Sobre el programa de Hilbert i l'aritmètica formalment recursiva

Francesc Tomàs

La present és continuació de l'exposició [1], publicada en aquesta mateixa revista. Procurarem que sigui, però, en bona mesura, entenedora per ella mateixa.

En [1] es recordaven els trets més importants del programa formalista finitari de Hilbert i les dificultats amb què topà. S'observava, ja sigui com a fet històric o com a conseqüència dels treballs de Gödel, que no es pot demostrar finitàriament la consistència d'una aritmètica formalitzada suficientment àmplia, si l'instrument de formalització es la lògica de primer ordre o càlcul de predicats. Es veia també com quedava motivada la noció de *formalisme recursiu* com a instrument de formalització alternatiu; mitjançant el qual es pot presentar una aritmètica finitàriament consistent més potent que l'aritmètica recursiva, l'*aritmètica formalment recursiva* (**AFR**). És a aquesta **AFR**, que està dedicada l'exposició present.

Recordem, de manera més compacta que en [1], quina és la descripció general d'aquest nou instrument de formalització:

Un *formalisme recursiu* $\mathcal{F}$ consta de:

(*a*) un llenguatge proposicional, això és, un llenguatge formal sense quantificadors;

(*b*) una col·lecció de sistemes formals basats en la lògica proposicional, anomenats els *segments* de $\mathcal{F}$, que tenen el llenguatge mencionat a *a*) com a llenguatge comú, que difereixen entre ells tan sols en els seus postulats, i la consistència de cada un dels quals es demostra finitàriament;

(*c*) la metateoria finitària de la col·lecció de segments de $\mathcal{F}$.

Recordem que un raonament (o una metateoria, o demostració, o manipulació) és finitari si no s'usa en ell el principi del tercer exclòs per a conjunts infinits. Així, si volem, segons *c*), que la metateoria o manipulació dels segments d'un formalisme recursiu $\mathcal{F}$ resti finitària, aleshores no podrem admetre, per exemple, una demostració per casos en què es tingui, com a primer cas, que certa fórmula A no sigui un teorema en cap segment de $\mathcal{F}$ i, com a segon cas, que hi hagi algun segment de $\mathcal{F}$ en el qual A és un teorema. Només podem admetre una demostració d'aquesta mena si tenim la capacitat de decidir quin dels dos casos es compleix. No seria tampoc acceptable una demostració que considerés dos casos, segons que A fos, o no, un teorema del segment **V**, no poguéssim decidir quin dels dos casos es dóna; encara que en aquest cas l'ús del tercer exclòs infinitari estaria més amagat.

La col·lecció dels segments de $\mathcal{F}$ es descriu mitjançant certs principis que tenen un caire «recursiu», si entenem aquest terme en un sentit molt ample.

Recordem, sense gaire poliment, que $\mathbf{V} : \mathcal{A}$ significa que l'afirmación $\mathcal{A}$ és veritat en el segment $\mathbf{V}$. Cal recordar també que, si bé en el llenguatge dels segments d'un formalisme recursiu $\mathcal{F}$ no hi apareixen els quantificadors del càlcul de predicats, res, però, no ens priva d'usar els quantificadors intuïtius, constructius o efectius, que denotem $\exists^*$ i $\forall^*$. És també molt important tenir present el significat del símbol $\Rrightarrow$. L'expressió

$$\mathbf{V} : \mathcal{A} \Rrightarrow \mathcal{B}$$

significa «si $\mathbf{V} : \mathcal{A}$, aleshores $\mathbf{W} : \mathcal{B}$ per algún $\mathbf{W}$ posterior a $\mathbf{V}$", on, recordem-ho, $\mathbf{W}$ és *posterior* a $\mathbf{V}$ (en símbols, $\mathbf{V} < \mathbf{W}$) si tots els postulats de $\mathbf{V}$ són postulats de $\mathbf{W}$.

Finalment, cal recordar que $\mathcal{F} : \mathcal{A}$ significa que $\mathbf{V} : \mathcal{A}$ per a cada segment $\mathbf{V}$ de $\mathcal{F}$. Les afirmacions importants d'un formalisme recursiu $\mathcal{F}$ són de la mena $\mathcal{F} : \mathcal{A}$.

Així, doncs, per a exemplificar tot això, si volem demostrar que

$$\mathcal{F} : (\vdash A) \Rrightarrow (\exists^* t)\, [\vdash B\, [t/x]]$$

hem de demostrar, finitàriament, per a cada segment $\mathbf{V}$ de $\mathcal{F}$, que

$$\mathbf{V} : (\vdash A) \Rrightarrow (\exists^* t)\, [\vdash B\, [t/x]]$$

Ara bé, això vol dir que, en el cas que $\mathbf{V} : \vdash A$ (és a dir, en el cas $\mathbf{V} \vdash A$), hem d'exhibir algun $\mathbf{W}$ tal que $\mathbf{V} < \mathbf{W}$ per al qual hem de demostrar que

$$\mathbf{W} : (\exists^* t)\, [\vdash B\, [t/x]];$$

i això últim vol dir que hem d'exhibir algun terme t per al qual hem de demostrar que

$$\mathbf{W} \vdash B\, [t/x]$$

En l'exposició precursora [1] es descriu, a la secció 4, com a prototipus de formalisme recursiu, el formalisme **ARP** (aritmètica recursiva primitiva). El formalisme **AFR** només es descriu esquemàticament [1, secció 5], al mateix temps que s'assenyala una errada d'un treball anterior. En benefici de la claredat farem la descripció de **AFR** de bell nou, de manera diferent i més detallada que a [1]; i quan sigui avinent recordarem quina és aquella errada i com ha quedat plenament superada mitjançant la present versió de **AFR**, versió que és, en aquest i altres aspectes, més satisfactòria que la versió original de [2], que és la que es tenia en la ment en redactar [1]. Tot això es farà en la secció 1. També exposarem, en les seccions següents, alguns resultats nous sobre certs «quantificadors» definits en **AFR**, representats per $\exists^0$ i $\forall^0$, i sobre la ^{0}-lògica associada. Aquestes ^{0}-nocions seran clarament útils per a comparar **AFR** amb l'aritmètica clàssica; i en aquest punt es veurà novament com la present versió de **AFR** és millor que la precedent.

