



Treball Fi de Grau - Curs 2022/2023

Llenguatges formals i autòmats finits

Autora: Nuria Gallego Ariño

Tutor: ENRIC COSME LLÓPEZ

Índex

Capítol 1. Introducció	3
1. Resum	3
2. Preliminars	5
Capítol 2. Teoria de monoides	15
1. Primeres definicions	15
2. Monoide lliure	16
3. Submonoides	20
4. Congruències	20
5. Primer Teorema d'Isomorfisme	24
6. Congruències d'índex finit	26
7. Saturació	30
Capítol 3. Reconeixibilitat	35
1. Conceptes previs	35
2. Reconeixibilitat per monoides	39
3. Reconeixibilitat per autòmats	43
Bibliografia	49

CAPÍTOL 1

Introducció

1. Resum

La teoria de llenguatges formals i autòmats finits té un paper fonamental al camp de les ciències de la computació. Aquesta disciplina es centra a comprendre els límits i capacitats dels sistemes de computació. Tradicionalment s'han emprat per aquest estudi autòmats finits, que són models abstractes de màquines capaces de reconèixer i generar llenguatges formals.

Per introduir i començar a entendre aquesta matèria cal referir-se a les contribucions d'Alan Turing i Noam Chomsky. El primer és considerat el pare de la ciència de la computació i va crear el tan popular concepte de màquina de Turing als anys 30. El seu paper va ser fonamental per establir la base teòrica de la computació. El segon va introduir el concepte de gramàtica formal als anys 50 per tal d'establir una classificació que distingeix, en ordre de menys a més complexa, els llenguatges formals segons el nom de la gramàtica que els genera, entre:

- Llenguatges regulars, reconeguts per autòmats d'estat finit.
- Llenguatges lliures de context, reconeguts per autòmats de pila.
- Llenguatges sensibles al context, reconeguts per màquines de Turing amb cinta finita.
- Llenguatges recursivament enumerables, reconeguts per una màquina de Turing.

Aquesta contribució va ser crucial per comprendre l'estructura dels llenguatges naturals i formals estudiant les seues gramàtiques generatives.

La introducció del concepte d'autòmat va permetre aplicar aquests coneiximents al disseny de compiladors, verificació de sistemes i solució de problemes amb intel·ligència artificial. No obstant això, a mesura que avançava la investigació, van sorgir noves perspectives com la que presentem en aquest treball, l'àlgebraica. Aquesta pretén fer ús de conceptes i tècniques àlgebraiques per analitzar i manipular llenguatges regulars. Podem destacar les contribucions de Jacques Sakarovitch

[Sakarovitch, 2015] i Jean-Éric Pin [Pin, 2010]. El primer va desenvolupar l'àlgebra de les expressions regulars i la seua aplicació a l'anàlisi dels llenguatges regulars, el que va permetre crear algorismes eficients per al processament de llenguatges regulars. Va demostrar que les expressions regulars i els autòmats finits són equivalents en termes de representació i capacitat de reconeixement de llenguatges regulars. El segon, i curiosament més important perquè dóna peu a aquest treball, desenvolupa la teoria de les àlgebres de llenguatges, demostrant que els llenguatges regulars es poden representar mitjançant àlgebres de llenguatges finits. Aquesta representació algebraica permet l'estudi sistemàtic i estructurat dels llenguatges regulars, així com l'anàlisi de les propietats i operacions associades a ells.

En el present treball ens centrem en els llenguatges regulars, que serveixen per descriure patrons senzills i s'empren amplament en l'anàlisi lèxic de compiladors, expressions regulars, protocols de comunicació i molts altres contextos. Presentem una metodologia de reconeixement de llenguatges regulars mitjançant monoides que substitueix a la teoria tradicional d'autòmats finits. La importància d'aquesta perspectiva radica en la seua capacitat per a simplificar i generalitzar el procés de reconeixement de llenguatges regulars. L'ús de la teoria de monoides no només ens permet tindre una perspectiva més clara des del punt de vista matemàtic dels llenguatges regulars, sinó que també podem traslladar les nocions d'ordre entre les estructures algebraiques a l'àmbit dels llenguatges regulars i estudiar les relacions entre llenguatges. Així i tot, el que possiblement és el més interessant d'aquesta proposta és l'oportunitat d'entendre els llenguatges regulars estalviant-se la llarga i, en ocasions, tediosa presentació de la teoria d'autòmats gràcies a l'equivalència que provarem entre reconeixement per autòmats i per monoides.

L'estructura serà la següent. A la Secció 2 establim la base teòrica. Al Capítol 2 desenvolupem la teoria de monoides, a la Secció 1 es presenten les definicions necessàries, a la Secció 2 estudiem el monoide lliure que apareix a la part de reconeixibilitat, a la Secció 3 ampliem la teoria de monoides adreçada a submonoides, a la Secció 4 estudiem les congruències, a la Secció 5 enunciem el Primer Teorema d'Isomorfisme de monoides que ens serveix per a estudiar les congruències d'índex finit a la Secció 6 i els llenguatges saturats a la Secció 7. Finalment, al Capítol 3 introduïm la noció de reconeixibilitat que necessita la base teòrica definida a la Secció 1, és presentada des de la perspectiva dels monoides a la Secció 2 i la perspectiva dels autòmats i el resultat de l'equivalència apareix a la Secció 3.

2. Preliminars

Establim la notació bàsica emprada en aquest treball i alguna proposició que antecedeix als continguts a què s'ajusta el treball.

Comencem amb els ordinals que seran emprats en les enumeracions.

DEFINICIÓ 1.1 (Ordinal). *Direm que α és un ordinal si és un conjunt transitiu que està ben ordenat segons $\in$, és a dir, $\alpha = \{\beta \mid \beta \in \alpha\}$. El primer ordinal transfinit serà denotat $\mathbb{N}$, el conjunt dels nombres naturals. Emprant la construcció conjuntista dels naturals tenim $0 = \emptyset$ i per a $n \in \mathbb{N}$, $n = \{0, \dots, n-1\}$, de manera que $n+1 = n \cup \{n\}$. Podem definir la suma de naturals de manera recursiva amb les nocions plantejades:*

$$\begin{aligned} +: \quad \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (m, n) &\longmapsto \begin{cases} m & n = 0. \\ (m + k) + 1 & n = k + 1. \end{cases} \end{aligned}$$

2.1. Aplicacions i noms destacables. En aquesta subsecció posem nom i notació a diferents elements involucrats amb les aplicacions.

DEFINICIÓ 1.2 (Sub(A)). *Siga A un conjunt, Sub(A) denota la família de subconjunts d' A . Formalment,*

$$\text{Sub}(A) = \{X \mid X \subseteq A\}.$$

DEFINICIÓ 1.3 (Fnc(A, B)). *Siguen A i B conjunts. Una funció d' A en B és una relació $F \subseteq A \times B$ que satisfà que, per a tot $a \in A$, existeix un únic $b \in B$ tal que $(a, b) \in F$. Denotem per Fnc(A, B) al conjunt de totes les funcions d' A en B .*

DEFINICIÓ 1.4 (Hom(A, B)). *Siguen A i B conjunts. Una aplicació d' A en B és una tripleta $f = (A, F, B)$, també denotada $f: A \longrightarrow B$, en què F és una funció d' A en B . Denotem per Hom(A, B) al conjunt de totes les aplicacions d' A en B . Així,*

$$\text{Hom}(A, B) = \{A\} \times \text{Fnc}(A, B) \times \{B\}.$$

En el cas que $A = B$, escrivim End(A) en comptes d'Hom(A, A).

DEFINICIÓ 1.5 (Identitat). *Siga A un conjunt, denotem per id_A l'aplicació en End(A) tal que*

$$\begin{aligned} \text{id}_A: \quad A &\longrightarrow A \\ a &\longmapsto a \end{aligned}$$

Aquesta aplicació es diu identitat en A .

Anem a introduir a continuació les nocions d'imatge directa i d'imatge inversa d'una aplicació.

DEFINICIÓ 1.6 (Imatge directa). *Siguen A i B conjunts, donada $f: A \longrightarrow B$ aplicació d' A en B , aleshores la imatge directa de f és l'aplicació*

$$\begin{aligned} f[\cdot]: \text{Sub}(A) &\longrightarrow \text{Sub}(B) \\ X &\longmapsto \{f(x) \in B \mid x \in X\}. \end{aligned}$$

Notem que si $X \subseteq A$, $x \in X$, aleshores $f(x) \in B$. Així $f[X] \subseteq B$ i l'aplicació imatge directa està ben definida.

DEFINICIÓ 1.7 (Imatge inversa). *Siguen A i B conjunts, donada $f: A \longrightarrow B$ aplicació d' A en B , aleshores la imatge inversa de f és l'aplicació*

$$\begin{aligned} f^{-1}[\cdot]: \text{Sub}(B) &\longrightarrow \text{Sub}(A) \\ Y &\longmapsto \{a \in A \mid f(a) \in Y\}. \end{aligned}$$

En aquest cas està ben definida per la pròpia definició de f .

Els següents dos conjunts que apareixen són importants per a la teoria de monoides que presentarem en el següent capítol.

DEFINICIÓ 1.8 (Conjunt imatge). *Siguen A i B conjunts, donada $f: A \longrightarrow B$ aplicació d' A en B , aleshores el conjunt imatge de f és el conjunt format per les imatges per f dels elements d' A . El denotem*

$$\text{Im}(f) = f[A] = \{f(x) \in B \mid x \in A\}.$$

DEFINICIÓ 1.9 (Nucli de l'aplicació). *Siguen A i B conjunts, donada $f: A \longrightarrow B$ aplicació d' A en B , aleshores el nucli de f és el conjunt de parelles d'elements d' A que tenen la mateixa imatge per f . El denotem*

$$\text{Ker}(f) = \{(a, a') \in A \times A \mid f(a) = f(a')\}.$$

DEFINICIÓ 1.10 (Injecció canònica). *Siga A un conjunt i $X \subseteq A$, la injecció canònica de X en A és l'aplicació*

$$\begin{aligned} \text{in}_X: X &\longrightarrow A \\ x &\longmapsto x. \end{aligned}$$

De manera que la restricció d'una aplicació f , que tinga domini A , a X és $f \upharpoonright_X = f \circ \text{in}_X$.

2.2. Relacions binàries. Continuem construint la nostra teoria ara centrant-nos en les relacions definides sobre elements d'un conjunt i els objectes matemàtics que se'n deriven.

DEFINICIÓ 1.11 (Relació binària). *Siga A un conjunt, una relació binària, Φ , en A és un subconjunt del producte cartesià $A \times A$. És a dir,*

$\Phi \subseteq A \times A$. En aquest cas, si $(x, y) \in \Phi$ direm que x està Φ -relacionat amb y . Aquest fet també pot denotar-se per $x\Phi y$.

DEFINICIÓ 1.12 (Relació binària d'equivalència). *Siga A un conjunt, una relació binària en A , Φ , és d'equivalència si satisfà les següents propietats:*

- *Reflexiva: Tot $x \in A$ està Φ -relacionat amb si mateix. És a dir, per a tot $x \in A$, $x\Phi x$.*
- *Simètrica: Siguen $x, y \in A$, x està Φ -relacionat amb y si, i només si, y està Φ -relacionat amb x . És a dir, per a tots $x, y \in A$, si $x\Phi y$, aleshores $y\Phi x$.*
- *Transitiva: Per a qualssevol $x, y, z \in A$, que x i y , y i z estiguin Φ -relacionats implica que x i z també ho estiguin. Per a tots $x, y, z \in A$, si $x\Phi y, y\Phi z$ aleshores $x\Phi z$.*

Denotem per $\text{Equiv}(A)$ al conjunt de les relacions binàries d'equivalència en A .

DEFINICIÓ 1.13 (Refinament). *Siga A un conjunt, donades dues relacions binàries d'equivalència en A , Φ i Ψ , direm que Ψ és un refinament de Φ si està continguda en aquesta, és a dir, si $\Psi \subseteq \Phi$.*

PROPOSICIÓ 1.14 ($\text{Equiv}(A)$ és tancat per a interseccions). *Siga A un conjunt, donades dues relacions binàries d'equivalència en A , Φ i Ψ , aleshores $\Phi \cap \Psi$ és relació d'equivalència i és refinament de Φ i Ψ .*

DEMOSTRACIÓ. En primer lloc observem que $\Psi \cap \Phi \subseteq \Phi, \Psi$. Ja que els elements satisfan $(a, b) \in \Phi \cap \Psi$ si, i només si, $(a, b) \in \Phi$ i també $(a, b) \in \Psi$. Vegem que la intersecció és també relació binària d'equivalència verificant que compleix les tres propietats de la definició. Com Φ, Ψ satisfan aquestes propietats, per tots $x, y, z \in A$,

- (1) Tant $(x, x) \in \Phi$ com $(x, x) \in \Psi$, per tant $(x, x) \in \Phi \cap \Psi$. Equivalentment, $\Phi \cap \Psi$ compleix la reflexivitat.
- (2) Tan per Φ com per Ψ , que x estiga relacionat amb y succeïx, si, i només si, y relacionat amb x . Així, $(x, y) \in \Phi \cap \Psi$ si, i només si, $(y, x) \in \Phi \cap \Psi$. Del qual es deriva la simetria de $\Phi \cap \Psi$.
- (3) Les dues relacions, Φ i Ψ , verifiquen que si contenen a (x, y) i (y, z) , necessàriament també contenen a (x, z) . Per aquest motiu, si $(x, y), (y, z) \in \Phi \cap \Psi$, aleshores $(x, z) \in \Phi \cap \Psi$. Queda demostrat que $\Phi \cap \Psi$ satisfà la propietat transitiva.

Com queda provat que $\Phi \cap \Psi$ pertany a $\text{Equiv}(A)$ i a més està continguda tant a Φ com a Ψ , hem demostrat que és refinament d'aquestes relacions. $\square$

Gràcies a les relacions d'equivalència en un conjunt podem agrupar els elements en classes que constitueixen una partició del conjunt.

DEFINICIÓ 1.15 (Classe). *Siga A un conjunt i $\Phi \in \text{Equiv}(A)$, per a cada $x \in A$, la Φ -classe d'equivalència de x és el conjunt dels elements d' A que estan Φ -relacionats amb x . És a dir,*

$$[x]_{\Phi} = \{y \in A \mid x\Phi y\}.$$

PROPOSICIÓ 1.16 (Propietat de les classes d'equivalència). *Siga A un conjunt, $\Phi \in \text{Equiv}(A)$, per a tots $x, y \in A$ es compleix*

$$y \in [x]_{\Phi} \text{ si, i només si, } [x]_{\Phi} = [y]_{\Phi} \text{ si, i només si, } [x]_{\Phi} \cap [y]_{\Phi} \neq \emptyset.$$

DEMOSTRACIÓ. Seguint la definició de classe d'equivalència, tenim que $y \in [x]_{\Phi}$ si, i només si, $x\Phi y$. Al mateix temps, per tot $z \in A$ tal que $z \in [x]_{\Phi}$, com $x\Phi z$ i Φ és transitiva, $y\Phi z$ i així $z \in [y]_{\Phi}$. Acabem de veure que $y \in [x]_{\Phi}$ si, i només si, $[x]_{\Phi} = [y]_{\Phi}$.

Per una altra banda, $[x]_{\Phi} \cap [y]_{\Phi} \neq \emptyset$ equival a què existeix un z que pertany a aquesta intersecció. Per definició $z\Phi x$ i $z\Phi y$. Finalment, per la transitivitat de Φ , $x\Phi y$, el qual acabem de provar que equival tant a $y \in [x]_{\Phi}$ com a $[x]_{\Phi} = [y]_{\Phi}$.

Hem demostrat la triple equivalència que satisfan les classes d'equivalència. $\square$

Pel fet que les classes siguin disjunctes, podem descomposar A com unió de les seues classes, on cadascuna es pot representar agafant com a representant qualsevol element de la classe.

DEFINICIÓ 1.17 (Conjunt quocient). *Siga A un conjunt, donada $\Phi \in \text{Equiv}(A)$ podem construir el quocient de Φ sobre A com el conjunt de les classes d'equivalència que defineix Φ en A . Es denota*

$$A/\Phi = \{[x]_{\Phi} \mid x \in A\}.$$

DEFINICIÓ 1.18 (Projecció). *Siga A un conjunt, donada una relació $\Phi \in \text{Equiv}(A)$, la projecció d' A mitjançant Φ és l'aplicació*

$$\begin{aligned} \text{pr}_{\Phi}: \quad A &\longrightarrow A/\Phi \\ x &\longmapsto [x]_{\Phi}. \end{aligned}$$

A partir d'aquest moment, tenim definida la base de la teoria de conjunts que necessitem al nostre univers matemàtic. Doncs, seguim amb conceptes més específics que ocupen l'interés d'aquest treball.

