UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

SOLUCIÓ DE LÖB AL PROBLEMA DE HENKIN

Autor: Roger Vidal Agraz

Director: Dr. Enrique Casanovas
Realitzat a: Facultat de Matemàtiques i Informàtica

Barcelona, 19 de gener de 2020

Abstract

Inspired by Gödel's work, Henkin presented in 1952 the following problem: In any standard formal system of first-order arithmetic, a formula can be constructed which expresses that itself is provable. Is this formula provable? Or is it independent?

In this thesis all the necessary tools to build the proof that Löb shared 3 years after answering affirmatively Henkin's question are studied.

Resum

Seguint els passos de Gödel, el problema que Henkin va plantejar al 1952 era el següent: A un sistema formal estǹdard (en lògica de primer ordre) capaç de descriure l'aritmètica, podem construir una fórmula que digui de si mateixa que és demostrable. La pregunta, doncs, és: aquesta formula és demostrable al sistema? O per contra és independent?

A aquest treball desenvoluparem totes les eines necessàries per veure la demostració que va fer Löb 3 anys més tard responent afirmativament a la pregunta.

2010 Mathematics Subject Classification. 03F30, 03F40

Agraïments

Primer de tot vull agrair al meu tutor Enrique Casanovas la seva gran paciència, ajuda i guia en aquest treball.

A la Marta Bustins, l'Isaac Fernández, l'Ester Calveras, l'Eloi Sans i l'Aida Chaikh per la seva ajuda.

A la meva família i als meus amics i amigues per animar-me i aguantar-me durant tot aquest temps.

Finalment, a les bibliotecàries de la biblioteca de matemàtiques de la UB per la paciència, l'ajuda i per el treball que els hi he donat.

Índex

1 Introducció

El projecte

El Teorema de Löb s'emmarca en un sistema formal per a l'aritmètica, en el qual es pugui definir una fórmula (que compleix una sèrie de condicions anomenades condicions de demostrabilitat de Hilbert-Bernays-Löb, i que enunciem a 4.21) que expressa d'una altra fórmula que és demostrable. En aquest context, es pot construir una fórmula que parli de la seva pròpia demostrabilitat. Aquesta és la fórmula que va crear i utilitzar Gödel als anys 30 del segle passat per demostrar el primer dels seus famosos teoremes d'incompletessa. Allà la feia servir precisament per parlar d'una fórmula que no era demostrable. Anys més tard, Henkin va plantejar el problema contrari; preguntava si era demostrable la fórmula que digués de si mateixa que sí era demostrable. El teorema que demostrarem confirma que aquesta darrera fórmula és, en efecte, demostrable.

Nosaltres, però, ens cenyirem a demostrar-ho dins l'aritmètica de Peano (el sistema formal estàndard per l'aritmètica dels nombres naturals) en un sistema de lògica de primer ordre. Per fer-ho, sobretot ens guiarem pel llibre *"The logic of provability"*, de *G. Boolos* [1], però donant fortes pinzellades dels apunts de l'assignatura *Mathematical Logic* de *E. Casanovas* del màster de Lògica Pura i Aplicada [2].

Actualment tota aquesta teoria de la demostrabilitat s'ha separat de la filosofia i la metamatemàtica i s'axiomatitza a la lògica modal, on s'assumeixen coses que nosaltres haurem de demostrar i on la fórmula que parla de la demostrabilitat s'ha transformat en un símbol bàsic d'aquesta lògica ($\Box$) que expressa la necessitat d'una certa altra fórmula. Nosaltres no entrarem a aquest àmbit (tot i que doni moltíssim de si), ni a debatre gaire sobre totes les qüestions filosòfiques que es deriven del teorema que demostrarem (que també poden ser moltes i molt interessants).

Així doncs, en aquest treball començarem explorant el sistema marc de lògica de primer ordre on després fonamentarem l'aritmètica dels naturals de Peano partint dels axiomes. Parlarem també del concepte de veritat o certesa (i.e. de semàntica) que definirem, ja que, com es veurà a les conclusions, el centre d'aquest treball va obrir la porta a noves paradoxes en el llenguatge natural. També veurem com es poden demostrar algunes propietats aritmètiques formalment en aquest sistema i veurem les definicions formals en lògica de primer ordre de molts conceptes aritmètics bàsics.

Després, un cop haguem construït totes les eines necessàries, començarem a donar voltes a les esmentades condicions de demostrabilitat i construirem una fórmula que demostrarem que les compleix i que expressa la demostrabilitat. També haurem de fer una aturada a les codificacions de Gödel per passar de fórmules a nombres naturals on poder parlar de l'aritmètica dins l'aritmètica, així com veure el lema diagonal de Gödel, ja que l'autorreferència d'una fòrmula és central en aquest treball.

Finalment, demostrarem el teorema de Löb, veurem un corol·lari que no hem volgut deixar de posar i farem un petit comentari de les paradoxes que hem comentat.

Estructura de la Memòria

Començarem el treball amb un breu context històric sobre els orígens del problema i fent cinc cèntims sobre la història de la solució.

El següent capítol l'iniciarem definint els conceptes més bàsics del llenguatge que farem servir. Seguirem enunciant els axiomes sobre els que ens recolzarem per construir l'aritmètica i definint alguns conceptes bàsics més. Seguidament entrarem a parlar de semàntica i de què entenem per ser veritat i començarem a donar algunes definicions i a enunciar i demostrar alguns teoremes simples de l'aritmètica. Per continuar definirem les classes de fórmules que utilitzarem majorment durant la resta del treball i demostrarem alguns fets importants sobre elles. A més, demostrarem un teorema força important del treball. Acabarem el capítol definint, enunciant i demostrant les eines aritmètiques que encara ens manquen.

El quart capítol l'iniciarem establint la codificació que farem servir per traslladarnos dels enunciats lògics als nombres naturals i, a la següent secció, ens traslladarem a la pròpia aritmètica. Tot seguit enunciarem les Condicions de Demostrabilitat i donarem una fórmula que demostrarem que compleix les condicions esmentades. Per acabar, enunciarem i demostrarem el lema diagonal que permet l'autoreferència de les fórmules.

Un cop definides i demostrades totes les eines necessàries, al següent capítol enunciarem i demostrarem el propi Teorema de Löb.

Per acabar, al darrer capítol, parlarem breument d'algunes conseqüències del teorema, a més d'enunciar i demostrar un corol·lari molt maco, i acabarem comentant les conclusions del treball.

2 Breu context històric

Al II Congrés Internacional de Matemàtics de París de l'any 1900, David Hilbert va anunciar la famosa llista del que ell considerava com els principals problemes oberts de les matemàtiques d'aquell moment.

Un d'ells, el segon concretament, deia el següent: *"La compatibilitat dels axiomes de l'aritmètica: Demostrar que els axiomes no són contradictoris, és a dir, demostrar que basant-se en els axiomes no es podrà arribar mai a resultats contradictoris mitjançant un nombre finit de deduccions lògiques"*.

30 anys més tard i enmig d'una polèmica a la comunitat matemàtica entre els intuicionistes encapçalats per L. E. J. Brouwer i els formalistes de D. Hilbert, Gödel va publicar la demostració dels seus famosos Teoremes d'Incompletesa en un article titulat *"Sobre proposicions formalment indecidibles de Principia Mathematica i sistemes relacionats"* a la revista *"Monatshefte für Mathematik"*. Aquests teoremes van acabar amb l'esmentada polèmica i van ensorrar les esperances de Hilbert d'axiomatitzar les matemàtiques. El primer dels teoremes diu que, a un sistema axiomàtic consistent que permeti descriure l'aritmètica dels nombres naturals, es pot demostrar que existeix una fórmula que diu de si mateixa que no és demostrable. Així doncs, si aquesta fórmula és demostrable caiem en contradicció i el sistema no és consistent, però, per altra banda, si la fórmula no és demostrable, el sistema no és complet; és a dir, hi ha alguna veritat aritmètica que no es pot demostrar.

20 anys més tard d'això, L. Henkin, en una secció de la revista *"The Journal of Symbolic Logic"* on enunciaven problemes oberts de la lògica, plantejava el següent problema:

"Si Σ és qualsevol sistema formal estàndard adequat per a la teoria de nombres recursiva, una formula (que té un cert nombre enter q com el seu nombre de Gödel) pot ser construïda de manera que expressi la proposició que la fórmula amb nombre de Gödel q és demostrable a Σ. Aquesta fórmula és demostrable o independent a Σ?"

i.e. la pregunta era si era demostrable el cas contrari al de Gödel.

De tota manera, en aquest enunciat, no queda del tot clar què és el que s'havia de demostrar, ja que, com G. Kreisel va avançar un any més tard, la resposta pot ser tant sí com no, depenent de com s'expressi la pròpia demostrabilitat. Així doncs, tal com Kreisel entenia la pròpia demostrabilitat, va construir dues fórmules expressant la demostrabilitat i una sentència que expressava la seva pròpia demostrabilitat. Una era demostrable i l'altre no.

Un any més tard d'això, el 1954, M. H. Löb va anunciar la solució al problema de Henkin en una xerrada al XII Congrés Internacional de Matemàtics d'Amsterdam i, a l'any següent, va publicar a la mateixa revista on s'havia enunciat el problema un article amb la demostració completa i ampliada amb suggeriments del propi Henkin.

Per a aquesta demostració, Löb va entendre aquesta referència a la pròpia demostrabilitat com l'entenem avui dia, i.e. calia demostrar una fórmula φ tal que $\Sigma \vdash \varphi \leftrightarrow \mathrm{B}(\ulcorner\varphi\urcorner)$, amb la fórmula $\mathrm{B}(x)$ complint les Condicions de Demostrabilitat que avui anomenem de Hilbert-Bernays-Löb, bastant similars a les Condicions de Demostrabilitat de Hilbert-Bernays (ja establertes per Bernays anys abans i que Kreisel va ignorar) i que són una fusió d'aquestes i les Condicions de Demostrabilitat de Löb.

3 Aritmètica de Peano

A aquest capítol, definirem la lògica de primer ordre que farem servir, enunciarem els axiomes en què ens recolzarem, parlarem de la semàntica i justificarem la construcció de les fórmules per significar conceptes complexos a partir de les poques eines de les que disposarem a l'inici i enunciarem i demostrarem uns pocs teoremes sobre els nombres naturals.

3.1 Notació bàsica

En aquesta secció començarem explicant els símbols que farem servir al llarg del treball, tant a la part lògica com a la part aritmètica del mateix.

El símbol "$\vdash$"serà el que farem servir, com és habitual al camp de la lògica, per significar "es dedueix que...".

També construirem la lògica de primer ordre partint dels símbols bàsics "$\rightarrow$", "$\bot$", "$=$", "$\forall$", "(", i ")", significant respectivament "*implica*", "*contradicció* ", "*igual*", el quantificador universal "*per tot*" i, finalment, els símbols d'obrir i tancar parèntesis.

De la mateixa manera, els altres elements bàsics per construir l'aritmètica de Peano (en endavant AP) són les variables $x, y, z, v_0, v_1, ...$, i, a més dels símbols anteriors, els símbols bàsics no lògics de l'aritmètica: la constant "$\mathbf{0}$", el símbol del successor "$\boldsymbol{s}$" i els símbols de la suma "$\mathbf{+}$" i del producte "$\mathbf{\times}$".

Sovint, per alleugerir la notació, farem servir la negació "$\neg\varphi$" com l'oració "$\varphi \rightarrow \bot$", la desigualtat "$s \neq t$" com l'oració "$\neg s = t$", el símbol del quantificador existencial "$\exists$", en la forma "$\exists x\varphi$", que el definim com l'oració "$\neg\forall x\neg\varphi$", la disjunció "$\varphi \vee \psi$" que serà "$\neg\varphi \rightarrow \psi$", la conjunció "$\varphi \wedge \psi$" com "$\neg(\varphi \rightarrow \neg\psi)$" i, per acabar, la doble implicació "$\varphi \leftrightarrow \psi$" serà "$\neg((\varphi \rightarrow \psi) \rightarrow \neg(\psi \rightarrow \varphi))$".

També utilitzarem de vegades el símbol "$\equiv$"per a significar que dues fórmules són equivalents entre elles.

Entrem ara a definir alguns dels conceptes més bàsics que farem servir durant el treball.

Definició 3.1. *Seqüència Finita*

Sigui A un conjunt. Una seqüència finita s de longitud k (un nombre natural) és un element de A^k, on A^k és el producte cartesià d'A per A k vegades. Així doncs, per cada $i < k$, l'objecte s_i, que és el seu valor a i, és un element d'A.

Definició 3.2. *Terme* d'AP. Ho definim recursivament:

i) Cada variable és un terme.

ii) $\mathbf{0}$ és un terme.

iii) Si t és un terme, $\boldsymbol{s}t$ també ho és.

iv) Si t i t' són termes, $(t + t')$ i $(t \times t')$ també ho són.

Definició 3.3. *Fórmula atòmica:*

φ és una fórmula atòmica si φ és $\bot$ o bé existeixen termes t i t' tals que φ és $t = t'$.

Definició 3.4. *Fórmula d'AP:*

φ és una fórmula d'AP si existeix una seqüència finita de longitud k tal que el valor k-èssim de la mateixa és φ i, per cada $i < k$, el valor i-èssim és o bé una fórmula atòmica o bé $(s_j \to s_l)$ amb s_j i s_l valors anteriors a l'i-èssim o bé $\forall v_l s_j$ amb v_l una variable i s_j un valor anterior a l'i-èssim.

També definim la que serà la regla d'inferència lògica d'AP:

Definició 3.5. *Conseqüència de Modus Ponens:*

φ és conseqüència de Modus Ponens de $(\psi \to \varphi)$ i ψ.

Finalment, introduïm un grapat de conceptes més que utilitzarem al principi de la següent secció.

Definició 3.6. *Aparició lligada* d'una variable, *Aparició lliure* d'una variable, *Variable lliure* i *Variable lligada.*

Una aparició lligada de la variable x a la fórmula φ és una aparició de x que està a l'abast d'un quantificador $\forall$, i.e. existeixen una fórmula ψ i dues seqüències finites de símbols χ i τ tals que φ és $\chi * \forall x \psi * \tau$ (on χ i τ poden ser seqüències buides, $*$ l'utilitzem per significar que concatenem les fórmules i comptant que x és una aparició dins de ψ). En aquest cas diem que la aparició de $\forall$ lliga l'aparició de x.

En cas contrari, diem que és una aparició lliure.

La variable x és lliure a φ si com a mínim té una aparició lliure a φ.

