Treball Fi de Grau - Curs 2019/ 2020

El primer teorema d'incompletesa de Gödel

Autor: **Hermes Casani Mompó**

Tutor: Enric Cosme Llópez

Grau en Matemàtiques

Índex

Motivació

Al llarg dels cursos i les assignatures que he estudiat a la facultat de matemàtiques, s'ha mencionat repetidament la naturalesa axiomàtica d'aquesta ciència. Recorde especialment la introducció del *Lema de Zorn* en l'assignatura d'equacions diferencials, on ens van explicar que aquesta proposició, clau per demostrar resultats elementals d'aquesta disciplina, no podia deduir-se dels elements anteriors de la construcció. Posteriorment, a altres assignatures de distintes àrees d'estudi, tornava a emprar-se el *Lema de Zorn* per demostrar teoremes importants. És per això que vaig començar a interessar-me i a reunir informació, en forma de cerques de navegador fortuïtes i lectures divulgatives on vaig descobrir la lògica matemàtica i als matemàtics formalistes. I totes aquestes lectures conduïen, sense excepció, als resultats d'incompletesa de Gödel.

Així doncs, per al meu treball de fi de grau m'he proposat el repte d'estudiar els arguments de Gödel en detall, amb el propòsit de comprendre amb precisió el significat del seu primer teorema d'incompletesa i les seues implicacions en les matemàtiques del segle XX, i comprovar si la meua formació matemàtica és suficient per a entendre aquest resultat important, tot i que la lògica matemàtica és una disciplina que no apareix al pla d'estudis de la facultat.

Introducció

Al congrés de París de l'any 1900, David Hilbert va reunir una llista de 10 problemes no resolts, amb la pretensió de convertir-la en una mena de guia a seguir per a la creació matemàtica en el nou segle. Aquesta llista, que va ser ampliada posteriorment fins a incloure 24 problemes, va ser ben rebuda pels científics, i resoldre els problemes que s'hi plantejaven esdevingué un dels reptes principals per la comunitat matemàtica de l'època. De fet, esta considerada una de les col·leccions de problemes més importants de tota la història de les matemàtiques. Açò es deu, principalment, a la gran influència de Hilbert com a investigador; alguns aventuren a dir que ell va ser l'últim gran matemàtic amb un coneixement transversal de les diferents disciplines d'aquesta ciència, i és per això que els problemes que va incloure en la famosa llista ocupen àrees d'estudi molt diverses. En la segona posició d'aquesta, Hilbert planteja escaridament el següent problema:

"Provar la consistència dels axiomes de l'aritmètica".

A què es referia exactament Hilbert amb això? Per comprendre bé aquesta idea cal remuntar-se a la Grècia clàssica d'Euclides. En el seu tractat *Els elements*, un dels textos més influents de la ciència, Euclides va introduir el que hui coneixem com *mètode axiomàtic*. Aquest consisteix a proporcionar una col·lecció de proposicions que s'accepten com a vertaderes sense requerir cap prova, anomenades *axiomes*. A partir d'uns certs axiomes sobre els elements bàsics de la geometria, Euclides va reunir en la seua obra un seguit de deduccions fetes pels seus coetanis, consolidant els conceptes essencials del que hui coneixem com geometria euclidiana. Al llarg dels segles, aquesta construcció axiomàtica va considerar-se un model científic perfecte, on una basta construcció de proposicions vertaderes es deduïen d'una petita col·lecció d'axiomes que resulten trivials per a la nostra intuïció.

Tant és així, que aquest mètode axiomàtic de la geometria euclidiana va caracteritzar, fins i tot, les mateixes matemàtiques. Es va crear un estat d'opinió en el qual tots els sectors del pensament matemàtic podrien dotar-se d'una formulació axiomàtica que suportara el pes de les infinites proposicions de cada àrea d'estudi. Arquimedes va tractar de traslladar aquesta idea a la física i va proporcionar una formulació axiomàtica per als coneixements de l'època. També cal tindre present la influència del pensament clàssic pitagòric en aquest context, el qual considera que els nombres i les matemàtiques són un conjunt de proporcions i regles que governen l'univers, de forma que res del que es deduïra dels intuïtius i certs axiomes d'Euclides podria ser erroni, o antinatural, ja que es referien a la natura mateixa de l'espai.

Però entre els axiomes que va proposar Euclides, n'hi havia un que no resultava tan trivial per a tots els grecs i generava certa confusió. Aquest, encara que originalment es va enunciar d'altra forma, pot formular-se com segueix:

"Donada una recta i un punt exterior a la recta, existeix una única línia paral·lela a la recta que passa pel punt donat".

La confusió es deu al fet que alguns matemàtics de l'època pensaven que aquest axioma no era realment necessari per a construir la geometria euclidea, i podia eliminar-se de la llista d'axiomes. Així, tractaren de provar que aquest es pot demostrar partint dels altres axiomes, amb poc èxit. De fet, les matemàtiques haurien d'esperar més de mil vuit-cents anys, fins al segle XIX i als treballs de Gauss, Bolyai i Lobachevski, per donar una resposta negativa a aquesta idea. Després de tants segles tractant de deduir aquest axioma dels altres, aquest resultat va tindre una importància intel·lectual principal. Mai abans en matemàtiques

s'havia demostrat la *impossibilitat* de provar un cert resultat dins d'un sistema determinat [4]. Així doncs, els matemàtics del segle XIX es van preguntar quines serien les implicacions de reemplaçar aquest axioma per d'altres, com ara:

"Donada una recta i punt extern a la recta, no existeix cap recta paral·lela a la primera que passa pel punt donat".

Aquest postulat, juntament amb la resta d'axiomes d'Euclides, dóna la base del que es coneix com a geometria riemanniana. Afegint axiomes com aquest, que podríem considerar antiintuïtius, s'obtenien construccions alternatives a la geometria euclidiana, però igualment interessants. Així, es va estendre el pensament que les matemàtiques són la ciència de la deducció. Al matemàtic no li importa realment si els axiomes que accepta són o no vertaders; la importància d'aquesta ciència radica en l'estudi del procés deductiu. Aquesta idea es resumeix en el famós epigrama de Russell:

"La matemàtica pura és la ciència en la qual no sabem allò del que estem parlant ni si allò que diem és vertader".

Al mateix temps que s'experimentava amb noves geometries, els matemàtics d'aquest segle XIX van reprendre el treball fet per Euclides d'atorgar una base axiomàtica apropiada a les diferents teories matemàtiques. És a dir, escollir una certa col·lecció d'axiomes que permeta deduir *totes les veritats* matemàtiques d'una certa àrea d'estudi. I d'entre totes aquestes teories de la matemàtica, l'aritmètica, per la seua simplicitat i presència en pràcticament totes les altres arees, va establir-se com a punt de partida en aquesta empresa. Així, Giuseppe Peano va proposar un conjunt d'axiomes que presumiblement axiomatitzarien l'aritmètica, igual que els axiomes d'Euclides axiomatitzaven la geometria.

D'aquesta forma, mentre una part dels matemàtics cercava axiomatitzar l'aritmètica, i el reemplaçament d'alguns axiomes euclidians permetia crear geometries alternatives a les convencionals, dos nous grans problemes apareixien. El primer és que en incorporar nous axiomes «gratuïtament» a una teoria, podria donar-se el cas d'arribar a una incoherència en algun punt de la construcció, és a dir, que d'un conjunt d'axiomes d'un cert sistema es pogueren deduir teoremes mútuament contradictoris. Aquest temor no havia aparegut abans quan els matemàtics clàssics desenvolupaven la geometria euclidiana, ja que la consideraven una part de la mateixa natura de l'espai. Però ara que es reemplaçaven els axiomes euclidians per d'altres antiintuïtius, aquesta possibilitat va convertir-se en una preocupació principal. A les teories que no tenen aquest tipus de contradiccions se les va anomenar consistents.

Per entendre el segon problema que va aparèixer, considerem la coneguda conjectura de Goldbach en l'aritmètica dels nombres naturals:

"Tot nombre enter parell superior a dos es pot escriure com a suma de dos nombres primers".

Per molt de temps els matemàtics han tractat de cercar una prova o un contraexemple a aquesta conjectura sense èxit. Fins ara, s'ha pogut comprovar amb mètodes computacionals que la conjectura és certa per als quatre primers trilions de nombres parells. Açò porta a pensar que la conjectura deu ser vertadera, tot i que ningú ha aconseguit construir una prova matemàtica que la demostre per a qualsevol nombre. El que Hilbert i Russell pensaven, és que simplement ningú havía tingut la idea brillant que demostra la falsedat o la validesa del teorema, i sería només qüestió de temps que un geni els sorprengera finalment amb l'argument correcte, que esperaven, seria una conseqüència dels axiomes de Peano.

Però, i si no fora així, i el resultat fóra vertader però tal prova no existira partint d'aquests axiomes? O, més encara, i si la prova no existira triarem els axiomes que triarem? Estaríem doncs en una situació delicada. A les teories axiomàtiques que eviten aquesta situació, és a dir, les teoríes en que tota proposició vertadera pot ser deduïda del sistema axiomàtic, les anomenem completes.

Com podem provar la consistència i la completesa d'un sistema axiomàtic? El problema requereix una nova forma de fer matemàtiques. Matemàtiques que ens permeten estudiar les estructures de les mateixes

matemàtiques. Metamatemàtiques. Aquesta ambiciosa empresa, anomenada formalització de les matemàtiques, consisteix en construir una nova àrea matemàtica en la qual s'estudien totes les possibles construccions deductives d'un cert sistema matemàtic i els recursos que empren els matemàtics quan treballen qualsevol àrea d'estudi. Per fer això, aquest sistema considera les demostracions matemàtiques com a meres cadenes de símbols i caràcters, i identifica les cadenes correctes i formalitza el sistema de deduccions en matemàtiques, és a dir, es defineix amb rigor quan una certa cadena de símbols és la deducció d'una altra cadena de símbols.

Una vegada formalitzada la matemàtica, podran donar-se definicions rigoroses de consistència i completesa i comprovar quan una certa teoria ho és. A més, s'esperava que les demostracions de consistència i completesa prodrien dur-se a terme evitant procediments que no feren referència a un nombre infinit de propietats estructurals i operacions. A tals procediments els anomenem finitistes. De forma semblant, s'exigía una prova absoluta, és a dir, s'exigía no pressupossar la consistència de cap altre conjunt d'axiomes. Aquest projecte es coneix com el programa formalista de Hilbert. El segon problema de la llista pot enunciar-se en aquestos termes com segueix:

"Provar que la teoría aritmètica de Peano és completa i consistent mitjançant una prova finitista i absoluta."

Grans matemàtics de principis del segle XX, com ara Frege, Rusell i el mateix Hilbert tenien ferma confiança en el triomf del programa formalista, que permetria provar la consistència i la completesa de les diferents àrees de la matemàtica, començant per l'aritmètica bàsica dels nombres naturals. De fet, molts matemàtics dedicaren bona part de les seues investigacions a aquest programa, i la publicació matemàtica en aquest àmbit va proliferar les primeres tres dècades del segle vint. Però tot canviaria a continuació.

Kurt Gödel va publicar el 1931 els seus coneguts teoremes d'incompletesa que, a pesar de seguir provocant polèmica en els nostres dies, pareixen recolzar irremeiablement el fet que existeixen certes proposicions dins de les teories aritmètiques consistents que no poden ser demostrades a partir d'una col·lecció donada d'axiomes. El treball de Gödel va provocar una gran crisi en la filosofia de les matemàtiques, i pareixia condemnar el programa de Hilbert definitivament. Així, sembla que no és possible tindre consistència i completesa simultàniament en la teoria aritmètica dels nombres naturals. Si sabem que existeixen proposicions que, tot i que són certes, no poden ser demostrades, podríem pensar que tal volta la conjectura de Goldbach és una d'aquestes veritats indemostrables.
En aquest treball reconstruirem els arguments de Gödel. Amb aquest propòsit, seguirem el següent esquema:

1. Al primer capítol presentarem una introducció a la formalització de les matemàtiques. Introduirem els llenguatges formals de primer ordre, les deduccions sintàctiques, i definirem les teories formals. Finalment, introduirem la teoria de l'aritmètica de Peano.

2. Al segon capítol presentarem la teoria de la computabilitat, una branca desenvolupada posteriorment a la publicació de Gödel que farem servir com drecera per a arribar al resultat de Gödel amb més precisió. Per fer això, seguirem els apunts de Kim [2]. Així doncs, no seguirem la construcció original de Gödel. Aquest és el capítol més important, on construirem un sistema robust de codificacions per als nombres naturals i el relacionarem amb els llenguatges formals del primer capítol.

3. A l'últim capítol, introduïrem el concepte de representabilitat i donarem la definició de consistència i completesa en termes de la codificació construida als capítols anteriors, per provar el primer teorema de Gödel.

Notació i definicions bàsiques.

Notació. Emprarem els següents convenis:

- Donat $n \in \mathbb{N}$ denotem per $\mathbb{N}^n$ al producte cartesià $\mathbb{N} \times \underset{n \text{ vegades}}{...} \times \mathbb{N}$ i per $\mathbf{n}$ al conjunt $\{1, 2, 3, ..., n\}$. A més a més considerarem que $0 \in \mathbb{N}$ en tot el treball, amb $\mathbf{0} = \varnothing$. Emprarem l'expressió $(x_i)_{i \in \mathbf{n}}$ per referirnos a l'element $(x_1, \cdots, x_n)$ de $\mathbb{N}^n$.
- Si A i B són conjunts, definim el següent conjunt:

$$\mathrm{Hom}(A, B) = \{f : A \longrightarrow B \mid f \text{ és una funció}\}$$

- Si A és un conjunt, amb $\mathrm{Sub}(A)$ ens referirem al conjunt de tots els subconjunts de A.

Definició 1. (*Relació*) Un subconjunt R de $\mathbb{N}^n$ s'anomena **relació n-ària**. Si $(x_i)_{i \in \mathbf{n}} \in R$ direm que els naturals $x_1, x_2, ..., x_n$ satisfan la relació R. A més a més escriurem $R((x_i)_{i \in \mathbf{n}})$ per denotar que $(x_i)_{i \in \mathbf{n}} \in R$.

Definició 2. Definim la **funció característica** de R com l'aplicació:

$$\begin{array}{rccl} \mathcal{X}_R : & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_i)_{i \in \mathbf{n}} & \longmapsto & \begin{cases} 1 & \text{si } (x_i)_{i \in \mathbf{n}} \notin R; \\ 0 & \text{si } (x_i)_{i \in \mathbf{n}} \in R. \end{cases} \end{array}$$

Definició 3. Si $Q, P \subseteq \mathbb{N}^n$ són relacions n-àries.

(a) Al conjunt $\mathbb{N}^n \setminus P$ l'anomenem **negació** de P i el denotem per $\neg P$.

(b) Al conjunt $P \cup Q$ l'anomenem **conjunció** de P i Q i el denotem per $P \vee Q$.

(c) Al conjunt $P \cap Q$ l'anomenem **disjunció** de P i Q i el denotem per $P \wedge Q$

Capítol 1

Un model de l'aritmètica

1.1 Àlgebres de termes

El nostre objectiu és considerar les mateixes matemàtiques com a objecte d'estudi. Per tant necessitarem una bona eina per referir-nos a elles. Com a exemple, per veure quins tipus d'elements necessitarem, reprendrem la conjectura de Goldbach. Si amb P denotem el conjunt de nombres primers i amb $2\mathbb{N}$ denotem els nombres naturals parells, cal adonar-se que podem expressar la conjectura de dues formes, d'una com ja l'hem introduït i d'altra en forma simbòlica:

"Tot nombre enter parell superior a dos es pot escriure com a suma de dos nombres primers."

$$\text{“}2\mathbb{N}(x) \wedge x > 2 \to \exists q, p(P(q) \wedge P(p) \wedge (x = p + q))\text{.”}$$

Ens centrarem només en les expressions del segon tipus. Així, podem considerar que la conjectura de Goldbach no és més que una certa cadena de símbols. Cadascun d'aquests símbols, però, té un significat totalment delimitat. Necessitem distingir, doncs, entre *sintaxi* i *semàntica*. Amb *sintaxi* ens referim al conjunt de símbols, a l'alfabet de les matemàtiques. En *semàntica*, al significat dels símbols i de les combinacions d'aquests. Comencem definint l'estructura del que serà el conjunt de totes les *paraules* que podem formar amb un alfabet, o col·lecció de símbols S, sense importar si aquestes paraules o cadenes de símbols tenen o no significat matemàtic. Per tal que siga més compacte, les paraules amb n símbols de S les definirem com funcions sobre el conjunt $\mathbf{n}$.

Definició 4. Siga S un conjunt. El **monoide lliure** S^* és la 3-tupla $(S, \curlywedge, \lambda)$ on:

- S^* és el conjunt de les **paraules** de S:

$$S^* = \bigcup_{n \in \mathbb{N}} \mathrm{Hom}(\mathbf{n}, S),$$

  és a dir, el conjunt de totes les funcions $w : \mathbf{n} \to S$, per a algun $n \in \mathbb{N}$.

- A $\curlywedge$ l'anomenem concatenació. Si $w : \mathbf{n} \to S$, $v : \mathbf{m} \to S$ són dues paraules:

$$\begin{array}{rccl} w \curlywedge v : & \mathbf{n}{+}\mathbf{m} & \longrightarrow & S \\ & i & \longmapsto & \begin{cases} w(i) & \text{si } 0 \leqslant i < n; \\ v(i-n) & \text{si } n \leqslant i < n+m. \end{cases} \end{array}$$

- A λ l'anomenem paraula buida en S, i és l'única funció de $\mathbf{0} = \varnothing$ a S.

Cal ressaltar que, per a tot conjunt S, $(S, \curlywedge, \lambda)$ és un monoide. Ja tenim definides les paraules, o cadenes de símbols d'un cert alfabet, i també hem definit la concatenació, que no és més que l'operació que combina dues paraules, una darrere de l'altra. Ara anem a parar atenció als tipus de símbols amb els quals contarà el nostre alfabet de les matemàtiques.

Quins tipus d'elements necesitem distinguir? Pensem en els símbols que emprem habitualment en qualsevol teoría matemàtica i en el cas particular de l'aritmètica:

1. Símbols de constants.
2. Els símbols que denoten funcions matemàtiques n-àries, que en el cas de l'aritmètica són funcions de la forma $f : \mathbb{N}^n \longrightarrow \mathbb{N}$, per a un $n \geqslant 1$ natural.
3. Els símbols que denoten relacions matemàtiques n-àries, que en el cas particular de l'aritmètica són de la forma $R \subseteq \mathbb{N}^n$, per a un $n \geqslant 1$ natural.
4. Els símbols que denoten operadors lógics com ara $\rightarrow, \forall, \wedge, \neg$, etc..

Comencem formalitzant les constants i les funcions del primer i el segon apartat. D'ara en avant, cal pensar en Σ com el conjunt de símbols que representen o bé funcions de n variables definides sobre un cert conjunt, o bé constants.

Definició 5. Una **signatura** Σ és un conjunt amb una funció anomenada **aritat**. Aquesta funció deu tindre la següent forma:

$$\mathrm{ar} : \Sigma \longrightarrow \mathbb{N}$$

Així, per a cada $\sigma \in \Sigma$ tindrem que $\mathrm{ar}(\sigma) = n$, per a cert $n \in \mathbb{N}$.

En particular, als elements d'una signatura que representen funcions amb aritat 0 els anomenem símbols **constants**. Ara definirem la interpretació semàntica que tindran els símbols d'una signatura Σ. És a dir, identificarem cada símbol amb una operació definida sobre un cert conjunt A, que, en l'exemple de laritmètica, serà el conjunt dels nombres naturals. A aquestes estructures les anomenarem Σ-*àlgebres*.

Definició 6. Siga Σ una signatura i A un conjunt. Una **estructura de Σ-àlgebra** per a A és un parell (A, F), que abreujarem amb $\mathbf{A}$, on F és la funció que per a cada símbol de funció $\sigma \in \Sigma$ d'aritat n actua de la següent forma:

$$\begin{array}{rccc} F: & \Sigma & \longrightarrow & \mathrm{Hom}(A^n, A) \\ & \sigma & \longmapsto & \sigma^{\mathbf{A}} \end{array} \qquad \begin{array}{rcl} : A^n & \longrightarrow & A \\ (a_j)_{j\in\mathbf{n}} & \longmapsto & \sigma^{\mathbf{A}}((a_j)_{j\in\mathbf{n}}) \end{array}$$

és a dir, F interpreta cada símbol de funció σ d'aritat n de Σ com una operació n-ària en A, denotada per $\sigma^{\mathbf{A}}$. De vegades, si el context és clar, escriurem simplement σ. Per al cas particular d'un símbol constant σ d'aritat 0, la seua imatge vía F és un element d'A.

A continuació introduïm els *homomorfismes* en aquestes estructures particulars.

Definició 7. Siguen $\mathbf{A} = (A, F)$, $\mathbf{B} = (B, G)$ dues Σ-àlgebres. Una funció $f : \mathbf{A} \longrightarrow \mathbf{B}$ és un **homomorfisme** si, per a tot $\sigma \in \Sigma$ amb $\mathrm{ar}(\sigma) = n$ i per a tot $(a_j)_{j\in\mathbf{n}} \in A^n$, es té que

$$f(\sigma^{\mathbf{A}}((a_j)_{j\in\mathbf{n}})) = \sigma^{\mathbf{B}}((f(a_j))_{j\in\mathbf{n}}).$$

Denotarem per $\mathrm{Sub}(\mathbf{A})$ el conjunt de totes les subàlgebres d'$\mathbf{A}$ i per **Sub(A)** el reticle $(\mathrm{Sub}(\mathbf{A}), \subseteq)$, on les subàlgebres estaran ordenades per inclusió. Per afinar el concepte de Σ-àlgebra, emprarem *l'operador de subàlgebra*, que ens permetrà definir *l'àlgebra de termes* d'un llenguatge robustament. Previament, definim quan un conjunt X és tancat amb l'operació d'una Σ-àlgebra.

Definició 8. Siguen $\mathbf{A}$ una Σ-àlgebra, un conjunt $X \subseteq A$ i un símbol d'operació $\sigma \in \Sigma$ tal que $\mathrm{ar}(\sigma) = n$. Direm que X és **tancat** per l'aplicació $\sigma^{\mathbf{A}}$, si per a tot $(a_j)_{j\in\mathbf{n}} \in X^n$, es compleix que $\sigma^{\mathbf{A}}((a_j)_{j\in\mathbf{n}}) \in X$.

Definició 9. Siga $\mathbf{A}$ una Σ-àlgebra. Denotem per $\mathrm{Sg}_{\mathbf{A}}$ a l'operador anomenat **operador de subàlgebra generada en** A, donat per:

$$\begin{array}{rccl} \mathrm{Sg}_{\mathbf{A}}: & \mathrm{Sub}(\mathbf{A}) & \longrightarrow & \mathbf{Sub(A)} \\ & X & \longmapsto & \mathrm{Sg}_{\mathbf{A}}(X) = \bigcap\{Y \in \mathrm{Sub}(\mathbf{A}) \mid X \subseteq Y\} \end{array}$$

Notem que $\mathrm{Sg}_{\mathbf{A}}$ és l'operador que associa a cada subconjunt X d'A la subàlgebra d'$\mathbf{A}$ generada per X, és a dir, la menor subàlgebra en $\mathbf{A}$ que conté a X.

Ara volem centrar-nos en els símbols que representen relacions matemàtiques en una certa teoria, com ho poden ser la relació ser un nombre primer P o ser un nombre parell $2\mathbb{N}$, que hem introduït anteriorment. D'ara en avant cal pensar en Θ com el conjunt dels símbols que representen relacions en una certa teoria matemàtica. Raonarem de forma semblant al que hem fet amb els símbols de funcions, però aquesta volta identificarem cada símbol de relació amb un subconjunt d'un cert conjunt A, que en el cas de l'aritmètica serà el conjunt dels nombres naturals.

Definició 10. Siga Θ una signatura i siga A un conjunt. Una **estructura de Θ-model relacional** per a A és un parell (A, F), denotat per $\mathbf{A}$, on:

$$\begin{array}{rccll} F: & \Theta & \longrightarrow & \mathrm{Sub}(A^{ar(\theta)}) & \\ & \theta & \longmapsto & \theta^A & \subseteq A^{ar(\theta)} \end{array}$$

és a dir, F interpreta cada símbol de relació θ d'aritat n com una relació n-ària en A, denotada per $\theta^{\mathbf{A}}$.

A continuació necessitem introduir el concepte de *morfisme relacional*, inspirat en el concepte clàssic d'homomorfisme.

