



Treball Fi de Grau - Curs 2022/2023

Autòmats finits i llenguatges formals

Autor: CARMEN TUDELA ESPARZA

Tutor: ENRIC COSME LLÓPEZ

Índex

Introducció	3
Capítol 1. Estructures algebraiques	5
1. Monoide	5
2. Submonoides	6
3. Monoide quocient i congruències	7
4. Primer Teorema d'Isomorfia	11
Capítol 2. Paraules, llenguatges i autòmats	13
1. Propietat Universal del Monoide Lliure	14
2. Autòmats finits i llenguatges reconeixibles	19
3. Autòmats deterministes	22
4. Autòmats complets, accessibles, coaccessibles i ajustats	23
5. Autòmat estàndard	25
Capítol 3. Operacions i llenguatges reconeixibles	27
1. Operacions booleanes	27
2. Producte	29
3. Estrella	31
4. Quocients	33
5. Inverses de morfismes	34
Capítol 4. Autòmat minimal i monoide sintàctic	35
1. Autòmat minimal	35
2. Autòmats i monoides	40
3. Monoide sintàctic i morfisme sintàctic	42
4. Saturació en A^*	44
5. Congruència sintàctica	46
Capítol 5. Llenguatges racionals i llenguatges reconeixibles	51
Conclusions	55
Bibliografia	57

Introducció

Com podem trobar en el llibre de Hopcroft [HMU08], la teoria d'autòmats és l'estudi de dispositius de càlcul abstractes. En la dècada dels anys quaranta i cinquanta, els investigadors estudiaren les màquines més simples, les quals denominem: autòmats finits. Al principi es van proposar per modelar el funcionament del cervell, però resultaren molt útils per a molts altres propòsits. A més, també a finals de la dècada dels anys cinquanta del Segle XX, N. Chomsky va iniciar l'estudi dels llenguatges formals, que encara que no són màquines estrictament, estos llenguatges estan molt relacionats amb els autòmats abstractes.

En el primer capítol, s'estudien les estructures bàsiques necessàries per al desenvolupament de la teoria d'autòmats i llenguatges formals, per fer-ho hem utilitzat les notes de [SB81] i [Pin21]. En concret, comencem introduint els conceptes de monoides i submonoides, així com algunes de les seues propietats bàsiques, que seran útils més endavant. També s'introdueix el concepte de congruència, que serà necessari per a la construcció del monoide quocient. Finalment, s'explica el primer Teorema d'Isomorfia, que serà molt útil per establir relacions entre els monoides i els autòmats.

El segon capítol té com a objectiu presentar l'objecte de treball principal: l'autòmat finit. Per fer-ho, s'introdueixen diversos conceptes previs necessaris com ara l'alfabet, la paraula i el monoide lliure. Amb aquest últim s'explica la Propietat Universal que permet construir homomorfismes de monoides. A continuació, es defineix el concepte de llenguatge i s'introdueix el conjunt de llenguatges racionals. A partir d'ací ja es pot definir l'estructura d'autòmat finit i de llenguatge reconeixible. També es presenta una eina fonamental, el Lema del Bombeig, que ajuda a identificar els llenguatges que no poden ser reconeguts per un autòmat finit. Finalment, es presenten diferents tipus d'autòmats, com ara els deterministes, els complets, els accessibles, els coaccessibles, els ajustats i els estàndards, i s'analitzen algunes de les seues propietats i la seua capacitat per reconèixer diferents tipus de llenguatges. Totes aquestes idees les hem tret de les notes en [Pin10].

En el següent capítol s'analitzen les propietats dels llenguatges reconeixibles. Es veu que aquests llenguatges són tancats per a les operacions booleanes (unió, intersecció i complementari), per al producte i per a l'operació estrella. També s'observa que el quocient d'un llenguatge reconeixible és reconeixible, i que les imatges inverses dels morfismes també preserven la reconeixibilitat dels llenguatges.

Al quart capítol establim certes relacions entre els autòmats i els monoides. En primer lloc definim l'autòmat de Nerode, donarem propietats i la congruència a la què dona lloc. A més veurem que l'autòmat de Nerode és minimal i reconeix el mateix llenguatge que l'original. Després introduïm el concepte de monoide sintàctic, construït a partir de la congruència donada pel nucli. Veurem el que significa que un llenguatge siga reconegut per un monoide i demostrarem que és equivalent a que siga reconegut per un autòmat. Definirem llenguatge saturat per una congruència, que estableix una relació entre les paraules i que ens servirà per definir la congruència sintàctica, la major congruència que satura al llenguatge. Aquesta congruència ens permetrà construir el monoide quocient i, a més, veurem que la congruència sintàctica és equivalent a la congruència donada per la relació del nucli.

Per acabar el nostre treball demostrarem que el conjunt de llenguatges racionals és el mateix que el conjunt de llenguatges reconeixibles. La demostració de que els llenguatges reconeixibles estan inclosos en els racionals és directa. Per a l'altra inclusió farem servir la demostració que es troba en el llibre [FR04].

També cal aclarir en aquesta introducció un parell de qüestions de notació. Donat un $n \in \mathbb{N}$, si tenim expressions del tipus $j \in n$ en aquest cas entenem n com el conjunt de naturals menors estrictes que n , és a dir, $n = \{0, \dots, n-1\}$. A més, quan considerem els autòmats deterministes denotarem per $\cdot$ a les seues transicions. Ja que, donat un estat, per a cada lletra o paraula, sols hi ha una transició definida.

CAPÍTOL 1

Estructures algebraiques

En aquest capítol s'introdueixen les nocions algebraiques i els continguts necessaris per a poder desenvolupar la teoria d'autòmats.

En primer lloc presentarem l'estructura de monoide i alguns exemples bàsics. També introduïm el concepte d'homomorfisme entre monoides. A continuació, introduïm la subestructura d'un monoide amb exemples bàsics, propietats i alguns conceptes relacionats. Continuem amb les congruències sobre els monoides i com formen el conjunt quocient. I per últim, introduïm el Primer Teorema d'Isomorfia per a monoides.

1. Monoide

Donarem la definició de monoide i alguns exemples. A més, introduïm el concepte d'homomorfisme de monoides.

DEFINICIÓ 1.1. *Un monoide és una estructura algebraica que consisteix en una terna $(M, \cdot, 1)$, on M és un conjunt, $\cdot$ una operació binària interna associativa i $1 \in M$ és l'element neutre. És a dir, donats $x, y, z \in M$ qualsevol es compleix:*

- (1) $x \cdot y \in M$. Operació binària interna;
- (2) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Associativitat;
- (3) $1 \cdot x = x \cdot 1 = x$. Element neutre.

NOTA 1.2. *Normalment obviarem l'operació " $\cdot$ " quan considerem monoides amb una operació multiplicativa. Si l'estructura està clara, escriurem M en compte de $(M, \cdot, 1)$.*

PROPOSICIÓ 1.3. *En un monoide, l'element neutre és únic.*

DEMOSTRACIÓ. Suposem que existeixen dos elements neutres, 1 i $1'$. Aleshores per la definició d'element neutre tenim que $1' = 11' = 1'1 = 1$. $\square$

EXEMPLE 1.4. *Alguns exemples de monoides:*

- (1) *Considerem l'estructura algebraica de grup, que consisteix en una terna $(G, \cdot, 1)$ on l'operació " $\cdot$ " és associativa, tenim l'existència d'un element neutre $1 \in G$ i també l'existència d'un*

element invers per a cada element de G . Aleshores tenim que un grup és un cas particular de monoide.

- (2) *El conjunt dels nombres naturals $\mathbb{N}$ amb la suma habitual i el 0 com a neutre és un monoide.*

DEFINICIÓ 1.5. *Siguen M i N monoides i siga $f : M \longrightarrow N$ una aplicació. Direm que $f : M \longrightarrow N$ és homomorfisme de monoides si preserva l'operació de cada monoide, és a dir, si per a tot $m_1, m_2 \in M$ es compleix:*

$$f(m_1 m_2) = f(m_1) f(m_2).$$

i, a més, $f(1) = 1$.

Direm que dos monoides M i N són isomorfs si existeix $f : M \longrightarrow N$ isomorfisme de monoides, és a dir, un homomorfisme de monoides bijectiu. En aquest cas escriurem $M \cong N$.

2. Submonoide

A continuació introduïrem la noció de submonoide. Presentarem alguns exemples. També introduïrem el conjunt de submonoides d'un monoide.

DEFINICIÓ 1.6. *Siga M un monoide, i siga $N \subseteq M$. Direm que N és submonoide del monoide M si es compleix que $1 \in N$ i l'operació de M restringida a N és interna, és a dir, si $m, n \in N$ aleshores $mn \in N$. En aquest cas N té estructura de monoide amb les operacions de M . Escriurem $N \leq M$ per a denotar que N és submonoide de M .*

Donat un monoide M podem considerar el conjunt que conté a tots els submonoides de M i el denotem per

$$\text{Sub}(M) = \{N \mid N \leq M\}.$$

PROPOSICIÓ 1.7. *Siga M un monoide i siga N un submonoide, aleshores l'aplicació inclusió $\text{in}_N : N \longrightarrow M$ és homomorfisme de monoides injectiu.*

DEMOSTRACIÓ. Si N és submonoide de M aleshores, si $n, m \in N$ es té que

$$\text{in}_N(nm) = nm = \text{in}_N(n)\text{in}_N(m).$$

Notem que la primera igualtat la tenim perquè $nm \in N$, en ser N submonoide de M .

Anem a veure que és injectiu. Siguen $n, m \in N$ de manera que $\text{in}_N(n) = \text{in}_N(m)$, aleshores tenim que $n = m$ ja que $n, m \in N$. $\square$

EXEMPLE 1.8. *Alguns exemples de submonoides:*

- (1) *Si M és un monoide, aleshores 1 i M són submonoides.*

- (2) Si considerem un grup G com a monoide, aleshores els seus subgrups són també submonoides.
- (3) Si considerem el monoide dels nombres naturals, aleshores el conjunt de nombres parells és un submonoide.

LEMA 1.9. Siga M un monoide, I un conjunt d'índexs i $\{N_i \mid i \in I\}$ una família de submonoides de M , aleshores $\bigcap_{i \in I} N_i$ és un submonoide de M .

DEMOSTRACIÓ. Anem a demostrar-ho utilitzant la definició de submonoide. Per una banda tenim que la intersecció dels N_i està inclosa en M ja que tots els N_i són submonoides. Per altra banda, el neutre de M està en la intersecció dels N_i , ja que està en tots els N_i en ser submonoides. Per últim, si tenim dos elements qualsevol n_1, n_2 en la intersecció dels N_i , aleshores $n_1, n_2 \in N_i$ per a tot $i \in I$. Per tant $n_1 n_2 \in N_i$ per a tot $i \in I$, en ser tots submonoides, i així $n_1 n_2$ està en la intersecció dels N_i . $\square$

DEFINICIÓ 1.10. Si tenim M un monoide aleshores podem considerar per a cada X subconjunt de M :

$$\text{Sg}(X) = \bigcap \{N \mid X \subseteq N \text{ i } N \leq M\}.$$

Llegim $\text{Sg}(X)$ com el “submonoide generat per X ”.

LEMA 1.11. Siga M un monoide, I un conjunt d'índexs i $\{N_i \mid i \in I\}$ una família de submonoides de M , aleshores

$$(\text{Sg}(\bigcup_{i \in I} N_i), \cdot, 1)$$

és un submonoide de M .

3. Monoide quocient i congruències

En aquesta secció, definirem les congruències d'un monoide i presentarem el concepte de conjunt quocient. Demostrarem que el conjunt quocient, junt a l'operació definida forma un monoide.

DEFINICIÓ 1.12. Donat un monoide M i una relació d'equivalència $\Theta \subseteq M \times M$, diem que Θ és una relació de congruència en M si per a tot $m_1, m_2, n_1, n_2 \in M$ tals que $(m_1, m_2), (n_1, n_2) \in \Theta$, tenim $(m_1 n_1, m_2 n_2) \in \Theta$.

Donat un monoide M , definim el conjunt de totes les congruències sobre el monoide M com:

$$\text{Con}(M) = \{\Theta \subseteq M \times M \mid \Theta \text{ és una congruència en } M\}.$$

DEFINICIÓ 1.13. *Siga M un monoide, definim la relació diagonal com el següent conjunt:*

$$\Delta_M = \{(m, m) \mid m \in M\} \subseteq M \times M.$$

i definim la relació total com el següent conjunt:

$$\nabla_M = M \times M.$$

PROPOSICIÓ 1.14. *Donat un monoide M , les relacions diagonal i total són congruències en M . A més, si $\Theta \in \text{Con}(M)$, aleshores $\Delta_M \subseteq \Theta \subseteq \nabla_M$. És a dir Δ_M i ∇_M són, respectivament, la menor i la major congruència en $\text{Con}(M)$.*

DEMOSTRACIÓ. És fàcil veure que Δ_M i ∇_M són relacions d'equivalència. Donarem únicament la demostració de compatibilitat amb l'operació en M .

Anem a demostrar que la relació diagonal és una congruència en M . Considerem $m_1, m_2, n_1, n_2 \in M$ de manera que $(m_1, m_2), (n_1, n_2) \in \Delta_M$, per la pròpia definició tenim que $m_1 = m_2$ i $n_1 = n_2$. Per tant $m_1 n_1 = m_2 n_2$ o, el que és equivalent, $(m_1 n_1, m_2 n_2) \in \Delta_M$. Aleshores la relació diagonal és una congruència.

Ara anem a demostrar que la relació total també és una congruència en M . Siguen $m_1, m_2, n_1, n_2 \in M$ de manera que $(m_1, m_2), (n_1, n_2) \in \nabla_M = M \times M$, aleshores $m_1 n_1, m_2 n_2 \in M$, en ser M un monoide. Per tant $(m_1 n_1, m_2 n_2) \in \nabla_M$.

Si $\Theta \in \text{Con}(M)$, aleshores per definició $\Theta \subseteq M \times M = \nabla_M$. A més, $\Delta_M \subseteq \Theta$ perquè Θ és reflexiva. $\square$

DEFINICIÓ 1.15. *Siga M un monoide i Θ una relació de congruència sobre M . Anomenem conjunt quocient al conjunt format per les classes d'equivalència dels elements de M respecte de Θ i el denotem per*

$$M/\Theta = \{[m]_\Theta \mid m \in M\}.$$

A continuació, veurem que el conjunt quocient que hem definit admet estructura de monoide amb el producte de representants de cada classe. Aquest monoide serà anomenat monoide quocient.

PROPOSICIÓ 1.16. *Considerem un monoide M i Θ una relació de congruència en M , aleshores M/Θ té estructura de monoide amb l'operació $\cdot$ i l'element neutre $[1]_\Theta$.*

DEMOSTRACIÓ. Hem de veure que l'operació $\cdot$ està ben definida, que és associativa, compatible amb la relació Θ i que $[1]_\Theta$ és l'element neutre.

Ben definida i compatible amb Θ : Si $[m_1]_\Theta, [m_2]_\Theta, [n_1]_\Theta, [n_2]_\Theta$ són classes en M/Θ tals que $[m_1]_\Theta = [m_2]_\Theta$ i $[n_1]_\Theta = [n_2]_\Theta$. Aleshores

sabem que $(m_1, m_2), (n_1, n_2) \in \Theta$ i per tant com que Θ és una relació de congruència sobre M tenim $(m_1 n_1, m_2 n_2) \in \Theta$, és a dir, $[m_1 n_1]_\Theta = [m_2 n_2]_\Theta$.

Associativa: Siguen $[m_1]_\Theta, [m_2]_\Theta, [m_3]_\Theta \in M/\Theta$, aleshores

$$\begin{aligned} ([m_1]_\Theta [m_2]_\Theta) [m_3]_\Theta &= ([m_1 m_2]_\Theta) [m_3]_\Theta \\ &= [(m_1 m_2) m_3]_\Theta \\ &= [m_1 (m_2 m_3)]_\Theta \\ &= [m_1]_\Theta ([m_2 m_3]_\Theta) \\ &= [m_1]_\Theta ([m_2]_\Theta [m_3]_\Theta). \end{aligned}$$

Notem que la tercera igualtat l'obtenim ja que l'operació de M és associativa en ser M monoide.

Element neutre: Siga $[m]_\Theta \in M/\Theta$ qualsevol, aleshores:

$$\begin{aligned} [m]_\Theta [1]_\Theta &= [m1]_\Theta \\ &= [m]_\Theta \\ &= [1m]_\Theta \\ &= [1]_\Theta [m]_\Theta. \end{aligned}$$

Notem que la segona i la tercera igualtat es donen en ser 1 el neutre del monoide M . $\square$

PROPOSICIÓ 1.17. *Siga M un monoide i $\Theta \subseteq M \times M$ una relació de congruència en M . Aleshores l'aplicació projecció $\text{pr}_\Theta : M \longrightarrow M/\Theta$, que a cada $m \in M$ li fa correspondre la seua classe d'equivalència $[m]_\Theta$, és un homomorfisme de monoides suprajectiu.*

DEMOSTRACIÓ. Siguen $m, n \in M$, aleshores

$$\begin{aligned} \text{pr}_\Theta(mn) &= [mn]_\Theta \\ &= [m]_\Theta [n]_\Theta \\ &= \text{pr}_\Theta(m) \text{pr}_\Theta(n). \end{aligned}$$

Notem que la segona igualtat ve donada en ser Θ una congruència. A més, $\text{pr}_\Theta(1) = [1]_\Theta$, per definició. Aleshores pr_Θ és un homomorfisme.

Falta provar que és suprajectiu. Notem que si $[m]_\Theta \in M/\Theta$, aleshores existeix almenys un element $m \in M$ de manera que $\text{pr}_\Theta(m) = [m]_\Theta$. $\square$

LEMA 1.18. *Siga M un monoide, I un conjunt d'índexs i $\{\Theta_i \mid i \in I\}$ una família arbitrària de congruències en M , aleshores $\bigcap_{i \in I} \Theta_i$ és una congruència en M .*

DEMOSTRACIÓ. Començarem demostrant que $\bigcap_{i \in I} \Theta_i$ és una relació d'equivalència, després veurem que és compatible amb el producte.

Reflexiva: $(m, m) \in \bigcap_{i \in I} \Theta_i$ perquè $(m, m) \in \Theta_i$ per a tot $i \in I$.

Simètrica: Si $(m_1, m_2) \in \bigcap_{i \in I} \Theta_i$ aleshores tenim que $(m_1, m_2) \in \Theta_i$ per a tot $i \in I$. Ara, com cada Θ_i és relació d'equivalència, tenim també $(m_2, m_1) \in \Theta_i$ per a tot $i \in I$, per tant podem concloure que $(m_2, m_1) \in \bigcap_{i \in I} \Theta_i$.

