Elsőrendű elméletek

Mekis Péter
ELTE BTK Logika Tanszék

2011. december 17.

Tartalomjegyzék

1. Bevezetés **1**

2. Egy próbaelmélet: harmonikus szeretettan **2**

3. Még egy próbaelmélet: Parmenidész világa **6**

4. Peano-aritmetika: relációs változat **6**

5. A klasszikus elsőrendű nyelvek bővítése műveleti jelekkel **12**

6. Peano-aritmetika: műveleti jeles változat **13**

7. Néhány bizonyítás a Peano-aritmetikában **14**

8. Az aritmetika nyelvének kifejezőereje **15**

1. Bevezetés

Nem csak köznyelvi érvek formalizálására szeretnénk használni a logikát, hanem olyan keretelméletként is, amely tudományos elméletek leírására és vizsgálatára szolgál. A huszadik században e téren a klasszikus elsőrendű logika vált standard eszközzé. A matematikai, fizikai, nyelvészeti stb. elméleteket rendszerint elsőrendű keretek között fogalmazzák meg; de léteznek például elsőrendben formalizált metafizikai elméletek is. Az ilyen elméleteket röviden *elsőrendű elméletnek* nevezzük.

Elsőrendű elméleten egy klasszikus elsőrendű nyelv zárt formuláinak tetszőleges T halmazát értjük. A halmaz elemeit az elmélet axiómáinak nevezzük, ezek logikai következményeit pedig az elmélet tételeinek. Ez nagyon tág meghatározás. Tetszőleges formulahalmaz elemeit elfogadjuk axiómák gyanánt; nemcsak azt nem követeljük meg, hogy véges sok axiómánk legyen, de első közelítésben azt sem, hogy az axiómáink rendszert alkossanak.

Gyakorlati szempontból nagyon fontos azonban, hogy egy elmélet kifejthető legyen véges jelsorozattal. Ez nem minden formulahalmaz esetén lehetséges. Persze ha véges sok axiómánk van, akkor ilyen probléma nem merül fel. Az ilyen elméleteket végesen axiomatizáltnak mondjuk. De akkor sem mindig reménytelen az elmélet kifejtése, ha végtelen sok axiómánk van. Ilyenkor gyakran egyetlen sémával rövidítünk végtelen sok formulát – pont úgy, ahogy az elsőrendű nyelvek szintaxisának és szemantikájának szabályaiban tettük. Ezeket axiómasémának nevezzük. Nem adunk pontos meghatározást a formula- vagy axiómaséma fogalmára; a lényeg az, hogy az ilyen sémák minden esetben egy szintaktikai rekurzív meghatározást rövidítenek. A sémákkal kifejtett elméleteket rekurzívan axiomatizálhatónak nevezzük.

Egy elsőrendű nyelv valamely $\mathcal{M} = \langle U, \varrho \rangle$ interpretációját elsőrendű struktúrának is nevezzük. Az elsőrendű elméletek valójában arra tesznek kísérletet, hogy struktúrákat vagy struktúratípusokat írjanak le. Egy $\mathcal{M}$ struktúrát akkor nevezünk egy adott T elmélet modelljének, ha annak minden axiómáját igazzá teszi. (Zárt formulák igazságértéke független a változóértékeléstől, ezért azt nem tekintjük a modell részének.) Így jelöljük szimbólummal, ha $\mathcal{M}$ modellje T-nek: $\mathcal{M} \models T$. (Alsó indexszel jelezhetjük, hogy az $U_\mathcal{M}$ alaphalmaz vagy a $\varrho_\mathcal{M}$ interpretációfüggvény az $\mathcal{M}$ struktúra része; de ez a jelölés nehézkessé válik, ha az $\mathcal{M}_1$ és az $\mathcal{M}_2$ struktúrákat magukat is indexszel különböztetjük meg. Ha ez nem okoz félreértést, ilyenkor az alaphalmazra és az interpretációfüggvényre is a modell indexével utalunk: U_1, U_2, ϱ_1, ϱ_2.)

Ha egy elméletnek nincs modellje, akkor kielégíthetetlennek vagy ellentmondásosnak mondjuk; ha van, akkor kielégíthetőnek vagy ellentmondásmentesnek. Ha egy adott nyelvhez tartozó $\mathcal{M} = \langle U, \varrho \rangle$ és $\mathcal{M}' = \langle U', \varrho' \rangle$ interpretációk csak alaphalmazuk (a tárgyalási univerzum) elemeiben különböznek, de ugyanannyi individuumból állnak, és a szerkezetük is megegyezik, akkor ezeket izomorfnak mondjuk. (A pontos meghatározást mellőzzük; néha úgy fogalmazzák meg szemléletesen az izomorfiát, hogy a struktúrát nem befolyásolja, hogy kavicsokból vagy söröskorsókból épül fel.) Egy elméletet kategorikusnak mondunk, ha bármely két modellje izomorf; tehát ha az alaphalmaz elemeinek megválasztásától eltekintve bármely két modellje egyforma.

Természetes elvárás egy tudományos elmélettel szemben, hogy az legyen egyfelől kielégíthető, másfelől kategorikus. Később látni fogjuk, hogy kivételesen egyszerű esetektől eltekintve az elsőrendű elméletek esetében ez nem megvalósítható. (Lásd a Löwenheim-Skolem tételek tárgyalását.)

Már említettük, hogy ha egy φ formula következménye a T elméletnek, azt az elmélet tételének mondjuk. Ha sem φ, sem $\sim\varphi$ nem tétele az elméletnek, akkor φ-t (T-től) független formulának mondjuk. Ha egy elméletnek nincsenek független formulái, akkor azt negációteljesnek mondjuk. Ismét csak természetes elvárás egy elmélet negációteljessége. Ha tetszőleges formulaahalmazt megengedünk az elmélet axiómái gyanánt, akkor ez teljesíthető is. Később látni fogjuk azonban, hogy rekurzívan axiomatizált elméletek esetében ez az elvárás sem teljesíthető: egy kielégíthető rekurzív elmélet csak nagyon egyszerű esetekben lehet negációteljes. (Lásd Gödel nemteljességi tételének tárgyalását.)

