Φ # Logiikka I Ψ

Kaarlo Reipas

17. huhtikuuta 2012

Tämä materiaali on vielä keskeneräinen.

Sisältö

1 Johdanto

Tämä materiaali seuraa rakenteeltaan ja sisällöltään jossain määrin Hannele Salmisen ja Jouko Väänäsen kirjaa *Johdatus logiikkaan*.

1.1 Mitä logiikka on?

Siinä missä esimerkiksi matematiikka etsii vastauksia matemaattisiin kysymyksiin, logiikka tutkii kysymyksiä itsessään. Minkälaisia asioita ylipäätään voidaan kysyä, ja miten näihin kysymyksiin voidaan saada vastauksia?

Logiikan perustavin käsite on *lause*, eli väittämä. Lauseet ovat merkkijonoja, joilla pyritään ilmaisemaan jotakin asiaintilaa, väitteitä jotka voivat olla joko totta tai epätotta tilanteesta riippuen. Esimerkiksi suomenkielinen lauseet

$$\text{Aurinko paistaa.} \tag{1}$$
$$\text{Vettä sataa.} \tag{2}$$

ovat totta jos aurinko paistaa tai jos vettä sataa. Lause

Aurinko paistaa ja vettä sataa.

on taas totta jos sekä lauseet 1 että 2 ovat totta. Jotkin lauseet ovat totta riippumatta siitä, minkälainen sää ulkona on. Esimerkiksi

Joko aurinko paistaa tai se ei paista.

selvästi pitää paikkansa aina. Pitääkö lause *Muista tuoda kaupasta piimää!* paikkaansa? Onko se ylipäätään lause? Entä lause *Enksd dfvj hihihihi.*? Jotta voimme puhua ja todistaa lauseita ja niiden totuutta koskevia väittämiä, pitää meidän määritellä formaalisti, mitä lauseet ylipäätänsä ovat.

Lauseen käsitteelle on useita eri tilanteisiin sopivia määritelmiä. *Propositiologiikan lause* on näistä kenties yksinkertaisin. *Predikaattilogiikan lause* on hieman monimutkaisempi käsite, joka sallii propositiologiikkaa rikkaamaan semantiikan, eli *mallit*, joissa lauseet voivat päteä tai olla pätemättä. Mallin käsite on hyvin yleinen, ja kattaa esimerkiksi algebralliset struktuurit ja erilaiset tietokannat.

Kappaleessa 2 määrittelemme propositiolauseet, näiden totuuden sekä todistuksen. Lisäksi tutkimme lauseiden rakennetta ja käymme läpi totuuteen liittyviä apuvälineitä, kuten semanttiset puut ja totuusfunktiot. Lisäksi todistamme totuuden ja todistuvuuden yhteyteen liittyviä lauseita.

Kappaleessa 3 määrittelemme predikaattilogiikan kaavat ja lauseet, näiden semantiikan eli mallit, sekä totuuden ja todistuksen. Lisäksi tutkimme näihin liittyviä käsitteitä ja todistamme totuuden ja todistuvuuden yhteyteen liittyviä lauseita.

2 Propositiologiikka

Tässä kappaleessa määrittelemme propositiologiikan lauseet, niiden syntaksin ja semantiikan, totuuden sekä todistuksen käsitteen. Todistamme *propositiologiikan eheyslauseen* sekä *propositiologiikan täydellisyyslauseen.*

2.1 Lauseet

Määrittelemme seuraavaksi propositiologiikan lauseet, jotka ovat kenties yksinkertaisin mahdollinen lauseen formalisaatio. Tästä syystä niillä ei myöskään voi ilmaista kovin monimutkaisia asioita, hienosti ilmaistuna *niillä ei ole kovin rikasta semantiikkaa.*

Symboleja $p_0, p_1, p_2, \ldots$ sanotaan **propositiosymboleiksi**. Seuraavia symboleja sanotaan **konnektiiveiksi**:

$\neg$	negaatio (... ei päde)
$\wedge$	konjunktio (sekä ... että ... pätee)
$\vee$	disjunktio (ainakin toinen lauseista ... ja ... pätee)
$\rightarrow$	implikaatio (mikäli ... pätee, niin ...)
$\leftrightarrow$	ekvivalenssi (molemmat väitteet joko pätevät, tai eivät päde)

2.1 Määritelmä. Propositiologiikan lauseiksi sanotaan seuraavien sääntöjen avulla propositiosymboleista, konnektiiveista sekä sulkumerkeistä "(" ja ")" muodostettuja merkkijonoja:

1. Propositiosymbolit $p_0, p_1, p_2, \ldots$ ovat propositiologiikan lauseita.

2. Mikäli merkkijonot A ja B ovat propositiologiikan lauseita, niin merkkijonot $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ sekä $(A \leftrightarrow B)$ ovat propositiologiikan lauseita.

Isoilla kirjaimilla $A, B, C, \ldots$ merkitään mielivaltaisia merkkijonoja, joiden kuitenkin usein vaaditaan olevan propositiologiikan lauseita. Propositiosymbolit kuvaavat atomisia väittämiä, joita ei voida hajottaa pienempiin osiin, kun taas konnektiiveja $\neg, \wedge, \vee, \rightarrow$ sekä $\leftrightarrow$ käytetään muodostamaan yksinkertaisista väittämistä monimutkaisempia väittämiä.

2.2 Esimerkki. Merkitään propositiosymboleilla p_0, p_1 sekä p_2 seuraavia väittämiä:

p_0: On kesä.
p_1: Linnut laulavat.
p_2: Saniainen kukkii.

Esimerkiksi lause *Linnut eivät laula.* voidaan nyt formalisoida merkinnällä $\neg p_1$, ja lause *Jos saniainen kukkii, niin ei ole kesä mutta linnut laulavat.* merkinnällä $(p_2 \rightarrow (\neg p_0 \wedge p_1))$. Lause $(p_0 \leftrightarrow p_2)$ ilmaisee, että *saniainen kukkii jos on kesä, mutta ei muulloin.*

Formaali kieli antaa mahdollisuuden muodostaa myös käytännön kannalta järjettömiä lauseita, kuten $\neg\neg\neg p_2$ (ei pidä paikkaansa että ei päde että saniainen ei kuki), $(p_0 \wedge \neg p_0)$ (on kesä ja ei ole kesä) tai $(p_0 \wedge (p_0 \vee p_0))$ (on kesä, minkä lisäksi joko on kesä tai on kesä).

Logiikassa asetetaan hyvin suuri paino **syntaksin** ja **semantiikan** välille. Syntaksilla tarkoitetaan niitä lauseiden ominaisuuksia, jotka liittyvät lauseiden ulkoasuun, kun esimerkiksi lauseessa olevien symbolien määrä, tai tieto siitä, alkaako lause isolla alkukirjaimella. Semantiikalla taas tarkoitetaan lauseen merkitykseen tai "totuuteen" liittyviä seikkoja. Jotta syntaksin ja semantiikan yhteyksiä voidaan tutkia, on tärkeää pitää nämä käsitteet visusti erossa toisistaan. Esimerkiksi väittämät

Jokainen kokonaisluku on joko parillinen taikka pariton.

ja

Mikäli luonnollinen luku ei ole pariton, niin se on parillinen.

kuvaavat samaa asiantilaa, mutta syntaktisilta ominaisuuksiltaan eli ulkoasultaan ne poikkeavat. Ne esimerkiksi alkavat eri symboleilla eivätkä ne ole samanpituisia. Samoin esimerkiksi propositiologiikan lauseet $(p_0 \vee p_1)$ ja $(p_1 \vee p_0)$ ovat *ekvivalentteja* (määritellään myöhemmin), mutta kuitenkin eri lauseita. Lauseella yksinkertaisesti tarkoitetaan yllämainitut ehdot täyttävää merkkijonoa.

2.3 Esimerkki. Seuraavat merkkijonot ovat propositiologiikan lauseita. Sulkuihin kirjoitettu numero kertoo, kuinka monta symbolia lauseessa on.

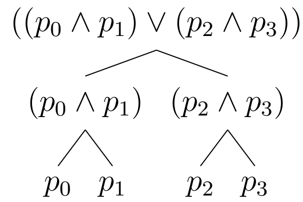
$$\begin{array}{ll}
\neg p_0 & (2) \\
((p_0 \wedge \neg p_0) \to (p_1 \wedge \neg p_1)) & (15) \\
(p_3 \to \neg\neg\neg p_{33}) & (8) \\
\neg(p_9 \to ((p_0 \wedge p_4) \leftrightarrow \neg p_{999})) & (15)
\end{array}$$

Seuraavat merkkijonot *eivät* ole propositiologiikan lauseita:

$$\begin{array}{ll}
p_5 p_4 & (p_9) \\
)\to))\neg\neg & (p_1 \wedge p_2 \wedge p_3) \\
p_1 \to p_1 & (\lambda x.xx)(\lambda x.xx) \\
\text{Kauno on kissa.} & (p_6 = p_7) \\
((p_0 \leftrightarrow p_0) \leftarrow p_1) & ((p_0 \wedge (p_2 \to \neg p_0))
\end{array}$$

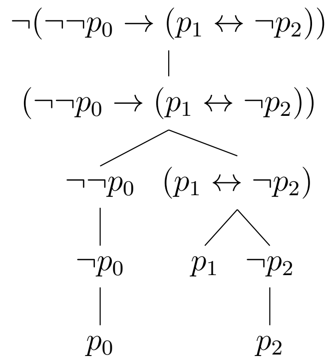
2.2 Lauseiden rakenne

Lauseet muodostuvat pienemmistä lauseista, jotka puolestaan muodostuvat pienemmistä lauseista, jotka muodostuvat pienemmistä lauseista ja niin edelleen, kunnes lopulta kaikki lauseet hajoavat pienimpiin osasiinsa, propositiosymboleiksi. Lauseen **alilause** on lauseen osa, joka itsekin on lause. Esimerkiksi lauseen $((p_0 \wedge p_1) \vee (p_2 \wedge p_3))$ alilauseita ovat p_0, p_1, p_2, p_3, $(p_0 \wedge p_1)$, $(p_2 \wedge p_3)$ sekä lause itse. Lauseiden rakennetta voidaan havainnollistaa **jäsennyspuilla**. Lauseen $((p_0 \wedge p_1) \vee (p_2 \wedge p_3))$ jäsennyspuu näyttää seuraavalta:

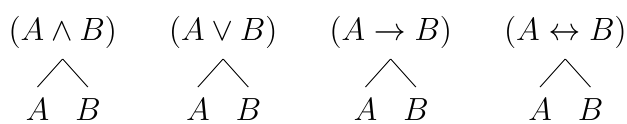


Jäsennyspuun voidaan ajatella kuvaavan, miten lause on muodostettu alilauseistaan. Ylläolevaa jäsennyspuuta luetaan alhaalta ylöspäin näin: ensin propositiosymboleista p_0 ja p_1 muodostetaan lause $(p_0 \wedge p_1)$ ja symboleista p_2 ja p_3 muodostetaan lause $(p_2 \wedge p_3)$. Näistä kahdesta lauseesta muodostetaan sitten disjunktio $((p_0 \wedge p_1) \vee (p_2 \wedge p_3))$.

Lauseen $\neg(\neg\neg p_0 \rightarrow (p_1 \leftrightarrow \neg p_2))$ jäsennyspuu puolestaan näyttää tältä:

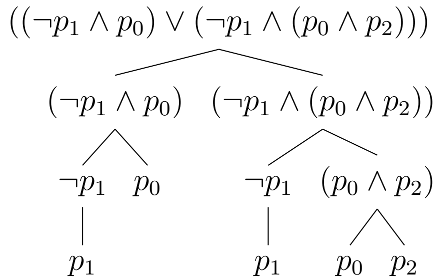


Jäsennyspuun *juurena*, eli ylimpänä solmuna, on lause, jota ollaan jäsentämässä. Puun *lehtinä*, eli alimpina solmuina, ovat ne propositiosymbolit, joita lauseessa esiintyy. Mikäli jossakin solmussa on lause, joka on muodostettu konjunktiolla, disjunktiolla, implikaatiolla tai ekvivalenssilla, puu haarautuu tässä solmussa kahdeksi solmuksi, joissa on ne lauseet, joista jäsennettävä lause on kyseisellä konnektiivilla muodostettu:



Mikäli lause on toisen lauseen negaatio, "haarautuminen" tarkoittaa vain yhden lisähaaran syntymistä:

Lauseen A **välittömäksi alilauseeksi** sanotaan sellaista lauseen A alilausetta, joka on lauseen A jäsennyspuussa heti lauseen A alapuolella. Lauseen A **pääkonnektiiviksi** sanotaan konnektiivia, jolla A muodostetaan välittömistä alilauseistaan. Ylläolevaa puuta tarkastelemalla huomataan, että lauseen $\neg(\neg\neg p_0 \rightarrow (p_1 \leftrightarrow \neg p_2))$ ainoa välitön alilause on lause $(\neg\neg p_0 \rightarrow (p_1 \leftrightarrow \neg p_2))$, ja pääkonnektiivi on $\neg$. Tutkimalla jäsennyspuuta



nähdään, että lauseen $((\neg p_1 \wedge p_0) \vee (\neg p_1 \wedge (p_0 \wedge p_2)))$ välittömät alilauseet ovat $(\neg p_1 \wedge p_0)$ ja $(\neg p_1 \wedge (p_0 \wedge p_2))$, ja pääkonnektiivi on $\vee$.

Lause	Alilauseet	Pää-konnektiivi
$(p_0 \leftrightarrow \neg p_7)$	$(p_0 \leftrightarrow \neg p_7)$, p_0, $\neg p_7$, p_7	$\leftrightarrow$
$((\neg p_1 \vee p_0) \vee (p_0 \wedge \neg p_1))$	$((\neg p_1 \vee p_0) \vee (p_0 \wedge \neg p_1))$, $(\neg p_1 \vee p_0)$, $(p_0 \wedge \neg p_1)$, $\neg p_1$, p_0, p_1	$\vee$
$\neg(A \wedge (B \wedge \neg A))$	$\neg(A \wedge (B \wedge \neg A))$, $(A \wedge (B \wedge \neg A))$, $(B \wedge \neg A)$, $\neg A$, sekä lauseet A ja B ja näiden alilauseet	$\neg$

2.3 Induktio lauseen rakenteen suhteen

Kerrataan luonnollisten lukujen induktioperiaate:

Luonnollisten lukujen induktioperiaate. *Olkoon* $A \subset \mathbb{N}$ *sellainen, että* $0 \in A$ *ja aina kun* $n \in A$*, niin* $n+1 \in A$*. Tällöin* $A = \mathbb{N}$*.*

Induktioperiaate lausutaan usein seuraavassa muodossa: Olkoon P jokin luonnollisten lukujen ominaisuus. Mikäli pätee

1. luvulla 0 on ominaisuus P
2. jos luvulla n on ominaisuus P, niin luvulla $n+1$ on ominaisuus P

niin jokaisella luonnollisella luvulla on ominaisuus P. Nämä kaksi muotoilua ovat kuitenkin yksi ja sama, sillä joukko A voidaan valita olemaan niiden lukujen, joilla on ominaisuus P, joukko, eli

$$A = \{n \in \mathbb{N} \colon \text{luvulla } n \text{ on ominaisuus } P\}.$$

2.4 Esimerkki. Olkoon $x \in \mathbb{R}$, $x > 0$ ja $n \in \mathbb{N}$. Tällöin $(1+x)^n \geq 1 + nx$ (Bernoullin epäyhtälö).

Todistus. Todistetaan väite induktiolla luvun n suhteen. Oletetaan, että $x \in \mathbb{R}$, $x > 0$ ja $A = \{n \in \mathbb{N} \colon \ (1+x)^n \geq 1 + nx\}$. Koska

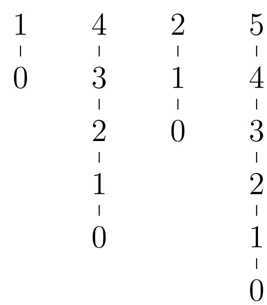
$$(1+x)^0 = 1 \geq 1 = 1 + 0 \cdot x,$$

niin $0 \in A$. Oletetaan nyt, että $n \in A$, eli että $(1+x)^n \geq 1 + nx$. Tällöin

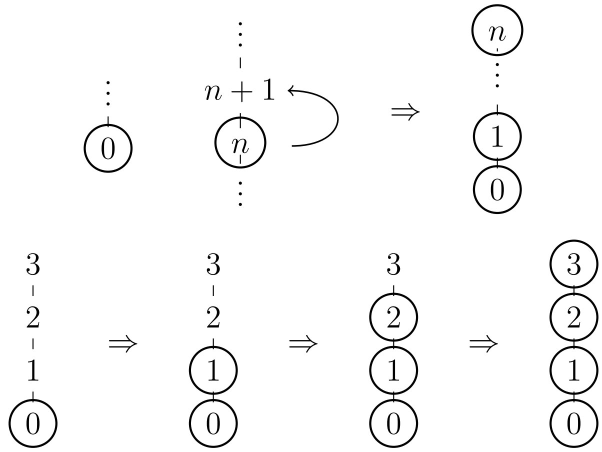
$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n \\ &\overset{i.o.}{\geq} (1+x)(1+nx) \\ &= 1 + nx + x + nx^2 \\ &\geq 1 + (n+1)\,x, \end{aligned}$$

eli myös $n+1 \in A$. Nyt induktioperiaatteen nojalla $A = \mathbb{N}$, eli jokainen luonnollinen luku toteuttaa epäyhtälön $(1+x)^n \geq 1 + nx$. □

Luonnollisten lukujen induktioperiaatetta voidaan havainnollistaa seuraavasti: jokainen luonnollinen luku nollaa lukuunottamatta voidaan ajatella muodostetuksi sitä edeltävästä luonnollisesti luvusta lisäämällä tähän lukuun yksi. Näin luonnollisille luvuille voidaan piirtää seuraavanlaisia jäsennyspuita:



Luonnollisten lukujen induktio vastaa sitä, että todetaan jonkin ominaisuuden olevan luvulla 0 (alkuaskel), ja että tämä ominaisuus periytyy jäsennyspuussa aina askeleen ylöspäin (induktioaskel). Tällöin voidaan kiivetä puuta ylös, kunnes päädytään sen päähän, kuten kuvassa:



Tutustumme seuraavaksi *rakenteelliseen induktioon*, jota matemaattisessa logiikassa tarvitaan usein. Siinä missä luonnollisten lukujen induktio antaa tavan todistaa, että jokaisella luonnollisella luvulla on jokin ominaisuus, rakenteellisella induktiolla voidaan todistaa esimerkiksi, että jokaisella propositiolauseella on jokin ominaisuus. Kun luonnollisten lukujen induktiossa kiivetään ylös luonnollisten lukujen jäsennyspuuta, rakenteellisessa induktiossa puut ovat monimutkaisempia. Rakenteellista induktiota käsitellään yleisemmin kappaleessa B.

Propositiolauseiden induktioperiaate. *Olkoon P kaikkien propositiolauseiden joukko ja $Q \subset P$. Oletetaan, että*

(i) $p_n \in Q$ *jokaisella* $n \in \mathbb{N}$

(ii) $\neg A \in Q$ *aina kun* $A \in Q$

(iii) $(A \wedge B) \in Q$ *aina kun* $A, B \in Q$

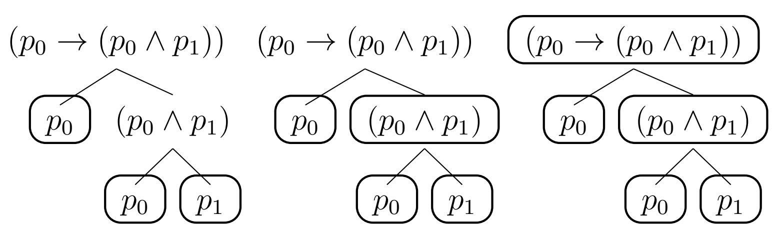
(iv) $(A \vee B) \in Q$ *aina kun* $A, B \in Q$

(v) $(A \rightarrow B) \in Q$ *aina kun* $A, B \in Q$

(vi) $(A \leftrightarrow B) \in Q$ *aina kun* $A, B \in Q$

Tällöin $Q = P$.

Propositiolauseiden induktioperiaatteessa kohta (i) on analoginen luonnollisten lukujen induktioperiaatteen kohdan "$0 \in A$" kanssa. Sitä voikin hyvin kutsua *alkuaskeleeksi*. Siinä missä luonnollisten lukujen induktiossa induktioaskelia on vain yksi, propositiolauseiden induktioperiaatteessa jokaista konnektiiviä vastaa oma induktioaskeleensa. Ideana on kiivetä jäsennyspuuta ylöspäin, kuten luonnollisten lukujen induktiossakin. Tällä kertaa tarvitsemme vain useammanlaisia induktioaskelia, koska haarautumisia on useanlaisia.



Emme ole vielä todistaneet propositiologiikan induktioperiaatetta. Sitä varten määrittelemme seuraavaksi propositiolauseiden joukon hieman täsmällisemmin kuin aikaisemmin. Määritellään rekursiivisesti joukot P_n jokaisella $n \in \mathbb{N}$:

$$\begin{aligned} P_0 &= \{p_n \colon n \in \mathbb{N}\} \\ P_{n+1} &= P_n \cup \{\neg A \colon A \in P_n\} \cup \{(A \wedge B) \colon A, B \in P_n\} \\ &\quad \cup \{(A \vee B) \colon A, B \in P_n\} \cup \{(A \rightarrow B) \colon A, B \in P_n\} \\ &\quad \cup \{(A \leftrightarrow B) \colon A, B \in P_n\} \end{aligned}$$

Joukkoja P_n voidaan ajatella eräänlaisina hierarkian tasoina. Jokaisen tason lauseet on saatu edellisen tason lauseista soveltamalla jotakin konnektiivia kerran. Lisäksi jokaiselle tasolle kuuluu myös kaikki edellisten tasojen lauseet, eli

$$P_0 \subset P_1 \subset P_2 \subset P_3 \subset \dots$$

Olkoon nyt

$$P = \bigcup_{n \in \mathbb{N}} P_n.$$

Joukko P siis sisältää kaikki propositiolauseet.

taso	esimerkkilauseita
0	$p_3, p_9, p_2, \dots$
1	$(p_3 \to p_1), (p_1 \wedge p_6), \neg p_7, \dots$
2	$((p_0 \to p_2) \wedge p_1), \neg\neg p_6, ((p_0 \to p_2) \vee (p_5 \to p_2)), \dots$
3	$((\neg p_3 \to (p_2 \vee p_1)) \wedge \neg p_0), (\neg\neg p_0 \wedge p_2) \dots$
4	$((((p_8 \wedge p_1) \wedge p_0) \wedge (\neg p_6 \wedge \neg p_7)) \wedge \neg\neg p_9), \dots$
$\vdots$	

Lause on intuitiivisesti sitä monimutkaisempi, mitä korkeammalla se tulee vastaan tässä tasohierarkiassa.

Propositiolauseiden induktioperiaatteen todistus. Olkoon $Q \subset P$ joukko propositiolauseita, joka sisältää propositiosymbolit $p_0, p_1, \dots$, ja on *suljettu konnektiivien sovellusten suhteen*, eli mikäli $B, C \in Q$, niin jokainen lauseista $\neg B$, $(B \wedge C)$, $(B \vee C)$, $(B \to C)$ ja $(B \leftrightarrow C)$ kuuluu joukkoon Q. Näytetään induktiolla luvun n suhteen, että $P_n \subset Q$ jokaisella $n \in \mathbb{N}$.

Oletuksen nojalla Q sisältää propositiosymbolit, joten $P_0 \subset Q$. Oletetaan sitten, että $P_n \subset Q$, ja $A \in P_{n+1}$. Joukon P_{n+1} määritelmän nojalla A joko kuuluu joukkoon P_n, jolloin induktio-oletuksen nojalla $A \in Q$, tai jotakin seuraavista muodoista: $\neg B$, $(B \wedge C)$, $(B \vee C)$, $(B \to C)$ tai $(B \leftrightarrow C)$, missä lauseet B ja C kuuluvat hierarkian alempaan tasoon P_n. Induktio-oletuksen nojalla tällöin $B, C \in Q$, ja koska Q on suljettu konnektiivien sovellusten suhteen, $A \in Q$. Siis $P_{n+1} \subset Q$.

Luonnollisten lukujen induktioperiaatteen nojalla $P_n \subset Q$ jokaisella $n \in \mathbb{N}$, eli

$$P = \bigcup_{n \in \mathbb{N}} P_n \subset Q,$$

joten $Q = P$.

$\square$

Propositiolauseiden induktiosta käytetään usein nimitystä *induktio lauseen rakenteen suhteen.* Lisäksi usein eri konnektiivejä vastaavat kohdat käsitellään samalla tavalla, joten nämä jätetään usein kirjoittamatta auki. Klassinen esimerkki propositiolauseiden induktiosta:

2.5 Esimerkki. Olkoon $|A|_v$ merkkijonossa A esiintyvien vasempien sulkumerkkien määrä ja olkoon $|A|_o$ merkkijonossa A esiintyvien oikeiden sulkumerkkien määrä. Siis esimerkiksi

$$|)\neg p_8(\to))\to)|_v = 1 \quad \text{ja} \quad |)\neg p_8(\to))\to)|_o = 4.$$

Jokaisessa propositiolauseessa A on yhtä monta vasenta ja oikeaa sulkua, eli $|A|_v = |A|_o$ jokaisella propositiolauseella A.

Todistus. Induktio lauseen A rakenteen suhteen. Väite pätee triviaalisti, kun A on propositiosymboli, sillä silloin siinä ei ole ollenkaan sulkumerkkejä.

Oletetaan, että väite pätee propositiolauseella A, eli että $|A|_v = |A|_o$. Negaatiomerkin lisääminen lauseen alkuun ei muuta siinä olevien sulkujen määrää, joten

$$|\neg A|_v = |A|_v \overset{i.o.}{=} |A|_o = |\neg A|_o\,.$$

Siis väite pätee lauseelle $\neg A$.