La variable x és lligada a φ si com a mínim té una aparició lligada a φ.

Observació 3.7. La definició de variable lliure també es pot donar constructivament: La variable x és lliure a la fórmula φ si existeix una seqüència finita $s_0, ..., s_n$ tal que: s_n és φ, s_0 és una fórmula atòmica de la forma $t = t'$ i x és a t o a t' i per cada $j < i$ existeix una variable y diferent de x i una fórmula ψ tal que $s_{j+1} = s_j \to \psi$, o bé $s_{j+1} = \psi \to s_j$, o bé $s_{j+1} = \forall y s_j$.

A banda d'això, també cal comentar que, tal i com hem definit el quantificador existencial "$\exists$", una aparició de x de la forma $\exists x \varphi$ també és una aparició lligada.

Definició 3.8. *Variable lliurement substituïble*

La variable x és lliurement substituïble pel terme t a la fórmula φ si és lliure a φ i no hi ha cap ocurrència lliure de x a φ que caigui a l'abast d'un quantificador que lligui una variable de t.

Definició 3.9. *Substitució:*

El resultat $t^* = t'\binom{x}{t}$ de *substituir la variable x pel terme t al terme t'* és quelcom tant senzill com substituir totes les aparicions de x pel terme t, al terme t'

Observació 3.10. De la mateixa manera es defineix el resultat $\varphi\binom{x}{t}$ de *substituir les aparicions lliures de la variable x pel terme t a la fórmula φ.*

3.2 Construcció de l'Aritmètica de Peano

Per començar amb la construcció de l'Aritmètica de Peano, ens cal enunciar els axiomes sobre els que es recolza.

Per una banda, tenim totes les tautologies de la lògica proposicional, que es caracteritzen en els següents axiomes bàsics:

Definició 3.11. Axiomes de la lògica proposicional (Axioma LP):

i) $\varphi \to (\psi \to \varphi)$

ii) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

iii) $((\varphi \to \bot) \to \bot) \to \varphi$

Per una altra banda, els axiomes bàsics del quantificador universal:

Definició 3.12. Axiomes de la quantificació (Axioma Q):

i) $\forall x\varphi \to \varphi\binom{x}{t}$ amb x essent lliurement substituïble per t a φ.

ii) $\forall x(\varphi \to \psi) \to (\forall x\varphi \to \forall x\psi)$

iii) $\varphi \to \forall x\varphi$ amb la variable x no essent lliure a φ.

Per continuar, els axiomes bàsics de la igualtat:

Definició 3.13. Axiomes de la igualtat (Axioma I):

i) $x = x$

ii) $(x = y) \to (y = x)$

iii) $x = y \to (y = z \to x = z)$

iv) $x_1 = y_1 \to (x_2 = y_2 \to ...(x_n = y_n \to Fx_1...x_n = Fy_1...y_n))$ Essent F una de les funcions bàsiques d'AP (i.e. $+, \times,$ o $\boldsymbol{s}$),

Finalment, a banda dels axiomes lògics, tenim els següents axiomes bàsics no lògics:

Definició 3.14. Axiomes pel successor, la suma i el producte (Axioma SSP):

i) $\mathbf{0} \neq \boldsymbol{s}x$

ii) $\boldsymbol{s}x = \boldsymbol{s}y \to x = y$

iii) $x + \mathbf{0} = x$

iv) $x + \boldsymbol{s}y = \boldsymbol{s}(x + y)$

v) $x \times \mathbf{0} = \mathbf{0}$

vi) $x \times \boldsymbol{s}y = (x \times y) + x$

vii) $(\forall x(x = \mathbf{0} \to \varphi) \wedge \forall y[\forall x(x = y \to \varphi) \to \forall x(x = \boldsymbol{s}y \to \varphi)]) \to \varphi$

L'axioma vii) d'aquesta llista, es mereix un comentari a part. Es tracta de l'*axioma d'inducció* i és l'altre mètode de demostració de que disposarem, a banda de la regla d'inferència *Modus Ponens*.

Definició 3.15. *Generalització:*

Diem que ψ és una generalització de φ si existeix un $n \geqslant 0$ i unes variables $x_1, ..., x_n$ tals que $\psi = \forall x_1 ... \forall x_n \varphi$.

Així doncs, els axiomes són totes les generalitzacions de totes les fórmules que apareixen als anteriors llistats d'axiomes.

Definició 3.16. *Demostració:*

Una demostració d'una fórmula φ a AP és una seqüència finita de fórmules, tals que la darrera és φ i les anteriors són o bé un axioma d'AP o bé conseqüència de Modus Ponens d'anteriors fórmules de la seqüència.

Observació 3.17. També direm que una fórmula φ *és demostrable en AP* si existeix una demostració de φ i ho notarem $\text{AP} \vdash \varphi$.

Definició 3.18. *Terme tancat:*

Un terme és tancat si no conté cap variable.

Definició 3.19. *Sentència:*

Una fórmula φ és una sentència si no conté variables lliures.

3.3 Semàntica de l'Aritmètica de Peano

Ara entrarem a parlar de semàntica; és a dir, d'interpretacions i de veritats.

A aquesta introducció passarem de puntetes per alguns conceptes, sense endinsar-nos gaire. Així doncs, comencem parlant de què vol dir ser veritat en lògica en general.

Un llenguatge L de lògica de primer ordre és el conjunt de símbols no lògics amb els que es treballa. En el nostre cas, seran el zero ($\mathbf{0}$), el successor ($\boldsymbol{s}$) i la suma i el producte ($+$ i $\times$).

Ara, un cop fixat el vocabulari, hem de definir què és una *L-estructura*. Això és, un parell ordenat $\mathcal{M} = (M, I)$, tal que M és un conjunt no buit que serà l'*univers* de l'estructura (i.e. el conjunt de tots els objectes que poden haver) i I és una aplicació anomenada *interpretació*, tal que per a cada símbol $s \in L$, compleix que:

- Si $c \in L$ és una constant, $c^{\mathcal{M}} \in L$.
- Si $F \in L$ és una funció n-ària, $F^{\mathcal{M}} : M^n \to M$
- Si $R \in L$ és una relació n-ària, $R^{\mathcal{M}} \subseteq M^n$

Una *assignació* a una L-estructura $\mathcal{M}$ és una aplicació del conjunt de totes les variables en l'univers M de $\mathcal{M}$.

Suposem que s és una assignació. Ara cal definir la *denotació* $t^{\mathcal{M}}$ d'un L-terme t a $(\mathcal{M}, s)$ com l'element $t^{\mathcal{M}}[s]$ de l'univers M de $\mathcal{M}$ caracteritzat recursivament per:

- Si x és una variable $x^{\mathcal{M}}[s] = s(x)$
- Si $c \in L$ és una constant $c^{\mathcal{M}}[s] = c^{\mathcal{M}}$

- Si $F \in L$ és una funció n-ària i $t_1, ..., t_n$ són L-termes, $(Ft_1, ..., t_n)^{\mathcal{M}}[s] = F^{\mathcal{M}}(t_1^{\mathcal{M}}[s], ..., t_n^{\mathcal{M}}[s])$

A continuació, hem de definir una relació de *satisfacció* (o *veritat*) entre fórmules de L i assignacions a $\mathcal{M}$. $\mathcal{M} \models \varphi[s]$ significa, doncs, que s satisfà φ a $\mathcal{M}$ i entendrem que φ és *veritat* (o es compleix) a $\mathcal{M}$ segons s. Per definir bé la relació primer introduirem una mica de notació. Si x és una variable, s una assignació a $\mathcal{M}$ i $a \in M$, llavors s_a^x és la assignació a $\mathcal{M}$ tal que $s_a^x(x) = a$ i que coincideix en la resta de variables. Llavors la relació de satisfacció es defineix recursivament:

- $\mathcal{M} \models t_1 = t_2[s]$ si i només si $t_1^{\mathcal{M}}[s] = t_2^{\mathcal{M}}[s]$
- $\mathcal{M} \models Rt_1, ..., t_n[s]$ si i només si $\langle t_1^{\mathcal{M}}[s], ..., t_n^{\mathcal{M}}[s]\rangle \in R^{\mathcal{M}}$
- $\mathcal{M} \not\models \bot\ [s]$
- $\mathcal{M} \models (\varphi \to \psi)[s]$ si i només si, o bé $\mathcal{M} \models \psi[s]$, o bé $\mathcal{M} \not\models \varphi[s]$
- $\mathcal{M} \models \forall x\varphi[s]$ si i només si $\mathcal{M} \models \varphi[s_a^x]$ per a tot $a \in M$

Ara, doncs, diem que la fórmula φ és *conseqüència lògica* del conjunt de fórmules Γ (i.e. $\Gamma \models \varphi$) si es compleix que per a cada L-estructura $\mathcal{M}$ i per a cada assignació s de la mateixa, si $\mathcal{M} \models \Gamma[s]$ (i.e. $\mathcal{M} \models \psi[s]$ per a cada fórmula ψ de Γ), llavors $\mathcal{M} \models \varphi[s]$.

Ens resta enunciar un teorema força important de la lògica de primer ordre que, tot i que no demostrarem, per comoditat farem servir molt fortament tot i que sense mencionar-ho i ni tant sols parar-nos a reflexionar per què passem del càlcul deductiu a la conseqüència lògica. Nosaltres l'aplicarem a AP, però és extensible a d'altres sistemes.

Teorema 3.20. (de Completesa de Gödel) Donat un conjunt de fórmules Γ i una fórmula φ, llavors $\Gamma \vdash \varphi$ si i només si $\Gamma \models \varphi$.

També donarem per suposat que el càlcul que utilitzem és correcte, així que comptem amb el *teorema de deducció* (Tenint un conjunt de fórmules Σ i dues fórmules més, φ i ψ, es compleix que si $\Sigma \cup \{\varphi\} \vdash \psi$, llavors $\Sigma \vdash (\varphi \to \psi)$), o amb altres resultats, com que si $\Sigma \vdash \varphi$, i x és una variable que no és lliure a φ, llavors $\Sigma \vdash \forall x\varphi$; que $\neg\neg\varphi \equiv \varphi$; o que $\forall x\varphi \vdash \exists x\varphi$.

També hem de començar a tractar amb numerals. El numeral d'un nombre és la representació que es fa del nombre en AP. Com que a AP només tenim el símbol de constant $\mathbf{0}$ i el símbol del successor $\boldsymbol{s}$, no podem escriure els nombres normalment, sinó que hem d'escriure'ls com el successor del successor, etc, del $\mathbf{0}$ o, en tot cas, com a resultat d'operacions bàsiques entre numerals. Així, per exemple, el número 3 té com a numeral el $\boldsymbol{sss0}$, que denotarem com a $\mathbf{3}$ per alleugerir aquesta farragosa notació.

Ara, simplificant tota la introducció de la secció, una sentència d'AP direm que és *veritat* si és veritat a $(\mathbb{N}, +, \times, 0, s)$.

Cada terme tancat t denota un únic nombre natural: $\mathbf{0}$ denota 0 i, si t i t' denoten n i n', llavors $\boldsymbol{s}t$, $t + t'$ i $t \times t'$ denoten $n + 1$, $n + n'$ i $n \times n'$. El *numeral* $\boldsymbol{n}$ per al nombre n és, com hem dit abans, el terme tancat que resulta de n aparicions del símbol successor $\boldsymbol{s}$ seguides del símbol zero $\mathbf{0}$.

La sentència $\exists x\varphi$ és veritat si, per algun nombre n, $\varphi\binom{x}{\boldsymbol{n}}$ és veritat i, una fórmula φ i una seqüència $v_0, ..., v_m$ de variables diferents que incloguin totes les variables lliures de φ defineix una relació m-ària entre els nombres $n_0, ..., n_m$ si $\varphi\binom{v_0}{\boldsymbol{n_0}}...\binom{v_m}{\boldsymbol{n_m}}$ és veritat.

Podria semblar, però, que amb les eines de què disposem fins ara, seria difícil demostrar cap propietat sobre l'aritmètica, però de fet l'AP pot expressar i demostrar moltes propietats sobre els nombres naturals. Veiem una mostra:

Teorema 3.21. Si i + j = k, llavors AP $\vdash \boldsymbol{i+j=k}$

Demo: Ho farem per inducció. Si $i+j=k$, i $j=0$, llavors $i=k$. Així el numeral $\boldsymbol{j}$ és $\mathbf{0}$, i per l'Axioma *iii*) SSP, AP $\vdash \boldsymbol{i+j=i+0=i=k}$. Llavors, suposem cert per a j, i veie-m'ho per a $j+1$: Si $i+(j+1)=k$, llavors, per algun m, $i+j=m$ amb $k=m+1$, i per tant $\boldsymbol{k=sm}$, així, AP $\vdash \boldsymbol{i+j=m}$, d'on, per l'Axioma *iv*) SSP, AP $\vdash \boldsymbol{i+sj=s(i+j)=sm=k}$ □

Acabem de veure, doncs, que AP és capaç de demostrar una trivialitat dels naturals. També pot demostrar propietats força més complexes, com veurem a continuació, tot i que aprofitarem l'avinentesa per definir intercaladament alguns conceptes que ens seran necessaris o útils.

Definició 3.22. $x < y$ (resp. $x > y$) és la fórmula:

$$\exists z\, x + \boldsymbol{s}z = y \,(\text{resp. } \exists z\, y + \boldsymbol{s}z = x)$$

A vegades també utilitzarem, quan convingui, $x \leqslant y$ com la fórmula $(x<y)\vee(x=y)$.

Teorema 3.23. Inducció forta o completa:

Per qualsevol fórmula $\varphi(x)$, es compleix:

$$\text{AP } \vdash \forall x(\forall y(y<x\to\varphi(y))\to\varphi(x))\to\varphi(x)$$

Notació 1. Escrivim $\varphi(x)$ enlloc de φ per fer èmfasi sobre una variable lliure.

A més, per escurçar la notació, abreujarem com a $A\leftrightarrow B, \leftrightarrow C, \leftrightarrow$ *etc* l'expressió $(A\leftrightarrow B)\wedge(B\leftrightarrow C)\wedge$, *etc*.

Demo: Suposem veritat $\forall x(\forall y(y<x\to\varphi(y))\to\varphi(x))$. Definim $\psi(x)$ com $\forall y(y<x\to\varphi(y))\wedge\varphi(x)$. És clar que si demostrem $\psi(x)$, amb la suposició inicial tindrem $\varphi(x)$. Per inducció, n'hi ha prou de demostrar $\psi(\mathbf{0})$ i $\forall x(\psi(x)\to\psi(\boldsymbol{s}x))$.