1. Descripció de AFR (aritmètica formalment recursiva)

1.1. *El llenguatge.* Els símbols del llenguatge (dels segments) de **AFR** són 0, S, E, M, $=$, la coma, els parèntesis, les *variables* (representades per x, y, z, x_1, w, etc.) i els *operadors* de diferents graus positius (representats per $\mathbf{f}, \mathbf{g}, \mathbf{f}_1, \mathbf{a}$, etc.). El símbol S és un operador de grau 1 (mentre que 0, E, M, no són operadors). Entre els operadors de grau 2 és convenient tenir $+i$. Els termes del llenguatge, representats per $a, b, ..., f, g, ..., x, y, z_1, a_1$, etc., es defineixen així: 1) 0 ès un *terme*; 2) les variables són *termes*; 3) si f es operador de grau n i $a_1, ..., a_n$ són termes, aleshores les expressions $\mathbf{f}(a_1, ..., a_n)$, $\mathrm{Ef}(a_1, ..., a_{n-1})$ i $\mathrm{Mf}(a_1, ..., a_{n-1})$ son *termes*. Per tant, les expressions 0, S(0), S(S(0)), ... són termes, que s'anomenen *numerals*. Les *fórmules atòmiques* de **AFR**, són les expressions $a = b$ en las que a i b són termes. Les *fórmules* s'obtenen de les atòmiques de la manera habitual en la lògica proposicional, usant els connectius $\vee$, $\wedge$, $\neg$, $\Rightarrow$.

1.2. *Nombres i numerals.* Diem que el terme a és un **V**-*nombre*, i escrivim $a \in \mathrm{N_V}$, si podem exhibir numerals $c_1, ..., c_r$ (per r no fix) per als quals podem demostrar que

$$\mathbf{V} \vdash a = c_i \vee ... \wedge a = c_r$$

Si podem demostrar $\mathbf{V} \vdash a = c$ per a algun numeral c direm que a és un **V**-nombre *computable.* Diem que el terme f és **V**-*funció* de les variables $x_1, ..., x_n$ i escrivim $f \in \mathrm{N_V}(x_1, ..., x_n)$, si $f[a_i/x_i] \in \mathrm{N_V}$ sempre que els a_i siguin numerals. Si $f[a_i/x_i]$ és computable per a cada col·lecció de numerals a_i direm que f és *computable.*

1.3. *Els principis.* El formalisme **AFR** està definit per mitjà de tres principis, PR.1, PR.2 i PR.3. El primer és:

PR.1. El sistema formal basat en la lògica proposicional que té el llenguatge que acabem de descriure i que té, com a sols postulats, els postulats de la igualtat és un *segment* de **AFR**, el segment *inicial*, denotat **I**.

(Els postulats de la igualtat són: $a = a$, per a cada numeral a; $\neg\, a = b$, per a cada dos numerals diferents a i b; $a = b \Rightarrow b = a$, per a cada dos termes constants a i b; $a = b \wedge f = g \Rightarrow f' = g$, sempre que a, b, f, g siguin termes constants i que f' s'obtingui de f per substitució d'una presència de a per b).

El principi PR.2 ens diu que sempre que r i s siguin **V**-funcions, de $x_1, ..., x_n$, i de $x_1, ..., x_n, y, z$, respectivament, per un cert segment **V**, aleshores també és un segment el sistema formal que s'obté en afegir a **V** els postulats que defineixen un terme $\mathbf{f}(x_1, ..., x_n, y)$ com a funció obtinguda de r i s per recursió primitiva, i certs altres postulats que tendeixen a donar a $\mathrm{Ef}(x_1, ..., x_n)$ i a $\mathrm{Mf}(x_1, ..., x_n)$ els sentits de «funció que val 1 o 0 segons que existeixi, o no, un nombre y tal que $\mathbf{f}(x_1, ..., x_n, y) = 0$» i de «mínim y tal que $\mathbf{f}(x_1, ..., x_n, y) = 0$, si existeix un tal y». L'expressió formal d'aquest principi és:

PR.2. Si **U** és un segment de **AFR**, n és un enter no negatiu, $r \in \mathrm{N_U}(x_1, ..., x_n)$, $s \in \mathrm{N_U}(x_1, ..., x_n, y, z)$ i **f** és un operador de grau n + 1 nou per a **U** (això és, que no apareix en cap postulat de **U** que no sigui un postulat de la igualtat); aleshores també és un *segment* de **AFR** el que s'obté en afegir a **U** els esquemes de postulats (I)-(VII) següents, per a qualssevol numerals b_i, d, i qualsevol enter positiu m:

(I) $r[b_i/x_i] = d \Rightarrow \mathbf{f}(b_i, ..., b_n, 0) = d$
(II) $s[b_i/x_i]\ [y/c]\ [\mathbf{f}(b_1, ..., b_n, c)/z] = d \Rightarrow \mathbf{f}(b_1, ..., b_n, \mathrm{S}(c)) = d$
$(\mathrm{III})_0$ $\mathbf{f}(b_1, ..., b_n, 0) = 0 \Rightarrow \mathbf{Mf}(b_1, ..., b_n) = 0$
(III)′ $\neg\ \mathbf{f}(b_1, ..., b_n, 0) = 0 \wedge ... \wedge \neg\ \mathbf{f}(b_1, ..., b_n, c) = 0$
$\wedge\ \mathbf{f}(b_1, ..., b_n, \mathrm{S}(c)) = 0 \Rightarrow \mathbf{Mf}(b_1, ..., b_n) = \mathrm{S}(c)$
(IV) $\mathbf{f}(b_1, ..., b_n, c) = 0 \Rightarrow \mathbf{Ef}(b_1, ..., b_n) = \mathrm{S}(0)$
(V) $\mathbf{Ef}(b_1, ..., b_n) = 0 \vee \mathbf{Ef}(b_1, ..., b_n) = \mathrm{S}(0)$
(VI) $\mathbf{Mf}(b_1, ..., b_n) = c \Rightarrow \mathbf{f}(b_1, ..., b_n, c) = 0$
(VII) $\mathrm{S}^m\ (d) = \mathbf{Mf}(b_1, ..., b_n) \Rightarrow \neg\ \mathbf{f}(b_1, ..., b_n, d) = 0$

D'acord amb la condició *b*) de la descripció de la noció de formalisme recursiu, en la redacció de PR.2 s'està acceptant tàcitament que sabem com demostrar en general, de manera finitària, la consistència del sistema formal que s'obté en afegir els casos de (I)-(VII) com a nous postulats (suposada demostrada finitàriament la consistència de **U**). Aquest és, en efecte, el cas; i la demostració és senzilla. També és pot demostrar finitàriament i molt fàcilment, la consistència de l'inicial **I**.

El tercer principi, PR.3, es pot veure com un succedani en **AFR** de la regla de $\exists\vdash$eliminació del càlcul de predicats. Això és aparent en el seu enunciat, que és el següent:

PR.3. Si: 1) **U** és un segment de **AFR** i $\mathbf{g}(x_1, ..., x_n, y)$ és una **U**-funció de les x_i i y, on g no és S; 2) h_i, k_i i m_j són **U**-funcions de les variables $z_1, ..., z_q$ per a $i \equiv 1, ..., p$, $j \equiv 1, ..., n$; 3) tenim, per a qualssevol numerals $d_1, ..., d_q, c$, que $\mathbf{U} \vdash (\mathbf{g}(m_1, ..., m_n, c) = 0 \Rightarrow \mathrm{V}^p_{i\equiv 1} \neg\ h_i = k_i)\ [d_j/z_j]$; 4) s'ha demostrat finitàriament que **U** és consistent amb l'esquema

$$(\mathrm{VIII}) \qquad (\mathbf{Eg}(m_1, ..., m_n) = \mathrm{S}(0) \Rightarrow \mathrm{V}^p_{i\equiv 1} \neg\ h_i = k_i)\ [d_j/z_j]$$

(per a tots els numerals d_i); aleshores també és un *segment* de **AFR** el que s'obté d'afegir a **U**, com a nous postulats, els casos de (VIII).

(Potser no és ociós notar que la forma del segon membre de les implicacions del principi té una motivació tècnica i no és, en la pràctica, una veritable limitació).

La idea de PR.3 és que, en diferents circumstàncies, i afegint-hi les adequades col·leccions de condicions de diferents menes, es pugui satisfer la condició de consistència 4) del principi, obtenint així noves menes de segments que ens siguin d'utilitat. Vist així, PR.3 és com una font de principis particulars que no podem ni volem encabir en un sol principi general per al qual es pugui satisfer 4) d'una vegada.

1.4. *Dos metateoremes.* Suposem que + és un operador de grau dos i que en algun segment de **AFR** es tenen els teoremes que fan que $+(x, y)$ sigui una **V**-funció que té les propietats de la suma usual. Pensem que s'han demostrat, per algun procediment inductiu, tal com es fa a [1, p. 30], per exemple, que $\mathbf{V} \vdash +(a, b) = +(b, a)$ per a qualssevol numerals a i b. Suposem, però, que c i d són V-nombres que no són numerals. Per a poder estar segurs que es satisfà $\mathbf{V} \vdash +(c, d) = +(d, c)$ necessitem el següent *metateorema d'inducció*, que es demostra molt fàcilment:

Per a qualsevol segment **V** de **AFR**, si A és una fórmula de **AFR** i tenim $\mathbf{V} \vdash A[a_i/x_i]$ per a qualssevol numerals a_i, aleshores el mateix és cert sempre que els a_i siguin V-nombres.

L'altre metateorema molt important, la demostració del qual, però, és més complicada, és:

M-*metateorema.* Suposem que els esquemes (I)-(VII) de PR.2 són postulats d'un segment **V**, per a un cert $\mathbf{f}(x_i, y)$ (i certs r i s). Aleshores:

1) Per a $a_i \in N_V$ i cada numeral $S^m(0)$,

$$\mathbf{V} \vdash \mathbf{f}(a_i, S^m(0)) = 0 \Rightarrow (\mathbf{Mf}(a_i) = 0 \vee \ldots \vee \mathbf{Mf}(a_i) = S^m(0)) \wedge \mathbf{f}(a_i, \mathbf{Mf}(a_i)) = 0$$

2) Per a $a_i \in N_V$ i $c \in N_V$,

$$\mathbf{V} \vdash \mathbf{f}(a_i, c) = 0 \Rightarrow \mathbf{f}(a_i, \mathbf{Mf}(a_i)) = 0$$

3) Per a numerals a_i, si $\mathbf{V} \vdash \mathbf{f}(a_i; \mathbf{Mf}(a_i)) = 0$, aleshores $\mathbf{Mf}(a_i) \in N_V$.