Transitiva: Si $(m_1, m_2), (m_2, m_3) \in \bigcap_{i \in I} \Theta_i$, aleshores tenim que $(m_1, m_2), (m_2, m_3) \in \Theta_i$ per a tot $i \in I$. Per la propietat transitiva que tenen cada un dels Θ_i , tenim que $(m_1, m_3) \in \Theta_i$ per a tot $i \in I$, aleshores $(m_1, m_3) \in \bigcap_{i \in I} \Theta_i$.

Compatible amb el producte: Siguen $(m_1, m_2), (n_1, n_2) \in \bigcap_{i \in I} \Theta_i$ aleshores $(m_1, m_2), (n_1, n_2) \in \Theta_i$, per a tot $i \in I$. Per tant, com que cada un dels Θ_i és relació de congruència, tenim que $(m_1 n_1, m_2 n_2) \in \Theta_i$, per a tot $i \in I$, aleshores $(m_1 n_1, m_2 n_2) \in \bigcap_{i \in I} \Theta_i$. $\square$

PROPOSICIÓ 1.19. *Siga M un monoide i $\Theta_1, \Theta_2 \in \text{Con}(M)$ amb $\Theta_1 \subseteq \Theta_2$. L'aplicació*

$$\begin{aligned} \varphi: M/\Theta_1 &\longrightarrow M/\Theta_2 \\ [m]_{\Theta_1} &\longmapsto [m]_{\Theta_2} \end{aligned}$$

és un homomorfisme de monoides suprajectiu. En particular $|M/\Theta_2| \leq |M/\Theta_1|$

DEMOSTRACIÓ. En primer lloc veurem que φ és un homomorfisme de monoides.

Notem que $\varphi([1]_{\Theta_1}) = [1]_{\Theta_2}$. D'altra banda, siguen $m, n \in M$

$$\begin{aligned} \varphi([m]_{\Theta_1} [n]_{\Theta_1}) &= \varphi([mn]_{\Theta_1}) \\ &= [mn]_{\Theta_2} \\ &= [m]_{\Theta_2} [n]_{\Theta_2} \\ &= \varphi([m]_{\Theta_1}) \varphi([n]_{\Theta_1}). \end{aligned}$$

Falta demostrar que φ és suprajectiva. Si $[m]_{\Theta_2}$ és un element qualsevol de M/Θ_2 , per a l'element $[m]_{\Theta_1} \in M/\Theta_1$ es té que $\varphi([m]_{\Theta_1}) = [m]_{\Theta_2}$. Per tant φ és un homomorfisme de monoides suprajectiu. $\square$

DEFINICIÓ 1.20. *Direm que el monoide M és finit quan M és finit. Donada una congruència Θ en M direm que té índex finit quan M/Θ és finit.*

DEFINICIÓ 1.21. *Donat un monoide M , definim el conjunt format per totes les congruències d'índex finit sobre el monoide M com*

$$\text{Con}_{\text{if}}(M) = \{\Theta \subseteq M \times M \mid \Theta \text{ congruència en } M \text{ d'índex finit}\}.$$

Anem a veure a continuació que si Θ_1 és una congruència d'índex finit del monoide M i Θ_2 és una congruència de M que conté a Θ_1 , aleshores Θ_2 és una congruència d'índex finit.

COROL·LARI 1.22. *Siga M un monoide, $\Theta_1 \in \text{Con}_{\text{if}}(M)$ i $\Theta_2 \in \text{Con}(M)$ de manera que $\Theta_1 \subseteq \Theta_2$, aleshores $\Theta_2 \in \text{Con}_{\text{if}}(M)$.*

DEMOSTRACIÓ. Se segueix de la Proposició 1.19. $\square$

4. Primer Teorema d'Isomorfia

Anem a veure el Primer Teorema d'Isomorfia, que ens servirà per analitzar i comparar diferents autòmats des d'una perspectiva algebraica.

DEFINICIÓ 1.23. *Siguen M i N dos monoides i siga $f : M \longrightarrow N$ un homomorfisme de monoides. Definim el nucli de f com*

$$\text{Ker}(f) = \{(m_1, m_2) \in M \times M \mid f(m_1) = f(m_2)\}$$

i el conjunt imatge de f com

$$\text{Im}(f) = \{n \in N \mid \exists m \in M (f(m) = n)\}.$$

PROPOSICIÓ 1.24. *Siguen M i N dos monoides i siga $f : M \longrightarrow N$ un homomorfisme de monoides, aleshores tenim que:*

- (1) $\text{Ker}(f)$ és una congruència en M ;
- (2) $\text{Im}(f)$ és un submonoide de N ;
- (3) $M/\text{Ker}(f) \cong \text{Im}(f)$.

DEMOSTRACIÓ. $\text{Ker}(f)$ és una congruència en M : Notem que $\text{Ker}(f)$ és una relació d'equivalència, ja que compleix la propietat reflexiva, simètrica i transitiva. Falta comprovar la compatibilitat amb l'operació del monoide. Siguen $(m_1, m_2), (n_1, n_2) \in \text{Ker}(f)$ per definició de $\text{Ker}(f)$ tenim que $f(m_1) = f(m_2)$ i $f(n_1) = f(n_2)$. Aleshores

$$\begin{aligned} f(m_1 n_1) &= f(m_1) f(n_1) \\ &= f(m_2) f(n_2) \\ &= f(m_2 n_2). \end{aligned}$$

La primera i la tercera igualtat les obtenim en ser f un homomorfisme de monoides. Així $(m_1 n_1, m_2 n_2) \in \text{Ker}(f)$.

$\text{Im}(f)$ és un submonoide de N : Hem de comprovar que $1 \in \text{Im}(f)$ i que si $n_1, n_2 \in \text{Im}(f)$ aleshores $n_1 n_2 \in \text{Im}(f)$.

Notem que $1 \in M$, aleshores en ser f un homomorfisme de monoides $f(1) = 1 \in N$.

D'altra banda, siguen $n_1, n_2 \in \text{Im}(f)$, aleshores existeixen $m_1, m_2 \in M$ de manera que $f(m_1) = n_1$ i $f(m_2) = n_2$. Per tant:

$$n_1 n_2 = f(m_1) f(m_2) = f(n_1 n_2) \in \text{Im}(f).$$

La segona igualtat es té en ser f un homomorfisme de monoides.

$M/\text{Ker}(f)$ i $\text{Im}(f)$ són isomorfs: Definim la següent aplicació

$$\begin{aligned} f^b : M/\text{Ker}(f) &\longrightarrow \text{Im}(f) \\ [m]_{\text{Ker}(f)} &\longmapsto f(m) \end{aligned}$$

Anem a veure primer que f^b està ben definida. Considerem dos elements $m, n \in M$ de manera que $[m]_{\text{Ker}(f)} = [n]_{\text{Ker}(f)}$, que és el mateix que dir que $(m, n) \in \text{Ker}(f)$ aleshores per definició de $\text{Ker}(f)$ tenim que $f(m) = f(n)$ i així ja hem demostrar que f^b està ben definida. Notem que si repetim l'argument que hem fet servir per a veure que f^b està ben definida però en sentit contrari tenim també que f^b és injectiva.

Anem a veure ara que f^b és una aplicació suprajectiva. Siga $n \in \text{Im}(f)$ aleshores sabem que existeix un element $m \in M$ de manera que $f(m) = n$, per tant podem considerar la classe d'equivalència d'eixe element respecte $\text{Ker}(f)$, $[m]_{\text{Ker}(f)}$, així ja tenim que existeix un element del domini tal que la seua imatge per f^b ens dona l'element n , per tant f^b és suprajectiva. A més, f^b és homomorfisme de monoides ja que si tenim $m, n \in M$, aleshores

$$\begin{aligned} f^b([m]_{\text{Ker}(f)}[n]_{\text{Ker}(f)}) &= f^b([mn]_{\text{Ker}(f)}) \\ &= f(mn) \\ &= f(m)f(n) \\ &= f^b([m]_{\text{Ker}(f)})f^b([n]_{\text{Ker}(f)}). \end{aligned}$$

La primera igualtat la tenim en ser $\text{Ker}(f)$ una congruència i la tercera en ser f un homomorfisme. Per tant f^b és un homomorfisme bijectiu, és a dir, és un isomorfisme. Concloem que $M/\text{Ker}(f) \cong \text{Im}(f)$. $\square$

CAPÍTOL 2

Paraules, llenguatges i autòmats

En aquest capítol anem a presentar les definicions més importants utilitzades en la teoria d'autòmats. Entre aquests conceptes s'inclouen el d'alfabet, paraula i llenguatge. Després presentem la Propietat Universal del Monoide Lliure, que estableix una relació entre els llenguatges i els monoides. Més tard, estudiarem el concepte d'autòmat finit com un model matemàtic que ens permet reconèixer llenguatges formals i veurem les components de l'autòmat finit, com els estats, l'alfabet, les transicions i els estats d'acceptació. A més, discutirem la noció de llenguatges reconeixibles per autòmats finits.

DEFINICIÓ 2.1. *Un alfabet és un conjunt dels elements del qual s'anomenen lletres. Donat un alfabet A , una paraula és una aplicació*

$$w : n \longrightarrow A.$$

Definim la longitud de la paraula w com el seu domini.

DEFINICIÓ 2.2. *Definim el monoide de totes les paraules sobre A com $(A^*, \wedge, \lambda)$ on:*

- $A^* = \bigcup_{n \in \mathbb{N}} \text{Hom}(n, A)$, el conjunt de les paraules sobre A .
- $\wedge$ és l'operació binària anomenada concatenació, de manera que si tenim dues paraules $u : n \longrightarrow A$ i $w : m \longrightarrow A$ amb $n, m \in \mathbb{N}$ aleshores la concatenació de u i w , és a dir $u \wedge w$, o també escrit uw , és la paraula

$$\begin{aligned} u \wedge w : n + m &\longrightarrow A \\ z &\longmapsto \begin{cases} u(z) & \text{si } z \in n; \\ w(z - n) & \text{si } z \in [n, m - 1]. \end{cases} \end{aligned}$$

- λ és la paraula buida, és a dir, l'única aplicació de 0 en A

$$\lambda : 0 \longrightarrow A$$

Aleshores $(A^, \wedge, \lambda)$ és un monoide que s'anomena monoide lliure sobre A i que es denota normalment per A^* .*

DEFINICIÓ 2.3. *Definim l'aplicació inclusió com l'aplicació entre A i A^* definida com segueix*

$$\begin{array}{lcl} \text{in}_A : A & \longrightarrow & A^* \\ a & \longmapsto & \text{in}_A(a) : \begin{array}{lcl} 1 & \longrightarrow & A \\ 0 & \longmapsto & a \end{array} \end{array}$$

és a dir, $\text{in}_A(a)$ és la paraula de longitud 1 que forma la lletra a .

1. Propietat Universal del Monoide Lliure

La següent propietat és molt important en la teoria d'autòmats ja que permet establir la relació entre els monoides lliures i els autòmats finits. A més també s'utilitza per a demostrar l'equivalència entre els autòmats finits i els llenguatges regulars que més avant veurem.

TEOREMA 2.4 (Propietat Universal del Monoide Lliure). *Si M és un monoide i $f : A \longrightarrow M$ una aplicació, aleshores existeix un únic homomorfisme de monoides $f^\# : A^* \longrightarrow M$ tal que $f^\# \circ \text{in}_A = f$, on in_A és l'aplicació inclusió d' A en A^* .*

DEMOSTRACIÓ. Siga $w \in A^*$, si $w = \lambda$, definim $f^\#(\lambda) = 1$.

D'altra forma si $w \neq \lambda$ es podrà expressar com a $w = w_0 \cdots w_{n-1} = (w_i)_{i \in n}$. En aquest cas definim:

$$f^\#(w) = f(w_0) \cdots f(w_{n-1}) = \prod_{i \in n} f(w_i).$$

Necessitem veure que $f^\#$ és homomorfisme de monoides, és a dir, que preserva l'1 i que és compatible amb el producte.

Per una banda, notem que, per definició, es té que

$$f^\#(\lambda) = 1.$$

Ara, si $u = (u_i)_{i \in n}$ i $w = (w_j)_{j \in m}$ són dues paraules en A^* es té que

$$\begin{aligned} f^\#(u \wedge w) &= f^\#((u_i)_{i \in n} \wedge (w_j)_{j \in m}) \\ &= f^\#(u_0 \cdots u_{n-1} w_0 \cdots w_{m-1}) \\ &= f(u_0) \cdots f(u_{n-1}) f(w_0) \cdots f(w_{m-1}) \\ &= f^\#((u_i)_{i \in n}) f^\#((w_j)_{j \in m}) \\ &= f^\#(u) f^\#(w). \end{aligned}$$

Així, $f^\#$ és un homomorfisme de monoides.

Notem que, si $a \in A$, aleshores $f^\#(\text{in}_A(a)) = f(a)$. Per tant, es té la igualtat $f^\# \circ \text{in}_A = f$.

Només quedarà veure la unicitat. Siga $g : A^* \longrightarrow M$ un altre homomorfisme de monoides que satisfà l'equació $g \circ \text{in}_A = f$. Aleshores, en

ser g homomorfisme, es té que $g(\lambda) = 1$. Per altra banda, si $u = (u_i)_{i \in n}$ és una paraula qualsevol en A^* es té que

$$\begin{aligned}
 g(u) &= g((u_i)_{i \in n}) \\
 &= g(u_0 \wedge \cdots \wedge u_{n-1}) \\
 &= g(u_0) \cdots g(u_{n-1}) && (g \text{ és homomorfisme}) \\
 &= g(\text{in}_A(u_0)) \cdots g(\text{in}_A(u_{n-1})) \\
 &= f(u_0) \cdots f(u_{n-1}) && (g \circ \text{in}_A = f) \\
 &= f^\#(u_0 \wedge \cdots \wedge u_{n-1}) \\
 &= f^\#((u_i)_{i \in n}) \\
 &= f^\#(u).
 \end{aligned}$$

Concloem que $g = f^\#$.

Açò conclou la demostració del teorema. $\square$

Utilitzant la Propietat Universal sobre el monoide lliure definit anteriorment, podem veure que conceptes con la longitud d'una paraula o el nombre d'ocurrències d'una lletra són exemples concrets d'homomorfismes de monoides.

DEFINICIÓ 2.5. *Siga A un alfabet. Considerem el monoide $(\mathbb{N}, +, 0)$ i l'aplicació:*

$$\begin{aligned}
 |\cdot| : A &\longrightarrow \mathbb{N} \\
 a &\longmapsto 1
 \end{aligned}$$

per la Propietat Universal existeix un únic homomorfisme de monoides

$$|\cdot|^\# : A^* \longrightarrow \mathbb{N}$$

tal que $|\cdot|^\# \circ \text{in}_A = |\cdot|$.

Aquesta aplicació s'anomena longitud i compleix:

- (1) $|\lambda| = 0$;
- (2) $|uw| = |u| + |w|$.

DEFINICIÓ 2.6. *Siga A un alfabet. Considerem el monoide $(\mathbb{N}, +, 0)$ i l'aplicació:*

$$\begin{aligned}
 |\cdot|_a : A &\longrightarrow \mathbb{N} \\
 z &\longmapsto \begin{cases} 1 & \text{si } z = a; \\ 0 & \text{altre cas.} \end{cases}
 \end{aligned}$$

per la Propietat Universal existeix un únic homomorfisme de monoides

$$|\cdot|_a^\# : A^* \longrightarrow \mathbb{N}$$

tal que $|\cdot|_a^\# \circ \text{in}_A = |\cdot|_a$.

Aquesta aplicació s'anomena ocurrència de la lletra a i compleix:

- (1) $|\lambda|_a = 0$;
- (2) $|uw|_a = |u|_a + |w|_a$.

DEFINICIÓ 2.7. Anomenem llenguatge a qualsevol subconjunt $L \subseteq A^*$. Les operacions que poden ser definides en els llenguatges són:

- (1) Operacions booleanes: l'unió, intersecció i el complementari.
- (2) Quocients: siga $L \subseteq A^*$ i $w \in A$ aleshores:

$$w^{-1}L = \{v \in A^* \mid wv \in L\};$$

$$Lw^{-1} = \{v \in A^* \mid vw \in L\}.$$

En general, siguen $L, K \subseteq A^*$. Aleshores:

$$K^{-1}L = \{v \in A^* \mid \exists k \in K (kv \in L)\};$$

$$LK^{-1} = \{v \in A^* \mid \exists k \in K (vk \in L)\}.$$

- (3) Producte: siguen L_1 i L_2 dos llenguatges, aleshores:

$$L_1L_2 = \{u_1u_2 \in A^* \mid u_1 \in L_1, u_2 \in L_2\}.$$

- (4) Estrella i suma: Si $L \subseteq A^*$, $L^*[L^+]$ és el submonòide [semigrup] d' A^* generat per L .

$$L^* = \{w_0 \wedge \cdots \wedge w_{n-1} \mid n \in \mathbb{N} \text{ i } w_0, \dots, w_{n-1} \in L\}$$

$$L^+ = \{w_0 \wedge \cdots \wedge w_{n-1} \mid n \in \mathbb{N} \setminus \{0\} \text{ i } w_0, \dots, w_{n-1} \in L\}$$

Notem que $L^* = L^+ + 1$, on $1 = \{\lambda\}$.

També podem definir les potències de L com segueix:

$$\begin{cases} L^0 = \{\lambda\}; \\ L^{n+1} = L(L^n). \end{cases}$$

$$\text{de manera que } L^* = \bigcup_{n \in \mathbb{N}} L^n \text{ i } L^+ = \bigcup_{n \in \mathbb{N}^*} L^n.$$

A continuació estudiem com es comporten les operacions de llenguatge amb els homomorfismes.

LEMA 2.8. Siguen A i B dos alfabetes i siguen L i K dos llenguatges d' A^* , $(L_i)_{i \in \mathbb{N}}$ una família de llenguatges d' A^* i $\varphi : A^* \longrightarrow B^*$ un homomorfisme de monòides. Aleshores:

- (1) $\varphi[LK] = \varphi[L]\varphi[K]$.
- (2) $\varphi[L^*] = (\varphi[L])^*$.
- (3) $\varphi[\bigcup_{i \in \mathbb{N}} L_i] = \bigcup_{i \in \mathbb{N}} \varphi[L_i]$.

DEMOSTRACIÓ. Anem a veure que $\varphi[LK] = \varphi[L]\varphi[K]$. Siga $u \in LK$, per definició podem escriure $u = lk$ de manera que $l \in L$ i $k \in K$. Així, en ser φ un homomorfisme, tenim que

$$\varphi(u) = \varphi(lk) = \varphi(l)\varphi(k) \in \varphi[L]\varphi[K].$$

Per tant $\varphi[LK] \subseteq \varphi[L]\varphi[K]$.