Així doncs, per l'axioma *i*) SSP , $\forall y\,\neg\, y<\mathbf{0}$, i amb l'axioma *iii*) LP, tenim $\forall y(y<\mathbf{0}\to\varphi(y))$, que amb la suposició inicial ens dóna $\varphi(\mathbf{0})$ i per tant $\psi(\mathbf{0})$.

Ara suposem cert $\psi(x)$. Com AP $\vdash (x<\boldsymbol{s}y)\leftrightarrow(\exists z\, x+\boldsymbol{s}z=\boldsymbol{s}y), \leftrightarrow (\exists z\,\boldsymbol{s}(x+z)=\boldsymbol{s}y), \leftrightarrow (\exists z\, x+z=y), \leftrightarrow^* (x+\mathbf{0}=y\vee\exists w\, x+\boldsymbol{s}w=y), \leftrightarrow (x=y\vee x<y)$ (amb $\leftrightarrow^*$ justificat amb l'axioma *i*) SSP), tenim $\forall y(y<\boldsymbol{s}x\to\varphi(y))$, i altre cop juntament amb la suposició inicial, tenim $\varphi(\boldsymbol{s}x)$ i, per tant, $\psi(\boldsymbol{s}x)$.

□

3.4 Pseudotermes, Σ-fórmules i Δ-fórmules

Passem a definir algunes estructures lògiques que ens caldran per abastar algunes funcions (com per exemple el residu de la divisió entera o l'exponenciació, tot i que aquesta darrera no la definirem) d'AP que encara poden ser complicades amb les eines que disposem fins ara.

Notació 2. Per alleugerir la notació escriurem ν per abreujar "$v_1, v_2, ..., v_n$".

Definició 3.24. *Pseudoterme* o *Pterme*:

Una fórmula $\varphi(\nu, y)$ és un Pterme si la fórmula $\exists y(\varphi(\nu, y) \wedge \forall z(\varphi(\nu, z) \to y = z))$ (Que a abreujarem com $\exists! y\, \varphi(\nu, y)$) és demostrable en AP.

Observació 3.25. Així doncs, els Ptermes $\varphi(\nu, y)$ defineixen funcions n-àries que no ens permetien tractar els termes dels quals disposàvem.

Més endavant, definirem uns quants Ptermes. A la definició formal, definirem el concepte començant per una lletra majúscula (p.exm. $Max(x, y, z)$), però com per definició de Pterme existeix un únic nombre que compleixi la propietat a la qual es refereix el Pterme ("y"a la definició anterior, o "z"al exemple de $Max(x, y, z)$), farem servir el mateix nom però començant amb minúscula per obviar (i significar) el "resultat"(i.e. seguint l'exemple anterior $max(x, y) = z$).

Notació 3. Utilitzarem les expressions "$(\forall y < x)\varphi$", i, "$(\exists y < x)\varphi$", per abreujar respectivament "$\forall y(y < x \to \varphi)$", i, "$\exists y(y < x \wedge \varphi)$".

Definició 3.26. Σ*-fórmula estricta,* Σ*-fórmula* i Σ*-sentència*

Una Σ-fórmula estricta és un element de la classe més petita de fórmules que inclouen totes les fórmules $x = y$, $\mathbf{0} = x$, $\boldsymbol{s}x = y$, $x + y = z$, $x \times y = z$ i que, si inclou φ i ψ, també inclou $\varphi \wedge \psi$, $\varphi \vee \psi$, $\exists x\varphi$ i $(\forall x < y)\varphi$.

Una Σ-fórmula, és una fórmula equivalent a AP a una Σ-fórmula estricta.

Una Σ-sentència és una Σ-fórmula que és una sentència.

Observació 3.27. Per norma general, el que aquí anomenem Σ-fórmula, s'anomena Σ_1-fórmula, però com no farem servir les classes de fórmules Σ_2, Σ_3, etc, ens estalviarem el subíndex.

Observació 3.28. També cal comentar que la negació de totes les fórmules bàsiques de les Σ fórmules estrictes, així com les desigualtats pertinents i la negació de les mateixes són Σ-fórmules. Vegem-ho amb un parell d'exemples, ja que la resta de casos són molt similars.

$x < y$ és una Σ-fórmula, ja que és equivalent a $\exists u \exists v(x + v = y \wedge \boldsymbol{s}u = v)$, que és una Σ-fórmula estricta.

$\neg(x = y)$ (o $x \neq y$) és una Σ-fórmula, ja que és equivalent a $(x < y) \vee (y < x)$, que és una Σ-fórmula.

$\neg(x < y)$ és una Σ-fórmula, ja que és equivalent a $(y < x) \vee (x = y)$, que és una Σ-fórmula.

Com a segon exemple, podem veure que $x+y < z$ és una Σ-fórmula, ja que és equivalent a la Σ-fórmula estricta $\exists u \exists v \exists w(x + y = w \wedge w + u = z \wedge \boldsymbol{s}v = u)$

$\neg(x + y = z)$ (o $x + y \neq z$) és equivalent a la Σ-fórmula $(x + y < z) \vee (z < x + y)$

$\neg(x + y < z)$ és equivalent a la Σ-fórmula $(z < x + y) \vee (x + y = z)$.

Definició 3.29. Δ*-fórmula*

Una Δ-fórmula és una fórmula φ tal que, tant φ com $\neg\varphi$ són Σ-fórmules.

Demostrarem ara uns quants fets importants sobres les fórmules Δ que ens seran molt útils durant la resta del treball.

Lema 3.30. Per a cada terme $t(x_1, ..., x_n)$ existeix una Δ-fórmula φ amb $x_1, ..., x_n$ variables lliures, i una variable y diferent de $x_1, ..., x_n$, tal que

$$\mathrm{AP} \vdash \varphi \leftrightarrow y = t$$

Demo: Ho farem per inducció sobre t. Els casos $t = x_1$, i $t = \mathbf{0}$ són obvis, ja que podem escollir $y = x_1$ i $y = \mathbf{0}$ respectivament.

Cas $t = \boldsymbol{s}t'$: Per hipòtesi d'inducció, tenim una Δ-fórmula φ, tal que $\mathrm{AP} \vdash \varphi(x) \leftrightarrow x = t$. Així doncs:

$$\mathrm{AP} \vdash x = \boldsymbol{s}t \leftrightarrow \exists y(x = \boldsymbol{s}y \wedge \varphi(y)), \leftrightarrow \forall y(\varphi(y) \rightarrow x = \boldsymbol{s}y)$$

Com el que hi ha dins d'ambdós parèntesis és Σ i, en concret, la negació del de dins del segon parèntesi (i.e. $\exists y(\neg(\varphi(y) \rightarrow x = \boldsymbol{s}y))$) també ho és, $\forall y(\varphi(y) \rightarrow x = \boldsymbol{s}y)$ és Δ

Cas $t = t_1 + t_2$: Per hipòtesi d'inducció, tenm dues Δ-fórmules φ_1, φ_2, tals que $\mathrm{AP} \vdash (\varphi_1 \leftrightarrow x = t_1) \wedge (\varphi_2 \leftrightarrow x = t_2)$. Com

$$\mathrm{AP} \vdash x = t_1 + t_2 \leftrightarrow \exists y_1 \exists y_2(\varphi_1(y_1) \wedge \varphi_2(y_2) \wedge x = y_1 + y_2), \leftrightarrow \forall y_1 \forall y_2(\varphi_1(y_1) \wedge \varphi_2(y_2) \rightarrow x = y_1 + y_2)$$

Altre cop, la negació del que hi ha dins del parèntesi és Σ, així que $\forall y_1 \forall y_2(\varphi(y_1) \wedge \varphi(y_2) \rightarrow x = y_1 + y_2)$ és Δ.

El cas $t = t_1 \times t_2$ és anàleg a l'anterior. $\square$

Lema 3.31. Per a cada fórmula atòmica φ existeix una Δ-fórmula ψ tal que $\mathrm{AP} \vdash \varphi \leftrightarrow \psi$

Demo: Ho farem per inducció sobre φ.

Si φ és $\bot$, tenim que

$$\mathrm{AP} \vdash \bot \leftrightarrow \exists x(x \neq x), \leftrightarrow \forall x(x \neq x)$$

i la negació d'aquesta darrera fórmula és Δ

Si φ és $t = t'$, per 3.30 dues Δ-fórmules φ, φ' tals que $\mathrm{AP} \vdash (x = t \leftrightarrow \varphi) \wedge (x = t' \leftrightarrow \varphi')$. I així

$$\mathrm{AP} \vdash t = t' \leftrightarrow \exists x(\varphi(x) \wedge \varphi'(x)), \leftrightarrow \forall x(\varphi(x) \rightarrow \varphi'(x)))$$

La negació de $\forall x(\varphi(x) \rightarrow \varphi'(x))$ és Σ, i hem trobat una fórmula equivalent Δ $\square$

Lema 3.32. Si φ i ψ són Σ, $(\varphi \wedge \psi)$ i $\varphi \vee \psi$ són Σ. També es compleix per a fórmules Δ.

Demo: Si φ i ψ són Σ, existeixen φ' i ψ' Σ-fórmules estrictes tals que $\mathrm{AP} \vdash \varphi \leftrightarrow \varphi'$ i $\mathrm{AP} \vdash \psi \leftrightarrow \psi'$. Llavors, tenim que:

$$\mathrm{AP} \vdash (\varphi \wedge \psi) \leftrightarrow (\varphi' \wedge \psi')$$

Anàlogament per la disjunció.

Si φ i ψ són fórmules Δ, com que $\neg(\varphi \wedge \psi)$ és equivalent a $\neg\varphi \vee \neg\psi$ i $\neg(\varphi \vee \psi)$ és equivalent a $\neg\varphi \wedge \neg\psi$, es veu fent servir la primera part del lema. $\square$

Lema 3.33. Si φ és una Σ-fórmula, $\forall x < t(\varphi)$, i, $\exists x < t(\varphi)$ són Σ.

El mateix es compleix per a Δ-fórmules.

Demo: Si φ és Σ, existeix ψ Σ-fórmula estricta tal que $\mathrm{AP} \vdash \varphi \leftrightarrow \psi$ i, per tant, obviament

$$\mathrm{AP} \vdash \exists x\varphi \leftrightarrow \exists x\psi \tag{3.1}$$

Ara

$$\mathrm{AP} \vdash (\forall x < t)\varphi \leftrightarrow \exists y(y = t \wedge (\forall x < y)\psi)$$

Tenim que $(\forall x < y)\psi$ és Σ estricta, i $y = t$ també per 3.31. Com la conjunció de Σ és Σ, per 3.1 $(\forall x < t)\varphi$ és Σ.

El cas $(\exists x < t)\varphi$ és anàleg.

Si φ és Δ, tenim que $\neg(\forall x < t)\varphi$ és equivalent a $(\exists x < t)\neg\varphi$ i, per tant, per això que acabem de veure, també és Δ. Amb $\neg(\exists x < t)\varphi$ passa el mateix, en ser equivalent a $(\forall x < t)\neg\varphi$. □

Teorema 3.34. Si φ és una fórmula acotada (i.e. Construida amb $\neg, \wedge, \vee, \forall x < t, \exists x < t$), tenim que φ és Δ.

Demo: Per inducció sobre φ.

Cas φ fórmula atòmica: φ és Δ per 3.31.

Cas $\neg\varphi$: Per hipòtesi d'inducció, φ és acotada, així que $\neg\varphi$ també i, com φ és Δ, obviament $\neg\varphi$ també (ja que $\neg\neg\varphi \equiv \varphi$).

Cas $\varphi \wedge \psi$ i $\varphi \vee \psi$: Tenim que per hipòtesi, φ i ψ són Δ i, per 3.32, $\varphi \wedge \psi$ també és Δ. Anàlogament per a $\varphi \vee \psi$.

Cas $(\forall x < t)\varphi$, i $(\exists x < t)\varphi$: Per hiòtesi, φ és Δ i, per 3.33, $(\forall x < t)\varphi$ és Δ. Anàlogament per a $(\exists x < t)\varphi$. □

Observació 3.35. Com acabem de veure, les Δ-fórmules inclouen totes les fórmules atòmiques, les fórmules $t < t'$, i són tancades amb les operacions booleanes i les quantificacions acotades.

Observació 3.36. Notem també que si $\varphi(\nu, y)$ és Σ i Pterme, llavors és Δ, ja que si $\varphi(\nu, y)$ és Pterme, en ser demostrable $\exists! y\, \varphi(\nu, y)$, $\neg\varphi(\nu, y)$ és equivalent a la fórmula $\exists z(\varphi(\nu, z) \wedge z \neq y)$, que és Σ si ho és $\varphi(\nu, y)$.

Observació 3.37. També val la pena comentar que, arrel del teorema que demostrarem a continuació, si $\varphi(\nu)$ és una Δ-fórmula, i m una n-tupla de nombres naturals, llavors o bé $\mathrm{AP} \vdash \varphi(\boldsymbol{m})$ o bé $\mathrm{AP} \vdash \neg\varphi(\boldsymbol{m})$, així que totes les Δ-fórmules són decidibles.

Així doncs, ara anem a demostrar un teorema que serà clau en els darrers capítols del treball.

Notació 4. Abans d'enunciar-lo i demostrar-lo, però, notarem com "$\bigvee[x = \boldsymbol{j} : j < i]$", la disjunció de totes les sentències $x = \boldsymbol{j}$ per tot $j < i$ amb $i > 0$.

Si $i = 0$, "$\bigvee[x = \boldsymbol{j} : j < i]$"serà "$\bot$".

Teorema 3.38. Si φ és una Σ-sentència veritable, llavors $\mathrm{AP} \vdash \varphi$

Veiem primer un lema que ens caldrà per la demostració.

Lema 3.39. Si t i t' son termes tancats i $t = t'$ és cert, llavors AP $\vdash t = t'$.

Demo: Si t i t' denoten n i n', és fàcilment demostrable per inducció sobre t que AP $\vdash t = \boldsymbol{n}$ i AP $\vdash t' = \boldsymbol{n'}$. Si $t = t'$ és cert, llavors $n = n'$ i $\boldsymbol{n}$ és el mateix numeral que $\boldsymbol{n'}$, així que AP $\vdash t = t'$. □

Demostrem ara el Teorema:

Demo(Teorema): Ho demostrarem per inducció sobre φ.

Si φ és una fórmula atòmica veritable, llavors AP $\vdash \varphi$ pel lema.

