Una fusió dels programes recursivista i formalista finitari: la noció de formalisme recursiu com a substitutiva del càlcul de predicats*

Francesc Tomàs

1 La noció de sistema formal

És freqüent la presentació de les teories matemàtiques com (o per mitjà de) *sistemes formals*. Potser la manera més ràpida de donar la idea del que és un sistema formal és definir-lo com un mecanisme de producció de *teoremes*. Aquests teoremes són certes expressions que formen part de la col·lecció de les anomenades *fórmules* del sistema del que es tracti. Les fórmules són certs seguits o combinacions de *símbols* o signes del sistema formal, com si fossin frases formades amb aquests símbols segons certes regles. Un sistema formal produeix teoremes de la manera següent: primer es defineixen perfectament unes certes fórmules, anomenades *postulats* o *axiomes*, que són, perquè així ho convenim, els primers teoremes del sistema formal; i després es defineixen amb tota precisió unes *regles d'inferència*, cada una de les quals obliga que, cada vegada que una fórmula satisfaci certes condicions en relació amb una certa col·lecció de teoremes, aquesta fórmula sigui també un teorema. Aquestes condicions que imposen les regles d'inferència han de ser tals que la comprovació de si estan o no satisfetes per una col·lecció de teoremes donada i una fórmula donada sigui sempre una comprovació factible i totalment mecànica o objectiva. La regla d'inferència més coneguda i usada és la "modus ponens": si A i $A \Rightarrow B$ són teoremes, B és teorema. De la mateixa manera que per a les regles d'inferència, la constatació de si una fórmula donada és o no un axioma ha de ser també un procediment purament mecànic, tal com, per exemple, veure si es troba en una col·lecció finita donada, o si és un "cas" d'un "esquema" d'axiomes (tal com s'exemplificarà més endavant). Tot aquest complex de símbols, axiomes i regles d'inferència ha de ser donat de manera tan precisa i controlada que faci possible el disseny d'un algorisme que ens permeti d'anar escrivint una llista (infinita, en general) de tots els teoremes del sistema formal, llista en la qual cada fórmula

(*) Conferència organitzada per la Societat, pronunciada el 19–11–87.

que sigui un teorema hi hagi d'aparèixer tard o d'hora. En general, però, no hi haurà cap algorisme que ens permeti decidir si una fórmula qualsevol és un teorema o no.

En un sistema formal, hi ha l'aspecte lògic i l'aspecte específic del sistema. Clàssicament, l'aspecte lògic d'un sistema formal, o lògica del sistema, pot ser el *càlcul proposicional* o bé el *càlcul de predicats* (o *lògica de primer ordre*). En el primer cas els símbols lògics del sistema formal són $\vee, \wedge, \neg$ i $\Rightarrow$ (disjunció, conjunció, negació i implicació). En el segon cas hem d'afegir a aquests símbols els *quantificadors* $\exists$ i $\forall$ (existencial i universal, respectivament). Les formes d'aquests símbols poden variar.

Un sistema formal ha de tenir altres símbols, com els parèntesis, la coma, possiblement uns símbols anomenats *variables*, etc. El més freqüent és trobar $=$ entre els símbols d'un sistema formal. Trobem $+$ i $\cdot$ entre els símbols dels sistemes formals que s'usen per a l'aritmètica, però no en altres sistemes, com alguns que formalitzen la geometria, per exemple. Hi ha una varietat il·limitada de possibilitats.

Amb alguns dels símbols d'un sistema formal es constitueixen certes expressions anomenades *termes*. Els termes són les expressions que prenen, en el sistema, el lloc que en l'aritmètica intuïtiva o informal tenen els nombres naturals, o en la geometria ingènua els punts. Així, per exemple, en un sistema que pretengui ser una formalització de l'aritmètica no ens ha d'estranyar que $0, 0', 0'', 0''', \ldots, x + y, x \cdot y, \ldots$, siguin termes, els primers dels quals són la contrapartida formal de $0, 1, 2, \ldots$.

Amb els termes i alguns símbols es formen unes altres expressions, les *fórmules atòmiques*, que podriem dir que són, o s'interpreten com, els judicis més primitius. En molts sistemes formals trobem entre les fórmules atòmiques les expressions $a = b$ on a i b són termes. Però en algun sistema formal per a la geometria, per exemple, podem trobar-hi també fórmules atòmiques com $Gr(c, d, e)$, on c, d i e són termes, i on l'agrupació Gr es pot veure com un sol símbol. En el sistema que tenim en ment, la fórmula $Gr(c, d, e)$ pot ser descrita com la contrapartida formal del judici "c, d i e estan alineats".

A partir de les fórmules atòmiques es constitueixen totes les fórmules segons les regles següents:

- *Si la lògica del sistema és el càlcul proposicional*:

  1) les fórmules atòmiques són *fórmules*;
  2) si A i B són fórmules, aleshores les expressions $\neg(A)$, $(A)\vee(B)$, $(A)\wedge(B)$ i $(A) \Rightarrow (B)$ també són *fórmules* (en les quals se suprimeixen parèntesis segons inveterats hàbits matemàtics).

- *Si la lògica del sistema és el càlcul de predicats*: les anteriors i, a més:

  3) si A és una fórmula i x és (o representa) una variable, aleshores les expressions $(\exists x)A$ i $(\forall x)A$ també són *fórmules*.

En qualsevol dels dos casos les regles que es dónen són les soles que, reiterades, poden fer que una expressió sigui una fórmula.

Els axiomes d'un sistema poden també ser lògics o específics del sistema, mentre que les regles d'inferència poden ser qualificades de lògiques totes elles. Els axiomes lògics i les regles d'inferència es poden expressar de diferents maneres equivalents. Escollim la que apareix en el llibre *"Introduction to Metamathematics"* de S.C. Kleene (Wolters-Nordhoff and North-Holland, 1971).

- *Si la lògica del sistema és el càlcul proposicional*:

  Axiomes lògics:
  $A \Rightarrow (B \Rightarrow A)$
  $(A \Rightarrow B) \Rightarrow \big((A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)\big)$
  $A \Rightarrow (B \Rightarrow A \wedge B)$
  $A \wedge B \Rightarrow A$
  $A \wedge B \Rightarrow B$
  $A \Rightarrow A \vee B$
  $B \Rightarrow A \vee B$
  $(A \Rightarrow C) \Rightarrow \big((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C)\big)$
  $(A \Rightarrow B) \Rightarrow \big((A \Rightarrow \neg B) \Rightarrow \neg A\big)$
  $\neg\neg A \Rightarrow A$

  Regla d'inferència:
  $\dfrac{A,\ A \Rightarrow B}{B}$ (és a dir, si A i $A \Rightarrow B$ són teoremes, aleshores B és teorema)

- *Si la lògica del sistema és el càlcul de predicats*:

  Axiomes lògics: els anteriors i, a més:
  $(\forall x)A(x) \Rightarrow A(t)$
  $A(t) \Rightarrow (\exists x)A(x)$

  Regles d'inferència: l'anterior i, a més:
  $$\frac{C \Rightarrow A(x)}{C \Rightarrow (\forall x)A(x)} \qquad \frac{A \Rightarrow C}{(\exists x)A(x) \Rightarrow C}$$

Els axiomes i regles d'inferència són *esquemes*, en el sentit que A, B i C són fórmules qualssevol del sistema formal, o bé poden ser fórmules d'una certa classe, tal com fórmules constants, per exemple, cosa que succeirà en uns exemples que veurem més endavant. També cal dir que x és (o representa) una variable. S'escriu $A(x)$ en lloc de A per cridar l'atenció sobre la variable x; i en aquest cas s'escriu $A(t)$ per representar el resultat de substituir x per t en A. Cal dir també que s'exigeix que en C no aparegui x *lliure* (és a dir, que

cada presència de x en C ha de formar part d'alguna expressió $(\exists x)D$ o $(\forall x)D$ continguda en C). També s'exigeix que t sigui un terme *lliure per* x *en* $A(x)$ (cosa que ara no cal que recordem què vol dir).

Així, doncs, per a descriure un sistema formal hem de dir, primer, si la seva lògica és el càlcul proposicional o el de predicats. Després cal definir els seus símbols, termes i fórmules atòmiques. Finalment, cal dir quins són els seus axiomes específics. Per exemple, en el sistema formal per a l'aritmètica que apareix en el llibre de Kleene tenim, entre altres axiomes específics, l'axioma d'inducció, o esquema d'inducció:

$$A(0) \wedge (\forall x)[A(x) \Rightarrow A(x')] \Rightarrow A(x)$$

En el mateix sistema hi ha vuit axiomes específics més, que són:

$$\begin{array}{lll} a' = b' \Rightarrow a = b\,; & \neg a' = 0\,; & a = b \Rightarrow (a = c \Rightarrow b = c)\,; \\ a = b \Rightarrow a' = b'\,; & a + 0 = a\,; & a + b' = (a + b)'\,; \\ a \cdot 0 = 0\,; & a \cdot b' = a \cdot b + a. & \end{array}$$

En aquest sistema tenim, recordem-ho per a referències posteriors i per a explicar els axiomes anteriors, el següent: 1) 0 és un *terme*; 2) cada variable és un *terme*; 3) si a i b són termes , $(a)'$, $(a + b)$ i $(a) \cdot (b)$ són *termes*. Les *fórmules atòmiques* són les expressions $a = b$ en les quals a i b són termes.

Aquest sistema basat en el càlcul de predicats que acabem de descriure, o un d'equivalent, és el que s'anomena *aritmètica clàssica.*

Donat un sistema formal, demostrar que una certa fórmula A és un teorema vol dir exhibir una llista de fórmules

$$A_1, A_2, \ldots, A_n,$$

tal que:

a) A_n és la fórmula A;
b) cada A_i, o bé és un postulat o bé s'obté de membres anteriors de la llista per alguna regla d'inferència (del càlcul proposicional o del càlcul de predicats, segons quina sigui la lògica del sistema).

Com ja s'ha fet notar, la comprovació que una tal llista és una demostració de A és un procés totalment mecànic, encara que el camí que hagi portat a obtenir o inventar la llista-demostració no s'hagi recorregut mecànicament. En molts casos, el trobar una certa demostració és, com tothom sap, el resultat d'una inventiva i imaginació portentoses. Però una vegada obtinguda la demostració i escrita en el llenguatge d'un sistema formal, no hi haurà cap possibilitat de diversitat d'opinions sobre si és o no una demostració. La comprovació, per part de qualsevol persona, que és una demostració es reduirà a constatar coses tals com, per exemple, que en l'aritmètica clàssica que s'ha descrit les expressions 0 i $0'$ són termes, que $0 = 0'$ i $0 = 0$ són fórmules atòmiques, que la fórmula

$$0 = 0' \Rightarrow (0 = 0 \Rightarrow 0 = 0')$$

és un cas de l'esquema $A \Rightarrow (B \Rightarrow A)$, que la fórmula

$$a = 0 \Rightarrow (\forall x)[x + a = x]$$

s'infereix de $a = 0 \Rightarrow x + a = x$ segons la segona de les regles d'inferència pròpies del càlcul de predicats, etc.