A fenti fogalmak tesztelésére a természetes számok standard elméletét, a Peano-aritmetikát fogjuk használni. A Peano-aritmetika olyan pontosan írja le a természetes számok struktúráját, amennyire csak ez egy elsőrensű elmélet keretei között lehetséges. Ehhez képest némileg meglepő, hogy a Peano-aritmetika – feltéve, hogy kielégíthető – se nem kategorikus, se nem negációteljes.

2. Egy próbaelmélet: harmonikus szeretettan

A harmonikus szeretettan nem komoly elmélet; csak arra szánjuk, hogy bemutassuk rajta az elsőrendű elméletek néhány jellegzetességét. axiómái arra tesznek kísérletet, hogy megszabják azokat a feltételeket, amelyek teljesülése esetén a szeretet a világban harmonikusan oszlik el. Az elmélet nyelvében egyetlen nem-logikai konstans van; ez az L kétargumentumú predikátum. "xLy" szándékolt jelentése: "x szereti y-t". Két axiómánk van:

HSZ1 A szeretet kölcsönös. (Akit szeretünk, az viszontszeret; a szeretet *szimmetrikus* reláció.)

$$\forall x\ \forall y\ (xLy \supset yLx)$$

HSZ2 A szeretet továbbadódik. (A szeretteink szerettei nekünk magunknak is szeretteink; a szeretet *tranzitív* reláció.)

$$\forall x\ \forall y\ \forall z\ \big((xLy\ \&\ yLz) \supset xLz\big)$$

Nézzük meg, mi következik az axiómáinkból, és mi nem! Megfogalmazhatjuk például a következő sejtést:

Sejtés Mindenki szereti önmagát.

$$\forall x\ xLx$$

Következik-e az önszeretet törvénye a szeretet harmonikus eloszlásából? Látszólag igen. Vegyük ugyanis a nyelv egy tetszőleges interpretációját, és ebben két individuumot, amelyek közül az első szereti a másodikat. Ekkor az első axióma értelmében a második is szeretni fogja az elsőt; és így a második axióma miatt az első is szereti önmagát. De ebben a gondolatmenetben éltünk egy olyan előfeltevéssel, amelyet az axiómáink nem szavatolnak; éspedig azzal, hogy a kiválasztott individuum szeret legalább egyvalakit. Nevezzük mizantrópnak azokat, akik senkit sem szeretnek; és jelöljük az elméletnek ezt a definiált fogalmát M-vel:

Meghatározás Mizantrópnak mondjuk azokat, akik nem szeretnek senkit.

$$Mx \underset{\text{def}}{\Longleftrightarrow} \sim\exists y\ xLy$$

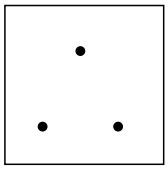
A mizantrópokat, úgy tűnik, kihagytuk a számításból. Gondolatmenetünk valójában a következő tételt bizonyította:

1. tétel Aki nem mizantróp, az szereti önmagát.

$$\forall x\ (\sim Mx \supset xLx)$$

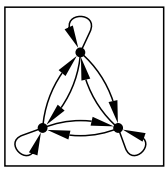
De mi a helyzet akkor, ha a világ csupa mizantrópokból áll? Ebben az esetben egyáltalán nincs szeretet a világban, következésképpen sem az első, sem a második axiómánkra nem találhatunk ellenpéldát. Tekintsünk tehát egy olyan $\mathcal{M}_1$ struktúrát, amelyben $\varrho_1(L)$ üres halmaz.

1. ábra. $\mathcal{M}_1$: Mizantróp-világ.



$\mathcal{M}_1$ modellje az elméletünknek. De nem az egyetlen. Azt a végletet sem zárhatjuk ki, amelyben $\varrho_{\mathcal{M}}(L) = U_{\mathcal{M}} \times U_{\mathcal{M}}$, vagyis keresztül-kasul mindenki szereti egymást és önmagát is. Legyen $\mathcal{M}_2$ egy ilyen struktúra: $\mathcal{M}_2$-ben megint csak nincs ellenpélda egyik axiómánkra

2. ábra. $\mathcal{M}_2$: Filantróp-világ.



sem; tehát ez is modellje lesz az elméletünknek. Annyit tehát máris megállapíthatunk, hogy a harmonikus szeretettan elmélete nem határozza meg egyértelműen a szeretési viszonyokat; az elmélet nem kategorikus.

Nevezzük filantrópnak azokat, akik mindenkit szeretnek, és jelöljük ezt az új fogalmat F-fel:

Meghatározás Filantrópnak mondjuk azokat, akik mindenkit szeretnek.

$$Fx \underset{\text{def}}{\iff} \forall y\ xLy$$

Az első axióma értelmében mindenki szereti a filantrópokat. De ennél többet is mondhatunk.

2. tétel Ha van legalább egy filantróp, akkor mindenki filantróp.

$$\exists x\ Fx \supset \forall x\ Fx$$

Az állítás igazolásához tegyük fel, hogy létezik legalább egy filantróp. Tekintsünk közülük egyet, és vegyünk egy tetszőleges másik individuumot. Megmutatjuk, hogy ez az utóbbi is filantróp. Ehhez tekintsünk egy harmadik individuumot. Mivel az első filantróp, ő mindkét másikat szereti. Mivel a szeretet kölcsönös, ők is szeretik az elsőt. Tehát a második szereti az elsőt, az első pedig a harmadikat; de mivel a szeretet továbbadódik, így a második is szereti a harmadikat. Tehát a másodikként választott individuum tetszőleges individuumot szeret; vagyis ő is filanróp. És ez természetesen igaz bárki másra is.

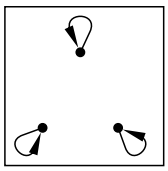
Vajon akkor az lenne a helyzet, hogy vagy csupa mizantrópból, vagy csupa filantrópból áll a világ? Nem. Nevezzük narcisztikusnak azokat, akik csak magukat szeretik:

Meghatározás Narcisztikusnak mondjuk azokat, akik kizárólag önmagukat szeretik.

$$Nx \underset{\text{def}}{\iff} \forall y\ (xLy \equiv x = y)$$

Tekintsünk ismét egy szélsőséges esetet: az $\mathcal{M}_3$ struktúrában a világ csupa narcisztikus individuumból áll. A narcisztikus egyedek jól megférnek elméletünkben a mizantrópokkal.

3. ábra. $\mathcal{M}_3$: Nárcisz-világ.



