1. Gödel

Lemma – (Primitív rekurzív függvények reprezentálhatósága) – Ha Γ a PA egy pr. rekurzív bővítése és $R(x_1, ..., x_n)$ pr. rekurzív számelméleti reláció, akkor létezik olyan r jelű n-VÁLTOZÓS FORMULA, hogy minden $x_1, ..., x_n$ természetes számra:

$$R(x_1, ..., x_n) \to \Gamma \vdash R(x_1, ..., x_n) \longleftrightarrow \Pr_{\Gamma} r[17 \to Z(x_1), ..., ... \to Z(x_n)]$$

és

$$\sim R(x_1, ..., x_n) \to \Gamma \vdash \sim R(x_1, ..., x_n) \longleftrightarrow \Pr_{\Gamma} \mathrm{Neg}\, r[17 \to Z(x_1), ..., .. \to Z(x_n)]$$

ahol $\Pr_\Gamma$ az az egyváltozós számelméleti reláció, ami pontosan akkor igaz egy kódra, ha amit kódol, akkor az levezethető Γ-ból. (Tehát a levezethetőség-igazság szempontjából a pr. relációk problémamentesek.)

(Bizonyítás vázlat: $R(x_1, ..., x_n) = \varphi(x_1, ..., x_n) = 0$ definívcióval van értelmezve, ahol φ pr. számlemeti függvény, amelynek felépítésére vontkozó indukció megfelelő: 0, f, rekurzió-indukció, helyettesítés.)

Lemma – (Diagonalizációs lemma) – Ha Γ a PA egy pr. rekurzív bővítése, akkor létezik olyan egybváltozós $A(x)$ reláció és ennek r kódja, amelyre teljesül, hogy minden x számra:

$$\sim (x \Pr_{\Gamma}(17\, \mathrm{Gen}\, r)) \to \Gamma \vdash A(x) \longleftrightarrow \Pr_{\Gamma} r[17 \to Z(x)]$$

és

$$x \Pr_{\Gamma}(17\, \mathrm{Gen}\, r) \to \Gamma \vdash \sim A(x) \longleftrightarrow \Pr_{\Gamma} \mathrm{Neg}\, r[17 \to Z(x)]$$

Bizonyítás. Legyen

$$Q(x, y) :=\sim (x \Pr_{\Gamma} y[19 \to Z(y)])$$

ekkor a reprezentációs tétel miatt létezik olyan q kód, mely egy KÉTVÁLTOZÓS RELÁCIÓT kódok, hogy

$$Q(x, y) \to \Gamma \vdash Q(x, y) \longleftrightarrow \Pr_{\Gamma} q[17 \to Z(x), 19 \to Z(y)]$$

és

$$\sim Q(x, y) \to \Gamma \vdash \sim Q(x, y) \longleftrightarrow \Pr_{\Gamma} \mathrm{Neg}\, q[17 \to Z(x), 19 \to Z(y)]$$

Most lekötjük az első változóját:

$$p := 17\, \mathrm{Gen}\, q$$

és az ennek a kódnak megfelelő számnevet behelyettesítjük a q MÁSDIK VÁLTOZÓJÁBA (y-ba):

$$r := q[19 \to Z(p)]$$

Ekkor tehát:

$$p[19 \to Z(p)] = (17\, \mathrm{Gen}\, q)[19 \to Z(p)] = (17\, \mathrm{Gen}\, q[19 \to Z(p)]) = 17\, \mathrm{Gen}\, r$$

Mi történt? Elkészítettük a következő mondat formális megfelelőjét:

> „A formula, amit úgy kapunk, hogy az ‚A formula, amit úgy kapunk, hogy az y formula nevét az egyetlen változójába helyettesítjük, nem levezethető.' formula nevét az egyetlen változója helyére helyettesítjük nem levezethető."

Mi lesz igaz erre?

1. Ha megcsináljuk, amit mond, akkor ugyanazt kapjuk.
2. Saját magáról beszél.
3. Ha igaz, akkor nem levezethető. Ha hamis, akkor levezethető.

Tétel – Gödel első nemteljességi tétele – FORMULÁK egy Γ primitív rekurzív, ω-KONZISZTENS halmazára létezik olyan r OSZTÁLYJEL, hogy

$$\sim \underset{\Gamma}{\mathrm{Pr}}\,(v\,\mathrm{Gen}\,r) \text{ és } \sim \underset{\Gamma}{\mathrm{Pr}}\,\mathrm{Neg}(v\,\mathrm{Gen}\,r)$$

ahol v az r SZABAD VÁLTOZÓJA.

Bizonyítás. Nyilván $(17\,\mathrm{Gen}\,r)$ lesz ez és ez egy formulát kódol, ami $\forall x, A(x)$ alakú, ami a G Gödel-mondat.

