



Treball Fi de Grau - Curs 2018/2019

Caracterització de les congruències d'índex finit en el monoide lliure d'un generador

Autor: Pascual Pitarch Pérez

Tutor: ENRIC COSME LLÓPEZ

Índex

1	Introducció.	2
2	Preliminars	4
2.1	Conjunts parcialment ordenats	4
2.2	Monoide	6
2.3	Submonoide	7
2.4	Monoide quocient i congruències	8
2.5	Teorema d'isomorfia	13
2.6	Monoide lliure	15
3	Autòmates	18
3.1	Models d'autòmates.	18
3.2	Propietats de clausura.	24
4	Congruències d'índex finit sobre $\mathbb{N}$	30
4.1	Introducció i exemples	30
4.2	Caracterització de les congruències d'índex finit en $\mathbb{N}$	32
4.3	Operacions en congruències d'índex finit	35
4.4	Aplicacions	38
5	Conclusió	39

Capítol 1

Introducció.

L'objectiu d'aquest treball és entendre les ferramentes que s'utilitzen per a caracteritzar llenguatges reconeixibles. Aquestes ferramentes són la teoria d'autòmats finits i les congruències d'índex finit desenvolupades per Myhill [Myh57] i Nerode [Ner58]. Treballarem des dels dos punts de vista per fer entendre i deixar ben clar quines són les limitacions de cada eina i quins són els avantatges en cada cas.

Aquest treball es troba dins del camp de les estructures algebraïques i de la teoria de la computació i llenguatges formals. Així començarem parlant primer un poc sobre la base algebraica amb algunes definicions de conjunts d'ordre, l'estructura algebraica del monoide, homomorfismes entre monoides, congruències, conjunts quocients, teorema d'isomorfia i el cas particular del monoide lliure. Vorem també que tant el conjunt de submonoides com el de congruències amb les seues respectives operacions i l'ordre habitual d'inclusió, tenen estructures de reticle i que les congruències d'índex finit són un filtre del reticle de totes les congruències. Per a tot aquests resultats hem necessitat l'ajuda de coneixements que hem anat adquirint al llarg del grau en les diferents assignatures d'àlgebra i de llibres com [BS81].

En el capítol següent pasem a parlar sobre autòmats, enllaçant un poc amb el monoide lliure, i la propietat de reconeixibilitat dels llenguatges formals. Tots aquests conceptes han sigut totalment nous i s'han hagut de treballar amb lectures de llibres i articles com [Pin12] i [BLR15], i l'ajuda del tutor Enric Cosme. En la primera meitat del segle XX era el moment en el que els grans matemàtics de tot el món com ara Hilbert, tractaven de trobar un únic sistema axiomàtic de manera que les matemàtiques pogueren reduir-se a un sistema computacional en el qual es podria deduir la veracitat o falsetat de qualsevol enunciat matemàtic. Però, en 1931, l'austriac Kurt Gödel va publicar el "Teorema de incompletitud" en el qual demostrava que hi havia resultats que no es podia provar ni la seua veracitat ni la seua falsetat. Més tard, en 1937, el matemàtic Alan Turing, va presentar la seua màquina de Turing, que és el tipus d'autòmata més complex que existeix i amb més poder computacional, i va demostrar que molts problemes perfectament definits i enunciats no és podien resoldre mitjançant eixa màquina. La teoria dels autòmats sorgix a meitat del segle XX arran d'aquests fets per determinar quins llenguatges podrien ser reconeguts per aquest autòmats. Aquesta teoria parteix amb el teorema de Kleene,

que mostra que la classe de llenguatges reconeixibles (és a dir, reconeguts per autòmats finits), coincideix amb la classe de llenguatges racionals, que són donats per expressions racionals. Es va observar ràpidament que aquestes definicions bàsicament combinatòries es podien interpretar de manera molt rica en termes algebraics i lògics. Gràcies a aquesta teoria comencen a desenvolupar-se els primers computadors. En aquest capítol el que vorem serà un dels autòmats més simples, l'autòmata finit i ens trobem amb un dels resultats més importants del treball, si no el que més, que és el teorema de Myhill-Nerode [Myh57][Ner58] que ens relaciona i posa al mateix nivell el que hem vist fins el moment, la saturació d'un llenguatge respecte congruències d'índex finit i la reconeixibilitat d'un llenguatge. Després també vorem algunes propietats de clausura entre llenguatges reconeixibles i sempre fent les demostracions des de dos punts de vista, primer per autòmats finits, demostracions les quals hem tret les idees de [Pin12] i després amb les congruències d'índex finit, demostracions les quals hem tret les idees de l'article [CC18].

A continuació passem ja a caracteritzar les congruències d'índex finit sobre el cas particular del monoide de nombres naturals, el qual vorem que és isomorf al monoide lliure d'un generador i ens servirà per, juntament amb el teorema de Myhill-Nerode [Myh57][Ner58], determinar si un subconjunt dels nombres naturals donat, pot ser reconegut per un autòmata finit o no. Vorem, per acabar, que l'exemple dels nombres primers és un llenguatge no reconeixible.

També cal aclarir en aquesta introducció un parell de qüestions de notació. En algunes ocasions, donat un $n \in \mathbb{N}$, si tenim expressions del tipus $j \in n$ en aquest cas entenem n com el conjunt de naturals menors estrictes que eixe n , és a dir, $n = \{0, \dots, n-1\}$. Si tenim una aplicació f entre dos conjunts A i B , aleshores l'aplicació $f[\cdot]$ és una aplicació que va de subconjunts de A en subconjunts de B , és a dir, donat $X \subseteq A$, aleshores $f[X] = \{y \in B \mid \exists x \in X (y = f(x))\}$.

Capítol 2

Preliminars

En aquest capítol tractarem d'entendre nocions algebraiques bàsiques i continguts que es considera que són importants a l'hora d'entendre el que vindrà més tard per a que siga d'alló més autocontingut possible.

Començem amb definicions bàsiques de teoria d'ordre amb exemples per comprendre millor les definicions. Després presentarem l'estructura de monoide amb la subestructura de monoide i destaquem que el conjunt de submonoides amb les operacions que vorem més endavant i l'ordre habitual d'inclusió formen un reticle. A continuació vorem les congruències que podem fer sobre els monoides i com formem el conjunt quocient. Destaquem en aquesta part també que el conjunt de totes les congruències que es poden fer sobre un monoide formen un reticle i que les congruències d'índex finit formen un filtre d'aquest reticle. Continuarem amb el teorema d'isomorfia amb un exemple de monoides isomorfs. Per finalitzar, presentem un cas particular de monoide, el monoide lliure format sobre un alfabet, demostrem la propietat universal del monoide lliure i destaquem en un exemple que el monoide lliure sobre un alfabet amb només una lletra és isomorf als nombres naturals.

2.1 Conjunts parcialment ordenats

Definició 2.1. Siga $\leq$ una relació binària definida en un conjunt P . Direm que $\leq$ és un *ordre parcial* si donats $a, b, c \in P$ qualsevol es compleixen les següents propietats:

1. $a \leq a$ (reflexivitat);
2. Si $a \leq b$ i $b \leq a$, aleshores $a = b$ (antisimetria);
3. Si $a \leq b$ i $b \leq c$, aleshores $a \leq c$ (transitivitat).

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

Exemple 2.2.

1. El conjunt de nombres naturals amb l'ordre habitual, $(\mathbb{N}, \leq)$ és un conjunt parcialment ordenat.
2. En el conjunt de nombres naturals podem definir una relació binària, la divisió. Donats $x, y \in \mathbb{N}$, direm que x divideix a y , i denotem $x \mid y$, si existeix un enter k de manera que $y = kx$. Aleshores, el conjunt dels nombres naturals amb la divisió, $(\mathbb{N}, \mid)$ és un conjunt parcialment ordenat.

Definició 2.3. Si tenim un conjunt parcialment ordenat $(P, \leq)$ i prenem un subconjunt qualsevol X de P , definim *fita superior* de X en P als elements $p \in P$ de manera que $x \leq p$ per a tot $x \in X$, i definim *fita inferior* de X en P als elements $p \in P$ de manera que $p \leq x$ per a tot $x \in X$.

Definició 2.4. Si tenim un conjunt parcialment ordenat $(P, \leq)$ i prenem un subconjunt qualsevol X de P , definim *suprem* de X en P , i escrivim $\sup(X)$, a la menor de les fites superiors de X i definim *ínfim* de X en P , i escrivim $\inf(X)$, a la major de les fites inferiors de X .

Definició 2.5. Direm que un conjunt parcialment ordenat $(P, \leq)$ és un *reticle complet* si per a qualsevol subconjunt X de P existeix $\sup(X)$ i $\inf(X)$ i estan en P . Els elements $\sup(X)$ i $\inf(X)$ els denotem per $\bigvee X$ i $\bigwedge X$ respectivament.

Definició 2.6. Si tenim un conjunt parcialment ordenat $(P, \leq)$, aleshores si prenem un subconjunt qualsevol X de P , definim *mínim* de X i denotem $\min(X)$ al element $p \in X$ de manera que $p \leq x$ per a tot $x \in X$, i definim també *màxim* de X i denotem $\max(X)$ al element $p \in X$ de manera que $p \leq x$ per a tot $x \in X$.

Nota 2.7. Notem que el mínim i el màxim d'un subconjunt d'un conjunt parcialment ordenat no tenen perquè existir sempre.

Definició 2.8. Si tenim un conjunt parcialment ordenat $(P, \leq)$, es diu *ben ordenat* si tot subconjunt no buit de P té mínim.

Proposició 2.9. $(\mathbb{N}, \leq)$ és un conjunt ben ordenat.

Definició 2.10. Donat un conjunt parcialment ordenat $(P, \leq)$, aleshores direm que un subconjunt no buit X de P és un *filtre* si es compleixen les següents condicions:

1. Si tenim dos elements $a, b \in X$, aleshores $a \wedge b \in X$;
2. Si tenim un element $a \in X$ i donat $b \in P$ tenim que $a \leq b$, aleshores $b \in X$.

2.2 Monoide

Definició 2.11. Un *monoide* és una estructura algebraica que consisteix en una terna $\mathbf{M} = (M, \cdot, 1)$, on M és un conjunt d'elements, $\cdot$ una operació binària interna associativa i $1 \in M$ és l'*element neutre*. És a dir, si donats $x, y, z \in M$ qualsevol es compleix :

1. $x \cdot y \in M$ (operació binària interna);
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativitat);
3. $1 \cdot x = x \cdot 1 = x$ (element neutre).

Nota 2.12. Normalment obviarem l'operació “ $\cdot$ ” quan considerem monoides amb una operació multiplicativa.

Proposició 2.13. *En un monoide, l'element neutre és únic.*

Demostració. Suposem que existeixen dos elements neutres, 1 i $1'$, aleshores per la definició d'element neutre tenim que $1' = 11' = 1'1 = 1$. ■

Exemple 2.14.

1. Considerem l'estructura algebraica de grup, que consisteix en una terna $(G, \cdot, 1)$ on l'operació “ $\cdot$ ” és associativa, tenim l'existència d'element neutre $1 \in G$ i també l'existència d'un element invers, és a dir, que per qualsevol $a \in G$ existeix un $b \in G$ de manera que $a \cdot b = b \cdot a = 1$. Aleshores tenim que un grup és un cas particular de monoide.
2. El conjunt de matrius de tamany n sobre un cos $\mathbb{K}$ amb el producte habitual de matrius amb la matriu identitat com a element neutre $(M_n(\mathbb{K}), \cdot, I_n)$, també és un monoide.
3. El conjunt amb dos elements, 0 i 1 amb el producte habitual i l' 1 com a element neutre del producte $(\{0, 1\}, \cdot, 1)$, també és un monoide.
4. Per a un conjunt Ω amb $|\Omega| = n$, definim $T_n = \{f : \Omega \longrightarrow \Omega \mid f \text{ aplicació}\}$. Aleshores aquest conjunt amb la composició d'aplicacions com a operació del conjunt i la identitat com a element neutre $\mathbf{T}_n = (T_n, \circ, id_n)$, és un monoide que denominem monoide de transformacions d'un conjunt amb n elements.
5. El conjunt dels nombres naturals amb la suma habitual i el 0 com a neutre $\mathbf{N} = (\mathbb{N}, +, 0)$, és un monoide.

Definició 2.15. Siguen $\mathbf{M} = (M, \cdot, 1)$ i $\mathbf{N} = (N, \star, 1_\star)$ monoides i siga $f : M \longrightarrow N$ una aplicació. Direm que $f : \mathbf{M} \longrightarrow \mathbf{N}$ és *homomorfisme de monoides* si preserva l'operació de cada monoide, és a dir, si $\forall m_1, m_2 \in M$ es compleix:

$$f(m_1 \cdot m_2) = f(m_1) \star f(m_2).$$

De la definició es dedueix que $f(1) = 1_\star$.

Definició 2.16. Direm que $\mathbf{M}$ és un monoide *commutatiu* si compleix que donats $n, m \in M$ qualsevols, tenim que $m \cdot n = n \cdot m$.

2.3 Submonoide

Podem considerar ara una subestructura dins del monoide, la de submonoide i a més, vorem que ser submonoide compleix una sèrie de propietats interessants.

Definició 2.17. Siga $\mathbf{M}$ un monoide, si tenim un conjunt N tal que $N \subseteq M$, direm que N és *submonoide* del monoide $\mathbf{M}$ si es compleix que $1 \in N$ i l'operació de $\mathbf{M}$ restringida a N és interna, és a dir, si $m, n \in N$ aleshores $m \cdot n \in N$.

Anem a veure una de les conseqüències que té ser submonoide.

Proposició 2.18. Siga $\mathbf{M}$ un monoide i siga N submonoide de $\mathbf{M}$, aleshores l'aplicació inclusió $\text{in}_N: N \longrightarrow M$ és homomorfisme de monoides.

Demostració. Si N és submonoide de $\mathbf{M}$ aleshores, si $n, m \in N$

$$\begin{aligned}\text{in}_N(nm) &= nm \\ &= \text{in}_N(n)\text{in}_N(m).\end{aligned}$$

Notem que la primera igualtat la tenim perquè $n \cdot m \in N$ per ser N submonoide de $\mathbf{M}$. ■

Exemple 2.19.

1. Si $\mathbf{M}$ és un monoide, aleshores 1_M i $\mathbf{M}$ són submonoides.
2. Si considerem un grup $\mathbf{G}$ com a monoide, aleshores els subgrups de $\mathbf{G}$ són també submonoides.
3. Si considerem el monoide de les matrius de tamany n sobre un cos $\mathbb{K}$, tenim que el subconjunt de les matrius invertibles és un submonoide.
4. Si considerem el monoide dels nombres naturals, aleshores el conjunt de nombres parells és un submonoide.

Definició 2.20. Donat un monoide $\mathbf{M}$ podem considerar el conjunt que conté a tots els submonoides de $\mathbf{M}$ i el denotem per $\text{Sub}(\mathbf{M}) = \{N \mid N \text{ és submonoide de } \mathbf{M}\}$.

Lema 2.21. Siga $\mathbf{M}$ un monoide, I un conjunt d'índexs i $\{A_i \mid i \in I\}$ una família de submonoides de $\mathbf{M}$ qualsevol, aleshores $\bigcap_{i \in I} A_i$ és un submonoide de $\mathbf{M}$.

Demostració. Anem a demostrar-ho per la definició de submonoide. Per una banda tenim que la intersecció dels A_i està inclosa en M ja que tots els A_i són submonoides. Per altra part, el neutre de M està en la intersecció dels A_i , ja que està en tots els A_i per ser submonoides. Per últim, si tenim dos elements qualsevol a_1, a_2 en la intersecció dels A_i , aleshores $a_1, a_2 \in A_i \forall i \in I$, per tant $a_1 a_2 \in A_i \forall i \in I$, per ser tots submonoides, i així $a_1 a_2$ està en la intersecció dels A_i . ■

Definició 2.22. Si tenim $\mathbf{M}$ un monoide aleshores podem considerar per a cada X subconjunt de $\mathbf{M}$:

$$\mathbf{Sg}(X) = \bigcap \{ \mathbf{N} \mid X \subseteq \mathbf{N} \text{ i } \mathbf{N} \text{ és submonoide de } \mathbf{M} \}$$

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

Lema 2.23. Siga $\mathbf{M}$ un monoide, I un conjunt d'índexs i $\{ \mathbf{A}_i \mid i \in I \}$ una família de submonoides de $\mathbf{M}$ qualsevol, aleshores $\mathbf{Sg}(\bigcup_{i \in I} \mathbf{A}_i)$ és un submonoide de $\mathbf{M}$.

Teorema 2.24. Siga $\mathbf{M}$ un monoide, I un conjunt d'índexs i $A = \{ \mathbf{A}_i \mid i \in I \}$ una família de submonoides de $\mathbf{M}$ qualsevol. Definim les operacions:

$$\bigwedge_{i \in I} \mathbf{A}_i = \bigcap_{i \in I} \mathbf{A}_i, \quad \bigvee_{i \in I} \mathbf{A}_i = \mathbf{Sg}(\bigcup_{i \in I} \mathbf{A}_i).$$

Amb aquestes operacions, $\text{Sub}(\mathbf{M})$ amb l'ordre habitual és un reticle complet. Denotarem aquest reticle per $\mathbf{Sub}(\mathbf{M}) = (\text{Sub}(\mathbf{M}), \subseteq)$.

