

Curs 5

II.2.3 Acțiuni ale monoizilor

Observația II.2.3.1. Fie (M, \cdot, e) un monoid. Atunci M , împreună cu operația binară $m \cdot_{op} n = n \cdot m, \forall m, n \in M$, formează un monoid cu același element neutru e , numit monoidul opus lui M și notat M^{op} . Dacă M este comutativ, atunci clar M^{op} coincide cu M . Dacă M este grup, atunci funcția $M \rightarrow M^{op}, m \mapsto m^{-1}$ este un izomorfism de monoizi. Dacă M nu este grup și nici comutativ, atunci monoizii M și M^{op} nu mai sunt neapărat izomorfi.

Exemplul II.2.3.2. Fie $M = \{e, a, b\}$ cu operația binară $a \cdot a = a \cdot b = a$, $b \cdot a = b \cdot b = b$ și elementul neutru e . Se verifică ușor că M este un monoid necomutativ. Dacă ar exista un izomorfism $f : M \rightarrow M^{op}$, atunci f trebuie să fie bijectivă și $f(e) = e$. Există numai două cazuri posibile: $f = \mathbf{1}_M$ sau

$$f(a) = b, \quad f(b) = a$$

Dar $\mathbf{1}_M : M \rightarrow M^{op}$ nu e morfism de monoizi. Rămâne deci al doilea caz. Din condiția $f(a \cdot b) = f(a) \cdot_{op} f(b) = f(b) \cdot f(a)$, rezultă $b = f(a) = f(a \cdot b) = f(b) \cdot f(a) = a \cdot b = a$, fals.

Definiția II.2.3.3. Fie (M, \cdot, e) un monoid și X o mulțime. Spunem că M acționează pe X la dreapta (sau că X este o M -mulțime) dacă există o funcție $\delta : X \times M \rightarrow X$ astfel încât:

$$(A1) \quad \delta(x, e) = x, \forall x \in X.$$

$$(A2) \quad \delta(x, m \cdot n) = \delta(\delta(x, m), n), \forall x \in X, m, n \in M.$$

Vom nota $\delta(x, m) = x \triangleleft m$; spunem că elementul $m \in M$ acționează pe $x \in X$ prin $x \triangleleft m \in X$. Relațiile (A1) - (A2) se scriu atunci:

$$x \triangleleft e = x \text{ și } x \triangleleft (m \cdot n) = (x \triangleleft m) \triangleleft n$$

Exemplul II.2.3.4. (i) Fie (M, \cdot, e) un monoid și X o mulțime. Atunci funcția $\delta : X \times M \rightarrow X$, $\delta(x, m) = x$ (deci scriem $x \triangleleft m = x$), definește o acțiune a lui M pe X , numită acțiune trivială: prin construcție, avem $x \triangleleft e = x$ și $(x \triangleleft m) \triangleleft n = x \triangleleft n = x = x \triangleleft (m \cdot n)$, pentru orice $x \in X, m, n \in M$.

(ii) Fie (M, \cdot, e) un monoid. Atunci operația binară " \cdot " pe M determină o acțiune a monoidului pe el însuși $\delta : M \times M \rightarrow M$, $\delta(x, m) = x \cdot m$, $\forall x, m \in M$, numită acțiune regulată (deci scriem $x \triangleleft m = x \cdot m$). Axiomele **(A1)**-**(A2)** sunt verificate: $x \triangleleft e = x \cdot e = x$ și $(x \triangleleft m) \triangleleft n = (x \cdot m) \cdot n = x \cdot (m \cdot n) = x \triangleleft (m \cdot n)$.

(iii) Fie (M, \cdot, e) monoid și X o mulțime pe care M acționează la dreapta prin $X \times M \rightarrow X$, $(x, m) \mapsto x \triangleleft m$. Atunci funcția $\mathcal{P}(X) \times M \rightarrow \mathcal{P}(X)$, $(A, m) \mapsto A \triangleleft m = \{x \triangleleft m \mid x \in A\}$, $\forall A \subseteq X, m \in M$, definește o acțiune a lui M pe mulțimea părților lui X . Verificăm:

$$\begin{aligned} A \triangleleft e &= \{x \triangleleft e \mid x \in A\} \\ &= \{x \mid x \in A\} \\ &= A \\ (A \triangleleft m) \triangleleft n &= \{x \triangleleft m \mid x \in A\} \triangleleft n \\ &= \{(x \triangleleft m) \triangleleft n \mid x \in A\} \\ &= \{x \triangleleft (m \cdot n) \mid x \in A\} \\ &= A \triangleleft (m \cdot n) \end{aligned}$$

Exercițiul II.2.3.5. Dacă (M, \cdot, e) este un monoid și X o mulțime pe care M acționează la dreapta, atunci M acționează și pe produsul cartezian $X^n = \underbrace{X \times \dots \times X}_{n \text{ ori}}$, $\forall n \in \mathbb{N}^*$.