Si $\varphi \wedge \psi$ és cert, llavors φ i ψ són certes, així que AP $\vdash \varphi$ i AP $\vdash \psi$ i, per tant AP $\vdash \varphi \wedge \psi$. Similarment AP $\vdash \varphi \vee \psi$, si $\varphi \vee \psi$ és cert.

Si $\exists x \varphi(x)$ és cert, hi ha algun n tal que $\varphi(\boldsymbol{n})$ és cert, així que AP $\vdash \varphi(\boldsymbol{n})$ i, per tant AP $\vdash \exists x \varphi$.

Si $(\forall x < \boldsymbol{i})\varphi$ és cert, llavors per cada $j < i$, $\varphi(\boldsymbol{j})$ és cert, així que per cada $j < i$, AP $\vdash \varphi(\boldsymbol{j})$ i AP $\vdash x = \boldsymbol{j} \to \varphi$. D'altra banda AP $\vdash x < \boldsymbol{i} \leftrightarrow \bigvee [x = \boldsymbol{j} : j < i]$ (fàcilment demostrable per inducció), així que AP $\vdash x < \boldsymbol{i} \to \varphi$ i, per tant, AP $\vdash (\forall x < \boldsymbol{i})\, \varphi$.

Finalment, si φ és equivalent a AP a una sentència demostrable a AP, φ és demostrable a AP. □

3.5 Altres definicions i teoremes de l'aritmètica necessaris

Definició 3.40. $y|x$ és la fórmula:

$$\exists z\, z \times y = x$$

A més, és una Δ-fórmula, ja que és equivalent a $(x = \mathbf{0} \wedge y = \mathbf{0}) \vee (x \neq \mathbf{0} \wedge (\exists z < x)(z \times y = x))$.

Teorema 3.41.

$$\text{AP} \vdash x \times (y + z) = (x \times y) + (x \times z)$$

Demo: Es demostra fàcilment per inducció sobre z. □

Definició 3.42. $\text{Res}(x, y, r)$ és el Σ-Pterme:

$$(r < y \wedge \exists z\, (x = z \times y + r)) \vee (y = \mathbf{0} \wedge r = x)$$

Als naturals amb l'AP obviament no podem tenir la operació resta definida igual que als enters. Així doncs, definirem una pseudoresta que notarem amb el símbol usual de la resta "$-$" i que anomenarem, seguint a *G. Boolos* monus:

Definició 3.43. $\text{Monus}(x, y, z)$ és el Σ-Pterme

$$(x = y + z) \vee (x < y \wedge z = \mathbf{0})$$

Definició 3.44. Prim(p) és la Δ-fórmula (ja que el quantificador es pot acotar per $p\mathbf{+1}$):

$$p \neq \mathbf{0} \wedge p \neq \mathbf{1} \wedge \forall x(x|p \to x = \mathbf{1} \vee x = p)$$

Definició 3.45. Coprim(x, y) és la Δ-fórmula (el quantificador es pot acotar per x o per y):

$$\forall z(z|x \wedge z|y \to z = \mathbf{1})$$

Teorema 3.46. (Identitat de Bézout):

AP $\vdash \forall a > \mathbf{1} \forall b > \mathbf{1}(\text{Coprim}(a, b) \to \exists x \exists y(ax \mathbf{+ 1} = by))$.

Demo: Anomenem a un nombre j, *nombre bo* si $\exists x \exists y\, ax + j = by$. Hem de provar, llavors, que 1 és un *nombre bo* en els supòsits de l'enunciat. a és un *nombre bo*, ja que es pot prendre $x = b - 1$, i $y = a$ i, obviament, b també és un *nombre bo*, prenent $x = 0$, i $y = 1$. Ara, si j és un *nombre bo*, també ho és zj (multiplicant x i y per z) i, si j i j' són *nombres bons* i $j \geqslant j'$, $j - j'$ també és un *nombre bo*, ja que si $ax + j = by$ i $ax' + j' = by'$, prenent $x'' = x + by' + (b-1)x'$ i $y'' = y + ax' + (a-1)y'$, es té que $ax'' + (j - j') = by''$.

Sigui d el *nombre bo* positiu més petit, llavors, si j és un *nombre bo*, $d|j$, ja que sinó existirien q, r tals que $j = qd + r$, amb $0 < r < d$, i comptant que qd seria un *nombre bo* i $j > qd$, tindriem que $r = j - qd$ seria també un *nombre bo* entrant amb contradicció amb que d era el *nombre bo* més petit.

Llavors, com a i b són *nombres bons* i coprimers, i si $d|a$, i $d|b$, $d = 1$, tenim que 1 és un *nombre bo*.

Finalment, com que l'enunciat es tracta d'una Σ-fórmula, per 3.38, queda demostrat que és un teorema d'AP. □

Observació 3.47. Aquest darrer argument de la Σ-fórmula de la demostració anterior serà un argument que s'utilitzarà en totes les demostracions que fem a continuació, ja que realitzarem totes elles fora de la rígida formalitat d'AP. Així doncs, tot i que ho obviarem, aquest argument exacte serà el que conclourà totes les demostracions d'aquest capítol.

Teorema 3.48. AP $\vdash a > b \to \forall c(c(a - b) = ca - cb)$

Demo. Suposem $a > b$. Llavors, per definició de *monus*, tenim que $a = b + z$ i així, monus$(a, b) = a - b = z$. Per tant, multiplicant a ambdues bandes per c, tenim que $c(a - b) = cz$ equival a $ca = c(b + z)$ i per 3.41 $ca = cb + cz$. Recorrent finalment a la definició de monus altre cop, tenim que $ca - cb = cz = c(a - b)$. □

Lema 3.49. (d'Euclides):

AP $\vdash (\text{Prim}(p) \wedge p|ab) \to (p|a \vee p|b)$

Demo: Suposem que p divideix ab. Llavors, per definició de "|", existeix un z tal que $pz = ab$. Si p no divideix a, llavors a i p són coprimers i, pel teorema 3.46, existeixen x, y tals que $ax + 1 = py$. Llavors, multiplicant per b, tenim $bax + b = bpy$. Com $bax > bpy$ o bé $bax = bpy$, tenim que $bax - bpy = b$. Ara, com que $pz = ab$, $pzx - bpy = b$ i, per tant, per 3.48, $p(zx - by) = b$. □

Teorema 3.50. AP $\vdash (p|a \wedge p|b \wedge a > b) \to p|(a - b)$

Demo: Com $p|a$, tenim que existeix x tal que $px = a$. Per altre banda, com $p|b$, existeix y tal que $py = b$. Com $a > b$, tenim que existeix z tal que $a - b = z$ i, com $a = px$ i $b = py$, tenim que $px - py = z$ i, per tant, per 3.48, $p(x - y) = z = (a - b)$. □

Definició 3.51. $\mathrm{Mcm}[m(i) : i < k](l)$ és el Pterme:

$$(\forall i < k\,(m(i) > \mathbf{0}) \wedge l > \mathbf{0} \wedge \forall i < k\,(m(i)|l) \wedge \forall j < l\,\neg[j > \mathbf{0} \wedge \forall i < k\,(m(i)|j)])$$

$$\vee\,(\exists i < k\,(m(i) = \mathbf{0} \wedge l = \mathbf{0}))$$

Teorema 3.52. $\mathrm{AP} \vdash (\mathrm{Prim}(p) \wedge p|\mathrm{mcm}[m(i) : i < k]) \to \exists i < k(p|m(i))$

Demo: Ho farem per inducció sobre k. Si $k = 0$, $\mathrm{mcm}[m(i) : i < 0] = 1$ i p no divideix $\mathrm{mcm}[m(i) : i < 0]$. Suposem que $p|\mathrm{mcm}[m(i) : i < k + 1]$, llavors $\mathrm{mcm}[m(i) : i < k+1]|\mathrm{mcm}[m(i) : i < k] \times m(k)$, per construcció de mcm. Ara, per 3.49, o bé $p|\mathrm{mcm}[m(i) : i < k]$ d'on, per hipòtesi d'indcció, existeix un i tal que $p|m(i)$, o bé $p|m(k)$.

□

Teorema 3.53. Xinès del residu:

$$\mathrm{AP} \vdash [\forall i < k(1 < m(i) \wedge h(i) < m(i)) \wedge \forall i \forall j(i < j < k \to \mathrm{Coprim}(m(i), m(j)))] \to$$

$$\exists a < \mathrm{mcm}[m(i) : i < k]\ \forall i < k\ \mathrm{res}(a, m(i)) = h(i)$$

Demo: Suposem cert l'antecedent i ho demostrarem per inducció sobre $n < k + 1$.

Si $n = 0$, sigui $a = 0$. $a < 1 = \mathrm{mcm}[m(i) : i < 0]$.

Suposem $n < k$, $a < \mathrm{mcm}[m(i) : i < n]$ i $\mathrm{res}(a, m(i)) = h(i)$ per tot $i < n$. Sigui $l = \mathrm{mcm}[m(i) : i < n], m = m(n)$. m i l són coprimers, ja que si $p|l$, pel teorema 3.52 existeix algun $i < n$, tal que $p|m(i)$, i com $m(i)$ i m són coprimers, p no divideix m.

Ja que l i m son coprimers, per 3.46, existeixen x, y tals que $lx+1 = my$, i multiplicant a ambdues bandes per $a+(l-1)h(n)$, veiem que per alguns x', y', $lx'+a+(l-1)h(n) = my'$. Anomenem $a' = l(x' + h(n)) + a$, llavors $a' = my' + h(n)$. Si $i < n$, llavors, com $m(i)|l$, $\mathrm{res}(a', m(i)) = \mathrm{res}(a, m(i)) = h(i)$, i $\mathrm{res}(a', m(n)) = \mathrm{res}(a', m) = h(n)$, ja que $h(n) < m(n) = m$. Sigui $l' = \mathrm{mcm}[m(i) : i < n + 1]$, si $a' < l'$, hem acabat. Si $a' > l'$ o $a' = l'$, llavors sigui b el major múltiple de l' que sigui més petit o igual que a' i sigui $a'' = a' - b$. Tenim, doncs, que $a'' < l'$ i, com $m(i)|l'|b$, per tot $i < n + 1$, $\mathrm{res}(a'', m(i)) = \mathrm{res}(a' - b, m(i)) = \mathrm{res}(a', m(i)) = h(i)$.

□

Definició 3.54. $\mathrm{Max}[m(i) : i < k](l)$ és el Σ-Pterme:

$$\exists i < k\,(m(i) = l) \wedge \forall i < k\,(m(i) < l \vee m(i) = l)$$

Definició 3.55. $\mathrm{Max}(x, y, z)$ és el Σ-Pterme:

$$(x > y \wedge z = x) \vee (x < y \wedge z = y) \vee (x = y \wedge z = x)$$

Definició 3.56. Beta(a, b, i, r) és el Σ-Pterme:

$$\text{res}(a, \mathbf{1}+(\boldsymbol{i}+\mathbf{1}) \times b) = r$$

Lema 3.57. de la funció β de Gödel

Sigui $h(i)$ una successió de Ptermes arbitraris amb $i < k$, llavors

AP $\vdash$ Per cada k existeixen a, b, tals que per cada $i < k$, beta$(a, b, i) = h(i)$. A més, si $m = \max(k, \max[h(i) : i < k]) + 1$, a i b es poden escollir de manera que $b < \text{mcm}[i+1 : i < m] + 1$ i $a < \text{mcm}[1 + (i+1)b : i < k]$

Demo: Sigui m com al lema, llavors $m > k$ i, per cada $i < k$, $m > h(i)$. Sigui $b = \text{mcm}[i+1 : i < m]$ i suposant que $i < j < k$, mostrarem que $1+(i+1)b$, i $1+(j+1)b$ són coprimers. Suposem que $p|(1+(i+1)b)$ i que $p|(1+(1+j)b)$. Llavors, per 3.50, p divideix la seva diferència $(j-i)b$ i, per tant, o bé $p|(j-i)$ o bé $p|b$. Com $0 < j-i < k < m$, $(j-i)|b$ i, en qualsevol cas, $p|b$, així doncs $p|(i+1)b$, però, com $p|(1+(i+1)b)$, p divideix la diferència, i.e. $p|1$, contradicció.

Per tant, si $i < j < k$, $(1+(1+i)b)$ i $(1+(1+j)b)$ són coprimers. A més, per cada $i < k$, $h(i) < m < b+1 < 1+(1+i)b+1$, i $1 < 1+(i+1)b$. Ara, pel *Teorema xinès del residu*, prenent $m(i) = 1+(1+i)b$, per algun $a < \text{mcm}[1+(i+1)b : i < k]$, beta$(a, b, i) = h(i)$ per tot $i < k$.

Tot i que aquest lema l'hem enunciat amb paraules, per facilitar la lectura, també es tracta d'una Σ-fórmula, així que també es demostra per 3.38. □

4 Sintaxi de l'Aritmètica de Peano dins de l'Aritmètica de Peano

Per discutir sobre la sintaxi d'AP dins de la pròpia AP, hem de codificar qualsevol seqüència, tant de símbols lògics com de no lògics, en el llenguatge de la pròpia AP; és a dir, els hem de traduir a nombres de manera injectiva, per tal que a cada seqüència li correspongui unívocament un sol nombre i, per tant, poguem fer el camí invers. Aquesta codificació de símbols s'anomena numeració de Gödel (tot i que no farem servir la numeració que va idear Gödel originalment). Començarem definint-la abans d'entrar a demostrar com s'ho fa AP per demostrar coses sobre la seva pròpia sintaxi.

Definició 4.1. *Nombre de Gödel d'un símbol*

El nombre de Gödel d'un símbol, que notarem com Gö$(\cdot)$, és el nombre que assignem a cada símbol bàsic del llenguatge que utilitzem. En el nostre cas, per l'elecció que hem fet a l'inici del capítol anterior, fem l'assignació de la següent manera:

i) Gö$(\bot) = 1$

ii) Gö$(\to) = 3$

iii) Gö$(\forall) = 5$

iv) Gö$(=) = 7$

v) Gö$(\mathbf{0}) = 9$

vi) Gö$(\boldsymbol{s}) = 11$

vii) Gö$(\mathbf{+}) = 13$

viii) Gö$(\mathbf{\times}) = 15$

A banda d'això, a la variable i-èssima li assignarem el nombre $2i + 17$.

Observació 4.2. D'aquesta manera, cadascun dels símbols bàsics d'AP, tenen un nombre senar. Això ens servirà per diferenciar-los de les seqüències finites, ja que degut a la assignació que les hi donarem a continuació, tindran totes un nombre parell.