Modelljeinkben mindkettőből lehet egy vagy több. Viszont szélsőséges esetben a narcisztikusság nyilvánvalóan egybeesik a filantrópiával:

3. tétel Ha van narcisztikus filantróp, akkor egyetlen individuum létezik.

$$\exists x\ (Nx\ \&\ Fx) \supset \forall x\ \forall y\ x = y$$

Aki nem mizantróp és nem narcisztikus, az legalább két másik individuumot szeret. A fentiek alapján világos, hogy ezek egymást is szeretni fogják:

4. tétel Akiket ugyanaz szeret, azok egymást is szeretik.

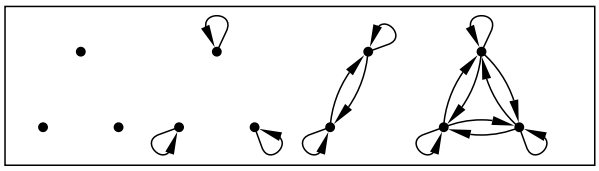
$$\forall y\ \forall z\ \big(\exists x\ (xLy\ \&\ xLz) \supset yLz\big)$$

Bizonyítás: Legyen adott x, y és z úgy, hogy xLy és xLz. Ekkor a szeretet kölcsönössége miatt yLx, és így a szeretet továbbadódása miatt yLz. □

Azokat a relációkat, amelyekre igaz a 4. tétel, euklidészinek is szokták nevezni; feltehetőleg Euklidész 1. axiómájára utalva (és ha így van, akkor pontatlanul).[1]

Mit mondhatunk tehát azokról, akik se nem filantrópok, se nem mizantrópok, se nem narcisztikusak? Ezek az individuumok kisebb-nagyobb csoportokba tömörülnek, amelyekben mindenki szeret mindenkit; de senki nem szeret senkit a csoporton kívül. Az $\mathcal{M}_4$ struktóra elméletünk egy tipikus modellje, amely a mizantrópok és a narcisztikusok mellett ilyen szeretetkommunákból áll:

4. ábra. $\mathcal{M}_4$: Egy tipikus modell.



Hogy tudnánk tételbe foglalni a szeretetkommunákról fentebb elmondottakat? Egyáltalán: tudjuk-e definiálni a *szeretetkommuna* fogalmát elméletünkben, ahogy például a *mizantrópia* esetében sikerült? Ez sajnos nem lehetséges. A *szeretetkommuna* ugyanis másodrendű fogalom; olyan tulajdonság, amellyel csoportok rendelkeznek, nem emberek. Az elsőrendű nyelvek viszont csak individuumok tulajdonságait képesek kifejezni. Ez persze nem végzetes probléma; a *szeretetkommunába tartozás* már individuumok tulajdonsága. Akkor mondhatjuk, hogy x szeretetkommunába tartozik, ha van egy vagy több olyan x-től különböző y, akiket x szeret, és akik őt is meg egymást is mind keresztül-kasul szeretik. Hogy tudjuk ezt elsőrendű nyelven elmondani? Mivel a csoport létszáma határozatlan, első próbálkozásra a kommunába tartozást (K) definiáló formula akár végtelen hosszúra is sikerülhet (x kommunába tartozik, ha kéttagú kommunába tartozik, vagy háromtagúba, vagy négytagúba stb.):

$$^{*}\ Kx \underset{\text{def}}{\Longleftrightarrow} xLx\ \&\ \exists y\ (y \neq x\ \&\ xLy\ \&\ yLx\ \&\ yLy)$$

$$\vee \ldots \vee$$

$$\exists y_1\ \ldots \exists y_n\ (x \neq y_1\ \&\ \ldots\ \&\ x \neq y_n\ \&\ y_1 \neq y_2\ \&\ \ldots\ \&\ y_{n-1} \neq y_n\ \&$$
$$xLy_1\ \&\ \ldots\ \&\ xLy_n\ \&\ y_1Lx\ \&\ \ldots y_nLx\ \&$$
$$y_1Ly_1\ \&\ y_1Ly_2\ \&\ \ldots\ \&\ y_{n-1}Ly_n\ \&\ y_nLy_n)$$

$$\vee \ldots$$

Ez – túl azon, hogy nehézkes – nem jólformált elsőrendű formula. Annyit azonban elsőrendű eszközökkel is elmondhatunk, hogy ha x szeret valamely y-t és y'-t, akkor azok egymást is szeretik – ami persze nem más, mint a fenti 4. tétel. Azt mondjuk tehát, hogy x kommunába

[1] Mint *A klasszikus predikátumlogika elemei* c. jegyzetben láttuk, az axióma úgy hangzik, hogy „ami ugyanazzal egyenlő, az egymással is egyenlő", nem pedig úgy, hogy „amivel ugyanaz egyenlő, az egymással is egyenlő".

tartozik, ha (a) szereti önmagát; (b) szeret valaki mást is; (c) akit szeret, az viszontszereti őt; (d) akiket szeret, azok egymást is szeretik.

$$Kx \underset{\text{def}}{\Longleftrightarrow} \underbrace{xLx}_{\text{(a)}} \;\&\; \underbrace{\exists y\ (y \neq x\ \&\ xLy)}_{\text{(b)}} \;\&\; \underbrace{\forall y\ (xLy \supset yLx)}_{\text{(c)}} \;\&\; \underbrace{\forall y\ \forall z\ \big((xLy\ \&\ xLz) \supset yLz\big)}_{\text{(d)}}$$

(Az axiómáink persze fölöslegessé teszik a definíció (a), (c) és (d) pontját; de azt szeretnénk, ha nem az axiómáktól függene az adekvátsága.)

A 4. tétel értelmében a kommunába tartozás egészen triviális tulajdonsággá válik, hiszen aki nem mizantróp és nem narcisztikus, az mind kommunába tartozik. Ez lesz a zárótételünk:

5. tétel Mindenki mizantróp vagy narcisztikus vagy kommunába tartozik.

$$\forall x\ (Mx \vee Nx \vee Kx)$$

Bizonyítás: Az állítás közvetlenül következik a definíciókból és a 4. tételből. □

3. Még egy próbaelmélet: Parmenidész világa

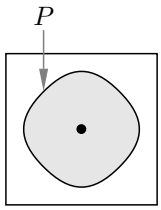
Ez sem komoly elmélet; csupán meg szeretnénk mutatni, hogy létezik kategorikus elsőrendű elmélet. Nyelvünkben egyetlen egyargumentumú predikátum van, P; "Px" szándékolt jelentése az, hogy "x pusztulhatatlan". Egyetlen axiómánk a következő:

P1 Egyetlen létező van, és az pusztulhatatlan.

$$\exists x\ (\forall y\ y = x\ \&\ Px)$$

Ennek az egyaxiómás elméletnek bármely modelljében az alaphalmaz egyelemű, és P terjedelme ez az egyelemű halmaz:

5. ábra. $\mathcal{M}_p$: Parmenidész világa.