Aquesta mena de comprovacions, així com l'operació de comptar, o de comprovar que 3 i 4 fan 7, constitueixen la mena de matemàtica que Hilbert anomena *finitària* (finit), la matemàtica que no és posada en dubte per ningú, a la qual també podem anomenar combinatòria, manipulativa, concreta, constructiva, etc. Altres menes de raonament, com, per exemple, un raonament en el qual calgui acceptar que tots els conjunts es poden ben-ordenar, seran posats en dubte per molts matemàtics.

El que ens interessa fer ressaltar és el següent:

Les demostracions de teoremes en un sistema formal es poden escriure de manera absolutament correcta, com llistes que satisfan a) i b). La comprovació que una tal llista és una demostració és objectiva i purament mecànica; és un exercici en matemàtiques constructives, les matemàtiques que no són posades en dubte per ningú.

No s'ha d'amagar, però, que allò que es pot posar en dubte és la correcció dels axiomes, o la consistència del sistema, o fins i tot l'adequació del formalisme. Però això és el que es discutirà en la secció següent.

De moment, farem algunes consideracions suplementàries.

La primera és que, per raons pràctiques, s'usen també regles d'inferència derivades. Així, per exemple, s'usa la regla de la *demostració per casos*, que es podria escriure com

$$\frac{B \Rightarrow C\ ,\ (\neg B) \Rightarrow C}{C}$$

regla que es demostra constructivament que és veritable (donades una demostració de $B \Rightarrow C$ i una de $(\neg B) \Rightarrow C$ es mostra com construir una demostració de C).

Una altra regla derivada que s'usa molt és el *teorema de la deducció*: si, en afegir a un sistema formal una fórmula A com un nou postulat, s'obté que B és un teorema en el nou sistema resultant, aleshores en el sistema original és un teorema $A \Rightarrow B$, sempre que en la demostració de B en el nou sistema no s'hagin aplicat les regles d'inferència exclusives del càlcul de predicats per a la variable x, si x apareix lliure en A.

Convé assenyalar un altre punt important, en l'aspecte lògic. Hi ha una classe de fórmules, anomenades *idènticament veritables* o *tautològiques*: una fórmula Z, escrita a partir de fórmules $Y_1, \ldots, Y_n$ sense usar altres símbols lògics que $\vee, \wedge, \neg, \Rightarrow$, és una fórmula *tautològica* si per a qualsevol combinació de valors V (veritable) o F (fals) que assignem a les Y_i sempre obtenim, com a valor de Z calculat d'acord amb les *taules de veritat*, el valor V. Les taules de veritat són regles que forcen els valors de $A \vee B$, $A \wedge B$, $\neg A$ i $A \Rightarrow B$ en base als

valors de A i B. Són regles que estan d'acord amb els continguts intuïtius dels connectius $\vee, \wedge, \neg$ i $\Rightarrow$, i són les següents:

A	$\neg A$
V	F
F	V

A	B	$A \vee B$	$A \wedge B$	$A \Rightarrow B$
V	V	V	V	V
V	F	V	F	F
F	V	V	F	V
F	F	F	F	V

Així, doncs, per exemple, si A és V i B es F, $A \vee B$ és V, $A \wedge B$ és F i $A \Rightarrow B$ és F.

Totes les fórmules tautològiques són teoremes, demostrables per mitjà dels axiomes lògics del càlcul proposicional, sense necessitat dels axiomes lògics exclusius del càlcul de predicats ni dels axiomes específics del sistema formal de què es tracti. Aquestes fórmules tautològiques es prenen, en la pràctica, com si fossin axiomes. De fet, una presentació possible de la lògica proposicional clàssica és admetre com a axiomes totes les fórmules tautològiques.

Una altra simplificació possible és que en una demostració es poden admetre com a membres A_i de la llista-demostració teoremes ja demostrats abans, cosa que és molt fàcilment justificable. Per a més simplificacions es poden consultar el llibre ja citat de Kleene o el de Mendelson (*"Introduction to Mathematical Logic"* , van Nostrand, 1964), entre altres. Sense totes aquestes simplificacions les demostracions serien intolerablement llargues.

Més encara, en l'ús d'un sistema formal el més freqüent és que l'aspecte lògic romangui parcialment o totalment sobreentès, i fins i tot que l'ús de la lògica sigui inconscient. També és freqüent l'ús de sistemes que són subsidiaris d'altres sistemes, com ara d'una teoria de conjunts formal. En aquests casos poden restar sobrentesos la lògica i els axiomes específics d'aquest altre sistema. En tots aquests casos potser és preferible parlar de *sistemes axiomàtics.*

És també cert que la fonamentació de la matemàtica com a sistema formal no és la sola possibilitat imaginable, ni es pretén que la lògica clàssica de la que hem estat parlant sigui la sola possible, o "veritable" lògica. Potser és la que ha estat més acceptada però al seu costat hi ha també, per exemple, la lògica *intuïcionista,* que no accepta l'axioma $\neg\neg A \Rightarrow A$. Al respecte es pot consultar el llibre de Kleene o bé el de Heyting *"Intuitionism, an introduction"* (North Holland, 1956, 1966, 1971). Però aquí continuarem parlant de la lògica clàssica i dels sistemes formals en el sentit en què ho hem fet fins ara.

2 La filosofia formalista de les matemàtiques i la crítica constructivista

Pensem, per a alguna fórmula A, en la fórmula

(*) $$(\exists x)A(x) \vee (\forall x)[\neg A(x)]$$

Observem que les fórmules $(X \Rightarrow Y) \Rightarrow ((\neg Y) \Rightarrow (\neg X))$ i $((\neg X) \Rightarrow Y) \Rightarrow (X \vee Y)$ són tautològiques, per a qualssevol X i Y, segons les taules següents, en les quals U i W representen la primera i la segona d'aquestes fórmules, respectivament:

X	Y	$X \Rightarrow Y$	$\neg X$	$\neg Y$	$(\neg X) \Rightarrow Y$	$(\neg Y) \Rightarrow (\neg X)$	$X \vee Y$	U	W
V	V	V	F	F	V	V	V	V	V
V	F	F	F	V	V	F	V	V	V
F	V	V	V	F	V	V	V	V	V
F	F	V	V	V	F	V	F	V	V

Admetent aquestes tautologies com si fossin axiomes tindrem aleshores, com a demostració de $(*)$, la llista

$$A(x) \Rightarrow (\exists x)A(x),$$

$$\big(A(x) \Rightarrow (\exists x)A(x)\big) \Rightarrow \big((\neg(\exists x)A(x)) \Rightarrow (\neg A(x))\big),$$

$$\big(\neg(\exists x)A(x)\big) \Rightarrow \big(\neg A(x)\big)\ ,\ \big(\neg(\exists x)A(x)\big) \Rightarrow (\forall x)\big(\neg A(x)\big),$$

$$\big((\neg(\exists x)A(x) \Rightarrow (\forall x)(\neg A(x))\big) \Rightarrow \big((\exists x)A(x) \vee (\forall x)(\neg A(x))\big),$$

$$(\exists x)A(x) \vee (\forall x)[\neg A(x)]$$

Així, doncs, $(*)$ és un teorema de l'aritmètica clàssica.

Suposem, en general, que B i C són fórmules amb un cert contingut intuïtiu, és a dir que signifiquen quelcom per a nosaltres. El contingut intuïtiu que aleshores s'ha d'atribuir a $(\exists x)B(x)$ és que hi ha un terme t per al qual és veritat $B(t)$. El contingut intuïtiu de $(\forall x)C(x)$ és que per a cada terme t és veritat $C(t)$. Això, doncs, el contingut intuïtiu de $(*)$ haurà de ser:

> "$\neg A(t)$ per a tots els termes t , o bé existeix un terme u tal que $A(u)$".

Ara bé, aquesta és una forma del principi del tercer exclòs per a col·leccions infinites (la col·lecció de termes de l'aritmètica clàssica, o la col·lecció dels naturals), i una tal forma del tercer exclòs és objecte de polèmica entre els matemàtics, si més no. Un *constructivista* no l'accepta. Per exemple, si pretenem definir el nombre a com 0 o 1 segons que hi hagi un t tal que $A(t)$ o bé que $\neg A(t)$ per a tots els t, un constructivista ens dirà que no hem definit res, a menys que donem la manera de decidir si a és 0 o és 1. Així, doncs, la posició constructivista, com també *l'intuicionisme* de Brouwer, rebutja l'aritmètica clàssica perquè en aquest sistema formal es demostren com a teoremes afirmacions que tenen continguts intuïtius que consideren que no són veritables. Parlant a nivell intuïtiu, fora de formalismes, un constructivista o un intuïcionista consideren

que no s'ha demostrat que existeix un t tal que $A(t)$ a menys que s'exhibeixi un tal t. També consideren que només s'ha demostrat $A \vee \neg A$ si s'ha demostrat A o s'ha demostrat $\neg A$. De manera que un constructivista no pot acceptar un sistema en el qual $(*)$ és una veritat demostrada, per a cada A, ja que en general en el sistema de l'aritmètica clàssica no se sap decidir, per a cada A, si és cert que $(\exists x)A(x)$ o que $(\forall x)[\neg A(x)]$. Sobre el constructivisme es pot consultar *"Foundations of Constructive Mathematics"* de Beeson (Springer, 1985).

La resposta *formalista* a aquesta crítica és la següent: així com els matemàtics han introduït objectes ideals tals com (diu Hilbert) l'imaginari i o els ideals de la teoria dels nombres algèbrics, així mateix hem de considerar les expressions $(\exists x)A(x), (\forall x)B(x)$ com a proposicions ideals que no tenen un significat concret. Però així com i es pot veure com a un símbol concret que es manipula constructivament, així mateix aquestes proposicions ideals s'han de veure com a nous objectes concrets, les fórmules, que es manipulen de manera finitària, o concreta, o constructiva, d'acord amb les regles del càlcul de predicats. El sol perill que els formalistes troben en l'ús dels sistemes formals és el de la *inconsistència.* Un sistema formal és inconsistent si hi ha alguna fórmula A tal que A és un teorema i $\neg A$ també; i és *consistent* en cas contrari. Hilbert, cap de l'escola formalista, diu que és indispensable demostrar la consistència del sistema formal de què es tracti i que, això sí, aquesta consistència s'ha de demostrar usant només les matemàtiques més segures, les finitàries o constructives. L'exposició més recomanada del programa formalista és la que es troba en l'article de Hilbert *"Über das Unendliche"* (Math. Ann. 95 (1926)), del qual hi ha traducció a l'anglès (*"On the infinite"*) en el recull *"From Frege to Gödel"* editat per J. van Heijenoort (Harvard University Press, 1967). Potser ara és un bon moment per a recordar que Frege va ser qui va posar les bases del càlcul de predicats. De Gödel, l'altra lògic que dóna nom al recull, n'haurem de parlar tot seguit.

