Matemaattinen logiikka

Jouko Väänänen

November 29, 2010

Contents

1 Johdanto

Logiikan peruskäsitteitä

- lause ("Jokaisella ei-negatiivisella luvulla on neliöjuuri")
- kaava ("Luvulla x on neliöjuuri", "x saa enemmän palkkaa kuin y")
- malli (Rationaalilukujen kunta, tietokanta)
- todistus (Wilesin todistus Fermat'n suurelle lauseelle)
- totuus (Lause "Jokaisella ei–negatiivisella luvulla on neliöjuuri" on tosi reaalilukujen kunnassa muttei rationaalilukujen kunnassa)

  [Ei ole tärkeää tietää tässä vaiheessa mitä *kunnat* ovat!]

Määrittelemme yllämainitut peruskäsitteet matemaattisen tarkasti ja todistamme niiden perusominaisuudet:

- Helppo: Todistuvat lauseet ovat tosia kaikissa malleissa.
- Vaikeampi: Lause joka on tosi kaikissa malleissa on todistuva.
- Vaikea: Monet matematiikan kannalta tärkeät todistuskäsitteen ovat *epätäydellisiä*, eli on olemassa lauseita, joita ei voi todistaa niissä todeksi eikä epätodeksi.

1.1 Merkintöjä

Käytämme tavallisia joukko-opillisia merkintöjä, kuten

$$\{a_1, \ldots, a_n\}, A \cap B, A \cup B, A \setminus B, \emptyset.$$

Luonnollisten lukujen joukkoa $\{0, 1, 2, \ldots\}$ merkitään $\mathbb{N}$. Alkioiden a ja b järjestettyä paria merkitään $\langle a, b\rangle$. Sille pätee

$$\langle a, b\rangle = \langle c, d\rangle \iff a = c \text{ ja } b = d.$$

Järjestettyä jonoa merkitään $\langle a_1, \ldots, a_n\rangle$. Sille pätee vastaavasti:

$$\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle \iff a_1 = b_1 \text{ ja ... ja } a_n = b_n.$$

Karteesista tuloa $A \times A$ merkitään A^2 ja n-kertaista tuloa A^n.

2 Propositiologiikka

Propositiologiikassa tutkitaan hyvin yksinkertaisten, mutta täsmällisesti määriteltyjen lauseiden loogisia ominaisuuksia. Näitä lauseita kutsutaan propositiolauseiksi ja ne muodostuvat niin sanotuista propositiosymboleista

$$p_0, p_1, \ldots$$

konnektiiveilla

$\neg$	negaatio
$\wedge$	konjunktio
$\vee$	disjunktio
$\rightarrow$	implikaatio
$\leftrightarrow$	ekvivalenssi

Propositiologiikan matemaattisessa tarkastelussa on yksinkertaisinta valita tietyt konnektiivit perussymboleiksi joiden avulla muut määritellään. Puolalaisen Łukasiewiczin mukaisesti valitsemme negaation ja implikaation. Propositiolauseiden keskeinen ominaisuus on todistuvuus, joka alla määritellään.

Määritelmä 2.1 Propositiolauseiden *joukko määritellään seuraavasti:*

(P1) Propositiosymbolit $p_0, p_1, \ldots$ *ovat propositiolauseita.*

(P2) Jos A *on propositiolause niin* $\neg A$ *on propositiolause.*

(P3) Jos A *ja* B *ovat propositiolauseita niin* $(A \rightarrow B)$ *on propositiolause.*

Proposilogiikan aksioomien *joukko määritellään seuraavasti*

- *Jos* A *ja* B *ovat propositiolauseita, niin*

  (A1) $(A \rightarrow (B \rightarrow A))$

  on aksiooma.

- *Jos* A *ja* B *ovat propositiolauseita, niin*

  (A2) $((\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B))$

  on aksiooma

- *Jos A, B ja C ovat propositiolauseita, niin*

  (A3) $(((A \to (B \to C)) \to ((A \to B) \to (A \to C)))$

  on aksiooma.

Lausejoukosta S todistuvien propositiolauseiden joukko määritellään seuraavasti

(T1) Jokainen S:n alkio on todistuva joukosta S.

(T2) Jokainen aksiooma on todistuva joukosta S.

(T3) Jos A ja $(A \to B)$ ovat todistuvia joukosta S niin myös B on todistuva joukosta S.

Jos A on todistuva joukosta S, merkitään $S \vdash A$. Jos $\emptyset \vdash A$, merkitään $\vdash A$ ja sanotaan, että A on todistuva.

Aksiooman (A1) idea on, että jos tiedämme A:n todeksi, ei asia muutu vaikka lisäämme uuden oletuksen B. Aksioomaa (A2) kutsutaan *kontraposition laiksi.* Se kertoo epäsuoran todistuksen idean: jos B:n kielto on ristiriidassa A:n kanssa ja tiedämme A:n todeksi, niin B:n on oltava tosi. Aksiooma (A3) on eräänlainen implikaation transitiivisuusominaisuus: jos A:sta seuraa B ja ehdolla A myös B:stä seuraa C, niin myös A:sta seuraa C.

Sopimus: Propositiolauseen ulommaisia sulkuja ei aina merkitä näkyviin.

Esimerkki 2.2 *Seuraavat ovat propositiolauseita*

$$p_0$$
$$(p_0 \to p_0)$$
$$(p_1 \to \neg(p_2 \to p_1))$$
$$(((p_0 \to p_1) \to \neg p_2) \to p_3).$$

Seuraavat ovat todistuvia propositiolauseita

$$(p_0 \to (p_1 \to p_0))$$
$$((\neg p_0 \to \neg p_1) \to (p_1 \to p_0))$$
$$(((p_0 \to (p_1 \to p_0)) \to ((p_0 \to p_1) \to (p_0 \to p_0)))$$
$$((p_0 \to p_1) \to (p_0 \to p_0)).$$

Viimeksimainittu seuraa Modus Ponensilla ensimmäisestä ja kolmannesta.

Esimerkki 2.3

$\{A, (A \to B)\} \vdash B$
$\{A\} \vdash (B \to A)$
$\{(\neg B \to \neg A)\} \vdash (A \to B)$
$\{(\neg B \to \neg A), A\} \vdash B$
$\{(A \to (B \to C))\} \vdash ((A \to B) \to (A \to C))$
$\{(A \to (B \to C)), (A \to B)\} \vdash (A \to C)$
$\{(A \to (B \to C)), (A \to B), A\} \vdash C$

Lause 2.4 $\vdash (A \to A)$

Todistus. Idea on seuraava: (A3):n nojalla

$$((A \to (B \to A)) \to ((A \to B) \to (A \to A)))$$

on todistuva. Toisaalta $(A \to (B \to A))$ on todistuva, joten MP:lla saadaan

$$((A \to B) \to (A \to A)).$$

Kaikki olisi hyvin, jos $(A \to B)$ olisi todistuva. Mutta valitaan B siten että $(A \to B)$ on todistuva. Valitaan $B = (A \to A)$. Siis:

1.	$(A \to (B \to A))$	(A1)
2.	$((A \to (B \to A)) \to ((A \to B) \to (A \to A)))$	(A3)
3.	$((A \to B) \to (A \to A))$	MP 1,2
4.	$(A \to B)$	(A1)
5.	$(A \to A)$	MP 3,4

□

Lause 2.5 $\vdash (\neg A \to (A \to B))$

Todistus. Aksiooma (A1) antaa

$$(\neg A \to (\neg B \to \neg A)),$$

mikä yhdistettynä aksioomaan (A2)

$$((\neg B \to \neg A) \to (A \to B))$$

ja aksioomaan (A3) johtaa toivottuun lopputulokseen. Merkitään selvyyden vuoksi $C = (\neg B \to \neg A)$ ja $D = (A \to B)$.

1.	$(C \to D)$	(A2)
2.	$((C \to D) \to (\neg A \to (C \to D)))$	(A1)
3.	$(\neg A \to (C \to D))$	MP 1,2
4.	$((\neg A \to (C \to D)) \to ((\neg A \to C) \to (\neg A \to D))$	(A3)
5.	$((\neg A \to C) \to (\neg A \to D))$	MP 3,4
6.	$(\neg A \to C)$	(A1)
7.	$(\neg A \to D)$	MP 5,6

□

Todistame nyt erittäin hyödyllisen todistuvien lauseiden yleisen ominaisuuden. Se osoittaa, että implikaation ja todistamisen välillä on intuitiotamme vastaava suhde.

Lause 2.6 (Deduktiolause) *Jos* $S \cup \{A\} \vdash B$ *niin* $S \vdash (A \to B)$ *(ja kääntäen).*

Todistus. Käytämme induktiota todistuvien lauseiden joukon mukaisesti.

1. $B \in S$. Siis $S \vdash B$. Toisaalta $S \vdash (B \to (A \to B))$, joten MP antaa $S \vdash (A \to B)$.

2. $B = A$. Lauseen 2.4 nojalla $S \vdash (A \to B)$.

3. B on aksiooma. Jälleen $S \vdash B$, ja kuten yllä $S \vdash (A \to B)$.

4. B on saatu MP:lla lauseista C ja $(C \to B)$ joille väite jo pätee, eli

   $$S \vdash (A \to C) \text{ ja } S \vdash (A \to (C \to B)).$$

   Koska (A3):n nojalla $S \vdash ((A \to (C \to B)) \to ((A \to C) \to (A \to B)))$, saamme MP:lla $S \vdash ((A \to C) \to (A \to B))$ ja uudelleen MP:lla $S \vdash (A \to B)$. □

Lemma 2.7 $\vdash (A \to ((A \to B) \to B))$.

Todistus. MP–säännön nojalla $\{A, (A \to B)\} \vdash B$. Deduktiolauseen nojalla $\{A\} \vdash ((A \to B) \to B)$ ja edelleen samalla perusteella $\vdash (A \to ((A \to B) \to B))$. □

Kaikki propositiolauseet eivät ole todistuvia, kuten esimerkiksi pelkkä p_0, tai vaikkapa $\neg(p_0 \to p_0)$. Todistaminen on ristiriidatonta siinä mielessä, että ei ole olemassa lausetta A jolle

$$\vdash A \text{ ja } \vdash \neg A.$$

Kätevä tapa osoittaa, että jokin lause ei ole todistuva on *totuusjakauma*.

Määritelmä 2.8 Totuusjakauma *on mikä tahansa funktio* $v : \mathbb{N} \to \{0, 1\}$. *Jos* A *on propositiolause, niin* A*:n* totuusarvo $v(A)$ *totuusjakaumassa* v *määritellään seuraavasti:*

$$v(p_n) = \quad v(n)$$

$$v(\neg A) = \quad \begin{cases} 0, \textit{ jos } v(A) = 1 \\ 1, \textit{ jos } v(A) = 0 \end{cases}$$

$$v((A \to B)) = \quad \begin{cases} 0, \textit{ jos } v(A) = 1 \textit{ ja } v(B) = 0 \\ 1, \textit{ muuten} \end{cases}$$

$$(\quad = \quad v(A) \cdot v(B) + 1 - v(A) \ )$$

Lause A on *tautologia* jos $v(A) = 1$ kaikilla v. Jos A on tautologia kaikilla $A \in S$, merkitään

$$v(S) = 1.$$

Jos $S = \emptyset$, sovimme että $v(S) = 1$ kaikilla v.

Esimerkki 2.9 $(p_n \to p_n)$ *on tautologia, sillä* $v((p_n \to p_n)) = 0$ *vain jos* $v(p_n) = 1$ *ja* $v(p_n) = 0$*, mikä on mahdotonta.* $(p_n \to \neg p_n)$ *ei ole tautologia, sillä jos* $v(n) = 1$ *saadaan* $v((p_n \to \neg p_n)) = 0$*.* $(\neg\neg A \to A)$ *on aina tautologia, sillä* $v((\neg\neg A \to A)) = 0$ *vain jos* $v(\neg\neg A) = 1 - (1 - v(A)) = v(A) = 1$ *ja* $v(A) = 0$*.*

Lause 2.10 *Todistuvat lauseet ovat tautologioita.*

Tämä seuraa hieman yleisemmästä tuloksesta:

Lause 2.11 *Jos* $v(S) = 1$ *ja* $S \vdash A$*, niin* $v(A) = 1$*.*

Todistus. Käytämme induktiota todistuksen käsitteen suhteen.

1. $A \in S$. Nyt $v(A) = 1$, koska $v(S) = 1$

2. A on aksiooma. Tarkastellaan kukin aksiooma erikseen. Jos $v((A \to (B \to A))) = 0$, niin $v(A) = 1$ ja $v((B \to A)) = 0$, eli $v(A) = v(B) = 1$ ja $v(A) = 0$, mikä on mahdotonta. Siis (A1) on tautologia. Aksioomien (A2) ja (A3) todistaminen jää harjoitustehtäväksi.

3. A seuraa MP:lla lauseista B ja $(B \to A)$ jotka ovat todistuvia joukosta S. Induktio oletuksena oletetaan, että $v(B) = 1$ ja $v((B \to A)) = 1$. Tästä seuraa $v(A) = 1$. □

Esimerkki 2.12 *Lause p_n ei ole todistuva, koska $v(p_n) = 0$ kun $v(n) = 0$. Lause $(p_0 \to \neg p_0)$ ei ole todistuva (ks. esimerkki 2.9). Lause $A = (p_0 \to (p_0 \to p_1))$ ei ole todistuva, sillä jos $v(0) = 1$ ja $v(1) = 0$, niin $v(A) = 0$.*

Otamme käyttöön seuraavat lyhenteet:

$$\begin{array}{rcll} (A \vee B) & = & (\neg A \to B) & \text{(disjunktio)} \\ (A \wedge B) & = & \neg(A \to \neg B) & \text{(konjunktio)} \\ (A \leftrightarrow B) & = & \neg((A \to B) \to \neg(B \to A)) & \text{(ekvivalenssi)} \end{array}$$

Esimerkki 2.13
$$\begin{array}{rcl} v((A \vee B)) & = & v(A) + v(B) - v(A) \cdot v(B) \\ v((A \wedge B)) & = & v(A) \cdot v(B) \\ v((A \leftrightarrow B)) & = & v((A \to B)) \cdot v((B \to A)) \end{array}$$

Esimerkki 2.14 *Seuraavat lauseet ovat tautologioita*

$$\begin{array}{c} ((A \vee B) \leftrightarrow (B \vee A)) \\ ((A \wedge B) \leftrightarrow (B \wedge A)) \\ ((A \leftrightarrow B) \leftrightarrow (B \leftrightarrow A)) \\ (\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)) \\ (\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B))) \\ (\neg(A \to B) \leftrightarrow (A \wedge \neg B))) \\ (\neg\neg A \leftrightarrow A) \\ \neg(A \ \wedge \ \neg A) \\ (A \ \vee \ \neg A) \end{array}$$

Tautologioiden tutkimiseen on kehitetty *totuustaulutekniikka*. Totuustaulun eri riveillä on kaikki relevantit totuusarvokombinaatiot. Jos tutkitaan lauseista A, B muodostettua propositiolausetta, riittää tuntea lauseiden A ja B totuusarvot:

A	$\neg A$
1	0
0	1

A	B	$(A \to B)$
1	1	1
1	0	0
0	1	1
0	0	1

A	B	$(A \wedge B)$
1	1	1
1	0	0
0	1	0
0	0	0

A	B	$(A \vee B)$
1	1	1
1	0	1
0	1	1
0	0	0

A	B	$(A \leftrightarrow B)$
1	1	1
1	0	0
0	1	0
0	0	1

Esimerkki 2.15 *Lauseen* $(((A \to B) \wedge (B \to C)) \to (A \to C))$ *totuustaulu*

A	B	C	$(((A$	$\to$	$B)$	$\wedge$	$(B$	$\to$	$C))$	$\to$	$(A$	$\to$	$C))$
1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1	0	0	1	1	0	0
1	0	1	1	0	0	0	0	1	1	1	1	1	1
1	0	0	1	0	0	0	0	1	0	1	1	0	0
0	1	1	0	1	1	1	1	1	1	1	0	1	1
0	1	0	0	1	1	0	1	0	0	1	0	1	0
0	0	1	0	1	0	1	0	1	1	1	0	1	1
0	0	0	0	1	0	1	0	1	0	1	0	1	0

Itse implikaation totuusarvoksi saatiin aina 1. *Siis lause on tautologia.*

On olemassa lauseita joiden muodosta ilmenee että kyseessä on tautologia, kuten

$$((A \wedge B) \to (A \vee C)).$$

Ei siis ole väliä, mitä A, B ja C ovat. Sen sijaan

$$((A \wedge B) \to (A \wedge C))$$

on tautologia joillakin C (esimerkikisi jo $C = B$), mutta ei kaikilla (esimerkiksi jos $A = p_0$, $B = p_1$ ja $C = p_2$).

Esimerkki 2.16

A	B	$((A$	$\to$	$B)$	$\wedge$	$\neg$	$A)$	$\to$	$\neg$	B
1	1	1	1	1	0	0	1	1	0	1
1	0	1	0	0	0	0	1	1	1	0
0	1	0	1	1	1	1	0	0	0	1
0	0	0	1	0	1	1	0	1	1	0

Nähdään että lause saa totuusarvon 0 kun $v(A) = 0$ ja $v(B) = 1$. Tämä on mahdollista esimerkiksi jos $A = p_0$ ja $B = p_1$: asetetaan $v(0) = 0$ ja $v(1) = 1$.

Määritelmä 2.17 *Propositiolausejoukko S on* ristiriitainen*, jos on olemassa A siten, että*

$$S \vdash A \text{ ja } S \vdash \neg A.$$

Muussa tapauksessa S on ristiriidaton*. S on* täydellinen *jos se on ristiriidaton ja kaikille lauseille A pätee*

$$S \vdash A \text{ tai } S \vdash \neg A$$

Huom. jos $v(S) = 1$, niin S on ristiriidaton.

Lause 2.18 *Seuraavat ehdot ovat ekvivalentit:*

(1) *S on ristiriitainen.*

(2) *kaikille B pätee $S \vdash B$.*

Todistus. Oletetaan $S \vdash A$ ja $S \vdash \neg A$. Olkoon B mielivaltainen. Lauseen 2.5 nojalla

$$S \vdash \neg A \to (A \to B).$$

Soveltamalla sääntöä MP kahdesti saadaan $S \vdash B$. Olkoon toisaalta (2) tosi. Tällöin mille tahansa A pätee $S \vdash A$ ja $S \vdash \neg A$ joten S on ristiriitainen. □

Lause 2.19 *Seuraavat ehdot ovat ekvivalentit:*

(1) $S \vdash A$

(2) $S \cup \{\neg A\}$ *on ristiriitainen.*

Todistus. Jos $S \vdash A$, niin $S \cup \{\neg A\} \vdash A$ ja $S \cup \{\neg A\} \vdash \neg A$, joten (2) seuraa. Olkoon sitten (2) tosi. Päättelemme seuraavasti:

1.	$S \cup \{\neg A\} \vdash \neg B$	Lause 2.18
2.	$S \vdash \neg A \to \neg B$	Deduktiolause, 1
3.	$S \vdash (\neg A \to \neg B) \to (B \to A)$	(A2)
4.	$S \vdash B \to A$	MP 2,3
5.	$S \vdash B$	Valitaan $B = (A \to A)$
6.	$S \vdash A$	MP 4,5

□

Lause 2.20 *Olkoon S täydellinen. Tällöin*

(1) $S \vdash \neg A \iff S \nvdash A$

(2) $S \vdash (A \to B) \iff (S \nvdash A$ *tai* $S \vdash B)$

Todistus. (1) Jos $S \vdash \neg A$, niin ristiriidattomuuden nojalla $S \nvdash A$. Jos taas $S \nvdash A$, niin täydellisyyden nojalla $S \vdash \neg A$.
(2) Olkoon aluksi $S \vdash (A \to B)$. Jos $S \vdash A$, niin $S \vdash B$. Siis $S \nvdash A$ tai $S \vdash B$. Olkoon kääntäen $S \nvdash A$. Tällöin kohdan 1 nojalla $S \vdash \neg A$. Lauseen 2.5 nojalla $S \vdash (A \to B)$. Olkoon lopuksi $S \vdash B$. Aksiooman (A1) nojalla $S \vdash (A \to B)$. □

Lause 2.21 *Jos $S \vdash A$, niin on olemassa äärellinen $S_A \subseteq S$ siten, että $S_A \vdash A$*

Todistus. Käytämme induktiota.

1. $A \in S$. Valitaan $S_A = \{A\}$.

2. A on aksiooma. Valitaan $S_A = \emptyset$

3. A seuraa MP:lla lauseista B ja $B \to A$. Induktio oletuksena oletetaan, että joukot $S_B \subseteq S$ ja $S_{B\to A} \subseteq S$ on jo valittu siten, että

$$S_B \vdash B \text{ ja } S_{B\to A} \vdash B \to A.$$

Olkoon $S_A = S_B \cup S_{B\to A}$. Nyt MP:n perusteella $S_A \vdash A$. □

Lause 2.22 (Ketjulause) *Jos $S_0 \subseteq S_1 \subseteq \ldots$ ovat ristiriidattomia propositiolausejoukkoja niin $S = \bigcup_{n=0}^{\infty} S_n$ on ristiriidaton.*

Todistus. Olkoon $S \vdash A$ ja $S \vdash \neg A$. Valitaan äärellinen $S' \subseteq S$ siten, että $S' \vdash A$ ja $S' \vdash \neg A$ (Lause 2.18). Olkoon $n \in \mathbb{N}$ sellainen että $S' \subseteq S_n$. Nyt $S_n \vdash A$ ja $S_n \vdash \neg A$, vastoin oletusta. □

Lause 2.23 (Lindenbaumin lemma) *Jos S on ristiriidaton joukko propositiolauseita, niin on olemassa täydellinen $S' \supseteq S$.*

Todistus. Olkoon $A_0, A_1, \ldots$ kaikkien propositiolauseiden numeroituva jono. Asetetaan $S_0 = S$. Jos S_n on määritelty, olkoon S_{n+1} saatu seuraavasti:

Tapaus 1 $S_n \vdash A_n$. Asetetaan $S_{n+1} = S_n \cup \{A_n\}$. Jos S_{n+1} on ristiriitainen, seuraa Lauseesta 2.21 $S_{n+1} \vdash \neg A_n$, Deduktiolauseesta $S_n \vdash A_n \to \neg A_n$ ja lopulta MP:sta $S_n \vdash \neg A_n$, vastoin oletusta, että S_n on jo valittu ristiriidattomaksi. Siis S_{n+1} on ristiriidaton.

Tapaus 2 $S_n \nvdash A_n$. Asetetaan $S_{n+1} = S_n \cup \{\neg A_n\}$. Jos S_{n+1} on ristiriitainen seuraa Lauseesta 2.19 $S_n \vdash A_n$, vastoin oletusta. Siis S_{n+1} on ristiriidaton.

Olkoon $S' = \bigcup_{n=0}^{\infty} S_n$. Ketjulauseen nojalla S' on ristiriidaton. Selvästi S' on täydellinen. □

Lause 2.24 *Jos S on ristiriidaton joukko propositiolauseita, niin on olemassa totuusjakauma v siten että $v(S) = 1$.*

Todistus. Lindenbaumin lemman nojalla on olemassa täydellinen $S' \supseteq S$. Olkoon

$$v(n) = \begin{cases} 1 \text{ jos } S' \vdash p_n \\ 0 \text{ jos } S' \vdash \neg p_n. \end{cases}$$

Apuväite: $v(A) = 1$ jos ja vain jos $S' \vdash A$. Käytetään induktiota lauseen A suhteen.

1. $A = p_n$. Tämä seuraa v:n määritelmästä.

2. $A = \neg B$. $v(\neg B) = 1$ joss $v(B) \neq 1$
   joss $S' \nvdash B$ ind.ol.noj.
   joss $S' \vdash \neg B$ Lause 2.20!.

3. $A = (B \to C)$. $v((B \to C)) = 1$ joss $v(B) \neq 1$ tai $v(C) = 1$
   joss $S' \nvdash B$ tai $S' \vdash C$ ind.ol.noj.
   joss $S' \vdash (B \to C)$ (Lause 2.20).

Siis apuväite on todistettu. Koska $S \subseteq S'$, saadaan $v(S) = 1$. □

Korollaari 2.25 Propositiologiikan täydellisyyslause

(1) *A on todistuva jos ja vain jos A on tautologia.*

(2) *$S \vdash A$ jos ja vain jos $v(A) = 1$ kaikilla totuusjakaumilla, joille $v(S) = 1$.*

Todistus. (1) seuraa (2):sta valitsemalla $S = \emptyset$. Todistamme siis vain (2):n. Jos $S \vdash A$, niin Lauseen 2.11 nojalla $v(A) = 1$ aina kun $v(S) = 1$. Jos taas $S \nvdash A$, niin Lauseen 2.18 nojalla $S \cup \{\neg A\}$ on ristiriidaton. Lauseen 2.24 nojalla on nyt olemassa v siten, että $v(S) = 1$ ja $v(A) = 0$. □

3 Struktuurit

Binäärinen relaatio on mikä tahansa joukko järjestettyjä pareja. Jos R on binäärinen relaatio, niin R:n *määrittelyjoukko* on joukko

$$\mathrm{dom}(R) = \{x| \text{ on olemassa } y \text{ siten että } \langle x, y\rangle \in R\}.$$

Vastaavasti R:n *arvojoukko* on joukko

$$\mathrm{ran}(R) = \{y| \text{ on olemassa } x \text{ siten että } \langle x, y\rangle \in R\}.$$

Siis

$$R \subseteq \mathrm{dom}(R) \times \mathrm{ran}(R).$$

n-paikkainen relaatio on mikä tahansa joukko järjestettyjä n-jonoja. Relaatio on

- *refleksiivinen A:ssa*, jos $\langle x, x\rangle \in R$ kun $x \in A$
- *irrefeleksiivinen A:ssa*, jos $\langle x, x\rangle \notin R$ kun $x \in A$
- *symmetrinen*, jos $\langle x, y\rangle \in R$ implikoi $\langle y, x\rangle \in R$
- *asymmetrinen*, jos $\langle x, y\rangle \in R$ implikoi $\langle y, x\rangle \notin R$
- *transitiivinen*, jos $\langle x, y\rangle \in R$ ja $\langle y, z\rangle \in R$ implikoi $\langle x, z\rangle \in R$
- *intransitiivinen*, jos $\langle x, y\rangle \in R$ ja $\langle y, z\rangle \in R$ implikoi $\langle x, z\rangle \notin R$
- *trikotominen A:ssa*, jos kaikille $x, y \in A$ pätee täsmälleen yksi vaihtoehdoista $\langle x, y\rangle \in R$, $x = y$, $\langle y, x\rangle \in R$
- *ekvivalenssirelaatio A:ssa* jos R on refleksiivien A:ssa ja symmterinen ja transitiivinen.
- *järjestysrelaatio A:ssa* jos R on transitiivinen ja trikotominen A:ssa.

Jos R on ekvivalenssirelaatio A:ssa, niin kaikille $x \in A$ määritellään

$$\begin{aligned} [x] &= \{y \in A | \langle x, y\rangle \in R\} \\ A/R &= \{[x] | x \in A\}. \end{aligned}$$

Relaatio R on *funktio*, jos kaikille $x \in \mathrm{dom}(R)$ on olemassa täsmälleen yksi y siten että $\langle x, y\rangle \in R$. Merkitään $f(x) = y$. $f : A \to B$ tarkoittaa, että f on funktio, $\mathrm{dom}(f) = A$ ja $\mathrm{ran}(f) \subseteq B$. Jos lisäksi $\mathrm{ran}(f) = B$, niin f on *surjektio*. Jos f on funktio ja kaikille $y \in \mathrm{ran}(f)$ on olemassa täsmälleen yksi x siten että $\langle x, y\rangle \in f$, niin f on *injektio*. $f : A \to B$ on *bijektio* jos f on injektio ja surjektio. Joukko A on äärellinen jos on olemassa $n \in \mathbb{N}$ ja bijektio

$$f : A \to \{0, \ldots, n-1\}.$$

A on numeroituva jos on olemassa injektio

$$f : A \to \mathbb{N}.$$

Tällöin on aina olemassa myös surjektio $g : \mathbb{N} \to A$, paitsi jos $A = \emptyset$.