Demostració. Anem a veure que $\bigcap_{i \in I} \mathbf{A}_i$ és ínfim de A i que $\mathbf{Sg}(\bigcup_{i \in I} \mathbf{A}_i)$ és suprem de A . Si considerem $\mathbf{N}_1$ un submonoide de $\mathbf{M}$ tal que està contingut en $\mathbf{A}_i \forall i \in I$, aleshores $\mathbf{N}_1 \subseteq \bigcap_{i \in I} \mathbf{A}_i$. Així tenim que $\bigcap_{i \in I} \mathbf{A}_i$ és ínfim de la família de submonoides A . Ara considerem $\mathbf{N}_2$ un submonoide de $\mathbf{M}$ que conté a $\mathbf{A}_i \forall i \in I$, aleshores $\bigcup_{i \in I} \mathbf{A}_i \subseteq \mathbf{N}_2$ i per tant, per com està definit $\mathbf{Sg}(\bigcup_{i \in I} \mathbf{A}_i)$ tenim que $\mathbf{Sg}(\bigcup_{i \in I} \mathbf{A}_i) \subseteq \mathbf{N}_2$. D'aquesta forma tenim que $\mathbf{Sg}(\bigcup_{i \in I} \mathbf{A}_i)$ és suprem de la família de submonoides.

Per (2.21) i (2.23) tenim que aquest ínfim i suprem són monoides, per tant $\text{Sub}(\mathbf{M})$, amb les operacions definides en l'enunciat, és un reticle complet amb l'ordre habitual. ■

Corol·lari 2.25. Siga $\mathbf{M}$ un monoide aleshores $\bigwedge \text{Sub}(\mathbf{M}) = 1_{\mathbf{M}}$ i $\bigvee \text{Sub}(\mathbf{M}) = \mathbf{M}$.

2.4 Monoide quocient i congruències

Definició 2.26. Donat un monoide $\mathbf{M}$ i una relació d'equivalència $\Phi \subseteq \mathbf{M} \times \mathbf{M}$, es diu que Φ és una relació de congruència en $\mathbf{M}$ si per a tot $(m_1, m_2), (n_1, n_2) \in \Phi$, tenim $(m_1 \cdot n_1, m_2 \cdot n_2) \in \Phi$.

Definició 2.27. Siga $\mathbf{M}$ un monoide, aleshores definim la *diagonal* com el següent conjunt, $\Delta_{\mathbf{M}} = \{ (m, m) \mid m \in \mathbf{M} \} \subseteq \mathbf{M} \times \mathbf{M}$.

Exemple 2.28.

1. Si tenim el monoide $\mathbf{M}$ aleshores $\Delta_{\mathbf{M}}$ i $\mathbf{M}^2 = \mathbf{M} \times \mathbf{M}$, són congruències.
2. Considerem el monoide de les matrius de tamany n sobre un cos $\mathbb{K}$. Si relacionem aquestes matrius en funció de si tenen el mateix determinant o no, tindrem la següent relació $\Phi = \{ (x, y) \in M_n(\mathbb{K}) \times M_n(\mathbb{K}) \mid \det(x) = \det(y) \}$. Tenim que Φ és una congruència, anem a comprovar-ho.

Clarament Φ és relació d'equivalència, per tant només cal vore que és relació de congruència. Siguen $x_1, x_2, y_1, y_2 \in M_n(\mathbb{K})$ de manera que $(x_1, y_1), (x_2, y_2) \in \Phi$, és a dir, $\det(x_1) = \det(y_1)$ i $\det(x_2) = \det(y_2)$, aleshores, com sabem per propietats dels determinants que el determinant del producte és el producte dels determinants, tenim que $\det(x_1 x_2) = \det(x_1) \det(x_2) = \det(y_1) \det(y_2) = \det(y_1 y_2)$ i així $(x_1 x_2, y_1 y_2) \in \Phi$

Definició 2.29. Siga $\mathbf{M}$ un monoide i Φ una relació de congruència sobre $\mathbf{M}$. Anomenem *conjunt quocient* al conjunt format per les classes d'equivalència dels elements de $\mathbf{M}$ respecte de Φ i el denotem per $\mathbf{M}/\Phi = \{[m]_\Phi \mid m \in M\}$.

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

Proposició 2.30. Considerem un monoide $\mathbf{M}$ i Φ una relació de congruència en $\mathbf{M}$, aleshores $\mathbf{M}/\Phi = (\mathbf{M}/\Phi, *, [1]_\Phi)$ és un monoide, on l'operació “ $*$ ” està definida de la següent manera:

$$\begin{aligned} *: \quad \mathbf{M}/\Phi \times \mathbf{M}/\Phi &\longrightarrow \mathbf{M}/\Phi \\ ([m_1]_\Phi, [m_2]_\Phi) &\longmapsto [m_1]_\Phi * [m_2]_\Phi = [m_1 m_2]_\Phi \end{aligned}$$

Demostració. Hem de vore que l'operació “ $*$ ” està ben definida, que és associativa, que és compatible amb la relació Φ i que $[1]_\Phi$ és l'element neutre.

Ben definida i compatible amb Φ :

Siguen $([m_1]_\Phi, [m_2]_\Phi), ([n_1]_\Phi, [n_2]_\Phi) \in \mathbf{M}/\Phi \times \mathbf{M}/\Phi$ tal que $[m_1]_\Phi = [n_1]_\Phi$ i $[m_2]_\Phi = [n_2]_\Phi$.

Aleshores sabem que $(m_1, n_1), (m_2, n_2) \in \Phi$ i per tant com que Φ és una relació de congruència sobre $\mathbf{M}$ tenim $(m_1 m_2, n_1 n_2) \in \Phi$, és a dir, $[m_1 m_2]_\Phi = [n_1 n_2]_\Phi$.

Associativa: Siguen $[m_1]_\Phi, [m_2]_\Phi, [m_3]_\Phi \in \mathbf{M}/\Phi$

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

Notem que la tercera igualtat l'obtenim ja que l'operació de $\mathbf{M}$ és associativa en ser $\mathbf{M}$ monoide.

Element neutre: Siga $[m]_\Phi \in \mathbf{M}/\Phi$ qualsevol, aleshores,

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

Notem que la segona i la quarta igualtat es dona en ser 1 el neutre del monoide $\mathbf{M}$. ■

Proposició 2.31. Siga $\mathbf{M}$ un monoide i $\Phi \subseteq M \times M$ una relació de congruència en $\mathbf{M}$. Aleshores l'aplicació projecció $\text{pr}_\Phi: \mathbf{M} \longrightarrow \mathbf{M}/\Phi$, que a cada $m \in M$ li fa correspondre la seua classe de congruència $[m]_\Phi$, és un homomorfisme de monoides.

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

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

Notem que la segona igualtat ve donada per ser Φ una congruència. Aleshores pr_Φ és un homomorfisme. ■

Definició 2.32. Donat un monoide $\mathbf{M}$, definim el conjunt de totes les congruències sobre el monoide $\mathbf{M}$ com $\text{Con}(\mathbf{M}) = \{\Phi \subseteq M \times M \mid \Phi \text{ és una congruència en } \mathbf{M}\}$.

Lema 2.33. Siga $\mathbf{M}$ un monoide, I un conjunt d'índexs i $\{\Phi_i \mid i \in I\}$ una família arbitrària de congruències en $\mathbf{M}$ qualsevol, $\bigcap_{i \in I} \Phi_i$ és una congruència en $\mathbf{M}$.

Demostració. Començarem provant que $\bigcap_{i \in I} \Phi_i$ és una relació d'equivalència.

- Reflexiva: $(m, m) \in \bigcap_{i \in I} \Phi_i$ perquè $(m, m) \in \Phi_i$ ($\forall i \in I$).
- Simètrica: Si $(m_1, m_2) \in \bigcap_{i \in I} \Phi_i$ aleshores tenim que $(m_1, m_2) \in \Phi_i$ ($\forall i \in I$). Ara, com cada Φ_i és relació d'equivalència, tenim també $(m_2, m_1) \in \Phi_i$ ($\forall i \in I$), per tant podem concloure que $(m_2, m_1) \in \bigcap_{i \in I} \Phi_i$.
- Transitiva: Si $(m_1, m_2), (m_2, m_3) \in \bigcap_{i \in I} \Phi_i$, aleshores $(m_1, m_2), (m_2, m_3) \in \Phi_i$ ($\forall i \in I$). Per la propietat transitiva que tenen cada un dels Φ_i tenim que $(m_1, m_3) \in \Phi_i$ ($\forall i \in I$), aleshores $(m_1, m_3) \in \bigcap_{i \in I} \Phi_i$.

Ara sols ens queda vore que és relació de congruència.

Siguen $(m_1, m_2), (n_1, n_2) \in \bigcap_{i \in I} \Phi_i$ aleshores $(m_1, m_2), (n_1, n_2) \in \Phi_i$ ($\forall i \in I$). Per tant, com que cada un dels Φ_i és relació de congruència, tenim que $(m_1 n_1, m_2 n_2) \in \Phi_i$ ($\forall i \in I$), aleshores $(m_1 n_1, m_2 n_2) \in \bigcap_{i \in I} \Phi_i$. ■

Lema 2.34. Siga $\mathbf{M}$ un monoide, I un conjunt d'índexs i $\{\Phi_i \mid i \in I\}$ una família arbitrària de congruències en $\mathbf{M}$ qualsevol, aleshores tenim que:

$$\Psi = \{(a, b) \in M \times M \mid \exists m \in \mathbb{N}, (a_j)_{j=0}^m \in M^{m+1}, (a_{j-1}, a_j) \in \bigcup_{i \in I} \Phi_i \quad \forall 1 \leq j \leq m\}$$

és una congruència en $\mathbf{M}$.

Demostració. Anem a vore primer que és relació d'equivalència:

- Reflexiva: Si $a \in M$, com $(a, a) \in \Phi_i$ per a tot $i \in I$ per ser totes congruències, aleshores $(a, a) \in \bigcup_{i \in I} \Phi_i$ i per tant $(a, a) \in \Psi$.
- Simètrica: Siga $(a, b) \in \Psi$, aleshores existeix una successió $(a_j)_{j=0}^m \in M^{m+1}$, sent $a_0 = a$ i $a_m = b$, tal que per a tot $j \in \{1, \dots, m\}$, tenim $(a_{j-1}, a_j) \in \bigcup_{i \in I} \Phi_i$. Per tant, si prenem la successió inversa $(a_{m-j})_{j=0}^m$ tenim que per a tot $j \in \{1, \dots, m\}$, $(a_{m-j-1}, a_{m-j}) \in \bigcup_{i \in I} \Phi_i$ per la propietat simètrica de cada congruència de la família, aleshores $(b, a) \in \Psi$.
- Transitiva: Siguen $(a, b), (b, c) \in \Psi$, aleshores existeixen dos successions $(a_j)_{j=0}^m \in M^{m+1}$ i $(a_j)_{j=m}^{m+s} \in M^{s+1}$, sent $a_0 = a, a_m = b$ i $a_{m+s} = c$, tal que per a tot $j \in \{1, \dots, m+s\}$, tenim $(a_{j-1}, a_j) \in \bigcup_{i \in I} \Phi_i$. Per tant, si unim les dos successions $(a_j)_{j=0}^{m+s}$, tenim que $(a, c) \in \Psi$.

Una volta ja tenim que és relació d'equivalència, ens queda vore que l'operació del monoide és compatible amb la relació Ψ .

Si tenim $(a_0, a_m), (b_0, b_s) \in \Psi$, aleshores existeixen dos successions $a = (a_j)_{j=0}^m \in M^{m+1}$ i $b = (b_k)_{k=0}^s \in M^{s+1}$ amb $m, s \in \mathbb{N}$, de manera que per a tot $j \in \{1, \dots, m\}$ i per a tot $k \in \{1, \dots, s\}$, tenim que cada $(a_{j-1}, a_j) \in \bigcup_{i \in I} \Phi_i$ i $(b_{k-1}, b_k) \in \bigcup_{i \in I} \Phi_i$.

Ara com que $(b_0, b_0), (a_m, a_m) \in \Phi_i$ per a tot $i \in I$ per la propietat reflexiva que tenen cada una de les congruències Φ_i , aleshores tenim que el producte $(a_{j-1}b_0, a_jb_0) \in \bigcup_{i \in I} \Phi_i$ per a tot $j \in \{1, \dots, m\}$ ja que cada $(a_{j-1}, a_j) \in \bigcup_{i \in I} \Phi_i$. En particular està en alguna congruència Φ_i per a algun $i \in I$ i en multiplicar per (b_0, b_0) continua estant en la mateixa congruència, per tant $(a_mb_{k-1}, a_mb_k) \in \bigcup_{i \in I} \Phi_i$ per a tot $k \in \{1, \dots, s\}$ pel mateix raonament.

Notem que l'últim element de la successió ab_0 (s'enten que cada component de la successió a es multiplica per b_0 per la dreta) que és a_mb_0 coincideix amb el primer element de la successió a_mb , per tant si unim les dos successions ens queda una única successió que uneix (a_0b_0, a_mb_s) de manera que cada un dels sements de la successió està en $\bigcup_{i \in I} \Phi_i$, així ja tenim que $(a_0b_0, a_mb_s) \in \Psi$ i concloem que Ψ és una congruència. ■

Teorema 2.35. Siga $\mathbf{M}$ un monoide, I un conjunt d'índexs i $\{\Phi_i \mid i \in I\}$ una família de congruències en $\mathbf{M}$ qualsevol. Definim les operacions:

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

$$\bigvee_{i \in I} \Phi_i = \{(a_0, a_m) \in M \times M \mid \exists (a_j)_{j=0}^m \in M^{m+1}, (a_{j-1}, a_j) \in \bigcup_{i \in I} \Phi_i \quad \forall 1 \leq j \leq m\}.$$

Amb aquestes operacions, $\text{Con}(\mathbf{M})$ amb l'ordre habitual és un reticle complet. Denotarem aquest reticle per $\mathbf{Con}(\mathbf{M}) = (\text{Con}(\mathbf{M}), \subseteq)$.

Demostració. Si considerem Ψ_1 una congruència en $\mathbf{M}$ tal que està continguda en $\Phi_i \forall i \in I$, aleshores $\Psi_1 \subseteq \bigcap_{i \in I} \Phi_i$. Així tenim que $\bigcap_{i \in I} \Phi_i$ és ínfim de la família de congruències. Ara considerem Ψ_2 una congruència en $\mathbf{M}$ que conté a $\Phi_i \forall i \in I$, així tenim $\bigcup_{i \in I} \Phi_i \subseteq \Psi_2$. Per tant,

sigui $(a, b) \in \bigvee_{i \in I} \Phi_i$ aleshores existeix un camí $(a_j)_{j=0}^m \in M^{m+1}$, sent $a_0 = a$ i $a_m = b$, tal que per a tot $j \in \{1, \dots, m\}$, tenim $(a_{j-1}, a_j) \in \bigcup_{i \in I} \Phi_i \subseteq \Psi_2$ i com Ψ_2 és una congruència en $\mathbf{M}$ tenim per la propietat transitiva que $(a, b) \in \Psi_2$. En conclusió obtenim que $\bigvee_{i \in I} \Phi_i \subseteq \Psi_2$, per tant $\bigvee_{i \in I} \Phi_i$ és suprem de la família de congruències.

Per (2.33) i (2.34) tenim que aquest ínfim i suprem són congruències en $\mathbf{M}$, per tant $\text{Con}(\mathbf{M})$, amb les operacions definides en l'enunciat, és un reticle complet per l'ordre habitual donat per la inclusió. ■

Corol·lari 2.36. *Siga $\mathbf{M}$ un monoide aleshores $\bigwedge \text{Con}(\mathbf{M}) = \Delta_{\mathbf{M}}$ i $\bigvee \text{Con}(\mathbf{M}) = \mathbf{M}^2$.*

Definició 2.37. Direm que el monoide $\mathbf{M}$ és *finit* quan $\mathbf{M}$ és finit. Donada una congruència Φ en $\mathbf{M}$ direm que té *índex finit* quan $\mathbf{M}/\Phi$ és finit.

Definició 2.38. Donat un monoide $\mathbf{M}$, definim

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

com el conjunt format per totes les congruències d'índex finit sobre el monoide $\mathbf{M}$.

Siga $\mathbf{M}$ un monoide no finit, aleshores la intersecció arbitrària de congruències d'índex finit no necessàriament ha de ser una congruència d'índex finit. Ja vorem un exemple d'aquesta situació més endavant. No obstant la intersecció finita de congruències d'índex finit i el suprem d'un nombre finit de congruències d'índex finit, si que continua sent una congruència d'índex finit. La notació que hem emprat al teorema (2.35) ens servirà per a aquest cas també.