Hilbert i els formalistes volgueren portar a terme aquest programa, intentant demostrar constructivament la consistència de l'aritmètica clàssica. Un dels intents introduïa l'expressió $\varepsilon(A)$ amb el contingut intuïtiu d'objecte prototípic que satisfà A, si hi ha un tal objecte, i definia aleshores $(\forall x)A$ i $(\exists x)A$ com $A(\varepsilon(\neg A))$ i $A(\varepsilon(A))$, respectivament. Una versió primitiva d'aquesta ε, l'operador τ, ha deixat rastre en la teoria de conjunts segons Bourbaki. En tots els intents, però, sempre restava una escletxa per on s'escapava la demostració finitària de la consistència. Però les esperances de l'escola formalista no es van perdre fins que, el 1931, Gödel publicà un dels treballs més famosos en la història de les matemàtiques: *"Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I"* (sobre proposicions formalment indecidibles dels Principia Mathematica i sistemes relacionats I), aparegut a Monatshefte für Mathematik und Physik 38, pp. 173-198. Hi ha també una traducció a l'anglès en el recull ja citat de van Heijenoort i una traducció al castellà en *"Obras completas"* de Kurt Gödel (AU 286, 1981). Els *"Principia Mathematica"* a què es refereix l'article és l'obra monumental de Whitehead i

Russell. En aquest article de Gödel es demostra allò que avui expressaríem dient que per a cada sistema formal consistent basat en el càlcul de predicats que pretengui formalitzar l'aritmètica podem trobar una fórmula que és veritable i que no és un teorema del sistema. Basant-nos en aquest resultat es demostra que cap demostració de la consistència d'un tal sistema no és "formalitzable dins del sistema". La conclusió d'aquesta segona part és que cap sistema formal amb les característiques esmentades, que contingui o formalitzi (o representi) tota l'aritmètica constructiva i que sigui consistent, no pot ser constructivament consistent, ja que si ho fos la demostració constructiva de la seva consistència hauria de ser "formalitzable dins del sistema". Gödel declara expressament que el seu resultat no va en contra del programa formalista de Hilbert perquè, diu, és possible que hi hagi procediments constructius que no estiguin recollits en l'aritmètica clàssica; però el fet és que el treball de Gödel ha estat considerat gairebé com una demostració absoluta de la impossibilitat de demostrar constructivament la consistència de l'aritmètica clàssica o de qualsevol sistema formal consistent basat en el càlcul de predicats que contingui prou aritmètica. Aquesta actitud troba un fort suport en l'anomenada "tesi de Church" (que no discutirem en aquest moment).

No obstant aquest aparent fracàs del programa formalista estricte, és un fet que un formalisme moderat va guanyar, per així dir-ho, la batalla al constructivisme. Això es palesa en la gran acceptació que han tingut les teories de conjunts formals. En el desenvolupament de les teories de conjunts formals es cercava eliminar les paradòxes conegudes, sense pensar que una demostració de la consistència, constructiva o no, fos indispensable o exigible. Tot això no és impediment, però, perquè la teoria de conjunts passi per moments crítics ni perquè es continuïn conreant les matemàtiques constructives o s'assagin noves vies de fonamentació. En el recull de van Heijenoort es poden trobar traduccions a l'anglès dels articles de Zermelo *"Untersuchungen über die Grundlagen der Mengenlehre I"* (Math. Ann. 65 (1908) i de von Neumann *"Eine Axiomatisierung der Mengenlehre"* (Jour. für die Reine und Angewandte Math. 154(1925); Berichtigung, id. 155), traduïts com a *"Investigation on the foundations of set theory I"* i *"An axiomatization of set theory"*. Tenen relació amb els temes tractats els articles de Gödel *"Zur intuitionistischen Arithmetik und Zahlentheorie"* (Ergebnisse eines mathematischen Kolloquiums, ed. per K. Menger, 1932) (traduït al castellà en *"Obras Completas"* de Gödel, AU286, amb el títol de *"Sobre la teoría de números y la aritmética intuicionista"*) i *"Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes"* (Dialectica, 12, U952)), del qual hi ha traducció a l'anglès en Journal of Philosophical Logic, 9(1980) i al castellà en les *"Obras Completas"* (*"Sobre una ampliación todavía no utilizada del punto de vista finitario"*).

En resum, el programa *formalista finitari* pot veure's en la forma original, com el propòsit de formalitzar l'aritmètica de la manera següent:

A) *com un sistema formal basat en el càlcul de predicats*;

B) *de manera constructivament consistent.*

Els esdeveniments, incloent el treball de Gödel, mostren que no podem assolir l'exigència B) sense deixar córrer l'exigència A). L'actitud majoritària dels formalistes ha estat, ho acabem de recordar, la de deixar de banda l'exigència B). Però hi ha també la possibilitat *d'abandonar* A) *sense abandonar* B). Aquesta és la possibilitat que examinarem a continuació, on proposem la noció de *formalisme recursiu* com a substitutiva de la noció de sistema formal basat en el càlcul de predicats, per tal d'assolir l'exigència B).

3 La idea recursivista i la seva aplicació en el programa formalista: la noció de formalisme recursiu

En 1923, Thoralf Skolem, després d'haver estudiat els *"Principia Mathematica"* i mogut per idees semblants a les de l'intuicionisme, va desenvolupar un tros d'aritmètica sense usar els quantificadors amb tota la seva força, mitjançant la "manera recursiva de pensar". L'article de Skolem, *"Begründung der elementaren Arithmetik ..."* té una traducció a l'anglès en el recull ja citat de van Heijenoort amb el títol de *"The foundations of elementary arithmetic established by means of the recursive mode of thought, without the use of apparent variables ranging over finite domains"*. El resultat del treball de Skolem és el desenvolupament constructiu d'un tros d'aritmètica ara conegut com *aritmètica recursiva primitiva.*

Recordem, per començar, com es defineix, informalment, la classe $\mathcal{P}$ de les funcions *recursives primitives.* $\mathcal{P}$ és la mínima classe de funcions de $\mathbf{N}^n$ en $\mathbf{N}$ (per $n > 0$ no fix) que satisfà les condicions següents:

C1. La funció constant $(x_1, \ldots, x_n) \longmapsto c$ pertany a la classe, per a cada $c \in \mathbf{N}$ i cada $n > 0$. La funció projecció $(x_1, \ldots, x_n) \longmapsto x_i$ pertany a la classe sempre que $1 \leq i \leq n$. La funció *successor* $S : \mathbf{N} \longrightarrow \mathbf{N}$, definida com $S(x) = x + 1$, pertany a la classe.

C2. Si les funcions $f : \mathbf{N}^n \longrightarrow \mathbf{N}$ i $g_i : \mathbf{N}^r \longrightarrow \mathbf{N}$ pertanyen a la classe, per a $i = 1, \ldots, n$, aleshores la composició $h : \mathbf{N}^r \longrightarrow \mathbf{N}$, definida com

$$h(y_1, \ldots, y_r) = f(g_1(y_1, \ldots, y_r), \ldots, g_n(y_1, \ldots, y_r))$$

també pertany a la classe.

C3. Si les funcions $f : \mathbf{N}^n \longrightarrow \mathbf{N}$ i $g : \mathbf{N}^{n+2} \longrightarrow \mathbf{N}$ pertanyen a la classe, aleshores també pertany a la classe la funció $h : \mathbf{N}^{n+1} \longrightarrow \mathbf{N}$ definida per *recursió primitiva* a partir de f i g com

$$\begin{aligned} h(x_1, \ldots, x_n, 0) &= f(x_1, \ldots, x_n) \\ h(x_1, \ldots, x_n, y+1) &= g(x_1, \ldots, x_n, y, h(x_1, \ldots, x_n, y)) \end{aligned}$$

(on, en el cas $n = 0$, en lloc d'una funció f hem de tenir un element $f \in \mathbf{N}$ i la primera igualtat és $h(0) = f$).

Tenim, per exemple, que la suma és una funció recursiva primitiva:

Prenem, en C3, $n = 1$, $f(x_1) = x_1$, $g(x_1, x_2, x_3) = S(x_3)$, on sabem que $f \in \mathcal{P}$ perquè és una projecció i $g \in \mathcal{P}$ perquè és la composició de la projecció $(x_1, x_2, x_3) \longmapsto x_3$ i S. Tenim aleshores que $h \in \mathcal{P}$ i que

$$\begin{aligned} h(x_1, 0) &= x_1 \\ h(x_1, S(x_2)) &= S(h(x_1, x_2)) \end{aligned}$$

Però la funció $x_1 + x_2$ té les mateixes propietats que h,

$$\begin{aligned} x_1 + 0 &= x_1 \\ x_1 + S(x_2) &= S(x_1 + x_2) \end{aligned}$$

i això permet demostrar fàcilment, per inducció, que

$$x_1 + x_2 = h(x_1, x_2)$$

i que, per tant, la suma pertany a $\mathcal{P}$.

En un desenvolupament de l'aritmètica recursiva el que faríem seria definir la suma com la funció h. Després en demostraríem, per inducció, les propietats. A continuació definiríem el producte i en demostraríem les propietats, etc., fins a arribar als teoremes sobre el màxim comú divisor i la descomposició en primers. Per a tractar la divisió amb residu, per exemple, hauríem de definir, recursivament, les funcions quocient i residu i demostrar-ne les propietats.

En el que s'acaba de dir sense fixar cap marc lògic especial podem pensar, però, que cada vegada que introduïm una funció per recursió primitiva el que fem és introduir uns nous axiomes que són els que defineixen la funció. En el cas de la suma aquests axiomes són els esquemes

$$\left.\begin{aligned} x_1 + 0 &= x_1 \\ x_1 + S(x_2) &= S(x_1 + x_2) \end{aligned}\right\} \text{per a tots els naturals } x_1, x_2$$

Aquesta darrera observació i algunes altres consideracions són les que han suggerit la següent noció de *formalisme recursiu* com a possible instrument de formalització que pugui substituir la noció de sistema formal basat en el càlcul de predicats, en el programa formalista.

Descripció

Un *formalisme recursiu* és una col·lecció de sistemes formals basats en el càlcul proposicional (això és, sense quantificadors) amb un llenguatge comú (és a dir, els mateixos símbols, termes i fórmules), tots ells constructivament consistents.

Donat un formalisme recursiu $\mathcal{F}$, anomenem *segments* de $\mathcal{F}$ els sistemes formals que els constitueixen.

Si $\mathbf{V}$ és un segment de $\mathcal{F}$ i A és una fórmula (del llenguatge comú de tots els segments), s'escriu $\mathbf{V} \vdash A$ per a indicar que A é un teorema de $\mathbf{V}$.

Segons la definició, dos segments, $\mathbf{U}$ i $\mathbf{V}$, de $\mathcal{F}$ només poden diferir en els seus axiomes. Si tots els axiomes de $\mathbf{U}$ són axiomes de $\mathbf{V}$ direm que $\mathbf{V}$ és *posterior* a $\mathbf{U}$ i escriurem $\mathbf{U} < \mathbf{V}$.

La descripció que s'ha donat de formalisme recursiu és incompleta puix que no s'ha dit com s'ha d'usar. Descriurem a continuació la manera d'usar-lo i farem algunes altres observacions pertinents.