(La part 3) és molt important, ja que el fet $\mathbf{V} \vdash \mathbf{f}(a_i, \mathbf{Mf}(a_i)) = 0$ pot ser inútil si no sabem que $\mathbf{Mf}(a_i)$ és un V-nombre i que, per tant, se li pot aplicar el metateorema d'inducció).

1.5. *El desenvolupament de l'anàlisi matemàtica basada en* **AFR**. A partir del segment inicial **I** de **AFR** usem PR.2 repetidament per a introduir $+(x, y)$ i $\cdot(x, y)$ (escrites $x + y$ i $x \cdot y$) com a funcions d'un segment posterior a **I**, amb el significat usual d'aquests operadors, tal com es fa a [1,4.3]; però a més a més, com en aquell lloc, introduim la funció *predecessor* $\mathbf{p}(x)$ (amb la propietat $\mathbf{p}(0) = 0$, $\mathbf{p}(S(a)) = a$), la funció *diferència no negativa* $x \dot{-} y$ (amb la propietat $a \dot{-} 0 = a$, $a \dot{-} S(b) = \mathbf{p}(a \dot{-} b)$), la funció $a(x)$ (amb la propietat $\mathbf{a}(0) = 0$, $\mathbf{a}(S(c)) = S(0)$), la funció $\mathbf{b}(x)$ (amb la propietat $\mathbf{b}(0) = S(0)$, $\mathbf{b}(S(c)) = 0$) i la funció representada com 2^x (amb la propietat $2^0 = S(0)$, $2^{S(c)} = (S(S(0))) \cdot 2^c$). Obtenim així un segment **B**, al que anomenem *bàsic.*

Introduït **B**, oblidarem definitivament tots els segments de **AFR** que no siguin posteriors a ell. Aleshores es demostra el teorema de Bolzano-Weierstrass en la forma següent:

$$\mathbf{AFR}: \{\varphi(x) \in Q'(x) \;\&\; \alpha \in Q \;\&\; \beta \in Q \;\&\; (\forall^* n)[-\alpha < \varphi(n) < \beta]\} \Rrightarrow (\exists^* \mathbf{q}(x))[\mathbf{q}(x) \in N(x) \;\&\; (\forall^* n)[\vdash \mathbf{q}(S(n)) > \mathbf{q}(n) \;\&\; \varphi(\mathbf{q}(x)) \in R(x)]]$$

on, usant les expressions auxiliars fraccionàries $a - b/c$ (en les quals a, b, c s'han de pensar, respectivament, com el «minuend», el «substraend» i el «denominador»), entenem que

$$\alpha \equiv r_1 - s_1/t_1,\ \beta \equiv r_2 - s_2/t_2,\ \varphi(x) \equiv \mathrm{f} - g/h,$$
$$\varphi(\mathbf{q}(x)) \equiv f[\mathbf{q}(x)/x] - g\,[\mathbf{q}(x)/x]/h[\mathbf{q}(x)/x],$$
$$r_i - s_i/t_i \in \mathrm{Q} \equiv r_i \in \mathrm{N}\ \ \&\ \ s_i \in \mathrm{N}\ \ \&\ \ t_i \in \mathrm{N}\ \ \&\ |\!\vdash\!| \neg\ t_i = 0,$$
$$f - g/h \in \mathrm{Q}'(x) \equiv f \in \mathrm{N}(x)\ \ \&\ \ g \in \mathrm{N}(x)\ \ \&\ \ h \in \mathrm{N}(x),$$

on l'expressió $a - b/c < d - e/f$ es defineix de la manera més evident, usant les funcions de **B**, i on, en general, si

$$\psi(x) \equiv p - q/k,$$

definim

$$\psi(x) \in \mathrm{R}(x) \equiv \psi(x) \in \mathrm{Q}'(x)\ \ \&\ \ (\mathrm{E}^*\mathbf{m}(x)\,[\mathbf{m}(x) \in \mathrm{N}(x)$$
$$\&\ \ (\forall^* n,\, r)\,[\,|\psi(\mathbf{m}(n) + r) - \psi(\mathbf{m}(n))| < 1/n]]$$

(amb la definició òbvia de $|(a - b/c) - (d - e/f)|$; i entenent que $1/n \equiv \mathrm{S}(0) - 0/n$).

Potser també cal dir que el domini de $\forall^*$ són els numerals.

Així, doncs, el teorema afirma, en llenguatge planer, el següent: per a qualsevol **V**, si $\varphi(x)$ és (en **V**) una successió afitada de racionals, aleshores, per un cert $\mathbf{W} > \mathbf{V}$ podem trobar una successió creixent d'índexs, $\mathbf{q}(x)$, tal que $\varphi(\mathbf{q}(x))$ és una successió fonamental (en **W**). És a dir, a partir de **V**, mitjançant postulacions permeses per PR.2 i PR.3, podem arribar a un **W** posterior per al qual podem exhibir uns termes $\mathbf{q}(x)$ i $\mathbf{m}(x)$ per als quals podem demostrar

$$\mathbf{q}(x) \in N_{\mathrm{W}}(x),\ (\forall^* n)[\mathbf{W} \vdash \mathbf{q}(\mathrm{S}(n)) > \mathbf{q}(n)],\ \mathbf{m}(x) \in N_{\mathrm{W}}(x),$$
$$(\forall^* n,\, r)\,[\mathbf{W} \vdash\ |\varphi(\mathbf{q}(\mathbf{m}(n) + r) - \varphi(\mathbf{q}(\mathbf{m}(n))| < 1/n]$$

La demostració, llarga i delicada, no es repetirà aquí.