Proposició 2.39. *Siga $\mathbf{M}$ un monoide i $\Phi_1, \Phi_2 \in \text{Con}_{\text{if}}(\mathbf{M})$, aleshores $\Phi_1 \wedge \Phi_2 \in \text{Con}_{\text{if}}(\mathbf{M})$.*

Demostració. Ja sabem que $\Phi_1 \wedge \Phi_2 = \Phi_1 \cap \Phi_2 \in \text{Con}(\mathbf{M})$ pel resultat (2.33), per tant només queda veure que és una congruència d'índex finit. Considerem l'aplicació:

$$\begin{aligned} f: \mathbf{M}/(\Phi_1 \cap \Phi_2) &\longrightarrow \mathbf{M}/\Phi_1 \times \mathbf{M}/\Phi_2 \\ [m]_{\Phi_1 \cap \Phi_2} &\longmapsto ([m]_{\Phi_1}, [m]_{\Phi_2}) \end{aligned}$$

Veiem que f està ben definida. Siga $[m]_{\Phi_1 \cap \Phi_2} = [n]_{\Phi_1 \cap \Phi_2}$ que és el mateix que $(m, n) \in \Phi_1 \cap \Phi_2$, per tant com (m, n) està en les dos congruències Φ_1 i Φ_2 tenim que $[m]_{\Phi_i} = [n]_{\Phi_i}$ per a $i = 1, 2$. Així f està ben definida.

També f és injectiva. Siguen $[m]_{\Phi_1 \cap \Phi_2}, [n]_{\Phi_1 \cap \Phi_2} \in \mathbf{M}/\Phi_1 \cap \Phi_2$ de manera que $([m]_{\Phi_1}, [m]_{\Phi_2}) = ([n]_{\Phi_1}, [n]_{\Phi_2})$, aleshores es compleix que $[m]_{\Phi_1} = [n]_{\Phi_1}$ i $[m]_{\Phi_2} = [n]_{\Phi_2}$ i per tant també tenim que $(m, n) \in \Phi_1 \cap \Phi_2$. En conclusió obtenim que $[m]_{\Phi_1 \cap \Phi_2} = [n]_{\Phi_1 \cap \Phi_2}$ i així l'aplicació f és injectiva.

Com f és injectiva i el seu codomini és finit, perquè el producte cartesià de conjunts finits és finit, tenim que el domini també és finit i ja hem demostrat que $\Phi_1 \cap \Phi_2 \in \text{Con}_{\text{if}}(\mathbf{M})$. ■

Proposició 2.40. Siga $\mathbf{M}$ un monoide, $\Phi_1 \in \text{Con}_{\text{if}}(\mathbf{M})$ i $\Phi_2 \in \text{Con}(\mathbf{M})$ de manera que $\Phi_1 \subseteq \Phi_2$, aleshores $\Phi_2 \in \text{Con}_{\text{if}}(\mathbf{M})$.

Demostració. Considerem l'aplicació f següent:

$$\begin{aligned} f: \mathbf{M}/\Phi_1 &\longrightarrow \mathbf{M}/\Phi_2 \\ [m]_{\Phi_1} &\longmapsto [m]_{\Phi_2} \end{aligned}$$

Ara anem a veure que està ben definida. Siguen $m, n \in \mathbf{M}$ de manera que $[m]_{\Phi_1} = [n]_{\Phi_1}$ tenim $(m, n) \in \Phi_1$ com partim de la hipòtesi de que $\Phi_1 \subseteq \Phi_2$, aleshores $(m, n) \in \Phi_2$ i per tant $[m]_{\Phi_2} = [n]_{\Phi_2}$. Així f està ben definida.

Ara anem a veure també que f és sobrejectiva. Siga $[m]_{\Phi_2} \in \mathbf{M}/\Phi_2$ per a algun $m \in \mathbf{M}$, podem considerar $[m]_{\Phi_1}$ i així $f([m]_{\Phi_1}) = [m]_{\Phi_2}$ i concloem que f és sobrejectiva.

Ara com f és sobrejectiva i el domini és finit, aleshores el codomini és finit també i per tant $\Phi_2 \in \text{Con}_{\text{if}}(\mathbf{M})$. ■

Corol·lari 2.41. Siga $\mathbf{M}$ un monoide i $\Phi_1, \Phi_2 \in \text{Con}_{\text{if}}(\mathbf{M})$, aleshores $\Phi_1 \vee \Phi_2 \in \text{Con}_{\text{if}}(\mathbf{M})$

Demostració. Sabem que $\Phi_1 \vee \Phi_2 \in \text{Con}(\mathbf{M})$ per la proposició (2.34) i com $\Phi_1 \subseteq \Phi_1 \vee \Phi_2$ per la proposició anterior (2.40) ja tenim que $\Phi_1 \vee \Phi_2 \in \text{Con}_{\text{if}}(\mathbf{M})$. ■

Corol·lari 2.42. Siga $\mathbf{M}$ un monoide, aleshores $\text{Con}_{\text{if}}(\mathbf{M})$ és un filtre en $(\text{Con}(\mathbf{M}), \subseteq)$.

Demostració. Per les proposicions (2.39) i (2.40) tenim que $\text{Con}_{\text{if}}(\mathbf{M})$ és un filtre. ■

2.5 Teorema d'isomorfia

Aquest resultat que anem a veure és molt important ja que l'utilitzarem prou voltes al llarg de tot el treball.

Definició 2.43. Siguen $\mathbf{M}$ i $\mathbf{N}$ dos monoides i siga $f: \mathbf{M} \longrightarrow \mathbf{N}$ un homomorfisme de monoides definim el *nucli* de f com $\text{Ker}(f) = \{(m_1, m_2) \in \mathbf{M} \times \mathbf{M} \mid f(m_1) = f(m_2)\}$ i el *conjunt imatge* de f com $\text{Im}(f) = \{n \in \mathbf{N} \mid \exists m \in \mathbf{M} (f(m) = n)\}$.

Definició 2.44. Direm que dos monoides $\mathbf{M}$ i $\mathbf{N}$ són *isomorfs* si $\exists f: \mathbf{M} \longrightarrow \mathbf{N}$ isomorfisme de monoides, és a dir, un homomorfisme de monoides bijectiu. En aquest cas escriurem $\mathbf{M} \cong \mathbf{N}$.

Proposició 2.45. Siguen $\mathbf{M}$ i $\mathbf{N}$ dos monoides i siga $f: \mathbf{M} \longrightarrow \mathbf{N}$ un homomorfisme de monoides, aleshores tenim que:

1. $\text{Ker}(f)$ és una relació de congruència en $\mathbf{M}$;
2. $\text{Im}(f)$ és un submonoide de $\mathbf{N}$ amb la restricció de les operacions;
3. $\mathbf{M}/\text{Ker}(f) \cong \text{Im}(f)$.

Demostració. 1. Notem que $\text{Ker}(f)$ és una relació d'equivalència, ja que compleix la propietat reflexiva, simètrica i transitiva. Falta comprovar la compatibilitat de l'operació del monoide.

Siguem $(m_1, m_2), (n_1, n_2) \in \text{Ker}(f)$ per definició de $\text{Ker}(f)$ tenim que $f(m_1) = f(m_2)$ i $f(n_1) = f(n_2)$. Aleshores

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

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

2. L'aplicació inclosió entre $\text{Im}(f)$ i $\mathbf{N}$, $\text{in}_{\text{Im}(f)}: \mathbf{Im}(f) \longrightarrow \mathbf{N}$ és homomorfisme de monoides ja que f ho és.
3. Volem comprovar que $\mathbf{M}/\text{Ker}(f) \cong \mathbf{Im}(f)$ així que definim la següent funció:

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

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

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

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

Notem que la primera igualtat la tenim en ser $\text{Ker}(f)$ una congruència i la tercera en ser f un homomorfisme. Per tant F és un homomorfisme bijectiu, és a dir, és un isomorfisme. Podem concloure així que $\mathbf{M}/\text{Ker}(f) \cong \mathbf{Im}(f)$. ■

Exemple 2.46. Prenem el monoide dels naturals amb la suma habitual $\mathbf{N} = (\mathbb{N}, +, 0)$ i definim la següent relació sobre $\mathbf{N}$

$$\Phi = \{(0, 0)\} \cup \{(p, q) \mid p, q \geq 1\}$$

Aquesta relació és una relació de congruència ja que compleix ser relació d'equivalència i la suma de dos elements de Φ també està en Φ .

I ara podem obtenir el conjunt quocient $\mathbf{N}/\Phi = \{[0]_\Phi, [1]_\Phi\}$ i amb l'operació induïda per la congruència, és a dir, la suma dels representants, tenim un monoide finit a partir d'altre que no ho és.

Ara per altra banda, com que $(\{0, 1\}, \max, 0)$ és un monoide per ser el max associatiu, podem considerar el següent homomorfisme de monoides:

$$F: \mathbf{N} \longrightarrow \{0, 1\}$$

$$n \longmapsto \begin{cases} 0 & \text{si } n = 0 \\ 1 & \text{si } n \neq 0 \end{cases}$$

Clarament tenim que $\text{Ker}(F) = \Phi$ aleshores per (2.45) tenim que $\mathbf{N}/\Phi \cong (\{0, 1\}, \max, 0)$.

2.6 Monoide lliure

Siga A un conjunt que anomenem *alfabet*, format per elements que anomenem *lletres*. Si $n \in \mathbb{N}$ podem definir la següent aplicació $w: n \longrightarrow A$ que anomenem *paraula de A de llargària n* .

Denotem per A^* com el *conjunt de totes les paraules en A* . Aquest conjunt està dotat del que anomenarem *operació concatenació* “ λ ”, de manera que donades dos paraules $w: n \longrightarrow A$ i $u: m \longrightarrow A$ aleshores:

$$\begin{aligned} \lambda: A^* \times A^* &\longrightarrow A^* \\ (w, u) &\longmapsto w \lambda u: n + m \longrightarrow A \\ j &\longmapsto \begin{cases} w(j) & \text{si } j \in n, \\ u(j - n) & \text{si } j - n \in m, \end{cases} \end{aligned}$$

També podem considerar les paraules simplement com la concatenació de lletres de manera que $w = (a_0 \cdots a_{n-1})$ i la concatenació de paraules w i $u = (b_0 \cdots b_{s-1})$ en aquest cas seria $wu = (a_0 \cdots a_{n-1} b_0 \cdots b_{s-1})$.

L'operació λ té element neutre, que anomenem la *paraula buida* i denotem per $\lambda: 0 \longrightarrow A$. Aquesta operació és associativa, ja que siguin $w, u, v \in A^*$ $w = (a_0 \cdots a_{n-1})$, $u = (b_0 \cdots b_{m-1})$ i $v = (c_0 \cdots c_{l-1})$ i per tant

$$\begin{aligned} (wu)v &= (a_0 \cdots a_{n-1} b_0 \cdots b_{m-1})(c_0 \cdots c_{l-1}) \\ &= (a_0 \cdots a_{n-1} b_0 \cdots b_{m-1} c_0 \cdots c_{l-1}) \\ &= (a_0 \cdots a_{n-1})(b_0 \cdots b_{m-1} c_0 \cdots c_{l-1}) \\ &= w(uv). \end{aligned}$$

Per tant el conjunt A^* amb l'operació concatenació i el neutre λ té estructura de monoide, que anomenarem *monoide lliure sobre A* .

Ara anem a definir la següent aplicació que anomenarem *inserció de generadors*:

$$\begin{aligned} \eta_A: A &\longrightarrow A^* \\ a &\longmapsto (a): \begin{array}{l} 1 \longrightarrow A \\ 0 \longmapsto a \end{array} \end{aligned}$$

Aquesta aplicació el que fa és incloure a cada lletra a de A com a paraula en A^* formada únicament per la lletra a . Per simplificar la notació un poc, usualment escriurem $a = (a)$.

Definició 2.47. Donat un alfabet A anomenem *llenguatge de A^** a qualsevol $\mathcal{L} \subseteq A^*$.

Proposició 2.48 (Propietat universal del monoide lliure). *Siga A un alfabet, $\mathbf{M}$ un monoide i $f: A \longrightarrow \mathbf{M}$ una aplicació, aleshores tenim que existeix un únic homomorfisme de monoides $f^*: A^* \longrightarrow \mathbf{M}$ tal que $f = f^* \circ \eta_A$.*

Demostració. Anem a provar-ho construint el homomorfisme de manera que $f^*(\lambda) = 1_{\mathbf{M}}$ i si $w = (a_0 a_1 \cdots a_{n-1}) \in A^*$ definim $f^*(w) = f(a_0)f(a_1) \cdots f(a_{n-1})$. Clarament així f^* és un homomorfisme de monoides.

Ara suposem que existeix un altre homomorfisme de monoides g entre A^* i $\mathbf{M}$ tal que $f = g \circ \eta_A$. Aleshores tenim que

$$\begin{aligned} g(a_0 \cdots a_{n-1}) &= g(a_0) \cdots g(a_{n-1}) \\ &= f(a_0) \cdots f(a_{n-1}) \\ &= f^*(a_0 \cdots a_{n-1}). \end{aligned}$$

Notem que la segon igualtat la tenim perquè si considerem a_i com a paraula de A aleshores $g(a_i) = g(\eta_A(a_i))$ considerant ara a_i com a lletra i tenint en compte que $f = g \circ \eta_A$ ja ho tindríem. ■

Exemple 2.49.

1. Si $|A| = 1$, considerem $A = \{a\}$. Si agafem una paraula $w \in A^*$ de llargària n per a algun $n \in \mathbb{N}$ tenim que $w = a^n$. Ara fem l'aplicació $f: A \longrightarrow \mathbf{N}$ tal que $f(a) = 1$ aleshores per la propietat universal del monoide lliure tenim que existeix un homomorfisme de monoides $f^*: A^* \longrightarrow \mathbf{N}$ tal que $f = f^* \circ \eta_A$, aleshores

$$\begin{aligned} f^*(a^n) &= f^*(a \cdots a) \\ &= f(a) + \cdots + f(a) \\ &= 1 + \cdots + 1 \\ &= n. \end{aligned}$$

D'aquesta manera f^* és clarament una bijecció, anem a veure que $\text{Ker}(f^*) = \Delta_{A^*}$.

Per altra banda prenem la congruència Δ_{A^*} que recordem que és de la forma $\Delta_{A^*} = \{(x, x) \in A^* \times A^* \mid x \in A^*\}$ i l'homomorfisme identitat $\text{id}_{A^*}: A^* \longrightarrow A^*$ tenim que $\text{Ker}(\text{id}_{A^*}) = \{(x, y) \in A^* \times A^* \mid x = \text{id}_{A^*}(x) = \text{id}_{A^*}(y) = y\} = \Delta_{A^*}$ aleshores d'aquesta manera per la proposició (2.45) tenim que $A^*/\Delta_{A^*} \cong A^*$.

Aleshores ara per la proposició (2.45) altra volta tenim que $A^*/\Delta_{A^*} \cong A^* \cong \mathbf{N}$, és a dir que el monoide lliure d'un generador és isomorf al monoide dels naturals cosa que serà molt important per a després.

2. Si $|A| = 2$ aleshores $A^* \not\cong \mathbf{N}^2$ perquè A^* no és commutatiu però $\mathbf{N}^2$ si ho és. Notem que la imatge per un homomorfisme d'un monoide commutatiu també és un monoide commutatiu per tant no pot haver un homomorfisme entre un monoide commutatiu i altre que no ho és, encara menys un isomorfisme.

Capítol 3

Autòmates

Una de les rames que anem a tractar en aquest treball i que tractarem en aquest capítol és la teoria d'autòmates que és troba dins de la teoria de la computació i estretament relacionada amb la teoria de llenguatges formals.

En aquest capítol presentarem tres tipus d'autòmates i també la seua equivalència en quant a llenguatges que reconeixen. Després vorem el resultat més important del treball, el teorema de Myhill-Nerode [Myh57][Ner58] que ens relacionarà el que hem vist fins ara de congruències sobre un monoide amb els autòmates. També vorem propietats de clausura dels llenguatges reconeixibles des de dos punts de vista diferents, emprant autòmates i emprant congruències d'índex finit, recalcant el fet de fer les dos demostracions per veure les limitacions i els avantatges de cada eina per entendre-les millor.

3.1 Models d'autòmates.

Dins del món dels autòmates anem a destacar fonamentalment tres tipus diferents, no obstant vorem que en realitat els tres tipus són equivalents. En qualsevol cas parlarem d'autòmata finit, però primer que res, anem a veure que és un autòmata.

Definició 3.1. Un *autòmata no determinista* sobre un alfabet A és una tupla $\mathbf{X} = (X, \alpha, I, O)$ on:

- X és un conjunt finit d'estats;
- $\alpha: A \longrightarrow \mathcal{P}(X)^X = \{f \mid f: X \longrightarrow \mathcal{P}(X)\}$ és l'aplicació de transicions;
- $I \subseteq X$ conjunt d'estats inicials (inputs);
- $O \subseteq X$ conjunt d'estats finals (outputs).

