Bevezetés a matematikai logikába

E. Szabó László

MTA-ELTE Elméleti Fizika Kutatócsoport

Tudománytörténet és Tudományfilozófia Tanszék

E-mail: leszabo@hps.elte.hu

http://hps.elte.hu/leszabo

2007. december 6.

Tartalomjegyzék

1. Mi a logika?

Tudományszociológiai értelemben a logika a matematika egyik ága ÉS a filozófia egyik ága. (A világ nagy egyetemein pl. matematika és filozófia tanszékeken is szokás logikával foglalkozni.)

Egy logika általában a következőkből áll:

- Formális nyelv
- deduktív (következtetési) rendszer
- modell-elméleti szemantika (mi mit jelent, mi mikor igaz vagy hamis, stb.)

Ezek tipikusan matematikai fogalmak.

Filozófiai értelemben—azt szokás mondani—a logika a helyes gondolkodás/következtetés tudománya. A következtetés episztemikus (a megismeréssel összefüggő) mentális aktivitás. Milyen filozófiai relevanciája van tehát a logika matematikai aspektusainak? Szokásos válaszok:

- a logika a helyes gondolkodás mélystruktúrája
- a természetes nyelvet, elégtelenségei miatt, egy formalizált nyelvvel és a formalizált következtetési szabályokkal kell helyettesíteni

- a logika a természetes nyelv matematikai modellje

Az igazi kérdés tehát az, hogy

2. Mi teszi a logika következtetési szabályait „helyessé”?

Alapvetően az IGAZSÁG-MEGŐRZŐ TULAJDONSÁGA, vagyis, hogy igaz premisszákból igaz konklúziókra vezetnek.

Bár áttételesen beépül a racionális gondolkodás és érvelés társadalmilag/történetileg kialakult normáiba, mindenekelőtt a nyelv használatával összefüggő társadalmi normákba, s ezért úgy tűnhet, hogy semmiféle tapasztalásra nincs szükség egy következtetés helyességének megítéléséhez, ez a tulajdonság alapvetően EMPIRIKUSAN tesztelhető.

$$\begin{array}{ccc} \text{ha a premisszák igazak} & \Rightarrow & \text{a következtetések igazak} \\ \updownarrow & & \updownarrow \\ \text{világ tényei} & & \text{világ tényei} \end{array}$$

A logikai következtetés helyességének kérdése ott tűnik problematikusnak, ahol ezt a legkevésbé várnánk: A MATEMATIKÁBAN! Mi teszi helyessé azt a következtetést, hogy

ha az Euklideszi axiómák igazak $\Rightarrow$ igaz, hogy $a^2 + b^2 = c^2$

Honnan tudjuk ugyanis, hogy $a^2 + b^2 = c^2$ igaz?!

3. Mi tesz egy matematikai állítást igazzá?

3.1. Realizmus, platonizmus, intuicionizmus

A REALIZMUS szerint (pl. J. S. Mill) *a matematikai állítások akkor igazak, ha megfelelnek a minket körülvevő fizikai valóságnak.* Más szóval, a matematika empirikus tudomány: a matematikai állítások a fizikai világ legáltalánosabb tulajdonságait fejezik ki. E felfogás fontos szerepet töltött be a matematika történetében, manapság azonban senki sem gondolja komolyan, hiszen a matematika fogalmai nincsenek közvetlen megfelelésben a valóság elemeivel, például a végtelen fogalmának semmi sem felel meg a külső (a matematikán kívüli) világban.

A MATEMATIKAI PLATONIZMUS a matematika klasszikus fogalmainak *önálló létezést tulajdonít*, függetlenül attól, gondoljuk-e azokat vagy nem, s úgy véli, a matematikai állítások igazságát pusztán e fogalmak analízisével, logikai úton fedezhetjük fel.

AZ INTUICIONISTÁK tagadják a matematikai objektumoknak – az értelemszerűen véges – *konstrukciójuktól független* létezését, ám helyette „saját istenük" (Curry kifejezése[1]), az Intuíció létezésében hisznek, vagyis valami olyasmiben, ami az egyetemes emberi

[1]Haskell B. Curry: *Outlines of a Formalist Philosophy of Mathematics*, North-Holand, Amsterdam 1951.

értelem számára *a priori adott*, garantálva ezzel a matematika *objektivitását és használhatóságát.*

Realisták, platonisták és intuicionisták mind hisznek azonban abban, hogy a matematikai állításoknak *jelentésük* van, s ha – a Hilbert-programot követve – formalizáljuk is a matematika nyelvezetét, azt azért tesszük, hogy e jelentést precízebben és tömörebben adhassuk vissza.

3.2. A matematika formalista felfogása

szerint az igazság ezzel szemben az, hogy *a matematikai objektumoknak nincs jelentése.* A matematika a formális rendszerek tudománya: *Jeleket* definiálunk és *szabályokat*, melyek alapján e jeleket kombinálhatjuk. Ahogy Hilbert mondta „A matematika egy játék, melyet a papírlapra írt, jelentés nélküli szimbólumokkal játszunk, egyszerű szabályok szerint." „Pont, egyenes és sík helyett folyamatosan mondhatnánk, asztalt, széket és söröskorsót" – mondta egy másik alkalommal az euklideszi geometriára utalva.

A matematikának semmi köze nincs a végtelen metafizikai fogalmához, és közömbös a térre, időre, valószínűségre vagy a folytonosságra vonatkozó intuíciónkkal szemben. A matematika nem produkál, és nem old meg Zénón-paradoxonokat! „Leírhatok egy jelet, mondjuk α-t, és elnevezhetem az egész számok kardinalitásának. Aztán rögzíthetem a rá vonatkozó manipulációs szabályokat",

mondja Dieudonné.[2] Az egész finitista próbálkozás felesleges. Ha a papírra azt írom $10^{10^{10}}$, ez éppúgy csak egy jel, amellyel manipulálhatok, mint bármelyik más. A matematika jelenlegi gyakorlata azt mutatja, hogy minél precízebben látjuk be valamely matematikai állítás igazságát, annál nyilvánvalóbb, hogy őt kizárólag az teszi igazzá, hogy levezethető az rendszer axiómáiból a rendszerben érvényes következtetési szabályok segítségével – függetlenül attól, hogy egyébként milyen filozófiai nézeteket vall egy matematikus. Jól jellemzi a helyzetet Jean Dieudonné-nek, a francia Bourbaki csoport egyik vezéralakjának sokat idézett mondása : „In everyday life, we speak as Platonists, treating the objects of our study as real things that exist independently of human thought. If challenged on this, however, we retreat to some sort of formalism, arguing that in fact we are just pushing symbols around without making any metaphysical claims. Most of all, however, we want to do mathematics rather than argue about what it actually is. We're content to leave that to the philosophers."

Tehát,

1. A formalizmus lényege, hogy egy állítás bizonyításának/levezetésének létezése nem más, mint a szóban forgó állítás *igazságfeltétele*.

2. Az axiómák sem azért „igazak", mert valamiféle referenciájuk

[2]Lásd Arend Heyting: *Intuitionism: an Introduction*, North-Holland, Amsterdam 1956.

van a valóságos (vagy valamiféle platóni) világra, hanem mert (triviálisan) levezethetők (tudniillik az axiómákból), más szóval definíció szerint igazak.

3. A matematikában az igazság fogalma általában értelmetlen, csak egy adott axiómarendszerre nézve értelmes (ahol az axiómarendszerbe a következtetési szabályokat is beleértjük). Annak a kijelentésnek, hogy „a háromszög szögeinek összege 180 fok" az igazságáról nincs értelme anélkül beszélnünk, hogy ne specifikálnánk, hogy melyik axiómarendszerben (tehát melyik geometriában) van értve.

4. A matematika története ebben a vonatkozásban nem egységes. A matematika reális interpretációja például szinte kihalt a nem-euklideszi geometriák megszületése után. Korábbi korokban elfogadottnak tekintett bizonyításokat ma nem tekintünk elfogadható, precíz formális bizonyításnak. Mint – kissé sarkítva – Russell írja Boole *Laws of Thought*-ja (1854) volt „az első könyv, amelyet matematikáról írtak".

3.3. Matematikai elmélet mint formális rendszer

Általában tehát egy matematikai elmélet egy formális nyelv, amely szimbólumokat tartalmaz, szintaktikai szabályokat arra nézve, hogy ezekből a szimbólumokból hogyan lehet összetettebb un. formulákat és formula-sorozatokat előállítani, és logikai szabályokat,

amelyek következtetési szabályokat mondanak ki bizonyos formulák „átalakítására”, egyikről a másikra való „áttérésre”.

Példa (Paul Lorenzen)

Jelek: Olyan stringek, amelyek két betűből állnak, a és b.

Axiómák:

$$L = \begin{cases} a \\ X \vdash Xb \quad \text{(Rule 1)} \\ X \vdash aXa \quad \text{(Rule 2)} \end{cases}$$

Például,

Tétel: $aababb$

Bizonyítás:

$$\underset{}{a} \underset{(1)}{\vdash} \underset{}{ab} \underset{(2)}{\vdash} \underset{}{aaba} \underset{(1)}{\vdash} \underset{}{aabab} \underset{(1)}{\vdash} \underset{}{aababb}$$

(lásd komputer program!)

3.4. Ha a matematika csak jelentés nélküli szimbólumokból áll, hogyan lehet, hogy alkalmazható a valóságra?

E kérdés tévedésen nyugszik: a matematika nem „alkalmazható” a valóságra. A *fizikai elméletek,* azok valóban referálnak a valóság elemeire!

Egy P fizikai elmélet – ideális esetben – két komponensből áll: $P = L + S$, ahol L egy formális rendszer, melyben általában *felhasználunk* korábban, a matematikában és a logikában konstruált formális rendszereket, S pedig egy, a formális rendszerből az empirikus világba mutató szemantika. Például, bizonyos fizikai elméletben a tér-koordinátáknak mint fizikai mennyiségeknek a leírásában az euklideszi geometria alkalmazva van. Ennek a ténynek azonban semmi köze sincs az olyan matematikai állítások igazságához, mint $a^2 + b^2 = c^2$: egy ilyen állítás egyszerűen azért igaz, mert levezethető a szóban forgó rendszer axiómáiból.

Természetesen, érdekes filozófiai kérdés, hogy hogyan működik az S szemantika. Ennek a kérdésnek azonban semmi köze sincs a matematikai problémákhoz! Jól látszik ez, ha arra gondolunk, hogy a fizikai tér(idő)re vonatkozó új kísérleti tény megváltoztathatja a fizikai elméletet, például az egész euklideszi geometriát egy másikkal váltjuk fel – legalábbis a relativitáselmélet történetének szokásos értelmezése szerint –, míg ez a változás teljesen érintetlenül hagyja magát az euklideszi geometriát.

A P fizikai elmélet egy A mondata két különböző értelemben lehet igaz:

Igazság$_1$: A egy tétele L-nek, vagyis levezethető L-ben (ami egy matematikai igazság az L formális rendszeren belül, vagyis az L formális rendszerre vonatkozó tény).

Igazság$_2$: Az S szemantika szerint, A a világ egy (az elmélet

által leírt rendszerre vonatkozó) empirikus tényére referál.

Például, „A ponttöltés elektrosztatikus tere $\frac{kQ}{r^2}$” mondat a Maxwell-féle elektrodinamika egy tétele – levezethetjük a Maxwell-egyenletekből –, másfelől, a Maxwell-elmélet szimbólumait az empirikus világgal összekötő szemantika szerint, a ponttöltésre vonatkozó tényt fejez ki.

Az elmélet célja, hogy e kétféle igazságfogalom minél nagyobb mértékben egybeessen. A két igazságfogalom egybeesése azonban empirikus kérdés: Az Igazság_1 és az Igazság_2 egymástól teljesen függetlenek, abban az értelemben, hogy az egyikből nem következik automatikusan a másik. Sőt, tegyük fel, hogy Γ igaz_2 mondatoknak egy halmaza, továbbá, hogy A levezethető Γ-ból az L rendszerben. Nem teljesül automatikusan (ha tetszik, *a priori*), hogy A egy igaz_2 mondat. Ez ugyanis egy empirikus kérdés. Ha az, akkor ez a tény megerősítheti az egész $P = L + S$ fizikai elméletet, beleértve az L-beli következtetési szabályok P-ben való alkalmazhatóságát is. Tehát, 1) a logika szabályait éppúgy mi találjuk ki, mint a matematika más részeit, 2) a logika szabályainak alkalmazhatósága a világ leírására szolgáló elméletekben, egy empirikus kérdés, amely 3) elválaszthatatlan a fizikai elmélet többi részének empirikus konfirmációjától. Következésképpen az az állítás, hogy a „logika a helyes következtetés tudománya” egyszerűen értelmetlen.

4. Meta-matematika

A meta-matematika a matematiká*ról*, illetve a matematika egy elméleté*ről* szóló elmélet. Minthogy egy matematikai elmélet nem szól semmiről, a benne szereplő szimbólumoknak nincs abban az értelemben jelentése, hogy referálnának valamire a valóságban, így a meta-matematikai elmélet nem lehet matematikai elmélet. A meta-matematikai elmélet valójában egy fizikai elmélet (abban az általános értelemben, ahogyan azt definiáltuk):

Meta-matematikai elmélet		Tárgy-elmélet, pl. aritmetika
(M, S)	$\overset{S}{\Longleftrightarrow}$	L

Tehát egy meta-matematikai elmélete az L formális rendszernek azt jelenti (azt kell[ene] jelentenie), hogy adott egy másik formális rendszer M és egy szemantika S, ami M-et és L-et összeköti. Például olyan mondatokat tudunk mondani M-ben, mint „az A formula L-ben nem bizonyítható", amely az L egy tulajdonságát hivatott állítani. Jelöljük az egyszerűség kedvéért ezt a mondatot $nb(A)$-val. Az ilyen és hasonló mondatoknak van egy Igazság$_2$ értelemben vett igazsága az (M, S)-ben. Vagyis egy M-beli formula akkor igaz$_2^M$, ha az S szemantika értelmében ő egy olyan állítás L-ről, amely tényszerűen fennáll L-re. Például, $nb(A)$ akkor igaz$_2^M$,

ha nem létezik A-nak bizonyítása L-ben, más szóval, ha nem igaz, hogy A igaz$_1^L$.

Azonban, *mint minden más fizikai elmélet esetében* Igazság$_2^M$ semmiből nem vezethető le. Még egyszer, ugyanúgy, ahogyan semmiből nem lehet pl. levezetni, hogy a Maxwell-egyenletek Coulomb-mező megoldása valóban azonos a ponttöltés körüli mezővel. Mert ez empirikus kérdés. Ezt majd szemelőt kell tartanunk az olyan tételek értékelésekor, mint a Turing-gépek megállási problémája, vagy a Gödel nem-teljességi tétel.

5. Elsőrendű formális nyelv

5.1. Ábécéje

- individuum változók halmaza: $x_1, x_2, x_3, \ldots$
- individuum konstansok (esetleg nincs): $a_1, a_2, a_3, \ldots$
- függvény-jelek (esetleg nincs): f_i^n
- egy- vagy többváltozós predikátum-jelek (esetleg nincs): P_i^n
- két logikai konnektív: $\neg$ (nem) $\rightarrow$ (ha...akkor, implikálja)
- egy kvantifikátor: $\forall$ (minden, univerzális kvantor)

- mellékszimbólumok: (, , és) (a bal zárójel, a vessző és a jobb zárójel)

Megjegyzés

- A „nem (negáció)", „ha...akkor (implikáció)", valamint „minden" szavak csupán a szimbólumok elnevezései (matematikai terminusai), nem szabad e szimbólumokra úgy gondolni mint amiknek ilyen *jelentése* van. Ezzel szemben a „halmaz" szó nem halmazelméleti terminusként van használva (hiszen még nincs halmazeléletünk!), hanem abban a hétköznapi értelemben mint szimbólumoknak a sokasága. Éppen ezért, ezen a ponton, kerüljük az olyan állításokat, mint hogy „megszámlálhatóan végtelen individuum változónk van", stb.

- „Elsőrendű" arra utal, hogy van benne kvantifikálás (nem nulladrendű) viszont csak individuum változókra vonatkoznak (nincsenek predikátum változók és azokra történő kvantifikálás, stb.)

- A függvény-jelekre nem szabad itt úgy gondolnunk, mint (a naiv halmazelméletben, más szóval, korábbi tanulmányaikban megszokott) „függvényre", vagyis „hozzárendelésre". Csak egy jel, egy szintaktikai egység, melynek segítségével lehet olyat írni, hogy $f^n\,(t_1, t_2, \ldots t_n)$.

5.2. Terminus (term)

A *terminus* fogalmát a következő definícióval adjuk meg:

1. az individuum változók és az individuum konstansok terminusok.

2. Ha f^n egy függvény-jel, és $t_1, t_2, \ldots t_n$ terminusok, akkor $f^n(t_1, t_2, \ldots t_n)$ is terminus.

3. Más nincs.

5.3. Helyesen képzett formula (well-formed formula, wf)

(a) Ha $t_1, t_2, \ldots t_n$ terminusok, akkor $P^n(t_1, t_2, \ldots t_n)$ egy wf. (Az ilyet atomi formulának hívjuk.)

(b) Ha ϕ, ψ tetszőleges két wf, akkor $(\phi \rightarrow \psi)$ is és $\neg\psi$ is az.

(c) Ha x egy individuum változó és ϕ egy wf, akkor $\forall x\phi$ is wf.

(d) Más nincs.

Rövidítések

A következő *rövidítéseket* definiáljuk:

$\phi \vee \psi$ (vagy) arra, hogy $(\neg\phi \rightarrow \psi)$

$\phi \wedge \psi$ (és) arra, hogy $\neg(\phi \rightarrow \neg\psi)$

$\phi \leftrightarrow \psi$ (akkor és csak akkor) arra, hogy $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$

$\exists x\phi$ (létezik, egzisztenciális kvantor) arra, hogy $\neg(\forall x\neg\phi)$

Megjegyzés

A „vagy (diszjunkció)”, „és (konjunkció)”, stb. elnevezések is csupán matematikai szakkifejezések. Nem kell hozzájuk a hétköznapi nyelvhasználat szerinti jelentést társítanunk.

HF

Mutassuk meg, hogy a $\{\neg, \rightarrow\}$ konnektívek helyett használhatnánk a $\{\neg, \wedge\}$ vagy $\{\neg, \vee\}$ párokat is a rendszer definíciójában! Hogy pl. $\phi \wedge \psi$ értelmezhető úgy mint $\neg(\neg\phi \vee \neg\psi)$ rövidítése (magát a formulát De Morgan-azonosságnak hívjuk), etc. Hasonlóképpen, $\forall$ helyett kezdhettük volna $\exists$-kel.

Kötött és szabad változó

Egy változót *kötött változónak* nevezünk, ha egy kvantifikátor vonatkozik rá. Egyébként *szabad változónak* nevezzük.