Per a demostrar l'altra inclusió anem a procedir anàlogament, considerem $z \in \varphi[L]\varphi[K]$. Aleshores existeix $x \in L$ i $y \in K$ de manera que

$$z = \varphi(x)\varphi(y) = \varphi(xy) \in \varphi[LK].$$

En l'última igualtat hem aplicat que φ és un homomorfisme de monoides.

Per tant $\varphi[L]\varphi[K] \subseteq \varphi[LK]$.

En segon lloc, anem a veure que $\varphi[L^*] = (\varphi[L])^*$. Siga $w \in (\varphi[L])^*$, per definició existeix un $n \in \mathbb{N}$ de manera que $w = w_0w_1 \cdots w_{n-1}$ on $w_0, w_1, \dots, w_{n-1} \in \varphi[L]$. Així per a cada $i \in \{0, 1, \dots, n-1\}$, existeixen $u_0, u_1, \dots, u_{n-1} \in L$ tal que $\varphi(u_i) = w_i$. Per tant:

$$w = \varphi(u_0)\varphi(u_1) \cdots \varphi(u_{n-1}) = \varphi(u_0u_1 \cdots u_{n-1}).$$

L'última igualtat es conseqüència de que φ és homomorfisme. Com que $u_0u_1 \cdots u_{n-1} \in L^*$, obtenim que $w \in \varphi[L^*]$.

Per a l'altra inclusió, siga $w \in L^*$, per definició existeix $n \in \mathbb{N}$ de manera que $w \in L^n$. Aleshores existeixen $w_0, \dots, w_{n-1} \in L$ de manera que

$$w = w_0 \cdots w_{n-1}.$$

Per tant, aplicant que φ es un homomorfisme:

$$\varphi(w) = \varphi(w_0 \cdots w_{n-1}) = \varphi(w_0) \cdots \varphi(w_{n-1}) \in (\varphi[L])^*,$$

ja que $\varphi(w_i) \in \varphi[L]$ per a cada $i \in \{0, \dots, n-1\}$.

Per últim demostrem que $\varphi[\bigcup_{i \in n} L_i] = \bigcup_{i \in n} \varphi[L_i]$. Per a la primera inclusió, siga $w \in \varphi[\bigcup_{i \in n} L_i]$, aleshores tenim que existeix $u \in \bigcup_{i \in n} L_i$ de manera que $w = \varphi(u)$, per tant existeix $i \in n$ tal que $u \in L_i$. Així:

$$w = \varphi(u) \in \varphi[L_i].$$

En conclusió, existeix un $i \in n$ de manera que $w \in \varphi[L_i]$, per tant $\varphi[\bigcup_{i \in n} L_i] \subseteq \bigcup_{i \in n} \varphi[L_i]$.

Per a l'altra inclusió, siga $w \in \bigcup_{i \in n} \varphi[L_i]$, aleshores existeix $i \in n$ de manera que $w \in \varphi[L_i]$, per tant existeix $u \in L_i$ tal que $w = \varphi(u)$. Tenim que $w \in \varphi[L_i]$ i $u \in L_i$, aleshores $u \in \bigcup_{i \in n} L_i$. Així:

$$w = \varphi(u) \in \varphi[\bigcup_{i \in n} L_i].$$

Açò conclou la demostració. □

A continuació presentem un dels conceptes que ens acompanyarà al llarg del treball, el conjunt de llenguatges racionals.

DEFINICIÓ 2.9. *Si A és un alfabet, aleshores definim el conjunt dels llenguatges racionals, denotat per $\text{Rat}(A^*)$, com el menor subconjunt d' A^* que satisfà:*

- (1) $\emptyset, \{\lambda\}, \{a\} \subseteq \text{Rat}(A^*)$, per a tot $a \in A$.
- (2) Si $(L_i)_{i \in n}$ és una família finita de llenguatges en $\text{Rat}(A^*)$ aleshores $\bigcup_{i \in n} L_i \in \text{Rat}(A^*)$.
- (3) Si L, K són llenguatges en $\text{Rat}(A^*)$ aleshores $LK \in \text{Rat}(A^*)$.
- (4) Si L és llenguatge en $\text{Rat}(A^*)$ aleshores $L^* \in \text{Rat}(A^*)$.

EXEMPLE 2.10. *Siga A un alfabet finit per al què $a \in A$ és una lletra, i L el llenguatge donat per*

$$L = \{w \in A^* \mid |w|_a = 0\}.$$

És a dir, L és el llenguatge que no conté paraules amb la lletra a . Notem que $A \setminus \{a\}$ és finit ja que A és finit, i per tant, és racional per ser la unió finita de llenguatges racionals. Així, $L = (A \setminus \{a\})^$ és racional perquè és el producte estrella d'un llenguatge racional.*

PROPOSICIÓ 2.11. *Siguen A i B alfabetes i siga $\varphi : A^* \longrightarrow B^*$ un homomorfisme de monoides. Si L és un llenguatge racional d' A^* , aleshores $\varphi[L]$ és un llenguatge racional de B^* .*

DEMOSTRACIÓ. Ho provarem per inducció.

Cas base

En el cas del buit, és trivial. $\varphi[\emptyset] = \emptyset \in \text{Rat}(B^*)$.

Per al cas de la paraula buida, com que φ és homomorfisme de monoides es compleix que $\varphi[\{\lambda\}] = \{\lambda\} \in \text{Rat}(B^*)$

Si a és una lletra en A , aleshores $\varphi[\{a\}] = \{\varphi(a)\} \in \text{Rat}(B^*)$.

Pas inductiu

Siga $(L_i)_{i \in n}$ una família de llenguatges racionals en $\text{Rat}(A^*)$ per a la que $\varphi[L_i] \in \text{Rat}(B^*)$ per a tot $i \in n$. Aleshores, pel Lema 2.8 tenim:

$$\varphi[\bigcup_{i \in n} L_i] = \bigcup_{i \in n} \varphi[L_i] \in \text{Rat}(B^*).$$

Siguen L i K dos llenguatges racionals en $\text{Rat}(A^*)$ tals que $\varphi[L], \varphi[K] \in \text{Rat}(B^*)$. Aplicant el Lema 2.8 tenim:

$$\varphi[LK] = \varphi[L]\varphi[K] \in \text{Rat}(B^*).$$

Siga L un llenguatge racional en $\text{Rat}(A^*)$ tal que $\varphi[L] \in \text{Rat}(B^*)$. Pel Lema 2.8 tenim:

$$\varphi[L^*] = (\varphi[L])^* \in \text{Rat}(B^*).$$

Queda així demostrada la proposició. □

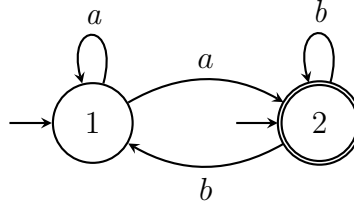


FIGURA 2.1. Autòmat de l'Exemple 2.13.

2. Autòmats finits i llenguatges reconeixibles

En aquesta secció presentem l'objecte d'estudi d'aquest treball: l'autòmat finit. També introduïrem el concepte de llenguatge reconeixible, aquell que pot ser acceptat per un autòmat finit. A més, veurem un teorema que ens proporciona una ferramenta per a identificar els llenguatges que no són reconeixibles.

DEFINICIÓ 2.12. *Un autòmat finit és una 5-tupla donada per la següent expressió $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$, on $\mathcal{Q}$ és un conjunt finit anomenat conjunt d'estats, A és un alfabet, E és un subconjunt de $\mathcal{Q} \times A \times \mathcal{Q}$ anomenat conjunt de transicions, i I i F són subconjunts de $\mathcal{Q}$ anomenats conjunt d'estats inicials i conjunt d'estats finals, respectivament.*

Notem que $\mathcal{A}$ és finit si $\mathcal{Q}$ és finit. En aquest cas podem representar l'autòmat $\mathcal{A}$ per un graf etiquetat d'acord a les transicions en E . A més, els estats inicials tindran una fletxa d'entrada i els finals estaran encerclats.

EXEMPLE 2.13. *Considerem l'autòmat $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ donat pel conjunt d'estats $\mathcal{Q} = \{1, 2\}$, els estats inicials $I = \{1, 2\}$, l'estat final $F = \{2\}$, l'alfabet $A = \{a, b\}$ i les transicions*

$$E = \{(1, a, 1), (2, b, 1), (1, a, 2), (2, b, 2)\}.$$

Este autòmat està representat en la Figura 2.1.

DEFINICIÓ 2.14. *Siga $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ un autòmat i siguen $p, p', q, q' \in \mathcal{Q}$ i $a, a' \in A$. Direm que dues transicions (p, a, q) i (p', a', q') són consecutives si $q = p'$. Un camí en un autòmat $\mathcal{A}$ és una seqüència de transicions consecutives*

$$c = (q_0, a_0, q_1), (q_1, a_1, q_2), \dots, (q_{n-1}, a_{n-1}, q_n)$$

també denotat per

$$c : q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} \dots \xrightarrow{a_{n-1}} q_n.$$

Un camí en $\mathcal{A}$ s'anomena inicial si q_0 és un estat inicial i final si q_n és un estat final. Un camí és exitós (o acceptat) si és inicial i final.

EXEMPLE 2.15. Considerem l'autòmat representat en la Figura 2.1. El camí

$$c : 1 \xrightarrow{a} 1 \xrightarrow{a} 2 \xrightarrow{b} 2 \xrightarrow{b} 1 \xrightarrow{a} 2 \xrightarrow{b} 2$$

és un camí exitós perquè comença en un estat inicial i acaba en un estat final. En canvi, el camí

$$c : 1 \xrightarrow{a} 1 \xrightarrow{a} 2 \xrightarrow{b} 2 \xrightarrow{b} 1 \xrightarrow{a} 2 \xrightarrow{b} 1$$

està igualment etiquetat, però no és exitós perquè acaba en 1, que no és un estat final.

NOTA 2.16. D'igual forma que hem definit les transicions d'un estat q a un altre estat q' mitjançant una lletra a , podem expandir aquest concepte i definir les transicions entre dos estats mitjançant una paraula.

Considerem l'autòmat $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ i el conjunt

$$\text{End}(\mathcal{P}(\mathcal{Q})) = \{f : \mathcal{P}(\mathcal{Q}) \longrightarrow \mathcal{P}(\mathcal{Q}) \mid f \text{ aplicació}\}$$

Notem que $\text{End}(\mathcal{P}(\mathcal{Q}))$ té estructura de monoide amb la composició d'aplicacions i la identitat com a neutre. Siga:

$$\begin{array}{ccc} E : A & \longrightarrow & \text{End}(\mathcal{P}(\mathcal{Q})) \\ a & \longmapsto & E_a : \mathcal{P}(\mathcal{Q}) \longrightarrow \mathcal{P}(\mathcal{Q}) \\ & & P \longmapsto P(a) \end{array}$$

on $P(a) = \{q \in \mathcal{Q} \mid \exists p \in P, (p, a, q) \in E\}$.

Com que $\text{End}(\mathcal{P}(\mathcal{Q}))$ és un monoide, per la Propietat Universal del monoide lliure podem estendre E a un únic homomorfisme

$$\begin{array}{ccc} E^\# : A^* & \longrightarrow & \text{End}(\mathcal{P}(\mathcal{Q})) \\ w & \longmapsto & E_w^\# \end{array}$$

de manera que $E^\# \circ \text{in}_A = E$. Notem que, per a un conjunt $P \in \mathcal{P}(\mathcal{Q})$, $E_w^\#(P)$ és el conjunt d'estats als quals es pot accedir des de P amb un camí etiquetat amb w .

DEFINICIÓ 2.17. Siga $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ un autòmat, definim $L_{\mathcal{A}} = \{w \in A^* \mid E_w^\#(I) \cap F \neq \emptyset\}$ com el llenguatge que reconeix l'autòmat $\mathcal{A}$. És a dir, reconeix les paraules w que etiqueten un camí exitós en A . Direm que dos autòmats $\mathcal{A}$ i $\mathcal{A}'$ són equivalents si $L_{\mathcal{A}} = L_{\mathcal{A}'}$.

DEFINICIÓ 2.18. Un llenguatge $L \subseteq A^*$ s'anomena reconeixible si existeix un autòmat finit $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ de manera que $L = L_{\mathcal{A}}$. En aquest cas direm que el llenguatge L es reconegut per l'autòmat $\mathcal{A}$.

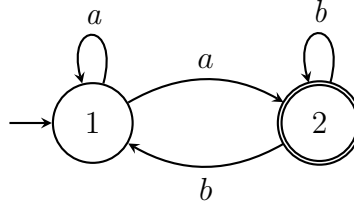


FIGURA 2.2. Autòmat de l'Exemple 2.19.

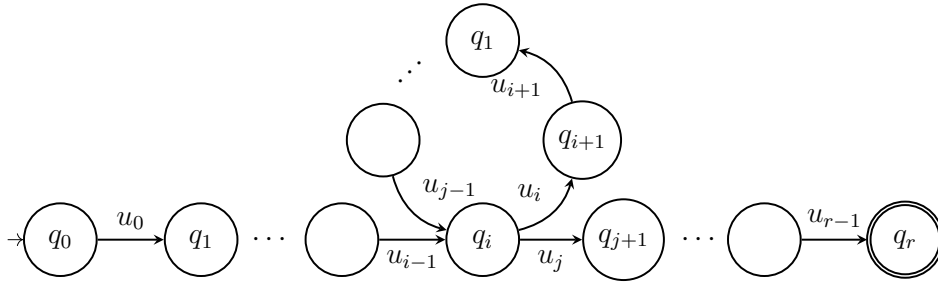


FIGURA 2.3. Lema del bombeig.

EXEMPLE 2.19. Podem veure que el llenguatge reconegut per l'autòmat de la Figura 2.2 és aA^* , el conjunt de paraules que comencen per la lletra a , ja que les fletxes que ixen de l'estat inicial estan totes etiquetades amb la lletra a .

PROPOSICIÓ 2.20 (Pumping lemma o lema del bombeig). Siga A un alfabet i siga $L \subseteq A^*$ un llenguatge reconeixible. Aleshores existeix un enter $n > 0$ de manera que tota paraula u de L amb longitud major o igual que n pot ser factoritzada com $u = xyz$ amb $x, y, z \in A^*$, $|xy| \leq n$, $y \neq \epsilon$, i per a tot $k \geq 0$, $xy^kz \in L$.

DEMOSTRACIÓ. Com que L és reconeixible, siga $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ l'autòmat que reconeix L , és a dir, $L = L_{\mathcal{A}}$. Suposem que $|\mathcal{Q}| = n$. Anem a veure que n satisfà les condicions del teorema.

Siga $u \in L$ amb longitud $r \geq n$, tenim que $u = u_0 \cdots u_{r-1}$. Siga $q_0 \xrightarrow{u_0} q_1 \longrightarrow \cdots \longrightarrow q_{r-1} \xrightarrow{u_{r-1}} q_r$ un camí exitós en $\mathcal{A}$ etiquetat amb u . Pel principi del colomar, com $r \geq n$ existeixen dos estats inicials en l'anterior camí que són iguals, suposem $q_i = q_j$ amb $0 \leq i, j < r$ i $i \neq j$. Aleshores, la paraula $u_{i+1} \cdots u_j$ és l'etiqueta d'un bucle al voltant de q_i , representat en la Figura 2.3.

Siga $x = (u_k)_{k \in [0, i]}$, $y = (u_k)_{k \in [i+1, j]}$ i $z = (u_k)_{k \in [j+1, r-1]}$. Notem que $|xy| \leq n$ i per a tot $k \geq 0$, tenim que $xy^kz \in L$, ja que xy^kz és l'etiqueta d'un camí exitós. $\square$

EXEMPLE 2.21. *El lema del bombeig permet veure que el llenguatge $L = \{a^n b^n \mid n \geq 0\}$ no és reconeixible. Suposem que L fora reconeixible, aleshores existeix un autòmat $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ finit que el reconeix. Suposem $|\mathcal{Q}| = m$. Siga la paraula $a^m b^m$. Pel Lema del bombeig podem factoritzar $a^m b^m = xyz$ i a més $xy^k z \in L$, $y \neq \lambda$ i $|xy| \leq m$. Tenim dos possibles casos:*

Primer cas: Suposem que y sols conté “a” o “b”. En particular que y sols tinga “a”, aleshores $y = a^l$ amb $l > 0$. Per tant, $xy^k z = x(a^l)^k z$ que no pertany al llenguatge L ja que no conté el mateix nombre de “a” i de “b”, entra en contradicció amb la definició del llenguatge. Analogament si y només conté “b”.

Segon cas: Suposem que y conté tant “a” com “b”. Aleshores $y = a^l b^r$ amb $l, r > 0$. Per tant, $xy^k z = x(a^l b^r)^k z = x(a^l)^k (b^r)^k z$ que novament no pertany al llenguatge L . Per la descomposició que hem de fer no tindrà el mateix nombre de “a” que de “b”.

Per tant podem concloure que el llenguatge L no és reconeixible.

3. Autòmats deterministes

Presentarem la noció d'autòmat finit determinista, que són una classe específica d'autòmats finits. Més avant, estudiarem el seu funcionament i veurem la seua capacitat de reconeixement de llenguatges.

DEFINICIÓ 2.22. *Un autòmat $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ és determinista si I conté exactament un estat inicial i si, per a tot estat $q \in \mathcal{Q}$ i per a tota lletra $a \in A$, sols existeix un estat q' de manera que $q \xrightarrow{a} q'$ és una transició en E . En aquest cas les transicions es poden veure com una aplicació de $\mathcal{Q} \times A$ en $\mathcal{Q}$ que denotarem per $\cdot$. Si q_0 és l'únic estat inicial, denotarem l'autòmat per $\mathcal{A} = (\mathcal{Q}, A, E, q_0, F)$ o per $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ segons convinga.*

PROPOSICIÓ 2.23. *Tot autòmat finit és equivalent a un autòmat determinista.*

DEMOSTRACIÓ. Siga $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ un autòmat. Considerem l'autòmat determinista donat per $D(\mathcal{A}) = (\mathcal{P}(\mathcal{Q}), A, E, I, \mathcal{F})$ on $\mathcal{F} = \{P \subseteq \mathcal{Q} \mid P \cap F \neq \emptyset\}$ i l'aplicació $E_a(P)$ definida en la Nota 2.16.

Anem a veure que $D(\mathcal{A})$ és equivalent a $\mathcal{A}$.

Si $u = (u_k)_{k \in \mathbb{N}}$ és una paraula acceptada per $\mathcal{A}$, aleshores hi ha un camí exitós per a u

$$c : q_0 \xrightarrow{u_0} q_1 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{u_{n-1}} q_n$$

La paraula u també defineix un camí

$$I = P_0 \xrightarrow{u_0} P_1 \longrightarrow \cdots \longrightarrow P_{n-1} \xrightarrow{u_{n-1}} P_n$$

en $D(\mathcal{A})$.

