi. Si* dice che $\mathfrak{A}'$ è sottoautoma di $\mathfrak{A}$ se $A'\subseteq A$, $X'\subseteq X$, $Y'\subseteq Y$ e δ',λ' sono le restrizioni di δ e λ rispettivamente. Se almeno uno degli insiemi A',X',Y' è incluso propriamente in A,X,Y, diciamo che $\mathfrak{A}'$ è sottoautoma proprio di $\mathfrak{A}$. Se $A'\subset A$, $X'=X$, $Y'=Y$ allora $\mathfrak{A}'$ si dice A-sottoautoma di $\mathfrak{A}$.

Un sottoautoma $\mathfrak{A}'$ di $\mathfrak{A}$ si dice iniziale quando l'eventuale stato iniziale di A è anche stato iniziale di A'.

Sia ora $B\subseteq A$· chiamiamo A' l'insieme di tutti gli stati del tipo bp con $b\in B$ e $p\in F(X)$; allora $\mathfrak{A}' = (A',X,Y,\delta,\lambda)$ è un automa che viene detto sottoautoma generato da B.

Sia $\mathfrak{A} = (A,X,\delta)$ un automa senza segnali di uscita; chiamiamo centro dell'automa l'automa $\mathfrak{A}' = (A,X',\delta)$ dove:

$$X' = \{x \in X \mid axy = ayx, \quad \text{per ogni} \quad a \quad \text{e per ogni} \quad y\}$$

Introduciamo ora il concetto di omomorfismo d'automi.

Siano $\mathfrak{A} = (A,X,Y,\delta,\lambda)$, $\mathfrak{A}' = (A',X',Y'\delta',\lambda')$ due automi.

Diciamo che le applicazioni $h_1: A \to A'$, $h_2: X \to X'$, $h_3: Y \to Y'$ costituiscono un omomorfismo da $\mathfrak{A}$ in $\mathfrak{A}'$ se accade:

$$h_1(\delta(a,x)) = \delta'(h_1(a),h_2(x))$$

$$h_3(\lambda(a,x)) = \lambda'(h_1(a),h_2(x)).$$

Evidente è la definizione di isomorfismo di automi.

Se esiste un omomorfismo da un automa $\mathfrak{A}$ su un automa $\mathfrak{A}'$, diciamo che $\mathfrak{A}'$ è <u>immagine omomorfa di $\mathfrak{A}$</u>.

Siano $\mathfrak{A}$ ed $\mathfrak{A}'$ due automi tali che $X = X'$ e $Y = Y'$; una applicazione $h: A \longrightarrow A'$ si dice <u>A-omomorfismo da $\mathfrak{A}$ in $\mathfrak{A}'$</u> se accade che:

$$h(\delta(a,x)) = \delta'(h(a),x)$$

$$\lambda(a,x) = \lambda'(h(a),x)$$

(in questo caso il ruolo di h_2 e h_3 è svolto evidentemente dalle identità in X e Y rispettivamente).

<u>Esempio</u>

Siano $\mathfrak{A}$ ed $\mathfrak{A}'$ due automi le cui tabelle sono:

$\mathfrak{A}$	a	b	c	d
x	(b,u)	(a,u)	(d,u)	(a,u)
y	(c,v)	(d,u)	(a,u)	(c,v)

$\mathfrak{A}'$	1	2	3
x	(2,u)	(1,u)	(1,u)
y	(2,v)	(3,v)	(2,v)

e sia $h: A \longrightarrow A'$ così definita:

$$h(a)=1, \quad h(b)=h(c)=2, \quad h(d) = 3$$

Si può verificare che h è un A-omomorfismo, $\mathfrak{A}'$ è un'immagine omomorfa di $\mathfrak{A}$ ma, mentre $\mathfrak{A}$ è di Moore, $\mathfrak{A}'$ non lo è.