Definició 11. Siguen $\mathbf{A} = (A, F)$, $\mathbf{B} = (B, G)$ dos Θ-models relacionals. Una funció $f : \mathbf{A} \longrightarrow \mathbf{B}$ és un **morfisme relacional** si, per a tot $\theta \in \Theta$ amb $\mathrm{ar}(\theta) = n$ i per a tot $(a_j)_{j\in\mathbf{n}} \in A^n$, es té que:

$$\theta^{\mathbf{A}}((a_j)_{j\in\mathbf{n}}) \quad \text{si, i només si,} \quad \theta^{\mathbf{B}}((f(a_j))_{j\in\mathbf{n}}).$$

Ja podem definir una primera estructura que permet interpretar tant els símbols de relació com els símbols de funció. A aquestes estructures les anomenarem *models*.

Definició 12. Siguen Σ i Θ signatures i A un conjunt. Una **estructura de (Σ, Θ)-model** per a A és la 3-tupla (A, F_Σ, F_Θ), abreujada $\mathbf{A}$ on:

- (A, F_Σ) és una Σ àlgebra.
- (A, F_Θ) és un Θ-model relacional.

També podem extendre el concepte d'homomorfisme als (Σ, Θ)-models.

Definició 13. Siguen Σ i Θ dues signatures. Considerem $\mathbf{A} = (A, F_\Sigma, F_\Theta)$, $\mathbf{B} = (B, F_\Sigma, F_\Theta)$ dos (Σ, Θ)-models per a A i B respectivament. Aleshores una funció $f : \mathbf{A} \longrightarrow \mathbf{B}$ és un (Σ, Θ)-**morfisme** si f és un morfisme relacional i un homomorfisme.

Fins ara, hem donat una interpretació als símbols de funció i relació. A continuació volem formalitzar allò que fem quan escrivim expressions del tipus $f(x_1, \cdots, x_n)$ en matemàtiques que, en la nostra notació primitiva, tindran la forma $fx_1 \cdots x_n$, és a dir, un símbol de funció d'aritat n que actua sobre n variables d'un conjunt de variables X o sobre altres funcions (composicions). Amb aquest propòsit introduïm el concepte *d'algebra de Σ-files*.

Definició 14. Siguen X un conjunt i Σ una signatura. Suposem que X i Σ són disjunts. Definim **l'àlgebra de Σ-files** en X, denotada per $\mathbf{W}_\Sigma(X)$, com segueix:

$$\mathbf{W}_\Sigma(X) = (X \cup \Sigma)$$

A més si $\sigma \in \Sigma$ és un símbol de funció amb $\mathrm{ar}(\sigma) = n$ definim la següent funció:

$$\begin{array}{rccc} \sigma^{\mathbf{W}_\Sigma(X)}: & \mathbf{W}_\Sigma(X)^n & \longrightarrow & \mathbf{W}_\Sigma(X) \\ & (w_j)_{j\in\mathbf{n}} & \longmapsto & \sigma \curlywedge \bigwedge\limits_{j\in\mathbf{n}} w_j \end{array}$$

Així, la funció $\sigma^{\mathbf{W}_\Sigma(X)}$ retorna la concatenació de n variables darrere un símbol d'operació n-ari.

Finalment, ja hem construït la infraestructura necessària per definir l'àlgebra de termes d'una Σ-àlgebra.

Definició 15. Anomenem **Σ-àlgebra de termes** en X, normalment denotada per $\mathbf{T}_\Sigma(X)$, a $\mathrm{Sg}_{\mathbf{W}_\Sigma(X)}(X)$, és a dir, la menor subàlgebra en $\mathbf{W}_\Sigma(X)$ que conté a X.

Així, la següent proposició, que se segueix directament de les definicions que hem donat, caracteritza l'àlgebra de termes, que per al nostre cas dels nombres naturals seran els mateixos nombres naturals i les expressions del tipus $(x_1, \cdots, x_n)$ i $f(x_1 \cdots x_n)$. La demostració d'aquest resultat pot consultar-se en [5].

Proposició 1. (Caracterització de l'àlgebra de termes). Siguen X un conjunt i Σ una signatura disjunts. Siga $P \in \mathbf{W}_\Sigma(X)$, aleshores $P \in \mathbf{T}_\Sigma(X)$ si, i només si, es verifica alguna de les següents condicions:

1. $P = x$, per a un únic $x \in X$.
2. $P = \sigma$, per a un únic $\sigma \in \Sigma$ d'aritat 0, és a dir, P és una constant.
3. $P = \sigma \curlywedge \bigwedge\limits_{j\in\mathbf{n}} P_j$, per a un únic $\sigma \in \Sigma$ amb $\mathrm{ar}(\sigma) = n$ i una única família $(P_j)_{j\in\mathbf{n}}$ en $\mathrm{T}_\Sigma(X)^n$.

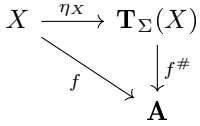
Per fer més familiar la notació, establim els següents criteris de notació per als símbols de funcions.

Notació. Siga $\sigma \in \Sigma$ amb $\mathrm{ar}(\sigma) = n$, normalment escriurem:

1. $\sigma((P_j)_{j\in\mathbf{n}})$ en compte de $\sigma \curlywedge \bigwedge\limits_{j\in\mathbf{n}} P_j$.
2. Si el símbol de funció és binari, és a dir, si $* \in \Sigma$ amb $ar(*) = 2$, escriurem $P_1 * P_2$ en compte de $*(P_1, P_2)$.

El següent resultat, del qual no inclouré la demostració, ens serà molt útil posteriorment per donar coherència a aquesta construcció que estem fent. La demostració d'aquest resultat pot trobar-se en [5].

Teorema 1. (Propietat universal de l'àlgebra de termes). Per a tota Σ-àlgebra $\mathbf{A}$, per a tot conjunt de variables X i per a tota $f : X \longrightarrow A$ existeix un únic Σ-homomorfisme $f^\# : \mathbf{T}_\Sigma(X) \longrightarrow \mathbf{A}$ que satisfà $f^\# \circ \eta_X = f$, és a dir, un únic Σ-homomorfisme que fa conmutatiu el següent diagrama:



on η_X és la funció que a cada variable x li assigna el terme x, és a dir:

$$\begin{array}{rccc} \eta_X: & X & \longrightarrow & \mathbf{T}_\Sigma(X) \\ & x & \longmapsto & x \end{array}$$

1.2 Els llenguatges formals de primer ordre

A la secció anterior hem presentat les nocions necessàries per definir els llenguatges formals de primer ordre, que introduïm a continuació.

Definició 16. Siguen Σ i Θ dues signatures i $X = \{x_i \mid i \in \mathbb{N}\}$ un conjunt de variables, de manera que aquests tres conjunts són disjunts dos a dos. Un **llenguatge formal de primer ordre** $\mathcal{L}$ és la tupla $(\Sigma, \Theta, \mathrm{Log}(X))$ on

$$\mathrm{Log}(X) = \{\rightarrow, \neg\} \cup \{\forall x \mid x \in X\}$$

és la signatura dels símbols lògics de $\mathcal{L}$. Ací, $\rightarrow$ serà un símbol d'operació binari i tant $\neg$ com $\forall x$ seran símbols unaris. A més, en tot llenguatge deu existir el símbol de relació binari $=$ en Θ. Al conjunt d'elements de la signatura Σ d'aritat zero els anomenarem constants del llenguatge, i el representarem amb el símbol Σ_0.

Evidentment, no totes les paraules d'un llenguatge tenen significat matemàtic. D'entre totes elles ens valdrem de la construcció que hem fet de l'àlgebra de termes per definir les *fórmules atómiques* i les *fórmules* del llenguatge. Amb les primeres volem captar les expressions del tipus $R(x_1, \cdots x_n)$, on R és una relació n-ària, i amb les segons expressarem l'àlgebra de termes que podem construir sobre les fórmules atòmiques mitjançant la signatura $\mathrm{Log}(X)$, és a dir, expressions que involucren símbols lògics.

Definició 17. Siga $\mathcal{L}$ un llenguatge.

- Anomenem **terme** a tot element de $\mathbf{T}_\Sigma(X)$.
- Anomenem **fòrmula atòmica** al següent conjunt:

$$\mathbf{At}_\Theta(X) = \{\theta((t_j)_{j\in\mathbf{n}}) \mid \theta \in \Theta, (t_j)_{j\in\mathbf{n}} \in \mathbf{T}_\Sigma(X)^n\} \cup \mathbf{T}_\Sigma(X) \tag{1.1}$$

- Anomenem **fórmula** a tot element de $\mathbf{T}_{\mathrm{Log}(X)}(\mathbf{At}_\Theta(X))$. Aquest conjunt el denotarem per $\mathrm{Form}(\mathcal{L}, X)$.

Notació. Si α i β són fórmules de $\mathcal{L}$, t_1, t_2 són dos termes i x és una variable, adoptem els següents convenis de notació:

(a) Amb $(\alpha \rightarrow \beta)$ expressem $\rightarrow \alpha\beta$.

(b) Amb $(t_1 = t_2)$ expressem $= t_1 t_2$.

(c) Amb $(t_1 \neq t_2)$ expressem $\neg(t_1 = t_2)$.

(d) Amb $(\alpha \vee \beta)$ expressem $(\neg\alpha \rightarrow \beta)$.

(e) Amb $(\alpha \wedge \beta)$ expressem $\neg(\neg\alpha \vee \neg\beta)$.

(f) Amb $(\alpha \leftrightarrow \beta)$ expressem $(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$.

(g) Amb $\forall x(\alpha)$ expressem $\forall x\alpha$.

(h) Amb $\exists x(\alpha)$ expressem $\neg\forall\alpha(x\neg\alpha)$.

El nostre objectiu ara és definir el que fem els matemàtics quan en una fórmula substituïm una variable per un terme, que en el nostre exemple dels naturals serà un nombre natural. Per definir-ho correctament, és necessari distingir entre variables *lliures* i *lligades*. Per entendre intuïtivament la necessitat d'aquesta distinció, considerem la següent expressió:

$$\forall n(\exists m(\varphi(n, m, z)))$$

Aquesta fórmula involucra tres variables, n, m i z. Podem substituir aquestes variables per un nombre natural? Tant n com m estan sotmeses a l'actuació dels quantificadors, i no té sentit platejar la seua substitució. Així direm que aquestes variables estan lligades. Per a la variable z, que no té cap element quantificador actuant, sí podem plantejar la seua substitució per un nombre natural, i direm que està lliure en aquesta fórmula. A continuació introduïm amb rigor aquesta idea.

Definició 18. Siga $\mathcal{L}$ un llenguatge formal. Definim quan una variable x_i està **lliure** en una fórmula γ en $\mathrm{Form}(\mathcal{L}, X)$ de forma recursiva com segueix:

(a) Si γ és una fórmula del tipus x_j per a una variable $x_j \in X$, direm que x_i està lliure en γ si $i = j$.

(b) Si γ és una fórmula del tipus $\sigma((P_j)_{j\in\mathbf{n}})$ per a un símbol d'operació $\sigma \in \Sigma$ d'aritat n i una família de termes $(P_j)_{j\in\mathbf{n}}$ en $\mathbf{T}_\Sigma(X)^n$, direm que x_i està lliure en γ si existeix un $j \in \mathbf{n}$ de manera que x_i és lliure en x_j.

(c) Si γ és una fórmula del tipus $\theta((P_j)_{j\in\mathbf{n}})$, per a un símbol de relació $\theta \in \Theta$ d'aritat n i una família de termes $(P_j)_{j\in\mathbf{n}}$ en $\mathbf{T}_\Sigma(X)^n$, direm que x_i és lliure en γ si existeix $j \in \mathbb{N}$ de forma que x_i és lliure en x_j.

(d) Si γ és una fórmula del tipus $\neg\alpha$, per a una fórmula $\alpha \in \mathrm{Form}(\mathcal{L}, X)$, direm que x_i és lliure en γ si x_i és lliure en α.

(e) Si γ és una fórmula del tipus $\alpha \to \beta$, per a unes fórmules $\alpha, \beta \in \mathrm{Form}(\mathcal{L}, X)$, direm que x_i és lliure en γ si x_i és lliure en α o és lliure en β.

(f) Si γ és una fórmula del tipus $\forall x_j(\alpha)$ per a alguna variable $x_j \in X$ i una fórmula α en $\mathrm{Form}(\mathcal{L}, X)$, direm que x_i és lliure en γ si x_i és lliure en α i $i \neq j$

Definició 19. Siga $\mathcal{L}$ un llenguatge formal. Definim quan una variable $x \in X$ està **lligada** en una fórmula γ en $\mathrm{Form}(\mathcal{L}, X)$ de forma recursiva com segueix:

(a) Si γ és una fórmula atòmica direm que x no és lligada en γ.

(b) Si γ és una fórmula del tipus α, per a alguna fórmula α en $\mathrm{Form}(\mathcal{L}, X)$, direm que x és lligada en γ si x és lligada en α.

(c) Si γ és una fórmula del tipus $\alpha \to \beta$, per a dues fórmules α, β en $\mathrm{Form}(\mathcal{L}, X)$, direm que x és lligada en γ si x és lligada en α o x és lligada en β.

(d) Si γ és una fórmula del tipus $\forall x_j(\alpha)$ per a una variable x_j en X i una fórmula α en $\mathrm{Form}(\mathcal{L}, X)$, direm que x_i és lligada en γ si x_i és lligada en α o bé $i = j$.

Amb aquestes dues definicions ja podem captar allò que fem quan substituïm una variable per un terme en un llenguatge.

Definició 20. Siga $x \in X$ una variable, i siga p un terme en $\mathbf{T}_\Sigma(x)$. Definim la **substitució** d'x per p en una fórmula γ, i ho denotem $\binom{x}{p}(\gamma)$, de forma recursiva com segueix:

(a) Si $\gamma = y$ per a alguna $y \in X$, definim la substitució en γ com segueix:

$$\binom{x}{p}(\gamma) = \begin{cases} \gamma & \text{si } y \neq x; \\ p & \text{si } y = x. \end{cases}$$

(b) Si $\gamma = \sigma((P_j)_{j\in\mathbf{n}})$, per a un símbol d'operació $\sigma \in \Sigma$ d'aritat n i una família de termes $(P_j)_{j\in\mathbf{n}}$ en $\mathbf{T}_\Sigma(X)^n$,definim la substitució com segueix:

$$\binom{x}{p}(\gamma) = \sigma(\left(\binom{x}{p}(P_j)\right)_{j\in\mathbf{n}})$$

(c) Si $\gamma = \theta((P_j)_{j\in\mathbf{n}})$, per a un símbol de relació $\theta \in \Theta$ d'aritat n i una familia de termes $(P_j)_{j\in\mathbf{n}}$ en $\mathbf{T}_\Sigma(X)^n$, definim la substitució en γ com segueix:

$$\binom{x}{p}(\gamma) = \theta(\left(\binom{x}{p}(P_j)\right)_{j\in\mathbf{n}})$$

(d) Si $\gamma = \neg\alpha$, per a una fórmula $\alpha \in \mathrm{Form}(\mathcal{L}, X)$, definim la substitució en γ com segueix:

$$\binom{x}{p}(\gamma) = \neg(\binom{x}{p}(\alpha))$$

(e) Si $\gamma = \alpha \to \beta$, per a unes fórmules $\alpha, \beta \in \mathrm{Form}(\mathcal{L}, X)$ definim la substitució em γ com segueix:

$$\binom{x}{p}(\gamma) = \binom{x}{p}(\alpha) \to \binom{x}{p}(\beta)$$

(f) Per últim, si $\gamma = \forall x_j(\alpha)$, per a alguna variable $x_j \in X$ i una fórmula α en $\mathrm{Form}(\mathcal{L}, X)$, definim la substitució en γ com segueix:

$$\binom{x_i}{p}(\gamma) = \begin{cases} \gamma & \text{si } x_i \text{ no és lliure en } \gamma; \\ \forall x_j(\binom{x_i}{p}(\alpha)) & \text{si } x_i \text{ és lliure en } \gamma \text{ i } x_j \text{ és lligat en } p.; \\ \forall x_k(\binom{x_i}{p}(\binom{x_j}{x_k}(\alpha))) & \text{si } x_i \text{ és lliure en } \gamma \text{ i } x_j \text{ es lliure en } p \text{ i } k \text{ és el menor índex ;} \\ & \text{tal que } x_k \text{ és lligat en } \gamma \text{ i en } p. \end{cases}$$

Si θ és una fórmula i t és un terme escriurem $\theta(t)$ per referir-nos a $\binom{x}{t}(\theta)$.

Definició 21. Una **$\mathcal{L}$-sentència** serà una fórmula del llenguatge $\mathcal{L}$ on totes les variables de la fórmula no són lliures en la fórmula.

1.3 El sistema deductiu Λ

En aquesta secció presentarem el sistema deductiu emprat al llibre d'Enderton [1]. En primer lloc, però, introduirem el concepte de valoració, que ens permetrà associar un valor de veritat a les fórmules d'un llenguatge. Com podem fer tal cosa? La idea és emprar l'estructura de model per relacionar els símbols i les expressions sintàctiques d'un llenguatge formal amb relacions matemàtiques sobre el conjunt matemàtic que modelen, on sí podem distinguir si una certa relació se satisfà o no.

Definició 22. Siga $\mathcal{L}$ un llenguatge, siga $X = \{x_i \mid i \in \mathbb{N}\}$ un conjunt de variables i siga $\mathbf{A} = (A, F_\Sigma, F_\Theta)$ un model de $\mathcal{L}$. Una **valoració** és una aplicació $\mathrm{val} : X \to \mathbf{A}$.

Notem que per la propietat universal de l'àlgebra de termes existeix un únic homomorfisme $\mathrm{val}^{\#} : \mathbf{T}_\Sigma(X) \longrightarrow \mathbf{A}$ que fa commutatiu el diagrama:

$$\begin{array}{ccc} X & \xrightarrow{\eta_X} & \mathbf{T}_\Sigma(X) \\ & \searrow^{\mathrm{val}} & \downarrow{\scriptstyle \mathrm{val}^{\#}} \\ & & \mathbf{A} \end{array}$$

Considerem ara una valoració particular. Donats $x \in X$, $a \in A$, considerem la següent funció:

$$\begin{array}{rccl} \mathrm{val}(\binom{x}{a}) : & X & \longrightarrow & \mathbf{A} \\ & x_i & \longmapsto & \begin{cases} a & \text{si } x_i = x \\ \mathrm{val}(x_i) & \text{en altre cas.} \end{cases} \end{array}$$

Aquesta darrera valoració ens permet indentificar quan una variable està sotmessa a l'acció d'un quantificador. L'últim diagrama ens permet treballar les valoracions sobre l'àlgebra de termes. Així, definim quan γ és **certa** en **$\mathbf{A}$ d'acord amb una valoració** val, i ho denotem per $\mathbf{A} \underset{\mathrm{val}}{\vDash} \gamma$, de forma recursiva com segueix:

1. Siga $\gamma = \theta((P_j)_{j\in\mathbf{n}})$ una fórmula atòmica amb un símbol de relació $\theta \in \Theta$ d'aritat n i una família de termes $(P_j)_{j\in\mathbf{n}}$ en $\mathbf{T}_\Sigma(X)^n$. Així, direm que

$$\mathbf{A} \underset{\mathrm{val}}{\vDash} \gamma \quad \text{si, i només si,} \quad \theta^{\mathbf{A}}((\mathrm{val}^{\#}(P_j)_{j\in\mathbf{n}})).$$

2. Siga $\gamma = \neg\alpha$, per a una fórmula α en $\mathrm{Form}(\mathcal{L}, X)$. Així direm que

$$\mathbf{A} \underset{\mathrm{val}}{\vDash} \gamma \text{ si, i només si } \mathbf{A} \underset{\mathrm{val}}{\nvDash} \alpha.$$

3. Si $\gamma = \alpha \to \beta$ per a fórmules $\alpha, \beta \in \mathrm{Form}(\mathcal{L}, X)$ direm que:

$$\mathbf{A} \underset{\mathrm{val}}{\vDash} \gamma \text{ si, i només si } \mathbf{A} \underset{\mathrm{val}}{\nvDash} \alpha \text{ o bé } \mathbf{A} \underset{\mathrm{val}}{\nvDash} \beta.$$

4. Si $\gamma = \forall x_j(\alpha)$ per a una variable $x_j \in X$ i una fórmula $\alpha \in \mathrm{Form}(\mathcal{L}, X)$ direm que:

$$\mathbf{A} \underset{\mathrm{val}}{\vDash} \gamma \text{ si, i només si } \forall a \in \mathbf{A}(\mathbf{A} \underset{\mathrm{val}\binom{x_j}{a}}{\nvDash} \alpha).$$

Definició 23. Siga $\mathcal{L}$ un llenguatge, siga $X = \{x_i \mid i \in \mathbb{N}\}$ un conjunt de variables i siga $\mathbf{A} = (A, F_\Sigma, F_\Theta)$ un model de $\mathcal{L}$, i α una fórmula en $\mathrm{Form}(\mathcal{L}, X)$. Direm que la fórmula α és **certa** en A i ho denotarem $A \vDash \alpha$ quan, per a tota valoració $\mathrm{val} : X \longrightarrow \mathbf{A}$, es té que $\mathbf{A} \underset{\mathrm{val}}{\vDash} \alpha$.

A més, escriurem $\varnothing \vDash \tau$ si, i només si, qualsevol valoració (per als símbols en τ) satisfà τ. En aquest cas direm que τ és una **tautologia**. Una fórmula γ **implica tautològicament** la fórmula α si per a tota valoració $\mathrm{val} : X \longrightarrow \mathbf{A}$ que verifica $\mathbf{A} \underset{\mathrm{val}}{\vDash} \gamma$, aleshores $\mathbf{A} \underset{\mathrm{val}}{\vDash} \alpha$. Per tant podem definir la següent aplicació:

$$\begin{array}{rccl} \mathcal{V}: & \mathrm{Form}(\mathcal{L}, X) & \longrightarrow & \{V, F\} \\ & \alpha & \longmapsto & \begin{cases} V \text{ si } \alpha \text{ és certa en A;} \\ F \text{ en altre cas.} \end{cases} \end{array}$$

Així, $\mathcal{V}$ ens permet assignar un valor de veritat a cada fórmula del llenguatge. Abans d'introduïr el sistema deductiu d'Enderton, definim la generalització d'una fórmula del llenguatge.

Definició 24. Direm que una fórmula φ és una **generalització** de ψ si, i només si, per a algun $n \geqslant 0$ i algunes variables $x_1, \ldots, x_n$

$$\varphi = \forall x_1 \cdots \forall x_n \psi.$$

Notem que la definició inclou el cas $n = 0$; qualsevol fórmula és una generalització de si mateixa.

Ara ja podem introduïr el sistema deductiu Λ, el qual serà la nostra base axiomàtica de la lògica.

Definició 25. (Sistema deductiu Λ) Per a un llenguatge $\mathcal{L}$, construïm el sistema deductiu Λ, format per sis grups d'axiomes i una regla d'inferència:

- **Axiomes**. Els axiomes lògics seran totes les generalitzacions de fórmules amb la següent estructura, on x i y són variables i α i β són fórmules:

  AG1. Tautologies.

  AG2. $\forall x\alpha \to \binom{t}{x}\alpha$, on t és substituïble per x en α.

  AG3. $\forall x(\alpha \to \beta) \to (\forall x\alpha \to \forall x\beta)$.

  AG4. $\alpha \to \forall x\alpha$, on x no està lliure en α.

  AG5. $x = x$.

  AG6. $x = y \to (\alpha \to \alpha')$, on α és una fórmula atòmica i α' sobté de α reemplaçant x en zero o més (però no necessàriament totes) posicions per y.

- **Modus ponens**. Aquesta regla d'inferència ens permetrà transformar els axiomes en noves fórmules:

$$\text{De } \alpha \text{ i } \alpha \to \beta \text{ és conseqüència immediata } \beta.$$

Considerem una col·lecció de fórmules Γ. Una **deducció sintàctica** en Λ a partir de Γ és una successió finita $\alpha_1, \ldots, \alpha_n$ de fórmules de $\mathcal{L}$ tals que cada α_i és un axioma de Λ, una fórmula de Γ o una inferència de les fórmules anteriors de la successió. Les fórmules de Γ es diuen **premisses** de la deducció. Una fórmula α és una **conseqüència** en Λ d'una col·lecció de fórmules Γ si α és l'última fórmula d'una deducció sintàctica en Λ a partir de Γ. Ho representarem amb la notació $\Gamma \vdash \alpha$.