DEFINICIÓ 1.19 (Transversal). *Siga A un conjunt i $\Phi \in \text{Equiv}(A)$, un transversal de Φ és un subconjunt d' A , $T \in \text{Sub}(A)$, que conté un i només un representant de cada Φ -classe en A . És a dir, per a tot $x \in A$ existeix un únic $y \in T$ tal que $y \in [x]_{\Phi}$.*

NOTA 1.20. En general, el concepte de transversal en Φ no és únic, ja que es podrien formar diferents transversals triant diferents representants de les Φ -classes. Per exemple, donada la congruència mòdul 2 en $\mathbb{Z}$, tant $T_1 = \{0, 1\}$ com $T_2 = \{2, 3\}$ són transversals.

DEFINICIÓ 1.21 (Saturat). Siga A un conjunt i $\Phi \in \text{Equiv}(A)$, un subconjunt $X \in \text{Sub}(A)$ direm que està Φ -saturat si per tot $x \in X$ i per a tot $y \in A$, si $x\Phi y$, aleshores $y \in X$.

Podem vore que un conjunt saturat és necessàriament unió de classes d'equivalència.

PROPOSICIÓ 1.22 (Caracterització de la saturació). Siga A un conjunt, $X \in \text{Sub}(A)$ i $\Phi \in \text{Equiv}(A)$. X està Φ -saturat si, i només si, X és unió de Φ -classes d'equivalència. De fet, si, i només si,

$$X = \bigcup_{x \in X} [x]_{\Phi}.$$

DEMOSTRACIÓ. Si X és Φ -saturat, donat $x \in X$, per a tot $y \in [x]_{\Phi}$, $y \in X$. Aleshores $[x]_{\Phi} \subseteq X$ per tot $x \in X$. Per tant, $\bigcup_{x \in X} [x]_{\Phi} \subseteq X$. Com per definició $X \subseteq \bigcup_{x \in X} [x]_{\Phi}$, arribem a què $X = \bigcup_{x \in X} [x]_{\Phi}$.

Per altra banda, si $X = \bigcup_{x \in X} [x]_{\Phi}$, per tot $x \in X$ tenim $[x]_{\Phi} \subseteq X$. Aleshores, per tot $x \in X$ i per a tot $y \in A$, si $x\Phi y$ aleshores $y \in [x]_{\Phi}$ i llavors $y \in X$. $\square$

DEFINICIÓ 1.23 (Saturació). Siga A un conjunt, $X \in \text{Sub}(A)$ i $\Phi \in \text{Equiv}(A)$, definim la Φ -saturació de X com

$$[X]^{\Phi} = \bigcup_{x \in X} [x]_{\Phi}.$$

PROPOSICIÓ 1.24. Siga A un conjunt, $X \in \text{Sub}(A)$ i $\Phi \in \text{Equiv}(A)$, la Φ -saturació de X és el menor subconjunt saturat d' A que conté a X . En aquest sentit, X està Φ -saturat si, i només si, $X = [X]^{\Phi}$.

DEMOSTRACIÓ. A la Proposició 1.22 vam vore que X és Φ -saturat si, i només si, $X = \bigcup_{x \in X} [x]_{\Phi}$. Seguint la definició de saturació ja tenim provat que X és Φ -saturat si, i només si, $[X]^{\Phi} = X$. Pel fet que Φ satisfà la propietat reflexiva, per tot $x \in X$ tenim que $x\Phi x$. Així $x \in [x]_{\Phi}$ i $X \subseteq [X]^{\Phi}$. Vegem ara que $[X]^{\Phi}$ és el menor subconjunt que és Φ -saturat i conté a X . Suposem que $Y \in \text{Sub}(A)$ i està Φ -saturat, és a dir, $Y = \bigcup_{y \in Y} [y]_{\Phi}$. Si $X \subseteq Y$, $[X]^{\Phi} = \bigcup_{x \in X} [x]_{\Phi} \subseteq \bigcup_{y \in Y} [y]_{\Phi} = Y$. $\square$

COROLLARI 1.25 (Idempotència de la saturació). Siga A un conjunt, $X \in \text{Sub}(A)$ i $\Phi \in \text{Equiv}(A)$, l'operació de Φ -saturació és una operació idempotent, és a dir, $[[X]^{\Phi}]^{\Phi} = [X]^{\Phi}$.

DEMOSTRACIÓ. Com $[X]^\Phi$ està Φ -saturat, per la proposició anterior $[[X]^\Phi]^\Phi$ és exactament $[X]^\Phi$. $\square$

A continuació, observarem una proposició que permet caracteritzar la inclusió entre dues relacions d'equivalència sobre A . Vorem si una relació és refinament de l'altra comparant la saturació mitjançant aquestes de cada subconjunt d' A .

PROPOSICIÓ 1.26. *Siga A un conjunt i $\Phi, \Psi \in \text{Equiv}(A)$ aleshores Φ és un refinament de Ψ si, i només si, per a tot $X \in \text{Sub}(A)$*

$$[[X]^\Psi]^\Phi = [X]^\Psi.$$

DEMOSTRACIÓ. Primer fem la demostració de la implicació d'esquerra a dreta. Suposem $\Phi \subseteq \Psi$ i $X \in \text{Sub}(A)$. Que $[X]^\Psi \subseteq [[X]^\Psi]^\Phi$ es deriva de la pròpia definició d'operador de saturació, doncs el Φ -saturat de $[X]^\Psi$ és el menor subconjunt d' A que conté a $[X]^\Psi$. Basta provar

$$[[X]^\Psi]^\Phi \subseteq [X]^\Psi.$$

Donat $a \in [[X]^\Psi]^\Phi$, existeix un $b \in [X]^\Psi$ tal que $a \in [b]_\Phi$. Per definició existeix $x_0 \in X$ tal que $(b, x_0) \in \Psi$. Tenim $(a, b) \in \Phi$ i $\Phi \subseteq \Psi$, llavors $(a, b) \in \Psi$. Per la transitivitat de Ψ , $(a, x_0) \in \Psi$. De manera que $a \in [x_0]_\Psi$ i $x_0 \in X$, que implica $a \in [X]^\Psi$.

Per a la implicació de dreta a esquerra, suposem que $X \in \text{Sub}(A)$ satisfà que la Φ -saturació de $[X]^\Psi$ és exactament ell mateix, $[X]^\Psi$. Provarem emprant reducció a l'absurd, suposant $\Phi \not\subseteq \Psi$. Això implica que existeix $(a, b) \in A \times A$ tal que $(a, b) \in \Phi$ i $(a, b) \notin \Psi$. És a dir $b \in [a]_\Phi$ però $b \notin [a]_\Psi$.

Considerem el cas de $\{a\} \in \text{Sub}(A)$. Per una banda, $b \notin [\{a\}]^\Psi$, doncs

$$[\{a\}]^\Psi = [a]_\Psi.$$

Per una altra banda

$$[[\{a\}]^\Psi]^\Phi = \bigcup_{x \in [a]_\Psi} [x]_\Phi.$$

Com $a \in [a]_\Psi$ i $b \in [a]_\Phi$, aleshores $b \in [[\{a\}]^\Psi]^\Phi$. Així doncs,

$$[[\{a\}]^\Psi]^\Phi \neq [\{a\}]^\Psi,$$

el qual contradiu la nostra hipòtesi. És a dir, assumint l'antecedent i negant el conseqüent arribem a una contradicció. La implicació és llavors certa. $\square$

La següent proposició permet entendre millor l'acció de saturar subconjunts d' A . En aquest cas, centrant-nos en l'operació d'intersecció.

PROPOSICIÓ 1.27. *Siga A un conjunt i $\Phi, \Psi \in \text{Equiv}(A)$ aleshores se satisfà que, per a qualsevol $X \in \text{Sub}(A)$,*

$$[X]^{\Phi \cap \Psi} \subseteq [X]^\Phi \cap [X]^\Psi.$$

DEMOSTRACIÓ. Notem que per a $X \in \text{Sub}(A)$ es té que

$$[X]^{\Phi \cap \Psi} = \bigcup_{x \in X} [x]_{\Phi \cap \Psi}.$$

Siga $y \in [X]^{\Phi \cap \Psi}$, aleshores existeix $x \in X$ tal que $y \in [x]_{\Phi \cap \Psi}$.

Notem que

$$\begin{aligned} [x]_{\Phi \cap \Psi} &= \{z \in X \mid (x, z) \in \Phi \cap \Psi\} \\ &= \{z \in X \mid (x, z) \in \Phi, (x, z) \in \Psi\} \\ &= \{z \in X \mid (x, z) \in \Phi\} \cap \{z \in X \mid (x, z) \in \Psi\} \\ &= [x]_\Phi \cap [x]_\Psi. \end{aligned}$$

Així, si $y \in [X]^{\Phi \cap \Psi}$, hem vist que existeix un $x \in X$ tal que $y \in [x]_\Phi$ i $y \in [x]_\Psi$. Per tant $y \in [X]^\Phi$ i $y \in [X]^\Psi$. Aleshores, $y \in [X]^\Phi \cap [X]^\Psi$. És a dir, $[X]^{\Phi \cap \Psi} \subseteq [X]^\Phi \cap [X]^\Psi$. $\square$

En canvi, el recíproc de la Proposició 1.27 no té per què ser cert.

EXEMPLE 1.28. *El recíproc de la Proposició 1.27 no té per què ser cert. Sobre $\mathbb{Z}$ considerem les congruències mòdul 5 i 7, denotades respectivament per Φ i Ψ . Denotem $A = \mathbb{Z}$ i triem $X = \{0, 2, 5\}$. Per a denotar la classe dels elements que són congruents a x mòdul n emprarem la notació $[x]_n$.*

Per una banda:

$$\begin{aligned} [X]^\Phi &= [0]_5 \cup [2]_5. \\ [X]^\Psi &= [0]_7 \cup [2]_7 \cup [5]_7. \end{aligned}$$

Per l'altra banda, com que $\text{mcd}(5, 7) = 1$, la relació $\Phi \cap \Psi$ és la congruència mòdul 35 sobre $\mathbb{Z}$. A més

$$[X]^{\Phi \cap \Psi} = [0]_{35} \cup [2]_{35} \cup [5]_{35}.$$

Notem que $7 \notin [X]^{\Phi \cap \Psi}$ però $7 \in [X]^\Phi \cap [X]^\Psi$, ja que $7 \equiv 2 \pmod{5}$ i $7 \equiv 0 \pmod{7}$. Per tant, $[X]^{\Phi \cap \Psi} \not\subseteq [X]^\Phi \cap [X]^\Psi$.

2.3. Relacions d'ordre i àlgebres booleanes. Les congruències a les seccions 4 i 6 i la saturació a la secció 7 seran estudiades des de les relacions d'ordre i l'àlgebra booleana, així que han de ser definides. Ho fem a continuació.

DEFINICIÓ 1.29 (Ordre parcial). Siga $\leq$ una relació binària definida en un conjunt P . Direm que $\leq$ és un ordre parcial si donats $a, b, c \in P$ es compleixen les següents propietats:

- Reflexiva, és a dir, $a \leq a$.
- Antisimètrica, és a dir, si $a \leq b$ i $b \leq a$ aleshores $a = b$.
- Transitiva, és a dir, si $a \leq b$ i $b \leq c$ aleshores $a \leq c$.

En aquest cas direm que $(P, \leq)$ és un conjunt parcialment ordenat.

El següent exemple ens dóna claredat sobre una estructura d'ordre senzilla amb què estem acostumats a treballar.

EXEMPLE 1.30. Donat un conjunt A , el conjunt de subconjunts amb amb la relació d'inclusió és un ordre parcial $(\text{Sub}(A), \subseteq)$. Notem que tot conjunt $X \in \text{Sub}(A)$ satisfà $X \subseteq X$, així que la relació és reflexiva. També, donats $X, Y \in \text{Sub}(A)$ tals que $X \subseteq Y$ i $Y \subseteq X$, aleshores deduïm que $X = Y$ i la relació és antisimètrica. Per últim, que els elements $X, Y, Z \in \text{Sub}(A)$ satisfacen $X \subseteq Y, Y \subseteq Z$ implica que $X \subseteq Z$. Amb això vegem que la relació $\subseteq$ és transitiva i concloem la prova.

Definim ara els elements destacables d'un ordre parcial.

DEFINICIÓ 1.31. Donat un conjunt parcialment ordenat $(P, \leq)$ i un subconjunt qualsevol $X \in \text{Sub}(P)$. Una fita superior de X en P és qualsevol element $p \in P$ tal que, per a tot $x \in X$, $x \leq p$. Anàlogament, una fita inferior de X en P és qualsevol element $p \in P$ tal que, per a tot $x \in X$, $p \leq x$. Definim el suprem de X en P , denotat per $\bigvee X$, si existeix, com la menor de les fites superiors de X en P . Anàlogament, definim $\bigwedge X$, l'ínfim de X en P , si existeix, com la major de les fites inferiors de X en P .

NOTA 1.32. Quan estudiem un subconjunt $X = \{x, y\}$ d'un ordre parcial $(P, \leq)$, per simplificar la notació emprarem $x \vee y$ en lloc de $\bigvee X$ per a referir-nos al suprem de X , que és el de x i y . Anàlogament, emprarem $x \wedge y$ en lloc de $\bigwedge X$ per a referir-nos a l'ínfim de X , que és el de x i y .

DEFINICIÓ 1.33. Donat un conjunt parcialment ordenat $(P, \leq)$ i un subconjunt $X \subseteq P$, el mínim de X en P , si existeix, és l'element $p \in X$ que verifica $p \leq x$ per a tot $x \in X$ i el denotem per $\min(X)$. Anàlogament, el màxim de X en P , si existeix, és l'element $p \in X$ que verifica $x \leq p$ per a tot $x \in X$ i el denotem per $\max(X)$.

DEFINICIÓ 1.34 (Filtre). Donat un conjunt $(P, \leq)$ parcialment ordenat, un filtre de P és un subconjunt $F \in \text{Sub}(P)$ que satisfà

- (1) No ha de ser buit, $F \neq \emptyset$.
- (2) Conté totes les fites superiors dels elements que conté, és a dir, si $x \in F$ i $y \in P$ satisfà $x \leq y$, aleshores $y \in F$.
- (3) Conté l'ínfim de qualssevol dos elements seus. Donats dos elements $x, y \in F$, aleshores $x \wedge y \in F$.

Per últim, definim unes estructures d'ordre parcial que compleixen unes característiques determinades.

DEFINICIÓ 1.35 (Reticle). *Un reticle és un conjunt parcialment ordenat $(P, \leq)$ que satisfà que tant l'ínfim com el suprem de tota parella d'elements $x, y \in P$ pertany a P .*

DEFINICIÓ 1.36 (Reticle complet). *Un reticle $(P, \leq)$ es diu complet si per a cada X subconjunt de P existeixen $\bigvee X$, $\bigwedge X$ i pertanyen a P . Notem que $\bigwedge \emptyset = 1$ i $\bigvee \emptyset = 0$, és a dir, un reticle complet està obligat a tindre màxim i mínim globals.*

DEFINICIÓ 1.37 (Àlgebra Booleana). *Un reticle $(B, \leq)$ és un àlgebra Booleana si*

- (1) *Existeixen màxims i mínims globals en B denotats, respectivament, per 1 i 0.*
- (2) *Tot element x del reticle té un complementari. Això vol dir que per a tot x existeix $\neg x$ al reticle tal que $x \vee \neg x = 1$ i $x \wedge \neg x = 0$. Notem que en aquestes condicions, $\neg: B \rightarrow B$ defineix una operació unària en B .*
- (3) *El reticle és distributiu en el sentit que, per a tots $x, y, z \in B$ es verifica que $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.*

En aquest cas escriurem $(B, \wedge, \vee, \neg, 0, 1)$.

CAPÍTOL 2

Teoria de monoides

Aquest capítol gira al voltant del monoide, perquè apareixerà a la noció de reconeixibilitat que és un dels objectius d'aquest treball. No obstant això, també aprofitem per estudiar ordres parcials, ja que s'observen qualitats i subestructures interessants, que van sorgint a mesura que treballem amb els conceptes de congruència i saturació en el monoide.

1. Primeres definicions

En primer lloc establim la terminologia del capítol a les següents definicions.