Ez az elmélet kategorikus. Modelljei csak abban különböznek egymástól, hogy mi képviseli bennük a parmenidészi létezőt. (Természetesen ugyanígy kategorikus elméletet kapnánk akkor is, ha azt állítanánk, hogy tizenhét létező van, és azok közül nyolc pusztulhatatlan; legfeljebb metafizikaként nem lenne ilyen vonzó.)

4. Peano-aritmetika: relációs változat

Most jóval nehezebb feladatra vállalkozunk. Megkíséreljük elsőrendű elméletbe foglalni a természetes számokról szóló iskolai tudásunkat; pontosabban annyit, amennyit csak lehet. Látni fogjuk, hogy ez messze nem minden.

Hogy előfeltevéseink a lehető legátlátatóbbak legyenek, a számneveken kívül megpróbálunk mindent predikátumokban kifejezni. A következő definiálatlan nem-logikai jeleket vesszük fel a nyelvünkbe:

0 névkonstans: 0 szándékolt jelentése nulla;

S kétargumentumú predikátum: xSy szándékolt jelentése az, hogy y rákövetkezője x-nek;

$+$ háromargumentumú predikátum: $+(x, y, z)$ szándékolt jelentése az, hogy z az x és y összege (a szokásos jelöléssel: $x + y = z$);

$\cdot$ háromargumentumú predikátum: $\cdot(x, y, z)$ szándékolt jelentése az, hogy z az x és y szorzata (a szokásos jelöléssel: $x \cdot y = z$).

Bár elméletünk a természetes számokról szól, nincs benne olyan szimbólum, amely a szándékolt olvasatban azt fejezné ki, hogy valami természetes szám. Persze bevezethetnénk egy N predikátumot ezzel a szándékolt jelentéssel, de nem tesszük. A harmonikus szeretettan emberekről szólt, mégsem volt benne az *ember* szónak megfelelő predikátum. Ehelyett a tárgyalási univerzumot kezeltük úgy, mint az emberek összességét. Másként fogalmazva: az *ember* fogalma formális fogalom volt az elméletben, amelyet egy grammatikai kategória reprezentált (ti. az egyedi terminusoké), nem pedig egy kifejezés. Ugyanígy járunk el a természetes számok elméletében is: az egyedi terminusok kategóriája felel meg a *természetes szám* fogalmának. (A továbbiakban – hacsak külön nem jelezzük – számon mindig természetes számot értünk.)

Az axiómákkal az alábbi struktúrát szeretnénk leírni:

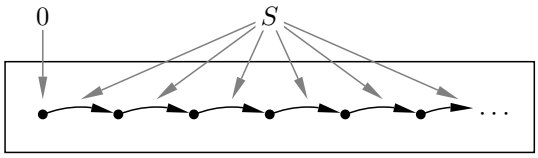
$$0, 1, 2, 3, 4, 5, 6, 7, \ldots$$

– vagy rovátkákkal:

$$, |, ||, |||, ||||, |||||, ||||||, |||||||, \ldots$$

Az elmélet szándékolt modelljéről tehát határozott elképzeléseink vannak. Az alább sorra vett axiómákra érdemes úgy gondolni, mint amelyek kizárnak egy-egy eltérési lehetőséget a megcélzott struktúrától.

6. ábra. $\mathbb{N}$: a természetes számok megcélzott struktúrája.



A1 Minden számnak van rákövetkezője.

$$\forall x\ \exists y\ xSy$$

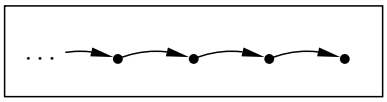
Ezzel az axiómával kizárjuk azt, hogy a számok sorozata egy ponton véget érjen (lásd az ábrát: $\mathcal{M}_1 \not\models \mathbf{A1}$).

A2 Egy számnak sincs két rákövetkezője.

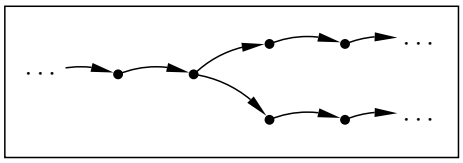
$$\forall x\ \forall y\ \forall y'\ \big((xSy\ \&\ xSy') \supset y = y'\big)$$

Ezzel kizárjuk, hogy elágazások keletkezzenek a számok sorozatában (lásd az ábrát: $\mathcal{M}_2 \models \mathbf{A1}; \mathcal{M}_2 \not\models \{\mathbf{A1}, \mathbf{A2}\}$).

7. ábra. $\mathcal{M}_1$: a számok sorozatának van végpontja.



8. ábra. $\mathcal{M}_2$: a számok sorozata elágazik.



A3 Nem lehet két számnak ugyanaz a rákövetkezője.

$$\forall x\ \forall x'\ \forall y\ \big((xSy\ \&\ x'Sy) \supset x = x'\big)$$

Ezzel kizárjuk, hogy párhuzamosan futó szálak összefussanak (lásd az ábrát: $\mathcal{M}_3 \models \{\mathbf{A1}, \mathbf{A2}\}; \mathcal{M}_3 \not\models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}\}$).

A4 A nulla egy számnak sem rákövetkezője.

$$\forall x\ (\sim xS0)$$

Ezzel biztosítjuk, hogy a számok sorozatának legyen kezdőpontja (lásd az ábrát: $\mathcal{M}_4 \models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}\}; \mathcal{M}_4 \not\models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}, \mathbf{A4}\}$).

Vajon sorra vettünk minden lényeges strukturális tulajdonságot? A fenti négy axióma biztosítja azt, hogy a számok nullától induló sorozata végtelen hosszan folytatódjon. Azt azonban még nem zártuk ki, hogy ezen a sorozaton kívül is legyenek számok. Egy ilyen lehetőség az, hogy van egy alternatív nulla, és a belőle induló alternatív számsorozat.