Struktuurit eli mallit, joita nyt lähdemme tutkimaan, muodostuvat universumista ja sen alkioille määritellyistä relaatioista ja funktioista. Struktuurin käsite on hyvin yleinen – se kattaa esimerkiksi kaikki algebralliset struktuurit (ryhmät, kunnat jne.) ja myös yleisimmät tietokannat. Siksi on hämmästyttävää että struktuureista voidaan sanoa mitään mielenkiintoista tai epätriviaalia. Asian ydin on seuraavassa luvussa määriteltävä predikaattilogiikka, joka on kuin luotu ilmaisemaan struktuurien ominaisuuksia ja jolla on syvällisiä matemaattisia ominaisuuksia.

Struktuuri on mikä tahansa joukko ($\neq \emptyset$) M varustettuna äärellisellä jonolla relaatioita, funktioita ja vakioita. (Relaatioita, funktioita ja vakiotita voi olla ääretönkin määrä, mutta yleensä varsin pieni äärellinen määrä.) Struktuuria, jonka universumi on M, relaatiot ovat $P_1, \ldots, P_n$, funktiot ovat $f_1, \ldots, f_m$ ja vakiot ovat $c_1, \ldots, c_k$, merkitään

$$M = (M, P_1, \ldots, P_n, f_1, \ldots, f_m, c_1, \ldots, c_k).$$

Esimerkki 3.1 Kokonaislukujen ryhmä *on struktuuri*

$$\mathbf{Z} = (\mathbb{Z}, +, 0),$$

missä $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *on funktio ja 0 vakio.*

Vastaavasti monet tutut algebralliset struktuurit ovat esimerkkejä struktuureista, kuten

$$\begin{array}{ll} \mathbf{Q} = (\mathbb{Q}, +, \cdot, 0, 1) & \textit{(rationaalilukujen kunta)} \\ \mathbf{R} = (\mathbb{R}, +, \cdot, 0, 1) & \textit{(reaalilukujen kunta)} \end{array}$$

Esimerkki 3.2 *Järjestämätöntä binäärijonoa*

100110001

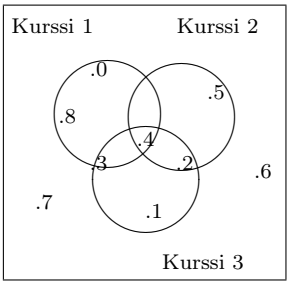
voidaan ajatella järjestämättömänä bittistruktuurina

$$(\{0, 1, \ldots, 8\}, \{0, 3, 4, 8\}),$$

jonka universumi on $\{0, 1, \ldots 8\}$ *ja jossa on 1–paikkainen relaatio (eli osajoukko). Universumi on joukko bittejä ja osajoukko kertoo, mitkä bitit ovat ykkösiä. Annettu binäärijono voi olla esimerkiksi opettajan kirjanpito siitä ketkä ovat suorittaneet tietyn kurssin. Jos kirjanpitoa pidetään useasta asiasta, tarvitaan useampia 1–paikkaisia relaatioita, jolloin syntyy* järjestämätön binäärinen taulukko *:*

Opiskelija	*Kurssi 1*	*Kurssi 2*	*Kurssi 3*
0	*1*	*0*	*0*
1	*0*	*0*	*1*
2	*0*	*1*	*1*
3	*1*	*0*	*1*
4	*1*	*1*	*1*
5	*0*	*1*	*0*
6	*0*	*0*	*0*
7	*0*	*0*	*0*
8	*1*	*0*	*0*

Sama kuvassa:



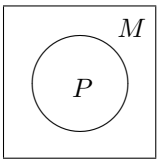
Tämäntyyppisen struktuurin yleinen muoto on

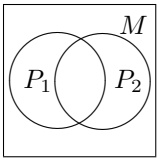
$$M = (M, P_1, P_2, P_3),$$

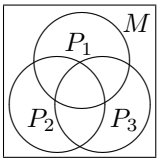
missä

$$P_1 \subseteq M$$
$$P_2 \subseteq M$$
$$P_3 \subseteq M.$$

Tällaista struktuuria sanotaan *monadiseksi*. 1–paikkaisia relaatioita P_i voi olla yksi, kaksi, kolme tai useampia – mikä tahansa määrä, kunhan ne kaikki ovat 1–paikkaisia:

(M, P) 

(M, P_1, P_2) 

(M, P_1, P_2, P_3) 

, ja niin edelleen.

Esimerkki 3.3 *Struktuuria $(M, \lhd)$, joka muodostuu universumista M ja sen järjestysrelaatiosta $\lhd$, sanotaan järjestetyksi joukoksi. Esimerkiksi*

$$\begin{array}{ll} (\mathbb{N}, \lhd), & \lhd = \{\langle n, m\rangle \in \mathbb{N} \times \mathbb{N} | n < m\} \\ (\mathbb{Q}, \lhd), & \lhd = \{\langle n, m\rangle \in \mathbb{Q} \times \mathbb{Q} | n < m\} \\ (\{0, 1, 2\}, \lhd), & \lhd = \{\langle 0, 2\rangle, \langle 2, 1\rangle, \langle 0, 1\rangle\} \end{array}$$

Struktuurit

$$M = (M, P_1, \ldots, P_n, f_1, \ldots, f_m, c_1, \ldots, c_k)$$

ja

$$M' = (M', P'_1, \ldots, P'_n, f'_1, \ldots, f'_m, c'_1, \ldots, c'_k)$$

ovat *isomorfiset*, jos on olemassa bijektio

$$\pi : M \to M'$$

siten, että

(1) $\langle a_1, \ldots, a_l\rangle \in P_i \iff \langle \pi(a_1), \ldots, \pi(a_l)\rangle \in P'_i$, kun $1 \leq i \leq n$

(2) $f'_i(\pi(a_1), \ldots, \pi(a_l)) = \pi(f_i(a_1, \ldots, a_l))$, kun $1 \leq i \leq m$

(3) $\pi(c_i) = c'_i$, kun $1 \leq i \leq k$.

Tällöin sanotaan että π on *isomorfismi* $M \to M'$

$$\pi : M \cong M'.$$

Jos lisäksi $M = M'$, niin sanotaan, että π on struktuurin M **automorfismi**.

Isomorfismin määritelmä näyttää mutkikkaalta mutta yksinkertaistuu, jos struktuureissa on vain vähän relaatioita ja funktioita.

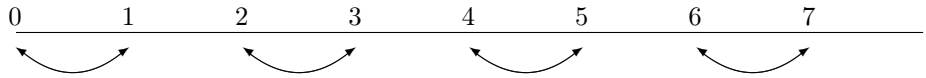
Esimerkki 3.4 *Tarkastellaan monadisia struktuureita*

$$\begin{aligned} M &= (\mathbb{N}, \{1, 3, 5, 7, \ldots\}) \\ M' &= (\mathbb{N}, \{0, 2, 4, 6, \ldots\}) \end{aligned}$$

Osoitamme että funktio $\pi : \mathbb{N} \to \mathbb{N}$*,*

$$\pi(n) = \begin{cases} 2k+1 & \text{jos } n = 2k \\ 2k & \text{jos } n = 2k+1 \end{cases}$$

on isomorfismi $M \to M'$*.*



π *on selvästi bijektio* $\mathbb{N} \to \mathbb{N}$*. Toisaalta* n *on pariton jos ja vain jos* $\pi(n)$ *on parillinen. Siis* π *on isomorfismi. Yleisemmin jos*

$$\begin{aligned} M &= (M, P), \quad & P &\subseteq M \\ M' &= (M', P'), \quad & P' &\subseteq M' \end{aligned}$$

niin bijektio $\pi : M \to M'$ *on ismorfismi, joss*

$$a \in P \iff \pi(a) \in P'$$

eli π*:n täytyy kuvata* P P'*:lle ja* $M \setminus P$ *joukolle* $M' \setminus P'$*. Jos* M *ja* M' *ovat äärellisiä, niin* $M \cong M'$ *jos ja vain jos* P*:ssä ja* P'*:ssä on yhtä monta alkiota.*

Esimerkki 3.5 *Järjestämättömät binäärijonot ovat isomorfiset jos niissä on sama määrä nollia ja sama määrä ykkösiä kummassakin.*

Vastaavasti kaksi binääristä taulukkoa (ks. Esim. 3.2) virittävät isomorfiset struktuurit jos niissä on sama määrä kunkin tyyppisiä rivejä:

Op.	*K1*	*K2*	*K3*		*Op.*	*K1*	*K2*	*K3*
0	*1*	*0*	*0*		*0*	*0*	*0*	*1*
1	*0*	*0*	*1*		*1*	*1*	*0*	*0*
2	*0*	*1*	*1*		*2*	*0*	*1*	*1*
3	*1*	*0*	*1*		*3*	*1*	*1*	*1*
4	*1*	*1*	*1*		*4*	*0*	*1*	*0*
5	*0*	*1*	*0*		*5*	*1*	*0*	*1*
6	*0*	*0*	*0*		*6*	*0*	*0*	*0*
7	*0*	*0*	*0*		*7*	*1*	*0*	*0*
8	*1*	*0*	*0*		*8*	*0*	*0*	*0*

Kaksi erilaista mutta isomorfista struktuuria voi syntyä esimerkiksi siten, että opettaja sotkee vahingossa rivien järjestyksen ja joutuu numeroimaan oppilaat uudelleen.

Esimerkki 3.6 *Järjestetyt joukot*

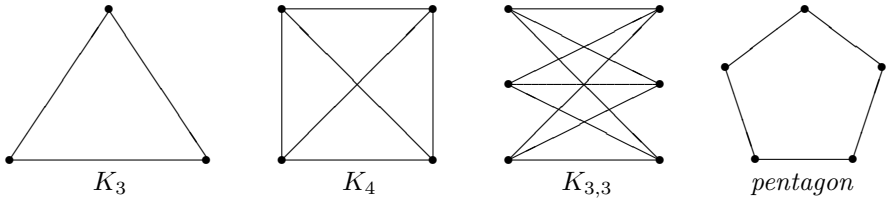
$$M = ((-\tfrac{\pi}{2}, \tfrac{\pi}{2}), <)$$
$$M' = (\mathbb{R}, <)$$

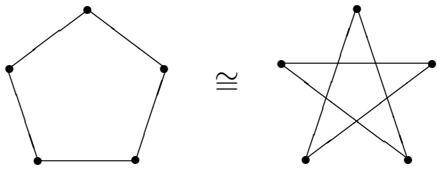
ovat isomorfiset, kuten kuvaus $x \mapsto \tan(x)$ *osoittaa. Sen sijaan*

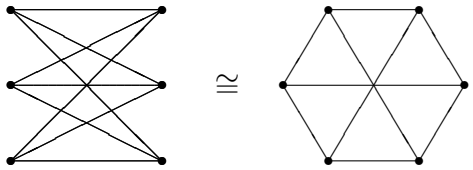
$$([-\frac{\pi}{2}, \frac{\pi}{2}], <) \ncong (\mathbb{R}, <),$$

kuten on helppo havaita pohtimalla minne isomorfismi kuvaisi reunapisteet $-\frac{\pi}{2}$ *ja* $\frac{\pi}{2}$.

Esimerkki 3.7 *Struktuuri* (M, R) *on* verkko, *jos* $R \subseteq M^2$ *on symmetrinen ja irrefleksiivinen. Esimerkkejä verkoista:*







Voidaksemme todistaa asioita struktuureista, meidän on sovittava yleispätevästä merkintätavasta struktuureille. Tätä varten otamme käyttöön aakkoston käsitteen. Aakkosto kertoo struktuurin "tyypin".

Aakkosto on joukko L relaatio–, funktio–, ja vakiosymboleita. Relaatio– ja funktiosymboleihin liittyy niin sanottu *paikkafunktio* $\#_L$. Ei ole merkitystä sillä, mitä symboleita käytettään. Yleensä relaatiosymboleita merkitään kirjaimella R, funktiosymboleita kirjaimella f, ja vakiosymboleita kirjaimella c. Relaatiosymbolia $\mathrm{R} \in L$ sanotaan $\#_L(\mathrm{R})$–paikkaiseksi relaatiosymboliksi. Funktiosymbolia $\mathrm{f} \in L$ sanotaan $\#_L(\mathrm{f})$–paikkaiseksi.

Määritelmä 3.8 *Jos L on aakkosto, niin L–struktuuri on pari*

$$M = \langle M, Tul_M \rangle$$

missä M on epätyhjä joukko, ja Tul_M on funktio siten, että

(1) $\mathrm{dom}(Tul_M) = L$

(2) $\mathrm{R} \in L \Longrightarrow Tul_M(\mathrm{R}) \subseteq M^{\#_L(\mathrm{R})}$

(3) $\mathrm{f} \in L \Longrightarrow Tul_M(\mathrm{f}) : M^{\#_L(\mathrm{f})} \to M$

(2) $\mathrm{c} \in L \Longrightarrow Tul_M(\mathrm{c}) \in M$.

Tarkastellaan esimerkiksi struktuuria

$$M = (M, P_1, \ldots, P_n, f_1, \ldots, f_m, c_1, \ldots, c_k).$$

Tehdään aakkosto

$$L = \{\mathrm{R}_1, \ldots, \mathrm{R}_n, \mathrm{f}_1, \ldots, \mathrm{f}_m, \mathrm{c}_1, \ldots, \mathrm{c}_k\},$$

missä $\#_L(\mathrm{R}_i)$ ja $\#_L(\mathrm{f}_i)$ noudattavat M:n paikkalukuja. Nyt M on L–struktuuri

$$\begin{array}{ll}
M = \langle M, Tul_M \rangle & \\
Tul_M(\mathrm{R}_i) = \{\langle a_1, \ldots, a_l \rangle \mid \langle a_1, \ldots, a_l \rangle \in P_i\} & (l = \#_L(\mathrm{R}_i)) \\
Tul_M(\mathrm{f}_i) : M^l \to M & (l = \#_L(\mathrm{f}_i)) \quad . \\
Tul_M(\mathrm{f}_i)(a_1, \ldots, a_l) = f_i(a_1, \ldots, a_l) & \\
Tul_M(\mathrm{c}_i) = M\text{:n alkio } c_i &
\end{array}$$

L–struktuurin M *redukti* aakkostoon $L' \subseteq L$ on L'–struktuuri

$$M\restriction L' = \langle M, Tul_M \restriction L' \rangle.$$

Tällöin M on $M'\restriction L'$:n *ekspansio* aakkostoon L. Esimerkiksi (M, R_1, R_2, f):n redukteja ovat (M, R_1), (M, R_2), (M, f), (M, R_1, f), (M, R_2, f),(M, R_1, R_2) ja (M), eli tyhjän aakkoston struktuuri. Yhteensä 8 reduktia, jos alkuperäinen struktuuri lasketaan mukaan

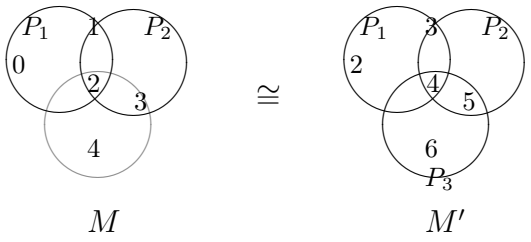
Esimerkki 3.9 *Monadisella struktuurilla*

$$M = (\mathbb{N}, \{0, 1, 2\}, \{1, 2, 3\}), L = \{\mathrm{P}_1, \mathrm{P}_2\}$$

on ekspansio joka on ismorfinen struktuurin

$$M' = (\mathbb{N}, \{2, 3, 4\}, \{3, 4, 5\}, \{4, 5, 6\}), L = \{\mathrm{P}_1, \mathrm{P}_2, \mathrm{P}_3\}$$

kanssa.



Lisäämme struktuuriin M relaation (osajoukon) $2, 3, 4$ ja tämän jälkeen funktio

$$\pi(n) = \begin{cases} n+2 & jos\ n \leq 4 \\ 0 & jos\ n = 5 \\ 1 & jos\ n = 6 \\ n & jos\ n > 6 \end{cases}$$

on isomorfismi M:n ekspansion ja M':n välillä.

Esimerkki 3.10 *Olkoon*

$$L = \{\mathrm{P}, \mathrm{S}, \mathrm{L}\}$$

*(*P*="piste", *S*="suora", *L*="leikkaa"). Tämä aakkosto soveltuu geometrian tutkimiseen. Karteesinen tasogeometria muodostaa L–struktuurin*

$$M = (P \cup S, P, S, L)$$

missä

$$\begin{array}{rcl} P & = & \text{tason } \mathbb{R}^2 \text{ pisteiden joukko} \\ S & = & \text{tason } \mathbb{R}^2 \text{ suorien joukko} \\ L & = & \{\langle p, s\rangle \subseteq P \times S | \text{ piste } p \text{ on suoralla } s\}. \end{array}$$

Niin sanotut epäeuklidiset geometriat ovat hyvin paljon mallin M kaltaisia, mutta eivät isomorfisia. M:n kanssa ei–isomorfinen geometria saadaan myös jos lähdetään $\mathbb{R}^2$:n sijasta avaruudesta $\mathbb{R}^n$, $n > 2$.

Esimerkki 3.11 *Olkoon*

$$L = \{\mathrm{P}, \mathrm{J}, \varepsilon, \}$$

*(*A*="alkio", *J*="joukko"). Jos A on joukko, saamme L–struktuurin*

$$\begin{array}{rcl} M & = & (A \cup \mathcal{P}(A), A, J, \varepsilon) \\ J & = & \mathcal{P}(A) \\ \varepsilon & = & \{\langle x, y\rangle | x \in P, y \in J, x \in y\}. \end{array}$$

4 Predikaattilogiikka

Predikaattilogiikka on matemaattinen väline struktuurien ominaisuuksien tutkimiseen. Osoittautuu, että ominaisuuksilla jotka ovat ilmaistavissa predikaattilogiikassa, on tärkeitä yhteisiä ominaisuuksia. Predikaattilogiikkaa voi ajatella ohjelmointikielenä, jonka avulla voi kysyä struktuurien ominaisuuksia.

Kuten ohjelmointikieltenkin kohdalla, predikaattilogiikan määritelmä on moniosainen ja laaja. Predikaattilogiikan ytimen muodostavat tietyt ns. loogiset symbolit, joiden käyttöön kaikki muu perustuu.

Loogisia symboleja ovat:

muuttujasymbolit	$v_0, v_1, \ldots$
konnektiivit	$\neg, \rightarrow$
kvanttori	$\forall$
sulkumerkit	$(,)$

Jos L on aakkosto, niin **L-termit** määritellään seuraavalla induktiivisella määritelmällä.

(1) Pelkkä muuttujasymboli v_n on L-termi.

(2) Pelkkä vakiosymboli c $\in L$ on L-termi.

(3) Jos f $\in L, \#_L(\mathrm{f}) = n$ ja $t_1, \ldots, t_n$ ovat L-termejä, niin f$t_1 \ldots t_n$ on L-termi.

Jos aakkosto L ei sisällä funktiosymboleita, niin L-termejä ovat vain muuttujat ja mahdolliset vakiosymbolit. Ehto (3) sen sijaan tuo runsaasti mitä mutkikkaimpia L-termejä.

Esimerkki 4.1 *Tarkastellaan struktuurin (ryhmän)*

$$\mathbf{Z} = (\mathbf{Z}, +, 0)$$

aakkostoa $L = \{+, 0\}$. *(Symbolit* $+$ *ja* 0 *ovat nyt siis kahdessa roolissa, toisaalta funktiosymboli ja vakiosymboli, toisaalta funktio ja vakio) L-termejä ovat:*

0
$v_0, v_1, v_2, \ldots$
$+t_0t_1$ *(esim.* $+00, +v_0v_1$*)*
$++t_0t_1t_2$
$+++t_0t_1t_2t_3$
jne.

Oleellisesti L-termit ovat muuttujien summalausekkeita.

Esimerkki 4.2 *Tarkastellaan struktuurin (kunnan)* $\mathbf{R} = (\mathbf{R}, +, \cdot, 0, 1)$ *aakkostoa*
$L = \{+, \cdot, 0, 1\}$. *L-termejä ovat:*

0
1
$v_0, v_1, v_2, \ldots$
$+t_0t_1$, $\cdot t_0t_1$
$++t_0t_1{\cdot}t_2t_3, \cdot{+}t_0t_1{+}t_2t_3$
$\cdot\cdot t_0t_1{\cdot}t_2t_3$
jne.

Oleellisesti kyse on polynomeista. Voidaan sanoa, että termit ovat polynomien yleistyksiä.

Termien arvoja lasketaan aivan kuten polynomien arvoja. Valitaan muuttujille arvot ja sitten suoritetaan merkityt laskutoimitukset.

Olkoon M L-struktuuri. M:n **tulkintojono** on mikä tahansa funktio

$$s : \mathbb{N} \to M.$$

L-termin t **arvo** M:ssä tulkintajonolla s,

$$t^M\langle s\rangle$$

määritellään seuraavasti:

$$\begin{array}{ll}
\text{Tapaus 1: } t = v_i, & t^M\langle s\rangle = s(i) \\
\text{Tapaus 2: } t = \mathrm{c}, & t^M\langle s\rangle = Tul_M(c) \\
\text{Tapaus 3: } t = \mathrm{f}_i t_1 \dots t_n, & t^M\langle s\rangle = Tul_M(\mathrm{f}_i)(t_1^M\langle s\rangle, \dots, t_n^M\langle s\rangle).
\end{array}$$

Termin arvon laskeminen on yleistys polynomin arvon laskemisesta annetuilla muuttujien arvoilla.

$$\begin{aligned}
\mathbf{Z} &= (\mathbf{Z}, +, 0) \\
(++v_0v_1v_2)^{\mathbf{Z}}\langle s\rangle &= (+v_0v_1)^{\mathbf{Z}}\langle s\rangle + v_2^{\mathbf{Z}}\langle s\rangle \\
&= v_0^{\mathbf{Z}}\langle s\rangle + v_1^{\mathbf{Z}}\langle s\rangle + v_2^{\mathbf{Z}}\langle s\rangle \\
&= s(0) + s(1) + s(2) \\
\mathbf{R} &= (\mathbf{R}, +, \cdot, 0, 1) \\
(\cdot+v_0v_1v_2)^{\mathbf{R}}\langle s\rangle &= (+v_0v_1)^{\mathbf{R}}\langle s\rangle \cdot v_2^{\mathbf{R}}\langle s\rangle \\
&= (v_0^{\mathbf{R}}\langle s\rangle + v_1^{\mathbf{R}}\langle s\rangle) \cdot v_2^{\mathbf{R}}\langle s\rangle \\
&= (s(0) + s(1)) \cdot s(2)
\end{aligned}$$

Lemma 4.3 *Olkoot M ja M' L-struktuureja ja $\pi : M \cong M'$. Olkoon $s : \mathbb{N} \to M$ ja $s' : \mathbb{N} \to M'$ siten että kaikilla $n \in \mathbb{N}$*

$$s'(n) = \pi(s(n)).$$

Tällöin kaikille L-termeille t pätee

$$t^{M'}\langle s'\rangle = \pi(t^M\langle s\rangle).$$

Tod. *Harjoitustehtävä.* □

Eräs matematiikan hyödillisimmistä käsitteistä on yhtälön käsite. Uusia ja uusia menetelmiä kehitetään yhtälön ratkaisemiseksi. Yhtälön käsite on keskeinen myös logiikassa, vaikka loogikot eivät kehitäkään menetelmiä niiden ratkaisemiseksi. Logiikassa yhtälöt edustavat alkeellisinta muuttujien ja vakioiden välistä riippuvuutta. Siksi yhtälöitä kutsutaan logiikassa atomikaavoiksi.

Jos L on aakkosto ja t_1 ja t_2 ovat L-termejä, niin

$$\approx t_1 t_2$$

on **L-yhtälö**. Esimerkkejä L-yhtälöistä ovat:

$$\begin{array}{ll} \approx v_0 v_1 & \\ \approx +v_0 c v_0 & \#_L(+) = 2 \\ \approx \cdot v_0 v_1 + v_2 v_3 & \#_L(+) = \#_L(\cdot) = 2 \\ \approx \mathrm{f}\mathrm{f}\mathrm{f} v_0 v_1 & \#_L(\mathrm{f}) = 1. \end{array}$$

L-yhtälö $\approx t_1 t_2$ luetaan siten että $\approx$-merkin jälkeen etsitään suppein termi t_1 ja loput muodostavat termin t_2. Siispä

$$\approx v_0 v_1 v_2$$

ei ole L-yhtälö ja $\approx \mathrm{f}\mathrm{f} v_0 v_1 v_2 v_3$ on L-yhtälö vain jos $\#_L(\mathrm{f}) = 2$.

Tyypillinen tehtävä matematiikassa on annetun yhtälön ratkaisujoukon määrääminen. Vastaavasti L-yhtälölle voidaan määritellä niiden tulkintajonojen joukko, jotka "toteuttavat" sen.

Olkoon L aakkosto, M L-struktuuri ja $\approx t_1 t_2$ L-yhtälö. Määritellään

$$Tul_M(\approx t_1 t_2) = \{s | t_1^M \langle s \rangle = t_2^M \langle s \rangle\}.$$

Tämä joukko muodostuu siis kaikista tulkintojonoista s, jotka antavat saman arvon t_1:lle ja t_2:lle, aivan kuten algebrassa yhtälön $x^2 + 2x + 1 = y^3$ ratkaisujoukko muodostuu kaikista pareista $\langle a, b \rangle$, joille yhtälö $a^2 + 2a + 1 = b^3$ pätee (esimerkiksi kokonaislukujen joukossa).

Esimerkkejä:

$$Tul_M(\approx v_0v_1) = \{s|s(0) = s(1)\}$$
$$Tul_M(\approx v_0\mathrm{c}) = \{s|s(0) = \mathrm{c}^M\}$$
$$Tul_{\mathbf{Z}}(\approx +v_0v_1v_2) = \{s|s(0) + s(1) = s(2)\}$$
$$Tul_{\mathbf{R}}(\approx \cdot v_0v_0v_2) = \{s|s(0)^2 = s(1)\}.$$

Jos $P(x)$ on x:n polynomi, on helppo kirjoittaa termi t, jossa x:ää on merkitty v_0:lla, siten että

$$Tul_{\mathbf{R}}(\approx tv_1) = \{s|P(s(0)) = s(1)\}.$$

Jos merkitään

$$^{\mathbb{N}}M = \{s|s : \mathbb{N} \to M\}$$

niin aina $Tul_M(\approx t_1t_2) \subseteq {}^{\mathbb{N}}M$. Mitä suurempi joukko $Tul_M(\approx t_1t_2)$ on, sitä enemmän yhtälöllä $\approx t_1t_2$ on ratkaisuja. Varsin yleisenä ääritapauksena esiintyy $Tul_M(\approx t_1t_2) = {}^{\mathbb{N}}M$, jolloin yhtälö toteutuu kaikilla muuttujien arvoilla, eli ilmaisee eräänlaisen yleisen lainalaisuuden, kuten $x + 1 = 1 + x$ kokonaislukujen ryhmässä ja $(x + y)^2 = x^2 + 2xy + y^2$ rationaalilukujen kunnassa. Voi olla myös $Tul_M(\approx t_1t_2) = \emptyset$, jolloin yhtälö ei toteudu millään muuttujien arvoilla, kuten $x + x = 1$ kokonaislukujen ryhmässä tai $x^2 = 2$ rationaalilukujen kunnassa.