Com veiem, aquesta és una versió del teorema de B.-W., que és efectiva en el sentit que precisem a continuació. Per a demostrar les afirmacions que s'acaben d'escriure s'exhibeixen el segment **W**, la successió creixent (el terme) $\mathbf{q}(x)$ i el testimoni (el terme) $\mathbf{m}(x)$, i es demostra que aquests són **W**-funcions de x, encara que, en general, no són computables. Per començar, la mateixa $\varphi(x)$ no necessita ser una tríade de funcions computables.

Els mots «efectiu» i «constructiu» estan molt gastats, en el sentit que és difícil que quan es diu que una funció es dóna efectivament, o constructivament, no es sobreentengui que es dóna computablement. Però acabem de veure de quina manera cal entendre que el teorema de B.-W. de **AFR** es autènticament efectiu, encara que les funcions que s'exhibeixen no siguin computables. Podríem dir, per no caure en paranys semàntics, que l'anàlisi matemàtica basada en **AFR** és *exhibitòria.*

Les conseqüències del teorema de B.-W. (teorema de Bolzano i d'existència de màxim) no presenten cap dificultat en la seva demostració. Al respecte es pot consultar [2], tenint en compte, però, el que es diu a la següent subsecció 1.6.

1.6. *Una errada de* [2] *i la seva superació en la present versió de* **AFR**. La present versió de **AFR** difereix de la de [2] només en el principi PR.3 (a part de mínimes diferències de notació). La diferència important és que en el PR.3 de [2] es demanen certes condicions addicionals que permeten donar una demostració finitària general de la consistència del sistema que s'obté d'afegir l'esquema de postulats (VIII) però que limiten al camp d'acció del principi. A [2] s'afirma que es pot demostrar el teorema de Bolzano-Weierstrass, però la pretesa demostració del lema básic [2, pp. 63-68] és errònia per la següent raó. A [3] es demostra el «metateorema de minimització» en la següent forma: per a numerals b_i, per a qualsevol segment **V** i qualsevol operador **h**, si $\mathbf{V} \vdash \mathrm{E}\,\mathbf{h}(b_i) = \mathrm{S}(0)$, aleshores $\mathbf{Mh}(b_i) \in \mathrm{N}_{\mathrm{V}}$ i $\mathbf{V} \vdash \mathbf{h}(b_i, \mathbf{Mh}(b_i)) = 0$; però tant a [3, p. 48] com a [2, p. 40] s'enuncia com si fos cert per a **V**-nombres b_i, en general, i en la pretesa demostració mencionada s'usa d'aquesta manera en els passos de (11) a (12) i de (19) a (20), cosa que la invalida. De fet, no sembla que en la versió de [2] es pugui demostrar el teorema de B.-W.; però en la present versió, més poderosa, sí que es pot, com ja s'ha mencionat. També és invàlida la proposició 3.13 de [2], relativa a la tricotomia en els reals, perquè s'usa la mateixa versió no justificada del metateorema de minimització, al final de la p. 56 i en la p. 57. No sabem si la proposició és certa en la present versió. Sobre la tricotomia es pot veure el final de la secció 2, més endavant. En la present versió de **AFR**, en què la col·lecció de segments és més gran, el metateorema de minimització ja no és cert (ni per a numerals). En el seu lloc tenim el M-metateorema de 1.4.

2. Definició dels quantificadors $\exists^\circ$ i $\forall^\circ$ de AFR

Introduïm uns símbols nous, $\exists^\circ$ y $\forall^\circ$. Definim les *°-fórmules* com les expressions produïdes a partir de les fórmules atòmiques de **AFR** per mitjà de $\neg, \wedge, \vee, \Rrightarrow$, $\exists^\circ$ i $\forall^\circ$, com si aquests darrers símbols fossin els quantificadors del càlcul de predicats. Les fórmules de **AFR** són, precisament, les °-fórmules en les quals no apareixen $\exists^\circ$ ni $\forall^\circ$.

Per a cada °-formula A definirem què representa l'expressió $m \in \mathrm{T}(A)$, que llegirem «m és una *traducció* de A», i quina és la seva interpretació en cada segment de **AFR** (posterior a **B**). La conveniència de tal definició no quedarà clara fins que, a continuació, definim també la noció $\vdash^{\circ}$ de *°-teorema*. Donarem la definició de $m \in \mathrm{T}(A)$ recursivament en els passos següents, en el primer dels quals les x_i son totes les variables presents en a o en b, en el segon totes les presents en m', etc.

$$
\begin{aligned}
& m \in \mathrm{T}(a = b) \equiv (\forall^* a_i)\,[\vdash (m = |a - b|)\,[a_i/x_i]] \\
& m \in \mathrm{T}(\neg A) \equiv (\exists^* m')\,[m' \in \mathrm{T}(A) \;\;\&\;\; (\forall^* a_i)[\vdash (m = \mathbf{b}(m'))\,[a_i/x_i]]] \\
& m \in \mathrm{T}(A \vee B) \equiv (\exists^* m', m'')\,[m' \in \mathrm{T}(A) \;\;\&\;\; m'' \in \mathrm{T}(B) \\
& \qquad\qquad\qquad\qquad\qquad\qquad \& \;\; (\forall^* a_i)\,[\vdash (m = m' \cdot m'')\,[a_i/x_i]]] \\
& m \in \mathrm{T}((\exists^\circ y)A) \equiv (\exists^* m')(\exists^* \mathbf{f}(x_i,y))\,[m' \in \mathrm{T}(A) \\
& \qquad\qquad\qquad\qquad \& \;\; (\forall^* a_i,b)\,[\vdash \mathbf{f}(a_i,b) = (m'[a_i/x_i]\,[b/y]) \\
& \qquad\qquad\qquad\qquad\qquad \wedge\; m[a_i/x_i] = \mathbf{b}(\mathrm{E}\mathbf{f}(a_i))]]
\end{aligned}
$$

No cal escriure les definicions corresponents a $\Rightarrow$, $\wedge$ i $\forall^\circ$, que són les òbvies. Completem la definició amb

$$\mathbf{V}: m \in \mathrm{T}(a = b) \equiv m \in \mathrm{T_V}(a = b) \equiv (\forall^* a_i)\, [\mathbf{V} \vdash (m = |a - b|)\, [a_i/x_i]]$$
$$\mathbf{V}: m \in \mathrm{T}(\neg A) \equiv m \in \mathrm{T_V}(\neg A) \equiv (\exists^* m')\, [m' \in \mathrm{T_V}(A) \;\; \& \;\; (\forall^* a_i)\, [\mathbf{V} \vdash (m = \mathbf{b}(m'))\, [a_i/x_i]]]$$

etc.