Ennek a lehetőségnek a kivédésére felvehetnénk a következő axiómát (de nem tesszük):

(1) A nullán kívül minden rákövetkezője valaminek.

$$\forall x\ (x \neq 0 \supset \exists y\ ySx)$$

Az ábrán szereplő modellt ezzel elkerültük (ti. $\mathcal{M}_5 \not\models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}, \mathbf{A4}, (1)\}$). De messzire ezzel sem jutunk: egy, a nullával kezdődő sorozaton kívüli szám akár önmaga rákövetkezője is lehetne (lásd az ábrát: $\mathcal{M}_6 \models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}, \mathbf{A4}, (1)\}$).

Ez újabb ad hoc feltevésbe hajszol bennünket:

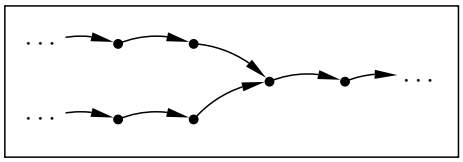
(2) Egyetlen szám sem következik önmagára.

$$\sim\exists x\ xSx$$

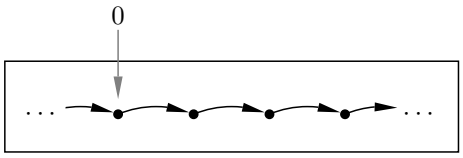
Ezzel ismét megúszunk egy devián modellt (ti. $\mathcal{M}_6 \not\models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}, \mathbf{A4}, (1), (2)\}$); de mi van, ha hosszabb a körkörösség? Ez ismét devián modellhez vezetne (lásd az ábrát: $\mathcal{M}_7 \models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}, \mathbf{A4}, (1), (2)\}$). Tovább menekülünk a következő hipotézishez:

(3) Nincsenek rákövetkezési körök.

9. ábra. $\mathcal{M}_3$: egybetorkollás a számok sorozatában.



10. ábra. $\mathcal{M}_4$: a nulla nem kezdőpont.



Ezt a hipotézist nem könnyű elsőrendben megfogalmazni, hiszen a kör hossza határozatlan:

$$\sim\exists x\ xSx\ \&\ \sim\exists x\ \exists x'\ (xSx'\ \&\ x'Sx)\ \&\ \sim\exists x\ \exists x'\ \exists x''\ (xSx'\ \&\ x'Sx''\ \&\ x''Sx)\ \&\ \ldots$$

Hogy a végtelen formulát elkerüljük, kezelhetjük úgy a hipotézist, mint ami végtelen sok formulát képvisel; tehát formulasémaként:

$$\sim\exists x_0\ \ldots\exists x_n\ (x_0Sx_1\ \&\ \ldots\ \&\ x_{n-1}Sx_n\ \&\ x_nSx_0)$$

Itt a számindexek csak arra szolgálnak, hogy jelezzék, hogy kell a sémának megfelelő egyes formulákat előállítani.

Világos, hogy (3) $\Rightarrow$ (2) (sőt: a (3) sémának (2) az egyik konkrét esete), tehát ez az előző hipotézis általánosítása. A felvételével kizárhatjuk a körkörösséget (ti. $\mathcal{M}_7 \not\models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}, \mathbf{A4}, (1), (2)\} \cup (3)$ – azért használunk uniójelet, mert (3) séma, amely egy formulahalmazt képvisel). De még mindig nem vagyunk biztonságban. Hogy tudnánk kizárni azt, hogy a nullától induló számsorozaton kívül van egy alternatív sorozat, amely az egész számokéhoz hasonlóan mindkét irányban végtelen? (Lásd az ábrát: $\mathcal{M}_8 \models \{\mathbf{A1}, \mathbf{A2}, \mathbf{A3}, \mathbf{A4}, (1), (2)\} \cup (3))$.

Ezt a struktúratípust már nem lesz könnyű elkerülni. Megpróbálkozhatunk azzal, hogy minden nullától különböző szám elérhető egy, két, három, négy stb. lépésben a nullából:

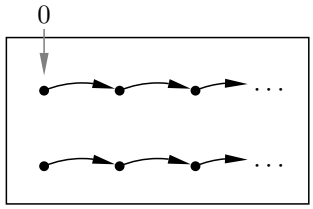
(4) Minden szám benne van a nullával induló számsorozatban.

$$\forall x\ \big(x = 0 \vee 0Sx \vee \exists y\ (0Sy\ \&\ ySy) \vee \exists y\ \exists y'\ (0Sy\ \&\ ySy'\ \&\ y'S0) \vee \ldots\big)$$

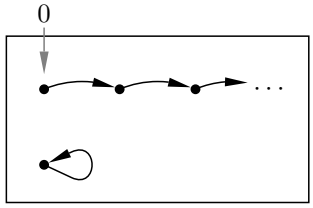
Ez ismét egy végtelen formula; és sajnos nem is tudjuk sémává alakítani, hiszen az egyes véges tagjait nem konjunkció, hanem diszjunkció köti.

Az alternatív számsorozat kizárására Dedekind egy nagyszerű ötletét vesszük elő. Akkor mondjuk, hogy egy T aritmetikai tulajdonság öröklődik a rákövetkezésre, ha minden szám, amely rendelkezik T-vel, megfertőzi vele a rákövetkezőjét is. Az egy sorozatba tartozást pedig azzal a követelménnyel biztosítjuk, hogy ha egy aritmetikai tulajdonság igaz nullára és öröklődik a rákövetkezésre, akkor a tulajdonság igaz minden számra. Mivel tulajdonságokra predikátummal tudunk utalni, a keresett axióma a következő formát ölti:

11. ábra. $\mathcal{M}_5$: van egy alternatív nulla.



12. ábra. $\mathcal{M}_6$: van egy szám, amely önmagára következik.