II.2.4 Submonoidi. Morfisme de monoizi. Monoid factor

Definiția II.2.4.1. Fie (M, \cdot, e) un monoid și $N \subseteq M$. Spunem că N este un submonoid dacă:

(S1) $e \in N$.

(S2) $\forall m, n \in N \implies m \cdot n \in N$.

Orice submonoid este în particular un monoid cu operația binară indusă, dar nu orice submulțime a unui monoid care este la rândul său monoid cu operația

indusă este submonoid. De exemplu, fie $M = (\{a, b\}, \circ, \mathbf{1}_{\{a,b\}})$ monoidul tuturor funcțiilor $\{a, b\} \rightarrow \{a, b\}$ cu operația de compunere. Luăm $N = \{f_a\}$, unde f_a este funcția constantă în a . Atunci $f_a \circ f_a = f_a$, deci N este monoid în raport cu compunerea, dar N nu e submonoid deoarece $\mathbf{1}_{\{a,b\}} \notin N$.

Observația II.2.4.2. Fie $N \subseteq M$ submonoid și X o mulțime pe care M acționează la dreapta prin $\delta : X \times M \rightarrow X$. Atunci restricția lui δ la N , $\delta|_{X \times N} : X \times N \rightarrow X$ definește o acțiune a lui N pe X .

Fie (M, \cdot, e) un monoid și $X, Y \subseteq M$. Produsul submulțimilor X, Y este submulțimea

$$X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\}$$

Se obține astfel o operație binară pe mulțimea submulțimilor lui M $\mathcal{P}(M)$; $\mathcal{P}(M)$, împreună cu această operație formează un monoid cu elementul neutru $\{e\}$ și element zero \emptyset . De remarcat că dacă $N \subseteq M$ este submonoid, atunci N este element idempotent (adică $N \cdot N = N$) în $\mathcal{P}(M)$ (exercițiu!).

Reamintim: fie A o mulțime, pe care o vom numi *alfabet*. Un *string* α (de lungime n) este un element din $A^n = \underbrace{A \times \dots \times A}_n, \forall n \in \mathbb{N}^*$, scris

$\alpha = a_1 \dots a_n$, fără paranteze sau virgulă. Convenim existența unui string vid (de lungime 0), notat ϵ . Mulțimea tuturor stringurilor se va nota A^* (formal, $A^* = \cup A^n, n \geq 0$, unde $A^0 = \{\epsilon\}$). Pe A^* , definim o operație numită *concatenare* prin:

$$\alpha \cdot \beta = a_1 \dots a_n b_1 \dots b_m$$

dacă $\alpha = a_1 \dots a_n \in A^*$, $\beta = b_1 \dots b_m \in A^*$. De asemenea, convenim că

$$\alpha \cdot \epsilon = \epsilon \cdot \alpha, \forall \alpha \in A^*$$

Atunci (A^*, \cdot, ϵ) devine un monoid, numit *monoidul liber* peste A .

Definiția II.2.4.3. Fie $(M, \cdot, e_M), (N, \cdot, e_N)$ monoizi. O funcție $f : M \rightarrow N$ se numește morfism de monoizi dacă:

$$(M1) \quad f(e_M) = f(e_N)$$

$$(M2) \quad f(mm') = f(m)f(m'), \forall m, m' \in M$$

Un izomorfism de monoizi este un morfism bijectiv.

Exemplul II.2.4.4. Funcția $l : A^* \rightarrow \mathbb{N}, l(\alpha) = |\alpha|$ este un morfism de monoizi, căci $|\epsilon| = 0$ și $|\alpha\beta| = |\alpha| + |\beta|, \forall \alpha, \beta \in A^*$. Dacă $A = \{a\}$, atunci l este chiar un izomorfism.