Podem provar per inducció sobre i que, per a $0 \leq i \leq n$, $q_i \in P_i$.

Si c és un camí exitós, es té que $q_0 \in I = P_0$. Suposem que $q_{i-1} \in P_{i-1}$. Aleshores $q_{i-1} \xrightarrow{u_i} q_i$ és una transició, obtenim que $q_i \in E_{u_i}(P_{i-1}) = P_i$. Per a $i = n$, tenim que $q_n \in P_n$ i que si c és un camí existós, $q_n \in F$. Per tant $P_n \in \mathcal{F}$. Aleshores u és acceptada per $D(\mathcal{A})$.

D'altra banda, siga $u = (u_k)_{k \in n}$ una paraula acceptada per $D(\mathcal{A})$ i siga

$$I = P_0 \xrightarrow{u_0} P_1 \longrightarrow \cdots \longrightarrow P_{n-1} \xrightarrow{u_{n-1}} P_n$$

el camí exitós definit per u . Si P_n és un estat final, podem triar un element $q_m \in P_n \cap F$. Podem ara seleccionar per a $i \in n$ un element q_{i-1} de P_{i-1} de manera que $q_{i-1} \xrightarrow{u_i} q_i$ és una transició de $\mathcal{A}$. Si $q_0 \in I$ i $q_n \in F$, el camí

$$q_0 \xrightarrow{u_0} q_1 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{u_{n-1}} q_n$$

és exitós, i per tant u és una paraula acceptada per $\mathcal{A}$. $\square$

NOTA 2.24. *La construcció presentada en la Proposició 2.23 converteix un autòmat no determinista d' n estats en un autòmat determinista amb 2^n estats.*

4. Autòmats complets, accessibles, coaccessibles i ajustats

En aquesta secció veurem els conceptes d'autòmat complet, accessible, coaccessible i ajustat, que es refereixen a diferents propietats dels autòmats finits.

DEFINICIÓ 2.25. *Un autòmat $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ és complet si, per a cada estat $q \in \mathcal{Q}$ i per a cada lletra $a \in A$, hi ha almenys un estat q' de manera que $q \xrightarrow{a} q'$ és una transició.*

EXEMPLE 2.26. *L'autòmat representat en la Figura 2.4 no és complet ni determinista. No és determinista perquè les transicions $(1, a, 1)$ i $(1, a, 2)$ estan etiquetades igual i tenen el mateix origen. No és complet perquè no hi ha cap transició de la forma $2 \xrightarrow{a} q$. D'altra banda, l'autòmat representat en la Figura 2.5 és complet i determinista.*

DEFINICIÓ 2.27. *Un autòmat $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ és accessible si tots els estats són accessibles, és a dir, si existeix un camí des d'un estat inicial a qualsevol altre estat. I és coaccessible si per a cada estat final existeix almenys un camí que el connecta amb un estat inicial. Finalment, un autòmat és ajustat si es simultàniament accessible i coaccessible.*

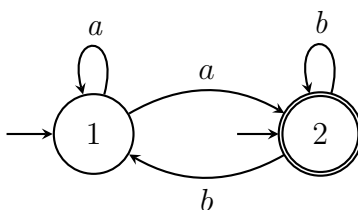


FIGURA 2.4. Autòmat no complet i no determinista.

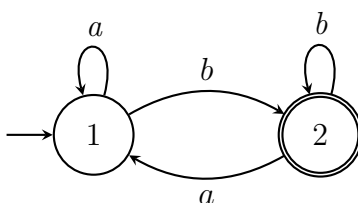


FIGURA 2.5. Autòmat complet i determinista.

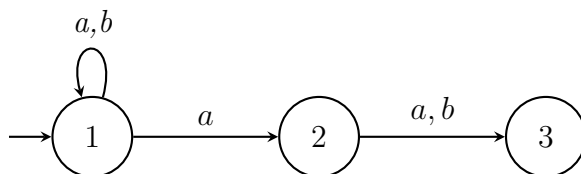


FIGURA 2.6. Autòmat no determinista.

PROPOSICIÓ 2.28. *Tot autòmat determinista és equivalent a un autòmat ajustat.*

DEMOSTRACIÓ. Considerem un autòmat determinista. Ens quedem amb aquell subconjunt d'estats als quals es pot accedir des de l'estat inicial. Este autòmat és determinista i ajustat. A més reconeix el mateix llenguatge ja que hem preservat els estats i transicions rellevants per al reconeixement de paraules. $\square$

EXEMPLE 2.29. Considerem el llenguatge $A = \{a, b\}$. Considerem l'autòmat no determinista representat en la Figura 2.6, després obtenim un autòmat determinista $D(\mathcal{A})$ en funció de la construcció vista en la Proposició 2.23, representat en la Figura 2.7. Ara ens quedem sols amb els estats que són accessibles, així ens queda l'autòmat de la Figura 2.8.

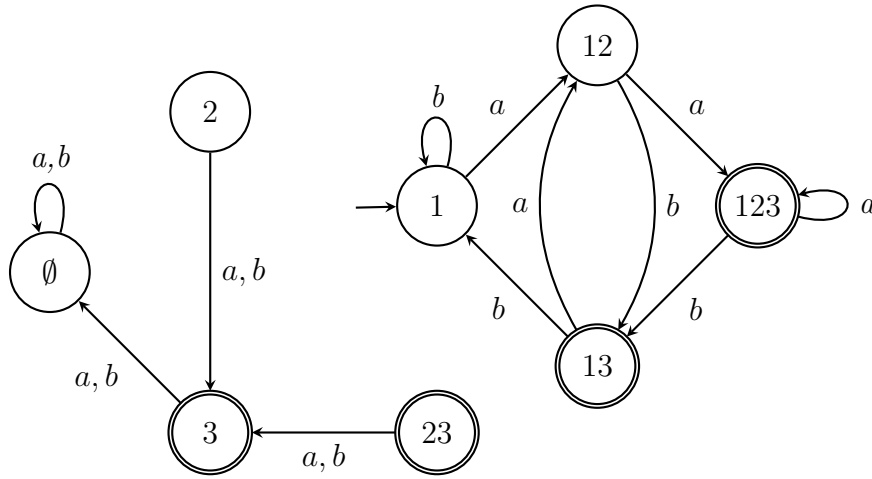


FIGURA 2.7. Autòmat determinista equivalent a l'autòmat de la Figura 2.6 obtingut seguint el procediment de la Proposició 2.23.

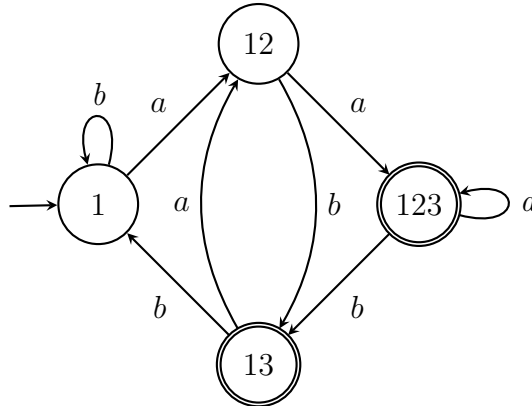


FIGURA 2.8. Autòmat determinista i ajustat equivalent a l'autòmat de la Figura 2.7 obtingut seguint el procediment de la Proposició 2.28.

5. Autòmat estàndard

La construcció que anem a fer en aquest apartat sembla un poc artificial, però l'utilitzarem més endavant en l'estudi de les operacions producte i estrellà.

DEFINICIÓ 2.30. *Un autòmat determinista és estàndard si no té cap transició que acabe en l'estat inicial.*

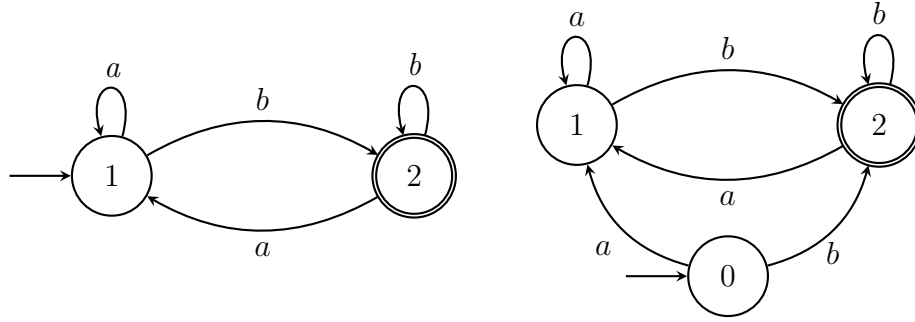


FIGURA 2.9. Autòmat i la seua estandardització.

PROPOSICIÓ 2.31. *Tot autòmat determinista és equivalent a un autòmat determinista estàndard.*

DEMOSTRACIÓ. Siga $\mathcal{A} = (\mathcal{Q}, A, E, q_0, F)$ un autòmat determinista. Si $\mathcal{A}$ no és estàndard, siga p un nou estat i $\mathcal{A}' = (\mathcal{Q} \cup \{p\}, A, E', p, F')$ és un autòmat estàndard definit per $E' = E \cup \{(p, a, q) \mid (q_0, a, q) \in E\}$ i que té com a conjunt d'estats finals

$$F' = \begin{cases} F & \text{si } q_0 \notin F; \\ F \cup \{p\} & \text{si } q_0 \in F. \end{cases}$$

Aleshores el camí

$$q_0 \xrightarrow{a_0} q_1 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{a_{n-1}} q_n$$

és exitós en $\mathcal{A}$ si, i sols si, el camí

$$p \xrightarrow{a_0} q_1 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{a_{n-1}} q_n$$

és exitós en $\mathcal{A}'$.

Per tant, $\mathcal{A}$ i $\mathcal{A}'$ són equivalents. $\square$

EXEMPLE 2.32. *Anem a veure un exemple d'estandardització d'un autòmat. Es pot veure a la Figura 2.9 on l'autòmat de l'esquerra és l'original i a la dreta es troba la seua estandardització que hem obtés fent servir la Proposició 2.31.*

CAPÍTOL 3

Operacions i llenguatges reconeixibles

En aquest capítol anem a veure com es poden obtenir nous llenguatges reconeixibles a partir d'altres que ja sabem que són reconeixibles. Per a fer-ho, considerarem les operacions booleanes, el producte, l'operació estrella, quocients i imatges inverses de morfismes.

1. Operacions booleanes

En aquest apartat considerem les operacions d'unió, intersecció i complement.

PROPOSICIÓ 3.1. *L'unió de dos llenguatges reconeixibles és reconeixible.*

DEMOSTRACIÓ. Siguen L, L' dos llenguatges reconeixibles d' A^* , reconeguts pels autòmats $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ i $\mathcal{A}' = (\mathcal{Q}', A, E', I', F')$, respectivament.

Suposem que $\mathcal{Q}$ i $\mathcal{Q}'$ són conjunts disjunts. De manera que podem identificar E i E' amb subconjunts de $(\mathcal{Q} \cup \mathcal{Q}') \times A \times (\mathcal{Q} \cup \mathcal{Q}')$. Aleshores $L \cup L'$ és reconeixible per l'autòmat $(\mathcal{Q} \cup \mathcal{Q}', A, E \cup E', I \cup I', F \cup F')$. $\square$

EXEMPLE 3.2. Si L i L' són reconeguts pels autòmats $\mathcal{A}$ i $\mathcal{A}'$, respectivament, representats a la Figura 3.1. Aleshores $L \cup L'$ és reconegut per l'autòmat representat en la Figura 3.2.

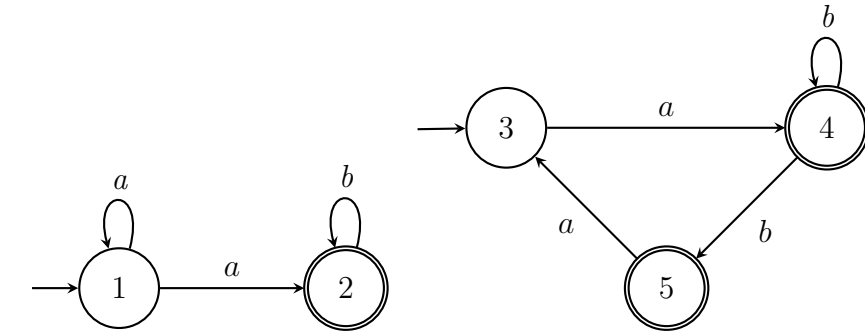


FIGURA 3.1. Autòmats $\mathcal{A}$ i $\mathcal{A}'$ de l'Exemple 3.2.

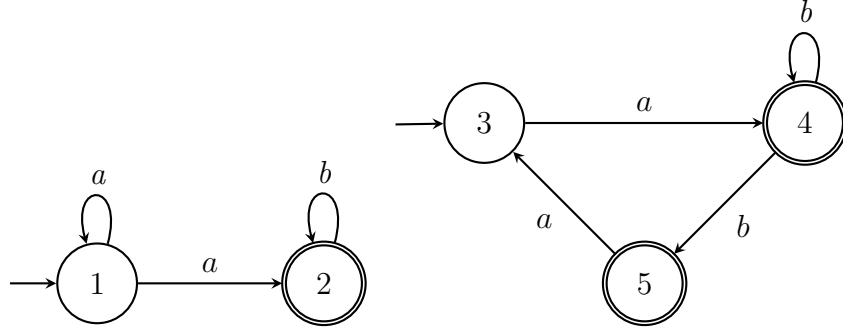


FIGURA 3.2. Autòmat que reconeix $L \cup L'$ de l'Exemple 3.2.

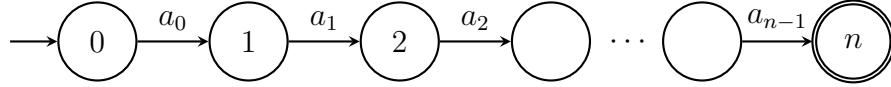


FIGURA 3.3. Autòmat que reconeix $(a_k)_{k \in \mathbb{N}}$.

DEMOSTRACIÓ. Com que els llenguatges reconeixibles són tancats sota la unió, és suficient provar que cada paraula és reconeixible. Però és clar que el llenguatge $\{(a_k)_{k \in \mathbb{N}}\}$ és reconegut per l'autòmat representat en la Figura 3.3. $\square$

PROPOSICIÓ 3.4. *La intersecció de dos llenguatges reconeixibles és reconeixible.*

DEMOSTRACIÓ. Siguen L i L' llenguatges reconeixibles d' A^* reconeguts pels autòmats $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$ i $\mathcal{A}' = (\mathcal{Q}', A, E', I', F')$, respectivament. Considerem l'autòmat $\mathcal{B} = (\mathcal{Q} \times \mathcal{Q}', A, T, I \times I', F \times F')$, on:

$$T = \{((q_1, q'_1), a, (q_2, q'_2)) \mid (q_1, a, q_2) \in E \text{ i } (q'_1, a, q'_2) \in E'\}$$

La paraula $u = (u_k)_{k \in \mathbb{N}}$ és l'etiqueta d'un camí exitós en $\mathcal{B}$

$$(q_0, q'_0) \xrightarrow{u_0} (q_1, q'_1) \longrightarrow \cdots \longrightarrow (q_{n-1}, q'_{n-1}) \xrightarrow{u_{n-1}} (q_n, q'_n)$$

si, i sols si, els camins

$$q_0 \xrightarrow{u_0} q_1 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{u_{n-1}} q_n$$

$$q'_0 \xrightarrow{u_0} q'_1 \longrightarrow \cdots \longrightarrow q'_{n-1} \xrightarrow{u_{n-1}} q'_n$$

són camins exitosos en $\mathcal{A}$ i $\mathcal{A}'$ respectivament. Per tant, $\mathcal{B}$ reconeix $L \cap L'$. $\square$

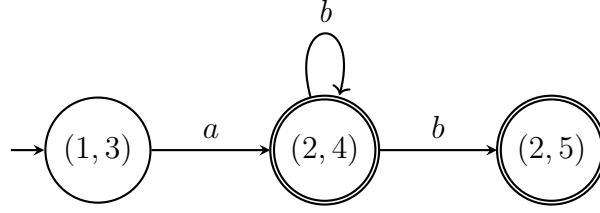


FIGURA 3.4. Autòmat ajustat que reconeix $L \cap L'$ de l'Exemple 3.2.

NOTA 3.5. En relació a la Proposició 3.4, sols es calcula l'autòmat ajustat de l'autòmat producte.

EXEMPLE 3.6. Siguen L i L' els llenguatges reconeguts pels autòmats $\mathcal{A}$ i $\mathcal{A}'$ respectivament, representats en la Figura 3.1. Aleshores fent servir la construcció de la Proposició 3.4, $L \cap L'$ es reconegut per l'autòmat ajustat representat en la Figura 3.4.

PROPOSICIÓ 3.7. El complementari d'un llenguatge reconeixible és un llenguatge reconeixible.

DEMOSTRACIÓ. Siga L un llenguatge reconeixible d' A^* i siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista complet que reconeix L . Aleshores l'autòmat $\mathcal{A}' = (\mathcal{Q}, A, \cdot, q_0, \mathcal{Q} - F)$ reconeix $A^* - L$. De fet, com que $\mathcal{A}$ i $\mathcal{A}'$ són ahora deterministes i complets, tota paraula u d' A^* és l'etiqueta d'exactament un camí que comença per q_0 . Siga q el final d'aquest camí. Aleshores u pertany a L si, i sols si, q pertany a F i u pertany a $A^* - L$ si, i sols si, q pertany a $\mathcal{Q} - F$. $\square$

EXEMPLE 3.8. El llenguatge $(ab)^*$ es reconegut per l'autòmat determinista complet $\mathcal{A}$ que es troba a la Figura 3.5, i el seu complementari és reconegut per l'autòmat $\mathcal{A}'$ representat en la Figura 3.5 resultat d'aplicar la Proposició 3.7.

2. Producte

En aquesta secció anem a veure com construir nous llenguatges reconeixibles a partir de l'operació producte i d'altres llenguatges reconeixibles. També ho il·lustrarem amb un exemple.

PROPOSICIÓ 3.9. El producte de dos llenguatges reconeixibles és reconeixible.