A5$_2$ Ha egy tulajdonság igaz nullára és öröklődik a rákövetkezésre, akkor igaz minden számra.

$$\forall T\ \big((T0\ \&\ \forall x\ \forall y\ ((Tx\ \&\ xSy) \supset Ty)\big) \supset \forall x\ Tx\big)$$

Ez a formula még mindig nem sérti az elsőrendű nyelvek szintaxisát; ugyanis nem csak individuumok (számok), hanem individuumok halmazai (számtulajdonságok) felett is kvantifikálunk benne. Az ilyen kvantifikációt másodrendű kvantifikációnak nevezzük; azt a logikát pedig, amely megengedi a másodrendű kvantifikációt, másodrendű logikának. (Lásd később.) De ez a verzió már alkalmas arra, hogy elsőrendű sémává szelídítsük:

A5 Ha egy nyitott aritmetikai formula igaz nullára és öröklődik a rákövetkezésre, akkor igaz minden számra.

$$\big(\varphi(0)\ \&\ \forall x\ \forall y\ ((\varphi(x)\ \&\ xSy) \supset \varphi(y))\big) \supset \forall x\ \varphi(x)$$

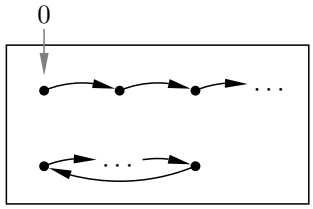
– ahol $\varphi(x)$ a Peano-aritmetika nyelvének tetszőleges nyitott formulája (amelyben nem szerepel szabadon y).

A Peano–axiómarendszernek ezt a nevezetes axiómasémáját *indukciós sémának* nevezzük. A segítségével végre sikerült kizárnunk a párhuzamos számsorozatok létezését; és egyben a hurkokét és körökét is, így feleslegessé váltak az (1)-(3) ad hoc hipotézisek: $\mathcal{M}_8 \not\models \{\mathbf{A1}, \mathbf{A1}, \mathbf{A2}, \mathbf{A4}\} \cup \mathbf{A5}$, de $\mathbb{N} \models \{\mathbf{A1}, \mathbf{A1}, \mathbf{A2}, \mathbf{A4}\} \cup \mathbf{A5}$.

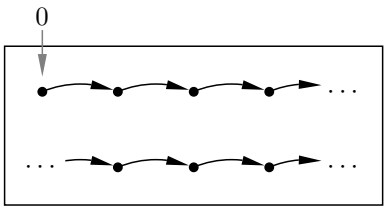
Ezzel, amennyire csak egy elsőrendű elmélet keretei között lehetséges, tisztáztuk a természetes számok rákövetkezési viszonyait. Most rátérhetünk a műveletek viselkedésére. Mivel ezeket relációként vezettük be, a kifejtés meglehetősen nehézkes lesz; a következő szakaszban nagyon sokat egyszerűsítünk rajta.

Az összeadás és a szorzás tulajdonságait az indukciós sémával összhangban adjuk meg. Először a nulla hozzáadására vonatkozó szabályokat rögzítjük, majd azt, hogy egy szám rákövetkezőjének hozzáadásahogyan függ az eredeti szám hozzáadásától; és ugyanígy járunk el a szorzás esetében is. Mindenekelőtt azonban azt kell biztosítani, hogy egyáltalán létezik bármely két szám összege és szorzata.

13. ábra. $\mathcal{M}_7$: számok körbekövetik egymást.



14. ábra. $\mathcal{M}_8$: párhuzamos számsorozat.



A6 Bármely két számnak van összege.

$$\forall x\ \forall y\ \exists z\ \ +(x,y,z)$$

A7 Bármely két számnak van szorzata.

$$\forall x\ \forall y\ \exists z\ \ \cdot(x,y,z)$$

Azt már fölösleges kikötni, hogy csak egy összeg, illetve szorzat létezik; ez bizonyítható a következő axiómákból.

A8 Egy számhoz nullát hozzáadva visszakapjuk az eredeti számot.

$$\forall x\ \forall y\ (+(x,0,y) \supset x = y)$$

A9 Ha egy szám rákövetkezőjét adjuk hozzá egy másik számhoz, akkor az eredmény rákövetkezőjét kapjuk.

$$\forall x\ \forall y\ \forall y'\ \forall z\ \forall z'\ \big((ySy'\ \&\ +(x,y,z)\ \&\ +(x,y',z')) \supset zSz'\big)$$

A10 Egy számot nullával szorozva nullát kapunk.

$$\forall x\ \forall y\ (\cdot(x,0,y) \supset y = 0)$$

A11 Ha egy szám rákövetkezőjével szorzunk egy másik számot, akkor az eredeti szorzat és a másik szám összegét kapjuk.

$$\forall x\ \forall y\ \forall y'\ \forall z\ \forall z'\ \big((ySy'\ \&\ \cdot(x,y,z)\ \&\ \cdot(x,y',z')) \supset +(z,x,z')\big)$$

Ezzel végére értünk az axiómák sorának. A Peano-aritmetika relációs változatán az **A1-A11** axiómák összességét értjük (mivel **A5** séma, ez valójában végtelen sok axiómát jelent). Most következhetne a rendszer mozgásba lendítése fogalmak definiálásával és tételek bizonyításával. Nem ezt fogjuk tenni; hanem egyszerűbb formában újraépítjük az elméletet.

Az **A9** és **A11** műveleti axiómák áttekinthetetlenségét az okozta, hogy műveleti jelek híján kénytelenek voltunk az összeadást és a szorzást háromtagú relációkként értelmezni. Ha a logikai eszköztárunkban lennének műveleti jelek is, akkor könnyebb dolgunk lenne.

5. A klasszikus elsőrendű nyelvek bővítése műveleti jelekkel

Bevezetjük a nem-logikai konstansok egy új kategóriáját a klasszikus elsőrendű nyelvekbe: a *műveleti jelekét*. A predikátumokhoz hasonlóan ezeket is az argumentumszámuk jellemzi; a függvényjelek olyan kifejezések, amelyekbe egy vagy több egyedi terminust behelyettesítve egyedi terminust kapunk. (A műveleti jeleket nevezik *függvényjeleknek* vagy *névfunktoroknak* is.) Műveleti jelekre az f, g stb. paraméterekkel utalunk. A relációkhoz hasonlóan ha nem okoz félreértést, elhagyjuk az argumentumokat körülvevő zárójeleket: $f(x)$ helyett fx-et, $g(x,y)$ helyett xgy-t írunk.