Observația II.2.4.5. Fie $f : M \longrightarrow N$ un morfism de monoizi. Atunci pentru orice $M' \subseteq M$ submonoid, $f(M') \subseteq N$ este submonoid. Reciproc, dacă $N' \subseteq N$ e submonoid, atunci $f^{-1}(N') \subseteq M$ e submonoid. În particular, dacă luăm $M' = M$, obținem că $\text{Im} f$ e submonoid în N .

Demonstrație. Reamintim că $f(M') = \{f(m) \mid m \in M'\}$ și $f^{-1}(N') = \{m \in M \mid f(m) \in N'\}$. Arătăm acum că $f(M')$ e submonoid: cum $e_N = f(e_M)$ și $e_M \in M'$ (M' este submonoid), rezultă $e_N \in f(M')$. Acum, fie $m, m' \in M'$. Atunci $f(m)f(m') = f(m \cdot m') \in f(M')$ deoarece $m \cdot m' \in M'$. Treceam la a doua afirmație, privind $f^{-1}(N')$: $f(e_M) = e_N \in N'$, deci $e_M \in f^{-1}(N')$. Dacă $m, m' \in f^{-1}(N')$, atunci $f(m) \cdot f(m') \in N'$. Dar N' e submonoid, deci $f(m \cdot m') = f(m) \cdot f(m') \in N'$, adică $m \cdot m' \in f^{-1}(N')$. \square

Definiția II.2.4.6 (Congruență). O relație de echivalență \mathcal{R} pe monoidul M se numește congruență dacă

$$(C) \quad m\mathcal{R}m' \implies (m \cdot n)\mathcal{R}(m' \cdot n) \text{ și } (n \cdot m)\mathcal{R}(n \cdot m'), \forall m, m', n \in M.$$

Reamintim că fiecărei relații de echivalență \mathcal{R} îi corespunde o partiție a monoidului M în clase de echivalență $([m]_{\mathcal{R}})_{m \in M}$, unde $[m]_{\mathcal{R}} = \{n \in M \mid m\mathcal{R}n\}$. Mulțimea claselor de echivalență s-a notat cu M/\mathcal{R} și se numește mulțimea factor.

Exemplul II.2.4.7. Pe A^* luăm relația

$$\alpha\mathcal{R}\beta \iff |\alpha| = |\beta|$$

Este în mod evident o relație de echivalență; în plus, pentru orice $\gamma \in A^*$, $|\alpha\gamma| = |\alpha| + |\gamma| = |\beta| + |\gamma| = |\beta\gamma|$ și analog $|\gamma\alpha| = |\gamma\beta|$, deci \mathcal{R} este o congruență.

Dacă $|\alpha| = n$, atunci $[\alpha]_{\mathcal{R}} = \{\beta \in A^* \mid \alpha\mathcal{R}\beta\} = A^n$ este mulțimea tuturor stringurilor de lungime n .

Dacă (M, \cdot, e) este un monoid și \mathcal{R} o congruență pe M , atunci putem defini o operație binară pe mulțimea factor M/\mathcal{R} prin:

$$[m]_{\mathcal{R}} \cdot [m']_{\mathcal{R}} = [m \cdot m']_{\mathcal{R}}, \forall m, m' \in M$$

Această definiție nu depinde de reprezentanții claselor de echivalență: dacă $[m]_{\mathcal{R}} = [n]_{\mathcal{R}}$ și $[m']_{\mathcal{R}} = [n']_{\mathcal{R}}$, atunci $m\mathcal{R}n$ și $m'\mathcal{R}n'$. Rezultă $m \cdot m'\mathcal{R}n \cdot n'$ și $n \cdot m'\mathcal{R}n \cdot n'$, de unde $m \cdot m'\mathcal{R}n \cdot n'$, adică $[m \cdot m']_{\mathcal{R}} = [n \cdot n']_{\mathcal{R}}$. Mai mult, operația astfel definită este asociativă și admite elementul neutru $[e]_{\mathcal{R}}$ (exercițiu!), deci $(M/\mathcal{R}, \cdot, [e]_{\mathcal{R}})$ este un monoid. Fie $\pi_{\mathcal{R}} : M \longrightarrow M/\mathcal{R}$ funcția care asociază fiecărui element clasa sa de echivalență: $\pi_{\mathcal{R}}(m) = [m]_{\mathcal{R}}$ ($\pi_{\mathcal{R}}$ se numește *surjecție canonică*). Atunci $\pi_{\mathcal{R}}$ este surjectivă (de ce?) și morfism de monoizi: $\pi_{\mathcal{R}}(e) = [e]_{\mathcal{R}}$ prin construcție și $\pi_{\mathcal{R}}(m \cdot m') = [m \cdot m']_{\mathcal{R}} = [m]_{\mathcal{R}}[m']_{\mathcal{R}} = \pi_{\mathcal{R}}(m)\pi_{\mathcal{R}}(m')$, $\forall m, m' \in M$.