Például:

- A $\exists x P(x, y)$ formulában (röviden formulának fogjuk nevezni a wf-t) x kétszer kötött változóként van jelen, y szabad.

- A $\forall x \forall y(P(x, y) \rightarrow Q(y))$ formulában x és y minden előfordulása kötött. A $\forall x$ kvantifikálás hatóköre a $\forall y(P(x, y) \rightarrow Q(y))$ részformula. A $\forall y$ hatóköre a $P(x, y) \rightarrow Q(y)$ részformula.

- A $\forall x\,(P(x, y) \rightarrow \forall y Q(y))$ formulában az x kétszer kötött, az y egyszer szabad és két helyen kötött.

Egy ϕ formulában a t *terminus szabad az x változóra nézve*, ha x-nek nincsen ϕ-ben olyan szabad előfodulása, amely beleesik valamely t-ben előforduló y változóra vonatkozó $\forall y$ kvantifikáció hatókörébe. Más szóval, t terminust büntetlenül behelyettesíthetjük x minden ϕ-beli szabad előfordulásába, anélkül hogy összetütközésbe kerülnénk a ϕ-ben előforduló kvantifikációkkal (ellenkező esetben ugyanis erősen megváltoztatná a formula „értelmét"). Tekintsük a

$$\forall x P(x, y) \rightarrow \forall z Q(z, y)$$

formulát. Ebben a formulában például az $f^2(x, v)$ terminus nem szabad y változóra nézve. Azért nem, mert y-nak van szabad előfordulása egy $\forall x$ kvantifikáció hatókörében, miközben $f^2(x, v)$-ben előfordul x (tehát ha $f^2(x, v)$-t behelyettesítenénk y helyére, azzal egy újabb x-et hoznánk be a kvantifikáció alá) . Ezzel szemben például $g^2(y, z)$ szabad x-re nézve, vagy y szabad x-re nézve.

Mondat

Egy formulát *mondatnak* (vagy *zárt* formulának) nevezünk, ha nem tartalmaz szabad változót.

Prenex formátum

Egy formulát *prenex formátumúnak* mondunk, ha a következő alakú:

$$(K_1 x_1)(K_2 x_2) \ldots (K_n x_n)\, \phi$$

ahol minden K_i vagy $\forall$ vagy $\exists$, ϕ pedig egy olyan formula, amelyben nincs kvantifikáció. (Az olyan formulát, amelyben egyáltalán nincs kvantifikálás prenex formátumúnak tekintjük.)

6. A predikátum kalkulus (PC)

6.1. A PC axiómái és a következtetési szabályok

A PC egy, a fenti értelemben vett formális nyelv +

Axiómák (Axióma sémák)

A következőkben, ϕ, ψ, χ formulák, $x, y, y_1, y_2, \ldots y_n, \ldots$ változók, és jelölje $\phi(y)$ az a formulát, melyet úgy kapunk, hogy a $\phi(x)$ formulában az x változót, annak minden szabad előfordulása esetében y-nal helyettesítjük.

(PC1) $(\phi \to (\psi \to \phi))$

(PC2) $((\phi \to (\psi \to \chi)) \to (\phi \to \psi) \to (\phi \to \chi))$

(PC3) $((\neg\phi \to \neg\psi) \to (\psi \to \phi))$

(PC4) $(\forall x\,(\phi \to \psi) \to (\phi \to \forall x\psi))$ ha x nem fordul elő szabadon ϕ-ben.

(PC5) $(\forall x\phi \to \phi)$ ha x nem fordul elő szabadon ϕ-ben.

(PC6) $(\forall x\phi(x) \to \phi(t))$ feltéve, hogy a t terminus szabad x-re nézve $\phi(x)$-ben.

Következtetési szabályok

(MP) ϕ-ből és $(\phi \to \psi)$-ből következik ψ (Modus Ponens)

(G) ϕ-ből következik $\forall x\phi$ (Generalizáció)

Megjegyzés

- Az axiómák tehát egyszerűen a nyelv kiválasztott formulái. („Alapigazságok”, stb. csak verbális dekoráció).

- Egy formális nyelv + néhány axióma + a következtetési szabályok együttesét általában *formális rendszernek* hívjuk.

PC egy tétele

Ha a PC egy ϕ formulája véges számú lépésben levezethető az axiómákból a következtetési szabályok alkalmazásával, akkor a ϕ-t *tételnek* nevezzük és azt írjuk, hogy $\vdash \phi$.

Bizonyítás

Egy *bizonyítás* formuláknak egy (véges) sorozata, úgy, hogy mindegyik formula vagy axióma, vagy a sorozatban szereplő korábbi formulából van levezetve a következtetési szabályok valamelyikének alkalmazásával. A sorozat utolsó formulája nyilvánvalóan egy tétel. (Tulajdonképpen a sorozat minden formulája egy tétel).

$\Sigma \vdash \phi$

Gyakran extra axiómákat adunk a rendszerhez és a bővebb rendszerben konstruálunk bizonyításokat. Ha Σ ilyen extra axiómák halmaza, akkor azt írjuk, hogy $\Sigma \vdash \phi$, ha ϕ levezethető abban a bővebb rendszerben, melyet úgy kapunk, hogy a Σ-ba tartozó formulákat mint axiómákat hozzáadjuk az eredeti PC axiómákhoz.

PC egy kiterjesztése

Azt a formális rendszert, melyet PC-ből úgy nyerünk, hogy a PC axiómáit egy Σ formula halmazzal bővítjük, PC PC(Σ) kiterjesztésének nevezzük.

Konzisztencia

Formulák egy Σ halmazáról azt mondjuk, hogy *konzisztens*, ha

nem létezik olyan ϕ formula, melyre egyszerre fennállna, hogy $\Sigma \vdash \phi$ és $\Sigma \vdash \neg\phi$.

Bizonyítottan ekvivalens formulák

Két ϕ és ψ formula *bizonyítottan ekvivalens*, ha $\vdash (\phi \leftrightarrow \psi)$.

Kis kitérő: *Kijelentéskalkulus*

Alphabet of symbols:

$\sim, \supset, (,), p, q, r$, etc.

Well-formed formulas:

1. p, q, r, etc. are wfs.
2. If A, B are wfs. then $(\sim A)$, $(A \supset B)$, are wfs.
3. All wfs. are generated by 1. and 2.

Axiom schemes:

(SC1) $A \supset (B \supset A)$

(SC2) $(A \supset (B \supset C) \supset ((A \supset B) \supset (A \supset C)))$

(SC3) $(((\sim A) \supset (\sim B) \supset (B \supset A)))$

Modus Ponens:

(MP) A and $(A \supset B)$ implies B

A kijelentéskalkulus konzisztenciájának „bizonyítása”

Definition:

A *coloring* of SC is a function v whose domain is the set of wfs. of SC and whose range is the set $\{red, blue\}$ such that, for any wfs. A, B of SC,

(i) $v(A) \neq v(\sim A)$

(ii) $v(A \supset B) = blue$ if and only if $v(A) = red$ and $v(B) = blue$

Definition:

A wfs. A is *stably red* if for every coloring v, $v(A) = red$.

Proposition 1:

For every formula A, if A is a theorem of SC then A is stably red.

Proof:

Let A be a theorem. The proof is by induction on the number n of wfs. of SC in a sequence of wfs. which constitutes a proof of A in SC.

$n = 1$ A is an axiom. One can easily verify that every axiom of SC is stably red.

$n > 1$ Induction hypothesis: all theorems of SC which have proofs in fewer than n steps are stably red.

Assume that the proof of A contains n wfs. Now, either A is an axiom, in which case it is stably red, or A follows by (MP) from previous wfs. in the proof. These two wfs. must have the form B and $(B \supset A)$. But, since B and $(B \supset A)$ are stably red, it follows from (ii) that A is stably red.

Proposition 2:

SC is consistent.

Proof:

As is known (nemsokára be fogjuk bizonyítani!), one can easily proof that if both X and $\sim X$ are theorems in SC then arbitrary formula is a theorem. Consequently, if there exists at least one formula in SC which is not a theorem, then SC is consistent. By virtue of Proposition 1 one has to show that there is a formula Y in SC which is not stably red, that is, there is a coloring v such that $v(Y) = blue$. Let Y be $\sim p \supset q$. Taking into account (i) and (ii), $v(Y)$ is determined by $v(p)$ and $v(q)$. Since $v(Y) = blue$ whenever $v(p) = blue$ and $v(q) = blue$, Y cannot be a theorem of SC.

Formális (kétértékű) értékelés (szemantika)

Igazságérték

Igazságérték egy olyan függvény, amelynek értelmezési tartománya a SC formálinak halmaza, értékkészlete pedig az $\{Igaz, Hamis\}$ halmaz, és az alábbi tulajdonságokat elégíti ki: A PC tetszőleges két A, B formulájára

(i) $v(A) \neq v(\sim A)$

(ii) $v(A \supset B) = Hamis$ akkor és csak akkor ha $v(A) = Igaz$ és $v(B) = Hamis$

Taulológia

Az A formulát tautológiának nevezzük, ha tetszőleges v igazságértékfüggvényre teljesül, hogy $v(A) = Igaz$.

A fenti tételekből következik, hogy az SC minden axiómája ta-

utológia, és SC minden tétele tautológia.

6.2. Elemi tételek

1. Tétel. *Tetszőleges ϕ formulára $\phi \to \phi$.*

Bizonyítás

1. $\phi \to ((\phi \to \phi) \to \phi)$ [(PC1)-ből]
2. $(\phi \to ((\phi \to \phi) \to \phi)) \quad \to \quad (\phi \to (\phi \to \phi)) \quad \to \quad (\phi \to \phi)$ [(PC2)-ből]
3. $(\phi \to (\phi \to \phi)) \to (\phi \to \phi)$ [1. és 2. alapján (MP)-ből]
4. $\phi \to (\phi \to \phi)$ [(PC1)-ből]
5. $\phi \to \phi$ [4. és 3. alapján (MP)-vel]

2. Tétel (Szintaktikai kompaktság). *Legyen Σ formulák egy halmaza. $\Sigma \vdash \phi$, akkor és csak akkor, ha Σ valamely véges Σ' részére $\Sigma' \vdash \phi$.*

Bizonyítás

A tétel triviális következménye annak a ténynek, hogy minden bizonyítás formulák egy *véges* sorozata.

3. Tétel. *Ha a Σ formulahalmaz inkonzisztens (nem konzisztens), akkor tetszőleges formula levezethető belőle, tehát $\Sigma \vdash \phi$ minden ϕ-re.*

Bizonyítás

Feltevésünk szerint tehát van olyan ψ formula, hogy $\Sigma \vdash \psi$ és ezzel együtt $\Sigma \vdash \neg\psi$. Legyen ϕ tetszőleges. Most megadjuk ϕ egy levezetését Σ-ból:

(1) $\neg\psi$ [feltétel]
(2) $\neg\psi \to (\neg\phi \to \neg\psi)$ [(PC1)]
(3) $\neg\phi \to \neg\psi$ [(1), (2), (MP)]
(4) $(\neg\phi \to \neg\psi) \to (\psi \to \phi)$ [(PC3)]
(5) $\psi \to \phi$ [(3), (4), (MP)]
(6) ψ [feltétel]
(7) ϕ [(5), (6), (MP)]

4. Tétel (Dedukciótétel). $\Sigma \cup \{\phi\} \vdash \psi$, *és* ψ *levezetése nem tartalmazza (G) alkalmazását olyan* x *változóra nézve, amelyik szabadon fordul elő* ϕ*-ben, akkor* $\Sigma \vdash \phi \to \psi$.

Bizonyítás

Ha $\Sigma \cup \{\phi\} \vdash \psi$, akkor létezik olyan

$$\chi_1, \chi_2, \ldots \chi_k, \ldots \chi_n$$

formulasorozat, amelyik ψ bizonyítása. Teljes indukcióval megmutatjuk, hogy a tétel a bizonyításban szereplő minden χ_k formulára igaz, tehát igaz χ_n-re (azaz ψ-re) is.

Tekintsük χ_1-et. χ_1 vagy logikai axióma, vagy eleme Σ-nak, vagy azonos ϕ-vel. Az első két esetben (PC1)-ből és (MP)-ből

kapjuk, hogy $\Sigma \vdash \phi \to \chi_1$. Ha χ_1 azonos ϕ-vel, akkor az 1. tételből triviálisan következik. Ezzel beláttuk, hogy a tétel igaz χ_1-re.

(Indukciós feltevés) Állításunk igaz minden χ_i-re, ha $i < k$.

Ennek alapján megmutatjuk, hogy igaz χ_k-ra. Három lehetőség van:

1. χ_k logikai axióma, vagy eleme $\Sigma \cup \{\phi\}$-nek. Ekkor ugyanúgy bizonyítunk, mint a χ_1 esetében.

2. χ_k-t az (MP) alkalmazásával kaptuk valamely korábbi χ_i és $\chi_i \to \chi_k$ formulák alapján. Ekkor a következőképpen bizonyítunk:
   $\phi \to \chi_i$ [(Indukciós feltevés)]
   $\phi \to (\chi_i \to \chi_k)$ [(Indukciós feltevés)]
   $(\phi \to (\chi_i \to \chi_k)) \to ((\phi \to \chi_i) \to (\phi \to \chi_k))$ [(PC2)-ből]
   $(\phi \to \chi_i) \to (\phi \to \chi_k)$ [(MP)-ből]
   $\phi \to \chi_k$ [(MP)-ből]

3. χ_k-t az (G) alkalmazásával kaptuk valamely korábbi χ_i-ből valamely y változóra vett generalizációval. Mivel a levezetés nem tartalmazza (G) alkalmazását olyan x változóra nézve, amelyik szabadon fordul elő ϕ-ben, y nem jelenthet meg ϕ-ben szabad változóként, hiszen a generalizációban alkalmaztuk. Tehát
   $\phi \to \chi_i$[(Indukciós feltevés)]
   $\forall y\, (\phi \to \chi_i)$ [(G)-ből]

$\forall y\,(\phi \to \chi_i) \to (\phi \to \forall y \chi_i)$ [(PC4)-ből]
$\phi \to \forall y \chi_i$ [(MP)-ből]
$\phi \to \chi_k$

Ezzel a tételt bebizonyítottuk.

5. Tétel. *Ha* $\Sigma \cup \{\phi\} \vdash \psi$ *és* ϕ *zárt, akkor* $\Sigma \vdash \phi \to \psi$.

A dedukciótétel alkalmazásával további fontos és gyakran használható tételeket bizonyítunk.

6. Tétel (Hipotetikus Szillogizmus (HS)). *Tetszőleges* ϕ, ψ *és* χ *esetén:* $\{\phi \to \psi, \psi \to \chi\} \vdash \phi \to \chi$

Bizonyítás

(1) $\phi \to \psi$ [feltevés]
(2) $\psi \to \chi$ [feltevés]
(3) ϕ [feltevés]
(4) ψ [(1), (3), MP]
(5) χ [(2), (4), MP]

Bebizonyítottuk tehát, hogy $\{\phi \to \psi, \psi \to \chi, \phi\} \vdash \chi$. Végül, a dedukciótétel alkalmazásával kapjuk, hogy $\{\phi \to \psi, \psi \to \chi\} \vdash \phi \to \chi$.

7. Tétel. *Tetszőleges* ϕ*-re és* ψ*-re:* $\neg\psi \to (\psi \to \phi)$

Bizonyítás

(1) $\neg\psi \to (\neg\phi \to \neg\psi)$ [(PC1)]
(2) $(\neg\phi \to \neg\psi) \to (\psi \to \phi)$ [(PC3)]
(3) $\neg\psi \to (\psi \to \phi)$ [(1), (2), (HS)-tétel]

8. Tétel. *Tetszőleges ϕ-re:* $(\neg\phi \to \phi) \to \phi$

Bizonyítás
Először azt fogjuk megmutatni, hogy $\{\neg\phi \to \phi\} \vdash \phi$:
(1) $\neg\phi \to \phi$ [feltevés]
(2) $\neg\phi \to (\neg\neg(\neg\phi \to \phi) \to \neg\phi)$ [(PC1)]
(3) $(\neg\neg(\neg\phi \to \phi) \to \neg\phi) \to (\phi \to \neg(\neg\phi \to \phi))$ [(PC3)]
(4) $\neg\phi \to (\phi \to \neg(\neg\phi \to \phi))$ [(2), (3), (HS)]
(5) $(\neg\phi \to (\phi \to \neg(\neg\phi \to \phi)))$
$\to ((\neg\phi \to \phi) \to (\neg\phi \to \neg(\neg\phi \to \phi)))$ [(PC2)]
(6) $(\neg\phi \to \phi) \to (\neg\phi \to \neg(\neg\phi \to \phi))$ [(4), (5), (MP)]
(7) $\neg\phi \to \neg(\neg\phi \to \phi)$ [(1),(6), (MP)]
(8) $(\neg\phi \to \neg(\neg\phi \to \phi)) \to ((\neg\phi \to \phi) \to \phi)$ [(PC3)]
(9) $(\neg\phi \to \phi) \to \phi$ [(7), (8), (MP)]
(10) ϕ [(1), (9), (MP)]
Innen a tétel állítása a dedukciótétellel azonnal adódik.

9. Tétel. *Tetszőleges ϕ-re:* $\neg\neg\phi \to \phi$

Bizonyítás

Először azt fogjuk megmutatni, hogy $\{\neg\neg\phi\} \vdash \phi$:

(1) $\neg\neg\phi$ [feltevés]

(2) $\neg\neg\phi \to (\neg\phi \to \neg\neg\phi)$ [(PC1)]

(3) $\neg\phi \to \neg\neg\phi$ [(1), (2), (MP)]

(4) $(\neg\phi \to \neg\neg\phi) \to (\neg\phi \to \phi)$ [(PC3)]

(5) $\neg\phi \to \phi$ [(3), (4), (MP)]

(6) ϕ [(5), 8. Tétel, (MP)]

Innen a tétel állítása a dedukciótétellel azonnal következik.

Ezt felhasználva, adódik a fordított irányú tétel:

10. Tétel. *Tetszőleges ϕ-re:* $\phi \to \neg\neg\phi$

Bizonyítás

(1) $\neg\neg\neg\phi \to \neg\phi$ [9. Tétel]

(2) $(\neg\neg\neg\phi \to \neg\phi) \to \phi \to \neg\neg\phi$ [(PC3)]

(3) $\phi \to \neg\neg\phi$ [(1), (2), (MP)]

A 9. és 10. Tételeket számos további tétel levezetésénél használhatjuk.