Oletetaan sitten, että väite pätee lauseilla A ja B, eli $|A|_v = |A|_o$ ja $|B|_v = |B|_o$. Lauseessa $(A \wedge B)$ on vasempia sulkuja yksi enemmän kuin lauseissa A ja B yhteensä. Sama pätee oikeille suluille, joten

$$|(A \wedge B)|_v = 1 + |A|_v + |B|_v \overset{i.o.}{=} 1 + |A|_o + |B|_o = |(A \wedge B)|_o\,,$$

eli väite pätee myös lauseelle $(A \wedge B)$.

Kohdat $(A \vee B)$, $(A \to B)$ sekä $(A \leftrightarrow B)$ todistetaan kuten konjunktio.

Siis propositiolauseiden induktioperiaatteen nojalla väite pätee jokaiselle propositiolauseelle. □

2.6 Esimerkki. Minkään propositiolauseen viimeinen merkki ei ole negaatiomerkki $\neg$.

Todistus. Todistetaan väite induktiolla lauseen rakenteen suhteen.

$\boxed{p_i}$ Lauseen, joka koostuu vain yhdesta propositiosymbolista, viimeinen merkki on tietysti tämä propositiosymboli.

$\boxed{\neg}$ Olkoon A lause, joka toteuttaa väitteen, eli ei lopu negaatiomerkkiin. Lauseen $\neg A$ viimeinen merkki on selvästi sama kuin lauseen A viimeinen merkki, joten myöskään lause $\neg A$ ei lopu negaatiomerkkiin.

$\boxed{\wedge}$ Olkoot A ja B lauseita, joista kumpikaan ei lopu negaatiomerkkiin. Lause $(A \wedge B)$ selvästi loppuu oikeaan sulkumerkkiin), joten se ei lopu negaatiomerkkiin.

$\boxed{\vee}$ Olkoot A ja B lauseita, joista kumpikaan ei lopu negaatiomerkkiin. Lause $(A \vee B)$ selvästi loppuu oikeaan sulkumerkkiin), joten se ei lopu negaatiomerkkiin.

$\boxed{\to}$,$\boxed{\leftrightarrow}$ Kuten kohdat $\boxed{\wedge}$ ja $\boxed{\vee}$.

$\square$

2.7 Esimerkki. Jos propositiolauseessa on parillinen määrä symboleja, siinä esiintyy negaatiosymboli.

Todistus. Todistetaan induktiolla lauseen A rakenteen suhteen, että jos lauseessa A ei esiinny negaatiosymbolia, siinä on pariton määrä symboleja. Koska tutkimme vain lauseita, joiden muodostuksessa ei ole käytetty negaatiosymbolia, meidän ei tarvitse käsitellä kohtaa $\boxed{\neg}$.

Merkitään lauseessa olevien symbolien määrää $|A|$.

$\boxed{p_i}$ Jos $A = p_i$ jollakin i, niin lauseessa A on tasan yksi symboli, joten siinä on pariton määrä symboleja.

$\boxed{\wedge}$ Oletetaan, että lauseissa A ja B on pariton määrä symboleja. Tällöin lauseessa $(A \wedge B)$ on lauseiden A ja B symbolien lisäksi kolme symbolia: (, $\wedge$ sekä). Siis

$$|(A \wedge B)| = |A| + |B| + 3,$$

joka on kolmen parittoman luvun summana pariton. Siis väite pätee myös lauseella $(A \vee B)$.

$\boxed{\vee}$ Oletetaan, että lauseissa A ja B on pariton määrä symboleja. Tällöin lauseessa $(A \vee B)$ on lauseiden A ja B symbolien lisäksi kolme symbolia: (, $\vee$ sekä). Siis

$$|(A \vee B)| = |A| + |B| + 3,$$

joka on taas kolmen parittoman luvun summana pariton. Siis väite pätee myös lauseella $(A \vee B)$.

$\boxed{\to}$,$\boxed{\leftrightarrow}$ Kuten kohdat $\boxed{\wedge}$ ja $\boxed{\vee}$.

$\square$

Seuraavan kappaleen todistuksissa on lisää esimerkkejä rakenteellisesta induktiosta.

2.4 Totuus

Olemme siis määritelleet erään kokoelman merkkijonoja ja päättäneet kutsua siihen kokoelmaan kuuluvia merkkijonoja *lauseiksi*. Lauseet pyrkivät olemaan hyvä matemaattinen malli *väittämille*, joten lauseille on määriteltävä totuuden käsite. Merkitsemme totuutta numerolla 1 ja epätotuutta numerolla 0.

2.8 Määritelmä. Totuusjakauma on mikä tahansa funktio $v\colon \mathbb{N} \to \{0,1\}$. Propositiolauseen A **totuusarvo jakaumalla** v, merkitään $v[A]$, määritellään seuraavasti:

1. $v[p_n] = v(n)$ jokaisella $n \in \mathbb{N}$.
2. $v[\neg A] = 0$ mikäli $v[A] = 1$ ja $v[\neg A] = 1$ mikäli $v[A] = 0$.
3. $v[(A \wedge B)] = 1$ jos sekä $v[A] = 1$ että $v[B] = 1$. Muutoin $v[(A \wedge B)] = 0$.
4. $v[(A \vee B)] = 1$ jos joko $v[A] = 1$ tai $v[B] = 1$. Muutoin $v[(A \vee B)] = 0$.
5. $v[(A \to B)] = 1$ jos joko $v[A] = 0$ tai $v[B] = 1$. Muutoin $v[(A \to B)] = 0$.
6. $v[(A \leftrightarrow B)] = 1$ jos $v[A] = v[B]$. Muutoin $v[(A \leftrightarrow B)] = 0$.

Mikäli $v[A] = 1$, sanomme, että lause A on tosi jakaumalla v, tai että jakauma v toteuttaa lauseen A. Jos taas $v[A] = 0$, sanomme, että lause A on epätosi jakaumalla v, tai että jakauma v ei toteuta lausetta A.

Totuusjakauma siis kertoo, mitkä atomisista väittämistä p_n ovat tosia ja mitkä epätosia. Kun tiedämme tämän, voimme päätellä myös monimutkaisempien lauseiden totuuden. Lauseen totuuden selvittämiseksi pitää siis ensin selvittää lauseen alilauseiden totuus.

2.9 Esimerkki. Olkoon v totuusjakauma, jonka arvo pisteissä 1, 2, ja 4 on nolla, ja muissa pisteissä yksi.

p_0	p_1	p_2	p_3	p_4	p_5	p_6		$\cdots$
1	0	0	1	0	1	1		$\cdots$

Tällöin lause p_5 on tosi jakaumalla v ja lause p_4 on epätosi jakaumalla v. Lause $(p_5 \vee p_4)$ on tosi, koska ainakin toinen lauseista p_5 ja p_4 on tosi. Lause $(p_5 \to p_4)$ taas on epätotta.

2.10 Esimerkki. Olkoon $v\colon \mathbb{N} \to \{0, 1\}$ sellainen, että $v(n) = 1$ kun n on parillinen ja $v(n) = 0$ muuten.

p_0	p_1	p_2	p_3	p_4	p_5	p_6		$\cdots$
1	0	1	0	1	0	1		$\cdots$

Selvitetään lauseen $((p_0 \vee \neg p_1) \leftrightarrow p_0)$ totuusarvo jakaumalla v.

Koska $v[p_1] = 0$, niin $v[\neg p_1] = 1$ ja täten $v[(p_0 \vee \neg p_1)] = 1$. Siis $v[(p_0 \vee \neg p_1)] = 1 = v[p_0]$, ja täten

$$v[((p_0 \vee \neg p_1) \leftrightarrow p_0)] = 1.$$

Joissakin oppimateriaaleissa, kuten kirjassa [JohLog], totuutta ja epätotuutta merkitään esimerkiksi kirjaimin **t** ja **e** tai esimerkiksi **T** ja **F**. Numeroiden 0 ja 1 käytössä on se etu, että lauseiden totuuksia voi laskea kätevästi aritmeettisillä lausekkeilla. Esimerkiksi jos A ja B ovat mitä tahansa propositiolauseita, niin $v[\neg A] = 1 - v[A]$ ja $v[(A \wedge B)] = v[A] \cdot v[B]$. Disjunktiolle vastaava merkintä on hieman kömpelö, mutta käytämme sitä ajoittain silti:

$$v[(A \vee B)] = 1 - (1 - v[A])\,(1 - v[B])\,.$$

2.5 Totuustaulut

Lauseen totuusarvoja eri jakaumilla on helppo laskea *totuustaululla*. Konnektiivien totuustaulut näyttävät seuraavilta:

A	$\neg A$
0	1
1	0

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

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

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

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

Totuustaulu voidaan piirtää näin: Koska lauseen A totuusarvoon vaikuttavat selvästi vain jakauman v arvot niillä luvuilla n, joilla p_n esiintyy lauseessa A, listataan ensimmäiselle riville kaikki lauseessa esiintyvät propositiosymbolit. Listataan sitten vasemmalle propositiosymboleiden totuusarvojen kaikki mahdolliset kombinaatiot. Täytetään sitten kunkin alilauseen totuusarvo kyseisen alilauseen pääkonnektiivin alapuolelle, lähtien sisimmäisistä alilauseista, eli niistä, jotka on muodostettu pelkistä propositiosymboleista yhdellä konnektiivilla.

Esimerkiksi lauseen $((p_0 \lor \neg p_1) \leftrightarrow p_0)$ totuusarvot kaikilla mahdollisilla totuusjakaumilla selviävät seuraavasta totuustaulusta:

p_0	p_1	$(($ p_0	$\lor$	$\neg$	p_1 $)$	$\leftrightarrow$	p_0 $)$
0	0	0	1	1	0	0	0
0	1	0	0	0	1	1	0
1	0	1	1	1	0	1	1
1	1	1	1	0	1	1	1

Taulusta nähdään, että lause $((p_0 \lor \neg p_1) \leftrightarrow p_0)$ on totta aina jos vähintään toinen lauseista p_0 ja p_1 on totta. Taulu täytetään sisältä päin. Järjestys on siis

$$\begin{array}{ccccccccc} ((& p_0 & \lor & \neg & p_1 &) & \leftrightarrow & p_0 &) \\ & 1. & 3. & 2. & 1. & & 4. & 1. & \end{array},$$

eli lauseen jäsennyspuu käydään läpi alhaalta ylöspäin:

$$4.\ ((p_0 \vee \neg p_1) \leftrightarrow p_0)$$

$$3.\ (p_0 \vee \neg p_1) \qquad 1.\ p_0$$

$$1.\ p_0 \quad 2.\ \neg p_1$$

$$1.\ p_1$$

Vaikka periaatteessa ei olisi väliä, missä järjestyksessä totuustaulun rivit olisivat, helpottaa totuustaulun lukemista huomattavasti, jos rivien järjestys on säännönmukainen. Tässä oppimateriaalissa kaikkien totuustaulujen rivit ovat kasvavassa suuruusjärjestyksessä, kun vasemmalle kirjattujen yksittäisten propositiosymbolien arvojen ajatellaan peräkkäin asetettuna muodostavan yhden binäärijärjestelmän luvun.

2.11 Määritelmä. Olkoon A jokin propositiolause. Mikäli $v[A] = 1$ jokaisella totuusjakaumalla v, sanotaan että A on **tautologia**. Mikäli $v[A] = 0$ jokaisella totuusjakaumalla v, sanotaan että A on **ristiriita**. Mikäli A ei ole tautologia eikä ristiriita, sanotaan että A on **kontingentti**.

2.12 Esimerkki. Lause $(p_0 \rightarrow (p_1 \rightarrow p_0))$ on tautologia, mikä näkyy sen totuustaulusta:

p_0	p_1	(	p_0	$\rightarrow$	(	p_1	$\rightarrow$	p_0	))
0	0		0	1		0	1	0	
0	1		0	1		1	0	0	
1	0		1	1		0	1	1	
1	1		1	1		1	1	1	

Lauseet $(p_0 \wedge \neg p_0)$ ja $((p_0 \rightarrow \neg p_0) \wedge (\neg p_0 \rightarrow p_0))$ ovat esimerkkejä ristiriidoista, ja lauseet $((p_0 \wedge p_1) \rightarrow \neg p_0)$ ja $((p_0 \wedge p_1) \vee (p_2 \wedge p_3))$ ovat kontingentteja.

Lauseita A ja B sanotaan **ekvivalenteiksi**, mikäli ne saavat jokaisella totuusjakaumalla saman totuusarvon, eli mikäli $(A \leftrightarrow B)$ on tautologia. Tällöin merkitään $A \Leftrightarrow B$. Mikäli $(A \rightarrow B)$ on tautologia, sanotaan, että lause B on lauseen A **looginen seuraus**, ja merkitään $A \Rightarrow B$. B on siis tosi jokaisella sellaisella totuusjakaumalla, jolla A on tosi.

Mikäli A ja B ovat ekvivalentteja propositiologiikan lauseita, niin ne ovat myös triviaalisti toistensa loogisia seurauksia.

2.13 Esimerkki. Lauseet $(A \wedge B)$ sekä $\neg(\neg A \vee \neg B)$ ovat ekvivalentteja, olivat A ja B mitä hyvänsä propositiologiikan lauseita.

Todistus. Olkoot A ja B propositiologiikan lauseita ja v mielivaltainen totuusjakauma. Tällöin

$$\begin{aligned} v[(A \wedge B)] = 1 &\iff v[A] = 1 \text{ ja } v[B] = 1 \\ &\iff v[\neg A] = 0 \text{ ja } v[\neg B] = 0 \\ &\iff v[(\neg A \vee \neg B)] = 0 \\ &\iff v[\neg(\neg A \vee \neg B)] = 1 \end{aligned}$$

□

2.14 Esimerkki. Lauseet $(p_0 \to (p_1 \to p_2))$ ja $((p_0 \to p_1) \to p_2)$ eivät ole ekvivalentteja.

Todistus. Olkoon v jokin totuusjakauma, jolla $v(0) = v(1) = v(2) = 0$. Tällöin $v[(p_0 \to (p_1 \to p_2))] = 1$, mutta $v[((p_0 \to p_1) \to p_2)] = 0$. □

2.15 Esimerkki. $(p_0 \leftrightarrow p_1) \Rightarrow ((p_2 \to \neg p_1) \leftrightarrow (p_2 \to \neg p_0))$

Todistus. Olkoon v totuusjakauma, jolla $v[(p_0 \leftrightarrow p_1)] = 1$, eli $v[p_0] = v[p_1]$. Tällöin tietysti $v[\neg p_0] = v[\neg p_1]$. Mikäli $v[p_2] = 0$, triviaalisti $v[(p_2 \to \neg p_1)] = 1$ ja $v[(p_2 \to \neg p_0)] = 1$, joten v toteuttaa lauseen $((p_2 \to \neg p_1) \leftrightarrow (p_2 \to \neg p_0))$. Jos taas $v[p_2] = 1$, niin

$$\begin{aligned} v[(p_2 \to \neg p_1)] &= v[\neg p_1] \\ &= v[\neg p_0] \\ &= v[(p_2 \to \neg p_0)], \end{aligned}$$

joten tässäkin tapauksessa v toteuttaa lauseen $((p_2 \to \neg p_1) \leftrightarrow (p_2 \to \neg p_0))$. □

2.16 Lause. Olkoot $p_0, \dots, p_n$ propositiosymboleja, $B_0, \dots, B_n$ propositiolauseita ja v totuusjakauma. Olkoon v' totuusjakauma, joka saadaan totuusjakaumasta v korvaamalla symbolien $p_0, \dots, p_n$ totuusarvot lauseiden $B_0, \dots, B_n$ totuusarvoilla, eli

$$v'(i) = \begin{cases} v[B_i], & \text{kun } i \leq n \\ v(i), & \text{kun } i > n \end{cases}.$$

Määritellään jokaisella propositiolauseella A uusi propositiolause A', joka saadaan lauseesta A korvaamalla jokainen symbolin p_i esiintymä lauseella B_i. Tällöin millä tahansa totuusjakaumalla v ja lauseella A pätee:

$$v'[A] = v[A'].$$

Todistus. Todistetaan väite induktiolla lauseen A rakenteen suhteen.

$\boxed{p_i}$ Mikäli $A = p_i$, ja $i \leq n$, niin $A' = B_i$. Jakauman v' määritelmän nojalla $v'(i) = v[B_i]$, joten

$$v'[A] = v'[p_i] = v'(i) = v[B_i] = v[A'].$$

$\boxed{\neg}$ Oletetaan, että väite pätee lauseelle A, eli että $v'[A] = v[A']$. Nyt

$$\begin{aligned} v'[\neg A] = 1 &\iff v'[A] = 0 \\ &\overset{\text{i.o.}}{\iff} v[A'] = 0 \\ &\iff v[\neg A'] = 1 \\ &\iff v[(\neg A)'] = 1, \end{aligned}$$

joten väite pätee myös lauseelle $\neg A$.

$\boxed{\wedge}$ Oletetaan, että väite pätee lauseille A ja B. Nyt

$$\begin{aligned} v'[(A \wedge B)] = 1 &\iff v'[A] = 1 \text{ ja } v'[B] = 1 \\ &\overset{\text{i.o.}}{\iff} v[A'] = 1 \text{ ja } v[B'] = 1 \\ &\iff v[(A' \wedge B')] = 1 \\ &\iff v[(A \wedge B)'] = 1, \end{aligned}$$

joten väite pätee myös lauseelle $(A \wedge B)$.

$\boxed{\vee}$, $\boxed{\to}$, $\boxed{\leftrightarrow}$ Kuten kohta $\boxed{\wedge}$.

□

2.17 Korollaari (Tautologian sijoitussääntö). Olkoon A propositiolause, $p_0, \ldots, p_n$ propositiosymboleja, ja olkoot $B_0, \ldots, B_n$ propositiolauseita. Mikäli A on tautologia, niin lause, joka saadaan lauseesta A korvaamalla jokainen symbolin p_i esiintymä lauseella B_i, kun $i = 0, \ldots, n$, on myös tautologia.

Todistus. Olkoon v mielivaltainen totuusjakauma. Olkoon A' saatu lauseesta A korvaamalla jokainen symbolin p_i esiintymä lauseella B_i ja olkoon v' kuten edellisessä lauseessa. Tällöin edellisen lauseen nojalla $v'[A] = v[A']$. Koska A on tautologia, $v'[A] = 1$, joten $v[A'] = 1$.

Siis lauseen A' totuusarvo millä tahansa totuusjakaumalla on 1, joten lause A' on tautologia. □

Esimerkissä 2.12 totesimme, että lause $(p_0 \to (p_1 \to p_0))$ on tautologia. Sijoittamalla symbolin p_0 tilalle esimerkiksi lauseen $(p_9 \wedge \neg p_5)$ ja symbolin p_1 tilalle lauseen $(p_2 \leftrightarrow (\neg p_3 \vee p_4))$ saamme hankalan näköisen lauseen

$$((p_9 \wedge \neg p_5) \to ((p_2 \leftrightarrow (\neg p_3 \vee p_4)) \to (p_9 \wedge \neg p_5))).$$

Edellisen lauseen nojalla voimme suoraan sanoa, että tämä lause on tautologia. Tämä onkin kätevää, sillä lauseessa on 5 eri propositiosymbolia, joten lauseen totuustauluun tulisi rivejä peräti 32.

2.6 Semanttinen puu

Koska totuustaulun rivien määrä on 2^n, missä n on lauseessa esiintyvien *eri* propositiosymboleiden määrä, tulee hiemankin monimutkaisemman lauseen totuusaulusta helposti hyvin suuri. Mikäli tehtävänä on selvittää, millä totuusjakaumilla jokin lause toteutuu, on **semanttinen puu** oiva tapa tehdä tämä. Semanttista puuta ei pidä sekoittaa jäsennyspuuhun. Sana ”semantiikka” tarkoittaa asioiden merkitystä, propositiolauseiden kohdalla lähinnä niiden totuutta eri totuusjakaumilla. Semanttinen puu siis on työkalu lauseen *totuuden* tutkimiseen, kun taas jäsennyspuu on työkalu lauseen *rakenteen* tutkimiseen.

Tutkitaan, milloin lause $A = (p_0 \vee (\neg p_1 \wedge p_2))$ on tosi. Disjunktiolla muodostettu lause on tosi silloin, kun ainakin toinen disjunkteista on tosi, eli lauseen A voi toteuttaa joko toteuttamalla lauseen p_0 tai lauseen $(\neg p_1 \wedge p_2)$:

$$
\begin{array}{ccc}
 & (p_0 \vee (\neg p_1 \wedge p_2)) & \\
 & \diagup \quad \diagdown & \\
p_0 & & (\neg p_1 \wedge p_2)
\end{array}
$$

Lauseen $(\neg p_1 \wedge p_2)$ taas voi puolestaan toteuttaa vain toteuttamalla sekä lauseen $\neg p_1$ että lauseen p_2. Tästä syystä nämä lauseet merkataan samaan oksaan:

$$
\begin{array}{ccc}
 & (p_0 \vee (\neg p_1 \wedge p_2)) & \\
 & \diagup \quad \diagdown & \\
p_0 & & (\neg p_1 \wedge p_2) \\
 & & | \\
 & & \neg p_1 \\
 & & | \\
 & & p_2
\end{array}
$$

Tästä eteenpäin puuta ei voikaan enää jatkaa. Puun jokainen *oksa*, eli reitti juuresta lehtisolmuun kuvaa yhtä mahdollisuutta toteuttaa lause A. Puuhun on siis syntynyt kaksi oksaa, joten lauseen A toteuttamiseen on ainakin kaksi mahdollista keinoa. Mikäli edetään vasenta oksaa pitkin, nähdään, että toteuttamalla lause p_0, myös lause A toteutuu. Siis mikä tahansa totuusjakauma v, jolla $v(0) = 1$ toteuttaa lauseen A. Jos taas edetään oikeanpuoleista oksaa pitkin, nähdään, että lause A voidaan toteuttaa toteuttamalla tällä oksalla olevat lauseet $\neg p_1$ sekä p_2. Siis mikä tahansa totuusjakauma v, jolla $v(1) = 0$ ja $v(2) = 1$, toteuttaa lauseen A.

Entäpä lause $(p_0 \wedge \neg p_0)$? Konjunktion toteuttamiseksi tulee molempien konjunktien toteutua:

$$
\begin{array}{c}
(p_0 \wedge \neg p_0) \\
| \\
p_0 \\
| \\
\neg p_0
\end{array}
$$

Mikään totuusjakauma ei tietenkään voi toteuttaa samanaikaisesti sekä lausetta, että sen negaatiota, joten mikäli jollekin oksalle ilmestyy jokin lause ja sen negaatio, merkitään tämän oksan päähän rasti merkiksi siitä, että oksa ei voi toteutua.

$$\begin{array}{c} (p_0 \wedge \neg p_0) \\ | \\ p_0 \\ | \\ \neg p_0 \\ | \\ \times \end{array}$$

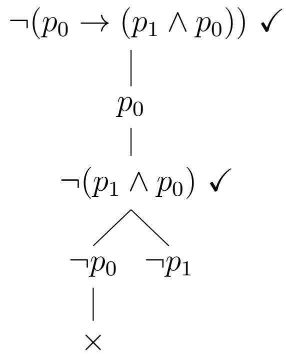
Oksaa, joka päättyy merkkiin $\times$, sanotaan **suljetuksi**. Muita oksia sanotaan **avoimiksi**.

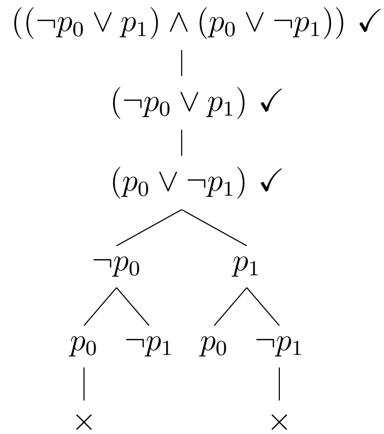
Tarkasti ottaen lauseen A semanttinen puu muodostetaan noudattamalla oheisen taulukon 1 sääntöjä. Puun *juureksi*, eli ylimmäksi solmuksi merkitään lause A. Seuraavia sääntöjä sovelletaan puun solmuihin, kunnes jokainen solmu, joka ei ole yksittäinen propositiosymboli, eikä propositiosymbolin negaatio, on käsitelty. Aina kun solmu on käsitelty, sen viereen laitetaan merkki ✓.

konnektiivi	säännöt
negaatio	$\begin{array}{c} \neg\neg A \\ \vert \\ A \end{array}$ $\begin{array}{c} \neg A \\ \vert \\ A \\ \vert \\ \times \end{array}$ $\begin{array}{c} A \\ \vert \\ \neg A \\ \vert \\ \times \end{array}$
konjunktio	$\begin{array}{c} (A \wedge B) \\ \vert \\ A \\ \vert \\ B \end{array}$ $\begin{array}{cc} \multicolumn{2}{c}{\neg(A \wedge B)} \\ / & \backslash \\ \neg A & \neg B \end{array}$
disjunktio	$\begin{array}{cc} \multicolumn{2}{c}{(A \vee B)} \\ / & \backslash \\ A & B \end{array}$ $\begin{array}{c} \neg(A \vee B) \\ \vert \\ \neg A \\ \vert \\ \neg B \end{array}$
implikaatio	$\begin{array}{cc} \multicolumn{2}{c}{(A \to B)} \\ / & \backslash \\ \neg A & B \end{array}$ $\begin{array}{c} \neg(A \to B) \\ \vert \\ A \\ \vert \\ \neg B \end{array}$
ekvivalenssi	$\begin{array}{cc} \multicolumn{2}{c}{(A \leftrightarrow B)} \\ / & \backslash \\ A & \neg A \\ \vert & \vert \\ B & \neg B \end{array}$ $\begin{array}{cc} \multicolumn{2}{c}{\neg(A \leftrightarrow B)} \\ / & \backslash \\ A & \neg A \\ \vert & \vert \\ \neg B & B \end{array}$

Kuva 1: Semanttisen puun säännöt

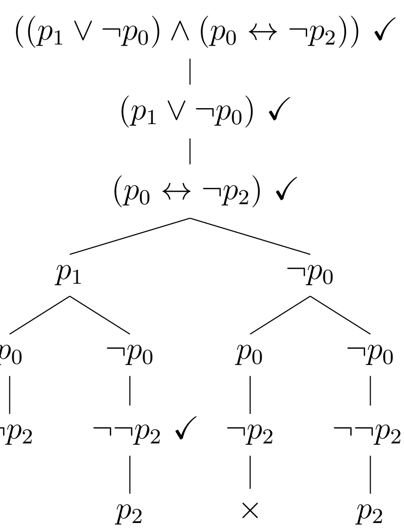
Kun jotakin sääntöä sovelletaan solmuun A, säännön soveltamisesta syntyvät uudet solmut lisätään *jokaisen* solmun A kautta kulkevan *avoimen* oksan päähän. Esimerkiksi lauseiden $\neg(p_0 \to (p_1 \wedge p_0))$ ja $((\neg p_0 \vee p_1) \wedge (p_0 \vee \neg p_1))$ semanttiset puut näyttävät seuraavilta:





Edellisestä puusta voidaan nähdä, että lause $\neg(p_0 \to (p_1 \wedge p_0))$ pätee kaikilla totuusjakaumilla, joilla $v[p_0] = 1$ ja $v[p_1] = 0$. Lause $((\neg p_0 \vee p_1) \wedge (p_0 \vee \neg p_1))$ on tosi niillä totuusjakaumilla, joilla $v[p_0] = v[p_1] = 0$ tai $v[p_0] = v[p_1] = 1$.