3.1 Observació

Cal dir, en primer lloc, i com a únic principi general, que l'ús d'un formalisme recursiu $\mathcal{F}$ per a desenvolupar una teoria matemàtica ha de ser estrictament constructiu o finitari, de la mateixa manera que l'ús d'un sistema formal per a demostrar teoremes és constructiu, tal com ho hem recordat en la primera secció.

3.2 Observació

Bo i quedant ben clar que la lògica de cada segment és el càlcul proposicional i que no tenim els quantificadors $\exists$ i $\forall$ del càlcul de predicats, no és menys clar que podem fer afirmacions existencials i universals, sempre que siguin constructives. Podem dir, per exemple, que existeix un terme t tal que la fórmula $A(t)$ és un teorema del segment $\mathbf{V}$, si aquesta afirmació va acompanyada de l'exhibició del tal t i de la demostració de que $\mathbf{V} \vdash A(t)$. També podem afirmar constructivament coses tals com que $\mathbf{V} \vdash A(t_i)$ per a tots els termes d'una llista infinita $t_1, t_2, \ldots$. La demostració d'aquesta afirmació consistirà a donar un algorisme que ens proporcioni una demostració de $\mathbf{V} \vdash A(t_i)$ per a cada i. Aquest algorisme, en particular, pot consistir en una demostració de $\mathbf{V} \vdash A(t_i)$ i un esquema o model de la demostració que

$$\mathbf{V} \vdash A(t_i) \Longrightarrow A(t_{i+1})$$

per a cada i. És a dir, pot ser una demostració per inducció.

En el present escrit usarem els símbols

$$\exists^* \, , \, \forall^*$$

com a quantificadors entesos en el sentit constructiu. Així escriurem, per exemple,

$$(\exists^* x)[\mathbf{V} \vdash A(x)] \;\; i \;\; (\forall^* x)[\mathbf{V} \vdash A(x)]$$

per indicar, respectivament, que podem trobar un terme t per al qual podem demostrar $\mathbf{V} \vdash A(t)$ i que per a cada terme t sabem com demostrar $\mathbf{V} \vdash A(t)$. Els termes t poden estar, en els dos casos, subjectes a formar part d'una certa subcol·lecció de termes.

Així, doncs, $\forall^*$ i $\exists^*$ no són part d'un càlcul de predicats sinó que són tan sols signes taquigràfics que s'usen com s'acaba de dir.

3.3 Observació

En un formalisme recursiu $\mathcal{F}$ es pot donar un cas com el següent: "si succeeix que $(\forall^* x)[\mathbf{V} \vdash A(x)]$, aleshores hi ha un segment $\mathbf{U}$ tal que $\mathbf{V} < \mathbf{U}$ i que $\mathbf{U} \vdash B$, per a certa fórmula B". Pot haver-hi, per exemple, un *principi* de $\mathcal{F}$ que ens asseguri tal cosa. De fet, tal principi pot ser de la forma "si $\mathbf{V}$ és un segment de $\mathcal{F}$ i $(\forall^* x)[\mathbf{V} \vdash A(x)]$, aleshores el sistema formal que s'obté d'afegir a $\mathbf{V}$ la fórmula B com un nou axioma també és un segment de $\mathcal{F}$". És clar que això és com un succedani de regla d'inferència infinitària, on la premissa constaria d'una infinitat d'afirmacions. La raó que es pot adduir a favor d'aquests principis d'un formalisme recursiu i en contra de les regles d'inferència infinitàries és la que es dóna a continuació. En l'intent de demostrar la consistència, la presència d'una regla d'inferència infinitària ens podria forçar a haver d'usar el principi del tercer exclòs per a col·leccions infinites, cosa que no és constructiva. Si, en canvi, hi ha un principi de la mena anterior, aquesta dificultat no apareix, ja que el principi és positiu, és a dir que no ens hem de preocupar més que del cas en què la premissa infinitària es satisfà.

3.4 Observació

Hi ha afirmacions que són interpretables, o susceptibles de ser veritables o falses, en qualsevol segment $\mathbf{V}$ de $\mathcal{F}$. Un exemple és l'afirmació

$$(\forall^* x)[\vdash A(x)],$$

que per ella mateixa no és una afirmació precisa, ja que $\vdash A(x)$ significa "$A(x)$ és un teorema" però no s'especifica en quin segment de $\mathcal{F}$. Convenim en què la interpretació de $(\forall^* x)[\vdash A(x)]$ en el segment $\mathbf{V}$ és

$$(\forall^* x)[\mathbf{V} \vdash A(x)]$$

Així, doncs, $(\forall^* x)[\vdash A(x)]$ *és veritat en* $\mathbf{V}$ si (és veritat que) $(\forall^* x)[\mathbf{V} \vdash A(x)]$.

De la mateixa manera, la interpretació de $\vdash B$ en $\mathbf{V}$ és $\mathbf{V} \vdash B$.

En general, si $\mathcal{C}$ és una afirmació interpretable en qualsevol segment escriurem

$$\mathbf{V} : \mathcal{C}$$

per a indicar que "$\mathcal{C}$ és veritat en $\mathbf{V}$" o que "la interpretació de $\mathcal{C}$ en $\mathbf{V}$ és veritat".

Usarem, en les mateixes circumstàncies,

$$\mathcal{F} : \mathcal{C}$$

per a indicar que $\mathbf{V} : \mathcal{C}$ per cada segment $\mathbf{V}$ de $\mathcal{F}$.

Si volem demostrar $\mathcal{F} : \mathcal{C}$ haurem de tenir algun algorisme o esquema que ens permeti, per a qualsevol segment $\mathbf{V}$ de $\mathcal{F}$, donar una demostració de $\mathbf{V} : \mathcal{C}$.

Usem el signe $\equiv$ per a indicar, en l'expressió $X \equiv Y$, que X representa Y, o a la inversa, o que X i Y representen el mateix.

3.5 Observació

Posem, per exemple,

$$\mathcal{A} \equiv (\forall^* t)[\vdash A(t)] \ , \quad \mathcal{B} \equiv \vdash B$$

En un exemple anterior (observació 3.3) hem parlat d'una afirmació que podem escriure així

(1)' "Si $\mathbf{V} : \mathcal{A}$, aleshores $\mathbf{U} : \mathcal{B}$ per algun $\mathbf{U} > \mathbf{V}$"

Si ara fem abstracció de $\mathbf{V}$ i expressem (1) com una afirmació interpretable en qualsevol segment, tindrem

(2) "Si $\mathcal{A}$, aleshores $\mathcal{B}$ en algun segment posterior"

La interpretació de (2) en $\mathbf{V}$ és (1).
Per a escriure afirmacions de la mena de (2) usarem un nou símbol,

$$\models\!\!\Rightarrow$$

i posarem, en general, si $\mathcal{C}$ i $\mathcal{D}$ són interpretables en qualsevol segment,

$$\mathcal{C} \models\!\!\Rightarrow \mathcal{D}$$

per tal de representar l'afirmació

"Si $\mathcal{C}$, aleshores $\mathcal{D}$ en un segment posterior",

de manera que

$$\mathbf{V} : \mathcal{C} \models\!\!\Rightarrow \mathcal{D}$$

significa

"Si $\mathbf{V} : \mathcal{C}$, aleshores $\mathbf{U} : \mathcal{D}$ per algun $\mathbf{U} > \mathbf{V}$"

i

$$\mathcal{F} : \mathcal{C} \models\!\!\Rightarrow \mathcal{D}$$

representa l'afirmació

"$\mathbf{V} : \mathcal{C} \models\!\!\Rightarrow \mathcal{D}$ per cada $\mathbf{V}$",

o sigui

"Per a cada $\mathbf{V}$, si $\mathbf{V} : \mathcal{C}$ aleshores $\mathbf{U} : \mathcal{D}$ per a algun $\mathbf{U} > \mathbf{V}$"

Així, doncs, demostrar $\mathcal{F} : \mathcal{C} \models\!\!\Rightarrow \mathcal{D}$ significa demostrar $\mathbf{V} : \mathcal{C} \models\!\!\Rightarrow \mathcal{D}$ per a cada segment $\mathbf{V}$ de $\mathcal{F}$, cosa que comporta tenir un procediment, o model, o algorisme, per a, donat qualsevol segment $\mathbf{V}$, i en el supòsit que tenim una demostració de $\mathbf{V} : \mathcal{C}$, trobar un cert $\mathbf{U}$ tal que $\mathbf{U} > \mathbf{V}$ i demostrar $\mathbf{U} : \mathcal{D}$ (sense oblidar que totes les demostracions han de ser constructives).

3.6 Observació

El desenvolupament d'una teoria mitjançant un formalisme recursiu $\mathcal{F}$ consistirà a demostrar afirmacions de la mena

$$\mathcal{F} : \mathcal{A} ,$$

on les $\mathcal{A}$ són afirmacions interpretables en qualsevol segment de $\mathcal{F}$ (i que en particular poden ser de la mena $\mathcal{B} \models\!\!\Rightarrow \mathcal{C}$).

A continuació definirem i tractarem amb un cert detall un formalisme recursiu per a l'aritmètica recursiva primitiva, denotat **ARP**, que és el prototip dels formalismes recursius. Posteriorment, i no tan detalladament, veurem un altre formalisme recursiu, més ample, *l'aritmètica formalment recursiva* (**AFR**), que és més poderós que l'aritmètica recursiva (general) i que pot ser vist com la contrapartida constructivament consistent de l'aritmètica clàssica.

4 El formalisme recursiu ARP (aritmètica recursiva primitiva)

4.1 Descripció de ARP

Els símbols de **ARP** són : 0, S, $=$, la coma, els parèntesis, les *variables*, els *operadors* i els connectius del càlcul proposicional, $\vee, \wedge, \neg, \Rightarrow$. Les variables, que només tenen una utilitat secundària, són els membres d'una llista infinita de símbols. Seran representades per x, y, z, x_1, etc. Per a cada natural n hi ha d'haver una llista infinita *d'operadors de grau n*. Els operadors es representen $\mathbf{f}, \mathbf{g}$, etc. Entre els operadors de grau 1 hi ha el símbol S.

Els *termes* es representen com a, b, c, a_1, etc, i es defineixen així: 1) 0 és un *terme* ; 2) cada variable és un *terme* ; 3) si $\mathbf{f}$ és un operador de grau n i $a_1, \ldots, a_n$ són termes, aleshores l'expressió $\mathbf{f}(a_1, \ldots, a_n)$ és un *terme*.

En particular, les expressions

$$0, S(0), S(S(0)), \ldots$$

són termes, que s'anomenen *numerals*.

Les fórmules *atòmiques* són les expressions $a = b$ en les quals a i b són termes.

Cal potser recalcar que tots els axiomes lògics seran suposats constants (sense variables), o bé que d'entre les fórmules tautològiques només admetrem com a axiomes o teoremes les que són constants. Això, i el fet que tots els axiomes específics dels segments de **ARP** seran constants, farà que tots els teoremes siguin constants, cosa que ens obligarà a treballar amb esquemes d'axiomes i de teoremes. Així, doncs, per exemple, tindrem un esquema d'axiomes que serà "$a = a$ per cada numeral a", que vol dir que són axiomes $0 = 0, S(0) = S(0)$, etc. Però la fórmula $x = x$ (on x és una variable) no serà axioma ni teorema.