Siirrymme nyt yhtälöistä mielivaltaisiin kaavoihin. Niillä voidaan ilmaista mutkikkaampia asiantiloja kuin pelkillä yhtälöillä. Kaavoilla voidaan ilmaista mm. yhtälöiden konjunktioita eli yhtälöryhmiä ja yhtälöiden kieltoja eli epäyhtälöitä.

Määritelmä 4.4 *Olkoon L aakkosto. L-***kaavojen** *joukko määritellään seuraavasti:*

1. *Jos t_1 ja t_2 ovat L-termejä, niin $\approx t_1t_2$ on L-kaava.*
2. *Jos $\mathrm{R} \in L$, $\#_L(\mathrm{R}) = n$ ja $t_1, \ldots, t_n$ ovat L-termejä, niin $\mathrm{R}t_1 \ldots t_n$ on L-kaava.*
3. *Jos φ ja ψ ovat L-kaavoja ja $n \in \mathbb{N}$ niin $\neg\varphi, (\varphi \to \psi)$ ja $\forall v_n\varphi$ ovat L-kaavoja.*

Kohtien 1 ja 2 määrittelemiä kaavoja kutsutaan **atomikaavoiksi**. Käytämme seuraavia lyhenteitä:

$$\begin{array}{rcll} (\varphi \vee \psi) & = & (\neg\varphi \to \psi) & \text{(disjunktio)} \\ (\varphi \wedge \psi) & = & \neg(\varphi \to \neg\psi) & \text{(konjunktio)} \\ (\varphi \leftrightarrow \psi) & = & \neg((\varphi \to \psi) \to \neg(\psi \to \varphi)) & \text{(ekvivalenssi)} \\ \exists v_n\varphi & = & \neg\forall v_n\neg\varphi. & \end{array}$$

Yhtälön ratkaisujoukon käsite yleistyy kaikille kaavoille. Mihin tahansa L-kaavaan φ voidaan luonnollisella tavalla liittää ratkaisujoukko $Tul_M(\varphi)$. Tätä yleistystä varten sovimme seuraavasta merkinnästä: Jos $s : \mathbb{N} \to M, n \in \mathbb{N}$ ja $a \in M$, niin tulkintajono

$$s(a/n) \in {}^{\mathbb{N}}M$$

määritellään seuraavasti:

$$s(a/n)(i) = \begin{cases} a \; jos \; i = n \\ s(i) \; jos \; i \neq n. \end{cases}$$

Tulkintajono $s(a/m)$ on siis täsmälleen sama tukintajono kuin s paitsi että $s(m)$:n arvo on muutettu $s(a/m)$:ssä a:ksi. Siis $s(a/m)(m) = a$ ja muilla i:n arvoilla $s(a/m)(i) = s(i)$.

Jos $\mathcal{X} \subseteq {}^{\mathbb{N}}M$, olkoon

$$A_n(\mathcal{X}) = \{s | s(a/n) \in \mathcal{X} \text{ kaikilla } \; a \in M\}.$$

Siis

$$s \in A_n(\mathcal{X}) \leftrightarrow kaikilla \; a \in M : s(a/n) \in \mathcal{X}.$$

Tätä operaatiota käytetään nyt kvanttoreiden semantiikan täsmälliseen käsittelyyn. Seuraavaa määritelmää kutsutaan **Tarskin totuusmääritelmäksi**:

Määritelmä 4.5 *Jos L on aakkosto, φ on L-kaava ja M on L-struktuuri, niin*

$$Tul_M(\varphi)$$

määritellään seuraavasti:

1. $Tul_M(\approx t_1 t_2) = \{s | t_1^M\langle s\rangle = t_2^M\langle s\rangle\}$
2. $Tul_M(\mathrm{R}t_1 \ldots t_n) = \{s | \langle t_1^M\langle s\rangle, \ldots, t_n^M\langle s\rangle\rangle \in Tul_M(R)\}$

3. $Tul_M(\neg\varphi) = {}^{\mathbb{N}}M \setminus Tul_M(\varphi)$

4. $Tul_M((\varphi \to \psi)) = ({}^{\mathbb{N}}M \setminus Tul_M(\varphi)) \cup Tul_M(\psi)$

5. $Tul_M(\forall v_n\varphi) = A_n(Tul_M(\varphi))$.

$Tul_M(\varphi)$ on kaavan φ ***tulkinta*** *L-struktuurissa M. Sanomme, että* ***s toteuttaa*** *$\varphi : n$ M:ssä,*

$$M \models_s \varphi,$$

jos $s \in Tul_M(\varphi)$. Sanomme, että M ***toteuttaa*** *$\varphi : n$,*

$$M \models \varphi,$$

jos $Tul_M(\varphi) = {}^{\mathbb{N}}M$, joilloin sanomme myös että φ ***on tosi*** *M****:ssä*** *ja M on $\varphi : n$* ***malli****.*

Kaavan φ tulkinta struktuurissa M on siis eräs joukko tukintajonoja, nimittäin niiden tulkintajonojen joukko, jotka toteuttavat kaavan φ. Mitä suurempi $s \in Tul_M(\varphi)$ on sitä useampi tulkintajono toteuttaa kaavan φ. Toisaalta voi olla, että mikään s ei toteuta kaavaa φ.

Esimerkki 4.6 *1º $Tul_M((\varphi \wedge \psi)) = Tul_M(\varphi) \cap Tul_M(\psi)$.*
2º $Tul_M(\exists v_n\varphi) = \{s | s(a/n) \in Tul_M(\varphi)$ jollakin $a \in M\}$.
Tod. *Harjoitustehtävä.* □

Esimerkki 4.7 *Olkoon $\mathbf{R} = (\mathbf{R}, +, \cdot, 0, 1)$. Nyt $s \in Tul_{\mathbf{R}}(\exists v_0 \approx {+}{+}{\cdot}v_0v_0{\cdot}v_1v_0v_20)$ joss on olemassa $x \in \mathbf{R}$ siten että $s(x/0) \in Tul_M(\approx {+}{+} \cdot v_0v_0{\cdot}v_1v_0v_20)$ eli on olemassa $x \in \mathbf{R}$ siten että $x^2 + s(1) \cdot x + s(2) = 0$ eli yhtälöllä $x^2 + s(1) \cdot x + s(2) = 0$ on reaalinen ratkaisu.*

Esimerkki 4.8 *$L = \{\mathrm{f}\}, \#_L(\mathrm{f}) = 1, M = (M, f)$. Nyt f on injektio $M \to M$ joss*

$$Tul_M(\forall v_0\forall v_1(\approx \mathrm{f}v_0\mathrm{f}v_1 \to \approx v_0v_1)) = {}^{\mathbb{N}}M$$

ja f on surjektio $M \to M$ joss

$$Tul_M(\forall v_0\exists v_1 \approx \mathrm{f}v_1v_0) = {}^{\mathbb{N}}M.$$

Esimerkki 4.9 *Olkoon $L = \{+, 0\}$ ja $\mathbf{Z} = (\mathbf{Z}, +, 0)$. L-struktuuri $\mathbf{Z}$ on seuraavien L-kaavojen malli:*

1. $\approx +v_0+v_1v_2+{+}v_0v_1v_2$
2. $\approx +v_00v_0, \approx +0v_0v_0$
3. $\exists v_1(\approx +v_0v_10 \wedge \approx +v_1v_00)$.

Nämä ns. **ryhmäaksioomat** kirjoitetaan matematiikassa yleensä tutummalla merintätavalla:

$$x + (y + z) = (x + y) + z$$
$$x + 0 = x, 0 + x = x$$
$$\exists y(x + y = y + x = 0)$$

Algebrassa mitä tahansa L-struktuuria, joka toteuttaa ryhmäaksiomat 1-3 sanotaan **ryhmäksi**. Eräs viimeaikojen suuria tuloksia matematiikassa oli äärellisten ryhmien täydellinen luokittelu.

Esimerkki 4.10 *Lukuteoriassa tutkitaan luonnollisten lukujen* $0, 1, 2, 3, 4, \ldots$ *jaollisuus- ym. aritmeettisia ominaisuuksia. Lukuteorian* ***standardimalli*** *on*

$$\mathbb{N} = (\mathbb{N}, +, \cdot, 0, 1)$$

Monet luonnollisten lukujen ominaisuuksista ovat predikaattilogiikassa "määriteltävissä":

$s(0)$	*parillinen joss*	$\mathbb{N} \models_s \exists v_1 \approx \cdot{+}11v_1v_0$
$s(0)$	*alkuluku joss*	$\mathbb{N} \models_s \neg\exists v_1\exists v_2((\approx \cdot v_1v_2v_0 \wedge \neg \approx v_1v_0) \wedge \neg \approx v_11)$
$s(0)$	*neliö joss*	$\mathbb{N} \models_s \exists v_1 \approx \cdot v_1v_1v_0$.

Määritelmä 4.11 *L-kaava* ψ *on L-kaavan* φ ***looginen seuraus****,* $\varphi \models \psi$*, jos kaikille L-struktuureille M ja kaikille* $s : \mathbb{N} \to M$ *pätee:*

$$\textit{Jos } M \models_s \varphi \textit{ niin } M \models_s \psi.$$

Looginen seuraus $\varphi \models \psi$ tarkoittaa, että valittiinpa minkälainen struktuuri tahansa ja minkälainen tulkintajono muuttujien tulkitsemiseksi tahansa, niin jos φ toteutuu, myös ψ toteutuu. Tämä seuraussuhde on "loogista" siinä mielessä, että sillä, miten struktuuri ja tulkintajono valitaan ei ole mitään merkitystä eli ψ seuraa φ:stä pelkästään loogisen muotonsa perusteella. Esimerkiksi jos φ on konjunktio $(\psi \wedge \theta)$, niin tietenkin ψ seuraa φ:stä. Kvanttoreiden johdosta looginen seuraus voi kuitenkin olla äärimmäisen mutkikasta. Ei ole olemassa mitään yleistä mekaanista menetelmää sen ratkaisemiseksi seuraako annettu kaava loogisesti toisesta vai ei. Tämä on kuuluisa **Churchin lause**.

Esimerkki 4.12 $\neg\forall v_n\varphi \models \exists v_n\neg\varphi$.
Tod. *Oletetaan* $s \in Tul_M(\neg\forall v_n\varphi)$. *Siis* $s \notin A_n(Tul_M(\varphi))$. *Siis on olemassa* $a \in M$ *siten että* $s(a/n) \notin Tul_M(\varphi)$. *Siis* $M \models_s \exists v_n\neg\varphi$.
□

Esimerkki 4.13 $\forall v_0\exists v_1 \mathrm{R}v_0v_1 \not\models \exists v_0\forall v_1 \mathrm{R}v_0v_1$.
Tod. *Olkoon* $M = (\mathbb{N}, <)$ *ja* $s : \mathbb{N} \to \mathbb{N}$. $s(a/0)(a+1/1) \in Tul_M(\mathrm{R}v_0v_1)$ *joten* $s(a/0) \in Tul_M(\exists v_1 \mathrm{R}v_0v_1)$ *olipa* $a \in \mathbb{N}$ *mikä hyvänsä. Siis* $s \in Tul_M(\forall v_0\exists v_1 \mathrm{R}v_0v_1)$. *Toisaaalta jos* $s \in Tul_M(\exists v_0\forall v_1 \mathrm{R}v_0v_1)$ *niin on olemassa* $a \in \mathbb{N}$ *siten että* $s(a/0) \in A_1(Tul_M(\mathrm{R}v_0v_1))$. *Erityisesti* $s(a/0)(a/1) \in Tul_M(\mathrm{R}v_0v_1)$ *mikä on ristiriita. Siis* $s \notin Tul_M(\exists v_0\forall v_1 \mathrm{R}v_0v_1)$.
□

Esimerkki 4.14 $\exists v_0\forall v_1\varphi \models \forall v_1\exists v_0\varphi$.
Tod. *Olkoon* $M \models_s \exists v_0\forall v_1\varphi$. *Siis jollakin* $a \in M$ $M \models_{s(a/0)} \forall v_1\varphi$. *Nyt voimme todistaa* $M \models_s \forall v_1\exists v_0\varphi$. *Olkoon näet* $b \in M$ *mielivaltainen. Tiedämme että* $M \models_{s(a/0)(b/1)} \varphi$. *Mutta* $s(a/0)(b/1) = s(b/1)(a/0)$, *joten* $M \models_{s(b/1)} \exists v_0\varphi$. *Koska b oli mielivaltainen, pätee* $M \models_s \forall v_1\exists v_0\varphi$.
□

Esimerkki 4.15 $\forall v_0(\mathrm{P}v_0 \vee \mathrm{Q}v_0) \not\models (\forall v_0\mathrm{P}v_0 \vee \forall v_0\mathrm{Q}v_0)$.

Tod. *Olkoon* $M = (\{0,1\}, \{0\}, \{1\})$, *missä* $\{0\} = Tul_M(\mathrm{P})$ *ja* $\{1\} = Tul_M(\mathrm{Q})$. *Olkoon* $s : \mathbb{N} \to \{0,1\}$. *Jos* $a \in \{0,1\}$, *niin* $a = 0$ *tai* $a = 1$, *joten* $M \models_{s(a/0)} (\mathrm{P}v_0 \vee \mathrm{Q}v_0)$. *Toisaalta* $M \not\models_s \forall v_0\mathrm{P}v_0$, *koska* $M \not\models_{s(1/0)} \mathrm{P}v_0$. *Samoin* $M \not\models_s \forall v_0\mathrm{Q}v_0$. *Siis* $M \not\models_s (\forall v_0\mathrm{P}v_0 \vee \forall v_0\mathrm{Q}v_0)$
□

Määritelmä 4.16 *L-kaava* φ *on* ***validi****,* $\models \varphi$, *jos* $M \models_s \varphi$ *pätee kaikille L-struktuureille M ja kaikille* $s : \mathbb{N} \to M$. *Ekvivalentisti*

$$Tul_M(\varphi) = {}^{\mathbb{N}}M.$$

Validisuus on eräs loogisen seurauksen erikoistapaus. Validi kaava seuraa loogisesti mistä tahansa kaavasta, koska se on aina tosi. Validi kaava ilmaisee yleisen "loogisen maailman" totuuden, joka ei riipu struktuurista eikä muuttujien arvoista. Validi kaava on aina tosi pelkän muotonsa vuoksi. Esimerkiksi $(\varphi \to \varphi)$ on validi, jopa riippumatta siitä mikä φ on. Tästä

ei pidä vetää sitä johtopäätöstä, että validisuus olisi jotenkin triviaali ominaisuus. Edellämainitun Churchin lauseen nojalla näet validisuuttakaan ei voi tarkistaa mekaanisesti, joten kaikki validit kaavat eivät ole yhtä selviä tapauksia kuin $(\varphi \to \varphi)$. Implikaatio $(\varphi \to \psi)$ voi olla validi hyvin syvällisestä matemaattisesta syystä. Ajatellaanpa lukuteoriaa. Nyt φ olla äärellinen konjunktio parhaista tunnetuista lukuteorian aksioomeista, jolloin kysymys kaavan $(\varphi \to \psi)$ validisuudesta on käytännössä (joskaan ei teoriassa) yhtä vaikea ratkaista kuin kysymys, onko ψ tosi lukuteorian standardimallissa.

Esimerkki 4.17 *1.* $\varphi \models \psi$ *joss* $\models (\varphi \to \psi)$

2. $\varphi \models (\psi \wedge \neg\psi)$ *joss* φ*:llä ei ole malleja joss* $\varphi \models \psi$ *kaikille* ψ*.*

Tod. *Harj. teht.* □

5 Kaavojen ominaisuuksia

Muuttuja v_0 esiintyy seuraavissa kahdessa kaavassa

$$\mathrm{R}v_0v_1 \tag{1}$$

$$\forall v_0 \mathrm{R}v_0v_1 \tag{2}$$

Ero johon kiinnitämme huomion on siinä, että kaavan (1) totuus riippuu v_0:n tulkinnasta, kun taas kaavan (2) totuus ei riipu. Vertaa lausekkeisiin

$$x^2 + y - 5 \tag{3}$$

$$\int_0^1 x^2 dx + y \tag{4}$$

Lausekkeen (3) arvo riippuu x:n arvosta, mutta lausekkeen (4) arvo ei. Sanomme että v_0 esiintyy (1):ssä vapaana, mutta (2):ssa sidottuna. Tarkempi määritelmä seuraa.

Kaavan **alikaava** on sen osa, joka itsekin on kaava. Tämä käsite voidaan määritellä induktiivisesti seuraavasti.

1. Atomikaavan alikaavoja ovat vain kaava itse.

2. Kaavan $\neg\varphi$ alikaavoja ovat $\neg\varphi$ ja φ:n alikaavat.

3. Kaavan $(\varphi \to \psi)$ alikaavoja ovat $(\varphi \to \psi)$, φ:n alikaavat ja ψ:n alikaavat.

4. Kaavan $\forall v_n \varphi$ alikaavoja ovat $\forall v_n \varphi$ sekä φ:n alikaavat.

Muuttujan v_n esiintymä kaavassa on **sidottu** jos se osuu muotoa $\forall v_n \psi$ olevaan alikaavaan. Muuten esiintymä on **vapaa**. Induktiivinen määritelmä samalle asialle:

1. Atomikaavassa muuttujat esiintyvät aina vapaana.

2. $\neg\varphi$:ssä on samat sidotut esiintymät kuin φ:ssä.

3. $(\varphi \to \psi)$:ssä muuttujan esiintymä on sidottu jos se on sidottu esiintymä φ:ssä tai sidottu esiintymä ψ:ssä.

4. $\forall v_n \varphi$:ssä muuttujan v_m esiintymä on sidottu, jos se on sidottu esiintymä φ:ssä tai jos $n = m$.

Esimerkki 5.1
$$\begin{array}{lll} (\underset{s}{\forall v_0} \mathrm{R} \underset{s}{v_0} \underset{s}{v_1} \to \underset{s}{\forall v_1} \mathrm{R} \underset{s}{v_1} \underset{v}{v_0}), & s = & \textit{sidottu esiintymä} \\ \underset{s}{\forall v_0} (\mathrm{R} \underset{s}{v_0} \underset{v}{v_1} \to \underset{s}{\forall v_1} \mathrm{R} \underset{s}{v_1} \underset{s}{v_0}), & v = & \textit{vapaa esiintymä} \end{array}$$

Seuraava lause osoittaa, että kaavan φ toteutuvuus annetulla tulkintajonolla s riippuu funktion s arvoista $s(n)$ vain sellaisilla argumentin n arvoilla, joilla v_n esiintyy *vapaana* kaavassa φ. Aivan erityisesti toteutuvuus riippuu vain niistä arvoista $s(n)$, joilla v_n ylipäätään esiintyy φ:ssä. Nämä tulokset eivät tietenkään ole yllättäviä eivätkä mitenkään syvällisiä kaavojen ominaisuuksia. Mielenkiintoista on oikeastaan vain se, miten tällainen seikka *todistetaan*. Todistus on logiikalle tyypillinen induktiotodistus.

Lause 5.2 *Olkoon L aakkosto, φ L-kaava ja M L-struktuuri. Olkoot s ja s' M:n tulkintajonoja siten että*

$$s(n) = s'(n)$$

jos v_n esiintyy vapaana φ:ssä. Tällöin

$$M \models_s \varphi \iff M \models_{s'} \varphi.$$

Tod. Olkoon $\mathcal{E}$ niiden L-kaavojen φ joukko, joille väite pätee. Osoitamme nyt

1. L-atomikaavat ovat $\mathcal{E}$:ssä
2. $\varphi \in \mathcal{E} \Longrightarrow \neg\varphi \in \mathcal{E}$
3. $\varphi, \psi \in \mathcal{E} \Longrightarrow (\varphi \to \psi) \in \mathcal{E}$
4. $\varphi \in \mathcal{E}, n \in \mathbb{N} \Longrightarrow \forall v_n \varphi \in \mathcal{E}$

Näistä ehdoista seuraa, että väite pätee kaikille L-kaavoille.

1. (a) $\approx t_1 t_2 \in \mathcal{E}$. Helposti nähdään (Vaatii oman pienen induktiotodistuksensa) että $t_i^M\langle s\rangle = t_i^M\langle s'\rangle$. Siis

$$\begin{aligned} M \models_s \approx t_1 t_2 &\iff t_1^M\langle s\rangle = t_2^M\langle s\rangle \\ &\iff t_1^M\langle s'\rangle = t_2^M\langle s'\rangle \\ &\iff M \models_{s'} \approx t_1 t_2 \end{aligned}$$

   (b) $\mathrm{R}t_1 \dots t_n \in \mathcal{E}$:

$$\begin{aligned} M \models_s \mathrm{R}t_1, \dots, t_n &\iff \langle t_1^M\langle s\rangle, \dots, t_n^M\langle s\rangle\rangle \in Tul_M(\mathrm{R}) \\ &\underset{\text{kuten ed.}}{\iff} \langle t_1^M\langle s'\rangle, \dots, t_n^M\langle s'\rangle\rangle \in Tul_M(\mathrm{R}) \\ &\iff M \models_{s'} \mathrm{R}t_1 \dots t_n. \end{aligned}$$

2. Oletetaan $\varphi \in \mathcal{E}$. Nyt

$$\begin{aligned} M \models_s \neg\varphi &\iff M \not\models_s \varphi \underset{ind.ol.}{\iff} M \not\models_{s'} \varphi \\ &\iff M \models_{s'} \neg\varphi. \end{aligned}$$

3. Oletetaan $\varphi, \psi \in \mathcal{E}$. Kuten yllä, $(\varphi \to \psi) \in \mathcal{E}$.
4. Oletetaan $\varphi \in \mathcal{E}$ ja $n \in \mathbb{N}$. Osoitamme, että $\forall v_n \varphi \in \mathcal{E}$. Olkoon sitä varten $s : \mathbb{N} \to M$ ja $s' : \mathbb{N} \to M$ s.e. $s(i) = s'(i)$ kun v_i esiintyy vapaana $\forall v_n\varphi$:ssä.

$$\begin{aligned} M \models_s \forall v_n \varphi &\iff \text{kaikilla } a \in M : M \models_{s(a/n)} \varphi \\ &\underset{1}{\iff} \text{kaikilla } a \in M : M \models_{s'(a/n)} \varphi \\ &\iff M \models_{s'} \forall v_n \varphi. \end{aligned}$$

□

Määritelmä 5.3 *L-kaava on* **L-lause***, jos siinä ei esiinny mikään muuttuja vapaana.*

Yleensä $M \models \varphi$ tarkoittaa, että $M \models_s \varphi$ kaikilla $s : \mathbb{N} \to M$. Jos φ on L-lause, niin edellisen lauseen nojalla $M \models_s \varphi$ kaikilla $s : \mathbb{N} \to M$ jos ja vain jos $M \models_s \varphi$ jollakin $s : \mathbb{N} \to M$. Lauseen totuus mallissa on siis riippumaton tulkintajonosta.

Seuraava tärkeä ja laajasti sovellettu perustavanlainen lause osoittaa, että isomorfia säilyttää totuuden. Se osoittaa, että logiikan välinein ei voi erottaa toisistaan kahta isomorfista struktuuria. Näin täytyykin olla. Isomorfisilla struktuureilla on sama "rakenne" ja logiikka käyttää struktuureita nimen omaan esimerkkeinä "rakenteista". Siksi on tärkeää, että logiikan kaavat ovat yhtä mieltä isomorfisista struktuureista.

Lause 5.4 ("Isomorfia säilyttää totuuden") *Olkoot M ja M' L-struktuureita ja $\pi : M \to M'$ isomorfismi. Tällöin kaikille L-kaavoille φ ja tulkintajonoille $s \in {}^{\mathbb{N}}M$ pätee*

$$M \models_s \varphi \iff M' \models_{\pi \circ s} \varphi.$$

Todistus Olkoon $\mathcal{E}$ niiden kaavojen φ joukko, joille pätee: "Kaikille $s \in {}^{\mathbb{N}}M$: $M \models_s \varphi \iff M' \models_{\pi \circ s} \varphi$". Todistamme induktiolla, että kaikki kaavat ovat $\mathcal{E}$:ssä.

1. $\approx t_1 t_2 \in \mathcal{E}$, sillä:

$$\begin{aligned} M \models_s \approx t_1 t_2 &\iff t_1^M\langle s\rangle = t_2^M\langle s\rangle \text{ määritelmän mukaan} \\ &\iff \pi(t_1^M\langle s\rangle) = \pi(t_2^M\langle s\rangle) \text{ koska } \pi \text{ on injektio} \\ &\iff t_1^{M'}\langle \pi \circ s\rangle = t_2^{M'}\langle \pi \circ s\rangle \text{ lemman 4.3 mukaan} \\ &\iff M' \models_{\pi \circ s} \approx t_1 t_2 \text{ määritelmän mukaan.} \end{aligned}$$

2. $\mathrm{R}t_1 \dots t_n \in \mathcal{E}$, sillä:

$$\begin{aligned} M \models_s \mathrm{R}t_1 \dots t_n &\iff \langle t_1^M\langle s\rangle, \dots, t_n^M\langle s\rangle\rangle \in Tul_M(\mathrm{R}) \text{ määritelmän mukaan} \\ &\iff \langle \pi t_1^M\langle s\rangle, \dots, \pi t_n^M\langle s\rangle\rangle \in Tul_{M'}(\mathrm{R}) \text{ koska } \pi \text{ on isomorfismi.} \\ &\iff \langle t_1^{M'}\langle \pi \circ s\rangle, \dots, t_n^{M'}\langle \pi \circ s\rangle\rangle \in Tul_{M'}(\mathrm{R}) \text{ lemman 4.3 nojalla} \\ &\iff M' \models_{\pi \circ s} \mathrm{R}t_1 \dots t_n \text{ määritelmän mukaan.} \end{aligned}$$

[1]Huomaa että $s(a/n)(i) = s'(a/n)(i)$ aina kun v_i esiintyy vapaana φ:ssä, sillä jos $i = n$, niin $s(a/n)(i) = a = s'(a/n)(i)$. Toisaalta jos $i \neq n$, niin v_i esiintyy vapaana myös $\forall v_n \varphi$:ssä ja $s(a/n)(i) = s(i) = s'(i) = s'(a/n)(i)$, joten induktio-oletusta voidaan soveltaa.

3. Oletetaan $\varphi \in \mathcal{E}$ ja todistetaan $\neg\varphi \in \mathcal{E}$.

$$\begin{aligned} M \models_s \neg\varphi &\iff M \not\models_s \varphi \text{ määritelmän mukaan} \\ &\iff M' \not\models_{\pi\circ s} \varphi \text{ oletuksen } \varphi \in \mathcal{E} \text{ mukaan} \\ &\iff M' \models_{\pi\circ s} \neg\varphi \text{ määritelmän mukaan.} \end{aligned}$$

4. Oletetaan $\varphi \in \mathcal{E}$ ja $\psi \in \mathcal{E}$ ja todistetaan $(\varphi \to \psi) \in \mathcal{E}$. Triviaali!

5. Oletetaan $\varphi \in \mathcal{E}$ ja $n \in \mathbb{N}$. Teemme ensin seuraavan havainnon: jos $a \in M$, niin

$$(\pi \circ s)(\pi(a)/n) = \pi \circ (s(a/n))) \tag{5}$$

$$\begin{aligned} M \models_s \forall v_n\varphi &\iff \text{Kaikilla } a \in M \;\; M \models_{s(a/n)} \varphi \\ &\underset{ind.ol.}{\iff} \text{Kaikilla } a \in M \;\; M' \models_{\pi\circ(s(a/n))} \varphi \\ &\underset{(5)}{\iff} \text{Kaikilla } a \in M \;\; M' \models_{(\pi\circ s)(\pi(a)/n)} \varphi \\ &\underset{\pi \;\; surj.}{\iff} \text{Kaikilla } a' \in M' \;\; M' \models_{(\pi\circ s)(a'/n)} \varphi \\ &\iff M' \models_{\pi\circ s} \forall v_n\varphi \end{aligned}$$

□

Seuraava korollaari on yllä todistetun lauseen varsinainen käyttötapa: isomorfisissa malleissa samat lauseet ovat tosia.