Come mostra l'esempio precedente, un omomorfismo tra automi non "conserva" la proprietà di "essere di Moore". Così, se $\mathcal{A}$ ed $\mathcal{A}'$ sono di Moore, per mettere in evidenza questo fatto, si può far vedere che un omomorfismo "conserva" la proprietà di "essere di Moore" se accade che:

$$h_1(\delta(a,x)) = \delta'(h_1(a),h_2(x))$$

$$h_3(\mu(a)) = \mu'(h_1(a))$$

In maniera abbastanza ovvia si può parlare di endomorfismi di un automa in sè, di automorfismi, ecc..

Si può anche dimostrare che gli endomorfismi di un automa in sè formano semigruppo con la usuale operazione di prodotto.

Passiamo ora ad introdurre il concetto di automa fattoriale.

Diciamo che una relazione di equivalenza R (in A) è una <u>congruenza</u> se:

$$aRb \Longrightarrow \delta(a,x) \; R \; \delta(b,x) \wedge \lambda(a,x) = \lambda(b,x) \qquad \text{per ogni} \quad x \in X.$$

Se R è una confruenza, indicato con A_R l'insieme delle classi di equivalenza di elementi di A, definiamo:

$$\hat{\mathcal{A}} = (A_R, X, Y, \hat{\delta}, \hat{\lambda})$$

dove $\hat{\delta}([a], x) = [\delta(a,x)]$

$\hat{\lambda}([a], x) = \lambda(a,x)$

Si può provare che la definizione è ben posta e che $\hat{\mathfrak{A}}$ è un automa, che definiamo <u>automa fattoriale</u> e indichiamo con $\mathfrak{A}/R$.

A questo proposito si può provare un importante teorema.

<u>Teorema 19.1</u>

Sia $\mathfrak{A}$ un automa ed R una congruenza su A. Allora $\mathfrak{A}/R$ è immagine omomorfa di $\mathfrak{A}$; viceversa se l'automa $\mathfrak{A}'$ è immagine omomorfa di $\mathfrak{A}$, esiste una congruenza R tale che $\mathfrak{A}' = \mathfrak{A}/R$.
(Omettiamo la dimostrazione).

Vogliamo ora introdurre il concetto di applicazione d'automa e di automa inferiore e superiore.

Sia $p = x_1x_2\ldots\ldots x_k \in F(X)$; diciamo che $x_1x_2\ldots\ldots x_i\,(i \leq k)$ è una <u>parte iniziale</u> di p; se $p = p_1qp_2$, q non vuoto e $\neq p$, diciamo che q è una <u>sottoparte propria</u> di p.

Sia ora $a \in A$; definiamo una applicazione $\alpha_a : F(X) \longrightarrow F(Y)$ in modo che: $\alpha_a(p) = \lambda(a,p)$.

Se a è lo stato iniziale di $\mathfrak{A}$, si scrive $\alpha_{\mathfrak{A}}$ invece di α_a e si dice che è <u>applicazione indotta da $\mathfrak{A}$</u>.

Una applicazione $\alpha : F(X) \longrightarrow F(Y)$ si chiama <u>applicazione d'automa</u> se esiste un automa iniziale $\mathfrak{A}$ che induce α (cioè tale che $\alpha = \alpha_{\mathfrak{A}}$).

Le applicazioni d'automa sono caratterizzate dal seguente teorema:

Teorema 19.2

Una applicazione $\alpha' \cdot F(X) \longrightarrow F(Y)$ è una applicazione d'automa se e solo se:

i) α conserva la lunghezza di ogni parola;

ii) l'immagine di ogni parte iniziale è ancora una parte iniziale.

Omettiamo la dimostrazione del teorema, ma interessa rilevare che nella dimostrazione si usa una applicazione $\alpha_p : F(X) \longrightarrow F(Y)$ tale che $\alpha(pq) = \alpha(p)\alpha_p(q)$. Applicazioni di questo tipo, dette stati dell'applicazione α, ci portano ad introdurre il concetto di automa inferiore nel modo seguente.

Sia A_α l'insieme degli stati α_p di una applicazione α, al variare di p in $F(X)$. Si può provare allora che $\mathcal{U}_\alpha=(A_\alpha, \alpha, X,Y,\delta_\alpha, \lambda_\alpha)$, dove $\delta_\alpha(\alpha_p,x) = \alpha_{px}$, $\lambda_\alpha(\alpha_p,x) = \alpha_p(x)$, è un automa, detto automa inferiore di α.