Així queda descrit el llenguatge comú de tots els segments de **ARP**. Cada segment de **ARP** quedarà determinat per la seva col·lecció d'axiomes o postulats

específics, segons els principis que s'enunciaran més endavant. De moment ens convé llistar els següents *esquemes de postulats inicials* (EPI), que seran axiomes de tots els segments de **ARP**:

EPI 1. $a = a$ per a cada numeral a

EPI 2. $\neg a = b$, sempre que a i b siguin numerals diferents

EPI 3. $a = b \wedge f = g \Longrightarrow f' = g$, sempre que a, b, f i g siguin termes constants i que f' s'obtingui de f en substituir una presència de a per b.

EPI 4. $a = b \Longrightarrow b = a$, sempre que a i b siguin termes constants.

Abans d'enunciar els principis de **ARP** ens cal introduir, per a un segment **V** de **ARP** i per a termes a i r, la notació següent:

$a \in N_{\mathbf{V}}$ (que es llegeix "a és un **V**-nombre") significa que podem exhibir algun numeral c per al qual podem demostrar que $\mathbf{V} \vdash a = c$.

$r \in N_{\mathbf{V}}(x_1, \ldots, x_n)$ (que es llegeix "r és **V**-funció de $x_1, \ldots, x_n$") significa que

$$r[c_i/x_i] \in N_{\mathbf{V}}$$

per a qualssevol numerals $c_1, \ldots, c_n$.

En la definició anterior, i com sempre, d'ara endavant, usem, en general,

$$t\left[\frac{d_i}{y_i}\right] \quad \text{o bé} \quad t[d_i/y_i]$$

per a representar el resultat de substituir les y_i pels termes d_i, en el terme t. Usarem una notació anàloga per a fórmules A en lloc de termes t.

Continuarem usant sistemàticament $\equiv$ per a denotar la identitat, en el sentit que $X \equiv Y$ significa que X i Y representen o són el mateix. Usarem $\not\equiv$ per a negar $\equiv$.

Podem notar, per exemple, que si **f** és un operador de grau 2 tenim

$$\mathbf{f}(y_1, y_2)[d_i/y_i] \equiv \mathbf{f}(d_1, d_2)$$

Els dos principis que ens diuen quins sistemes formals són segments de **ARP** són els següents:

PRINCIPI 1. El sistema formal basat en el càlcul proposicional que té el llenguatge que acabem de descriure i que té com a únics postulats específics tots els casos de EPI 1,2,3 i 4 és un *segment* de **ARP**, el segment *inicial*, denotat **I**.

PRINCIPI 2. Si : 1) **T** és un segment de **ARP** i n és un natural; 2) $r \in N_{\mathbf{V}}(x_1, \ldots x_n)$ i $s \in N_{\mathbf{V}}(x_1, \ldots, x_n, y, z)$; 3) **f** és un operador de grau $n+1$, *nou* per a **T** (això és, **f** no apareix en cap postulat específic de **T** que no sigui un

cas de EPI 3 o EPI 4); aleshores el sistema formal que s'obté de **T** en afegir-li els següents esquemes de postulats també és un *segment* de **ARP**:

$$\text{(I)} \qquad r\left[\frac{a_i}{x_i}\right] = c \Rightarrow \mathbf{f}(a_1, \ldots, a_n, 0) = c;$$

$$\text{(II)} \qquad s\left[\frac{a_i}{x_i}\right]\left[\frac{b}{y}\right]\left[\frac{\mathbf{f}(a_1, \ldots, a_n, b)}{z}\right] = d \Rightarrow \mathbf{f}\Big(a_1, \ldots, a_n, S(b)\Big) = d;$$

per a qualssevol numerals $a_1, \ldots, a_n, c$ i d.

(Observeu que seria una notació molt arriscada, per a un terme r, usar $r(a_i)$ per representar $r[a_i/x_i]$, ja que podria fer pensar que r és un operador, cosa que un terme no és mai. D'altra banda tenim, com ja s'ha assenyalat,

$$\mathbf{f}(a_1, \ldots, a_n, e) \equiv \mathbf{f}(x_1, \ldots, x_n, y)[a_i/x_i][e/y]).$$

Podríem afegir que res no és un segment de **ARP** si no és per les raons anteriors.

D'aquesta manera queda perfectament descrit **ARP**. Però per a poder assegurar que satisfà totes les condicions d'un formalisme recursiu encara ens falta demostrar constructivament la consistència de cada segment. A continuació donarem una idea d'aquesta demostració essencialment trivial.

4.2 La consistència de ARP

Recordem, abans de començar, que una *valoració lògica* és qualsevol funció del conjunt de fórmules en el conjunt { V,F } que sigui compatible amb les taules de veritat de $\vee, \wedge, \neg, \Rightarrow$. Això fa que una valoració (lògica) sigui determinada pels seus valors en les fórmules atòmiques.

Anomenem *primitius* els termes de **ARP** que són de la forma $\mathbf{f}(a_1, \ldots, a_n)$, per a n no fix, on $\mathbf{f}$ és operador de grau n diferent de S i els a_i són numerals.

Anomenem *identificació* tota fórmula atòmica $b = c$ en la qual b és un terme primitiu i c és un numeral. Una col·lecció D d'identificacions és *admissible* si no hi ha dues identificacions de D, $b = c_1$, i $b = c_2$, tals que $c_1 \not\equiv c_2$. D'ara endavant només considerarem col·leccions d'identificacions que siguin admissibles. Donada una col·lecció D d'identificacions, definirem una col·lecció N_D de termes de **ARP**, una funció $\#_D$ de N_D en la col·lecció de numerals i una valoració lògica W_D de la manera següent: considerem qualsevol terme d de **ARP** i fem, si és possible, l'operació de substituir una presència d'un terme primitiu b pel numeral c, per a alguna identificació $b = c$ de D ; amb el resultat obtingut fem, si podem, una altra operació de la mateixa mena, i així successivament, fins que arribem a un terme d' per al qual una tal operació ja no sigui possible, i que és independent de l'ordre en què s'han fet aquestes operacions. En aquest moment, si d' és un numeral (i només en aquest cas) posem

$$d \in N_D \quad \text{i} \quad \#_D(d) \equiv d'$$

Definim aleshores W_D començant per definir

$$W_D(d_1 = d_2) \equiv \begin{cases} \text{V}, & \text{si } d_1 \text{ i } d_2 \text{ pertanyen a } N_D \text{ i } \#d_1 \equiv \#d_2 \\ \text{F}, & \text{si no} \end{cases}$$

i estenem la definició a totes les fórmules mitjançant les taules de veritat.

Ens referim a la valoració W_D com la *D-valoració.*

Si D és una col·lecció infinita podem pensar en el perill de no poder decidir, per a cada d, si $d \in N_D$ o no. Si sempre podem decidir-ho, aleshores les definicions que s'han donat són constructives. En la discussió que farem a continuació aquestes definicions sempre seran constructives, per a la manera en què es definiran les col·leccions D, si bé no escriurem la comprovació d'aquesta constructivitat.

Tenim:

4.2.1 Observació

Cada D-valoració és compatible amb tots els casos de EPI 1, 2, 3 i 4.

4.2.2 Observació

Si $W_D(a = c) \equiv V$, aleshores $a \in N_D$ i $\#_D(a) \equiv c$, si c és numeral..

Considerem ara qualsevol segment **V** de **ARP**. Tenim

$$\mathbf{I} \equiv \mathbf{V}_0 < \mathbf{V}_1 < \ldots < \mathbf{V}_n \equiv \mathbf{V},$$

on cada $\mathbf{V}_{i+1}$ ha estat obtingut per adjunció a $\mathbf{V}_i$, d'acord amb el principi 2, de certs esquemes

$$(\text{I})_{i+1} \qquad r_{i+1}[a_j/x_j] = c \;\Rightarrow\; \mathbf{f}_{i+1}(a_1, \ldots, a_{n(i+1)}, 0) = c$$

$$(\text{II})_{i+1} \qquad s_{i+1}\left[\frac{a_j}{x_j}\right]\left[\frac{b}{y}\right]\left[\frac{\mathbf{f}_{i+1}(a_1, \ldots, a_{n(i+1)}, b)}{z}\right] = d$$

$$\Rightarrow\; \mathbf{f}_{i+1}\big(a_1, \ldots, a_{n(i+1)}, S(b)\big) = d$$

Definirem una successió de col·leccions d'identificacions

$$\phi \equiv D_0 \subseteq D_1 \subseteq \ldots \subseteq D_n$$

de manera tal que cada D_i-valoració serà compatible amb (valdrà V en) tots els postulats específics de $\mathbf{V}_i$, per $i \equiv 0, \ldots, n$.

Fet això, ja haurem demostrat la consistència del segment arbitrari **V**. En efecte, si la D-valoració és compatible amb tots els postulats de **V**, donat que una valoració lògica compatible amb A i amb $A \Rightarrow B$ ha de ser compatible amb B, i donat que tota valoració lògica és compatible amb totes les fórmules tautològiques, tindrem que aquesta valoració ha de valer V en tots els membres

de cada demostració i, per tant, ha de valer V en tots els teoremes; però, com que si una valoració lògica val V en C ha de valer F en $\neg C$, ja haurem demostrat que C i $\neg C$ no podem mai ser, totes dues, teoremes.

Ens convé destacar per ella mateixa l'observació següent:

4.2.3 Observació

Cada valoració compatible amb tots els postulats d'un segment és compatible amb tots els teoremes del segment.

Descriurem, doncs, el pas de D_i a D_{i+1} en el supòsit que la D_i-valoració és compatible amb tots els postulats de $\mathbf{V}_i$.

Ordenem d'alguna manera constructiva les $n(i+1)$-ades de numerals:

$$(a_1^{(1)},\ldots,a_{n(i+1)}^{(1)}),(a_1^{(2)},\ldots,a_{n(i+1)}^{(2)}),(a_1^{(3)},\ldots,a_{n(i+1)}^{(3)}),\ldots$$

Aleshores considerem la doble successió

$$(a_1^{(1)},\ldots,a_{n(i+1)}^{(1)};0),\qquad (a_1^{(2)},\ldots,a_{n(i+1)}^{(2)};0),\ldots$$

$$(a_1^{(1)},\ldots,a_{n(i+1)}^{(1)};S(0)),\quad (a_1^{(2)},\ldots,a_{n(i+1)}^{(2)};S(0)),\ldots$$

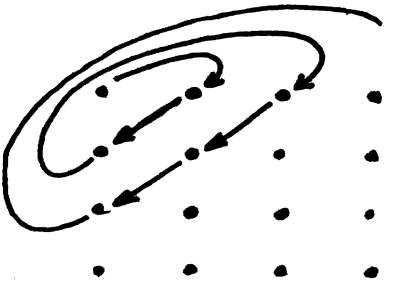
$$\ldots\ldots\qquad\qquad\ldots\ldots$$

Ordenem aquesta doble successió diagonalment segons l'ordre

$$(a_1^{(j)},\ldots,a_{n(i+1)}^{(j)};k)<(a_1^{(r)},\ldots,a_{n(i+1)}^{(r)};s)$$

si $j+k<r+s$ o bé $j+k=r+s$ i $k<s$.