Si $a \in A$, com $\alpha(a) \in \mathcal{P}(X)^X$ denotem $\alpha(a)(x) = x_a$ i l'anomenem *conjunt d'estats al qual podem accedir des de x mitjançant a* .

Notem que $\mathcal{P}(X)^X$ té estructura de monoide. Si tenim dos aplicacions $f, g \in \mathcal{P}(X)^X$, és a dir, $f: X \rightarrow \mathcal{P}(X)$ i $g: X \rightarrow \mathcal{P}(X)$, definim ara $g \diamond f: X \rightarrow \mathcal{P}(X)$ de manera que si tenim un element $x \in X$ aleshores, $g \diamond f(x) = \bigcup_{y \in f(x)} g(y)$, així la “composició” $\diamond$ és associativa. Definim també l’operació neutra, $1: X \rightarrow \mathcal{P}(X)$ que a un element x li fa correspondre $\{x\}$. Així $\mathcal{P}(X)^X = (\mathcal{P}(X)^X, \diamond, 1)$ té estructura de monoide.

Aleshores com tenim $\alpha: A \rightarrow \mathcal{P}(X)^X$, per la propietat universal del monoide lliure (2.48) tenim que existeix un homomorfisme de monoides $\alpha^*: A^* \rightarrow \mathcal{P}(X)^X$. Per a $w \in A^*$, $\alpha^*(w) \in \mathcal{P}(X)^X$, aleshores siga $x \in X$ denotem $\alpha^*(w)(x) = x_w$ i l’anomenem *conjunt d’estats al qual podem accedir des de x mitjançant la paraula w* .

Definició 3.2. Un autòmata no determinista amb *transicions buides* és un autòmata no determinista en que es permeten transicions buides, és a dir, tal que existeixen elements $y \in \alpha^*(\lambda)(x)$ amb $y \neq x$.

Definició 3.3. Donat un autòmata no determinista sense transicions buides (X, α, I, O) sobre A , diem que és *determinista* si I només té un element i donat $a \in A$ i $x \in X$, x_a té només un element. En aquest cas prenem l’aplicació de transicions en $X^X = \{f \mid f: X \rightarrow X\}$ de manera que $\alpha: A \rightarrow X^X$.

Notem que X^X també té estructura de monoide amb la composició habitual d’aplicacions i la identitat com a neutre. Aleshores podem aplicar la propietat universal (2.48) i tenim que existeix $\alpha^*: A^* \rightarrow X^X$ homomorfisme de monoides de manera que si $w \in A^*$ i $w = (a_0 \cdots a_n)$, aleshores $\alpha^*(w) = \alpha(a_0) \cdots \alpha(a_n)$.

Exemple 3.4. Un exemple de autòmata no determinista sense transicions buides seria el següent. Considerem $X = \{x, y, z\}$, $A = \{a, b\}$, $I = \{x, z\}$, $O = \{y\}$ i per últim com a aplicació de transicions prenem $\alpha(a) = \alpha_a: X \rightarrow \mathcal{P}(X)$, tal que $x_a = \{x, z\}$, $y_a = z$ i $z_a = y$, i $\alpha(b) = \alpha_b: X \rightarrow \mathcal{P}(X)$ tal que $x_b = y$, $y_b = x$ i $z_b = z$.

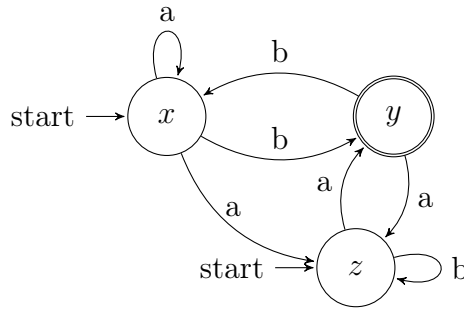


Figura 3.1: Diagrama d’un autòmata no determinista.

En aquest diagrama, la fletxa amb un “start” denota els estats inicials, les fletxes ens diuen quin és el següent estat si emprem la lletra en la que està etiquetada i dos cercles concèntrics denoten els estats finals.

Definició 3.5. Siga $\mathbf{X}$ un autòmata, definim $\mathcal{L}_{\mathbf{X}} = \{w \in A^* \mid \exists x \in I (x_w \cap O \neq \emptyset)\}$ com el llenguatge que reconeix l'autòmata $\mathbf{X}$. Açò és que reconeix les paraules w tal que, el conjunt d'estats al qual es pot accedir des d'algun estat inicial x mitjançant w , conté algun estat final.

Definició 3.6. Direm que dos autòmates $\mathbf{X}$ i $\mathbf{X}'$ són *equivalents* si reconeixen els mateixos llenguatges, és a dir, si $\mathcal{L}_{\mathbf{X}} = \mathcal{L}_{\mathbf{X}'}$.

Ara anem a vore un resultat que ens donarà la capacitat de poder determinitzar un autòmata que no és determinista i també poder eliminar les transicions buides.

Proposició 3.7. *Tot autòmata és equivalent a un autòmata determinista.*

Demostració. Siga $\mathbf{X} = (X, \alpha, I, O)$ un autòmata no determinista amb transicions buides farem altre autòmata no determinista $\mathbf{X}' = (X, \alpha', I', O')$ el qual ja no tindrà transicions buides i anem a vore que són equivalents. Notem que l'únic que no canviem és el conjunt d'estats, la resta ho canviem tot. En tindre $\mathbf{X}$ transicions buides, l'aplicació de transicions és de la forma $\alpha: A \cup \{\lambda\} \rightarrow \mathcal{P}(X)^X$, al nou conjunt d'estats inicials hem d'afegir aquells estats als quals es pot accedir des d'un estat inicial amb una transició buida, és a dir, $I' = I \cup \alpha(\lambda)[I]$ i al conjunt d'estats finals hem d'afegir aquells estats als quals es pot accedir des d'un estat final amb una transició buida, és a dir, $O' = O \cup \alpha(\lambda)[O]$. Per tant, ara definim $\alpha': A \rightarrow \mathcal{P}(X)^X$ de manera que si tenim una lletra $a \in A$ aleshores la nova aplicació de transicions queda com $\alpha'(a)(x) = \alpha(a)(x) \cup \{z \in X \mid \exists y \in \alpha(a)(x), (z \in \alpha(\lambda)(y))\}$.

Volem vore que els llenguatges que reconeixen els dos autòmates són el mateix, per tant anem a comprovar si es compleix la igualtat $\mathcal{L}_{\mathbf{X}} = \mathcal{L}_{\mathbf{X}'}$.

Siga w una paraula reconeguda per $\mathbf{X}$, $w \in \mathcal{L}_{\mathbf{X}}$. Aleshores existeix un camí en l'autòmata $\mathbf{X}$ etiquetat en la paraula w que transforma un estat inicial en un de final. Si aquest camí no ha utilitzat transicions buides, aleshores aquest camí es pot reproduir en l'autòmata $\mathbf{X}'$. Si per contra si que ha utilitzat transicions buides, suposem que per a passar d'un estat x a un y s'ha utilitzat una transició buida, aleshores com que en l'autòmata $\mathbf{X}'$ tenim que aquests passos s'han incorporat a banda, podem reproduir el mateix pas des de x , al qual hem accedit sense transicions buides. D'aquesta manera tenim que $w \in \mathcal{L}_{\mathbf{X}'}$.

Siga ara w una paraula reconeguda per l'autòmata $\mathbf{X}'$, $w \in \mathcal{L}_{\mathbf{X}'}$. Així existeix un camí en l'autòmata $\mathbf{X}'$ etiquetat amb la paraula w que transforma un estat inicial en un final. Notem ara que per a cada pas entre dos estats x i y , es pot donar en l'autòmata $\mathbf{X}$ o vindria donat per una transició buida que hem incorporat en la construcció de l'autòmata $\mathbf{X}'$. En qualsevol cas, en l'autòmata $\mathbf{X}$ podem trobar un camí etiquetat en la paraula w que transforma un estat inicial en un final.

Per tant ja tenim que $\mathcal{L}_{\mathbf{X}'} = \mathcal{L}_{\mathbf{X}}$, i per tant els dos autòmates $\mathbf{X}$ i $\mathbf{X}'$ són equivalents.

Ara suposem que tenim $\mathbf{X}$ un autòmata no determinista i anem a vore que és equivalent a un autòmata determinista. Considerem ara l'autòmata $\mathbf{D}(\mathbf{X}) = (\mathcal{P}(X), \alpha, I, O')$ de manera que $O' = \{Y \in \mathcal{P}(X) \mid \exists y \in Y, y \in O\}$ i donat $Y \in \mathcal{P}(X)$ i $a \in A$ definim $Y_a = \{x_a \mid x \in Y\}$ així es clar que $\mathbf{D}(\mathbf{X})$ és un autòmata determinista ja que només té un element de $\mathcal{P}(X)$ com

a estat inicial i donat $Y \in \mathcal{P}(X)$ i $a \in A$ tenim que existeix com a molt un element soles $Y' \in \mathcal{P}(X)$ tal que $Y_a = Y' = \{x_a \mid x \in Y\}$.

Siga $w \in \mathcal{L}_X$, aleshores existeix un camí en l'autòmata X etiquetat amb la paraula w que ens porta d'un estat inicial a un estat final. Aleshores, aquest camí ens portaria a un estat final de $\mathcal{P}(X)$ amb l'autòmata $\mathbf{D}(X)$ per tant $w \in \mathcal{L}_{\mathbf{D}(X)}$.

Ara siga w una paraula reconeguda per l'autòmata $\mathbf{D}(X)$, $w \in \mathcal{L}_{\mathbf{D}(X)}$, aleshores w és l'únic camí que porta l'únic estat inicial a un estat final de $\mathcal{P}(X)$ aleshores existeix un estat de I , que anomenem x de manera que x_w és un estat final i per tant $w \in \mathcal{L}_X$.

Aleshores $\mathcal{L}_X = \mathcal{L}_{\mathbf{D}(X)}$ i per tant X i $\mathbf{D}(X)$ són dos autòmats equivalents. Concloem finalment que tot autòmata és equivalent a un atòmata determinista. ■

Exemple 3.8. En aquest exemple vorem com podem anar transformant els autòmats de manera que siguin equivalents fent cas a la demostració constructiva de (3.7).

Primer partirem d'un autòmata no determinista amb transicions buides on el conjunt d'estats és $X = \{x, y, z\}$, $A = \{a, b\}$, $I = \{x\}$ i $O = \{x, y\}$.

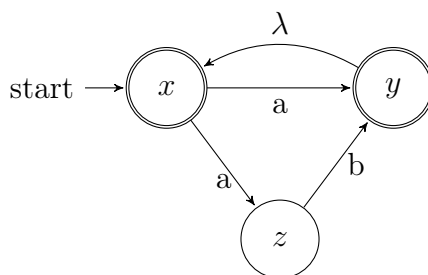


Figura 3.2: Diagrama d'un autòmata no determinista amb transicions buides.

Ara el que anem a fer és llevar la transició buida, però afegint les transicions que siguin necessàries per a que el nou autòmata siga equivalent a l'anterior. Com $x_a = y$, $z_b = y$ i podem accedir a x des de y amb una transició buida, aleshores afegirem les transicions de manera que $x_a = \{x, y\}$ i $z_b = \{y, x\}$. D'aquesta manera obtenim un nou autòmata no determinista sense transicions buides com podem vore en la figura 3.3.

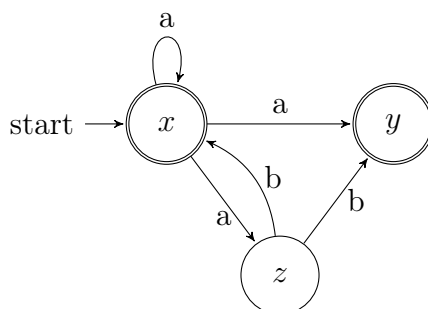


Figura 3.3: Diagrama d'un autòmata no determinista sense transicions buides.

Ara volem fer altre autòmata però determinista. El que feiem en la demostració de (3.7) era considerar el conjunt de parts de X i les transicions seran les mateixes però evaluades en cada element del conjunt estat que se'ns quede. D'aquesta manera aconseguim tindre un autòmata determinista que ens quedaria de la forma que podem vore en la figura 3.4.

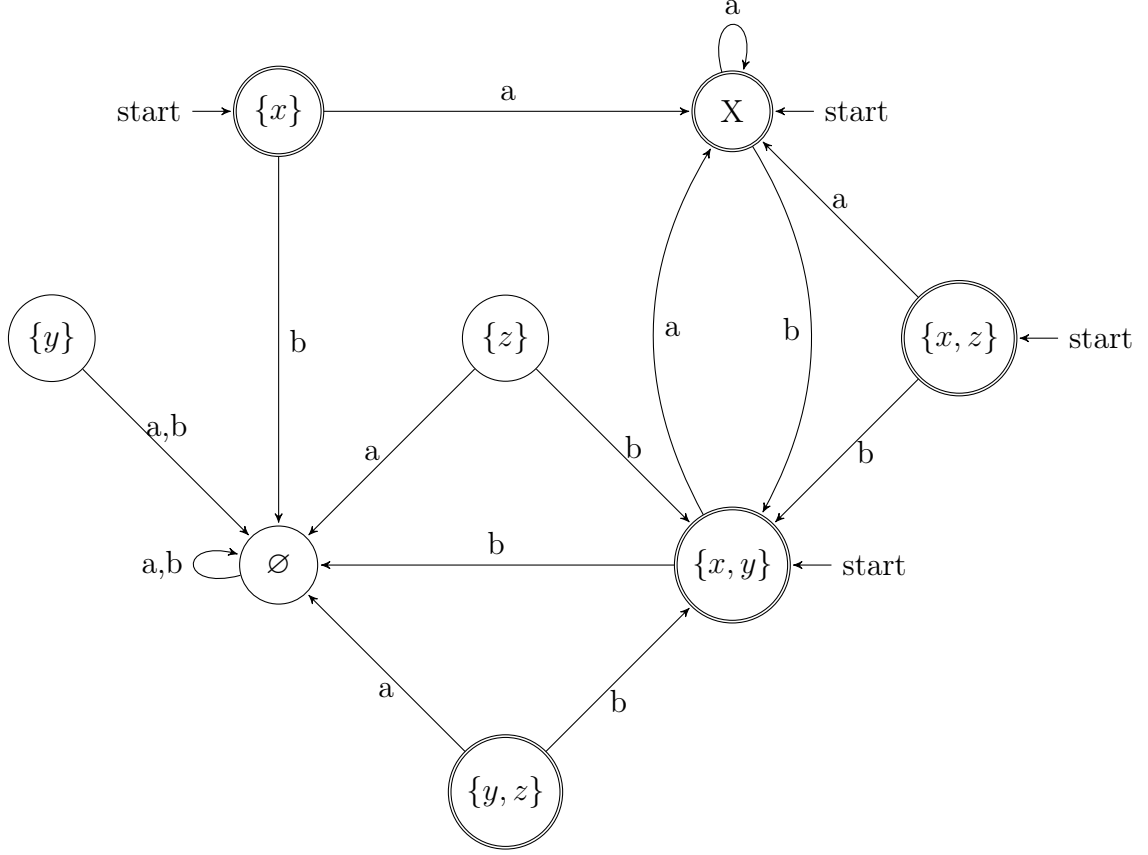


Figura 3.4: Diagrama d'un autòmata determinista.

Aquests tres autòmates que hem vist són els tres equivalents, és a dir reconeixen les mateixes paraules. Per exemple aba és una paraula reconeguda pels tres autòmates.

Definició 3.9. Un llenguatge $\mathcal{L} \subseteq \mathbf{A}^*$ s'anomena reconeixible si existeix un autòmata finit $\mathbf{X} = (X, \alpha, I, O)$ tal que $\mathcal{L} = \mathcal{L}_{\mathbf{X}}$.

Definició 3.10. Siga $\mathcal{L} \subseteq A^*$ un llenguatge i siga $\Phi \in \text{Con}(\mathbf{A}^*)$ direm que $\mathcal{L}$ està saturat per a Φ si es compleix que:

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

Nota 3.11. La inclusió $\mathcal{L} \subseteq \bigcup_{w \in \mathcal{L}} [w]_\Phi$ es dona sempre ja que si tenim una paraula $v \in \mathcal{L}$ aleshores $v \in [v]_\Phi \subseteq \bigcup_{w \in \mathcal{L}} [w]_\Phi$, per tant per vore si un llenguatge està saturat per a Φ només cal comprovar l'altra inclusió.

A propòsit d'aquesta definició, ara donarem una condició necessària i també suficient per a saber si un llenguatge és o no reconeixible gràcies al treball fet en [Myh57] i [Ner58]. Aquest és el resultat més important de tot el treball.

Teorema 3.12 (Myhill-Nerode). *Siga $\mathcal{L} \subseteq A^*$ un llenguatge de $\mathbf{A}^*$, aleshores les següents afirmacions són equivalents:*

1. $\mathcal{L}$ és un llenguatge reconeixible.
2. Existeix $\Phi \in \text{Con}_{\text{if}}(\mathbf{A}^*)$ per a la qual $\mathcal{L}$ està saturat.