2.18 Esimerkki. Toteuttaako jokin totuusjakauma lauseen $((p_1 \vee \neg p_0) \wedge (p_0 \leftrightarrow \neg p_2))$?
Muodostetaan lauseen semanttinen puu:



Seuraamalla esimerkiksi vasemmanpuoleisinta oksaa, nähdään, että jos p_1, p_0 sekä $\neg p_2$ toteutuvat, myös lause $((p_1 \vee \neg p_0) \wedge (p_0 \leftrightarrow \neg p_2))$ toteutuu. Siis mikä tahansa totuusjakauma v, jolla $v(0) = v(1) = 1$ ja $v(2) = 0$, toteuttaa lauseen.

Tutkitaan, toteutuuko lause $\neg((p_0 \to p_1) \vee (p_1 \to p_0))$ jollakin totuusjakaumalla. Muodostetaan semanttinen puu.

$$
\begin{array}{c}
\neg((p_0 \to p_1) \vee (p_1 \to p_0)) \checkmark \\
| \\
\neg(p_0 \to p_1) \checkmark \\
| \\
\neg(p_1 \to p_0) \checkmark \\
| \\
p_0 \\
| \\
\neg p_1 \\
| \\
p_1 \\
| \\
\neg p_0 \\
| \\
\times
\end{array}
$$

Huomaamme, että puun jokainen (eli ainoa) oksa sulkeutuu, eli lause ei voi toteutua millään totuusjakaumalla. Tämä pätee yleisesti: Jos minkä tahansa lauseen semanttisen puun jokainen oksa sulkeutuu, on kyseinen lause ristiriita. Tämä antaa kätevän tavan näyttää jokin lause ristiriidaksi tai tautologiaksi.

Lauseen $\neg A$ semanttista puuta, jossa jokainen oksa sulkeutuu, sanotaan lauseen A **semanttiseksi todistukseksi**. Esimerkiksi ylläoleva semanttinen puu on lauseen $((p_0 \to p_1) \vee (p_1 \to p_0))$ semanttinen todistus. Lause $((p_0 \to p_1) \vee (p_1 \to p_0))$ on siis tautologia. Tämä voidaan tietysti varmistaa myös totuustaululla:

p_0	p_1	$((p_0 \to p_1) \vee (p_1 \to p_0))$
0	0	1 1 1
0	1	1 1 0
1	0	0 1 1
1	1	1 1 1

Semanttisen puun voi piirtää myös useammalle lauseelle $A_1, \ldots, A_n$. Tällöin etsitään totuusjakaumaa, jolla kaikki lauseet olisivat tosia. Lauseet laitetaan kaikki jonoon päällekkäin

$$
\begin{array}{c}
A_1 \\
| \\
A_2 \\
| \\
\vdots \\
| \\
A_n
\end{array}
$$

ja sitten aloitetaan sääntöjen soveltaminen. Lauseen B **semanttiseksi todistukseksi lauseista** $A_1, \ldots, A_n$ sanotaan lauseiden $A_1, \ldots, A_n, \neg B$ semanttista puuta, jossa kaikki haarat sulkeutuvat. Idea on, että lauseet $A_1, \dots, A_n$ ja $\neg B$ eivät voi olla samanaikaisesti tosia, eli jos lauseet A_i ovat tosia, myös lauseen B on oltava.

Kirjassa [JohLog] semanttiset puut ja todistukset määritellään hieman tarkemmin ja todistetaan, että lause B on lauseiden $A_1, \dots, A_n$ looginen seuraus jos ja vain jos sillä on semanttinen todistus lauseista $A_1, \dots, A_n$.

2.7 Totuusfunktio

Tutkitaan lausetta "jokainen propositiolauseista p_0, p_1, p_2 ja p_3 pätee". On selvää, millä totuusjakaumilla tämän lauseen pitäisi olla totta, siis lauseen semantiikka on hyvin määritelty jo suomenkielisen muotoilun perusteella. Syntaksi sen sijaan ei ole. Tarkoitetaanko lauseella propositiolausetta

$$(p_0 \wedge (p_1 \wedge (p_2 \wedge p_3)))$$

vai lausetta

$$((p_0 \wedge p_1) \wedge (p_2 \wedge p_3))?$$

Vaiko kenties lausetta

$$(((p_0 \wedge p_1) \wedge p_2) \wedge p_3)?$$

Nämä kaikki ovat kuitenkin ekvivalentteja lauseita, joten usein ei ole väliä, millä näistä tavoista suomenkielinen väittämä formalisoidaan.

2.19 Lause. Olkoot A, B ja C mitä tahansa propositiolauseita. Tällöin $(A \wedge (B \wedge C)) \Leftrightarrow ((A \wedge B) \wedge C)$ ja $(A \vee (B \vee C)) \Leftrightarrow ((A \vee B) \vee C)$.

Todistus. Selvä. $\square$

Tästä lähtien käytämme lyhenteitä kuten $(p_0 \wedge p_5 \wedge p_{10})$ tai $(p_6 \vee p_4 \vee p_2 \vee p_0)$, kun emme jaksa täsmentää, missä järjestyksessä konjunktiot tai disjunktiot otetaan. Konnektiiveja ei kuitenkaan saa sotkea keskenään. Esimerkiksi lauseet $(p_0 \wedge (p_1 \vee p_2))$ ja $((p_0 \wedge p_1) \vee p_2)$ eivät ole ekvivalentteja, joten merkinnässä $(p_0 \wedge p_1 \vee p_2)$ ei ole järkeä. Myöskään lauseet $(p_0 \to (p_1 \to p_2))$ ja $((p_0 \to p_1) \to p_2)$ eivät ole ekvilentteja, eli merkintä $(p_0 \to p_1 \to p_2)$ ei ole sallittu.

Itseasiassa myös ekvivalenssille pätee $(A \leftrightarrow (B \leftrightarrow C)) \Leftrightarrow ((A \leftrightarrow B) \leftrightarrow C)$. "Ketjutetulla ekvivalenssilla" eli esimerkiksi lauseella $(p_0 \leftrightarrow p_1 \leftrightarrow p_2)$ ei kuitenkaan ole järkevää intuitiivista tulkintaa luonnollisen kielen väittämänä, joten emme käytä vastaavaa lyhennettä ekvivalenssille.

Tutkitaan nyt seuraavaa kysymystä: onko olemassa sellaista lausetta A, jossa esiintyisi propositiosymbolit p_0, p_1 sekä p_2, ja jonka totuustaulu näyttäisi seuraavalta:

p_0	p_1	p_2	A
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Sama kysymys yleisessä tilanteessa: Onko mitä tahansa ”mahdollista totuustaulua” kohti olemassa lause, jonka totuustaulu se on? Muotoillaksemme tämän kysymyksen formaalimmin, määritellään **totuusfunktio**.

2.20 Määritelmä. n**-paikkainen totuusfunktio** on mikä tahansa funktio $f\colon \{0,1\}^n \to \{0,1\}$. Mikäli A on propositiologiikan kaava, jossa ei esiinny muita propositiosymboleja, kuin $p_0, \ldots, p_{n-1}$, niin **lauseen** A n**-paikkainen totuusfunktio** $T_A\colon \{0,1\}^n \to \{0,1\}$ on kaavan

$$T_A(x_0, \ldots, x_{n-1}) = v[A], \text{ missä } v(i) = \begin{cases} x_i, & \text{kun } i < n \\ 1 & \text{muulloin} \end{cases}$$

määrittelemä totuusfunktio.

Kaavan A totuusfunktio siis kertoo, minkä totuusarvon arvon lause saa kullakin siinä esiintyvien propositiosymbolien totuusarvojen kombinaatiolla, eli täsmälleen miltä lauseen A totuustaulu näyttää.

p_0	$\cdots$	p_{n-2}	p_{n-1}	A
0	$\cdots$	0	0	$T_A(0,\ldots,0,0)$
0	$\cdots$	0	1	$T_A(0,\ldots,0,1)$
0	$\cdots$	1	0	$T_A(0,\ldots,1,0)$
0	$\cdots$	1	1	$T_A(0,\ldots,1,1)$
$\vdots$		$\vdots$	$\vdots$	$\vdots$
1	$\cdots$	0	0	$T_A(1,\ldots,0,0)$
1	$\cdots$	0	1	$T_A(1,\ldots,0,1)$
1	$\cdots$	1	0	$T_A(1,\ldots,1,0)$
1	$\cdots$	1	1	$T_A(1,\ldots,1,1)$

2.21 Esimerkki. Olkoon $A = (p_0 \vee (p_1 \vee p_2))$. Tällöin lauseen A totuusfunktio saadaan kaavasta

$$T_A(x_0, x_1, x_2) = \begin{cases} 1, & \text{jos } x_0 = 1,\ x_1 = 1 \text{ tai } x_2 = 1 \\ 0, & \text{muulloin} \end{cases}.$$

Siis

$$\begin{array}{lcllcl} T_A(0,0,0) & = & 0 & T_A(1,0,0) & = & 1 \\ T_A(0,0,1) & = & 1 & T_A(1,0,1) & = & 1 \\ T_A(0,1,0) & = & 1 & T_A(1,1,0) & = & 1 \\ T_A(0,1,1) & = & 1 & T_A(1,1,1) & = & 1. \end{array}$$

2.22 Esimerkki. Olkoon $A = (p_0 \wedge \neg p_0)$. Tällöin lauseen A totuusfunktio saa ainoastaan arvon 0, eli $T_A(0) = T_A(1) = 0$.

2.23 Lause. Olkoot A ja B propositiolauseita, joissa ei esiinny muita propositiosymboleja kuin $p_0, \ldots, p_{n-1}$. Tällöin $A \Leftrightarrow B$ jos ja vain jos $T_A = T_B$.

Todistus. Oletetaan aluksi, että $A \Leftrightarrow B$. Olkoon $(x_0, \ldots, x_{n-1}) \in \{0,1\}^n$ ja v totuusjakauma, jolla

$$v(i) = \begin{cases} x_i, & \text{kun } i < n \\ 1 & \text{muulloin} \end{cases}.$$

Tällöin $T_A(x_0, \ldots, x_{n-1}) = v[A]$ ja $T_B(x_0, \ldots, x_{n-1}) = v[B]$. Koska lauseet A ja B ovat ekvivalentteja, $v[A] = v[B]$, joten $T_A(x_0, \ldots, x_{n-1}) = T_B(x_0, \ldots, x_{n-1})$.

Siis $T_A = T_B$.

Oletetaan sitten, että $T_A = T_B$. Olkoon $v \colon \mathbb{N} \to \{0,1\}$ mielivaltainen totuusjakauma. Olkoon v' uusi totuusjakauma, jolla

$$v'(i) = \begin{cases} v(i), & \text{kun } i < n \\ 1 & \text{muulloin} \end{cases}.$$

Koska totuusjakaumat v ja v' antavat propositiosymboleille $p_0, \ldots, p_{n-1}$ samat totuusarvot, eikä lauseissa A ja B esiinny muita symboleja, $v[A] = v'[A]$ ja $v[B] = v'[B]$. Tällöin

$$\begin{aligned} v[A] &= v'[A] \\ &= T_A(v(0), \ldots, v(n-1)) \\ &= T_B(v(0), \ldots, v(n-1)) \\ &= v'[B] \\ &= v[B]. \end{aligned}$$

□

Nyt voimme muotoilla alkuperäisen kysymyksemme hieman formaalimmin: Onko jokainen totuusfunktio jonkin propositiolauseen totuusfunktio?

2.24 Lause. Olkoon f n-paikkainen totuusfunktio. Tällöin on olemassa propositiolause A, jossa ei esiinny muita propositiosymboleja kuin $p_0, \ldots, p_{n-1}$ eikä muita konnektiiveja kuin $\neg$, $\wedge$ ja $\vee$, ja jolle pätee $T_A = f$.

Todistus. Olkoon f n-paikkainen totuusfunktio. Jos f saa vain arvon 0, voidaan valita $A = (p_0 \wedge \neg p_0)$. Jos f saa vähintään yhdellä syötteellä arvon 1, toimitaan seuraavasti. Määritellään jokaisella $\bar{x} = (x_0, \ldots, x_{n-1}) \in \{0,1\}^n$ propositiolause $A_{\bar{x}}$:

$$A_{\bar{x}} = (q_0 \wedge q_1 \wedge \ldots \wedge q_{n-1}), \quad \text{missä } q_i = \begin{cases} p_i, & \text{jos } x_i = 1 \\ \neg p_i, & \text{jos } x_i = 0 \end{cases}.$$

Ideana on siis, että propositiolause $A_{\bar{x}}$ saa arvon 1 vain silloin, kun totuusjakauman arvot vastaavat jonon $\bar{x}$ arvoja. Esimerkiksi jos $n = 5$ ja $\bar{x} = (0,1,1,0,1)$, niin

$$A_{\bar{x}} = (\neg p_0 \wedge p_1 \wedge p_2 \wedge \neg p_3 \wedge p_4)$$

ja $v[A_{\bar{x}}] = 1$ jos ja vain jos $v(0) = 0$, $v(1) = 1$, $v(2) = 1$, $v(3) = 0$ ja $v(4) = 1$.

Olkoon nyt $X = \{\bar{x} \in \{0,1\}^n : f(\bar{x}) = 1\}$. Koska f saa arvon 1 jollakin jonolla $\bar{x}$, X on epätyhjä. Olkoon A disjunktio kaikista niistä lauseista $A_{\bar{x}}$, joilla $\bar{x} \in X$.

Olkoon v totuusjakauma, jolla

$$v(i) = \begin{cases} x_i, & \text{kun } i < n \\ 1 & \text{muulloin} \end{cases}$$

Nyt selvästi $T_A = f$. □

Seuraava esimerkki toivottavasti valottaa hieman lauseen 2.24 todistusta.

2.25 Esimerkki. Olkoon f 3-paikkainen totuusfunktio, jonka arvot ovat:

$$\begin{array}{rclcrcl} f(0,0,0) & = & 0 & \quad & f(1,0,0) & = & 0 \\ f(0,0,1) & = & 0 & & f(1,0,1) & = & 0 \\ f(0,1,0) & = & 1 & & f(1,1,0) & = & 0 \\ f(0,1,1) & = & 1 & & f(1,1,1) & = & 1 \end{array}$$

Lauseet $A_{\bar{x}}$ toteutuvat ainoastaan yhdellä totuustaulun rivillä, esimerkiksi

$$\begin{array}{rcl} A_{(0,0,0)} & = & (\neg p_0 \wedge \neg p_1 \wedge \neg p_2) \\ A_{(0,0,1)} & = & (\neg p_0 \wedge \neg p_1 \wedge p_2) \\ A_{(1,0,1)} & = & (p_0 \wedge \neg p_1 \wedge p_2). \end{array}$$

Joukko X sisältää ne kolmikot (x_0, x_1, x_2), joilla $f(x_0, x_1, x_2) = 1$, eli $X = \{(0,1,0), (0,1,1), (1,1,1)\}$, ja tällöin

$$\begin{array}{rcl} A & = & A_{(0,1,0)} \vee A_{(0,1,1)} \vee A_{(1,1,1)} \\ & = & (\neg p_0 \wedge p_1 \wedge \neg p_2) \vee (\neg p_0 \wedge p_1 \wedge p_2) \vee (p_0 \wedge p_1 \wedge p_2). \end{array}$$

Lause siis sanoo vapaasti tulkittuna, että jokainen mahdollinen asiaintila voidaan ilmaista konnektiiveilla $\neg$, $\wedge$ sekä $\vee$. Hieman täsmällisemmin:

2.26 Määritelmä. Joukko K konnektiiveja on **täydellinen**, mikäli jokaisella $n \in \mathbb{N}$, jokaista totuusfunktiota $f\colon \{0,1\}^n \to \{0,1\}$ kohti löytyy jokin lause A, jossa ei esiinny muita konnektiiveja kuin joukossa K olevia, ja muita propositiosymboleja kuin $p_0, \dots, p_{n-1}$, ja jolla $f = T_A$.

Täydellisen konnektiivijoukon sisältävä konnektiivijoukko on tietysti itsekin täydellinen.

Ylläoleva lause siis sanoo, että konnektiivijoukko $\{\neg, \wedge, \vee\}$ on **täydellinen**, erityisesti, että joukko $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ on täydellinen. Lauseessa konstruoitu propositiolause A on esimerkki **disjunktiivisessa normaalimuodossa** olevasta lauseesta. Kappaleessa A puhutaan lisää tällaisista lauseista.

Muita täydellisiä konnektiivijoukkoja ovat esimerkiksi $\{\neg, \wedge\}$, $\{\neg, \vee\}$ sekä $\{\neg, \rightarrow\}$. Siis ylläolevan lauseen propositiolause A voidaan valita jopa niin, että siinä ei esiinny esimerkiksi muita konnektiiveja kuin $\neg$ ja $\wedge$.

2.27 Esimerkki. Konnektiivijoukko $\{\neg, \wedge\}$ on täydellinen.

Todistus. Näytetään aluksi, että jokaista propositiolausetta A kohti on olemassa ekvivalentti lause, jossa ei esiinny muita konnektiiveja kuin $\neg$ ja $\wedge$, ja jossa esiintyy samat propositiosymbolit kuin lauseessa A. Tämä onnistuu induktiolla lauseen A rakenteen suhteen.

$\boxed{p_i}$ Olkoon aluksi $A = p_i$ jollakin $i \in \mathbb{N}$. Lauseessa A ei esiinny konnektiiveja lainkaan, joten voimme valita lauseen A.

$\boxed{\neg}$ Oletetaan, että väite pätee lauseelle A ja näytetään, että se pätee myös lauseelle $\neg A$. Siis löytyy lause A', jossa ei ole muita konnektiiveja kuin $\neg$ ja $\wedge$, ja jolla $A \Leftrightarrow A'$. Nyt lauseessa $\neg A'$ ei esiinny muita konnektiiveja kuin $\neg$ ja $\wedge$. Koska mielivaltaisella totuusjakaumalla v pätee

$$\begin{aligned} v[\neg A'] = 1 \quad &\Longleftrightarrow \quad v[A'] = 0 \\ &\overset{\text{i.o.}}{\Longleftrightarrow} \quad v[A] = 0 \\ &\Longleftrightarrow \quad v[\neg A] = 1, \end{aligned}$$

niin $\neg A' \Leftrightarrow \neg A$. Voidaan siis valita lause $\neg A'$.

$\boxed{\wedge}$ Oletetaan, että väite pätee lauseille A ja B ja näytetään, että se pätee myös lauseelle $(A \wedge B)$. Olkoot A' ja B' lauseita, joissa ei esiinny muita konnektiiveja kuin $\neg$ ja $\wedge$, ja joille $A \Leftrightarrow A'$ ja $B \Leftrightarrow B'$. Tällöin lauseessa $(A' \wedge B')$ ei esiinny muita konnektiiveja kuin $\neg$ ja $\wedge$ ja

$$\begin{aligned} v[(A' \wedge B')] = 1 \quad &\Longleftrightarrow \quad v[A'] = 1 \text{ ja } v[B'] = 1 \\ &\overset{\text{i.o.}}{\Longleftrightarrow} \quad v[A] = 1 \text{ ja } v[B] = 1 \\ &\Longleftrightarrow \quad v[(A \wedge B)] = 1, \end{aligned}$$

joten $(A' \wedge B') \Leftrightarrow (A \wedge B)$. Lause $(A' \wedge B')$ siis kelpaa.

$\boxed{\vee}$ Oletetaan, että väite pätee lauseille A ja B ja näytetään, että se pätee myös lauseelle $(A \vee B)$. Olkoot A' ja B' kuten kohdassa $\boxed{\wedge}$. Tällöin lauseessa $\neg(\neg A' \wedge \neg B')$ ei esiinny muita konnektiiveja kuin $\neg$ ja $\wedge$ ja

$$\begin{aligned}
v[\neg(\neg A' \wedge \neg B')] = 1 &\iff v[(\neg A' \wedge \neg B')] = 0 \\
&\iff v[\neg A'] = 0 \text{ tai } v[\neg B'] = 0 \\
&\iff v[A'] = 1 \text{ tai } v[B'] = 1 \\
&\overset{\text{i.o.}}{\iff} v[A] = 1 \text{ tai } v[B] = 1 \\
&\iff v[(A \vee B)] = 1,
\end{aligned}$$

joten $\neg(\neg A' \wedge \neg B') \Leftrightarrow (A \vee B)$. Lause $\neg(\neg A' \wedge \neg B')$ siis kelpaa.

$\boxed{\rightarrow}$, $\boxed{\leftrightarrow}$ Jätetään lukijan vastuulle.

Olkoon nyt $n \in \mathbb{N}$ ja f jokin n-paikkainen totuusfunktio. Koska joukko $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ on täydellinen konnektiivijoukko, löytyy näistä muodostettu lause A, jolle pätee $f = T_A$. Olkoon nyt A' lauseen A kanssa ekvivalentti propositiolause, jossa esiintyy vain konnektiiveja $\neg$ ja $\wedge$, ja jossa esiintyy samat propositiosymbolit kuin lauseessa A. Tällöin $T_A = T_{A'}$, joten $f = T_{A'}$. Siis konnektiivijoukko $\{\neg, \wedge\}$ on täydellinen. $\square$

2.8 Päättely

Tässä kappaleessa tutustumme *päättelyyn*, eli todistamiseen, eli deduktioon. Matemaattisen logiikan ajatellaan muodostavan perusteet matematiikan tekemiselle, ja mitä olisikaan matematiikka ilman todistuksia. Todistaminen on prosessi, jossa lähdetään joistakin *aksioomista*, ja näistä aksioomista tehdään päätelmiä tarkasti määriteltyjen sääntöjen avulla. Todistaminen on siis hyvin syntaktista, eikä sitä pidä sekoittaa semanttiseen *totuuden* käsitteeseen. Todistamme myöhemmin propositiologiikan *eheyslauseen* ja *täydellisyyslauseen*, jotka kuvailevat tarkemmin todistamisen ja totuuden suhdetta.

Erilaisia todistusjärjestelmiä on useita. Tässä tutustumme näistä erääseen, jota nimitetään *luonnolliseksi päättelyksi*. Tarkastellaan klassista päättelyä

$$\frac{\begin{array}{l}\text{Jokainen mies on kuolevainen.}\\ \text{Sokrates on mies.}\end{array}}{\text{Sokrates on kuolevainen.}}$$

Koska *kvantifiointi* (ylläolevan päättelyn sana ”jokainen”, $\forall$) kuuluu propositiologiikan sijasta predikaattilogiikkaan, tarkastellaan päättelystä hieman yksinkertaistettua versiota

$$\frac{\begin{array}{l}\text{Jos Sokrates on mies, Sokrates on kuolevainen.}\\ \text{Sokrates on mies.}\end{array}}{\text{Sokrates on kuolevainen.}}$$

Merkitään propositiosymbolilla p_0 lausetta "Sokrates on mies" ja symbolilla p_1 lausetta "Sokrates on kuolevainen". Ylläoleva päättely näyttää tällöin luonnollisen päättelyn kielelle muotoiltuna seuraavalta:

$$\frac{(p_0 \to p_1) \quad p_0}{p_1} \,{\scriptstyle \to E}$$

Päättely luetaan seuraavasti: viiva kuvaa yhtä päättelyaskelta, ja sen oikeassa laidassa oleva merkintä kertoo, mitä päättelysääntöä on käytetty. Tässä on käytettä päättelysääntöä "$\to$ E", eli *implikaation eliminointia*. Ylimpinä olevat lauseet ovat päättelyssä käytetyt oletukset ja alimpana on johtopäätös. Päättelysääntö $\to E$ voidaan intuitiivisesti tulkita niin, että mikäli tiedämme, että väitteestä A seuraa aina väite B, ja lisäksi väite A pätee, myös väitteen B on pädettävä.

Esimerkki hieman pidemmästä päättelystä:

$$\frac{\dfrac{\dfrac{\neg\neg p_0}{p_0}\,{\scriptstyle \neg E} \quad (p_0 \to \neg p_1)}{\neg p_1}\,{\scriptstyle \to E} \quad \dfrac{(p_3 \land p_2)}{p_2}\,{\scriptstyle \land E}}{(\neg p_1 \land p_2)}\,{\scriptstyle \land I}$$

Tässä päättelyssä oletuksina eli aksioomina ovat siis lauseet $\neg\neg p_0$, $(p_0 \to \neg p_1)$ sekä $(p_3 \land p_2)$. Näistä päätellään johtopäätös $(\neg p_1 \land p_2)$.