11. Tétel. *Tetszőleges ϕ-re és ψ-re:* $(\phi \to \psi) \to (\neg\psi \to \neg\phi)$.

Bizonyítás

(1) $\phi \to \psi$ [feltétel]

(2) $\neg\neg\phi \to \phi$ [9. Tétel]

(3) $\neg\neg\phi \to \psi$ [(1), (2), (HS)]
(4) $\psi \to \neg\neg\psi$ [10. Tétel]
(5) $\neg\neg\phi \to \neg\neg\psi$ [(3), (4), (HS)]
(6) $(\neg\neg\phi \to \neg\neg\psi) \to (\neg\psi \to \neg\phi)$ [(PC3)]
(7) $\neg\psi \to \neg\phi$ [(5), (6), (MP)]
Végül a dedukciótételt alkalmazzuk.

12. Tétel. *Tetszőleges ϕ-re és ψ-re:* $\{\phi \to \psi, \phi \to \neg\psi\} \vdash \neg\phi$.

Bizonyítás
(1) $\phi \to \psi$ [feltétel]
(2) $\phi \to \neg\psi$ [feltétel]
(3) $(\phi \to \psi) \to (\neg\psi \to \neg\phi)$ [(PC3)]
(4) $\neg\psi \to \neg\phi$ [(1), (3), (MP)]
(5) $\phi \to \neg\phi$ [(2), (4), (HS)]
(6) $(\phi \to \neg\phi) \to (\neg\neg\phi \to \neg\phi)$ [11. Tétel]
(7) $\neg\neg\phi \to \neg\phi$ [(5), (6), (MP)]
(8) $(\neg\neg\phi \to \neg\phi) \to \neg\phi$ [8. Tétel]
(9) $\neg\phi$ [(7), (8), (MP)]

13. Tétel (Indirekt bizonyítás). *Legyen Σ formulák egy halmaza és legyen ϕ tetszőleges formula. $\Sigma \vdash \phi$ akkor és csak akkor, ha a $\Sigma \cup \{\neg\phi\}$ inkonzisztens.*

Bizonyítás

Ha $\Sigma \vdash \phi$, akkor $\Sigma \cup \{\neg\phi\} \vdash \phi$. Másrészt $\Sigma \cup \{\neg\phi\} \vdash \neg\phi$, tehát $\Sigma \cup \{\neg\phi\}$ valóban inkonzisztens.

Fordítva, ha $\Sigma \cup \{\neg\phi\}$ inkonzisztens, akkor van olyan ψ, hogy $\Sigma \cup \{\neg\phi\} \vdash \psi$ és $\Sigma \cup \{\neg\phi\} \vdash \neg\psi$. Tehát, a 4. tétel miatt $\Sigma \vdash \neg\phi \to \psi$. (Mivel ha $\Sigma \cup \{\neg\phi\}$ inkonzisztens, ψ mindig választható olyannak, hogy a dedukció-tétel feltételei teljesüljenek.) Hasonlóan kapjuk, hogy $\Sigma \vdash \neg\phi \to \neg\psi$. Alkalmazva a 12. Tételt, $\Sigma \vdash \neg\neg\phi$, majd a 9. Tétel felhasználásával $\Sigma \vdash \phi$.

14. Tétel. *Tegyük fel, hogy* $\Sigma \vdash \phi$ *és* $\Sigma \vdash \psi$. *Ekkor* $\Sigma \vdash \phi \wedge \psi$.

Bizonyítás

A 13. tételt fogjuk alkalmazni, vagyis belátjuk, hogy a $\Sigma \cup \{\neg(\phi \wedge \psi)\}$ inkonzisztens. Emlékezzünk, $\phi \wedge \psi$ annak a rövidítése, hogy $\neg(\phi \to \neg\psi)$. Tehát azt kell belátnunk, hogy $\Sigma \cup \{\phi \to \neg\psi\}$ inkonzisztens, ami triviálisan igaz, hiszen $\phi \to \neg\psi$ MP-vel azonnal maga után vonja, hogy $\Sigma \cup \{\neg(\phi \wedge \psi)\} \vdash \neg\psi$, ugyanakkor a feltevésünkből következően $\Sigma \cup \{\neg(\phi \wedge \psi)\} \vdash \psi$.

Hasonlóan triviális, hogy

15. Tétel. *Ha* $\Sigma \vdash \phi$ *vagy* $\Sigma \vdash \psi$, *akkor* $\Sigma \vdash \phi \vee \psi$.

16. Tétel. *Legyen* x *szabad változó a* $\phi(x)$ *formulában. Legyen továbbá* y *egy olyan változó, amelyik nem fordul elő* $\phi(x)$*-ben, sem kötött, sem szabad formában. Ekkor*

$$\vdash \forall x\phi(x) \leftrightarrow \forall y\phi(y)$$

Bizonyítás

1. $\forall x \phi(x)$
2. $\forall x \phi(x) \rightarrow \phi(y)$ [(PC6)]
3. $\phi(y)$ [(MP)]
4. $\forall y \phi(y)$ [(G)]

Vagyis beláttuk, hogy $\forall x \phi(x) \vdash \forall y \phi(y)$. A dedukció-tétel alkalmazásával tehát

$$\vdash \forall x \phi(x) \rightarrow \forall y \phi(y)$$

Teljesen hasonló módon bizonyítjuk a fordított irányt is.

17. Tétel. *Tetszőleges formulához létezik vele bizonyíthatóan ekvivalens prenex alakú formula.*

7. Interpretáció

7.1. Egy nem teljesen helyénvaló előzetes példa

Tekintsük a következő mondatokat a PC-ben:
(σ_1) $\forall x \forall y \left(P\left(x, y\right) \rightarrow P\left(x, y\right)\right)$
(σ_2) $\left(P\left(x, y\right) \wedge P\left(y, z\right)\right) \rightarrow P\left(x, z\right)$
(σ_3) $\forall y \exists x P\left(x, y\right)$

- Ha úgy interpretáljuk a $P(x, y)$ két változós predikátumot, mint a valaha élt emberek halmazában (*Sic!*) értelmezett „x őse y-nak" relációt, akkor nyilvánvalóan mindhárom mondat igaz.

- Ha úgy interpretáljuk $P(x, y)$-et, hogy az a $>$ reláció a természetes számok $\mathbb{N}$ halmazán, akkor ezek a mondatok mind igazak.

- Ha úgy interpretáljuk $P(x, y)$-et, hogy az a $<$ reláció az egész számok $\mathbb{Z}$ halmazán, akkor ezek a mondatok mind igazak.

- Ha úgy interpretáljuk $P(x, y)$-et, hogy az a $<$ reláció a természetes számok $\mathbb{N}$ halmazán, akkor a (σ_1) és (σ_2) a mondatok igazak, de a (σ_3) hamis.

Sokan „interpretáció" alatt a fenti példához hasonlóan azt értik, hogy a formális rendszer elemeinek a fizikai világ (a platonizmus és intuicionizmus szerint a platoni illetve mentális világ) olyan elemeit feleltetjük meg, melyek valamilyen intuitív értelemben kielégítik a szóban forgó formális rendszer axiómáit. A matematikai logiában interpretáció alatt mást értünk.

7.2. Interpretáció és modell

Interpretáció

Egy PC-ben értelmezett formális rendszer interpretációja egy

$$\mathcal{A} = \langle U, R_1^{n_1}, R_2^{n_2}, \ldots f_1^{m_1}, f_2^{m_2}, \ldots \rangle$$

struktúra, ahol

- U egy nem üres halmaz, melyet az interpretáció univerzumának fogunk nevezni.
- $R_1^{n_1}, R_2^{n_2}, \ldots$ az U-n értelmezett $n_1, n_2, \ldots$ argumentumos relációk, melyeket a formális rendszer $n_1, n_2, \ldots$ argumentumos $P_1^{n_1}, P_2^{n_2}, \ldots$ predikátumainak feleltetünk meg.
- $f_1^{m_1}, f_2^{m_2}, \ldots$ olyan $\underbrace{U \times U \times \ldots \times U}_{m_1} \rightarrow U$, $\underbrace{U \times U \times \ldots \times U}_{m_2} \rightarrow U$, stb. típusú függvények, melyek a formális rendszerben előforduló $m_1, m_2, \ldots$ argumentumos fügvényjeleket reprezentálják.

Szereposztás (értékelés)

A formális rendszerben előforduló $t_1, t_2, \ldots$ individum változókhoz és individum konstansokhoz rendre hozzárendeljük U-nak valamelyik elemét. (Több változóhoz is rendelhetjük ugyanazt az elemét U-nak.) Egy ilyen szereposztást röviden a következőképpen fogunk jelölni: $[u_1, u_2, \ldots]$

Teljesítés

Most definiáljuk egy ϕ formula *teljesülését* az $\mathcal{A}$ interpretációban egy adott $[u_1, u_2, u_3, \ldots]$ szereposztás mellett. Ezt úgy fogjuk jelölni, hogy

$$\mathcal{A} \models \phi\,[u_1, u_2, u_3, \ldots]$$

Felhasználva, hogy a nyelv helyesen képzett formuláit hogyan építjük fel (lásd a 5.3. bekezdést), a definíciót a következő módon adjuk meg:

1. $\mathcal{A} \models P_i^n\,(t_1, t_2, \ldots t_n)\,[u_1, u_2, u_3, \ldots]$ akkor és csak akkor, ha az $[u_1, u_2, u_3, \ldots]$ szereposztásnak megfelelően a $t_1, t_2, \ldots t_n$ terminusoknak megfeleltetett $u_{t_1}, u_{t_2}, \ldots u_{t_n}$ elemekre fennáll a P_i^n predikátumnak megfelelő R_i^n reláció, tehát

$$R_i^n\,(u_{t_1}, u_{t_2}, \ldots u_{t_n}) \tag{1}$$

   Értelemszerűen azt is megengedjük (összhangban a terminus definíciójával), hogy egy t_k terminus függvénykifejezés legyen, tehát pl. legyen t_k a $f^2\,(x_1, x_2)$ kifejezés. Ekkor az adott szereposztásban az x_1 és x_2 változókat az univerzum valamely u_{x_1} és u_{x_2} eleme reprezentálja. Az f^2 2-argumentumos függvényjelet pedig valamilyen $\widetilde{f} : U \times U \to U$ függvény. Ekkor az (1) relációban az u_{t_k} helyére az $\widetilde{f}\,(u_{x_1}, u_{x_2})$ kifejezést, azaz az $\widetilde{f}$ függvénynek az u_{x_1}, u_{x_2} helyen felvett értékét írjuk.

2. $\mathcal{A} \models \neg\phi\,[u_1, u_2, u_3, \ldots]$ akkor és csak akkor, ha nem igaz, hogy $\mathcal{A} \models \phi\,[u_1, u_2, u_3, \ldots]$.

3. $\mathcal{A} \models \phi \rightarrow \psi\,[u_1, u_2, u_3, \ldots]$ akkor és csak akkor, ha vagy $\mathcal{A} \models \neg\phi\,[u_1, u_2, u_3, \ldots]$ vagy $\mathcal{A} \models \psi\,[u_1, u_2, u_3, \ldots]$.

4. $\mathcal{A} \models \forall y \phi\,(x_1, x_2, \ldots x_n, y)\,[u_1, u_2, \ldots u_n]$ akkor és csak akkor, ha minden $[u_1, u_2, \ldots u_n, w]$ értékelésre (ahol $u_1, u_2, \ldots u_n$ fix) $\mathcal{A} \models \phi\,[u_1, u_2, \ldots u_n, w]$.

Ezzel egy formula teljesülésének fogalmát konstruktive megadtuk.

Igaz $\mathcal{A}$-ban

Ha egy $\mathcal{A} \models \phi\,[u_1, u_2, u_3, \ldots]$ minden $[u_1, u_2, u_3, \ldots]$ értékelés (szereposztás) esetén, akkor azt mondjuk, hogy ϕ formula *igaz* $\mathcal{A}$*-ban*, és azt írjuk, hogy $\mathcal{A} \models \phi$. Ha ϕ mondat, azaz nem tartalmaz szabad változót, akkor $\mathcal{A} \models \phi$ minden olyan esetben ha $\mathcal{A} \models \phi\,[u_1, u_2, u_3, \ldots]$ tetszőleges $[u_1, u_2, u_3, \ldots]$ értékelés esetén ($[u_1, u_2, u_3, \ldots]$-nek nincs jelentősége).

Univerzálisan igaz

Ha tetszőleges $\mathcal{A}$ interpretációra $\mathcal{A} \models \phi$, akkor azt mondjuk, hogy ϕ *univerzálisan igaz*, és ezt úgy jelöljük, hogy $\models \phi$.

Példa

Legyen $\mathcal{A} = \langle W, A \rangle$, ahol W a valaha élt emberek halmaza, és A az „őse” reláció. Vegyük pl. a $\exists x P(x, y)$ formulát. $\mathcal{A} \models \exists x P(x, y)\,[v]$ akkor és csak akkor, ha létezik olyan w ember, hogy $\mathcal{A} \models P(x, y)\,[w, v]$. Ez akkor és csak akkor áll fenn, ha $A(w, v)$. De ez tetszőleges v esetén igaz, hogy tudniillik van olyan w, akire $A(w, v)$. Tehát $\mathcal{A} \models \exists x P(x, y)\,[v]$ minden lehetséges v-re, ezért $\mathcal{A} \models \exists x P(x, y)$, azaz $\exists x P(x, y)$ igaz $\mathcal{A}$-ban.

Ezzel szemben, nyilván $\mathcal{N} \not\models \exists x P(x, y)$, ahol $\mathcal{N} = \langle \mathbb{N}, < \rangle$.

18. Tétel. *A PC axiómái univerzálisan igazak.*

Bizonyítás

pl. (PC6)-ra: Tegyük fel hogy hogy valamilyen $\mathcal{A}$ interpretációban a változók valamilyen $[u_1, u_2, u_3, \ldots]$ értékelése esetén, (PC6) nem igaz. Ez akkor és csak akkor lehetséges, ha $\mathcal{A} \models \forall x \phi(x) \, [u_1, u_2, u_3, \ldots]$ ugyanakkor $\mathcal{A} \not\models \phi(y) \, [u_1, u_2, u_3, \ldots]$. De ez ellentmondás, hiszen ha az y változó az értékelésben valamely u_i-nek felel meg, az előző formula éppen azt állítja, hogy a ϕ reláció fennáll minden lehetséges u_i mellett.

HF

Bizonyítsuk be a tételt a többi axiómára is.

Egy formulahalmaz modellje

Legyen Σ formulák egy halmaza PC-ben, és legyen az $\mathcal{A}$ interpretáció olyan, hogy $\mathcal{A} \models \phi$ minden $\phi \in \Sigma$ esetén. Ekkor azt mondjuk, hogy $\mathcal{A}$ a Σ egy *modellje*.

19. Tétel. *Legyen $\mathcal{A}$ egy tetszőleges interpretáció. Ha $\mathcal{A} \models \phi$ és $\mathcal{A} \models \phi \to \psi$, akkor $\mathcal{A} \models \psi$*

Bizonyítás

Legyen $[u_1, u_2, u_3, \ldots]$ tetszőleges értékelés. $\mathcal{A} \models \phi \, [u_1, u_2, u_3, \ldots]$ és $\mathcal{A} \models (\phi \to \psi) \, [u_1, u_2, u_3, \ldots]$. A teljesülés (implikációra vonatkozó) definíciójánál fogva: vagy

$\mathcal{A} \models \neg\phi\,[u_1, u_2, u_3, \ldots]$, ami feltevésünk szerint lehetetlen, vagy $\mathcal{A} \models \psi\,[u_1, u_2, u_3, \ldots]$. Mivel ez tetszőleges értékelésre igaz, a tételt bebizonyítottuk.

20. Tétel. *Legyen $\mathcal{A}$ egy tetszőleges interpretáció. $\mathcal{A} \models \phi$ akkor és csak akkor, ha $\mathcal{A} \models \forall x\phi$.*

Bizonyítás

Tegyük fel, hogy $\mathcal{A} \models \phi$. Ekkor $\mathcal{A} \models \phi\,[u_1, u_2, u_3, \ldots]$ tetszőleges $[u_1, u_2, u_3, \ldots]$ értékelésre, tehát $\mathcal{A} \models \phi\,[u_1, \ldots, u_i, \ldots]$ minden olyan értékelésre is, ahol az x változónak megfelelő u_i elemet változtatjuk csak, a többit fixen tartjuk. Tehát $\mathcal{A} \models \forall x\phi\,[u_1, u_2, u_3, \ldots]$ minden értékelésre, azaz $\mathcal{A} \models \forall x\phi$. Fordítva, ha $\mathcal{A} \models \forall x\phi$, akkor $\mathcal{A} \models \forall x\phi\,[u_1, u_2, u_3, \ldots]$ tetszőleges $[u_1, u_2, u_3, \ldots]$ értékelésre. Mivel az összes értékelést úgy is megkapjuk, ha előbb vesszünk egy értékelést és az x-nek megfelelő u_i elemet variáljuk, majd vesszük az összes ilyet, $\mathcal{A} \models \phi\,[u_1, \ldots, u_i, \ldots]$ minden lehetséges $[u_1, u_2, u_3, \ldots]$ esetén, tehát $\mathcal{A} \models \phi$.

21. Tétel. *Legyen PC(Σ) a PC egy tetszőleges Σ-kiterjesztése, és legyen $\mathcal{A}$ egy tetszőleges interpretáció. Ha a Σ axiómalista minden formulája igaz $\mathcal{A}$-ban, akkor $\mathcal{A}$ egy modellje PC(Σ)-nak, abban az értelemben, hogy minden olyan ϕ formulára, melyre $\Sigma \vdash \phi$, fennáll, hogy $\mathcal{A} \models \phi$.*

Bizonyítás

Tekintsünk egy tetszőleges ϕ formulát, melyre $\Sigma \vdash \phi$. Ez azt jelenti, hogy létezik ϕ-nek bizonyítása. Legyen a bizonyítás egy n formulából álló formulasorozat. Most teljes indukcióval megmutatjuk, hogy ϕ igaz $\mathcal{A}$-ban.

1. $n = 1$. ϕ axióma, tehát igaz $\mathcal{A}$-ban.

2. $n > 1$. Indukciós hipotézis: A bizonyítandó állítás igaz minden olyan ϕ tételre (azaz $\Sigma \vdash \phi$ formula esetében), amelynek bizonyítása maximum $n - 1$ lépésből áll.

3. Ekkor igaz az n lépésből álló bizonyítással rendelkező ϕ-re is. Ugyanis a következő esetek lehetségesek:

   (a) ϕ maga is axióma, tehát $\mathcal{A} \models \phi$.

   (b) ϕ a (MP)-ből (modus ponens) következik, mondjuk valamilyen korábbi χ_i és $\chi_i \to \phi$ felhasználásával. Mármost χ_i és $\chi_i \to \phi$ mindketten olyan Σ-ból levezethető tételek, amelyek bizonyítása maximum $n - 1$ lépésből áll, tehát a 19. tétel következtében $\mathcal{A} \models \phi$.