Congruență nucleară. Fie $f : M \rightarrow N$ o funcție. Considerăm relația $m\mathcal{R}_f m' \iff f(m) = f(m'), \forall m, m' \in M$. Atunci \mathcal{R}_f este o relație de echivalență, ale cărei clase vor fi $(f^{-1}(n))_{n \in \text{Im} f}$. Dacă M, N sunt monoizi și f este morfism, atunci \mathcal{R}_f este chiar o congruență: fie $m, m' \in M$ astfel încât $m\mathcal{R}_f m'$. Atunci $f(m) = f(m')$. Dacă $n \in M$, avem $f(m \cdot n) = f(m) \cdot f(n) = f(m') \cdot f(n) = f(m' \cdot n)$, deci $(m \cdot n)\mathcal{R}_f(m' \cdot n)$ și analog la stânga.

Să remarcăm că dacă \mathcal{R} este o congruență atunci congruența asociată surjecției canonice $\pi_{\mathcal{R}}$ este chiar \mathcal{R} : dacă $m\mathcal{R}_{\pi_{\mathcal{R}}} m'$, atunci $\pi_{\mathcal{R}}(m) = \pi_{\mathcal{R}}(m')$, deci $[m]_{\mathcal{R}} = [m']_{\mathcal{R}}$, echivalent cu $m\mathcal{R} m'$. În consecință, a da o congruență \mathcal{R} pe un monoid M este același lucru cu a da un morfism de monoizi cu domeniul M (pornind de la congruența \mathcal{R} , obținem morfismul de monoizi $\pi_{\mathcal{R}}$; invers, dacă $f : M \rightarrow N$ este un morfism de monoizi, atunci obținem congruența \mathcal{R}_f).

Teorema II.2.4.8. Fie $f : M \rightarrow N$ un morfism de monoizi. Atunci funcția $\tilde{f} : M/\mathcal{R}_f \rightarrow N$, $\tilde{f}([m]_{\mathcal{R}_f}) = f(m)$ este un morfism injectiv de monoizi cu imaginea $\text{Im} f$. În particular, rezultă că există un izomorfism de monoizi

$$M/\mathcal{R}_f \cong \text{Im} f$$

Demonstrație. Arătăm mai întâi că \tilde{f} e bine definită și injectivă: dacă $[m]_{\mathcal{R}_f} = [m']_{\mathcal{R}_f}$, atunci $m\mathcal{R}_f m'$, de unde $f(m) = f(m')$. \tilde{f} e morfism de monoizi:

$$\tilde{f}([m]_{M\mathcal{R}_f}) = f(e) = e$$

și

$$\begin{aligned} \tilde{f}([m]_{\mathcal{R}_f} \cdot [m']_{\mathcal{R}_f}) &= \tilde{f}([m \cdot m']_{\mathcal{R}_f}) \\ &= f(m \cdot m') \\ &= f(m) \cdot f(m') \\ &= \tilde{f}([m]_{\mathcal{R}_f}) \cdot \tilde{f}([m']_{\mathcal{R}_f}) \end{aligned}$$

Din construcție, $\text{Im} \tilde{f} = \text{Im} f$, deci avem izomorfismul $M/\mathcal{R}_f \cong \text{Im} f$. \square

Exemplul II.2.4.9. Fie $A = \{a, b\}$ și $M = A^*$. Am văzut mai devreme că funcția $l : A^* \rightarrow \mathbb{N}$, $l(\alpha) = |\alpha|$ este un morfism de monoizi (surjectiv). Fie \mathcal{R}_l congruența asociată:

$$\alpha\mathcal{R}_l\beta \iff |\alpha| = |\beta|, \forall \alpha, \beta \in A^*$$

Atunci $A^*/\mathcal{R}_l \cong (\mathbb{N})$ este un izomorfism de monoizi, dat de de $A^* \mapsto n$ (reamintim partiția în clase de echivalență: dacă $\alpha \in A^*$, $|\alpha| = n$, atunci $[\alpha]_{\mathcal{R}_l} = A^n$), unde operația binară pe A^n/\mathcal{R}_l este $(A^n, A^m) \mapsto A^{n+m}$.