Demostració. Primer anem a vore que 1. implica 2., per tant suposem que $\mathcal{L} \subseteq A^*$ és un llenguatge reconeixible, així podem trobar un autòmata finit $\mathbf{X} = (X, \alpha, I, O)$ per al qual $\mathcal{L}_{\mathbf{X}} = \mathcal{L}$. Per la proposició (3.7) podem suposar que $\mathbf{X}$ és un autòmata determinista.

Ara hem de trobar una congruència de $\mathbf{A}^*$ d'índex finit per a la qual $\mathcal{L}$ estiga saturat.

Per la propietat universal del monoide lliure (2.48) tenim que existeix un homomorfisme de monoides $\alpha^*: \mathbf{A}^* \longrightarrow \mathbf{X}^{\mathbf{X}}$, aleshores per (2.45) tenim que $\text{Ker}(\alpha^*)$ és una congruència en $\mathbf{A}^*$ i també tenim que $\mathbf{A}^*/\text{Ker}(\alpha^*) \cong \mathbf{Im}(\alpha^*) \leq X^X$ i com que X és un conjunt finit, també ho és X^X i per tant $\text{Ker}(\alpha^*)$ és una congruència d'índex finit.

Per últim, només ens queda comprovar que $\mathcal{L}$ està saturat per a $\text{Ker}(\alpha^*)$, és a dir vore si es compleix $\mathcal{L} = \bigcup_{w \in \mathcal{L}} [w]_{\text{Ker}(\alpha^*)}$. Tal i com hem comentat en la nota d'abans només cal comprovar $\mathcal{L} \subseteq \bigcup_{w \in \mathcal{L}} [w]_{\text{Ker}(\alpha^*)}$ per vore que està saturat. Com podem suposar que $\mathbf{X}$ és un autòmata determinista, sabem que I només té un element, per tant siga $w \in \mathcal{L} = \mathcal{L}_{\mathbf{X}}$, tenim que $x_w \in O$. Notem que

$$[w]_{\text{Ker}(\alpha^*)} = \{v \in A^* \mid (v, w) \in \text{Ker}(\alpha^*)\} = \{v \in A^* \mid \alpha^*(v) = \alpha^*(w)\}.$$

Aleshores si $v \in [w]_{\text{Ker}(\alpha^*)}$ tenim que $\alpha^*(v)(x) = \alpha^*(w)(x)$ per a $x \in X$ i com $\alpha^*(w)(x) \in O$, també $\alpha^*(v)(x) = x_v \in O$. Per tant concloem que $\mathcal{L} = \bigcup_{w \in \mathcal{L}} [w]_{\text{Ker}(\alpha^*)}$ i que $\mathcal{L}$ està saturat per a $\text{Ker}(\alpha^*)$.

Ara anem a vore la implicació que ens queda, vore que 2. implica 1., suposem que $\mathcal{L}$ està saturat per a $\Phi \in \text{Con}_{\text{if}}(\mathbf{A}^*)$.

Considerem l'autòmata $\mathbf{A}^*/\Phi = (\mathbf{A}^*/\Phi, \alpha, [\lambda]_\Phi, \text{pr}_\Phi[\mathcal{L}])$, on $\mathbf{A}^*/\Phi$ és un conjunt finit per ser Φ una congruència d'índex finit, si $a \in A$ aleshores $\alpha(a): \mathbf{A}^*/\Phi \longrightarrow \mathbf{A}^*/\Phi$ aplicació tal que $\alpha(a)([w]_\Phi) = [wa]_\Phi$, que està ben definida, $[\lambda]_\Phi \in \mathbf{A}^*/\Phi$ que és la classe d'equivalència de la paraula buida i per últim, $\text{pr}_\Phi: A^* \longrightarrow A^*/\Phi$ tal que $\text{pr}_\Phi(w) = [w]_\Phi$ per a qualsevol $w \in A^*$ i com $\mathcal{L} \subseteq A^*$ tenim que $\text{pr}_\Phi[\mathcal{L}] \subseteq A^*/\Phi$, per tant queda comprovat que $\mathbf{A}^*/\Phi$ és un autòmata.

Ara anem a vore que efectivament $\mathcal{L}$ és un llenguatge reconeixible, anem a vore quin és el llenguatge que reconeix l'autòmata $\mathbf{A}^*/\Phi$.

$$\begin{aligned}\mathcal{L}_{\mathbf{A}^*/\Phi} &= \{v \in A^* \mid \alpha^*(v)([\lambda]_\Phi) \in \text{pr}_\Phi[\mathcal{L}]\} \\ &= \{v \in A^* \mid [v]_\Phi \in \text{pr}_\Phi[\mathcal{L}]\} \\ &= \{v \in A^* \mid [v]_\Phi = [w]_\Phi \text{ amb } w \in \mathcal{L}\} \\ &= \bigcup_{w \in \mathcal{L}} [w]_\Phi \\ &= \mathcal{L}\end{aligned}$$

Notem que l'última igualtat la tenim perquè $\mathcal{L}$ està saturat per a Φ . D'aquesta manera tenim que $\mathcal{L} = \mathcal{L}_{\mathbf{A}^*/\Phi}$ i per tant $\mathcal{L}$ és un llenguatge reconeixible per a l'autòmata finit que hem definit. ■

Aquest resultat és molt important en aquest treball ja que gràcies a ell tenim una condició necessària i suficient per vore si un llenguatge és reconeixible o no i a més ens relaciona les congruències d'índex finit en un monoide i els autòmats, donant-nos aquesta equivalència, podent crear un autòmata a partir de les classes d'equivalència de la congruència d'índex finit. Més avant vorem un cas d'un monoide en particular en el que vorem com són totes les congruències d'índex finit i juntament amb el teorema de Myhill-Nerode (3.12) ens serà relativament fàcil vore si un llenguatge és reconeixible o no.

3.2 Propietats de clausura.

En aquesta secció anem a vore com es comporten els llenguatges reconeixibles amb operacions de clausura entre llenguatges reconeixibles com ara són la unió, la intersecció, el llenguatge complementari i la concatenació de llenguatge.

Tots aquests resultats els vorem des de dos punts de vista diferents, donarem una demostració emprant autòmats i altra abordant el problema des de les congruències d'índex finit, que gràcies al teorema de Myhill-Nerode (3.12) hem vist que són equivalents. D'aquesta manera vorem quines són les limitacions de cada mètode i les dificultats que ens podem trobar en cada cas.

Proposició 3.13. *Si tenim $\mathcal{K}, \mathcal{L} \subseteq A^*$ dos llenguatges reconeixibles, aleshores $\mathcal{K} \cap \mathcal{L}$ també és un llenguatge reconeixible.*

Demostració. Autòmats.

Per a la primera demostració, suposem que $\mathcal{K}, \mathcal{L}$ són dos llenguatges reconeixibles de A^* , aleshores tenim dos autòmats $\mathbf{X} = (X, \alpha, I, O)$, $\mathbf{X}' = (X', \alpha', I', O')$ que els reconeixen, respectivament. Com que $X \times X'$ és finit per ser producte cartesià de dos conjunts finits podem considerar l'autòmata $\mathbf{Y} = (X \times X', \beta, I \times I', O \times O')$ on tenim que β és l'aplicació de transicions que definim de la següent manera:

$$\begin{array}{lll} \beta: A & \longrightarrow & X \times X'^{X \times X'} \\ a & \longmapsto & \beta(a): \quad X \times X' \longrightarrow X \times X' \\ & & (x, x') \longmapsto (x_a, x'_a) \end{array}$$

Volem vore que $\mathcal{K} \cap \mathcal{L} = \mathcal{L}_{\mathbf{Y}}$, per tant si tenim que $w \in \mathcal{L}_{\mathbf{Y}}$ com podem suposar que l'autòmata $\mathbf{Y}$ és determinista per (3.7) i així $I = \{x\}$ i $I' = \{x'\}$ només tenen un element cadascún, aleshores $x_w \in O$ i $x'_w \in O'$ i també $w \in \mathcal{L}_{\mathbf{X}}$ i $w \in \mathcal{L}_{\mathbf{X}'}$, és a dir, $w \in \mathcal{K} \cap \mathcal{L}$. Notem que per a tindre l'altra inclusió és el mateix argument. En conclusió, $\mathbf{Y}$ és l'autòmata que reconeix $\mathcal{K} \cap \mathcal{L}$ i així és un llenguatge reconeixible.

Congruències.

Per a la segona demostració, suposem que $\mathcal{K}, \mathcal{L}$ són dos llenguatges reconeixibles de A^* , aleshores pel teorema (3.12) tenim que existeixen Φ_1, Φ_2 congruències d'índex finit de A^* de manera que $\mathcal{K} = \bigcup_{w \in \mathcal{K}} [w]_{\Phi_1}$ i $\mathcal{L} = \bigcup_{w \in \mathcal{L}} [w]_{\Phi_2}$. Si considerem ara la congruència $\Phi_1 \cap \Phi_2$, sabem que és una congruència d'índex finit per (2.33). Ara anem a demostrar que $\mathcal{K} \cap \mathcal{L}$ està saturat per a $\Phi_1 \cap \Phi_2$, és a dir, hem de demostrar

$$\mathcal{K} \cap \mathcal{L} = \bigcup_{w \in \mathcal{K} \cap \mathcal{L}} [w]_{\Phi_1 \cap \Phi_2}.$$

Com sempre només hem de comprovar una inclusió ja que l'altra és evident. Siga $u \in \mathcal{K} \cap \mathcal{L}$ i $v \in A^*$ de manera que $(u, v) \in \Phi_1 \cap \Phi_2$ volem vore que $v \in \mathcal{K} \cap \mathcal{L}$. Com $(u, v) \in \Phi_1 \cap \Phi_2$, aleshores $(u, v) \in \phi_1$ i $(u, v) \in \phi_2$. Com que $(u, v) \in \Phi_1$ i $u \in \mathcal{K}$, i $(u, v) \in \Phi_2$ i $u \in \mathcal{L}$ tenim que:

$$v \in [u]_{\Phi_1} \subseteq \bigcup_{w \in \mathcal{K}} [w]_{\Phi_1} = \mathcal{K} \quad \text{i} \quad v \in [u]_{\Phi_2} \subseteq \bigcup_{w \in \mathcal{L}} [w]_{\Phi_2} = \mathcal{L}.$$

Així $v \in \mathcal{K} \cap \mathcal{L}$ i ja tenim que $\mathcal{K} \cap \mathcal{L} = \bigcup_{w \in \mathcal{K} \cap \mathcal{L}} [w]_{\Phi_1 \cap \Phi_2}$. Aplicant (3.12) ja hem demostrat que $\mathcal{K} \cap \mathcal{L}$ és un llenguatge reconeixible. ■

Proposició 3.14. *Si tenim $\mathcal{K}, \mathcal{L} \subseteq A^*$ dos llenguatges reconeixibles, aleshores $\mathcal{K} \cup \mathcal{L}$ també és un llenguatge reconeixible.*

Demostració. Autòmates.

Per a la primera demostració, suposem que $\mathcal{K}, \mathcal{L}$ són dos llenguatges reconeixibles de A^* , aleshores tenim dos autòmates $\mathbf{X} = (X, \alpha, I, O)$, $\mathbf{X}' = (X', \alpha', I', O')$ que els reconeixen, respectivament. Considerem l'autòmata $\mathbf{Y} = (X \cup X', \beta, I \cup I', O \cup O')$ on tenim que és finit per ser X i X' finits i β és l'aplicació de transicions que definim de la següent manera:

$$\begin{array}{lll} \beta: A & \longrightarrow & X \cup X'^{X \cup X'} \\ a & \longmapsto & \beta(a): \quad X \cup X' \longrightarrow X \cup X' \\ & & x \longmapsto \begin{cases} \alpha(a)(x) & \text{si } x \in X, \\ \alpha'(a)(x) & \text{si } x \in X'. \end{cases} \end{array}$$

Aleshores **Y** reconeix clarament a $\mathcal{K} \cup \mathcal{L}$ i per tant tenim que $\mathcal{K} \cup \mathcal{L}$ és un llenguatge reconeixible.

Congruències.

Per a la segon demostració considerem ara la congruència $\Phi_1 \cap \Phi_2$ atra volta, sabem que és una congruència d'índex finit, vorem que també satura a $\mathcal{K} \cup \mathcal{L}$. Hem de demostrar

$$\mathcal{K} \cup \mathcal{L} = \bigcup_{w \in \mathcal{K} \cup \mathcal{L}} [w]_{\Phi_1 \cap \Phi_2}.$$

Com sempre només hem de comprovar una inclusió ja que l'altra és evident. Siga $u \in \mathcal{K} \cup \mathcal{L}$ i $v \in A^*$ de manera que $(u, v) \in \Phi_1 \cap \Phi_2$ volem vore que $v \in \mathcal{K} \cup \mathcal{L}$. Ara com $u \in \mathcal{K} \cup \mathcal{L}$, suposem primer que $u \in \mathcal{K}$, com $(u, v) \in \Phi_1 \cap \Phi_2$, aleshores $(u, v) \in \Phi_1$ i així

$$v \in [u]_{\Phi_1} \subseteq \bigcup_{w \in \mathcal{K}} [w]_{\Phi_1} = \mathcal{K} \subseteq \mathcal{K} \cup \mathcal{L}.$$

Ara suposem que $u \in \mathcal{L}$, com $(u, v) \in \Phi_1 \cap \Phi_2$, aleshores $(u, v) \in \Phi_2$ i així

$$v \in [u]_{\Phi_2} \subseteq \bigcup_{w \in \mathcal{L}} [w]_{\Phi_2} = \mathcal{L} \subseteq \mathcal{K} \cup \mathcal{L}.$$

En qualsevol cas tenim que $v \in \mathcal{K} \cup \mathcal{L}$ i ja tenim que $\mathcal{K} \cup \mathcal{L} = \bigcup_{w \in \mathcal{K} \cup \mathcal{L}} [w]_{\Phi_1 \cap \Phi_2}$. Aplicant (3.12) ja hem demostrat que $\mathcal{K} \cup \mathcal{L}$ és un llenguatge reconeixible. ■

Proposició 3.15. *Si tenim $\mathcal{L} \subseteq A^*$ un llenguatge reconeixible, aleshores el llenguatge complementari $A^* - \mathcal{L}$ també és reconeixible.*

Demostració. Autòmats.

Per a la primera demostració, suposem que $\mathcal{L}$ és un llenguatge reconeixible de A^* , aleshores tenim un autòmata $\mathbf{X} = (X, \alpha, I, O)$ que reconeix aquest llenguatge. Considerem ara l'autòmata $\mathbf{Y} = (X, \alpha, I, A^* - O)$, al qual li hem canviat solament el conjunt d'estats finals pel seu complement en A^* .

Volem vore que $A^* - \mathcal{L} = \mathcal{L}_{\mathbf{Y}}$, per tant si tenim que $w \in \mathcal{L}_{\mathbf{Y}}$ com podem suposar que l'autòmata $\mathbf{Y}$ és determinista per (3.7) i així $I = \{x\}$ només té un element i $x_w \in A^* - O$, per tant $w \notin \mathcal{L}$ i així $w \in A^* - \mathcal{L}$. Notem que per a tindre l'altra inclusió és el mateix argument. En conclusió, $\mathcal{L}_{\mathbf{Y}} = \mathcal{K} \cap \mathcal{L}$ i per tant $\mathcal{K} \cap \mathcal{L}$ és un llenguatge reconeixible.

Congruències.

Per a la segona demostració, suposem que $\mathcal{L}$ és un llenguatge reconeixible de A^* , aleshores pel teorema (3.12) tenim que existeix Φ congruència d'índex finit de A^* de manera que $\mathcal{L} = \bigcup_{w \in \mathcal{L}} [w]_{\Phi}$. Ara anem a vore que $A^* - \mathcal{L}$ està saturat per a la mateixa congruència, és a dir, hem de demostrar $A^* - \mathcal{L} = \bigcup_{w \in A^* - \mathcal{L}} [w]_{\Phi}$.

Com sempre només hem de comprovar una inclusió ja que l'altra és evident. Siga $v \in A^* - \mathcal{L}$ volem vore que $[v]_\Phi \subseteq A^* - \mathcal{L}$. Siga $u \in [v]_\Phi$, suposem per reducció a l'absurd que $u \in \mathcal{L}$. Com el llenguatge $\mathcal{L}$ està saturat per a Φ , aleshores $[u]_\Phi \subseteq \mathcal{L}$ i així com $(u, v) \in \Phi$, tenim que $v \in [v]_\Phi \subseteq \mathcal{L}$, cosa que ens crea la contradicció ja que $v \in A^* - \mathcal{L}$ i per tant $[v]_\Phi \subseteq A^* - \mathcal{L}$ i ja tenim que $A^* - \mathcal{L} = \bigcup_{w \in A^* - \mathcal{L}} [w]_\Phi$. Aplicant (3.12) ja hem demostrat que $A^* - \mathcal{L}$ és un llenguatge reconeixible. ■

Definició 3.16. Si tenim $\mathcal{K}, \mathcal{L} \subseteq A^*$ dos llenguatges, definim la *concatenació de dos llenguatges* de la següent manera:

$$\mathcal{KL} = \{kl \mid k \in \mathcal{K} \text{ i } l \in \mathcal{L}\}.$$

Proposició 3.17. Si tenim $\mathcal{K}, \mathcal{L} \subseteq A^*$ dos llenguatges reconeixibles, aleshores la concatenació $\mathcal{KL}$ també és un llenguatge reconeixible.