Korollaari 5.5 *Jos M ja M' ovat L-struktuureja ja $M \cong M'$, niin kaikille L-lauseille φ pätee.*

$$M \models \varphi \iff M' \models \varphi$$

Kahden mallin ei välttämättä tarvitse olla isomorfisia, jotta niissä olisi samat lauseet tosia. Tulemme näkemään, että on olemassa äärettömiä malleja, joissa on täsmälleen samat lauseet tosia, mutta silti mallit ovat ei-isomorfisia. Tämä havainto on pohjana seuraavalle tärkeälle määritelmälle:

Määritelmä 5.6 *L-struktuurit M ja M' ovat elementaalisti ekvivalentit,*

$$M \equiv M'$$

jos kaikille L-lauseille φ pätee

$$M \models \varphi \iff M' \models \varphi.$$

Korollaarin 5.5 sisältö voidaan nyt kutistaa toteamukseen: $M \cong M'$ implikoi $M \equiv M'$.

Määritelmä 5.7 *Olkoon M L-struktuuri ja $X \subseteq M^n$. Sanomme, että X on **määriteltävä relaatio** M**:ssä**, jos on olemassa L-kaava φ siten että kaikille $s : \mathbb{N} \to M$ pätee.*

$$M \models_s \varphi \iff \langle s(0), \ldots, s(n-1) \rangle \in X$$

*Alkio $a \in M$ on **määriteltävä alkio** M**:ssä** jos 1-paikkainen relaatio $\{a\}$ on määriteltävä relaatio M:ssä. Funktio $h : M^n \to M$ on **määriteltävä funktio** M**:ssä** jos n+1-paikkainen relaatio*

$$\{\langle a_0, \ldots, a_{n-1}, h(a_0, \ldots, a_{n-1}) \rangle | a_0, \ldots, a_{n-1} \in M\}$$

on.

Lause 5.8 ("Automorfismit säilyttävät määriteltävät relaatiot") *Olkoon M L-struktuuri ja $X \subseteq M^n$ määriteltävä relaatio M:ssä. Jos π on M:n automorfismi, niin kaikille $a_1, \ldots, a_n \in M$ pätee*

$$\langle a_1, \ldots, a_n \rangle \in X \iff \langle \pi(a_1), \ldots, \pi(a_n) \rangle \in X$$

Vastaava tulos pätee määriteltäville funktioille ja alkioille.

Tod. Olkoon φ L-kaava siten että

$$\langle s(0), \ldots, s(n-1) \rangle \in X \iff M \models_s \varphi.$$

Nyt

$$\begin{aligned} \langle s(0), \ldots, s(n-1) \rangle \in X &\iff M \models_s \varphi \\ &\iff M \models_{\pi \circ s} \varphi \text{ Lauseen 5.4 noj.} \\ &\iff \langle \pi(s(0)), \ldots, \pi(s(n-1)) \rangle \in X \end{aligned}$$

Väitös seuraa kun valitaan $s(i) = a_{i+1}$. □

Esimerkki 5.9 *Kuvassa 1 on 12:n alkion verkko $\mathcal{G} = (G, R)$ Alkio 2 on määriteltävissä, koska kaikilla s*

$$s(0) = 2 \iff \mathcal{G} \models_s \exists v_1 \forall v_2 (\mathrm{R} v_2 v_0 \to \approx v_2 v_1)$$

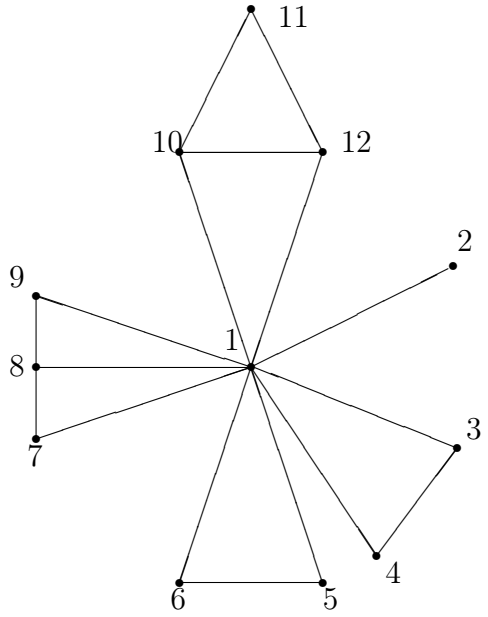


Figure 1: verkko

Olkoon

$$\begin{array}{ll}
\theta_2 & \neg \approx v_1 v_2 \\
\theta_3 & ((\theta_2 \wedge \neg \approx v_1 v_3) \wedge \neg \approx v_2 v_3) \\
\theta_4 & (((\theta_3 \wedge \neg \approx v_1 v_4) \wedge \neg \approx v_2 v_4) \wedge \neg \approx v_3 v_4) \\
\vdots & \\
\theta_{n+1} & (\ldots(\theta_n \wedge \neg \approx v_1 v_{n+1}) \wedge \neg \approx v_2 v_{n+1}) \wedge \ldots \wedge \neg \approx v_n v_{n+1})
\end{array}$$

Siis θ_n sanoo, että $v_1, \ldots, v_n$ ovat **eri** alkioita. Olkoon ψ_n kaava

$$\exists v_1 \ldots \exists v_n(\theta_n \wedge (\mathrm{R}v_0 v_1 \wedge \ldots \wedge \mathrm{R}v_0 v_n))$$

Siis ψ_n sanoo, että v_0:lla on ainakin n naapuria. Olkoon φ_n kaava $(\psi_n \wedge \neg\psi_{n+1})$, joka sanoo, että v_0:lla on tasan n naapuria.

Joukko $\{3, 4, 5, 6, 7, 9, 11\}$ on määriteltävä kaavalla φ_2. Joukko $\{8, 10, 12\}$ on määriteltävä kaavalla φ_3. Alkio 1 on määriteltävä kaavalla φ_{10}. Alkio 3

ei ole määriteltävä, koska

$$\pi(x) = \begin{cases} 4 & \text{jos } x = 3 \\ 3 & \text{jos } x = 4 \\ x & \text{muuten} \end{cases}$$

on $\mathcal{G}$:n automorfismi. Näin koko verkko $\mathcal{G}$ voidaan käydä läpi ratkaista, mitkä osajoukot ovat määriteltäviä ja mitkä eivät.

Esimerkki 5.10 *Mallin $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1)$ jokainen alkio on määriteltävä. $\mathcal{N}$:llä ei ole muita automorfismeja kuin identtinen kuvaus. ($\mathcal{N}$ on **jäykkä**). Mallin $\mathcal{Q} = (\mathbf{Q}, +, \cdot, 0, 1)$ jokainen alkio on määriteltävä (Harj.teht.). Mallin $(\mathbb{N}, <)$ jokainen alkio on määriteltävä, mutta mallin $(\mathbf{Q}, <)$ mikään alkio ei ole määriteltävä.*

Esimerkki 5.11 *Olkoon $\mathcal{G}$ kuten esimerkissä 5.9. Struktuurissa $\mathcal{G}' = (G, R, 3)$ on alkiolle 3 annettu nimi, esimerkiksi c_3. Nyt kaava $\approx v_0\mathrm{c}_3$ määrittelee alkion 3. Alkio 4 on määriteltävä kaavalla*

$$(\mathrm{R}v_0\mathrm{c}_3 \wedge \neg\varphi_{10}).$$

Joukot $\{3, 4\}$ ja $\{5, 6\}$, jotka eivät olleet määriteltäviä struktuurissa $\mathcal{G}$, ovat kuitenkin määriteltäviä struktuurissa $\mathcal{G}'$.

Seuraavassa on tyypillinen tilanne logiikassa: olemme kirjoittaneet kaavan, esim

$$\varphi = \exists v_2(\mathrm{R}v_0v_2 \wedge \mathrm{R}v_1v_2)$$

ja haluamme kaavan φ' joka sanoo v_0:sta ja v_2:sta saman kuin φ sanoo v_0:sta ja v_1:stä. Suora sijoitus ei käy, sillä näin saadaan

$$\exists v_2(\mathrm{R}v_0v_2 \wedge \mathrm{R}v_2v_2)$$

jossa on vain v_0 vapaa. Täytyy keksiä muuta!

Määritelmä 5.12 *Termi t on **sijoitettavissa muuttujaan** v_n **kaavassa** φ,*

$$\mathrm{SMK}(t, v_n, \varphi)$$

jos mikään termin t muuttujista ei tule sidotuksi sijoituksen jälkeen. Sijoittaminen tarkoittaa aina sijoittamista vapaisiin esiintymiin.

Esimerkki 5.13

Kaava	*Muuttujaan*	*voi sijoittaa*	*ei voi sijoittaa*
$\exists v_1 \approx v_0 v_1$	v_0	v_2	v_1
		$\mathrm{f}v_0$	$\mathrm{f}v_1$
$\mathrm{R}v_0 v_1$	v_1	*mitä tahansa*	-
$\exists v_0 \forall v_1 \approx \mathrm{f}v_0 v_1 v_2$	v_2	$\mathrm{f}v_2 v_3$	$\mathrm{f}v_0 v_1$
$\exists v_3 \forall v_4 \approx \mathrm{f}v_3 v_4 v_2$	v_2	$\mathrm{f}v_0 v_1$	$\mathrm{f}v_3 v_4$

Lause 5.14 *Kaikille t, v_n ja φ on olemassa φ^* siten, että $\models \varphi \leftrightarrow \varphi^*$ ja* $\mathrm{SMK}(t, v_n, \varphi^*)$.

Tod. Harj. teht. $\square$.

Lause 5.15 ("Sijoitettavuuslause") *Olkoon L aakkosto, M L-struktuuri ja $s : \mathbb{N} \to M$.*

1. *Olkoon t L-termi, jossa esiintyy muuttujat $v_0, \ldots, v_n$. Olkoot $t_0, \ldots, t_n$ L-termejä. Olkoon t' saatu t:stä korvaamalla v_i termillä t_i, kun $i = 0, ..., n$. Nyt $(t')^M\langle s\rangle = t^M\langle s'\rangle$, kun*

$$s'(i) = \begin{cases} t_i^M\langle s\rangle & i \leq n \\ s(i) & i > n \end{cases}$$

2. *Olkoon φ L-kaava jossa esiintyy muuttujat $v_0, \ldots, v_n$. Olkoot $t_0, \ldots, t_n$ L-termejä. Olkoon φ' saatu φ:stä korvaamalla v_i vapaissa esiintymissään termillä t_i, kun $0 \leq i \leq n$. Oletetaan, että $\mathrm{SMK}(t_i, v_i, \varphi)$ kun $0 \leq i \leq n$. Tällöin*

$$M \models_{s'} \varphi \iff M \models_s \varphi'$$

missä

$$s'(i) = \begin{cases} t_i^M\langle s\rangle & i \leq n \\ s(i) & i > n \end{cases}$$

Tod. Harj. teht. $\square$

6 Identiteetti

Kiinnitämme nyt huomiota identiteetin erityisominaisuuksiin. Tietyt identiteetin sisältävät kaavat ovat valideja varsin triviaaleista syistä, kuten nyt näemme.

Lemma 6.1 *Seuraavat L-kaavat ovat valideja olipa φ mikä L-atomikaava hyvänsä ja $t, t', t_1, \ldots, t_n, u_1, \ldots, u_n$ mitä L-termejä hyvänsä ja $m_1, ..., m_n$ mitä luonnollisia lukuja tahansa.*

1. $\approx tt$
2. $(\approx tt' \rightarrow \approx t't)$
3. $(((\approx t_1u_1 \wedge ... \wedge \approx t_nu_n) \wedge \varphi') \rightarrow \varphi'')$

missä φ' on saatu φ:stä korvaamalla muuttaja v_{m_i} termillä t_i kaikilla $1 \leq i \leq n$ ja φ'' vastaavasti korvaamalla muuttaja v_{m_i} termillä u_i.

Tod. Olkoon M L-struktuuri ja $s : \mathbb{N} \rightarrow M$. Kohdat 1 ja 2 ovat triviaaleja, joten todistamme kohdan 3. Oletetaan

$$M \models_s ((\approx t_1u_1 \wedge ... \wedge \approx t_nu_n) \wedge \varphi')$$

Siis

$$\begin{aligned} &t_i^M\langle s\rangle = u_i^M\langle s\rangle \qquad i = 1, \ldots, n \\ &M \models_s \varphi' \end{aligned}$$

Olkoon

$$s'(j) = \begin{cases} t_i^M\langle s\rangle & j = m_i \\ s(j) & \text{muuten} \end{cases}$$

ja

$$s''(j) = \begin{cases} u_i^M\langle s\rangle & j = m_i \\ s(j) & \text{muuten.} \end{cases}$$

Lauseen 5.15 nojalla

$$\begin{aligned} M \models_s \varphi' &\iff M \models_{s'} \varphi \\ M \models_s \varphi'' &\iff M \models_{s''} \varphi \end{aligned}$$

Koska nyt $s'(i) = s''(i)$ kaikilla i, saamme

$$M \models_s \varphi' \Longleftrightarrow M \models_s \varphi''$$

□

Lemman 6.1 kohtien (1) ja (2) kaavoja kutsutaan ***L*-identiteettiaksioomiksi**. Identiteettiaksioomat ovat yksinkertaisia, mutta joskus voi vaatia erityistä tarkkaavaisuutta nähdä, että tietty kaava on identiteettiaksiooma.

Esimerkki 6.2 *L-identiteettiaksioomeja:*

$$\approx v_0 v_0, \approx cc, \approx \mathrm{f} v_0 v_1 \mathrm{f} v_0 v_1$$

$$((\approx v_0 v_1 \wedge \mathrm{R} v_0) \rightarrow \mathrm{R} v_1)$$

$$((\approx v_0 v_1 \wedge \approx \mathrm{f} v_0 v_2) \rightarrow \approx \mathrm{f} v_1 v_2)$$

$$((\approx v_1 v_0 \wedge \approx v_1 v_2) \rightarrow \approx v_0 v_2).$$

7 Päättely

Predikaattilogiikan päättelyt ovat hyvin samantapaisia kuin propositiologiikankin päättelyt. Identiteetti ja kvanttorit tuovat uusia aksioomeja ja uuden säännön Modus Ponens säännön rinnalle. Myöhemmin osoitamme, että myös predikaattilogiikka toteuttaa täydellisyyslauseen: kaikki validit ovat todistuvia.

Jokainen predikaattilogiikan kaava on joko atomikaava, negaatiolla alkava kaava, kahden kaavan implikaatio tai universaalikvanttorilla alkava kaava. Jos atomikaavoja ja universaalikvanttorilla alkavia kaavoja ajatellaan propositiosymboleiksi, ovat predikaattilogiikan kaavat itse asiassa propositiolauseita. Näin voimme puhua esimerkiksi kaavojen

$$(\approx tt' \rightarrow \approx tt'), (\forall v_0 \varphi \vee \neg \forall v_0 \varphi)$$

tautologisuudesta. Kaavan φ tautologisuus tarkoittaa siis sitä, että kuvattiinpa atomikaavat ja universaalikvanttorilla alkavat kaavat luvuiksi 0 ja 1 millä tahansa totuusjakaumalla, niin φ saa tällä totuusjakaumalla arvon 1. On huomattava, että $\exists v_0 \varphi$ on lyhenne kaavasta $\neg \forall v_0 \neg \varphi$. Niinpä

$$(\forall v_i \neg \varphi \vee \exists v_i \varphi), \neg(\forall v_i \neg \varphi \wedge \exists v_i \varphi)$$

ovat tautologioita.

Päättely tarkoittaa jonoa kaavoja, missä jokainen jonon jäsen saadaan edeltäjistä niin sanottujen päättelysääntöjen avulla. Eräät päättelyjonon alkiot ovat erityisasemassa. Näitä ovat propositiologiikan aksioomat, L-identiteettiaksioomat ja ns. L-**kvanttoriaksioomat** eli L-kaavat:

$$(\forall v_j \psi \to \psi'),$$

missä ψ' on saatu ψ:stä sijoittamalla v_j:n vapaisiin esiintymiin termi t, josta oletetaan $\mathrm{SMK}(t, v_j, \psi)$.

Lemma 7.1 *L-kvanttoriaksioomat ovat valideja.*

Tod. Oletetaan $M \models_s \forall v_j \psi$ ja $\mathrm{SMK}(t, v_j, \psi)$. Siis $M \models_{s(a/j)} \psi$, kun $a = t^M\langle s \rangle$. Lauseen 5.15 nojalla $M \models_s \psi'$. Siis $\models \forall v_j \psi \to \psi'$.
□

Määritelmä 7.2 *Predikaattilogiikan L-*aksioomien *joukko määritellään seuraavasti*

- *L-kaavat jotka ovat propositiologiikan aksioomia ovat myös predikaattilogiikan L-aksioomia.*
- *L-identiteettiaksioomat ovat aksioomia.*
- *L-kvanttoriaksioomat ovat aksioomia.*

L-kaavojen joukosta Σ todistuvien L-kaavojen joukko määritellään seuraavasti

(T1) Jokainen Σ:n alkio on todistuva joukosta Σ.

(T2) Jokainen L-aksiooma on todistuva joukosta Σ.

(T3) Modus Ponens: Jos L-kaavat φ ja $(\varphi \to \psi)$ ovat todistuvia joukosta Σ niin myös ψ on todistuva joukosta Σ.

(T4) Yleistyssääntö: Jos L-kaava $(\psi \to \theta)$ on todistuva joukosta Σ ja v_j on muuttuja siten, että

- *v_j ei esiinny vapaana ψ:ssä*
- *v_j ei esiinny vapaana Σ:n kaavoissa*

niin $(\psi \to \forall v_j \theta)$ *on todistuva joukosta* Σ.

Jos L-kaava φ *on todistuva L-kaavojen joukosta* Σ*, merkitään* $\Sigma \vdash \varphi$*. Jos* $\emptyset \vdash \varphi$*, merkitään* $\vdash \varphi$ *ja sanotaan, että* φ *on* todistuva.

Todistuvuuden määritelmä voidaan yhtäpitävästi esittää seuraavassa vaihtoehtoisessa muodossa:

Määritelmä 7.3 *Olkoon L aakkosto ja* Σ *joukko L-kaavoja.* ***Todistus*** *eli* ***päättely*** Σ*:sta on jono* $\langle \varphi_1, \ldots, \varphi_n \rangle$ *L-kaavoja siten että jokainen* φ_i *toteuttaa jonkin seuraavista ehdoista:*

1. φ_i *on* Σ*:n alkio*
2. φ_i *on propositiologiikan aksiooma*
3. φ_i *on L-identiteettiaksiooma*
4. φ_i *on L-kvanttoriaksiooma*
5. φ_i *on saatu* ***Modus Ponens****-säännöllä aikaisemmista eli on olemassa* $j, k < i$ *siten että* $\varphi_j = (\varphi_k \to \varphi_i)$.
6. φ_i *on saatu* ***yleistyssäännöllä*** *aikaisemmista eli* $\varphi_i = (\psi \to \forall v_j \theta)$ *ja on olemassa* $k < i$ *siten että*
   - $\varphi_k = (\psi \to \theta)$
   - v_j *ei esiinny vapaana* ψ*:ssä*
   - v_j *ei esiinny vapaana* Σ*:n kaavoissa*

Selvästi, L-kaava φ on todistuva Σ:sta jos ja vain jos on olemassa todistus $\langle \varphi_1 \ldots \varphi_n \rangle$ Σ:sta siten että $\varphi_n = \varphi$.

Osoitimme edellä propositiologiikan yhteydessä, että kaikki tautologiat ovat todistuvia. Siksi voimme nyt hyväksyä todistuksen eräänä askeleena minkä tahansa tautologian.

Esimerkki 7.4 *Oletetaan, että* ψ' *on saatu kaavasta* ψ *sijoittamalla muuttujan* v_j *vapaisiin esiintymiin termi t ja lisäksi* $\mathrm{SMK}(t, v_j, \psi)$*. Tällöin* $\vdash (\psi' \to \exists v_j \psi)$*:*

1.	$(\forall v_j \neg\psi \to \neg\psi')$	*L-kvanttoriaksiooma*
2.	$((\forall v_j \neg\psi \to \neg\psi') \to (\psi' \to \neg\forall v_j \neg\psi))$	*tautologia*
3.	$(\psi' \to \exists v_j \psi)$	*MP 1,2*

Esimerkki 7.5 *Oletetaan $\Sigma \vdash (\psi \to \theta)$, missä v_j ei esiinny vapaana θ:ssa eikä Σ:n kaavoissa. Tällöin $\Sigma \vdash (\exists v_j \psi \to \theta)$.*

1.	$(\psi \to \theta)$	*oletuksen nojalla todistuva Σ:sta*
2.	$((\psi \to \theta) \to (\neg\theta \to \neg\psi))$	*tautologia*
3.	$(\neg\theta \to \neg\psi)$	*MP 1,2*
4.	$(\neg\theta \to \forall v_j \neg\psi)$	*yleistys 3*
5.	$((\neg\theta \to \forall v_j \neg\psi) \to (\neg\forall v_j \neg\psi \to \theta))$	*tautologia*
6.	$(\exists v_j \psi \to \theta)$	*MP 4,5*

□

Esimerkki 7.6 $\{\mathrm{Rc}, \forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0)\} \vdash \mathrm{Pc}$

1.	$(\forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0) \to (\mathrm{Rc} \to \mathrm{Pc}))$	*kvanttoriaksiooma*
2.	$\forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0)$	*oletus*
3.	$(\mathrm{Rc} \to \mathrm{Pc})$	*MP 1,2*
4.	Rc	*oletus*
5.	Pc	*MP 3,4*

□

Esimerkki 7.7 $\{\forall v_n \neg\varphi\} \vdash \neg\exists v_n \varphi$

1.	$(\forall v_n \neg\varphi \to \neg\neg\forall v_n \neg\varphi)$	*tautologia*
2.	$\forall v_n \neg\varphi$	*oletus*
3.	$\neg \underbrace{\neg\forall v_n \neg\varphi}_{\exists v_n \varphi}$	*MP 1,2*

□

Esimerkki 7.8 $\{\exists v_n \neg\varphi\} \vdash \neg\forall v_n \varphi$

1.	$(\forall v_n \varphi \to \varphi)$	*kvanttoriaksiooma*
2.	$((\forall v_n \varphi \to \varphi) \to (\forall v_n \varphi \to \neg\neg\varphi))$	*tautologia*
3.	$(\forall v_n \varphi \to \neg\neg\varphi)$	*MP 1,2*
4.	$(\forall v_n \varphi \to \forall v_n \neg\neg\varphi)$	*yleistys 3*
5.	$((\forall v_n \varphi \to \forall v_n \neg\neg\varphi) \to (\neg\forall v_n \neg\neg\varphi \to \neg\forall v_n \varphi))$	*tautologia*
6.	$(\underbrace{\neg\forall v_n \neg\neg\varphi}_{\exists v_n \neg\varphi} \to \neg\forall v_n \varphi)$	*MP 5,6*
7.	$\exists v_n \neg\varphi$	*oletus*
8.	$\neg\forall v_n \varphi$	*MP 6,7*

□

Lause 7.9 (Korrektisuuslause) *Jos* $\Sigma \vdash \varphi$*, niin* $\Sigma \models \varphi$*.*

Todistus. Olkoon $\langle \varphi_1, \ldots, \varphi_n \rangle$ kaavan φ todistus Σ:sta. Todistamme induktiolla n:n suhteen:

Väite: $\Sigma \models \varphi_i$.

1. φ_i on Σ:n alkio. Selvä tapaus.
2. φ_i on propositiologiikan aksiooma. Selvä tapaus.
3. φ_i identiteettiaksiooma. Lemma 6.1
4. φ_i kvanttoriaksiooma. Lemma 7.1
5. φ_i saatu Modus Ponensilla φ_j:stä ja φ_k:sta, kun $\varphi_k = (\varphi_j \to \varphi_i)$. Induktio-oletuksen nojalla $\Sigma \models \varphi_j$ ja $\Sigma \models \varphi_k$. Siis $\Sigma \models \varphi_i$.
6. φ_i on saatu yleistyksellä eli

   $$\varphi_i = (\psi \to \forall v_k \theta)$$

   $$\varphi_j = (\psi \to \theta) \text{ jollakin } j < i,$$

   ja v_k ei ole vapaa ψ:ssä eikä Σ:ssa.

   Osoitetaan, että $\Sigma \vDash (\psi \to \forall v_k \theta)$. Olkoon $\mathcal{M} \vDash_s \Sigma$ ja $\mathcal{M} \vDash_s \psi$. Olkoon $a \in M$. Lauseen 5.2 nojalla $\mathcal{M} \vDash_{s(a/n)} \Sigma$ ja $\mathcal{M} \vDash_{s(a/n)} \psi$. Induktio-oletuksen nojalla $\Sigma \vDash (\psi \to \theta)$, joten $\mathcal{M} \vDash_{s(a/n)} \theta$. Olemme todistaneet, että $\mathcal{M} \vDash_s \forall v_k \theta$.

□

Korrektisuuslause antaa tärkeän keinon osoittaa, että $\Sigma \nvdash \varphi$:

Korollaari 7.10 *Jos* $\Sigma \nvDash \varphi$*, niin* $\Sigma \nvdash \varphi$*.*

Esimerkki 7.11 $\{\forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0), \mathrm{P\,c}\} \nvdash \mathrm{R\,c}$.

Todistus. Olkoon $\mathcal{M} = (\{0\}, Tul_{\mathcal{M}})$, missä $Tul_{\mathcal{M}}(\mathrm{c}) = 0$, $Tul_{\mathcal{M}}(\mathrm{R}) = \emptyset$ ja $Tul_{\mathcal{M}}(\mathrm{P}) = \{0\}$. Nyt $\mathcal{M} \vDash \forall v_0(\mathrm{R}v_0 \to \mathrm{P}v_0)$ ja $\mathcal{M} \vDash \mathrm{P\,c}$, mutta $\mathcal{M} \nvDash \mathrm{R\,c}$. □

Esimerkki 7.12 $\{\forall v_0 \exists v_1 \mathrm{R} v_0 v_1, \forall v_1 \exists v_0 \mathrm{R} v_0 v_1\} \nvdash \exists v_0 \mathrm{R} v_0 v_0$

Todistus. Olkoon $\mathcal{M} = (\{0,1\}, \{\langle 0,1\rangle, \langle 1,0\rangle\})$. Nyt

$$\mathcal{M} \vDash \forall v_0 \exists v_1 \mathrm{R} v_0 v_1,$$

$$\mathcal{M} \vDash \forall v_1 \exists v_0 \mathrm{R} v_0 v_1, \text{ mutta}$$

$$\mathcal{M} \nvDash \exists v_0 \mathrm{R} v_0 v_0.$$

□

Seuraava lemma osoittaa, että tietyissä tapauksissa vakio voidaan korvata muuttujalla. Esimerkiksi todistuksesta

(1)	$(\forall v_0 \neg \mathrm{R} v_0 \to \neg \mathrm{R}\,\mathrm{c})$	kv. aks.
(2)	$((\forall v_0 \neg \mathrm{R} v_0 \to \neg \mathrm{R}\,\mathrm{c}) \to (\mathrm{R}\,\mathrm{c} \to \neg \forall v_0 \neg \mathrm{R} v_0))$	tautologia
(3)	$(\mathrm{R}\,\mathrm{c} \to \neg \forall v_0 \neg \mathrm{R} v_0)$	MP 1,2
(4)	$(\mathrm{R}\,\mathrm{c} \to \exists v_0 \mathrm{R} v_0)$	lyhenne

Saadaan väitteen $\vdash (\mathrm{R} v_1 \to \exists v_0 \mathrm{R} v_0)$ todistus korvaamalla kaikkialla symboli c symbolilla v_1:

(1)	$(\forall v_0 \neg \mathrm{R} v_0 \to \neg \mathrm{R}\, v_1)$	kvanttoriaksiooma
(2)	$((\forall v_0 \neg \mathrm{R} v_0 \to \neg \mathrm{R}\, v_1) \to (\mathrm{R}\, v_1 \to \neg \forall v_0 \neg \mathrm{R} v_0))$	tautologia
(3)	$(\mathrm{R}\, v_1 \to \neg \forall v_0 \neg \mathrm{R} v_0)$	MP 1,2
(4)	$(\mathrm{R}\, v_1 \to \exists v_0 \mathrm{R} v_0)$	lyhenne

Merkintä: Jos φ on kaava ja t termi,

$$\varphi(t/v_n)$$

tarkoittaa kaavaa, joka saadaan φ:stä korvaamalla v_n vapaissa esiintymissään termillä t. Lauseeen 5.15 nojalla

$$\begin{aligned} &\mathrm{SMK}(t, v_n, \varphi) \implies \\ &M \models_s \varphi(t/v_n) \iff M \models_{s(a/n)} \varphi \text{ kun } a = t^M\langle s\rangle \end{aligned}$$

Eli, jos t on sijoitettavissa muuttujaan v_n kaavassa φ, niin kaavan $\varphi(t/v_n)$ totuusehdot voidaan laskea kun tunnetaan kaavan φ totuusehdot ja termin t arvot.