DEFINICIÓ 2.1 (Monoide). *Direm que $\mathbf{M} = (M, \cdot, 1)$ és un monoide si M és un conjunt, $\cdot$ és una operació binària associativa en M i $1 \in M$ és element neutre per a l'operació $\cdot$.*

EXEMPLE 2.2. *Notem que donat un grup $(G, \cdot, 1)$, com l'operació $\cdot$ és associativa i 1 és el seu element neutre, aleshores qualsevol grup és en particular un monoide.*

DEFINICIÓ 2.3 (Homomorfisme de monoides). *Donats dos monoides $\mathbf{M} = (M, \cdot_M, 1_M)$ i $\mathbf{N} = (N, \cdot_N, 1_N)$, un homomorfisme de $\mathbf{M}$ en $\mathbf{N}$ és una aplicació $f: M \rightarrow N$ que satisfà les següents propietats*

$$(1) f(1_M) = 1_N.$$

$$(2) \text{ Per tots } m_1, m_2 \in M, f(m_1 \cdot_M m_2) = f(m_1) \cdot_N f(m_2).$$

Un isomorfisme de monoides és un homomorfisme de monoides bijectiu. Si existeix un isomorfisme de monoides entre $\mathbf{M}$ i $\mathbf{N}$ direm que són isomorfs i ho denotarem per $\mathbf{M} \cong \mathbf{N}$.

En ocasions ens interessarà construir un monoide a partir de dos monoides $\mathbf{M}$ i $\mathbf{N}$. Això ho podem fer amb el monoide producte que definim a continuació.

DEFINICIÓ 2.4 (Monoide producte). *Donats dos monoides $\mathbf{M} = (M, \cdot_M, 1_M)$ i $\mathbf{N} = (N, \cdot_N, 1_N)$, podem definir el monoide producte com*

$\mathbf{M} \times \mathbf{N} = (M \times N, \cdot, (1_M, 1_N))$ on

$$\begin{aligned} \cdot: (M \times N) \times (M \times N) &\longrightarrow M \times N \\ ((m_1, n_1), (m_2, n_2)) &\longmapsto (m_1 m_2, n_1 n_2). \end{aligned}$$

DEMOSTRACIÓ. Per la definició de $\cdot$, hereda el fet de ser operació tancada en $\mathbf{M} \times \mathbf{N}$, ja que per $m_1, m_2 \in M$ i $n_1, n_2 \in N$ tenim que $(m_1, n_1) \cdot (m_2, n_2) \in M \times N$ donat que $m_1 m_2 \in M$ en ser monoide i $n_1 n_2 \in N$ pel mateix i implica que $(m_1 m_2, n_1 n_2) \in M \times N$. Com el producte és component a component, $(1_M, 1_N)$ és el neutre de $\mathbf{M} \times \mathbf{N}$ perquè 1_M és el de $\mathbf{M}$ i 1_N el de $\mathbf{N}$. $\square$

2. Monoide lliure

En segon lloc estudiem com, a partir d'un conjunt A , que anomenarem alfabet, podem crear una estructura de monoide $\mathbf{A}^*$, anomenat monoide lliure, els elements del qual són paraules. Els llenguatges construïts sobre aquest monoide són amb els quals treballarem la reconeixibilitat per autòmats i finalment l'equivalència dels conceptes de reconeixibilitat.

Comencem amb les primeres definicions al voltant del concepte de paraula.

DEFINICIÓ 2.5 (Paraula sobre un conjunt). *Siga A un conjunt, una paraula de longitud $n \in \mathbb{N}$ sobre A és una aplicació*

$$\begin{aligned} w: n &\longrightarrow A \\ i &\longmapsto w_i. \end{aligned}$$

On tractem n com a ordinal seguint la Definició 1.1. Així, podem representar la paraula w com

$$w = (w_i)_{i \in n} = w_0 \dots w_{n-1}.$$

DEFINICIÓ 2.6 (Paraules de longitud determinada). *Siga A un conjunt, $n \in \mathbb{N}$, definim el conjunt de paraules de longitud n sobre A com $\text{Hom}(n, A)$, descrit a la Definició 1.4. Denotem per λ a l'única aplicació en $\text{Hom}(0, A)$ i l'anomenarem paraula buida.*

A partir d'un alfabet A , definim a continuació A^* com el conjunt de totes les paraules.

DEFINICIÓ 2.7 (Conjunt de totes les paraules). *Donat un conjunt A , el conjunt de totes les paraules sobre A és la unió dels conjunts de paraules de longitud n , per a tot $n \in \mathbb{N}$. El denotem*

$$A^* = \bigcup_{n \in \mathbb{N}} \text{Hom}(n, A).$$

Una vegada que hem introduït el conjunt de les paraules sobre un conjunt, vorem a continuació que té estructura de monoide on l'operació és la concatenació de paraules i el neutre és la paraula buida.

PROPOSICIÓ 2.8 (Existència del monoide lliure). *Siga A un conjunt, $\mathbf{A}^* = (A^*, \lambda, \lambda)$ és un monoide, on λ és la concatenació de paraules, definida com segueix. Siguen $n, m \in \mathbb{N}$, donades $w \in \text{Hom}(n, A)$ i $v \in \text{Hom}(m, A)$ definim*

$$\begin{aligned} w \lambda v: \quad n + m &\longrightarrow A \\ i &\longmapsto \begin{cases} w_i & i \in n. \\ v_{i-n} & n \leq i < n + m. \end{cases} \end{aligned}$$

Aquest monoide rep el nom de monoide lliure sobre A .

DEMOSTRACIÓ. Per veure que $\mathbf{A}^*$ és un monoide, segons la Definició 2.1, comprovarem que λ és el neutre per a la concatenació ja que l'associativitat se segueix de la definició de λ .

Siga $w \in A^*$, per definició, existeix $n \in \mathbb{N}$ tal que $w \in \text{Hom}(n, A)$. Tenim $\lambda \in \text{Hom}(0, A)$ i $n + 0 = n$. Per definició de concatenació

$$\begin{aligned} w \lambda \lambda: \quad n &\longrightarrow A \\ i &\longmapsto w_i. \end{aligned}$$

De manera que $w \lambda \lambda = w$. Anàlogament per a $\lambda \lambda w = w$. □

DEFINICIÓ 2.9 (Inclusió de generadors). *Donat un conjunt A , existeix una aplicació d' A en A^* anomenada inclusió de generadors*

$$\begin{aligned} \text{in}_A: A &\longrightarrow A^* \\ a &\longmapsto a: 1 \longrightarrow A \\ 0 &\longmapsto a. \end{aligned}$$

NOTA 2.10. *Aquesta aplicació serveix per identificar la lletra $a \in A$ amb la paraula de longitud 1 en A^* , formada únicament pel símbol a .*

A continuació, treballarem sobre una proposició molt útil pel tema que ens pertoca, ja que exposa la capacitat d'extendre una aplicació que va d'un conjunt A en un monoide al monoide A^* de totes les paraules sobre A .

PROPOSICIÓ 2.11 (Propietat Universal del monoide lliure). *Siguen A un conjunt, $\mathbf{M} = (M, \cdot, 1)$ un monoide i $f: A \longrightarrow M$ una aplicació, llavors existeix un únic $f^\# : \mathbf{A}^* \longrightarrow \mathbf{M}$ homomorfisme de monoides tal que*

$$f^\# \circ \text{in}_A = f.$$

On in_A és la inclusió de generadors introduïda a la Definició 2.9.

DEMOSTRACIÓ. Per a provar l'existència de l'homomorfisme, fem una demostració constructiva donant una expressió per aquest. Construïrem $f^\sharp$ de manera recursiva sobre la longitud de la paraula. Siga $w \in A^*$, existeix $n \in \mathbb{N}$ tal que $w \in \text{Hom}(n, A)$. Distingim pel valor de n :

- Si $n = 0$, aleshores $w = \lambda$ i definim $f^\sharp(\lambda) = 1$. De manera que enviem el neutre d' A^* al neutre de $\mathbf{M}$.
- Si $n = 1$, aleshores existeix $a \in A$ tal que $w = a$ i definim $f^\sharp(a) = f(a)$. Ací gastem la Definició 2.9 per identificar el símbol $a \in A$ amb $\text{in}_A(a) \in A^*$ paraula de longitud 1. Tenim ací la igualtat $(f^\sharp \circ \text{in}_A)(a) = f(a)$.
- Si $n > 1$, podem descomposar per la dreta qualsevol paraula com la concatenació d'una paraula de longitud $n - 1$ amb una de longitud 1. És a dir, $w = v \wedge a$ on $v \in \text{Hom}(n-1, A)$ i $a \in A$. Això ens permet definir $f^\sharp(w) = f^\sharp(v) \cdot f(a)$ per tal d'obtindre una aplicació que siga homomorfisme dels monoides.

Desenvolupant aquest raonament de manera recursiva, obtenim que per a tot $n \in \mathbb{N}$, si $w \in \text{Hom}(n, A)$ amb $w = (w_i)_{i \in n}$, aleshores

$$f^\sharp(w) = f^\sharp((w_i)_{i \in n}) = f^\sharp(w_0 \wedge \dots \wedge w_{n-1}) = f(w_0) \cdot \dots \cdot f(w_{n-1}).$$

Aquesta està ben definida perquè, per a tot $i \in n$, $f(w_i) \in M$ per hipòtesi i el producte de $\mathbf{M}$ és una operació binària associativa en M .

Ara vorem que efectivament aquesta aplicació és homomorfisme, comprovant que la concatenació de paraules s'envia al producte de les imatges de les paraules. Realment se segueix de la definició, ja que a la construcció de $f^\sharp$ hem aplicat que la paraula $(w_i)_{i \in n}$ és la concatenació de les n paraules de longitud un $w_i = \text{in}_A(w_i)$ on $i \in n$,

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

D'aquesta manera, agafant un $v = (v_j)_{j \in m} \in A^*$, on $m \in \mathbb{N}$, comprovem

$$\begin{aligned} f^\sharp(w \wedge v) &= f^\sharp((w \wedge v_0 \wedge \dots \wedge v_{m-2}) \wedge v_{m-1}) \\ &= f^\sharp(w \wedge v_0 \wedge \dots \wedge v_{m-2}) \cdot f(v_{m-1}) \\ &= f^\sharp(w \wedge v_0 \wedge \dots \wedge v_{m-3}) \cdot f(v_{m-2}) \cdot f(v_{m-1}) \\ &\dots \\ &= f^\sharp(w) \cdot f(v_0) \cdot \dots \cdot f(v_{m-1}) \\ &= f^\sharp(w) \cdot f^\sharp(v). \end{aligned}$$

Per últim, vorem que aquest homomorfisme és únic. Suposem que $g: A^* \rightarrow \mathbf{M}$ és un homomorfisme de monoides que satisfà $g \circ \text{in}_A = f$.

Considerem $w = (w_i)_{i \in n} \in A^*$, aleshores

$$\begin{aligned} g(w_0 \dots w_{n-1}) &= g(w_0 \wedge \dots \wedge w_{n-1}) \\ &= g(w_0) \cdot \dots \cdot g(w_{n-1}) \\ &= g(\text{in}_A(w_0)) \cdot \dots \cdot g(\text{in}_A(w_{n-1})) \\ &= f(w_0) \cdot \dots \cdot f(w_{n-1}) \\ &= f^\#(w). \end{aligned}$$

La primera igualtat és la mateixa que s'ha gastat per construir $f^\#$, la segona ve de l'hipòtesi que g és homomorfisme de monoides, la tercera ve de la identificació exposada a la Definició 2.9, la quarta de l'hipòtesi $g \circ \text{in}_A = f$ i l'última de la definició de $f^\#$. Com coincideixen les imatges de g i $f^\#$ element a element, hem provat que es tracta de la mateixa aplicació. $\square$

Anem a fer servir la propietat universal per a construir homomorfismes entre un monoide lliure i el monoide $(\mathbb{N}, +, 0)$. Això ens donarà una visió més clara de l'utilitat d'aquesta última proposició i de com es fa servir.

DEFINICIÓ 2.12 (Longitud de paraula). *Siga A un conjunt, considerem l'aplicació*

$$\begin{array}{ccc} \kappa_1: & A & \longrightarrow \mathbb{N} \\ & a & \longmapsto 1 \end{array}.$$

Aplicant la propietat universal, existeix l'homomorfisme de monoides

$$\begin{array}{ccc} \kappa_1^\#: & A^* & \longrightarrow \mathbb{N} \\ & (w_i)_{i \in n} & \longmapsto \sum_{i=0}^{n-1} \kappa_1(w_i) = n \end{array}$$

Denotem aquest homomorfisme com $|\cdot|$ i el denominem longitud de paraula, ja que donat $w \in \text{Hom}(n, A)$, on $n \in \mathbb{N}$, $|w| = n$ que és el que hem definit com la seua longitud.

DEFINICIÓ 2.13 (Comptador de símbols). *Siga $A = \{a, b\}$ un alfabet i $f : A \longrightarrow \mathbb{N}$ tal que $f(a) = 1$ i $f(b) = 0$ aleshores podem construir per propietat universal un únic homomorfisme de monoides tal que, per $w \in \text{Hom}(n, A)$, $f^\#(w) = |\{i \in n \mid w_i = a\}|$. És l'homomorfisme que compta el nombre de símbols a d'una paraula i es denota per $|\cdot|_a$.*

NOTA 2.14. *Si haguérem definit l'aplicació f anterior sobre el monoide $(\mathbb{Z}_2, +, 0)$, $f : A \longrightarrow \mathbb{Z}_2$, aplicant en aquest cas la propietat universal tenim $f^\#(w) = |w|_a \bmod 2$. Un homomorfisme que retorna 0 si el nombre de símbols a en w és parell i 1 en altre cas.*

3. Submonoides

En aquesta secció, treballarem més base teòrica, ara respecte a la construcció de monoides a partir d'un monoide primigeni, que ens faran falta per a resultats posteriors.

DEFINICIÓ 2.15 (Tancament). *Donat un monoide $\mathbf{M} = (M, \cdot, 1)$ i un subconjunt $N \subseteq M$, direm que N és tancat en $\mathbf{M}$ si satisfà*

- *Conté l'element neutre, és a dir, $1 \in N$.*
- *El producte dels seus elements queda dins. És a dir, per a tots $n_1, n_2 \in N$ el seu producte $n_1 n_2 \in N$.*

PROPOSICIÓ 2.16 (Estructura de submonoides). *Si $\mathbf{M} = (M, \cdot, 1)$ és un monoide i $N \subseteq M$ és tancat, aleshores N admet també una estructura de monoide $\mathbf{N} = (N, \cdot, 1)$ amb el producte*

$$\begin{aligned} \cdot : N \times N &\longrightarrow N \\ (n_1, n_2) &\longmapsto n_1 n_2. \end{aligned}$$

En aquest cas, direm que $\mathbf{N}$ és submonoide de $\mathbf{M}$. D'aquesta manera l'aplicació d'injecció canònica $\text{in}_N : N \longrightarrow M$, introduïda a la Definició 1.10, és un homomorfisme de monoides injectiu.

DEMOSTRACIÓ. Que $\mathbf{N}$ siga un monoide es deriva directament de la definició de tancament, N conté l'element neutre, té una operació binària, $\cdot$, que és interna en ser N tancat i associativa ja que el producte és associatiu en M , en ser $\mathbf{M}$ monoide. Per tant, també ho ha de ser a la restricció a N .

La inclusió és injectiva per definició i aquesta en particular és homomorfisme de monoides perquè preserva el producte, doncs per tots $n_1, n_2 \in N$ tenim que $\text{in}_N(n_1 n_2) = n_1 n_2 = \text{in}_N(n_1) \text{in}_N(n_2)$. $\square$

4. Congruències

En quart lloc presentem les congruències sobre un monoide, ara que ja tenim els conceptes suficients per estudiar-les. La motivació de les congruències és, per una banda, l'estudi de la seua estructura d'ordre i, per l'altra, que donen lloc al concepte de saturació que apareix posteriorment.

DEFINICIÓ 2.17 (Congruència). *Donat un monoide $\mathbf{M} = (M, \cdot, 1)$ i una relació binària $\Phi \subseteq M \times M$, direm que Φ és congruència en $\mathbf{M}$ si $\Phi \in \text{Equiv}(M)$ i a més és compatible amb el producte $\cdot$. És a dir, per a tots $m_1, m_2, n_1, n_2 \in M$, si $(m_1, m_2), (n_1, n_2) \in \Phi$ aleshores $(m_1 n_1, m_2 n_2) \in \Phi$. Al conjunt de congruències en $\mathbf{M}$ el denotem per $\text{Cong}(\mathbf{M})$.*

Ens interessarà associar a cada congruència el quocient que determina sobre el monoide per entendre com el parteix. Vegem que aquest quocient també és un monoide amb l'operació del producte de classes i la classe del neutre com a neutre.