Definim ara la noció de $^\circ$-teorema:

$$\vdash^{\circ} A \equiv (\exists^* m)\, [m \in \mathrm{T}(A) \;\; \& \;\; (\forall^* a_i)\, [\vdash m[a_i/x_i] = 0]]]$$
$$\mathbf{V}: \vdash^{\circ} A \equiv \mathbf{V} \vdash^{\circ} A \equiv (\exists^* m)\, [m \in \mathrm{T_V}(A) \;\; \& \;\; (\forall^* a_i)\, [\mathbf{V} \vdash m[a_i/x_i] = 0]]]$$

on les x_i són totes les variables presents a m.

Una lectura atenta de les definicions mostra clarament com $(\exists^\circ x) A$ adquireix el significat intuïtiu d'existència no efectiva d'un b tal que $A\,[b/x]$. Per exemple, si $a \in \mathrm{N_V}(y)$, l'afirmació

$$\mathbf{V} \vdash^{\circ} (\exists^\circ y)\, [a = 0]$$

vol dir que $\mathbf{V} \vdash \mathrm{E}\mathbf{f} = \mathrm{S}(0)$ per a algun $\mathbf{f}(y)$ tal que

$$(*) \qquad (\forall^* b)\, [\mathbf{V} \vdash \mathbf{f}(b) = a\, [b/y]]$$

i, com que $\mathrm{E}\mathbf{f} = \mathrm{S}(0)$ té el contingut intuïtiu no efectiu de «existeix b tal que $\mathbf{f}(b) = 0$», (*) mostra el que afirmem.

No s'ha de pensar que la «$^\circ$-lògica» així descrita té les propietats del càlcul de predicats. Per començar, no val la regla *modus ponens* per $\vdash^{\circ}$, en general (o no sabem com demostrar-la). Ara ens podem preguntar:

Qüestió. És possible tenir $\mathbf{V} \vdash^{\circ} A$ i $\mathbf{V} \vdash^{\circ} \neg A$?

Observem que si A és $0 = 0$ això no és possible. Efectivament, en cas contrari tindríem, per certs m_1 i m_2, segons les definicions,

$$\mathbf{V} \vdash m_1 = 0, \;\; \mathbf{V} \vdash m_2 = 0, \;\; \mathbf{V} \vdash m_1 = |0 - 0|, \;\; \mathbf{V} \vdash m_2 = \mathbf{b}(|0 - 0|),$$

i això implicaria $\mathbf{V} \vdash 0 = \mathrm{S}(0)$, cosa que no succeeix perquè $\mathbf{V} \vdash \neg\, 0 = \mathrm{S}(0)$ i $\mathbf{V}$ és consistent.

Això, però, no ens permet deduir que la qüestió es resol negativament, ja que la $^\circ$-lògica no té les propietats del càlcul de predicats. D'una A tal que $\mathbf{V} \vdash^{\circ} A$ i $\mathbf{V} \vdash^{\circ} \neg A$ podríem dir que és $^\circ$-**V**-*inconsistent.* Com s'acaba de veure, la $^\circ$-**V**-inconsistència, si n'hi ha, és com una malaltia que no s'encomana, ja que hi ha fórmules, com $0 = 0$, que no són mai $^\circ$-**V**-inconsistents.

Convé observar el següent. El $^\circ$-llenguatge, encara que es provés que no hi ha

°-inconsistències, no és superior al *-llenguatge efectiu de **AFR**. Per exemple, també podríem demostrar el teorema de B.-W. en la forma

$$\begin{aligned}&\mathbf{AFR}: \varphi(x) \in Q'(x) \mathbin{\&} \alpha \in Q \mathbin{\&} \beta \in Q \mathbin{\&} (\forall^* n)\,[\vdash \alpha < \varphi(n) < \beta]\\ &\qquad \models\!\!\!> \;\vdash^{\circ} (\forall^\circ x)(\exists^\circ y_1)(\forall^\circ v)(\exists^\circ y_2)(\forall^\circ w)\,[|\psi(y_1 + w) - \varphi(v + y_2)| < 1/x],\end{aligned}$$

(on $1/x \equiv S(0) - 0/x$), però aquesta versió és més feble que la original.

Cal dir també que el °-llenguatge tot sol, sense $\exists^*$ i $\forall^*$, és insuficient per a expressar les afirmacions de l'anàlisi, del teorema de B.-W., en particular.