1. Indirekten tegyük fel, hogy G levezethető Γ-ból. Ekkor van olyan n szám, amely a levezetését kódolja, így

$$n\,\underset{\Gamma}{\mathrm{Pr}}(17\,\mathrm{Gen}\,r)) \to \Gamma \vdash A(n) \longleftrightarrow \underset{\Gamma}{\mathrm{Pr}}\,\mathrm{Neg}\,r[17 \to Z(n)]$$

a diaginalizációs lemma miatt. De ekkor G, mint egy univerzális állítás levezethető:

$$\underset{\Gamma}{\mathrm{Pr}}(17\,\mathrm{Gen}\,r))$$

vagy

$$\Gamma \vdash \forall x, A(x)$$

azaz minden x-re:

$$\underset{\Gamma}{\mathrm{Pr}}\,r[17 \to Z(x)])$$

így az $Z(n)$ számnévre is:

$$\underset{\Gamma}{\mathrm{Pr}}\,r[17 \to Z(n)])$$

ami ellentmond annak, hogy

$$\underset{\Gamma}{\mathrm{Pr}}\,\mathrm{Neg}\,r[17 \to Z(n)].$$

2. Indirekten tegyük fel, hogy G tagadása levezethető, azaz

$$\underset{\Gamma}{\mathrm{Pr}}\,\mathrm{Neg}(17\,\mathrm{Gen}\,r)$$

1.-ben bizonyítottuk, hogy $\sim \mathrm{Pr}_\Gamma\,(17\,\mathrm{Gen}\,r)$. Az azt jelenti, hogy akármilyen n természetes számra

$$\sim n\,\underset{\Gamma}{\mathrm{Pr}}\,(17\,\mathrm{Gen}\,r)$$

Van tehát egy olyan $A(x)$ predikátum (ez az r), amelyre az igaz, hogy minden n-re $A(n)$ levezethető, ugyanis ezt mondja a diagonalizációs lemma:

$$\sim (n\,\underset{\Gamma}{\mathrm{Pr}}(17\,\mathrm{Gen}\,r)) \to \Gamma \vdash A(n) \longleftrightarrow \underset{\Gamma}{\mathrm{Pr}}\,r[17 \to Z(n)]$$

ahonnan:

$$\underset{\Gamma}{\mathrm{Pr}}\,r[17 \to Z(n)]$$

de az indirekt feltevés miatt a generalizációjának a tagadása levezethető:

$$\underset{\Gamma}{\mathrm{Pr}}\,\mathrm{Neg}(17\,\mathrm{Gen}\,r)$$

□

2. Modern

A bizonyításellenőrzési (validálási) algoritmusok szempontjából lényeges, hogy a

$$\Gamma \vdash p : A$$

ternáris levezethetőség reláció **primitív rekurzívan** eldönthető: előre megbecsülhető, hogy hány lépésben lehet eldönteni, hogy teljesül vagy sem. Egyszerűen azt kell ellenőrizni, hogy a p levezetésfa gyökérpontjában az A állítás van-e. Maga az, hogy p egy levezetés, az is primitív rekurzív reláció. Ennél azt kell ellenőrizni, hogy minden csúcsában egy levezetési szabály egy esete szerepel-e. Az eljárás időbonyolultsága lineáris levélhosszban mérve, azaz kb. annyi esetet kell ellenőrizni, ahány levél a levezetésfában van. $\Gamma \vdash p : A$ Gödel-kódolással elkódolt verziója legyen: $\ulcorner p \urcorner \mathrm{Pr}_\Gamma \ulcorner A \urcorner$, ahol Pr_Γ számelméleti reláció, ami pont azt fejezi ki, amit $\Gamma \vdash p : A$, csak kódokkal. Az egyszerűség kedvéért Pr_Γ-val jelöljük azt a PA-ba lefordított predikátumot is, amelyik Pr_Γ formális megfelelője.

Reprezentációs lemma. Minden A mondatra, $\Gamma \supseteq PA$ primitív rekurzív mondathalmazra és p bizonyításra létezik olyan q bizonyítás, hogy

$$\Gamma \vdash p : A \longleftrightarrow \Gamma \vdash q : \ulcorner p \urcorner \underset{\Gamma}{\mathrm{Pr}} \ulcorner A \urcorner.$$

Figyeljük meg, hogy a : bal oldalán egy levezetés(fa) van, a jobb oldalán egy PA-beli formula. A jobb oldalon tehát csak **számnévként** tud egy természetes szám vagy egy levezetéskód vagy egy formulakód szerepelni.