Seuraavassa taulukossa on lista kaikista päättelysäännöistä.

konnektiivi	introduktio	eliminointi
negaatio	$\dfrac{\begin{matrix}[A] \\ \vdots \\ (B \land \neg B)\end{matrix}}{\neg A}\,{\scriptstyle \neg I}$	$\dfrac{\neg\neg A}{A}\,{\scriptstyle \neg E}$
konjunktio	$\dfrac{A \quad B}{(A \land B)}\,{\scriptstyle \land I}$	$\dfrac{(A \land B)}{A}\,{\scriptstyle \land E} \qquad \dfrac{(A \land B)}{B}\,{\scriptstyle \land E}$
disjunktio	$\dfrac{A}{(A \lor B)}\,{\scriptstyle \lor I} \qquad \dfrac{B}{(A \lor B)}\,{\scriptstyle \lor I}$	$\dfrac{(A \lor B) \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}\,{\scriptstyle \lor E}$
implikaatio	$\dfrac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{(A \to B)}\,{\scriptstyle \to I}$	$\dfrac{(A \to B) \quad A}{B}\,{\scriptstyle \to E}$
ekvivalenssi	$\dfrac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ A\end{matrix}}{(A \leftrightarrow B)}\,{\scriptstyle \leftrightarrow I}$	$\dfrac{(A \leftrightarrow B) \quad A}{B}\,{\scriptstyle \leftrightarrow E} \qquad \dfrac{(A \leftrightarrow B) \quad B}{A}\,{\scriptstyle \leftrightarrow E}$

Kun oletus hylätään ja merkitään hakasulkuihin, hakasulkujen yläindeksiin ja käytetyn päättelysäännön viereen merkitään sama numero, jotta on helpompi lukea, missä vaiheessa oletus on hylätty. Päättelysääntöä, jossa jokin oletus hylätään, voidaan käyttää vaikkei kyseistä oletusta ole edes tehty. Tällöin mitään ei merkitä hakasulkuihin. Esimerkiksi

$$\frac{B}{(A \to B)} \to I$$

on sallittu päättely. Jos tiedämme että lause B pätee aina, niin tietysti se pätee myös jos lause A pätee.

2.28 Esimerkki. Päätellään $(A \vee B)$ oletuksesta $(A \wedge B)$. Päättelyn voi tehdä monella tavalla, esimerkiksi näin: Koska sekä A että B pätevät, A pätee, joten ainakin jompikumpi lauseista A ja B pätee. Siis

$$\cfrac{\cfrac{(A \wedge B)}{A}\,{\scriptstyle \wedge E}}{(A \vee B)}\,{\scriptstyle \vee I}$$

Muutamassa päättelysäännössä jokin oletus on merkitty hakasulkuihin eli hylätty. Esimerkiksi päättelysääntö $\to I$,

$$\frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{(A \to B)}\,{\scriptstyle \to I}$$

toimii näin: Mikäli on olemassa päättely lauseelle B, jossa oletuksena on A, tiedämme, että lause A implikoi lauseen B, riippumatta siitä onko lause A tosi vai ei.

Mietitään seuraavaa väittämää:

Jos kreikkalaiset ovat ihmisiä ja ihmiset ovat kuolevaisia,
niin kreikkalaiset ovat kuolevaisia. (3)

Väite kuulostaa tautologiselta, joten pitäisi olla jokin keino todistaa (päätellä) se. Formalisoidaan väite:

p_0: x on kreikkalainen
p_1: x on ihminen
p_2: x on kuolevainen

Nyt väite 3 voidaan ajatella näin: oletuksista $(p_0 \to p_1)$ ja $(p_1 \to p_2)$ pitäisi päätellä

$(p_0 \to p_2)$. Merkitään tätä A. Sanallisesti todistus voisi mennä esimerkiksi näin:

> Oletetaan, että jokainen kreikkalainen on ihminen ja että jokainen ihminen on kuolevainen.
> Oletetaan, että x on kreikkalainen.
> Ensimmäisen oletuksen nojalla x on ihminen. Koska jokainen ihminen on kuolevainen toisen oletuksen nojalla, niin x on kuolevainen.
> Siis jokainen kreikkalainen on kuolevainen.

Oletus *x on kreikkalainen* hylätään siinä vaiheessa, kun tehdään päätelmä *jokainen kreikkalainen on kuolevainen*. Muotoillaan todistus luonnollisen päättelyn kielelle. Aluksi oletamme lauseet $(p_0 \to p_1)$, $(p_1 \to p_2)$. Seuraavaksi oletamme vielä lauseen p_0. Lauseista p_0 ja $(p_0 \to p_1)$ voimme tietysti päätellä lauseen p_1:

$$\frac{(p_0 \to p_1) \qquad p_0}{p_1}\,{\scriptstyle \to E}$$

Lauseesta p_1 ja lauseesta $(p_1 \to p_2)$ voimme puolestamme päätellä p_2:

$$\frac{(p_1 \to p_2) \qquad \dfrac{(p_0 \to p_1) \qquad p_0}{p_1}\,{\scriptstyle \to E}}{p_2}\,{\scriptstyle \to E}$$

Näemme siis, että lauseesta p_0 seuraa lause p_2, joten tiedämme, että $(p_0 \to p_2)$:

$$\frac{\dfrac{(p_1 \to p_2) \qquad \dfrac{(p_0 \to p_1) \qquad [p_0]^1}{p_1}\,{\scriptstyle \to E}}{p_2}\,{\scriptstyle \to E}}{(p_0 \to p_2)}\,{\scriptstyle \to I,1}$$

Tehdäksemme tämän päätelmän, meidän ei siis tarvitse oikeasti olettaa, että *x on kreikkalainen*, vaan päätelmä

> Oletetaan, että x on kreikkalainen.
> Ensimmäisen oletuksen nojalla x on ihminen. Koska jokainen ihminen on kuolevainen toisen oletuksen nojalla, niin x on kuolevainen.

on tavallaan todistuksen sivujuoni, jossa näytetään että kreikkalaisuudesta seuraa kuolevaisuus.

2.29 Esimerkki. Päätellään $(\neg A \wedge \neg B)$ oletuksesta $\neg(A \vee B)$. Siis mikäli tiedämme, että lause ”A tai B” *ei päde*, niin kumpikaan lauseista A ja B ei voi päteä.

$$\frac{\dfrac{\dfrac{\dfrac{[A]^1}{(A \vee B)}\,{\scriptstyle \vee I} \qquad \neg(A \vee B)}{((A \vee B) \wedge \neg(A \vee B))}\,{\scriptstyle \wedge I}}{\neg A}\,{\scriptstyle \neg I,1} \qquad \dfrac{\dfrac{\dfrac{[B]^2}{(A \vee B)}\,{\scriptstyle \vee I} \qquad \neg(A \vee B)}{((A \vee B) \wedge \neg(A \vee B))}\,{\scriptstyle \wedge I}}{\neg B}\,{\scriptstyle \neg I,2}}{(\neg A \wedge \neg B)}\,{\scriptstyle \wedge I}$$

2.30 Esimerkki. Päätellään lause $(A \leftrightarrow B)$ oletuksesta $(\neg A \leftrightarrow \neg B)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{[A]^3 \quad \dfrac{(\neg A \leftrightarrow \neg B) \quad [\neg B]^1}{\neg A}{\scriptstyle \leftrightarrow E}}{(A \wedge \neg A)}{\scriptstyle \wedge I}}{\neg\neg B}{\scriptstyle \neg I,1}}{B}{\scriptstyle \neg E} \qquad \dfrac{\dfrac{\dfrac{[B]^3 \quad \dfrac{(\neg A \leftrightarrow \neg B) \quad [\neg A]^2}{\neg B}{\scriptstyle \leftrightarrow E}}{(B \wedge \neg B)}{\scriptstyle \wedge I}}{\neg\neg A}{\scriptstyle \neg I,2}}{A}{\scriptstyle \neg E}}{(A \leftrightarrow B)}{\scriptstyle \leftrightarrow I,3}$$

2.31 Esimerkki. Ristiriidasta voidaan päätellä mitä tahansa. Olkoot A ja B mitä tahansa lauseita. Päätellään:

$$\dfrac{\dfrac{(A \wedge \neg A)}{\neg\neg B}{\scriptstyle \neg I}}{B}{\scriptstyle \neg E}$$

Tässä sääntöä $\neg I$ käytetään surkastuneessa muodossa: oletus $\neg B$ hylätään, vaikkei sitä ole edes tehty.

Päättelyitä merkitään yleensä kirjaimilla $\mathcal{P}, \mathcal{Q}, \mathcal{R}, \ldots$. Jokaisella päättelyllä on joukko oletuksia, sekä johtopäätös, jotka ovat kaikki propositiologiikan lauseita. Mikäli päättely $\mathcal{P}$ kirjoitetaan muodossa $\begin{matrix}\mathcal{P}\\ A\end{matrix}$, tarkoitetaan, että A on päättelyn $\mathcal{P}$ johtopäätös. Kirjoittamalla $\begin{matrix}A\\ \mathcal{P}\\ B\end{matrix}$ tarkoitetaan, että A joko kuuluu tai ei kuulu päättelyn $\mathcal{P}$ oletusten joukkoon, ja päättelyn johtopäätös on B. Tässä merkinnässä ideana on, että lause A on varattu *hylättäväksi*, eli kun päättely kirjoitetaan muodossa $\begin{matrix}[A]\\ \mathcal{P}\\ B\end{matrix}$ on oletus A hylätty.

Määrittelemme nyt lähestulkoon formaalisti, mitä päättelyt, eli todistukset ovat. Määritelmä on propositiolauseiden määritelmän kaltainen *rekursiivinen määritelmä*, jonka suhteen voidaan tehdä induktio aivan kuten propositiolauseiden tapauksessa. Näin tehdäänkin esimerkiksi eheyslauseen todistuksessa.

2.32 Määritelmä. Päättelyiden joukko määritellään seuraavasti:

$\boxed{A}$ Mikäli A on propositiologiikan lause, niin A on päättely, jonka ainut oletus on A ja johtopäätös A.

$\boxed{\neg}$ Mikäli $\begin{matrix}\mathcal{P}\\ \neg\neg A\end{matrix}$ on päättely, jonka johtopäätös on $\neg\neg A$, niin $\dfrac{\begin{matrix}\mathcal{P}\\ \neg\neg A\end{matrix}}{A}$ on päättely, jolla on samat oletukset kuin alkuperäisellä päättelyllä, ja jonka johtopäätöksenä on A. Mikäli $\begin{matrix}A\\ \mathcal{P}\\ (B \wedge \neg B)\end{matrix}$ on päättely, jonka oletusten joukko on Σ, niin $\dfrac{\begin{matrix}[A]\\ \mathcal{P}\\ (B \wedge \neg B)\end{matrix}}{\neg A}$ on päättely, jonka oletusten joukko on $\Sigma \setminus \{A\}$. Huomaa, että lauseen A *ei tarvitse* olla joukossa Σ. Mikäli se on, niin se **hylätään** tätä päättelysääntöä käytettäessä.

$\boxed{\wedge}$ Mikäli $\begin{matrix}\mathcal{P}\\(A\wedge B)\end{matrix}$ on päättely, niin sekä $\dfrac{\begin{matrix}\mathcal{P}\\(A\wedge B)\end{matrix}}{A}$ että $\dfrac{\begin{matrix}\mathcal{P}\\(A\wedge B)\end{matrix}}{B}$ ovat päättelyitä, joilla on samat oletukset kuin alkuperäisellä päättelyllä. Mikäli $\begin{matrix}\mathcal{P}\\A\end{matrix}$ ja $\begin{matrix}\mathcal{Q}\\B\end{matrix}$ ovat päättelyitä, joiden oletusten joukot ovat $\Sigma_\mathcal{P}$ sekä $\Sigma_\mathcal{Q}$, niin $\dfrac{\begin{matrix}\mathcal{P}\\A\end{matrix}\quad\begin{matrix}\mathcal{Q}\\B\end{matrix}}{(A\wedge B)}$ on päättely, jonka oletusten joukkona on $\Sigma_\mathcal{P}\cup\Sigma_\mathcal{Q}$.

$\boxed{\vee}$ Mikäli $\begin{matrix}\mathcal{P}\\A\end{matrix}$ on päättely, niin sekä $\dfrac{\begin{matrix}\mathcal{P}\\A\end{matrix}}{(A\vee B)}$ että $\dfrac{\begin{matrix}\mathcal{P}\\A\end{matrix}}{(B\vee A)}$ ovat päättelyitä, joilla on samat oletukset kuin alkuperäisellä päättelyllä. Mikäli $\begin{matrix}\mathcal{R}\\(A\vee B)\end{matrix}$, $\begin{matrix}A\\\mathcal{P}\\C\end{matrix}$ ja $\begin{matrix}B\\\mathcal{Q}\\C\end{matrix}$ ovat päättelyjä, joiden oletusten joukkoina ovat $\Sigma_\mathcal{R}$, $\Sigma_\mathcal{P}$ sekä $\Sigma_\mathcal{Q}$, niin $\dfrac{\begin{matrix}\mathcal{R}\\(A\vee B)\end{matrix}\quad\begin{matrix}[A]\\\mathcal{P}\\C\end{matrix}\quad\begin{matrix}[B]\\\mathcal{Q}\\C\end{matrix}}{C}$ on päättely, jonka oletusten joukkona on $\Sigma_\mathcal{R}\cup(\Sigma_\mathcal{P}\setminus\{A\})\cup(\Sigma_\mathcal{Q}\setminus\{B\})$.

$\boxed{\to}$ Mikäli $\begin{matrix}\mathcal{P}\\A\end{matrix}$ ja $\begin{matrix}\mathcal{Q}\\(A\to B)\end{matrix}$ ovat päättelyitä, joiden oletusten joukot ovat $\Sigma_\mathcal{P}$ sekä $\Sigma_\mathcal{Q}$, niin $\dfrac{\begin{matrix}\mathcal{P}\\A\end{matrix}\quad\begin{matrix}\mathcal{Q}\\(A\to B)\end{matrix}}{B}$ on päättely, jonka oletusten joukkona on $\Sigma_\mathcal{P}\cup\Sigma_\mathcal{Q}$. Mikäli $\begin{matrix}A\\\mathcal{P}\\B\end{matrix}$ on päättely, jonka oletusten joukkona on Σ, niin $\dfrac{\begin{matrix}[A]\\\mathcal{P}\\B\end{matrix}}{(A\to B)}$ on päättely, jonka oletusten joukkona on $\Sigma\setminus\{A\}$.

$\boxed{\leftrightarrow}$ Mikäli $\begin{matrix}\mathcal{P}\\A\end{matrix}$, $\begin{matrix}\mathcal{Q}\\B\end{matrix}$ sekä $\begin{matrix}\mathcal{R}\\(A\leftrightarrow B)\end{matrix}$ ovat päättelyitä, joiden oletusten joukot ovat $\Sigma_\mathcal{P}$, $\Sigma_\mathcal{Q}$ sekä $\Sigma_\mathcal{R}$, niin sekä $\dfrac{\begin{matrix}\mathcal{P}\\A\end{matrix}\quad\begin{matrix}\mathcal{R}\\(A\leftrightarrow B)\end{matrix}}{B}$ että $\dfrac{\begin{matrix}\mathcal{Q}\\B\end{matrix}\quad\begin{matrix}\mathcal{R}\\(A\leftrightarrow B)\end{matrix}}{A}$ ovat päättelyitä, jonka oletusten joukkona ovat $\Sigma_\mathcal{P}\cup\Sigma_\mathcal{R}$ sekä $\Sigma_\mathcal{Q}\cup\Sigma_\mathcal{R}$. Mikäli $\begin{matrix}A\\\mathcal{P}\\B\end{matrix}$ ja $\begin{matrix}B\\\mathcal{Q}\\A\end{matrix}$ ovat päättelyitä, jonka oletusten joukkoina ovat $\Sigma_\mathcal{P}$ sekä $\Sigma_\mathcal{Q}$, niin $\dfrac{\begin{matrix}[A]\\\mathcal{P}\\B\end{matrix}\quad\begin{matrix}[B]\\\mathcal{Q}\\A\end{matrix}}{(A\leftrightarrow B)}$ on päättely, jonka oletusten joukkona on $(\Sigma_\mathcal{P}\setminus\{A\})\cup(\Sigma_\mathcal{Q}\setminus\{B\})$.

2.33 Määritelmä. Olkoon Σ joukko propositiolauseita, ja A jokin propositiolause. Mikäli on olemassa päättely, jonka oletukset ovat kaikki joukossa Σ ja johtopäätös on A, sanotaan, että lause A on **todistuva joukosta** Σ. Tällöin merkitään $\Sigma \vdash A$. Mikäli $\emptyset \vdash A$, merkitään $\vdash A$.

Esimerkiksi $\{\neg(A \lor B)\} \vdash (\neg A \land \neg B)$ esimerkin 2.29 nojalla.

2.34 Esimerkki. $\{\neg A, (A \leftrightarrow B)\} \vdash \neg B$.

$$\dfrac{\dfrac{\dfrac{(A \leftrightarrow B) \quad [B]^1}{A}\,{\scriptstyle \leftrightarrow E} \qquad \neg A}{(A \land \neg A)}\,{\scriptstyle \land I}}{\neg B}\,{\scriptstyle \neg I,1}$$

2.35 Lause. Seuraavat ehdot ovat yhtäpitäviä millä tahansa lausejoukolla Σ.

1. $\Sigma \vdash (A \land \neg A)$ jollakin A.

2. $\Sigma \vdash B$ jokaisella propositiolauseella B.

Todistus. Suunta $\boxed{2 \Rightarrow 1}$ on selvä. Oletetaan siis, että $\Sigma \vdash (A \land \neg A)$ jollakin A, siis löytyy päättely $\begin{matrix} \mathcal{P} \\ (A \land \neg A) \end{matrix}$, jonka oletukset ovat kaikki joukossa Σ. Olkoon B mielivaltainen propositiolause. Tutkitaan päättelyä

$$\dfrac{\dfrac{\begin{matrix} [\neg B]^1 \\ \mathcal{P} \\ (A \land \neg A) \end{matrix}}{\neg\neg B}\,{\scriptstyle \neg I,1}}{B}\,{\scriptstyle \neg E}.$$

Tämän päättelyn oletukset löytyvät kaikki selvästi joukosta Σ, joten $\Sigma \vdash B$. $\square$

Mikäli Σ toteuttaa jomman kumman (ja siten molemmat) edellisen lauseen ehdoista, sanotaan, että Σ on **ristiriitainen**, muuten **ristiriidaton** eli **konsistentti**.

2.36 Lause. Olkoon Σ lausejoukko ja A propositiologiikan lause. Tällöin seuraavat ehdot ovat yhtäpitäviä.

1. $\Sigma \vdash A$.

2. $\Sigma \cup \{\neg A\}$ on ristiriitainen.

Todistus. $\boxed{\mathbf{1 \Rightarrow 2}}$ Oletetaan, että $\Sigma \vdash A$, eli löytyy päättely $\begin{matrix} \mathcal{P} \\ A \end{matrix}$, jonka kaikki oletukset ovat joukossa Σ. Tällöin päättely $\dfrac{\begin{matrix} \mathcal{P} \\ A \end{matrix} \quad \neg A}{(A \land \neg A)}\,{\scriptstyle \land I}$ osoittaa, että $\Sigma \cup \{\neg A\}$ on ristiriitainen.

$\boxed{\mathbf{2 \Rightarrow 1}}$ Oletetaan nyt, että $\Sigma \cup \{\neg A\}$ on ristiriitainen, eli löytyy päättely $\begin{array}{c}\neg A\\ \mathcal{P}\\ (p_0 \wedge \neg p_0)\end{array}$, jonka kaikki oletukset ovat joukossa $\Sigma \cup \{\neg A\}$. Tällöin päättely

$$\dfrac{\dfrac{\begin{array}{c}[\neg A]^1\\ \mathcal{P}\\ (p_0 \wedge \neg p_0)\end{array}}{\neg\neg A}\,{\scriptstyle \neg I,1}}{A}\,{\scriptstyle \neg E}$$

osoittaa, että $\Sigma \vdash A$.

□

2.9 Propositiologiikan eheys- ja täydellisyyslauseet

Eheys- ja täydellisyyslauseet ovat tärkeä linkki propositiologiikan syntaksin ja semantiikan välillä. Äkkiseltään ne saattavat väittämiltään vaikuttaa triviaaleilta, mutta sitä ne eivät missään nimessä ole. Niiden analogiat predikaattilogiikassa ovatkin huomattavasti vaikeammat todistaa.

Intuitiivisesti eheyslause sanoo, että päättelyjärjestelmämme on siinä mielessä "ehjä", että mikäli voimme päätellä eli todistaa jonkin lauseen, tämä lause todellakin pitää paikkansa. Emme siis pysty todistamaan ristiriitoja ristiriidattomista oletuksista. Täydellisyyslause taas sanoo, että päättelysääntöjemme kokoelma on siinä mielessä täydellinen, että pystymme todistamaan kaikki todet lauseet. Asiat, jotka voidaan todistaa, ovat siis täsmälleen ne, jotka ovat tosia.

Olkoon Σ joukko propositiolauseita ja A propositiolause. Mikäli millä tahansa totuusjakaumalla v, joka toteuttaa kaikki joukon Σ lauseet, v toteuttaa myös lauseen A, sanotaan, että A on **joukon Σ looginen seuraus**, ja merkitään $\Sigma \Rightarrow A$.

Propositiologiikan eheyslause. *Jos $\Sigma \vdash A$, niin $\Sigma \Rightarrow A$.*

Eheyslause on suora seuraus seuraavasta:

2.37 Lemma. Olkoon $\mathcal{P}$ päättely, jonka oletusten joukko on $\Sigma_{\mathcal{P}}$, ja johtopäätös A. Tällöin $\Sigma_{\mathcal{P}} \Rightarrow A$.

Todistus. Näytetään väite induktiolla päättelyn $\mathcal{P}$ rakenteen suhteen.

$\boxed{A}$ Jos päättely $\mathcal{P}$ koostuu vain triviaalista päätelmästä A, jonka oletuksena on A, $\Sigma_{\mathcal{P}} = \{A\}$. Jos totuusjakauma v toteuttaa kaikki joukon $\Sigma_{\mathcal{P}}$ lauseet, se toteuttaa lauseen A.

$\boxed{\neg}$ Oletetaan, että väite pätee päättelylle $\begin{array}{c}\mathcal{P}\\ \neg\neg A\end{array}$, eli että jos $v[B] = 1$ jokaisella $B \in \Sigma_{\mathcal{P}}$, niin $v[\neg\neg A] = 1$. Olkoon $\mathcal{Q}$ päättely $\dfrac{\begin{array}{c}\mathcal{P}\\ \neg\neg A\end{array}}{A}\,{\scriptstyle \neg E}$. Oletetaan, että v

toteuttaa kaikki päättelyn $\mathcal{Q}$ oletukset. Päättelyn $\mathcal{Q}$ oletukset ovat samat kuin päättelyssä $\mathcal{P}$, joten v toteuttaa myös kaikki päättelyn $\mathcal{P}$ oletukset. Induktio-oletuksen nojalla tällöin $v[\neg\neg A] = 1$. Koska $v[\neg\neg A] = v[A]$, $v[A] = 1$.

Oletetaan sitten, että väite pätee päättelylle $\begin{array}{c} A \\ \mathcal{P} \\ (B \wedge \neg B) \end{array}$. Siis mikäli v toteuttaa kaikki tämän päättelyn oletukset, niin v toteuttaa lauseen $(B \wedge \neg B)$. Tämä lause on kuitenkin ristiriita eikä voi toteutua, joten mikään totuusjakauma v ei voi toteuttaa kaikkia päättelyn $\mathcal{P}$ oletuksia samanaikaisesti. Olkoon nyt $\mathcal{Q}$ päättely $\dfrac{\begin{array}{c} [A] \\ \mathcal{P} \\ (B \wedge \neg B) \end{array}}{\neg A}$, ja oletetaan, että v toteuttaa kaikki päättelyn $\mathcal{Q}$ oletukset. Tällöin v ei voi toteuttaa lausetta A, sillä muuten se toteuttaisi kaikki päättelyn $\mathcal{P}$ oletukset, minkä totesimme mahdottomaksi. Siis $v[A] = 0$, joten $v[\neg A] = 1$.

$\boxed{\wedge}$ Oletetaan, että väite pätee päättelylle $\begin{array}{c} \mathcal{P} \\ (A \wedge B) \end{array}$ Olkoon $\mathcal{Q}$ päättely $\dfrac{\begin{array}{c} \mathcal{P} \\ (A \wedge B) \end{array}}{A}$ ja toteuttakoon v kaikki päättelyn $\mathcal{Q}$ oletukset. Koska päättelyillä $\mathcal{P}$ ja $\mathcal{Q}$ on samat oletukset, induktio-oletuksen nojalla $v[(A \wedge B)] = 1$, joten $v[A] = 1$. Samoin päättelylle $\dfrac{\begin{array}{c} \mathcal{P} \\ (A \wedge B) \end{array}}{B}$.

Oletetaan sitten, että väite pätee päättelyille $\begin{array}{c} \mathcal{P} \\ A \end{array}$ ja $\begin{array}{c} \mathcal{Q} \\ B \end{array}$. Olkoon $\mathcal{R}$ päättely $\dfrac{\begin{array}{c} \mathcal{P} \\ A \end{array} \quad \begin{array}{c} \mathcal{Q} \\ B \end{array}}{(A \wedge B)}$ ja toteuttakoon v kaikki sen oletukset. Nyt v tietysti toteuttaa kaikki päättelyiden $\mathcal{P}$ ja $\mathcal{Q}$ oletukset, joten indukio-oletuksen nojalla $v[A] = 1$ ja $v[B] = 1$, ja niin $v[(A \wedge B)] = 1$.