PROPOSICIÓ 2.18 (Monoide quocient). *Donat un monoide $\mathbf{M} = (M, \cdot, 1)$ i una congruència Φ sobre $\mathbf{M}$, el conjunt quocient M/Φ admet estructura de monoide: $\mathbf{M}/\Phi = (M/\Phi, \cdot, [1]_\Phi)$, on*

$$\begin{aligned} \cdot: M/\Phi \times M/\Phi &\longrightarrow M/\Phi \\ ([m]_\Phi, [n]_\Phi) &\longmapsto [mn]_\Phi. \end{aligned}$$

En aquestes condicions, la projecció introduïda a la Definició 1.18

$$\text{pr}_\Phi: \mathbf{M} \longrightarrow \mathbf{M}/\Phi$$

és un homomorfisme de monoides sobrejectiu.

DEMOSTRACIÓ. En primer lloc anem a comprovar que l'operació binària està ben definida. Efectivament, si $[m]_\Phi, [n]_\Phi$ estan a M/Φ , el seu producte definit com $[m]_\Phi [n]_\Phi = [mn]_\Phi$ està ben definit perquè com Φ és una congruència en $\mathbf{M}$

$$\text{si } m' \in [m]_\Phi \text{ i } n' \in [n]_\Phi, \text{ aleshores } m'n' \in [mn]_\Phi.$$

A més $[mn]_\Phi$ pertany al quocient perquè, com $\mathbf{M}$ és monoide, donats dos elements $m, n \in M$, aleshores $mn \in M$.

En segon lloc, l'element neutre és $[1]_\Phi$ ja que per a tot $[m]_\Phi \in M/\Phi$ se satisfà $[m]_\Phi [1]_\Phi = [m1]_\Phi = [m]_\Phi$, donat que 1 és el neutre de $\mathbf{M}$. Anàlogament per a $[1]_\Phi [m]_\Phi$.

En tercer lloc, vorem que la projecció és homomorfisme de monoides sobrejectiu.

L'aplicació està ben definida perquè, donat $m \in M$ la classe d'equivalència definida per Φ és un element del quocient per definició $\text{pr}_\Phi(m) = [m]_\Phi \in M/\Phi$.

Per a vore que és homomorfisme comprovem que el neutre s'envia al neutre i que la imatge per pr_Φ conserva l'estructura dels monoides amb les seues operacions. En efecte, $\text{pr}_\Phi(1) = [1]_\Phi$ i per la definició del producte del monoide quocient

$$\text{pr}_\Phi(mn) = [mn]_\Phi = [m]_\Phi [n]_\Phi = \text{pr}_\Phi(m) \text{pr}_\Phi(n).$$

És a dir la projecció respecta les operacions de $\mathbf{M}$ i $\mathbf{M}/\Phi$.

Finalment, la sobrejectivitat prové de l'observació que tot $[m]_\Phi$ és la imatge d'un element de M mitjançant la projecció. És a dir, existeix un $m \in M$ (per exemple el representant) tal que $\text{pr}_\Phi(m) = [m]_\Phi$. $\square$

NOTA 2.19. *Observem que a la definició del producte com operació del monoide quocient emprem el mateix símbol $\cdot$ que el producte de $\mathbf{M}$ per simplificar notació. Estem definint el producte de classes, elements del quocient, com la classe del producte dels representants.*

Per a un monoide $\mathbf{M}$, el conjunt parcialment ordenat $(\text{Cong}(\mathbf{M}), \subseteq)$ té propietats interessants. Vegem als següents resultats que, per a tota família de congruències en $\mathbf{M}$, el seu ínfim i suprem existeixen en $\text{Cong}(\mathbf{M})$.

PROPOSICIÓ 2.20 (Intersecció de congruències). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i siguin Ψ, Φ congruències en $\mathbf{M}$, aleshores $\Phi \cap \Psi$ és també congruència en $\mathbf{M}$.*

DEMOSTRACIÓ. Sabem que la intersecció de relacions d'equivalència és també relació d'equivalència, per tant $\Phi \cap \Psi \in \text{Equiv}(M)$. En primer lloc, comprovem que $\Phi \cap \Psi$ és en efecte congruència en $\mathbf{M}$ estudiant la compatibilitat de la relació d'equivalència amb el producte. Considerem $u_1, u_2, v_1, v_2 \in M$ tals que $(u_1, u_2), (v_1, v_2) \in \Phi \cap \Psi$ aleshores tenim que $(u_1, u_2), (v_1, v_2) \in \Phi$ i $(u_1, u_2), (v_1, v_2) \in \Psi$. Com aquestes són congruències, afirmem que $(u_1 v_1, u_2 v_2) \in \Phi, \Psi$. El qual significa que $(u_1 v_1, u_2 v_2) \in \Phi \cap \Psi$, evidenciant així que $\Phi \cap \Psi \in \text{Cong}(\mathbf{M})$. $\square$

COROL·LARI 2.21. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $(\Phi_i)_{i \in I}$ una família arbitrària de congruències en $\mathbf{M}$, aleshores $\bigcap_{i \in I} \Phi_i$ és una congruència en $\mathbf{M}$.*

DEMOSTRACIÓ. La prova consisteix en generalitzar la demostració de la Proposició 2.20 feta per a dues congruències. $\square$

TEOREMA 2.22. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, aleshores es té que $\mathbf{Cong}(\mathbf{M}) = (\text{Cong}(\mathbf{M}), \subseteq)$ és un reticle complet. En particular, per a tota família arbitrària $(\Phi_i)_{i \in I}$ de congruències en $\mathbf{M}$ l'ímfim és*

$$\bigwedge_{i \in I} \Phi_i = \bigcap_{i \in I} \Phi_i$$

i el suprem és

$$\bigvee_{i \in I} \Phi_i = \left\{ (m, m') \in M \times M \mid \exists s+1 \in \mathbb{N}, (m_j)_{j \in s+1} \in M^{s+1} \right. \\ \left. \left(m_0 = m, m_s = m', \forall j \in s \ (m_j, m_{j+1}) \in \bigcup_{i \in I} \Phi_i \right) \right\}.$$

DEMOSTRACIÓ. Primer fem la prova de l'ímfim. Suposem que $\Psi \in \text{Cong}(\mathbf{M})$ és una fita inferior de $(\Phi_i)_{i \in I}$. Llavors, satisfà que per a tot

$i \in I$, $\Psi \subseteq \Phi_i$. De manera que $\Psi \subseteq \bigcap_{i \in I} \Phi_i$ i per tant $\bigcap_{i \in I} \Phi_i$ és la major de les fites superiors. A més, sabem que és congruència pel Corol·lari 2.21, que ens permet concloure que $\bigwedge_{i \in I} \Phi_i = \bigcap_{i \in I} \Phi_i \in \text{Cong}(\mathbf{M})$.

Per la prova del suprem, hem de vore primer que, el que hem definit com $\bigvee_{i \in I} \Phi_i$, és una congruència. Provem primer que és relació d'equivalència en M i després la compatibilitat amb el producte.

La propietat reflexiva es compleix donat que, per a tot $m \in M$, $(m, m) \in \Phi_i$ per a tot $i \in I$ perquè Φ_i és relació d'equivalència. Per tant $(m, m) \in \bigcup_{i \in I} \Phi_i$.

Estudiem la propietat simètrica. Siga $(m, m') \in \bigvee_{i \in I} \Phi_i$, aleshores existeix $s+1 \in \mathbb{N}$ tal que $(m_j)_{j \in s+1} \in M^{s+1}$, $m_0 = m$, $m_s = m'$ i per a tot $j \in s$, $(m_j, m_{j+1}) \in \bigcup_{i \in I} \Phi_i$. Notem que si prenem la seqüència en ordre invers $(n_j)_{j \in s+1}$ a on $n_j = m_{s-j}$, com cada Φ_i satisfà la propietat simètrica, tindrem que $(n_j, n_{j+1}) = (m_{s-j}, m_{s-j+1}) \in \bigcup_{i \in I} \Phi_i$. Per tant $(m', m) \in \bigvee_{i \in I} \Phi_i$.

Comprovem finalment que satisfà la propietat transitiva. Donats $(m, m'), (m', m'') \in \bigvee_{i \in I} \Phi_i$ si $(m_j)_{j \in s+1}$ és tal que $m_0 = m$ i $m_s = m'$ i $(m_j)_{j=s}^{p+s}$ és tal que $m_s = m'$ i $m_{p+s} = m''$, considerem $(m_j)_{j \in p+s+1}$. Notem que $m_0 = m, m_{p+s} = m''$ i que per construcció tenim que $(m_j, m_{j+1}) \in \bigcup_{i \in I} \Phi_i$ per a tot $j \in p+s$. Per tant $(m, m'') \in \bigvee_{i \in I} \Phi_i$, satisfent la propietat transitiva i concloent la prova que és relació d'equivalència.

La compatibilitat amb el producte ve del fet que els elements de $\bigvee_{i \in I} \Phi_i$ estan relacionats per Φ_i per algun $i \in I$ i com $\Phi_i \in \text{Cong}(\mathbf{M})$, hereda la compatibilitat amb el producte.

Per últim, demostrem que la definició de $\bigvee_{i \in I} \Phi_i$ és adequada perquè és realment el suprem de $(\Phi_i)_{i \in I}$. Considerem $\Psi \in \text{Cong}(\mathbf{M})$ fita superior de $(\Phi_i)_{i \in I}$, és a dir, que per a tot $i \in I$, $\Phi_i \subseteq \Psi$. Això implica que $\bigcup_{i \in I} \Phi_i \subseteq \Psi$. Prenem $(m, m') \in \bigvee_{i \in I} \Phi_i$, de manera que existeix $(m_j)_{j \in s+1}$ on $m_0 = m$, $m_s = m'$ i $(m_j, m_{j+1}) \in \bigcup_{i \in I} \Phi_i$ per a tot $j \in s$. Com $(m_j, m_{j+1}) \in \Psi$ per a tot $j \in s$ i $\Psi \in \text{Cong}(\mathbf{M})$, per la propietat transitiva tenim que $(m, m') \in \Psi$. Això vol dir que $\bigvee_{i \in I} \Phi_i \subseteq \Psi$, de manera que $\bigvee_{i \in I} \Phi_i$ és la menor de les fites superiors i com és congruència, podem concloure que és el suprem de $(\Phi_i)_{i \in I}$ en $\text{Cong}(\mathbf{M})$.

Seguint la Definició 1.36 podem afirmar que $\text{Cong}(\mathbf{M})$ és un reticle complet, doncs cada subconjunt de $\text{Cong}(\mathbf{M})$ té ínfim i suprem continguts en $\text{Cong}(\mathbf{M})$. $\square$

Per acabar aquesta secció, apuntem quins són els extrems del reticle $\text{Cong}(\mathbf{M})$ al següent corol·lari.

COROLLARI 2.23. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, aleshores el mínim de $\mathbf{Cong}(\mathbf{M})$ és la relació diagonal en M ,*

$$\bigwedge \mathbf{Cong}(\mathbf{M}) = \Delta_M = \{(w, u) \in M \times M \mid w = u\},$$

i el màxim és la relació total en M

$$\bigvee \mathbf{Cong}(\mathbf{M}) = \nabla_M = M \times M.$$

5. Primer Teorema d'Isomorfisme

En cinqué lloc aplicarem els coneiximents assolits sobre homomorfismes de monoides i congruències. Donat un homomorfisme de monoides $f: \mathbf{M} \rightarrow \mathbf{N}$, estudiem el Primer Teorema d'Isomorfisme de monoides que enuncia que el nucli de f defineix una congruència en $\mathbf{M}$ i el seu quocient és isomorf a la imatge per f , que és submonoide de $\mathbf{N}$.

Per tal d'acurtar la demostració del teorema d'aquesta secció, provem a la següent proposició per separat resultats que s'hi empraran.

PROPOSICIÓ 2.24 (Propietats d'homomorfismes de monoides). *Si guen $\mathbf{M}, \mathbf{N}$ monoides i $f: \mathbf{M} \rightarrow \mathbf{N}$ un homomorfisme de monoides, aleshores:*

- (1) $\text{Im}(f)$ és un subconjunt tancat de $\mathbf{N}$.
- (2) $\text{Ker}(f)$ és una congruència en $\mathbf{M}$.

DEMOSTRACIÓ. Suposem que $\mathbf{M} = (M, \cdot_M, 1_M)$ i $\mathbf{N} = (N, \cdot_N, 1_N)$

Per vore que $f[M]$ és tancat, comprovem que conté l'element neutre i el producte dels seus elements. Per una banda $1_N \in f[M]$ perquè $1_M \in M$ i que f siga homomorfisme significa que envia el neutre al neutre, és a dir,

$$1_N = f(1_M).$$

Per altra banda, si $x, y \in f[M]$, existeixen $m_1, m_2 \in M$ tals que $x = f(m_1), y = f(m_2)$ i $m_1 m_2 \in M$ perquè $\mathbf{M}$ és monoide. Com f és homomorfisme, conserva el producte. Llavors

$$f(m_1)f(m_2) = f(m_1 m_2) \in f[M].$$

Hem vist que $\text{Im}(f)$ és tancat i per la Proposició 2.16 $\mathbf{Im}(f)$ és un submonoide de $\mathbf{N}$.

Continuem amb el segon punt de la proposició, comprovant primer que $\text{Ker}(f) \in \text{Equiv}(M)$. S'han de satisfer les següents propietats:

- Reflexiva: Donat que per a tot $m \in M$, $f(m) = f(m)$ és sempre cert, per definició $(m, m) \in \text{Ker}(f)$.

- Simètrica: Siguen $m_1, m_2 \in M$, tals que $(m_1, m_2) \in \text{Ker}(f)$. Aleshores $f(m_1) = f(m_2)$, d'on podem concloure que $f(m_2) = f(m_1)$. Així $(m_2, m_1) \in \text{Ker}(f)$.
- Transitiva: Si tenim $(m_1, m_2), (m_2, m_3) \in \text{Ker}(f)$ com $f(m_1) = f(m_2)$ i $f(m_2) = f(m_3)$ implica $f(m_1) = f(m_3)$, aleshores $(m_1, m_3) \in \text{Ker}(f)$.

Comprovem que $\text{Ker}(f)$ és compatible amb el producte en $\mathbf{M}$. Suposant que $(m, m'), (p, p') \in \text{Ker}(f)$ aleshores $f(m) = f(m')$ i $f(p) = f(p')$. Afegint que f és homomorfisme $f(mp) = f(m)f(p)$ i $f(m'p') = f(m')f(p')$. Així,

$$f(mp) = f(m)f(p) = f(m')f(p') = f(m'p').$$

Per tant $(mp, m'p') \in \text{Ker}(f)$. Així $\text{Ker}(f)$ és una congruència en $\mathbf{M}$. Per la Proposició 2.18, $\mathbf{M}/\text{Ker}(f)$ és un quocient de M . $\square$

Ara ja sí que podem enunciar i demostrar el teorema.

TEOREMA 2.25 (Primer Teorema d'Isomorfisme de monoides). *Si guen $\mathbf{M}$ i $\mathbf{N}$ monoides i $f: \mathbf{M} \longrightarrow \mathbf{N}$ un homomorfisme de monoides, aleshores el monoide quocient definit per la congruència nucli de l'aplicació és isomorf al monoide en el conjunt imatge, és a dir,*

$$\mathbf{M}/\text{Ker}(f) \cong \mathbf{Im}(f).$$

DEMOSTRACIÓ. Suposem que $\mathbf{M} = (M, \cdot_M, 1_M)$ i $\mathbf{N} = (N, \cdot_N, 1_N)$.

Com acabem de veure a la Proposició 2.24, $\text{Ker}(f)$ defineix una congruència en $\mathbf{M}$ i per la Proposició 2.18 $M/\text{Ker}(f)$ admet estructura de monoide:

$$\mathbf{M}/\text{Ker}(f) = (M/\text{Ker}(f), \cdot_{M/\text{Ker}(f)}, [1_M]_{\text{Ker}(f)}).$$

Els elements són de la següent forma:

$$[m]_{\text{Ker}(f)} = \{x \in M \mid f(x) = f(m)\}.$$

Anem a construir una aplicació que anomenem bijectivitzada de f .

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

L'ordre de la demostració serà primer veure que f^b és aplicació bijectiva i després que és homomorfisme de monoides.

Com tots els elements d'una $\text{Ker}(f)$ -classe tenen la mateixa imatge per f l'aplicació està ben definida. Donat $m' \in [m]_{\text{Ker}(f)}$, per la Definició 1.15, $[m]_{\text{Ker}(f)} = [m']_{\text{Ker}(f)}$ i per definició de nucli, $f(m) = f(m')$. Aleshores $f^b([m]_{\text{Ker}(f)}) = f^b([m']_{\text{Ker}(f)})$. Fent el recorregut a la inversa provem la injectivitat, doncs $f^b([m]_{\text{Ker}(f)}) = f^b([m']_{\text{Ker}(f)})$ implica

$f(m) = f(m')$ i per definició $(m, m') \in \text{Ker}(f)$, o el que és el mateix $[m]_{\text{Ker}(f)} = [m']_{\text{Ker}(f)}$.