Világos, hogy a Pr_Γ bináris predikátum *problémamentes* abban az értelemben, hogy $\Gamma \vdash p : A$ *igaz* pontosan akkor, ha $\ulcorner p \urcorner \mathrm{Pr}_\Gamma \ulcorner A \urcorner$ levezethető Γ-ból. Ez Pr_Γ primitív rekurzivitásából következik és nagyon lényeges tény.

Diagonális lemma. Ha $\Gamma \supseteq$ PA primitív rekurzív axiómarendszer, akkor létezik olyan $\forall x, A(x)$ alakú univerzális G mondat és ennek g Gödel-kódja, ahol $A(x)$ primitív rekurzív reláció és amire

$$\Gamma \vdash G \longleftrightarrow \forall x, \sim (x \,\mathrm{Pr}\, g) \qquad (\longleftrightarrow \Gamma \vdash q_1 :\ \forall x, A(x)) \qquad (D1)$$

továbbá minden p levezetésre és ennek $\ulcorner p \urcorner$ Gödel-kódjára léteznek q_1, q_2 levezetések, hogy

$$\begin{array}{lllll} \Gamma \nvdash p : G & \to & \Gamma \vdash q_1 : \sim \ulcorner p \urcorner \mathrm{Pr}\, g & (\longleftrightarrow \Gamma \vdash q_1 :\ A(x)) & (D2) \\ \Gamma \vdash p : G & \to & \Gamma \vdash q_2 :\ \ \ulcorner p \urcorner \mathrm{Pr}\, g & (\longleftrightarrow \Gamma \vdash q_2 : \sim A(x)) & (D3). \end{array}$$

Nyilván G azt mondja, hogy saját maga nem levezethető.

Megjegyzés. G egy Π_1 aritmetikai formula. Az A mondat Π_1-formula, ha $\forall x_1, ...x_n, P(x_1, ..., x_n)$ alakú, ahol P-ben csak korlátos kvantorok vannak (azaz P primitív rekurzív). Az ilyen formulák nagyon érdekesen viselkednek a **sztenderd modellben**, vagyis a véges von Neumann rendszámok halmazában, ω-ban. Ha egy Π_1-formula **hamis** ω-ban, akkor ez egy egyszerű kereső algoritmussal igazolható (egyszerűen futtatni kell az individuumok halmazán egy felsorolást és ellenőrizni, hogy P igaz vagy hamis ezeken az elemeken. Ez problémamentes, mert P primitív rekurzív és az algoritmikus megoldás cáfolni fogja A-t. Ha A igaz ω-ban, akkor ez nem igazolható kereső eljárással. Még az is lehet, hogy a sztenderd modellben igaz, de egy nem-sztenderd modellben egy troll Ω elem (végtelen bizonyítás) cáfolja A-t. Ha tehát G nem levezethető, az azért van, mert nem minden modellben igaz G. Ez a **Gödel-féle teljességi tétel** következménye, amely egy klasszikus logikai tétel. Gödel ezen tétele, amit a doktori dolgozatában igazolt, azt mondja ki, hogy egy mondat pontosan akkor levezethető egy elsőrendű elméletben, ha az elmélet minden halmazelméleti modelljében igaz. Filozófiai kérdés, hogy a modelleket hogyan "érjük" el, ha mással nem mint levezetéssel. A halmazelméleti nem-sztenderd modellek éppen ezekkel a végtelen természetes számokkal kapcsolatos ontológiai problémákkal terheltek. A teljességi tételre való hivatkozás nélkül, talán úgy fogalmazhatunk, hogy *nincs egységes bizonyítás,* ami G-t, mint univerzális mondatot igazolná.

Megjegyzés. A klasszikus logikában a $\sim G$ egy Σ_1 formula, azaz $\exists x_1, ...x_n, Q(x_1, ..., x_n)$ alakú, ahol Q primitív rekurzív formula. Ha egy ilyen formula **igaz** a **sztenderd modellben,** akkor ez egy keresési eljárással igazolható, úgy, hogy rátalálunk azokra az elemekre, amik igazzá teszik. Ha tényleg igaz, ezekre rá fogunk találni. És ez az effektív eljárás igazolni fogja, hogy a mondat bizonyítható. Ha azonban a sztenderd modellben hamis, akkor ezt nem fogjuk tudni kereső eljárással bizonyítani. Ha tehát $\sim G$ nem levezethető, akkor az a teljességi tétel értelmében azért van, mert nem minden modellben hamis G. A teljességi tételre való hivatkozás nélkül, talán úgy fogalmazhatunk, hogy *nincs konstruktív bizonyítás* a G-t igazoló levezetéskód megtalálására és annak igazolására, hogy ez a kód teljesíti a tőle elvártakat.