Demostració. Autòmats.

Per a la primera demostració, suposem que $\mathcal{K}, \mathcal{L}$ són dos llenguatges reconeixibles de A^* , aleshores tenim dos autòmats $\mathbf{X} = (X, \alpha, I, O)$, $\mathbf{X}' = (X', \alpha', I', O')$ que els reconeixen, respectivament. Per la proposició (3.7) podem suposar que $\mathbf{X}$ i $\mathbf{X}'$ són dos autòmats deterministes, així $I = \{x\}$, $I' = \{x'\}$ i podem suposar també que X i X' són conjunts disjunts. Considerem l'autòmata $\mathbf{Y} = (X \cup X', \beta, I, O')$ de tal manera que ara el conjunt d'estats és la unió dels dos conjunts dels anteriors autòmats, que continua sent un conjunt finit, el conjunt d'estats inicials és de l'autòmata que reconeix $\mathcal{K}$ i el conjunt d'estats finals és el de l'autòmata que reconeix $\mathcal{L}$ i β és l'aplicació de transicions que, donat $a \in A$ tenim que $\beta(a)(x) = \alpha(a)(x)$ si $x \in X$, $\beta(a)(x) = \alpha'(a)(x)$ si $x \in X'$ i $\beta(\lambda)(x) = \{x\} \cup I'$ per a tot $x \in O$. Aleshores tenim que $\mathbf{Y}$ és un autòmata no determinista amb transicions buides. Anem a vore ara que $\mathcal{L}_\mathbf{Y} = \mathcal{L}$. Siga $w \in \mathcal{L}_\mathbf{Y}$ tenim que existeix $x \in I$ de manera que $x_w \cap O' \neq \emptyset$, aleshores $w = ulv$ per a $u \in \mathcal{L}_\mathbf{X} = \mathcal{K}$ i $v \in \mathcal{L}_{\mathbf{X}'} = \mathcal{L}$ i per tant $w \in \mathcal{KL}$. Ara si tenim una paraula $w \in \mathcal{KL}$, aleshores existeixen $k \in \mathcal{K}$ i $l \in \mathcal{L}$ de manera que $w = kl$. Així, per una part com $\mathcal{K} = \mathcal{L}_\mathbf{X}$, tenim que $x_k \in O$ i per altra part, com $\mathcal{L} = \mathcal{L}_{\mathbf{X}'}$, tenim que $x'_l \in O'$. Notem que $\beta(\lambda)(x_k) = \{x_k, x'\}$, aleshores $x_{kl} \cap O' \neq \emptyset$ i així tenim ja que $w = kl \in \mathcal{L}_\mathbf{Y}$. En conclusió tenim que $\mathcal{L}_\mathbf{Y} = \mathcal{L}$ i per tant $\mathcal{KL}$ és un llenguatge reconeixible.

Congruències.

Per a la segona demostració, suposem que $\mathcal{K}, \mathcal{L}$ són dos llenguatges reconeixibles de A^* , aleshores pel teorema (3.12) tenim que existeixen Φ_1, Φ_2 congruències d'índex finit de A^* de manera que $\mathcal{K}$ i $\mathcal{L}$ són dos llenguatges saturats per a Φ_1 i Φ_2 respectivament, és a dir, $\mathcal{K} = \bigcup_{w \in \mathcal{K}} [w]_{\Phi_1}$ i $\mathcal{L} = \bigcup_{w \in \mathcal{L}} [w]_{\Phi_2}$. Si prenem la congruència $\Phi = \Phi_1 \cap \Phi_2$, sabem que és una congruència d'índex finit, de manera que $|A^*/\Phi| = p$. Com Φ_1 té índex finit, siguen $\{u_0^1, \dots, u_n^1\}$ un conjunt de transversals per a Φ_1 i com Φ_2 també té índex finit, siguen $\{u_0^2, \dots, u_m^2\}$ un conjunt de transversals per a Φ_2 . Anem a considerar un refinament de Φ que anomenarem Ψ de manera que $(w, v) \in \Psi$ si:

1. $(w, v) \in \Phi$;
2. Si $\forall i \in n$ i $\forall j \in m$ tenim que $w \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$ si i només si $v \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$.

Notem que $\Psi \subseteq \Phi$, però anem a vore si Ψ continua sent d'índex finit, per contra aquest refinament no ens servirà. El que fem en aquest refinament es que dins de cada classe $[w]_{\Phi}$, que hi ha p , hem de vore si w està en $[u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$ per a cada $i \in n$ i $j \in m$, però pot ser que diferents productes siguin iguals, és a dir, que $[u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2} = [u_k^1]_{\Phi_1}[u_l^2]_{\Phi_2}$ per a $i \neq k$ i $j \neq l$. En qualsevol cas el nombre de possibilitats està fitat per $p2^{mn}$, per tant $|A^*/\Psi|$ és finit.

Ens queda demostrar que Ψ és una congruència i que $\mathcal{KL}$ està saturat per a Ψ . Primer vorem que Ψ és una relació d'equivalència, com Φ compleix ser relació d'equivalència només cal comprovar la segona condició. La propietat reflexiva es compleix clarament. Siguen $w, v, x \in A^*$, si $(w, v) \in \Psi$ també $(v, w) \in \Psi$, aleshores es compleix la propietat simètrica i per últim, si tenim que $(w, v), (v, x) \in \Psi$ aleshores per a qualsevol $i \in n$ i $j \in m$ $w \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$ si i només si $v \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$ si i només si $x \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$ i per tant $(w, x) \in \Psi$ complint així la propietat transitiva. Ja tenim que Ψ és relació d'equivalència.

Vore que és una congruència és un poc més complex. Si tenim $(w, v), (w', v') \in \Psi$ volem arribar a que $(ww', vv') \in \Psi$. La primer condició es compleix clarament per ser Φ una congruència.

Anem a vore que es compleix que $ww' \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$ si i només si $vv' \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$, només farem una implicació ja que l'altra es faria de manera anàloga. Siguen $i \in n$ i $j \in m$ suposem que $ww' \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$, aleshores existeixen $\tilde{u}_i^1 \in [u_i^1]_{\Phi_1}$ i $\tilde{u}_j^2 \in [u_j^2]_{\Phi_2}$ de manera que $ww' = \tilde{u}_i^1 \tilde{u}_j^2$. Una vegada tenim açò, anem a separar per casos, el primer cas seria si tenim $|w| < |\tilde{u}_i^1|$, el segon cas si $|w| = |\tilde{u}_i^1|$ i el tercer cas és en el que $|w| > |\tilde{u}_i^1|$.

Primer demostrarem el segon cas que és el més fàcil dels tres. Si suposem que $|w| = |\tilde{u}_i^1|$ aleshores $w = \tilde{u}_i^1$ i $w' = \tilde{u}_j^2$ i per tant $w \in [u_i^1]_{\Phi_1}$ i $w' \in [u_j^2]_{\Phi_2}$. Com $(w, v) \in \Phi \subseteq \Phi_1$ i $(w', v') \in \Phi \subseteq \Phi_2$, per la propietat transitiva de Φ_1 i Φ_2 tenim que $v \in [u_i^1]_{\Phi_1}$ i que $v' \in [u_j^2]_{\Phi_2}$. Concloem que $vv' \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$.

Notem que el primer cas i el tercer són simètrics, per tant només cal fer la demostració d'un cas. Volem vore en quina classe d'equivalència estan v i v' . Suposem sense pèrdua de generalitat que $|w| < |\tilde{u}_i^1|$ per tant notem l'existència d'una paraula $u \in A^*$ tal que $wu = \tilde{u}_i^1$ i $u\tilde{u}_j^2 = w'$. Adonem-nos de que $w' = u\tilde{u}_j^2 \in [u]_{\Phi_1}[\tilde{u}_j^2]_{\Phi_2}$. Com $\{u_0^1, \dots, u_n^1\}$ és el conjunt de transversals de Φ_1 , aleshores existeix u_k^1 d'aquest conjunt de transversals de manera que $[u]_{\Phi_1} = [u_k^1]_{\Phi_1}$. Així $w' \in [u_k^1]_{\Phi_1}[u_j^2]_{\Phi_2}$ perquè $[\tilde{u}_j^2]_{\Phi_2} = [u_j^2]_{\Phi_2}$ i com $(w', v') \in \Psi$, tenim que $v' \in [u_k^1]_{\Phi_1}[u_j^2]_{\Phi_2}$. Per altra part com $(w, v) \in \Phi \subseteq \Phi_1$, aleshores $[v]_{\Phi_1} = [w]_{\Phi_1}$. Així tenim que $vv' \in [v]_{\Phi_1}[u_k^1]_{\Phi_1}[u_j^2]_{\Phi_2}$ però tenim que

$$\begin{aligned} [v]_{\Phi_1}[u_k^1]_{\Phi_1}[u_j^2]_{\Phi_2} &= [w]_{\Phi_1}[u]_{\Phi_1}[u_j^2]_{\Phi_2} \\ &= [wu]_{\Phi_1}[u_j^2]_{\Phi_2} \\ &= [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}. \end{aligned}$$

La segona igualtat la tenim per com funciona el producte de classes per a una congruència. D'aquesta manera tenim que $vv' \in [u_i^1]_{\Phi_1}[u_j^2]_{\Phi_2}$.

Per tant ara ja tenim que Ψ és una congruència en $\mathbf{A}^*$. Ara anem a veure que $\mathcal{KL}$ està saturat per Ψ . Com sempre, la inclusió $\mathcal{KL} \subseteq \bigcup_{x \in \mathcal{KL}} [x]_\Psi$ ja la tenim, ara ens queda veure l'altra inclusió.

Siga $x \in \mathcal{KL}$, aleshores existeixen $w \in \mathcal{K}$ i $v \in \mathcal{L}$ de manera que $x = wv$. Siga $y \in [x]_\Psi$, prenem u_k^1 un element del transversal $\{u_0^1, \dots, u_n^1\}$ per al qual $[w]_{\Phi_1} = [u_k^1]_{\Phi_1}$ i u_l^2 un element del transversal $\{u_0^2, \dots, u_m^2\}$ per al qual $[v]_{\Phi_2} = [u_l^2]_{\Phi_2}$, aleshores com $x = wv$ tenim que $x \in [u_k^1]_{\Phi_1} [u_l^2]_{\Phi_2}$. Com que $(x, y) \in \Psi$, deduïm que $y \in [u_k^1]_{\Phi_1} [u_l^2]_{\Phi_2}$ i notem que $[u_k^1]_{\Phi_1} [u_l^2]_{\Phi_2} \subseteq \mathcal{KL}$ perquè, per un costat tenim $w \in \mathcal{K}$, $[w]_{\Phi_1} = [u_k^1]_{\Phi_1}$ i $\mathcal{K}$ està saturat per a Φ_1 , per tant $[u_k^1]_{\Phi_1} \subseteq \mathcal{K}$ i per altra part tenim que $v \in \mathcal{L}$, $[v]_{\Phi_2} = [u_l^2]_{\Phi_2}$ i $\mathcal{L}$ està saturat per a Φ_2 , i per tant $[u_l^2]_{\Phi_2} \subseteq \mathcal{L}$. Podem concloure que $y \in \mathcal{KL}$ i per tant ja tenim que $\mathcal{KL}$ està saturat per a Ψ . Aplicant el teorema (3.12) tenim que $\mathcal{KL}$ és un llenguatge reconeixible. ■

Una vegada ja hem demostrat aquest resultat des dels dos punts de vista podem destacar que en els tres primers resultats, (3.13), (3.14) i (3.15) tenim que tant la demostració per autòmats com la demostració emprant congruències d'índex finit no generaven gran dificultat ja que no eren idees de les demostracions no eren molt i les congruències que empràvem eren congruències ja conegudes i estudiades en la secció anterior. No obstant, per a la demostració de la proposició (3.17), la demostració per autòmats tenia una idea molt assequible, ja que feiem la unió dels dos autòmats amb una transició buida però per a la demostració emprant congruències d'índex finit era necessària una idea un poc més elaborada, era necessari fer un refinament de la intersecció de les dos congruències, cosa que complica un poc més la demostració.

Així hem vist que en alguns casos resulta més fàcil gastar autòmats i en altres gastar congruències d'índex finit. Destaquem la importància del teorema de Mhyhill-Nerodes (3.12) ja que ens dona la possibilitat d'emprar qualsevol de les dos eines per fer veure propietats de llenguatges reconeixibles.

Capítol 4

Congruències d'índex finit sobre $\mathbb{N}$

Una vegada hem vist resultats generals sobre monoides i autòmats, i com els hem relacionat entre ells, anem a estudiar un cas particular, el monoide dels nombres naturals, que com ja hem vist en (2.49) és isomorf a el monoide lliure d'un generador .

El que anem a fer és caracteritzar com són totes les congruències d'índex finit que podem fer sobre el monoide dels nombres naturals, així com les possibles operacions entre congruències que ja hem definit abans en el capítol de preliminars.

4.1 Introducció i exemples

En aquesta secció vorem exemples de congruències que podem fer sobre el monoide de nombres naturals. La nostra intenció més avant serà amb aquesta informació extraure quina podria ser la forma de les congruències d'índex finit sobre els naturals que estem buscant.

Exemple 4.1.

1. Siga $n \in \mathbb{N}$ considerem la següent família de relacions en $\mathbb{N}$:

$$\Phi_n = \Delta_{\mathbb{N}} \cup \{(p, q) \in \mathbb{N} \times \mathbb{N} \mid p, q \geq n\}.$$

Anem a vore primer que Φ_n és un relació d'equivalència. La propietat reflexiva, la simètrica i la transitiva és compleixen clarament ja que tenim per una part la diagonal en $\mathbb{N}$ i l'altra component tenim que tots els elements estàn relacionats en tots a partir de n .

Ens queda vore que Φ_n és una congruència. Prenem dos parells de la relació, $(a, b)(c, d) \in \Phi_n$ volem vore que efectivament $(a + c, b + d) \in \Phi_n$. Anem a separar per casos.

Primer si suposem que $a = b$ i $c = d$ aleshores tenim que $(a + c, b + d) \in \Phi_n$ per la propietat reflexiva de Φ_n .

Ara si suposem $a = b$ i $c, d \geq n$ aleshores $a + c, b + d \geq n$ i per tant $(a + c, b + d) \in \Phi_n$. Notem que si suposem que $c = d$ i $a, b \geq n$ el cas és el mateix i es fa servir el mateix argument.

Per últim si suposem que $a, b, c, d \geq n$ aleshores també tenim que $(a+c, b+d) \in \Phi_n$ perquè $a+c \geq n$ i $b+d \geq n$.

En qualsevol cas tenim que $(a+c, b+d) \in \Phi_n$ aleshores podem concloure que Φ_n és una congruència en $\mathbf{N}$.

D'aquesta manera, com que Φ_n és una congruència en $\mathbf{N}$, tenim que el monoide quocient $\mathbf{N}/\Phi_n$ ens dona un nombre finit de classes d'equivalència, $n+1$ per a ser exactes.

Amb aquesta congruència Φ_n tenim la següent representació del conjunt quocient:

$$[0] \longrightarrow [1] \longrightarrow \dots \longrightarrow [n-1] \longrightarrow [n] \bigcup$$

Cada fletxa indica el successor de cada element de la classe.

2. Siga $r \in \mathbf{N}^*$, considerem la família de relacions en $\mathbf{N}$:

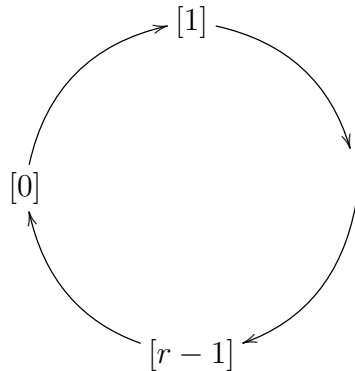
$$\Psi_r = \{(a, b) \in \mathbf{N} \times \mathbf{N} \mid a \equiv b \pmod{r}\}.$$

Anem a veure que Ψ_r és una relació d'equivalència. La propietat reflexiva es compleix clarament. Si tenim $a, b, c \in \mathbf{N}$ de manera que $(a, b) \in \Psi_r$ tenim que $a - b = kr$ per a algun $k \in \mathbf{Z}$, i per tant tenim que $b - a = -kr = k'r$ i $k' \in \mathbf{Z}$, per tant $(b, a) \in \Psi_r$ i així es compleix la propietat reflexiva. I per a la propietat transitiva, si tenim que $(a, b), (b, c) \in \Psi_r$, tenim que $a \equiv b \pmod{r}$ i $b \equiv c \pmod{r}$, és a dir que $a - b = kr$ i $b - c = lr$ per a $k, l \in \mathbf{Z}$, aleshores $a - c = kr + lr = (k+l)r$ i $k+l \in \mathbf{Z}$, per tant $a \equiv c \pmod{r}$ i $(a, c) \in \Psi_r$.