   (c) Hasonlóan, ha ϕ a (G) (generalizáció) alkalmazásával következik valamely korábbi χ_i formulából, akkor a 20. tétel következtében $\mathcal{A} \models \phi$.

7.3. Teljességi tétel

22. Tétel (Teljességi tétel). *Egy ϕ formula akkor és csak akkor bizonyítható PC-ben (vagyis csak a PC axiómáiból), ha univerzálisan igaz. Szokásos jelöléseinket használva, $\vdash \phi$ akkor és csak akkor, ha $\models \phi$.*

Bizonyítás

1. $\vdash \phi \Rightarrow \models \phi$

Mint már bebizonyítottuk, a PC axiómái univerzálisan igazak. A 21. tételből következően tehát PC minden tétele univerzálisan igaz.

Fontos következmény

A predikátum kalkulus konzisztens. Ugyanis ha nem volna az, tehát $\vdash \phi$ és $\vdash \neg\phi$ egyszerre állna fenn, akkor ebből következne, hogy $\models \phi$ és $\models \neg\phi$, azaz lenne olyan $\mathcal{A}$ interpretáció és olyan értékelés, hogy egyszerre $\mathcal{A} \models \phi\,[u_1, \ldots, u_i, \ldots]$ és nem $\mathcal{A} \models \phi\,[u_1, \ldots, u_i, \ldots]$.

2. $\models \phi \Rightarrow \vdash \phi$

Ez akkor teljesül, ha abból, hogy ϕ nem tétel, következik, hogy nem univerzálisan igaz. Vagyis azt kell megmutatnunk, hogy ha $\nvdash \phi$, akkor $\neg\phi$-nek létezik modellje. $\neg\phi$-nek ugyanis csak akkor létezik modellje, ha ϕ nem univerzálisan igaz. Az 13. tétel következtében, ha $\nvdash \phi$, akkor a $\{\neg\phi\}$ egy elemű formulahalmaz konzisztens. Ezért, a Gödel–Henkin-tétel következtében – melyet az alábbiakban fogunk bizonyítani – létezik modellje. Márpedig ha ez igaz,

akkor ebben a modellben ϕ hamis, tehát ϕ nem univerzálisan igaz. Tehát $\models \phi$-ből következik $\vdash \phi$, és ezzel a tételt bebizonyítottuk.

Természetesen, most következik a Gödel–Henkin-tétel.

23. Tétel (Gödel–Henkin teljességi tétel). *Ha egy Σ formulahalmaz konzisztens, akkor létezik modellje, azaz létezik olyan $\mathcal{A}$ interpretáció, hogy $\mathcal{A} \models \phi$ minden $\phi \in \Sigma$ formulára.*

Bizonyítás

A bizonyítás sémája:

1. Elindulunk a PC(Σ)-tól

$\Downarrow$

2. $b_1, b_2, \ldots$ individuum konstansokat adunk hozzá a nyelvhez (ezeket fogjuk „tanúknak” hívni)

$\Downarrow$ ellenőrizzük, hogy az így bővített rendszer konzisztens-e

3. Felsoroljuk az összes olyan formulát, amelyben egy szabad változó szerepel: $\psi_0(v_0), \psi_1(v_1), \ldots$

$\Downarrow$

4. Minden a 3. pontban felsorolt formulával $\psi_i(v_i)$ formulával és egy alkalmas tanúval képezzük a $\exists v_i \psi_i(v_i) \rightarrow \psi_i(b_i)$ formulát, és új axiómaként hozzáadjuk a rendszerhez.

$\Downarrow$ ellenőrizzük a konzisztenciát

5. A *Lindenbaum-lemmát* alkalmazva egy $\Sigma^\star$ kibővített formulahalmazt veszünk úgy, hogy minden ϕ-re vagy $\Sigma^\star \vdash \phi$ vagy $\Sigma^\star \vdash \neg\phi$ teljesüljön.

$\Downarrow$

6. Definiálunk egy megfelelő $\mathcal{A}$ interpretációt a kiterjesztett $\Sigma^\star$-hez.

$\Downarrow$

8. Mivel Σ benne van a $\Sigma^\star$-ban, $\mathcal{A} \models \phi$ minden olyan ϕ-re, amely benne van Σ-ban, tehát az $\mathcal{A}$ interpretáció Σ egy modellje.

De előbb a Lindenbaum-lemma.

Teljes formulahalmaz

Formulák egy Σ halmazát teljesnek (komplettnek) nevezünk, ha a nyelv minden ϕ mondatára teljesül, hogy vagy $\Sigma \vdash \phi$, vagy $\Sigma \vdash \neg\phi$.

24. Tétel (Lindenbaum-lemma). *Ha Σ konzisztens, akkor létezik teljes és konzisztens kiterjesztése, vagyis olyan $\Sigma^\star$ kiterjesztése, hogy tetszőleges ϕ mondatra vagy $\Sigma^\star \vdash \phi$, vagy $\Sigma^\star \vdash \neg\phi$, de sohasem a kettő egyszerre.*

Bizonyítás

Soroljuk fel a PC összes mondatát: $\phi_1, \phi_2, \phi_3, \ldots$ Most lépésről lépésre felépítjük $\Sigma^\star$-ot. Legyen $\Sigma_0 = \Sigma$. Majd, legyen

$$\Sigma_1 = \begin{cases} \Sigma_0 & \text{ha } \Sigma_0 \vdash \neg\phi_1 \\ \Sigma_0 \cup \{\phi_1\} & \text{ha } \Sigma_0 \nvdash \neg\phi_1 \end{cases}$$

(Vegyük észre, hogy ezzel elértük, hogy Σ_1 konzisztens maradt, és vagy ϕ_1 vagy $\neg\phi_1$ levezethető.) Az eljárást ugyanígy folytatjuk:

$$\Sigma_{n+1} = \begin{cases} \Sigma_n & \text{ha } \Sigma_n \vdash \neg\phi_{n+1} \\ \Sigma_n \cup \{\phi_{n+1}\} & \text{ha } \Sigma_n \nvdash \neg\phi_{n+1} \end{cases}$$

Legyen $\Sigma^\star$ az így nyert legbővebb halmaz. $\Sigma^\star$ konzisztens és teljesíti, hogy a PC tetszőleges ϕ_i mondatára vagy $\Sigma^\star \vdash \phi$, vagy $\Sigma^\star \vdash \neg\phi$. Ezzel a lemmát bebizonyítottuk.

Most részletezzük a Gödel–Henkin-tétel bizonyítását.

2 Adjuk hozzá a $b_1, b_2, \ldots$ individuum konstansokat a nyelvhez. Nevezzük ezeket tanúknak. Az így kibővített nyelvet hívjuk PC^+-nak és a kibővült nyelvben a vizsgált formulahalmazt Σ^+-nak. Könnyen belátható, hogy az így nyert bővített rendszer is konzisztens, ha az eredeti az volt. Tegyük fel ugyanis, hogy nem az, azaz létezik olyan ϕ formula, hogy ő is és $\neg\phi$ is levezethető. Ez azt jelenti, hogy a két bizonyításban, amelyek véges formulasorozatok csak véges sok tanú fordul elő, melyeket mind helyettesíthetünk olyan eredeti szabad változókkal, melyek sehol máshol nem fordulnak elő. Ezzel a két bizonyítást az eredeti rendszer két bizonyításává alakítottuk, és ez ellentmondás, hiszen az eredeti rendszerről feltettük, hogy konzisztens.

3 Soroljuk fel a PC^+ összes olyan formuláját, amelyben egyetlen szabad változó van: $\psi_1(v_1), \ldots \psi_n(v_n), \ldots$. Legyen θ_n a következő formula:

$$\exists v_n \psi_n(v_n) \rightarrow \psi_n(b_n)$$

ahol b_n az első olyan tanú, amelyik még nem fordult elő semelyik korábbi $\psi_i(v_n)$-ben vagy θ_i-ben. (Innen az elnevezés! b_n „tanúsítja”, hogy tényleg van olyan dolog, amelyre ψ_n tulajdonság fennáll.)

4a Most minden θ_n-t axiómaként hozzáadjuk a rendszerhez:

$$\begin{aligned} \Sigma^0 &= \Sigma^+ \\ \Sigma^{n+1} &= \Sigma^n \cup \{\theta_n\} \\ \Sigma^\infty &= \bigcup \Sigma^n \end{aligned}$$

4b Könnyű ellenőrizni, hogy minden Σ^n konzisztens, ha Σ^{n-1} az volt. A trükk az, hogy az újonnan bevezetett b úgy viselkedik, mint egy szabad változó.

4c Következésképpen Σ^∞ is konzisztens, hiszen minden bizonyítás csak véges hosszúságú, tehát véges sok formula fordulhat elő benne, tehát (lásd a hasonló gondolatmenetet a 2. pontban) Σ^∞ inkonzisztenciája valamely Σ^n inkonzisztenciáját jelentené.

5a A Lindenbaum-lemma alkalmazásával Σ^∞-t egy konzisztens és teljes $\Sigma^\star$ rendszerré bővítjük.

5b Tehát, tetszőleges ϕ-re és ψ-re

(1) $\Sigma^\star \vdash \phi$ vagy $\Sigma^\star \vdash \neg\phi$

(2) $\Sigma^\star \vdash \neg\phi$ akkor és csak akkor ha $\Sigma^\star \nvdash \phi$, részben (1) miatt ($\Sigma^\star$ teljessége) és mert $\Sigma^\star$ konzisztens is.

(3) $\Sigma^\star \vdash \phi \to \psi$ akkor és csak akkor ha $\Sigma^\star \vdash \neg\phi$ vagy $\Sigma^\star \vdash \psi$. Ugyanis,

$\Rightarrow$ (1)-ből vagy $\Sigma^\star \vdash \phi$ vagy $\Sigma^\star \vdash \neg\phi$, illetve $\Sigma^\star \vdash \psi$ vagy $\Sigma^\star \vdash \neg\psi$. Ha nem igaz, hogy $\Sigma^\star \vdash \neg\phi$, akkor $\Sigma^\star \vdash \phi$, ahonnan (MP)-vel $\Sigma^\star \vdash \psi$.

$\Leftarrow$ Ha $\Sigma^\star \vdash \psi$, akkor (PC1)-ből $\Sigma^\star \vdash \phi \to \psi$.

Ha $\Sigma^\star \vdash \neg\phi$, akkor (PC1)-ből $\Sigma^\star \vdash \neg\psi \to \neg\psi$ majd (PC3)-ból $\Sigma^\star \vdash \phi \to \psi$.

(4) $\Sigma^\star \vdash \exists v\psi\,(v)$ akkor és csak akkor ha $\Sigma^\star \vdash \psi(b)$ valamilyen b tanúra (hiszen így konstruáltuk a θ_n axiómákat).

6 Most konstruálunk egy modellt a $\Sigma^\star$ számára: $\mathcal{A} = \langle U, R\rangle$ ahol $U = \{b_1, b_2, \ldots\}$, az R reláció pedig a következő:

$$R\,(b_i, b_j) \text{ akkor és csak akkor, ha } \Sigma^\star \vdash P\,(b_i, b_j)$$

7 (1),(2),(3) és (4), valamint a **Teljesítés** c. bekezdés 1.–4. pontja alapján (felhasználva, hogy $\forall$ kifejezhető $\exists$ segítségével) könnyen látható, hogy

$$\mathcal{A} \models \phi \text{ akkor és csak akkor, ha } \Sigma^\star \vdash \phi$$

8 Mivel Σ benne van $\Sigma^\star$-ban, $\mathcal{A} \models \phi$ minden $\phi \in \Sigma$-ra. Vagyis, bebizonyítottuk, hogy ha Σ konzisztens, akkor létezik modellje.

Megjegyzés

A későbbiek szempontjából fontos észrevennünk, hogy valójában többet bizonyítottunk, mint ami feltétlenül szükséges lett volna. Valójában azt bizonyítottuk be, hogy Σ-nak létezik *megszámlálható* modellje, hiszen $U = \{b_1, b_2, \ldots\}$ egy megszámlálható halmaz.

Mutatus mutandis, a fenti bizonyítás alapján könnyen bizonyítható a teljességi tétel következő alakja:

25. Tétel (Teljességi tétel). *Legyen Σ egy tetszőleges konzisztens formulahalmaz és φ egy tetszőleges formula. $\Sigma \vdash \phi$ akkor és csak akkor, ha $\mathcal{A} \models \phi$ a Σ tetszőleges $\mathcal{A}$ modelljében.*

8. PC(=) (predikátum kalkulus identitással)

Az előzőekben megismert predikátum kalkulust egy további predikátum-jellel egészítjük ki. Legyen E („ugyanaz mint", „egyenlő") egy kétváltozós predikátum. E tulajdonságait a következő axiómák hozzáadásával rögzítjük:

8.1. Az egyenlőség axiómái

(E1) $E(x, x)$

(E2) $E(t, s) \to E\left(f^n\left(u_1, u_2, \ldots, t, \ldots u_n\right), f^n\left(u_1, u_2, \ldots, s, \ldots u_n\right)\right)$

(E3) $E(t, s) \to \left(\phi\left(u_1, u_2, \ldots, t, \ldots u_n\right) \to \phi\left(u_1, u_2, \ldots, s, \ldots u_n\right)\right)$

Kényelmesebb jelölés: $x = y \equiv E(x, y)$

HF.

Mutassuk meg, hogy E tranzitív és szimmetrikus.

8.2. PC(=) interpretációi

A PC(=)-nek vagy (bármely bővítésének) a korábbi értelemben lehetnek interpretációi. Ezekben nyilvánvalóan az $E(x, y)$ azonosság

predikátum is valamilyen alkalmas kétváltozós relációval interpretálva van. Legyen $\mathcal{A} = \langle U, R, S\rangle$ egy ilyen interpretáció az U univerzumon, ahol R (az egyszerűség kedvéért továbbra is egyetlen) P predikátumnak megfelelő reláció, S pedig az E predikátum reprezentáns relációja. S sok minden lehet, amely teljesíti az (E1)–(E3) axiómákból következő tulajdonságokat.

Normál interpretáció

Az $\mathcal{A}$ interpretációt *normál* interpretációnak nevezzük, ha S nem más, mint az U univerzum-halmaz elemein értelmezett szokásos azonosság. Pontosabban, (hogy egy rendes kétváltozós relációt adjunk meg) $S = \{\langle x, x\rangle : x \in U\}$.

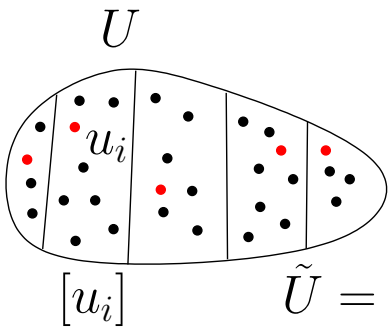
HF

Mutassuk meg, hogy ez a reláció teljesíti az egyenlőség axiómáiból következő tulajdonságokat!

26. Tétel. *Jelölje az $\{$Egyenlőség$\}$ az (E1)–(E3) axiómákból álló formulahalmazt és legyen Σ egy tetszőleges formulahalmaz. Ha a $\Sigma \cup \{$Egyenlőség$\}$ formulahalmaznak létezik modellje, akkor létezik normál modellje is.*

Bizonyítás

Legyen $\mathcal{A} = \langle U, R, S\rangle$ egy tetszőleges modellje $\Sigma \cup \{$Egyenlőség$\}$-nek, ahol S az E predikátumot reprezentáló reláció. Mivel S ekvivalencia reláció, vagyis reflexív, szimmetrikus és tranzitív, képezhetjük U halmaz elemeinek S szerinti ekvivalencia osztályait.



$$\forall u \forall u' \left(u, u' \in [u_i] \leftrightarrow S(u, u')\right)$$

Választva minden egyes ekvivalencia-osztályból egy elemet, egy olyan $\widetilde{U}$ halmazt kapunk, amelyre leszűkítve az R és S relációkat, az $\widetilde{\mathcal{A}} = \left\langle \tilde{U}, R|_{\widetilde{U}}, S|_{\widetilde{U}} \right\rangle$ struktúra a $\Sigma \cup \{\text{Egyenlőség}\}$ formulahalmaz egy normál modellje. Az egyenlőség axiómáiból következően az is megmutatható, hogy az ekvivalencia-osztályokon értelmezett relációk függetlenek a reprezentáns elemek választásától. Mivel most egyedüli célunk annak megmutatása, hogy *létezik* $\Sigma \cup \{\text{Egyenlőség}\}$-nek normál modellje, a konkrétan konstruált modellnek ez a tulajdonsága nem fontos. Csupán a következő két triviális észrevétel elégséges. Egyrészt, ha $\mathcal{A} \models \phi$, akkor $\widetilde{\mathcal{A}} \models \phi\left[\widetilde{u}_1, \widetilde{u}_2, \ldots\right]$ a változók tetszőleges $[\widetilde{u}_1, \widetilde{u}_2, \ldots]$ értékelése mellett, hiszen minden $[\widetilde{u}_1, \widetilde{u}_2, \ldots]$ értékelés egyben egy $\mathcal{A}$ interpretációbeli értékelés is, tehát $\widetilde{\mathcal{A}} \models \phi$. Másrészt, $S|_{\widetilde{U}} = \left\{ \langle \widetilde{u}, \widetilde{u} \rangle : \widetilde{u} \in \widetilde{U} \right\}$. Ugyanis két $\tilde{S}\left([u_i], [u_j]\right)$ csak akkor ha $S\left(u_i, u_j\right)$, ami éppen azt jelenti, hogy u_i és u_j egy ekvivalencia-osztályba tartoznak, tehát $[u_i] = [u_j]$. Ezzel a tételt bizonyítottuk.

27. Tétel (Teljességi tétel PC(=)-re). *Egy ϕ formula akkor és csak akkor bizonyítható PC(=)-ben, ha igaz minden normál in-*

terpretációban. Szimbolikusan írva, $\{Egyenlőség\} \vdash \phi$ *akkor és csak akkor, ha* $\models_N \phi$.

Bizonyítás

1. ($\{\text{Egyenlőség}\} \vdash \phi \Rightarrow \models_N \phi$)

Mivel a (PC1)–(PC6) és (E1)–(E3) axiómák igazak minden normál interpretációban, a 21. tétel következtében ha $\{\text{Egyenlőség}\} \vdash \phi$ akkor $\mathcal{A} \models \phi$ minden $\mathcal{A}$ normál interpretáció esetén.

2. ($\models_N \phi \Rightarrow \{\text{Egyenlőség}\} \vdash \phi$)

Természetesen, ezt is a Gödel–Henkin-tétel segítségével fogjuk belátni. Tegyük fel, hogy $\{\text{Egyenlőség}\} \nvdash \phi$. 13. tétel következtében ekkor az $\{\text{Egyenlőség}\} \cup \{\neg\phi\}$ formulahalmaz konzisztens, tehát a Gödel–Henkin-tétel következtében, van modellje. A 26. tétel következtében tehát van normál modellje is. Ez viszont azt jelenti, hogy van olyan normál modell, amelyben ϕ nem igaz, s ez ellentmondásban áll $\models_N \phi$ feltevésünkkel. Ezzel a tételt mindkét irányban bizonyítottuk.