Ara, per codificar les seqüències finites, les construirem com a parells ordenats d'objectes. Com els següents objectes més bàsics que tenim just per sobre dels símbols són els termes i les fórmules, considerarem que: per als termes, $\boldsymbol{s}t$ serà el parell ordenat $\langle \boldsymbol{s}, t\rangle$ i $t * t'$ amb $*$ significant $\boldsymbol{+}$, o $\boldsymbol{\times}$, serà el parell ordenat $\langle *, \langle t, t'\rangle\rangle$. D'altra banda, per les fórmules atòmiques que no siguin $\bot$ (en cas que sigui $\bot$ ja té el seu propi nombre de Gödel com a símbol bàsic), tindrem el parell $\langle =, \langle t, t'\rangle\rangle$, i per les fórmules, tindrem que $\varphi \to \psi$ serà el parell $\langle \to, \langle \varphi, \psi\rangle\rangle$ i $\forall x\varphi$ serà $\langle \forall, \langle x, \varphi\rangle\rangle$.

Observació 4.3. Notem ara que els símbols d'obrir i tancar parèntesi no tenen nombre de Gödel. Això és degut a com hem codificat les seqüències finites (de manera bastant similar a la notació polaca). Com hem vist, els parèntesis no ens calen en ser substituïts pel símple ordre de construcció del nombre de Gödel de la seqüència finita.

Amb aquesta manera d'estructurar tota seqüència finita, podrem codificar-la partint de l'assignació que hem fet abans. Donarem ara unes quantes definicions i lemes per construir la codificació i assegurar-nos que és injectiva.

Notem que, a partir d'aquí, deixarem de tenir fórmules i passarem a tenir nombres, ja que ara ens estem movent dins de la pròpia AP.

Definició 4.4. $\mathrm{Par}(x, y, z)$ és el Σ-Pterme

$$\boldsymbol{2}((x \boldsymbol{+} y)(x \boldsymbol{+} y) \boldsymbol{+} x \boldsymbol{+} \boldsymbol{1})$$

Escriurem (x, y) enlloc de $\mathrm{par}(x, y)$.

Lema 4.5. $\mathrm{AP} \vdash (x, y) = (x', y') \to x = x' \wedge y = y'$.

Demo: Suposem cert l'antecedent, llavors $(x+y)(x+y)+x+1 = (x'+y')(x'+y')+x'+1$. Si $x + y < x' + y'$, tenim que $(x + y)(x + y) + x + 1 < (x + y + 1)(x + y + 1) + 1 < (x' + y')(x' + y') + 1 \leqslant (x' + y')(x' + y') + x' + 1$, de manera que $x + y < x' + y'$ no es pot complir. Anàlogament passa si $x' + y' < x + y$. De manera que $x + y = x' + y'$.

D'altre banda, si $x + y = x' + y'$, però $x < x'$, tenim que $(x' + y')(x' + y') = (x+y)(x+y) < (x+y)(x+y)+x+1 < (x'+y')(x'+y')+x'+1$ i queda també descartat. De la mateixa manera, si $x+y = x'+y'$, però $y < y'$, trobem que $x = x+y-y = x'+y'-y > x'$ i, raonant anàlogament al cas anterior, tampoc es pot complir, així que $x = x'$ i $y = y'$.

Tot i que la fórmula de l'enunciat no es tracta d'una Σ-fórmula i, per tant, no podem recórrer a 3.38, aquesta demostració informal es pot convertir en una demostració formal d'AP. □

Corol·lari 4.6. $\mathrm{AP} \vdash x < x' \to (x, y) < (x', y)$

$\mathrm{AP} \vdash y < y' \to (x, y) < (x, y')$

Definició 4.7. $\mathrm{Pr}(x, y)$ és el Σ-Pterme

$$(\exists z < x\,(y, z) = x \vee (\neg\exists w < x \exists z < x\,(w, z) = x \wedge y = \boldsymbol{0}))$$

$\mathrm{Sn}(x, y)$ és el Σ-Pterme

$$(\exists z < x\,(z, y) = x \vee (\neg\exists z < x \exists w < x\,(z, w) = x \wedge y = \mathbf{0}))$$

Observació 4.8. Notem que $\mathrm{pr}((x, y)) = x$ i $\mathrm{sn}((x, y)) = y$

Ara sí que estem preparats per començar a definir tots els elements necessaris per a codificar les seqüències finites.

Definició 4.9. SeqFin(s): És la Δ-fórmula

$$\exists a < s\, \exists b < s\, \exists k < s\, (s = ((a,\, b),\, k) \wedge$$
$$\forall c < s\, \forall d < s\, ((c,\, d) < (a,\, b) \rightarrow \exists i < k\, \mathrm{beta}(c,\, d,\, i) \neq \mathrm{beta}(a,\, b,\, i)))$$

El parell (a, b) representa la pròpia seqüència finita de nombres, el nombre k indica la longitud de la seqüència i la condició final de la funció beta serveix per garantir la unicitat de la seqüència finita, ja que de tots els parells (a, b) que poden codificar la seqüència, triem el més petit.

Definició 4.10. $\mathrm{lg}(s) = \mathrm{sn}(s)$

$\mathrm{lg}(s)$ és un Σ-Pterme i, obviament, es refereix a la longitud de la seqüència finita.

Definició 4.11. $\mathrm{val}(s, i)$ és el Σ-Pterme

$$\mathrm{val}(s, i) = \mathrm{beta}(\mathrm{pr}(\mathrm{pr}(s)), \mathrm{sn}(\mathrm{pr}(s)), i)$$

Escriurem s_i enlloc de $\mathrm{val}(s, i)$, ja que ens estem referint a l'i-èssim objecte de la seqüència finita.

Definició 4.12. $\mathrm{Concat}(s, s', s'')$ és el Σ-Pterme

$$\mathrm{SeqFin}(s'') \wedge \mathrm{lg}(s'') = \mathrm{lg}(s) + \mathrm{lg}(s') \wedge \forall i < \mathrm{lg}(s)\, s''_i = s_i \wedge \forall i < \mathrm{lg}(s')\, s''_{\mathrm{lg(s)+i}} = s'_i$$

Escriurem $s * s'$ en lloc de $\mathrm{concat}(s, s')$.

Definició 4.13. $\mathrm{Trunc}(s, e, j, s')$ és el Σ-Pterme

$$(\neg e < j + \mathbf{1} < \mathrm{lg}(s) + \mathbf{1} \wedge s' = \mathbf{0}) \vee$$
$$(e < j + \mathbf{1} < \mathrm{lg}(s) + \mathbf{1} \wedge \mathrm{SeqFin}(s') \wedge \mathrm{lg}(s') = j - e \wedge \forall i < j - e\, s'_i = s_{e+i})$$

Escirurem $s_{[e,j)}$ enlloc de $\mathrm{trunc}(s, e, j)$.

Com haviem avançat abans, acabem de veure que, en efecte, la codificació que hem triat és injectiva i que ens permet passar d'objectes lògics i aritmètics a nombres i desfer després el camí.

4.1 Numerals

Ara ens començarem a moure només entre els numerals. Seguint la numeració que hem introduït al principi del capítol, a cadascun dels símbols els assignem el numeral corresponent a cadascun dels nombres assignats als símbols. Per simplificar la lectura, farem servir els símbols $\ulcorner\cdot\urcorner$ per referir-nos al numeral del nombre Gö$(\cdot)$. Així, per exemple el numeral $\ulcorner\forall\urcorner$ serà $\boldsymbol{sssss}\mathbf{0}$ o $\mathbf{5}$.

Aquesta notació també la farem servir per a fórmules, de manera que $\ulcorner\varphi\urcorner$ serà el numeral assignat a la seqüència finita que forma φ.

Definició 4.14. Variable(v): És la Δ-fórmula

$$\exists i < v\, v = \mathbf{2} \times i + \mathbf{17}$$

Definició 4.15. Term(t): És la Σ-fórmula

$$\exists s\,[\mathrm{SeqFin}(s) \wedge \mathrm{lg}(s) > \mathbf{0} \wedge s_{lg(s)-1} = t \wedge$$
$$\forall i < \mathrm{lg}(s)\,(s_i = \ulcorner\mathbf{0}\urcorner \vee \mathrm{Var}(s_i) \vee \exists j,k < i\,[s_i = (\ulcorner\boldsymbol{s}\urcorner, s_j) \vee$$
$$s_i = (\ulcorner\mathbf{+}\urcorner, (s_j, s_k)) \vee s_i = (\ulcorner\mathbf{\times}\urcorner, (s_j, s_k))])]$$

Definició 4.16. FormAt(x): És la Σ-fórmula

$$(\exists t < x\, \exists t' < x\,[\mathrm{Term}(t) \wedge \mathrm{Term}(t') \wedge x = (\ulcorner=\urcorner, (t,t'))] \vee x = \ulcorner\bot\urcorner)$$

Definició 4.17. Formula(x): És la Σ-fórmula

$$\exists s[\mathrm{SeqFin}(s) \wedge \mathrm{lg}(s) > \mathbf{0} \wedge s_{lg(s)-1} = x \wedge$$
$$\forall i < \mathrm{lg}(s)(\mathrm{FormAt}(s_i) \vee \exists j,k < i\ s_i = (\ulcorner\rightarrow\urcorner, (s_j, s_k)) \vee \exists j < i\, \exists v[\mathrm{Var}(v) \wedge s_i = (\ulcorner\forall\urcorner, (v, s_j))])]$$

Per últim, tres definicions a partir de les quals construirem la definició del predicat de demostrabilitat:

Definició 4.18. Gen(x,y) és la Σ-fórmula:

$$\exists s(\mathrm{SeqFin}(s) \wedge \mathrm{lg}(s) > 0 \wedge s_{\mathrm{lg}(s)-1} = y \wedge$$
$$s_0 = x \wedge \forall i < lg(s) - \mathbf{1}[\exists v(\mathrm{Var}(v) \wedge s_{i+1} = (\ulcorner\forall\urcorner, (v, s_i)))])$$

Definició 4.19. Ax(x) és la Σ-fórmula

$$(\mathrm{Ax1LP}(x) \vee ... \vee \mathrm{Ax1Q}(x) \vee ... \vee \mathrm{Ax1I}(x) \vee ... \vee \mathrm{Ax7SSP}(x))$$

On, per exemple, si anomenem Ax1LP al primer axioma de la lògica proposicional, i.e. $\varphi \rightarrow (\psi \rightarrow \varphi)$, llavors $Ax1LP(x)$ és la Σ-fórmula

$$\exists y < x(\mathrm{Gen}(y,x) \wedge \exists u < y\, \exists v < y[\mathrm{Formula}(u) \wedge \mathrm{Formula}(v) \wedge y = (\ulcorner\rightarrow\urcorner, (u, (\ulcorner\rightarrow\urcorner, (v,u))))])$$

Anàlogament als altres axiomes de la llista que hem donat a la secció 3.2.

Definició 4.20. ConseqModPon(x,y,z): És la Δ-fórmula

$$(\mathrm{Formula}(x) \wedge \mathrm{Formula}(z) \wedge y = (\ulcorner\rightarrow\urcorner, (x,z)))$$

4.2 Predicat de demostrabilitat

A la secció anterior hem definit tots els conceptes necessaris per definir la fórmula clau d'aquest treball: *Bew*(x). Aquesta fórmula és un predicat de demostrabilitat:

Definició 4.21. Un *Predicat de Demostrabilitat* és una fórmula arbitrària B de AP (tot i que es pot generalitzar a altres teories) que, donades qualsevol parell de sentències φ i ψ, amb $\ulcorner\varphi\urcorner$ i $\ulcorner\psi\urcorner$ els seus respectius nombres de Gödel, compleix les següents propietats (anomenades condicions de demostrabilitat de Hilbert-Bernays-Löb):

i) Si $AP \vdash \varphi$, llavors $AP \vdash B(\ulcorner\varphi\urcorner)$

ii) $AP \vdash B(\ulcorner(\varphi \to \psi)\urcorner) \to (B(\ulcorner\varphi\urcorner) \to B(\ulcorner\psi\urcorner))$

iii) $AP \vdash B(\ulcorner\varphi\urcorner) \to B(\ulcorner B(\ulcorner\varphi\urcorner)\urcorner)$

Més concretament, farem servir Bew($\ulcorner\varphi\urcorner$), que és una sentència fruit de substituir la variable lliure x pel numeral $\ulcorner\varphi\urcorner$. Així doncs, Bew($\ulcorner\varphi\urcorner$) és una sentència que afirma que φ **és** demostrable.

Definició 4.22. Bew(x) és la Σ-fórmula

$$\exists s(\mathrm{SeqFin}(s) \wedge s_{lg(s)-1} = x \wedge \forall i < \lg(s) - 1\ [\mathrm{Ax}(s_i) \vee$$
$$\exists j < i\, \exists k < i\, \mathrm{ConseqModPon}(s_j, s_k, s_i)])$$

i.e. que existeix una seqüència finita tal que el darrer element de la seqüència, és allò que volem demostrar i els anteriors elements o bé són axiomes o bé són conseqüències d'axiomes o elements anteriors mitjançant modus ponens.

Observació 4.23. Anomenem així aquesta fórmula per conservar la notació original de Gödel, i.e. Bew com abreviació de "Beweisbar", "Demostrable"en alemany.

4.3 Teoremes importants sobre *Bew(x)*

Per demostrar el *Teorema de Löb* en el qual es centra aquest treball, ens cal demostrar que Bew($\ulcorner\varphi\urcorner$) compleix les condicions de *Predicat de Demostrabilitat*, que efectivament es tracta d'una Σ-sentència i, com a prerequisit per a una de les demostracions, que compleix la condició addicional següent: que si φ és una Σ-sentència, llavors AP $\vdash \varphi \to$ Bew($\ulcorner\varphi\urcorner$).