$\boxed{\vee}$ Oletetaan, että väite pätee päättelylle $\begin{array}{c} \mathcal{P} \\ A \end{array}$. Olkoon $\mathcal{Q}$ päättely $\dfrac{\begin{array}{c} \mathcal{P} \\ A \end{array}}{(A \vee B)}$ ja toteuttakoon v kaikki päättelyn $\mathcal{Q}$ oletukset. Päättelyissä $\mathcal{P}$ ja $\mathcal{Q}$ on samat oletukset, joten induktio-oletuksen nojalla $v[A] = 1$. Tällöin myös $v[(A \vee B)] = 1$. Samoin päättelylle $\dfrac{\begin{array}{c} \mathcal{P} \\ A \end{array}}{(B \vee A)}$.

Oletetaan sitten, että $\begin{array}{c} \mathcal{R} \\ (A \vee B) \end{array}$, $\begin{array}{c} A \\ \mathcal{P} \\ C \end{array}$ ja $\begin{array}{c} B \\ \mathcal{Q} \\ C \end{array}$ ovat päättelyjä, joille väite pätee. Olkoon $\mathcal{S}$ päättely $\dfrac{\begin{array}{c} \mathcal{R} \\ (A \vee B) \end{array} \quad \begin{array}{c} [A] \\ \mathcal{P} \\ C \end{array} \quad \begin{array}{c} [B] \\ \mathcal{Q} \\ C \end{array}}{C}$ ja olkoon v totuusjakauma, jolla päättelyn

$\mathcal{S}$ oletukset toteutuvat. Tällöin erityisesti päättelyn $\mathcal{R}$ oletukset toteutuvat, ja päättelyiden $\mathcal{P}$ ja $\mathcal{Q}$ oletukset toteutuvat, mahdollisesti lauseita A ja B lukuunottamatta. Koska päättelyn $\mathcal{R}$ oletukset toteutuvat, niin induktio-oletuksen nojalla $v[(A \vee B)] = 1$. Siis joko $v[A] = 1$ tai $v[B] = 1$. Jos $v[A] = 1$, niin päättelyn $\mathcal{P}$ kaikki oletukset ovat voimassa, joten induktio-oletuksen nojalla $v[C] = 1$. Mikäli taas $v[B] = 1$, niin päättelyn $\mathcal{Q}$ kaikki oletukset toteutuvat, joten induktio-oletuksen nojalla $v[C] = 1$. Kummassakin tapauksessa v toteuttaa lauseen C.

$\boxed{\rightarrow}$, $\boxed{\leftrightarrow}$ Jätetään lukijan tarkistettaviksi.

$\square$

Eheyslauseen todistus. Oletetaan, että $\Sigma \vdash A$. Löytyy siis jokin päättely $\mathcal{P}$, jonka oletusten joukko $\Sigma_{\mathcal{P}}$ sisältyy joukkoon Σ, ja jonka johtopäätös on A. Olkoon v totuusjakauma, jolla kaikki joukon Σ lauseet ovat tosia. Tällöin v toteuttaa erityisesti kaikki joukon $\Sigma_{\mathcal{P}}$ lauseet. Lauseen 2.37 nojalla $v[A] = 1$. $\square$

Eheyslauseen nojalla emme siis voi päätellä asioita, jotka eivät pidä paikkaansa. Meillä on nyt siis keino näyttää, että jotakin lausetta *ei* voida päätellä.

2.38 Esimerkki. $\{(p_0 \vee p_1), (p_0 \rightarrow (p_1 \vee p_2)), (p_1 \rightarrow p_2)\} \nvdash p_1$

Todistus. Merkitään $\Sigma = \{(p_0 \vee p_1), (p_0 \rightarrow (p_1 \vee p_2)), (p_1 \rightarrow p_2)\}$. Olkoon v totuusjakauma, jolla $v(0) = v(2) = 1$ ja $v(1) = 0$. Tällöin v toteuttaa jokaisen lauseista $(p_0 \vee p_1)$, $(p_0 \rightarrow (p_1 \vee p_2))$, ja $(p_1 \rightarrow p_2)$, mutta $v[p_1] = 0$. Siis $\Sigma \not\Rightarrow p_1$. Jos pätisi $\Sigma \vdash p_1$, niin eheyslauseen nojalla $\Sigma \Rightarrow p_1$, mikä olisi ristiriita. Täten $\Sigma \nvdash p_1$. $\square$

Siirrymme seuraavaksi täydellisyyslauseen todistukseen, joka on eheyslausetta hankalampi. Sanomme, että joukko Σ propositiolauseita on **täydellinen** (sanalla täydellinen ei tässä juuri ole yhteyttä täydellisyyteen siinä mielessä, mitä täydellisyyslauseessa tarkoitetaan), mikäli jokaisella propositiolauseella A, joko $A \in \Sigma$ tai $\neg A \in \Sigma$. Täydellinen joukko intuitiivisesti sisältää "ainakin puolet" kaikista propositiolauseista. Jos Σ on täydellinen ja ristiriidaton, joukkoon Σ ei voida enää lisätä yhtään uutta lausetta tekemättä siitä ristiriitaista, eli $\Sigma \cup \{A\}$ on ristiriitainen jokaisella $A \notin \Sigma$.

2.39 Lemma. Olkoon Σ ristiriidaton joukko propositiolauseita ja olkoon A propositiolause. Tällöin joko $\Sigma \cup \{A\}$ tai $\Sigma \cup \{\neg A\}$ on ristiriidaton.

Todistus. Oletetaan, että kumpikaan ei ole. Siis löytyy päättelyt $\dfrac{\mathcal{P}}{(p_0 \wedge \neg p_0)}$, jonka oletukset kuuluvat joukkoon $\Sigma \cup \{A\}$, ja $\dfrac{\mathcal{Q}}{(p_0 \wedge \neg p_0)}$ jonka oletukset kuuluvat joukkoon $\Sigma \cup \{\neg A\}$. Jää lukijan taakaksi varmistaa, että löytyy päättely $\mathcal{R}$, jonka oletusten joukko on $\emptyset$ ja johtopäätös $(A \vee \neg A)$. Tutkitaan päättelyä

$$\dfrac{\begin{array}{c} \\ \mathcal{R} \\ (A \vee \neg A) \end{array} \quad \begin{array}{c} [A]^1 \\ \mathcal{P} \\ (p_0 \wedge \neg p_0) \end{array} \quad \begin{array}{c} [\neg A]^1 \\ \mathcal{Q} \\ (p_0 \wedge \neg p_0) \end{array}}{(p_0 \wedge \neg p_0)} \vee E{,}1 \, .$$

Tämän oletukset sisältyvät kaikki joukkoon Σ, joten $\Sigma \vdash (p_0 \wedge \neg p_0)$. Σ on siis ristiriitainen. $\square$

2.40 Lemma (Lindenbaumin lemma). Olkoon Σ ristiriidaton joukko propositiolauseita. Tällöin on olemassa täydellinen, ristiriidaton $\Sigma' \supset \Sigma$.

Todistus. Kappaleessa 2.3 konstruoimme propositiolauseiden joukon P numeroituvana yhdisteenä numeroituvista joukoista $P_0, P_1, P_2, \ldots$, joten kaikkia propositiolauseita on numeroituvasti ääretön määrä. Olkoon $A_0, A_1, A_2, \ldots$ lista, joka luettelee kaikki propositiolauseet.

Määritellään rekursiivisesti kasvava jono lausejoukkoja. Olkoon $\Sigma_0 = \Sigma$, ja jokaisella $n \in \mathbb{N}$ olkoon

$$\Sigma_{n+1} = \begin{cases} \Sigma_n \cup \{A_n\}, & \text{jos } \Sigma_n \cup \{A_n\} \text{ on ristiriidaton} \\ \Sigma_n \cup \{\neg A_n\}, & \text{muuten} \end{cases}$$

Näin saadut lausejoukot Σ_n ovat edellisen lemman nojalla kaikki ristiriidattomia. Olkoon nyt $\Sigma' = \bigcup_{n \in \mathbb{N}} \Sigma_n$. Myös Σ' on ristiriidaton: jos se ei olisi, löytyisi päättely $\mathcal{P}$, jonka oletukset olisivat kaikki joukossa Σ', ja jonka johtopäätöksenä olisi $(p_0 \wedge \neg p_0)$. Koska todistuksissa on aina vain äärellisen monta oletusta, kaikki päättelyn $\mathcal{P}$ oletukset löytyivät jo jostain joukosta Σ_n, jolloin pätisi $\Sigma_n \vdash (p_0 \wedge \neg p_0)$. Joukko $\Sigma' \supset \Sigma$ on siis ristiriidaton. Lisäksi se on selvästi täydellinen. $\square$

Propositiologiikan täydellisyyslause. *Jos $\Sigma \Rightarrow A$, niin $\Sigma \vdash A$.*

Todistus. Oletetaan, että $\Sigma \nvdash A$. Tällöin lauseen 2.36 nojalla $\Sigma \cup \{\neg A\}$ on ristiriidaton, joten lemman 2.40 nojalla löytyy täydellinen, ristiriidaton $\Sigma' \supset \Sigma \cup \{\neg A\}$.

Määritellään nyt totuusjakauma v, niin että $v(n) = 1$ jos $p_n \in \Sigma'$, muulloin $v(n) = 0$. Näytetään induktiolla lauseen B rakenteen suhteen, että $v[B] = 1$ jos ja vain jos $B \in \Sigma'$.

$\boxed{p_n}$ Selvä.

$\boxed{\neg}$ Oletetaan, että väite pätee lauseelle B. Tällöin

$$\begin{aligned} v[\neg B] = 1 \quad &\iff \quad v[B] = 0 \\ &\overset{\text{i.o.}}{\iff} \quad B \notin \Sigma'. \end{aligned}$$

Jos $B \notin \Sigma'$, niin täydellisyyden nojalla $\neg B \in \Sigma'$. Jos taas $B \in \Sigma'$, niin ristiriidattomuuden nojalla $\neg B \notin \Sigma'$. Kummassakin tapauksessa $B \notin \Sigma' \iff \neg B \in \Sigma'$, joten $v[\neg B] = 1 \iff \neg B \in \Sigma'$.

$\boxed{\wedge}$ Oletetaan, että väite pätee lauseille B ja C. Jos $v[(B \wedge C)] = 1$, niin sekä $v[B] = 1$, että $v[C] = 1$. Induktio-oletuksen nojalla $B \in \Sigma'$ ja $C \in \Sigma'$. Jos pätisi $(B \wedge C) \notin \Sigma'$, niin täydellisyyden nojalla $\neg(B \wedge C) \in \Sigma'$. Lauseista B, C ja $\neg(B \wedge C)$ on kuitenkin helppo päätellä ristiriita, joten $(B \wedge C) \in \Sigma'$.

Oletetaan sitten, että $(B \wedge C) \in \Sigma'$. Ristiriidattomuuden nojalla $\neg B \notin \Sigma'$ ja $\neg C \notin \Sigma'$, joten täydellisyyden nojalla $B \in \Sigma'$ ja $C \in \Sigma'$. Induktio-oletuksen nojalla $v[B] = 1$ ja $v[C] = 1$, joten $v[(B \wedge C)] = 1$.

$\boxed{\vee}$ Oletetaan, että väite pätee lauseille B ja C. Jos $v[(B \vee C)] = 1$, niin joko $v[B] = 1$, tai $v[C] = 1$. Jos $v[B] = 1$, niin induktio-oletuksen nojalla $B \in \Sigma'$. Ristiriidattomuuden nojalla $\neg(B \vee C) \notin \Sigma'$, joten täydellisyyden nojalla $(B \vee C) \in \Sigma'$. Samoin, jos $v[C] = 1$.

Oletetaan nyt, että $(B \vee C) \in \Sigma'$. Tällöin ainakin jompikumpi lauseista B ja C on kuuluttava joukkoon Σ', sillä muutoin näiden negaatiot kuuluisivat joukkoon Σ' ja lauseista $\neg B$, $\neg C$ ja $(B \vee C)$ voitaisiin todistaa ristiriita. Mikäli $B \in \Sigma'$, induktio-oletuksen nojalla $v[B] = 1$, joten $v[(B \vee C)] = 1$. Samoin, jos $v[C] = 1$.

$\boxed{\rightarrow}$**,** $\boxed{\leftrightarrow}$ Jätetään lukijalle.

Siis jakauma v toteuttaa kaikki joukon Σ' lauseet, erityisesti kaikki joukon Σ lauseet, sekä lauseen $\neg A$. Siis A ei ole lauseen Σ looginen seuraus, eli $\Sigma \not\Rightarrow A$.

□

Yhdistämällä eheys- ja täydellisyyslauseet saadaan:

2.41 Korollaari. $\Sigma \vdash A \iff \Sigma \Rightarrow A$

3 Predikaattilogiikka

Siirrymme seuraavaksi propositiologiikasta predikaattilogiikkaan. Propositiologiikka on erittäin rajoittunut järjestelmä, jossa ei pysty ilmaisemaan monia hyvin yksinkertaisiakaan väittämiä. Tämä johtuu siitä, että propositiologiikan kielessä ei ole sanoja, joilla kuvata olioita. Predikaattilogiikassa otamme käyttöön *muuttujat*, joilla tämä onnistuu.

Propositiolauseiden semantiikka tarkoittaa käytännössä totuutta eri totuusjakaumilla. Totuusjakauma on kuitenkin hyvin rajoittunut mallinnus totuudelle tai ”mahdollisille tilanteille”, ja predikaattilogiikalla onkin propositiologiikkaa hyvin paljon rikkaampi semantiikka, mallit eli struktuurit. Totuus predikaattilogiikassa tarkoittaa totuutta jossakin mallissa. Malleja ovat esimerkiksi luonnolliset luvut, reaaliluvut, kompleksiluvut, erilaiset verkot ja järjestykset, algebralliset struktuurit, kuten monoidit, ryhmät, renkaat ja kunnat, relaatiotietokannat, erilaiset tietorakenteet sekä esimerkiksi kaikkien Facebookissa olevien ihmisten joukko kaveruussuhteineen. Mallin käsite on siis hyvin yleinen ja abstrakti.

Tämä kappale ei ole vielä valmis.

3.1 Relaatiot

Olkoon X jokin joukko. Joukon X **n-kertainen karteesinen tulo**, jota merkitään X^n tai $X \times X \times \ldots \times X$ (n kertaa), tarkoittaa kaikkien joukon X alkioiden n-pituisten jonojen joukkoa. Siis esimerkiksi $\mathbb{R}^2$ tarkoittaa reaalilukuparien eli tason pisteiden joukkoa, ja $\mathbb{R}^3$ tarkoittaa reaalilukukolmikoiden joukkoa.

Joukon X **kaksipaikkainen relaatio** R on mikä tahansa joukko joukon X alkioista muodostettuja pareja (x, y), joiden molemmat alkiot ovat joukossa X, siis $R \subset X^2$. Jos $(x, y) \in R$, sanotaan, että x **on y:n kanssa relaatiossa** R. Olkoon esimerkiksi X kaikkien koskaan eläneiden ihmisten joukko ja olkoon

$$R = \left\{(x, y) \in X^2 \colon x \text{ tietää, kuka } y \text{ on}\right\}.$$

Tällöin esimerkiksi *Einstein ja Gödel ovat relaatiossa R*, ja *Gödel ja Einstein ovat relaatiossa R*,

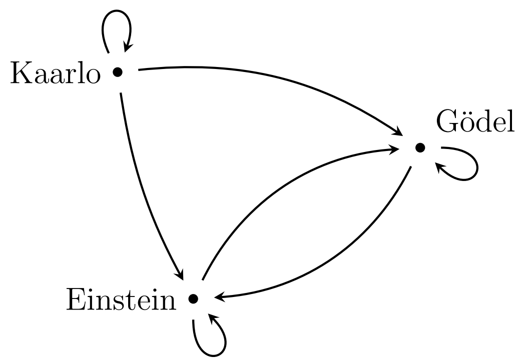
$$(\text{Einstein}, \text{Gödel}) \in R \quad \text{ja} \quad (\text{Gödel}, \text{Einstein}) \in R,$$

sillä Einstein ja Gödel olivat hyviä ystäviä. Myös

$$(\text{Kaarlo Reipas}, \text{Gödel}) \in R, \quad \text{mutta} \quad (\text{Gödel}, \text{Kaarlo Reipas}) \notin R,$$

sillä Gödel kuoli noin kymmenen vuotta ennen syntymääni, ja siten tuskin tiesi minusta mitään. Parien järjestyksellä on siis väliä, x ei välttämättä ole relaatiossa y:n kanssa, vaikka y olisi x:n kanssa. Todennäköisesti myös $(x, x) \in R$ suurimmalla osalla ihmisistä x, eli lähes kaikki ainakin jossain määrin tietävät, keitä itse ovat.

Relaatiota voi havainnollistaa **relaatiokaaviolla**. Relaation R relaatiokaavio on kuva, jossa merkitty jokaista joukon X alkiota pisteellä, ja piirretty nuoli pisteestä x pisteeseen y, mikäli $(x, y) \in R$. Tässä esimerkkinä osa edellämainitun relaation relaatiokaaviosta.



Se, että Gödel ei tuntenut Kaarloa, näkyy relaatiokaaviossa siten, että Gödelistä ei kulje nuolta Kaarloon.

3.1 Esimerkki. Olkoon $X = \mathbb{R}$ reaalilukujen joukko ja olkoon $R \subset X \times X$,

$$R = \{(x, y) \in X \times X \colon \text{luku } x \text{ on pienempi tai yhtäsuuri kuin luku } y\}.$$

Tällöin esimerkiksi $(3, \pi) \in R$ ja $(-99, 5) \in R$, mutta $(7, 6) \notin R$ ja $(4, 4) \in R$. Tätä relaatiota sanotaan **reaalilukujen järjestykseksi**, ja merkitään useimmiten symbolin R sijasta symbolilla $\leq$. Merkintä $(x, y) \in \leq$ lyhennetään tällöin $x \leq y$.

Relaatioita on erilaisia. Joukon X kaksipaikkaista relaatiota R sanotaan

- **refleksiiviseksi**, jos $(x, x) \in R$ jokaisella $x \in X$
- **irrefleksiiviseksi**, jos $(x, x) \notin R$ jokaisella $x \in X$
- **symmetriseksi**, jos $(x, y) \in R$ aina kun $(y, x) \in R$
- **antisymmetriseksi**, jos $(y, x) \notin R$ aina kun $(x, y) \in R$ ja $x \neq y$
- **transitiiviseksi**, jos $(x, z) \in R$ aina kun $(x, y) \in R$ ja $(y, z) \in R$
- **vertailulliseksi**, jos $(x, y) \in R$ tai $(y, x) \in R$ aina kun $x, y \in X$, $x \neq y$.

Järjestykset

3.2 Määritelmä. Relaatio on **osittaisjärjestys**, mikäli se on refleksiivinen, antisymmetrinen ja transitiivinen. Relaatio on **lineaarijärjestys**, mikäli se on näiden lisäksi vielä vertailullinen.

Joskus järjestysten määritelmässä refleksiivisyys korvataan irrefleksiivisyydellä. Tämän ei kuitenkaan pitäisi tuottaa sekaannusta, sillä refleksiiviset ja irrefleksiiviset järjestykset vastaavat yksikäsitteisesti toisiaan, refleksiivinen järjestys on helppo aina muuttaa irrefleksiiviseksi järjestykseksi ja päin vastoin. Esimerkiksi järjestys $<$ on irrefleksiivinen reaalilukujen joukossa, ja järjestys $\leq$ on vastaava refleksiivinen järjestys.

Lineaarijärjestyksiä ovat esimerkiksi reaalilukujen tavallinen järjestys $\leq$ tai sanakirjajärjestys kaikkien suomenkielisten sanojen joukossa. Osittaisjärjestyksiä ovat esimerkiksi luonnollisten lukujen jakorelaatio $|$ ($m|n$ mikäli $n = km$ jollakin kokonaisluvulla k) ja joukkojen sisältyvyysrelaatio $\subset$.

3.3 Esimerkki. Reaalilukujen relaatio $\leq$ on lineaarijärjestys.

Todistus. Osoitetaan lineaarijärjestykseltä vaadittavat ominaisuudet todeksi.

Selvästi $r \leq r$ millä tahansa reaaliluvulla $r \in \mathbb{R}$, joten $\leq$ on refleksiivinen.

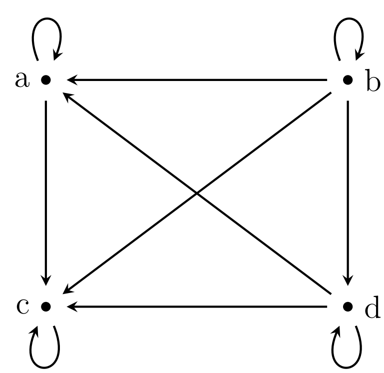
Olkoot r ja s reaalilukuja. Mikäli $r \leq s$ ja $s \leq r$, niin $r = s$, joten antisymmetrisyys on voimassa.

Olkoot $r, s, t \in \mathbb{R}$ reaalilukuja, joilla $r \leq s$ ja $s \leq t$. Tällöin tietysti $r \leq t$, joten transitiivisuus on voimassa.

Olkoot $r, s \in \mathbb{R}$, $r \neq s$. Tällöin tietysti jompikumpi luvuista r ja s on suurempi, joten joko $r \leq s$ tai $s \leq r$. Siis myös vertailullisuus on voimassa. $\square$

3.4 Esimerkki. Edellä mainittu tuntemisrelaatio R kaikkien koskaan eläneiden ihmisten joukossa ei ole lineaarijärjestys, eikä edes osittaisjärjestys. Se ei nimittäin toteuta esimerkiksi transitiivisuutta: vaikka x tuntee y:n ja y tuntee z:n, ei x välttämättä tunne z:aa. Myöskään antisymmetrisyys ei päde: esimerkiksi Einstein ja Gödel molemmat tunsivat toisensa.

3.5 Esimerkki. Olkoon $X = \{a, b, c, d\}$ ja $R \subset X^2$ seuraavan relaatiokaavion määräämä relaatio.



Tarkkailtuaan kaaviota hetken huomaa, että relaatio R on lineaarijärjestys. Sen voidaankin ajatella asettavan alkiot järjestykseen niin, että mikäli pisteestä x menee nuoli pisteeseen y, niin x on "pienempi tai yhtäsuuri" kuin y, tai tulee järjestyksessä ennen pistettä y. Relaation R määräämä järjestys on siis

$$b, d, a, c,$$

sillä $(b, d) \in R$, $(d, a) \in R$ ja $(a, c) \in R$.

Useampipaikkaiset relaatiot

Relaation *kaksipaikkaisuus* viittaa siihen, että kaksi alkiota ovat aina relaatiossa keskenään. Tällöin relaatio on siis joukko pareja. Tämä onkin useimmin käytetty relaatiotyyppi, mutta myös yksi- tai useampipaikkaiset relaatiot ovat joskus tarpeellisia.

3.6 Määritelmä. Olkoon X joukko, ja $n > 0$ luonnollinen luku. Joukkoa $R \subset X^n$, jonka alkiot ovat siis n-jonoja joukosta X, sanotaan **joukon X n-paikkaiseksi relaatioksi**.

3.7 Esimerkki. Olkoon $A \subset \mathbb{R}^3$ niiden reaalilukukolmikoiden (x, y, z) joukko, joilla $x + y + z = 0$. Esimerkiksi $(0, 0, 0)$, $(\pi, \pi - 1, 1 - 2\pi)$ ja $(8, -3, -5)$ kuuluvat relaatioon A, joukko-opillisella notaatiolla ilmaistuna $(0, 0, 0) \in A$, $(\pi, \pi - 1, 1 - 2\pi) \in A$ ja $(8, -3, -5) \in A$.

Esimerkkejä kolmikoista, jotka eivät kuulu relaatioon A ovat esimerkiksi $(1, 1, 1)$, $(0, 4, -5)$ ja $(6, 1, 6)$.

Yksipaikkaiset joukon X relaatiot, eli yhden alkion mittaiset jonot, voidaan yksinkertaisesti ajatella joukon X osajoukkoina. Tästä syystä niitä on kätevä havainnollistaa Vennin kaavioilla.

Esimerkkejä yksipaikkaisista relaatioista ovat esimerkiksi relaatio "olla positiivinen reaaliluku" reaalilukujen joukossa, "olla pitkätukkainen" kaikkien Logiikka I -kurssin osallistujien joukossa, ja "olla sateinen" kaikkien vuoden 2012 päivien joukossa.

3.8 Esimerkki. Olkoon $X = \{\text{tammikuu}, \text{helmikuu}, \text{maaliskuu}, \ldots, \text{joulukuu}\}$. Joukkoon X voidaan määritellä esimerkiksi seuraavanlaisia relaatioita:

- Kuukausien järjestys $\leq$. $x \leq y$, mikäli kuukausi x tulee samana vuonna ennen kuukautta y, tai $x = y$. Tämä on kaksipaikkainen relaatio.

- Yksipaikkainen relaatio $T = \{\text{tammikuu}, \text{helmikuu}, \text{marraskuu}, \text{joulukuu}\}$, eli $x \in T$, mikäli x on talvikuukausi.

- Kaksipaikkainen relaatio

$$Y = \{(x, y) : x \text{ ja } y \text{ ovat kuukausia, joissa on yhtä monta päivää}\}.$$

3.2 Aakkostot ja mallit

Määrittelemme seuraavaksi, mikä on malli. Intuitiivisesti se on joukko, jossa on jonkinlaista rakennetta, relaatioita, funktioita sekä kenties erityisasemassa olevia vakioita. Jätämme yksinkertaisuuden vuoksi funktiot pois, mutta kaikki lauseemme ja määritelmämme on helppo täydentää toimimaan myös funktiosymboleilla. Mallimme sisältävät siis ainoastaan relaatioita ja vakioita.

Tavoitteenamme on myöhemmin luoda predikaattilogiikan kieli, jossa voimme muotoilla mallejamme koskevia väitteitä, sekä tutkia niiden totuutta. Tästä syystä tarvitsemme nimiä malliemme relaatioille. Sanomme **aakkostoksi** mitä tahansa joukkoa L, joka koostuu relaatiosymboleista ja vakiosymboleista. Relaatio- ja vakiosymbolit voi olla mitä tahansa merkkejä, joilla haluamme merkata joitakin relaatioita ja vakioita. Jokaiseen relaatiosymboliin R liittyy **paikkaluku** $\#R$, joka kertoo kuinka monipaikkaisen relaation nimi kyseinen symboli on.