Gödel első nemteljességi tétele. Ha $\Gamma \supseteq PA$ primitív rekurzív axiómarendszer és ellentmondásmentes, akkor

1. $\Gamma \nvdash G$
2. ha Γ ω-konzisztens, akkor $\Gamma \nvdash \sim G$

Bizonyítás. 1. Tegyük fel, hogy $\Gamma \vdash G$, azaz van olyan p bizonyítás, amelyre

$$\Gamma \vdash p : G$$

a diagonalizációs lemma (D3) pontja miatt ekkor van olyan q bizonyítás, hogy

$$\Gamma \vdash q : \ulcorner p \urcorner \operatorname{Pr} g.$$

Másfelől a diagonalizációs lemma (D1) pontja miatt $\Gamma \vdash G$ ekvivalens $\Gamma \vdash \forall x, \sim (x \operatorname{Pr} g)$-vel, amiből az $x \to \ulcorner p \urcorner$ helyettesítéssel:

$$\Gamma \vdash \sim (\ulcorner p \urcorner \operatorname{Pr} g)$$

ami színtiszta ellentmondás.
2. Tudjuk, hogy Γ egy ω-konzisztens elmélet, azaz tetszőleges $A(x)$ predikátumra

$$\Gamma \vdash A(0), ..., \Gamma \vdash A(n), ... \to \Gamma \nvdash \sim \forall x, A(x).$$

Tegyük fel, hogy $\Gamma \vdash \sim G$, azaz $\Gamma \vdash \sim \forall x, \sim x \operatorname{Pr} g$. De az előbb kihoztuk, hogy

$$\Gamma \nvdash G$$

azaz minden n számnévre:

$$\Gamma \vdash \sim (n \operatorname{Pr} g)$$

mert n vagy nem bizonyítást kódol, vagy bizonyítást kódol, de akkor $\Gamma \nvdash G$ miatt nem lehet bizonyítása g-nek, így a (D2) miatt teljesül az előbbi reláció. Azaz $A(x) = \sim (x \operatorname{Pr} g)$ olyan predikátum, aminek a léte ellentmond annak, hogy Γ egy ω-konzisztens elmélet.

Tétel. Ha PA ellentmondásmentes, akkor PA+ $\sim G$ is ellentmondásmentes és ω-inkonzisztens is.

Bizonyítás. $\sim G$ az előző tétel miatt ebben az esetben független PA-tól. Továbbá

$$\text{minden } n\text{-re PA} \vdash\sim (n \operatorname{Pr} g), \text{ miközben PA+} \sim G \vdash\sim \forall x, \sim (x \operatorname{Pr} g) \quad (=\sim G),$$

hiszen a bővítésben $\sim G$ axióma, azaz PA+ $\sim G$ ω-inkonzisztens is.

Megjegyzés. Emlékezzünk vissza arra, hogy egy Γ elmélet ω-teljes, ha minden $A(x)$ predikátumra

$$\Gamma \vdash A(0), ..., \Gamma \vdash A(n), ... \to \Gamma \vdash \forall x, A(x).$$

Tétel. Ha PA ellentmondásmentes, akkor PA **nem ω-teljes** (az ω-inkonzisztenca feltétele nélkül is).

Hiszen

$$\text{minden } n\text{-re PA} \vdash\sim (n \operatorname{Pr} g), \text{ de közben PA} \nvdash \forall x, \sim (x \operatorname{Pr} g) \quad (= G).$$

Megjegyzés. A következő szakaszban (Rosser) azt is látni fogjuk, hogy PA nem csak nem ω-teljes, de mégcsak nem is (negáció) teljes (azaz $\Gamma \vdash A$ és $\Gamma \vdash\sim A$ közül legalább az egyik igaz), ha PA ellentmondásmentes. Ahogy Kalmár László viccesen fogalmazott a negációteljesség az ω-konzisztencia "mesterkélt" feltétele nélkül is fennáll. Persze láttuk, hogy a bizonyítás hézagmentesen használja fel az ω-konzisztenciát. Ezt a Rosser-trükkel tudjuk igazolni, ami szintén egy "mesterkélt" levezethetőségfogalmon alapul. Addig is azonban egy érdekes tétel.

Gödel második nemteljességi tétele. Ha $\Gamma \supseteq PA$ primitív rekurzív axiómarendszer, ellentmondásmentes, és ω-konzisztens, akkor a $\text{consis}_\Gamma = \forall x, \sim x \operatorname{Pr}_\Gamma \ulcorner\text{False}\urcorner$ konzisztenciamondat olyan, hogy

$$\Gamma \nvdash \text{consis}_\Gamma.$$

Bizonyítás. Az első nemteljességi tétel első felében beláttuk, tárgynyelvi szinten kódolható, konstruktív módon, hogy ha G levezethető, akkor Γ ellentmondásos. Ezt az argumentumot lekódolva teljesül:

$$\Gamma \vdash G \to\sim \text{consis}_\Gamma$$

Kontrapozícióval ebből:

$$\Gamma \vdash \text{consis}_\Gamma \to\sim G$$

Ha tehát Γ ω-konzisztens, akkor ha consis_Γ levezethető lenne, $\sim G$ is levezethető lenne.