Teorema 4.24. Bew($\ulcorner\varphi\urcorner$) és una Σ-sentència

Demo: Donat que Bew(x) és una Σ-fórmula (fàcilment verificable per construcció), donada qualsevol sentència φ d'AP, Bew($\ulcorner\varphi\urcorner$) és una Σ-sentència. □

Teorema 4.25. Si AP $\vdash \varphi$, llavors AP $\vdash$ Bew($\ulcorner\varphi\urcorner$)

(Condició *i*) de *Predicat de Demostrabilitat*)

Demo: Si φ és una sentència, i AP $\vdash \varphi$, hi ha una deducció que es codifica mitjançant un nombre que compleix la definició 4.22, així que Bew($\ulcorner\varphi\urcorner$) és una Σ-sentència certa i, per 3.38, tenim que AP $\vdash$ Bew($\ulcorner\varphi\urcorner$) □

Teorema 4.26. Siguin φ i ψ sentències d'AP, llavors

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner(\varphi \to \psi)\urcorner) \to (\mathrm{Bew}(\ulcorner\varphi\urcorner) \to \mathrm{Bew}(\ulcorner\psi\urcorner))$$

(Condició *ii*) de *Predicat de Demostrabilitat*)

Demo: Definim $\mathrm{Dem}(y, x)$ com la Δ-fórmula tal que $\exists y\ \mathrm{Dem}(y, x) = \mathrm{Bew(x)}$, i.e. y és la demostració de x. Llavors, n'hi ha prou amb veure que

$$\mathrm{AP} \vdash \mathrm{Dem}(y, \ulcorner(\varphi \to \psi)\urcorner) \wedge \mathrm{Dem}(y', \ulcorner\varphi\urcorner) \to \mathrm{Dem}(y * y' * (\ulcorner\psi\urcorner), \ulcorner\psi\urcorner)$$

Per la propia definició de la regla d'inferència de Conseqüència de Modus Ponens, essent y i y' les demostracions de $\varphi \to \psi$ i φ respectivament, es compleix. □

Per demostrar la propietat *iii*) del *Predicat de Demostrabilitat*, ens hem de fixar que és un corol·lari directe de 4.24 i de la condició addicional que si φ és una Σ-sentència, AP $\vdash \varphi \to \mathrm{Bew}(\ulcorner\varphi\urcorner)$.

Aquesta darrera propietat és clau per justificar que el *Teorema de Löb* respon afirmativament a la pregunta de Henkin. Intuïtivament, és obvia, ja que diu que, si a AP, una propietat es compleix, llavors pot ser demostrada. Tot i aquesta aparent simplicitat, és força llarga i farragosa de demostrar i, a més, requereix una sèrie de definicions i lemes previs per fer-ho. Així doncs, per aquests motius, només farem un esquema de la demostració, fixant-nos només en els casos més representatius.

Cal comentar que, de fet, no demostrarem la propietat que hem enunciat, sinó una propietat més forta, com veurem una mica més endevant.

Comencem, doncs, per definir alguns conceptes previs. Per començar ens cal veure que la funció que assigna a cada nombre n, el nombre de Gödel del seu numeral $\boldsymbol{n}$ és un Σ-Pterme.

Definició 4.27. $\mathrm{Num}(x, y)$ és el Σ-Pterme

$$\exists s(lg(s) = x + \mathbf{1} \wedge s_0 = \ulcorner\mathbf{0}\urcorner \wedge \forall i < x\ s_{i+1} = (\ulcorner\boldsymbol{s}\urcorner, s_i) \wedge s_x = y)$$

També ens caldrà un Σ-Pterme per assignar el seu numeral a les variables:

Definició 4.28. $\mathrm{var}(x) = \mathbf{2} \times x + \mathbf{17}$

Ara venen dos Σ-Ptermes: el primer defineix la substitució de variables per termes en termes que ens servirà per definir el segon, la substitució de variables lliures per termes en fórmules que, al seu torn, ens servirà per definir el que ens caldrà per la demostració de la condició addicional.

Definició 4.29. $\mathrm{Sub}_1(t, v, r, z)$ és el Σ-Pterme

$$\exists s \exists s'(\mathrm{SeqFin}(s) \wedge \mathrm{SeqFin}(s') \wedge \mathrm{lg}(s) = \mathrm{lg}(s') \wedge s_{lg(s)-1} = r \wedge s'_{lg(s')-1} = z \wedge$$

$$\forall i < \mathrm{lg}(s)[(s_i = \ulcorner\mathbf{0}\urcorner \wedge s'_i = \ulcorner\mathbf{0}\urcorner) \vee (\mathrm{Var}(s_i) \wedge v = s_i \wedge s'_i = t) \vee (\mathrm{Var}(s_i) \wedge v \neq s_i \wedge s_i = s'_i)$$
$$\vee(\exists j < i[s_i = (\ulcorner\boldsymbol{s}\urcorner, s_j) \wedge s'_i = (\ulcorner\boldsymbol{s}\urcorner, s'_j)]) \vee (\exists j, k < i[s_i = (\ulcorner+\urcorner, (s_j, s_k)) \wedge s'_i = (\ulcorner+\urcorner, (s'_j, s'_k))])$$
$$\vee(\exists j, k < i[s_i = (\ulcorner\times\urcorner, (s_j, s_k)) \wedge s'_i = (\ulcorner\times\urcorner, (s'_j, s'_k))])])$$

Definició 4.30. $\mathrm{Sub}(t,v,x,z)$ és el Σ-Pterme

$$\exists s\exists s'(\mathrm{SeqFin}(s)\wedge\mathrm{SeqFin}(s')\wedge\mathrm{lg}(s)=\mathrm{lg}(s')\wedge s_{lg(s)-1}=x\wedge s'_{lg(s')-1}=z\wedge$$
$$\forall i<\mathrm{lg}(s)[(s_i=\ulcorner\bot\urcorner\wedge s'_i=s_i)$$
$$\vee(\exists r_1,r_2<x[\mathrm{Term}(r_1)\wedge\mathrm{Term}(r_2)\wedge s_i=(\ulcorner=\urcorner,(r_1,r_2))]\wedge$$
$$\exists r'_1,r'_2<z[\mathrm{Term}(r'_1)\wedge\mathrm{Term}(r'_2)\wedge s'_i=(\ulcorner=\urcorner,(r'_1,r'_2))]\wedge$$
$$\mathrm{sub}_1(t,v,r_1,r'_1)\wedge\mathrm{sub}_1(t,v,r_2,r'_2))$$
$$\vee(\exists j,k<i[s_i=(\ulcorner\to\urcorner,(s_j,s_k))\wedge s'_i=(\ulcorner\to\urcorner,(s'_j,s'_k))])$$
$$\vee(\exists j<i\exists w<x[\mathrm{Var}(w)\wedge w\neq v\wedge s_i=(\ulcorner\forall\urcorner,(w,s_j))\wedge s'_i=(\ulcorner\forall\urcorner,(w,s'_j))])$$
$$\vee(\exists j<i[s_i=(\ulcorner\forall\urcorner,(v,s_j))\wedge s'_i=(\ulcorner\forall\urcorner,(v,s_j))])])$$

Definim ara la substitució de l'i-éssima variable per un numeral $\boldsymbol{n}$ a una fórmula φ amb un cert nombre de Gödel z.

Definició 4.31. $\mathrm{su}(x,y,z)=\mathrm{sub}(\mathrm{num}(x),\ \mathrm{var}(y),\ z)$.

Així doncs, per exemple, a la fórmula $\varphi=(v_1=v_3)$ amb nombre de Gödel k, tindríem que $\mathrm{AP}\vdash\mathrm{su}(\mathbf{5},\mathbf{3},k)=\ulcorner v_1=\mathbf{5}\urcorner$.

Ara encara ens queda definir una nova notació que difereix subtilment de la que hem utilitzat fins ara: $\mathrm{Bew}[\varphi]$.

Definició 4.32. Suposem que φ té exactament $v_{k_1},...,v_{k_m}$ (amb $k_1<k_2<...<k_n$) com a variables lliures. Definim $\mathrm{Bew}[\varphi]$ com la fórmula:

$$\mathrm{Bew}(\mathrm{su}(v_{k_m},\boldsymbol{k}_m,...\mathrm{su}(v_{k_2},\boldsymbol{k}_2,(\mathrm{su}(v_{k_1},\boldsymbol{k}_1,\ulcorner\varphi\urcorner)))...))$$

.

És a dir, és la Σ-fórmula $\mathrm{Bew}(x)$ (4.22) amb x essent la fórmula que substitueix les variables lliures de φ pels numerals dels seus respectius índex, i.e. $\mathrm{Bew}(\varphi\binom{v_{k_1}}{\boldsymbol{k}_1}...\binom{v_{k_m}}{\boldsymbol{k}_m})$

Notem que aquesta fórmula és certa de $i_1,...,i_k$ si i només si $\varphi\binom{v_{k_1}}{\boldsymbol{i}_1}...\binom{v_{k_m}}{\boldsymbol{i}_m}$ és un teorema a AP i que és una fórmula que conté les mateixes variables lliures que φ. Si φ no té variables lliures, llavors $\mathrm{Bew}[\varphi]=\mathrm{Bew}\ (\ulcorner\varphi\urcorner)$.

Ara demostrarem dos lemes previs que ens caldran per demostrar la propietat:

Lema 4.33. Siguin φ i ψ dues fórmules d'AP:

$$\mathrm{AP}\vdash\mathrm{Bew}[\varphi\to\psi]\to(\mathrm{Bew}[\varphi]\to\mathrm{Bew}[\psi])$$

Demo: Per simplificar, suposarem que les variables lliures de φ són v_2 i v_3 i les de ψ són v_1 i v_3.

Llavors, $\mathrm{Bew}[\varphi]=\mathrm{Bew}(\mathrm{su}(v_3,\mathbf{3},(\mathrm{su}(v_2,\mathbf{2},\ulcorner\varphi\urcorner))))$,
$\mathrm{Bew}[\psi]=\mathrm{Bew}(\mathrm{su}(v_3,\mathbf{3},(\mathrm{su}(v_1,\mathbf{1},\ulcorner\psi\urcorner))))$, i
$\mathrm{Bew}[\varphi\to\psi]=\mathrm{Bew}(\mathrm{su}(v_3,\mathbf{3},\mathrm{su}(v_2,\mathbf{2},\mathrm{su}(v_1,\mathbf{1},\ulcorner\varphi\to\psi\urcorner))))$ i notem ara que:

$$\mathrm{AP}\vdash\mathrm{su}(v_3,\mathbf{3},\mathrm{su}(v_2,\mathbf{2},\mathrm{su}(v_1,\mathbf{1},\ulcorner\varphi\to\psi\urcorner)))=(\ulcorner\to\urcorner,\mathrm{su}(v_3,\mathbf{3},\mathrm{su}(v_2,\mathbf{2},\ulcorner\varphi\urcorner)),\mathrm{su}(v_3,\mathbf{3},\mathrm{su}(v_1,\mathbf{1},\ulcorner\psi\urcorner)))$$

i.e. que la substitució de numerals en la formació d'una fórmula condicional commuta. Ara, agafant la definició que hem donat a la demostració de 4.26 i seguint-la, tenim que

$$\mathrm{AP} \vdash \mathrm{Dem}(y, \mathrm{su}(v_3, \mathbf{3}, \mathrm{su}(v_2, \mathbf{2}, \mathrm{su}(v_1, \mathbf{1}, \ulcorner \varphi \to \psi \urcorner)))) \wedge \mathrm{Dem}(y', \mathrm{su}(v_3, \mathbf{3}, \mathrm{su}(v_2, \mathbf{2}, \ulcorner \varphi \urcorner))) \to$$

$$\mathrm{Dem}(y * y' * [\mathrm{su}(v_3, \mathbf{3}, \mathrm{su}(v_1, \mathbf{1}, \ulcorner \psi \urcorner))]), \mathrm{su}(v_3, \mathbf{3}, \mathrm{su}(v_1, \mathbf{1}, \ulcorner \psi \urcorner))$$

□

Lema 4.34. Sigui φ una fórmula d'AP. Si $\mathrm{AP} \vdash \varphi$, llavors $\mathrm{AP} \vdash \mathrm{Bew}[\varphi]$

Demo: Suposem, com a la demostració anterior, que φ té les mateixes variables lliures, i.e. v_2 i v_3.

Sigui $\psi = \forall v_2 \forall v_3 \varphi$. Ara, ψ és una sentència i, per 4.25, tenim que $\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner)$. Sigui també $\chi = \forall v_3 \varphi$. Volem veure que $\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \to \mathrm{Bew}[\chi]$ i tenim que:

$$\mathrm{AP} \vdash \exists y\, \mathrm{Dem}(y, (\ulcorner \to \urcorner, (\ulcorner \psi \urcorner, \mathrm{su}(v_2, \mathbf{2}, \ulcorner \chi \urcorner))))$$

$$\mathrm{AP} \vdash \mathrm{Dem}(y, (\ulcorner \to \urcorner, (\ulcorner \psi \urcorner, \mathrm{su}(v_2, \mathbf{2}, \ulcorner \chi \urcorner)))) \wedge \mathrm{Dem}(y', \ulcorner \psi \urcorner)$$

$$\to \mathrm{Dem}(y' * y * [\mathrm{su}(v_2, \mathbf{2}, \ulcorner \chi \urcorner)], \mathrm{su}(v_2, \mathbf{2}, \ulcorner \chi \urcorner))$$

i, per com hem definit $\mathrm{Dem}(x, y)$, trobem que

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \to \mathrm{Bew}(\mathrm{su}(v_2, \mathbf{2}, \ulcorner \chi \urcorner))$$

i.e.

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \to \mathrm{Bew}[\chi]$$

De la matexia manera, podem veure que

$$\mathrm{AP} \vdash \mathrm{Bew}[\chi] \to \mathrm{Bew}[\varphi]$$

i, per tant, tenim:

$$\mathrm{AP} \vdash \mathrm{Bew}[\varphi]$$

□

Així doncs, com ja hem avançat abans, demostrarem una versió més potent de la propietat: la demostrarem per a fórmules de la forma $\mathrm{Bew}[\varphi]$ en lloc de per a sentències, que són casos particulars. Per altra banda, com que $\mathrm{Bew}(\ulcorner \varphi \urcorner)$ és una sentència (per 4.24), trobem que la darrera propietat de *predicat de demostrabilitat* (que és el que realment ens interessa), també és un cas particular d'aquesta proposició.

Teorema 4.35. Si φ és una Σ-fórmula, $\mathrm{AP} \vdash \varphi \to \mathrm{Bew}[\varphi]$

Demo: Comencem observant que podem suposar que φ és una Σ-fórmula estricta, ja que si φ és Σ, existeix ψ Σ-fórmula estricta equivalent a φ, i.e. $\mathrm{AP} \vdash \varphi \to \psi$ i $\mathrm{AP} \vdash \psi \to \varphi$ i, llavors, per 4.34 tenim $\mathrm{AP} \vdash \mathrm{Bew}[\psi \to \varphi]$. Ara, per 4.33 trobem que $\mathrm{AP} \vdash \mathrm{Bew}[\psi] \to \mathrm{Bew}[\varphi]$ i, llavors, si $\mathrm{AP} \vdash \psi \to \mathrm{Bew}[\psi]$, concloem que $\mathrm{AP} \vdash \varphi \to \mathrm{Bew}[\varphi]$. Així doncs, repassarem els casos en els que φ és una Σ-fórmula estricta.