Aakkosto voi koostua esimerkiksi vain yhdestä relaatiosymbolista. Jos haluamme tutkia järjestyksiä, niin sopiva aakkosto tähän olisi esimerkiksi pelkästään kaksipaikkaisesta symbolista $\leq$ koostuva aakkosto $\{\leq\}$. Aakkosto voi kuitenkin olla monimutkaisempi, ja sisältää esimerkiksi äärettömän määrän symboleja.

3.9 Määritelmä. Olkoon L aakkosto, ja $\mathcal{M}$ epätyhjä joukko. Olkoon jokaista relaatiosymbolia $R \in L$, $\#R = n$, kohti $R^{\mathcal{M}}$ jokin joukon $\mathcal{M}$ n-paikkainen relaatio ja olkoon jokaista vakiosymbolia $c \in L$ kohti $c^{\mathcal{M}}$ jokin joukon $\mathcal{M}$ alkio.

Joukosta $\mathcal{M}$, relaatioista $R^{\mathcal{M}}$ ja vakioista $c^{\mathcal{M}}$ koostuvaa kokonaisuutta sanotaan **L-malliksi**. Relaatiota $R^{\mathcal{M}}$ sanotaan **relaatiosymbolin R tulkinnaksi mallissa $\mathcal{M}$** ja alkiota $c^{\mathcal{M}}$ sanotaan **vakiosymbolin c tulkinnaksi mallissa $\mathcal{M}$**.

Käytämme samaa merkintää $\mathcal{M}$ sekä mallin alkioiden joukosta, jota sanomme mallin **universumiksi**, että mallista kokonaisuutena. Mallin tarkalla joukko-opillisella esityksellä ei juuri ole väliä, joten emme spesifioi sitä.

Malli siis antaa aakkoston L symboleille merkityksen, eli semantiikan. Malli on predikaattilogiikalle, mitä totuusjakauma on propositiologiikalle. Se antaa formaalille kielellemme merkityksen ja kontekstin, jossa lauseet voivat olla tosia tai epätosia. Merkinnällä

$$\mathcal{M} = \left(\mathcal{M}, R_1^{\mathcal{M}}, R_2^{\mathcal{M}}, \ldots, c_1^{\mathcal{M}}, c_2^{\mathcal{M}}, \ldots\right)$$

tarkoitetaan aakkoston $\left\{R_1, R_2, \ldots, c_1^{\mathcal{M}}, c_2^{\mathcal{M}}, \ldots\right\}$ mallia $\mathcal{M}$, jossa symbolit R_i on tulkittu relaatioiksi $R_i^{\mathcal{M}}$ ja symbolit c_i vakioiksi $c_i^{\mathcal{M}}$.

Olkoon $L = \{\leq\}$ aakkosto ja $\mathcal{M}$ malli, jossa symbolin $\leq$ nimeämä relaatio $\leq^{\mathcal{M}}$ on lineaarijärjestys. Tällaisia malleja $\mathcal{M}$ sanotaan **järjestetyiksi joukoiksi**. Esimerkkejä järjestetyistä joukoista:

- Luonnollisten lukujen järjestetty joukko $\left(\mathbb{N}, \leq^{\mathbb{N}}\right)$.
- Kokonaislukujen järjestetty joukko $\left(\mathbb{Z}, \leq^{\mathbb{Z}}\right)$.
- Rationaalilukujen järjestetty joukko $\left(\mathbb{Q}, \leq^{\mathbb{Q}}\right)$.

- Reaalilukujen järjestetty joukko $\left(\mathbb{R}, \leq^{\mathbb{R}}\right)$.

- Joukko $N = \{0, 1, 2, \ldots, 1000\}$ järjestettynä takaperin, eli

$$1000 \leq^N 999 \leq^N 998 \leq^N \ldots \leq^N 0.$$

- Kaikkien koskaan eläneiden ihmisten joukko I järjestettynä niin, että $x \leq^I y$ jos henkilö x on syntynyt ennen henkilöä y (olettaen, etteivät ketkään kaksi henkilöä ole syntyneet täsmälleen samanaikaisesti).

On erittäin tärkeää huomata ero relaatiosymbolin R ja relaatiosymbolin tulkinnan $R^{\mathcal{M}}$ välillä. Ero on verrattavissa esimerkiksi "koira":n ja koiran eroon. "Koira" on suomenkielinen viidestä merkistä koostuva sana, jota voidaan käyttää tekstissä ja puheessa lauseiden muodostamiseen. Koira taas on neljästä jalasta, päästä ja hännästä koostuva yleensä karvainen eläin, eikä sitä saa helposti sijoitettua suomenkielisen lauseen osaksi. Sanalla "koira" voidaan viitata mihin tahansa kyseessä olevan eläinlajin edustajaan. Lause "koira on musta" voi olla totta tai epätotta riippuen siitä, mihin konkreettiseen koiraan sanalla "koira" viitataan.

Samoin symboli R soveltuu predikaattilogiikan kaavojen osaksi, kun taas relaatio $R^{\mathcal{M}}$ on konkreettinen relaatio jossakin joukossa. Esimerkiksi symbolilla $\leq$ voidaan viitata mihin tahansa ylläolevan esimerkin järjestykseen. Tulemme kaavojen totuutta määritellessämme huomaamaan, että kuten koirien tapauksessa, predikaattilogiikan kaava voi olla jossakin mallissa tosi ja jossakin mallissa epätosi, riippuen relaatiosta, johon symboli $\leq$ viittaa.

Verkot

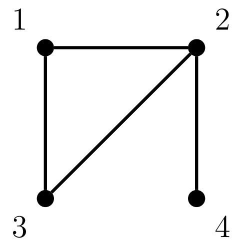
Olkoon $L = \{E\}$, missä E on kaksipaikkainen relaatiosymboli. Malleja $\left(\mathcal{G}, E^{\mathcal{G}}\right)$, joissa symbolin E tulkinta $E^{\mathcal{G}}$ on irrefleksiivinen ja symmetrinen relaatio, sanotaan **verkoiksi**. Relaatiota $E^{\mathcal{G}}$ sanotaan **särmä-** eli **viivarelaatioksi**. Verkon alkioita sanotaan sen **pisteiksi**. Mikäli $(p, q) \in E^{\mathcal{G}}$ sanotaan, että pisteestä p **menee viiva** pisteeseen q. Koska särmärelaatio on symmetrinen, voidaan myös sanoa, että pisteiden p ja q välillä on viiva, tai että pisteet ovat **naapureita**. Pisteen $p \in \mathcal{G}$ **aste** $\deg(p)$ on sen naapureiden lukumäärä, eli

$$\deg(p) = \left|\left\{q \in \mathcal{G} \colon\ (p, q) \in E^{\mathcal{G}}\right\}\right|.$$

3.10 Esimerkki. Olkoon $\mathcal{G} = \{1, 2, 3, 4\}$ ja

$$E^{\mathcal{G}} = \{(1,2), (2,1), (1,3), (3,1), (2,3), (3,2), (2,4), (4,2)\}.$$

Verkko $\left(\mathcal{G}, E^{\mathcal{G}}\right)$ näyttää seuraavalta:



3.3 Kaavat ja lauseet

Määrittelemme seuraavaksi ensimmäisen kertaluvun predikaattilogiikan kielen. Tämä on formaali kieli, jolla pystymme ilmaisemaan malleihin liittyviä asioita. Kuten propositiologiikan tapauksessa, on erittäin tärkeää pitää erillään syntaksi ja semantiikka, kaavat sekä niiden merkitykset. Kaavat ovat merkkijonoja, matemaattisia olioita, joiden ominaisuuksia tutkimme. Kaava pitää paikkaansa, jos asiaintila, johon kaava viittaa, pätee.

Oikeastaan ei ole vain yhtä predikaattilogiikan kieltä, vaan jokaista aakkostoa L kohti on oma kielensä, jolla voidaan puhua sen aakkoston malleista. Kielemme muodostuu aakkoston L symbolien lisäksi seuraavista symboleista:

$x_0, x_1, x_2, \ldots$	muuttujasymbolit
$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$	konnektiivit
$($, $)$	sulut
$=$	yhtäsuuruus
,	pilkku
$\forall, \exists$	universaali- ja eksistenssikvanttori

Aakkoston L vakiosymboleja sekä muuttujasymboleja yhdessä sanotaan **termeiksi**.

3.11 Määritelmä. Olkoon L aakkosto. **L-atomikaavoiksi** sanotaan seuraavia merkkijonoja:

1. Jos t ja u ovat termejä, niin $t = u$ on L-atomikaava.

2. Jos $R \in L$ on n-paikkainen relaatiosymboli, ja $t_1, \ldots, t_n$ ovat termejä, niin $R(t_1, \ldots, t_n)$ on L-atomikaava.

Intuitiivisesti muotoa $x_i = x_j$ oleva kaava tarkoittaa väitettä ”muuttujat x_i ja x_j saavat saman arvon”, mutta formaalisti se on tietysti vain eräs merkkijono muiden merkkijonojen joukossa. muotoa $R(x_{i_1}, \ldots, x_{i_n})$ oleva kaava taas kuvaa väitettä ”jono $(a_1, \ldots, a_n)$ kuuluu symbolin R nimeämään relaatioon, kun muuttujat x_{i_j} saavat arvot a_j”.

3.12 Määritelmä. Olkoon L aakkosto. **L-kaavat** saadaan rekursiivisesti atomikaavoista:

1. L-atomikaavat ovat L-kaavoja.

2. Mikäli φ ja ψ ovat L-kaavoja, niin $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ sekä $(\varphi \leftrightarrow \psi)$ ovat L-kaavoja.

3. Mikäli φ on L-kaava ja x_i on muuttujasymboli, niin $\forall x_i(\varphi)$ ja $\exists x_i(\varphi)$ ovat L-kaavoja.

Kuten propositiologiikassa, kaavojen **alikaavoja** ovat kaikki kaavan osat, jotka itsekin ovat kaavoja.

3.13 Esimerkki. Olkoon $L = \{A, B, \leq\}$, missä A ja B ovat yksipaikkaisia relaatiosymboleja ja $\leq$ on kaksipaikkainen relaatiosymboli. Tällöin L-kaavoja ovat esimerkiksi

$$\begin{array}{ll} (x_9 = x_5 \vee A(x_3)) & \forall x_0(x_0 = x_0) \\ \forall x_0(\exists x_1(\leq(x_0, x_1))) & (\exists x_0(A(x_0)) \leftrightarrow \forall x_1(B(x_1))) \\ \forall x_1(\forall x_2((\forall x_3(\neg x_3 = x_3) \vee \exists x_6(x_6 = x_6)))) & (\exists x_0((A(x_0) \leftrightarrow \neg A(x_0))) \wedge x_2 = x_0) \end{array}$$

Otamme heti käyttöön muutamia lyhennysmerkintöjä. Kaikkia sulkuja ei tarvitse merkitä näkyviin, jos on selvää, missä sulkujen tulisi olla, ja merkkaamme muuttujia myös muilla symboleilla kuin $x_0, x_1, \ldots$, esimerkiksi symboleilla $x, y, z, u, v, \ldots$. Lisäksi käytämme lyhennystä $t \neq u$ kaavasta $\neg t = u$. Kuten sulkujen käytössä, tämä on vain lyhenne, ja virallisesti kaavamme sisältävät vain muuttujia x_i. Lisäksi järjestysrelaatioiden tapauksessa merkintä "$\leq(x, y)$" lyhennetään "$x \leq y$". Käytämme esimerkiksi seuraavanlaisia lyhenteitä:

$$\begin{array}{l} \forall x_0(A(x_0) \vee \exists x_1(x_0 \leq x_1)) \\ A(u) \vee B(u) \\ \forall y \forall z(y \leq z \vee z \leq y) \end{array}$$

Sidotut ja vapaat muuttujat

Muuttuja voi esiintyä kaavoissa kahdenlaisissa rooleissa. Yksittäistä muuttujan x_i esiintymää kaavassa sanotaan **sidotuksi** eli **kvantifioiduksi**, jos se on osana jotakin muotoa $\forall x_i\varphi$ tai $\exists x_i\varphi$ olevaa alikaavaa. Muuten esiintymä on **vapaa**. Esimerkiksi kaavassa $R(x_0, x_0) \wedge \exists x_0 R(x_0, x_1)$ muuttujan x_0 kaksi ensimmäistä esiintymää ovat vapaita ja kolmas sidottu. Muuttujan x_1 ainut esiintymä on vapaa. Kaavaa, jossa ei ole yhtään vapaata muuttujaa, sanotaan **lauseeksi**.

Tällaisen jaottelun hyödyllisyyttä voidaan havainnollistaa seuraavalla esimerkillä: Olkoot A, B ja C seuraavat suomenkieliset väittämät:

$A =$ "Kokonaisluku x on parillinen."

$B =$ "Jokaisella kokonaisluvulla x pätee: x on parillinen."

$C =$ "Jollakin kokonaisluvulla x pätee: x on parillinen."

Väite A eroaa ilmeisellä tavalla väitteistä B ja C. Sekä väitteellä B että väitteellä C on totuusarvo, jonka tiedämme: Esimerkiksi luku -3 on kokonaisluku, joka ei ole parillinen, joten väite B ei päde, ja 4 on esimerkki kokonaisluvusta, joka on parillinen, joten väite C pätee. Väitteen A totuusarvoa ei sen sijaan voida tietää, ellei tiedetä mihin lauseessa esiintyvällä symbolilla x viitataan.

Lauseissa B ja C sanat ”jokainen” ja ”jokin” kvantifioivat muuttujan x. Näiden lauseiden totuudenmukaisuus ei riipu muuttujan x arvosta, vaan lauseiden totuusarvo päätetään kokeilemalla alilauseen ”x on parillinen” totuutta eri muuttujan x arvoilla. B toteutuu, jos jokainen tällainen kokeilu tekee lauseen alilauseen todeksi millä tahansa muuttujan x valinnalla, ja C toteutuu, jos on olemassa jokin tapa valita muuttujan x arvo niin, että alilause toteutuu.

Lauseen A totuusarvo jää siis potentiaalisesti riippumaan *vapaan* muuttujan x arvosta. Mikäli lauseessa ei esiinny vapaita muuttujia, voidaan sen totuusarvo päätellä ilman tietoa siinä ”esiintyvien muuttujien arvoista”.

Yksittäinen muuttuja voi esiintyä kaavassa useampaan kertaan, ja sen esiintymistä osa voi olla sidottuja ja osa vapaita. Näin on esimerkiksi kaavassa

$$\varphi = \exists y(\neg y = x) \wedge \forall x \forall y \forall z(x = y \vee y = z \vee z = x).$$

Kaava φ väittää, että mallissamme on olemassa jokin alkio, joka ei ole sama kuin x, ja tämän lisäksi mallissa ei ole mahdollista valita kolmea alkiota, jotka olisivat kaikki eri alkioita. Muuttuja x esiintyy sekä vapaana (vasemmassa konjunktissa) että sidottuna (oikeassa konjunktissa). Tällainen muuttujien käyttö on toki sallittua, mutta se voi tehdä kaavojen lukemisesta hankalaa. Onkin suositeltavaa kaavoja laatiessaan varmistaa, ettei sama muuttuja esiinny sekä sidottuna että vapaana.

Olkoon nyt L jokin aakkosto, φ L-kaava, x_i muuttuja ja t aakkoston L termi. Merkinnällä $\varphi(t/x_i)$ tarkoitetaan kaavaa, joka on muuten kuin φ, mutta kaikkien muuttujan x_i *vapaiden* esiintymien tilalle on sijoitettu termi t.[1] Siis esimerkiksi jos

$$\varphi = \forall x_0(x_0 = x_1) \vee \exists x_1(\neg x_1 = x_1),$$

niin

$$\varphi(c/x_1) = \forall x_0(x_0 = c) \vee \exists x_1(\neg x_1 = x_1).$$

Intuitiivisesti kaava $\varphi(t/x_i)$ sanoo termistä t sen, mitä φ sanoo muuttujasta x_i. Lisäksi sanomme, että **termi t on vapaa muuttujalle x_i kaavassa** φ, jos termin t ei sisällä muuttujaa, joka tulisi sijoituksessa $\varphi(t/x_i)$ sidotuksi.

Käytämme vastaavaa merkintää $t(t'/x_i)$ tarkoittamaan termiä, joka saadaan, kun termissä t muuttujan x_i paikalle sijoitetaan termi t'. Siis jos $t = x_i$, $t(t'/x_i) = t'$ ja muulloin $t(t'/x_i) = t$.

[1]Tämä notaatio poikkeaa hieman kirjan [JohLog] notaatiosta

Propositiolauseiden ja predikaattilogiikan kaavojen yhteys

Vaikka predikaattilogiikan kaavat ovat propositiologiikan kaavoja monimutkaisempia, on niiden määritelmissä kuitenkin samanlaisia piirteitä. Molempien rakennukseen voidaan käyttää konnektiiveja yhdistämään yksinkertaisempia lauseita. Propositiologiikkaan tutustuessamme olemme törmänneet monenlaisiin propositiolauseisiin, ja nämä tuttavuudet auttavat meitä jatkossakin:

3.14 Lause. Olkoon A propositiolause, jossa ei esiinny muita propositiosymboleja kuin $p_0, \ldots, p_n$. Olkoon L aakkosto ja olkoot $\varphi_0, \ldots, \varphi_n$ L-kaavoja. Tällöin merkkijono A', joka saadaan propositiolauseesta A korvaamalla symbolin p_i jokainen esiintymä kaavalla φ_i, kun $i \in \{0, \ldots, n\}$, on L-kaava.

Todistus. Todistetaan väite induktiolla propositiolauseen A rakenteen suhteen.

$\boxed{p_i}$ Oletetaan, että $A = p_i$ jollakin $i \in \mathbb{N}$. Tällöin $A' = \varphi_i$, joka oletuksen nojalla on L-kaava.

$\boxed{\neg}$ Oletetaan, että väite pätee propositiolauseelle A, eli A' on L-kaava. L-kaavojen määritelmän nojalla myös $\neg A'$ on L-kaava, ja kun propositiolauseesta $\neg A$ korvataan symbolit p_i kaavoilla φ_i, saadaan juurikin kaava $\neg A'$. Siis väite pätee myös propositiolauseelle $\neg A$.

$\boxed{\wedge}$ Oletetaan, että väite pätee propositiolauseille A ja B. Siis merkkijonot A' ja B', jotka saadaan korvaamalla propositiolauseista A ja B, ovat L-kaavoja. Kun propositiolauseessa $(A \wedge B)$ jokainen symbolin p_i esiintymä korvataan L-kaavalla φ_i, saadaan merkkijono $(A' \wedge B')$, joka L-kaavojen määritelmän nojalla on itsekin L-kaava. Siis väite pätee myös lauseelle $(A \wedge B)$.

$\boxed{\vee}$, $\boxed{\rightarrow}$, $\boxed{\leftrightarrow}$ Kuten kohta $\boxed{\wedge}$.

□

3.4 Totuus

Koska kaavoissa esiintyy muuttujia, riippuu kaavojen totuus siitä, mitä muuttujien paikalle sijoitetaan. Matematiikassa ”muuttuja” tarkoittaa yleensä jotakin kirjainta, jonka ajatellaan viittaavaan johonkin konkreettiseen olioon, tai usein ”mielivaltaiseen” olioon. Käytämme muuttujia, koska haluamme todistaa, että jokin väite pätee yleisesti, sijoitettiin muuttujaan sitten mikä tahansa konkreettinen olio. Yleisistä tuloksista saadaan sitten erikoistapauksia ”sijoittamalla” jonkin muuttujan paikalle jotakin. Formalisoidaan tämä idea:

Olkoon L aakkosto ja $\mathcal{M}$ L-malli. Funktiota s muuttujasymbolien joukolta $\{x_i \colon i \in \mathbb{N}\}$ malliin $\mathcal{M}$ sanotaan **tulkintajonoksi**. Tulkintajono siis kuvaa, eli tulkitsee jokaisen muuttujan x_i joksikin mallin $\mathcal{M}$ alkioksi, eli ”sijoittaa” muuttujalle x_i arvon $s(x_i)$.

Kun s on tulkintajono, x_i on muuttuja ja a on mallin $\mathcal{M}$ alkio, merkinnällä

$$s(a/x_i)$$

tarkoitetaan tulkintajonoa, joka antaa muuttujalle x_i arvon a ja kaikille muille muuttujille saman arvon kuin tulkintajono s. Siis

$$s(a/x_i)(x_j) = \begin{cases} a, & \text{kun } i = j \\ s(x_j), & \text{kun } i \neq j. \end{cases}$$

Tulkintajonon muutoksia voidaan toki ketjuttaa, esimerkiksi $s(a/x_1)(d/x_4)(c/x_2)(b/x_1)$. Tällöin vasemmanpuoleisimmat muutokset tapahtuvat ennen oikeanpuoleisia, eli esimerkiksi $s(a/x_1)(c/x_2)(b/x_1)$ antaisi muuttujalle x_1 arvon b, muuttujalle x_2 arvon c ja muille muuttujille samat arvot kuin tulkintajono s.

Jos s esimerkiksi olisi tulkintajono kokonaislukujen mallissa $\mathbb{Z}$, niin että $s(x_0) = 5$, $s(x_1) = -2$, $s(x_2) = 2$, $s(x_3) = 5$ ja $s(x_i) = -10$, kun $i > 3$, niin muunnetut tulkintajonot antaisivat muuttujille seuraavia arvoja:

	x_0	x_1	x_2	x_3	x_4	x_5	x_6	...
s	5	-2	2	5	-10	-10	-10	
$s(77/x_2)$	5	-2	77	5	-10	-10	-10	
$s(77/x_2)(0/x_4)$	5	-2	77	5	0	-10	-10	
$s(77/x_2)(0/x_4)(0/x_2)$	5	-2	0	5	0	-10	-10	
$s(0/x_0)(0/x_1)(0/x_2)$	0	0	0	5	-10	-10	-10	

Jos t on termi, niin **termin t arvo tulkintajonolla** s, merkitään $s(t)$ on $s(x_i)$ jos $t = x_i$ ja $c^{\mathcal{M}}$, jos $t = c$, $c \in L$.

Nyt voimme vihdoin määritellä, mitä tarkoittaa jonkin kaavan totuus jossakin mallissa. Määritelmä on rekursiivinen kaavojen rakenteen suhteen. Merkintä $\mathcal{M} \models_s \varphi$ luetaan ”malli $\mathcal{M}$ toteuttaa kaavan φ tulkintajonolla s”.

3.15 Määritelmä (Tarski). Olkoon L aakkosto ja $\mathcal{M}$ L-malli.

1. Kun t ja u ovat termejä, $\mathcal{M} \models_s t = u$ jos ja vain jos $s(t) = s(u)$.
2. Kun $t_1, \ldots, t_n$ ovat termejä, ja R on n-paikkainen relaatiosymboli, $\mathcal{M} \models_s R(t_1, \ldots, t_n)$ jos ja vain jos $(s(t_1), \ldots, s(t_n)) \in R^{\mathcal{M}}$.
3. $\mathcal{M} \models_s \neg\varphi$ jos ja vain jos $\mathcal{M} \not\models_s \varphi$.
4. $\mathcal{M} \models_s (\varphi \wedge \psi)$ jos ja vain jos $\mathcal{M} \models_s \varphi$ ja $\mathcal{M} \models_s \psi$.
5. $\mathcal{M} \models_s (\varphi \vee \psi)$ jos ja vain jos joko $\mathcal{M} \models_s \varphi$ tai $\mathcal{M} \models_s \psi$.
6. $\mathcal{M} \models_s (\varphi \rightarrow \psi)$ jos ja vain jos joko $\mathcal{M} \not\models_s \varphi$ tai $\mathcal{M} \models_s \psi$.
7. $\mathcal{M} \models_s (\varphi \leftrightarrow \psi)$ jos ja vain jos joko $\mathcal{M} \models_s \varphi$ ja $\mathcal{M} \models_s \psi$ tai $\mathcal{M} \not\models_s \varphi$ ja $\mathcal{M} \not\models_s \psi$.

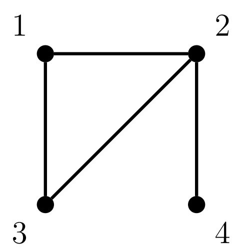
8. $\mathcal{M} \models_s \forall x_i(\varphi)$ jos ja vain jos millä tahansa mallin $\mathcal{M}$ alkiolla a $\mathcal{M} \models_{s(a/x_i)} \varphi$.

9. $\mathcal{M} \models_s \exists x_i(\varphi)$ jos ja vain jos löytyy jokin mallin $\mathcal{M}$ alkio a, jolla $\mathcal{M} \models_{s(a/x_i)} \varphi$.

Heti aluksi todettakoon, että mikäli s ja s' ovat kaksi tulkintajonoa, jotka antavat kaavassa φ *vapaina* esiintyville muuttujille samat arvot, niin $\mathcal{M} \models_s \varphi$ jos ja vain jos $\mathcal{M} \models_{s'} \varphi$. Tämä on helppo todistaa induktiolla kaavan φ rakenteen suhteen.

Erityisesti jos φ on lause (siinä ei siis ole vapaita muuttujia), ei tulkintajono s vaikuta lauseen φ totuuteen. Tällöin voidaan kirjoittaa $\mathcal{M} \models \varphi$, jos $\mathcal{M} \models_s \varphi$ jollakin (eli millä tahansa) tulkintajonolla s.

3.16 Esimerkki. Olkoon $G = \big(G, E^G\big)$ esimerkin 3.10 verkko



ja olkoon s jokin tulkintajono, jolla $s(x_0) = 1$ ja $s(x_1) = 4$. Tutkitaan kaavojen $E(x_0, x_1) \vee x_0 = x_1$, $\exists x_0(E(x_0, x_1))$ ja $\forall x_1(\neg E(x_1, x_0))$ totuutta mallissa $\mathcal{M}$ tulkintajonolla s.