Megjegyzés. Ezt a tételt a Hilbert-program bukását kifejező eredménynek is szokás tekinteni, holott Gödel ebben a cikkben maga mondja, hogy eredményei nem érintik a Hilbert-programot.

Megjegyzés. Természetesen értelmezhető a tétel egyfajta limitációs (határ-) tételnek. Ha ugyanis lenne PA ellentomdásmentességének olyan bizonyítása, amely végig PA(!) alapján menne, akkor ezt a bizonyítást le lehetne fordítani consis_Γ-vá, ami viszont nem levezethető. Ami valóban némiképp aláás egy olyan célkitűzést, hogy igazoljuk finit módon PA ellentmondásmentességét.

Megjegyzés. Ne felejtsük el azonban, hogy ha egy konzisztenciabizonyítás PA-ban halad, akkor a konzisztenciaállítás minden modellben igaz lesz, azaz a nemsztenderd modellekben is, azaz a végtelen bizonyításkódokat tartalmazó modellekben is. consis_Γ tehát túl sokat akar markolni. Hogy ő nem bizonyítható, az azt jelenti, hogy nincs a consis_Γ mondatnak, ami egy Π_1 mondat, egységes, tehát konstruktív bizonyítása. De nem is ezt a problémát akarjuk igazolni. Elég, ha csak a "véges" természetes számokat tartalmazó modellekben (sztenderd modellben) igaz consis_Γ. Vagy ha úgy tetszik bele kell tenni a "véges" szót abba az elméletbe, amelyik PA-ról beszél, ami azonban ettől már nem a PA lesz, hanem valami másodrendű PA. Tehát a Gödel-tételek pártlanul erős, mondhatni *túl* erős tételek.

3. Rosser

Az első Gödel-féle nem teljességi tétel *élesítése* Rosser-trükkjén alapul. Eszerint az

$$x \,\mathrm{Pr}\, y$$

bizonyíthatóság predikátumot, amelynek jelentése: "az x számmal kódolt bizonyítás bizonyítja az y számmal kódolt állítást" le kell cserélni a következőre:

$$x \overset{R}{\mathrm{Pr}} y \longleftrightarrow x \,\mathrm{Pr}\, y \wedge \forall z, z < x \rightarrow\sim (z \,\mathrm{Pr} \sim y)$$

Rosser-féle bizonyíthatóság jelentése: "az x számmal kódolt bizonyítás bizonyítja az y számmal kódolt állítást és minden x-nél kisebb kódú bizonyítás nem bizonyítja a szóban forgó állítás tagadását". Ez a következő nagyon hasznos tulajdonsággal rendelkezik:

$$\sim (x \overset{R}{\mathrm{Pr}} y) \longleftrightarrow\sim (x \,\mathrm{Pr}\, y) \vee \exists z, z < x \wedge z \,\mathrm{Pr} \sim y$$

Ha tehát Γ ellentmondásmentes, akkor $x \,\mathrm{Pr}\, y \longleftrightarrow x \,\mathrm{Pr}^R\, y$. Továbbá a korlátos kvantor miatt szintén rekurzív.

Gödel–Rosser-tétel. Ha $\Gamma \supseteq PA$ primitív rekurzív axiómarendszer és ellentmondásmentes, akkor az $R =\sim \forall x, \sim x \,\mathrm{Pr}^R\, r$ Rosser-mondatra és Gödel-kódjára r-re teljesül, hogy

$$\Gamma \nvdash R \text{ és } \Gamma \nvdash\sim R.$$

Bizonyítás. Analóg módon a Gödel-tételhez igazolható, hogy

$$\Gamma \nvdash R$$

Ebből viszont az következik, hogy minden n számnévre:

$$\Gamma \vdash\sim (n \overset{R}{\mathrm{Pr}} r)$$

azaz

$$\Gamma \vdash\sim (n \underset{\Gamma}{\overset{R}{\mathrm{Pr}}} r) \longleftrightarrow\sim (n \underset{\Gamma}{\mathrm{Pr}} r) \vee \exists z, z < n \wedge z \underset{\Gamma}{\mathrm{Pr}} \sim r$$

vagyis vagy nem bizonyítható R, vagy ha bizonyítható, akkor a tagadása is bizonyítható, ami ellentmond annak, hogy Γ ellentmondásmentes. Mivel ellentmondásmentes elméletben a két bizonyíthatóság-fogalom ekvivalens, ezért a tétel állítása igaz.