Lemma 7.13 ***(Vakioiden lemma)*** *Olkoon L aakkosto, φ L-kaava, $n \in \mathbb{N}$, $c \notin L$ ja Σ joukko L-kaavoja. Jos*

$$\Sigma \vdash \varphi(c/v_n)$$

niin on olemassa $m \in \mathbb{N}$ siten että

$$\Sigma \vdash \varphi(v_k/v_n)$$

kun $k \geq m$.

Tod. Olkoon $\langle \varphi_1, \ldots, \varphi_{n'} \rangle$ kaavan $\varphi(c/v_n)$ todistus Σ:sta. Olkoon $m \in \mathbb{N}$ niin suuri, että v_k ei esiinny kaavoissa $\varphi_1, \ldots, \varphi_{n'}$ kun $k \geq m$. Olkoon $k \geq m$ kiinteä. Jos θ on mikä tahansa kaava, niin olkoon θ' saatu kaavasta θ korvaamalla kaikkialla symboli c symbolilla v_k. Koska $c \notin L$, on $\theta' = \theta$ kaikilla L-kaavoilla θ. Koska kaavat φ_i ovat $L \cup \{c\}$-kaavoja, niille sama ei päde.

Väite $\langle \varphi'_1, \ldots, \varphi'_{n'} \rangle$ on todistus Σ:sta

1^o $\varphi_i \in \Sigma$: $\varphi'_i = \varphi_i$ joten $\varphi_i \in \Sigma$

2^o φ_i tautologia: Selvästi φ'_i on tautologia.

3^o φ_i on identiteettiaksiooma. Selvästi φ'_i on identiteettiaksiooma.

4^o φ_i on kvanttoriaksiooma $\forall v_j \psi \to \psi(t/v_j)$ missä $\mathrm{SMK}(t, v_j, \psi)$. Selvästi myös $\mathrm{SMK}(t, v_j, \psi')$, joten $\varphi'_i = \forall v_j \psi' \to \psi'(t/v_j)$ on kvanttoriaksiooma.

5^o φ_i on saatu MP:lla kaavoista φ_j ja $\varphi_k = (\varphi_j \to \varphi_i)$. Nyt φ'_i saadaan MP:lla kaavoista φ'_j ja $\varphi'_k = (\varphi'_j \to \varphi'_i)$.

6^o $\varphi_i = (\psi \to \forall v_j \theta)$ on saatu yleistyssäännöllä kaavasta $\varphi_k = (\psi \to \theta)$ ja v_j ei esiinny vapaana ψ:ssä. Nyt

$$\begin{aligned} \varphi'_k &= (\psi' \to \theta') \\ \varphi'_i &= (\psi' \to \forall v_j \theta') \end{aligned}$$

ja v_j ei esiinny vapaana ψ':ssa, joten φ'_i saadaan yleistyssäännöllä φ'_k:sta.

□

Lause 7.14 (Deduktioteoreema) *Jos ψ on lause ja $\Sigma \cup \{\psi\} \vdash \varphi$, niin $\Sigma \vdash (\psi \to \varphi)$.*

Tod. Olkoon $\varphi_1, \ldots, \varphi_n$ kaavan φ todistus $\Sigma \cup \{\psi\}$:stä.

Väite: $\Sigma \vdash (\psi \to \varphi_i)$ kaikilla $i = 1...n$.

1^o $\varphi_i \in \Sigma \cup \{\psi\}$. Selvästi $\Sigma \vdash (\psi \to \varphi_i)$

2^o φ_i tautologia. Selvästi $\Sigma \vdash (\psi \to \varphi_i)$

3^o φ_i on identiteettiaksiooma. Selvästi $\Sigma \vdash (\psi \to \varphi_i)$

4^o φ_i on kvanttoriaksiooma. Selvästi $\Sigma \vdash (\psi \to \varphi_i)$

5^o φ_i on saatu MP:lla φ_j:stä ja φ_k:sta, $\varphi_k = (\varphi_j \to \varphi_i)$. Käyttämällä tautologiaa $((\psi \to \varphi_j) \to ((\psi \to \varphi_k) \to (\psi \to \varphi_i)))$ nähdään että $\Sigma \vdash (\psi \to \varphi_i)$.

6^o φ_i on saatu yleistyssäännöllä φ_k:sta,

$$\begin{aligned} \varphi_i &= (\theta_1 \to \forall v_j \theta_2) \\ \varphi_k &= (\theta_1 \to \theta_2) \end{aligned}$$

ja v_j ei vapaa θ_1:ssä. Nyt

$$\Sigma \vdash ((\psi \wedge \theta_1) \to \theta_2)$$

ja v_j ei vapaa $(\psi \wedge \theta_1)$:ssä. Siis

$$\Sigma \vdash ((\psi \wedge \theta_1) \to \forall v_j \theta_2)$$

mistä seuraa

$$\Sigma \vdash (\psi \to \varphi_i)$$

□

8 Teoriat

Määritelmä 8.1 *Olkoon L aakkosto. L-**teoria** on mikä tahansa joukko L-lauseita. L-struktuuri M on L-teorian Σ **malli** jos $M \models \Sigma$. Σ on **ristiriitainen** jos on olemassa L-lause φ siten että*

$$\Sigma \vdash \varphi \text{ ja } \Sigma \vdash \neg\varphi$$

*muuten **ristiriidaton**.*

Lause 8.2 *Jos Σ:lla on malli, niin Σ on ristiriidaton.*

Todistus. Jos $\Sigma \vdash \varphi$ ja $\Sigma \vdash \neg\varphi$ niin korrektisuuslauseen nojalla Σ:lla ei voi olla mallia. □

Lause 8.3 *L on aakkosto ja M on L-struktuuri, niin*

$$Th(M) = \{\varphi \mid \varphi \ L - lause, M \models \varphi\}$$

on ristiriidaton L-teoria.

Todistus. Koska $M \models Th(M)$, seuraa $M \models \varphi$. □

Lause 8.3 antaa suuren määrän esimerkkejä ristiriidattomista teorioista:

$Th((\mathbb{N}, +, \cdot, 0, 1))$	tosi aritmetiikka
$Th((\mathbf{R}, +, \cdot, 0, 1))$	reaalilukujen kunnan teoria
$Th((\mathbb{N}, S, 0))$	seuraajafunktion teoria

Lemma 8.4 *Jos Σ on ristiriitainen joukko L-lauseita, niin on olemassa äärellinen $\Sigma_0 \subseteq \Sigma$ siten, että Σ_0 on ristiriitainen.*

Todistus. . Oletetaan, että $\Sigma \vdash \varphi \wedge \neg\varphi$. Olkoon $\varphi_1, \ldots, \varphi_n$ lauseen $\varphi \wedge \neg\varphi$ todistus Σ:sta. Olkoon $\Sigma_0 = \{\varphi_i | \varphi_i \in \Sigma\}$. Tällöin $\varphi_1, \ldots, \varphi_n$ on lauseen $\varphi \wedge \neg\varphi$ todistus Σ_0:sta. □

Lemma 8.5 *(Ketjulemma) Jos $\Sigma_0 \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \ldots$ ovat ristiriidattomia joukkoja L-lauseita, niin myös $\bigcup_{n=0}^{\infty} \Sigma_n$ on ristiriidaton.*

Todistus. . Olkoon $\Sigma' \subseteq \bigcup_{n=0}^{\infty} \Sigma_n$ äärellinen. Tällöin on olemassa $m \in \mathbb{N}$ sellainen, että $\Sigma' \subseteq \Sigma_m$. Koska Σ_m on ristiriidaton, on myös Σ' ristiriidaton. □

Lemma 8.6 *Olkoon φ lause. Tällöin $\Sigma \cup \{\varphi\}$ on ristiriitainen jos ja vain jos $\Sigma \vdash \neg\varphi$.*

Todistus. . Osoitetaan aluksi, että jos $\Sigma \cup \{\varphi\}$ on ristiriitainen, niin $\Sigma \vdash \neg\varphi$. Olkoon ψ sellainen, että $\Sigma \cup \{\varphi\} \vdash (\psi \wedge \neg\psi)$. Deduktioteoreeman nojalla $\Sigma \vdash (\varphi \to (\psi \wedge \neg\psi))$. Havaitaan, että lause $((\varphi \to (\psi \wedge \neg\psi)) \to \neg\varphi)$ on tautologia, joten käyttämällä MP:tä voidaan päätellä $\Sigma \vdash \neg\varphi$.

Väitteen toisen suunnan osoittamiseksi oletetaan, että $\Sigma \vdash \neg\varphi$. Tällöin $\Sigma \cup \{\varphi\} \vdash \neg\varphi$. Lause $(\neg\varphi \to (\varphi \to (\varphi \wedge \neg\varphi)))$ on tautologia, joten MP:llä saadaan $\Sigma \cup \{\varphi\} \vdash (\varphi \to (\varphi \wedge \neg\varphi))$, ja edelleen $\Sigma \cup \{\varphi\} \vdash (\varphi \wedge \neg\varphi)$. □

Korollaari 8.7 *$\Sigma \cup \{\neg\varphi\}$ on ristiriitainen jos ja vain jos $\Sigma \vdash \varphi$.* □

Määritelmä 8.8 *L-teoria* Σ *on* täydellinen *jos se on ristiriidaton ja kaikille L-lauseille* φ *pätee*

$$\Sigma \vdash \varphi \text{ tai } \Sigma \vdash \neg\varphi.$$

Esimerkki 8.9 $Th(\mathcal{M})$ *on täydellinen.*

Todistus. Jos $\mathcal{M} \vDash \varphi$, niin $\varphi \in Th(\mathcal{M})$. Jos $\mathcal{M} \vDash \neg\varphi$, niin $\neg\varphi \in Th(\mathcal{M})$. □

Lause 8.10 *(Lindenbaumin lemma) Olkoon L (numeroituva) aakkosto. Jos* Σ *on ristiriidaton L-teoria, niin on olemassa täydellinen L-teoria* Σ^* *siten että* $\Sigma \subseteq \Sigma^*$.

Tod. Koska L on numeroituva, voidaan kaikki L-lauseet luetella jonona $\varphi_0, \varphi_1, \varphi_2, \ldots$. Määritellään

$$\begin{aligned} \Sigma_0 &= \Sigma \\ \Sigma_{n+1} &= \begin{cases} \Sigma_n \cup \{\varphi_n\} & \text{jos } \Sigma_n \vdash \varphi_n \\ \Sigma_n \cup \{\neg\varphi_n\} & \text{muuten} \end{cases} \\ \Sigma^* &= \bigcup_{n=0}^{\infty} \Sigma_n \end{aligned}$$

Väite Σ_n on ristiriidaton jokaisella n.

1. $n = 0$: $\Sigma_n = \Sigma$
2. Induktio-oletus: Σ_n on ristiriidaton
3. $\Sigma_{n+1} = \Sigma \cup \{\varphi_n\}$ ja $\Sigma_n \vdash \varphi_n$. Jos Σ_{n+1} olisi ristiriitainen niin lemman 8.6 nojalla $\Sigma_n \vdash \neg\varphi_n$. Koska myös $\Sigma_n \vdash \varphi_n$, seuraa, että Σ_n on ristiriitainen vastoin induktio-oletusta.
4. $\Sigma_{n+1} = \Sigma_n \cup \{\neg\varphi_n\}$ ja $\Sigma_n \nvdash \varphi_n$. Jos Σ_{n+1} olisi ristiriitainen, niin korollaarin 8.7 nojalla $\Sigma_n \vdash \varphi_n$, vastoin oletusta. Väite todistettu. Lemman 8.5 nojalla Σ^* on ristiriidaton.

Väite Σ^* on täydellinen.
Jos φ_n on L-lause, niin $\varphi_n \in \Sigma_{n+1}$ tai $\neg\varphi_n \in \Sigma_{n+1}$, joten väite tosi. □

Lause 8.11 *Jos* Σ *on täydellinen L-teoria, niin kaikille L-lauseille* φ *ja* ψ *pätee:*

(i) $\Sigma \vdash \neg\varphi$ *joss* $\Sigma \nvdash \varphi$

(ii) $\Sigma \vdash (\varphi \to \psi)$ *joss* $(\Sigma \nvdash \varphi$ *tai* $\Sigma \vdash \psi)$

Tod. Kuten Lause 2.20. □

Lemma 8.12 *Olkoon L aakkosto ja Σ ristiriidaton joukko L-lauseita. Olkoon L' aakkosto siten että $L' \setminus L$ sisältää äärettömän monia vakiosymboleja. Jos $n \in \mathbb{N}$ ja φ on L'-lause, niin on olemassa vakiosymboli $c \in L' \setminus L$ siten, että $\Sigma \cup \{(\varphi(c/v_n) \to \forall v_n \varphi)\}$ on ristiriidaton.*

Tod. Valitaan $c \in L' \setminus L$ siten että c ei esiinny φ:ssä. Jos $\Sigma \cup \{(\varphi(c/v_n) \to \forall v_n \varphi\})$ on ristiriitainen, niin Lemman 8.6 nojalla $\Sigma \vdash \neg(\varphi(c/v_n) \to \forall v_n \varphi)$, joten helposti nähdään, että $\Sigma \vdash \varphi(c/v_n)$ ja $\Sigma \vdash \neg \forall v_n \varphi$. Vakioiden lemman nojalla $\Sigma \vdash \varphi(v_m/v_n)$ sopivalla $m \in \mathbb{N}$. Yleistyssäännöllä $\Sigma \vdash \forall v_m \varphi(v_m/v_n)$ mistä seuraa helposti $\Sigma \vdash \forall v_n \varphi$. Toisaalta juuri pääteltiin, että $\Sigma \vdash \neg \forall v_n \varphi$, vastoin oletusta, että Σ on ristiriidaton. □

Lause 8.13 *Olkoon L aakkosto ja Σ täydellinen L-teoria siten että kaikille L-lauseille $\forall v_n \varphi$ on olemassa $c \in L$ siten että $\Sigma \vdash (\varphi(c/v_n) \to \forall v_n \varphi)$. Tällöin on olemassa L-struktuuri M siten että kaikille L-lauseille φ pätee*

$$M \models \varphi \text{ joss } \Sigma \vdash \varphi.$$

Tod. Olkoon M_0 kaikkien L-vakiotermien joukko (vakiotermejä ovat kaikki ne termit, jotka eivät sisällä muuttujia). Olkoon M_0:ssa

$$t \sim t' \iff \Sigma \vdash \approx tt'$$
$$[t] = \{t' \in M_0 \mid t \sim t'\}$$

Väite 1 $\sim$ on ekvivalenssirelaatio M_0:ssa.
Tod. Identiteettiaksioomien nojalla

1. $\Sigma \vdash \approx tt$ joten $t \sim t$.
2. Jos $t \sim t'$ ja $t' \sim t''$ niin $\Sigma \vdash \approx tt'$ ja $\Sigma \vdash \approx t't''$ ja siis $\Sigma \vdash \approx tt''$ mistä $t \sim t''$.
3. Jos $t \sim t'$, niin $\Sigma \vdash \approx tt'$ mistä seuraa $\Sigma \vdash \approx t't$ ja siis $t' \sim t$.

Väite 2 Jos $\mathrm{R} \in Rel_L$, $\#_L(\mathrm{R}) = n$, $t_1, \ldots, t_n$ ovat L-termejä siten että $\mathrm{R}t_1 \ldots t_n \in \Sigma$ ja $t_1 \sim t'_1, \ldots, t_n \sim t'_n$, niin $\mathrm{R}t'_1 \ldots t'_n \in \Sigma$, sillä identiteettiaksioomien nojalla

$$\Sigma \vdash ((\approx t_1 t'_1 \wedge \ldots \wedge \approx t_n t'_n \wedge \mathrm{R}t_1 \ldots t_n) \rightarrow \mathrm{R}t'_1 \ldots t'_n)$$

□

Väite 3 Jos $\mathrm{f} \in Fun_L, \#_L(\mathrm{f}) = n$, ja $t_1, \ldots, t_n, t'_1, \ldots, t'_n$ ovat L-termejä siten että $t_1 \sim t'_1, \ldots, t_n \sim t'_n$ niin $\approx \mathrm{f}t_1 \ldots t_n \mathrm{f}t'_1 \ldots t'_n \in \Sigma$.
Tod. Seuraa identiteettiaksioomista.

Nyt määritellään L-struktuuri M seuraavasti:

$$M = M_0/\sim = \{[t] \mid t \in M_0\}$$

$$Tul_M(\mathrm{R}) = \{\langle [t_1], \ldots, [t_n] \rangle \mid \Sigma \vdash \mathrm{R}t_1 \ldots t_n\} \text{ kun } \mathrm{R} \in L \text{ ja } \#_L(\mathrm{R}) = n$$

$$Tul_M(\mathrm{f})([t_1], \ldots, [t_n]) = [\mathrm{f}t_1 ... t_n] \text{ kun } \mathrm{f} \in L \text{ ja } \#_L(\mathrm{f}) = n$$

$$Tul_M(c) = [c] \text{ kun } c \in L$$

Väitteiden 1-3 nojalla M on hyvinmääritelty. Nyt on todistettava $M \models \Sigma$. Tämä seuraa kun todistetaan.

Väite 4 Kaikille L-termeille $t_1, ..., t_n$ ja L-kaavoille φ, joissa on vapaana esiintyvät muuttujat $v_{k_1}, ..., v_{k_n}$, pätee

$$t_i^M = [t_i]$$

ja

$$M \models \varphi(t_1/v_{k_1}, ..., t_n/v_{k_n}) \Longleftrightarrow \Sigma \vdash \varphi(t_1/v_{k_1}, ..., t_n/v_{k_n}).$$

Tod. $c^M = [c]$ määritelmän mukaan.

$$\begin{aligned} (\mathrm{f}t_1 \ldots t_n)^M &= Tul_M(\mathrm{f})(t_1^M, \ldots, t_n^M) \\ &= Tul_M(\mathrm{f})([t_1], \ldots, [t_n]) = [\mathrm{f}t_1 ... t_n] \end{aligned}$$

Siis $t^M = [t]$ kaikilla t.

1.

$$\begin{aligned} M \models \approx t_1 t_2 &\iff t_1^M = t_2^M \\ &\iff [t_1] = [t_2] \text{ määritelmä} \\ &\iff t_1 \sim t_2 \text{ määritelmä} \\ &\iff \Sigma \vdash \approx t_1 t_2 \text{ määritelmä} \end{aligned}$$

2.

$$\begin{aligned} M \models \mathrm{R} t_1 \dots t_n &\iff \langle t_1^M, \dots, t_n^M \rangle \in Tul_M(\mathrm{R}) \\ &\iff \langle [t_1], \dots, [t_n] \rangle \in Tul_M(\mathrm{R}) \\ &\iff \Sigma \vdash \mathrm{R} t_1 ... t_n \end{aligned}$$

3.

$$\begin{aligned} M \models \neg\varphi &\iff M \not\models \varphi \\ &\iff \Sigma \nvdash \varphi \text{ ind.ol.} \\ &\iff \Sigma \vdash \neg\varphi \text{ Lause 8.11} \end{aligned}$$

4.

$$\begin{aligned} M \models (\varphi \to \psi) &\iff M \not\models \varphi \text{ tai } M \models \psi \\ &\iff \Sigma \nvdash \varphi \text{ tai } \Sigma \vdash \psi \text{ ind.ol.} \\ &\iff \Sigma \vdash (\varphi \to \psi) \text{ Lause 8.11} \end{aligned}$$

5. Oletetaan $M \models \forall v_n \varphi$. On olemassa c siten että

$$\Sigma \vdash (\varphi(c/v_n) \to \forall v_n \varphi)$$

Selvästi $M \models \varphi(c/v_n)$, joten induktio-oletuksen nojalla $\Sigma \vdash \varphi(c/v_n)$. Nyt saadaan helposti $\Sigma \vdash \forall v_n \varphi$. Olkoon kääntäen $\Sigma \vdash \forall v_n \varphi$. Selvästi $\Sigma \vdash \varphi(c/v_n)$ kaikille $c \in L$. Osoitamme nyt että $M \models \forall v_n \varphi$ käymällä läpi kaikki mallin M alkiot. Jos $t \in M_0$, niin oletuksen nojalla on olemassa $c \in L$ siten että

$$\Sigma \vdash (\neg \approx ct \to \forall v_0 \neg \approx v_0 t).$$

Toisaalta, jos $\Sigma \vdash \forall v_0(\neg \approx v_0 t)$, niin yllä olevan nojalla $M \models \forall v_0(\neg \approx v_0 t)$, ristiriita. Siis $\Sigma \nvdash \forall v_0(\neg \approx v_0 t)$ ja välttämättä $\Sigma \vdash \approx ct$ eli $t^M = c^M$. Koska $M \models \varphi(c/v_n)$, pätee myös $M \models \varphi(t/v_n)$. Siis $M \models \forall v_n \varphi$. □

Lause 8.14 (Gödelin täydellisyyslause) *Olkoon L numeroituva. Tällöin $\Sigma \vdash \varphi$ joss $\Sigma \models \varphi$.*

Tod. Lauseen 7.9 nojalla $\Sigma \vdash \varphi$ implikoi $\Sigma \models \varphi$. Olkoon siis $\Sigma \models \varphi$, mutta $\Sigma \not\vdash \varphi$. Saamme ristiriidan osoittamalla että $\Sigma \cup \{\neg\varphi\}$:llä on malli. Koska $\Sigma \cup \{\neg\varphi\}$ on ristiriidaton riittää todistaa seuraava lause:

Lause 8.15 (Löwenheim-Skolemin lause) *Jos Σ on ristiriidaton joukko L-lauseita ja L on numeroituva, niin Σ:lla on numeroituva malli.*

Todistus. Olkoon $L' = L \cup \{c_n \mid n \in \mathbb{N}\}$, missä vakiosymbolit c_n ovat uusia. Helposti nähdään, että Σ on ristiriidaton joukko L'-lauseita (Lause 2.18!). Soveltamalla peräkkäin Lemmaa 8.12 saadaan ristiriidaton Σ_1 siten, että kaikille φ ja $n \in \mathbb{N}$ on olemassa $c \in L' \setminus L$ siten, että $(\varphi(c/v_n) \to \forall v_n\varphi) \in \Sigma_1$. Lindenbaumin lemman nojalla on olemassa täydellinen L'-teoria $\Sigma^* \supseteq \Sigma_1$. Lauseen 8.13 nojalla Σ_1:llä on malli M^*. Olkoon M L'-struktuurin M^* redukti (kts. sivu 21) aakkostoon L. Silloin $M \models \Sigma$. □

Lauseella 8.15 on mullistavia seurauksia:

- Työläs todistusten keksiminen voidaan unohtaa. Riittää tutkia malleja.
- Malleja voidaan konstruoida muotoilemalla sopiva ristiriidaton teoria.

Lause 8.16 (Kompaktisuuslause) *Jos Σ on joukko L-lauseita siten, että jokaisella äärellisellä $\Sigma_0 \subseteq \Sigma$ on malli, niin Σ:lla on malli.*

Todistus. Jos Σ:lla ei ole mallia, niin Σ on Lauseen 8.15 nojalla ristiriitainen. Lemman 8.4 nojalla Σ:lla on äärellinen ristiriitainen osajoukko Σ_0. Mutta silloin Σ_0:lla ei korrektisuuslauseen nojalla voi olla mallia. □

Esimerkki 8.17 *Olkoon L numeroituva aakkosto ja Σ L-teoria siten, että jos $M \models \Sigma$, niin M on äärellinen. Tällöin on olemassa $n \in \mathbb{N}$ siten, että jos $M \models \Sigma$, niin M:ssä on $\leq n$ alkiota. Perustelu: Oletetaan, että jokaiselle $n \in \mathbb{N}$ on olemassa $M_n \models \Sigma$ siten, että M_n:ssä on $> n$ alkiota. Olkoon*

$$\varphi_n = \forall v_1 \ldots \forall v_n \exists v_{n+1}(\neg \approx v_{n+1}v_1 \wedge \ldots \wedge \neg \approx v_{n+1}v_n).$$

Siis $M_n \models \Sigma \cup \{\varphi_m \mid m \leq n\}$. Olkoon

$$\Sigma' = \Sigma \cup \{\varphi_m \mid m \in \mathbb{N}\}.$$

Nyt Σ':n jokaisella äärellisellä osajoukolla on malli. Kompaktisuuslauseen nojalla Σ':lla on malli M. Oletuksen mukaan M on äärellinen. Toisaalta $M \models \varphi_n$ kaikilla $n \in \mathbb{N}$. Saatu ristiriita osoittaa, että väite on tosi. □

Esimerkki 8.18 *Olkoon $L = \{\oplus, \otimes, <, 0, 1\}$ ja $\mathfrak{R} = \langle \mathbb{R}, Tul_{\mathfrak{R}} \rangle$, missä*

$$Tul_{\mathfrak{R}}(<) = \{\langle x, y\rangle \mid x < y\},$$
$$Tul_{\mathfrak{R}}(\otimes)(x, y) = x \cdot y, Tul_{\mathfrak{R}}(\oplus)(x, y) = x + y,$$
$$Tul_{\mathfrak{R}}(0) = 0, Tul_{\mathfrak{R}}(1) = 1.$$

Olkoon $\Sigma = Th(\mathfrak{R})$. Σ:lla on malli ja L on numeroituva, joten Σ:lla on numeroituva malli. Itse asiassa, algebrallisten reaalilukujen järjestetty kunta on Σ:n numeroituva malli.

Lause 8.19 *Olkoon L numeroituva. L-teoria Σ on täydellinen ja suljettu päättelyn suhteen (eli jos φ on L-lause ja $\Sigma \vdash \varphi$, niin $\varphi \in \Sigma$) joss on olemassa L-struktuuri M siten, että $\Sigma = Th(M)$.*

Todistus. 1. Oletetaan, että Σ on täydellinen ja suljettu päättelyn suhteen. Täydellisyyslauseen nojalla (oikeastaan 8.15:n nojalla) Σ:lla on malli M. Jos $\varphi \in \Sigma$, niin $\varphi \in Th(M)$. Jos taas $\varphi \in Th(M)$ ja $\varphi \notin \Sigma$, niin $\Sigma \nvdash \varphi$, joten $\Sigma \vdash \neg\varphi$ ja lopulta $\neg\varphi \in \Sigma$, mistä seuraa $\neg\varphi \in Th(M)$, ristiriita. Siis $\Sigma = Th(M)$.