Però $\exists^\circ$ i $\forall^\circ$ poden ser útils per a expressar coses que no podem expressar amb el *-llenguatge. Per exemple, podem definir (usant $0 \equiv 0 - 0/S(0)$):

$$\begin{aligned}\varphi(x) \overset{\circ}{<} 0 &\equiv (\exists^\circ x)(\forall^\circ y)(\exists^\circ z)\,[0 > \varphi(y + z) + 1/x]\\ \varphi(x) \overset{\circ}{=} 0 &\equiv (\forall^\circ x)(\exists^\circ y)(\forall^\circ z)\,[|\varphi(y + z)| \leq 1/x]\\ \varphi(x) \overset{\circ}{>} 0 &\equiv (\exists^\circ x)(\forall^\circ y)(\exists^\circ z)\,[0 < \varphi(y + z) - 1/x]\end{aligned}$$

i tindríem una tricotomia en la forma

$$\mathbf{FRA}: \varphi(x) \in R(x) \models\!\!\!> \;\vdash^{\circ} \varphi(x) \overset{\circ}{<} 0 \vee \varphi(x) \overset{\circ}{=} 0 \vee \varphi(x) \overset{\circ}{>} 0,$$

mentre que no tenim una tricotomia efectiva.

El que està a la dreta de $\models\!\!\!>$, en l'afirmació anterior, significa que hi ha, per a un cert **W**, alguna traducció, m, de

$$\varphi(x) \overset{\circ}{<} 0 \quad \vee \quad \varphi(x) \overset{\circ}{=} 0 \quad \vee \quad \varphi(x) \overset{\circ}{>} 0$$

tal que $\mathbf{W} \vdash m = 0$. No és inversemblant que això pugui ser útil encara que no s'hagi demostrat la impossibilitat de tenir $\mathbf{W} \vdash \neg\, m' = 0$ per a alguna altra traducció m'.

3. AFR i l'aritmètica clàssica

En aquest tema ens serà útil la °-lògica que s'acaba de descriure. Escrivim les fórmules de l'aritmètica clàssica (A.C.) posant S(a) en lloc de l'habitual a', i posant $\exists^\circ$ i $\forall^\circ$ en lloc de $\exists$ i $\forall$. Així, cada fórmula de l'A.C. pot ser vista com una °-fórmula. Posarem A.C. $\vdash A$ per a indicar que A és un teorema de l'A.C. Es pot demostrar finitàriament:

Metateorema. Si la condició de consistència 4) de PR.3 es complís sempre, tindríem, per a cada fórmula A de l'A.C., el següent:

$$\text{si A.C.} \vdash A, \text{ aleshores } \mathbf{AFR}: \models\!\!\!> \;\vdash^{\circ} A$$

(on és clar que, en general, **AFR:** $\models\!\!\!>$ B significa **V**: $\models\!\!\!>$ B per a cada segment **V**; i això últim significa que podem exhibir un **W** > **V** per al qual podem demostrar **W** : B).

Com a conseqüència, donat que no tenim **AFR** : $\Vdash\!\!\!> \neg\, 0 = 0$, si poguéssim demostrar finitàriament que la condició 4) de PR.3 es satisfà en general, tindríem demostrat finitàriament que $\neg\, 0 = 0$ no és un teorema de l'A.C. i que aquesta és, per tant, consistent. Com que una tal demostració finitària de la consistència de A.C. no és possible o, almenys, no és d'esperar, resulta que no és tampoc possible, o d'esperar, que es pugui satisfer en general la condició 4) de PR.3. Això no implica que hagi d'existir un cas de PR.3 per al qual la consistència de l'esquema (VIII) amb el segment de partença no es pugui demostrar finitàriament.

Segons aquesta discussió podríem dir, vagament, que **AFR** ens dóna una visió superior de l'A.C., des de la qual es detecta els moments en què la consistència s'ha de controlar, que són aquells en què s'ha d'usar PR.3. De manera que podríem dir, en termes no rigurosos, que **AFR** conté la part de l'A.C. que és finitàriament consistent. És cert també que **AFR** conté més que això, ja que ens dóna la possibilitat de desenvolupar una anàlisi finitàriament consistent més potent que l'anàlisi recursiva i que és efectiva o exhibitòria.

La demostració del metateorema consisteix, amb la hipòtesi que la condició de consistència 4) de PR.3 sempre es satisfà, en demostrar que **AFR**: $\Vdash\!\!\!> \;\vdash^{\circ} A$ per a cada axioma A de A.C. i que les regles d'inferència del càlcul de predicats aplicades a A.C. són certes en la seva traducció a **AFR**. Per exemple, s'ha de demostrar, per a qualssevol fórmules A i B de A.C., que

si **AFR**: $\Vdash\!\!\!> \;\vdash^{\circ} A$ i **AFR**: $\Vdash\!\!\!> \;\vdash^{\circ} A \Rightarrow B$, aleshores **AFR**: $\Vdash\!\!\!> \;\vdash^{\circ} B$

L'essencial d'aquesta demostració ja ha estat fet a [4], on es considera la versió de **AFR** donada a [2] i no s'usen les °-nocions explícitament; però on és fàcil veure que les demostracions són adaptables al cas present. En el cas de *modus ponens*, que acabem d'escriure, volem demostrar, per a qualsevol **V**,

(a) existeix $\mathbf{W} > \mathbf{V}$ tal que $\mathbf{W} \vdash^{\circ} B$

Per a fer això sabem que

(b) existeix $\mathbf{V}_1 > \mathbf{V}$ tal que $\mathbf{V}_1 \vdash^{\circ} A$
(c) existeix $\mathbf{V}_2 > \mathbf{V}_1$ tal que $\mathbf{V}_2 \vdash^{\circ} A \Rightarrow$ B.

(b) ens diu que

$$(\forall^* a_i)[\mathbf{V}_1 \vdash m\,[a_i/x_i] = 0]$$

per a un cert $m \in \mathrm{T}(A)$; i (c) ens diu que

$$(\forall^* a_i)[\mathbf{V}_2 \vdash (\mathbf{b}(m') \cdot n)\,[a_i/x_i] = 0]$$

per a uns certs $m' \in \mathrm{T}(A)$ i $n \in \mathrm{T}(B)$, on podem suposar que les x_i són totes les variables presents a m, m', o n.