DEMOSTRACIÓ. Siguen L_1 i L_2 dos llenguatges reconeixibles d' A^* que són reconeguts pels autòmats $\mathcal{A}_1 = (\mathcal{Q}_1, A, E_1, I_1, F_1)$ i $\mathcal{A}_2 =$

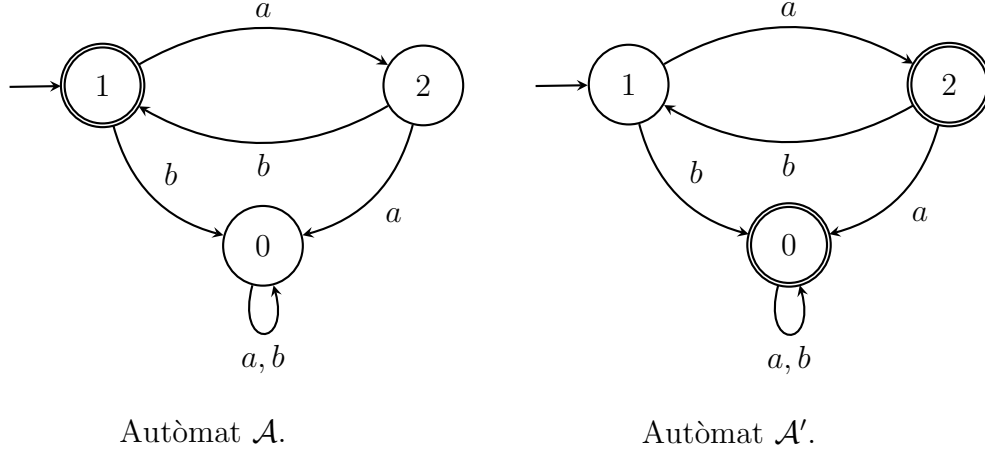
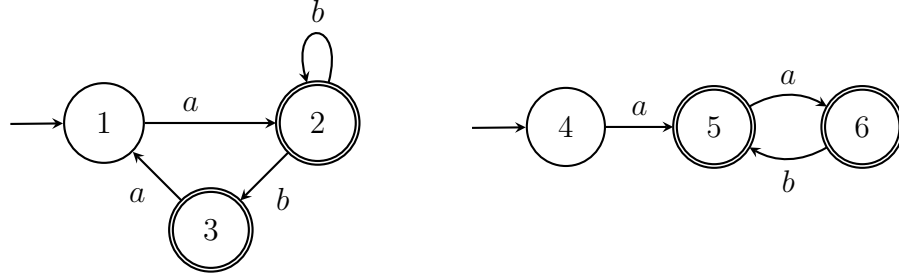


FIGURA 3.5. Complementació d'un autòmat determinista segons la Proposició 3.7.

$(\mathcal{Q}_2, A, E_2, I_2, F_2)$, respectivament. Podem suposar, per les Proposicions 2.23 i 2.31, que $\mathcal{A}_2$ és un autòmat estàndard determinista i, per tant, en particular $I_2 = \{i\}$. També podem suposar que $\mathcal{Q}_1$ i $\mathcal{Q}_2$ són disjunts. Siga ara $\mathcal{A} = (\mathcal{Q}, A, E, I, F)$, on:

$$\begin{aligned}
 \mathcal{Q} &= (\mathcal{Q}_1 \cup \mathcal{Q}_2) \setminus \{i\}; \\
 E &= E_1 \cup \{(q, a, q') \in E_2 \mid q \neq i\} \cup \{(q_1, a, q') \mid q_1 \in F_1 \text{ i } (i, a, q') \in E_2\}; \\
 I &= I_1; \\
 F' &= \begin{cases} F_2 & \text{si } i \notin F_2; \\ F_1 \cup (F_2 \setminus \{i\}) & \text{si } i \in F_2. \end{cases}
 \end{aligned}$$

Anem a veure que $\mathcal{A}$ reconeix $L_1 L_2$. Si u és una paraula de $L_1 L_2$, aleshores $u = u_1 u_2$ per a algun $u_1 \in L_1$ i $u_2 \in L_2$. Per tant, hi ha un camí exitós $c_1 : i_1 \xrightarrow{u_1} q_1$ en $\mathcal{A}_1$, amb $i_1 \in I_1$ i $q_1 \in F_1$, i hi ha un camí exitós $c_2 : i \xrightarrow{u_2} q_2$ en $\mathcal{A}_2$, amb $q_2 \in F_2$. Si $u_2 = \lambda$, aleshores L_2 conté la paraula buida i el camí c_1 és un camí exitós en $\mathcal{A}$ i u és acceptada per $\mathcal{A}$. Si u_2 no és la paraula buida, siga a la primera lletra de u_2 i siga $i \xrightarrow{a} q$ la primera transició de c_2 . Com que $q_1 \in F_1$, $q_1 \xrightarrow{a} q$ és per definició una transició d' E . A més, si $q' \xrightarrow{b} q''$ és una transició de c_2 diferent de la primera transició, llavors q' és el final de la transició d' $\mathcal{A}_2$. Com que $\mathcal{A}_2$ és estàndard, implica que $q' \neq i$, de la definició d' E , la transició $q' \xrightarrow{b} q''$ és també una transició d' $\mathcal{A}$. Siga c'_2 un camí d' $\mathcal{A}$ obtés reemplaçant en c_2 la primera transició $i \xrightarrow{a} q$ per $q_1 \xrightarrow{a} q$. El camí resultant $c_1 c'_2$ és un camí exitós en $\mathcal{A}$ d'etiqueta u i, per tant, és acceptat per $\mathcal{A}$.

FIGURA 3.6. Autòmats $\mathcal{A}_1$ i $\mathcal{A}_2$ de l'Exemple 3.10.

Per contra, siga u una paraula acceptada per $\mathcal{A}$. Llavors u és l'etiqueta d'un camí exitós $c : i_1 \xrightarrow{u} f$ d' $\mathcal{A}$. Com que els estats inicials d' $\mathcal{A}$ estan continguts en $\mathcal{Q}_1$, i com que no és una transició d' $\mathcal{A}$ que comença en $\mathcal{Q}_2$ i acaba en $\mathcal{Q}_1$, c visita primer alguns estats de $\mathcal{Q}_1$ i després possiblement alguns de $\mathcal{Q}_2$. Si tots els estats visitats per c estan en $\mathcal{Q}_1$, un ha de ser en particular $f \in \mathcal{Q}_1$. Però açò és possible sols si $\lambda \in L_2$, i en aquest cas, c és també un camí exitós d' $\mathcal{A}_1$, i per tant $u \in L_1 \subseteq L_1 L_2$. Si c visita alguns estats de $\mathcal{Q}_2$, aleshores c conté una única transició de la forma $e = (q_1, a, q_2)$ amb $q_1 \in F_1$ i $q_2 \in \mathcal{Q}_2$. Per tant, $c = c_1 e c_2$, on c_1 és un camí en $\mathcal{A}_1$ i c_2 és un camí en $\mathcal{A}_2$. Denotant per u_1 i u_2 l'etiqueta de c_1 i c_2 respectivament, tenim que $u = u_1 a u_2$. Com que c_1 és un camí exitós en $\mathcal{A}_1$, tenim que $u_1 \in L_1$. A més, per definició d' E , $e' = (i, a, q_2)$ és una transició d' $\mathcal{A}_2$. Per tant, el camí $e' c_2$ és un camí exitós en $\mathcal{A}_2$ amb etiqueta $a u_2$. D'açò se segueix que $u \in L_1 L_2$, demostrant la proposició. $\square$

EXEMPLE 3.10. Si L_1 i L_2 són llenguatges reconeguts pels autòmats $\mathcal{A}_1$ i $\mathcal{A}_2$ representats en la Figura 3.6, aleshores $L_1 L_2$ és reconegut per l'autòmat representat en la Figura 3.7 després d'aplicar la construcció vista en la Proposició 3.9.

3. Estrella

A continuació anem a veure com construir nous llenguatges reconeixibles mitjançant l'operació estrella i altres llenguatges reconeixibles. A més, veurem un exemple.

PROPOSICIÓ 3.11. *L'estrella d'un llenguatge reconeixible és un llenguatge reconeixible.*

DEMOSTRACIÓ. Siga L un llenguatge reconeixible d' A^* , reconegut per l'autòmat estàndard determinista $\mathcal{A} = (\mathcal{Q}, A, E, q_0, F)$. Siga $\mathcal{A}' =$

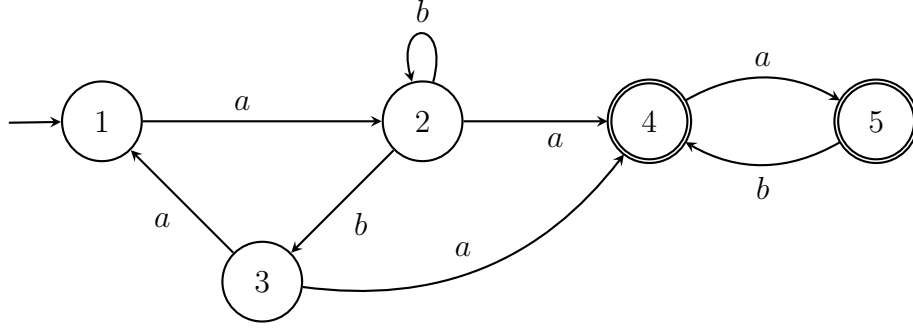


FIGURA 3.7. Autòmat que reconeix L_1L_2 segons la Proposició 3.9.

$(\mathcal{Q}, A, E', \{q_0\}, F \cup \{q_0\})$ un autòmat no determinista definit per:

$$E' = E \cup \{(q, a, q') \mid q \in F \text{ i } (q_0, a, q') \in E\}.$$

Anem a demostrar que $\mathcal{A}'$ reconeix L^* . Si u és una paraula de L^* , llavors u és la paraula buida, la qual és acceptada per $\mathcal{A}'$ ja que q_0 és un estat final, o $u = (u_k)_{k \in n}$ amb $u_0, \dots, u_{n-1} \in L - \{\lambda\}$. Cada u_i és l'etiqueta d'un camí exitós en $\mathcal{A}$, anomenem $c_i : q_0 \xrightarrow{u_i} q_i$ amb $q_i \in F$. Siga a_i la primera lletra d' u_i i siga i i siga $q_0 \xrightarrow{a_i} p_i$ la primera transició de c_i . Siga $i \in n$. Com $q_{i-1} \in F$, la definició d' E' mostra que $q_{i-1} \xrightarrow{a_i} p_i$ és una transició d' $\mathcal{A}'$. Denotem per c'_i el camí obtés de reemplaçar en c_i la primera transició $q_0 \xrightarrow{a_i} p_i$ per $q_{i-1} \xrightarrow{a_i} p_i$. Açò defineix per a $1 \leq i \leq n-1$, un camí $c'_i : q_{i-1} \xrightarrow{u_i} q_i$ en $\mathcal{A}'$. Aleshores, el camí $c_0c'_1 \dots c'_{n-1}$ és un camí exitós amb etiqueta u en $\mathcal{A}'$ i, per tant, u és acceptada per $\mathcal{A}'$.

Ara, siga u una paraula acceptada per $\mathcal{A}'$. Si $u = \lambda$ tenim que, $u \in L^*$. D'altra banda, u és l'etiqueta d'un camí exitós no buit c d' $\mathcal{A}'$. Este camí pot ser factoritzat com:

$$c = q_0 \xrightarrow{u_0} q_1 \xrightarrow{a_1} q'_1 \xrightarrow{u_1} q_2 \xrightarrow{a_2} q'_2 \longrightarrow \dots \longrightarrow q_n \xrightarrow{a_n} q'_n \xrightarrow{u_n} q_{n+1}$$

on les transicions $e_1 = q_1 \xrightarrow{a_1} q'_1$, $e_2 = q_2 \xrightarrow{a_2} q'_2$, $\dots$, $e_n = q_n \xrightarrow{a_n} q'_n$ són exactament transicions d' $E' - E$ que ocorren en c . Aleshores per definició d' E' , obtenim que, per a $i \in n$, $q_i \in F$ i $e'_i = (q_0, a_i, q'_i) \in E$. A més, $q_{n+1} \in F \cup \{q_0\}$ ja que c és un camí exitós. Per tant, els camins

$$q_0 \xrightarrow{a_i} q'_i \xrightarrow{u_i} q_{i+1}$$

són camins d' $\mathcal{A}$. Per a $i \in n$, aquests camins són exitosos, ja que $q_i \in F$. A més, com que $\mathcal{A}$ és estàndard, q_{n+1} és diferent de q_0 i per tant $q_{n+1} \in F$. Consegüentment $a_iu_i \in L$ per a $i \in n$. Com que

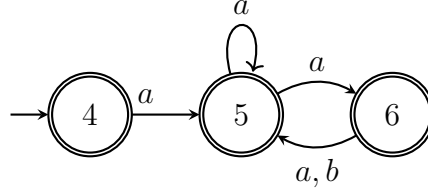


FIGURA 3.8. Autòmat que reconeix L^* de l'Exemple 3.12.

$q_0 \xrightarrow{u_0} q_1$ també és un camí exitós d' $\mathcal{A}$, també es té que $u_0 \in L$ i, per tant, $u \in L^*$. $\square$

EXEMPLE 3.12. Si L és un llenguatge reconegut per l'autòmat determinista estàndard $\mathcal{A}_2$ representat en la Figura 3.6, aleshores L^* és reconegut per l'autòmat no determinista representat en la Figura 3.8.

4. Quocients

En aquesta secció veurem que els quocients de llenguatges reconeixibles són reconeixibles també. Veurem primer els quocients per l'esquerra d'una paraula i després el cas general.

PROPOSICIÓ 3.13. Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista que reconeix el llenguatge L d' A^* . Aleshores, per a cada paraula u d' A^* el llenguatge $u^{-1}L$ és reconegut per l'autòmat $\mathcal{A}_u = (\mathcal{Q}, A, \cdot, q_0 \cdot u, F)$, obtingut a partir d' $\mathcal{A}$ canviant l'estat inicial.

DEMOSTRACIÓ. Notem que es donen les següents igualtats:

$$\begin{aligned}
 u^{-1}L &= \{v \in A^* \mid uv \in L\} \\
 &= \{v \in A^* \mid q_0 \cdot (uv) \in F\} \\
 &= \{v \in A^* \mid (q_0 \cdot u) \cdot v \in F\}.
 \end{aligned}$$

Per tant $u^{-1}L$ és acceptat per $\mathcal{A}_u$. $\square$

PROPOSICIÓ 3.14. Tot quocient d'un llenguatge reconeixible és reconeixible.

DEMOSTRACIÓ. Siga $(\mathcal{Q}, A, E, I, F)$ un autòmat que reconeix el llenguatge L d' A^* i siga K un llenguatge d' A^* . No assumim que K és reconeixible. Sent

$$I' = \{q \in \mathcal{Q} \mid q \text{ és el final del camí inicial amb etiqueta en } K\}$$

és senzill veure que l'autòmat $\mathcal{B} = (\mathcal{Q}, A, E, I', F)$ reconeix $K^{-1}L$. Per al llenguatge LK^{-1} , és una prova similar considerant l'autòmat

$(\mathcal{Q}, A, E, I, F')$, on

$$F' = \{q \in \mathcal{Q} \mid q \text{ és l'origen d'un camí final amb etiqueta en } K\}.$$

Açò conclou la demostració. $\square$

5. Inverses de morfismes

Anem a demostrar que els llenguatges reconeixibles són tancats per a inverses de morfismes.

PROPOSICIÓ 3.15. *Siga $\varphi : A^* \longrightarrow B^*$ un homomorfisme de monoides. Si L és un llenguatge reconeixible de B^* , aleshores $\varphi^{-1}[L]$ és un llenguatge reconeixible d' A^* .*

DEMOSTRACIÓ. Siga $\mathcal{B} = (\mathcal{Q}, B, E, I, F)$ un autòmat que reconeix L i siga $\mathcal{A} = (\mathcal{Q}, A, T, I, F)$ on

$$T = \{(p, a, q) \mid \text{hi ha un camí etiquetat per } \varphi(a) \text{ des de } p \text{ fins a } q \text{ en } \mathcal{B}\}$$

Vegem que $\mathcal{A}$ reconeix $\varphi^{-1}[L]$. Primer, si u és acceptada per $\mathcal{A}$, hi ha un camí exitós en $\mathcal{A}$ etiquetat per u . Consegüentment, hi ha un camí exitós en $\mathcal{B}$ etiquetat per $\varphi(u)$. Aleshores $\varphi(u)$ és acceptat per $\mathcal{B}$ i $u \in \varphi^{-1}[L]$.

Siga ara $u = (u_k)_{k \in n}$ una paraula de $\varphi^{-1}[L]$. Com que la paraula $\varphi(u)$ és acceptada per $\mathcal{B}$, hi ha un camí exitós en $\mathcal{B}$ etiquetat per $\varphi(u)$. Anem a factoritzar aquest camí com

$$q_0 \xrightarrow{\varphi(u_0)} q_1 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{\varphi(u_{n-1})} q_n$$

Aquests camins defineixen al mateix temps un camí exitós en $\mathcal{B}$ etiquetat per u :

$$q_0 \xrightarrow{u_0} q_1 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{u_{n-1}} q_n$$

que demostra que u és acceptada per $\mathcal{A}$. $\square$

CAPÍTOL 4

Autòmat minimal i monoide sintàctic

L'autòmat minimal i el monoide sintàctic són dos conceptes importants en la teoria d'autòmats i llenguatges formals. En aquest capítol veurem com es relacionen entre ells i amb el concepte de llenguatge reconeixible.

D'una banda l'autòmat minimal és un autòmat finit determinista que té la mateixa capacitat de reconeixement que un autòmat finit donat, però amb la menor quantitat d'estats possibles. És únic per a cada llenguatge reconeixible i és important per a la simplificació i optimització dels autòmats.

D'altra banda, el monoide sintàctic és un objecte algebraic associat a un llenguatge reconeixible donat. És un monoide construït a partir de les paraules del llenguatge, amb la seua operació i l'element neutre. Serveix per a classificar els llenguatges reconeixibles i per a identificar propietats d'aquests.

1. Autòmat minimal

En aquesta secció definim l'autòmat minimal de Nerode i les propietats que satisfà. Presentarem la relació de Nerode, denotada per $\sim$ i demostrarem que es tracta d'una congruència. A partir d'aquesta propietat, donat un autòmat $\mathcal{A}$ construirem l'autòmat quocient $\mathcal{A}/\sim$ i veurem que el llenguatge que reconeixen $\mathcal{A}$ i $\mathcal{A}/\sim$ és el mateix.