9. Modell-elmélet

A modell-elmélet az elsőrendű formális rendszerek konkrét interpretációival foglalkozik, azzal például, hogy mit lehet a formális rendszerrel kapcsolatban mondani a modelljei alapján, hogyan viszonyulnak egymáshoz egy adott formális rendszer modelljei, stb.

9.1. Példa egy axiómarendszer modelljére

Tekintsük mondatoknak a következő Σ halmazát PC(=)-ben:

(n1) $\forall x\,(\neg P(x,x))$

(n2) $\forall x\forall y\,(\neg\,(P(x,y)\wedge P(y,x)))$

(n3) $\forall x\forall y\forall z\,(P(x,y)\wedge P(y,z)\rightarrow P(x,z))$

(n4) $\forall x\forall y\,(P(x,y)\vee P(y,x)\vee E(x,y))$

(n5) $\exists x\forall y\,(\neg P(y,x))$

(n6) $\forall x\exists y\,(P(x,y)\wedge\forall z\,(\neg\,(P(x,z)\wedge P(z,y))))$ (van a nagyobbak között legkisebb)

(n7) $\forall x\,(\exists y P(y,x)\rightarrow\exists y\,(P(y,x)\wedge\forall z\,(\neg\,(P(y,z)\wedge P(z,x)))))$ (ha van kisebb, van a kisebbek között legnagyobb)

Vegyük a következő struktúrát: $\mathcal{N}=\langle N,<,=\rangle$, ahol N nem más, mint a természetes számok $\mathbb{N}$ halmaza, és $<$ a „kisebb” reláció, $=$ pedig az azonosság reláció. Nyilvánvaló, hogy $\mathcal{N}$ egy normál modellje Σ-nak. (A következőkben a predikátum kalkulusba beleértjük az egyenlőség axiómáit és modell alatt normál modellt értünk.) Tisztán a halmazokra és relációkra vonatkozó — itt nem részletezett — megfontolásokkal megmutatható, hogy

28. Tétel. *Ha $\mathcal{A}$ tetszőleges modellje Σ-nak, ugyanazok a mondatok igazak $\mathcal{A}$-ban, mint amelyek igazak $\mathcal{N}$-ben.*

E tétel fontos következménye, hogy

29. Tétel. *Tetszőleges ψ mondatra, $\mathcal{N}\models\psi$ akkor és csak akkor, ha $\Sigma\vdash\psi$.*

Bizonyítás

Tegyük fel, hogy $\Sigma \nvdash \psi$. Ekkor $\Sigma \cup \{\neg\psi\}$ konzisztens, következésképpen, a Gödel–Henkin-tétel miatt létezik modellje, mondjuk $\mathcal{A}$. Tehát $\mathcal{A} \models \neg\psi$. A 28. tétel következtében $\mathcal{N} \models \neg\psi$, ami ellentmondás, tehát beláttuk, hogy ha $\mathcal{N} \models \psi$ akkor $\Sigma \vdash \psi$. Fordítva, mivel a Σ-ba tartozó mondatok igazak $\mathcal{N}$-ben, és a következtetési szabályok megőrzik ezt a tulajdonságot (19. és 20. tételek), $\Sigma \vdash \psi$ implikálja $\mathcal{N} \models \psi$-t.

Mivel tehát egy mondat akkor és csak akkor igaz $\mathcal{N}$-ben, ha levezethető a Σ axiómákból, azt mondjuk, hogy „axiomatizáltuk $\mathcal{N}$ igaz mondatait". Vagyis $\mathcal{N}$ igaz mondatai levezethetők a logikai axiómákból + az egyenlőség axiómáiból + Σ-ból.

9.2. Milyen mértékben határozza meg Σ magát az $\mathcal{N}$ interpretációt?

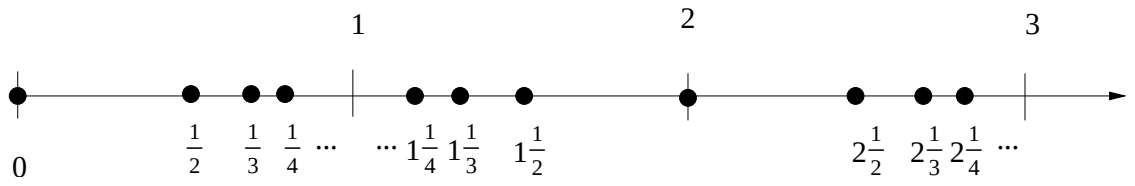
$\mathcal{N}$ nem az egyetlen modellje Σ-nak. Pl. $\mathcal{M} = \langle M, <, = \rangle$, ahol $M = \{1, 2, 3, \ldots\}$ is egy modellje Σ-nak. Világos viszont, hogy az

$$x \in N \mapsto x + 1 \in M$$

hozzárendelés egy a $<$ és $=$ relációkat megőrző izomorfizmus $\mathcal{N}$ és $\mathcal{M}$ között. Tehát ez nem lényegesen más interpretáció.

Van azonban Σ-nak olyan interpretációja is, amelyik nem izomorf az $\mathcal{N}$ struktúrával. Tekintsük a következő pontok halmazát a számegyenesen:

$$B = \left\{1 - \frac{1}{n} : n \in \mathbb{N} \setminus \{0\}\right\} \cup \left\{1 + \frac{1}{n} : n \in \mathbb{N} \setminus \{1\}\right\} \cup \left\{3 - \frac{1}{n} : n \in \mathbb{N} \setminus \{0\}\right\}$$



Könnyen belátható, hogy $\mathcal{B} = \langle B, <, = \rangle$ egy modellje Σ-nak. $\mathcal{N}$ és $\mathcal{B}$ azonban nyilvánvalóan nem izomorfak. Pl. az $1\frac{1}{2} \in B$ elem előtt végtelen sok kisebb elem létezik, és N egyetlen eleme sem rendelkezik ezzel a tulajdonsággal, stb.

Vagyis, a Σ axiómarendszer nem determinálja egyértelműen az interpretációt, sőt, még csak nem is határolja körül az interpretáló struktúrát. Amit tudunk az az, hogy Σ-ból levezethető minden olyan mondata a formális rendszernek, amelyik igaz $\mathcal{N}$-ben.

30. Tétel. *Ha Σ inkonzisztens, akkor van olyan véges részhalmaza, amelyik inkonzisztens.*

Bizonyítás

Ha Σ inkonzisztens, akkor létezik olyan ϕ formula, melyre $\Sigma \vdash \phi$ és $\Sigma \vdash \neg\phi$, más szóval $\Sigma \vdash \phi \wedge \neg\phi$. Ez azt jelenti, hogy létezik olyan véges $\chi_1, \chi_2, \chi_3, \ldots \chi_n$ formulasorozat, amelyik bizonyítása $\phi \wedge \neg\phi$-nek. Mivel a $\chi_1, \chi_2, \chi_3, \ldots \chi_n$ lista véges, azon formulák

száma a sorozatban, amelyek benne vannak Σ-ban, véges, tehát létezik véges részhalmaza Σ-nak, melyből $\phi \wedge \neg\phi$ levezethető. Ezzel a tételt bizonyítottuk.

A Gödel–Henkin-tételből tudjuk, hogy ha Σ konzisztens (de lehet végtelen), akkor létezik modellje. Ezt használjuk fel a következő tétel bizonyításában.

31. Tétel (Kompaktsági tétel). *Ha Σ minden véges részhalmazának van modellje, akkor Σ-nak is van modellje.*

Bizonyítás

Ha Σ minden véges részhalmazának van modellje, akkor Σ minden véges részhalmaza konzisztens. A 30. tétel következtében maga Σ is konzisztens, tehát — a Gödel–Henkin-tétel miatt — van modellje.

Példák

1

Egészítsük ki a fentebb használt nyelvet egy c individuum konstanssal. A korábban vizsgált Σ mondathalmazt pedig a következő mondatokkal:

ψ_1 $\exists v_1 P(v_1, c)$

ψ_2 $\exists v_1 \exists v_2 P(v_1, v_2) \wedge P(v_2, c)$

ψ_3 $\exists v_1 \exists v_2 \exists v_3 P(v_1, v_2) \wedge P(v_2, v_3) \wedge P(v_3, c)$

$\vdots$

ψ_n $\exists v_1 \exists v_2 \exists v_3 \ldots \exists v_n P(v_1, v_2) \wedge P(v_2, v_3) \wedge \ldots \wedge P(v_n, c)$

$\vdots$

Legyen $\Sigma^\star = \Sigma \cup \{\psi_1, \psi_2, \psi_3, \ldots\}$. Most tetszőleges véges $\Sigma' \subset \Sigma^\star$ részhalmaznak megadjuk egy modelljét. Legyen k a legnagyobb olyan n, melyre $\psi_n \in \Sigma'$. Világos, hogy $\langle N, <, =, k\rangle$ egy modellje Σ'-nek, ahol $k \in N$ a c individuum konstanst reprezentáló eleme az univerzumnak. Ha ugyanis egy tetszőleges $\phi \in \Sigma'$ mondat benne van Σ-ban, akkor $\langle N, <, =, k\rangle \models \phi$, hiszen ϕ igaz $\langle N, <, =\rangle$-ban. Ha viszont ϕ nem más, mint valamely ψ_n, ahol $n \leq k$, akkor megint $\langle N, <, =, k\rangle \models \phi$. Hiszen ψ_1 azt mondja, hogy létezik valami, amely kisebb c-nél. És ha c-t úgy interpretáljuk, mint n, ahol $n \geq 1$, akkor ez igaz. ψ_2 azt mondja, hogy két dolog létezik: a második kisebb c-nél, és az első kisebb a másodiknál. És ez igaz $\langle N, <, =, n\rangle$-ben, ha $n \geq 2$. És így tovább, $\langle N, <, =, k\rangle \models \psi_n$ minden $n \leq k$. Tehát $\Sigma^\star$ minden véges részhalmazának létezik modellje. A kompaktsági tétel következtében tehát $\Sigma^\star$-nak is létezik modellje.

Jelöljük ezt a modellt $\mathcal{A}$-val. E modellben minden olyan mondat igaz, amely igaz volt $\langle N, <, =\rangle$-ban, hiszen $\langle N, <, =\rangle \models \phi$ akkor és csak akkor, ha $\Sigma \vdash \phi$. $\mathcal{A}$ tartalmazni fogja az első, a második, a harmadik, stb. elemet a Σ axiómáknak megfelelően. *De tartalmaznia kell a c konstansnak megfelelő univerzum-elemet is!* Ez nem lehet valamelyik természetes szám, hiszen legyen $c = n$. ψ_{n+1} azt mondja, legyen $c > n$, és ez lehetetlen. Tehát az $\mathcal{A}$ modell a természetes számokon kívül tartalmaz még valamit, amely nagyobb minden természetes számnál. Amit így konstruáltunk az

a természetes számok ún. *nem-standard modellje.*

Bonyolultabb, de teljesen hasonló módon lehet megalkotni a nem-standard modelljét az $\langle N, <, =, +, \cdot \rangle$ igaz mondatainak is.

2

A kompaktsági tétel egy másik alkalmazására példa a következő tétel.

32. Tétel. *Legyen Σ mondathalmaz olyan, hogy létezik neki tetszőlegesen nagy véges normál modellje. Ekkor létezik végtelen normál modellje is.*

Bizonyítás

Egészítsük ki a Σ mondatokat tartalmazó nyelvet a $c_1, c_2, \ldots$ individuum konstansok végtelen halmazával. Legyen $\Sigma^\star = \Sigma \cup \{\neg E(c_i, c_j) : i \neq j\}$. Most megmutatjuk, hogy $\Sigma^\star$-nak létezik modellje. Legyen $\Sigma' \subset \Sigma^\star$ tetszőleges véges részhalmaz. Σ', a Σ-ba tartozó mondatokon túl, csak véges sok $\neg E(c_i, c_j)$ mondatot tartalmaz. Ezek csak véges sok c_i individuum konstanst tartalmaznak, melyek mind megtalálhatók a $c_1, c_2, \ldots c_n$ között, valamilyen megfelelően nagy n-re. Mivel feltételezésünk szerint Σ-nak létezik tetszőlegesen nagy véges modellje, feltehető, hogy létezik olyan $\langle U, \ldots \rangle$ modell, hogy benne választható n darab $u_1, u_2, \ldots u_n$ eleme az univerzumnak, úgy, hogy mindegyik különböző. Könnyen belátható, hogy $\langle U, \ldots u_1, u_2, \ldots u_n \ldots \rangle$ modellje az Σ' mondathalmaznak, úgy, hogy a $c_1, c_2, \ldots c_n$ konstansokat az $u_1, u_2, \ldots u_n$ elemek

reprezentálják. A kompaktsági tétel alkalmazásával tehát $\Sigma^\star$-nak létezik modellje, következésképpen normál modellje is (26. tétel). Legyen ez $\langle B, \ldots b_1, b_2, \ldots\rangle$, ahol $b_1, b_2, \ldots$ a $c_1, c_2, \ldots$ konstansok reprezentánsai. $\langle B, \ldots b_1, b_2, \ldots\rangle$ modellje a Σ mondathalmaznak is hiszen Σ része $\Sigma^\star$-nak, és mivel $b_i \neq b_j$ ha $i \neq j$, B végtelen elemű univerzum. Ezzel a tételt bizonyítottuk.

10. A Löwenheim–Skolem–Tarski-tétel

A Gödel–Henkin-tétel bizonyítása után megjegyeztük, hogy valójában azt bizonyítottuk be, hogy tetszőleges konzisztens Σ-nak létezik *megszámlálható* modellje. E modell természetesen nem feltétlenül normál modell. A 26. tétel következtében azonban létezik normál modellje is. A 26. tétel bizonyításában adott konstrukcióból világosan látszik, hogy a normál modell univerzumának számossága nem lehet nagyobb, mint a kiindulásul vett modell univerzumának számossága (az ekvivalencia osztályok száma nem lehet nagyobb, mint az elemek száma!). Ezzel beláttuk, hogy egy megszámlálható nyelv konzisztens mondathalmazának létezik megszámlálható normál modellje.

Hogy e megállapításunk fontosságát érzékeltessük, tekintsük az

$$\mathcal{R} = \langle R, <, =, +, \cdot\rangle$$

struktúrát, ahol R nem más, mint a valós számok $\mathbb{R}$ halmaza. Tekintsünk egy alkalmas nyelvet (amely megszámlálható) e struktúra

leírására. Jelöljük Σ^R-rel e nyelv mindazon mondatainak halmazát, melyek igazak $\mathcal{R}$-ben. A fenti megállapításaink alapján, mivel Σ^R egy megszámlálható nyelv mondatainak konzisztens halmaza, létezik neki megszámlálható normál modellje. Legyen ez

$$\widetilde{\mathcal{R}} = \left\langle \widetilde{R}, \widetilde{<}, \widetilde{=}, \widetilde{+}, \widetilde{\cdot} \right\rangle$$

ahol $\widetilde{R}$ megszámlálható halmaz. Ez nagyon meglepő, ha arra gondolunk, hogy ugyanazok a mondatok lesznek igazak $\mathcal{R}$ és $\widetilde{\mathcal{R}}$ interpretációban, különösen, ha az $\widetilde{R}$ megszámlálható halmaz elemeit valós számoknak tekintjük.

Valójában azt is be lehet bizonyítani, hogy nem csak kisebb számosságú modell létezik, hanem nagyobb számosságú is:

33. Tétel (Löwenheim–Skolem–Tarski). *Ha egy megszámlálható nyelv Σ mondathalmazának létezik végtelen normál modellje, akkor létezik tetszőleges számosságú végtelen normál modellje is.*

11. Turing-gépek és rekurzív függvények

A logika eddigi tárgyalása során számos esetben merült fel annak a gondolata, hogy valami egyszerű mechanikus szabályok alkalmazásával levezethető, kiszámítható. A Turing-gép fogalma és elmélete a mechanikus kiszámíthatóság koncepcióját kívánja megragadni a matematikában.

11.1. A Turing-gép leírása

A gépnek van egy szalagja, amely kis négyzetekre van osztva.

Egy olvasó fej egyszerre egyetlen négyzet tartalmát tudja beolvasni, vagy átírni. Továbbá tud a szalagon egy kockával előre vagy hátra lépni. A gép egy meghatározott ábécét használ: $S_0, S_1, \ldots S_n$, ahol S_0 megállapodás szerint az üres kockának felel meg. Feltételezzük, hogy a gépnek véges sok belső állapota lehetséges: $q_0, q_1, \ldots q_m$. Feltételezzük, hogy a gép egy adott pillanatban a pillanatnyi belső állapota és az éppen beolvasott négyzet tartalma által *egyértelműen determinált módon* teszi meg a következő lépést. Ez a lépés a következők egyike lehet:

(i) megváltoztatja a beolvasott kockában beírt szimbólumot

(ii) egy kockával jobbra lép

(iii) egy kockával balra lép

Mint ebből kiderül, a gép működése egyértelműen megadható a következő fajta négyesekből álló véges táblázat segítségével:

	Állapot	Beolvasott	Akció	Új állapot	
(i)	q_i	S_j	S_k	q_l	átírás
(ii)	q_i	S_j	R	q_l	lépés jobbra
(iii)	q_i	S_j	L	q_l	lépés balra

A gép működésének determinisztikus jellege abban nyilvánul meg, hogy nincs két négyes, amelyik ugyanazzal a ⟨állapot, jel⟩ párral kezdődne. Ha a gép egy olyan ⟨állapot, jel⟩ párhoz érkezik, amelyhez nem tartozik négyes, akkor megáll.

Azt a szituációt, melyben a q_k állapotú gép egy adott jellel ellátott kockáját olvassa be a szalagnak

			$\downarrow q_k$				
$\dots$	S_{i_0}	S_{i_1}	S_{i_1}	S_{i_3}	S_{i_4}	S_{i_5}	$\dots$

a következőképpen fogjuk jelölni:

$$\dots S_{i_0} S_{i_1} q_k S_{i_2} S_{i_3} S_{i_4} S_{i_5} \dots$$

Nevezzük az ilyen stringet *szituáció stringnek*. Például, tegyük fel, a gép a következő instrukciókat kapja:

$$q_1\, S_1\, L\, q_2$$
$$q_2\, S_2\, L\, q_2$$

A szalag nem üres része mondjuk a következő:

$$S_1\, S_2\, S_2\, S_1\, S_2\, \dots S_1$$

és a q_1 állapotú gép éppen a második S_1-et fogja beolvasni. Vagyis

$$S_1\, S_2\, S_2\, q_1\, S_1\, S_2\, \dots S_1$$

Ekkor a $q_1\, S_1\, L\, q_2$ négyesnek megfelelő műveletet hajtja végre, és a következő szituáció fog előállni:

$$S_1\, S_2\, q_2\, S_2\, S_1\, S_2\, \ldots S_1$$

Ekkor a $q_2\, S_2\, L\, q_2$ instrukció szerint azt kapjuk, hogy

$$S_1\, q_2\, S_2\, S_2\, S_1\, S_2\, \ldots S_1$$

majd

$$q_2\, S_1\, S_2\, S_2\, S_1\, S_2\, \ldots S_1$$

és mivel egyetlen instrukció sem kezdődik $q_2\, S_1$-gyel, a gép megáll.