Cas $\varphi \equiv (u + v = w)$: Aquest cas és una reelaboració de la demostració de 3.21. Suposem que φ és la fórmula $v_5 \mathbf{+} v_2 = v_3$ i volem demostrar que $\mathrm{AP} \vdash \forall v_5 \forall v_2 \forall v_3 (v_5 \mathbf{+} v_2 =$

$v_3 \to \mathrm{Bew}[v_5 + v_2 = v_3]$). Ho explicarem de paraula, però l'argument que donarem pot ser formalitzable a AP. Sigui i_5 arbitrari (v_5 juga el rol de i_5, a la formalització) i farem inducció sobre i_2. Suposem que, per a un arbitrari i_3, tenim que $i_5 + 0 = i_3$. Ara per l'axioma *iii*) SSP, tenim que $i_5 = i_3$ i, per tant, $\boldsymbol{i}_5 = \boldsymbol{i}_3$. Com $v_0 \boldsymbol{+ 0} = v_0$ és un axioma, la seva generalització $\forall v_0 v_0 \boldsymbol{+ 0} = v_0$ també i, per tant, $\forall v_0 v_0 \boldsymbol{+ 0} = v_0 \to \boldsymbol{i}_5 \boldsymbol{+ 0} = \boldsymbol{i}_5$ és demostrable, així que $\boldsymbol{i}_5 \boldsymbol{+ 0} = \boldsymbol{i}_3$ és demostrable.

Suposem ara un i_2 arbitrari i suposem que, per a tot i_3, $\boldsymbol{i}_5 \boldsymbol{+ i}_2 = \boldsymbol{i}_3$ és demostrable si $i_5 + i_2 = i_3$. Sigui $i_4 = i_2 + 1$. Demostrarem que, per a tot i_3, $\boldsymbol{i}_5 \boldsymbol{+ i}_4 = \boldsymbol{i}_3$ és demostrable si $i_5 + i_4 = i_3$. Assumim doncs aquesta darrera premisa amb un i_3 arbitrari. Llavors, $i_5 + (i_2 + 1) = (i_5 + i_2) + 1 = i_3$. Com el 0 no és successor de cap nombre, $i_3 \neq 0$, així que existeix algun nombre i_1 tal que $i_1 + 1 = i_3$. Tenim, doncs, que $(i_5 + i_2) + 1 = i_1 + 1$ i, per tant, $i_5 + i_2 = i_1$. Per la hipòtesi d'inducció, $\boldsymbol{i}_5 \boldsymbol{+ i}_2 = \boldsymbol{i}_1$ és demostrable i, amb l'axioma *iv*) SSP que escribim $\forall v_0 \forall v_1 v_0 \boldsymbol{+ s} v_1 = \boldsymbol{s}(v_0 + v_1)$, tenim que $\boldsymbol{i}_5 \boldsymbol{+ si}_2 = \boldsymbol{si}_1$, però com $\boldsymbol{si}_2$ és $\boldsymbol{i}_4$ i $\boldsymbol{si}_1$ és $\boldsymbol{i_3}$, trobem que $\boldsymbol{i}_5 \boldsymbol{+ i}_4 = \boldsymbol{i}_3$ és demostrable. Així, hem vist que $\boldsymbol{i}_5 \boldsymbol{+ i}_2 = \boldsymbol{i}_1$ és demostrable si $i_5 + i_2 = i_1$ i, per tant, si $i_4 = i_2 + 1$ i $i_3 = i_1 + 1$, és demostrable que $\boldsymbol{i}_5 \boldsymbol{+ i}_4 = \boldsymbol{i}_3$.

Ara, per inducció, per a tot i_3, $\boldsymbol{i}_5 \boldsymbol{+ i}_2 = \boldsymbol{i}_3$ és demostrable si $i_5 + i_2 = i_3$. Així, si $i_5 + i_2 = i_3$, el resultat $\boldsymbol{i}_5 \boldsymbol{+ i}_2 = \boldsymbol{i}_3$ de substituir respectivament $\boldsymbol{i}_2, \boldsymbol{i}_3, \boldsymbol{i}_5$ per la $2^a, 3^a,$ i 5^a variable a la fórmula $v_5 + v_2 = v_3$ és demostrable.

Els casos per a altres eleccions de variables es fan anàlogament.

Els casos $\varphi \equiv (u = v), \boldsymbol{0} = v, \boldsymbol{s}u = v$ i $u \boldsymbol{\times} v = w$, també es fan de manera similar.

Per a probar el teorema, doncs, ens queda demostrar que $\mathrm{AP} \vdash \varphi \to \mathrm{Bew}[\varphi]$ si φ prové de conjunció, disjunció, quantificació existencial o quantificació universal acotada de fórmules ψ tals que $\mathrm{AP} \vdash \psi \to \mathrm{Bew}[\psi]$

- Cas $\varphi \equiv (\psi \wedge \chi)$: Tenim
$$\mathrm{AP} \vdash \psi \to \mathrm{Bew}[\psi]$$
$$\mathrm{AP} \vdash \chi \to \mathrm{Bew}[\chi]$$
Llavors
$$\mathrm{AP} \vdash \varphi \to (\mathrm{Bew}[\psi] \wedge \mathrm{Bew}[\chi])$$
També tenim (per *modus ponens*) que
$$\mathrm{AP} \vdash \psi \to (\chi \to \varphi)$$
Per 4.34 tenim
$$\mathrm{AP} \vdash \mathrm{Bew}[\psi \to (\chi \to \varphi)]$$
i per 4.33, que
$$\mathrm{AP} \vdash \mathrm{Bew}[\psi \to (\chi \to \varphi)] \to (\mathrm{Bew}[\psi] \to \mathrm{Bew}[\chi \to \varphi])$$
i que
$$\mathrm{AP} \vdash \mathrm{Bew}[\chi \to \varphi] \to (\mathrm{Bew}[\chi] \to \mathrm{Bew}[\varphi])$$
i ara, per *modus ponens* altre cop
$$\mathrm{AP} \vdash \varphi \to \mathrm{Bew}[\varphi]$$
- Cas $\varphi \equiv (\psi \vee \chi)$: Es fa de manera molt similar a la conjunció.

- Cas $\varphi \equiv (\exists x \psi)$: Tenim

$$\mathrm{AP} \vdash \psi \to \mathrm{Bew}[\psi]$$

i també

$$\mathrm{AP} \vdash \psi \to \varphi$$

Ara, per 4.33 i 4.34, tenim

$$\mathrm{AP} \vdash \mathrm{Bew}[\psi] \to \mathrm{Bew}[\varphi]$$

i, per tant,

$$\mathrm{AP} \vdash \psi \to \mathrm{Bew}[\varphi]$$

Com que la variable x no és lliure a φ, tampoc és lliure a $\mathrm{Bew}[\varphi]$, que té les mateixes variables lliures. Així que, com que $\varphi \equiv \exists x \psi$, ψ implica $\forall x \psi$, i $\forall x \psi$ implica $\exists x \psi$,

$$\mathrm{AP} \vdash \varphi \to \mathrm{Bew}[\varphi]$$

- Cas $\varphi \equiv ((\forall x < y)\psi)$: Sigui χ una fórmula arbitraria, volem probar que $\mathrm{Bew}[\chi\binom{y}{\boldsymbol{s}y}]$ és equivalent a $\mathrm{Bew}[\chi]\binom{y}{\boldsymbol{s}y}$. Suposem que y és v_k, la k-èssima variable. Llavors, com

$$\mathrm{AP} \vdash \mathrm{su}(y, \boldsymbol{k}, \ulcorner \chi \binom{y}{\boldsymbol{s}y} \urcorner) = su(\boldsymbol{s}y, \boldsymbol{k}, \ulcorner \chi \urcorner)$$

fixant-nos en que $\mathrm{Bew}[\chi\binom{y}{\boldsymbol{s}y}]$ és $\mathrm{Bew}(\mathrm{su}(y, \boldsymbol{k}, \ulcorner \chi\binom{y}{\boldsymbol{s}y} \urcorner))$ i que $\mathrm{Bew}[\chi]\binom{y}{\boldsymbol{s}y}$ és $\mathrm{Bew}(\mathrm{su}(\boldsymbol{s}y, \boldsymbol{k}, \ulcorner \chi \urcorner))$, tenim que

$$\mathrm{AP} \vdash \mathrm{Bew}[\chi \binom{y}{\boldsymbol{s}y}] \leftrightarrow \mathrm{Bew}[\chi] \binom{y}{\boldsymbol{s}y} \tag{4.1}$$

De la mateixa manera, com que y no és lliure en $\chi\binom{y}{\mathbf{0}}$, tenim

$$\mathrm{AP} \vdash \mathrm{su}(y, \boldsymbol{k}, \ulcorner \chi \binom{y}{\mathbf{0}} \urcorner) = \ulcorner \chi \binom{y}{\mathbf{0}} \urcorner = \mathrm{su}(\mathbf{0}, \boldsymbol{k}, \ulcorner \chi \urcorner)$$

i

$$\mathrm{AP} \vdash \mathrm{Bew}[\chi \binom{y}{\mathbf{0}}] \leftrightarrow \mathrm{Bew}[\chi] \binom{y}{\mathbf{0}}$$

Ara, suposem que existeix ψ tal que $\mathrm{AP} \vdash \psi \to \mathrm{Bew}[\psi]$ i φ és $(\forall x < y)\psi$. Llavors, $\varphi\binom{y}{\mathbf{0}}$ és $\forall x(x < \mathbf{0} \to \psi\binom{y}{\mathbf{0}})$, però com

$$\mathrm{AP} \vdash \neg x < \mathbf{0}$$

tenim

$$\mathrm{AP} \vdash \varphi \binom{y}{\mathbf{0}}$$

i, per 4.34, tenim

$$\mathrm{AP} \vdash \mathrm{Bew}[\varphi \binom{y}{\mathbf{0}}]$$

i, per la discussió anterior,

$$\mathrm{AP} \vdash \mathrm{Bew}[\varphi] \binom{y}{\mathbf{0}}$$

$$\mathrm{AP} \vdash \varphi \binom{y}{\mathbf{0}} \to \mathrm{Bew}[\varphi] \binom{y}{\mathbf{0}}$$

i.e.

$$\mathrm{AP} \vdash (\varphi \to \mathrm{Bew}[\varphi])\binom{y}{\mathbf{0}}$$

Llavors, com que

$$\mathrm{AP} \vdash x < \boldsymbol{s}y \leftrightarrow x < y \vee x = y$$

$$\mathrm{AP} \vdash \varphi\binom{y}{\boldsymbol{s}y} \leftrightarrow (\varphi \wedge \psi)$$

i ara, per 4.33 i 4.34,

$$\mathrm{AP} \vdash \mathrm{Bew}[\varphi] \wedge \mathrm{Bew}[\psi] \to \mathrm{Bew}[\varphi\binom{y}{\boldsymbol{s}y}]$$

però com

$$\mathrm{AP} \vdash \psi \to \mathrm{Bew}[\psi]$$

$$\mathrm{AP} \vdash (\varphi \to \mathrm{Bew}[\varphi]) \to (\varphi\binom{y}{\boldsymbol{s}y} \to \mathrm{Bew}[\varphi] \wedge \mathrm{Bew}[\psi])$$

i, per (4.1),

$$\mathrm{AP} \vdash (\varphi \to \mathrm{Bew}[\varphi]) \to (\varphi\binom{y}{\boldsymbol{s}y} \to \mathrm{Bew}[\varphi]\binom{y}{\boldsymbol{s}y})$$

$$\mathrm{AP} \vdash (\varphi \to \mathrm{Bew}[\varphi]) \to (\varphi \to \mathrm{Bew}[\varphi])\binom{y}{\boldsymbol{s}y}$$

i, per tant,

$$\mathrm{AP} \vdash \forall y(\varphi \to \mathrm{Bew}[\varphi]) \to (\varphi \to \mathrm{Bew}[\varphi])\binom{y}{\boldsymbol{s}y}$$

i, finalment, per l'axioma d'inducció

$$\mathrm{AP} \vdash \varphi \to \mathrm{Bew}[\varphi]$$

□

Un cop demostrada aquesta condició adicional, ja només ens queda veure, com hem avançat abans, la tercera condició de *predicat de demostrabilitat*, que a aquestes alçades és un simple corol·lari.

Teorema 4.36. $\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner\varphi\urcorner) \to \mathrm{Bew}(\ulcorner\mathrm{Bew}(\ulcorner\varphi\urcorner)\urcorner)$

(Condició *iii*) de *Predicat de Demostrabilitat*)

Demo: Com hem dit abans, prové directament de 4.24 i de 4.35. □

4.4 Lema Diagonal

Un concepte clau a les demostracions de Gödel dels seus *Teoremes d'incompletesa* és l'autoreferència. Aquest concepte permet que una certa fórmula lògica afirmi coses sobre sí mateixa. En ser el *Teorema de Löb*, un teorema fortament emparentat amb el *Primer teorema d'incompletesa* de Gödel, aquest lema ens és imprescindible.

Lema 4.37. Diagonal Generalitzat:

Suposem que $u_0, ...u_n$ i $v_0, ..., v_m$ (que abreujarem com a ν) són variables diferents i que $\psi_0(u_0, ...u_n, \nu), ..., \psi_n(u_0, ..., u_n, \nu)$ són fórmules amb totes les variables lliures entre $u_0, ..., u_n, \nu$. Llavors, existeixen fórmules $\varphi_0(\nu), ..., \varphi_n(\nu)$ amb totes les variables lliures entre ν, tals que:

$$\begin{aligned} &\mathrm{AP} \vdash \varphi_0(\nu) \leftrightarrow \psi_0(\ulcorner\varphi_0(\nu)\urcorner, ..., \ulcorner\varphi_n(\nu)\urcorner, \nu) \\ &\vdots \\ &\mathrm{AP} \vdash \varphi_n(\nu) \leftrightarrow \psi_n(\ulcorner\varphi_0(\nu)\urcorner, ..., \ulcorner\varphi_n(\nu)\urcorner, \nu) \end{aligned}$$

Demo: Sigui $\mathrm{Su}(x, y_0, ..., y_n, z)$ el Σ-Pterme per a la funció n-ària de substitució, que en els valors $a, b_0, ..., b_n$ substitueix les variables $y_0, ..., y_n$ pels numerals $\boldsymbol{b}_0, ..., \boldsymbol{b}_n$, a la fórmula amb nombre de Gödel a (fem servir aquesta notació per ser una mena de generalització de 4.31).