Tarskin totuusmääritelmän nojalla $\mathcal{M} \models_s E(x_0, x_1) \vee x_0 = x_1$ joss $\mathcal{M} \models_s E(x_0, x_1)$ tai $\mathcal{M} \models_s x_0 = x_1$. Koska

$$(s(x_0), s(x_1)) = (1, 4) \notin E^G,$$

$\mathcal{M} \not\models_s E(x_0, x_1)$. Koska $s(x_0) = 1 \neq 4 = s(x_1)$, niin $\mathcal{M} \not\models_s x_0 = x_1$. Siis $\mathcal{M} \not\models_s E(x_0, x_1) \vee x_0 = x_1$.

Tutkitaan seuraavaksi kaavan $\exists x_0(E(x_0, x_1))$ totuus. Koska $(2, 4) \in E^G$ ja $(2, 4) = (s(2/x_0)(x_0), s(2/x_0)(x_1))$,

$$\mathcal{M} \models_{s(2/x_0)} E(x_0, x_1).$$

Siispä $\mathcal{M} \models_s \exists x_0(E(x_0, x_1))$.

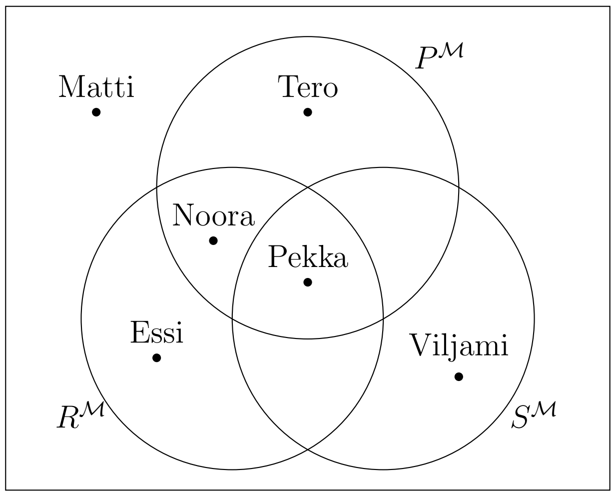
Lopuksi kaava $\forall x_1(\neg E(x_1, x_0))$. Koska

$$(2, 1) = (s(2/x_1)(x_1), s(2/x_1)(x_0)) \in E^G,$$

$\mathcal{M} \models_{s(2/x_1)} E(x_1, x_0)$, joten $\mathcal{M} \not\models_{s(2/x_1)} \neg E(x_1, x_0)$. Siis ei pidä paikkaansa, että jokaisella alkiolla $a \in G$, G toteuttaisi kaavan $\neg E(x_1, x_0)$ tulkintajonolla $s(a/x_1)$, joten $G \not\models_s \forall x_1(\neg E(x_1, x_0))$.

3.17 Esimerkki. Olkoon $L = \{P, R, S\}$, missä P, R ja S ovat yksipaikkaisia relaatiosymboleja, ja olkoon $\mathcal{M} = \big(\mathcal{M}, P^{\mathcal{M}}, R^{\mathcal{M}}, S^{\mathcal{M}}\big)$ L-malli, jonka alkioina ovat ovat Matti, Pekka, Tero, Viljami, Noora ja Essi, ja

$$\begin{array}{ll} P^{\mathcal{M}} = \{\text{Pekka}, \text{Tero}, \text{Noora}\} & \text{(pyöräilyä harrastavat)} \\ R^{\mathcal{M}} = \{\text{Pekka}, \text{Noora}, \text{Essi}\} & \text{(rullaluistelua harrastavat)} \\ S^{\mathcal{M}} = \{\text{Pekka}, \text{Viljami}\} & \text{(shakkia harrastavat).} \end{array}$$



Tutkitaan kaavan $P(x_0) \wedge (R(x_0) \wedge S(x_0))$ totuutta mallissa $\mathcal{M}$ mielivaltaisella tulkintajonolla s. Tarskin totuusmääritelmän nojalla

$$\begin{aligned} \mathcal{M} \models_s P(x_0) \wedge (R(x_0) \wedge S(x_0)) &\iff \mathcal{M} \models_s P(x_0) \text{ ja } \mathcal{M} \models_s (R(x_0) \wedge S(x_0)) \\ &\iff \mathcal{M} \models_s P(x_0), \mathcal{M} \models_s R(x_0) \text{ ja } \mathcal{M} \models_s S(x_0) \\ &\iff s(x_0) \in P^{\mathcal{M}}, s(x_0) \in R^{\mathcal{M}} \text{ ja } s(x_0) \in S^{\mathcal{M}} \\ &\iff s(x_0) \in P^{\mathcal{M}} \cap R^{\mathcal{M}} \cap S^{\mathcal{M}}. \end{aligned}$$

Koska Pekka on ainut mallin $\mathcal{M}$ alkio, joka kuuluu kaikkiin kolmeen relaatioon, $\mathcal{M}$ toteuttaa kaavan $P(x_0) \wedge (R(x_0) \wedge S(x_0))$ tulkintajonolla s jos ja vain jos s antaa muuttujalle x_0 arvon Pekka. Toisaalta

$$\begin{aligned} &\mathcal{M} \models_s \forall x_0 (P(x_0) \vee (R(x_0) \vee S(x_0))) \\ &\iff \text{jokaisella } a \in \mathcal{M},\ \mathcal{M} \models_{s(a/x_0)} P(x_0) \vee (R(x_0) \vee S(x_0)) \\ &\iff \dots \\ &\iff \text{jokaisella } a \in \mathcal{M},\ s(a/x_0)(x_0) \in P^{\mathcal{M}} \cup R^{\mathcal{M}} \cup S^{\mathcal{M}} \\ &\iff \text{jokaisella } a \in \mathcal{M},\ a \in P^{\mathcal{M}} \cup R^{\mathcal{M}} \cup S^{\mathcal{M}}, \end{aligned}$$

eli $\mathcal{M} \models_s \forall x_0(P(x_0) \vee (R(x_0) \vee S(x_0)))$ jos ja vain jos jokainen mallin $\mathcal{M}$ alkio kuuluu ainakin johonkin relaatioista $P^{\mathcal{M}}$, $R^{\mathcal{M}}$ ja $S^{\mathcal{M}}$. Koska Matti ei kuulu näistä relaatioista mihinkään, $\mathcal{M} \not\models_s \forall x_0(P(x_0) \vee (R(x_0) \vee S(x_0)))$.

Äkkiseltään Tarskin totuusmääritelmä saattaa vaikuttaa triviaalilta tai kiertopäätelmältä. Tätä se ei kuitenkaan ole, vaan se toimii eräänlaisena käännöstyökaluna, jonka avulla voimme kääntää formaalin predikaattilogiikan kielemme väittämiä suomenkielisiksi luonnollisen kielen väittämiksi. Olkoon R on kaksipaikkainen relaatio, ja $\mathcal{M}$ malli, jonka aakkostoon R kuuluu. Tutkitaan kaavan $\varphi = \forall x_0 \forall x_1(R(x_0, x_1) \to R(x_1, x_0))$ totuutta mallissa $\mathcal{M}$.

Koska millä tahansa $a, b \in \mathcal{M}$

$$\begin{aligned}
&\mathcal{M} \models_{s(a/x_0)(b/x_1)} R(x_0, x_1) \to R(x_1, x_0) \\
&\iff \text{joko } \mathcal{M} \not\models_{s(a/x_0)(b/x_1)} R(x_0, x_1) \\
&\qquad \text{tai } \mathcal{M} \models_{s(a/x_0)(b/x_1)} R(x_1, x_0) \\
&\iff \text{joko } (s(a/x_0)(b/x_1)(x_0), s(a/x_0)(b/x_1)(x_1)) \notin R^{\mathcal{M}} \\
&\qquad \text{tai } (s(a/x_0)(b/x_1)(x_1), s(a/x_0)(b/x_1)(x_0)) \in R^{\mathcal{M}} \\
&\iff \text{joko } (a, b) \notin R^{\mathcal{M}} \text{ tai } (b, a) \in R^{\mathcal{M}} \\
&\iff \text{jos } (a, b) \in R^{\mathcal{M}}, \text{ niin } (b, a) \in R^{\mathcal{M}},
\end{aligned}$$

niin $\mathcal{M} \models \varphi$ jos ja vain jos relaatio $R^{\mathcal{M}}$ on symmetrinen. Kaavan φ voidaankin ajatella olevan lauseen "R on symmetrinen relaatio" käännös predikaattilogiikan kielelle.

3.18 Määritelmä. Olkoon L aakkosto, ja φ L-kaava. Mikäli φ on totta missä tahansa L-mallissa millä tahansa tulkintajonolla, sanotaan, että φ on **validi**.

Validit kaavat ovat siis loogisia totuuksia, joiden totuus ei riipu mistään malleista saati muuttujien tulkinnasta. Validisuus on ikään kuin predikaattilogiikan yleistys propositiologiikan tautologisuudelle. Esimerkiksi seuraavat kaavat ovat valideja:

$$\begin{array}{ll}
x_0 = x_0 & x_0 = x_1 \vee x_1 = x_1 \\
\forall x_0(x_0 = x_0) & \forall x_0 \forall x_1 \forall x_2(R(x_0, x_1) \vee \neg R(x_0, x_1)) \\
P(x_0) \to P(x_0) & \neg \exists x_5(\neg x_5 = x_5)
\end{array}$$

Koska mallimme ovat aina epätyhjiä, myös esimerkiksi kaava $\exists x_0(x_0 = x_0)$ aina totta.

3.19 Esimerkki. Kaava $\varphi = \forall x_0 \exists x_1(x_0 = x_1)$ on validi. (Minkä tahansa aakkoston mielessä.)

Todistus. Olkoon $\mathcal{M}$ mikä tahansa malli ja s mikä tahansa mallin $\mathcal{M}$ tulkintajono.

Huomataan, että

$$\begin{aligned}
\mathcal{M} \models_s \varphi \quad &\iff \quad \text{millä tahansa } a \in \mathcal{M}\ \mathcal{M} \models_{s(a/x_0)} \exists x_1(x_0 = x_1) \\
&\iff \quad \text{millä tahansa } a \in \mathcal{M} \text{ löytyy } b \in \mathcal{M}, \text{ jolla } \mathcal{M} \models_{s(a/x_0)(b/x_1)} x_0 = x_1 \\
&\iff \quad \text{millä tahansa } a \in \mathcal{M} \text{ löytyy } b \in \mathcal{M}, \\
&\qquad\quad \text{jolla } s(a/x_0)(b/x_1)(x_0) = s(a/x_0)(b/x_1)(x_1) \\
&\iff \quad \text{millä tahansa } a \in \mathcal{M} \text{ löytyy } b \in \mathcal{M}, \text{ jolla } a = b.
\end{aligned}$$

Riittää siis näyttää, että jokaista alkiota $a \in \mathcal{M}$ kohti löytyy jokin alkio $b \in \mathcal{M}$, joka on sama alkio kuin a. Tällainen alkio tietysti aina löytyy, sillä a itse on sellainen! Siispä $\mathcal{M} \models_s \varphi$. Koska tämä päti mielivaltaisella mallilla $\mathcal{M}$ ja tulkintajonolla s, kaava φ on validi. □

3.20 Esimerkki. Olkoon $L = \{\leq\}$. L-kaava $\forall x(x \leq y \vee \neg x \leq y)$ on validi, mutta kaava $\forall x(x \leq x)$ ei ole.

Todistus. Olkoon $\mathcal{M}$ L-malli ja s jokin sen tulkintajono. Koska

$$\begin{aligned}
\mathcal{M} \models_s \forall x(x \leq y \vee \neg x \leq y) \quad &\iff \quad \text{millä tahansa } a \in \mathcal{M},\ \mathcal{M} \models_{s(a/x)} (x \leq y \vee \neg x \leq y) \\
&\iff \quad \text{millä tahansa } a \in \mathcal{M},\ \mathcal{M} \models_{s(a/x)} x \leq y \\
&\qquad\quad \text{tai } \mathcal{M} \models_{s(a/x)} \neg x \leq y) \\
&\iff \quad \text{millä tahansa } a \in \mathcal{M},\ s(a/x)(x) \leq s(a/x)(y) \\
&\qquad\quad \text{tai } s(a/x)(x) \not\leq s(a/x)(y) \\
&\iff \quad \text{millä tahansa } a \in \mathcal{M},\ a \leq s(y) \text{ tai } a \not\leq s(y)
\end{aligned}$$

ja millä tahansa $a, b \in \mathcal{M}$ pätee joko $(a, b) \in \leq^{\mathcal{M}}$ tai $(a, b) \notin \leq^{\mathcal{M}}$,

$$\mathcal{M} \models_s \forall x(x \leq y \vee \neg x \leq y).$$

Siis kaava $\forall x(x \leq y \vee \neg x \leq y)$ on validi.

Näytetään nyt, että kaava $\forall x(x \leq x)$ ei ole validi. Olkoon $\mathcal{M}$ malli, jonka universumina on joukko $\{14\}$ ja $\leq^{\mathcal{M}} = \emptyset$. Olkoon s tulkintajono, joka antaa jokaiselle muuttujalle arvon 14. Koska $(14, 14) \notin \leq^{\mathcal{M}}$,

$$\mathcal{M} \not\models_{s(14/x)} x \leq x,$$

ja täten $\mathcal{M} \not\models_s \forall x(x \leq x)$. Siis kaava $\forall x(x \leq x)$ ei ole validi. □

Propositiologiikan tautologioista saadaan valideja lauseita, kun propositiosymbolien paikalle sijoitetaan predikaattilogiikan kaavoja. Tämä seuraa hieman vahvemmasta tuloksesta:

3.21 Lemma. Olkoon A propositiolause, jossa ei esiinny muita propositiosymboleja kuin $p_0, \ldots, p_n$. Olkoon L aakkosto, olkoot $\varphi_0, \ldots, \varphi_n$ L-kaavoja ja olkoon A' saatu lauseesta A korvaamalla jokainen symbolin p_i esiintymä kaavalla φ_i, kun $i \in \{0, \ldots, n\}$. Olkoon $\mathcal{M}$ L-malli, s tulkintajono ja v mikä tahansa totuusjakauma, jolle jokaisella $i \in \{0, \ldots, n\}$ pätee

$$v(i) = 1 \text{ jos ja vain jos } \mathcal{M} \models_s \varphi_i$$

Tällöin $v[A] = 1$ jos ja vain jos $\mathcal{M} \models_s A'$.

Todistus. Helppo induktio lauseen A rakenteen suhteen. □

3.22 Lause. Olkoon A propositiologiikan tautologia, jossa ei esiinny muita propositiosymboleja kuin $p_0, \ldots, p_n$. Olkoon L aakkosto ja $\varphi_0, \ldots, \varphi_n$ L-kaavoja. Tällöin kaava A', joka on saatu lauseesta A korvaamalla jokainen symbolin p_i esiintymä kaavalla φ_i, kun $i \in \{0, \ldots, n\}$, on validi.

Todistus. Olkoon $\mathcal{M}$ mikä tahansa malli ja s mikä tahansa sen tulkintajono. Olkoon v totuusjakauma, jolla

$$v(i) = 1 \text{ jos ja vain jos } i \leq n \text{ ja } \mathcal{M} \models_s \varphi_i.$$

Koska A on tautologia, $v[A] = 1$, joten edellisen lemman nojalla $\mathcal{M} \models_s A'$. □

3.23 Esimerkki. Kaava $\varphi = \neg((x < y \vee y < x) \wedge \neg(x < y \vee y < x))$ on edellisen lauseen nojalla validi, sillä se on saatu tautologiasta

$$\neg(p_0 \wedge \neg p_0)$$

sijoittamalla symbolin p_0 paikalle kaava $(x < y \vee y < x)$.

Propositiologiikan tautologioista tällä tavalla sijoittamalla saatuja kaavoja sanotaan **predikaattilogiikan tautologioiksi** eli lyhyemmin **tautologioiksi**. Ne ovat siis erikoistapaus valideista lauseista. Vaikka validisuus ja tautologisuus äkkiseltään vaikuttavat samankaltaisilta ominaisuuksilta, on niillä kuitenkin yksi huomattava ero. Sekä propositio- että predikaattilogiikassa tautologia voidaan tunnistaa helposti syntaktisista ominaisuuksistaan, mutta valideja lauseita ei voida. Ei siis ole mahdollista ohjelmoida tietokonetta tunnistamaan sille syötettyjä valideja lauseita, mutta tautologioiden tunnistaminen kyllä onnistuu.

3.24 Määritelmä. Olkoon L aakkosto ja olkoot φ ja ψ L-kaavoja. Mikäli ψ pätee jokaisella L-mallilla $\mathcal{M}$ ja tulkintajonolla s, joilla myös φ pätee, sanotaan, että kaava ψ on kaavan φ **looginen seuraus**, ja merkitään $\varphi \Rightarrow \psi$. Mikäli $\varphi \Rightarrow \psi$ ja $\psi \Rightarrow \varphi$, sanotaan, että kaavat φ ja ψ ovat **loogisesti ekvivalentit**, ja merkitään $\varphi \Leftrightarrow \psi$.

Olkoon nyt Σ joukko L-kaavoja. Jos jokainen malli ja tulkintajono, jotka toteuttavat kaikki joukon Σ kaavat, toteuttavat myös kaavan φ, sanotaan, että φ on **kaavajoukon Σ looginen seuraus** ja merkitään $\Sigma \Rightarrow \varphi$.

3.25 Esimerkki. Olkoon L mielivaltainen aakkosto ja φ mielivaltainen L-kaava. Tällöin $\forall x\varphi \Rightarrow \exists x\varphi$.

Todistus. Olkoon $\mathcal{M}$ mielivaltainen L-malli ja s jokin sen tulkintajono. Oletetaan, että $\mathcal{M} \models_s \forall x\varphi$.

Olkoon a mikä tahansa mallin $\mathcal{M}$ alkio (mallit ovat epätyhjiä, joten niistä löytyy aina ainakin yksi alkio). Koska $\mathcal{M} \models_s \forall x\varphi$, erityisesti $\mathcal{M} \models_{s(a/x)} \varphi$ ja täten $\mathcal{M} \models_s \exists x\varphi$. $\square$

3.26 Esimerkki. $\exists x\forall y R(x,y) \Rightarrow \forall y\exists x R(x,y)$.

Todistus. Olkoot $\mathcal{M}$ ja s sellaisia, että $\mathcal{M} \models_s \exists x\forall y R(x,y)$. Totuuden määritelmän nojalla löytyy siis alkio $a \in \mathcal{M}$ niin, että oli $b \in \mathcal{M}$ mikä tahansa, niin pätee $\mathcal{M} \models_{s(a/x)(b/y)} R(x,y)$.

Olkoon nyt $b \in \mathcal{M}$ mielivaltainen. Koska $\mathcal{M} \models_{s(a/x)(b/y)} R(x,y)$, ja $s(a/x)(b/y) = s(b/y)(a/x)$, $\mathcal{M} \models_{s(b/y)(a/x)} R(x,y)$. Siis $\mathcal{M} \models_{s(b/y)} \exists x R(x,y)$. Koska b oli mielivaltainen, $\mathcal{M} \models_s \forall y\exists x R(x,y)$. $\square$

3.5 Isomorfia

Kun määrittelimme mallit, ideana oli formalisoida käsite ”joukko jossa on jotakin rakennetta”. Valitsimme symbolit, joilla voimme nimetä tätä ”rakennetta” ja määrittelimme kaavat, joilla voimme puhua tästä rakenteesta. Juuri tämä ”rakenne” on se, mikä malleissa on kiinnostavaa, eikä niinkään mallien alkiot itsessään. Malleja, joiden rakenne on samanlainen sanotaan isomorfisiksi. Määrittelemme tämän täsmällisesti seuraavien esimerkkien jälkeen.

3.27 Esimerkki. Olkoon $L = \left\{\ddot{A}, I\right\}$ aakkosto, $\#\ddot{A} = \#I = 2$, ja olkoon

$$\mathcal{M} = \{\text{Carl Gustaf}, \text{Silvia}, \text{Victoria}, \text{Daniel}, \text{Estelle}\}$$

Ruotsin kuninkaallisista muodostettu L-malli, jossa $\ddot{A}(x,y)$ tulkitaan ”x on y:n äiti” ja $I(x,y)$ tulkitaan ”x on y:n isä”, siis

$$\begin{aligned} \ddot{A}^{\mathcal{M}} &= \{(\text{Silvia}, \text{Victoria}), (\text{Victoria}, \text{Estelle})\} \\ I^{\mathcal{M}} &= \{(\text{Carl Gustaf}, \text{Victoria}), (\text{Daniel}, \text{Estelle})\}. \end{aligned}$$

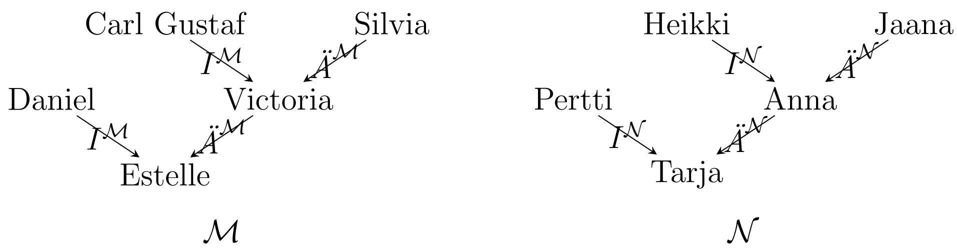
Olkoon $\mathcal{N}$ L-malli, jonka alkioiden joukko on

$$\{\text{Heikki}, \text{Tarja}, \text{Jaana}, \text{Pertti}, \text{Anna}\}$$

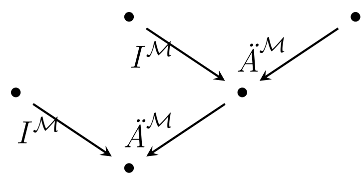
ja jossa relaatiosymbolien tulkinnat ovat

$$\begin{aligned} \ddot{A}^{\mathcal{N}} &= \{(\text{Jaana}, \text{Anna}), (\text{Anna}, \text{Tarja})\} \\ I^{\mathcal{N}} &= \{(\text{Heikki}, \text{Anna}), (\text{Pertti}, \text{Tarja})\}. \end{aligned}$$

Näiden perheiden sukupuut näyttävät seuraavilta:



Nämä mallit ovat siis hyvin samanlaisia. Mikäli unohdetaan mallien alkiot ja tarkastellaan vain niiden rakennetta, se näyttää tältä:



Tietyssä mallit $\mathcal{M}$ ja $\mathcal{N}$ *ovat sama malli*. Niiden alkioiden välillä on vastaavuus (Carl Gustaf vastaa Heikkiä, Silvia Jaanaa jne.) joka *säilyttää mallien rakenteen.*

3.28 Määritelmä. Olkoon L aakkosto ja $\mathcal{M}$ sekä $\mathcal{N}$ L-malleja. Olkoon $f\colon \mathcal{M} \to \mathcal{N}$ bijektio. Kuvausta f sanotaan **isomorfismiksi**, jos seuraavat ehdot ovat voimassa:

1. Jokaisella vakiosymbolilla $c \in L$ pätee $f(c^{\mathcal{M}}) = c^{\mathcal{N}}$.
2. Jokaisella relaatiosymbolilla $R \in L$, $\#R = n$, pätee $(a_1, \ldots, a_n) \in R^{\mathcal{M}} \iff (f(a_1), \ldots, f(a_n)) \in R^{\mathcal{N}}$.

Isomorfismia mallilta itselleen sanotaan **automorfismiksi**.

Mikäli on olemassa isomorfismi mallista $\mathcal{M}$ malliin $\mathcal{N}$, sanotaan, että mallit ovat **isomorfiset**.

Mallien välinen isomorfia on refleksiivinen, symmetrinen ja transitiivinen ominaisuus. Jotta mallit voisivat olla keskenään isomorfiset, tulee niiden olla erityisesti samankokoiset, sillä muuten niiden välillä ei ole olemassa yhtään bijektiota, eikä siten isomorfismiakaan.

Esimerkissä 3.27 isomorfismi mallien $\mathcal{M}$ ja $\mathcal{N}$ välillä olisi kuvaus $f\colon \mathcal{M} \to \mathcal{N}$, jolla

$$\begin{aligned}
&f(\text{Carl Gustaf}) = \text{Heikki}\\
&f(\text{Silvia}) = \text{Jaana}\\
&f(\text{Victoria}) = \text{Anna}\\
&f(\text{Daniel}) = \text{Pertti}\\
&f(\text{Estelle}) = \text{Tarja}.
\end{aligned}$$

3.29 Esimerkki. Olkoon $L = \{R\}$, $\#R = 2$, ja $\mathbb{Z}$ L-malli, jonka universumina on kokonaisluvut ja

$$R^{\mathbb{Z}} = \{(a, b) : a + 1 = b\} = \{\ldots, (-1, 0), (0, 1), (1, 2), (2, 3), \ldots\}.$$

Malli $\mathbb{Z}$ näyttää siis tältä:

$$\cdots \quad \to \overset{-2}{\bullet} \to \overset{-1}{\bullet} \to \overset{0}{\bullet} \to \overset{1}{\bullet} \to \overset{2}{\bullet} \to \overset{3}{\bullet} \to \overset{4}{\bullet} \to \quad \cdots$$

Olkoon $\mathcal{M}$ L-malli, jonka universumina on joukko $\{2^n : n \in \mathbb{Z}\}$, ja jossa

$$\leq^{\mathcal{M}} = \left\{(a, b) \in \mathcal{M}^2 : b = 2a\right\}.$$

Malli $\mathcal{M}$ näyttää seuraavalta:

$$\cdots \quad \to \overset{\frac{1}{4}}{\bullet} \to \overset{\frac{1}{2}}{\bullet} \to \overset{1}{\bullet} \to \overset{2}{\bullet} \to \overset{4}{\bullet} \to \overset{8}{\bullet} \to \overset{16}{\bullet} \to \quad \cdots$$

Tällöin mallit $\mathbb{Z}$ ja $\mathcal{M}$ ovat isomorfiset.