Ens queda veure que Ψ_r és una congruència. Prenem dos parells de la relació, $(a, b), (c, d) \in \Psi_r$, i volem veure si $(a+c, b+d) \in \Psi_r$. Com $(a, b), (c, d) \in \Psi_r$ tenim que $a - b = pr$ i $c - d = qr$ per a $p, q \in \mathbf{Z}$ aleshores obtenim que $a+c - (b+d) = a-b + c-d = pr + qr = (p+q)r$. Per tant $(a+c, b+d) \in \Psi_r$ i ja tenim que Ψ_r és una congruència.

D'aquesta manera, com que Ψ_r és una congruència en $\mathbf{N}$, tenim que el monoide quocient $\mathbf{N}/\Psi_r$ ens dona un nombre finit de classes d'equivalència, r per a ser exactes.

Amb aquesta congruència Φ_n tenim la següent representació del conjunt quocient, que és isomorf a un grup cíclic d'ordre r :



3. Ara anem a considerar una generalització de les dos famílies, Φ_n i Ψ_r per a $(n, r) \in \mathbb{N} \times \mathbb{N}^*$, que denotarem de la següent manera:

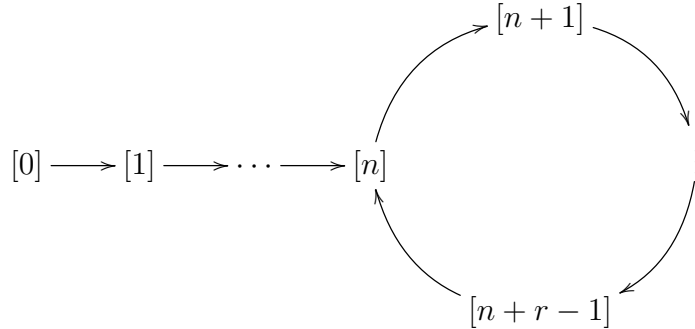
$$\Theta_{n,r} = \Delta_{\mathbb{N}} \cup \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a, b \geq n \text{ i } a \equiv b \pmod{r}\}$$

Aquest conjunt de relacions, $\Theta_{n,r}$ és relació d'equivalència com hem provat ja en els anteriors dos exemples.

Només ens queda veure que es tracta d'una congruència. Suposem que tenim $a, b, c, d \in \mathbb{N}$ de manera que $(a, b), (c, d) \in \Theta_{n,r}$. Anem a separar per casos. Si suposem que $a = b, c = d$, aleshores per la propietat reflexiva de $\Theta_{n,r}$ tenim que $(a + c, b + d) \in \Theta_{n,r}$. Si ara suposem que $a = b$ i $c, d \geq n$ de manera que $c \equiv d \pmod{r}$ aleshores $a + c - (b + d) = a + c - a - d = c - d$, per tant $a + c \equiv b + d \pmod{r}$ i així $(a + c, b + d) \in \Theta_{n,r}$. Si suposem $a, b \geq n$ de manera que $a \equiv b \pmod{r}$ i $c = d$, estem en el mateix cas que abans i farem el mateix argument. Per últim, si suposem ara que $a, b, c, d \geq n$ de manera que $a \equiv b \pmod{r}$ i $c \equiv d \pmod{r}$, tenim que $r \mid (a - b)$ i $r \mid (c - d)$. Per tant, $r \mid (a + c - b - d)$, i així tenim que $(a + c, b + d) \in \Theta_{n,r}$. Aleshores ja hem demostrat que $\Theta_{n,r}$ és una congruència.

D'aquesta manera, com que $\Theta_{n,r}$ és una congruència en $\mathbb{N}$, tenim que el monoide quocient $\mathbb{N}/\Theta_{n,r}$ ens dona un nombre finit de classes d'equivalència, $n + r$ per a ser exactes.

Amb aquesta congruència $\Theta_{n,r}$ tenim el següent diagrama del conjunt quocient:



4.2 Caracterització de les congruències d'índex finit en $\mathbb{N}$

En aquesta secció anem a demostrar quina serà la forma que han de tindre les congruències d'índex finit i una sèrie de resultats previs que farem servir per a que la demostració del teorema siga més entensible.

Siga $\varphi \in \text{Con}_f(\mathbb{N})$, com $\mathbb{N}$ és infinit i $\mathbb{N}/\varphi$ és finit, l'aplicació $\text{pr}_\varphi : \mathbb{N} \longrightarrow \mathbb{N}/\varphi$ que a cada natural a li fa correspondre $\text{pr}_\varphi(a) = [a]_\varphi$ no és injectiva. Aleshores existeixen $a, b \in \mathbb{N}$ de manera que $a \neq b$ però $[a]_\varphi = [b]_\varphi$. Per tant existeixen naturals que estàn relacionats respecte φ amb més naturals a part d'ells mateixa.

Definició 4.2. Siga $\varphi \in \text{Con}_{\text{if}}(\mathbf{N})$ definim el següent conjunt:

$$L_\varphi = \{a \in \mathbb{N} \mid [a]_\varphi \text{ té més d'un element}\}.$$

Aquest conjunt és el conjunt que conté els elements de $\mathbb{N}$ que tinguen més d'un element relacionats amb ells respecte de Φ .

Com el conjunt de nombres naturals és un conjunt ben ordenat, aleshores existeix $n = \min(L_\varphi)$.

Proposició 4.3. Considerant el monoide $\mathbf{N}$ i $\varphi \in \text{Con}_{\text{if}}(\mathbf{N})$, aleshores si $n = \min(L_\varphi)$, llavors $L_\varphi = \{a \in \mathbb{N} \mid a \geq n\}$.

Demostració. La inclusió cap a la dreta ($\subseteq$) és clara en ser $n = \min(L_\varphi)$.

Ara, com sabem que $n \in L_\varphi$, aleshores sabem que $[n]_\varphi$ té més d'un element, i com n és el mínim de L_φ , sabem que existeix un natural $m \neq n$, així $m > n$, de manera que $[m]_\varphi = [n]_\varphi$.

Ara si $l \in \mathbb{N}$ qualsevol tal que $l \geq n$, volem vore que $[l]_\varphi$ té més d'un element. Com $l \geq n$, podem considerar que $l = n + k$ per a algun $k \in \mathbb{N}$. Sabem que $(n, m) \in \varphi$ i també $(k, k) \in \varphi$ per la propietat reflexiva de φ , aleshores $(n + k, m + k) \in \varphi$ també per ser φ una congruència en $\mathbb{N}$. Per tant, $[n + k]_\varphi = [m + k]_\varphi$ i així ja tenim que per a qualsevol $l \geq n$, $[l]_\varphi$ té més d'un element.

Aleshores tenim $L_\varphi = \{a \in \mathbb{N} \mid [a]_\varphi \text{ té més d'un element}\} = \{a \in \mathbb{N} \mid a \geq n\}$. ■

Definició 4.4. Siga $\varphi \in \text{Con}_{\text{if}}(\mathbf{N})$ definim el següent conjunt:

$$M_n = \{b \in \mathbb{N}^* \mid [n + b]_\varphi = [n]_\varphi\}.$$

Notem que M és no buit ja que com hem vist en la demostració de la proposició (4.3) tenim que existeix un natural $m > n = \min(L_\varphi)$ de manera que $[m]_\varphi = [n]_\varphi$ i així podem prendre $b = m - n \in \mathbb{N}^*$ i d'aquesta manera tenim que $[n + b]_\varphi = [m]_\varphi = [n]_\varphi$ i $b \in M$.

Denotem per $r = \min(M)$ i així $[n + r]_\varphi = [n]_\varphi$.

Siga $a \in L_\varphi$ podem considerar la següent família:

$$M_a = \{b \in \mathbb{N}^* \mid [a + b]_\varphi = [a]_\varphi\}.$$

En aquest cas denotem per $r_a = \min(M_a)$. Notem que $r = \min(M_n)$

Ara demostrarem una sèrie de lemes a propòsit d'aquestes definicions que farem servir més endavant en el teorema de caracterització.

Lema 4.5. Siga $\varphi \in \text{Con}_{\text{if}}(\mathbf{N})$. Si prenem $a \in L_\varphi$ i $b \in M_a$, aleshores tenim que $(a, a + kb) \in \varphi$ per a qualsevol $k \in \mathbb{N}$.

Demostració. Com tenim que $b \in M_a$ aleshores sabem per la definició de M_a que $(a, a + b) \in \varphi$. Ara per la propietat reflexiva de φ tenim que $(b, b) \in \varphi$ i com que φ és una congruència tenim que $(a + b, a + 2b) \in \varphi$. Per la propietat transitiva de φ arribem a que $(a, a + 2b) \in \varphi$ també. Si continuem fent aquest procés repetidamet obtenim que $(a, a + kb) \in \varphi$ per a qualsevol $k \in \mathbb{N}$. ■

Notem que $(a, a + kr_a), (a, a + kr), (n, n + kr) \in \varphi$ també, ja que són cassos particulars del lema (4.5).

Lema 4.6. *Siga $\varphi \in \text{Con}_{\text{if}}(\mathbf{N})$. Si prenem $a \in L_\varphi$ i $b \in M_a$, aleshores tenim que $r_a \mid b$. En particular si $b \in M$, tenim que $r \mid b$.*

Demostració. Per ser $r_a = \min(M_a)$ tenim que $r_a \leq b$ per tant podem considerar que $b = pr_a + z$ amb $0 \leq z < r_a$ i $p \in \mathbf{N}$.

Com volem vore que $r_a \mid b$, anem a provar que $z = 0$. Anem a provar-ho per reducció a l'absurd, per tant suposem que $z \neq 0$. Per una part tenim que com $b \in M_a$ aleshores $(a, a + b) \in \varphi$ i per altra, pel lema (4.5) tenim que $(a, a + pr_a) \in \varphi$ i per la propietat reflexiva de φ tenim també que $(z, z) \in \varphi$, per tant, com φ és una congruència, es té que $(a + z, a + b) \in \varphi$. Per la propietat transitiva de φ obtenim que $(a, a + z) \in \varphi$, és a dir, que $z \in M_a$, però com $z < r_a$ seria una contradicció ja que $r_a = \min(M_a)$. Aleshores ja tenim que $z = 0$ i podem concloure que $r_a \mid b$ en ser $b = pr_a$ per a un $p \in \mathbf{N}$. ■

Corol·lari 4.7. *Siga $\varphi \in \text{Con}_{\text{if}}(\mathbf{N})$. Considerem dos naturals $a, a' \in L_\varphi$ tal que $a < a'$, aleshores tenim que $r_{a'} \mid r_a$.*

Demostració. Volem vore que $r_a \in M_{a'}$ perquè d'aquesta manera aplicant el lema (4.6) tindrem que $r_{a'} \mid r_a$. Com $a < a'$, podem suposar que $a' = a + l$ per a $l \in \mathbf{N}$. Aleshores per una part tenim que $(a, a + r_a) \in \varphi$ degut a que $r_a \in M_a$ i per altra part, $(l, l) \in \varphi$ per la propietat reflexiva de φ . Per tant, com que φ és una congruència, tenim que $(a + l, a + l + r_a) \in \varphi$ i com que $a + l = a'$ apleguem a que $(a', a' + r_a) \in \varphi$. En conclusió obtenim que $r_a \in M_{a'}$ i pel lema (4.6) ja tenim que $r_{a'} \mid r_a$. ■

Corol·lari 4.8. *Siga $\varphi \in \text{Con}_{\text{if}}(\mathbf{N})$, aleshores es té que $r_a = r$ per a tot $a \in L$.*

Demostració. Primer que tot, com $n < a$, si apliquem el corol·lari (4.7) tenim que $r_a \mid r$. Ara per a vore que $r_a = r$ sols és necessari vore que $r \mid r_a$.

Com que $n \leq a$ perquè $a \in L_\varphi$ i $n = \min(L_\varphi)$, aleshores existeix algun natural p de manera que $a < n + pr$, i pel corol·lari (4.7) altra volta tenim que $r_{n+pr} \mid r_a$. Ara el que anem a provar és que $r \mid r_{n+pr}$.

Per una part ara tenim que $(n + pr, n + pr + r_{n+pr}) \in \varphi$ per la definició de M_{n+pr} i per altra part tenim que $(n, n + pr) \in \varphi$ en ser un cas particular del lema (4.5) com havíem dit en la nota posterior, aleshores per la propietat transitiva de φ tenim que $(n, n + pr + r_{n+pr}) \in \varphi$ i pel lema (4.6) podem dir que $r \mid pr + r_{n+pr}$ i per tant $r \mid r_{n+pr}$. En conclusió obtenim que $r \mid r_a$ i així $r = r_a$ per a qualsevol $a \in L_\varphi$. ■

Nota 4.9. Notem que d'aquests resultats obtenim el següent resultat:

$$\varphi \in \text{Con}_{\text{if}}(\mathbf{N}), \quad a \in L_\varphi, \quad b \in M_a \implies r \mid b$$

Ara anem a demostrar el resultat més rellevant d'aquest capítol amb l'ajuda dels lemes i corol·laris que acabem de demostrar. Aquest resultat caracteritza totes les congruències d'índex finit del monoide del nombres naturals.

Teorema 4.10. *Si tenim el monoide $\mathbf{N} = (\mathbb{N}, +, 0)$ totes les congruències d'índex finit en $\mathbf{N}$ són els elements de la família de congruències següent:*

$$\Theta_{n,r} = \Delta_{\mathbb{N}} \cup \{(p, q) \mid p, q \geq n \text{ i } p \equiv q \pmod{r}\} \quad n \in \mathbb{N}, \quad r \in \mathbb{N}^*.$$

Demostració. Siga $\varphi \in \text{Con}_{\text{if}}(\mathbf{N})$ volem vore que existeixen $n \in \mathbb{N}$, $r \in \mathbb{N}^*$ de manera que $\varphi = \Theta_{n,r}$.

Siga $(a, b) \in \varphi$, si $a < n$ aleshores $a \notin L_{\varphi}$ i per tant $[a]_{\varphi}$ només té un element. Així que $b = a$ i podem concloure que $(a, b) \in \Theta_{n,r}$.

Anem al cas $a, b \geq n$ i $a \neq b$, aleshores $a, b \in L_{\varphi}$ i les classes d'equivalència $[a]_{\varphi} = [b]_{\varphi}$ tenen més d'un element. Podem suposar sense pèrdua de generalitat que $a < b$, aleshores prenem $b = a + c$ per a algún $c \in \mathbb{N}$. Com $(a, b) \in \varphi$ també tenim que $(a, a + c) \in \varphi$, cosa que ens diu que $c \in M_a$ i ara pel lema (4.6) i el corol·lari (4.8) tenim que $r \mid c = b - a$. En conclusió obtenim que $a \equiv b \pmod{r}$ i així $(a, b) \in \Theta_{n,r}$. Ja tenim que $\varphi \subseteq \Theta_{n,r}$, ara ens falta l'altra inclusió.

Si tenim el parell $(a, b) \in \Theta_{n,r}$, podem suposar que $a \neq b$, en cas contrari ja tindriem $(a, b) \in \varphi$. Com $a \neq b$ sabem que $a, b \geq n$ i per tant $a \in L_{\varphi}$. També sabem que $a \equiv b \pmod{r}$, per tant $b - a = kr$. Així tenim que, pel lema (4.5) i el corol·lari (4.8) el parell $(a, a + kr) \in \varphi$ i com tenim que $b = a + kr$ ens queda que $\Theta_{n,r} \subseteq \varphi$. D'aquesta manera ja queda provat que $\varphi = \Theta_{n,r}$. ■

4.3 Operacions en congruències d'índex finit

Proposició 4.11. *Si tenim $\Theta_{n_1,r_1}, \Theta_{n_2,r_2} \in \text{Con}_{\text{if}}(\mathbf{N})$, aleshores les següents afirmacions són equivalents:*

1. $\Theta_{n_1,r_1} \subseteq \Theta_{n_2,r_2}$.
2. $n_2 \leq n_1$ i $r_2 \mid r_1$.

Demostració. Primer anem a vore que 2. implica 1., per tant suposem que $n_2 \leq n_1$ i $r_2 \mid r_1$. Siga $(a, b) \in \Theta_{n_1,r_1}$, si $a = b$ aleshores $(a, b) \in \Theta_{n_2,r_2}$ per la propietat reflexiva de Θ_{n_2,r_2} . Ara podem suposar que $a \neq b$ aleshores sabem que $a, b \geq n_1$ i com que $n_2 \leq n_1$ tenim que $a, b \geq n_2$. Partim de la hipòtesi de que $r_2 \mid r_1$ per tant existeix un $l \in \mathbb{N}$ tal que $r_1 = lr_2$ i com que $a \equiv b \pmod{r_1}$ per ser $a, b \geq n_1$, aleshores $a - b = kr_1 = klr_2$ i així $a \equiv b \pmod{r_2}$.