DEFINICIÓ 4.1. *Siga L un llenguatge d' A^* . L'autòmat de Nerode de L és un autòmat determinista $\mathcal{A}(L) = (\mathcal{Q}, A, \cdot, L, F)$ on $\mathcal{Q} = \{u^{-1}L \mid u \in A^*\}$, $F = \{u^{-1}L \mid u \in L\}$ i la funció transició està definida, per a cada $a \in A$, per la fórmula*

$$(u^{-1}L) \cdot a = a^{-1}(u^{-1}L) = (ua)^{-1}L.$$

Cada estat d' $\mathcal{A}(L)$ és el quocient per l'esquerra de L per una paraula, i per tant és un llenguatge d' A^ . L'estat inicial és el llenguatge L , i el conjunt d'estats finals és el conjunt de tots els quocients a esquerra de L per una lletra de L .*

PROPOSICIÓ 4.2. *Un llenguatge L és reconeixible si, i sols si, el conjunt $\{u^{-1}L \mid u \in A^*\}$ és finit. En aquest cas, L és reconeixible pel seu autòmat de Nerode.*

DEMOSTRACIÓ. Suposem que L és reconeixible. Siga l'autòmat determinista $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ que reconeix L . Aleshores $u^{-1}L$ és reconeixible per $\mathcal{A}_u = (\mathcal{Q}, A, \cdot, q_0 \cdot u, F)$ com ja hem vist a la Proposició 3.13. Si n és el cardinal de $\mathcal{Q}$, sols podem fer com a molt n autòmats de la forma $\mathcal{A}_u$. Per tant el conjunt $\{u^{-1}L \mid u \in A^*\}$ és finit.

Per contra, si el conjunt $\{u^{-1}L \mid u \in A^*\}$ és finit, l'autòmat de Nerode associat és finit i reconeix L . De fet, una paraula $u \in L$ és acceptada per $\mathcal{A}(L)$ si, i sols si, $L \cdot u = u^{-1}L$ és un estat final, és a dir si $u \in L$. D'açò se segueix que L és reconeixible. $\square$

A continuació introduïm el concepte de morfisme entre autòmats deterministes i el seu ordre associat.

DEFINICIÓ 4.3. *Siguem $\mathcal{A} = (\mathcal{Q}, A, E, q_0, F)$ i $\mathcal{A}' = (\mathcal{A}', A, E', q'_0, F')$ dos autòmats deterministes. Un morfisme d'autòmats d' $\mathcal{A}$ en $\mathcal{A}'$ és una funció suprajectiva de $\mathcal{Q}$ en $\mathcal{Q}'$ tal que $\varphi(q_0) = q'_0$, $\varphi^{-1}[F'] = F$ i, per a cada $u \in A^*$ i $q \in \mathcal{Q}$, $\varphi(qu) = \varphi(q)u$. Escrivim $\mathcal{A}' \leq \mathcal{A}$ si hi ha un morfisme d' $\mathcal{A}$ en $\mathcal{A}'$.*

Siga L un llenguatge reconeixible. La proposició següent mostra que l'autòmat de Nerode de L és minimal per a $\leq$, respecte els autòmats que reconeixen L . Per aquesta raó se l'anomena l'autòmat complet minimal de L .

PROPOSICIÓ 4.4. *Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat accessible i complet determinista que reconeix L . Per a cada estat q de $\mathcal{Q}$, siga L_q el llenguatge reconegut per $(\mathcal{Q}, A, \cdot, q, F)$. Aleshores*

$$\mathcal{A}(L) = (\{L_q \mid q \in F\}, A, \cdot, L_{q_0}, \{L_q \mid q \in F\})$$

on per a tot $a \in A$ i per a tot $q \in \mathcal{Q}$, $L_q \cdot a = L_{q \cdot a}$. A més, l'assignació $q \mapsto L_q$ defineix un morfisme d' $\mathcal{A}$ en $\mathcal{A}(L)$.

DEMOSTRACIÓ. Siga q un estat de $\mathcal{Q}$. Com que q és accessible, hi ha una paraula u de A^* tal que $q_0 \cdot u = q$, i per la Proposició 3.13, tenim que $L_q \cdot a = L_{q \cdot a}$. Conseqüentment, si u és una paraula, tenim que $u^{-1}L = L_q$ amb $q = q_0 \cdot u$. Per tant,

$$\{L_q \mid q \in \mathcal{Q}\} = \{u^{-1}L \mid u \in A^*\} \text{ i } \{L_q \mid q \in F\} = \{u^{-1}L \mid u \in L\},$$

el que demostra la primera part de la proposició.

A més, per a tot $a \in A$, tenim que

$$\varphi(q \cdot a) = L_{q \cdot a} = L_q \cdot a = \varphi(q) \cdot a$$

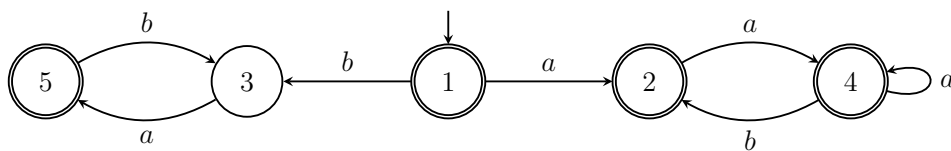


FIGURA 4.1. Autòmat minimal de l'Exemple 4.6.

el que demostra que l'assignació $\varphi : q \mapsto L_q$ és un morfisme d' $\mathcal{A}$ en $\mathcal{A}(L)$. $\square$

NOTA 4.5. *El càlcul directe de l'autòmat de Nerode és possiblement el mètode a mà més eficient, ja que directament obtenim l'autòmat minimal. En la pràctica, comencem pel quocient $L = \lambda^{-1}L$ i fem una taula de quocients de L . Per a cada quocient R , és suficient calcular els quocients $a^{-1}R$ per a cada lletra a . Aquests quocients es comparen amb una llista existent de quocients i possiblement afegim a aquesta llista si no es troba ja inclòs. Però hi ha una dificultat: comparar dos expressions racionals no és sempre fàcil, ja que un determinat llenguatge pot ser representat per dos expressions racionals molt diferents.*

EXEMPLE 4.6. *Per a l'alfabet $A = \{a, b\}$ i el llenguatge $L = (a(ab)^*) \cup (ba)^*$, tenim que $\lambda^{-1}L = L_1$ i*

$$\begin{array}{ll} a^{-1}L_1 = (ab)^*(a(ab)^*)^* = L_2; & b^{-1}L_1 = a(ba)^* = L_3; \\ a^{-1}L_2 = bL_2 \cup L_2 = L_4; & b^{-1}L_2 = \emptyset; \\ a^{-1}L_3 = (ba)^* = L_5; & b^{-1}L_3 = \emptyset; \\ a^{-1}L_4 = a^{-1}(bL_2 \cup L_2) = L_4; & b^{-1}L_4 = b^{-1}(bL_2 \cup L_2) = L_2; \\ a^{-1}L_5 = \emptyset; & b^{-1}L_5 = a(ba)^* = L_3. \end{array}$$

que dóna l'autòmat minimal representat en la Figura 4.1.

A continuació introduïm la congruència de Nerode sobre un autòmat.

DEFINICIÓ 4.7. *Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista. Direm que $p, q \in \mathcal{Q}$ estan relacionats si, i sols si, per a tota $u \in A^*$*

$$p \cdot u \in F \text{ si, i sols si, } q \cdot u \in F.$$

Ho denotarem per $p \sim q$. La relació $\sim$ rep el nom de congruència de Nerode.

La següent proposició justifica el nom.

PROPOSICIÓ 4.8. *Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista. Aleshores la relació $\sim$ és una relació d'equivalència en $\mathcal{Q}$.*

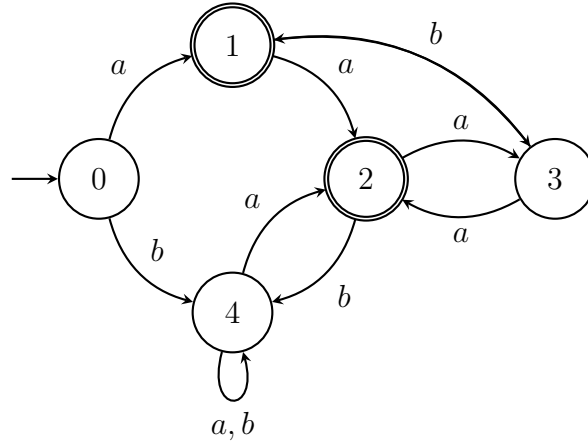


FIGURA 4.2. L'autòmat de l'Exemple 4.9.

DEMOSTRACIÓ. **Reflexiva:** $p \sim p$, ja que per a tota $u \in A^*$, $p \cdot u \in F$ si, i sols si, $p \cdot u \in F$.

Simètrica: Suposem que $p \sim q$, açò vol dir que per a tota $u \in A^*$, $p \cdot u \in F$ si, i sols si, $q \cdot u \in F$. Així per a tota $u \in A^*$, $q \cdot u \in F$ si, i sols si, $p \cdot u \in F$, és a dir, $q \sim p$.

Transitiva: Suposem que $p \sim q$ i $q \sim r$, aleshores tenim:

Per a tota $u \in A^*$, $p \cdot u \in F$ si, i sols si, $q \cdot u \in F$

Per a tota $u \in A^*$, $q \cdot u \in F$ si, i sols si, $r \cdot u \in F$

Per tant, per a tota $u \in F$, $p \cdot u \in F$ si, i sols si, $r \cdot u \in F$, és a dir, $p \sim r$. $\square$

EXEMPLE 4.9. Considerem l'autòmat de la Figura 4.2 Notem que:

$0, 3, 4 \notin [1]_{\sim}$ perquè $1 \cdot \lambda \in F$ però $3 \cdot \lambda, 4 \cdot \lambda, 0 \cdot \lambda \notin F$.

$0, 3, 4 \notin [2]_{\sim}$ pel mateix motiu.

$0 \notin [3]_{\sim}$ ja que $0 \cdot b = 4 \notin F$, mentre que $3 \cdot b = 1 \in F$.

$0 \notin [4]_{\sim}$ ja que $0 \cdot a = 1 \in F$, mentre que $4 \cdot a = 4 \notin F$.

$4 \notin [3]_{\sim}$ ja que $3 \cdot b \in F$ i $4 \cdot b \notin F$.

$1 \notin [2]_{\sim}$ ja que $1 \cdot ab \in F$, però $2 \cdot ab \notin F$.

Per tant, podem concloure que $\sim = \Delta_{\mathcal{Q}}$, és a dir, $\sim$ es la relació diagonal. Així

$$\mathcal{Q}/\sim \cong \mathcal{Q}.$$

PROPOSICIÓ 4.10. Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista. Aleshores la relació de Nerode és una congruència a dreta, és a dir, si $p \sim q$ i $u \in A^*$, aleshores $p \cdot u \sim q \cdot u$

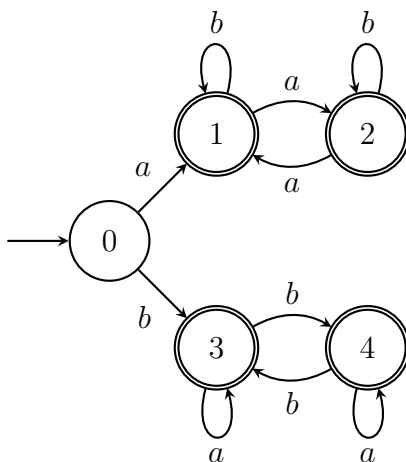


FIGURA 4.3. L'autòmat de l'Exemple 4.11.

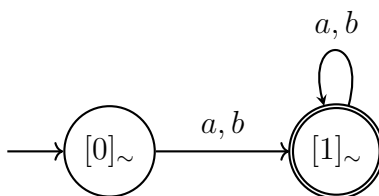


FIGURA 4.4. L'autòmat de Nerode de l'Exemple 4.11.

DEMOSTRACIÓ. Notem que si $w \in A^*$, com que $(p \cdot u) \cdot w = p \cdot (uw)$ i $(q \cdot u) \cdot w = q \cdot (uw)$, i a més és té per hipòtesi que $p \cdot (uw) \in F$ si, i sols si, $q \cdot (uw) \in F$. Aleshores:

$$(p \cdot u) \cdot w \in F \text{ si, i sols si, } (q \cdot u) \cdot w \in F$$

és a dir, que $p \cdot u \sim q \cdot u$. □

EXEMPLE 4.11. Considerem l'autòmat de la Figura 4.3, anem a veure la congruència de Nerode en aquest cas. En primer lloc analitzem les classes d'equivalència:

$$[0]_{\sim} = \{0\}; \quad [1]_{\sim} = \{1, 2, 3, 4\}.$$

L'autòmat quocient resultant de la congruència de Nerode es veu en la Figura 4.4.

DEFINICIÓ 4.12. Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista i siga $\sim$ la congruència de Nerode. Aleshores $\mathcal{Q}/\sim$ admet la següent estructura de transició entre classes

$$\begin{aligned} \cdot : \mathcal{Q}/\sim \times A &\longrightarrow \mathcal{Q}/\sim \\ ([q]_{\sim}, a) &\longmapsto [q \cdot a]_{\sim} \end{aligned}$$

Definim l'autòmat que resulta de fer el quocient per la congruència de Nerode per $\mathcal{A}/\sim = (\mathcal{Q}/\sim, A, \cdot, [q_0]_\sim, F')$ on $\cdot$ son les transicions que hem construït anteriorment i on els estats finals venen donats per $F' = \{[q]_\sim \in \mathcal{Q}/\sim \mid q \in F\}$.

PROPOSICIÓ 4.13. Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista. L'aplicació quocient

$$\begin{aligned} \text{pr}_\sim : \mathcal{Q} &\longrightarrow \mathcal{Q}/\sim \\ q &\longmapsto [q]_\sim \end{aligned}$$

és un homomorfisme d'autòmats.

PROPOSICIÓ 4.14. Siga $\mathcal{A}$ un autòmat accessible complet i determinista i siga $\mathcal{A}/\sim$ l'autòmat que resulta de fer el quocient per la congruència de Nerode.

Aleshores $L_{\mathcal{A}} = L_{\mathcal{A}/\sim}$, és a dir, $\mathcal{A}$ i $\mathcal{A}/\sim$ són equivalents.

DEMOSTRACIÓ. Anem a veure la primera inclusió, agafem una paraula que reconeix $\mathcal{A}$ i volem veure que $\mathcal{A}/\sim$ també la reconeix. Siga $w \in L_{\mathcal{A}}$ aleshores existeix $q_n \in F_{\mathcal{A}}$ de manera que

$$q_0 \xrightarrow{w} q_n.$$

Com $\text{pr}_\sim$ és homomorfisme d'autòmats

$$[q_0]_\sim \xrightarrow{w} [q_n]_\sim \in F_{\mathcal{A}/\sim}.$$

Per tant el llenguatge que reconeix $\mathcal{A}$ està inclòs en el que reconeix $\mathcal{A}/\sim$.

Anem a veure l'altra inclusió seguint el mateix procediment. Siga $w \in L_{\mathcal{A}/\sim}$, aleshores existeix $[q_n]_\sim \in F_{\mathcal{A}/\sim}$ de manera que

$$[q_0]_\sim \xrightarrow{w} [q_n]_\sim.$$

Per la definició de $\mathcal{A}/\sim$, q_0 és l'estat inicial d' $\mathcal{A}$ i q_n està relacionat amb un q'_n que és estat final d' $\mathcal{A}$. Per tant existeix almenys un camí de la forma

$$q_0 \xrightarrow{w} q'_n \in F_{\mathcal{A}}$$

és a dir, $w \in L_{\mathcal{A}}$. □

2. Autòmats i monoides

En esta secció anem a veure un procediment pel qual a cada autòmat determinista podem associar-li un monoide finit. També veurem com a partir d'un homomorfisme de monoides podem determinar el llenguatge que reconeix un autòmat.

NOTA 4.15. Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ autòmat determinista i l'aplicació

	$\varphi^\#(\lambda)$	$\varphi^\#(a)$	$\varphi^\#(b)$	$\varphi^\#(aba)$
0	0	0	0	0
1	1	2	0	2
2	2	0	1	0

TAULA 4.1. Representació de $\varphi^\#$ en l'Exemple 4.16.

$\circ$	$\varphi^\#(\lambda)$	$\varphi^\#(a)$	$\varphi^\#(b)$	$\varphi^\#(ab)$	$\varphi^\#(ba)$	0
$\varphi^\#(\lambda)$	$\varphi^\#(\lambda)$	$\varphi^\#(a)$	$\varphi^\#(b)$	$\varphi^\#(ab)$	$\varphi^\#(ba)$	0
$\varphi^\#(a)$	$\varphi^\#(a)$	$\varphi^\#(aa)$	$\varphi^\#(ba)$	$\varphi^\#(a)$	0	0
$\varphi^\#(b)$	$\varphi^\#(b)$	$\varphi^\#(ab)$	$\varphi^\#(aa)$	0	$\varphi^\#(b)$	0
$\varphi^\#(ab)$	$\varphi^\#(ab)$	0	$\varphi^\#(bab)\varphi^\#(b)$	$\varphi^\#(ab)$	0	0
$\varphi^\#(ba)$	$\varphi^\#(ba)$	$\varphi^\#(a)$	0	0	$\varphi^\#(ba)$	0
0	0	0	0	0	0	0

TAULA 4.2. Taula de multiplicació de l'Exemple 4.16.

$$\begin{aligned} \varphi : A &\longrightarrow \text{End}(\mathcal{Q}) \\ a &\longmapsto \varphi(a) : \mathcal{Q} \longrightarrow \mathcal{Q} \\ &\quad q \longmapsto q \cdot a \end{aligned}$$

Com $\text{End}(\mathcal{Q})$ té estructura de monoide amb la composició d'aplicacions i l'aplicació identitat com a neutre, per la Propietat Universal d' A^* , podem estendre φ a $\varphi^\# : A^* \longrightarrow \text{End}(\mathcal{Q})$ homomorfisme de monoides tal que $\varphi^\# \circ \text{in}_A = \varphi$ on

$$\begin{aligned} \varphi^\#(w) : \mathcal{Q} &\longrightarrow \mathcal{Q} \\ q &\longmapsto q \cdot w \end{aligned}$$

Notem que:

$$\varphi^\# : A^* \longrightarrow \text{End}(\mathcal{Q})$$

Aleshores $\varphi^\#[A^*] = \{\varphi^\#(w) \mid w \in A^*\}$ és un submonoide d' $\text{End}(\mathcal{Q})$. Notem que, si $\mathcal{Q}$ és finit $|\text{End}(\mathcal{Q})| = |\mathcal{Q}|^{|\mathcal{Q}|}$, aleshores $\varphi^\#[A^*]$ és un monoide finit.

EXEMPLE 4.16. Considerem l'autòmat $\mathcal{A}$ de la Figura 3.5, que reconeix el llenguatge $(ab)^*$. En la Taula 4.1 es troba la presentació de les funcions $\varphi^\#(w)$ per a algunes $w \in (ab)^*$. En particular, notem que $\varphi^\#(aba) = \varphi^\#(a)$ ja que les dues columnes són iguals, fet que ens indica que arribem al mateix lloc amb la paraula aba que amb la lletra a .