11.2. Példák elemi műveleteket végrehajtó Turing-gépekre

Egy S_j jel keresése

Állapot	Beolvasott	Akció	Új állapot
q_0	S_0	R	q_0
q_0	S_1	R	q_0
$\vdots$			
q_0	S_{j-1}	R	q_0
q_0	S_j	S_j	q_1
q_0	S_{j+1}	R	q_0
$\vdots$			
q_0	S_n	R	q_0

A gép megáll amikor S_j-t talál.
Mozogjon jobbra és mindenre tegyen vesszőt

$$\left.\begin{array}{cccc} q_0 & S' & R & q_0 \\ q_0 & S & S' & q_0 \end{array}\right\} \text{ az abc minden } S, S' \text{ jelére}$$

Ha azt akarjuk, hogy a gép megálljon egy adott jelnél, például $\square$-nál, akkor a táblázatból eltávolítjuk azokat a sorokat, amelyek második eleme $\square$.

Nyilvánvalóan semmi akadálya annak, hogy több elemi műveletet végrehajtani képes Turing-gépet egy komplexebb Turing-géppé rakjunk össze. Hogy a gépeket egymástól megkülönböztessük, az állapotaikat kell megfelelően átnevezni. Pl. a fenti két gépből, készítsünk olyan Turing-gépet, amelyik jobbra mozogva megkeres az első S_j-t, majd onnantól fogva mindenre tesz egy vesszőt! A második gép állapotait átnevezzük, méghozzá éppen úgy, hogy legyen a második gép q_0 állapota az első gép q_1 állapota. Tehát az összetett gép táblázata

$$
\begin{array}{cccc}
q_0 & S_0 & R & q_0 \\
q_0 & S_1 & R & q_0 \\
\vdots & & & \\
q_0 & S_{j-1} & R & q_0 \\
q_0 & S_j & S_j & q_1 \\
q_0 & S_{j+1} & R & q_0 \\
\vdots & & & \\
q_0 & S_n & R & q_0 \\
q_1 & S'_j & R & q_1 \\
q_1 & S_j & S'_j & q_1
\end{array}
$$

HF

Minden jelet tegyen egy kockával jobbra. [Trükk: a gép úgy tud emlékezni egy információra, hogy egy az információnak megfelelő állapotban van. (Vagyis a Turing-gép egy Markov-folymat!)]

HF

A gép a szalagon egy egyesekből álló blokkot lemásol a szalag üres helyére.

Parciális rekurzív függvény

Egy n természetes számot egyszerűen úgy lehet reprezentálni a Turing-gép számára, hogy megadunk a szalagon egy n hosszúságú 1-ekből álló sorozatot, majd egy üres kockát. A Turing-gépek között lesznek olyanok, amelyek az ilyen tartalmú szalagot inputként használva valahol megállnak. Jelölje $f(n)$ a szalagon az olvasó-

fejtől balra lévő egyesek számát. Ezzel a Turing-gép által végrehajtott művelet nem más, mint egy $f : X \subset \mathbb{N} \to \mathbb{N}$ leképezés.

Egy $f : X \subset \mathbb{N} \to \mathbb{N}$ parciális függvényt *parciális rekurzív függvénynek* nevezünk, ha a fenti értelemben reprezentálható egy alkalmas Turing-géppel. Pl. a fenti HF-ból következik, hogy az $f(n) = 2n$ függvény parciális rekurzív függvény.

Eldönthető problémaosztály

Tegyük fel, hogy valamely kérdéseknek/problémáknak egy osztálya megfogalmazható egy véges abc segítségével úgy, hogy felvihető egy Turing-gép szalagjára. (A szokásos meghatározás szerint) Q típusú problémáknak egy osztálya *kiszámítható (eldönthető, megoldható)*, ha létezik olyan M Turing-gép, amely – alkalmazva az osztályba tartozó tetszőleges Q kérdésre – az 1-en áll meg, ha a Q-ra adott válasz IGEN és $\square$-n, ha a válasz NEM.

PL. Legyen Q az a kérdés, hogy adott három természetes szám esetén, (a, b, c), igaz-e, hogy c az a és b legnagyobb közös osztója? Ennek eldöntésére, ismert egyszerű algoritmus alapján, könnyen konstruálható olyan Turing-gép, amely ezt a fenti értelemben eldönti.

11.3. A Turing-gépek standard leírása

Mivel a Turing-gépek véges számú szimbólumot használnak. az általánosság csorbítása nélkül feltehetjük, hogy ezek a jelek a $\square, 1, 1', 1'', \ldots$. Az állapotokat is jelölhetjük a $q, q', q'', \ldots$ jelek-

kel. A gép működését megadhatjuk tehát a $\square, 1, ', q, R, L$ jelekből álló stringek segítségével, pl. a

$$\begin{array}{cccc} q_0 & 1 & R & q_1 \\ q_1 & 1'' & 1' & q_2 \end{array}$$

utasításokból álló táblázat megadható egyértelműen a következő stringgel:

$$q\,1\,R\,q'\,q'\,1''\,1'\,q''$$

Sőt, mindent kifejezhetünk a $\square, 1, 1', 1'', \ldots$ abc-vel:

$$\begin{array}{rcl} \square & \leftrightarrow & \square \\ 1 & \leftrightarrow & 1 \\ ' & \leftrightarrow & 1' \\ q & \leftrightarrow & 1'' \\ R & \leftrightarrow & 1''' \\ L & \leftrightarrow & 1'''' \end{array}$$

Az M Turing-gép működését meghatározó táblázatot tehát egyetlen $\square, 1, 1', 1'', 1''', 1''''$-stringgel megadhatjuk. Ezt a jelsorozatot $\lceil M \rceil$-mel fogjuk jelölni, és a Turing-gép *standard leírásának* nevezzük.

11.4. Egy eldönthetetlen problémaosztály („Halting problem")

Tekintsük a következő kérdést:

Q_M : Megáll-e az M Turing-gép egy $\square$ jelen, ha az $\lceil M \rceil$ jelsorozatra alkalmazzuk?

A Q_M kérdés egyértelműen megadottnak tekinthető az $\lceil M \rceil$ megadásával. Jelölje $\{Q_M\}_M$ az ilyen kérdések osztályát, ahol M tetszőleges Turing-gépet jelöl. Arra keresünk választ, vajon létezhet-e olyan algoritmikus eljárás, magyarul olyan Turing-gép, amely képes megválaszolni *minden* a $\{Q_M\}_M$ osztályba tartozó kérdést.

Képzeljünk el egy S gépet, amelyik teljesíti ezt a feladatot, tehát beolvassa az $\lceil M \rceil$ stringet és 1-en áll meg, ha a válasz a Q_M kérdésre IGEN, és $\square$-n, ha a válasz NEM. A probléma, hogy hogyan viselkedik ez a gép — melynek tetszőleges $\lceil M \rceil$-re működnie kellene —, ha az inputja éppen $\lceil S \rceil$? Ha S megáll az 1-en, az azt jelenti, hogy a Q_S kérdésre a válasz IGEN, azaz az S a $\square$-n áll meg ha $\lceil S \rceil$-ra alkalmazzuk. És fordítva, ha S a $\square$-n áll meg, az azt jelenti, hogy a Q_S kérdésre a válasz NEM, tehát az S gép nem áll meg a $\square$-n. Mindkét esetet egyfajta ellentmondásnak szokás tekinteni, és a szokásos konklúzió az, hogy ilyen S gép nem létezik. Más szóval, hogy a Q_M problémaosztály *algoritmikusan nem megoldható, eldönthetetlen.*

Megjegyzés

Könnyen gondolhatjuk, hogy a probléma abból származik, hogy a gép az IGEN és NEM válaszokat az 1 és $\square$ jeleken való megállással közli, és hogy más lenne a helyzet, ha a gép a $\square$-n állna meg, ha a válasz IGEN és 1-en, ha NEM. Ez azonban nem igaz. Ha létezik

ilyen T gép, akkor könnyen konstruálható egy másik gép, amely a T IGEN jelzését 1-be, a NEM jelzését $\Box$-ba konvertálja, s a két gép kombinációja megint egy olyan Turing-gép lenne, ami eleget tesz az eredeti feltételeinknek, s a fenti argumentum alkalmazható, tehát nem létezhet ilyen gép, következésképpen nem létezhet T sem.

Megjegyzés

Könnyen belátható az is, hogy a helyzeten semmit sem változtat, ha a Q_M kérdést másképpen kódoljuk, hiszen mindig találni olyan Turing-gépet, amelyik a M egy tetszőleges másik kódolását az $\lceil M \rceil$ stringbe konvertálja, és viszont.

Megjegyzés

Mivel hat különböző karaktert használunk, megtehető, hogy az $\lceil M \rceil$ stringet egy hatos számrendszerbeli számként reprezentáljuk. Definiáljuk (*Sic!*) a következő függvényt:

$$\psi(M) = \begin{cases} 1 & \text{ha } Q_M\text{-re a válasz IGEN} \\ 0 & \text{ha } Q_M\text{-re a válasz NEM} \end{cases}$$

Mivel nincs olyan gép, amely ezt megoldaná, a ψ függvény nem parciálisan rekurzív. (Nagyon problematikus példa!)

11.5. Univerzális Turing-gép

Azt gondolhatnánk, hogy a probléma abból fakad, hogy nem lehetséges olyan gépet konstruálni, amely képes átfogni az összes lehetséges Turing-gép működését. Belátható azonban, hogy ilyen gép

létezik. *Univerzális Turing-gépnek* nevezzünk egy olyan U gépet, amely képes arra, hogy beolvassa egy tetszőleges gép $\lceil M \rceil$ standard leírását, és beolvasva egy tetszőleges $\lceil P \rceil$ kódját a szalagnak szimulálja M működését a P szalag-tartalom mellett. (Annak leírását, hogy egy ilyen univerzális Turing-gép hogyan működik, lásd Crossley 40-41 oldal.)

A „Halting" probléma univerzális Turing-gépre

Vizsgáljuk tehát azt a szituációt, amikor az U univerzális Turing-gép az M gépet fogja szimulálni, amikor az az $\lceil M \rceil$ stringre van alkalmazva. Más szóval, U számára adott a

$$W_M = * \lceil M \rceil * * \lceil \lceil M \rceil \rceil *$$

string, mint input. (A $*$ csak segéd jel, amely jelzi a gép számára, hogy mettől meddig terjed egy egybefüggő része a beolvasott stringnek.) Tekintsük a következő kérdést:

Q_W : Megáll-e az U univerzális Turing-gép egy $\square$ jelen, ha a W jelsorozatra alkalmazzuk?

Legyen $\{Q_W\}_W$ az ilyen kérdések osztálya. Létezik-e Turing-gép, amelyik képes megválaszolni a $\{Q_W\}_W$ osztályba tartozó összes kérdést? Válaszunk az, hogy nem.

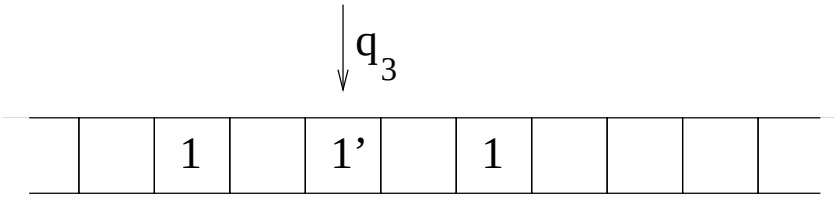
34. Tétel. *A $\{Q_W\}_W$ problémaosztály nem eldönthető.*

Bizonyítás

$\{Q_W\}_W$ nyilván tartalmazza az olyan Q_W kérdéseket is, ahol $W = W_M$. Mivel ilyenkor U szimulálja M működését, U akkor és csak akkor áll meg $\square$-n ha M $\square$-n áll meg, ha M-et $\lceil M \rceil$-re alkalmazzuk. Más szóval, a $\{Q_W\}_W$ problémaosztály csak akkor lehetne eldönthető, ha a $\{Q_M\}_M$ problémaosztály eldönthető lenne.

11.6. Turing-gépek mint string-átalakítók

Mivel a Turing-gép működése közben egy adott pillanatban a szalagjára csak véges sok jel van írva, az adott szituációt egyetlen stringgel lehet jellemezni, amely tartalmazza azt az információt, hogy milyen jelek vannak a szalag azon szakaszára írva, amelyik tartalmazza az éppen beolvasott kockát, a beolvasó fej pillanatnyi pozícióját, és a gép állapotát. Például a



pillanatnyi helyzetet a következő szituáció-stringgel lehet leírni:

$$*1\square q_3 1'\square 1*$$

A gép következő lépésének végrehajtása után egy új szituáció áll elő. Hogy egy W szituációról milyen soron következő W' szituációra jutunk, azt a W-ben megjelenő $q_i S_j$ kombináció határozza meg. A következő szituáció-string átalakítási szabályok vannak:

négyes	transzformáció
$q_iS_jS_kq_l$	$q_iS_j \rightarrowtail q_lS_k$
$q_iS_jRq_l$	$q_iS_jS_k \rightarrowtail S_jq_lS_k$ minden S_k-ra $q_iS_j* \rightarrowtail S_jq_l\square*$
$q_iS_jLq_l$	$S_kq_iS_j \rightarrowtail q_lS_kS_j$ minden S_k-ra $*q_iS_j \rightarrowtail *q_l\square S_j$

Tehát a $*$-nak az a hatása, hogy ha a jobbra vagy balra lépéshez már nincs hely akkor új üres kockát iktat be.

Ezzel a módszerrel egy tetszőleges M gép reprezentálható a megfelelő string-transzformációs szabályok halmazával. Minden szituáció-stringre valamelyik átalakítási szabály vonatkozik, és az egymást követő átalakítások során nyert stringek valóban tükrözik az M gép működése közben kialakuló szituációkat. Az a szituáció-string, amelynél a gép megáll a $\square$ jelnél, tartalmaz egy $q_h\square$ kombinációt, olyat, amely sehol sem jelenik meg a transzformációs szabályok bal oldalán.

Vezessük be erre az esetre a következő transzformációs szabályokat:

$$\left.\begin{array}{lcl} q_h\square & \rightarrowtail & \Diamond \\ \Diamond S & \rightarrowtail & \Diamond \\ S\Diamond & \rightarrowtail & \Diamond \end{array}\right\} \text{ minden } S\text{-re}$$

ahol $\Diamond$ egy újonnan bevezetett szimbólum. Ezzel elérjük, hogy a szituáció-string akkor és csak akkor fejlődik $\Diamond$-ba, ha az M gép megáll $\square$-nél.

M-kalkulus

Nevezzük az így kiegészített transzformációs szabályokat M-kalkulusnak. Azt fogjuk írni, hogy $W \rightarrowtail W'$ ha létezik transzformációknak olyan sorozata az M-kalkulusban, hogy az a W stringet a W' stringbe viszi.

$W \rightarrowtail \Diamond$ akkor és csak akkor, ha a szituáció, amelyet W leír, az M gép megállásához vezet $\Box$-n.

Legyen most az M gép az univerzális Turing-gép. Tekintsük a következő kérdést:

Q'_W: Igaz-e, hogy $W \rightarrowtail \Diamond$ az U-kalkulusban?

És jelölje $\{Q'_W\}_W$ az ilyen kérdések osztályát, ahol W egy tetszőleges szituáció-string. A 34. tétel triviális következménye:

35. Tétel. *A $\{Q'_W\}_W$ problémaosztály nem eldönthető.*

11.7. A string-átalakítások reprezentációja a predikátum kalkulusban

Az elsőrendű nyelv, amelyet használni fogunk, a következőket tartalmazza:

$\Box, 1, \Diamond, *, \ldots$ konstansok az U-kalkulusban

f függvény, amely stringeket fűz össze

Tr két argumentumos predikátum a transzformációk leírására

Függvény a betűk összefűzésére

Az $f(x, y)$ függvényt röviden csak (x, y)-nal fogjuk jelölni, és a következő axiómának tesz eleget:

(1) $(x\,(yz)) = ((xy)\,z)$

Így tetszőleges string konstans terminusnak tekinthető. Pl. az $*\Box q_3 1*$ string úgy írható, mint $(*\,(\Box\,(q_3\,(1\,(*)))))$. (1) axióma következtében a zárójeleket tetszés szerint átcsoportosíthatjuk, tehát nincs jelentőségük, ezért elhagyjuk.

A stringek átalakítására vonatkozó axiómák

Legyen t_1 és t_2 két tetszőleges terminus. A $Tr\,(t_1, t_2)$-re vonatkozóan elég sok axiómát kívánunk rögzíteni ahhoz, hogy garantálva legyen, hogy tetszőleges két szituáció-stringet leíró W_1 és W_2 konstansra a $Tr\,(W_1, W_2)$ akkor és csak akkor legyen levezethető, ha $W_1 \rightarrowtail W_2$. Elsőként,

(2) $Tr\,(xTy, xT'y)$ valahányszor $T \rightarrowtail T'$ az U-kalkulusban.

Világos, hogy ez az axiómaséma garantálni fogja a megkívánt tulajdonságot, minden olyan $W_1 = XTY$ és $W_2 = XT'Y$ stringekre, ahol T a transzformációs szabályok egyikben a baloldalon szerepel, vagyis, amikor W_2 közvetlen következménye W_1-nek valamely $T \rightarrowtail T'$ transzformációval.

Most nyilván hozzá kell tennünk a következő axiómát:

(3) $(Tr(x, y) \wedge Tr(y, z)) \rightarrow Tr(x, z)$

Ezzel elértük, hogy (1)$\wedge$(2)$\wedge$(3) $\vdash Tr\,(W_1, W_2)$ akkor és csak akkor, ha $W_1 \rightarrowtail W_2$.

Az axiómák eliminálása, eldönthetetlenség

Mivel véges sok axiómánk van (mert véges sok $T \rightarrowtail T'$ transz-

formációs szabály van), ezeket egyetlen nagy konjunkcióba összefoglalhatjuk. Legyen ez ϕ. Tehát, $W_1 \rightarrowtail W_2$ akkor és csak akkor, ha $\phi \vdash Tr\,(W_1, W_2)$, ami akkor és csak akkor, ha $\vdash \phi \rightarrow Tr\,(W_1, W_2)$. Speciálisan:

36. Tétel. *$W \rightarrowtail \Diamond$ akkor és csak akkor, ha $\vdash \phi \rightarrow Tr\,(W, \Diamond)$*

.