4. Church

Church tézise vagy a **Church–Turing-tézis** az effektív eljárásokról szól. Lényegében azt mondja ki, hogy akárhogy is próbáljuk meg definiálni az effektív kiszámíthatóság foglamát, rekurzív függvényekkel, lambda-kiszámíthatósággal vagy Turing-géppel ugyahhoz a függvényosztályhoz jutunk. A rekurzív függvények osztályához a parciálisan rekurzív függvényeken keresztül jutunk el. Ha a primitív rekurzióhoz (nulla, rákövetkezés, helyettesítés, primitív rekurzív definíció, tehát lényegében a finit matematikához) hozzávesszük a μ-operációt (minimalizációt), akkor a parciálisan rekurzív számelméleti függvényeket kapjuk:

$$(\mu x)(\varphi(x, x_1, ..., x_n) = 0)$$

rögzített $x_1, ..., x_n$-re az a legkisebb x szám, amire a $\varphi(x, x_1, ..., x_n) = 0$ egyenlőség teljesül, ahol φ korábban definiált parciálisan rekurzív függvény. $\mu x, \varphi$ definiált, ha van a fenti egyenlőségnek megoldása, és nem definiált, ha nincs. Ebből származik a parcialitás, a nem mindenhol definiáltság. Ezt úgy kell elképzelni, hogy néha egy számítási eljárás végtelen ciklusba képes merülni annak ellenére, hogy az algoritmus effektív. A Church-tézis szerint a parciálisan rekurzív számelméleti függvények az effektív eljárással kiszámítható számelméleti függvények.

Rekurzív számelméleti függvénynek nevezzük a paricálisan rekurzív φ számelméleti függvény, ha mindenhol értelmezett. Néha "totálisan" rekurzívnak is nevezzük ezt a fogalmat. Egyes számleméleti relációk eldönthetők, mások félig eldönthetők. Az **eldönthető relációkhoz** létezik egy effektív eljárás, ami minden bemenetre véges lépésben eldönti, hogy igaz rá a reláció vagy hamis. A **félig eldönthető relációk** olyanok, hogy létezik egy effektív eljárás, ami véges lépésben lefut, ha a reláció igaz (a hamis kimenetelt nem találja meg feltétlenül). Világos, hogy egy reláció rekurzív, ha ő és negációja egyaránt félig eldönthető.

A Church-tézis empirikus alapja az, hogy kiderült, hogy a rekurzív függvények, Turing-géppel kiszámítható függvények, lambda-kiszámítható függvények mind-mind ugyanahhoz a függvényosztályhoz vezetnek.

Az általánosítással a primitív rekurzív függvények nem veszítenek a jelentősségükből, sőt! Ha bolondbiztos algoritmusokat akarunk, akkor érdemes megmaradni a PR bonyolultsági osztály keretei között, azaz a primitív rekurzív függvényeknél. A proof assistantekben csak primitív rekurzív függvényeket lehet definiálni, mert nem szándékozzuk alapból beépítani a programnyelvbe a bizonyításnélküliséget.

A Gödel-tételkör rekurzívan általánosítható: egy trükk segítségével, amit Kleene talált ki, a rekurzív relációk is reprezentálhatókká tehetők PA-ban és rekurzív kiterjesztéseikben, így a fenti három tételt ki lehet mondani úgy, hogy Γ-t rekurzívnak vesszük. Világos, hogy ez elméleti jelentősségű eredmény, mert a proof assistantek pr. r. függvényekkel dolgoznak. Sőt, ultrafinit függvényekkel: ami nem polinomidőben számolódik ki, az "nem létezik".

1936-ra világossá vált, hogy Hilbert azon problémája, hogy járjunk annak a végére, hogy van-e olyan effektív eljárás, ami a PA minden mondatáról eldönti, hogy igaz vagy sem negatívan oldható meg. Ami a világos megfogalmazához szükséges volt, az az effektív eljárás mibenlétének feltárása és a kérdés olyan átfogalmazása, amelyben a probléma a levezethetőségre van kihegyezve (bár az igaz-hamis kérdésre sincs algoritmikus válasz).

Church-tétel. Ha a PA egy rekurzív bővítése ellentmondásmentes, akkor nincs olyan effektív eljárás, amely minden mondatáról eldöntené, hogy levezethető Γ-ból van nem.