A més, una fórmula α és un **teorema** de F si és l'última fórmula d'una demostració en F. Aquest sistema deductiu permet deduir sintàcticament, a partir dels seus grups d'axiomes i la regla d'inferència, proposicions lògiques que involucren només els símbols que són comuns en tots els llenguatges formals. Per tant aquest sistema només pot deduir proposicions elementals de la lògica de primer ordre, com per exemple:

$$\text{Si } \alpha, \text{ aleshores } \alpha \to \alpha.$$

Així doncs Λ és una infraestructura sintàctica de la lògica. Per referir-nos a d'altres objectes matemàtics, com els nombres naturals i les operacions aritmètiques, ens caldrà afegir més axiomes que involucren els símbols que els representen. A les ampliacions del sistema deductiu Λ les anomenarem *teories formals*, i les presentarem a la propera secció. Però abans, presentem una sèrie de propietats bàsiques del sistema deductiu Λ que emprarem més endavant.

Proposició 2. (**Regla T**). Si $\Gamma \vdash \alpha_1, \ldots, \Gamma \vdash \alpha_n$ i $\{\alpha_1, \ldots, \alpha_n\}$ implica tautològicament β, aleshores $\Gamma \vdash \beta$.

Demostració. Com $\alpha_1 \to \cdots \to \alpha_n \to \beta$ és una tautologia, aleshores és un axioma lògic. Per tant, si apliquem el modus ponens n voltes tenim allò que volíem.

Teorema 2. (Principi de generalització) Si per a una fórmula φ i una col·lecció de fórmules Γ es verifica $\Gamma \vdash \varphi$, i x no està lliure en les fórmules Γ, aleshores $\Gamma \vdash \forall x \varphi$.

Demostració. La demostració pot trobar-se a la pàgina 117 de [1].

Teorema 3. (Teorema de la deducció) Si Γ és una col·lecció de fórmules, i $\gamma \vdash \varphi$, per a unes fórmules γ i φ, aleshores $\Gamma \vdash (\gamma \to \varphi)$.

Demostració. La demostració pot trobar-se a la pàgina 118 de [1].

Ara provarem que del sistema deductiu Λ es poden deduir sintàcticament les propietats reflexiva, simètrica i transitiva del símbol $=$, com caldria esperar. La propietat transitiva correspon al Exercici 11 del segon capítol de [1].

Proposició 3. El símbol $=$ té les següents propietats sintàctiques:

1. (Reflexiva). $\Lambda \vdash \forall x (x = x)$.
2. (Simetrica). $\Lambda \vdash \forall x \forall y (x = y \to y = x)$.
3. (Transitiva). $\Lambda \vdash \forall x \forall y \forall z (x = y \to y = z \to x = z)$.

Demostració. 1. La propietat reflexiva l'hem introduït en el grup d'axiomes AG5.

2. La propietat reflexiva se segueix del següent raonament:

$$\Lambda \vdash x = y \to x = x \to y = x \tag{1.2}$$
$$\Lambda \vdash x = x \tag{1.3}$$
$$\Lambda \vdash x = y \to y = x \tag{1.4}$$
$$\Lambda \vdash \forall x \forall y (x = y \to y = x) \tag{1.5}$$

On hem emprat AG6, AG5, la regla T i el principi de generalització, en eixe ordre.

3. La propietat transitiva se segueix del següent raonament:

$$\Lambda \vdash x = y \tag{1.6}$$
$$\Lambda \vdash y = x \tag{1.7}$$
$$\Lambda \vdash y = z \tag{1.8}$$
$$\Lambda \vdash y = x \to \varphi(y) \to \varphi(x) \tag{1.9}$$
$$\Lambda \vdash y = z \to x = z \tag{1.10}$$
$$\Lambda \vdash x = y \to (y = z \to x = z) \tag{1.11}$$
$$\Lambda \vdash \forall x \forall y \forall z (x = y \to (y = z \to x = z)) \tag{1.12}$$

On (1.6) és la nostra premisa, en (1.7) hem aplicat la propietat simètrica a la premissa, en (1.9) fem ús de AG6, en (1.10) identifiquem $\varphi(y)$ amb la fórmula $y = z$ del pas anterior, en (1.11), pel teorema de deducció (1.6) $\to$ ((1.8) $\to$ (1.10)). Per acabar hem aplicat el principi de generalització a cada variable a l'últim pas.

1.4 La teoría aritmètica Q

Per als nostres propòsits, una **teoria axiomàtica** (de primer ordre) sobre un cert llenguatge $\mathcal{L}$ serà una col·lecció d'axiomes que inclouran una sèrie de fórmules de $\mathcal{L}$, les quals anomenarem axiomes propis de la teoria, i els axiomes i regles d'inferència de Λ, als quals anomenarem axiomes lògics. Després de tota aquesta construcció general de les seccions anteriors, ja tenim les eines suficients per a formalitzar l'aritmètica dels nombres naturals.

Definició 26. Considerem el **llenguatge de l'aritmètica** $\mathcal{L}_{\mathbb{N}}$, format pels següents conjunts:

(a) Una signatura de símbols de funció $\Sigma_{\mathbb{N}} = \{0, S, +, \cdot\}$ amb tres símbols de funció $S, +, \cdot$, d'aritats 0, 1, 2 i 2 respectivament.

(b) Una signatura de símbols de relació $\Theta_{\mathbb{N}} = \{=, <\}$ amb un símbol de relació $<$, d'aritat 2, a més del símbol obligatori $=$, d'aritat 2.

Recordant els convenis d'escriptura que hem introduït a la secció anterior, si t_1, t_2 són dos termes de $\mathcal{L}_{\mathbb{N}}$, escriurem

$$t_1 + t_2 \text{ per referir-nos a } +t_1t_2,$$
$$t_1 \cdot t_2 \text{ per referir-nos a } \cdot t_1t_2.$$

Definició 27. Sobre el llenguatge $\mathcal{L}_{\mathbb{N}}$ definim la **teoria Q** donada pels axiomes:

Q1. $\forall x(Sx \neq 0)$. L'intepretació d'aquest axioma és que el símbol 0 no és el succesor de cap nombre.

Q2. $\forall x \forall y\,(Sx = Sy \to x = y)$. És a dir, si dos nombres tenen el mateix succesor aleshores són ser iguals.

Q3. $\forall x(x + 0 = x)$. És a dir, si sumem zero a qualsevol nombre el resultat és el mateix nombre.

Q4. $\forall x \forall y\,(x + Sy = S(x + y))$. Amb aquest axioma definim recursivament la suma habitual de nombres naturals.

Q5. $\forall x(x \cdot 0 = 0)$. És a dir, el resultat de multiplicar qualsevol nombre natural per zero és zero.

Q6. $\forall x \forall y\,(x \cdot Sy = x \cdot y + x)$. Amb aquest axioma definim recursivament el producte dels nombres naturals.

Q7. $\forall x \neg(x < 0)$. Amb aquest axioma captem que cap nombre natural pot ser menor que zero.

Q8. $\forall x \forall y(x < Sy \longleftrightarrow x < y \vee x = y)$. És a dir, que un nombre és menor que el succesor d'un segon nombre si i només si és menor o igual que el segon.

Q9. $\forall x \forall y(x < y \vee x = y \vee y < x)$. Amb aquest axioma captem l'ordre total dels nombres naturals.

A més, per a tota fórmula α que tinga lliure la variable x, considerem el següent esquema axiomàtic:

$$(({}^{x}_{0})\alpha \wedge \forall x(\alpha \to ({}^{x}_{Sx})\alpha) \to \alpha.$$

Aquest esquema determina infinits axiomes, un per a cada fórmula α possible. L'anomenarem **esquema inductiu**. Si afegim l'esquema inductiu a la col·lecció d'axiomes de Q, obtenim una nova teoria anomenada **aritmètica de Peano**. Donat un nombre natural n, definim la següent fórmula de $\mathcal{L}_{\mathbb{N}}$:

$$\underline{n} = \underbrace{SS\cdots S}_{n \text{ voltes}}0.$$

Cal adonar-se que aquesta col·lecció d'axiomes Q i aquesta darrera fórmula conformen un model per a l'aritmètica, si interpretem el símbol 0 com el nombre natural 0, el símbol S com la funció unària que a cada natural li assigna el seu successor i, els símbols d'operació $+$ i $\cdot$ com les operacions suma i producte, i els símbols de relació $=$ i $<$ amb les relacions igualtat i menor igual de l'aritmètica. Per acabar el capítol, provarem algunes propietats sintàctiques de la teoria Q que emprarem més endavant en la prova del teorema de representabilitat en Q, a l'últim capítol.

Lema 1. Siguen $m, n \in \mathbb{N}$ tals que $m = n$, aleshores $Q \vdash \underline{m} = \underline{n}$. A més, si $m \neq n$, aleshores $Q \vdash \neg(\underline{m} = \underline{n})$.

Demostració. Si $m = n$ el resultat és clar, ja que

$$\underline{m} = \underbrace{SS\cdots S}_{m \text{ voltes}}0 = \underbrace{SS\cdots S}_{n \text{ voltes}}0 = \underline{n}.$$

Ara si $m \neq n$, ho provem per inducció sobre n.

- Per al cas base, si $n = 0$, i $m \neq 0$ el resultat es cert, ja que si $m \neq n$ aleshores podem expressar $\underline{m}$ de la forma Sx per a cert terme $x \in \mathcal{L}$. Aleshores de l'Axioma Q1 ($\forall x(Sx \neq 0)$) se segueix:

  $$Q \vdash \neg(\underline{m} = 0).$$

- Suposem que el resultat és cert per a n. Així, si $m \in \mathbb{N}$ amb $m \neq n + 1$, volem provar que

  $$Q \vdash \neg(\underline{m} = \underline{n+1}).$$

  Distingim dos casos:

  1. Si $m = 0$, notem que podem expressar $\underline{n+1}$ com $S\underline{n}$. De l'Axioma Q1 deduïm:

     $$Q \vdash \neg(0 = \underline{n+1}).$$

  2. Suposem ara que $m \neq 0$, aleshores $\underline{m}$ és de la forma $\underline{m} = S(\underline{m-1})$. Com $m \neq n+1$ i $m-1 \neq n$, si apliquem la hipòtesi inductiva deduïm

     $$Q \vdash \neg(\underline{m-1} = \underline{n}).$$

     Si emprem l'Axioma Q2($\forall x \forall y(Sx = Sy \to x = y)$). Deduïm que

     $$Q \vdash \forall x \forall y(x \neq y \to Sx \neq Sy).$$

     A més com $\underline{n+1} = S\underline{n}$ i $\underline{m} = S(\underline{m-1})$, obtenim:

     $$Q \vdash \neg(\underline{m} = \underline{n+1}).$$

     Així, el lema queda provat.

Lema 2. Siguen $m, n \in \mathbb{N}$, aleshores $Q \vdash \underline{m} + \underline{n} = \underline{m+n}$.

Demostració. Fem una prova per inducció sobre n.

- Si $n = 0$, el resultat se segueix de l'axioma Q3($Q \vdash \forall x(x + 0 = x)$), ja que per a qualsevol $m \in \mathbb{N}$ m+0=m i també
$$\underline{m} + 0 = \underline{m} = \underline{m + 0}.$$

- Suposem que el resultat es verifica per a n. Volem provar que també es verifica per a $n + 1$. Per hipotesi, si $m \in \mathbb{N}$ aleshores
$$Q \vdash (\underline{m} + \underline{n} = \underline{m+n}).$$
Notem que $\underline{n+1} = S\underline{n}$. D'altra banda, l'Axioma Q4 ens diu que
$$Q \vdash \forall x \forall y(x + Sy = S(x + y))$$
Aleshores
$$Q \vdash (\underline{m} + S\underline{n} = S(\underline{m} + \underline{n})).$$
Notem que $\underline{m} + \underline{n+1}$ és una abreviatura de $\underline{m} + S\underline{n}$. D'altra banda $\underline{m+n+1} = S(\underline{m+n})$. Per hipòtesi inductiva:
$$Q \vdash \underline{m} + \underline{n} = \underline{m+n}.$$
Aleshores si emprem la tautología $\vdash x = y \to Sx = Sy$ obtenim:
$$Q \vdash S(\underline{m} + \underline{n}) = S(\underline{m+n}).$$
Finalment per la transitivitat de la igualtat
$$Q \vdash \underline{m} + \underline{n+1} = \underline{m+n+1}.$$
Per tant el lema queda provat.

Lema 3. Siguen $m, n \in \mathbb{N}$, aleshores $Q \vdash \underline{m} \cdot \underline{n} = \underline{m \cdot n}$.

Demostració. Fem inducció sobre n.

- Per al cas base $n = 0$, el l'Axioma Q5 implica que
$$\underline{m} \cdot 0 = 0 = \underline{m \cdot 0},$$
com volíem.

- Suposem que el resultat és cert per a n, és a dir $Q \vdash \underline{m} \cdot \underline{n} = \underline{m \cdot n}$. Notem que $S\underline{n} = \underline{n+1}$ i així:
$$Q \vdash \underline{m} \cdot \underline{n+1} = \underline{m \cdot n} + \underline{m} \tag{1.13}$$
$$Q \vdash \underline{m} \cdot \underline{n+1} = \underline{m \cdot n} + \underline{m} \tag{1.14}$$
$$Q \vdash \underline{m} \cdot \underline{n+1} = \underline{m \cdot n + m} = \underline{m \cdot (n+1)} \tag{1.15}$$
on hem aplicat l'Axioma Q6 en (1.13), l'hipòtesi inductiva en (1.14), i hem tret factor comú en (1.15). Per tant de la transitivitat de l'igualtat obtenim el resultat.

Lema 4. Siguen $m, n \in \mathbb{N}$:

1. Si $m < n$, aleshores $Q \vdash \underline{m} < \underline{n}$.
2. Si $m \geqslant n$, és te que $Q \vdash \neg(\underline{m} < \underline{n})$.

Demostració. Anem a fer inducció sobre n en tots dos casos.

- Per al cas base $n = 0$, no podem trobar un $m \in \mathbb{N}$ tal que $m < 0$, per tant només caldria considerar la segona part de l'enunciat. Així, si $m \in \mathbb{N}$ amb $m > 0$ aleshores de l'Axioma Q7:

$$Q \vdash \neg(\underline{m} < 0)$$

com volíem.

- Suposem-ho cert per a n. Aleshores si $m \in \mathbb{N}$ tenim les següents hipòtesis inductives per a cada cas:

1. Si $m < n$, aleshores $Q \vdash (\underline{m} < \underline{n})$;
2. Si $m \geqslant n$, aleshores $Q \vdash \neg(\underline{m} < \underline{n})$.

Anem a provar-ho per a $n + 1$. En primer lloc considerem el primer cas i suposem que $m < n + 1$. Aleshores pot ocórrer:

- $m < n$, i en aquest cas $Q \vdash \underline{m} < \underline{n}$ per la hipòtesi inductiva.
- $m = n$. Aleshores $Q \vdash \underline{m} = \underline{n}$ pel Lema 1.

En tots dos casos, si apliquem l'axioma Q8:

$$\forall x \forall y(x < Sy \longleftrightarrow x < y \vee x = y)$$

i la Regla T, se segueix

$$Q \vdash \underline{m} < S\underline{n} = \underline{n+1}.$$

Per al segon cas, suposem que $m \geqslant n + 1$, i per tant poden donar-se els següents dos casos:

- $m > n$, i per tant $Q \vdash \neg(\underline{m} < \underline{n})$ per la hipòtesi inductiva.
- $m \neq n$. Aleshores $Q \vdash \neq (\underline{m} = \underline{n})$ pel Lema 1.

Novament, de l'axioma Q8 i la regla T se segueix que $Q \vdash \neg(\underline{m} < \underline{n} + 1)$, com volíem.

En resum, en aquest capítol hem formalitzat l'aritmètica mitjançant la teoría aritmètica de Peano. Per fer això, en primer lloc hem construït les àlgebres de termes i les fórmules d'un llenguatge, que no són més que certes cadenes de símbols. Després, mitjançant el concepte de model, hem pogut assignar a cada fórmula un valor de veritat i hem introduït el sistema de deducció formal Λ. Finalment, hem ampliat Λ amb el llenguatge $\mathcal{L}_{\mathbb{N}}$ i els axiomes de la teoria Q.

Com hem vist a la introducció, una vegada introduïda aquesta formalització és natural preguntar-se si la teoría aritmètica de Peano és completa i consistent, és a dir, si d'aquesta es poden deduir totes les proposicions vertaderes de la teoría i no poden deduir-se proposicions mutuament contradictòries. Per respondre aquesta pregunta, treballarem la teoría de la recursivitat al següent capítol.

Capítol 2

Recursivitat

2.1 Funcions i relacions recursives

2.1.1 L'axiomàtica de la teoría de la recursivitat

En la primera meitat del segle passat els matemàtics es preguntaven quines operacions podrien dur a terme les màquines programables, és a dir, quines operacions eren computables. Tot i que les computadores amb què comptaven en l'època encara eren prototips experimentals primitius -mecànics la majoria d'ells- la investigació en aquesta àrea va ser molt fructífera i es va avançar significativament cap al concepte de computadora moderna. D'entre tots els matemàtics que investigaren aquesta àrea, Alan Turing és el més conegut, i a ell li devem el concepte de màquina de Turing, un model general que abstrau i capta les propietats de les màquines programables.

Així, en aquest treball una operació serà computable si és computable per una màquina de Turing. Per als nostres propòsits, no ens caldrà treballar la definició de màquina de Turing, ja que l'estudi d'aquesta disciplina va permetre establir quines són les funcions elementals a partir de les quals, i mitjançant unes regles particulars, és possible descriure qualsevol altra funció computable. Les enumerem a continuació.

Definició 28. Considerem les següents funcions elementals:

F1. Per a $n \in \mathbb{N}$, $i \in \mathbf{n}$, considerem la projecció i-èssima:

$$\begin{array}{rccc} \Pi_i^n: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_j)_{j\in\mathbf{n}} & \longmapsto & x_i \end{array}$$

F2. La suma de naturals:

$$\begin{array}{rccc} +: & \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ & (x_1, x_2) & \longmapsto & x_1 + x_2 \end{array}$$

F3. El producte de naturals:

$$\begin{array}{rccc} \cdot: & \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ & (x_1, x_2) & \longmapsto & x_1 \cdot x_2 \end{array}$$

F4. La funció característica de la relació binaria menor estricte.

$$\begin{array}{rccc} \mathcal{X}_<: & \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ & (x_1, x_2) & \longmapsto & \begin{cases} 1 & \text{si } x_1 \geqslant x_2; \\ 0 & \text{en altre cas.} \end{cases} \end{array}$$

Considerem ara una altra funció que serà principal en la construcció, la funció minimització.

Definició 29. (**Funció minimització**). Siga $G : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$ una funció tal que per a tota seqüència de nombres naturals $(x_i)_{i\in\mathbf{n}} \in \mathbb{N}^n$, existeix algun $x \in \mathbb{N}$ de manera que

$$G((x_i)_{i\in\mathbf{n}}, x) = 0. \tag{2.1}$$

Aleshores podem considerar la següent **funció minimització**:

$$\begin{array}{rccl} \mu x.G: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_i)_{i\in\mathbf{n}} & \longmapsto & min\{x \in \mathbb{N} \mid G((x_i)_{i\in\mathbf{n}}, x) = 0\}. \end{array}$$

Com que estem suposant que existeix almenys un x que verifica (2.1), aleshores aquesta funció està ben definida. Ara definim la composició habitual de funcions definides sobre els nombres naturals.

Definició 30. Siguen $G : \mathbb{N}^n \longrightarrow \mathbb{N}^m$ i $H : \mathbb{N}^m \longrightarrow \mathbb{N}$ dues funcions. Anomenem **funció composada** de H amb G a la funció:

$$\begin{array}{rccl} H \circ G: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_i)_{i\in\mathbf{n}} & \longmapsto & H(G((x_i)_{i\in\mathbf{n}})). \end{array}$$

Ara ja estem en condicions de definir quan una funció definida sobre els nombres naturals és recursiva.

Definició 31. (**Funció recursiva**) Una funció de $\mathbb{N}^n$ a $\mathbb{N}$ direm que és **recursiva** o **computable** si és alguna de les funcions $\mathbf{F1}, \mathbf{F2}, \mathbf{F3}, \mathbf{F4}$ o és el resultat d'aplicar un nombre finit de vegades alguna de les següents lleis:

(R1) Si $G : \mathbb{N}^n \longrightarrow \mathbb{N}$ és una funció recursiva i $(H_i)_{i\in\mathbf{n}}$ és una família de funcions recursives amb $H_i : \mathbb{N}^m \longrightarrow \mathbb{N}$ per a cada $i \in \mathbf{n}$, aleshores la composició

$$\begin{array}{rccl} G \circ ((H_i)_{i\in\mathbf{n}}): & \mathbb{N}^m & \longrightarrow & \mathbb{N} \\ & (x_j)_{j\in\mathbf{m}} & \longmapsto & G((H_i(x_j)_{j\in\mathbf{m}})_{i\in\mathbf{n}}). \end{array}$$

és una funció recursiva. A aquesta composició l'anomenarem **composició recursiva**.

(R2) Siga $G : \mathbb{N}^{n+1} \longrightarrow \mathbb{N}$ una funció recursiva que verifica les condicions exigides en la definició de funció minimització. Aleshores la minimització $\mu x.G : \mathbb{N}^n \longrightarrow \mathbb{N}$ és una funció recursiva.

A més, podem extendre aquest concepte a les relacions mitjançant les funcions característiques:

Definició 32. (**Relació recursiva**) Una relació $R \subseteq \mathbb{N}^n$ direm que és **recursiva** o **computable** si la funció característica de R, $\mathcal{X}_R$, és una funció recursiva.

2.1.2 Propietats de les funcions recursives

Ara que ja hem donat la definició de les funcions recursives, anem a comprovar que les següents funcions, composicions i relacions matemàtiques habituals, que emprarem repetidament en aquest capítol, són recursives.

Propietat 1. Donada una funció $\sigma : \mathbf{m} \longrightarrow \mathbf{n}$, si $G : \mathbb{N}^m \longrightarrow \mathbb{N}$ és una funció recursiva aleshores la funció

$$\begin{array}{rccl} F: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_i)_{i\in\mathbf{n}} & \longmapsto & G((x_{\sigma(j)})_{j\in\mathbf{m}}), \end{array}$$

que fa actuar G sobre una permutació dels índexs d'una certa seqüencia també és recursiva.

Demostració. Notem que

$$F((x_i)_{i\in\mathbf{n}}) = G((x_{\sigma(j)})_{j\in\mathbf{m}}) = G \circ ((\Pi^n_{\sigma(j)}((x_i)_{i\in\mathbf{n}}))_{j\in\mathbf{m}}).$$

És a dir, F pot expressar-se com una composició recursiva, i per tant és recursiva.

Propietat 2. Siga $Q \subseteq \mathbb{N}^m$ una relació recursiva i siga $(H_i)_{i\in\mathbf{m}}$ una família de funcions de manera que, per a cada $i \in \mathbf{m}$, la funció $H_i : \mathbb{N}^n \longrightarrow \mathbb{N}$ és recursiva. Aleshores la relació

$$P = \{(x_i)_{i\in\mathbf{n}} \in \mathbb{N}^n \mid Q((H_j((x_i)_{i\in\mathbf{n}}))_{j\in\mathbf{m}})\},$$

també és una relació recursiva. És a dir, les relacions que actuen sobre la imatge de funcions recursives són recursives.

Demostració. Donat un $(x_i)_{i\in\mathbf{n}} \in \mathbb{N}^n$ es verifica

$$\mathcal{X}_P((x_i)_{i\in\mathbf{n}}) = \mathcal{X}_Q \circ ((H_j((x_i)_{i\in\mathbf{n}}))_{j\in\mathbf{k}}),$$

on aquesta última expressió és una composició recursiva, i per tant la relació P és recursiva.

Propietat 3. Si $P \subseteq \mathbb{N}^{n+1}$ és una relació recursiva tal que, per a tota seqüència $(x_i)_{i\in\mathbf{n}} \in \mathbb{N}^n$ existeix un $x \in \mathbb{N}$ de manera que $P((x_i)_{i\in\mathbf{n}}, x)$, aleshores la funció

$$\begin{array}{rccc} F: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_i)_{i\in\mathbf{n}} & \longmapsto & \mu x.P((x_i)_{i\in\mathbf{n}}, x), \end{array}$$

que dona el mínim nombre natural que verifica la relació, és una funció recursiva.

Demostració. Com $F((x_i)_{i\in\mathbf{n}}) = \mu x.\mathcal{X}_P((x_i)_{i\in\mathbf{n}}, x)$ i $\mathcal{X}_P$ és una funció recursiva podem aplicar **(R2)** per concloure que F és recursiva.