Per tant, podem abreviar la resta d'elements de $(ab)^*$ per a , b , ab , ba i obtenim la taula de multiplicació.

Obtenim la Taula 4.2 sabent que $\varphi^\#(aa) = \varphi^\#(bb) = 0$, $\varphi^\#(bab) = \varphi^\#(b)$ i $\varphi^\#(aba) = \varphi^\#(a)$.

NOTA 4.17. La Nota 4.15 descriu un procés que permet associar un monoide finit a cada autòmat determinista.

$\circ$	$[\lambda]$	$[a]$	$[b]$	$[ab]$	$[ba]$	$[aa]$
$[\lambda]$	$[\lambda]$	$[a]$	$[b]$	$[ab]$	$[ba]$	$[aa]$
$[a]$	$[a]$	$[aa]$	$[ba]$	$[a]$	$[aa]$	$[aa]$
$[b]$	$[b]$	$[ab]$	$[aa]$	$[aa]$	$[b]$	$[aa]$
$[ab]$	$[ab]$	$[aa]$	$[b]$	$[ab]$	$[aa]$	$[aa]$
$[ba]$	$[ba]$	$[a]$	$[aa]$	$[aa]$	$[ba]$	$[aa]$
$[aa]$	$[aa]$	$[aa]$	$[aa]$	$[aa]$	$[aa]$	$[aa]$

TAULA 4.3. Taula multiplicativa del monoide $A^*/\text{Ker}(\varphi^\#)$ de l'Exemple 4.21.

PROPOSICIÓ 4.18. Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista. Aleshores $L_{\mathcal{A}} = (\varphi^\#)^{-1}[\mathcal{X}]$ on $\mathcal{X} = \{\varphi^\#(w) \mid (q_0) \cdot w \in F\}$.

DEMOSTRACIÓ. Siga $w \in L_{\mathcal{A}}$, aleshores $(q_0) \cdot w \in F$. Així, $\varphi^\#(w) \in \mathcal{X}$. Per tant $w \in [\varphi^\#]^{-1}[\mathcal{X}]$. Per contra, si $w \in [\varphi^\#]^{-1}[\mathcal{X}]$ aleshores $\varphi^\#(w) \in \mathcal{X}$, és a dir $(q_0) \cdot w \in F$. Per tant, $w \in L_{\mathcal{A}}$. $\square$

NOTA 4.19. Notem que en l'Exemple 4.16, $\mathcal{X} = \{\varphi^\#(\lambda), \varphi^\#(ab)\}$.

3. Monoide sintàctic i morfisme sintàctic

En aquesta secció, el que anem a fer és construir el monoide sintàctic, que ve definit per la relació d'equivalència del nucli de l'aplicació construïda en la Nota 4.15. Veurem el que significa ser reconeixible per monoides i establim l'equivalència entre reconeixibilitat per monoides i reconeixibilitat per autòmats.

DEFINICIÓ 4.20. Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista i siga $\varphi^\# : A^* \longrightarrow \text{End}(\mathcal{Q})$ l'homomorfisme de monoides presentat en la Nota 4.15. Pel Primer Teorema d'Isomorfia:

$$A^*/\text{Ker}(\varphi^\#) \cong \text{Im}(\varphi^\#).$$

Anomenem monoide sintàctic de l'autòmat $\mathcal{A}$ a $A^*/\text{Ker}(\varphi^\#)$. Siguen $v, w \in A^*$, notem que $(v, w) \in \text{Ker}(\varphi^\#)$ si, i sols si, $\varphi^\#(v) = \varphi^\#(w)$.

A més, denotarem per $M(\mathcal{A}(L)/\text{Ker}(\varphi^\#))$ al monoide sintàctic associat a $\mathcal{A}(L)/\text{Ker}(\varphi^\#)$.

Introduïm una nova notació per a simplificar. Escriurem $[a]$ en compte de $[a]_{\text{Ker}(\varphi^\#)}$ per a denotar la classe d'equivalència d'a resultant de fer la congruència pel nucli de $\varphi^\#$.

EXEMPLE 4.21. Vegem que el monoide $A^*/\text{Ker}(\varphi^\#)$ associat a l'autòmat de l'Exemple 3.5 és el monoide de la Taula 4.3.

A continuació introduïm la noció de reconeixibilitat de llenguatges per monoides.

DEFINICIÓ 4.22. *Un llenguatge $L \subseteq A^*$ és reconeixible per monoides si existeix un monoide finit M i un homomorfisme de monoides $f : A^* \longrightarrow M$ i un subconjunt $C \subseteq M$ tal que $L = f^{-1}[C]$.*

La següent proposició demostra l'equivalència de la reconeixibilitat d'un llenguatge per autòmats o per monoides.

PROPOSICIÓ 4.23. *Siga A un alfabet i siga $L \subseteq A^*$ un llenguatge d' A^* . Aleshores són equivalents:*

- L és reconeixible per autòmats.
- L és reconeixible per monoides.

DEMOSTRACIÓ. Suposem que $L \subseteq A^*$ és reconeixible per un autòmat finit. Siga $\mathcal{A} = (\mathcal{Q}, A, \cdot, q_0, F)$ un autòmat determinista que reconeix L és a dir, tal que $L = L_{\mathcal{A}} = \{w \in A^* \mid q_0 \cdot w \in F\}$.

Considerem el conjunt de les aplicacions de $\mathcal{Q}$ en $\mathcal{Q}$

$$\text{End}(\mathcal{Q}) = \{f : \mathcal{Q} \longrightarrow \mathcal{Q} \mid f \text{ aplicació}\}.$$

$\text{End}(\mathcal{Q})$ té estructura de monoide finit amb la composició d'aplicacions i té a $\text{id}_{\mathcal{Q}}$ com a neutre. Considerem l'aplicació:

$$\begin{array}{rcl} \varphi : A & \longrightarrow & \text{End}(\mathcal{Q}) \\ a & \longmapsto & \varphi(a) : \mathcal{Q} \longrightarrow \mathcal{Q} \\ & & q \longmapsto q \cdot a \end{array}$$

Per la Propietat Universal existeix un únic homomorfisme de monoides $\varphi^{\#} : A^* \longrightarrow \text{End}(\mathcal{Q})$ tal que $\varphi^{\#} \circ \text{in}_A = \varphi$. Notem que:

$$\begin{array}{rcl} \varphi^{\#}(w) : \mathcal{Q} & \longrightarrow & \mathcal{Q} \\ q & \longmapsto & q \cdot w \end{array}$$

Considerem $C = \{f : \mathcal{Q} \longrightarrow \mathcal{Q} \mid f(q_0) \in F\} \subseteq \text{End}(\mathcal{Q})$. A més,

$$\begin{aligned} (\varphi^{\#})^{-1}[C] &= \{w \in A^* \mid \varphi^{\#}(w) \in C\} \\ &= \{w \in A^* \mid \varphi^{\#}(w)(q_0) \in F\} \\ &= \{w \in A^* \mid q_0 \cdot w \in F\} \\ &= L. \end{aligned}$$

Ara suposem que $L \subseteq A^*$ és reconeixible per monoides. Siga M un monoide finit i $f : A^* \longrightarrow M$ homomorfisme de monoides i $C \subseteq M$ tals que $L = f^{-1}[C]$.

Considerem l'autòmat següent: $\mathcal{A} = (M, A, \cdot, 1, C)$ on

$$\begin{aligned} \cdot : M \times A &\longrightarrow M \\ (m, a) &\longmapsto m \cdot f(a) \end{aligned}$$

Es comprova que $\mathcal{A}$ és un autòmat determinista. A més:

$$\begin{aligned} L_{\mathcal{A}} &= \{w \in A^* \mid 1 \cdot f(w) \in C\} \\ &= \{w \in A^* \mid f(w) \in C\} \\ &= f^{-1}[C] \\ &= L. \end{aligned}$$

Açò demostra la proposició. $\square$

4. Saturació en A^*

En esta secció definirem el concepte de llenguatge saturat per una congruència, un concepte que és útil perquè ens permet demostrar quan certs llenguatges són reconeixibles. També veurem propietats relacionades.

DEFINICIÓ 4.24. *Siga A un alfabet, Θ una relació d'equivalència en A^* i $L \subseteq A^*$. Direm que L està saturat per Θ si*

$$L = \bigcup_{w \in L} [w]_{\Theta}.$$

És a dir, si L pot escriure's com a unió de les Θ -classes dels seus elements.

Anomenarem Θ -saturat de L al subconjunt

$$L^{\Theta} = \bigcup_{w \in L} [w]_{\Theta}.$$

Denotem per Θ -Sat al conjunt de llenguatges Θ -saturats, és a dir,

$$\Theta\text{-Sat} = \{L \subseteq A^* \mid L = L^{\Theta}\}.$$

NOTA 4.25. *Siga A un alfabet i $L \subseteq A^*$. La inclusió $L \subseteq \bigcup_{w \in L} [w]_{\Theta}$ sempre es té. Així, per a veure que $L \subseteq A^*$ és saturat per Θ és suficient comprovar la inclusió de dreta a esquerra.*

PROPOSICIÓ 4.26. *Siga A un alfabet i Θ una relació d'equivalència en A^* . L'aplicació*

$$\begin{aligned} (\cdot)^{\Theta} : \mathcal{P}(A^*) &\longrightarrow \mathcal{P}(A^*) \\ L &\longmapsto L^{\Theta} \end{aligned}$$

és un operador de clausura.

DEMOSTRACIÓ. Per a veure que és un operador de clausura hem de provar que es extensiu, monòton i idempotent.

$(\cdot)^{\Theta}$ és extensiu. Si $L \subseteq A^*$, aleshores $L \subseteq L^{\Theta}$, açò es té per la Nota 4.25.

$(\cdot)^\Theta$ és monòton. És a dir, si $L_1, L_2 \subseteq A^*$ i $L_1 \subseteq L_2$, aleshores $L_1^\Theta \subseteq L_2^\Theta$. Anem a comprovar que $L_1^\Theta \subseteq L_2^\Theta$. Siga $z \in L_1^\Theta = \bigcup_{w \in L_1} [w]_\Theta$, així existeix $w \in L_1$ de forma que $z \in [w]_\Theta$. Com que $L_1 \subseteq L_2$, aleshores $w \in L_2$. Així $z \in \bigcup_{w \in L_2} [w]_\Theta$. Per tant $L_1^\Theta \subseteq L_2^\Theta$.

$(\cdot)^\Theta$ és idempotent. És a dir, si $L \subseteq A^*$, aleshores $(L^\Theta)^\Theta = L^\Theta$. Sempre es té que $L^\Theta \subseteq (L^\Theta)^\Theta$. Sols queda comprovar l'altra inclusió. Siga $z \in (L^\Theta)^\Theta = \bigcup_{w \in L^\Theta} [w]_\Theta$, així existeix $u \in L^\Theta$ de forma que $z \in [u]_\Theta$. Com $u \in L^\Theta = \bigcup_{w \in L} [w]_\Theta$. Així existeix $v \in L$ de forma que $u \in [v]_\Theta$. Per tant,

$$z \in [v]_\Theta \subseteq \bigcup_{w \in L} [w]_\Theta = L^\Theta.$$

Açò conclou la demostració. $\square$

PROPOSICIÓ 4.27. *Siga A un alfabet i siguin Θ_1, Θ_2 relacions d'equivalència en A^* . Si $\Theta_1 \subseteq \Theta_2$, aleshores $\Theta_2\text{-Sat} \subseteq \Theta_1\text{-Sat}$.*

DEMOSTRACIÓ. Siga $L \subseteq A^*$ en $\Theta_2\text{-Sat}$. Aleshores

$$L = L^{\Theta_2} = \bigcup_{w \in L} [w]_{\Theta_2}.$$

Volem veure que L està en $\Theta_1\text{-Sat}$. És a dir, volem veure que $L = L^{\Theta_1}$. És suficient comprovar la inclusió de dreta a esquerra. Siga $z \in L^{\Theta_1} = \bigcup_{w \in L} [w]_{\Theta_1}$. Així existeix $u \in L$ tal que $z \in [u]_{\Theta_1}$, és a dir, $(z, u) \in \Theta_1$. Com $\Theta_1 \subseteq \Theta_2$, trobem que $(z, u) \in \Theta_2$, és a dir:

$$z \in [u]_{\Theta_2} \subseteq \bigcup_{w \in L} [w]_{\Theta_2} = L^{\Theta_2} = L.$$

Per tant $L^{\Theta_1} \subseteq L$ i L és $\Theta_1\text{-Sat}$. $\square$

Les següents proposicions descriuen els llenguatges saturats per a les relacions diagonal i total sobre un alfabet.

PROPOSICIÓ 4.28. *Siga A un alfabet. Es considera la relació total $\nabla_{A^*} = A^* \times A^*$ sobre A^* que, com sabem, és relació d'equivalència en A^* . Aleshores $\nabla_{A^*}\text{-Sat} = \{A^*, \emptyset\}$.*

DEMOSTRACIÓ. Anem a veure que A^* i $\emptyset$ són $\nabla_{A^*}\text{-Sat}$ i, a més, són els únics subconjunts $\nabla_{A^*}\text{-Sat}$.

D'una banda per veure que A^* és $\nabla_{A^*}\text{-Sat}$, hem de veure que $A^* = (A^*)^{\nabla_{A^*}}$. Tan sols hem de provar la inclusió de dreta a esquerra. Tenim:

$$(A^*)^{\nabla_{A^*}} = \bigcup_{w \in A^*} [w]_{\nabla_{A^*}} \subseteq A^*.$$

Per a veure que $\emptyset$ és $\nabla_{A^*}\text{-Sat}$, hem de veure que $\emptyset = (\emptyset)^{\nabla_{A^*}}$. Tan sols hem de provar la inclusió a esquerra. Tenim:

$$(\emptyset)^{\nabla_{A^*}} = \bigcup_{w \in \emptyset} [w]_{\nabla_{A^*}} \subseteq \emptyset.$$

Açò demostra que A^* i $\emptyset$ són llenguatges $\nabla_{A^*}\text{-Sat}$.

Ara anem a comprovar que estos són els únics. Siga $\emptyset \subset L \subseteq A^*$ un llenguatge $\nabla_{A^*}\text{-Sat}$ no buit. Així existeix un $w \in L$. Notem que

$$A^* = [w]_{\nabla_{A^*}} \subseteq L.$$

Per tant, $L = A^*$.

Així, $\nabla_{A^*}\text{-Sat} = \{\emptyset, A^*\}$. $\square$

PROPOSICIÓ 4.29. *Siga A un alfabet. Es considera la relació diagonal $\Delta_{A^*} = \{(w, v) \in A^* \times A^* \mid w = v\}$ sobre A^* que, com sabem, és relació d'equivalència en A^* . Aleshores $\Delta_{A^*}\text{-Sat} = \mathcal{P}(A^*)$.*

DEMOSTRACIÓ. Òbviament $\Delta_{A^*}\text{-Sat} \subseteq \mathcal{P}(A^*)$. Siga ara $L \subseteq A^*$ un llenguatge. Anem a demostrar que $L = L^{\Delta_{A^*}}$. És suficient demostrar la inclusió de dreta a esquerra. Siga $v \in L^{\Delta_{A^*}} = \bigcup_{w \in L} [w]_{\Delta_{A^*}}$, així existeix $w \in L$ per al que $v \in [w]_{\Delta_{A^*}}$, així $v = w$. Per tant $v \in L$.

Així $\Delta_{A^*}\text{-Sat} = \mathcal{P}(A^*)$. $\square$

5. Congruència sintàctica

En aquesta secció definim la congruència sintàctica, la major congruència que satura a un llenguatge. Veurem que un llenguatge és reconeixible per monoides si, i sols si, la seua congruència sintàctica és d'índex finit. La congruència sintàctica s'utilitza per a definir el monoide quocient, que és un monoide obtés a partir del monoide de transicions. També veurem que la congruència presentada en la Nota 4.15 és igual a la congruència sintàctica.

DEFINICIÓ 4.30. *Siga A un alfabet i $L \subseteq A^*$. Definim la congruència sintàctica associada a L com segueix: Si $v, w \in A^*$, direm que estan relacionades per $\sim_L$ si satisfan que, per a tot $x, y \in A^*$,*

$$xvy \in L \text{ si, i sols si, } xwy \in L.$$

La següent proposició justifica la importància de la congruència sintàctica.

PROPOSICIÓ 4.31. *Siga A un alfabet i L un llenguatge en A^* , aleshores la relació $\sim_L$ introduïda en la Definició 4.30 és una congruència del monoide lliure A^* que satura L . A més, $\sim_L$ és la major congruència d' A^* que satura a L .*

DEMOSTRACIÓ. $\sim_L$ és relació d'equivalència.

Reflexiva. Per a tota $w \in A^*$ i per a tot $x, y \in A^*$ es té que $xwy \in L$ si, i sols si, $xwy \in L$, per tant $w \sim_L w$.

Simètrica. Per a tot parell $v, w \in A^*$ tals que $v \sim_L w$ es té que, per a tot $x, y \in A^*$

$$xvy \in L \text{ si, i sols si, } xwy \in L.$$

Per tant, per a tot $x, y \in A^*$

$$xwy \in L \text{ si, i sols si, } xvy \in L,$$

és a dir $w \sim_L v$.

Transitiva. Siguen $v, w, u \in A^*$ tals que $v \sim_L w$ i $w \sim_L u$. Siguen $x, y \in A^*$, aleshores es té la següent equivalència

$$xvy \in L \text{ si, i sols si, } xwy \in L \text{ si, i sols si, } xuy \in L.$$

Així, $v \sim_L u$.

$\sim_L$ és congruència en A^* . Siguen $v, w \in A^*$ tals que $v \sim_L w$. Siguen $v', w' \in A^*$ tals que $v' \sim_L w'$. Volem veure que $vv' \sim_L ww'$. Si $x, y \in A^*$,

$$xvv'y \in L \text{ si, i sols si, } xwv'y \in L \text{ si, i sols si, } xww'y \in L.$$

Així, $vv' \sim_L ww'$.

$\sim_L$ satura a L . Hem de comprovar que $L = L^{\sim_L}$. Només cal comprovar que $L^{\sim_L} \subseteq L$. Siga $z \in L^{\sim_L} = \bigcup_{w \in L} [w]_{\sim_L}$, aleshores existeix $u \in L$ tal que $z \in [u]_{\sim_L}$ és a dir, per a tota parella $x, y \in A^*$ tenim $xyz \in L$ si, i sols si, $xuy \in L$. En particular per a $x = y = \lambda$, trobem que $z \in L$ si, i sols si, $u \in L$. I com que $u \in L$, aleshores $z \in L$.