El problema és que m i m' no són el mateix terme, ni sabem que hagin de ser iguals en algun sentit. Però si la condició 4) de PR.3 sempre es complís podríem demostrar, per a algun $\mathbf{W} > \mathbf{V}_2$,

$$\text{(d)} \qquad (\forall^* a_i)[\mathbf{W} \vdash m\,[a_i/x_i] = [a_i/x_i]],$$

i aleshores tindríem

$$(\forall^* a_i)[\mathbf{W} \vdash n\,[a_i/x_i] = 0]$$

que ens dóna (a).

Un cas particular de demostració de (d), que ens dóna idea de com procedir en general, per inducció sobre la llargària d'una fórmula, és el següent. Suposem que $A \equiv (\exists^\circ y)\, C$ i que tenim $s \in \mathrm{T_U}(C)$. Suposem, per a un $\mathbf{V} > \mathbf{U}$, que

$$\begin{aligned}(\forall^* a_i, b)[\mathbf{V} \vdash\ & \mathbf{f}_1(a_i,b) = s[a_i/x_i][b/y]\\ & \wedge \mathbf{f}_2(a_i,b) = s[a_i/x_i][b/y]\\ & \wedge m_1\,[a_i/x_i] = \mathbf{b}(\mathrm{E}\mathbf{f}_1(a_i))\\ & \wedge m_2\,[a_i/x_i] = \mathbf{b}(\mathrm{E}\mathbf{f}_2(a_i))]\end{aligned}$$

Tenim, doncs, $m_1 \in \mathrm{T_V}((\exists^\circ y)C)$, $m_2 \in \mathrm{T_V}((\exists^\circ y)C)$, i voldríem demostrar que m_1 es igual a m_2, és a dir, que en algun $\mathbf{V}' > \mathbf{V}$,

$$\text{(**)} \qquad (\forall^* a_i)[\mathbf{V}' \vdash \mathrm{E}\mathbf{f}_1(a_i) = \mathrm{E}\mathbf{f}_2(a_i)]$$

Tenim clarament, per l'esquema (IV) de PR.2 corresponent a $\mathbf{f}_1$, i per hipòtesi,

$$(\forall^* a_i, b)\,[\mathbf{V} \vdash \mathrm{E}f_1(a_i) = 0 \Rightarrow \neg\, \mathbf{f}_1\,(a_i,b) = 0$$

$$\Rightarrow \neg\, \mathbf{f}_2\,(a_i,b) = 0]$$

i, per PR.3, si es complís 4), podríem postular

$$(\forall^* a_i)\,[\mathbf{V}_1 \vdash \neg\, \mathrm{E}\mathbf{f}_1(a_i) = 0 \vee \neg\, \mathrm{E}\mathbf{f}_2(a_i) = \mathrm{S}(0)],$$

equivalent, segons (V) de PR.2, a

$$(\forall^* a_i)[\mathbf{V}_1 \vdash \mathrm{E}\mathbf{f}_1(a_i) = 0 \Rightarrow \mathrm{E}\mathbf{f}_2(a_i) = 0]$$

Amb una nova utilització de PR.3 podríem obtenir (**), tal com volíem.

4. El formalisme AFRL

Anomenem *aritmètica formalment recursiva lliure* (**AFRL**) el formalisme que s'obté de **AFR** en suprimir l'exigència de consistència 4) de PR.3 (finitària o no). Aquest formalisme **AFRL** ja no és un formalisme recursiu perquè ja no exigim que la consistència de cada segment es demostri finitàriament (ni de cap altra manera). És clar, però, pel que s'ha vist al llarg d'aquesta exposició, que **AFRL** conté l'aritmètica clàssica i, a més a més, permet el desenvolupament d'una anàlisi matemàtica efectiva o exhibitòria en la qual es demostra el teorema de Bolzano-Weierstrass.

Pot ser, per tant, interessant la pregunta sobre el grau de fiabilitat de **AFRL** pel que fa a consistència (potser no finitària). Podem preguntar, per exemple, si és, en aquest aspecte, tan fiable com l'aritmètica clàssica, o com l'aritmètica de segon ordre, o si és més de fiar que les teories de conjunts formals.

Acabarem l'exposició recordant que el programa finitari de Hilbert, que és el motor de la recerca que es ressenya aquí, ha estat tema de treballs recents. Al respecte es pot veure [5], [6], [7], [8].

Referències

[1] F. Tomàs. Una fusió dels programes recursivista i formalista finitari: la noció de formalisme recursiu com a substitutiva del càlcul de predicats. *Butlletí de la Soc. Catalana de Mat.* n.° 2 (1988) pp. 7-36.

[2] Id. Anàlisi formalment recursiva. *Pub. Mat. UAB* 30 (1986), pp. 35-75.

[3] Id. Aritmètica i anàlisi formalment recursives. *Pub. Mat. UAB* 28 (1984), pp. 19-78.

[4] G. Arenas & F. Tomàs. Formally recursive arithmetic and classical arithmetic. *An. Inst. Mat. Univ. Nac. Autónoma México* 26 (1986), pp. 1-19.

[5] W. Sieg. Hilbert's program sixty years later. *The J. of Symb. Logic* 53 (1988), pp. 338-348.

[6] S. G. Simpson. Partial realizations of Hilbert's program. *The J. of Symb. Logic* 53, pp. 349-363.

[7] S. Feferman. Hilbert's program relativized: proof theoretical and foundational realizations. *The J. of Symb. Logic* 53, pp. 364-384.

[8] R. K. Meyer & I. Urbas. Conservative extension in relevant arithmetic. *Zeitschr. f. Math. Logik und Grundl. der Math.* 32 (1986), pp. 45-50.

Instituto de Matemáticas UNAM