Propietat 4. Donat $c \in \mathbb{N}$, l'aplicació constant

$$\begin{array}{rccc} \mathcal{K}_c^n: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_i)_{i\in\mathbf{n}} & \longmapsto & c \end{array}$$

és una funció recursiva.

Demostració. Fem la prova per inducció sobre c. Si $c = 0$

$$\mathcal{K}_0^n((x_i)_{i\in\mathbf{n}}) = 0 = \mu x.\Pi_{n+1}^{n+1}((x_i)_{i\in\mathbf{n}}, x),$$

i aquesta última funció és recursiva per **(R2)**. Ara per al pas inductiu:

$$\begin{aligned} \Pi_{c+1}^n((x_i)_{i\in\mathbf{n}}) &= c+1 \\ &= min\{x \in \mathbb{N} : c < x\} \\ &= min\{x \in \mathbb{N} : \Pi_{c+1}^n((x_i)_{i\in\mathbf{n}}, x) < x\} \\ &= \mu x.(\Pi_c^n((x_i)_{i\in\mathbf{n}}) < x), \end{aligned}$$

on aquesta darrera funció es recursiva en ser una composició recursiva

Propietat 5. Si $Q, P \subseteq \mathbb{N}^n$ són relacions recursives aleshores:

(a) La relació negació $\neg P := \mathbb{N}^n - P$ és recursiva.

(b) La relació conjunció $P \vee Q := P \cup Q$ és recursiva.

(c) La relació disjunció $P \wedge Q := P \cap Q$ és recursiva.

Demostració. (a) La relació $P \vee Q := P \cup Q$ és recursiva, ja que

$$\mathcal{X}_{P\vee Q}((x_i)_{i\in\mathbf{n}}) = \mathcal{X}_P((x_i)_{i\in\mathbf{n}})\mathcal{X}_Q((x_i)_{i\in\mathbf{n}}).$$

(b) La relació $P \wedge Q := P \cap Q$ és recursiva, ja que, per la llei de Morgan,

$$P \wedge Q = \neg(\neg P \vee (\neg Q)).$$

(c) La relació $(\neg P \vee (\neg Q))$ és recursiva pels apartats (a) i (b) anteriors.

Propietat 6. Les relacions $=, \leqslant, \geqslant, >$ en $\mathbb{N}^2$ són recursives.

Demostració. Si $a, b \in \mathbb{N}$, el resultat se segueix de les següents equivalències i d'aplicar la Propietat 5:

(a) Notem que $a = b \Leftrightarrow \neg(a < b) \wedge \neg(b < a)$.

(b) Notem que $a \geqslant b \Leftrightarrow \neg(a < b)$.

(c) Notem que $a > b \Leftrightarrow (a \geqslant b) \wedge \neg(a = b)$.

(d) Notem que $a \leqslant b \Leftrightarrow \neg(a > b)$.

Definició 33. Considerem dues seqüències $(x_i)_{i\in\mathbf{n}} \in \mathbb{N}^n$, $(y_i)_{i\in\mathbf{m}} \in \mathbb{N}^m$, una funció $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ i una relació $P \subseteq \mathbb{N}^{m+1}$. Aleshores:

(a) Escriurem $\mu x < f((x_i)_{i\in\mathbf{n}})P(x, (y_i)_{i\in\mathbf{m}})$ per denotar a

$$\mu x.(P(x, (y_i)_{i\in\mathbf{m}}) \vee x = f((x_i)_{i\in\mathbf{n}})).$$

Aquesta minimització retorna el menor nombre natural x menor que $f((x_i)_{i\in\mathbf{n}}))$ de manera que $P(x, (y_i)_{i\in\mathbf{m}})$, si aquest existeix, o $f((x_i)_{i\in\mathbf{n}}))$ en altre cas.

(b) Escriurem $\exists x < f((x_i)_{i\in\mathbf{n}})P(x, (y_i)_{i\in\mathbf{m}})$ per denotar la sentència lògica

$$(\mu x < f((x_i)_{i\in\mathbf{n}})P(x, (y_i)_{i\in\mathbf{m}})) < f((x_i)_{i\in\mathbf{n}}).$$

Aquesta darrera sentència es verifica si existeix un natural $x < f((x_i)_{i\in\mathbf{n}})$ de manera que $P(x, (y_i)_{i\in\mathbf{m}})$.

(c) Escriurem $\forall x < f((x_i)_{i\in\mathbf{n}})P(x, (y_i)_{i\in\mathbf{m}})$ per denotar la sentència lògica

$$\neg(\exists x < f((x_i)_{i\in\mathbf{n}})(\neg P(x, (y_i)_{i\in\mathbf{m}}))).$$

Aquesta es verifica si tot nombre natural $x < f((x_i)_{i\in\mathbf{n}})$ satisfà $P(x, (y_i)_{i\in\mathbf{m}})$.

Propietat 7. Siga $P \subseteq \mathbb{N}^{n+1}$ una relació recursiva. Aleshores la funció

$$\begin{array}{rccc} F: & \mathbb{N}^{n+1} & \longrightarrow & \mathbb{N} \\ & (a, (y_i)_{i\in\mathbf{n}}) & \longmapsto & \mu x < aP(x, (y_i)_{i\in\mathbf{m}}), \end{array}$$

que donat un nombre natural A i una seqüència de nombres naturals, retorna el mínim nombre natural menor que a que satisfà la relació P, és recursiva.

Demostració. Considerem una seqüència $(y_i)_{i\in\mathbf{n}}$ i un nombre $a \in \mathbb{N}$. Aleshores

$$F(a, (y_i)_{i\in\mathbf{n}}) = \mu x < aP(x, (y_i)_{i\in\mathbf{m}}) = \mu x(P \vee B),$$

on estem considerant les funcions:

$$\mathcal{X}_P : \begin{array}{ccc} \mathbb{N}^{n+1} & \longrightarrow & \mathbb{N} \\ (a, (y_i)_{i\in\mathbf{n}}) & \longmapsto & \begin{cases} 1 & \text{si } \neg P(a, (y_i)_{i\in\mathbf{n}}); \\ 0 & \text{si } P(a, (y_i)_{i\in\mathbf{n}}). \end{cases} \end{array} \qquad \beta : \begin{array}{ccc} \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ (x, a) & \longmapsto & \begin{cases} 1 & \text{si } x = a; \\ 0 & \text{si } x \neq a. \end{cases} \end{array}$$

Com $B(a, a) = 0$ i $\mathcal{X}_P((y_i)_{i\in\mathbf{n}}, a) = 0$ se segueix que

$$\mathcal{X}_P((y_i)_{i\in\mathbf{n}}, a) \vee \beta(a, a) = 0,$$

i per tant podem aplicar la Propietat 3 per concloure que F és recursiva.

Propietat 8. Considerem una relació recursiva $R \subseteq \mathbb{N}^{n+1}$. Aleshores:

(a) La relació

$$P(a,(y_i)_{i\in\mathbf{n}}) = \exists x < aR(x,(y_i)_{i\in\mathbf{n}}), \text{ que es verifica si, i només si, } \mu x < aR(x,(y_i)_{i\in\mathbf{n}}) < a,$$

és recursiva, ja que hem vist que la relació $<$ ho és i $\mu x < aR(x,(y_i)_{i\in\mathbf{n}})$ també ho és per la Propietat 7.

(b) La relació

$$Q(a,(y_i)_{i\in\mathbf{n}}) = \forall x < aR(x,(y_i)_{i\in\mathbf{n}}), \text{ que es verifica si, i només si, } \neg(\exists x < a(\neg(R(x,(y_i)_{i\in\mathbf{n}}))) < a,$$

és recursiva, ja que hem vist que la negació d'una relació recursiva és recursiva. Per tant, pel punt anterior, aquesta expressió és recursiva, ja que podem expressar-la com una composició recursiva.

Nota. **(Recursivitat i nombres primers)** Aquesta darrera propietat té implicacions notables. Donat $z \in \mathbb{N}$ denotem per $\mathrm{Div}(y,z)$ la relació donada per

$$\mathrm{Div}(y,z) \quad \text{si, i només si,} \quad \exists x < z+1(z = xy),$$

relació que es satisfà quan un nombre natural y divideix a z. Per la Propietat 8 és recursiva. A més a més la relació donada per

$$\mathrm{PN}(z) \quad \text{si, i només si,} \quad \neg(\exists y(y \neq 1 \wedge y \neq z \wedge \mathrm{Div}(y,z)))$$

també és recursiva per la Propietat 5 i la Propietat 6. D'ací es dedueix que **el conjunt de nombres primers és recursiu**, i és per això que els emprarem per codificar els elements dels llenguatges formals més endavant.

Propietat 9. La resta de naturals:

$$-_{\mathbb{N}}: \begin{array}{ccc} \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ (a,b) & \longmapsto & \begin{cases} a-b & \text{si } a \geqslant b \\ 0 & \text{en altre cas.} \end{cases} \end{array}$$

és recursiva.

Demostració. Tenim que $a -_{\mathbb{N}} b = \mu x(G \vee \mathcal{X}_<)$ on:

$$G: \begin{array}{ccc} \mathbb{N}^3 & \longrightarrow & \mathbb{N} \\ (a,b,x) & \longrightarrow & \begin{cases} 0 & \text{si } b+x=a; \\ 1 & \text{en altre cas.} \end{cases} \end{array} \qquad \mathcal{X}_<: \begin{array}{ccc} \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ (a,b) & \longmapsto & \begin{cases} 0 & \text{si } a<b; \\ 1 & \text{en altre cas.} \end{cases} \end{array} \tag{2.2}$$

i per tant és recursiva.

Propietat 10. Si $(G_i)_{i\in\mathbf{m}}$ és una familia de funcions recursives de manera que $G_i : \mathbb{N}^n \longrightarrow \mathbb{N}$ per a cada $i \in \mathbf{m}$ i $R_1, R_2, ..., R_m \subseteq \mathbb{N}^n$ són una família de relacions recursives verificant que $\forall (x_i)_{i\in\mathbf{n}} \exists! i: \ R_i((x_i)_{i\in\mathbf{n}})$ aleshores:

$$F((x_i)_{i\in\mathbf{n}}) = \begin{cases} G_1((x_i)_{i\in\mathbf{n}}) & \text{si } R_1((x_i)_{i\in\mathbf{n}}); \\ \quad \vdots & \\ G_m((x_i)_{i\in\mathbf{n}}) & \text{si } R_m((x_i)_{i\in\mathbf{n}}) \end{cases}$$

és recursiva. És a dir, si definim una funció emprant una família de relacions recursives que conformen una partició de $\mathbb{N}^n$, aleshores la relació és recursiva.

Demostració. Només cal adonarse de que

$$F = G_1\mathcal{X}_{\neg R_1} + ... + G_m\mathcal{X}_{\neg R_m}.$$

Per tant F és recursiva

Propietat 11. Si $(Q_i)_{i\in\mathbf{m}}$ és una familia de relacions recursives amb $Q_i \subseteq \mathbb{N}^n$ per a cada i i $(R_i)_{i\in\mathbf{m}} \subseteq \mathbb{N}^n$ són una familía de relacions recursives verificant que $\forall(x_i)_{i\in\mathbf{n}}\exists!i : \ R_i((x_i)_{i\in\mathbf{n}}))$ aleshores la relació $P \subseteq \mathbb{N}^n$ definida per

$$P((x_i)_{i\in\mathbf{n}})) \text{ sii } \begin{cases} Q_1((x_i)_{i\in\mathbf{n}}) & \text{si } R_1((x_i)_{i\in\mathbf{n}}) \\ \quad\vdots & \\ Q_m((x_i)_{i\in\mathbf{n}}) & \text{si } R_m((x_i)_{i\in\mathbf{n}}) \end{cases}$$

és recursiva, és a dir, si definim una relació per casos emprant una familía de relacions recursives que conformen una partició de $\mathbb{N}^n$, aleshores la relació és recursiva.

Demostració.

$$\mathcal{X}_P((x_i)_{i\in\mathbf{n}}) = \begin{cases} \mathcal{X}_{Q_1}((x_i)_{i\in\mathbf{n}}) & \text{si } R_1((x_i)_{i\in\mathbf{n}}); \\ \quad\vdots & \\ \mathcal{X}_{Q_m}((x_i)_{i\in\mathbf{n}}) & \text{si } R_m((x_i)_{i\in\mathbf{n}}). \end{cases}$$

i aquesta darrera funció és recursiva per la Propietat 10.

Així, ja tenim una infraestructura bàsica per reconèixer funcions recursives en altres contexts. A continuació platejarem una qüestió important de les funcions recursives.

2.1.3 Teorema de la negació

En aquesta secció aprofundirem en el concepte de funció recursiva, treballant la condició més forta de *relació recursivament enumerable.*

Definició 34. (**Recursivament enumerable**) Una relació $P \subseteq \mathbb{N}^n$ és **recursivament enumerable** si existeix una relació recursiva $Q \subseteq \mathbb{N}^{n+1}$ tal que, per a cada seqüència $(x_i)_{i\in\mathbf{n}} \in \mathbb{N}^n$,

$$P((x_i)_{i\in\mathbf{n}}) \quad \text{si, i només si,} \quad \exists x Q((x_i)_{i\in\mathbf{n}}, x).$$

Nota. Ens adonem que si una relació R és recursiva aleshores és recursivament enumerable ja que per a cada $(x_i)_{i\in\mathbf{n}} \in \mathbb{N}^n$ es té

$$R((x_i)_{i\in\mathbf{n}}) \quad \text{si, i només si,} \quad \exists x(R((x_i)_{i\in\mathbf{n}}) \wedge x = x).$$

El següent teorema dóna una resposta suficient, almenys per als nostres propòsits, a la pregunta que obria la secció. Aquest teorema l'emprarem a l'últim capítol quan tractem les teories *decidibles.*

Teorema 4. (De la Negació) Una relació $R \subseteq \mathbb{N}^n$ és recursiva si, i només si, R i $\neg R$ són recursivament enumerables.

Demostració. Suposem que R és recursiva. Aleshores $\neg R$ és recursiva per la Propietat 5. Així, tant R com $\neg R$ seràn recursivament enumerables per la nota anterior. Per al recíproc, suposem que tant R com $\neg R$ són recursivament enumerables. Aleshores existiràn dues relacions recursives $P, Q \subset \mathbb{N}^{n+1}$ de manera que, per a cada $(x_i)_{i\in\mathbf{n}}$:

$$R((x_i)_{i\in\mathbf{n}}) \quad \text{si, i només si,} \quad \exists x Q((x_i)_{i\in\mathbf{n}}, x)$$
$$\neg R((x_i)_{i\in\mathbf{n}}) \quad \text{si, i només si,} \quad \exists x P((x_i)_{i\in\mathbf{n}}, x).$$

Definim la funció:

$$\begin{array}{rccl} F: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_i)_{i\in\mathbf{n}} & \longmapsto & \mu x.(Q((x_i)_{i\in\mathbf{n}}, x) \vee P((x_i)_{i\in\mathbf{n}}, x)) \end{array}$$

La funció F és recursiva per la Propietat 3 ja que, necesàriament, alguna de les sentències $R((x_i)_{i\in\mathbf{n}})$ o $\neg R((x_i)_{i\in\mathbf{n}})$ ha de verificarse. Ara distingim dos casos:

1. Si $Q((x_i)_{i\in\mathbf{n}}, F((x_i)_{i\in\mathbf{n}})$ aleshores existeix un x (que serà $F((x_i)_{i\in\mathbf{n}})$) de manera que $Q((x_i)_{i\in\mathbf{n}}, x)$ i, per tant, $R((x_i)_{i\in\mathbf{n}})$, és a dir, $(x_i)_{i\in\mathbf{n}}$ verifica la relació R.

2. D'altra banda, si $\neg Q((x_i)_{i\in\mathbf{n}}, F((x_i)_{i\in\mathbf{n}}))$, aleshores

   $$P((x_i)_{i\in\mathbf{n}}, F((x_i)_{i\in\mathbf{n}})),$$

   ja que $F((x_i)_{i\in\mathbf{n}})$ satisfà

   $$Q((x_i)_{i\in\mathbf{n}}, F((x_i)_{i\in\mathbf{n}})) \vee P((x_i)_{i\in\mathbf{n}}, F((x_i)_{i\in\mathbf{n}})).$$

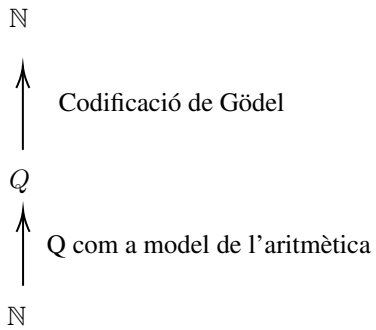
   Per tant $\neg R((x_i)_{i\in\mathbf{n}})$ es verifica. D'ací

   $$R((x_i)_{i\in\mathbf{n}}) \quad \text{si, i només si,} \quad Q((x_i)_{i\in\mathbf{n}}, F((x_i)_{i\in\mathbf{n}})$$

Per tant R és necessàriament recursiva.

2.2 La codificació de Gödel

Entrem ara en la part central del raonament de Gödel. Construirem un sistema de codificació recursiu de seqüències de nombres naturals, amb el propòsit de codificar totes les paraules formades per símbols d'un llenguatge $\mathcal{L}$. El que és sorprenent és que en cap moment necessitarem una estructura més gran que la dels mateixos nombres naturals. Gödel va descobrir que és possible codificar unívocament (assignar un nombre natural) qualsevol axioma, proposició, o demostració construïda en l'aritmètica Q sobre els nombres naturals. Com a exemple, a la conjectura de Goldbach li correspondria un únic nombre natural. Podem resumir el pla de Gödel en el següent esquema:



Farem aquesta construcció en general, per a qualsevol llenguatge formal, i després aplicarem la construcció a la teoría Q a l'últim capítol. L'esquema que seguirem en aquesta secció és el següent:

1. Primer introduirem la funció β de Gödel, que ens permetrà codificar seqüències de nombres naturals.

2. A continuació construirem un sistema de codificació emprant la funció β de Gödel, que ens permetrà treballar còmodament amb aquesta funció.

3. Seguidament assignarem un nombre natural a cada element dels llenguatges formals mitjançant una funció injectiva.

4. Després, codificarem els axiomes que constitueixen el sistema deductiu Λ.

5. Finalment codificarem el conjunt de totes les conseqüències sintàctiques d'una teoria axiomàtica qualsevol T.

2.2.1 La funció β de Gödel

Necessitem una nota i dos lemes previs abans d'introduir el lema de la funció β.

Nota. Per a un $n \geqslant 2$ considerem una seqüència $x_1, \cdots, x_n \in \mathbb{N} \setminus \{0,1\}$ de manera que tota parella de naturals de la seqüència són coprimers entre si. Considerem també el següent conjunt $A = \{x_1, \ldots x_n\}$. Si $B \subset A$, aleshores necessàriament $B = \{y_1, \ldots, y_m\}$, per a certs $y_1, \ldots, y_m \in A$, $m < n$. Considerem el producte $y = y_1 \ldots y_m$ dels elements de B. Aleshores com que els elements de A són coprimers dos a dos, es té que per a qualsevol $x \in A$

$$x | y = y_1 \ldots y_m \quad \text{si, i només si} \quad x \in B.$$

Lema 5. Si $k|z$ per a un $z \neq 0$, aleshores els nombres $1 + (j+k)z$ i $1 + jz$ són coprimers per a tot $j \in \mathbb{N}$

Demostració. En primer lloc, notem que

$$\begin{aligned} jz &\equiv 0 \mod z, \\ jz+1 &\equiv 1 \mod z, \end{aligned}$$

per a tot $j \in \mathbb{N}$. Si p és un nombre primer tal que $p|z$, aleshores $p \nmid 1 + jz$. Per provar el lema raonem per reducció a l'absurd. Suposem per tant que $1 + (j+k)z$ i $1 + jz$ no són coprimers per a cert $j \in \mathbb{N}$. Per tant existeix un nombre primer q tal que:

$$\begin{aligned} &q | 1 + jz, \\ &q | 1 + (j+k)z = 1 + jz + kz. \end{aligned}$$

D'ací se segueix que $q|kz$, necessàriament. Aleshores o bé $q|k$ o bé $q|z$. Però per hipòtesi $k|z$ i per tant en qualsevol cas $q|z$. Per tant $q|z$ i $q|1 + jz$ però açò és una contradicció amb el que hem vist al principi de la prova, ja que q és primer.

Lema 6. La funció

$$\begin{array}{rccc} J: & \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ & (a,b) & \longmapsto & (a+b)^2 + (a+1) \end{array}$$

és injectiva.

Demostració. En primer lloc notem que si $a + b < a' + b'$, aleshores

$$\begin{aligned} J(a,b) =& (a+b)^2 + a + 1 \\ \leqslant& (a+b)^2 + 2(a+b) + 1 \\ =& (a+b+1)^2 \\ \leqslant& \left(a' + b'\right)^2 \\ <& J\left(a', b'\right). \end{aligned}$$

Per tant, si $J(a,b) = J\left(a', b'\right)$, es té

$$a + b = a' + b', \tag{2.3}$$

ja que si

$$a + b < a' + b' \text{ o bé } a' + b' < a + b$$

no se satisfaria la igualtat pel que acabem de demostrar. A més

$$0 = J\left(a', b'\right) - J(a,b) = a' - a,$$

cosa que implica que $a = a'$ i que $b = b'$ per (1.2), i per tant el lema queda demostrat.

Teorema 5. (Funció β de Gödel) Existeix una funció recursiva $\beta : \mathbb{N}^2 \to \mathbb{N}$, anomenada **funció β de Gödel**, que verifica:

1. $\beta(a,i) \leqslant a-1$, per a tot $a, i \in \mathbb{N}$.

2. Per a $a_1, \ldots, a_n \in \mathbb{N}$, existeix un $a \in \mathbb{N}$ tal que $\beta(a,i) = a_i$, per a tot $i \in \mathbf{n}$.

Demostració. Definim β de la forma següent:

$$\beta(a,i) = \mu x < a-1(\exists y < a(\exists z < a(a = J(y,z) \wedge \mathrm{Div}(1 + (J(x,i)+1)\cdot z, y)))), \tag{2.4}$$

on J és la funcó definida al lema previ. La funció β és recursiva per les propietats de la secció anterior, ja que és una composició de funcions recursives i disjuncions. A més, $\beta(a,i) \leqslant a-1$ per a tot $i \in \mathbf{n}$ per definició, fet que prova 1.

Per provar 2, donats $a_1, \ldots, a_n \in \mathbb{N}$, volem trobar un $a \in \mathbb{N}$ tal que $\beta(a,i) = a_i$ per a tot $i \in \mathbf{n}$. Triem els nombres:

$$c = \max_{i \in \mathbf{n}} \{J(a_i, i) + 1\} \qquad \text{i} \qquad z = c! = \prod_{0<j<c} j.$$

Notem que per l'elecció de z que hem fet

$$j | z, \text{ per a tot } 0 < j < c. \tag{2.5}$$

Donats $j, l \in \mathbb{N}$ tals que $1 \leqslant j < l \leqslant c$, com $0 < l - j < c$ tenim que $(l-j)|z$ per (1.3). Per tant pel **Lema 5** els nombres $1 + jz$ i $1 + lz$ són coprimers. Considerem els conjunts

$$A = \{1 + (j+1)z : j \in \mathbf{c}\}, \quad B = \{1 + (J(a_i, i) + 1)z : i \in \mathbf{n}\}.$$

Hem vist que els elements de A són coprimers dos a dos. A més per l'elecció de c que hem fet es té que $B \subset A$, ja que

$$J(a_i, i) = (a_i + i)^2 + a_i + 1 < c$$

per a tot $i \in \mathbf{n}$.

Per la Nota existeix un $y \in \mathbb{N}$ tal que per a tot $j < c$ es verifica:

$$1 + (j+1)z | y \quad \text{si, i només si} \quad j = J(a_i, i) \text{ per a algun } i < n \qquad (*).$$

Siga $a = J(y,z)$. Notem que per a cada a_i es verifiquen les següents propietats:

(a) $a_i < y < a$ i $z < a$. Açò es així ja que $y, z < (y+z)^2 + (y+1) = J(y,z) = a$, i a més

$$a_i < 1 + (a_i + i)^2 + a_i + 1 + 1)z = 1 + (J(a_i, i) + 1)z < y,$$

per $(*)$.

(b) $\mathrm{Div}(1 + (J(a_i, i) + 1)\cdot z, y)$. Açò és una conseqüencia inmediata de $(*)$.