Siga $y \in \text{Im}(f)$, aleshores existeix $m \in M$ tal que $y = f(m)$. La classe d'equivalència de m és la preimatge per f^b de y , ja que $f^b([m]_{\text{Ker}(f)}) = f(m)$. Amb això provem la sobrejectivitat.

Una vegada hem vist que f^b és aplicació bijectiva, estudiem si és homomorfisme de monoides. Notem que $f^b([1_M]_{\text{Ker}(f)}) = f(1_M)$ per definició de f^b i $f(1_M) = 1_N$ ja que f és homomorfisme. Per tant

$$f^b([1_M]_{\text{Ker}(f)}) = 1_N.$$

És a dir, f^b envia el neutre en el neutre. Al mateix temps, donats $[m]_{\text{Ker}(f)}, [m']_{\text{Ker}(f)} \in M/\text{Ker}(f)$, es té que

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

L'anterior seqüència d'igualtats s'obté per la definició del producte en $\mathbf{M}/\text{Ker}(f)$ i en ser f homomorfisme de monoides. Així que f^b respecta els productes dels monoides. Amb tot això, podem afirmar que f^b és certament un isomorfisme de monoides. $\square$

6. Congruències d'índex finit

En aquesta secció reprenem l'estudi que vam fer del reticle $\mathbf{Cong}(\mathbf{M})$ per aprofundir en l'estructura que defineixen les congruències que determinen sobre el monoide un quocient finit.

A la següent definició posem nom a aquestes congruències.

DEFINICIÓ 2.26 (Índex de la congruència). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $\Phi \in \mathbf{Cong}(\mathbf{M})$. Definim l'índex de la congruència com el cardinal de M/Φ . Direm que Φ és una congruència d'índex finit si M/Φ és un conjunt finit. Denotarem per $\mathbf{Cong}_{\text{if}}(\mathbf{M})$ al conjunt de congruències en $\mathbf{M}$ que tenen índex finit.*

Gràcies al Primer Teorema d'Isomorfisme de monoides, coneguem una congruència d'índex finit al monoide lliure. Apareix al següent corollari.

COROLLARI 2.27 (Nucli com a congruència d'índex finit). *Siga A i $\mathbf{M} = (M, \cdot, 1)$ un monoide finit, si $f: A \rightarrow M$ és una aplicació, aleshores $\text{Ker}(f^\#)$, on $f^\#: A^* \rightarrow \mathbf{M}$ és l'homomorfisme de monoides*

definit a la Propietat Universal, defineix una congruència d'índex finit en $\mathbf{A}^*$.

DEMOSTRACIÓ. La Proposició 2.11 de la Propietat Universal indica que existeix un únic homomorfisme de monoides $f^\sharp: \mathbf{A}^* \longrightarrow \mathbf{M}$ tal que $f^\sharp \circ \text{in}_A = f$. Pel Teorema 2.25, Primer Teorema d'Isomorfisme, afegim que $\text{Ker}(f^\sharp)$ és una congruència en $\mathbf{A}^*$ satisfent $\mathbf{A}^*/\text{Ker}(f^\sharp) \cong \mathbf{Im}(f^\sharp)$. Com $\mathbf{Im}(f^\sharp)$ és submonoid de $\mathbf{M}$ i $\mathbf{M}$ és finit per hipòtesi, $\mathbf{Im}(f^\sharp)$ i $\mathbf{A}^*/\text{Ker}(f^\sharp)$ també. Queda demostrat que $\text{Ker}(f^\sharp)$ és una congruència d'índex finit. $\square$

Existeix una relació entre l'ordre i l'índex de les congruències. En particular, donada una congruència d'índex finit Φ en el monoid $\mathbf{M}$, totes les congruències majors que Φ es troben també a $\text{Cong}_{\text{if}}(\mathbf{M})$. Això apareix al següent resultat.

PROPOSICIÓ 2.28 (Relació entre l'ordre i l'índex de les congruències). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoid i $\Phi, \Psi \in \text{Cong}(\mathbf{M})$. Si Φ és congruència d'índex finit en $\mathbf{M}$ i $\Phi \subseteq \Psi$ aleshores Ψ és congruència d'índex finit en $\mathbf{M}$.*

DEMOSTRACIÓ. Provarem la finitud de M/Ψ mitjançant la construcció del següent homomorfisme de monoides sobrejectiu

$$\begin{aligned} \varphi: \quad M/\Phi &\longrightarrow M/\Psi \\ [w]_\Phi &\longmapsto [w]_\Psi \end{aligned}$$

Aquesta aplicació està ben definida perquè dos elements del domini que siguin iguals, és a dir, $w, w' \in M$ tals que $[w]_\Phi = [w']_\Phi$, satisfan que $(w, w') \in \Phi$ i per hipòtesi $(w, w') \in \Psi$. Aleshores $\varphi([w]_\Phi) = [w]_\Psi = [w']_\Psi = \varphi([w']_\Phi)$. A més és homomorfisme gairebé per definició, ja que $\varphi([1]_\Phi) = [1]_\Psi$ i

$$\varphi([w]_\Phi [w']_\Phi) = \varphi([ww']_\Phi) = [ww']_\Psi = [w]_\Psi [w']_\Psi$$

per la definició de monoid quocient.

Notem que per a tot element del codomini, $[w]_\Psi \in M/\Psi$ existeix $[w]_\Phi \in M/\Phi$ tal que $\varphi([w]_\Phi) = [w]_\Psi$. Amb això confirmem que φ és sobrejectiva i, com M/Φ té un cardinal finit, $|M/\Psi| \leq |M/\Phi|$. Assegurem així que Ψ té índex finit en M . $\square$

Hem vist que per a cada element Φ de $\text{Cong}_{\text{if}}(\mathbf{M})$, qualsevol cadena que continga elements majors que Φ està continguda en $\text{Cong}_{\text{if}}(\mathbf{M})$. D'aquesta manera, podríem recórrer $\text{Cong}_{\text{if}}(\mathbf{M})$ en sentit ascendent, seguint l'ordre de l'inclusió, fins el màxim ∇_M . En canvi, per trobar elements d'ordre inferior que Φ hem de recurrir a la intersecció de Φ amb un altre element $\Psi \in \text{Cong}_{\text{if}}(\mathbf{M})$ com mostra el següent corollari.

COROLLARI 2.29. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i siguen Ψ, Φ congruències d'índex finit en $\mathbf{M}$, aleshores $\Phi \cap \Psi$ també és una congruència d'índex finit en $\mathbf{M}$.*

DEMOSTRACIÓ. Per la Proposició 2.20 sabem que $\Phi \cap \Psi \in \text{Cong}(\mathbf{M})$. Estudiem ara l'índex de $\Phi \cap \Psi$. Partim de què $\mathbf{M}/\Phi, \mathbf{M}/\Psi$ són finits, el qual ens assegura que $\mathbf{M}/\Phi \times \mathbf{M}/\Psi$ és un monoide finit. Considerem l'aplicació

$$\begin{aligned} f: \mathbf{M} &\longrightarrow \mathbf{M}/\Phi \times \mathbf{M}/\Psi \\ m &\longmapsto ([m]_\Phi, [m]_\Psi). \end{aligned}$$

Vegem que f és homomorfisme de monoides. Primer notem que $f(1) = ([1]_\Phi, [1]_\Psi)$ que és el neutre de $\mathbf{M}/\Phi \times \mathbf{M}/\Psi$ ja que $[1]_\Phi$ és el neutre de $\mathbf{M}/\Phi$ i $[1]_\Psi$ és el neutre de $\mathbf{M}/\Psi$. Per a la compatibilitat amb el producte, considerem m_1, m_2 elements de M . Donat que Φ, Ψ són congruències en $\mathbf{M}$, tenim les igualtats $[m_1 m_2]_\Phi = [m_1]_\Phi [m_2]_\Phi$ i $[m_1 m_2]_\Psi = [m_1]_\Psi [m_2]_\Psi$. Per tant

$$\begin{aligned} f(m_1 m_2) &= ([m_1 m_2]_\Phi, [m_1 m_2]_\Psi) \\ &= ([m_1]_\Phi [m_2]_\Phi, [m_1]_\Psi [m_2]_\Psi) \\ &= ([m_1]_\Phi, [m_1]_\Psi) ([m_2]_\Phi, [m_2]_\Psi) \\ &= f(m_1) f(m_2). \end{aligned}$$

Amb això hem provat que f és homomorfisme de monoides.

El nucli de f és

$$\text{Ker}(f) = \{(m_1, m_2) \in M \times M \mid ([m_1]_\Phi, [m_1]_\Psi) = ([m_2]_\Phi, [m_2]_\Psi)\}.$$

És a dir, $(m_1, m_2) \in \text{Ker}(f)$ si, i només si, $[m_1]_\Phi = [m_2]_\Phi$ i $[m_1]_\Psi = [m_2]_\Psi$. Per tant $\text{Ker}(f) = \Phi \cap \Psi$.

Per acabar, apliquem el Teorema 2.25 per obtindre $\mathbf{M}/\text{Ker}(f) \cong \mathbf{Im}(f)$. Donat que $\mathbf{Im}(f)$ és submonoide de $\mathbf{M}/\Phi \times \mathbf{M}/\Psi$, que hem vist que és finit, aleshores el quocient és també finit i concloem que $\Phi \cap \Psi$ és una congruència d'índex finit. $\square$

Finalment, hem arribat a l'enunciat en referència a l'estructura de $\text{Cong}_{\text{if}}(\mathbf{M})$ dins $\text{Cong}(\mathbf{M})$. És el del següent corollari.

COROLLARI 2.30. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, aleshores la família de congruències d'índex finit en $\mathbf{M}$, $\text{Cong}_{\text{if}}(\mathbf{M})$, és un filtre de $\text{Cong}(\mathbf{M})$.*

DEMOSTRACIÓ. Per provar-ho, comprovarem la veracitat dels tres punts que apareixen a la Definició 1.34.

Vegem 1. La congruència total $\nabla_M = M \times M$ pertany a $\text{Cong}_{\text{if}}(\mathbf{M})$. Qualsevol dos elements de M , w, w' , satisfan $(w, w') \in \nabla_M$. De manera que ∇_M només defineix una única classe d'equivalència en M . Acabem la demostració del primer punt amb el fet que $M/\nabla_M = \{[1]_{\nabla_M}\}$, on 1 és l'element neutre de M .

La condició 2. queda demostrada amb l'ús de la Proposició 2.28 que justament enuncia que si $\Phi \in \text{Cong}_{\text{if}}(\mathbf{M})$, $\Psi \in \text{Cong}(\mathbf{M})$ i $\Phi \subseteq \Psi$, aleshores $\Psi \in \text{Cong}_{\text{if}}(\mathbf{M})$.

La condició 3. està provada ja que $\Phi, \Psi \in \text{Cong}_{\text{if}}(\mathbf{M})$, l'ímfim d'aquestes congruències és $\Phi \wedge \Psi = \Phi \cap \Psi$. Emprant el Corol·lari 2.29, que indica precisament que $\Phi \cap \Psi \in \text{Cong}_{\text{if}}(\mathbf{M})$ tindriem el resultat buscat. $\square$

COROLLARI 2.31. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, $\Phi, \Psi \in \text{Cong}_{\text{if}}(\mathbf{M})$ aleshores el suprem també és una congruència d'índex finit. És a dir $\Phi \vee \Psi \in \text{Cong}_{\text{if}}(\mathbf{M})$.*

DEMOSTRACIÓ. Per definició $\Phi \subseteq \Phi \vee \Psi$, com Φ és una congruència d'índex finit, aplicant la Proposició 2.28 podem afirmar doncs que efectivament $\Phi \vee \Psi \in \text{Cong}_{\text{if}}(\mathbf{M})$. $\square$

Hem vist que la finitud de l'índex de la congruència es comporta bé amb l'operació de suprem de congruències d'índex finit però que no tan bé amb els ínfims. Mirem per exemple l'índex del mínim de $\text{Cong}(\mathbf{M})$.

NOTA 2.32. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide. La relació diagonal $\Delta_M = \{(w, w) | w \in M\}$ només té índex finit si M és finit donat que n'hi ha una classe distinta per cada element de M . Això implica que $\mathbf{M}/\Delta_M \cong \mathbf{M}$ i que el quocient que determina té el cardinal de M .*

Tanquem la secció arreplegant els resultats que hi han aparegut.

NOTA 2.33. *Els resultats que hem obtingut respecte a l'ordre parcial $(\text{Cong}(\mathbf{M}), \subseteq)$ i el filtre $\text{Cong}_{\text{if}}(\mathbf{M})$ podem resumir-los en:*

- ∇_M és el màxim i Δ_M el mínim de $\text{Cong}(\mathbf{M})$. Només el primer està a $\text{Cong}_{\text{if}}(\mathbf{M})$.
- $\text{Cong}_{\text{if}}(\mathbf{M})$ és tancat per l'operació d'intersecció $\cap$ que coincideix amb l'ímfim de dues congruències.
- Com les fites superiors dels elements es queden a $\text{Cong}_{\text{if}}(\mathbf{M})$, si dibuixàrem el graf del reticle $\text{Cong}(\mathbf{M})$, en pintar la regió que ocupa $\text{Cong}_{\text{if}}(\mathbf{M})$ seria diferent segons el cardinal de M . Si M fora finit, aleshores el filtre ocuparia tot el reticle, ja que la congruència mínima Δ_M tindria índex finit per la Nota 2.32 i la resta de congruències, en ser fites superiors, estarien en $\text{Cong}_{\text{if}}(\mathbf{M})$ també. En cas contrari, si M fora infinit, el filtre

ocuparia una secció superior i no completa del reticle. Sabem que per cada element que trobarem Φ a $\text{Cong}_{\text{if}}(\mathbf{M})$, hauríem d'incloure a la regió pintada tots els elements per damunt de Φ al graf i, per cada Ψ a $\text{Cong}_{\text{if}}(\mathbf{M})$, inclouríem també $\Phi \cap \Psi$.

7. Saturació

L'objectiu d'aquesta secció és conèixer com són els llenguatges saturats per diferents congruències en $\mathbf{M}$.

NOTA 2.34. En aquesta secció donat un monoide $\mathbf{M} = (M, \cdot, 1)$, anomenarem llenguatge a cada subconjunt L de M .

DEFINICIÓ 2.35 (Llenguatges saturats). Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, denotem per $\text{Sat}(\mathbf{M})$ a la família de llenguatges saturats per alguna congruència en $\mathbf{M}$.

$$\text{Sat}(\mathbf{M}) = \{[L]^\Phi \mid L \in \text{Sub}(M), \Phi \in \text{Cong}(\mathbf{M})\}.$$

Així mateix, per cada $\Phi \in \text{Cong}(\mathbf{M})$ denotem per $\Phi - \text{Sat}(\mathbf{M})$ a la família de llenguatges saturats per Φ

$$\Phi - \text{Sat}(\mathbf{M}) = \{[L]^\Phi \mid L \in \text{Sub}(M)\}.$$

Notem que

$$\text{Sat}(\mathbf{M}) = \bigcup_{\Phi \in \text{Cong}(\mathbf{M})} \Phi - \text{Sat}(\mathbf{M}).$$

En tot monoide existeixen llenguatges saturats per alguna congruència i, de fet, a la següent nota tenim dos llenguatges que estan saturats per qualsevol congruència.

NOTA 2.36. Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, aleshores $\emptyset$ i M estan saturats per qualsevol congruència $\Phi \in \text{Cong}(\mathbf{M})$. És a dir,

$$[\emptyset]^\Phi = \emptyset \qquad [M]^\Phi = M.$$

Així $\{M, \emptyset\} \subseteq \Phi - \text{Sat}(\mathbf{M})$ per a tota $\Phi \in \text{Cong}(\mathbf{M})$.

La saturació també es comporta bé amb l'operació d'intersecció, com indica la següent proposició.

PROPOSICIÓ 2.37. Siga $\mathbf{M}$ un monoide, Φ una congruència en $\mathbf{M}$ i $(L_i)_{i \in I}$ una família de llenguatges, aleshores $[\bigcap_{i \in I} L_i]^\Phi \subseteq \bigcap_{i \in I} [L_i]^\Phi$. Si $L_i \in \Phi - \text{Sat}(\mathbf{M})$ per a tot $i \in I$, aleshores la inclusió anterior és, en particular, una igualtat.