Llavors, per cada $i < n + 1$, sigui g_i el nombre de Gödel de

$$\psi_i(\mathrm{su}(y_0, y_0, ..., y_n), ..., \mathrm{su}(y_n, y_0, ..., y_n), \nu)$$

i sigui $\varphi_i(\nu)$, la fórmula

$$\psi_i(\mathrm{su}(\boldsymbol{g}_0, \boldsymbol{g}_0, ..., \boldsymbol{g}_n), ..., \mathrm{su}(\boldsymbol{g}_n, \boldsymbol{g}_0, ..., \boldsymbol{g}_n), \nu)$$

Així doncs, tan sols ens cal demostrar que

$$\mathrm{AP} \vdash \mathrm{su}(\boldsymbol{g}_i, \boldsymbol{g}_0, ..., \boldsymbol{g}_n) = \ulcorner\varphi_i(\nu)\urcorner$$

Però el resultat de substituir les variables $y_0, ..., y_n$ pels numerals $\boldsymbol{g}_0, ..., \boldsymbol{g}_n$ a la fórmula amb nombre de Gödel g_i, i.e. a la formula

$$\psi_i(\mathrm{su}(y_0, y_0, ..., y_n), ..., \mathrm{su}(y_n, y_0, ..., y_n), \nu)$$

és la fórmula $\varphi_i(\nu)$ i, per tant, $\mathrm{su}(g_i, g_0, ..., g_n) = \mathrm{Gö}(\varphi_i(\nu))$. Així que la Σ sentència $\mathrm{su}(\boldsymbol{g}_i, \boldsymbol{g}_0, ..., \boldsymbol{g}_n) = \ulcorner\varphi_i(\nu)\urcorner$ és certa i, per 3.38,

$$\mathrm{AP} \vdash \mathrm{su}(\boldsymbol{g}_i, \boldsymbol{g}_0, ..., \boldsymbol{g}_n) = \ulcorner\varphi_i(\nu)\urcorner$$

□

Corol·lari 4.38. Lema Diagonal (o del Punt Fix)

Suposem que $\psi(x)$ és una fórmula d'AP que no conté cap variable lliure diferent de x. Llavors existeix una sentència φ d'AP tal que

$$\mathrm{AP} \vdash \varphi \leftrightarrow \psi(\ulcorner\varphi\urcorner)$$

Demo: És el cas del *Lema Diagonal Generalitzat* amb $n = 0$, i $m = 0$. □

5 Teorema de Löb

Arribats a aquest punt, ja disposem de totes les eines necessàries per enunciar i demostrar el Teorema central d'aquest treball: El *Teorema de Löb*.

Al número 17 del *The Journal of Symbolic Logic* de 1952, *Leon Henkin* plantejava en el número 3 de la llista de problemes irresolts, "*Un problema referent a la demostrabilitat*". Recordem-lo: si Σ és qualsevol sistema formal estàndard adequat per a la Teoria recursiva de nombres, una fórmula (que té un cert nombre enter q com a *nombre de Gödel*) pot ser construïda de manera que expressi la proposició que la fórmula amb nombre de Gödel q és demostrable a Σ. Aquesta fórmula és demostrable o independent (i.e. no decidible) a Σ?

Al número 20 de 1955 de la mateixa revista, *M. H. Löb* publicava un article on donava una resolució al problema de *Henkin*. Després d'unes poques consideracions i discussions sobre el tema, enuncia les condicions que ha de satisfer Bew(x) perquè es compleixi el seu teorema. Les condicions que dóna, són les mateixes condicions que hem donat a 4.21 en un altre ordre més una condició supèrflua (la que va enumerar com a segona i que es desprèn directament de les nostres condicions i) i ii), que són respectivametnt iv) i i) en el seu ordre original) i una condició més restrictiva que la que hem donat a 4.35 com a iii) condició. De manera anecdòtica enunciem les que no coincideixen amb les nostres:

- Si $\mathrm{AP} \vdash \varphi \to \psi$, llavors $\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner\varphi\urcorner) \to \mathrm{Bew}(\ulcorner\psi\urcorner)$.
- Si $f(x)$ és un terme recursiu, llavors $\mathrm{AP} \vdash f(x) = 0 \to \mathrm{Bew}(\ulcorner f(x) = 0\urcorner)$. (Hem demostrat un resultat més general a 4.35)

Evidentment, després passa l'enunciat i demostració del seu teorema.

Observació 5.1. No enunciarem i demostrarem el *Teorema de Löb* en la seva forma original, ja que per començar utilitza una notació arcaica (aquí ens hem referit a les fórmules i sentències com φ o ψ, Löb, al seu article, s'hi referia com $\mathfrak{S}$, $\mathfrak{T}$ o $\mathfrak{K}$, a més, es referia a Bew com $\tilde{\mathfrak{B}}(\{\mathfrak{S}\})$). A més deixa diferents detalls a l'aire i, utilitza algunes funcions i propietats que no hem definit en aquest treball.

Així doncs, l'enunciat original era:

Si $\mathfrak{S}$ *és qualsevol fórmula tal que* $\tilde{\mathfrak{B}}(\{\mathfrak{S}\}) \to \mathfrak{S}$ *és un teorema, llavors* $\mathfrak{S}$ *és un teorema.*

Però, com hem dit abans, l'enunciarem i demostrarem en una notació més moderna i adequada al to del treball.

Teorema 5.2. de Löb

Si $\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner\varphi\urcorner) \to \varphi$, llavors $\mathrm{AP} \vdash \varphi$.

Demo: Sigui $\chi(x)$ la fórmula $(\mathrm{Bew}(x) \to \varphi)$. Per 4.38 existeix una sentència ψ tal que

$$\mathrm{AP} \vdash \psi \leftrightarrow \chi(\ulcorner\psi\urcorner) \qquad \text{i.e.}$$

$$\mathrm{AP} \vdash \psi \leftrightarrow (\mathrm{Bew}(\ulcorner\psi\urcorner) \to \varphi) \tag{5.1}$$

així que:

$$\mathrm{AP} \vdash \psi \to (\mathrm{Bew}(\ulcorner\psi\urcorner) \to \varphi) \qquad \text{per 5.1} \tag{5.2}$$

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \to (\mathrm{Bew}(\ulcorner \psi \urcorner) \to \varphi) \urcorner) \qquad \text{per 4.25} \tag{5.3}$$

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \to (\mathrm{Bew}(\ulcorner \psi \urcorner) \to \varphi \urcorner)) \to (\mathrm{Bew}(\ulcorner \psi \urcorner) \to \mathrm{Bew}(\ulcorner (\mathrm{Bew}(\ulcorner \psi \urcorner) \to \varphi) \urcorner)) \tag{5.4}$$

per 4.26 i tenim que:

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \to \mathrm{Bew}(\ulcorner (\mathrm{Bew}(\ulcorner \psi \urcorner) \to \varphi) \urcorner) \tag{5.5}$$

de 5.3 i 5.4. D'altra banda, per 4.26, tenim que:

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner \psi \urcorner) \to \varphi \urcorner) \to (\mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner \psi \urcorner) \urcorner) \to \mathrm{Bew}(\ulcorner \varphi \urcorner)) \tag{5.6}$$

amb la qual cosa, de 5.5 i 5.6, tenim que:

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \to (\mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner \psi \urcorner) \urcorner) \to \mathrm{Bew}(\ulcorner \varphi \urcorner)) \tag{5.7}$$

També tenim, per 4.36,

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \to \mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner \psi \urcorner) \urcorner) \tag{5.8}$$

i, de 5.7 i 5.8, treiem:

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \to \mathrm{Bew}(\ulcorner \varphi \urcorner) \tag{5.9}$$

Ara, utilitzant la hipòtesi $\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \varphi \urcorner) \to \varphi$ i 5.9, tenim que:

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \to \varphi \tag{5.10}$$

De 5.1 i 5.10 deduïm que:

$$\mathrm{AP} \vdash \psi \tag{5.11}$$

Ara, de 5.11 i 4.25, tenim

$$\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \psi \urcorner) \tag{5.12}$$

i, finalment, de 5.12 i 5.10, deduïm:

$$\mathrm{AP} \vdash \varphi$$

□

Aquest teorema, en efecte, respon afirmativament a la pregunta de *L. Henkin*, ja que la pregunta plantejada equival a preguntar si és demostrable una fórmula φ tal que $\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \varphi \urcorner) \leftrightarrow \varphi$. Obviament, com que la hipòtesi del *Teorema de Löb* és la implicació esquerra-dreta de la condició de la fórmula amb les condicions proposades, també queda resposta.

6 Corol·laris, comentaris i conclusions

6.1 Corol·laris i comentaris

Com acabem de comentar, aquest teorema requereix de menys condicions que les plantejades per Henkin, però es dedueix la resposta $\mathrm{AP} \vdash \varphi \leftrightarrow \mathrm{Bew}(\ulcorner \varphi \urcorner)$, ja que, si acceptem la hipòtesi de partida $\mathrm{AP} \vdash \mathrm{Bew}(\ulcorner \varphi \urcorner) \to \varphi$, tenim que $\mathrm{AP} \vdash \varphi$; i, com que també tenim (com diu 4.35) que $\mathrm{AP} \vdash \varphi \to \mathrm{Bew}(\ulcorner \varphi \urcorner)$, concloem la doble implicació.

Al llegir i corretgir el teorema i la demostració enviades per Löb, Henkin va idear una nova paradoxa del llenguatge natural, naixent de l'autoreferencia i la noció de veritat. Així doncs, de la frase (que anomenarem A):

" Si aquesta frase és veritat, llavors B és veritat"

es pot deduir qualsevol afirmació B.

Resulta que si A és veritat, també ho és B, així que A és veritat. Parem a mirar-nos-ho amb més deteniment. La frase A és un condicional, així que serà certa si l'antecedent és fals o, si l'antecedent és cert i el conseqüent també, però en aquest darrer cas, que l'antecedent sigui cert inclou que el conseqüent també ho és. Tenim, doncs, que la frase A, és veritat i, en conseqüència, també és veritat B, sigui el que sigui.

Aquesta paradoxa, que neix de la falta de claredat del concepte de veritat en el llenguatge natural i de la manca de formalitat del mateix, resulta que és una versió sense negació de la *Paradoxa de Rusell* i Henkin afirmava que se'n podrien derivar testos d'inconsistència en sistemes formals que no continguessin la negació.

També val la pena comentar un corol·lari molt maco: Resulta que el *Segon Teorema d'Incompletesa* de *Gödel* es dedueix directament del *Teorema de Löb*.

Corol·lari 6.1. Segon Teorema d'Incompletesa de Gödel

Si AP és consistent, llavors AP $\nvdash \neg\text{Bew}(\ulcorner\bot\urcorner)$

Demo: Si AP $\vdash \neg\text{Bew}(\ulcorner\bot\urcorner)$, llavors, per definició de "$\neg$", tenim que
AP $\vdash \text{Bew}(\ulcorner\bot\urcorner) \to \bot$ i, pel *Teorema de Löb*, tindriem que AP $\vdash \bot$ i, per tant, AP seria inconsistent. □

6.2 Conclusions

Conclou aquí un petit viatge per la teoria de la demostrabilitat. Des que es va publicar el Teorema de Löb i l'actualitat, s'ha recorregut un llarg camí que ha portat la demostrabiliat i l'autoreferència a fusionar-se amb, i fer avançar a, la lògica modal. Precisament la necessitat en la lògica modal ($\Box\varphi$) s'assimila al concepte que hem desenvolupat de demostrabilitat i alguns dels conceptes que hem hagut de demostrar al present treball han agafat rang d'axioma a la lògica modal (p. exm. $\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$ es pot entendre com una reformulació de la segona condició de Predicat de Demostrabilitat 4.21).

Tot i que, des d'aquesta fusió, el teorema de Löb s'ha formalitzat en lògica modal i s'ha generalitzat, nosaltres ens hem centrat en la demostració amb les eines que existien quan es va demostrar.

Així doncs, pel camí hem après sobre la fonamentació de l'aritmètica de Peano, sobre la codificació de Gödel, sobre les condicions de demostrabilitat i sobre l'autorreferencia amb el lema diagonal per, finalment, arribar a la demostració que ens havíem proposat. Per fer aquest viatge hem utilitzat eines vistes a les assignatures de Lògica Matemàtica i Modelització Matemàtica de Formes de Raonament (optatives de quart del Grau de Matemàtiques), així com sobretot de l'assignatura Mathematical Logic (del Màster de Lògica Pura i Aplicada), però també hem hagut de fer una recerca bibliogràfica interessant entre alguns lògics importants de finals del segle XX.

Referències

[1] Boolos, G. : *The Logic of Provability*, Cambridge University Press, 1993.

[2] Casanovas, E. : *Mathematical Logic* (Apuntes de curso de Màster), Universitat de Barcelona, 2018.

[3] Löb, M. H. : Solution of a Problem of Leon Henkin. *The Journal of Symbolic Logic*, Vol. 20, No. 2, pàg 115-118, Association for Symbolic Logic, 1955.

[4] Henkin, L. : A problem concerning provability, problem 3, *The Journal of Symbolic Logic*, Vol. 17, pàg 160, Association for Symbolic Logic, 1952.

[5] Smoryński, C. : The Development of Self-Reference: Löb's Theorem. A Drucker, T. (Ed.), *Perspectives on the History of Mathematical Logic*, pag 110-133, Birkhäuser Boston, 1991.

[6] Curch, A. : *Introduction to mathematical logic*, Princeton University Press, 1956.

[7] Enderton, H. B. : *A mathematical introduction to logic* Academic Press, 1972.

[8] Shoenfield, J. R. : *Mathematical Logic*, Addison-Wesley Publishing Company, 1967.

[9] Gödel, K : *Obras completas*, Alianza Editorial, 2018.

[10] Piñeiro, G. E. : *La intuición tiene su lógica. Gödel, Los teoremas de incompletitud*, RBA Contenidos Editoriales y Audiovisuales, 2012.

[11] Sánchez, J. M. : *Gödel, Hilbert y el teorema de incompletitud*, URL: https://www.investigacionyciencia.es/revistas/investigacion-y-ciencia/apolo-11-770/gdel-hilbert-y-el-teorema-de-incompletitud-17636 (visitat el 04-01-2020).