(c) Per a tot $x < a_i$,

$$1 + (J(x,i) + 1)z \nmid y.$$

Per veure això, com que J és injectiva, si $x < a_i$ aleshores $J(x,i) \neq J(a_i, i)$, i a més, per a cada $j \neq i$, es té que $J(x,i) \neq J(a_j, j)$. Aleshores el nombre $1 + (J(x,i) + 1)$ no divideix a y per $(*)$.

Cal notar, a més que si triem uns $y' \neq y$ i $z' \neq z$ es té que $J(y,z) \neq J(y', z')$, Per tant, d'acò últim i de (a), (b), i (c) se segueix que a_i és el mínim natural que verifica la sentència (2.4), és a dir, $\beta(a,i) = a_i$.

2.2.2 Codificació de seqüències

Ara introduïm el sistema de codificació que ens permetrà codificar la teoria aritmètica Q, i provar el primer teorema d'incompletesa de Gödel. En primer lloc, definim la *codificació seqüencial*, que a cada seqüència de nombres naturals li assigna un únic nombre natural fent ús de la funció minimització i la funció β de Gödel. Cal destacar que, encara que totes aquestes operacions que definirem seguidament són computables des d'un punt de vista teòric, no ens preocuparem per la seua implementació. De fet, en la pràctica aquestes funcions treballen amb nombres tan grans que la seua implementació és inviable.

Definició 35. Anomenem **codificació seqüencial** a la funció:

$$\begin{array}{rccl} \langle\cdot\rangle: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (a_i)_{i\in\mathbf{n}} & \longmapsto & \mu x.\,(\beta(x,0)=n \wedge \beta(x,1)=a_1 \wedge \cdots \wedge \beta(x,n)=a_n) \end{array}$$

Al nombre $\langle(a_i)_{i\in\mathbf{n}}\rangle$ l'anomenem codificació seqüencial (o simplement codificació) de la seqüencia $(a_i)_{i\in\mathbf{n}}$.

Nota. De la definició se segueixen:

(a) Pel teorema de la funció β, la funció $\langle\cdot\rangle$ està ben definida per a tota seqüència $(a_i)_{i\in\mathbf{n}}$, i és recursiva en ser composició d'una minimització recursiva **(R2)** i per la Propietat 5 i la Propietat 6.

(b) A més, $\langle\cdot\rangle$ és injectiva ja que si
$$\langle a_1,\ldots,a_n\rangle = \langle b_1,\ldots,b_m\rangle,$$
aleshores, necessàriament $n=m$ i $a_i=b_i$ per a cada $i\in\mathbf{n}$ per la definició de $\langle\cdot\rangle$.

(c) La codificació seqüencial de la seqüència buida és
$$\langle\rangle = \mu x(\beta(x,0)=0) = 0.$$

Hem definit una codificació que identifica cada seqüència de naturals amb un nombre natural. Ara volem desfer el procés, és a dir, donada una codificació (un nombre natural que codifica una sequència), volem recuperar cada element de la seqüència que codifica. Per fer això emprem la funció definida a continuació.

Definició 36. Per a cada $i\in\mathbb{N}$, considerem la següent funció:

$$\begin{array}{rccl} (\cdot)_i: & \mathbb{N} & \longrightarrow & \mathbb{N}^n \\ & a & \longmapsto & \beta(a,i). \end{array}$$

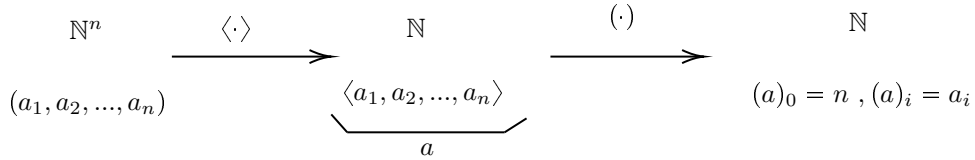
Pel teorema de la funció β, $(\cdot)_i$ és recursiva per a cada i. Per al cas $i=0$, a $(\cdot)_0$ l'anomenarem **longitud** de la seqüència.

Nota. De la definició anterior se segueix:

(a) Donat $(a_i)_{i\in\mathbf{n}}\in\mathbb{N}^n$ observem que
$$\langle(a_i)_{i\in\mathbf{n}}\rangle = \mu x.\,(\beta(x,0)=n \wedge \beta(x,1)=a_1 \wedge \cdots \wedge \beta(x,n)=a_n) = a'$$
per a cert $a'\in\mathbb{N}$, on hem emprat teorema de la funció β . Per tant, aquest a' deu complir:
$$(\langle(a_i)_{i\in\mathbf{n}}\rangle)_i = (a')_i = \beta(a',i) = a_i. \tag{2.6}$$
D'igual forma
$$(\langle(a_i)_{i\in\mathbf{n}}\rangle)_0 = n.$$

(b) Si $a>0$, tenim que $(a)_0 < a$ i $(a)_i < a$ per el primer apartat del teorema de la funció β.

Açò pot resumir-se amb en el següent diagrama:



La definició anterior ens permet recuperar totalment les seqüències originals a partir de les seues codificacions en els nombres naturals, però com podem assegurar que un cert nombre natural arbitrari és o no la codificació d'alguna seqüència? Aprofitant la construcció que hem fet, la següent relació ens permet identificar els nombres naturals que són codificacions d'alguna seqüència, i a més a més, veurem que aquesta relació és recursiva.

Definició 37. Donat $a \in \mathbb{N}$ definim la relació $\mathrm{Seq} \subseteq \mathbb{N}$ donada per

$$\mathrm{Seq(a)} \quad \text{si, i només si,} \quad \forall x < a\,((x)_0 \neq (a)_0 \vee \exists i < (a)_0\,((x)_{i+1} \neq (a)_{i+1})\,. \tag{2.7}$$

Nota. La relació Seq té les següents propietats:

(a) Seq és recursiva, ja que l'expressió (2.7) que la defineix ho és per les Propietats 5, 6 i 8.

(b) Per entendre millor l'utilitat d'aquesta relació notem que

$$\neg\mathrm{Seq(a)} \text{ si, i només si, } \exists x < a\,((x)_0 = (a)_0 \wedge \forall i < (a)_0\,((x)_{i+1} = (a)_{i+1})\,. \tag{2.8}$$

És a dir, $\neg$Seq(a) si

$$a \neq \mu x.\,\big(\beta(x,0) = (a)_0 \wedge \beta(x,1) = (a)_1 \wedge \cdots \wedge \beta(x,(a)_0) = a_{(a)_0}\big)\,.$$

En altres paraules, a no és la codificació seqüencial de $(a)_1, (a)_2, \cdots (a)_{(a)_0}$. Per tant Seq(a) es verifica quan $a \in \mathbb{N}$ és la codificació seqüencial de $(a)_1, (a)_2, \cdots (a)_{(a)_0}$, és a dir

$$a = \langle (a)_1, (a)_2, \cdots (a)_{(a)_0}\rangle.$$

A continuació introduïm una nova ferramenta que ens permetrà recuperar la codificació de la subseqüència formada pels primers i termes d'una seqüència a partir de la codificació de tota la seqüència.

Definició 38. La funció **seqüència inicial** ve donada per:

$$\begin{array}{rccl} \mathrm{In}: & \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ & (a,i) & \longmapsto & \mu x.((x)_0 = i \wedge \forall j < i\,((x)_{j+1} = (a)_{j+1})\,. \end{array}$$

Nota. La funció In verifica:

(a) In és una funció recursiva en ser una minimització recursiva i per les propietats 5 i 6 .

(b) Per a $1 \leqslant i \leqslant n$, si apliquem la definició de codificació seqüencial obtenim:

$$\mathrm{In}\,(\langle a_1, \ldots, a_n\rangle, i) = \mu x.(\beta(x,0) = i \wedge \beta(x,1) = \beta(a,1) \wedge \cdots \wedge \beta(x,i) = \beta(a,i)) = \langle a_1, \ldots, a_i\rangle.$$

Incorporem al nostre sistema la funció concatenació, que donades dues codificacions ens retorna la codificació de la concatenació de les seqüències.

Definició 39. La funció **concatenació** ve donada per:

$$\begin{array}{rccl} *: & \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ & (a,b) & \longmapsto & \mu x.((x)_0 = (a)_0 + (b)_0) \wedge \forall i < (a)_0((x)_{i+1} = (a)_{i+1}) \wedge \forall j < (b)_0((x)_{(a)_0+j+1} = (b)_{j+1})), \end{array}$$

Nota. La funció concatenació verifica:

(a) $*$ és una funció recursiva per ser una minimització recursiva i per les Propietats 5 i 6.

(b) De la definició se segueix (on estem emprant la notació $a * b$ per denotar $*(a, b)$):

$$\langle a_1, \cdots, a_n \rangle * \langle b_1, \cdots, b_m \rangle = \langle a_1, \cdots, a_n, b_1, \cdots, b_n \rangle.$$

En aquest punt, ja hem construït un sistema de codificació suficientment robust per als nostres propòsits. Ara, és necessari introduir un tipus particular de funció definida per recursió.

Definició 40. Donades una funció $F : \mathbb{N} \times \mathbb{N}^k \longrightarrow \mathbb{N}$ i un $(b_i)_{i\in\mathbf{k}} \in \mathbb{N}^k$ definim recursivament la funció:

$$\begin{array}{rccl} \bar{F}: & \mathbb{N} \times \mathbb{N}^k & \longrightarrow & \mathbb{N} \\ & (a, (b_i)_{i\in\mathbf{k}}) & \longmapsto & \begin{cases} 0 & \text{si } a = 0; \\ \langle F(0, (b_i)_{i\in\mathbf{k}}), F(1, (b_i)_{i\in\mathbf{k}}), \cdots, F(a-1, (b_i)_{i\in\mathbf{k}}) \rangle & \text{si } a > 0. \end{cases} \end{array}$$

Nota. De la definició se segueixen:

(a) Notem que l'expressió:

$$\bar{F}(a+1, (b_i)_{i\in\mathbf{k}}))_{a+1} = (\langle F(a, (b_i)_{i\in\mathbf{k}}), \cdots, F(a, (b_i)_{i\in\mathbf{k}}) \rangle)_{a+1} = F(a, (b_i)_{i\in\mathbf{k}}) \tag{2.9}$$

on aquesta última igualtat se segueix de (2.6).

(b) Podem relacionar l'expressió de F amb les definicions anteriors, i així F és recursiva:

$$\begin{aligned} \bar{F}(a, (b_i)_{i\in\mathbf{k}}) =& \langle F(0, (b_i)_{i\in\mathbf{k}}), F(1, (b_i)_{i\in\mathbf{k}}), \cdots, F(a-1, (b_i)_{i\in\mathbf{k}}) \rangle \\ =& \mu x.((x)_0 = a \wedge \forall i < a((x)_{i+1} = F(i, (b_i)_{i\in\mathbf{k}})). \end{aligned} \tag{2.10}$$

(c) Si $x < a$ aleshores per 2.6

$$\begin{aligned} (\bar{F}(x, b))_x &= (\langle F(0, b), \cdots, F(x-1, b) \rangle)_x \\ &= (\langle F(0, b), \cdots, F(x-1, b), \cdots, F(a-1, b) \rangle)_x = F(a, b))_x \end{aligned} \tag{2.11}$$

2.2.3 Més propietats de les funcions recursives

Provem una sèrie de propietats tècniques que necessitarem més endavant.

Propietat 12. Donada la funció $G : \mathbb{N} \times \mathbb{N} \times \mathbb{N}^n \longrightarrow \mathbb{N}$ i l'element $(b_i)_{i\in\mathbf{n}} \in \mathbb{N}^n$, es defineix recursivament, per a cada $a \in \mathbb{N}$, la funció $F : \mathbb{N} \times \mathbb{N}^n \longrightarrow \mathbb{N}$ com la següent composició:

$$\begin{array}{rcl} F(0, (b_i)_{i\in\mathbf{n}}) &=& G(\bar{F}(0, (b_i)_{i\in\mathbf{n}}), 0, (b_i)_{i\in\mathbf{n}}), \\ F(1, (b_i)_{i\in\mathbf{n}}) &=& G(\bar{F}(1, (b_i)_{i\in\mathbf{n}}), 1, (b_i)_{i\in\mathbf{n}}), \\ F(2, (b_i)_{i\in\mathbf{n}}) &=& G(\bar{F}(2, (b_i)_{i\in\mathbf{n}}), 2, (b_i)_{i\in\mathbf{n}}), \\ & \vdots & \\ F(a, (b_i)_{i\in\mathbf{n}}) &=& G(\bar{F}(a, (b_i)_{i\in\mathbf{n}}), a, (b_i)_{i\in\mathbf{n}}). \end{array}$$

Així definida, F és recursiva.

Demostració. Tenim que:

$$F(a, (b_i)_{i\in\mathbf{n}}) = G(\bar{F}(a, (b_i)_{i\in\mathbf{n}}), a, (b_i)_{i\in\mathbf{n}})$$

on, aplicant la definició obtenim

$$\begin{aligned} \bar{F}(a, (b_i)_{i\in\mathbf{n}}) &= \mu x.((x)_0 = a \wedge \forall i < a((x)_{i+1} = F(i, (b_i)_{i\in\mathbf{n}})) \\ &= \mu x.((x)_0 = a \wedge \forall i < a((x)_{i+1} = G(\bar{F}(i, (b_i)_{i\in\mathbf{n}}), i, (b_i)_{i\in\mathbf{n}}). \end{aligned}$$

A més a més es té que:

$$\begin{aligned}\bar{F}(i,(b_i)_{i\in\mathbf{n}}) &= \mu y.((y)_0 = i \wedge \forall j < i((y)_{j+1} = F(j,(b_i)_{i\in\mathbf{n}})) \\ &= \mu y.((y)_0 = i \wedge \forall j < i((y)_{j+1} = (\bar{F}(j+1,(b_i)_{i\in\mathbf{n}}))_{j+1})),\end{aligned}$$

on hem aplicat l'expressió (2.6) en la darrera igualtat. Si recordem la definició de $\mathrm{In}(x,i)$:

$$\mathrm{In}(x,i) = \mu y.((y)_0 = i \wedge \forall j < i((y)_{j+1} = (x)_{j+1}).$$

Per tant, com que $(x)_{i+1} = F(i,(b_i)_{i\in\mathbf{n}})$, per a cada $i < a$, es possible expressar $\bar{F}$ com la següent composició:

$$\bar{F}(a,(b_i)_{i\in\mathbf{n}}) = G(\bar{F}(a,(b_i)_{i\in\mathbf{n}}),a,(b_i)_{i\in\mathbf{n}}) = G(\mathrm{In}(x,i),i,(b_i)_{i\in\mathbf{n}}).$$

Com que ja sabem que la funció In és recursiva, s'obte que $\bar{F}$ és una composició recursiva i, per tant, també ho serà F.

Propietat 13. Donades les funcions recursives $G : \mathbb{N}\times\mathbb{N}^n \longrightarrow \mathbb{N}$ i $H : \mathbb{N}\times\mathbb{N}^n \longrightarrow \mathbb{N}$ aleshores la següent funció, definida recursivament com segueix:

$$\begin{array}{rccl} F: & \mathbb{N}\times\mathbb{N}^n & \longrightarrow & \mathbb{N}; \\ & (a,(b_i)_{i\in\mathbf{n}}) & \longmapsto & \begin{cases} F(G(a,(b_i)_{i\in\mathbf{n}}),(b_i)_{i\in\mathbf{n}}) & \text{si } G(a,(b_i)_{i\in\mathbf{n}}) < a \\ H(a,(b_i)_{i\in\mathbf{n}}) & \text{en altre cas .} \end{cases} \end{array}$$

és recursiva.

Demostració. (a) Si $G(a,(b_i)_{i\in\mathbf{n}}) \geqslant a$ el resultat és clar ja que H és recursiva.

(b) Suposem que $G(a,(b_i)_{i\in\mathbf{n}}) < a$. Aleshores es verifica

$$\begin{aligned}F(G(a,(b_i)_{i\in\mathbf{n}}),(b_i)_{i\in\mathbf{n}}) &= (\bar{F}(G(a,(b_i)_{i\in\mathbf{n}})+1,(b_i)_{i\in\mathbf{n}})_{G(a,(b_i)_{i\in\mathbf{n}})+1} \\ &= (\bar{F}(a,(b_i)_{i\in\mathbf{n}}))_{G(a,(b_i)_{i\in\mathbf{n}})+1} = \beta(\bar{F}(a,(b_i)_{i\in\mathbf{n}}),G(a,(b_i)_{i\in\mathbf{n}})+1).\end{aligned}$$

On hem aplicat (2.9) en la primera igualtat i que $G(a,(b_i)_{i\in\mathbf{n}})+1 \leqslant a$ per aplicar (2.11). Notem, a més, que aquesta darrera expressió es pot escriure com:

$$\beta(\bar{F}(a,(b_i)_{i\in\mathbf{n}}),G(a,(b_i)_{i\in\mathbf{n}})+1) = G'(F(a,(b_i)_{i\in\mathbf{n}}),a,(b_i)_{i\in\mathbf{n}}).$$

on

$$\begin{array}{rccl} G': & \mathbb{N}\times\mathbb{N}\times\mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x,y,(z_i)_{i\in\mathbf{n}}) & \longmapsto & \beta(x,G(y,z)+1). \end{array}$$

és una funció recursiva en ser una composició recursiva. Per tant, podem aplicar la propietat anterior per concloure que F és recursiva.

Propietat 14. Donades les funcions recursives $G : \mathbb{N}\times\mathbb{N}^n \longrightarrow \mathbb{N}$ i $H : \mathbb{N}^2\times\mathbb{N}^n \longrightarrow \mathbb{N}$, la següent funció:

$$\begin{array}{rccl} F: & \mathbb{N}\times\mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (a,(b_i)_{i\in\mathbf{k}}) & \longmapsto & \begin{cases} H(F(a-1,(b_i)_{i\in\mathbf{n}}),a-1,(b_i)_{i\in\mathbf{n}}) & \text{si } a > 0; \\ G((b_i)_{i\in\mathbf{n}}) & \text{en altre cas .} \end{cases} \end{array}$$

és recursiva.

Demostració. (a) Si $a \leqslant 0$ el resultat és clar en ser G recursiva.

(b) Si $a > 0$, observem que:

$$H(F(a-1,(b_i)_{i\in\mathbf{n}}),a-1,(b_i)_{i\in\mathbf{n}}) = H(\beta(\bar{F}(a,(b_i)_{i\in\mathbf{n}}),a),a-1,(b_i)_{i\in\mathbf{n}}).$$

On hem aplicat (2.9). Podem aplicar la Propietat 12 per acabar la demostració.

Propietat 15. Siguen $Q \subseteq \mathbb{N}^{n+1}$ i $R \subseteq \mathbb{N}^{n+1}$ dues relacions recursives, i siga $H : \mathbb{N} \times \mathbb{N}^n \longrightarrow \mathbb{N}$ una funció recursiva verificant $H(a,(b_i)_{i\in\mathbf{n}}) < a$ si $Q(a,(b_i)_{i\in\mathbf{n}})$. Aleshores la relació $P \subseteq \mathbb{N}^{n+1}$ donada per:

$$P(a,(b_i)_{i\in\mathbf{n}}) \quad \text{si, i només si,} \quad \begin{cases} P(H(a,(b_i)_{i\in\mathbf{n}}),(b_i)_{i\in\mathbf{n}}) & \text{si } Q(a,(b_i)_{i\in\mathbf{n}}); \\ R(a,(b_i)_{i\in\mathbf{n}}) & \text{en altre cas.} \end{cases}$$

és recursiva.

Demostració. Per provar-ho, considerem la següent funció:

$$\begin{array}{rccl} H': & \mathbb{N}\times\mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (a,(b_i)_{i\in\mathbf{n}}) & \longmapsto & \begin{cases} H(a,(b_i)_{i\in\mathbf{n}}) & \text{si } Q(a,(b_i)_{i\in\mathbf{n}})>0; \\ a & \text{en altre cas.} \end{cases} \end{array}$$

Per construcció, sabem per les propietats anterior que H' és recursiva. Ara només cal adonar-se que:

$$\mathcal{X}_P(a,(b_i)_{i\in\mathbf{n}}) = \begin{cases} \mathcal{X}_P(H'(a,(b_i)_{i\in\mathbf{n}}),(b_i)_{i\in\mathbf{n}}) & \text{si } H'(a,(b_i)_{i\in\mathbf{n}}) < a; \\ \mathcal{X}_R(a,(b_i)_{i\in\mathbf{n}}) & \text{en altre cas.} \end{cases}$$

per concloure la prova.

Nota. A conseqüència d'aquestes últimes propietats, les següents funcions també són recursives:

(a) La funció factorial.

$$\begin{array}{rccl} \cdot!: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \begin{cases} (n-1)!\cdot n & \text{si } n>0; \\ 1 & \text{si } n=0. \end{cases} \end{array}$$

(b) La funció exponencial.

$$\begin{array}{rccl} \cdot^n: & \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ & (n,m) & \longmapsto & \begin{cases} m^{n-1}\cdot m & \text{si } n>0; \\ 1 & \text{si } n=0. \end{cases} \end{array}$$

Considerem ara la relació $A \subseteq \mathbb{N}^2$ donada per

$$A(a,c) \quad \text{si, i només si,} \quad \mathrm{Seq}(c) \wedge (c)_0 = a \wedge \forall i < a\,((c)_{i+1} = 0 \vee (c)_{i+1} = 1)\,.$$

Aquesta relació ens permeteix saber si un nombre donat és la codificació d'una seqüencia d'unos i zeros. Per com està definida és recursiva. Siga $F : \mathbb{N}^2 \to \mathbb{N}$ la funció definida com

$$F(a,i) = \begin{cases} \mu x(A(a,x)) & \text{si } i=0; \\ \mu x(F(a,i-1) < x \wedge A(a,x)) & \text{si } 0<i<2^a; \\ 0 & \text{en altre cas.} \end{cases}$$

Considerem, a més, la funció $\mathrm{bd} : \mathbb{N} \to \mathbb{N}$ donada per

$$\begin{array}{rccl} \mathrm{bd}: & \mathbb{N} & \to & \mathbb{N} \\ & n & \longmapsto & F\,(n, 2^n-1)\,. \end{array}$$

Per les propietats anteriors, tant F com bd són recursives. Notem que, per com hem definit F, podem emprar aquesta definició equivalent:

$$\mathrm{bd}(n) = \max\{< c_1c_2\ldots c_n > |\ c_i \in \{0,1\}\}. \tag{2.12}$$

Aquesta caracterització l'emprarem més endavant per a codificar els valors de veritat.

2.2.4 Codificació de l'aritmètica

En aquest pas anem a codificar els elements d'un llenguatge $\mathcal{L}$. Per com l'hem definit, un llenguatge $\mathcal{L}$ sobre un conjunt de variables X no és més que un conjunt numerable de símbols, i per tant podem fer correspondre cada símbol amb un únic nombre natural, és a dir, podem construir una funció injectiva $h : \mathcal{L} \longrightarrow \mathbb{N}$. Com a exemple, podem construir-la de la següent forma:

1. Per a cada variable $x_i \in X$ definim $h(x_i) = 2^i$.
2. Per a numerar els símbols lògics podem definir:

$$\begin{aligned} h(\rightarrow) &= 3, \\ h(\neg) &= 5, \\ h(\forall x_i) &= 2^i \times 7 \text{ per a cada variable } x_i \in X. \end{aligned}$$

   Aquesta definició ens permetra recuperar el nombre que representa la variable sobre la qual actua el quantificador, dividint per set.
3. A cada símbol de funció $\sigma_i \in \Sigma$, podem associar-li el valor $h(\sigma_i) = 11^i$.
4. Per últim, per a cada símbol de relació $\theta_i \in \Theta$, podem definir el valor $h(\theta_i) = 13^i$.

Hi han moltes possibles opcions, però si emprem nombres primers per numerar-los, com que ja hem provat que la relació "ser un nombre primer" és recursiva, aleshores tant $h[\Sigma]$ com $h[\Theta]$ seran subconjunts que podran expressar-se mitjançant relacions recursives. A més a més $h[\mathrm{Log}(X)]$ també serà recursiu per les propietats de les funcions recursives.
A continuació comencem a codificar els elements dels llenguatges formals. Definim una codificació $\lceil\cdot\rceil$, és a dir, una funció que identifica cada paraula d'un llenguatge $\mathcal{L}$ amb un nombre natural.