DEMOSTRACIÓ. Siga $z \in [\bigcap_{i \in I} L_i]^\Phi$, per definició aquest està Φ -relacionat amb un w_0 que pertany a $\bigcap_{i \in I} L_i$. Notem que això implica que per a cada $i \in I$ existeix $w_0 \in L_i$ tal que $(z, w_0) \in \Phi$. Conseqüentment $z \in [L_i]^\Phi$ per a tot $i \in I$, és a dir, $z \in \bigcap_{i \in I} [L_i]^\Phi$.

Notem que si $L_i = [L_i]^\Phi$ per a tot $i \in I$, pel resultat acabat de provar tindriem

$$\left[\bigcap_{i \in I} L_i \right]^\Phi \subseteq \bigcap_{i \in I} L_i.$$

Com hem vist a demostracions anteriors, això és suficient per a provar que $\bigcap_{i \in I} L_i$ està Φ -saturat. $\square$

Ens centrem ara als llenguatges saturats pels extrems de $\text{Cong}(\mathbf{M})$.

COROL·LARI 2.38. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, aleshores els llenguatges saturats per ∇_M són M i $\emptyset$, mentre que tots els llenguatges estan saturats per Δ_M .*

DEMOSTRACIÓ. Comprovem primer que

$$\nabla_M - \text{Sat}(\mathbf{M}) = \{M, \emptyset\}.$$

Agafem un llenguatge L saturat per ∇_M , tenint en compte que per a qualsevol $w \in M$, $[w]_{\nabla_M} = M$. Per casos:

- Si $L = \emptyset$ aleshores $[\emptyset]^{\nabla_M} = \emptyset$.
- En cas contrari, existeix $w \in L$ i com

$$[L]^{\nabla_M} = \bigcup_{w \in L} [w]_{\nabla_M} = M,$$

aleshores $L = M$.

Queda provada la primera afirmació. Ara estudiem la validesa de

$$\Delta_M - \text{Sat}(\mathbf{M}) = \text{Sub}(M).$$

Considerem ara un llenguatge qualsevol L en $\text{Sub}(M)$, tenint en compte que per a qualsevol $w \in M$, $[w]_{\Delta_M} = \{w\}$. Per tant

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

D'aquesta manera afirmem que tot llenguatge a $\text{Sub}(M)$ és Δ_M -saturat. Termina la demostració de la segona afirmació. $\square$

Ara volem estudiar com és la relació de l'ordre entre el conjunt dels llenguatges saturats per la intersecció de congruències i la intersecció dels saturats per cada congruència.

COROLLARI 2.39. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i Φ, Ψ congruències en $\mathbf{M}$, aleshores*

$$\Phi - \text{Sat}(\mathbf{M}) \cap \Psi - \text{Sat}(\mathbf{M}) \subseteq (\Phi \cap \Psi) - \text{Sat}(\mathbf{M}).$$

DEMOSTRACIÓ. Siga $L \in \Phi - \text{Sat}(\mathbf{M}) \cap \Psi - \text{Sat}(\mathbf{M})$, és a dir, L està saturat per Φ i per Ψ . Això vol dir que $[L]^\Phi = [L]^\Psi = L$. Per tant $[L]^\Phi \cap [L]^\Psi = L$. Per definició, $L \subseteq [L]^{\Phi \cap \Psi}$ i, per la Proposició 1.27 també podem afirmar que $[L]^{\Phi \cap \Psi} \subseteq [L]^\Phi \cap [L]^\Psi$. De manera que ens queda la seqüència d'inclusions

$$L \subseteq [L]^{\Psi \cap \Phi} \subseteq [L]^\Phi \cap [L]^\Psi = L.$$

Amb això provem que $[L]^{\Phi \cap \Psi} = L$, és a dir, que L està saturat per $\Phi \cap \Psi$. Això equival a $L \in (\Phi \cap \Psi) - \text{Sat}(\mathbf{M})$. $\square$

Anàlogament, estudiem a continuació la relació d'ordre entre el conjunt dels llenguatges saturats per dues congruències ordenades, en ambdós casos, segons la relació d'inclusió.

PROPOSICIÓ 2.40. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i siguin Ψ, Φ congruències en $\mathbf{M}$ tals que $\Phi \subseteq \Psi$. Aleshores es dona la següent inclusió de conjunts*

$$\Psi - \text{Sat}(\mathbf{M}) \subseteq \Phi - \text{Sat}(\mathbf{M}).$$

DEMOSTRACIÓ. Suposem que $L \subseteq M$ està saturat per Ψ . D'aquesta forma, sabem que $[L]^\Psi = L$. Per la Proposició 1.26 sabem que $[[L]^\Psi]^\Phi = [L]^\Psi$, substituint ara L per $[L]^\Psi$ tenim que $[L]^\Phi = L$. Així hem provat que $L \in \Phi - \text{Sat}(\mathbf{M})$ i conclou la demostració. $\square$

Els resultats obtinguts en aquesta secció fins aquest moment, ens serveixen per a concloure que el conjunt de llenguatges saturats per una congruència admeten l'estructura d'àlgebra Booleana.

PROPOSICIÓ 2.41. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i Φ una congruència en $\mathbf{M}$, aleshores*

$$\Phi - \text{Sat}(\mathbf{M}) = (\Phi - \text{Sat}(\mathbf{M}), \cup, \cap, \neg, \emptyset, M),$$

on $\neg L = M - L$ per a $L \in \text{Sub}(M)$, és un àlgebra Booleana.

DEMOSTRACIÓ. En primer lloc vegem que $(\Phi - \text{Sat}(\mathbf{M}), \subseteq)$ és un reticle.

Per una banda comprovem que la inclusió i la unió de conjunts, $\cap, \cup$, són operadors binaris en $\Phi - \text{Sat}(\mathbf{M})$. Siguen $L, K \in \Phi - \text{Sat}(\mathbf{M})$, per la Proposició 2.37 sabem que $L \cap K \in \Phi - \text{Sat}(\mathbf{M})$. Vegem ara que la unió també està Φ -saturada.

Donat $z \in [L \cup K]^\Phi$, seguint la definició, sabem que existeix $w \in L \cup K$ tal que $(z, w) \in \Phi$. Si $w \in L$, com $L = [L]^\Phi$, aleshores $z \in L \subseteq L \cup K$.

Si $w \in K$, com $K = [K]^\Phi$, aleshores $z \in K \subseteq L \cup K$. Amb això tenim que $[L \cup K]^\Phi \subseteq L \cup K$ i per tant $L \cup K \in \Phi - \text{Sat}(\mathbf{M})$.

La primera premisa queda comprovada.

Per altra banda, per la Nota 2.36 sabem que $\bigvee(\Phi - \text{Sat}(\mathbf{M})) = M$ i $\bigwedge(\Phi - \text{Sat}(\mathbf{M})) = \emptyset$.

Queda provat que $(\Phi - \text{Sat}(\mathbf{M}), \subseteq)$ és un reticle.

Per provar que és àlgebra Booleana basta comprovar que el complementari és una operació unària interna, ja que la distributiva es compleix amb $\cup$ i $\cap$. Triem $L \in \Phi - \text{Sat}(\mathbf{M})$, volem veure que $[M - L]^\Phi \subseteq M - L$. Donat $z \in [M - L]^\Phi$, per definició existeix $w \in M - L$ tal que $(z, w) \in \Phi$. Com a més $L = [L]^\Phi$, si $z \in L$, arribaríem a la contradicció de què $w \in L$. Per tant, necessàriament $z \in M - L$ i conclou la demostració. $\square$

CAPÍTOL 3

Reconeixibilitat

En aquest capítol introduïm la noció de reconeixibilitat des dels dos punts de vista que es discuteixen a aquest treball. En primer lloc estudiarem la via dels monoides que s'ha anat preparant al llarg del capítol anterior. En segon lloc vorem la perspectiva històrica de la reconeixibilitat per autòmats finits. Donat que en últim lloc provarem l'equivalència de les nocions de reconeixibilitat, serà suficient amb conèixer la definició d'autòmat per concloure la nostra teoria de reconeixibilitat de llenguatges regulars. Haurem aconseguit els mateixos resultats que una teoria plantejada des dels autòmats però des d'una perspectiva diferent i purament algebraica.

1. Conceptes previs

Per poder desenvolupar la noció de reconeixibilitat per monoides necessitem presentar primerament les translacions, necessàries per a definir una congruència que va a caracteritzar la possibilitat de reconèixer un llenguatge.

DEFINICIÓ 3.1 (Translació elemental). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, una translació elemental de M és una aplicació de la forma*

$$\begin{array}{ccc} -m: & M & \longrightarrow M \\ & x & \longmapsto xm \end{array} \quad o \quad \begin{array}{ccc} m-: & M & \longrightarrow M \\ & x & \longmapsto mx \end{array}$$

per a algun $m \in M$. Denotarem per $\text{Etl}(M)$ a la família de translacions elementals sobre M , així

$$\text{Etl}(M) = \{-m: M \longrightarrow M \mid m \in M\} \cup \{m-: M \longrightarrow M \mid m \in M\}.$$

NOTA 3.2. *Notem que $\text{id}_M = 1- = -1$. Aleshores l'aplicació identitat és un exemple de translació elemental de M .*

DEFINICIÓ 3.3 (Translació). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, una translació de M és una composició finita de translacions elementals de M . És a dir, $t: M \longrightarrow M$ és translació de M si existeix $n \in \mathbb{N}$ tal que*

$$t = \bigcirc_{i=1}^n e_i \quad \text{on, per a cada } 1 \leq i \leq n, \ e_i \in \text{Etl}(M).$$

Denotarem per $\text{TI}(M)$ al conjunt de translacions sobre M , així

$$\text{TI}(M) = \left\{ \bigcirc_{i=1}^n e_i : M \longrightarrow M \mid n \in \mathbb{N}, \{e_i\}_{i=1}^n \subseteq \text{Etl}(M) \right\}.$$

EXEMPLE 3.4. Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $m, m', p, q \in M$, podem considerar la següent translació

$$\begin{aligned} (-m) \circ (-m') \circ (p-) \circ (q-): \quad M &\longrightarrow M \\ x &\longmapsto pqxm'm \end{aligned}$$

Les translacions ens serviran per a reconèixer quan una relació binària d'equivalència en un monoide és també una congruència. Ho vegem a la següent proposició.

PROPOSICIÓ 3.5 (Sobre la caracterització de congruències). Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $\Phi \in \text{Equiv}(M)$. Les següents afirmacions són equivalents.

- (1) Φ és congruència en $\mathbf{M}$.
- (2) Φ està tancada per a translacions elementals. És a dir, donats dos elements Φ -relacionats, per a tota translació elemental, les imatges dels elements per aquesta també estan Φ -relacionades.
- (3) Φ està tancada per a translacions. És a dir, donats dos elements Φ -relacionats, per a tota translació, les imatges dels elements per aquesta també estan Φ -relacionades.

DEMOSTRACIÓ. Vegem en primer lloc que tota congruència està tancada per translacions elementals. Agafem una translació elemental $e \in \text{Etl}(M)$, així $e \in \{-m, m-\}$ per a cert $m \in M$. Siguen dos elements $x, y \in M$ tals que $(x, y) \in \Phi$. Per la reflexivitat de Φ , $(m, m) \in \Phi$, i en ser congruència és compatible amb el producte, així:

$$e(x) = xm, e(y) = ym \quad \text{o} \quad e(x) = mx, e(y) = my.$$

De qualsevol forma $(e(x), e(y)) \in \Phi$.

Seguidament, comprovem que tancament per translacions elementals implica tancament per translacions. Emprarem que tota translació és composició de translacions elementals per a provar aquest resultat per inducció sobre el nombre de translacions elementals de les quals es compon la translació $t \in \text{TI}(M)$.

Quan $t \in \text{Etl}(M)$, només es compon d'una translació elemental, Φ està tancada per t per hipòtesi. La nostra hipòtesi inductiva és que per a tot $s \in \mathbb{N}$ tal que $1 \leq s \leq n-1$ donades qualssevol $e_1, \dots, e_{n-1} \in \text{Etl}(M)$

$$(x, y) \in \Phi \quad \text{implica} \quad \left(\bigcirc_{i=1}^{n-1} e_i(x), \bigcirc_{i=1}^{n-1} e_i(y) \right) \in \Phi$$

Si $t = \bigcirc_{i=1}^n e_i$ és composició de n translacions elementals

$$t(x) = e_n((\bigcirc_{i=1}^{n-1} e_i)(x)), \quad t(y) = e_n((\bigcirc_{i=1}^{n-1} e_i)(y)).$$

Suposant que $(x, y) \in \Phi$ tenim, emprant la hipòtesi inductiva, que $((\bigcirc_{i=1}^{n-1} e_i)(x), (\bigcirc_{i=1}^{n-1} e_i)(y)) \in \Phi$. Fent servir el cas base, com e_n és translació elemental, concloem $(t(x), t(y)) \in \Phi$.

Per acabar, suposarem que Φ està tancada per translacions. Anem a demostrar que Φ ha de ser congruència.

Suposem que tenim $x, y, z, t \in M$ i $(x, y), (z, t) \in \Phi$. Considerem les translacions $-z, y-$, per hipòtesi

$$(-z(x), -z(y)) = (xz, yz) \in \Phi \quad \text{i} \quad (y-(z), y-(t)) = (yz, yt) \in \Phi.$$

Com Φ és una relació d'equivalència, per la propietat transitiva, tenim que $(xz, yt) \in \Phi$. Això significa que $\Phi \in \text{Cong}(\mathbf{M})$. $\square$

A continuació introduïrem una congruència que està definida per a cada llenguatge L d'un monoide $\mathbf{M}$. Aquesta relacionarà els elements de L tancats per totes les translacions sobre M .

DEFINICIÓ 3.6 (Congruència sintàctica). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $L \subseteq M$, definim la congruència sintàctica de L en M com*

$$\Omega^{\mathbf{M}}(L) = \{(x, y) \in M \times M \mid \forall t \in \text{TI}(M), (t(x) \in L \leftrightarrow t(y) \in L)\}.$$

Necessitarem també conèixer la següent funció que comprova si un element pertany a un llenguatge.

DEFINICIÓ 3.7 (Funció característica). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $L \subseteq M$ un llenguatge, la funció característica de L es defineix com $\chi_L : M \rightarrow 2$ on*

$$\chi_L(m) = \begin{cases} 1 & \text{si } m \in L; \\ 0 & \text{si } m \notin L. \end{cases}$$

El seu nucli és

$$\begin{aligned} \text{Ker}(\chi_L) &= \{(x, y) \in M \times M \mid \chi_L(x) = \chi_L(y)\} \\ &= \{(x, y) \in M \times M \mid x \in L \leftrightarrow y \in L\}. \end{aligned}$$

Ara podem conèixer algunes propietats de la congruència sintàctica.

PROPOSICIÓ 3.8 (Propietats de la congruència sintàctica). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, $L \subseteq M$, la relació $\Omega^{\mathbf{M}}(L)$ verifica;*

- (1) $\Omega^{\mathbf{M}}(L)$ és congruència en $\mathbf{M}$.
- (2) $\Omega^{\mathbf{M}}(L) \subseteq \text{Ker}(\chi_L)$.

(3) Si $\Phi \in \text{Cong}(\mathbf{M})$ és tal que $\Phi \subseteq \text{Ker}(\chi_L)$, aleshores també es té que $\Phi \subseteq \Omega^{\mathbf{M}}(L)$.

DEMOSTRACIÓ. Per a la primera proposició comprovarem que Φ és congruència veient que és tancada per translacions, com hem apuntat a la Proposició 3.5. Donada una translació $t \in \text{Tl}(M)$ i dos elements $x, y \in M$ relacionats per la congruència sintàctica, per construcció sabem que $t(x) \in L$ si, i només si, $t(y) \in L$. Així, $\Omega^{\mathbf{M}}(L)$ és tancada per translacions i per tant és una congruència en $\mathbf{M}$.

Pel segon enunciat només cal considerar la translació identitat. Si-guen $(x, y) \in \Omega^{\mathbf{M}}(L)$, com $\text{id}_M \in \text{Tl}(M)$

$$\text{id}_M(x) = x \in L \text{ si, i només si, } \text{id}_M(y) = y \in L.$$

Això implica que $(x, y) \in \text{Ker}(\chi_L)$.

Per a l'última afirmació considerem $\Phi \in \text{Cong}(\mathbf{M})$ satisfent la hipòtesi. És a dir, $\Phi \subseteq \text{Ker}(\chi_L)$. Donats $x, y \in M$ tals que $(x, y) \in \Phi$, per la Proposició 3.5 podem afirmar que per a tota translació $t \in \text{Tl}(M)$, $(t(x), t(y)) \in \Phi$. Com hem suposat que Φ és refinament de $\text{Ker}(\chi_L)$, aleshores $t(x) \in L$ si, i només si, $t(y) \in L$. Com aquest argument es pot repetir per a cada translació de $\text{Tl}(M)$, aleshores $(x, y) \in \Omega^{\mathbf{M}}(L)$. $\square$

La congruència sintàctica d'un llenguatge és una congruència interessant perquè és la més gran que el satura.