Definiáljuk a következő kérdést:

Q_ψ: Igaz-e, hogy $\vdash \psi$?

És legyen $\{Q_\psi\}_\psi$ az ilyen kérdések osztálya, ahol ψ tetszőleges formulája PC-nek.

37. Tétel. *A $\{Q_\psi\}_\psi$ problémaosztály nem eldönthető.*

Bizonyítás

Ha a $\{Q_\psi\}_\psi$ problémaosztály eldönthető lenne, akkor eldönthető lenne a $\phi \rightarrow Tr\,(W, \Diamond)$ típusú formulákra vonatkozó szűkebb osztály is. A 36. tétel miatt azonban ez csak akkor lehetne igaz, ha eldöntető lenne a $\{Q'_W\}_W$ problémaosztály, ami — mint a 35. tétel kimondja — nem áll fenn, s ezzel a tételt bizonyítottuk.

Tekintsük végül a következő kérdést:

Q'_ψ: Igaz-e, hogy $\models \psi$?

És legyen $\left\{Q'_\psi\right\}_\psi$ az ilyen kérdések osztálya, ahol ψ tetszőleges formulája PC-nek. A teljességi tétel kimondja (22. tétel), hogy $\vdash \psi$

akkor és csak akkor, ha $\models \psi$. Vagyis a 37. tétellel együtt azt is bizonyítottul, hogy

38. Tétel. *A* $\left\{Q'_\psi\right\}_\psi$ *problémaosztály nem eldönthető.*

Megjegyzés

1

Elkerülendő a félreértéseket, amelyekkel a populáris irodalomban gyakran találkozunk, ne gondoljunk többet a fenti eldönthetetlenségi tételek mögé, mint amit valójában bizonyítottunk! *A tételek nem azt állítják, hogy az adott problémaosztályba tartozó problémák nem dönthetők el algoritmikusan!* A tételek azt állítják, hogy *nem létezik egyetlen* algoritmus (Turing-gép), amely az osztályba tartozó *összes* kérdést meg tudja válaszolni.

2

A „Halting" probléma tárgyalásánál felbukkan az „önreferencia" motívuma. Világosan kell látni azonban, hogy ennek nincs különösebb jelentősége, és semmi köze nincs a „megismerhető-e a világ, amelynek mi is részei vagyunk" jellegű endofizikai problémához és más episztemológiai kérdéshez. Egyáltalán, a szóban forgó matematikai tételek mögött — még ha le is fordítjuk őket valamilyen valóságos szituációra — semmiféle metafizikai mélység nincs. Amikor az univerzális Turing-gép a $*\lceil M\rceil **\lceil\lceil M\rceil\rceil *$ stringet olvassa be, akkor egyszerűen olyan utasítások összességét programozzuk bele, melynek alapján egyszerre kellene neki igent és nemet mondania, amit nyilván nem tud, ugyanúgy, mint egy biciklivel nem

lehet egyszerre jobbra és balra kanyarodni, vagy kérdéses mi történik egy autóval, ha egyszerre nyomjuk a féket és a gázt.

12. Az aritmetika axiómái

Az aritmetika axiomatikus elméletét a PC(=)-ben fogjuk megfogalmazni:

(A1) $\neg\,(0 = sx)$

(A2) $(sx = sy) \to (x = y)$

(A3) $x + 0 = x$

(A4) $x + sy = s(x + y)$

(A5) $x \cdot 0 = 0$

(A6) $x \cdot sy = (x \cdot y) + x$

(A7) $(\psi(0) \wedge \forall x\,(\psi(x) \to \psi(sx))) \to \forall x \psi(x)$

ahol természetesen $x = y$, $x + y$ illetve $x \cdot y$ az $E(x, y)$, $+(x, y)$ illetve $\cdot(x, y)$ helyett áll, ahol E az egyenlőség predikátum, $+$ és $\cdot$ pedig függvények. Az s függvény szemléletes jelentése a „hozzáadunk egyet" művelet, ψ pedig egy tetszőleges formula. (A7)-et az *indukció axiómasémájának* is szokás nevezni. Ezeknek az axiómáknak a halmazát úgy fogjuk jelölni, hogy {aritmetika}.

HF

- Adjuk meg ebben a nyelvben azt a formulát, amelynek szemléletes jelentése az lenne, hogy egy szám a másiknak osztója.

- Adjuk meg azt a formulát, amelynek szemléletes jelentése az, hogy egy szám prím szám.

Vezessük be a $1, 2, 3, \ldots$ jeleket a következő terminusok jelölésére:

1: $s0$

2: $ss0$

$\vdots$

k: $\underbrace{s \ldots ss}_{k \text{ darab}} 0$

$\vdots$

Megjegyzés

1

A jelölésekben használjuk a számokat és írunk olyat, hogy „k-darab", stb. Vegyük észre, hogy ezek csak kényelmi, tipográfiai eszközök, és nem történik lényegi hivatkozás valamilyen „előzetesen ismert aritmetikára".

2

Gyakran olvashatunk az irodalomban olyan gondolatmeneteket, amelyek a „szándékolt interpretációról" szólnak. Természetesen, lehet valamilyen intuíciónk előzetesen arról, hogy az axiomatikusan felépítendő matematikai struktúrától mit várunk. De ennek szigorú, elméleti, matematikai értelemben nyilván nem lehet semmiféle jelentősége. (A matematikában egyébként is számtalanszor elfogadunk formális elméleti gondolatmenetek útján nyert konklúziókat, melyek esetleg ellentmondanak a „józan észnek", vagy az

előzetes intuitív várakozásainknak. Gondoljunk például arra, hogy intuitíve több racionális számnak kellene lennie, mint egész számnak, mégis elfogadjuk a formális bizonyítást, hogy a két halmaz számossága azonos.)

Összegezve tehát, az aritmetika *az*, amit most axiomatikusan felépítünk!

3

Természetesen lehet arról beszélni, hogy egy axiomatikusan felépített aritmetika hasznos matematikai struktúra-e számunkra, abban az értelemben, hogy használható-e a világ leírásában, vagyis a fizikai elméletekben. Tehát az aritmetika axiomatikus felépítése során lehet az a szándékunk, hogy egy olyan struktúrát hozzunk létre, amely majd alkalmas lesz — egy megfelelő fizikai elmélet részeként — annak leírására, hogy hogyan működik a pénztárgép, vagy alkalmazható lesz abban a fizikai elméletben, amelyet egy juhász használ a nyájba tartozó juhok nyilvántartására, stb.

4

Egyelőre nem tudjuk tehát azt sem, hogy pl. „2+2=4". Ezt csak akkor állíthatjuk, ha bebizonyítottuk. Tehát, bizonyítsuk be, hogy $2 + 2 = 4$!

39. Tétel. $\{aritmetika\} \vdash 2 + 2 = 4$ *a PC(=)-ben.*

Bizonyítás

A jelölések definícióját alapul véve tehát azt kell bizonyítanunk, hogy $ss0 + ss0 = ssss0$:

1. $ss0 + ss0 = s(ss0 + s0)$ [(A4)-ből]

2. $s(ss0 + s0) = ss(ss0 + 0)$ [(A4)-ből]

3. $ss0 + ss0 = ss(ss0 + 0)$ [1. és 2. alapján (E2) és (MP) felhasználásával]

4. $ss0 + 0 = ss0$ [(A3)-ból]

5. $ss0 + ss0 = ssss0$ [3. és 4. alapján (E3) és (MP) felhasználásával]

HF

Bizonyítsuk be, hogy „$2 \cdot 2 \neq 5$”, azaz, hogy $\{\text{aritmetika}\} \vdash \neg(2 \cdot 2 = 5)$!

5

Félreértések elkerülése érdekében felhívjuk a figyelmet arra, hogy az itt alkalmazott jelölések eltérnek a tankönyvekben szokásos jelölésektől. Az itt számokkal jelölt $1, 2, \ldots$, és számoknak, tehát „egynek”, „kettőnek”, stb. nevezett individuum konstansok rendszerint valamilyen megkülönböztető jelölést kapnak, $\bar{1}, \bar{2}, \bar{3}, \ldots$ (lásd Crossley), vagy $0^{(1)}, 0^{(2)}, 0^{(3)}$, (lásd Hamilton), stb. És rendszerint nem is nevezik őket számoknak, hanem „számjegyeknek”, „számneveknek” (numerals, numeral terms), megkülönböztetésül az „igazi” számoktól, azaz valamilyen értelemben már előzetesen létező számelmélet szám-fogalmától, melyeknek a fenti értelemben

vett axiomatikus aritmetika valamiféle „axiomatizált” elmélete. Az itt szorgalmazott felfogás szerint azonban az aritmetika az, amit itt axiomatikusan megadunk. Nincsenek „aritmetikai igazságok” mások, mint amiket az axiomatikus aritmetikában az axiómákból levezethetünk. Semmi okunk tehát arra, hogy éppen azt jelöljük valami mással, ami van, és azt jelöljük $1, 2, 3, \ldots$-mal, ami nincs!

13. Gödel inkomplettségi tétel

13.1. Gödel-számozás

Egy formula Gödel-száma

Az aritmetikában használt jelekhez számokat rendelünk:

$$\begin{array}{rcl} 0 & \Leftrightarrow & 1 \\ s & \Leftrightarrow & 2 \\ + & \Leftrightarrow & 3 \\ \cdot & \Leftrightarrow & 4 \\ = & \Leftrightarrow & 5 \\ (& \Leftrightarrow & 6 \\ ) & \Leftrightarrow & 7 \\ , & \Leftrightarrow & 8 \\ x & \Leftrightarrow & 9 \\ | & \Leftrightarrow & 10 \\ \neg & \Leftrightarrow & 11 \\ \wedge & \Leftrightarrow & 12 \\ \exists & \Leftrightarrow & 13 \end{array}$$

A változók jelölésére használjuk a $x_|, x_{||}, x_{|||}, \ldots$ jeleket. Tekintsük az aritmetika egy formuláját, például

$$+(s(s(0)), s(s(0))) = s(s(s(s(0))))$$

Ehhez a következőképpen rendelünk számot:

$$\begin{array}{cccccccccc} + & (& s & (& s & \ldots &) &) &) \\ 3 & 6 & 2 & 6 & 2 & \ldots & 7 & 7 & 7 \\ 2 & 3 & 5 & 7 & 11 & \ldots & 113 & 127 & 131 \end{array}$$

$$2^3 3^6 5^2 7^6 11^2 \ldots 113^7 127^7 131^7$$

Világos, hogy ezzel a módszerrel minden ϕ formulához egyértelműen hozzárendeltünk egy számot. Ezt a számot a ϕ formula *Gödel-számának* nevezzük, és $\lceil\phi\rceil$-vel fogjuk jelölni. Természetesen, nem minden természetes szám Gödel-száma valamilyen formulának. De ha az, a prímfelbontás egyértelműsége miatt, egyértelmű, hogy milyen formula Gödel-számáról van szó.

Egy formula sorozat Gödel-száma

Legyen $\phi_1, \phi_2, \phi_3, \ldots$ formulák egy sorozata. A formulasorozathoz rendelt Gödel-szám: $2^{\lceil\phi_1\rceil}3^{\lceil\phi_2\rceil}5^{\lceil\phi_3\rceil}\ldots$ Világos, hogy a prímfelbontás egyértelműsége miatt egy formulasorozat Gödel-száma egyértelműen meghatározza, hogy milyen formulák sorozatáról van szó.

13.2. Gödel-mondat

Tekintsük a következő meta-elméleti (tehát az aritmetikáról szóló) predikátumot:

$Pf^M(x, y)$: az x Gödel-számú formulasorozat az y Gödel-számú formula bizonyítása.

Most kicsit bonyolítsuk meg:

$Pf^M(x, y, z)$: x azon formula bizonyításának a Gödel-száma, melyet az y Gödel-számú, egy szabad változót tartalmazó formulából kapunk, úgy, hogy a változó helyére a z számot (individuum változót) helyettesítjük.

A $Pf^M(x, y, z)$ állításra úgy tekinthetünk, mint számok közötti

relációra, vagyis az állítás akkor és csak akkor igaz, ha a megfelelő reláció fennáll. Ha mondunk három számot, x, y, z, akkor egyszerű aritmetikai algoritmusoknak a (természetesen bonyolult) sorozatával eldönthető, hogy a $Pf^M(x, y, z)$ mondat igaz-e vagy hamis. Hiszen számok prímfelbontását, és más hasonló aritmetikai műveleteket kell ehhez elvégezni. (A megfelelő reláció rekurzíve megadható.) Ennek alapján megmutatható, hogy létezik olyan $Pf(x, y, z)$ formulája az aritmetikának, amelyre

$$\begin{array}{rl} \{\text{aritmetika}\} \vdash Pf(x, y, z) & \text{ha } Pf^M(x, y, z) \text{ igaz} \\ \{\text{aritmetika}\} \vdash \neg Pf(x, y, z) & \text{ha } Pf^M(x, y, z) \text{ hamis} \end{array} \tag{2}$$

Tekintsük most a $\neg\exists x Pf(x, y, y)$ formulát az aritmetikában. Legyen ennek a formulának a Gödel-száma g. A következő mondatot Gödel-mondatnak szokás nevezni:

$$\neg\exists x Pf(x, g, g)$$

és G-vel fogjuk jelölni.

40. Tétel. *Sem G, sem $\neg G$ nem vezethető le az aritmetikában, tehát*

$$\begin{array}{l} \{aritmetika\} \nvdash G \\ \{aritmetika\} \nvdash \neg G \end{array}$$

Bizonyítás

Tegyük fel, hogy G bizonyítható, vagyis hogy $\{\text{aritmetika}\} \vdash \neg\exists x Pf(x, g, g)$. Legyen a bizonyítását alkotó formulasorozat Gödel-száma m. Tekintettel arra, hogy a g Gödel-számú formula a $\neg\exists x Pf(x, y, y)$, ez azt jelenti, hogy m a Gödel-száma azon formula bizonyításának, melyet úgy kapunk, hogy a g Gödel-számú formulában a változó helyére g-t helyettesítünk. Azaz, a $Pf^M(m, g, g)$ mondat igaz, más szóval az m, g, g számokra fennáll a megfelelő reláció, vagyis $\{\text{aritmetika}\} \vdash Pf(m, g, g)$, ami ellentmondás.

Most tegyük fel, hogy $\neg G$ bizonyítható, tehát $\{\text{aritmetika}\} \vdash \neg\neg\exists x Pf(x, g, g)$, vagyis $\{\text{aritmetika}\} \vdash \exists x Pf(x, g, g)$. De az az első részben éppen azt bizonyítottuk, hogy $\{\text{aritmetika}\} \nvdash \neg\exists x Pf(x, g, g)$, más szóval, hogy nincs olyan formulasorozat, amely bizonyítása lenne $\neg\exists x Pf(x, g, g)$-nek. Ez azonban azt jelenti, hogy 1 nem Gödel-száma egy megfelelő bizonyításnak, vagyis $Pf^M(1, g, g)$ hamis, hasonlóan, $Pf^M(2, g, g)$ hamis, és így tovább. Következésképpen,

$$\begin{aligned} \{\text{aritmetika}\} &\vdash \neg Pf(1, g, g) \\ \{\text{aritmetika}\} &\vdash \neg Pf(2, g, g) \\ &\vdots \end{aligned}$$

ami ellentmondás, ha feltesszük, hogy az aritmetika ω-konzisztens, ami azt jelenti, hogy nem létezik olyan egy szabad változót tartalmazó $\phi(x)$ formula, amelyre egyszerre fennállna, hogy

$$\{\text{aritmetika}\} \vdash \exists x \phi(x)$$

$$\begin{aligned} \{\text{aritmetika}\} &\vdash \neg\phi(1) \\ \{\text{aritmetika}\} &\vdash \neg\phi(2) \\ \{\text{aritmetika}\} &\vdash \neg\phi(3) \\ &\vdots \end{aligned}$$

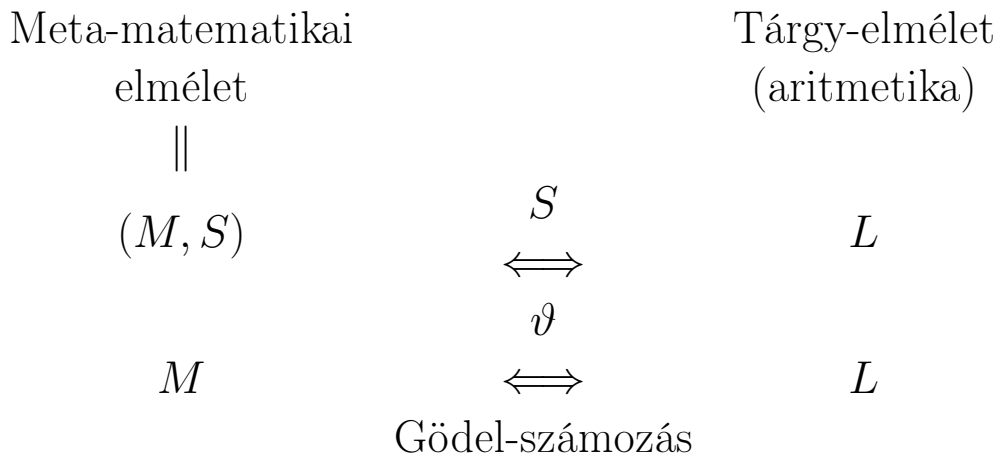
A tétel alapján tehát azt mondhatjuk, hogy az aritmetika vagy nem ω-konzisztens, vagy létezik benne olyan mondat, amelyre az áll, hogy sem ő, sem a negáltja nem bizonyítható.

Megjegyzés

Gödel-féle eredeti bizonyítás kis módosításával sikerült gyengébb feltétel mellett is bebizonyítani a tételt, nevezetesen, hogy ha az aritmetika *konzisztens*, akkor létezik benne olyan mondat, hogy sem ő sem a negáltja nem bizonyítható.

13.3. Bizonyítás és Igazság

"Röviden, Gödel megmutatta, hogy a bizonyítás az igazságnál gyengébb fogalom, függetlenül a használt axiómarendszertől." — írja Hofstadter a *Gödel, Escher, Bach* c. művében. Vitatkoznunk kell ezzel a széles körben elterjedt nézettel, noha a tétel jelentésének egy ilyenfajta értelmezése nem áll távol Gödel platonista nézeteivel. Tekintsük át újra a Gödel-tétel bizonyításának sémáját:



Vagyis, adott egy meta-matematikai elmélete az L formális rendszernek. Ez azt jelenti, hogy adott egy másik formális rendszer M és egy szemantika S, ami M-et és L-et összeköti. Például olyan mondatokat tudunk mondani M-ben, mint „a ϕ formula L-ben nem bizonyítható”, amely az L egy tulajdonságát hivatott állítani. Jelöljük az egyszerűség kedvéért ezt a mondatot $nb(\phi)$-vel. Az ilyen és hasonló mondatoknak van egy Igazság$_2$ értelemben vett igazsága az (M, S)-ben. Vagyis egy M-beli formula akkor igaz_2^M, ha az S szemantika értelmében ő egy olyan állítás L-ről, amely tényszerűen fennáll L-re. Például, $nb(\phi)$ akkor igaz_2^M, ha nem létezik ϕ-nak bizonyítása L-ben, más szóval, ha nem igaz, hogy ϕ igaz_1^L.