Definició 41. (Codificació de Gödel) Donat un llenguatge $\mathcal{L}$, considerem la funció $\lceil\cdot\rceil : \mathrm{Form}(\mathcal{L}, X) \longrightarrow \mathbb{N}$, anomenada **codificació de Gödel**, definida de forma recursiva com segueix:

1. **(G1)** Per a cada variable o constant $x \in X \cup \Sigma_0$ en el nostre llenguatge, definim $\lceil x\rceil = \langle h[X]\rangle$.
2. **(G2)** Per a cada família de termes $(t_j)_{j\in\mathbf{n}} \in \mathbf{T}_\Sigma(X)$ i cada símbol de funció $\sigma \in \Sigma \setminus \Sigma_0$ definim:

$$\lceil\sigma((t_j)_{j\in\mathbf{n}})\rceil = \langle H[\Sigma], \lceil t_1\rceil, \lceil t_2\rceil, \cdots, \lceil t_n\rceil\rangle.$$

3. **(G3)** Per a cada família de termes $(t_j)_{j\in\mathbf{n}} \in \mathbf{T}_\Sigma(X)$ i cada símbol de relació $\theta \in \Theta$ definim:

$$\lceil\theta((t_j)_{j\in\mathbf{n}})\rceil = \langle h(\theta), \lceil t_1\rceil, \lceil t_2\rceil, \cdots, \lceil t_n\rceil\rangle.$$

4. **(G4)** Per a les fórmules $\alpha, \beta \in \mathrm{Form}(\mathcal{L}, X)$ i per a una variable $x \in X$, definim:

$$\begin{aligned} \lceil\alpha \rightarrow \beta\rceil &= \langle h(\rightarrow), \lceil\alpha\rceil, \lceil\beta\rceil\rangle, \\ \lceil\neg\alpha\rceil &= \langle h(\neg), \lceil\alpha\rceil\rangle, \\ \lceil\forall x\alpha\rceil &= \langle h(\forall x), \lceil x\rceil, \lceil\alpha\rceil\rangle. \end{aligned}$$

Per a cada fórmula $\gamma \in \mathrm{Form}(\mathcal{L}, X)$ del llenguatge $\mathcal{L}$, anomenem a $\lceil\gamma\rceil$ el **nombre de Gödel** de γ. Com que la funció h és injectiva, i la codificació seqüencial també ho és, **la codificació de Gödel serà injectiva**.

Ara hem arribat a un dels punts principals de l'argumentació. Anem a provar que el conjunt de codificacions de Gödel de totes les fórmules d'una certa teoria axiomàtica construïda sobre un llenguatge $\mathcal{L}$ i amb el conjunt d'axiomes lògics Λ, és recursiu. Per fer-ho, ho comprovem per a cada classe dels elements del llenguatge $\mathcal{L}$ i el sistema deductiu, en els següents 17 passos.

Pas 1. Els conjunts de nombres naturals $\mathrm{Vble} = \{\ulcorner v \urcorner \in \mathbb{N} \mid v \in h[X]\} \subseteq \mathbb{N}$ i $\mathrm{Const} = \{\ulcorner c \urcorner \in \mathbb{N} \mid c \in h[\Sigma_0]\} \subseteq \mathbb{N}$ són recursius.

Demostració. Notem que:

$$\mathrm{Vble}(x) \quad \text{si, i només si,} \quad x = \langle (x)_1 \rangle \wedge h[X]\,((x)_1)\,,$$

és a dir, x és un nombre que codifica una seqüència de longitud 1 de manera que el seu únic element és la imatge mitjançant h d'un símbol de variable. De forma semblant:

$$\mathrm{Const}(x) \quad \text{si, i només si,} \quad x = \langle (x)_1 \rangle \wedge h[\Sigma_0]\,((x)_1)\,.$$

Sabem de la secció anterior que la codificació seqüencial és recursiva, i a més de les Propietats 5,6 i del fet que $h[X]$ i $h[\Sigma]$ són recursives, se segueix que ambdues relacions són recursives.

Pas 2. El conjunt de nombres naturals $\mathrm{Term} = \{\ulcorner t \urcorner \in \mathbb{N} \mid t \text{ és un terme de } \mathcal{L}\} \subseteq \mathbb{N}$ és recursiu.

Demostració. Sabem que els termes són paraules del tipus

$$\sigma a_1 a_2 \cdots a_l$$

per a un símbol d'operació $\sigma \in \Sigma$ d'aritat l, o bé expressions que pertanyen al pas anterior (variables i constants de $\mathcal{L}$) . Açò ho podem excriure de la següent forma:

$$\mathrm{Term}(a) \quad \text{si, i només si,} \quad \begin{cases} \forall j < ((a)_0 - 1)\,\mathrm{Term}\,((a)_{j+2}) & \text{si } \mathrm{Seq}(a) \wedge h[\Sigma]\,((a)_1) \wedge \mathrm{ar}((a)_1) = (a)_0 - 1; \\ \mathrm{Vble}(a) \vee \mathrm{Const}(a) & \text{en altre cas.} \end{cases} \tag{2.13}$$

És a dir, si a és la codificació d'una seqüència que en la primera posició té un símbol de funció d'aritat la longitud de la seqüència menys 1, s'ha de complir que els símbols a partir de la segona posició corresponen a termes. L'altre cas possible és quan estem en el pas anterior. Per tant, com que sabem que el conjunt Seq és recursiu i per les Propietats 10, 5, 6 i del fet que $h[\Sigma]$ és recursiva, més el Pas 1 concloem que aquesta relació és recursiva.

Pas 3. El conjunt de nombres naturals $\mathrm{At} = \{\ulcorner \sigma \urcorner \in \mathbb{N} \mid \sigma \text{ és una fórmula atòmica de } \mathcal{L}\} \subseteq \mathbb{N}$ és recursiu.

Demostració. Recordem que les fórmules atòmiques són paraules del tipus:

$$\theta a_1 a_2 \cdots a_l$$

on $\theta \in \Theta$ és un símbol de relació d'aritat l i $a_1 a_2 \cdots a_l$ són símbols de termes de $\mathcal{L}$, és a dir,

$$\begin{aligned} \mathrm{At}(a) \quad \text{si, i només si,} \quad & \mathrm{Seq}(a) \wedge h[\Theta]\,((a)_1) \wedge (\mathrm{ar}\,((a)_1) = (a)_0 - 1) \\ & \wedge \forall j < ((a)_0 - 1)\,(\mathrm{Term}\,((a)_{j+2})) \end{aligned}$$

És a dir, si a és la codificació d'una seqüencia que té un símbol de relació a la primera posició seguit de termes del llenguatge, respetant l'aritat del símbol. Pels passos anteriors, per les Propietats 5 i 6 i del fet que $h[\Theta]$ és recursiva, l'expressió que defineix $\mathrm{At}(a)$ és recursiva.

Pas 4. El conjunt de nombres naturals $\mathrm{Form} = \{\ulcorner \varphi \urcorner \in \mathbb{N} \mid \varphi \text{ és una fórmula en } \mathcal{L}\} \subseteq \mathbb{N}$ és recursiu.

Demostració. Recordem que les fórmules són paraules del tipus:

$$\neg\alpha, \quad \alpha \to \beta, \quad \forall x(\alpha),$$

i combinacions d'aquestes, on α i β són fórmules atòmiques, és a dir,

$$\mathrm{Form}(a) \quad \text{si, i només si,} \quad \begin{cases} \mathrm{Form}\left((a)_2\right) & \text{si } a = \langle h(\neg), (a)_2\rangle; \\ \mathrm{Form}\left((a)_2\right) \wedge \mathrm{Form}\left((a)_3\right) & \text{si } a = \langle h(\rightarrow), (a)_2, (a)_3\rangle; \\ \mathrm{Form}\left((a)_2\right) & \text{si } a = \langle h(\forall x), (a)_2\rangle; \\ \mathrm{At}(a) & \text{en altre cas.} \end{cases} \tag{2.14}$$

De nou per la Propietat 10 i dels passos anteriors se segueix que és recursiva.

Pas 5. Ara expressarem recursivament les substitucions en un llenguatge. Per fer-ho considerem la funció:

$$\begin{array}{rccc} \mathrm{Sub}: & \mathbb{N}^3 & \longrightarrow & \mathbb{N} \\ & (\lceil\varphi\rceil, \lceil x\rceil, \lceil u\rceil) & \longmapsto & \binom{x}{u}\varphi. \end{array}$$

per a un terme u, una variable x, i on φ pot ser o bé una fórmula o bé un terme de $\mathcal{L}$, és recursiva.

Demostració. Expressem inductivament la funció de la següent forma:

$$\mathrm{Sub}(a,b,c) = \begin{cases} c & \text{si } \mathrm{Vble}(a) \wedge a = b; \\ \langle (a)_1, \mathrm{Sub}\left((a)_2, b, c\right), \ldots & \text{si } (a)_0 > 1 \wedge (a)_1 \neq h(\forall x) \wedge \mathrm{Seq}(a); \\ \ldots, \mathrm{Sub}\left((a)_{(a)_0}, b, c\right)\rangle & \\ \langle (a)_1, \mathrm{Sub}\left((a)_2, b, c\right)\rangle & \text{si } a = \langle h(\forall x), (a)_2\rangle \wedge h(\forall x)/7 \neq b; \\ a & \text{en altre cas.} \end{cases}$$

Notem que si aquesta funció estiguera ben definida, aleshores seria recursiva per les propietats del tema anterior i els pasos previs. Veiem que Sub està ben definida per inducció sobre a:

- Si $a = 0$ aleshores $(a)_0 = 0$, i per tant estarem en el primer o últim cas. Per tant la funció està ben definida per qualsevols b i c en aquest cas.
- Si $a \neq 0$, aleshores $(a)_i < a$ per a tot $i \leqslant (a)_0$, com vam veure a la secció anterior, i per tant és possible calcular els valors $\mathrm{Sub}\left((a)_i, b, c\right)$.

Així, $\mathrm{Sub}(a,b,c)$ està ben definit en qualsevol cas.

Pas 6. En aquest pas captem la definició de variable lliure i l'expresarem amb una relació recursiva. Donades una $\mathcal{L}$-fórmula φ, un terme t, i una variable $x \in X$ del llenguatge, aleshores la relació $\mathrm{Free} \subseteq \mathbb{N}^2$, definida com:

$$\begin{array}{rll} \mathrm{Free}(\lceil\varphi\rceil, \lceil x\rceil) & \text{si, i només si,} & \text{x està lliure en } \varphi, \\ \mathrm{Free}(\lceil t\rceil, \lceil x\rceil) & \text{si, i només si,} & \text{x està lliure en } t, \end{array}$$

és una relació recursiva.

Demostració. Si recordem la definició de variable lliure, podem expressar la relació de la forma:

$$\mathrm{Free}(a,b) \quad \text{si, i només si,} \quad \begin{cases} \exists j < \left((a)_0 - 1\right)\left(\mathrm{Free}\left((a)_{j+2}, b\right)\right) & \text{si } (a)_0 > 1 \wedge (a)_1 \neq h(\forall x); \\ \mathrm{Free}\left((a)_3, b\right) \wedge h(\forall x)/7 \neq b & \text{si } (a)_0 > 1 \wedge (a)_1 = h(\forall x); \\ a = b & \text{en altre cas.} \end{cases}$$

L'únic que estem fent ací és distinguir quan una certa variable està baix l'efecte d'un quantificador en la fórmula codificada pel nombre a. Aquesta definició inductiva està ben definida si raonem de forma igual a l'anterior pas. A més, clarament és recursiva pel que hem vist a la secció anterior.

Pas 7. El conjunt de nombres naturals $\text{Sent} = \{\ulcorner\varphi\urcorner \in \mathbb{N} \mid \varphi \text{ es una sentència de } \mathcal{L}\} \subseteq \mathbb{N}$ és recursiu.

Demostració. D'acord a la Definició 21, una $\mathcal{L}$-sentència és una fórmula on totes les variables que apareixen en la fórmula no són lliures en la fórmula. Açò podem expressar-ho de la següent forma:

$$\text{Sent}(a) \quad \text{si, i només si,} \quad \text{Form}(a) \wedge \forall b < a(\neg\text{Vble}(b) \vee \neg\text{Free}(a,b)).$$

Per tant, per la Propietat 5 de la secció anterior i els passos previs, és recursiu.

Pas 8. Construim ara una relació recursiva que ens permeta conéixer si un terme es pot substituir per una variable en una fórmula del llenguatge, a partir de les seues codificacions. Per fer-ho, considerem la relació $\text{Subst}(a,b,c) \subseteq \mathbb{N}^3$ definida per a una fórmula φ, una variable x, i un terme t de $\mathcal{L}$ com segueix:

$$\text{Subst}(\ulcorner\varphi\urcorner, \ulcorner x\urcorner, \ulcorner t\urcorner) \text{ si, i només si, t es pot substituir per } x \text{ en } \varphi.$$

Aquesta funció és recursiva.

Demostració. Basant-nos en la definició de substitució del primer capítol, definim la següent relació per recursió:

$$\text{Subst}(a,b,c) \quad \text{si, i només si,} \quad \begin{cases} \text{Subst}((a)_2,b,c) & \text{si } a = \langle h(\neg),(a)_2\rangle; \\ \text{Subst}((a)_2,b,c) \wedge \text{Subst}((a)_3,b,c) & \text{si } a = \langle h(\to),(a)_2,(a)_3\rangle; \\ \neg\text{Free}(a,b) \vee (\neg\text{Free}(c,h(\forall x)/7) & \text{si } a = \langle h(\forall x),(a)_2\rangle \wedge \text{Subst}((a)_2,b,c)); \\ 0=0 & \text{en altre cas.} \end{cases} \tag{2.15}$$

Raonant com abans, aquesta relació està ben definida, i a més és recursiva per la Propietat 5 i les propietats de la secció (2.2.3).

Pas 9. Definim la relació $\text{False} \subseteq \mathbb{N}^2$ inductivament com segueix:

$$\text{False}(a,b) \quad \text{si, i només si,} \quad \begin{cases} \neg\text{False}((a)_2,b) \wedge \text{False}((a)_3,b) & \text{si } a = \langle h(\to),(a)_2,(a)_3\rangle \wedge \text{Form}((a)_2) \wedge \text{Form}((a)_3); \\ \neg\text{False}((a)_2,b) & \text{si } a = \langle h(\neg),(a)_2\rangle \wedge \text{Form}((a)_2); \\ \text{Form}(a) \wedge (b)_a = 0 & \text{en altre cas.} \end{cases} \tag{2.16}$$

Pel mateix raonament que al Pas 5, aquesta relació està ben definida i és recursiva per les propietats de la secció (2.2.3).

Nota. L'utilitat d'aquesta relació és la següent:
Considerem un $b \in \mathbb{N}$ i un conjunt finit $A \subseteq \text{Form}(\mathcal{L}, X)$. Aleshores podem construir una assignació $v_b : A \longrightarrow \{V,F\}$, definida com segueix:

$$v_b(\varphi) = F \quad \text{si, i només si,} \quad (b)_{\ulcorner\varphi\urcorner} = 0.$$

Ara, per a qualsevol altra asignació $v : A \longrightarrow \{V,F\}$, ordenem les fórmules de $A = \{\varphi_1, \varphi_2, \cdots, \varphi_n\}$ de manera que

$$\ulcorner\varphi_1\urcorner < \ulcorner\varphi_2\urcorner < \cdots < \ulcorner\varphi_n\urcorner,$$

i per a cada $1 \leqslant j \leqslant \ulcorner\varphi_n\urcorner$ definim:

$$c_j = \begin{cases} 0 & \text{si } j = \ulcorner\varphi_i\urcorner \text{ per a cert } i \leqslant n \text{ i } v(\varphi_i) = F; \\ 1 & \text{en altre cas.} \end{cases}$$

Esquemàticament, açò és:

$$\begin{array}{ccccc} \ulcorner\varphi_1\urcorner & < & \ulcorner\varphi_2\urcorner & < \cdots < & \ulcorner\varphi_n\urcorner \\ \downarrow & & \downarrow & \cdots & \downarrow \\ \langle c_1, & & c_2, & \cdots & c_n\rangle \end{array}$$

D'aquesta forma si triem $b = \langle c_1, \cdots, c_{\ulcorner\varphi_n\urcorner}\rangle$, es compleix que

$$v_b(\varphi) = v(\varphi)$$

per a tota fórmula φ en A. Per tant per a qualsevol fórmula φ en A,

$$v(\varphi) = F \quad \text{si, i només si,} \quad v_b(\varphi) = F \quad \text{si, i només si,} \quad \text{False}(\ulcorner\varphi\urcorner, b)$$

és a dir, **podem expressar mitjançant una relació recursiva quan una certa fórmula és falsa o vertadera en el llenguatge $\mathcal{L}$.**

Pas 10. En aquest pas expressem el conjunt de tautologíes recursivament, és a dir, el conjunt Taut$= \{\ulcorner\sigma\urcorner \in \mathbb{N} \mid \ \sigma$ és una tautología$\} \subseteq \mathbb{N}$ és recursiu.

Demostració. Per provar-ho recordem la funció recursiva (2.12):

$$\begin{array}{rccl} \text{bd}: & \mathbb{N} & \to & \mathbb{N} \\ & n & \longmapsto & \max\{\langle c_1, \ldots, c_n\rangle | c_i \in \{0, 1\}\} \end{array}$$

Recordem que una fórmula τ és una tautología si, i només si, τ és certa per a qualsevol valoració. Podem expressar açò de la següent forma:

$$\text{Taut}(a) \quad \text{si, i només si,} \quad \text{Form}(a) \wedge \forall b < (\text{bd}(a) + 1)(\neg\ \text{False}\ (a, b)),$$

és a dir, volem que a codifique una certa fórmula i que a més qualsevol valoració dels elements de dita fórmula tinguen un valor de veritat. Per la Propietat 5 i el pasos previs aquesta relació és recursiva.

Pas 11. El grup d'axiomes AG2 és recursiu, és a dir, $\underline{\text{AG2}} = \{\ulcorner\varphi\urcorner \in \mathbb{N} | \varphi$ està en el grup de axiomes $2\} \subseteq \mathbb{N}$ és una relació recursiva.

Demostració. Recordem que el segon grup d'axiomes està format per les fòrmules del tipus

$$\forall x\varphi \to (\tfrac{t}{x})\varphi,$$

on t és substituïble per x en φ. És a dir, per a un nombre $a \in \mathbb{N}$, $\underline{\text{AG2}}(a)$ si, i només si,

$$\exists x, y, z < a(\text{Vble}(x) \wedge \text{Form}(y) \wedge \text{Term}(z) \wedge \text{Subst}(y, x, z) \wedge a =< h(\to), \langle h(\forall x), y\rangle, \text{Subst}(y, x, z)\rangle).$$

Pas 12. El grup d'axiomes AG3 és recursiu, és a dir, el conjunt $\underline{\text{AG3}} = \{\ulcorner\varphi\urcorner \in \mathbb{N} | \varphi$ és un axioma del grup $3\} \subseteq \mathbb{N}$ és recursiu.

Demostració. Recordem que el grup d'axiomes AG3 està composat per les fòrmules del tipus

$$\forall x\left(\psi \to \psi'\right) \to \left(\forall x\psi \to \forall x\psi'\right).$$

Açò podem expressar-ho emprant la nostra codificació, mitjançant la següent expressió recursiva:

$$\begin{array}{r} \underline{\text{AG3}}(a) \text{ si, i només si } \exists x, y, z < a(\text{Vble}(x) \wedge \text{Form}(y) \wedge \text{Form}(z) \\ \wedge a = \langle h(\to), \langle h(\forall x), \langle h(\to), y, z\rangle\rangle \\ \langle h(\to), \langle h(\forall x), y\rangle, \langle h(\forall), x, z\rangle\rangle\rangle). \end{array}$$

Pas 13. El grup d'axiomes AG4 és recursiu, és a dir, el conjunt AG4 = $\{\lceil\varphi\rceil \in \mathbb{N} | \varphi$ és un axioma del grup 4$\} \subseteq \mathbb{N}$ és recursiu.

Demostració. Com AG4 està format per les fórmules de la forma $\varphi \to \forall x(\varphi)$, on x no està lliure en φ, podem expressar els axiomes de AG4 de la següent forma:

$$\begin{aligned} \text{AG4}(a) \quad \text{si, i només si,} \quad & \exists x, y < a(\ \text{Vble}(x) \wedge \text{Form}(y) \\ & \wedge \neg\text{Free}(y, x) \wedge a = \langle h(\to), y, \langle h(\forall x), y\rangle\rangle). \end{aligned}$$

Pas 14. El conjunt de nombres de Gödel del grup d'axiomes AG5 és recursiu, és a dir, el conjunt $\underline{\text{AG5}} = \{\lceil\varphi\rceil \in \mathbb{N} | \varphi$ és un axioma del group AG5 $\} \subseteq \mathbb{N}$ és recursiu.

Demostració. Recordem que el grup AG5 estava format per les fórmules del tipus $x = x$ per a una variable x. Açò podem expressar-ho fàcilment emprant la nostra codificació de la següent forma:

$$\underline{\text{AG5}}(a) \quad \text{si, i només si,} \quad \exists x < a\ (\ \text{Vble}(x) \wedge a = \langle h(=), x, x\rangle).$$

Per tant és recursiu ja que aquesta última expressió és recursiva per la Propietat 5 i els passos anteriors.

Pas 15. El conjunt de nombres de Gödel que codifiquen el grup d'axiomes AG6 és recursiu, és a dir $\underline{\text{AG6}} = \{\lceil\varphi\rceil \in \mathbb{N} | \varphi$ és un d'axioma del grup 6$\} \subseteq \mathbb{N}$, és recursiu.

Demostració. Recordem que AG6 és el conjunt de fórmules de la forma $x = y \to (\alpha \to \alpha')$, on α és una fórmula atòmica i α' sobté de α reemplaçant x per y en zero o més posicions. Aquesta relació pot expressar-se emprant la nostra codificació de la següent forma, com indica Kim en [2]:

$$\begin{aligned} \underline{\text{AG6}}(a) \quad \text{si, i només si,} \quad & \exists x, y, b, c < a(\text{Vble}(x) \wedge \text{Vble}(y) \wedge \text{At}(b) \wedge \text{At}(c) \wedge (b)_0 = (c)_0 \\ & \wedge (b)_1 = (c)_1 \in h[\Theta] \wedge [2 \leqslant \forall j \leqslant (b)_0\, ((b)_j = (c)_j \in \text{Vble} \vee ((c)_j = y \wedge (b)_j = x)) \\ & \vee [(b)_0 = (c)_0 = 3 \wedge (c)_1 = (b)_1 = h(=) \wedge ((b)_2)_1 = ((c)_2)_1 = ((b)_3)_1 = ((c)_3)_1 \in h(\Sigma) \\ & \wedge 2 \leqslant \forall j \leqslant ((b)_2)_0\, \forall i \in \{2,3\} \left(((b)_i)_j = ((c)_i)_j \in Vble \vee \left(((c)_i)_j = y \wedge ((b)_i)_j = x\right)\right)] \\ & \wedge a = \langle h(\to), \langle h(=), x, y\rangle, \langle h(\to), b, c\rangle\rangle). \end{aligned}$$

Per tant, per les propietats de la codificació seqüencial, la Propietat 5, i els passos anteriors, la relació és recursiva.

Pas 16. Considerem la relació $\text{Gen}(a, b) \subseteq \mathbb{N}^2$, definida de la forma següent:

$$\text{Gen}(\lceil\varphi\rceil, \lceil\psi\rceil) \quad \text{si, i només si,} \quad \varphi \text{ és una generalització de } \psi,$$

és a dir, $\varphi = \forall x_1 \ldots \forall x_n \psi$ per a una col·lecció finita de variables $x_i \in \mathbb{N}$. Aleshores $\text{Gen}(a, b)$ és recursiva.

Demostració. Si recordem la definició de genealització, podem expressar-la mitjançant la següent expressió:

$$\text{Gen}(a, b) \quad \text{si, i només si,} \quad \begin{cases} a =< h(\forall), (a)_2, (a)_3 > \wedge \text{Vble}\,((a)_2) \wedge \text{Gen}\,((a)_3, b) & \text{si } a > b; \\ 0 = 0 & \text{si } a = b; \\ 0 = 1 & \text{si } a < .b \end{cases}$$

Per tant és recursiva.

Pas 17. Per últim considerem el conjunt de nombres de Gödel que codifiquen totes les generalitzacions dels d'axiomes lògics, és a dir, considerem el conjunt $\underline{\Lambda} = \{\lceil\sigma\rceil \in \mathbb{N} | \sigma \in \Lambda\} \subseteq \mathbb{N}$, on

$$\Lambda = \text{AG2} \cup \text{AG3} \cup \text{AG4} \cup \text{AG5} \cup \text{AG6}.$$

Aleshores $\underline{\Lambda}$ és recursiva.