COROLLARI 3.9 (Saturació per la congruència sintàctica). *Donat un monoide $\mathbf{M} = (M, \cdot, 1)$ i $L \subseteq M$, $\Omega^{\mathbf{M}}(L)$ és la major congruència en $\mathbf{M}$ que satura a L . Major en el sentit que si una altra congruència Φ en $\mathbf{M}$ satura a L , aquesta és un refinament de $\Omega^{\mathbf{M}}(L)$. És a dir, $\Phi \subseteq \Omega^{\mathbf{M}}(L)$.*

DEMOSTRACIÓ. Seguint la Proposició 1.24, volem vore que $L = [L]^{\Omega^{\mathbf{M}}(L)}$. Per definició $L \subseteq [L]^{\Omega^{\mathbf{M}}(L)}$, així només cal demostrar l'altra inclusió. Siga $z \in [L]^{\Omega^{\mathbf{M}}(L)}$, per definició existeix $b \in L$ tal que $z \in [b]_{\Omega^{\mathbf{M}}(L)}$. Com $(z, b) \in \Omega^{\mathbf{M}}(L)$, per a la translació $\text{id}_M \in \text{Tl}(M)$ tenim que $z \in L$ si, i només si, $b \in L$. Donat que $b \in L$, també $z \in L$.

Només falta vore que $\Omega^{\mathbf{M}}(L)$ és la major congruència que satura a L . Si Φ és una congruència en $\mathbf{M}$ que satura a L , donats $(x, y) \in \Phi$

$$x \in L \text{ si, i només si, } x, y \in [y]_{\Phi} \subseteq [L]^{\Phi} = L \text{ si, i només si, } y \in L.$$

De manera que $\Phi \subseteq \text{Ker}(\chi_L)$ i per la Proposició 3.5 podem afirmar que $\Phi \subseteq \Omega^{\mathbf{M}}(L)$. $\square$

2. Reconeixibilitat per monoides

Aquesta secció es dedica a l'estudi de la reconeixibilitat de llenguatges per monoides. Està estretament relacionat amb el concepte que ha sigut presentat als resultats immediatament anteriors, la saturació per la congruència sintàctica.

Arribat aquest punt, podem finalment presentar la noció de reconeixibilitat.

DEFINICIÓ 3.10 (Reconeixible). *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $L \subseteq M$. Direm que el llenguatge L és reconeixible si existeix un monoide finit $\mathbf{N} = (N, \cdot, 1)$, un subconjunt $Y \subseteq N$, i un homomorfisme de monoides $f : \mathbf{M} \rightarrow \mathbf{N}$ tal que*

$$L = f^{-1}[Y].$$

Denotarem per $\text{Rec}(\mathbf{M})$ al conjunt dels llenguatges reconeixibles en $\mathbf{M}$.

Introduïm una proposició que ens dona tres formes equivalents de la noció de reconeixibilitat.

PROPOSICIÓ 3.11. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $L \in \text{Sub}(M)$ un llenguatge, els següents enunciats són equivalents:*

- (1) *L és reconeixible.*
- (2) *L està saturat per a una congruència $\Phi \in \text{Cong}(\mathbf{M})$ d'índex finit.*
- (3) *$\Omega^{\mathbf{M}}(L)$ té índex finit.*

DEMOSTRACIÓ. Suposem (1), és a dir, que L és reconeixible. D'acord a la Definició 3.10, existeix un monoide finit $\mathbf{N} = (N, \cdot, 1)$, un subconjunt $Y \subseteq N$ i un homomorfisme de monoides $f : \mathbf{M} \rightarrow \mathbf{N}$ de forma que $L = f^{-1}[Y]$. Considerem el nucli de l'homomorfisme f , és a dir, $\text{Ker}(f)$. Pel que hem vist a la Proposició 2.24, $\text{Ker}(f)$ és una congruència en $\mathbf{M}$. A més, pel Primer Teorema d'Isomorfisme de monoides, Teorema 2.25, $\mathbf{M}/\text{Ker}(f) \cong \mathbf{Im}(f)$. Recordem per la Proposició 2.24 que $\mathbf{Im}(f)$ és un submonoide de $\mathbf{N}$. Com que $\mathbf{N}$ és finit, trobem que $\mathbf{Im}(f)$ és un submonoide finit. Com existeix una bijecció entre $\mathbf{Im}(f)$ i $\mathbf{M}/\text{Ker}(f)$, aquest segon ha de ser finit i, en definitiva, $\text{Ker}(f)$ és congruència d'índex finit en M .

Anem a demostrar que L està saturat per a $\text{Ker}(f)$, és a dir, anem a demostrar que

$$L = [L]^{\text{Ker}(f)}.$$

D'acord a la Proposició 1.24, de l'anterior igualtat només cal comprovar l'inclusió de dreta a esquerra. Siga z un element en $[L]^{\text{Ker}(f)}$, aleshores existirà un $w \in L$ de forma que $(z, w) \in \text{Ker}(f)$. Per la definició

de nucli, trobem que $f(z) = f(w)$. En particular, com que $w \in L$ i $L = f^{-1}[Y]$, trobem que $f(w) \in Y$. Aleshores també tenim que $f(z) \in Y$. Per tant, $z \in f^{-1}[Y] = L$.

Queda així demostrat (2).

Suposem ara (2), és a dir, que L està saturat per una congruència d'índex finit Φ en $\mathbf{M}$. Volem demostrar que $\Omega^{\mathbf{M}}(L)$ té índex finit. Notem que, pel Corol·lari 3.9, com que L està saturat per Φ , aleshores $\Phi \subseteq \Omega^{\mathbf{M}}(L)$. Com que Φ té índex finit, per la Proposició 2.28 podem afirmar que $\Omega^{\mathbf{M}}(L)$ també té índex finit.

Queda així demostrat (3).

Finalment suposem (3), és a dir, suposem que la congruència sintàctica de L en $\mathbf{M}$, és a dir, $\Omega^{\mathbf{M}}(L)$, té índex finit. Volem provar que L és reconeixible.

En aquest cas considerem el monoide quocient $\mathbf{M}/\Omega^{\mathbf{M}}(L)$. Aquest monoide és finit perquè $\Omega^{\mathbf{M}}(L)$ té índex finit. Considerem l'aplicació projecció, que per la Proposició 2.18 és homomorfisme de monoides

$$\text{pr}_{\Omega^{\mathbf{M}}(L)}: \mathbf{M} \longrightarrow \mathbf{M}/\Omega^{\mathbf{M}}(L)$$

i el subconjunt $Y = \text{pr}_{\Omega^{\mathbf{M}}(L)}[L]$. Anem a demostrar que

$$L = \text{pr}_{\Omega^{\mathbf{M}}(L)}^{-1}[Y].$$

Comprovem les dues inclusions.

Per a l'inclusió d'esquerra a dreta, siga $w \in L$, aleshores $\text{pr}_{\Omega^{\mathbf{M}}(L)}(w)$ és un element en Y . Per tant, w pertany a $\text{pr}_{\Omega^{\mathbf{M}}(L)}^{-1}[Y]$.

Ara, per a l'inclusió de dreta a esquerra, siga $z \in \text{pr}_{\Omega^{\mathbf{M}}(L)}^{-1}[Y]$. Aleshores $\text{pr}_{\Omega^{\mathbf{M}}(L)}(z)$ pertany a Y . Així, existeix un $w \in L$ de forma que $\text{pr}_{\Omega^{\mathbf{M}}(L)}(z) = \text{pr}_{\Omega^{\mathbf{M}}(L)}(w)$. Açò és equivalent a dir que $(z, w) \in \Omega^{\mathbf{M}}(L)$. Recordem que, d'acord al Corol·lari 3.9, L sempre està saturat per la congruència sintàctica $\Omega^{\mathbf{M}}(L)$. Així, com que $(z, w) \in \Omega^{\mathbf{M}}(L)$ i $w \in L$, concloem que $z \in L$.

Queda així demostrat (1). □

Continuem estudiant l'espai dels llenguatges reconeixibles en un monoide amb la relació d'ordre donada per la inclusió. És a dir, l'ordre parcial $\mathbf{Rec}(\mathbf{M}) = (\text{Rec}(\mathbf{M}), \subseteq)$. Comencem provant que és un conjunt no buit.

PROPOSICIÓ 3.12. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, aleshores tant M com $\emptyset$ són llenguatges reconeixibles. És a dir, $\{M, \emptyset\} \subseteq \text{Rec}(\mathbf{M})$.*

DEMOSTRACIÓ. Considerem el monoide trivial $\mathbf{1} = (1, \cdot, 0)$. Vegem que l'aplicació

$$\begin{aligned} K_0: \mathbf{M} &\longrightarrow \mathbf{1} \\ m &\longmapsto 0 \end{aligned}$$

és un homomorfisme de monoides. En efecte $K_0(1) = 0$, així que envia el neutre de $\mathbf{M}$ al neutre de $\mathbf{1}$. També notem que per $m_1, m_2 \in M$, com $K_0(m_1) = K_0(m_2) = K_0(m_1 m_2) = 0$, aleshores $K_0(m_1 m_2) = K_0(m_1) K_0(m_2) = 0$ i així sabem que K_0 és compatible amb el producte en $\mathbf{1}$.

Finalment, tenim que

$$(K_0)^{-1}[\emptyset] = \emptyset \qquad (K_0)^{-1}[1] = M.$$

Això prova que $\emptyset, M \in \text{Rec}(\mathbf{M})$. □

Ara que sabem que hi ha llenguatges reconeixibles, comprovem quines operacions són tancades en $\text{Rec}(\mathbf{M})$.

PROPOSICIÓ 3.13 (Aritmètica de la reconeixibilitat). *Siguen $\mathbf{M} = (M, \cdot, 1)$ un monoide i $L, K \in \text{Sub}(M)$ llenguatges reconeixibles, aleshores: (1) $L \cap K$, (2) $L \cup K$ i (3) $M - L$ són llenguatges reconeixibles.*

DEMOSTRACIÓ. Vegem 1. Per hipòtesi $\Omega^{\mathbf{M}}(L), \Omega^{\mathbf{M}}(K)$ tenen índex finit i pel Corol·lari 2.29, $\Phi = \Omega^{\mathbf{M}}(L) \cap \Omega^{\mathbf{M}}(K)$ també ho té. Vegem que satura a $L \cap K$. Per defecte tenim que $L \cap K \subseteq [L \cap K]^{\Phi}$ així que hem de provar $[L \cap K]^{\Phi} \subseteq L \cap K$. Prenem $z \in [L \cap K]^{\Phi}$ i per definició existeix $w \in L \cap K$ tal que $(z, w) \in \Phi$. Com $\Omega^{\mathbf{M}}(L) \subseteq \text{Ker}(\chi_L)$ i $\Omega^{\mathbf{M}}(K) \subseteq \text{Ker}(\chi_K)$ per la Proposició 3.8, es dona que $z \in L$ si, i només si, $w \in L$ al mateix temps que $z \in K$ si, i només si, $w \in K$. O el que és el mateix $z \in L \cap K$ si, i només si, $w \in L \cap K$. Partíem de $w \in L \cap K$, així que $z \in L \cap K$ i concloem que $[L \cap K]^{\Phi} \subseteq L \cap K$.

Vegem 2. Anem a comprovar que Φ també satura a $L \cup K$. Com hem observat a altres ocasions, basta provar que $[L \cup K]^{\Phi} \subseteq L \cup K$. Agafem $z \in [L \cup K]^{\Phi}$, pel qual existeix un $w \in L \cup K$ tal que $(z, w) \in \Phi$. Anàlogament a la prova anterior, $z \in L$ si, i només si, $w \in L$ i $z \in K$ si, i només si, $w \in K$. De forma que $z \in L \cup K$ si, i només si, $w \in L \cup K$. Com $w \in L \cup K$, z també pertany a aquest conjunt.

Vegem 3. Utilitzem la mateixa propietat per mostrar que $M - L$ és reconeixible: la saturació mitjançant una congruència d'índex finit. En aquest cas la congruència és $\Omega^{\mathbf{M}}(L)$, d'índex finit en ser L reconeixible. Siga $z \in [M - L]^{\Omega^{\mathbf{M}}(L)}$, existeix $w \in (M - L)$ tal que $(z, w) \in \Omega^{\mathbf{M}}(L)$. Raonant com els dos altres punts, tenim que $z \in L$ si, i només si, $w \in L$. Arribant a què $z \in (M - L)$ i provant $[M - L]^{\Omega^{\mathbf{M}}(L)} = M - L$. □

El que acabem d'observar ens permet arribar a la conclusió que $\text{Rec}(\mathbf{M})$ admet estructura d'àlgebra Booleana.

COROLLARI 3.14. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide, aleshores*

$$\mathbf{Rec}(\mathbf{M}) = (\text{Rec}(\mathbf{M}), \vee, \wedge, \neg, \emptyset, M),$$

on $\neg L$ és el complementari en M de $L \in \text{Sub}(M)$, és un àlgebra Booleana.

DEMOSTRACIÓ. Primer notem que, donat $L \in \text{Sub}(M)$, $\neg L$ va a denotar a $M - L$. Ja sabem que $(\text{Rec}(\mathbf{M}), \subseteq)$ és un reticle, doncs per la Proposició 3.13 podem afirmar que, per tots $L, K \in \text{Rec}(\mathbf{M})$, tant $L \vee K = L \cup K$ com $L \wedge K = L \cap K$ pertanyen a $\text{Rec}(\mathbf{M})$. Com $\emptyset, M$ són reconeixibles per la Proposició 3.12, necessàriament són els extrems i així $\max(\text{Rec}(\mathbf{M})) = M$, $\min(\text{Rec}(\mathbf{M})) = \emptyset$.

L'existència d'un complementari per a cada $L \in \text{Rec}(\mathbf{M})$ ve donada per la Proposició 3.13, que prova que $\neg L = M - L \in \text{Rec}(\mathbf{M})$. La distributiva respecte a $\vee, \wedge$ no cal provar-la perquè sabem que $\cup, \cap$ són mútuament distributives i $\vee = \cup, \wedge = \cap$.

Queda provat que $\mathbf{Rec}(\mathbf{M})$ és un àlgebra Booleana. $\square$

Acabem aquest capítol mostrant als dos últims resultats altres operacions per les quals la reconeixibilitat és tancada, que són la preimatge per una translació i la preimatge per un homomorfisme de monoides.

PROPOSICIÓ 3.15. *Siga $\mathbf{M} = (M, \cdot, 1)$ un monoide i $L \in \text{Sub}(M)$ un llenguatge reconeixible. Siga $t \in \text{Ti}(M)$ una translació, aleshores $t^{-1}[L]$ és un llenguatge reconeixible.*

DEMOSTRACIÓ. Suposem que $L \in \text{Rec}(\mathbf{M})$. Per la Proposició 3.11 podem afirmar que $\Omega^{\mathbf{M}}(L)$ és una congruència en $\mathbf{M}$ d'índex finit. L'objectiu és comprovar que $\Omega^{\mathbf{M}}(L)$ satura a $t^{-1}[L]$, equivalentment

$$[t^{-1}[L]]^{\Omega^{\mathbf{M}}(L)} = t^{-1}[L].$$

Com hem fet a moltes altres demostracions, l'única inclusió que hem de comprovar és la d'esquerra a dreta. Doncs, agafem $z \in [t^{-1}[L]]^{\Omega^{\mathbf{M}}(L)}$. Per definició, existeix $w \in t^{-1}[L]$ tal que $(z, w) \in \Omega^{\mathbf{M}}(L)$. Com $\Omega^{\mathbf{M}}(L)$ està tancada per a translacions, d'acord a la Proposició 3.5, i $t \in \text{Ti}(M)$, tenim que $(t(z), t(w)) \in \Omega^{\mathbf{M}}(L)$.

Donat que $w \in t^{-1}[L]$, afirmem que $t(w) \in L$. Ja que $L \in \Omega^{\mathbf{M}}(L) - \text{Sat}(\mathbf{M})$, emprant el Corollari 3.9, $t(w) \in L$ i també $(t(z), t(w)) \in \Omega^{\mathbf{M}}(L)$, podem concloure que $t(z) \in L$. És a dir, hem obtingut que $z \in t^{-1}[L]$ i així $[t^{-1}[L]]^{\Omega^{\mathbf{M}}(L)} \subseteq t^{-1}[L]$. Queda demostrat que $t^{-1}[L]$ és reconeixible emprant la Proposició 3.11. $\square$

PROPOSICIÓ 3.16. *Siguen $\mathbf{M}$ i $\mathbf{N}$ monoides i $f: \mathbf{M} \rightarrow \mathbf{N}$ un homomorfisme de monoides. Donat $K \in \text{Sub}(\mathbf{N})$ reconeixible, aleshores $f^{-1}[K] \in \text{Sub}(\mathbf{M})$ és reconeixible.*

DEMOSTRACIÓ. Seguint la definició de reconeixibilitat, com K és reconeixible, existeix un monoide $\mathbf{P}$ finit, un homomorfisme de monoides $g: \mathbf{N} \rightarrow \mathbf{P}$ i un subconjunt $S \subseteq P$ de forma que $K = g^{-1}[S]$.