2. Olkoon kääntäen $\Sigma = Th(M)$. Tietenkin Σ on suljettu päättelyn suhteen. Jos φ on L-lause, niin $\varphi \in Th(M)$ tai $\neg\varphi \in Th(M)$, joten $\Sigma \vdash \varphi$ tai $\Sigma \vdash \neg\varphi$ ja Σ on osoitettu täydelliseksi. □

Lause 8.20 *L-teoria Σ on täydellinen joss sen kaikki mallit ovat elementaarisesti ekvivalentteja.*

Todistus. 1. Olkoon Σ täydellinen ja $M \models \Sigma$, $M' \models \Sigma$. Jos $M \not\equiv M'$, niin on olemassa L-lause φ siten, että $M \models \varphi \not\Leftrightarrow M' \models \varphi$. Jos $\Sigma \vdash \varphi$, niin $M \models \varphi$ ja $M' \models \varphi$. Muuten $\Sigma \vdash \neg\varphi$, jolloin $M \not\models \varphi$ ja $M' \not\models \varphi$. Saatu ristiriita osoittaa, että $M \equiv M'$.

2. Olkoon Σ epätäydellinen. Siis on olemassa L-lause φ siten, että $\Sigma \nvdash \varphi$ ja $\Sigma \nvdash \neg\varphi$. Täydellisyyslauseen nojalla $\Sigma \not\models \varphi$ and $\Sigma \not\models \neg\varphi$. On siis olemassa $M \models \Sigma \cup \{\neg\varphi\}$ ja $M' \models \Sigma \cup \{\varphi\}$. Näin ollen $M \not\equiv M'$. □

L-teoria on $\aleph_0$-*kategorinen*, jos sen numeroituvat äärettömät mallit ovat isomorfisia. ($\aleph_0$ luetaan alef nolla)

Lause 8.21 (Łoś-Vaught) *Olkoon L numeroituva ja Σ $\aleph_0$-kategorinen L-teoria jolla ei ole äärellisiä malleja. Tällöin Σ on täydellinen.*

Todistus. Olkoot $M \models \Sigma$ ja $M' \models \Sigma$ (käytämme lausetta 8.20). Olkoon $\Sigma_1 = Th(M)$ ja $\Sigma_2 = Th(M')$. Lauseen 8.15 (Löwenheim-Skolemin lause) nojalla teorialla Σ_1 on numeroituva malli M_1 ja teorialla Σ_2 on numeroituva malli M_2. $\aleph_0$-kategorisuuden nojalla $M_1 \cong M_2$. Korollaarin 5.5 nojalla $M_1 \equiv M_2$. Nyt

$$M \equiv M_1 \equiv M_2 \equiv M',$$

joten $M \equiv M'$. □

Esimerkki 8.22 *Olkoon $L = \{\mathrm{R}\}$, missä $\#_L(\mathrm{R}) = 1$. Olkoot $M = \langle \mathbb{R}, Tul_M \rangle$ ja $M' = \langle \mathbb{Q}, Tul_{M'} \rangle$, missä $Tul_M(\mathrm{R}) = \mathbb{Q}$ ja $Tul_{M'}(\mathrm{R}) = \mathbb{N}$. Selvästi $M_1 \ncong M_2$, koska $\mathbb{R}$ on ylinumeroituva. Mutta $M \equiv M'$, sillä molemmat mallit ovat $\aleph_0$-kategorisen lausejoukon Σ malleja, kun Σ muodostuu lauseista*

$$\begin{aligned}\forall v_0 \ldots \forall v_n \exists v_{n+1} \exists v_{n+2} [& \neg \approx v_{n+1} v_0 \wedge \ldots \wedge \neg \approx v_{n+1} v_n \wedge \\ & \neg \approx v_{n+2} v_0 \wedge \ldots \wedge \neg \approx v_{n+2} v_n \wedge \\ & \mathrm{R} v_{n+1} \wedge \neg \mathrm{R} v_{n+2},]\end{aligned}$$

missä $n \in \mathbb{N}$. Σ on $\aleph_0$-kategorinen, koska sen numeroituvissa malleissa R ja $-R$ ovat numeroituvasti äärettömiä.

Tiheän järjestyksen teoria ilman reunapisteitä DLO on seuraavanlainen aakkoston $L = \{<\}$ $\#_L(<) = 2$ lausejoukko ($t < t'$ ja selvyyden vuoksi joskus myös $(t < t')$ ovat lyhenteitä kaavalle $< tt'$):

$$\begin{aligned}&\forall v_0 \neg (v_0 < v_0) \\ &\forall v_0 \forall v_1 \forall v_2 ((v_0 < v_1 \wedge v_1 < v_2) \rightarrow v_0 < v_2) \\ &\forall v_0 \forall v_1 (v_0 < v_1 \vee \approx v_0 v_1 \vee v_1 < v_0) \\ &\forall v_0 (\exists v_1 (v_0 < v_1) \wedge \exists v_1 (v_1 < v_0)) \\ &\forall v_0 \forall v_1 \exists v_2 (v_0 < v_1 \rightarrow (v_0 < v_2 \wedge v_2 < v_1)\end{aligned}$$

Lause 8.23 *Teoria DLO on $\aleph_0$-kategorinen.*

Tod. Olkoot M ja M' DLO:n numeroituvia malleja. Olkoon $M = \{d_n | n \in \mathbb{N}\}$ ja $M' = \{d'_n | n \in \mathbb{N}\}$. Olkoon $f_0 = \{\langle d_0, d'_0 \rangle\}$. Oletetaan, että on määritelty

$$f_n = \{\langle x_0, y_0 \rangle, \ldots, \langle x_{2n}, y_{2n} \rangle\}$$

ja

$$x_0 < x_1 < \ldots < x_{2n},\ y_0 <' y_1 <' \ldots <' y_{2n}$$

missä $<$ tarkoittaa relaatiota $Tul_M(<)$ ja $<'$ relaatiota $Tul_{M'}(<)$. Olkoon $d_m \in M \setminus \{x_0, \ldots, x_{2n}\}$ sellainen että m on minimaalinen. Nyt joko $d_m < x_0$ tai $x_i < d_m < x_{i+1}$ jollakin $i < 2n$ tai $x_{2n} < d_m$. Kussakin tapauksessa voidaan valita sellainen $y \in M' \setminus \{y_0, \ldots, y_{2n}\}$ että vastaavasti $y < y_0$ tai $y_i < y < y_{i+1}$ tai $y_{2n} < y$. Tulemme kuvaamaan alkion d_m alkiolle y. Nyt etsimme vastaavasti alkion M':sta ja valitsemme sille alkukuvan x. Olkoon $d'_k \in M' \setminus \{y_0, \ldots, y_{2n}, y\}$ sellainen että k on minimaalinen. Valitaan $x \in M \setminus \{x_0, \ldots, x_{2n}, d_m\}$ kuten y yllä. Lopuksi asetetaan

$$f_{n+1} = f_n \cup \{\langle d_m, y \rangle, \langle x, d'_k \rangle\}$$

Olkoon

$$f = \bigcup_{n=0}^{\infty} f_n.$$

Nyt

$$d_n \in dom(f_n) \subseteq dom(f)$$
$$d'_n \in ran(f_n) \subseteq ran(f)$$

Selvästi, $f : M \to M'$ on isomorfismi. □

Esimerkki 8.24 *Teorian DLO mallit* $M = \langle \mathbf{R}, Tul_M(<) \rangle$ *ja* $M' = \langle \mathbf{Q}, Tul_M(<) \rangle$,

$$Tul_M(<) = \{\langle x, y \rangle \in \mathbf{R}^2 | x < y\}$$
$$Tul_M(<) = \{\langle x, y \rangle \in \mathbf{Q}^2 | x < y\}$$

ovat elementaarisesti ekvivalentteja lauseen 8.23 ja lauseen 8.21 nojalla: $M \equiv M'$.

9 Lukuteoria

Lukuteorialla tarkoitetaan tässä luonnollisten lukujen $0, 1, 2, \ldots$ aritmeettisia ominaisuuksia eli yhteen- ja kertolaskun avulla esitettäviä ominaisuuksia. Hämmästyttävän suuri osa matematiikkaa palautuu lukuteoriaan. Esimerkiksi

$$\sqrt{2} > 1.414$$

voidaan esittää lukuteoreettisessa muodossa

$$\exists x(2 \cdot 10^6 = 1414^2 + x)$$

(voidaan valita $x = 604$). Sarjakehitelmien avulla tavanomaisia transsendenttisia funktioita $\sin(x)$, $\cos(x)$, $\ln(x)$ jne koskevat väitteet kääntyvät lukuteoreettisiksi väitteiksi. Myös logiikan keskeiset käsitteet, kuten todistuvuus, ristiriidattomuus, validisuus jne, kääntyvät lukuteorian kielelle. Tämän osoittaminen on esillä olevan luvun päätarkoitus. Sen jälkeen on mahdollista todistaa tärkeitä tuloksia lukuteorian rajoituksista.

Määritelmä 9.1 Lukuteorian aakkosto *on*

$$L = \{\oplus, \otimes, 0, 1, \exp\},\ \#_L(\oplus) = \#_L(\otimes) = \#_L(\exp) = 2.$$

Peanon aksioomat lukuteorialle *ovat*

(P1) $\forall v_0 \neg \approx \oplus v_0 1\ 0$

(P2) $\forall v_0 \forall v_1 (\approx \oplus v_0 1 \oplus v_1 1 \rightarrow \approx v_0 v_1)$

(P3) $\forall v_0 \approx \oplus v_0 0 v_0$

(P4) $\forall v_0 \forall v_1 \approx \oplus v_0 \oplus v_1 1 \oplus \oplus v_0 v_1 1$

(P5) $\forall v_0 \approx \otimes v_0 0\ 0$

(P6) $\forall v_0 \forall v_1 \approx \otimes v_0 \oplus v_1 1 \oplus \otimes v_0 v_1 v_0$

(P7) $\forall v_0 \approx \exp v_0 0\ 1$

(P8) $\forall v_0 \forall v_1 \approx \exp v_0 \oplus v_1 1\ \otimes v_0 \exp v_0 v_1$

(P9) $\forall v_{n_0} \cdots \forall v_{n_k} ((\varphi(0/v_0) \wedge \forall v_0 (\varphi \rightarrow \varphi(\oplus v_0 1/v_0))) \rightarrow \forall v_0 \varphi)$ *(Induktioskeema)*

missä φ käy läpi kaikki L-kaavat ja $v_{n_0} \dots v_{n_k}$ on φ:ssä vapaana esiintyvien muuttujien $\neq v_0$ luettelo. Merkitsemme Peanon aksioomien ääretöntä joukkoa kirjaimella P. **Lukuteorian standardimalli** *on $\mathcal{N} = \langle \mathbb{N}, Tul_{\mathcal{N}} \rangle$, missä*

$$Tul_{\mathcal{N}}(\oplus)(x, y) = x + y, \;\; Tul_{\mathcal{N}}(\otimes)(x, y) = x \cdot y$$

$$Tul_{\mathcal{N}}(\exp)(x, y) = x^y,$$

$$Tul_{\mathcal{N}}(0) = 0, \;\; Tul_{\mathcal{N}}(1) = 1$$

Lause 9.2 *$\mathcal{N} \vDash P$ ja P on siis ristiriidaton.*

Todistus. Vain induktioskeema ansaitsee oman tarkastelunsa. Olkoon φ L-kaava, jossa esiintyy vapaana $v_0, v_{n_0}, \cdots, v_{n_k}$. Olkoon $s : \mathbb{N} \to \mathbb{N}$. Olkoon

$$X = \{i \in \mathbb{N} \mid \mathcal{N} \vDash_{s(i/0)} \varphi\}$$

Oletetaan $\mathcal{N} \vDash_s (\varphi(0/v_0) \wedge \forall v_0(\varphi \to \varphi(\oplus v_0 1/v_0)))$. Siis $0 \in X$ ja $i + 1 \in X$ aina kun $i \in X$. Induktioperiaatteesta seuraa $X = \mathbb{N}$. Siis $\mathcal{N} \vDash_s \forall v_0 \varphi$. $\square$

Huom. Eräs matematiikan perusteiden kuuluisista kysymyksistä kuuluu, voidaanko lausejoukon P ristiriidattomuus todistaa "finitistisesti" eli ilman, että oletetaan äärettömän struktuurin $\mathcal{N}$ olemassaolo. Gödel todisti vuonna 1931, että teoria $\{\varphi \mid P \vdash \varphi\}$ on epätäydellinen ja että lausejoukon P ristiriidattomuutta ei voi todistaa pelkästään P:stä lähtemällä. Gentzen todisti vuonna 1943 lausejoukon P ristiriidattomuuden lausejoukkoa P vahvemmassa teoriassa.

Lause 9.3 *Teorialla P on malleja, jotka eivät ole isomorfisia $\mathcal{N}$:n kanssa. (Niitä sanotaan* **epästandardeiksi** *malleiksi.)*

Todistus. Olkoon $L' = \{\oplus,\ \otimes,\ \exp,\ 0,\ 1,\ c\}$, joka on muuten kuten L paitsi että c on uusi vakiosymboli. Olkoon Σ L'-lauseiden joukko, joka muodostuu P:n lauseista ja lauseista

$$\neg \approx c0\ ,\ \neg \approx c1\ ,\ \neg \approx c \oplus 1\ 1\ ,\ \neg \approx c \oplus \oplus 1\ 1\ 1\ ,\ \dots$$

eli jos merkitään

$$\mathrm{n{+}1} = \oplus \underline{n}\ 1$$

niin

$$\Sigma = P \cup \{\neg \approx c\underline{n} \mid n \in \mathbb{N}\}.$$

Jos $\Sigma_0 \subseteq \Sigma$ on äärellinen, niin on olemassa $k \in \mathbb{N}$ siten että

$$\Sigma_0 \subseteq P \cup \{\neg \approx c\underline{n} \mid n \in \mathbb{N},\ n < k\}.$$

Olkoon $\mathcal{N}'$ L'-struktuuri $\langle \mathbb{N}, \mathrm{Tul}_{\mathcal{M}} \rangle$ joka on muuten kuten $\mathcal{N}$ (eli $\mathcal{N}' \restriction L = \mathcal{N}$) mutta $\mathrm{Tul}_{\mathcal{N}'}(c) = k$. Tällöin $\mathcal{N}' \models \Sigma_0$. Kompaktisuuslauseen nojalla Σ:lla on malli $\mathcal{M}' = \langle M, \mathrm{Tul}_{L'} \rangle$. Erityisesti, jos $\mathcal{M} = \mathcal{M}' \restriction L$, niin $\mathcal{M} \models P$.

Väite $\mathcal{M} \ncong \mathcal{N}$

Todistus. Oletetaan $\pi : \mathcal{M} \cong \mathcal{N}$. Olkoon $m = \pi(\mathrm{Tul}_{\mathcal{M}'}(c))$. Jos $n \in \mathbb{N}$, niin

$$\mathcal{M}' \models \neg \approx c\underline{n}$$

joten isomorfisuuden nojalla $m \neq \mathrm{Tul}_{\mathcal{N}}(\underline{n})$. Mutta $\mathrm{Tul}_{\mathcal{N}}(n) = n$ joten valinta $n = m$ johtaa ristiriitaan. □

Lause 9.4 $P \vdash \forall v_0 \approx \oplus 0 v_0 v_0$.

Todistus. Täydellisyyslauseen nojalla riittää osoittaa $P \models \forall v_0 \approx \oplus 0 v_0 v_0$. Olkoon siis $\mathcal{M} = \langle M, \mathrm{Tul}_{\mathcal{M}} \rangle \models P$ ja $s : \mathbb{N} \to M$. Merkitään $\mathrm{Tul}_{\mathcal{M}}(\oplus) = +'$, $\mathrm{Tul}_{\mathcal{M}}(\otimes) =\cdot'$, $\mathrm{Tul}_{\mathcal{M}}(0) = 0'$ ja $\mathrm{Tul}_{\mathcal{M}}(1) = 1'$. Sovellamme induktiota (P7) kaavaan

$$\varphi =\approx \oplus 0 v_0 v_0.$$

$\varphi(0/v_0)$ on kaava $\approx \oplus 0\ 0\ 0$. $\mathcal{M} \models_s \varphi(0/v_0)$ seuraa aksioomasta (P3). Olkoon sitten $a \in M$ ja $\mathcal{M} \models_{s(a/0)} \varphi$. Siis $0' +' a = a$. $\varphi(\oplus v_0 1/v_0) =\approx \oplus 0 \oplus v_0 1 \oplus v_0 1$ joten $\mathcal{M} \models_{s(a/0)} \varphi(\oplus v_0 1/v_0)$ joss $0' +' (a +' 1') = a +' 1'$. Koska $\mathcal{M} \models$ (P4), on $0' +' (a +' 1') = (0' +' a) +' 1'$. Oletuksen nojalla saadaan $0' +' (a +' 1') = a +' 1'$. Koska a oli mielivaltainen, seuraa

$$\mathcal{M} \models \forall v_0 [\varphi \to \varphi(\oplus v_0 1/v_0)].$$

Koska $\mathcal{M} \models$ (P7), seuraa $\mathcal{M} \models \forall v_0 \varphi$. □

Lukuteorian todistukset perustuvat yleensä induktioon. Onkin epätriviaali tehtävä löytää lause φ siten että $\mathcal{N} \models \varphi$ mutta $P \nvdash \varphi$. Tällaisia φ kuitenkin on. Tämän päivän tutkijat yrittävät löytää tällaisia lauseita φ

mahdollisimman läheltä "tavallista" matematiikkaa, mutta toistaiseksi kaikissa esimerkeissä on jotain logiikkaan liittyvää. Kurt Gödel osoitti, että lausella $\varphi =$ "P on ristiriidaton" on tämä ominaisuus. Todistamme hieman heikomman väitteen: $\{\varphi \mid P \vdash \varphi\}$ on epätäydellinen teoria. Tätä varten tutkimme lukuteorian funktioiden määriteltävyyttä.

10 Primitiivirekursiiviset funktiot

Primitiivirekursiiviset funktiot ovat funktioita, joiden arvo annetuilla argumenteilla voidaan aina mekaanisesti laskea äärellisessä ajassa. Tarkastellaan esimerkiksi yhteenlaskua

$$\begin{aligned} x + 0 &= x \\ x + (y + 1) &= (x + y) + 1. \end{aligned}$$

tai kertolaskua

$$\begin{aligned} x \cdot 0 &= 0 \\ x \cdot (y + 1) &= (x \cdot y) + x. \end{aligned}$$

Yleinen muoto tämän tyyppiselle määrittelylle on:

$$\begin{aligned} f(x, 0) &= g(x) \\ f(x, y + 1) &= h(y, f(x, y), x). \end{aligned}$$

Nyt esimerkiksi $f(5, 3)$ voidaan laskea "rekursiivisesti":

$$\begin{aligned} f(5, 3) &= f(5, 2 + 1) \\ &= h(2, f(5, 2), 5) \\ &= h(2, f(5, 1 + 1), 5) \\ &= h(2, h(1, f(5, 1), 5), 5) \\ &= h(2, h(1, f(5, 0 + 1), 5), 5) \\ &= h(2, h(1, h(0, f(5, 0), 5), 5), 5) \\ &= h(2, h(1, h(0, g(5), 5), 5), 5) \end{aligned}$$

Jos vaikkapa $g(x) = x^2$ ja $h(y, z, x) = y + z + x$, niin

$$f(5, 3) = h(2, h(1, h(0, g(5), 5), 5), 5) = 2 + 1 + 0 + 25 + 5 + 5 + 5 = 43.$$

Rekursiivisesti määritellyillä funktioilla on merkitystä toisaalta tietokoneella laskettavan funktion mallina, toisaalta esimerkkeinä lukuteoriassa määriteltävistä funktioista.

Määritelmä 10.1 Primitiivirekursiiviset (p.r.) *funktiot määritellään seuraavasti:*

(PR1) Nollafunktio $Z(n) = 0$ *on primitiivirekursiivinen.*

(PR2) Seuraajafunktio $S(n) = n + 1$ *on primitiivirekursiivinen.*

(PR3) Projektiofunktio $Pr_i^n(x_1, \ldots, x_n) = x_i$ *on primitiivirekursiivinen, kun* $1 \leq i \leq n$

(PR4) Jos $f : \mathbb{N}^n \to \mathbb{N}$ *on primitiivirekursiivinen ja* $g_i : \mathbb{N}^m \to \mathbb{N}$ *ovat primitiivirekursiivisia kun* $1 \leq i \leq n$*, niin* **yhdistetty** *funktio*

$$h(x_1, \ldots, x_m) = f(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m))$$

on primitiivirekursiivinen.

(PR5) Jos $f : \mathbb{N}^n \to \mathbb{N}$ *on primitiivirekursiivinen ja* $g : \mathbb{N}^{n+2} \to \mathbb{N}$ *on primitiivirekursiivinen, niin* **rekursiolla saatu** *funktio*

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

on primitiivirekursiivinen. Tapauksessa $n = 0$ *määritelmä on seuraava*

$$\begin{cases} h(0) = a \text{ (vakio)} \\ h(y + 1) = g(y, h(y)) \end{cases}$$

Esimerkki 10.2 1° **Identtinen** *funktio* $id(x) = x$ *on primitiivirekursiivinen, sillä* $id(x) = Pr_1^1(x)$

2° *Jos* $f : \mathbb{N}^2 \to \mathbb{N}$ *on primitiivirekursiivinen, niin*

$$g(x, y) = f(y, x)$$

on primitiivirekursiivinen, sillä $g(x, y) = f(Pr_2^2(x, y),\ Pr_1^2(x, y))$.

3° **Yhteenlasku** $a(y, x) = y + x$ *on primitiivirekursiivinen, sillä*

$$\begin{cases} a(0, x) = x = id(x) \\ a(y + 1, x) = y + x + 1 = S(Pr_2^3(y, a(y, x), x)) \end{cases}$$

4° **Kertolasku** $b(y, x) = y \cdot x$ *on primitiivirekursiivinen, sillä*

$$\begin{cases} b(0, x) = 0 = Z(x) \\ b(y + 1, x) = b(y, x) + x = a(Pr_2^3(y, b(y, x), x), Pr_3^3(y, b(y, x), x)) \end{cases}$$

5° **Eksponenttifunktio** $c(y, x) = x^y$ *on primitiivirekursiivinen. (Harj.teht.)*

6° **Vakiofunktio** $C_k(x) = k$ *on primitiivirekursiivinen. (Harj.teht.)*

7° **Rajoitettu vähennyslasku**

$$x \dot{-} y = \begin{cases} x - y & jos\ x \geq y \\ 0 & jos\ x < y \end{cases}$$

on primitiivirekursiivinen. (Harj.teht.)

Määritelmä 10.3 *Relaatio* $R \subseteq \mathbb{N}^n$ *on primitiivirekursiivinen, jos sen karakteristinen funktio*

$$f_R(x_1, \ldots, x_n) = \begin{cases} 1, & jos\ \langle x_1, \ldots, x_n \rangle \in R \\ 0, & jos\ \langle x_1, \ldots, x_n \rangle \notin R \end{cases}$$

on primitiivirekursiivinen.

Esimerkki 10.4 1° *Relaatio* $R = \{0\}$ *(eli relaatio* $x = 0$*) on primitiivirekursiivinen, koska* $f_R(x) = 1 \dot{-} x$.

2° *Relaatio* $R = \{x \in \mathbb{N} \mid x > 0\}$ *on primitiivirekursiivinen, koska* $f_R(x) = 1 \dot{-} (1 \dot{-} x)$. *Merkitään* $sg(x) = f_R(x)$.

3° *Jos* $R \subseteq \mathbb{N}^n$ *ja* $S \subseteq \mathbb{N}^n$ *ovat primitiivirekursiivisia, niin* $\mathbb{N}^n \setminus R$, $R \cap S$ *ja* $R \cup S$ *ovat primitiivirekursiivisia, koska*

$$f_{\mathbb{N}^n \setminus R}(x_1, \ldots, x_n) = 1 \dot{-} f_R(x_1, \ldots, x_n)$$

$$f_{R \cap S}(x_1, \ldots, x_n) = f_R(x_1, \ldots, x_n) \cdot f_S(x_1, \ldots, x_n)$$

$$f_{R \cup S}(x_1, \ldots, x_n) = f_R(x_1, \ldots, x_n) + f_S(x_1, \ldots, x_n) \dot{-} f_R(x_1, \ldots, x_n) \cdot f_S(x_1, \ldots, x_n).$$

4° $R = \{\langle x, y \rangle \in \mathbb{N}^2 \mid x \leq y\}$ *on primitiivirekursiivinen, koska* $f_R(x, y) = 1 \dot{-} (x \dot{-} y)$

5° $x = y \Leftrightarrow x \leq y$ *ja* $y \leq x$ *joten* $x = y$ *on primitiivirekursiivinen.*

6° $x < y \Leftrightarrow x \leq y$ *ja* $x \neq y$ *joten* $x < y$ *on primitiivirekursiivinen.*

7° *Jos* $R_i \subseteq \mathbb{N}^n$, $1 \leq i \leq m$, *ovat primitiivirekursiivisia ja*

$$R_i \cap R_j = \varnothing \text{ kun } i \neq j \text{ ja } \bigcup_{i=1}^{m} R_i = \mathbb{N}^n$$

ja funktiot $f_i : \mathbb{N}^n \to \mathbb{N}$, $1 \leq i \leq m$, *ovat primitiivirekursiivisia, niin funktio*

$$h(x_1, \ldots, x_n) = \begin{cases} f_1(x_1, \ldots, x_n) & \text{jos } R_1(x_1, \ldots, x_n) \\ \vdots & \\ f_m(x_1, \ldots, x_n) & \text{jos } R_m(x_1, \ldots, x_n) \end{cases}$$

on primitiivirekursiivinen, sillä

$$h(x_1, \ldots, x_n) = \sum_{i=1}^{m} f_i(x_1, \ldots, x_n) \cdot f_{R_i}(x_1, \ldots, x_n).$$

8° *Jos* $f : \mathbb{N}^{n+1} \to \mathbb{N}$ *on primitiivirekursiivinen, niin*

$$g(x_1, \ldots, x_n) = \prod_{i=0}^{x_1} f(i, x_1, \ldots, x_n)$$

ja

$$h(x_1, \ldots, x_n) = \sum_{i=0}^{x_1} f(i, x_1, \ldots, x_n)$$

ovat primitiivirekursiivisia sillä jos

$$\begin{cases} g'(0, x_1, \ldots, x_n) = f(0, x_1, \ldots, x_n) \\ g'(y+1, x_1, \ldots, x_n) = g'(y, x_1, \ldots, x_n) \cdot f(y+1, x_1, \ldots, x_n) \end{cases}$$

niin

$$g(x_1, \ldots, x_n) = g'(x_1, x_1, \ldots, x_n)$$

ja jos

$$\begin{cases} h'(0, x_1, \ldots, x_n) = f(0, x_1, \ldots, x_n) \\ h'(y+1, x_1, \ldots, x_n) = h'(y, x_1, \ldots, x_n) + f(y+1, x_1, \ldots, x_n) \end{cases}$$

niin

$$h(x_1, \ldots, x_n) = h'(x_1, x_1, \ldots, x_n)$$

.