A tétel bizonyításában ezek után megjelenik egy másik leképezés is, a Gödel-számozás által generált ϑ leképezés. (Szokás ezt Gödel-izomorfizmusnak nevezni.) Gyakran tévesen azt állítják, hogy ϑ „megőrzi az igazságot”, vagyis, hogy ha α igaz_2^M, akkor

$\vartheta(\alpha)$ igaz L-ben. Más szóval, hogy Gödel-zseniális trükkje éppen az volt, hogy az aritmetikáról szóló meta-matematikai elméletet reprezentálta magában az aritmetikában.

Erről azonban nincs szó. Vegyük észre, hogy a bizonyításban nem is használtuk ki, hogy ϑ egy igazság-megőrző izomorfizmus lenne. Csupán azt tettük fel (láttuk be), hogy speciálisan a $Pf^M(x,y,z)$ típusú meta-elméleti mondatokon az. Vagyis, hogy ha $Pf^M(x,y,z)$ Igaz_2^M, akkor $\{\text{aritmetika}\} \vdash Pf(x,y,z)$, ahol $Pf(x,y,z)$ a $\vartheta\left(Pf^M(x,y,z)\right)$ formulát jelöli, és ha $Pf^M(x,y,z)$ nem Igaz_2^M, akkor $\{\text{aritmetika}\} \vdash \neg Pf(x,y,z)$.

Téves tehát minden olyan megfogalmazás, hogy a G Gödel-mondat, vagyis a $\neg\exists x Pf(x,g,g)$ aritmetikai mondat azzal a meta-elméleti jelentéssel bír, hogy „G (vagyis saját maga) nem bizonyítható L-ben", vagyis $nb(G)$. Ezt csak akkor mondhatnánk, ha valóban megadtunk volna egy olyan igazság-megőrző leképezést M-ből L-be, amelyik kiterjed $nb(G)$-re is és amelyre igaz, hogy $\vartheta\left(nb(G)\right) = G$. Éppen a bizonyított tétel teszi ezt lehetetlenné. Ha ugyanis, G valóban reprezentálná az $nb(G)$ meta-matematikai állítást, akkor teljesülnie kellene, hogy $nb(G)$ akkor és csak akkor Igaz_2^M, ha az őt reprezentáló $G = \vartheta\left(nb(G)\right)$ formula Igaz_1^L, azaz $\vdash_L G$. De a tétel szerint G nem bizonyítható, tehát az $nb(G)$ meta-matematikai állítás Igaz_2^M, ezzel szemben nem aáll fenn, hogy $\vdash_L G$, tehát G nem reprezentálhatja az $nb(G)$ meta-elméleti mondatot.

Természetesen, ezzel együtt az is értelmetlen, hogy „a G mondat »igaz«, hiszen azt állítja, hogy ő nem bizonyítható, és — minthogy

bebizonyítottuk, hogy nem bizonyítható — igazat állít."

Megjegyzés

Gyakori felvetés, hogy a tételben levezetett állítás önmagában is paradox. Az tudniillik, hogy van olyan mondata az aritmetikának, amelyre az áll, hogy sem ő sem a negáltja nem bizonyítható. Nem kétséges, hogy a matematikai platonista számára ez az tény zavarbaejtő. Minthogy a matematika tanítása erősen platonista szemléletet alakit ki már gyermekkorban, sokan gondolják úgy, hogy mivel a Gödel-mondat az aritmetika egy mondata, egy számokról tett kijelentés, szükségképpen vagy igaz vagy hamis. Nem tehetünk mást, mint hogy hangsúlyozzuk: aritmetika az, amit itt axiomatikusan megadtunk. És az mondható „igaznak" az aritmetikában, amit az adott rendszerben bizonyítani lehet.

14. Gödel második inkomplettségi tétele

Az aritmetika akkor és csak akkor konzisztens, ha $\{\text{aritmetika}\} \nvdash 0 = 1$. Ha ugyanis $\{\text{aritmetika}\} \vdash 0 = 1$, akkor (A1)-ből és (A2)-ből azonnal a negáltja is következik, tehát a rendszer inkonzisztens. Másfelől, ha a rendszer inkonzisztens, akkor a 3. tételből következően bármilyen mondat levezethető, így az is, hogy $0 = 1$. Az „aritmetika konzisztens" meta-matematikai állítás tehát ekvivalens

azzal a meta-matematikai állítással, hogy „nem vezethető le a $0 = 1$ formula az aritmetikában”.

Jelöljük a $0 = 1$ formula Gödel-számát k-val, és tekintsük most a következő $Consis$-nek nevezett mondatot:

$$\forall x \neg Pf(x, k)$$

Bonyolult bizonyítással levezethető az aritmetikában, hogy $Consis \rightarrow G$ ahol G a $\neg \exists x Pf(x, g, g)$ Gödel-mondatot jelöli. Ha tehát $Consis$ levezethető lenne az aritmetikában, azaz $\{\text{aritmetika}\} \vdash Consis$, akkor a $\{\text{aritmetika}\} \vdash Consis \rightarrow G$-ből (MP)-vel azonnal következne G, melyről viszont bebizonyítottuk, hogy nem levezethető. Vagyis igaz a következő tétel:

41. Tétel (Gödel II. inkompletségi tétel). *A $Consis$ mondat nem vezethető le az aritmetikában.*

Megjegyzés

A tételt rendszerint úgy interpretálják, hogy az aritmetika konzisztenciáját nem lehet magában az aritmetikában bizonyítani. Ez az interpretáció azonban hamis: Nem igaz, hogy a $Consis$ mondat, vagyis a $\forall x \neg Pf(x, k)$ a „Nem vezethető le a $0 = 1$ formula az aritmetikában”, vagy a vele ekvivalens „Az aritmetika konzisztens” meta-elméleti mondatot reprezentálja. Ahhoz ugyanis, hogy

a $Consis$ valóban reprezentálja „az aritmetika konzisztens" meta-matematikai mondatot az aritmetikában, (2) értelmében annak kellene teljesülnie, hogy $\vdash_L Consis$, ha a rendszer konzisztens, és $\vdash_L \neg Consis$, ha a rendszer inkonzisztens. De ez nem teljesül! Hiszen éppen akkor, ha az aritmetika konzisztens, $Consis$ nem tétel (második Gödel-tétel). Ráadásul, amikor az aritmetika inkonzisztens, akkor tétel.

Bizonyos értelemben semmilyen L rendszer konzisztenciáját nem lehetséges magában a renszerben reprezentálni a (2) értelemben. Hiszen tegyük fel, hogy ψ lenne az L azon formulája, amelyik az „L konzisztens" meta-matematikai mondatot reprezentálja. A legtöbb, ami megvalósulhat, hogy L konzisztens és a ψ mondat levezethető. E tény azonban sohasem tekinthető a konzisztencia indikátorának, hiszen ψ nyilván akkor is levezethető, ha L inkonzisztens. A $Consis$ esetében, mint megállapítottuk, a helyzet csak rosszabb!

A helytelen értelmezés forrása természetesen az, hogy az egyébként *jelentés nélküli* $\forall x \neg Pf(x, k)$ formulát valamiféle intuíció alapján meta-matematikai jelentéssel ruházzuk fel.

15. Halmazelmélet

15.1. „Naiv" halmazelmélet — formális (axiomatikus) halmazelmélet

Szokás azt mondani, hogy azért kell a halmazelméletet „axiomatizálni", mert a „naiv" halmazelméletben bizonyos paradoxonok fogalmazhatók meg, és az axiomatikus módszerrel ezek kiküszöbölhetők. Természetesen nem ezért kell megadnunk a halmazelmélet axiomatikus elméletét, hanem azért, hogy egyáltalán legyen halmazelmélet. Más szóval, nincs „naiv" halmazelmélet! (Legfeljebb abban a didaktikai értelemben, ha egy tankönyvben bevezetünk néhány halmazelméleti fogalmat és kimondunk néhány halmazelméleti tételt, anélkül, hogy megadnánk ezek bizonyítását.)

Ernst Zermelo (1905) és Abraham Fraenkel (1920) után, a halmazelmélet itt tárgyalt axiomatikus elméletét ZF-nek szokás nevezni.

A halmazelméletet a PC(=)-ben adjuk meg. Az egyenlőségen kívül a nyelv tartalmazni fog egy kétváltozós predikátumot, $\in$ („eleme").

15.2. A halmazelmélet (ZF) axiómái

(ZF1) $\exists x \forall u \neg (u \in x)$
(üres halmaz axióma) Mivel ez az axióma garantálja az üres halmaz

létezését, bevezetjük az üres halmaz jelölésére a $\emptyset$ jelet.

(ZF2) $\forall x \forall y \left(\forall u \left(u \in x \leftrightarrow u \in y\right) \leftrightarrow x = y\right)$

(meghatározottsági axióma) Az axióma azt fejezi ki, hogy a halmazokat egyértelműen meghatározza, hogy mik az elemei.

Jelölés

$u \subseteq v$ a következő formula rövidítése: $\forall x \left(x \in u \rightarrow x \in v\right)$

(ZF3) $\forall x \forall y \exists z \forall u \left(u \in z \leftrightarrow u = x \vee u = y\right)$

(páraxióma) Vagyis két halmazból lehet képezni egy olyan halmazt, amelynek ők az elemei.

Jelölés

Az axióma által garantált z halmazt szokás a következőképpen jelölni: $\{x, y\}$

(ZF4) $\forall x \exists y \forall z (z \in y \leftrightarrow \exists u \left(u \in x \wedge z \in u\right))$

(az unió axiómája)

Jelölés

Azt az objektumot, amelynek létezését (ZF4) garantálja $\cup x$-el fogjuk jelölni. Pl. két halmaz uniójára, vagyis az $\cup \{x, y\}$ halmazra bevezetjük az $x \cup y$ jelölést.

(ZF5) $\forall x \exists y \forall z \left(z \in y \leftrightarrow z \subseteq x\right)$

(a hatványhalmaz axiómája)

Jelölés

Az axióma által garantált y halmazt szokás 2^x-el jelölni.

(ZF6) $\forall x \exists y \phi \left(x, y\right) \rightarrow \forall z \exists u \forall v \left(v \in u \leftrightarrow \exists o \left(o \in z \wedge \phi \left(o, v\right)\right)\right)$, ahol $\phi \left(x, y\right)$ tetszőleges két szabad változót tartalmazó formula, melyben feltesszük, hogy a $\forall v$ és $\forall o$ kvantifikációk nem fordulnak

elő.

(helyettesítési axiómaséma)

(ZF7) $\exists x\,(\emptyset \in x \wedge \forall y\,(y \in x \rightarrow y \cup \{y\} \in x))$ ($\{y\}$ a rövidítése az $\{y, y\}$-nak)

(a végtelen halmaz axiómája)

(ZF8) $\forall x\,(\neg x = \emptyset \rightarrow \exists y\,(y \in x \wedge \neg\exists z\,(z \in y \wedge z \in x)))$

(regularitási axióma) Vagyis, hogy minden nem üres x halmaznak van olyan eleme, amely diszjunkt x-től. Ezzel elérjük azt, hogy egyetlen halmaz sem lehet eleme önmagának.

(ZF1)–(ZF8) elégséges ahhoz, hogy a matematika egy jelentős részét felépítsük. Pl. a természetes számok egy modelljét a következő halmazokból álló univerzumon adhatjuk meg:

0 $\emptyset$

1 $\{\emptyset\}$

2 $\{\emptyset, \{\emptyset\}\}$

3 $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$

$\vdots$

ZFC

(AC) Tetszőleges nem üres x halmazhoz létezik olyan y halmaz, amelyre igaz, hogy x minden elemével pontosan egy közös eleme van.

Kontinuum Hipotézis

(CH) Valós számokból álló tetszőleges végtelen halmaz vagy megszámlálható számosságú, vagy kontinuum számosságú.

E két utolsó axiómát illetően kérdések merültek fel. Le lehet-e

vezetni ezeket a (ZF1)–(ZF8)-ból? És ha nem, konzisztens módon hozzávehetők-e az alap ZF rendszerhez, külön-külön, és együtt? Ezekre a kérdésekre részben 1938-ban Gödel egyik munkájában, majd később (1963) Cohen munkáiban kaptunk választ. Gödel megmutatta, hogy ha a ZF konzisztens, akkor (AC) és (CH) konzisztens módon hozzávehető az axiómarendszerhez. Cohen azt mutatta meg, hogy sem (AC) illetve (CH), sem a negáltjaik nem vezethetők le a ZF-ből, tehát független axiómákról van szó. (Egymástól is függetlenek.)

Megjegyzés

1

Az interpretációról és a modell-elméletről szóló fejezetekben mélyen hallgattunk arról, hogy honnan vannak halmazok és azokon értelmezett relációk. Pontosabban, hogy honnan vesszük, hogy azok az állítások, amelyeket az interpretációt jelentő halmazelméleti struktúrákra vonatkozóan tettünk, igazak. Ezek a fejezetek most váltak teljessé, azzal, hogy megadtuk a halmazelmélet axiómáit. Például, a 38. oldalon a teljesítés fogalmának definíciójában, $\mathcal{A} \models P(x_1, x_2)[u_1, u_2]$ akkor és csak akkor, ha $\{ZF\} \vdash \{u_1, u_2\} \in R$. Természetesen a modell-elméleti szemantika még ezzel sem teljesen problémamentes. Hiszen az interpretálandó elsőrendű nyelv elemei és a halmazelméleten belül, mint másik elsőrendű nyelven belül definiált, az interpretációt nyújtó struktúra elemei közötti megfeleltetés nincs valamely formális, elsőrendű nyelv keretei között megadva, hanem a metanyelv, ha tet-

szik a köznapi magyar nyelv segítségével van elmesélve. Valamint a az teljesülés definíciójában valójában nem a ZF-ben levezethető állításokra hagyatkozunk, hanem a ZF-ről szóló metamatematikai állításokra. Világosan látszik ez a „$\mathcal{A} \models \neg P(x_1, x_2)[u_1, u_2]$ akkor és és csak akkor, ha $\{ZF\} \nvdash \{u_1, u_2\} \in R$" definícióban.

2

Első pillantásra bizarrnak tűnhet, a halmazelméletnek a modelljeiről beszélni, hiszen ez azt jelenti, hogy a halmazelméletnek a halmazelméletben adjuk meg az interpretációját. Valójában itt nincs semmi probléma, és formálisan ugyanúgy járunk el, mint más axiómarendszerek esetében.

3

Az axiómarendszerekkel kapcsolatban gyakran teszik fel a kérdést: „Van-e valami, ami a szóban forgó axiómákat kielégíti?" Sőt, azt is meg szokás kérdezni, hogy „Azok a dolgok, amelyeknek az axiómáiról van szó, kielégítik-e ezeket az axiómákat? És azt is, hogy „Vajon csak azok a dolgok tesznek-e eleget a szóban forgó axiómáknak, amelyeknek szándékunk szerinti axiómáiról van szó?" Ezek értelmetlen kérdések. Említettük már, hogy értelmetlen „szándékolt interpretációról" és valaminek az „axiomatizálásáról" beszélni, továbbá nincs „standard aritmetika", amelyet „axiomatizálunk" és nincs „naiv halmazelmélet", amelyet „axiomatizálunk". A szigorú értelemben vett matematika számára ezek az elméletek akkor léteznek, ha megadjuk a megfelelő axiomatikus felépítését, méghozzá az itt megismert PC(=)-ben. És ezek az elméletek semmi egyebek,

mint amelyeket ilyen módon axiomatikusan megadunk. Ontológiai értelemben értelmetlen olyan „dolgokról” beszélni, amelyek „eleget tesznek” ezeknek az axiómáknak, vagy amelyek „tulajdonságait” ezek az axiómák „tükrözik”. Amik léteznek, azok egyszerűen azok a jelek és azok a szintaktikai szabályok (mechanizmusok), amelyek az adott deduktív rendszerben használatosak.

Ez természetesen a lehetséges matematikai-filozófiai irányzatokon belül egy radikálisan formalista álláspont, s az olvasó más felfogású könyvekben más állásponttal találkozhat. (A filozófiai természetű kérdésekben, mint a legtöbb nyitott tudományos kérdésben, az a szép, hogy egymással vitatkozó álláspontok lehetségesek. Ez persze nem jelenti azt, hogy a filozófiai kérdésekkel kapcsolatban tetszőleges álláspont hangoztatható. Egy-egy felfogás mögött, jól kimunkált argumentumok sora húzódik meg.) Az itt képviselt formalista álláspont alátámasztásául egyetlen, alapvetően episztemológiai argumentumot említünk meg, melyet az olvasó figyelmébe ajánlunk minden más, a formalizmustól eltérő matematika-filozófiai irányzat értékelésének kritériumaként. Nevezetesen, annak megfontolását, hogy „Honnan tudjuk, hogy egy matematikai állítás helyes?” Ha a deduktív rendszerben megadott axiomatikus elmélet „valaminek az axiomatikus elmélete”, honnan tudjuk, hogy az a valami micsoda és hogy eleget tesz-e az axiómáknak, hogy mik a tulajdonságai, hogy valamely rájuk vonatkozó állítás helytálló-e, stb. A világban létező fizikai dolgokról minden ismeretünk a tapasztalatra épül. Minden elméleti következtetésünk próbája a

tapasztalat. A matematikai objektumokra vonatkozó állítások helyességének forrása nem lehet a tapasztalat, az nyilvánvaló. Senkinek sem jut eszébe, hogy a laboratóriumba siessen eldönteni, hogy a 6 páros szám-e, vagy hogy egy megszámlálhatóan végtelen számosságú halmaz hatványhalmazának számossága nagyobb-e, mint az eredeti halmaz számossága! Nyilvánvaló, hogy nem az egyes személyek intuícióján alapuló szubjektív vélekedésekről van szó, sőt, még csak nem is valamiféle egyetemes emberi intuíción alapuló közvélekedésről, hiszen ezeknek az állításoknak a helyességét nem pszichológusok, vagy szociológusok, vagy közvéleménykutatók döntik el, hanem matematikusok. Méghozzá úgy, hogy bebizonyítják, azaz, jól definiált szabályok szerint egyértelműen megadott axiómákból levezetik.