Si posem l'anterior homomorfisme de monoides amb f obtenim un homomorfisme de monoides $g \circ f: \mathbf{M} \rightarrow \mathbf{P}$. El nostre objectiu és provar que $(g \circ f)^{-1}[S] = f^{-1}[K]$ i així, $f^{-1}[K]$ és reconeixible per definició.

Vegem la inclusió d'esquerra a dreta agafant $z \in (g \circ f)^{-1}[S]$. Així $g(f(z)) \in S$ i també $f(z) \in g^{-1}[S] = K$. És a dir, $z \in f^{-1}[K]$.

Vegem la inclusió de dreta a esquerra agafant $z \in f^{-1}[K]$. Així $f(z) \in K = g^{-1}[S]$ i també $g(f(z)) \in S$. És a dir, $z \in (g \circ f)^{-1}[S]$. $\square$

3. Reconeixibilitat per autòmats

En aquest capítol introduïm breument la perspectiva tradicional de l'estudi dels llenguatges regulars fent ús d'autòmats finits. El nostre interès és presentar la forma convencional, per entendre així l'esforç que suposa a nivell conceptual. Per finalitzar, provarem l'equivalència que existeix entre la noció de reconeixibilitat per autòmats i la que hem treballat fins aquest moment del treball, per monoides.

Presentem inicialment el concepte d'autòmat finit sobre un alfabet.

DEFINICIÓ 3.17 (Autòmat finit). *Un autòmat per a l'alfabet A és una tupla $\mathcal{A} = (Q, q_0, \delta, F)$ on*

- Q és un conjunt finit d'estats.
- $q_0 \in Q$ és l'estat inicial.
- $F \subseteq Q$ és el conjunt d'estats finals.
- δ és una funció de transició de la forma $\delta: Q \times A \rightarrow Q$.

Plantegem un exemple d'un autòmat que ens va a ajudar a entendre aquesta perspectiva de la reconeixibilitat.

EXEMPLE 3.18. *Vegem un autòmat finit per a l'alfabet $A = \{a, b\}$. Tindrem $\mathcal{A} = (Q, q_0, \delta, F)$ on $Q = \{q_0, q_1, q_2, q_3\}$, $F = \{q_2\}$ i representem δ , com sol ser habitual, amb la taula de transicions següent. La interpretem com, per a cada estat de la primera columna, q , en passar la imatge per δ amb el símbol x d'una altra columna, arribem a l'estat $\hat{q}$. D'una altra forma $\delta(q, x) = \hat{q}$.*

Per a poder enunciar la reconeixibilitat per autòmats necessitem els dos resultats següents.

Q	a	b
q_0	q_1	q_3
q_1	q_1	q_2
q_2	q_1	q_2
q_3	q_3	q_3

TAULA 1. Taula de transicions.

PROPOSICIÓ 3.19 (Monoide d'endomorfismes). *Siga Q un conjunt, les aplicacions de Q en Q admeten estructura de monoide amb la composició d'aplicacions i la identitat com a neutre. És a dir,*

$$\mathbf{End}(Q) = (\text{End}(Q), \circ, \text{id}_Q)$$

és un monoide.

DEMOSTRACIÓ. Per definició $\circ$ és una operació binària associativa en $\text{End}(Q)$ ja que, per a tots $f, g, h \in \text{End}(Q)$ $(f \circ g) \circ h = f \circ (g \circ h)$. A més a més, id_Q funciona com element neutre per a aquesta operació donat que per a tot $f \in \text{End}(Q)$, $f \circ \text{id}_Q = \text{id}_Q \circ f = f$. Emprant la Definició 2.1, afirmem que $\mathbf{End}(Q)$ és un monoide. $\square$

PROPOSICIÓ 3.20. *Siga A l'alfabet de l'autòmat $\mathcal{A} = (Q, q_0, \delta, F)$, aleshores existeix un homomorfisme de monoides*

$$\delta^\# : \mathbf{A}^* \longrightarrow \mathbf{End}(Q)$$

tal que $\text{Ker}(\delta^\#)$ és una congruència en $\mathbf{A}^$ d'índex finit.*

DEMOSTRACIÓ. Podem considerar

$$\begin{aligned} \delta : A &\longrightarrow \text{End}(Q) \\ w &\longmapsto \delta(\cdot, w) : Q \longrightarrow Q \\ q &\longmapsto \delta(q, w) \end{aligned}$$

Atenent-nos al Corol·lari 2.27, com δ és una aplicació d'un conjunt A a un monoide finit, $\mathbf{End}(Q)$ podem estendre-la utilitzant la Proposició 2.11 de la Propietat Universal. D'aquesta forma podem definir

$$\begin{aligned} \delta^\# : \quad A^* &\longrightarrow \text{End}(Q) \\ (w_i)_{i \in n} &\longmapsto \delta(w_0) \cdot \dots \cdot \delta(w_{n-1}) \end{aligned}$$

Pel Primer Teorema d'Isomorfisme de monoides, Teorema 2.25, sabem que $A^*/\text{Ker}(\delta^\#) \cong \mathbf{Im}(\delta^\#)$. Com hem vist al llarg d'aquest treball, sabem que $\mathbf{Im}(\delta^\#)$ és un monoide finit ja que és submonoide de $\mathbf{End}(Q)$ que és finit també. Amb això podem concloure que $\text{Ker}(\delta^\#)$ és una congruència d'índex finit en $\mathbf{A}^*$. $\square$

Ha arribat el moment de presentar la reconeixibilitat per autòmats.

DEFINICIÓ 3.21 (Reconeixibilitat per autòmat). *Donat un autòmat $\mathcal{A} = (Q, q_0, \delta, F)$ per a l'alfabet A i $w \in A^*$, direm que $\mathcal{A}$ reconeix w si $\delta^\#(q_0, w) \in F$. D'aquesta forma podem descriure el llenguatge reconegut per l'autòmat $\mathcal{A}$ com*

$$\mathcal{L}(\mathcal{A}) = \{w \in A^* \mid \delta^\#(q_0, w) \in F\},$$

és a dir, el conjunt de totes les paraules que, en aplicar-se sobre l'estat inicial, retornen un estat final. D'aquesta forma, siga $L \in \text{Sub}(A^)$ un llenguatge, direm que L és reconeixible per autòmats si existeix un autòmat finit $\mathcal{A} = (Q, q_0, \delta, F)$ sobre A per al qual $L = \mathcal{L}(\mathcal{A})$.*

Continuem amb l'exemple que havíem proposat per a desenvolupar un cas pràctic de reconeixibilitat per autòmats.

EXEMPLE 3.22. *L'autòmat vist a l'Exemple 3.18 determinat per la Taula 1 serveix per a reconèixer el llenguatge de les paraules sobre $A = \{a, b\}$ que comencen per a i acaben per b . L'objecte autòmat té l'avantatge de poder ser representat gràficament. Normalment els estats són nodes i les transicions es representen amb arestes, l'estat inicial té una fletxa sense origen, l'estat final un doble cercle. Seguint eixos estàndards, aquest autòmat té la forma de la Figura 1.*

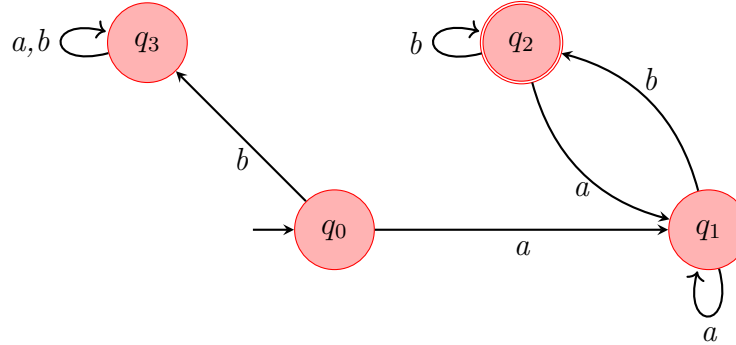


FIGURA 1. Autòmat que reconeix llenguatges de paraules que comencen en a i acaben en b .

Com podem comprovar, per poder arribar a l'estat d'acceptació q_2 des de q_0 és necessari que la cadena introduïda comence per a , passant així a q_1 . Un pic aquí, a partir de la primera b la paraula podria ser acceptada. En cas que la cadena tinga més símbols, notem que cada cop que apareix una a a la cadena, ha d'haver-hi una b que la segueixca per tal d'acabar a q_2 .

L'últim, i més important, resultat del present treball és el resultat que el motiva, l'equivalència entre les dues nocions de reconeixibilitat estudiades.

TEOREMA 3.23 (Equivalència de reconeixibilitat). *Siga A un conjunt i $L \in \text{Sub}(A^*)$, aleshores L és reconeixible per monoides si, i només si, és reconeixible per autòmats.*

DEMOSTRACIÓ. Suposem que L és reconeixible per monoides. Per definició existeix un monoide finit $\mathbf{M} = (M, \cdot, 1)$, un homomorfisme de monoides $f: A^* \rightarrow M$ i $C \in \text{Sub}(M)$ tal que $f^{-1}[C] = L$. Construïm un autòmat $\mathcal{A} = (M, 1, \delta, C)$ on

$$\begin{aligned} \delta: \quad M \times A &\longrightarrow M \\ (m, a) &\longmapsto mf(a) \end{aligned}$$

Com hem fet a la Proposició 3.20, δ pot vore's com una aplicació d' A en $\text{End}(M)$. Aplicant la Propietat Universal del monoide lliure, Proposició 2.11, podem estendre δ a un homomorfisme de monoides $\delta^\#: \mathbf{A}^* \rightarrow \mathbf{End}(M)$ que pot vore's com una aplicació de la forma

$$\begin{aligned} \delta^\#: \quad M \times A^* &\longrightarrow M \\ (m, (w_i)_{i \in n}) &\longmapsto mf(w_0) \cdot \dots \cdot f(w_{n-1}). \end{aligned}$$

Vegem que $L = \mathcal{L}(\mathcal{A})$ provant la doble inclusió. Agafem $w \in L$, per tant $f(w) \in C$, i trobem que en ser 1 l'element neutre de $\mathbf{M}$

$$f(w) = 1 \cdot f(w) = \delta^\#(1, w) \in C.$$

Llavors, $w \in \mathcal{L}(\mathcal{A})$.

De l'altra banda només cal pegar-li la volta al resultat anterior. Donat $w \in \mathcal{L}(\mathcal{A})$, per definició $\delta^\#(1, w) \in C$ però

$$\delta^\#(1, w) = f(w) \in C,$$

la qual cosa implica que $w \in f^{-1}[C] = L$. Queda provada la implicació d'esquerra a dreta.

Suposem ara que L és reconeixible per un autòmat $\mathcal{A} = (Q, q_0, \delta, F)$. Considerem $\delta^\#$ de la Proposició 3.20 i sabem que $\text{Ker}(\delta^\#)$ és una congruència d'índex finit en $\mathbf{A}^*$. Fent servir la Proposició 3.11, podem justificar la reconeixibilitat de L provant que està saturat per $\text{Ker}(\delta^\#)$. Com hem realitzat ja a demostracions anteriors, és suficient que verifiquem $[L]^{\text{Ker}(\delta^\#)} \subseteq L$. Donat $z \in [L]^{\text{Ker}(\delta^\#)}$ existeix $w \in L$ tal que $(z, w) \in \text{Ker}(\delta^\#)$. Això vol dir que $\delta^\#(w) = \delta^\#(z)$, és a dir, que tenen la mateixa imatge per $\delta^\#$. En particular,

$$\delta^\#(w)(q_0) = \delta^\#(z)(q_0).$$

Tenim que $w \in L = \mathcal{L}(\mathcal{A})$, aleshores $\delta^\#(w)(q_0) \in F$. Podem concloure que $z \in L$.

Queda provada l'altra implicació. $\square$

Acabem aquest treball vegen un exemple de llenguatge reconeixible per a un alfabet A que conté la lletra a . En primer lloc recuperem un homomorfisme de monoides per tal de comprovar la reconeixibilitat per monoides i finalment vorem l'autòmat que el reconeix.

EXEMPLE 3.24. *Siga A un conjunt qualsevol de símbols i $a \in A$, considerem el monoide $\mathbf{A}^* = (A^*, \cdot, \lambda)$. Volem comprovar que el llenguatge format per les cadenes d' A^* que tenen un nombre parell d' a , que denotem per L , és reconeixible.*

Per la primera part considerem el grup $(\mathbb{Z}_2, +, 0)$ on la suma és mòdul 2. A partir de l'aplicació $f: A \rightarrow \mathbb{Z}_2$ que assigna $f(a) = \bar{1}$ i $f(b) = \bar{0}$ per tot $b \in A - \{a\}$, per la Propietat Universal del monoide lliure, sabem que podem estendre f a

$$\begin{aligned} f^\#: \mathbf{A}^* &\longrightarrow \mathbb{Z}_2 \\ w &\longmapsto |w|_a \bmod 2. \end{aligned}$$

Com $\mathbb{Z}_2$ és un grup finit i $L = f^{-1}[\{\bar{0}\}]$, hem provat la reconeixibilitat per monoides.

Per la segona part considerem l'autòmat $\mathcal{A} = (\{q_0, q_1\}, q_0, \delta, q_0)$ a on $\delta(q_i, b) = q_i$ per a $i \in \{0, 1\}$, per a tot $b \in A - \{a\}$ i $\delta(q_0, a) = q_1$, $\delta(q_1, a) = q_0$. Aquest autòmat té la representació següent, per a tot $b \in A - \{a\}$

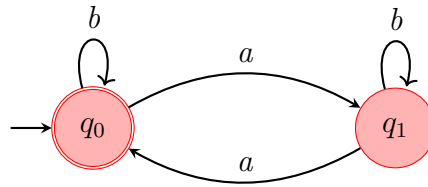


FIGURA 2. Autòmat que reconeix el llenguatge de totes les paraules amb un nombre parell de lletres a .

És fàcil veure que $\mathcal{A}$ reconeix L ja que l'estat de l'autòmata canviarà entre q_0 i q_1 només quan aparegui una a a la cadena a reconèixer. Com partim de q_0 i aquest és l'estat d'acceptació, la cadena és acceptada si el nombre d' a llegides és parell.

L'objectiu d'aquest treball era proposar una alternativa a la perspectiva dels autòmats per a la reconeixibilitat de llenguatges regulars

passant per estructures de monoides. Hem pogut desenvolupar la teoria de monoides i conèixer estructures d'ordre entre els llenguatges gràcies a l'utilització d'elements algebraics. Plantejades les dues vies per a la reconeixibilitat i provada la seua equivalència, observem que entre aquestes resideixen diferències en com s'ha de descriure els llenguatges reconeixibles. L'algebrista permet donar una demostració clara en terminologia i completa de quan un llenguatge és reconeixible mentre que la dels autòmats pot resultar més intuïtiva de plantejar perquè els autòmats són visuals i es poden construir algorísmicament. Al cap i a la fi, ambdues nocions fan referència a la mateixa cosa i el valor que trobem a aquesta pluralitat és comptar amb eines que ens amplien les opcions i recursos per treballar amb el reconeiximent de llenguatges regulars.

Bibliografia

- Climent Vidal, Juan i Cosme Llópez, Enric (2020). “Congruence-based proofs of the recognizability theorems for free many-sorted algebras”. A: *Journal of Logic and Computation* 30.2, pàg. 561-633.
- Navarro Arroyo, Vicent (2022). “Lògica categorial”. Universitat de València. URL: <https://www.uv.es/coslloen/Arxiu/Fitxers/TFG/2022Navarro.pdf>.
- Pin, Jean-Éric (2010). “Mathematical foundations of automata theory”. A: *Lecture notes LIAFA, Université Paris*.
- Pitarch Pérez, Pasqual (2019). “Caracterització de les congruències d’índex finit en el monoide lliure d’un generador”. Universitat de València. URL: <https://www.uv.es/coslloen/Arxiu/Fitxers/TFG/2019Pitarch.pdf>.
- Sakarovitch, Jacques (2015). *Automata and rational expressions*. arXiv: 1502.03573 [cs.FL].