9° *Jos* $R \subseteq \mathbb{N}^{n+1}$ *on primitiivirekursiivinen, niin relaatio*

$$S = \{\langle x_1, \ldots, x_n \rangle \mid (\forall z \leq x_1)(\langle z, x_1, \ldots, x_n \rangle \in R)\}$$

on primitiivirekursiivinen, sillä

$$f_S(x_1, \ldots, x_n) = \prod_{i=0}^{x_1} f_R(i, x_1, \ldots, x_n).$$

Samoin

$$S = \{\langle x_1, \ldots, x_n \rangle \mid (\exists z \leq x_1)(\langle z, x_1, \ldots, x_n \rangle \in R)\}$$

on primitiivirekursiivinen, sillä

$$f_S(x_1, \ldots, x_n) = 1 \dot{-} (1 \dot{-} \sum_{i=0}^{x_1} f_R(i, x_1, \ldots x_n)).$$

10° *Jos* $R \subseteq \mathbb{N}^{n+1}$ *on primitiivirekursiivinen ja* $f : \mathbb{N}^n \to \mathbb{N}$ *on saatu* **rajoitetulla minimalisaatiolla** *R:stä, eli*

$$f(x_1, \ldots, x_n) = \begin{cases} \textit{pienin } z \leq x_1 \textit{ siten että } \langle z, x_1, \ldots, x_n \rangle \in R, \\ \textit{jos sellaisia on olemassa} \\ 0 \quad \textit{muuten} \end{cases}$$

niin f *on primitiivirekursiivinen, sillä jos*

$$f'(0, x_1, \ldots, x_n) = 0$$

$$f'(y+1, x_1, \ldots, x_n) = \begin{cases} f'(y, x_1, \ldots, x_n) \quad \textit{jos } (\exists u \leq y)(\langle u, x_1, \ldots, x_n \rangle \in R) \\ y+1 \quad \textit{jos } \langle y+1, x_1, \ldots, x_n \rangle \in R \textit{ ja} \\ \qquad\quad \neg(\exists u \leq y)(\langle u, x_1, \ldots, x_n \rangle \in R) \\ 0 \quad \textit{muuten} \end{cases}$$

niin

$$f(x_1, \ldots, x_n) = f'(x_1, x_1, \ldots, x_n).$$

11° *Olkoon* $[x]$ *reaaliluvun* x *kokonaisosa*

$f(x, y) = [x/y]$ *on primitiivirekursiivinen, koska*

$f(x, y) = (\mu z \leq x)(z \cdot y + y > x)$ *(Sovimme, että* $[n/0] = 0$*.)*

$g(x) = [\sqrt{x}\ ]$ *on primitiivirekursiivinen, koska*

$g(x) = (\mu z \leq x)((z+1)^2 > x)$

$h(x) = [^2 \log(x+1)]$ *on primitiivirekursiivinen, koska*

$h(x) = (\mu z \leq x)(2^{z+1} > x + 1)$ □

Parifunktioksi kutsumme primitiivirekursiivista funktiota

$$\pi(x, y) = \frac{1}{2}((x+y)^2 + 3x + y).$$

Tämä on bijektio $\mathbb{N}^2 \to \mathbb{N}$ (Harj.teht.) joten voimme määritellä projektiofunktiot

$$\rho(z) = (\mu x \leq z)(\exists y \leq z)(\pi(x, y) = z)$$

$$\sigma(z) = (\mu y \leq z)(\exists x \leq z)(\pi(x, y) = z)$$

ja

$$\rho(\pi(x,y)) = x,\ \sigma(\pi(x,y)) = y.$$

$\pi(x,y)$ siis **koodaa** luvut x ja y yhdeksi luvuksi. Funktiot ρ ja σ **purkavat** tämän koodin.

Tarvitsemme nyt joitakin tietoja lukuteoriasta. Kaikille $x \in \mathbb{N}$ ja $y \in \mathbb{N} \setminus \{0\}$ on olemassa yksikäsitteiset $q \in \mathbb{N}$ ja $r \in \mathbb{N}$ siten että seuraava **jakoidentiteetti** pätee:

$$\boxed{x = q \cdot y + r\ ,\ r < y.}$$

Luku r on **jakojäännös**. Merkitään $r = rm(x,y)$. Sovitaan $rm(x,0) = x$ kaikilla x. Jos $rm(x,y) = 0$, on y luvun x **tekijä** ja merkitään $y \mid x$, y **jakaa** x:n. Sovitaan $0 \nmid x$ kaikilla $x \neq 0$. Luonnollinen luku x on **alkuluku**, $x \in Pr$, jos sen tekijät ovat 1 ja x ja jos lisäksi $x > 1$. Luvut x ja y ovat **suhteellisia alkulukuja**, jos niillä ei ole muita yhteisiä tekijöitä kuin 1 ja lisäksi $x, y > 1$. Tällöin merkitään $\langle x,y\rangle \in RP$ (lyhenne sanoista *relative primes*).

Esimerkki 10.5 *Yllä määritellyt lukuteorian peruskäsitteet ovat kaikki primitiivirekursiivisia.*

1° *Jakojäännösfunktio* $rm(x,y)$ *on primitiivirekursiivinen, koska*

$$rm(x,y) = (\mu z \leq x)(\exists n \leq x)[(x = ny + z \text{ ja } z < y \text{ ja } y > 0)$$

$$\text{tai } (y = 0 \text{ ja } z = x)].$$

2° *Jaollisuusrelaatio* $y \mid x$ *on primitiivirekursiivinen, koska*

$$y \mid x \iff rm(x,y) = 0.$$

3° *Relaatio RP, eli "x ja y ovat suhteellisia alkulukuja", on primitiivirekursiivinen, koska*

$$\langle x,y\rangle \in RP \iff x > 1 \text{ ja } y > 1 \text{ ja ei } (\exists n \leq x)(n \mid x \text{ ja } n \mid y \text{ ja } n > 1).$$

4° *Alkulukujen joukko* Pr *on primitiivirekursiivinen, koska*

$$x \in Pr \iff x > 1 \text{ ja ei } (\exists n \leq x)(n \mid x \text{ ja } n > 1 \text{ ja } n < x).$$

Merkitään peräkkäisiä alkulukuja seuraavasti:

$$\begin{array}{lll} p_0 = 2 & p_3 = 7 & p_{100} = 547 \\ p_1 = 3 & p_4 = 11 & p_{101} = \cdots \\ p_2 = 5 & p_5 = 13 & \vdots \end{array}$$

Eräs matematiikan perustotuuksia on, että jokainen kokonaisluku $m > 0$ voidaan esittää yksikäsitteisesti alkulukujen tulona

$$m = 2^{a_0} \cdot 3^{a_1} \cdot \ \ldots \ \cdot p_k^{a_k},$$

missä $a_k \neq 0$, paitsi jos $m = 1$ jolloin $m = 2^0$. Tämä on luvun m **alkulukukehitelmä**. Se saadaan yksinkertaisesti jakamalla lukua m peräkkäin ensin 2:lla niin monta kertaa kuin jako menee tasan, sitten 3:lla, sitten 5:llä ja niin edelleen. Alkulukukehitelmän yksikäsitteisyyden vuoksi

$$a_i = (\mu z \leq m)(p_i^z \mid m \text{ ja } p_i^{z+1} \nmid m).$$

Käytämme alkulukukehitelmää mielivaltaisen lukujonon koodaamiseen. Jotta jonon pituuskin tulisi koodattua, lisäämme eksponentteihin aina ykkösen. Jonon

$$\langle a_0, \ldots, a_k \rangle$$

koodi on luku

$$m = 2^{a_0+1} \cdot 3^{a_1+1} \cdot \ \ldots \ \cdot p_k^{a_k+1}. \tag{6}$$

Kääntäen, jos $m > 1$ on annettu niin merkitään:

$$\begin{aligned} k &= \mathrm{len}(m) = (\mu z \leq m)(p_{z+1} \nmid m) \\ a_i &= (m)_i = (\mu z \leq m)(p_i^{z+2} \nmid m). \end{aligned}$$

Siis, jos $\langle a_0, \ldots, a_k \rangle \ \in \mathbb{N}^{k+1}$, niin

$$\begin{aligned} k &= \mathrm{len}(2^{a_0+1} \cdot \ldots \cdot p_k^{a_k+1}) \\ a_i &= \ (2^{a_0+1} \cdot \ldots \cdot p_k^{a_k+1})_i. \end{aligned}$$

Nyt voimme sekä koodata mielivaltaisen jonon

$$\langle a_0, \ldots, a_k \rangle$$

yhdeksi luvuksi m että purkaa mielivaltaisen luvun $m > 0$ jonoksi

$$\langle (m)_0, ..., (m)_{len(m)} \rangle.$$

Koodin purku on mielekästä vain jos m todella on muotoa (6). Erikoistapauksena määritellään $\text{len}(1) = \text{len}(0) = 0$ ja $(m)_i = 0$ kun $m = 0$ tai $m = 1$.

Esimerkki 10.6 *Koodaamisessa käytetyt funktiot ovat kaikki primitiivirekursiivisia:*

1° Funktio $n \mapsto p_n$ on primitiivirekursiivinen. (Harj.teht.)

2° Funktio $\text{len}(x)$ on primitiivirekursiivinen. Seuraa kohdasta 1°.

3° Funktio $\langle x, y \rangle \mapsto (x)_y$ on primitiivirekursiivinen. Seuraa kohdasta 1°.

Primitiivirekursiivisten funktioiden perhe on suljettu mutkikkaampienkin rekursiivisten määritelmien suhteen kuin vain (PR5) sivulla 62. Käytämme nyt koodausta tämän todistamiseen ja ensimmäiseksi tarkastelemme kahden funktion samanaikaista rekursiivista määritelmää:

Lemma 10.7 *(Kaksoisrekursio) Olkoon*

$$\begin{cases} f_1(0, x) = g_1(x) \\ f_2(0, x) = g_2(x) \\ f_1(y + 1, x) = h_1(y, f_1(y, x), f_2(y, x), x) \\ f_2(y + 1, x) = h_2(y, f_1(y, x), f_2(y, x), x) \end{cases}$$

missä g_1, g_2, h_1, h_2 ovat primitiivirekursiivisia Tällöin f_1 ja f_2 ovat primitiivirekursiivisia

Tod Seuraava menetelmä on usein hyödyllinen: määritellään *apufunktio*

$$f^*(y, x) = 2^{f_1(y,x)+1} \cdot 3^{f_2(y,x)+1}$$

ja osoitetaan, että f^* on primitiivirekursiivinen. Sen jälkeen

$$f_1(y, x) = (f^*(y, x))_0$$
$$f_2(y, x) = (f^*(y, x))_1$$

ovat primitiivirekursiivisia. Siis sen sijaan, että yrittäisimme osoittaa funktiot f_1 ja f_2 suoraan primitiivirekursiivisiksi, keskitymme apufunktioon f^* ja määrittelemme funktiot f_1 ja f_2 tämän avulla. Funktiolle f^* saamme seuraavat yhtälöt:

$$\begin{aligned} f^*(0,x) &= 2^{g_1(x)+1} \cdot 3^{g_2(x)+1} \\ f^*(y+1,x) &= 2^{f_1(y+1,x)+1} \cdot 3^{f_2(y+1,x)+1} \\ &= 2^{h_1(y,f_1(y,x),f_2(y,x),x)+1} \cdot 3^{h_2(y,f_1(y,x),f_2(y,x),x)+1} \\ &= 2^{h_1(y,(f^*(y,x))_0,(f^*(y,x))_1,x)+1} \cdot 3^{h_2(y,(f^*(y,x))_0,(f^*(y,x))_1,x)+1} \end{aligned}$$

Jos merkitään

$$g^*(x) = 2^{g_1(x)+1} \cdot 3^{g_2(x)+1}$$

ja

$$h^*(y,z,x) = 2^{h_1(x,(z)_0,(z)_1,x)+1} \cdot 3^{h_2(x,(z)_0,(z)_1,x)+1},$$

niin g^* ja h^* ovat primitiivirekursiivisia ja

$$\begin{aligned} f^*(0,x) &= g^*(x) \\ f^*(y+1,x) &= h^*(y, f^*(y,x), x) \end{aligned}$$

□

Toinen tavallista rekursiota mutkikkaampi määritelmä on esimerkiksi:

$$\begin{cases} h(0,x) = f_1(x) \\ h(1,x) = f_2(x) \\ h(y+2,x) = g(y, h(y,x), h(y+1,x), x). \end{cases}$$

Tässä esimerkissä funktion arvon $h(y,x)$ laskemiseksi on laskettava sekä $h(y-1,x)$ että $h(y-2,x)$, kun tavallisessa rekursiosäännössä

$$\begin{cases} h(0,x) = f(x) \\ h(y+1,x) = g(y, h(y,x), x). \end{cases}$$

funktion arvon $h(y,x)$ laskemiseksi on laskettava vain $h(y-1,x)$. Voidaan myös ajatella, että funktion arvon $h(y,x)$ laskemiseksi on laskettava $h([y/2]-1,x)$. Kaikkien tämänkaltaisten tapausten käsittelemiseksi todistamme yleisen yleisen tuloksen (Lause 10.8). Jos $f(y,x_1,\ldots,x_n)$ on funktio, niin merkitään

$$\tilde{f}(y,x_1,\ldots,x_n) = \prod_{i=0}^{y} p_i^{f(i,x_1,\ldots,x_n)+1}$$

jolloin siis

$$f(i, x_1, \ldots, x_n) = (\tilde{f}(y, x_1, \ldots, x_n))_i.$$

Huom Jos f on primitiivirekursiivinen, niin myös $\tilde{f}$ on primitiivirekursiivinen. Jos $\tilde{f}$ on primitiivirekursiivinen, niin f on.

Lause 10.8 *Jos*

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

missä g ja h ovat primitiivirekursiivisia, niin f on primitiivirekursiivinen.

Tod Riittää osoittaa, että $\tilde{f}$ on primitiivirekursiivinen.

$$\begin{cases} \tilde{f}(0, x_1, \ldots, x_n) = 2^{g(x_1,\ldots,x_n)+1} \\ \tilde{f}(y+1, x_1, \ldots, x_n) = \tilde{f}(y, x_1, \ldots, x_n) \cdot p_{y+1}^{h(y,\tilde{f}(y,x_1,\ldots,x_n),x_1,\ldots,x_n)+1} \end{cases}$$

□

Esimerkki 10.9 *Fibonacci lukujen jono määritellään seuraavasti:*

$$\begin{cases} a_0 = 0 \\ a_1 = 1 \\ a_{n+2} = a_n + a_{n+1} \end{cases}$$

Funktio $f(n) = a_n$ on primitiivirekursiivinen, sillä $f(0) = 0$ ja $f(n+1) = (\tilde{f}(n))_{n \dot{-} 1} + (\tilde{f}(n))_n + (1 \dot{-} n)$.

11 Rekursiiviset funktiot

Primitiivirekursiivisten funktioiden perhe todettiin suljetuksi rajoitetun minimalisaation suhteen. Rajoitettu minimalisaatio on eräänlainen etsintäoperaatio, kun tiedetään ehdoton yläraja sille kuinka suuria lukuja käydään läpi. Rekursiivisten funktioiden perhe yleistää tätä sen verran, että etsintä sallitaan, vaikka ei tiedettäisi ylärajaa, kunhan tiedetään, että ratkaisu löytyy. Ero voi vaikuttaa hiuksen hienolta, mutta itse asiassa rekursiivsten funktioiden perhe on paljon laajempi kuin primitiivirekursiivisten funktioiden perhe.

Olkoon $R \subseteq \mathbb{N}^{n+1}$ ja $f : \mathbb{N}^n \to \mathbb{N}$. Sanomme, että f on saatu **minimalisaatiolla** R:stä jos

1. Kaikilla $x_1, \ldots, x_n \in \mathbb{N}$ on olemassa y siten että $\langle y, x_1, \ldots, x_n \rangle \in R$
2. Kaikilla $x_1, \ldots, x_n \in \mathbb{N}$ pätee, että $f(x_1, \ldots, x_n)$ on pienin y siten että $\langle y, x_1, \ldots, x_n \rangle \in R$

Tällöin merkitään

$$\boxed{f(x_1, \ldots, x_n) = \mu y(\langle y, x_1, \ldots, x_n \rangle \in R)}$$

Määritelmä 11.1 ***Rekursiivisten funktioiden*** *perhe määritellään seuraavasti:*

1. $S, Pr_i^n, +, \cdot, \dot{-}, x^y$ *ovat rekursiivisia.*
2. *Yhdistämällä rekursiivisista funktioista saatu funktio on rekursiivinen.*
3. *Jos $R \subseteq \mathbb{N}^{n+1}$ on relaatio siten että f_R on rekursiivinen funktio (eli R on* ***rekursiivinen relaatio****) ja $f(x_1, \ldots, x_n) = \mu y(\langle y, x_1, \ldots, x_n \rangle \in R)$ niin f on rekursiivinen.*

Voidaaan heti havaita, että rekursiivisten funktioiden joukko sisältää relaatiot $x = y$, $x < y$ ja $x \leq y$ ja on suljettu konjukntion, disjunktion ja komplementin suhteen. Myös rajoitettu kvantifiointi säilyttää rekursiivisuuden koska

$$\begin{aligned}
&(\forall z \leq y)(\langle z, x_1, \ldots, x_n \rangle \in R) \iff \\
&(\mu z)(\langle z, x_1, \ldots, x_n \rangle \notin R \vee z = y + 1) = y + 1 \\
&(\exists z \leq y)(\langle z, x_1, \ldots, x_n \rangle \in R) \iff \\
&(\mu z)(\langle z, x_1, \ldots, x_n \rangle \in R \vee z = y + 1) < y
\end{aligned}$$

Näin ollen myös $rm(x, y)$, $\pi(x, y)$, $\rho(x, y)$ ja $\sigma(x, y)$ ovat rekursiivisia.

Huom. Jos $R = \{\langle y, x_1, \ldots, x_n \rangle \mid y = f(x_1, \ldots, x_n)\}$ on primitiivirekursiivinen, niin f ei ole välttämättä primitiivirekursiivinen, mutta se on rekursiivinen, koska $f(x_1, \ldots, x_n) = \mu y(\langle y, x_1, \ldots, x_n \rangle \in R)$.

Lause 11.2 *Jos*

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

missä g ja h ovat rekursiivisia, niin f on rekursiivinen.

Tod. Todistamme aluksi, että funktio $n \mapsto p_n$ on rekursiivinen. Koodaamme annetulla n ja jonon $p_0, p_1, ..., p_n$ yhdeksi luvuksi z:

$$z = 2^0 \cdot 3^1 \cdot ... \cdot p_n^n.$$

Nyt siis $b = p_n$ toteuttaa ehdot

$$b \text{ on alkuluku} \tag{7}$$

$$(n = 0 \text{ ja } b = 2) \text{ tai } (n > 0,\ 3|z,\ 3^2 \not| z) \tag{8}$$

Jos p ja q ovat peräkkäisiä alkulukuja, $p < q$ ja $i < n$, niin

$$p^i|z \iff q^{i+1}|z \tag{9}$$

$$b^n|z \text{ mutta ei } b^{n+1}|z \tag{10}$$

Olkoon R kolmikkojen $\langle z, b, n\rangle$ joukko, missä z b ja n toteuttavat yllä olevan ominaisuuden. On helppo nähdä (induktiolla) että R on rekursiivinen relaatio ja että kaikille n on olemassa yksi ja vain yksi z ja yksi ja vain yksi b jotka toteuttavat ehdon $\langle z, b, n\rangle \in R$. Nyt $p_n$on helppo laskea luvusta $(\mu z)(\exists y \leq z)R(z, y, n)$.

Palaamme nyt alkuperäiseen tehtävään ja käytämme hyväksi tietoa, että funktio $n \mapsto p_n$ on rekursiivinen: Koodaamme annetuilla y ja $\vec{x}$ jonon $f(0, \vec{x}), f(1, \vec{x}), \ldots, f(y, \vec{x})$ yhdeksi luvuksi z:

$$z = 2^{f(0,\vec{x})+1} \cdot 3^{f(1,\vec{x})+1} \cdot \ldots \cdot {p_y}^{f(y,\vec{x})+1}$$

Nyt siis

$$\begin{aligned} (z)_0 &= f(0, \vec{x}) \\ (z)_1 &= f(1, \vec{x}) \\ &\vdots \\ (z)_y &= f(y, \vec{x}) \end{aligned}$$

On selvää, että

$$f(y,\vec{x}) = (\mu z((z)_0 = g(\vec{x}) \wedge \forall i < y((z)_{i+1} = h(i,(z)_i,\vec{x}))))_y$$

Siis f on rekursiivinen. □

Lause 11.2 pätee myös jos määritelmän 11.1 kohdasta (1) jätetään funktio x^y pois. Tällöin ylläesitelty koodaus korvataan ns. *kiinalaisella jäännöslauseella*.

Olemme siis nähneet, että rekursiivisten funktioiden perhe on suljettu samojen operaatioiden suhteen kuin primitiivirekursiivistenkin funktioiden perhe. Lisäksi rekursiivisuus säilyy rajoittamattomassa minimalisaatiossa. Itse asiassa rekursiivisten funktioiden perhe on suljettu mutkikkaampien rekursiosääntöjen suhteen. Ackermannin funktio

$$\begin{aligned} A(0,x) &= x+1 \\ A(y+1,0) &= A(y,1) \\ A(y+1,x+1) &= A(y,A(y+1,x)) \end{aligned}$$

on esimerkki rekursiivisesta funktiosta, joka ei ole primitiivirekursiivinen.

Ns. *Churchin teesin* mukaan rekursiivisten funktioiden perhe on täsmälleen sama kuin ylipäätään tietokoneella laskettavien funktioiden perhe. Tällä teesillä on vahva empiirinen todistusaineisto: kaikki erilaiset yritykset määritellä tietokoneella laskettavan (tai mekaanisesti laskettavan) funktion käsite ovat osoittautuneet ekvivalenteiksi rekursiivisuuden käsitteen kanssa.

12 Määriteltävyys lukuteoriassa

Osoitamme tässä luvussa, että rekursiiviset funktiot ovat määriteltävissä (kts. määritelmä 5.7) lukuteorian standardimallissa. Yksinkertaisuuden vuoksi laajennamme lukuteorian aakkostoa eksponenttifunktiolla. Olkoon $L = \{\oplus, \otimes, 0, 1, \underline{exp}\}$, missä $\underline{exp}$ on 2-paikkainen funktiosymboli. Olkoon $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, \overline{exp})$, missä $\overline{exp}(n,m) = n^m$ ja $exp(0,0) = 1$.

Palautamme mieleen, että funktiota $f : M^n \to M$ sanotaan **määriteltäväksi** struktuurissa M (kts. määritelmä 5.7) jos relaatio

$$\{\langle x_1,\ldots,x_n,y\rangle | f(x_1,\ldots,x_n) = y\}$$

on määriteltävissä M:ssä.

Lause 12.1 *Olkoon L aakkosto ja M L-struktuuri. Struktuurissa M määriteltävien funktioiden perhe on suljettu yhdistämisen suhteen: Olkoot $f : M^n \to M$ ja $g_i : M^m \to M$ $(1 \leq i \leq n)$ määriteltäviä. Tällöin myös $h : M^m \to M$,*

$$h(x_1, \ldots, x_m) = f(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m))$$

on määriteltävä.

Tod. Olkoon φ L-kaava siten että

$$M \models_s \varphi \Longleftrightarrow f(s(0), \ldots, s(n-1)) = s(n)$$

ja ψ_i L-kaavoja $(1 \leq i \leq n)$ siten että

$$M \models_s \psi_i \Longleftrightarrow g_i(s(0), \ldots, s(m-1)) = s(m).$$

Kaavassa φ siis muuttuja v_n näyttelee funktion f arvon roolissa kun argumentit ovat $v_0, ..., v_{n-1}$. Vastaavasti, kaavassa ψ_i muuttuja v_m näyttelee funktion g_i arvon roolissa kun argumentit ovat $v_0, ..., v_{m-1}$. Nyt $h(a_0, ..., a_{m-1}) = a_m$ jos ja vain jos on olemassa luvut $b_0, ..., b_n$ siten, että kaikilla $i = 0, ..., n$ $g_i(a_0, ..., a_{m-1}) = b_i$ ja lisäksi $f(b_0, ..., b_n) = a_m$. Kirjoitamme saman predikaattilogiikassa. Etsimme aluksi muuttujia jotka eivät esiinny ym. kaavoissa. Olkoon sen vuoksi k suurempi kuin mikään j, jolla v_j esiintyy kaavoissa $\varphi, \psi_1, \ldots, \psi_n$.

$$\begin{array}{rcl} h(s(0), \ldots, s(m-1)) = s(m) & & \\ & \Longleftrightarrow & \\ M \models_s & \exists v_k \ldots \exists v_{k+n}(\varphi(v_k/v_0, \ldots, v_{k+n}/v_n) \wedge & \\ & \psi_1(v_k/v_m) \wedge & \\ & \psi_2(v_{k+1}/v_m) \wedge \ldots & \\ & \ldots \wedge \psi_n(v_{k+n-1}/v_m) \wedge & \\ & \approx v_{k+n}v_m) & \end{array}$$

□

Lause 12.2 *Mallissa $\mathcal{N}$ määriteltävien funktioiden ja relaatioiden perhe on suljettu minimalisaation suhteen: Jos $R \subseteq \mathbb{N}^{n+1}$ on määriteltävissä $\mathcal{N}$:ssä ja $f : \mathbb{N}^n \to \mathbb{N}$ siten että*

$$f(x_1, \ldots, x_n) = \mu y(\langle x_1, \ldots, x_n, y\rangle \in R)$$

niin f on määriteltävissä $\mathcal{N}$:ssä.

Tod. Olkoon φ lukuteorian kaava siten että

$$\mathcal{N} \models_s \varphi \Longleftrightarrow \langle s(0), \ldots, s(n) \rangle \in R$$

Olkoon k suurempi kuin mikään i, jolla v_i esiintyy φ:ssä. Nyt

$f(x_1, ..., x_n) = y \Longleftrightarrow (\langle x_1, \ldots, x_n, y \rangle \in R$ ja kaikille $z < y$ pätee$\langle x_1, \ldots, x_n, z \rangle \notin R)$

Siispä

$$f(s(0), \ldots, s(n-1)) = s(n) \Longleftrightarrow$$
$$\mathcal{N} \models_s \varphi \wedge \forall v_k(\exists v_{k+1} \approx \oplus \oplus v_k v_{k+1} 1 v_n \rightarrow \neg\varphi(v_k/v_n))$$

□

Lause 12.3 *Rekursiiviset funktiot ja relaatiot ovat määriteltävissä $\mathcal{N}$:ssä.*

Tod. Lähtöfunktiot Z, S, $+$, $\cdot$, Pr_i^n, $\dot{-}$ ja m^n ovat selvästi määriteltävissä, joten väite seuraa lauseista 12.1 ja 12.2. □

Aloitamme nyt prosessin, jota kutsutaan *Gödel-numeroinniksi.* Siinä liitetään predikaattilogiikan termeihin ja kaavoihin luonnollisia lukuja tietyllä yksikäsitteisellä tavalla. Näin voidaan soveltaa lukuteoriaa termeihin ja kaavoihin. Jos w on jono merkkejä

$$0, 1, \oplus, \otimes, \underline{exp}, \approx, (,), \rightarrow, \neg, \forall, v_i$$
$$w = w_0 \ldots w_k$$

niin w:n Gödel-luku $\ulcorner w \urcorner$ on luonnollinen luku

$$\ulcorner w \urcorner = {p_0}^{\#(w_0)+1} \cdot \ldots \cdot {p_k}^{\#(w_k)+1}$$

missä

$\#(0) = 0$	$\#(\approx) = 5$	$\#(\neg) = 9$
$\#(1) = 1$	$\#(() = 6$	$\#(\forall) = 10$
$\#(\oplus) = 2$	$\#()) = 7$	$\#(v_i) = 11 + i$
$\#(\otimes) = 3$	$\#(\rightarrow) = 8$	
$\#(\underline{exp}) = 4$		

Esimerkiksi

$$\ulcorner \approx v_0 v_1 \urcorner = 2^6 \cdot 3^{12} \cdot 5^{13} = 2767921875000000$$

$$\ulcorner \forall v_1 \approx \oplus v_0 v_1 v_2 \urcorner = 2^{11} \cdot 3^{13} \cdot 5^6 \cdot 7^3 \cdot 11^{12} \cdot 13^{13} \cdot 17^{14} =$$

$$28007936356982926935822353319130081970870987330120688960000000$$

Lause 12.4 *Joukko* $\mathrm{Trm} = \{\ulcorner t \urcorner \mid t \text{ L-termi}\}$ *on primitiivirekursiivinen.*

Tod. Seuraavat relaatiot ovat primitiivirekursiivisia:

$$\begin{aligned}
Nolla(x) &\iff x = \ulcorner 0 \urcorner \\
Yksi(x) &\iff x = \ulcorner 1 \urcorner \\
Muuttuja(x) &\iff x = \ulcorner v_i \urcorner \text{ jollakin } i \leq x \\
x * y = z &\iff len(z) = len(x) + len(y) + 1 \text{ ja} \\
&\quad\ (\forall i \leq len(x))((z)_i = (x)_i) \text{ ja} \\
&\quad\ (\forall i \leq len(y))((z)_{len(x)+i+1} = (y)_i) \\
Summa(x,y,z) &\iff z = \ulcorner \oplus \urcorner * x * y \\
Tulo(x,y,z) &\iff z = \ulcorner \otimes \urcorner * x * y \\
Exp(x,y,z) &\iff z = \ulcorner exp \urcorner * x * y
\end{aligned}$$

$x * y$ on ns. **jonotulo**[2]. Osoitamme nyt että f_{Trm} on primitiivirekursiivinen funktio. Huomaa että $f_{\mathrm{Trm}}(z) = 1$ joss

$Nolla(z)$ tai

$Yksi(z)$ tai

[2]Huomaa että

$$2^{a_0+1} \cdot \ldots \cdot p_n^{a_n+1} * 2^{a_{n+1}+1} \cdot \ldots \cdot p_m^{a_{n+m+1}+1} = 2^{a_0+1} \cdot \ldots \cdot p_{n+m+1}^{a_{n+m+1}+1}.$$

Esimerkiksi $288 * 10800 = 2^5 \cdot 3^2 * 2^4 \cdot 3^3 \cdot 5^2 = 2^5 \cdot 3^2 \cdot 5^4 \cdot 7^3 \cdot 11^2 = 7470540000$.