Anche $\mathcal{U}^\alpha = (F(X), e\ X,Y,\delta^\alpha,\lambda^\alpha)$, dove $\delta^\alpha(p,x) = px$, $\lambda^\alpha(p,x) = \overbrace{\alpha(px)}$, è un automa, detto automa superiore di α (con $\overbrace{\alpha(p\ x)}$ intendiamo l'ultima lettera di $\alpha(p\ x)$.

A questo punto è possibile enunciare il

Teorema 19.3

Se α è una applicazione d'automa e $\mathcal{U}$ è connesso inizialmente, allora $\mathfrak{U}_\alpha$ è immagine omomorfa di $\mathfrak{U}$ che, a sua volta, è immagine omomorfa di $\mathfrak{U}^\alpha$.

20. Esempio

Sia $X = \{x,y\}$, $Y = \{u,v,w\}$ e $\alpha : F(X) \longrightarrow F(Y)$ con le condizioni

i) $\alpha(e) = e$

ii) $\alpha(x^k) = u^k$ $(k \geq 1)$;

iii) $\alpha(y^k) = v^k$ $(k \geq 1)$;

iv) $p = x^k yq \Longrightarrow \alpha(p) = u^k w^{m+1}$ dove m è la lunghezza di q;

v) $p = y^k x\, q \Longrightarrow \alpha(p) = v^k w^{m+1}$ dove m è la lunghezza di q.

Determiniamo gli stati di α ; si ha:

$$\alpha(x^{k+1}) = u^{k+1} = \alpha(x)\alpha_x(x^k) = u\alpha_x(x^k)$$

$$\alpha(xy^k) = uw^k = \alpha(x)\alpha_x(y^k) = u\alpha_x(y^k)$$

$$\alpha(xx^k yq) = u^{k+1}w^{m+1} = \alpha(x)\alpha_x(x^k yq) = u\alpha_x(x^k yq)$$

$$\alpha(xy^k xq) = uw^{k+m+1} = \alpha(x)\alpha_x(y^k xq) = u\alpha_x(y^k xq)$$

Quindi α_x è definita come segue:

$$\alpha_x : \begin{cases} e \longrightarrow e \\ x^k \longrightarrow u^k \\ y^k \longrightarrow w^k \\ x^k yq \longrightarrow u^k w^{m+1} \\ y^k xq \longrightarrow w^{k+m+1} \end{cases}$$

Pertanto $\alpha_x \neq \alpha$ *in quanto, ad esempio,* $\alpha(y^k) = v^k$ *mentre* $\alpha_x(y^k) = w^k$.

Facendo dei conti analoghi per α_{x^2} *, si vede che* $\alpha_x = \alpha_{x^2}$.

Continuando a fare conti si prova che:

$$A_\alpha = \{\alpha , \alpha_x , \alpha_y , \alpha_{xy}\}$$

dove:

$$\alpha_y : \begin{cases} e \longrightarrow e \\ x^k \longrightarrow w^k \\ y^k \longrightarrow v^k \\ x^k yq \longrightarrow w^{k+m+1} \\ y^k xq \longrightarrow v^k w^{m+1} \end{cases}$$

$$\alpha_{xy}: \begin{cases} e \longrightarrow e \\ x^k \longrightarrow w^k \\ y^k \longrightarrow w^k \\ x^k yq \longrightarrow w^{k+m+1} \\ y^k xq \longrightarrow w^{k+m+1} \end{cases}$$

Possiamo quindi considerare l'automa inferiore $\mathfrak{A}_\alpha$, che risulta essere un automa di Moore.

La sua tabella è:

$\mathfrak{A}_\alpha$	α	α_x	α_y	α_{xy}
x	(α_x, u)	(α_x, u)	(α_{xy}, w)	(α_{xy}, w)
y	(α_y, v)	(α_{xy}, w)	(α_y, v)	(α_{xy}, w)

Osserviamo che il grafo di $\mathfrak{A}_\alpha$ è un <u>grafo ad albero</u>.