A korábbiakban bevezetett logikai eszközeinket köznyelvi példákkal motiváltuk. Nehéz azonban olyan köznyelvi példamondatot találni, amelynek logikai fordításában kézenfekvő volna a műveleti jelek használata; ezért is nem használtunk eddig műveleti jeleket. A számtani példák viszont kétségkívül meggyőzőek. Tekintsük a rákövetkezést kéttagú reláció helyett egybemenetű műveletnek, az összeadást pedig háromtagú reláció helyett kétbemenetű műveletnek. Ekkor $S(x,y)$ helyett az $y = s(x)$ azonossági kijelentést írhatjuk, $+(x,y,z)$ helyett pedig $x + y = z$-t. Így az $1 + 1 = 2$ mondat a következő formát ölti:

$$s(0) + s(0) = s(s(0)).$$

Ugyanez predikátumokkal kifejezve kevésbé átlátható:

$$\forall x\ \forall y\ \big((0Sx\ \&\ xSy) \supset +(x,x,y)\big)$$

Ha pedig azt akarjuk kifejezni, hogy bármely számra $x+(y+z) = (x+y)+z$, azt műveleti jelekkel közvetlenül megtehetjük:

$$\forall x\ \forall y\ \forall z\ \big(x + (y + z) = (x + y) + z\big);$$

míg ugyanez relációkban kifejezve reménytelenül bonyolulttá válik:

$$\forall x\ \forall y\ \forall z\ \forall u\ \forall v\ \forall w\ \big((+(y,z,u)\ \&\ +(x,u,v)\ \&\ +(x,y,w)) \supset +(w,z,v)\big).$$

A példákból az is kiderül, hogy a predikátumokkal szemben a műveleti jelek beágyazhatók egymásba. Míg a

$$+(x,+(y,z),v)$$

nem jólformált kifejezés, hiszen $+(y,z)$ formula, nem pedig egyedi terminus, addig az

$$v = x + (y + z)$$

jólformált. Hasonlóképpen jólformált például a $2 + 2 = 4$ összefüggést kifejező

$$ss0 + ss0 = sss0$$

is. (Mint említettük, elhagyjuk a félreértés nélkül elhagyható zárójeleket; $sss0$ az $s(s(s(0)))$ összetett terminust rövidíti.)

Szintaxis

Az egyedi terminusokat rekurzív meghatározással tudjuk bevezetni:

(1) A változók terminusok.

(2) A névkonstansok terminusok.

(3) Ha f egy n-argumentumú műveleti jel, $t_1, \ldots, t_n$ pedig terminusok, akkor $f(t_1, \ldots, t_n)$ terminus.

A formulaképzési szabályok változatlanok maradnak.

Szemantika

A ϱ interpretációfüggvény értelmezési tartományát kiterjesztjük a műveleti jelekre, hiszen ezek is a nyelv nem-logikai konstansai. Egy n-argumentumú műveleti jel jelölete egy olyan függvény, amely individuumok rendezett n-esehez rendel individuumokat:

$$\varrho(f) : U^n \longrightarrow U;$$

Így az egyedi terminusok jelöletét is rekurzív meghatározással rögzíthetjük:

(1) Ha t változó, akkor $|t|_{U,\varrho,v} = v(t)$.

(2) Ha t névkonstans, akkor $|t|_{U,\varrho,v} = \varrho(t)$.

(3) Ha $t = f(t_1, \ldots, t_n)$, akkor $|t|_{U,\varrho,v} = \varrho(f)\big(|t_1|_{U,\varrho,v}, \ldots, |t_n|_{U,\varrho,v}\big)$.

A formulák igazságfeltételei változatlanok maradnak.

Most már nekiláthatunk a Peano-aritmetika újrafogalmazásának.

6. Peano-aritmetika: műveleti jeles változat

A műveleti jelekkel kifejtett aritmetika nyelvében a következő primitív jelekre támaszkodunks:

0 névkonstans: nulla;

s egyargumentumú műveleti jel: sx az x rákövetkezője;

$+$ kétargumentumú műveleti jel: $x + y$ az x és az y összege;

$\cdot$ kétargumentumú műveleti jel: $x \cdot y$ az x és az y szorzata.

A műveleti jelek használata fölöslegessé teszi az **A1**, **A2**, **A6** és **A7** axiómákat; hiszen a mveleti jeleket nem használhatnánk, ha nem létezne bármely bemenetre pontosan egy eredményük. (A műveleti jeles változatnak ez az eleganciája bizonyos szempontbó hátrány; a számokkal szembeni elvárásaink egy része a nyelv szintaxisában van elrejtve.)

A többi axiómát újraszámozzuk:

PA1 A nulla egy számnak sem rákövetkezője (vö. **A6**).

$$\forall x \ \sim sx = 0$$

PA2 Nem lehet két számnak ugyanaz a rákövetkezője (vö. **A3**).

$$\forall x \ \forall x' \ (sx = sx' \ \supset \ x = x')$$

PA3 Ha egy tulajdonság (a) igaz nullára és (b) öröklődik a rákövetkezésre, akkor (c) igaz minden számra (vö. **A5**).

$$\big(\underbrace{\varphi(0)}_{\text{(a)}} \ \& \ \underbrace{\forall x \ (\varphi(x) \supset \varphi(sx))}_{\text{(b)}}\big) \underbrace{\supset \forall x \ \varphi(x)}_{\text{(c)}}$$

PA4 Egy számhoz nullát hozzáadva visszakapjuk az eredeti számot (vö. **A8**).

$$\forall x \ x + 0 = x$$

PA5 Ha egy szám rákövetkezőjét adjuk hozzá egy másik számhoz, akkor az eredmény rákövetkezőjét kapjuk (vö. **A9**).

$$\forall x\ \forall y\ x + sy = s(x + y)$$

PA6 Egy számot nullával szorozva nullát kapunk (vö. **A10**).

$$\forall x\ x \cdot 0 = 0$$

PA7 Ha egy szám rákövetkezőjével szorzunk egy másik számot, akkor az eredeti szorzat és a másik szám összegét kapjuk (vö. **A11**).

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

Ezzel másodszor is végére értünk az axiómák kifejtésének; a Peano-aritmetika műveleti jeles változatán a **PA1-PA7** axiómák összességét értjük (ez ismét csak végtelen sok axióma). Most már igazán ideje, hogy definíciókkal és tételekkel mozgásba hozzuk a rendszert.