És a dir que ordenem la doble successió segons l'esquema



Procedim així, per a definir D_{i+1}:

1r.) En el primer pas, això és, per $(a_1^{(1)},\ldots,a_{n(i+1)}^{(1)};0)$, considerem tots els casos de $(I)_{i+1}$ per $a_j\equiv a_j^{(1)}$. Com que

$$r_{i+1}[a_j^{(1)}/x_j]$$

és un $\mathbf{V}_i$-nombre, segons la hipòtesi del principi 2 tindrem

$$\mathbf{V}_i \vdash r_{i+1}[a_j^{(1)}/x_j] = c_1$$

per a algun numeral c_1. Per tant, i com que la D_i-valoració és compatible amb tots els postulats de $\mathbf{V}_i$, segons l'observació 4.2.3 la D_i-valoració ha de ser compatible amb la fórmula:

$$r_{i+1}[a_j^{(1)}/x_j] = c_1$$

i, segons l'observació 4.2.2, i amb la notació $D(i) \equiv D_i$, tenim

$$c_i \equiv \#_{D(i)}(r_{i+1}[a_j^{(1)}/x_j])$$

i, per numerable,

$$W_{D(i)}(r_{i+1}[a_j^{(1)}/x_j] = e) \equiv \mathrm{F} \text{ sempre que } e \not\equiv c_1$$

Afegim aleshores a D_i la identificació

$$\mathbf{f}_{i+1}(a_1^{(1)}, \ldots, a_{n(i+1)}^{(1)}, 0) = c_1,$$

que denotem id_1, i tindrem que la $D_i \cup \{id_1\}$-valoració és compatible amb tots els postulats de $\mathbf{V}_i$ i amb tots els casos de $(I)_{i+1}$ per $a_j \equiv a_j^{(1)}$.

2n.) En el segon pas, per $(a_1^{(2)}, \ldots, a_{n(i+1)}^{(2)}; 0)$, considerem tots els casos de $(I)_{i+1}$ per $a_j \equiv a_j^{(2)}$ i procedim com abans, però per a $D_i \cup \{id_1\}$ en lloc de D_i. En aquest cas afegim a $D_i \cup \{id_1\}$ la identificació

$$\mathbf{f}_{i+1}(a_1^{(2)}, \ldots, a_{n(i+1)}^{(2)}, 0) = \#_{D(i)}(r_{i+1}[a_j^{(2)}/x_j]),$$

que denotem id_2, i tindrem que la $D_i \cup \{id_1, id_2\}$-valoració és compatible amb tots els postulats de $\mathbf{V}_i$ i amb tots els casos de $(I)_{i+1}$ per $a_j \equiv a_j^{(1)}$ i per $a_j \equiv a_j^{(2)}$.

3r.) En el tercer pas, per $(a_1^{(1)}, \ldots, a_{n(i+1)}^{(1)}; S(0))$, considerem tots els casos de $(I)_{i+1}$ per a $a_j \equiv a_j^{(1)}$ i $b \equiv 0$. Observem aleshores, amb la notació

$id(1) \equiv id_1$, $id(2) \equiv id_2$ i $n \equiv n(i+1)$, que

$$s_{i+1}\left[\frac{a_j^{(1)}}{x_j}\right]\left[\frac{0}{y}\right]\left[\frac{\mathbf{f}_{i+1}(a_1,\ldots,a_n,0)}{z}\right] \in N_{D(i)\cup\{id(1),id(2)\}}$$

$$\#_{D(i)\cup\{id(1),id(2)\}}\left(s_{i+1}\left[\frac{a_j^{(1)}}{x_j}\right]\left[\frac{0}{y}\right]\left[\frac{\mathbf{f}_{i+1}(a_1,\ldots,a_n,0)}{z}\right]\right)$$

$$\equiv \#_{D(i)}\left(s_{i+1}\left[\frac{a_j^{(1)}}{x_j}\right]\left[\frac{0}{y}\right]\left[\frac{\#_{D(i)\cup\{id(1),id(2)\}}(\mathbf{f}_{i+1}(a_1^{(1)},\ldots,a_n^{(1)},0))}{z}\right]\right)$$

$$\equiv \#_{D(i)}\left(s_{i+1}\left[\frac{a_j^{(1)}}{x_j}\right]\left[\frac{0}{y}\right]\left[\frac{c_1}{z}\right]\right) \equiv c_2$$

A partir d'aquest moment procedim com en els passos anteriors, és a dir, afegim la identificació

$$id_3 \equiv \mathbf{f}_{i+1}(a_1^{(1)},\ldots,a_{n(i+1)}^{(1)}, S(0)) = c_2$$

i observem que la $D_i \cup \{id_1, id_2, id_3\}$-valoració és compatible amb $\mathbf{V}_i$ i amb tots els casos de $(I)_{i+1}$ per a $a_j \equiv a_j^{(1)}$ i $a_j \equiv a_j^{(2)}$ i amb tots els casos de $(II)_{i+1}$ per a $a_j \equiv a_j^{(1)}$ i $b \equiv 0$.

En el quart pas, per a $(a_1^{(3)},\ldots,a_{n(i+1)}^{(3)};0)$, es procedeix com en el primer i segon passos. En el cinquè pas, per a $(a_1^{(2)},\ldots,a_{n(i+1)}^{(2)};S(0))$, es procedeix com en el tercer pas. En el sisè pas, per a $(a_1^{(1)},\ldots,a_{n(i+1)}^{(1)};S(S(0)))$, es procedeix de manera semblant al tercer i cinquè passos, etc.

D'aquesta manera queda definida

$$D_{i+1} \equiv D_i \cup \{id_1, id_2, id_3, \ldots\}$$

i la D_{i+1}-valoració és compatible amb tots els postulats de $\mathbf{V}_{i+1}$.

4.3 La utilització de ARP per a desenvolupar l'aritmètica recursiva primitiva.

Tinguem present el que s'ha discutit a 3.1 - 3.5. Pensem en l'expressió $b \in N$ com una expressió interpretable o susceptible de ser veritat (o no) en cada segment. La seva interpretació en el segment $\mathbf{V}$ és

$$b \in N_{\mathbf{V}},$$

això és

$$(\exists^* c(\text{numeral}))[\mathbf{V} \vdash b = c].$$

També podem expressar $b \in N$ com

$$\big(\exists^* c(\text{numeral})\big)[\vdash b = c].$$

De la mateixa manera, l'expressió $r \in N(x_1, \ldots, x_n)$, que es pot expressar com

$$\big(\forall^* a_i(\text{numerals})\big)\,[r[a_i/x_i] \in \mathbf{N}]$$

o com

$$\big(\forall^* a_i(\text{numerals})\big)\,[\exists^* c(\text{numeral})[\vdash r[a_i/x_i] = c]],$$

té, com a interpretació en el segment $\mathbf{V}$,

$$\big(\forall^* a_i(\text{numerals})\big)\,[r[a_i/x_i] \in N_{\mathbf{V}}]$$

o bé

$$\big(\forall^* a_i(\text{numerals})\big)\,[\big(\exists^* c(\text{numeral})\big)\,[\mathbf{V} \vdash r[a_i/x_i] = c]].$$

Recordem també que **ARP** : $\mathcal{A}$ significa "$\mathbf{V}$: $\mathcal{A}$ per a cada segment $\mathbf{V}$ de **ARP**".

Desenvoluparem una petita part de l'aritmètica recursiva, com a mostra.

Tenim, per començar,

4.3.1

ARP : $S(x) \in N(x)$

Hem de demostrar que $S(x) \in N_{\mathbf{V}}(x)$ per cada $\mathbf{V}$, això és, que per a cada numeral a hi ha un numeral c tal que $\mathbf{V} \vdash S(a) = c$. Però si a és numeral, $S(a)$ també ho és, de manera que podem prendre $c \equiv S(a)$ i se satisfà $\mathbf{V} \vdash S(a) = c$ a causa de EPI 1.

4.3.2

ARP : $x_i \in N(x_1, \ldots, x_n)$ sempre que $1 \leq i \leq n$

La demostració també és trivial.

4.3.3

$$\begin{aligned}\mathbf{ARP}\ :\ & r \in N(x_1, \ldots, x_n)\ \&\ s \in N(x_1, \ldots, x_n, y, z)\\ & \Longrightarrow (\exists^* t)[t \in N(x_1, \ldots, x_n, y, z)\\ & \&(\forall^* a_1, \ldots, a_n, b)[\vdash t[a_j/x_j][0/y] = r[a_j/x_j]\\ & \&\vdash t\left[\frac{a_j}{x_j}\right]\left[\frac{S(b)}{y}\right] = s\left[\frac{a_j}{x_j}\right]\left[\frac{b}{y}\right]\left[\frac{t[a_j/x_j]\,[b/y]}{z}\right]]]\end{aligned}$$

on t ha de ser un terme i els a_i i b numerals. De fet, el terme t pot ser de la forma $\mathbf{f}(x_1, \ldots, x_n, y)$.

El que hem de demostrar (constructivament) és:

"Per a cada **V**, si $r \in N_{\mathbf{V}}(x_1, \ldots, x_n)$ i $s \in N_{\mathbf{V}}(x_1, \ldots, x_n, y, z)$, aleshores hi ha un segment **U** posterior a **V** i algun terme t tal que $t \in N_{\mathbf{U}}(x_1, \ldots, x_n, y)$ i que, per a qualssevol numerals a_i, b,

$$\mathbf{U} \vdash t[a_j/x_j][0/y] = r[a_j/x_j]$$

$$\mathbf{U} \vdash t\left[\frac{a_j}{x_j}\right]\left[\frac{S(b)}{y}\right] = s\left[\frac{a_j}{x_j}\right]\left[\frac{b}{y}\right]\left[\frac{t[a_j/x_j][b/y]}{z}\right]"$$

La demostració és així: suposem que tenim

$$r \in N_{\mathbf{V}}(x_1, \ldots, x_n) \quad \text{i} \quad s \in N_{\mathbf{V}}(x_1, \ldots, x_n, y, z).$$

Apliquem el principi 2 al segment **V** amb un operador **f** nou per a **V** i afegim a **V** els esquemes de postulats (I) i (II) corresponents, obtenint així un segment que serà el nostre **U**. Aleshores posem $t \equiv \mathbf{f}(x_1, \ldots, x_n, y)$ i demostrem fàcilment les afirmacions $t \in N_{\mathbf{U}}(x_1, \ldots, x_n, y)$, etc (per a la qual cosa hem d'usar naturalment, els postulats inicials EPI 1, 2, 3 i 4).

Pot ser útil recordar a un hipotètic lector no simpatitzant de la lògica matemàtica que els raonaments que s'han de fer a **ARP** els podem fer amb la mateixa naturalitat amb què raonem habitualment en matemàtiques, tenint només en compte quin és el sentit de $\Longrightarrow$ i altres observacions de 3.1 - 3.5, en particular la relativa al fet que $\exists^*$ i $\forall^*$ tenen un sentit constructiu.