Demostració. Aquesta relació podem expressar-la fàcilment emprant la nostra codificació i les relacions dels passos anteriors com segueix:

$$\begin{aligned}\underline{\Lambda}(a) \quad \text{si, i només si,} \quad & \exists b < a+1(\text{Form}(a) \wedge \text{Gen}(a,b) \\ & \wedge (\text{Taut}(b) \vee \underline{\text{AG2}}(b) \vee \underline{\text{AG3}}(b) \vee \underline{\text{AG4}}(b) \vee \underline{\text{AG5}}(b) \vee \underline{\text{AG6}}(b)\ )\ ).\end{aligned}$$

Per tant, pels passos anteriors i la Propietat 5, aquesta relació és recursiva.

2.2.5 Codificació de les teoríes axiomatizables

Ja hem construit la infraestructura necessària per codificar totes les fórmules i axiomes lògics d'una teoría recursivament. Per tant, el següent pas és definir una nova codificació per codificar seqüències de $\mathcal{L}$-fórmules.

Definició 42. Considerem la següent funció:

$$\begin{array}{rccc} \llbracket\cdot\rrbracket: & \text{Form}(L,X)^n & \longrightarrow & \mathbb{N} \\ & (\varphi_i)_{i\in\mathbf{n}} & \longmapsto & \langle\lceil\varphi_1\rceil,\cdots,\lceil\varphi_n\rceil\rangle \end{array}$$

Per com hem definit la codificació de Gödel, aquesta funció és injectiva i recursiva.

Definició 43. Siga un llenguatge $\mathcal{L}$ i una teoría T incloent els axiomes Λ en el llenguatge $\mathcal{L}$. Definim el conjunt dels nombres de Gödel de totes les possibles expressions sintàctiques ben construïdes dins de la teoria T, és a dir,

$$\underline{\text{T}} = \{\lceil\sigma\rceil \in \mathbb{N} \mid \sigma \in \text{T}\}.$$

Amb aquesta definició podrem codificar el conjunt de totes les conseqüencies sintàctiques d'una teoria. En aquest punt ja podem donar la definició de teoría axiomatizable.

Definició 44. (Teoria axiomatizable) Direm que una teoría T construida sobre un llenguatge $\mathcal{L}$ és **axiomatizable** si existeix una teoría S que axiomatiza T, complint que $\underline{\text{S}}$ és recursiva. És a dir, el conjunt de conseqüencies lògiques de S (CnS) és igual al conjunt de conseqüències lògiques de T (CnT).

Definició 45. Emprarem els següents conjunts:

1. El conjunt de totes les deduccions de T:

$$\text{Ded}_\text{T} = \{\llbracket\varphi_1,\ldots,\varphi_n\rrbracket \in \mathbb{N} | \varphi_1,\ldots,\varphi_n \text{ és una deducció de T}\} \subseteq \mathbb{N}.$$

2. El conjunt de totes les demostracions de la teoría T:

$$\text{Pf}_\text{T} = \underline{\text{Cn}}\text{T} = \{\lceil\sigma\rceil \in \mathbb{N} | \text{T} \vdash \sigma\}.$$

Teorema 6. Els conjunts Pf_T i Ded_T poden expressar-se emprant la codificació de Gödel.

Demostració. Comencem amb Ded_T. Això es deu a la possiblitat d'expressar la relació mitjançant les relacions que hem construit a la secció anterior:

$$\begin{aligned}&\text{Ded}_\text{T}(a) \quad \text{si, i només si,} \quad \text{Seq}(a) \wedge (a)_0 \neq 0 \\ &\wedge \forall j < (a)_0\,(\underline{\Lambda}\,((a)_{j+1}) \vee \underline{\text{T}}\,((a)_{j+1}) \vee \exists i,k < j+1\,((a)_{k+1} = \langle h(\rightarrow),(a)_{i+1},(a)_{j+1}\rangle))\end{aligned} \tag{2.17}$$

És a dir, un cert nombre $a \in \mathbb{N}$ és la codificació d'una deducció si la longitud de la seqüència que codifica té longitud major que zero, i cada una de les fórmules de la seqüència és, o bé un axioma de Λ, o bé una fórmula de la toería T, o bé l'aplicació del Modus Ponens a aquestes fórmules. Es molt important notar que si $\underline{\mathrm{T}}$ és recursiu, aleshores la relació $\mathrm{Ded_T}$ és recursiva per que així ho és la expressió (2.17), per les propietats de la secció anterior.

Ara considerem la relació: $\mathrm{Prf_T} \subseteq \mathbb{N}^2$, donada per :

$$\mathrm{Prf_T}(a,b) \quad \text{si, i només si,} \quad \mathrm{Ded_T}(b) \wedge a = (b)_{(b)_0},$$

és a dir, la relació que indica si una fórmula α, codificada per un nombre natural a, és la última deducció d'una seqüència de fórmules de la teoría codificada pel nombre de Gödel b. De nou, si la relació $\underline{\mathrm{T}}$ és recursiva, aleshores $\mathrm{Prf_T}$ és una relació recursiva per la Propietat 5. Per últim, es possible reinterpretar la definició de $\mathrm{Pf_T}$ en termes de la relació $\mathrm{Prf_T}$ de la següent forma:

$$\mathrm{Pf_T}(a) \quad \text{si, i només si,} \quad \mathrm{Sent}(a) \wedge \exists x\, \mathrm{Prf_T}(a,x) \tag{2.18}$$

és a dir, la relació és satisfà per a un nombre natural a si aquest codifica una sentència α del llenguatge $\mathcal{L}$, de manera que existeix certa seqüència de $\mathcal{L}$-fórmules, codificades per un nombre de Gödel x, que són una prova de α.

Baix quines condicions la relació Pf_T és recursiva? Per respondre aquesta pregunta, introduïm els següents teoremes, que manifesten la relació entre les teoríes axiomatizables i la recursivitat. Aquests resultats ens seràn de profit per provar els resultats d'incompletesa.

Teorema 7. Si T és una teoria axiomatizable sobre un llenguatge $\mathcal{L}$, alehores $\mathrm{Pf_T} = \underline{\mathrm{CnT}}$ és recursivament enumerable.

Demostració. Com T és axiomatizable, per definició existeix una teoria S que axiomatitza T, on $\underline{\mathrm{S}}$ és recursiva. Com la teoria S axiomatitza a T, per definició CnS=CnT. Pel teorema anterior, com que estem suposant que $\underline{\mathrm{S}}$ és recursiva, sabem que $\mathrm{Ded_S}$ i $\mathrm{Prf_S}$ són relacions recursives, i per tant per la caracterització (2.18) del teorema anteorior, $\mathrm{Pf_S}$ serà una relació recursivament enumerable. Però $\mathrm{Pf_S} = \mathrm{Pf_T}$, ja que $\mathrm{CnS} = \mathrm{CnT}$.

Abans de provar el segon teorema, definim els conceptes de completesa i decidibilitat en una teoría rigorosament.

Definició 46. (Teoria completa) Una teoría T direm que és **completa** si per a qualsevol $\mathcal{L}$-sentència α,

$$P \nvdash \alpha \quad \text{si, i només si,} \quad \mathrm{T} \vdash \neg\alpha.$$

Definició 47. (Teoria decidible) Direm que una teoria axiomatizable T és **decidible** si $\underline{\mathrm{CnT}}$ és recursiu.

Teorema 8. Si T és axiomatizable i complet en $\mathcal{L}$, aleshores T és decidible.

Demostració. Volem provar que CnT és recursiu. Pel teorema anterior ja sabem que $\mathrm{Pf_T} = \underline{\mathrm{Cn\ T}}$ és recursivament enumerable, per tant, pel Teorema 4, és suficient provar que $\neg Pf_{\mathrm{T}}$ és recursivament enumerable. Notem que com T és complet, aleshores per a qualsevol sentència

$$P \nvdash \alpha \quad \text{si, i només si,} \quad \mathrm{T} \vdash \neg\alpha$$

per definició de teoría completa. Ens adonem que és possible relacionar $\neg\mathrm{Pf_T}$ amb el nostre sistema de codificació de la següent forma, basant-nos en la caracterització (2.18):

$$\neg\mathrm{Pf_T}(a) \quad \text{si, i només si,} \quad \neg\ \mathrm{Sent(a)} \vee \exists m\, \mathrm{Prf_T}(\langle h(\neg), a\rangle, m).$$

És a dir, una fórmula α no és provable en una teoria T si, o bé el nombre natural a que la codifica no és la codificació d'una sentència, o bé existeix alguna seqüència de fórmules que proven la negació de α. Amb aquesta caracterització, veïem que $\neg\mathrm{Pf_T}$ és recursivament enumerable. Per tant pel Teorema de la Negació, $\mathrm{Pf_T}$ és recursiva.

Així doncs ens adonem que la prova d'aquestos resultats importants es redueix a comprovar que certes relacions són recursives, mostrant la practicitat de la codificació de Gödel que hem construït a aquest capítol.

Capítol 3

Incompletesa

3.1 Teorema de la Representabilitat en Q

Recordem la teoria Q presentada al final del primer capítol. En aquesta secció vam identificar cada símbol del llenguatge $\mathcal{L}_{\mathbb{N}}$ amb un nombre natural emprant la següent expressió:

$$\underline{n} = \underbrace{SS\cdots S}_{n \text{ voltes}}0.$$

A continuació introduïm el concepte de representabilitat en la teoria Q, que ens permetrà relacionar funcions i relacions definides sobre els nombres naturals amb expressions sintàctiques en la teoria Q.

Definició 48. Una funció $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ és representable en Q si existeix una $\mathcal{L}_{\mathbb{N}}$-fórmula $\varphi\left((x_i)_{i\in\mathbf{n}}, y\right)$ tal que:

$$Q \vdash \forall y(\varphi((\underline{k_i})_{i\in\mathbf{n}}, y) \longleftrightarrow y = \underline{f((k_i)_{i\in\mathbf{n}})})$$

per a tot $k_1, \ldots, k_n \in \mathbb{N}$. En aquest cas direm que φ representa a f en Q.

Definició 49. Una relació $P \subseteq \mathbb{N}^n$ és representable en Q si existeix una $\mathcal{L}_{\mathbb{N}}$ -fórmula $\varphi\left((x_i)_{i\in\mathbf{n}}\right)$ tal que, per a tota seqüència $(k_i)_{i\in\mathbf{n}} \in \mathbb{N}^n$:

$$\text{si } P((k_i)_{i\in\mathbf{n}}) \text{ aleshores } Q \vdash \varphi((\underline{k_i})_{i\in\mathbf{n}}),$$

i a més

$$\text{si } \neg P((k_i)_{i\in\mathbf{n}}) \text{ aleshores } Q \vdash \neg\varphi((\underline{k_i})_{i\in\mathbf{n}}).$$

De nou, en aquest cas direm que φ representa a P en Q.

L'objectiu d'aquesta secció és relacionar el concepte de representabilitat amb les funcions i relacions recursives. Per fer-ho, necessitem uns lemes previs.

Lema 7. Per a qualsevol relació $P \subseteq \mathbb{N}^n, P$ és representable en Q si, i només si, la funció χ_P és representable en Q.

Demostració. Comencem suposant que P és representable i que $\varphi\left((x_i)_{i\in\mathbf{n}}, y\right)$ representa P. Siga ψ la fórmula construida com segueix:

$$\psi((x_i)_{i\in\mathbf{n}}, y) \quad \text{si, i només si,} \quad (\varphi((x_i)_{i\in\mathbf{n}}) \wedge y = 0) \vee (\neg\varphi((x_i)_{i\in\mathbf{n}}) \wedge y = \underline{1}).$$

Anem a provar que $\psi((x_i)_{i\in\mathbf{n}}, y)$ representa χ_P :

Suposem que $P\left((k_i)_{i\in\mathbf{n}}\right)$ es verifica. Aleshores:

$$Q \vdash \varphi((\underline{k_i})_{i\in\mathbf{n}}) \tag{3.1}$$

$$\vdash \varphi((\underline{k_i})_{i\in\mathbf{n}}) \rightarrow (y = 0 \longleftrightarrow \psi((\underline{k_i})_{i\in\mathbf{n}}, y) \tag{3.2}$$

$$Q \vdash y = 0 \longleftrightarrow \psi((k_i)_{i\in\mathbf{n}}, y). \tag{3.3}$$

On (3.1) se segueix de la hipòtesi de que P és representable, (3.2) és una tautología ja que hem suposat que es verifica P per a aquests k_i i (3.3) se segueix del Modus Ponens. Per tant, tenim el que volíem.

De forma semblant, si $\neg P\left((k_i)_{i\in\mathbf{n}}\right)$ se satisfà, aleshores:

$$Q \vdash \neg\varphi((\underline{k_i})_{i\in\mathbf{n}}) \tag{3.4}$$

$$\vdash \varphi((\underline{k_i})_{i\in\mathbf{n}}) \to (y = \underline{1} \longleftrightarrow \psi(((\underline{k_i})_{i\in\mathbf{n}}, y) \tag{3.5}$$

$$Q \vdash y = \underline{1} \longleftrightarrow \psi((\underline{k_i})_{i\in\mathbf{n}}, y). \tag{3.6}$$

Aplicant el mateix procediment que abans. Aleshores, $\psi((x_i)_{i\in\mathbf{n}}, y)$ representa a χ_P.

Ara suposem que χ_P és representable per una funció $\psi((x_i)_{i\in\mathbf{n}}, y)$. Aleshores $\psi((x_i)_{i\in\mathbf{n}}, 0)$ representa P, ja que si $P\left((k_i)_{i\in\mathbf{n}}\right)$ aleshores $\chi_P((k_i)_{i\in\mathbf{n}}) = 0$ i de la definició de funció representable tenim:

$$Q \vdash \left(\psi\left((\underline{k_i})_{i\in\mathbf{n}}, y\right) \longleftrightarrow y = 0\right).$$

Si substituïm y per 0, obtenim $Q \vdash \psi\left((\underline{k_i})_{i\in\mathbf{n}}, 0\right)$, com volíem. De forma semblant, quan $\neg P\left((k_i)_{i\in\mathbf{n}}\right)$ es satisfà, es té $\chi_P((k_i)_{i\in\mathbf{n}}) = 1$, i de la definició de funció representable:

$$Q \vdash \left(\psi\left((\underline{k_i})_{i\in\mathbf{n}}, y\right) \longleftrightarrow y = \underline{1}\right).$$

i com que $Q \vdash \neg(0 = \underline{1})$ podem concloure que $Q \vdash \neg\psi\left((\underline{k}_i)_{i\in\mathbf{n}}, 0\right)$, com volíem. Per tant, P és representable.

Lema 8. Per a una fórmula φ en $\mathcal{L}_{\mathbb{N}}$, se compleix

$$Q \vdash \left(\left(\tbinom{x}{0}\right)\varphi \to \cdots \to \left(\left(\tbinom{x}{\underline{k-1}}\right)\varphi \to (x < \underline{k} \to \varphi)\right)\right).$$

Demostració. Fem inducció sobre k. Per al cas base, si k és 0, es té

$$Q \vdash (x < 0 \to \varphi)$$

per l'Axioma Q7. Considerem aleshores la nostra hipòtesi inductiva:

$$Q \vdash \left(\tbinom{x}{0}\right)\varphi \to \cdots \to \left(\left(\tbinom{x}{\underline{k-1}}\right)\varphi \to (x < \underline{k} \to \varphi)\right).$$

Volem provar:

$$Q \vdash \left(\tbinom{x}{0}\right)\varphi \to \cdots \to \left(\left(\tbinom{x}{\underline{k}}\right)\varphi \to (x < \underline{k+1} \to \varphi)\right).$$

És a dir, volem provar que $\Gamma \vdash \varphi$ on

$$\Gamma = Q \cup \left\{\left(\tbinom{x}{0}\right)\varphi, \cdots, \left(\tbinom{x}{\underline{k}}\right)\varphi, x < \underline{k+1}\right\}.$$

Ens adonem que, per l'Axioma Q8,

$$\Gamma \vdash x < \underline{k} \vee x = \underline{k}.$$

En el primer cas, l'esquema inductiu implica que $\Gamma \vdash \varphi$. En el segon cas,

$$\vdash (x = \underline{k} \to \left(\left(\tbinom{x}{\underline{k}}\right)\varphi \longleftrightarrow \varphi\right)),$$

és una tautología, i per tant del Modus Ponens se segueix $\Gamma \vdash \varphi$. En tots dos casos, Γ prova φ.

Lema 9. Considerem un natural $n \in \mathbb{N}$ i una $\mathcal{L}$-fórmula φ. Suposem que es verifiquen:

(a) $Q \vdash \neg\left(\tbinom{x}{\underline{k}}\right)\varphi$, per a cada $k < n$,

(b) $Q \vdash \left(\tbinom{x}{\underline{n}}\right)\varphi$.

Aleshores per a un terme $z \neq x$, que no apareix en la fórmula φ, se segueix:

$$Q \vdash \left((\varphi \wedge \forall z\left(z < x \to \neg\left(\left(\tbinom{x}{z}\right)\varphi\right)\right)\right) \longleftrightarrow x = \underline{n}\right).$$

Demostració. Definim la fórmula $\psi(x)$ com segueix:

$$\psi(x) \quad \text{si, i només si,} \quad (\varphi \wedge \forall z\,(z < x \to \neg\,(\binom{x}{z}\varphi)))\,.$$

Suposem en primer lloc que $x = \underline{n}$. En aquest cas ens adonem que

$$\vdash x = \underline{n} \to (\psi(x) \longleftrightarrow (\binom{x}{\underline{n}}\varphi \wedge \forall z\,(z < \underline{n} \to \neg\,(\binom{x}{z}\varphi))))$$

és una tautología, per com hem definit la fórmula ψ. Ara bé, per (a) i pel Lema 8, tenim:

$$Q \vdash (x < \underline{n} \to \neg\varphi) \tag{3.7}$$

i, aplicant substitució i generalització obtenim

$$Q \vdash \forall z\,(z < \underline{n} \to \neg\,(\binom{x}{z}\varphi))\,.$$

Combinant açò amb (b) i la tautología anterior, concloem

$$Q \vdash (x = \underline{n} \to \psi).$$

Ara fem l'altra implicació, és a dir, suposem que $Q \vdash \psi$. Ens adonem que la següent expressió,

$$\vdash \forall z\,(z < x \to \neg\binom{x}{z}\varphi) \to (\underline{n} < x \to \neg\,(\binom{x}{z}\varphi))\,,$$

és una tautología. Així (b) implica

$$Q \vdash \psi \to \neg(\underline{n} < x).$$

Ara bé,

$$Q \cup \{\psi, x < \underline{n}\} \vdash \varphi \wedge \neg\varphi,$$

per (3.7) i la definició de ψ. Per tant

$$Q \vdash \psi \to \neg(x < \underline{n}),$$

i per l'Axioma Q9 es té:

$$Q \vdash \psi \to x = \underline{n}.$$

Ara ja podem demostrar el teorema de representabilitat en la teoria aritmètica Q. Aquest resultat intervindrà directament en la prova del teorema Gödel.

Teorema 9. (Representabilitat en Q). Tota funció o relació recursiva és representable en Q.

Demostració. És suficient provar la representabilitat de les funcions bàsiques en la definició de recursivitat.

1. **F1, F2, F3 i F4**. En primer lloc ho comprovem per a les funcions elementals $\Pi_i^n, +, \cdot$, i $\chi_<$:

   - Per a $+$, la fórmula φ, definida com segueix:

     $$\varphi\,(x_1, x_2, y) \quad \text{si, i només si,} \quad y = x_1 + x_2$$

     representa a $+$ en Q, ja que per a qualsevols $m, n \in \mathbb{N}$, aplicant el Lema 2:

     $$\begin{array}{l} Q \vdash \underline{m} + \underline{n} = \underline{m+n}, \\ Q \vdash y = \underline{m} + \underline{n} \longleftrightarrow y = \underline{m+n}, \\ Q \vdash \varphi(\underline{m}, \underline{n}, y) \longleftrightarrow y = \underline{m+n}, \text{ i per tant,} \\ Q \vdash \forall y(\varphi(\underline{m}, \underline{n}, y) \longleftrightarrow y = \underline{m+n}), \end{array}$$

     com volíem.

- Per a $\cdot$, veiem que la fórmula φ definida com:

$$\varphi(x_1, x_2, y) \quad \text{si, i només si,} \quad y = x_1 \cdot x_2,$$

representa a $\cdot$ en Q, ja que de nou, per a qualsevols $m, n \in \mathbb{N}$, aplicant el Lema 3:

$$\begin{aligned} &Q \vdash \underline{m} \cdot \underline{n} = \underline{m \cdot n}, \\ &Q \vdash y = \underline{m} \cdot \underline{n} \longleftrightarrow y = \underline{m \cdot n}, \\ &Q \vdash \varphi(\underline{m}, \underline{n}, y) \longleftrightarrow y = \underline{m \cdot n}, \text{ i per tant,} \\ &Q \vdash \forall y(\varphi(\underline{m}, \underline{n}, y) \longleftrightarrow y = \underline{m \cdot n}). \end{aligned}$$

- Per a $\chi_<$, pel Lema 5 sabem que serà representable si, i només si, la relació $<(\cdot, \cdot)$, on per a uns naturals n, m

$$<(m, n) \quad \text{si, i només si,} \quad \exists j \in \mathbb{N} \text{ tal que } n = m + j,$$

és representable. Del Lema 4 se segueix:

$$\begin{aligned} \text{Si } &< (m, n) \text{ aleshores } Q \vdash \underline{m} < \underline{n}. \\ \text{Si } \neg &< (m, n) \text{ aleshores } Q \vdash \neg(\underline{m} < \underline{n}). \end{aligned}$$

Per tant és representable.

- Per a cada $n \in \mathbb{N}$ i cada $i \in \mathbf{n}$ la projecció i-éssima Π_i^n és representable per la fórmula següent:

$$\varphi((x_i)_{i \in \mathbf{n}}, y) \quad \text{si, i només si,} \quad x_i = y.$$

En particular, per qualsevols $(k_i)_{i \in \mathbf{n}} \in \mathbb{N}^n$:

$$\Pi_i^n((k_i)_{i \in \mathbf{n}}) = k_i,$$

i per tant

$$Q \vdash (\varphi\left((\underline{k_i})_{i \in \mathbf{n}}, y\right) \longleftrightarrow y = \underline{k_i} \longleftrightarrow y = \underline{\Pi_i^n((k_i)_{i \in \mathbf{n}})}).$$

Per la tria que hem fet de φ. El principi de generalització completa la prova.