Reamintim că pentru orice alfabet A , monoidul A^* are următoarea proprietate : pentru orice monoid M și pentru orice funcție $f : A \rightarrow M$, există un unic morfism de monoizi $f^* : A^* \rightarrow M$ care extinde pe f (adică $f^*(a) = f(a), \forall a \in A$), și anume:

$$\begin{aligned} f^*(\epsilon) &= e_M \\ f^*(\alpha) &= f(a_1) \cdot \dots \cdot f(a_n), \text{ dacă } \alpha = a_1 \dots a_n \in A^* \end{aligned}$$

Fie acum X o mulțime și $\delta : X \times A^* \rightarrow X$ o acțiune a monoidului stringurilor pe X . Cum $A \subseteq A^*$, prin restricție se obține o funcție $\delta_A : X \times A \rightarrow X$. Reciproc, orice funcție $\delta_A : X \times A \rightarrow X$ determină o acțiune a monoidului A^* pe X , prin funcția $\delta : X \times A^* \rightarrow X$, definită recursiv astfel:

$$\begin{aligned} \delta(x, \epsilon) &= x \\ \delta(x, \alpha a) &= \delta_A(\delta(x, \alpha), a), \forall \alpha \in A^*, a \in A \end{aligned}$$

Atunci funcția δ astfel definită verifică în mod clar (A1). Verificăm și (A2) $\delta(x, \alpha\beta) = \delta(\delta(x, \alpha), \beta)$, prin inducție după $|\beta|$: dacă $|\beta| = 0$, adică $\beta = \epsilon$, atunci

$$\begin{aligned} \delta(\delta(x, \alpha), \beta) &= \delta(\delta(x, \alpha), \epsilon) \\ &= \delta(x, \alpha) \\ &= \delta(x, \alpha\epsilon) \\ &= \delta(x, \alpha\beta) \end{aligned}$$

Presupunem acum afirmația adevărată pentru stringuri de lungime mai mică sau egală cu n și fie $\beta \in A^*$, $|\beta| = n + 1$. Atunci putem scrie $\beta = \gamma a$, cu $\gamma \in A^*$, $|\gamma| \leq n$, $a \in A$ și avem

$$\begin{aligned} \delta(x, \alpha\beta) &= \delta(x, \alpha\gamma a) \\ &= \delta_A(\delta(x, \alpha\gamma), a) \\ &= \delta_A(\delta(\delta(x, \alpha), \gamma), a) \\ &= \delta(\delta(x, \alpha), \gamma a) \\ &= \delta(\delta(x, \alpha), \beta) \end{aligned}$$

II.2.5 Automate

Definiția II.2.5.1. Un automat determinist finit (DFA) este un tuplu $\mathcal{A} = (X, A, I, F, \delta)$, unde

- (i) X este o mulțime finită, numită mulțimea stărilor;

(ii) A este un alfabet finit;

(iii) $I \subseteq X$ este o submulțime numită mulțimea stărilor inițiale, iar $F \subseteq X$ mulțimea stărilor finale;

(iv) $\delta : X \times A \rightarrow X$ este o funcție numită funcția de tranziție.

Din observația precedentă rezultă că un DFA peste un alfabet A este de fapt o mulțime peste care acționează monoidul stringurilor A^* , împreună cu două submulțimi bine determinate (submulțimile stărilor de intrare și de ieșire).

Definiția II.2.5.2. Un automat nedeterminist finit (N DFA) este un tuplu $\mathcal{A} = (X, A, I, F, E)$ ca mai sus, cu diferența că în loc de o funcție de tranziție $\delta : X \times A \rightarrow X$, avem o relație $E \subseteq X \times A \times X$.

Dacă $(x, a, y) \in E$ sau $\delta(x, a) = y$, vom nota $x \xrightarrow{a} y$ și vom spune că automatul a trecut din starea x în starea y la primirea input-ului a .