En conclusió, tenint $(a, b) \in \Theta_{n_1,r_1}$ de manera que $a \neq b$ hem aplegat a que $a, b \geq n_2$ i que $a \equiv b \pmod{r_2}$ aleshores $\Theta_{n_1,r_1} \subseteq \Theta_{n_2,r_2}$.

Anem a veure ara que 1. implica 2., per tant suposem ara que $\Theta_{n_1, r_1} \subseteq \Theta_{n_2, r_2}$. Sabem que $(n_1, n_1 + r_1) \in \Theta_{n_1, r_1}$ pel lema (4.5) i aleshores $(n_1, n_1 + r_1) \in \Theta_{n_2, r_2}$ perquè $\Theta_{n_1, r_1} \subseteq \Theta_{n_2, r_2}$. Com $n_1 \neq n_1 + r_1$ perquè $r_1 \neq 0$, tenim que $n_1, n_1 + r_1 \geq n_2$ i així $n_2 \leq n_1$.

Per altra banda tenim que $n_1 \equiv n_1 + r_1 \pmod{r_2}$, per tant $n_1 + r_1 - n_1 = kr_2$, és a dir, $r_1 = kr_2$ i així tenim que $r_2 \mid r_1$.

En conclusió, tenint $\Theta_{n_1, r_1} \subseteq \Theta_{n_2, r_2}$ hem aplegat a que $n_2 \leq n_1$ i que $r_2 \mid r_1$. ■

Proposició 4.12. *Siguen $\Theta_{n_1, r_1}, \Theta_{n_2, r_2} \in \text{Con}_{\text{if}}(\mathbb{N})$ aleshores tenim que:*

$$\Theta_{n_1, r_1} \cap \Theta_{n_2, r_2} = \Theta_{\max(n_1, n_2), \text{mcm}(r_1, r_2)}$$

Demostració. Sabem que $\Theta_{n_1, r_1} \cap \Theta_{n_2, r_2} \in \text{Con}_{\text{if}}(\mathbb{N})$ per (2.39) volem veure que $\Theta_{n_1, r_1} \cap \Theta_{n_2, r_2} = \Theta_{n, r}$ on $n = \max(n_1, n_2)$ i $r = \text{mcm}(r_1, r_2)$.

Siga $(a, b) \in \Theta_{n_1, r_1} \cap \Theta_{n_2, r_2}$, si $a = b$, aleshores $(a, b) \in \Theta_{n, r}$ per la propietat reflexiva.

Suposem $a \neq b$ aleshores $a, b \geq n_1, n_2$ i per tant $a, b \geq \max(n_1, n_2)$.

També sabem que $a \equiv b \pmod{r_i}$, $i = 1, 2$, suposem sense pèrdua de generalitat que $b < a$, aleshores tenim que $r_i \mid a - b$, $i = 1, 2$ i per tant $r = \text{mcm}(r_1, r_2) \mid a - b$ i $a \equiv b \pmod{r}$. Així ja tenim que $(a, b) \in \Theta_{n, r}$.

Com $n_i \leq \max(n_1, n_2) = n$ i $r_i \mid \text{mcm}(r_1, r_2) = r$ per a $i = 1, 2$, aleshores per la proposició (4.11) tenim que $\Theta_{n_i, r_i} \subseteq \Theta_{n_1, r_1} \cap \Theta_{n_2, r_2}$ i podem concloure que $\Theta_{n, r} = \Theta_{n_1, r_1} \cap \Theta_{n_2, r_2}$. ■

Ara que ja sabem quina forma tenen les interseccions de congruències d'índex finit en el monoide dels nombres naturals anem a veure un contraexemple que ens demostra que les interseccions arbitràries de congruències d'índex finit no necessàriament ha de ser una congruència d'índex finit.

Exemple 4.13. *Si considerem el monoide dels nombres naturals anem a veure una intersecció infinita de congruències d'índex finit que ens dona una congruència que no té índex finit. Considerem la família de congruències d'índex finit $\{\Theta_{n, 1} \mid n \in \mathbb{N}\}$ anem a veure que $\bigcap_{n \in \mathbb{N}} \Theta_{n, 1} = \Delta_{\mathbb{N}}$. La inclusió $\bigcap_{n \in \mathbb{N}} \Theta_{n, 1} \supseteq \Delta_{\mathbb{N}}$ és clara ja que, com sabem per (2.33) la intersecció de congruències és una congruència. Ara per veure l'altra inclusió, només cal notar que siguen $(x, y) \in \bigcap_{n \in \mathbb{N}} \Theta_{n, 1}$ qualsevol, sempre existirà un $n' \in \mathbb{N}$ tal que $(x, y) \in \Theta_{n', 1}$ i $x, y \leq n'$, per tant $x = y$ i així $(x, y) \in \Delta_{\mathbb{N}}$. Aleshores ja tenim que $\bigcap_{n \in \mathbb{N}} \Theta_{n, 1} = \Delta_{\mathbb{N}}$.*

Com l'aplicació identitat $\text{id}_{\mathbb{N}}$ és un homomorfisme tal que $\text{Ker}(\text{id}_{\mathbb{N}}) = \Delta_{\mathbb{N}}$ aleshores per (2.45) tenim que $\mathbb{N}/\text{Ker}(\text{id}_{\mathbb{N}}) \cong \mathbb{N}$. Com que els nombres naturals són infinits, concloem que $\Delta_{\mathbb{N}}$ és una congruència que no té índex finit.

Proposició 4.14. *Siguen $\Theta_{n_1, r_1}, \Theta_{n_2, r_2} \in \text{Con}_{\text{if}}(\mathbb{N})$ aleshores tenim que:*

$$\Theta_{n_1, r_1} \vee \Theta_{n_2, r_2} = \Theta_{\min(n_1, n_2), \text{mcd}(r_1, r_2)}.$$

Demostració. Sabem que $\Theta_{n_1, r_1} \vee \Theta_{n_2, r_2} \in \text{Con}_{\text{if}}(\mathbb{N})$ per (2.41), i denotem $\Theta_{m, s} = \Theta_{n_1, r_1} \vee \Theta_{n_2, r_2}$. Com $\Theta_{n_i, r_i} \subseteq \Theta_{m, s}$ per a $i = 1, 2$, tenim que $m \leq n_i$ i $s \mid r_i$ per a $i = 1, 2$ per la proposició (4.11). Per tant $m \leq n'$ i $s \mid r'$ i així per la proposició (4.11) altra volta $\Theta_{n', r'} \subseteq \Theta_{n_1, r_1} \vee \Theta_{n_2, r_2}$.

Ara com $n' = \min(n_1, n_2) \leq n_i$ i $r' = \text{mcd}(r_1, r_2) \mid r_i$, per la proposició (4.11) tenim que $\Theta_{n_i, r_i} \subseteq \Theta_{n, r}$ per a $i = 1, 2$, aleshores $\Theta_{n_1, r_1} \cup \Theta_{n_2, r_2} \subseteq \Theta_{n, r}$ i com $\Theta_{m, s}$ és la menor congruència que conté a la unió, tenim que $\Theta_{n_1, r_1} \vee \Theta_{n_2, r_2} \subseteq \Theta_{n, r}$. Per tant, podem concloure que $\Theta_{n_1, r_1} \vee \Theta_{n_2, r_2} = \Theta_{n', r'}$. ■

Exemple 4.15. Si considerem les congruències d'índex finit sobre els naturals, $\Theta_{2,3}$ i $\Theta_{4,2}$ tenim per (4.12) que $\Theta_{2,3} \cap \Theta_{4,2} = \Theta_{4,6}$ i per (4.14) tenim que $\Theta_{2,3} \vee \Theta_{4,2} = \Theta_{2,1}$. Anem a vore el diagrama de Hasse corresponent a les interseccions i els supremes de les congruències.

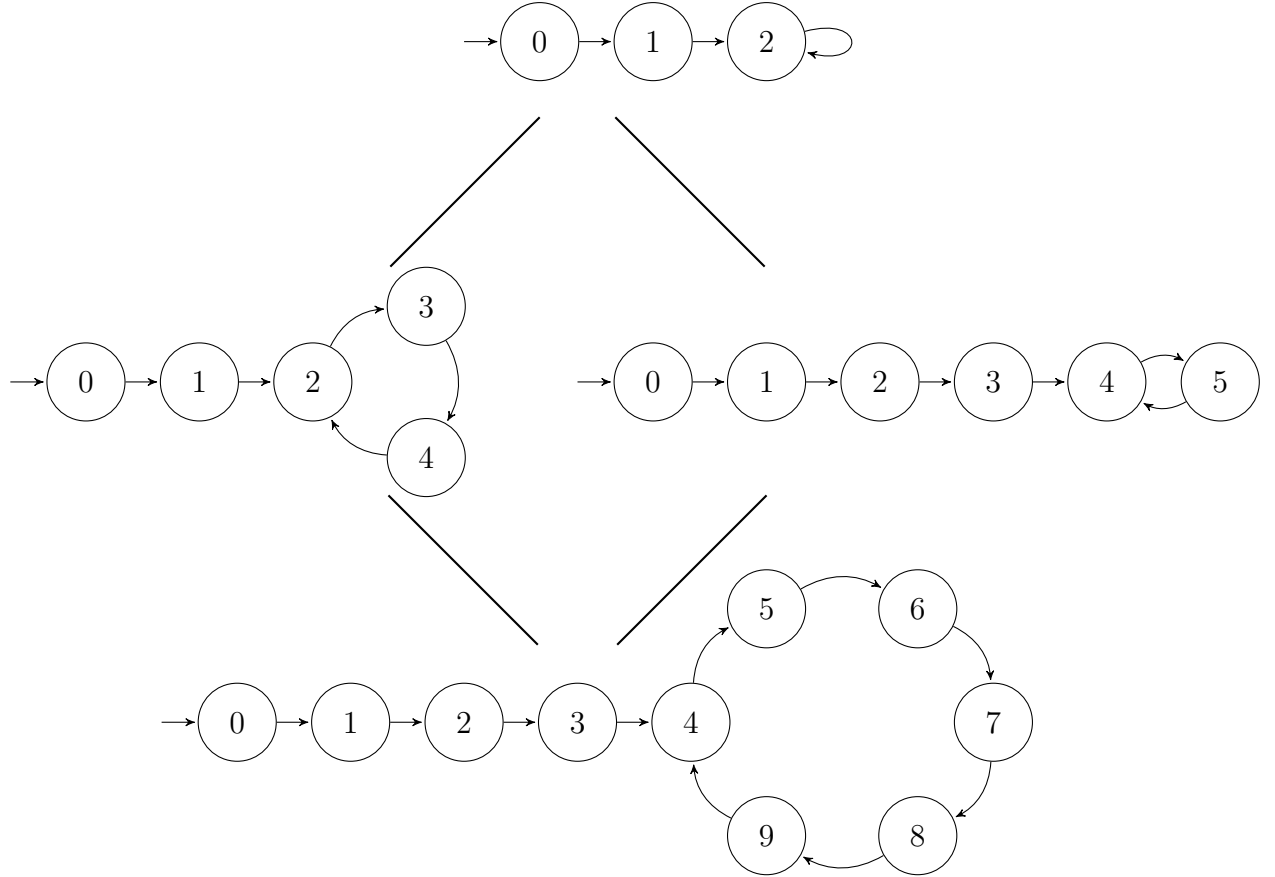


Figura 4.1: Diagrama d'un autòmata determinista.

Corol·lari 4.16. Tot autòmata sobre un alfabet amb una única lletra és equivalent a un autòmata del tipus $(\mathbb{N}/\varphi, +1, 0, O)$ per a $\varphi \in \text{Con}_{\text{if}}(\mathbb{N})$ un conjunt de classes d'equivalència finals O .

4.4 Aplicacions

Aquesta teoria que hem desenvolupat ens serveix per vore si donat un subconjunt de nombres naturals existeix algun autòmata finit que el reconega.

Per exemple si prenem $\mathbb{P}$ el conjunt dels nombres primers, ens preguntem si existira algun autòmata que reconega aquest conjunt.

Proposició 4.17. *No existeix cap autòmata finit que reconega el conjunt del nombres primers.*

Demostració. Si considerem el monoide lliure d'un generador $\mathbf{A}^*$, que és isomorf al monoide dels naturals, tenim que podem vore el conjunt de nombres primers com un llenguatge dels nombres naturals, aleshores el problema es tracta en vore si $\mathbb{P}$ és un llenguatge reconeixible o no. Pel teorema de Myhill-Nerode (3.12) transformem el nostre problema en vore si existeix una congruència d'índex finit en els naturals per a la qual tenim que $\mathbb{P}$ estiga saturat, que pel teorema (4.10) sabem que la congruència pertany a la família $\Theta_{n,r}$ per a $(n, r) \in \mathbb{N} \times \mathbb{N}^*$, per tant volem vore si $\mathbb{P}$ està saturat per a $\Theta_{n,r}$, és a dir si $\mathbb{P} = \bigcup_{x \in \mathbb{P}} [x]_{\Theta_{n,r}}$.

Suposem per reducció a l'absurd que $\mathbb{P}$ està saturat per a $\Theta_{n,r}$. Siga $p \in \mathbb{P}$, com que els nombres primers són infinits podem considerar un $k \in [p]_{\Phi}$ de manera que $n < k$ ja que les classes d'equivalència dels nombres menors estrictes que n només contenen un element. Aleshores com que $n < k$ tenim pel lema (4.5) que $(k, k + k'r) \in \Theta_{n,r}$ per a qualsevol $k' \in \mathbb{N}$, en particular per a $k' = k$. Aleshores com $(p, k), (k, k + kr) \in \Theta_{n,r}$ per la propietat transitiva, tenim que $(p, k + kr) \in \Theta_{n,r}$ així $k + kr \in [p]_{\Theta_{n,r}}$ i com hem suposat que $\mathbb{P}$ està saturat per a $\Theta_{n,r}$, aleshores $k + kr \in \mathbb{P}$ però $k + kr$ es pot descomposar en $k(1 + r)$ i per tant no és primer, fet que ens fa entrar en contradicció per haver suposat que $\mathbb{P}$ està saturat per a $\Theta_{n,r}$. Així, el conjunt de nombres primers no pot estar saturat per a cap congruència d'índex finit sobre els naturals. Concloem que $\mathbb{P}$ no és un llenguatge reconeixible. ■

Capítol 5

Conclusió

Una vegada realitzat el treball cal destacar una sèrie de observacions que considerem importants i que hem extret al llarg del treball. Primer que res, el més important de tot és els resultats que hem fet gràcies al teorema de Myhill-Nerode [Myh57][Ner58], que ens ha donat la possibilitat de posar al mateix nivell els autòmats i les congruències d'índex finit per a extraure resultats de reconeixibilitat en llenguatges formals. Ho hem desenvolupat amb les dos demostracions per vore que en alguns casos resultava més fàcil simplement amb autòmats, introduir transicions buides o modificar els conjunts, que emprar congruències d'índex finit, ja que aquesta última eina resultava un camí un poc més complex i amb idees que necessitaven més elaboració, com hem vist en el cas de la proposició (3.17).

També hem vist que en el cas del monoide dels naturals, el fet d'haver demostrat quina forma tenen totes les congruències d'índex finit, ens ha ajudat a saber d'una manera més fàcil si un llenguatge (subconjunt dels naturals) és reconeixible o no, com hem vist en el cas dels nombres primers.

També hem après com es comporten aquestes congruències al fer interseccions i suprems amb elles. Aquest fet ens ha ajudat finalment a adonar-nos que tot autòmata finit sobre un alfabet format per només una lletra són equivalents a un autòmata $(\mathbb{N}/\varphi, +1, 0, O)$ gràcies al fet de que el monoide lliure d'un generador i els nombres naturals són isomorfs.

En definitiva, hem vist quina utilitat tenen les congruències d'índex finit dins de la computació en la teoria d'autòmats amb un cas senzill que és el d'un llenguatge format amb només una lletra, però es podria, amb un alfabet amb més lletres, ajudant-nos en la teoria desenvolupada en el capítol 3 i alguns resultats més que podem vore en [Pin12] i [CC18], extraure més conclusions al respecte.

Bibliografia

- [BLR15] A. Ballester Bolinches, E. Cosme Llópez, and J. J. M. M. Rutten, *The dual equivalence of equations and coequations for automata*, Inf. Comput. **244** (2015), 49–75.
- [BS81] S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Graduate texts in mathematics, vol. 78, Springer, 1981.
- [CC18] J. Climent and E. Cosme, *Congruence based proofs of the recognizability theorems for free many-sorted algebras*, CoRR **abs/1808.08217** (2018).
- [Myh57] J. Myhill, *Finite automata and the representation of events*, WADD Technical Report **57-624** (1957), 112–137.
- [Ner58] A. Nerode, *Linear automaton transformations*, Proceedings of the American Mathematical Society **9** (1958), no. 4, 541–544.
- [Pin12] J. É. Pin, *Mathematical foundations of automata theory*, 2012.