$Muuttuja(z)$ tai

$(\exists x \leq z)(\exists y \leq z)$

$Summa(x, y, z)$ tai
$Tulo(x, y, z)$ tai
$Exp(x, y, z))$ ja $f_{\mathrm{Trm}}(x) = f_{\mathrm{Trm}}(y) = 1)$.

Jos $x \leq z$, niin $f_{\mathrm{Trm}}(x) = (\tilde{f}_{\mathrm{Trm}}(z))_x$. Siis $f_{\mathrm{Trm}}(z) = 1 \iff Nolla(z)$ tai $Yksi(z)$ tai $Muuttuja(z)$ tai $(\exists x < z)(\exists y < z)((Summa(x, y, z)$ tai $Tulo(x, y, z)$ tai $Exp(x, y, z))$ ja $(\tilde{f}_{\mathrm{Trm}}(z))_x = (\tilde{f}_{\mathrm{Trm}}(z))_y = 1)$. Ekvivalenssin oikea puoli on muotoa:

$$\langle z - 1, \tilde{f}_{\mathrm{Trm}}(z - 1)\rangle \in R$$

missä R on primitiivirekursiivinen relaatio, koska x ja y yllä voidaan valita z:aa aidosti pienemmiksi, pätee

$$\begin{cases} f_{\mathrm{Trm}}(0) = 0 \\ f_{\mathrm{Trm}}(z + 1) = f_R(z, \tilde{f}_{\mathrm{Trm}}(z)) \end{cases}$$

Siis f_{Trm} on primitiivirekursiivinen □

Lause 12.5 *Joukko* $\mathrm{Fml} = \{\ulcorner\varphi\urcorner \mid \varphi$ *L-kaava*$\}$ *on primitiivirekursiivinen.*

Tod. Harjoitustehtävä. □

Määrittelemme nyt sijoitusoperaation joka on puhtaasti lukuteoreettinen, mutta "koodaa" merkkijonoilla tapahtuvan sijoittamisen. Olkoon $Sub \subseteq \mathbb{N}^3$ relaatio

$\langle x, y, z\rangle \in Sub \iff$ On olemassa jonot w ja w' siten että $x = \ulcorner w\urcorner$, $y = \ulcorner w'\urcorner$ ja w' on saatu w:stä korvaamalla jokainen v_0 symbolilla $\underline{z}$.

Lemma 12.6 *Ralaatio Sub on primitiivirekursiivinen*

Tod. Olkoon $E \subseteq \mathbb{N}$ primitiivirekursiivinen joukko

$$E = \{x \in \mathbb{N} | (\forall y \leq x)((x)_y \neq \#(v_0))\}$$

Nyt

$$\begin{aligned} \langle x, y, z \rangle \in Sub \quad \text{joss} \\ & (x \in E \text{ ja } x = y) \text{ tai} \\ & (\exists i < x)(\exists j < x)(\exists k < y)(\langle i, k, z \rangle \in Sub \\ & \text{ja } x = i * \ulcorner v_0 \urcorner * j \text{ ja } y = k * \ulcorner \underline{z} \urcorner * j \\ & \text{ja } j \in E) \end{aligned}$$

Funktio $z \mapsto \ulcorner \underline{z} \urcorner$ on selvästi primitiivirekursiivinen Siis Sub on. □

Pyrimme nyt osoittamaan, että lukuteorian lauseen φ Gödel-numeron ominaisuus "φ on tosi" ei ole määriteltävä ja sen vuoksi ei myöskään rekursiivinen. Lyhyesti sanottuna, totuus ei ole rekursiivisesti esitettävissä. Yhdistettynä Churchin teesiin (kts. sivu 11) tämä merkitsee sitä, että lukuteorian väitteiden totuutta ei voi mekaanisesti tarkistaa. Tämä Gödelin tulos vuodelta 1931 aiheutti suuren kohun, joka ei vieläkään ole laantunut.

Gödelin tuloksen takana on ikivanha totuuteen liittyvä paradoksi, ns. **valehtelijan paradoksi**. Mies sanoo valehtelevansa, puhuuko hän totta? Jos puhuu, niin hän valehtelee. Jos taas hän ei puhu totta, hän valehtelee ja siis puhuukin totta. Sama hieman toisin esitettynä: Tarkastellaan lausetta

$$\text{Lause (11) on epätosi.} \tag{11}$$

Onko lause (11) tosi vai epätosi? Jos se on tosi, se on epätosi. Jos se taas on epätosi, se on tosi. Emme pysty siis ratkaisemaan lauseen (11) totuutta. Tästä voi päätellä että lauseessa (11) on jotain vikaa.

Gödelin historiallinen saavutus oli korvata "epätosi" käsitteellä "todistumaton" ja osoittaa lauseen 12.3 avulla, että seuraavanlainen lause on todella olemassa:

$$\text{Lause (12) on todistumaton.} \tag{12}$$

Onko lause (12) todistuva? Jos se, se on korrektisuuslauseen nojalla tosi ja siis todistumaton. Niinpä (12) ei voi olla todistuva. Mutta silloin (11) onkin tosi. Olemme saanett esimerkin todesta lauseesta, jota ei voi todistaa.

Gödelin tuloksen todistus perustuu ns. Gödelin kiintopistelauseeseen (Lause 12.7). Siinä tarkastellaan mielivaltaista lukuteorian kaavaa φ, jossa

on yksi vapaa muuttuja v_0. Kaava φ ilmaisee siis jonkin muuttujan v_0 lukuteoreettisen ominaisuuden. Toisaalta v_0 voi itse olla arvoltaan jonkin lukuteorian lauseen ψ Gödel-luku. Siispä tässä tapauksessa φ ilmaisee jonkin lauseen ψ Gödel-luvun lukuteoreettisen ominaisuuden. Kiintopistelause sanoo, että ψ voidaan valita siten, että kun v_0 tulkitaan ψ:n Gödel-luvuksi, niin φ ilmaisee täsmälleen ominaisuuden ψ. Toisin sanottuna, lause $\varphi(\underline{\ulcorner\psi\urcorner}/v_0)$ sanoo saman asian kuin lause ψ:kin, kun $\underline{\ulcorner\psi\urcorner}$ tarkoittaa vakiotermiä $\overline{\oplus ... \oplus 01}$ ($\ulcorner\psi\urcorner$ kappaletta $\oplus$-merkkejä).

Matematiikassa on erilaisia kiintopistelauseita, esimerkiksi seuraava: Jos f on suljetun välin $[0,1]$ jatkuva funktio itselleen, niin on olemassa välin piste x siten että $f(x) = x$. Eräs tapa löytää sellainen x on seuraava: lasketaan $f(0), f(f(0)), f(f(f(0))), ...$ ja osoitetaan, että tämä suppenee jotakin pistettä x kohden. Sitten käytetään jatkuvuutta ja saadaan $f(x) = x$. Laskimellakin voi helposti löytää ratkaisun yhtälölle $\cos(x) = x$.

Logiikassa kiintopisteitä löydetään periaatteessa samalla tavalla, siis iteroimalla. Äärettömät lauseet eivät kuitenkaan ole sallittuja preidkaattilogiikassa. Sen korvaa eräänlainen sijoitusoperaatiolla aikaansaatava *diagonalisaatio*.

Lause 12.7 (Gödelin kiintopistelause) *Jos φ on lukuteorian kaava, niin on olemassa kaava ψ siten että kaikille $s : \mathbb{N} \to \mathcal{N}$.*

$$\mathcal{N} \models_s \psi \iff \mathcal{N} \models_s \varphi(\underline{\ulcorner\psi\urcorner}/v_0)$$

ja lisäksi kaavoilla ψ ja $\varphi(\underline{\ulcorner\psi\urcorner}/v_0)$ on samat vapaat muuttujat.

Tod. Olkoon σ kaava, jolle

$$\langle s(0), s(1), s(2)\rangle \in Sub \iff \mathcal{N} \models_s \sigma$$

Muista: $\langle \ulcorner w\urcorner, \ulcorner w'\urcorner, z\rangle \in Sub \iff w'$ saadaan korvaamalla jokainen v_0 w:ssä termillä $\underline{z}$. Voidaan olettaa, että v_0 ei esiinny sidottuna σ:ssa eikä v_0 tai v_1 φ:ssä. Olkoon θ kaava

$$\exists v_1(\varphi(v_1/v_0) \wedge \sigma(v_0/v_2)).$$

Kannattaa huomata, että

$$\mathcal{N} \models_{s(\ulcorner w\urcorner/0)} \theta \iff \mathcal{N} \models_{s(\ulcorner w'\urcorner/0)} \varphi,$$

missä w' on saatu w:stä korvaamalla v_0 termilla $\underline{\ulcorner w \urcorner}$. Olkoon $k = \ulcorner \theta \urcorner$ ja $\psi = \theta(\underline{k}/v_0)$. Nyt

$$\begin{aligned}
\mathcal{N} \models_s \psi &\iff \mathcal{N} \models_s \theta(\underline{k}/v_0) \\
&\iff \mathcal{N} \models_{s(\ulcorner \theta \urcorner/0)} \theta \\
&\iff \mathcal{N} \models_{s(\ulcorner w' \urcorner/0)} \varphi, \text{ missä } w' \text{ saadaan } \theta\text{:sta} \\
&\qquad \text{korvaamalla } v_0 \text{ termillä } \underline{\ulcorner \theta \urcorner} (= \underline{k}) \\
&\iff \mathcal{N} \models_{s(\ulcorner \psi \urcorner/0)} \varphi \\
&\iff \mathcal{N} \models_s \varphi(\underline{\ulcorner \psi \urcorner}/v_0)
\end{aligned}$$

□

Lause 12.8 (Tarskin lause) *Joukko* $\mathrm{Tr} = \{\ulcorner \psi \urcorner \mid \psi$ *on L-lause ja* $\mathcal{N} \models \psi\}$ *ei ole määriteltävissä* $\mathcal{N}$*:ssä.*

Tod. Oletetaan, että olisi olemassa L-kaava φ siten että $s(0) \in \mathrm{Tr} \iff \mathcal{N} \models_s \varphi$ [3]. Gödelin kiintopistelauseen nojalla on olemassa L-kaava ψ siten että $\mathcal{N} \models_s \psi \iff \mathcal{N} \models_s \neg\varphi(\underline{\ulcorner \psi \urcorner}/v_0)$. Olkoon $s(0) = \ulcorner \psi \urcorner$. Koska ψ on L-lause pätee

$$\begin{aligned}
\mathcal{N} \models_s \psi &\iff \ulcorner \psi \urcorner \in \mathrm{Tr} \\
&\iff s(0) \in \mathrm{Tr} \\
&\iff \mathcal{N} \models_s \varphi \\
&\iff \mathcal{N} \models_s \varphi(\underline{\ulcorner \psi \urcorner}/v_0), \text{ koska } s(0) = \ulcorner \psi \urcorner \\
&\iff \mathcal{N} \not\models_s \psi
\end{aligned}$$

ristiriita. □

Korollaari 12.9 Tr *ei ole rekursiivinen joukko.*

Tod. Lause 12.3! □

[3] Voidaan olettaa että φ:n ainoa vapaa muutuja on v_0.

13 Rekursiivisesti numeroituvat joukot

Rekursiivinen joukko on intuitiivisesti ajatellen sellainen joukko, että mistä tahansa luonnollisesta luvusta voidaan mekaanisesti äärellisessä ajassa ratkaista kuuluuko se tähän joukkoon vai ei. Toisin sanottuna, rekursiivisen joukon karakteristinen funktio on mekaanisesti (algoritmisesti) laskettavissa. Rekursiivisesti numeroituvat joukot ovat sellaisia, että meillä on jälleen mekaaninen algoritmi tarkastaa kuuluuko annettu luku joukkoon vai ei, mutta tämä mekaaninen algoritmi ei välttämättä pysähdy. Sama toisin sanoin: voimme alkaa luetella joukon alkioita, mutta ne eivät välttämättä tule suuruusjärjestyksessä ja niinpä emme tiedä pulpahtaako esimerkiksi 15 esiin tässä luettelossa kohta, pitkän ajan kuluttua vai ei koskaan.

Määritelmä 13.1 *Joukko $A \subseteq \mathbb{N}$ on **rekursiivisesti numeroituva** (lyh. r.n.), jos $A = \emptyset$ tai on olemassa rekursiivinen funktio $f : \mathbb{N} \to \mathbb{N}$ siten että*

$$A = \{f(n) \mid n \in \mathbb{N}\}.$$

Huom. Kysymys $m \in A$? voidaan ratkaista laskemalla $f(0), f(1)$,... kunnes $f(n) = m$, jos $m \in A$. Mutta jos $m \notin A$, on laskettava kaikki äärettömän monta arvoa $f(0), f(1)$,... ennen kuin vastaus $m \notin A$ selviää.

Lause 13.2 *Jokainen rekursiivinen joukko on rekursiivisesti numeroituva.*

Tod. Olkoon $A \neq \emptyset$ rekursiivinen eli f_A on rekursiivinen funktio. Olkoon $a \in A$ mielivaltainen. Asetetaan

$$f(n) = \begin{cases} n, & \text{jos } f_A(n) = 1 \\ a, & \text{jos } f_A(n) = 0 \end{cases}$$

Nyt f on rekursiivinen ja $A = \{f(n) \mid n \in \mathbb{N}\}$. □

Lause 13.3 *Olkoon $A \subseteq \mathbb{N}$. Seuraavat ehdot ovat ekvivalentteja:*

(1) A on rekursiivinen.
(2) A ja $\mathbb{N} \setminus A$ ovat rekursiivisesti numeroituvia

Tod. (1) $\Rightarrow$ (2) seuraa Lauseesta 13.2 koska rekursiivisen joukon komplementti on aina rekursiivinen.
(2) $\Rightarrow$ (1). Olkoon

$$A = \{f(n) \mid n \in \mathbb{N}\}$$
$$\mathbb{N} \setminus A = \{g(n) \mid n \in \mathbb{N}\}$$

missä f ja g ovat rekursiivisia. Jos

$$h(n) = \mu m(f(m) = n \text{ tai } g(m) = n)$$

niin h on rekursiivinen ja

$$n \in A \Longleftrightarrow f(h(n)) = n,$$

joten A on rekursiivinen. □

Lause 13.4 *Rekursiivisesti numeroituvien joukkojen perhe on suljettu yhdisteen ja leikkauksen suhteen.*

Tod. Ensin:

Lemma 13.5 *Joukko $A \subseteq \mathbb{N}$ on rekursiivisesti numeroituva jos ja vain jos on olemassa rekursiivinen relaatio $R \subseteq \mathbb{N} \times \mathbb{N}$ siten että*

$$(*) \qquad n \in A \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, m\rangle \in R)$$

Tod. Olkoon aluksi $A \subseteq \mathbb{N}$ rekursiivisesti numeroituva, esim.

$$A = \{f(n) \mid n \in \mathbb{N}\}$$

missä f on rekursiivinen. Olkoon

$$R = \{\langle n, m\rangle \mid f(m) = n\}.$$

Nyt R on rekursiivinen ja $(*)$ pätee.
Olkoon kääntäen R rekursiivinen siten että $(*)$ pätee. Olkoon $a \in A$ ja

$$f(n) = \begin{cases} \rho(n) & \text{jos } \langle \rho(n), \sigma(n)\rangle \in R \\ a & \text{muuten} \end{cases}$$

Nyt f on rekursiivinen. Jos $n \in \mathbb{N}$ ja $\langle \rho(n), \sigma(n) \rangle \in R$, niin $(*)$ nojalla $\rho(n) \in A$ eli $f(n) \in A$. Jos taas $n \in A$ ja $\langle n, m \rangle \in R$ niin $n = f(\pi(n, m))$. Siis

$$A = \{f(n) \mid n \in \mathbb{N}\}.$$

□

Korollaari Rekursiivisesti numeroituvat joukot ovat määriteltävissä $\mathcal{N}$:ssä.

Palataan Lauseen 14.4 todistukseen. Olkoon

$$n \in A \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, m \rangle \in R)$$
$$n \in B \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, m \rangle \in R').$$

Tällöin

$$n \in A \cup B \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, m \rangle \in R \text{ tai } \langle n, m \rangle \in R')$$
$$n \in A \cap B \Longleftrightarrow (\exists m \in \mathbb{N})(\langle n, \rho(m) \rangle \in R \text{ ja } \langle n, \sigma(m) \rangle \in R').$$

□

Lause 13.6 *Joukko*

$$\text{Thm} = \{\ulcorner \varphi \urcorner \mid P \vdash \varphi,\ \varphi \textit{ lukuteorian lause } \}$$

on rekursiivisesti numeroituva.

Tod. Olkoon Prf sellaisten lukujen joukko m joukko, että

$$\langle (m)_0, (m)_1, ...(m)_{len(m)} \rangle$$

on todistus.
Apuväite: Prf on primitiivirekursiivinen
Tod. Tarvitsemme sarjan havaintoja, joista jokainen on todistettavissa jo läpikäydyillä menetelmillä, joskin siinä on paljon vaivaa:

(1^0) $\mathrm{PeAx} = \{\ulcorner\varphi\urcorner \mid \varphi$ on Peanon aksioomien joukossa $\}$ on p.r.
(2^0) $\mathrm{PrAx} = \{\ulcorner\varphi\urcorner \mid \varphi$ on propositiologiikan aksiooma $\}$ on p.r.
(3^0) $\mathrm{IdAx} = \{\ulcorner\varphi\urcorner \mid \varphi$ on L-identiteettiaksiooma $\}$ on p.r.
(4^0) $\mathrm{KvAx} = \{\ulcorner\varphi\urcorner \mid \varphi$ on L-kvanttoriaksiooma $\}$ on p.r.
(5^0) $\mathrm{MP} = \{\langle\ulcorner\varphi\urcorner, \ulcorner(\varphi \to \psi)\urcorner, \ulcorner\psi\urcorner\rangle \mid \varphi, \psi$ lukuteorian kaavoja $\}$ on p.r.
(6^0) $\mathrm{Yl} = \{\ulcorner(\varphi \to \psi)\urcorner, \ulcorner(\varphi \to \forall v_j\psi)\urcorner \mid \varphi, \psi$ lukuteorian kaavoja ja v_j ei vapaa φ:ssa $\}$ on p.r.
(7^0) $\mathrm{Lau} = \{\ulcorner\varphi\urcorner \mid \varphi$ on lukuteorian kielen lause $\}$ on p.r.

Nyt

$$\begin{aligned} m \in \mathrm{Prf} \iff\ & \forall i \le len(m)((m)_i \in \mathrm{PeAx} \text{ tai } (m)_i \in \mathrm{PrAx} \text{ tai } (m)_i \in \mathrm{IdAx} \\ & \text{tai } (m)_i \in \mathrm{KvAx} \text{ tai} \\ & (\exists j \le i)(\exists k \le i)(\langle (m)_j, (m)_k, (m)_i\rangle \in \mathrm{MP}) \\ & \text{tai } (\exists j \le i)(\langle (m)_j, (m)_i\rangle \in \mathrm{Yl})). \end{aligned}$$

Lopuksi itse lauseen todistus:

$$n \in \mathrm{Thm} \iff \exists m(m \in \mathrm{Prf} \text{ ja } (m)_{len(m)} = n \text{ ja } n \in \mathrm{Lau}).$$

□

Korollaari 13.7 *On olemassa lukuteorian tosi lause, joka ei ole todistuva Peanon aksioomista.*

Tod. Määrittelimme Tarskin lauseessa joukon

$$\mathrm{Tr} = \{\ulcorner\varphi\urcorner \mid \mathbb{N} \models \varphi,\ \varphi \text{ lukuteorian lause } \}$$

ja osoitimme, että Tr ei ole määriteltävissä $\mathbb{N}$:ssä. Siis $\mathrm{Thm} \neq \mathrm{Tr}$. Korrektisuuslauseen nojalla $\mathrm{Thm} \subseteq \mathrm{Tr}$. Siis $\mathrm{Tr} \setminus \mathrm{Thm} \neq \emptyset$. □

Lause 13.8 (Gödelin 1. epätäydellisyyslause) *Peanon aksioomien teoria P on epätäydellinen eli on olemassa lukuteorian lause φ siten että $P \nvdash \varphi$ ja $P \nvdash \neg\varphi$.*

Tod. Korollaarin 13.7 nojalla on olemassa tosi lause φ siten että $P \nvdash \varphi$. Jos $P \vdash \neg\varphi$, niin $\mathbb{N} \models \neg\varphi$ eikä φ olekaan tosi. Siis $P \nvdash \neg\varphi$. $\square$

Lauseesta 13.8 seuraa että P:llä on kaksi mallia M_1 ja M_2 joista toisessa φ on tosi ja toisessa epätosi. P:n kaikki mallit eivät siis ole elementaarisesti ekvivalentteja eli epästandardimalleilla on lukuteoreettisia ominaisuuksia joita standardimallilla $\mathbb{N}$ ei ole.

Lauseen 13.6 nojalla on olemassa lukuteorian kaava Bew jossa on vapaana vain v_0 ja jolle pätee

$$s(0) \in \mathrm{Thm} \Longleftrightarrow \mathcal{N} \models_s Bew$$

eli jos φ on lukuteorian kielen lause, niin

$$P \vdash \varphi \Longleftrightarrow \mathcal{N} \models Bew(\underline{\ulcorner\varphi\urcorner}/v_0).$$

Gödelin kiintopistelauseen nojalla on olemassa lause ψ siten että (valitaan $\varphi = \neg Bew$):

$$\mathcal{N} \models \psi \Longleftrightarrow \mathcal{N} \models \neg Bew(\ulcorner\psi\urcorner/v_0).$$

Jos $P \vdash \psi$, niin $\mathcal{N} \models Bew(\underline{\ulcorner\psi\urcorner}/v_0)$, joten $\mathcal{N} \models \neg\psi$. Koska toisaalta $P \vdash \psi$ implikoi $\mathcal{N} \models \psi$, saadaan tulos

$$P \vdash \psi \Longrightarrow \mathcal{N} \models (\psi \wedge \neg\psi).$$

Siis $P \nvdash \psi$ eli $\mathcal{N} \models \neg Bew(\underline{\ulcorner\varphi\urcorner}/v_0)$

$$\text{eli } \mathcal{N} \models \psi.$$

Siis ψ on esimerkki todesta lauseesta, joka ei ole todistuva. Huomaa että

$$\psi \text{ sanoo " } \psi \text{ ei ole todistuva"}$$

eli ψ on eräs versio valehtelijan paradoksista.

Tiedämme, että P on ristiriidaton koska $\mathcal{N} \models P$. P:n ristiriidattomuus on ekvivalentti väitteen $P \nvdash \approx 0\,1$ kanssa (koska $P \vdash [\varphi \wedge \neg\varphi] \leftrightarrow \approx 0\,1$, olipa φ mikä kaava tahansa. Mutta

$$P \nvdash \approx 0\,1 \Longleftrightarrow \mathcal{N} \models \neg Bew(\ulcorner \approx 0\,1\urcorner/v_0)$$

minkä vuoksi otamme lauseelle $\neg Bew(\underline{\ulcorner \approx 0\,1\urcorner}/v_0)$ oman lyhenteen

$$Con(P)$$

joka tulee enlanninkielen sanasta “consistency” eli ristiriidattomuus.

Lause 13.9 (Gödelin 2. epätäydellisyyslause) *Peanon aksioomien ristiriidattomuus ei ole todistuva Peanon aksioomista eli $Con(P)$ on tosi lause jolle pätee*

$$P \nvdash Con(P)$$

Tod. (hahmotelma) Olkoon ψ kuten yllä. Kuten yllä, jos $P \vdash \psi$, niin $\mathcal{N} \models Bew(\underline{\ulcorner\psi\urcorner}/v_0)$. Tutkimalla lauseen 13.6 todistusta tarkkaan, voi osoittaa, että $P \vdash \psi$ implikoi jopa $P \vdash Bew(\underline{\ulcorner\psi\urcorner}/v_0)$. Tutkimalla Gödelin kiintopistelauseen todistusta tarkkaan, voi havaita, että jopa

$$P \vdash (\psi \leftrightarrow \neg Bew(\underline{\ulcorner\psi\urcorner}/v_0)).$$

Siis $P \vdash \psi$ implikoi $P \vdash \neg\psi$ eli $P \vdash \psi$ implikoi $P \vdash [\psi \wedge \neg\psi]$ eli $P \vdash\approx 01$ eli $\mathcal{N} \models \neg Con(P)$. Tämä päättely voidaan tehdä kokonaisuudessaan P:ssä, jolloin saadaan

$$P \vdash Bew(\underline{\ulcorner\psi\urcorner}/v_0) \rightarrow \neg Con(P)$$

eli

$$P \vdash Con(P) \rightarrow \neg Bew(\underline{\ulcorner\psi\urcorner}/v_0)$$

eli

$$P \vdash Con(P) \rightarrow \psi.$$

Jos siis $P \vdash Con(P)$, niin $P \vdash \psi$, vastoin aiemmin todistettua tietoa $P \nvdash \psi$. □

Gödelin 2. epätäydellisyyslause pätee kaikille matematiikan aksioomajoukoille jotka ovat riittävän yksinkertaisesti esitettyjä, jotta Lause 13.6 voidaan todistaa ja riittävän vahvoja jotta lukuteorian perusasiat ovat todistuvia. Misään tällaisessa aksioomasysteemissä ei voi todistaa sen omaa ristiriidattomuutta. Tämä voidaan tulkita (löysästi) siten, että matematiikassa ei voi koskaan todistaa matematiikan ristiriidattomuutta.

Lauseella 13.8 on sellainen mielenkiintoinen seuraus, että P:llä on epästandardimalli M jossa pätee

$$M \models \neg Con(P)$$

eli

$$M \models Bew(\underline{\ulcorner\approx 01\urcorner}/v_0).$$

Siis on olemassa M:n alkio t joka toteuttaa M:ssä kaikki todistuksen ehdot ja t:n viimeinen alkio on lause ≈ 01. Löysästi puhuen, M:ssä voidaan todistaa että $0 = 1$ mutta todistus on (ehkä) äärettömän pitkä.

Loppu