7. Néhány bizonyítás a Peano-aritmetikában

A nullától különböző természetes számokat értelemszerűen definiálhatjuk a rákövetkezéssel:

$$1 \underset{\text{def}}{=} s0$$

$$2 \underset{\text{def}}{=} s1$$

$$\dots$$

$$101 \underset{\text{def}}{=} s100$$

$$\dots$$

Most lássunk néhány egyszerű bizonyítást az axiómarendszerünkben.

Tétel $2 \cdot 2 = 4$ *Bizonyítás*: Elindulunk a baloldaltól, és a definíciók és axiómák mentén eljutunk a jobboldalhoz.

$$2 \cdot 2 \underset{\text{def.}}{=} ss0 \cdot ss0 \underset{\text{PA7}}{=} (ss0 \cdot s0) + ss0 \underset{\text{PA7}}{=} ((ss0 \cdot 0) + ss0) + ss0 \underset{\text{PA6}}{=}$$

$$(0 + ss0) + ss0 \underset{\text{PA5}}{=} s(0 + ss0) + s0 \underset{\text{PA5}}{=} ss(0 + ss0) + 0 \underset{\text{PA4}}{=}$$

$$ss(0 + ss0) \underset{\text{PA5}}{=} sss(0 + s0) \underset{\text{PA5}}{=} ssss(0 + 0) \underset{\text{PA4}}{=} ssss0 \underset{\text{def.}}{=} 4$$

A példából látható, hogy konkrét számokkal végzett műveletek kiszámolásához csak a műveleti axiómákra van szükség.

Tétel A nullán kívül minden szám rákövetkezője valamely számnak.

$$\forall x\ (x = 0 \vee \exists x'\ x'Sx)$$

Bizonyítás: Az indukciós sémát használjuk úgy, hogy annak utótagja legyen a tétel; így

$$\varphi(x) \Longleftrightarrow x = 0 \vee \exists x'\ x'Sx$$

Az előtag két felét kell bizonyítani; vagyis azt, hogy (1) $0 = 0 \vee \exists x'\ x'Sx$, és (2) $\forall x\ \forall y\ \big((x = 0 \vee \exists x'\ x'Sx)\ \&\ xSy\big) \supset (y = 0 \vee \exists x'\ x'Sy)\big)$. Vegyük észre, hogy (1) is, (2) is logikai igazság: (1) nulla azonos nullával; (2) egy szám rákövetkezőjére mindig igaz, hogy rákövetkezője valaminek. □

Tétel Az összeadás asszociatív.

$$\forall x\ \forall y\ \forall z\ (y+z)+x = y+(z+x)$$

Bizonyítás: Az indukciós sémát fogjuk használni, éspedig úgy, hogy $\varphi(x)$-et $\forall y\,\forall z\ (y+z)+x = y+(z+x)$-nek választjuk; tehát x azon tulajdonságának, hogy bármely háromtagú összeadás, amelynek harmadik tagja x, átzárójelezhető. Így a konkrét axióma, amelyre támaszkodunk, a következő lesz:

$$\big(\forall y\ \forall z\ (y+z)+0 = y+(z+0)\ \&$$

$$\forall x\ \big(\forall y\ \forall z\ (y+z)+x = y+(z+x) \supset \forall y\ \forall z\ (y+z)+sx = y+(z+sx)\big)\big) \supset$$

$$\forall x\ \forall y\ \forall z\ (y+z)+x = y+(z+x)$$

Mivel tételünk az axióma utótagja, azt kell megmutatnunk, hogy az előtag mindkét fele igaz. Legyen y és z tetszőlegesen adott. Ekkor egyrészt

$$(y+z)+0 \underset{\text{PA4}}{=} y+z \underset{\text{PA4}}{=} y+(z+0);$$

másrészt ha valamely x-re feltesszük, hogy $(y+z)+x = y+(z+x)$, akkor

$$(y+z)+sx \underset{\text{PA5}}{=} s((y+z)+x)$$

Az utóbbiban szereplő $(y+z)+x$ a feltevés szerint átzárójelezhető $y+(z+x)$-szé; így

$$s((y+z)+x) \underset{\text{felt.}}{=} s(y+(z+x)).$$

Az utóbbira ismét alkalmazhatjuk a **PA5** axiómát:

$$s((y+z)+x) \underset{\text{PA5}}{=} y+s(z+x) \underset{\text{PA5}}{=} y+(z+sx) \underset{\text{PA5}}{=}$$

– és kész a bizonyítás. □

8. Az aritmetika nyelvének kifejezőereje

Befejezésül lássuk néhány alapvető számtani fogalom meghatározását, és végül a számelmélet két nyitott problémáját.

Meghatározás Kisebb vagy egyenlő:

$$x \le y \underset{\text{def}}{\iff} \exists z\ y = x+z$$

Meghatározás Kisebb, mint:

$$x < y \underset{\text{def}}{\iff} x \le y\ \&\ x \neq y$$

Meghatározás Négyzetszám:

$$N(x) \underset{\text{def}}{\iff} \exists y\ x = y \cdot x$$

Meghatározás Oszthatóság:

$$x|y \underset{\text{def}}{\iff} \exists z\ y = x \cdot z$$

Meghatározás Páros szám:

$$P(x) \underset{\text{def}}{\iff} 2|x$$

Meghatározás Prímszám:

$$Pr(x) \underset{\text{def}}{\iff} \forall y \ \big(y|x \supset (y = 1 \vee y = x)\big)$$

Meghatározás Legnagyobb közös osztó:

$$x = LNKO(y, z) \underset{\text{def}}{\iff} x|y \ \& \ x|z \ \& \ \forall x' \ \big((x'|y \ \& \ x'|z) \supset x' \leq x\big)$$

Meghatározás Relatív prímek:

$$xRPy \underset{\text{def}}{\iff} \forall z \ \big((z|x \ \& \ z|y) \supset z = 1)\big)$$

Meghatározás Ikerprímek:

$$xIy \underset{\text{def}}{\iff} Prx \ \& \ Pry \ \& \ y = x + 2$$

Ikerprím-sejtés Nincs legnagyobb ikerprím-pár.

$$\sim \exists x \ \exists y \ \big(xIy \ \& \ \forall x' \ \forall y' \ (x'Iy' \supset x' \leq x)\big)$$

Goldbach-sejtés Bármely páros szám felbontható két prímszám összegére.

$$\forall x \ (Px \supset \exists y \ \exists z \ (Pr(y) \ \& \ Pr(z) \ \& \ x = y + z)$$