2. **(R2.)** Volem provar que la composició recursiva és representable, és a dir, si

$$\begin{aligned} &G : \mathbb{N}^k \longmapsto \mathbb{N} \text{ és una funció representable, i} \\ &H_i : \mathbb{N}^n \longmapsto \mathbb{N} \text{ és una família de funcions representables,} \end{aligned}$$

aleshores la composició:

$$\begin{array}{rccl} F: & \mathbb{N}^n & \longrightarrow & \mathbb{N} \\ & (x_j)_{j \in \mathbf{n}} & \longmapsto & G((H_i((x_j)_{j \in \mathbf{n}}))_{i \in \mathbf{k}}) \end{array}$$

també és representable. Suposem que G està representat en Q per una fórmula φ i cada H_i està representat en Q per la fórmula ψ_i. Anem a provar que F està representat per la següent fórmula α, definida com segueix:

$$\alpha((x_i)_{i \in \mathbf{n}}, y) \quad \text{si, i només si,} \quad \exists z_1, \ldots, z_k \left(\psi_1((x_i)_{i \in \mathbf{n}}, z_1) \wedge \cdots \wedge \psi_k((x_i)_{i \in \mathbf{n}}, z_k) \wedge \varphi(z_1, \ldots, z_k, y)\right).$$

És a dir, volem provar que si $(k_i)_{i \in \mathbf{n}} \in \mathbb{N}^n$,

$$Q \vdash \alpha\left((\underline{a_i})_{i \in \mathbf{n}}, y\right) \longleftrightarrow y = \underline{G(H_1((k_i)_{i \in \mathbf{n}}), \ldots, H_k((k_i)_{i \in \mathbf{n}}))}. \tag{3.8}$$

Anem a provar aquesta doble implicació. Com que cada ψ_i representa a cada H_i, aleshores si considerem la col·lecció de fórmules $\Gamma = Q \cup \left\{\alpha\left((\underline{k_i})_{i \in \mathbf{n}}, y\right)\right\}$, se segueix que

$$\Gamma \vdash \exists z_1, \ldots, z_k \left(z_1 = \underline{H_1((k_i)_{i \in \mathbf{n}})} \wedge \cdots \wedge z_k = \underline{H_k((k_i)_{i \in \mathbf{n}})} \wedge \varphi(z_1, \ldots, z_k, y)\right),$$

ja que $\varphi(z_1,\ldots,z_k,y)$ representa G per aquests z_i. Per tant se segueix:

$$\Gamma \vdash \exists z_1,\ldots,z_k(\varphi(\underline{H_1((k_i)_{i\in\mathbf{n}})},\ldots,\underline{H_k((k_i)_{i\in\mathbf{n}})},y))$$

i com que els z_i no apareixen en la fórmula,

$$\Gamma \vdash \varphi(\underline{H_1((k_i)_{i\in\mathbf{n}})},\ldots,\underline{H_k((k_i)_{i\in\mathbf{n}})},y).$$

Ara bé, com que φ representa a la funció G, d'aquesta última expressió se segueix que

$$\Gamma \vdash \underline{G\left(H_1((k_i)_{i\in\mathbf{n}}),\ldots,H_k((k_i)_{i\in\mathbf{n}})\right)},$$

com volíem. D'altra banda, per a la col·lecció de fórmules

$$\Sigma = Q \cup \left\{y = \underline{G\left(H_1((k_i)_{i\in\mathbf{n}}),\ldots,H_k((k_i)_{i\in\mathbf{n}})\right)}\right\},$$

es té:

$$\begin{array}{l}
\Sigma \vdash \varphi\left(\underline{H_1((k_i)_{i\in\mathbf{n}})},\ldots,\underline{H_k((k_i)_{i\in\mathbf{n}})},y\right),\\
\Sigma \vdash \exists z_1,\ldots,z_k\left(z_1 = \underline{H_1((k_i)_{i\in\mathbf{n}})} \wedge\cdots\wedge z_k = \underline{H_k((k_i)_{i\in\mathbf{n}})} \wedge \varphi(z_1,\ldots,z_k,y)\right),\\
\Sigma \vdash \exists z_1,\ldots,z_k\left(\psi_1((k_i)_{i\in\mathbf{n}},z_i)\wedge\cdots\wedge\psi_k((k_i)_{i\in\mathbf{n}},z_k)\wedge\varphi(z_1,\ldots,z_k,y)\right),\\
\Sigma \vdash \alpha\left((\underline{k_i})_{i\in\mathbf{n}},y\right).
\end{array}$$

Aleshores 3.8 es compleix.

3. **(R3)** Siga $G:\mathbb{N}^{n+1}\longrightarrow\mathbb{N}$ una funció representable tal que per a tot $(x_i)_{i\in\mathbf{n}}\in\mathbb{N}^n$ existeix un $x\in\mathbb{N}$ de manera que $G((x_i)_{i\in\mathbf{n}},x)=0$ és representable en Q. Aleshores volem provar que la minimització $\mu x.G:\mathbb{N}^n\longrightarrow\mathbb{N}$ és una funció representable en Q, on recordem que:

$$\begin{array}{rccl}
\mu x.G: & \mathbb{N}^n & \longrightarrow & \mathbb{N}\\
& (x_i)_{i\in\mathbf{n}} & \longmapsto & \min\{x\in\mathbb{N}\mid G((x_i)_{i\in\mathbf{n}},x)=0\}.
\end{array}$$

Suposem que G està representat en Q per la fórmula $\varphi((x_i)_{i\in\mathbf{n}},x,y)$. Considerem la fórmula

$$\psi((x_i)_{i\in\mathbf{n}},x)\quad\text{definida per}\quad (\tbinom{y}{0})\varphi\wedge\forall z\,(z<x\rightarrow\neg(\tbinom{x}{z})((\tbinom{y}{0})\varphi)).$$

Siguen $\mu x.G((a_i)_{i\in\mathbf{n}})=b\in\mathbb{N}$ i $k_i=G((a_i)_{i\in\mathbf{n}},i)$ per a $i\in\mathbb{N}$. Aleshores per la definició de representació de G per φ:

$$\begin{array}{l}
Q\vdash\varphi\left((\underline{a_i})_{i\in\mathbf{n}},\underline{i},y\right)\longleftrightarrow y=\underline{k_i},\\
Q\vdash\varphi\left((\underline{a_i})_{i\in\mathbf{n}},i,0\right)\longleftrightarrow 0=\underline{k_i}.
\end{array}$$

Per tant si $j<b$, de manera que $k_j\neq 0$, aleshores:

$$Q\vdash\neg\varphi\left((\underline{a_i})_{i\in\mathbf{n}},\underline{j},0\right),$$

D'altra banda, $k_b=G((a_i)_{i\in\mathbf{n}},b)=0$, així que

$$Q\vdash\varphi\left((\underline{a_i})_{i\in\mathbf{n}},\underline{b},0\right).$$

Per tant, si apliquem el Lema 7:

$$Q\vdash((\tbinom{y}{0})(\varphi((a_i)_{i\in\mathbf{n}},x,y))\wedge\forall z\,(z<x\rightarrow(\tbinom{x}{z})((\tbinom{y}{0})(\neg\varphi((a_i)_{i\in\mathbf{n}},x,y)))))\longleftrightarrow x=\underline{b}.$$

i per tant:

$$Q\vdash\psi((a_i)_{i\in\mathbf{n}},x)\longleftrightarrow x=\underline{b}.$$

Pel principi de generalització tenim que ψ representa $\mu x.G$ en Q, com volíem.

3.2 El primer teorema d'incompletesa de Gödel

Arribats a aquest punt, ja disposem de tots els elements necessaris per provar el primer teorema d'incompletesa de Gödel. Al capítol anterior hem construït un sistema de codificació que permet expressar recursivament tots els elements de la teoria Q, un conjunt de fórmules i sentències que fan referència a proposicions sobre els nombres naturals. El que veurem ara és que aquesta codificació ens permet construir expressions autoreferencials en la pròpia teoria Q. Donada una fórmula del llenguatge, podem definir perfectament la substitució d'una variable de la fórmula pel seu propi nombre de Gödel. A aquesta idea l'anomenem *diagonalització.*

Definició 50. Definim la **diagonalització** d'una fórmula φ en $\mathcal{L}_{\mathbb{N}}$ per a una variable $x \in X$, denotada per $\mathrm{d}(\varphi)$, a la fórmula

$$\mathrm{d}(\varphi) = \left(\begin{smallmatrix} x \\ \underline{\lceil\varphi\rceil} \end{smallmatrix}\right)\varphi.$$

És a dir, $\mathrm{d}(\varphi)$ és resultat de substituir la variable x pel terme $\underline{\lceil\varphi\rceil}$ de Q que representa el nombre de Gödel que codifica la pròpia fórmula φ.

Considerem ara la relació $\mathrm{Cons_T}$ donada per l'expressió

$$\neg \mathrm{Pf_T}(\lceil 0 \neq 0)\rceil)$$

Aquesta relació ens permet captar el concepte de **consistència** d'una teoría matemàtica tal i com l'hem presentat a la introducció del treball. Si $\mathrm{Con_T}$ se satisfà, aleshores de la teoría T pot deduir-se que $0 \neq 0$, és a dir, T no és consistent.

Lema 10. Es verifiquen:

(a) Existeix una funció recursiva $\mathrm{num} : \mathbb{N} \to \mathbb{N}$ tal que, per tot $n \in \mathbb{N}$,

$$\mathrm{num}(n) = \lceil\underline{n}\rceil.$$

(b) Existeix una funció $\mathrm{dg} : \mathbb{N} \to \mathbb{N}$ tal que per a qualsevol fórmula φ en $\mathcal{L}_{\mathbb{N}}$, es té:

$$\mathrm{dg}(\lceil\varphi\rceil) = \lceil d(\varphi)\rceil.$$

Demostració. Per a provar (a), construirem la funció per recursió. Per al cas base ($n = 0$) definim

$$\mathrm{num}(0) = \langle h(0)\rangle.$$

Definit d'aquesta forma es verifica la condició exigida, ja que el símbol constant $0 \in \Sigma_0$ representa el nombre natural 0. Suposem que la nostra funció està definida de manera que satisfà la propietat per a n, és a dir

$$\mathrm{num}(n) = \lceil\underline{n}\rceil.$$

Volem definir-la de manera que també ho verifique per a $n+1$. Així, considerem

$$\mathrm{num}(n+1) = \langle h(S), \mathrm{num}(n)\rangle,$$

on $S \in \Sigma$ és el símbol successor de $\mathcal{L}_{\mathbb{N}}$, d'aritat 1. Per la nostra hipòtesi inductiva, aquesta darrera expressió codifica la seqüència de naturals $(h(S), \lceil\underline{n}\rceil)$, és a dir, codifica la paraula $S\underline{n}$ del llenguatge. Per definició, sabem que $S\underline{n} = \underline{n+1}$, i per tant verifica la propietat desitjada i, a més a més, és recursiva.

Per a provar (b), per a cada nombre natural $a \in \mathbb{N}$ i per a una variable $x \in X$ definim:

$$\mathrm{dg}(a) = \mathrm{Sub}\left(a, \lceil x\rceil, \mathrm{num}(a)\right)$$

on $\mathrm{Sub} : \mathbb{N}^3 \to \mathbb{N}$ és la relació que hem introduït al capítol anterior. Aleshores notem que per la definició de diagonalització per a una variable x i la definició de la funció num:

$$\mathrm{dg}(\lceil\varphi\rceil) = \mathrm{Sub}\left(\lceil\varphi\rceil, \lceil x\rceil, \lceil\underline{\lceil\varphi\rceil}\rceil\right) = \lceil d(\varphi)\rceil,$$

i per tant, es completa la prova.

A continuació presentem el lema de la diagonalització, que permet identificar quan la teoría Q implica sintàcticament una certa fórmula amb el mateix nombre de Gödel de la fórmula.

Teorema 10. (Lema de la diagonalització o de l'autorreferència). Per a qualsevol $\mathcal{L}_{\mathbb{N}}$-fórmula o $\mathcal{L}_{\mathbb{N}}$-sentència $\varphi(x)$ amb una única variable lliure $x \in X$, existeix una $\mathcal{L}_{\mathbb{N}}$-sentència σ verificant:

$$Q \vdash \sigma \quad \text{si, i només si,} \quad \varphi(\underline{\lceil \sigma \rceil}).$$

Demostració. Per provar-ho, anem a emprar la funció dg que hem definit al lema anterior. Com que dg és recursiva, aleshores pel teorema de representació està representada en Q per una certa fórmula $\psi(x, y)$. Aleshores per definició de funció representable:

$$Q \vdash \forall y(\psi(\underline{n}, y) \longleftrightarrow y = \underline{\mathrm{dg}(n)}). \tag{3.9}$$

Siga $v_0 \in X$ una variable, considerem la $\mathcal{L}$-fórmula $\delta(v_0)$ donada per l'expressió

$$\exists y\left(\psi(v_0, y) \wedge \varphi(y)\right).$$

Considerem també el seu nombre de Gödel, $n = \lceil \delta(v_0) \rceil$. Ara, definim la fórmula σ com la diagonalització $\mathrm{d}(\delta(v_0))$, és a dir, el resultat de substituir la variable v_0 per el terme $\underline{n}$ en δ:

$$\exists y(\psi(\underline{n}, y) \wedge \varphi(y)). \tag{3.10}$$

Ara considerem el nombre natural

$$k = \mathrm{dg}(n) = \mathrm{dg}\left(\lceil \delta(v_0) \rceil\right),$$

on hem aplicat la definició de n a la darrera igualtat. Per l'apartat (b) del lema anterior sabem que:

$$\mathrm{dg}\left(\lceil \delta(v_0) \rceil\right) = \lceil \mathrm{d}(\delta(v_0)) \rceil = \lceil \sigma \rceil,$$

on hem aplicat la definició de σ en l'última igualtat. Aleshores si substituïm açò en (3.9) obtenim:

$$\mathrm{Q} \vdash (\psi(\underline{n}, y) \longleftrightarrow y = \underline{k}).$$

Però per la definició de σ (3.10):

$$\mathrm{Q} \vdash \sigma \quad \text{si, i només si,} \quad \exists y(y = \underline{k} \wedge \varphi(y)).$$

Ens adonem de l'equivalència sintàctica de les següents expressions:

$$\exists y(y = \underline{k} \wedge \varphi(y)) \quad \text{si, i només si,} \quad \varphi(\underline{k}) \quad \text{si, i només si,} \quad \varphi(\underline{\lceil \sigma \rceil}),$$

on hem aplicat la definició de k.

Abans de provar el resultat més important d'aquest treball, necesitem un lema previ.

Lema 11. Siga T una teoría sobre un llenguatge $\mathcal{L} \supseteq \mathcal{L}_{\mathrm{N}}$. Si $\underline{\mathrm{CnT}}$ és recursiva, aleshores $\underline{\mathrm{Cn}(\mathrm{T} \cup \mathrm{Q})}$ és una relació recursiva.

Demostració. Com el conjunt d'axiomes de la teoria Q és finit, és suficient provar que per a tota $\mathcal{L}$-sentència τ en el llenguatge $\mathcal{L}$, el conjunt $h(\mathrm{Cn}(\mathrm{T} \cup \{\tau\})$ és recursiu. Notem que si α és una $\mathcal{L}$-sentència, aleshores

$$\alpha \in \underline{\mathrm{Cn}(\mathrm{T} \cup \{\tau\}} \quad \text{si, i només si,} \quad \tau \to \alpha \in \mathrm{CnT}.$$

Així, si traduïm aquesta expressió emprant la nostra codificació, per a un nombre natural a:

$$a \in \underline{\mathrm{Cn}(\mathrm{T} \cup \{\tau\})} \quad \text{si, i només si,} \quad \mathrm{Sent}(a) \wedge \langle h(\to), \lceil \tau \rceil, a \rangle \in \underline{\mathrm{CnT}}$$

Per tant, com que la relació Sent i les codificació seqüencials i de Gödel són recursives, per la Propietat 5 es té que $h(\mathrm{Cn}(\mathrm{T} \cup \mathrm{Q}))$ és una relació recursiva.

Teorema 11. (Indecidibilitat forta en Q). Siga T una teoria sobre un llenguatge $\mathcal{L} \supseteq \mathcal{L}_{\mathrm{N}}$, és a dir, un llenguatge que conté el llenguatge dels naturals que hem treballat. Si $\mathrm{T} \cup \mathrm{Q}$ és consistent en $\mathcal{L}$, aleshores T **no** és decidible en $\mathcal{L}$.

Demostració. Recordem que una teoria T és decidible si, i només si, $\underline{\mathrm{CnT}}$ és recursiva. Raonarem per reducció a l'absurde, suposant que $\underline{\mathrm{CnT}}$ és recursiva. Aleshores, pel lema anterior es té que $\underline{\mathrm{Cn}(\mathrm{T} \cup \mathrm{Q})}$ també és recursiva, i per tant, pel teorema de la representabilitat en Q, existeix una fórmula $\beta(x)$ en Q que representa a la relació, és a dir:

$$\text{si } \underline{\mathrm{Cn}(\mathrm{T} \cup \mathrm{Q})}(\lceil\gamma\rceil) \text{ aleshores } \mathrm{Q} \vdash \beta(\underline{\lceil\gamma\rceil}), \tag{3.11}$$

i a més

$$\text{si } \neg\underline{\mathrm{Cn}(\mathrm{T} \cup \mathrm{Q})}(\lceil\gamma\rceil) \text{ aleshores } \mathrm{Q} \vdash \neg\beta(\underline{\lceil\gamma\rceil}), \tag{3.12}$$

per la definició de relació representable. Ara considerem la fórmula $\neg\beta(x)$. Pel lema de la diagonalització, existeix una sentència σ en el llenguatge $\mathcal{L}_{\mathbb{N}}$ de manera que:

$$\mathrm{Q} \vdash \sigma \quad \text{si, i només si,} \quad \neg\beta(\underline{\lceil\sigma\rceil}). \tag{3.13}$$

A aquesta expressió l'anomenem **sentència de Gödel**. En la lògica clàssica que estem tractant, poden donar-se dos casos:

(a) $\mathrm{T} \cup \mathrm{Q} \vdash \sigma$. Aleshores σ verifica que el seu nombre de Gödel compleix la relació, és a dir,

$$\underline{\mathrm{Cn}(\mathrm{T} \cup \mathrm{Q})}(\lceil\sigma\rceil).$$

Per tant per (3.11) es té

$$\mathrm{Q} \vdash \beta(\lceil\sigma\rceil).$$

Però aleshores per la sentència de Gödel (3.13) es té que necessàriament $\mathrm{Q} \vdash \neg\sigma$, és a dir, una contradicció.

(b) $\mathrm{T} \cup \mathrm{Q} \nvdash \sigma$. Aleshores σ verifica que el seu nombre de Gödel no compleix la relació, és a dir:

$$\neg\underline{\mathrm{Cn}(\mathrm{T} \cup \mathrm{Q})}(\lceil\sigma\rceil).$$

Però en aquest cas, per 3.12 se segueix que

$$\mathrm{Q} \vdash \neg\beta(\underline{\lceil\sigma\rceil}).$$

De nou, per la sentència de Gödel (3.13), se segueix que:

$$\mathrm{Q} \vdash \sigma.$$

hem arribat, doncs, altra contradicció. Per tant, $\underline{\mathrm{Cn}(\mathrm{T} \cup \mathrm{Q})}$ no pot ser recursiva, i així $\underline{\mathrm{Cn}\,\mathrm{T}}$ tampoc pot ser recursiva, és a dir, T no és decidible.

Corolari 1. (Primer teorema d'Incompletessa de Gödel.) Si T és una teoría sobre un llenguatge $\mathcal{L} \supseteq \mathcal{L}_{\mathbb{N}}$, amb $\mathrm{T} \cup \mathrm{Q}$ consistent i T axiomatizable, aleshores T no és completa.

Demostració. Raonem per reducció al absurde. Suposem que T és una teoría completa. Pel Teorema 8 de la última secció del capítol anterior, sabem que si T és completa i axiomatizable, aleshores T és decidible, contradient la indecidibilitat forta en Q. Per tant T no pot ser completa.

Acabem de provar que una teoria axiomàtica consistent que incloga els axiomes de la teoria aritmètica Q no pot ser completa. És a dir, no podem exigir consistència i completesa simultàniament. El punt clau de la demostració anterior i del raonament de Gödel és adonar-se de la possibilitat d'escriure la sentència de Gödel dins del sistema que hem construït. El seu significat és realment intrigant, i pot interpretar-se com:

"De Q es dedueix sintàcticament σ si, i només si, σ no és una conseqüència sintàctica de $\mathrm{Q} \cup \mathrm{T}$ ".

Així, la formalització de les matemàtiques que hem desenvolupat admet expressions com la sentència de Gödel, que ens ha permés arribar a una contradicció en el teorema d'indecidibilitat forta en Q.

Conclusions

Al capítol anterior hem provat finalment el primer teorema de Gödel. Aquest resultat frustra les exigències del programa formalista, conformant una resposta negativa al segon problema de Hilbert en els termes en què l'hem plantejat a la introducció d'aquest treball. Així i tot, els teoremes de Gödel no exclouen completament la possibilitat d'una prova de la consistència de l'aritmètica. Encara seria possible descobrir proves finitistes que no puguen ser representades en l'aritmètica, però ningú té una idea clara de com podria fer-se tal cosa, i tampoc és el que els matemàtics formalistes esperaven [4]. En qualsevol cas, d'aquest resultat, i de tota la construcció que hem desenvolupat per arribar a ell, s'extrauen conclusions molt interessants.

En primer lloc, hem vist que la formalització de les teories axiomatitzables pot dur-se a terme satisfactòriament, definint el conjunt de símbols dels llenguatges i introduint les regles de deducció sintàctica i els models, que ens han permès associar valors de veritat a les paraules del llenguatge mitjançant les valoracions. Així, hem emprat estructures algebraiques per a estudiar els processos deductius de les matemàtiques i tractar d'esclarir les seues limitacions.

Igual que els models matemàtics de la física proporcionen una descripció més o menys encertada de la difícil realitat que ens envolta, la formalització de les matemàtiques i la lògica matemàtica ofereixen una descripció aproximada de les matemàtiques. Com bromeja R. Cori a la introducció de [3], és igual d'optimista pensar que els humans som vectors habitant un espai cartesià a esperar que la lògica matemàtica siga capaç de captar la totalitat conceptual de les matemàtiques, però sense dubte l'estudi d'aquesta àrea és profitós, igual que l'estudi de l'àlgebra lineal ho és.

D'altra banda, és especialment interessant la codificació de Gödel, que a més de ser una eina per provar el primer teorema d'incompletesa, ens permet conéixer més a fons el conjunt dels nombres naturals: Hem provat que mitjançant la funció β de Gödel és possible codificar totes les proposicions de l'aritmètica dels naturals sense necessitar un conjunt més gran que els mateixos nombres naturals, conformant un curiós entrepà de la teoria l'aritmètica.

Ara bé, les conclusions que podem extraure dels teoremes de Gödel són les més importants i han estat la motivació d'aquest treball. El primer teorema de Gödel afirma que la teoria Q no és completa, i a més a més, encara que intentarem ampliar els axiomes de Q amb altra col·lecció d'axiomes T, la teoria resultant serà incompleta en qualsevol cas. És a dir, sempre existiran proposicions certes que no podran deduir-se de Q o de qualsevol ampliació de Q, com ho pot ser la teoria aritmètica de Peano. Així, aquest resultat posa l'ai al cor a la idea formada en els temps de la Grècia clàssica de que les distintes àrees matemàtiques podrien dotar-se d'una base axiomàtica que permetera conèixer totes les veritats de cada disciplina: El tractament axiomàtic de la teoria dels nombres, com hem vist, no pot suplir totes les veritats de l'aritmètica.

I el punt essencial de la prova del primer teorema és la possibilitat de construir expressions autoreferencials en la teoria Q mitjançant la codificació de Gödel, és a dir, fórmules de la teoria Q que involucren la seua mateixa codificació. I aquesta possibilitat ens ha permés construir la sentència de Gödel, la clau del seu argument. Així doncs, concloem que en la formalització de les matemàtiques que van dur a terme els matemàtics de principi del segle passat és inevitable la possibilitat d'arribar a expressions delicades d'aquest tipus. En un primer moment podem pensar que aquestes proposicions indecidibles que no poden provar-se a partir dels axiomes és limitaran a aquest racó autoreferencial de les matemàtiques, constituït per proposicions estranyes que no tenen un interés matemàtic real. Però altres matemàtics de la segona meitat del darrer segle, com J. Paris , van descobrir en [6] certes propietats autoreferencials dels nombres naturals que sí tenen

interés matemàtic en si mateixes.

Una altra conseqüència important dels teoremes de Gödel és la seua relació amb la computació i la teoria de la recursivitat. Una pregunta clàssica de les ciències computacionals és si en algun punt les màquines programables podran imitar el pensament humà i deduir teoremes com ho fan els matemàtics. Però com hem vist, el teorema de Gödel estableix que en l'àmbit teòric no és possible establir una base d'axiomes que permeten deduir totes les veritats de cada disciplina, és a dir, no pot construir-se una màquina programable en el sentit de Turing que resolga tots els problemes analíticament.

En definitiva, el teorema de Gödel no s'ha d'interpretar com un fracàs de la ciència, o com la incapacitat d'aquesta per explicar la realitat. Tampoc implica que la natura tinga límits prohibits per a la comprensió humana. Significa més bé que els recursos de l'intel·lecte humà no poden ser plenament formalitzats emprant la lògica de primer ordre. A més, no es descarta la possibilitat de descobrir nous principis de demostració i deducció. Com escriuen E. Nagel i R. Newman en [4], sembla que la ment humana posseeix unes capacitats deductives força superiors a les de les màquines programables en el sentit de Turing. El mateix treball de Gödel és un exemple d'açò, i no deu ser motiu de frustració científica, sinó d'una renovada apreciació de la creació matemàtica.

Bibliografía

[1] H. B. Enderton. *A mathematical introduction to logic.* Academic Press, 2001.

[2] B. Kim. *Complete proofs of Gödel's incompleteness theorems.* https://web.yonsei.ac.kr/bkim/goedel.pdf.

[3] R. Cori, D. Lascar. *Mathematical Logic: A course with exercises* . Oxford University Press, USA (2000).

[4] E. Nagel, J.R. Newman. *El teorema de Gödel.* http://zeus.lllf.uam.es/Master/El20Teorema20de20GC3B6del20.20Ernest20Nagel20.20James20R.20Newman.pdf

[5] J. Climent. *Teoría de modelos.*

[6] J. Paris. *A mathematical incompleteness in Peano Arithmetic.*