Bizonyítás. A tételt a primitív rekurzív esetre bizonyítjuk. Ha a $\mathrm{Pr}\, y := \exists x, (x \,\mathrm{Pr}\, y)$ primitív rekurzív reláció lenne, akkor a tagadása is. Vegyük a Rosser-mondatot és ennek r Gödel-kódját:

$$\Gamma \vdash R \longleftrightarrow \sim \exists x, (x \,\mathrm{Pr}\, r)$$

vagy másként:

$$\Gamma \vdash R \longleftrightarrow \sim \mathrm{Pr}\, r$$

Persze, ekkor $\mathrm{Pr}\, y$, lévén primitív rekurzív, reprezentálható is:

$$\Gamma \vdash A \to \Gamma \vdash \mathrm{Pr}\ulcorner A \urcorner$$

$$\Gamma \nvdash A \to \Gamma \vdash \sim \mathrm{Pr}\ulcorner A \urcorner$$

Lássuk a két esetet!
1. Tegyük fel, hogy $\Gamma \vdash R$. Ekkor a reprezentálhatóság miatt

$$\Gamma \vdash \mathrm{Pr}\, r$$

másfelől R jelentése miatt

$$\Gamma \vdash R \rightsquigarrow \Gamma \vdash \sim \mathrm{Pr}\, r$$

azaz Γ ellentmondásos, ami ellentmondás, mert Γ nem az.
2. A reprezentálhatóság miatt, majd R jelentése miatt:

$$\Gamma \nvdash R \rightsquigarrow \Gamma \vdash \sim \mathrm{Pr}\, r \rightsquigarrow \Gamma \vdash R$$

ami tiszta ellentmondás.

Persze a tétel igaz rekurzív függvényre is.

A bizonyítás későbbi, de első alakjában Alonso Church a tételt a tézisével igazolta és valahogy a következőképpen hangzott. Legyen $A(x)$ paraméteres problémasereg PA-ban (pl. az x paraméter esetén létezik y és z, hogy $x^3 + y^3 = z^3$). Ekkor nem létezik olyan effektív eljárás, ami minden x-re eldönti, hogy $A(x)$ igaz vagy sem.

5. Kleene

A Gödel-tétel ebben a gondolatkörben is levezethető, azaz van algoritmusokat használó bizonyítása. Ez a bizonyítás Stephen Kleene-re (ejtsd: klíni) vezethető vissza. A Church-tézis értelmében mindegy, hogy az algoritmust milyen formában definiáljuk. Természetesen itt a rekurzív aritmetikai függvényeket választjuk. Ezek a függvények felsorolhatók, voltaképpen mindegyikhez hozzárendelhető egy e Gödel-kód (nyilván ebben a kódban benne van, hogyan épül fel a függvény, ahol a minimalizációt is figyelembe kell venni). A központi fogalom ezek után a **Kleene-féle** T **predikátum** lesz, amelynek a kimente egy természetes szám, bemenetei pedig a következők. Ha f_e az e-edik parciális rekurzív függvény, n az input természetes szám, z pedig egy számításnak a Gödel-féle módon elkódolt számítástörténete. No, most már

$$T(e, n, z) = 0$$

pontosan akkor, ha az f_e függvény az n inputon a z kódú számítástörténetet produkálja. Hogy ez a függvény hogy épül fel, arra már láttunk példát a kurzusban: a $\Gamma \vdash p : A$ ternáris levezethetőség predikátum hasonló primitív rekurziv reláció, mint $T(e,n,z) = 0$.

Ezzel a relációval a parciálisan rekurzív függvények kifejezhetők, ráadásul egyetlen minimalizációval és primitív rekurzív függvénnyel.

Kleene normálforma tétele. T primitív rekurzív függvény, és minden f_e parciálisan rekuzív függvényre:

$$f_e(n) = U(\mu z.(T(e,n,z) = 0))$$

azokon az n helyeken, ahol f_e értelmezett. Itt U az a primitív rekurzív függvény, amelyiknek a feladata a számítástörténetből az output-ot leolvasása.

Egy f parciálisan rekurzív függvény **teljes kiterjesztése** a g totálisan értelmezet rekurzív függvény, ha minden olyan n-re, amire f értelmezett,

$$f(n) = g(n).$$

Egy f parciálisan rekurzív függvény **teljessé tehető**, ha van teljes kiterjesztése.

Nemteljességi lemma – még nem az :) . Nem minden parciálisan rekurzív függvény tehető teljessé.

Ugyanis egy ilyen függvény a nevezetes

$$f(n) := U(\mu z.(T(n,n,z) = 0)) + 1$$

Ha ez teljessé tehető lenne, akkor ki lehetne számítani azon a számon, ami a saját Gödel-kódja. Ha tehát $f = f_e$, akkor amiatt, hogy f_e az e-edik függvény:

$$f_e(e) = U(\mu z.(T(e,e,z) = 0))$$

másfelől f_e definíciója miatt:

$$f_e(e) = U(\mu z.(T(e,e,z) = 0)) + 1$$

ami színtiszta ellentmondás.

A reprezentációs tételt külön kimondjuk ebben a világban is, ugyanaz a bizonyítása, mint korábban, strukturális indukcióval.