L'afirmació 4.3.3 significa que podem introduir noves funcions per recursió primitiva.

4.3.4

$$\mathbf{ARP} : r \in N(x_1, \ldots, x_n) \;\&\; s_1 \in N(y_1, \ldots, y_n) \& \ldots$$
$$\ldots \& s_n \in N(y_1, \ldots, y_m) \text{ implica}$$
$$r[s_j/x_j] \in N(y_1, \ldots, y_m)$$

Aquí el que s'ha de demostrar és:

"Per a cada **V**, si $r \in N_{\mathbf{V}}(x_1, \ldots, x_n)$ i $s_i \in N_{\mathbf{V}}(y_1, \ldots, y_m)$ per a $i = 1, \ldots, n$, aleshores $r[s_j/x_j] \in N_{\mathbf{V}}(y_1, \ldots, y_m)$"

La demostració és trivial.

El principi 2 es pot usar no tan sols per a introduir noves funcions per recursió primitiva, sinò també per a canviar de notació. Si, per exemple, tenim la funció $r[s_i/x_i]$ de l'exemple anterior podem, si escollim bé les variables x_i i els termes r i s del principi 2, introduir, per a un cert **f**, postulats que ens assegurin que $\mathbf{f}(a_1, \ldots, a_m) = r[s_i/x_i][a_k/y_k]$ per a qualssevol numerals a_k.

Ja hem vist abans com s'introdueix la suma per recursió primitiva: a partir de **I** escollim, en el principi 2, $r \equiv x_1$, $s \equiv S(x_3)$ i $+$ com a operador (que suposem és a la llista dels operadors de grau 2). Tenim aleshores, en postular

(I) $$a_1 = c \Rightarrow +(a_1, 0) = c$$

(II) $$S(+(a_1, b)) = d \Rightarrow +(a_1, S(b)) = d,$$

que en el nou segment **U** es té

$$\left.\begin{array}{ll} \mathbf{U} \vdash +(a,0) & = a \\ \mathbf{U} \vdash +(a, S(b)) & = S(+(a,b)) \end{array}\right\} \text{per a qualssevol numerals } a, b$$

Aleshores es poden demostrar la commutativitat i l'associativitat. Per exemple, si usem la notació $a + b$ en lloc de $+(a, b)$, i si escrivim, com és habitual, A en lloc de $\vdash A$ o de $\mathbf{U} \vdash A$

i) $0 + 0 = 0$

ii) Per a qualsevol numeral b, si $0 + b = b$, aleshores

$$0 + S(b) = S(0 + b) = S(b)$$

iii) Per a i) i ii) tenim

$$0 + 0 = 0\,,\ 0 + S(0) = S(0)\,,\ 0 + S(S(0)) = S(S(0)), \ldots$$

això és, $0 + b = b$ per a cada numeral b

iv) $a + S(0) = S(a + 0) = S(a)$

v) Per a qualssevol numerals a i b, si $a + S(b) = S(a) + b$, aleshores

$$a + S(S(b)) = S(a + S(b)) = S(S(a) + b) = S(a) + S(b)$$

vi) De iv) i v) tenim, per a qualsevol numeral a,

$$a + S(0) = S(a) + 0, \quad a + S(S(0)) = S(a) + S(0),$$
$$a + S(S(S(0))) = S(a) + S(S(0)), \quad \text{etc}\,,$$

això és $a + S(b) = S(a) + b$ per a qualssevol numerals a i b

vii) $a + 0 = a = 0 + a$ per a cada a, segons iii).

viii) Per a qualssevol numerals a i b, si $a + b = b + a$, aleshores
$a + S(b) = S(a + b) = S(b + a) = b + S(a) = S(b) + a$, per vi)

ix) De vii) i viii) tenim, per a qualsevol numeral A,

$$a + 0 = 0 + a\,,\ a + S(0) = S(0) + a\,,\ a + S(S(0)) = S(S(0)) + a\,, \text{etc.},$$

això és $a + b = b + a$ per a qualssevol numerals a i b, que no és altra cosa sinó la llei commutativa.

Això il·lustra la manera com es pot anar copiant qualsevol exposició de l'aritmètica recursiva primitiva per a anar desenvolupant aquesta aritmètica

mitjançant **ARP**. Una tal exposició és, per exemple, la de Goodstein, *"Recursive number theory"* (North Holland, 1957). Una observació pertinent que podem fer és que en el desenvolupament podem escollir, en cada pas, l'operador **f** nou que usarem. Això és que, amb l'excepció de S, els operadors no tenen un significat fix. Aquesta situació es presenta en molts contexts matemàtics i no ens ha de sorprendre aquí. Per exemple, + podria usar-se en algun segment per a denotar el producte, o alguna altra operació, en lloc de la suma. És a dir, podríem tenir, per exemple,

$$\mathbf{W} \vdash +(S(0),0) = 0$$

en algun segment **W** (no posterior a **U**). Tindríem aleshores dues afirmacions que, vistes simultàniament, podriem repugnar, de primera intenció, però que són totalment inofensives. Aquestes són:

$$\mathbf{I} \ : \ 0 = 0 \Longmapsto +(S(0),0) = S(0)$$

$$\mathbf{I} \ : \ 0 = 0 \Longmapsto +(S(0),0) = 0$$

i no reflecteixen altra cosa qsinò el que ja s'ha dit: que en un segment + pot tenir un significat diferent del que té en un altre. També podem observar que en cap de les dues afirmacions anteriors no podem posar **ARP** en lloc de **I**. És a dir, no són afirmacions de les que constitueixen un desenvolupament matemàtic, segons l'observació 3.6.

Una conseqüència de tot això és que si volem expressar que la suma és commutativa no podrem escriure

$$\mathbf{ARP}\colon \big(\forall^* a, b\,(\text{numerals})\big)\big[\vdash +(a,b) = +(b,a)\big],$$

perquè aquesta afirmació és falsa, sinó que haurem d'escriure

$$\mathbf{ARP}\colon \text{si}\big(\forall^* a, b(\text{numerals})\big)\big[\vdash +(a,0) = a \wedge +(a,S(b)) = S(+(a,b))\big],$$

$$\text{aleshores } (\forall^* a, b \textit{ numerals})[\vdash +(a,b) = +(b,a)]$$

Una altra possibilitat és definir un segment **B** en què +, i potser altres operadors, com $\cdot$, tinguessin el significat usual, i considerar només els segments que són posteriors a **B**. És clar, però, que així podríem fixar els significats d'una col·lecció finita d'operadors, i no els de la infinitat restant. Encara una altra possibilitat és no considerar + i $\cdot$ com a operadors, sinó com a signes auxiliars que només s'usin per a representar operadors que tinguin, en un segment donat, les propietats de la suma i el producte.

L'aritmètica recursiva primitiva és la més constructiva de les matemàtiques. El presentar-la com un formalisme constructivament consistent no és, doncs, una gran feta. La seva presentació com el formalisme recursiu **ARP** és interessant perquè, en primer lloc, mostra que la noció de formalisme recursiu és molt natural, i en segon lloc, ja s'ha dit, perquè prepara molt bé la descripció de **AFR** que es farà a continuació.

5 L'aritmètica formalment recursiva (AFR)

5.1 Preliminars

Recordem que la classe $\mathcal{P}$ de les funcions recursives primitives és la mínima que satisfà les condicions C1, C2, C3. Considerem les condicions C4 i C5 següents, relatives, com les anteriors, a una classe de funcions de $\mathbf{N}^n$ en $\mathbf{N}$.

C4. Si $f\colon \mathbf{N}^{n+1} \longrightarrow \mathbf{N}$ pertany a la classe, aleshores la funció $f_E\colon \mathbf{N}^n \longrightarrow \mathbf{N}$, definida com a

$$f_E(x_1,\ldots,x_n) = \begin{cases} 1, & \text{si existeix } y \text{ tal que } f(x_1,\ldots,x_n,y) = 0 \\ 0, & \text{si no} \end{cases}$$

també pertany a la classe.

C5. Si $f\colon \mathbf{N}^{n+1} \longrightarrow \mathbf{N}$ pertany a la classe i la funció f_E (definida com a C4) té la propietat

$$f_E(x_1,\ldots,x_n) = 1 \text{ per cada } (x_1,\ldots,x_n) \in \mathbf{N}^n$$

aleshores la funció $f_M\colon \mathbf{N}^n \longrightarrow \mathbf{N}$ definida com a

$$f_M(x_1,\ldots,x_n) = \textit{minim } y \text{ tal que } f(x_1,\ldots,x_n,y) = 0$$

també pertany a la classe.

La mínima classe $\mathcal{R}$ de funcions que satisfà les condicions C1, C2, C3 i C5 (però no C4) és la classe de les funcions *recursives* o *diofàntiques*, també conegudes en alguna època com a funcions recursives generals. Sobre el nom de diofàntiques vegeu, per exemple, l'article de M. Davis *"Hilbert's tenth problem is unsolvable"*, Amer. Math. Monthly 80 (1973) pp. 233-269. Les funcions recursives són calculables o computables. La famosa tesi de Church afirma que la classe de les funcions recursives coincideix amb la de les computables de $\mathbf{N}^n$ en $\mathbf{N}$. Aquesta no és una afirmació matemàtica sinó l'afirmació que la noció matemàtica que correspon a la noció vaga de funció computable és la de funció recursiva. La tesi de Church és molt amplament acceptada. En aquest respecte es pot consultar el llibre de Kleene ja citat.

Anomenem *ultradiofàntiques* les funcions de la mínima classe $\mathcal{U}$ que satisfà les cinc condicions C1 - C5. Les funcions ultradiofàntiques no són totes computables, ja que la f_E no és computable, en general, encara que la f ho sigui.

L'aritmètica que es limita a la manipulació constructiva de les funcions recursives, o *aritmètica recursiva* (A.R.), és l'aritmètica constructiva per excel·lència. Podríem dir que l'aritmètica que manipula les funcions ultradiofàntiques és *l'aritmètica ultradiofàntica* (A.U.), que ja no és constructiva. L'A.U. és, grosso modo, l'aritmètica clàssica (A.C.). Ja tornarem més endavant sobre aquesta darrera afirmació.

L'A.U. es més poderosa que l'A.R. Això es mostra en el fet que la classe $\mathcal{U}$ és més gran que la classe $\mathcal{R}$, però es fa patent d'una manera més colpidora quan

comparem les anàlisis matemàtiques basades en una o l'altra aritmètica, cosa de la qual també parlarem més endavant.

L'aritmètica formalment recursiva **AFR** que presentarem a continuació vol ser una presentació de l'A.U. com a formalisme recursiu. Però cal senyalar des d'ara que en **AFR** apareix, degut a l'exigència de constructivitat de la demostració de la consistència, un factor limitador. Aquest factor, fet o fenomen, que es descriurà amb precisió més endavant, té a veure amb el pas de f a f_E, que en **AFR** no funciona ben bé com un operador, ja que f_E dependrà de la "forma" de f, per dir-ho així. Això farà, segons veurem, que **AFR** no contingui l'A.C., malgrat l'equivalència (grosso modo) entre aquesta i l'A.U. i el que **AFR** representi de manera acceptable aquesta última. D'altra banda, aquesta és una situació que era d'esperar-se, perquè d'altra manera (si **AFR** contingués l'A.C.) la consistència constructiva de **AFR** podria produir una demostració constructiva de la consistència de l'A.C., cosa, ja ho hem recordat, impossible o no esperable.