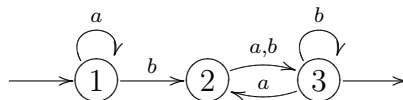
Să remarcăm că o relație $E \subseteq X \times A \times X$ este echivalentă cu o funcție $\tau : X \times A \rightarrow \mathcal{P}(X)$, unde $\tau(x, a) = \{y \in X \mid (x, a, y) \in E\}$ (și reciproc, pentru orice funcție $\tau : X \times A \rightarrow \mathcal{P}(X)$, obținem o relație E prin $(x, a, y) \in E \Leftrightarrow y \in \tau(x, a)$). Putem extinde o asemenea funcție la mulțimea părților prin $\mathcal{P}(X) \times A \rightarrow \mathcal{P}(X)$, $(X', a) \mapsto \{y \in X \mid \exists x \in X', y \in \tau(x, a)\}$, unde $X' \subseteq X$. În particular, fiecărui N DFA $\mathcal{A} = (X, A, I, F, E)$ îi corespunde un DFA prin $\text{Det}(\mathcal{A}) = (\mathcal{P}(X), A, \mathcal{I}, \mathcal{F}, \delta)$, unde $\mathcal{I} = \{I\} \subseteq \mathcal{P}(X)$, $\mathcal{F} = \{X' \subseteq X \mid X' \cap F \neq \emptyset\}$ și τ ca mai sus. De asemenea, să remarcăm că și un N DFA corespunde unei acțiuni a monoidului stringurilor A^* , numai că de această dată mulțimea pe care se acționează este $\mathcal{P}(X)$ și nu X .

În continuare, vom reprezenta automatele (N DFA sau DFA) prin grafuri orientate, astfel: nodurile grafului vor fi stările din X , iar între două noduri x și y există un arc cu eticheta $a \in A \Leftrightarrow (x, a, y) \in E$ (sau $\delta(x, a) = y$). Stările finale, respectiv inițiale vor fi marcate prin săgeți care ies, respectiv intră din noduri.

Exemplul II.2.5.3. Fie $\mathcal{A} = (X = \{1, 2, 3\}, A = \{a, b\}, I = \{1\}, F = \{2\}, \delta)$, unde $\delta : X \times A \rightarrow X$ e dată în tabelul următor:

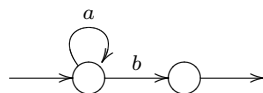
		A	
		a	b
X	1	1	2
	2	3	3
	3	2	3

Atunci automatul va avea reprezentarea

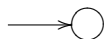


Un drum în automatul \mathcal{A} este o secvență finită de stări consecutive între care există tranziții, $x_0 \xrightarrow{a_1} x_1 \xrightarrow{a_2} \dots \xrightarrow{a_n} x_n$. Spunem că stringul $\alpha = a_1 \dots a_n$ este asociat drumului. Prin convenție, pentru orice stare $x \in X$ considerăm un drum vid cu stringul asociat ϵ . Spunem că un string $\alpha = a_1 \dots a_n$ este acceptat de automatul \mathcal{A} dacă există un drum cu $x_0 \in I$ stare inițială și $x_n \in F$ stare finală. În particular, stringul vid este acceptat dacă există o stare inițială care este și finală. Mulțimea stringurilor acceptate de un automat \mathcal{A} se numește *limbajul acceptat* de automatul \mathcal{A} și se va nota cu $L(\mathcal{A})$.

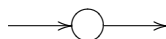
Exemplul II.2.5.4. (i) Un automat care acceptă limbajul $\{a^n b \mid n \in \mathbb{N}\}$



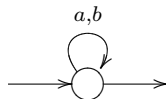
(ii) Un automat care acceptă limbajul vid.



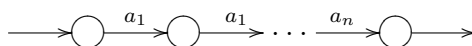
(iii) Un automat care acceptă limbajul format din stringul vid



(iv) Un automat care acceptă toate stringurile peste alfabetul $\{a, b\}$



(v) Un automat care acceptă doar stringul $\alpha = a_1 \dots a_n$



Spunem că două automate sunt *echivalente* dacă acceptă același limbaj.

Propoziția II.2.5.5. Orice N DFA este echivalent cu un DFA.