$\sim_L$ és la major congruència en A^* que satura a L . Siga Θ una congruència en A^* que satura a L , és a dir, $L = L^\Theta$. Anem a demostrar que $\Theta \subseteq \sim_L$. Siga $(v, w) \in \Theta$, siguen $x, y \in A^*$. Suposem que $xvy \in L$, com que $(v, w), (x, x), (y, y) \in \Theta$, aleshores $(xvy, xwy) \in \Theta$. Per tant:

$$xwy \in [xvy]_\Theta \subseteq \bigcup_{u \in L} [u]_\Theta = L^\Theta = L.$$

L'altra implicació és anàloga. Per tant obtenim que $(v, w) \in \sim_L$. $\square$

Abans hem vist que a cada autòmat finit li podíem associar un monoide. Per tant el llenguatge que reconeix eixe autòmat té associat un monoide. A més, mitjançant la saturació d'un llenguatge hem establert una relació entre les paraules del llenguatge, per tant podem obtenir el següent resultat.

PROPOSICIÓ 4.32. *Siga A un alfabet i $L \subseteq A^*$ un llenguatge. Les següents afirmacions són equivalents:*

- (1) $L \subseteq A^*$ és reconeixible per monoides.
- (2) L està saturat per una congruència d'índex finit.
- (3) $\sim_L$ té índex finit.

DEMOSTRACIÓ. Anem a veure que si L és un llenguatge reconeixible per monoides, aleshores L està saturat per una congruència d'índex

finit. Com $L \subseteq A^*$ és reconeixible per monoides, existeix M monoide finit, $f : A^* \rightarrow M$ homomorfisme de monoides i un subconjunt $C \subseteq M$ de forma que $L = f^{-1}[C]$. Considerem $\text{Ker}(f)$ que és congruència en A^* on, recordem

$$\text{Ker}(f) = \{(v, w) \in A^* \times A^* \mid f(v) = f(w)\}.$$

Pel Primer Teorema d'Isomorfia

$$A^*/\text{Ker}(f) \cong \text{Im}(f) \leq M.$$

Com que M és un monoide finit, $A^*/\text{Ker}(f)$ té índex finit. Falta veure que L està saturat per $\text{Ker}(f)$, només cal provar que $L^{\text{Ker}(f)} \subseteq L$. Siga $z \in L^{\text{Ker}(f)} = \bigcup_{w \in L} [w]_{\text{Ker}(f)}$, aleshores existeix $u \in L$ de manera que $z \in [u]_{\text{Ker}(f)}$, és a dir, $f(z) = f(u)$. Si considerem $f^{-1}(f(z))$. Com que $f(u) \in C$, tenim que $z \in f^{-1}[C] = L$, per tant $z \in L$.

Ara anem a demostrar que si L està saturat per una congruència d'índex finit aleshores $\sim_L$ té índex finit. Com que L està saturat per una congruència Θ d'índex finit, aleshores A^*/Θ és finit. Sabem per la Proposició 4.31 que $\sim_L$ satura a L . A més, $\sim_L$ és la major congruència en A^* amb aquesta propietat, aleshores $\Theta \subseteq \sim_L$. Així, per la Proposició 1.19, $\sim_L$ té índex finit. Per tant, $A^*/\sim_L$ és finit.

Per últim, suposem que $\sim_L$ té índex finit, aleshores $A^*/\sim_L$ és finit. Volem veure que $L \subseteq A^*$ és reconeixible per monoides. Sabem que $\sim_L$ satura a L , per tant

$$L = \bigcup_{w \in L} [w]_{\sim_L} = L^{\sim_L}.$$

Considerem l'aplicació projecció al quocient

$$\begin{array}{ccc} \text{pr}_{\sim_L} : & A^* & \longrightarrow & A^*/\sim_L \\ & w & \longmapsto & [w]_{\sim_L} \end{array}$$

vista a la Proposició 1.17, on vam demostrar que era un homomorfisme de monoides. Aleshores, com $L = \text{pr}_{\sim_L}^{-1}[\text{pr}_{\sim_L}[L]]$ concloem que L és reconeixible per monoides. $\square$

NOTA 4.33. *Tenim dues nocions amb l'adjectiu sintàctic associades a un llenguatge reconeixible $L \in A^*$. Per una banda:*

- (1) *Construïm l'autòmat de Nerode $\mathcal{A}(L)$ que hem vist en la Proposició 4.1. Per la Proposició 4.2 sabem que $\mathcal{A}(L)$ és finit.*
- (2) *Considerem l'equivalència de Nerode en $\mathcal{A}(L)$ vista en la Proposició 4.7 i que hem demostrat que és congruència en la Proposició 4.10. A partir d'ací, montem el quocient $\mathcal{A}(L)/\sim$ autòmat finit vist en la Definició 4.12 i que reconeix L , demostrat en la Proposició 4.14.*

- (3) Considerem el monoide sintàctic associat a $\mathcal{A}(L)/\sim$. És a dir, $M(\mathcal{A}(L)/\sim)$. Com hem vist en la Definició 4.20.

D'altra banda tenim:

- (1) Considerem la congruència sintàctica $\sim_L$ vista en la Definició 4.30 i que hem vist en la Proposició 4.32 que té índex finit.
- (2) Considerem el monoide quocient, el monoide sintàctic $A^*/\sim_L$.

NOTA 4.34. Recordem que $M(\mathcal{A}(L)/\sim)$ és un quocient d' A^* . Per a la construcció de $M(\mathcal{A}(L)/\sim)$ considerem

$$\begin{array}{ccc} \varphi : A & \longrightarrow & \text{End}(\mathcal{A}(L)/\sim) \\ a & \longmapsto & \cdot a : \quad \mathcal{A}(L)/\sim \longrightarrow \mathcal{A}(L)/\sim \\ & & [u^{-1}L]_{\sim} \longmapsto [(ua)^{-1}L]_{\sim} \end{array}$$

Per la Propietat Universal extenem φ a un homomorfisme de monoides

$$\begin{array}{ccc} \varphi^{\sharp} : A^* & \longrightarrow & \text{End}(\mathcal{A}(L)/\sim) \\ w & \longmapsto & \cdot w : \quad \mathcal{A}(L)/\sim \longrightarrow \mathcal{A}(L)/\sim \\ & & [u^{-1}L]_{\sim} \longmapsto [(uw)^{-1}L]_{\sim} \end{array}$$

Així

$$M(\mathcal{A}(L)/\sim) = A^*/\text{Ker}(\varphi^{\sharp}).$$

Anem a demostrar que $\text{Ker}(\varphi^{\sharp}) = \sim_L$. Ens servirà d'utilitat perquè permet veure que el monoide quocient és isomorf al monoide sintàctic. Aquest resultat és important perquè permet estudiar el monoide sintàctic d'un llenguatge a partir de la congruència sintàctica.

PROPOSICIÓ 4.35. Siga A un alfabet i $L \subseteq A^*$. Considerem $\varphi^{\sharp} : A^* \longrightarrow \text{End}(\mathcal{A}(L)/\sim)$ l'homomorfisme de monoides definit en la Nota 4.34. Aleshores $\text{Ker}(\varphi^{\sharp}) = \sim_L$.

DEMOSTRACIÓ. Siga $(w, v) \in \text{Ker}(\varphi^{\sharp})$ volem veure que $(w, v) \in \sim_L$. Siguen $x, y \in A^*$, volem veure que $xwy \in L$ si, i sols si, $xvy \in L$.

Suposem que $xwy \in L$ per tant $y \in (xw)^{-1}L$ Notem que:

$$\begin{aligned} (xw)^{-1}L &\in [(xw)^{-1}L]_{\sim} \\ &= \varphi^{\sharp}(w)([x^{-1}L]_{\sim}) \\ &= \varphi^{\sharp}(v)([x^{-1}L]_{\sim}) \\ &= [(xv)^{-1}L]_{\sim} \end{aligned}$$

Aleshores $y \in [(xv)^{-1}L]_{\sim}$. Per definició, existeix $z^{-1}L \in [(xv)^{-1}L]_{\sim}$ de forma que $y \in z^{-1}L$ on $z = xv$, és a dir, existeix $z^{-1}L \in [(xv)^{-1}L]_{\sim}$ on $z = xv$ de forma que $zy \in L$. Substituint z obtenim que $xvy \in L$. Notem que cada pas és una doble implicació. Per tant hem provat que $\text{Ker}(\varphi^{\sharp}) \subseteq \sim_L$.

Per a la inclusió inversa, prenim $(w, v) \in \sim_L$ i volem demostrar que aquest parell també pertany a $\text{Ker}(\varphi^\#)$. Siga $[u^{-1}L]_\sim$ un element arbitrari de $\mathcal{A}(L)/\sim$ volem veure que $\varphi^\#(w)([u^{-1}L]_\sim) = \varphi^\#(v)([u^{-1}L]_\sim)$. Recordem que:

$$\varphi^\#(w)[u^{-1}L]_\sim = [(uw)^{-1}L]_\sim$$

$$\varphi^\#(v)[u^{-1}L]_\sim = [(uv)^{-1}L]_\sim$$

Hem de veure que $[(uw)^{-1}L]_\sim = [(uv)^{-1}L]_\sim$. Açò es tindrà si, i només si per a cada paraula $z \in A^*$ es té que

$$((uw)^{-1}L) \cdot z \in L \text{ si, i sols si, } ((uv)^{-1}L) \cdot z \in L$$

Notem que:

$$((uw)^{-1}L) \cdot z \in L \text{ si, i sols si } uwz \in L$$

$$((uv)^{-1}L) \cdot z \in L \text{ si, i sols si } uvz \in L.$$

Com que $(w, v) \in \sim_L$, aleshores tenim:

$$uwz \in L \text{ si, i sols si, } uvz \in L$$

Aleshores hem vist que $[(uw)^{-1}L]_\sim = [(uv)^{-1}L]_\sim$. Per tant, $\sim_L \subseteq \text{Ker}(\varphi^\#)$.

Concloem que $\sim_L = \text{Ker}(\varphi^\#)$. □

CAPÍTOL 5

Llenguatges racionals i llenguatges reconeixibles

Si A és un alfabet, tenim dos grans famílies de llenguatges $\text{Rat}(A^*)$ i $\text{Rec}(A^*)$. En aquest capítol demostrarem que són iguals.

TEOREMA 5.1. *Siga A un alfabet, aleshores:*

$$\text{Rat}(A^*) \subseteq \text{Rec}(A^*).$$

DEMOSTRACIÓ. Recordem de la Definició 2.9 que $\text{Rat}(A^*)$ és el menor subconjunt d' A^* que satisfà:

- (1) $\emptyset, \{\lambda\}, \{a\} \in \text{Rat}(A^*)$;
- (2) Si $(L_i)_{i \in n}$ és una família de llenguatges racionals, aleshores $\bigcup_{i \in n} L_i \in \text{Rat}(A^*)$;
- (3) Si $L, K \in \text{Rat}(A^*)$ aleshores $LK \in \text{Rat}(A^*)$;
- (4) Si $L \in \text{Rat}(A^*)$ aleshores $L^* \in \text{Rat}(A^*)$.

Notem que $\emptyset \in \text{Rec}(A^*)$, perquè qualsevol autòmat finit sense estats finals reconeix el buit. A més, els llenguatges formats per una paraula, com $\{\lambda\}$ i $\{a\}$, també estan en $\text{Rec}(A^*)$ ja que poden ser reconeguts per un autòmat amb dos estats.

Si $(L_i)_{i \in n}$ és una família de llenguatges reconeixibles, vam veure en la Proposició 3.1 que la unió tornava a ser un llenguatge reconeixible.

Si $L, K \in \text{Rec}(A^*)$ vam demostrar en la Proposició 3.9 que $LK \in \text{Rec}(A^*)$ i en la Proposició 3.11 que $L^* \in \text{Rec}(A^*)$.

Com que $\text{Rec}(A^*)$ satisfà les 4 condicions que defineixen ser racional i $\text{Rat}(A^*)$ és el menor que les satisfà, aleshores $\text{Rat}(A^*) \subseteq \text{Rec}(A^*)$. $\square$

NOTA 5.2. *Sols ens quedarà comprovar que $\text{Rec}(A^*) \subseteq \text{Rat}(A^*)$, o el que és el mateix que tot llenguatge reconeixible pugui construir-se a partir de les 4 condicions que defineixen ser racional o, el que és el mateix, trobar un terme racional per al llenguatge reconeixible. Per exemple si podem escriure $L \in \text{Rec}(A^*)$ de la forma $L = (ab)^* + (a + b)^* + \lambda$ garantim que $L \in \text{Rat}(A^*)$.*

El problema de comprovar que $\text{Rec}(A^) \subseteq \text{Rat}(A^*)$ és el problema de descriure L amb les operacions concatenació, suma i producte estrella sobre les variables $a \in A$, λ i $\emptyset$. A este terme l'anomenarem expressió regular de L .*

Anem a veure com construir l'expressió regular d'un llenguatge reconeixible. Per a fer esta demostració ens hem basat en les notes de [FR04].

TEOREMA 5.3. *Tot llenguatge reconeixible $L \subseteq A^*$ admet una expressió regular. És a dir, si $\mathcal{A} = (\mathcal{Q}, A, \cdot, I, F)$ és un autòmat determinista que reconeix L , aleshores existeix una expressió regular α_A tal que $L_{\mathcal{A}} = L_{\alpha_A}$.*

DEMOSTRACIÓ. Suposem que $\mathcal{Q} = \{q_i \mid i \in n\}$. Per a cada $i, j \in n$ definim:

$$R_{ij} = \{w \in A^* \mid q_i \cdot w = q_j\}.$$

Així

$$L_{\mathcal{A}} = \bigcup_{i \in I} \bigcup_{j \in F} R_{ij}.$$

Definim:

$$R_{ij}^0 = \begin{cases} \{a \in A \mid q_i \cdot a = q_j\} & \text{si } i \neq j; \\ \{a \in A \mid q_j \cdot a = q_i\} \cup \{\lambda\} & \text{si } i = j. \end{cases}$$

Si $k \in n$, definim:

$$R_{ij}^k = \{w \in A^* \mid q_i \cdot w = q_j \text{ i } \forall (\lambda < w' < w)(q_i \cdot w' \in \{q_1, \dots, q_k\})\}$$

Aleshores ocorre:

- (1) $R_{ij}^k \subseteq R_{ij}^k$.
- (2) $R_{ij}^k = R_{ij}^n$.
- (3) $R_{ij}^k = R_{ij}^{k-1} \cup R_{ik}^{k-1} (R_{kk}^{k-1})^* R_{kj}^{k-1}$.

Anem a demostrar per inducció sobre $k \in n+1$ que R_{ij} admet expressió regular.

Cas base

$$R_{ij}^0 = \begin{cases} \{a \in A \mid q_i \cdot a = q_j\} & \text{si } i \neq j; \\ \{a \in A \mid q_j \cdot a = q_i\} \cup \{\lambda\} & \text{si } i = j. \end{cases}$$

Les expressions regulars corresponents a cada R_{ij}^0 seran:

$$\begin{cases} \sum_{a \in R_{ij}^0} a & \text{si } i \neq j; \\ \sum_{a \in R_{ij}^0 \setminus \{\lambda\}} a + \lambda & \text{si } i = j. \end{cases}$$

Hipòtesi inductiva

Suposem que R_{ij}^{k-1} admet expressió regular i provem-ho per a R_{ij}^k .

Així:

$$R_{ij}^k = R_{ij}^{k-1} \cup R_{ik}^{k-1} (R_{kk}^{k-1})^* R_{kj}^{k-1}$$

Així per hipòtesi inductiva existeixen expressions regulars $\alpha_{ij}^{k-1}, \alpha_{ik}^{k-1}, \alpha_{kk}^{k-1}$ i α_{kj}^{k-1} associades als respectius $R_{ij}^k, R_{ij}^{k-1}, R_{kk}^{k-1}$ i R_{kj}^{k-1} . Per tant prenim d'expressió regular per a R_{ij} l'expressió següent

$$\alpha_{ij}^k = \alpha_{ij}^{k-1} + \alpha_{ik}^{k-1} (\alpha_{kk}^{k-1})^* \alpha_{kj}^{k-1}.$$

Finalment, per a l'autòmat, prenim l'expressió regular següent:

$$\sum_{i \in I} \sum_{j \in F} \alpha_{ij}^n = \alpha_A.$$

Açò demostra que $\text{Rec}(A^*) \subseteq \text{Rat}(A^*)$. □

TEOREMA 5.4. *Siga A un alfabet, aleshores $\text{Rec}(A^*) = \text{Rat}(A^*)$.*

Conclusions

Per concloure aquest treball anem a destacar una sèrie de qüestions que considerem importants i que hem pogut demostrar al llarg del treball.

Primer que res, cal destacar dos grans blocs de llenguatges: els llenguatges racionals i els llenguatges reconeixibles. Amb els llenguatges racionals hem vist que eren tancats per a les operacions definides, i amb els llenguatges reconeixibles hem introduït un resultat molt important, el Lema del Bombeig, una eina que ens ha permès identificar els llenguatges que no eren reconeixibles.

En quant als autòmats, cal destacar els resultats que ens porten a l'equivalència entre el autòmats finits, deterministes, ajustats i deterministes estàndard.

D'una banda, hem introduït l'autòmat de Nerode que ens ha donat la possibilitat d'obtenir resultats de reconeixibilitat de llenguatges. També hem construït, a partir de la relació de Nerode, l'autòmat quocient, un autòmat minimal amb la capacitat de reconèixer el llenguatge original. Hem establert una equivalència entre els autòmats i els monoides que ens han permès arribar al resultat de que ser reconeixible per monoides era equivalent a ser reconeixible per autòmats.

D'altra banda, hem vist els llenguatges saturats i hem establert una relació entre les paraules d'un llenguatge que ens han portat a definir la congruència sintàctica. Amb aquesta congruència hem construït el monoide sintàctic. Aquestes eines ens han portat a demostrar que la congruència sintàctica era la mateixa congruència que definia el nucli de l'homomorfisme de Nerode, per tant hem obtingut que el monoide quocient era equivalent al monoide sintàctic.

Per últim hem pogut comprovar que els dos grans blocs de llenguatges, els racionals i els reconeixibles, també eren equivalents. És a dir, un llenguatge és reconeixible per autòmats si, i només si, admet una expressió regular.

Bibliografia

- [FR04] J. F. Ferri Rabasa. *Teoria d'autòmats i llenguatges formals*, volume 75. Universitat de València, 2004.
- [HMU08] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Teoría de autómatas, lenguajes y computación*. Addison Wesley, 2008.
- [Pin10] J.-É. Pin. Mathematical foundations of automata theory. *Lecture notes LIAFA, Université Paris*, 7:73, 2010.
- [Pin21] J.-É. Pin. *Handbook of automata theory*. 2021.
- [SB81] H. P. Sankappanavar and S. Burris. A course in universal algebra. *Graduate Texts Math*, 78:56, 1981.