5.2 Descripció de AFR

La descripció de **AFR** es pot trobar a Pub. Mat. UAB vol. 28 no. 1 (1984), pp.19-78 (" *Aritmètica i anàlisi formalment recursives*") o a la publicació 53 del C.R.M. de l'I.E.C., juliol 1987 ("Recursive formalisms and arithmetic"). La descripció següent difereix molt lleugerament d'aquestes. És una diferència d'estil.

Com que acabem de descriure **ARP** resulta que la manera més ràpida de descriure **AFR** és mitjançant una sèrie de modificacions en la definició de **ARP**. Així procedirem:

Modificació 1

Per a **AFR** hem de tenir E i M entre els símbols específics, a més dels de **ARP**, i hem d'afegir

$$E\mathbf{g}(a_1, \ldots, a_{n-1}) \text{ i } M\mathbf{g}(a_1, \ldots, a_{n-1})$$

a la col·lecció dels termes sempre que els a_i siguin termes i g un operador de grau n.

Modificació 2

La definició de $N_{\mathbf{V}}$ ha de ser com a continuació, per **AFR**:
$b \in N_{\mathbf{V}}$ significa "podem trobar numerals $c_1, \ldots, c_r$ (r no fix) tals que podem demostrar $\mathbf{V} \vdash b = c_1 \vee \ldots \vee b = c_r$".

Modificació 3

Mentre que els principis 1 i 2 de **ARP** continuen essent vàlids per a **AFR**, hem d'afegir els dos principis següents:

PRINCIPI 3. Si **W** és un segment de **AFR**, $u \in N_{\mathbf{W}}(x_1, \ldots, x_n, y)$ i **g** és un operador de grau $n+1$ nou per a **W**, aleshores el sistema obtingut adjuntant a **W** els següents esquemes d'axiomes també és un *segment* de **AFR**:

(A) $\mathbf{g}(a_1, \ldots, a_n, b) = u[a_i/x_i][b/y]$

(B) $\bigwedge_{i=0}^{m-1} \neg \mathbf{g}(a_1, \ldots, a_n, S^i(0)) = 0 \wedge \mathbf{g}(a_1, \ldots, a_n, S^m(0)) = 0 \Rightarrow M\mathbf{g}(a_1, \ldots, a_n) = S^m(0)$

(C) $\mathbf{g}(a_1, \ldots, a_n, c) = 0 \Rightarrow E\mathbf{g}(a_1, \ldots, a_n) = S(0)$

(D) $E\mathbf{g}(a_1, \ldots, a_n) = 0 \vee E\mathbf{g}(a_1, \ldots, a_n) = S(0)$

(per a tots els numerals a i b i cada natural m).

PRINCIPI 4. (exposat en forma extremadament simplificada). Si, després d'aplicar el principi 3, demostrem, en el nou segment **U** que s'obté en afegir els esquemes d'axiomes (A), (B), (C), (D), que

$$\mathbf{U} \vdash \neg \mathbf{g}(a_1, \ldots, a_n, c) = 0 \text{ per a tots els numerals } c,$$

aleshores el sistema obtingut adjuntant a **U** l'axioma següent és també un *segment* de **AFR**:

$$E\mathbf{g}(a_1, \ldots, a_n) = 0$$

Aquest principi 4 té, en una forma menys simplificada, funcions h_i de $z_i, \ldots, z_q$ en lloc dels numerals a_i, la hipòtesi

"$\mathbf{U} \vdash \neg \mathbf{g}(h_i[d_i/z_i], \ldots, h_n[d_i/z_i], c)$ per a qualssevol numerals d_i i c" en lloc de

"$\mathbf{U} \vdash \neg \mathbf{g}(a_i, \ldots, a_n, c) = 0$ per a cada numeral c"

i

"$E\mathbf{g}(h_1[d_i/z_i], \ldots, h_n[d_i/z_i]) = 0$ per a qualssevol numerals d_i"

en lloc de

"$E\mathbf{g}(a_1, \ldots, a_n) = 0$"

En la forma més general el principi es dóna de manera condicional.

Al mateix temps que es demostra constructivament la consistència de **AFR**, es demostra també el següent metateorema, dit *de minimització*:

AFR : $(\forall^* \mathbf{f}(\text{operador de grau } n+1))(\forall^* a_1, \ldots, a_n \text{ (numerals)})$

$[\text{si } \vdash E\mathbf{f}(a_1, \ldots, a_n) \doteq S(0), \text{ aleshores } M\mathbf{f}(a_1, \ldots, a_n) \in N$

$\text{i} \vdash \mathbf{f}(a_1, \ldots, a_n, M\mathbf{f}(a_1, \ldots, a_n)) = 0]$

Tenim, doncs, per a cada segment $\mathbf{V}$, si $\mathbf{V} \vdash \mathit{Ef}(a_1, \ldots, a_n) = S(0)$ aleshores $\mathbf{V} \vdash \mathbf{f}(a_1, \ldots, a_n, \mathit{Mf}(a_1, \ldots, a_n)) = 0$. Però potser convé assenyalar que el metateorema *no és, ni implica*, que l'afirmació $\mathit{Ef}(a_1, \ldots, a_n) = S(0) \Rightarrow \mathbf{f}(a_1, \ldots, a_n, \mathit{Mf}(a_1, \ldots, a_n)) = 0$ sigui un teorema. La demostració del metateorema de minimització ens dóna la manera, donada una demostració de $\mathbf{V} \vdash \mathit{Ef}(a_1, \ldots, a_n) = S(0)$, i només en aquest cas, de fer una demostració de $\mathit{Mf}(a_1, \ldots, a_n) \in N_{\mathbf{V}}$ i una demostració de

$$\mathbf{V} \vdash \mathbf{f}(a_1, \ldots, a_n, \mathit{Mf}(a_1, \ldots, a_n)) = 0$$

Les demostracions constructives de la consistència i del metateorema de minimització no es repetiran ara. Es poden trobar als articles citats al començament de 5.2. Són demostracions més complicades que la de la consistència de **ARP**.

Els postulats dels principis 3 i 4 i el metateorema de minimització mostren que $\mathit{Ef}(x_1, \ldots, x_n)$ i $\mathit{Mf}(x_1, \ldots, x_n)$ prenen en **AFR** els llocs de les funcions f_E i f_M de C4 i C5, respectivament.

El canvi en la definició de $N_{\mathbf{V}}$ per **AFR** (modificació 2) fa necessari el metateorema següent, que anomenem *d'inducció*, que es demostra trivialment:

Si $\mathbf{V} \vdash A[a_i/x_i]$ per a totes les col·leccions de numerals a_i, això mateix és cert sempre que $a_i \in N_{\mathbf{V}}$ per a cada i.

Si abolim la modificació 2 i traiem l'axioma (D) del principi 3, el que resta és un formalisme recursiu per a l'aritmètica recursiva.

En l'article "Anàlisi formalment recursiva" (Pub. Mat. UAB vol. 30 nos. 2-3 (1986) pp. 35-37) es desenvolupa una anàlisi basada en **AFR**, més poderosa que l'anàlisi constructiva. Però per un lapsus s'usa sistemàticament una extensió del metateorema de minimització en la que els arguments són nombres dels segments corresponents, i no únicament numerals; i aquesta és una extensió que no està demostrada. De manera que el saber com i fins a quin punt l'anàlisi formalment recursiva és més forta que l'anàlisi constructiva és encara un interessant problema obert. Sobre l'anàlisi constructiva en general es pot consultar el llibre ja citat de Beeson. Es pot trobar la pista de la que es podria anomenar escola russa a través de l'article de Demuth i Kučera *"Remarks on constructive mathematical analysis"* (Logic Colloquium 1974; Boffa, van Dalen & McAloon, editors, North Holland). Són importants, en anàlisi constructiva, el llibre de Goodstein (*"Recursive analysis"*, North Holland 1961) i el de Bishop (*"Foundations of constructive analysis "*, McGraw-Hill, 1967), entre altres.

Així queda exhibit un formalisme recursiu, la **AFR**, que és una aritmètica més poderosa que l'aritmètica constructiva i és (com tots els formalismes recursius) constructivament consistent, cosa que no és assolible amb un sistema formal basat en el càlcul de predicats.

5.3 Una limitació de AFR

Pot succeir que

$$(*) \qquad \mathbf{V} \vdash \mathbf{g}(a_1, \ldots, a_n, c) = \mathbf{h}(a_1, \ldots, a_n, c) \text{ per a tots els numerals } c$$

sense que la fórmula

$$(**) \qquad E\mathbf{g}(a_1, \ldots, a_n) = E\mathbf{h}(a_1, \ldots, a_n)$$

sigui un teorema enlloc. Si postulem que $(*)$ impliqui que $(**)$ és un teorema de $\mathbf{V}$ tindrem un formalisme que conté d'alguna manera l'aritmètica clàssica (vegeu l'article de G. Arenas i el que escriu, *"Formally recursive arithmetic and classical arithmetic"*, per aparèixer a An. Inst. Mat. Univ. Nac. Autónoma México), però aleshores, com és d'esperar, no podem demostrar constructivament la consistència d'aquest sistema ampliat.

Aquesta és la limitació a què ens referiem en la subsecció 5.1 Tenim, però: Si $(*)$ i $\mathbf{V} \vdash E\mathbf{g}(a_1, \ldots, a_n) = S(0)$, aleshores $\mathbf{V} \vdash E\mathbf{h}(a_1, \ldots, a_n) = S(0)$

L'afirmació es demostra basant-nos en el metateorema de minimització.

Notem també, anàlogament a una observació que hem fet en relació amb el metateorema de minimització, i relacionada amb ella, que *no* hem de confondre 1) amb l'afirmació "si $(*)$, aleshores $\mathbf{V} \vdash E\mathbf{g}(a_1, \ldots, a_n) = S(0) \Rightarrow E\mathbf{h}(a_1, \ldots, a_n) = S(0)$", afirmació que *no és* certa, en general, i que és equivalent a dir que $(*)$ impliqui que $(**)$ és un teorema de $\mathbf{V}$.

Aquesta limitació és font de problemes. Ho és, per exemple, quan es tracta de la tricotomia en els reals (en l'article ja citat *"Anàlisi formalment recursiva"*, per exemple). Són problemes, però, que no se'ns apareixen com insuperables, de manera que no s'ha de pensar que no es pugui arribar molt lluny en la fonamentació de les matemàtiques mitjançant formalismes recursius. Potser la bona actitud, en l'esperit del programa formalista finitari, és pensar en el fenomen de què parlem no com en un obstacle o impediment sinó com en un fet matemàtic amb el qual cal avenir-se.

Instituto de Matemáticas. Universidad Nacional Autónoma de Mexico.
Institut d'Estudis Catalans, Centre de Recerca Matemàtica.