Reprezentációs tétel. PA egy Γ primitív rekurzív bővítése, akkor bármely $f(x_1,...,x_n)$ primitív rekurzív számelméleti függvény estén van olyan $A(x_1,...,x_n)$ formula, hogy minden $a_1,...,a_n$ számra

1. $f(a_1,...,a_n) = 0$ akkor $\Gamma \vdash A(\ulcorner a_1 \urcorner, ..., \ulcorner a_n \urcorner)$
2. $f(a_1,...,a_n) \neq 0$ akkor $\Gamma \vdash\sim A(\ulcorner a_1 \urcorner, ..., \ulcorner a_n \urcorner)$

Elrekkentettük az "önhivatkozást" a nemteljességi lemmába, így a Gödel-tétel alábbi bizonyításában nem lesz önreferencialitás.

Gödel első nemteljességi tétele. Ha Γ a PA primitív rekurzív bővítése, ami ellentmondásmentes és ω-konzisztens, akkor létezik olyan G mondat, amire $\Gamma \nvdash G$ és $\Gamma \nvdash \sim G$.

Bizonyítás (Kleene). Indirekt egzisztenciabizonyítás lesz, de jól fog esni. Feltesszük, hogy mégis negációteljes Γ, azaz nincs olyan G mondat, mint fönn.

$T(e,n,z)$ reprezentálható primitív rekurzív függvény, legyen a reprezentációja az egyszerűség kedvéért $T(e,n,z)$. Vegyük a következő függvényt, tetszőleges e esetén! (Persze a $\vdash$ jel jobb oldalán minden reprezentált, T és a számok is.)

$$f_e^*(n) = \begin{cases} U(\mu z.(T(e,n,z) = 0)), & \text{ha } \exists z, T(e,n,z) = 0 \\ 0, & \text{ha } \Gamma \vdash \forall z, \sim T(e,n,z) \end{cases}$$

Ez a függvény effektíven kiszámítható, mert két effektív eljárást futtatunk az n bemeneten: egyfelől felsorolással megkeressük a $T(e,n,z) = 0$ egyenlet megoldását z-re, másfelől futtatunk egy keresést a Γ-beli bizonyítások felsorolható halmazán, hogy megtaláljuk $\forall z, \sim T(e,n,z)$ bizonyítását.

Világos, hogy a $\exists z, T(e,n,z) = 0$ mondat a metanyelvben van és igazi természetes számokról beszél (a sztenderd modellben van) míg $\Gamma \vdash \forall z, \sim T(e,n,z)$-ban $\vdash$ jel jobb oldalán számnevek és relációnevek vannak. Az esetszétválasztás első esete a természetes számok szándékolt jelentéséhez tartozó igazságra, a másik eset a levezethetőségre hivatkozik, így nem feltétlenül jó a definíció. Most belátjuk, hogy jó, azaz az esetek valóban kizárják egymást és valóban felölelnek minden lehetőséget.

1. Kölcsönösen kizárják egymást a fenti definíció esetei. Tegyük fel, hogy mind $\exists z, T(e,n,z) = 0$ mind $\Gamma \vdash \forall z, \sim T(e,n,z)$ igaz. Világos, hogy ekkor van k, hogy $T(e,n,z) = 0$. Ebből a reprezentációs tétel miatt $\Gamma \vdash T(e,n,k)$ teljesül, ami $\Gamma \vdash \forall z, \sim T(e,n,z)$-val együtt azt jelentené, hogy Γ ellentmondásos, aminek az ellenkezőjét tettük fel.

2. Ketten együtt elérik az összes lehetőséget. Tegyük fel, hogy $\exists z, T(e,n,z) = 0$ hamis, azaz minden k-ra $T(e,n,k) \neq 0$. Szintén a reprezentációs tétel miatt ebből $\Gamma \vdash \sim T(e,n,k)$ következik. Az $\sim T(e,n,x)$ tehát egy olyan formulasereg PA-ban, amely minden k számnévre levezethető. Az ω-konzisztencia miatt tehát $\Gamma \nvdash \sim \forall z, \sim T(e,n,z)$. De Γ a feltevés miatt negációteljes, muszáj $\sim \forall z, \sim T(e,n,z)$ negációjának, $\forall z, \sim T(e,n,z)$-nak levezethetőnek lennie: $\Gamma \vdash \forall z, \sim T(e,n,z)$.

f_e^* tehát *minden* e-re olyan *effektíven kiszámítható* függvény, ami *mindenhol értelmezett.* A Church–Turing-tézis értelmében ekkor f_e^* minden e-re egyben totálisan értelmezett *rekurzív* függvény is. Ám, ez azt jelenti, hogy az $f_e(n) = U(\mu z.(T(e,n,z) = 0))$ függvény az összes e esetén teljessé tehető, ami ellentmond annak, amit a nemteljességi lemmában igazoltunk.