Todistus. Olkoon $f : \mathbb{Z} \to \mathcal{M}$ kuvaus, jonka määrittelee ehto

$$f(n) = 2^n.$$

Kuvaus f on injektio, sillä jos $f(n) = f(k)$, $2^n = 2^k$ ja tämä pätee vain, jos $n = k$. Kuvaus on myös surjektio, sillä jos $y \in \mathcal{M}$, $y = 2^n$ jollakin $n \in \mathbb{Z}$. Tällöin $f(n) = 2^n = y$. Kuvaus on siis bijektio.

Isomorfisuuden tarkistamiseksi pitää vielä näyttää, että jokaisella $a_1, a_2 \in \mathbb{Z}$, $(a_1, a_2) \in R^{\mathbb{Z}}$ jos ja vain jos $(f(a_1), f(a_2)) \in R^{\mathcal{M}}$.

Olkoon aluksi $(a_1, a_2) \in R^{\mathbb{Z}}$. Tällöin relaation $R^{\mathbb{Z}}$ määritelmän nojalla $a_1 + 1 = a_2$. Nyt

$$\begin{aligned} a_1 + 1 = a_2 \quad &\Rightarrow \quad 2^{a_1+1} = 2^{a_2} \\ &\Rightarrow \quad 2 \cdot 2^{a_1} = 2^{a_2} \\ &\Rightarrow \quad 2f(a_1) = f(a_2), \end{aligned}$$

joten $(f(a_1), f(a_2)) \in R^{\mathcal{M}}$.

Oletetaan sitten, että $(f(a_1), f(a_2)) \in R^{\mathcal{M}}$, joten $2f(a_1) = f(a_2)$, eli $2 \cdot 2^{a_1} = 2^{a_2}$. Tällöin $2^{a_1+1} = 2^{a_2}$, joten $a_1 + 1 = a_2$, eli $(a_1, a_2) \in R^{\mathbb{Z}}$. Siis $(a_1, a_2) \in R^{\mathbb{Z}}$ jos ja vain jos $(f(a_1), f(a_2)) \in R^{\mathcal{M}}$.

Mallien $\mathbb{Z}$ ja $\mathcal{M}$ välille on siis löydetty jokin isomorfismi, joten ne ovat isomorfiset. $\square$

Edellisessä esimerkissä mallien $\mathbb{Z}$ ja $\mathcal{M}$ välillä on muitakin isomorfismeja kuin annettu f. Itseasiassa kuvaus $n \mapsto 2^{n+a}$ on isomorfismi millä tahansa vakiolla $a \in \mathbb{Z}$.

3.30 Esimerkki. Olkoon $\mathbb{R}$ reaalilukujen malli varustettuna järjestyksellä $<^{\mathbb{R}}$. Olkoon $a \in \mathbb{R}$ vakio ja olkoon $f : \mathbb{R} \to \mathbb{R}$ kuvaus $f(x) = x + a$. Näin määritelty kuvaus f on automorfismi.

Todistus. Kuvaus f on selvästi bijektio ja kaikilla reaaliluvuilla x ja y pätee $x < y$ jos ja vain jos $x + a < y + a$. □

3.31 Esimerkki. Olkoon $L = \{<\}$ ja olkoot $\mathbb{N}$ ja $\mathbb{Z}$ L-malleja, joissa kummassakin symbolin $<$ tulkinta on joukon luonnollinen järjestys. Mallit $\mathbb{N}$ ja $\mathbb{Z}$ *eivät ole* isomorfisia.

Todistus. Tehdään vastaoletus: löytyy jokin isomorfismi $f\colon \mathbb{N} \to \mathbb{Z}$. Olkoon $c = f(0)$. Koska $c \in \mathbb{Z}$, $c-1 \in \mathbb{Z}$, ja $(c-1, c) \in <^{\mathbb{Z}}$. Koska f on bijektio, löytyy jokin luonnollinen luku $n \in \mathbb{N}$, jolle $f(n) = c - 1$.

Koska $(f(n), f(0)) \in <^{\mathbb{Z}}$, isomorfismin määritelmän nojalla pitäisi päteä $(n, 0) \in <^{\mathbb{N}}$. Tämä ei kuitenkaan voi päteä, sillä mikään luonnollinen luku ei ole nollaa pienempi. Tämä on kaivattu ristiriita, joten vastaoletus on väärä ja alkuperäinen väite pätee. □

Jos mallit ovat rakenteeltaan täysin samanlaisia, pitäisi niissä tietysti päteä kaikki samat väitteet. Tämä pitääkin paikkansa, ja on suora seuraus seuraavasta lemmasta.

3.32 Lemma. Olkoon L aakkosto, $\mathcal{M}$ ja $\mathcal{N}$ L-malleja, $f\colon \mathcal{M} \to \mathcal{N}$ isomorfismi ja φ L-kaava. Olkoon s mielivaltainen mallin $\mathcal{M}$ tulkintajono ja s' mallin $\mathcal{N}$ tulkintajono, jolle pätee

$$s'(x_i) = f(s(x_i)) \text{ kaikilla } i \in \mathbb{N}.$$

Tällöin $\mathcal{M} \models_s \varphi$ jos ja vain jos $\mathcal{N} \models_{s'} \varphi$.

Todistus. Näytetään aluksi, että jokaisella L-termillä t, $s'(t) = f(s(t))$. Jos $t = x_i$, niin $s'(t) = s'(x_i) = f(s(x_i)) = f(s(t))$. Jos taas $t = c$ jollakin vakiosymbolilla $c \in \mathcal{M}$, $s'(c) = c^{\mathcal{N}} = f(c^{\mathcal{M}}) = s(c)$.

Osoitetaan sitten itse väite induktiolla kaavan φ rakenteen suhteen.

1. Oletetaan aluksi, että φ on atomikaava. Jos φ on muotoa $t = u$ joillakin termeillä t ja u, niin

$$\begin{aligned} \mathcal{M} \models_s \varphi &\iff s(t) = s(u) \\ &\overset{*}{\iff} f(s(t)) = f(s(u)) \\ &\iff s'(t) = s'(u) \\ &\iff \mathcal{N} \models_{s'} t = u. \end{aligned}$$

Kohdassa $*$ käytettiin tietoa siitä, että f on isomorfismi, erityisesti injektio. Jos taas φ on muotoa $R(t_1, \ldots, t_n)$ jollakin $R \in L$, $\#R = n$, niin

$$\begin{aligned} \mathcal{M} \models_s \varphi &\iff (s(t_1), \ldots, s(t_n)) \in R^{\mathcal{M}} \\ &\overset{*}{\iff} (f(s(t_1)), \ldots, f(s(t_n))) \in R^{\mathcal{N}} \\ &\iff (s'(t_1), \ldots, s'(t_n)) \in R^{\mathcal{N}} \\ &\iff \mathcal{N} \models_{s'} \varphi. \end{aligned}$$

Taas kohdassa $*$ käytettiin tietoa siitä, että f on isomorfismi. On siis näytetty, että väite pätee atomikaavoille.

2. Oletetaan, että $\varphi = \psi \wedge \theta$ joillakin ψ ja θ, joille väite jo pätee. Tällöin

$$\begin{aligned}\mathcal{M} \models_s \varphi &\iff \mathcal{M} \models_s \psi \text{ ja } \mathcal{M} \models_s \theta \\ &\overset{i.o.}{\iff} \mathcal{N} \models_{s'} \psi \text{ ja } \mathcal{N} \models_{s'} \theta \\ &\iff \mathcal{N} \models_{s'} \varphi\end{aligned}$$

   Muita konnektiiveja koskevat kohdat voidaan osoittaa samoin.

3. Oletetaan, että $\varphi = \exists x_i \psi$, väite pätee kaavalle ψ ja $\mathcal{M} \models_s \varphi$. Tällöin löytyy jokin alkio $a \in \mathcal{M}$, jolla $\mathcal{M} \models_{s(a/x_i)} \psi$. Koska tulkintajono, joka saadaan jonosta $s(a/x_i)$ kuvaamalla kaikki alkiot kuvauksella f on jono $s'(f(a)/x_i)$,

$$\mathcal{N} \models_{s'(f(a)/x_i)} \psi.$$

   Siispä $\mathcal{N} \models_{s'} \varphi$.

   Implikaatio toiseen suuntaan saadaan, kun funktion f sijasta käytetään käänteisfunktiota f^{-1}. Siis $\mathcal{M} \models_s \varphi$ jos ja vain jos $\mathcal{N} \models_{s'} \varphi$.

   Tapaus $\varphi = \forall x_i \psi$ voidaan todistaa samoin.

□

3.33 Lause. Olkoot $\mathcal{M}$ ja $\mathcal{N}$ isomorfisia L-malleja, ja olkoon φ L-lause. Tällöin $\mathcal{M} \models \varphi$ jos ja vain jos $\mathcal{N} \models \varphi$.

3.6 Määriteltävyys

Olemme määritelleet predikaattilogiikan kielen ja käyttäneet sitä erilaisten asioiden ilmaisemiseen. On kuitenkin paljon asioita, joista predikaattilogiikan kielellä ei voi puhua, ja tilanteita, joissa emme pysty kielellämme esimerkiksi erottamaan joitakin alkioita toisistaan. Tutkimme seuraavaksi kysymystä ”mitä ominaisuuksia predikaattilogiikan kielessä voi kuvailla?”.

3.34 Määritelmä. Olkoon L aakkosto ja $\mathcal{M}$ L-malli. Olkoon X jokin mallin $\mathcal{M}$ osajoukko. Joukko X on **määriteltävä osajoukko**, mikäli on olemassa kaava φ, jossa on vapaana tasan yksi muuttuja x_0, niin että

$$X = \left\{a \in \mathcal{M} \colon \mathcal{M} \models_{s(a/x_0)} \varphi\right\}$$

jollakin tulkintajonolla s.

Olkoon R jokin mallin $\mathcal{M}$ n-paikkainen relaatio. Relaatio R on **määriteltävä relaatio**, jos on olemassa kaava φ, jossa on vapaana tasan muuttujat $x_0, \ldots, x_{n-1}$, niin että

$$R = \left\{(a_0, \ldots, a_{n-1}) \in \mathcal{M} \colon \mathcal{M} \models_{s(a_0/x_0)\cdots(a_{n-1}/x_{n-1})} \varphi\right\}.$$

Edellisen määritelmän kaavaa φ sanotaan osajoukon X tai relaation R **määritteleväksi kaavaksi**. Osajoukko tai relaatio on siis määriteltävä, jos on olemassa jokin kaava, joka määrittelee sen, eli jos on olemassa jokin mallin alkioiden ominaisuus, joka osajoukon alkioilla on, mutta muilla ei ole. Lisäksi tämän ominaisuuden pitää olla kirjoitettavissa predikaattilogiikan kielellä. Huomaa, että osajoukon tai relaation määrittelevä kaava ei missään nimessä ole yksikäsitteinen. Jos esimerkiksi φ määrittelee osajoukon X, myös kaava $\varphi \vee \varphi$, $\varphi \wedge \varphi$ tai $\neg\neg\varphi$ määrittelee sen.

3.35 Esimerkki. Sekä tyhjä joukko $\emptyset$ että koko malli $\mathcal{M}$ ovat aina määriteltäviä. Lisäksi määriteltävän osajoukon komplementti sekä kahden määriteltävän osajoukon yhdiste ja leikkaus ovat määriteltäviä.

Todistus. Olkoon L mikä tahansa aakkosto ja $\mathcal{M}$ sen malli.

Tyhjän joukon määrittelee kaava $\neg x_0 = x_0$, sillä

$$\begin{aligned}\big\{a \in \mathcal{M} \colon \mathcal{M} \models_{s(a/x_0)} \neg x_0 = x_0\big\} &= \big\{a \in \mathcal{M} \colon \mathcal{M} \not\models_{s(a/x_0)} x_0 = x_0\big\} \\ &= \{a \in \mathcal{M} \colon s(a/x_0)(x_0) \neq s(a/x_0)(x_0)\} \\ &= \{a \in \mathcal{M} \colon a \neq a\} \\ &= \emptyset,\end{aligned}$$

ja vastaavasti koko mallin $\mathcal{M}$ määrittelee kaava $x_0 = x_0$.

Olkoot X ja Y mallin $\mathcal{M}$ määriteltäviä osajoukkoja, ja olkoot φ_X ja φ_Y kaavat, jotka määrittelevät ne. Tällöin kaava $\varphi_X \wedge \varphi_Y$ määrittelee joukon $X \cap Y$:

$$\begin{aligned}&\big\{a \in \mathcal{M} \colon \mathcal{M} \models_{s(a/x_0)} \varphi_X \wedge \varphi_Y\big\} \\ =\ &\big\{a \in \mathcal{M} \colon \mathcal{M} \models_{s(a/x_0)} \varphi_X \text{ ja } \mathcal{M} \models_{s(a/x_0)} \varphi_Y\big\} \\ =\ &\big\{a \in \mathcal{M} \colon \mathcal{M} \models_{s(a/x_0)} \varphi_X\big\} \cap \big\{a \in \mathcal{M} \colon \mathcal{M} \models_{s(a/x_0)} \varphi_X\big\} \\ =\ &X \cap Y.\end{aligned}$$

Vastaavasti kaava $\varphi_X \vee \varphi_Y$ määrittelee joukon $X \cup Y$ ja kaava $\neg\varphi_X$ määrittelee joukon $\mathcal{M} \setminus X$. □

3.36 Esimerkki. Olkoon $L = \{<\}$ ja $\mathbb{N}$ L-malli, jonka universumi on luonnollisten lukujen joukko ja jossa $<^{\mathbb{N}}$ on luonnollisten lukujen tavallinen järjestys. Tällöin joukot $\{0\}$ ja $\{3, 4, 5, \ldots\}$ ovat määriteltävä.

Todistus. Joukon $\{0\}$ alkioilla on ominaisuus ”minua pienempiä alkioita ei ole”, jota muilla alkioilla ei ole. Tämä voidaan muotoilla predikaattilogiikassa kaavalla $\neg\exists x_1(x_1 < x_0)$, sillä jokaisella $a \in \mathbb{N}$ pätee

$$\begin{aligned}&\mathbb{N} \models_{s(a/x_0)} \neg\exists x_1(x_1 < x_0) \\ \iff\ &\text{ei löydy alkiota } b \in \mathbb{N}, \text{ jolla } \mathbb{N} \models_{s(a/x_0)(b/x_1)} x_1 < x_0 \\ \iff\ &\text{ei ole olemassa alkiota } b \in \mathbb{N}, \text{ jolla } b <^{\mathbb{N}} a.\end{aligned}$$

Tämä pätee vain jos $a = 0$, eli

$$\{a \in \mathbb{N} \colon \mathbb{N} \models_{s(a/x_0)} \neg\exists x_1(x_1 < x_0)\} = \{0\}.$$

Joukon $\{3, 4, 5, \ldots\}$ alkiot taas toteuttavat väitteen ”on olemassa ainakin kolme minua pienempää eri alkiota”. Tämäkin voidaan sanoa predikaattilogiikassa kaavalla

$$\exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3 \wedge x_1 < x_0 \wedge x_2 < x_0 \wedge x_3 < x_0).$$

□

Isomorfismi säilyttää määriteltävät joukot

Joukon voi siis näyttää määriteltäväksi etsimällä kaavan, joka määrittelee sen. Logiikassa usein se mitä ei voida tehdä on kuitenkin kiinnostavampaa, kuin se mitä voidaan. Seuraava lause on kätevin tapa todistaa, että jokin joukko ei ole määriteltävä.

3.37 Lause. Olkoon $A \subset \mathcal{M}$ määriteltävä, ja olkoon $f \colon \mathcal{M} \to \mathcal{M}$ mallin $\mathcal{M}$ automorfismi. Tällöin millä tahansa $a \in \mathcal{M}$, $a \in A$ jos ja vain jos $f(a) \in A$.

Todistus. Olkoon φ kaava, joka määrittelee joukon A. Kaavassa φ on siis vapaana vain muuttuja x_0. Olkoon $a \in A$, eli

$$\mathcal{M} \models_{s(a/x_0)} \varphi.$$

Lemman 3.32 nojalla $\mathcal{M} \models_{s'} \varphi$, missä $s'(x_i) = f(s(a/x_0)(x_i))$ kaikilla $i \in \mathbb{N}$. Koska vain vapaiden muuttujien arvo vaikuttaa kaavan totuuteen, ja $s'(x_0) = f(s(a/x_0)(x_0)) = f(a)$, $\mathcal{M} \models_{s(f(a)/x_0)} \varphi$. Siispä $f(a) \in A$.

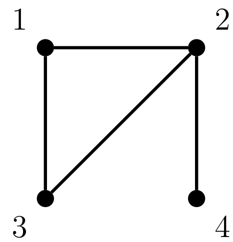
Koska määriteltävän joukon komplementti on määriteltävä, sama päättely sovellettuna joukon A sijasta joukkoon $\mathcal{M} \setminus A$ osoittaa, että jos $a \notin A$, $f(a) \notin A$. Siispä $a \in A$ jos ja vain jos $f(a) \in A$. □

3.38 Esimerkki. Olkoon $\mathbb{Z}$ kokonaislukujen malli varustettuna tavanomaisella järjestyksellä $<^{\mathbb{Z}}$. Tällöin $\{0\}$ *ei ole* määriteltävä.

Todistus. Olkoon $f \colon \mathbb{Z} \to \mathbb{Z}$ kuvaus, jolle $f(n) = n + 1$ jokaisella $n \in \mathbb{Z}$. Tämä kuvaus on bijektio, ja se säilyttää myös järjestyksen: $n <^{\mathbb{Z}} m$ jos ja vain jos $n+1 <^{\mathbb{Z}} m+1$. Siis se on isomorfismi. Jos joukko $\{0\}$ olisi määriteltävä, lauseen 3.37 nojalla $f(0) \in \{0\}$, sillä $0 \in \{0\}$. □

Itseasiassa edellisen esimerkin todistus on helppo yleistää mille tahansa joukolle $A \subset \mathbb{Z}$, $A \neq \emptyset$ ja $A \subset \mathbb{Z}$. Kokonaislukujen järjestetyllä joukolla ei siis ole muita määriteltäviä osajoukkoja kuin $\emptyset$ ja $\mathbb{Z}$.

3.39 Esimerkki. Olkoon $\mathcal{G}$ verkko



Tällöin joukko $\{4\}$ on määriteltävä, mutta joukko $\{1\}$ ei ole. Joukon $\{4\}$ alkioilla on se yhteinen ominaisuus, että niillä on vain yksi naapuri. Kaava

$$\exists x_1(E(x_0, x_1) \wedge \forall x_2(E(x_0, x_2) \rightarrow x_1 = x_2))$$

määrittelee joukon $\{4\}$.

Näytetään, että joukko $\{1\}$ ei ole määriteltävä. Olkoon $f \colon \mathcal{G} \to \mathcal{G}$ kuvaus, jolla $f(1) = 3$, $f(2) = 2$, $f(3) = 1$ ja $f(4) = 4$. Kuvaus f siis ainoastaan vaihtaa alkioiden 1 ja 3 paikat. Näin määritelty kuvaus on automorfismi, sillä se on selvästi bijektio, ja se säilyttää verkossa olevan rakenteen: jos $(a, b) \in E^{\mathcal{G}}$, niin $(f(a), f(b)) \in E^{\mathcal{G}}$ ja toisin päin. Jos ajatellaan että ylläolevassa kuvassa pisteet 1 ja 3 liu'utettaisiin toistensa paikoille, ei verkon ulkomuoto muuttuisi ollenkaan.

Koska $1 \in \{1\}$, jos $\{1\}$ olisi määriteltävä, pitäisi olla $f(1) = 3 \in \{1\}$. Tämä ei kuitenkaan pidä paikkaansa joten $\{1\}$ ei voi olla määriteltävä.

3.7 Semanttinen puu

Propositiologiikassa semanttisella puulla saatettiin helposti löytää jonkin propositiolauseen toteuttava totuusjakauma, tai osoittaa, että tällaista totuusjakaumaa ei ole olemassa. Predikaattilogiikassa semanttiset puut toimivat samalla tavalla, niiden avulla voidaan rakentaa malli ja tulkintajono, joilla jokin lause on tosi, tai vaihtoehtoisesti osoittaa, että tällaista mallia ja tulkintajonoa ei ole olemassa. Yksinkertaisuuden vuoksi teemme semanttisia puita **vain lauseille**. Pienet muutokset sääntöihin mahdollistaisivat semanttisten puiden käytön myös muiden kaavojen kanssa.

Propositiologiikassa semanttista puuta tehtäessä jokaisesta lauseesta tutkittiin, millä eri tavoilla lause on mahdollista toteuttaa. Kaikki propositiologiikasta tutut säännöt ovat edelleen voimassa, mutta kvanttoreita ja identiteettiä varten tarvitsemme uusia sääntöjä. Propositiologiikassa ei yksittäisiin propositiosymboleihin, eikä sellaisten negaatioihin voinut enää soveltaa mitään sääntöjä. Predikaattilogiikassa vastaavasti atomikaavat muodostavat kielen yksinkertaisimmat kaavat, joten niihin ei enää sääntöjä tarvitse soveltaa. Tutkitaan seuraavaksi, milloin kvanttorilla alkavat lauseet voivat toteutua.

Eksistenssikvanttorilla alkava lause $\exists x_i \varphi$ toteutuu, mikäli löytyy jokin alkio, joka sijoitettuna muuttujan x_i *vapaisiin* esiintymiin toteuttaa lauseen φ. Merkataan tällaista alkiota c_j. Eksistenssikvanttorin sääntö on siis

$$\begin{array}{c} \exists x_i \varphi \ \checkmark \\ | \\ \varphi(c_j/x_i) \end{array}$$

missä c_j on vakiosymboli, joka ei ennestään esiinny semanttisessa puussa. Jos esimerkiksi $\varphi = \exists x_0 \neg x_0 = c_3$, φ väittää, että on olemassa jokin alkio, joka poikkeaa alkiosta c_3. Ei olisi sallittua tehdä askelta

$$\begin{array}{c} \exists x_0 \neg x_0 = c_3 \ \checkmark \\ | \\ \neg c_3 = c_3 \end{array}$$

sillä vakiosymboli c_3 esiintyy jo puussa, ja näin saatu johtopäätös $\neg c_3 = c_3$ ei tietenkään voi toteutua, vaikka kaava φ voi.

Peräkkäisellä negaatiolla ja universaalikvanttorilla alkava lause voidaan purkaa samalla periaatteella: ”ei pidä paikkaansa, että kaikki alkiot toteuttaisivat lauseen φ” on yhtäpitävä lauseen ”on olemassa jokin alkio, joka ei toteuta lausetta φ” kanssa. Sääntö on siis

$$\begin{array}{c} \neg \forall x_i \varphi \ \checkmark \\ | \\ \neg \varphi(c_j/x_i) \end{array}$$

missä c_j on vakio, joka ei ennestään esiinny puussa.

3.40 Esimerkki. Olkoon $L = \{R\}$, missä R on kaksipaikkainen relaatiosymboli. Tutkitaan, milloin lause ”on olemassa alkio, joka ei ole kaikkien alkioiden kanssa relaatiossa R” toteutuu. Olkoon siis

$$\varphi = \exists x_3 \neg \forall x_1 R(x_3, x_1).$$

Piirretään lauseelle φ semanttinen puu:

$$\begin{array}{c} \exists x_3 \neg \forall x_1 R(x_3, x_1) \ \checkmark \\ | \\ \neg \forall x_1 R(c_0, x_1) \ \checkmark \\ | \\ \neg R(c_0, c_1) \end{array}$$

Lause siis toteutuu, jos jotkin alkiot c_0 ja c_1 eivät ole relaatiossa R.

Universaalikvanttorin sekä negatoidun eksistenssikvanttorin säännöt kaipaavat hieman enemmän selitystä. Universaalikvanttorilla alkavan lauseen paikkaansapitävyyttä ei voida päätellä tutkimalla mitään yksittäistä alkiota, vaan on ”käytävä läpi” kaikki mallin alkiot ja sijoitettava ne vuorotellen kaavaan. Universaalikvanttorin vaikutus mallissa on siis globaali, ja universaalikvanttorin sääntökin voi siitä syystä vaikuttaa monessa kohdassa semanttista puuta.

Säännöt ovat

$$\begin{array}{cc} \forall x_i \varphi & \neg\exists x_i \varphi \\ | & | \\ \varphi(c_j/x_i) & \neg\varphi(c_j/x_i) \end{array}$$

Näiden sääntöjen soveltaminen poikkeaa kuitenkin paljon muista säännöistä. Sääntöjä sovelletaan jokaiseen oksalla esiintyvään vakiosymboliin, **eikä niitä koskaan merkitä käsitellyiksi**, vaan niitä sovelletaan joka kerta, kun jollekin solmun sisältävälle oksalle ilmestyy uusia vakioita. Mikäli oksalla ei ennestään ole vakioita, sovelletaan sääntöä jollakin uudella vakiolla c_j.

3.41 Esimerkki. Tehdään kaavalle $\exists x_0 P(x_0) \wedge \exists x_0 \forall x_1 R(x_0, x_1)$ semanttinen puu:

$$\begin{array}{c} \exists x_0 P(x_0) \wedge \exists x_0 \forall x_1 R(x_0, x_1) \checkmark \\ | \\ \exists x_0 P(x_0) \checkmark \\ | \\ \exists x_0 \forall x_1 R(x_0, x_1) \checkmark \\ | \\ P(c_0) \\ | \\ \forall x_1 R(c_1, x_1) \\ | \\ R(c_1, c_0) \\ | \\ R(c_1, c_1) \end{array}$$

Nyt kaikki puun merkitsemättömät kaavat ovat atomikaavoja, lausetta $\forall x_1 R(c_1, x_1)$ lukuunottamatta. Lausetta $\forall x_1 R(c_1, x_1)$ taas on sovellettu kaikkiin puussa esiintyviin vakiosymboleihin joten puun rakentaminen voidaan lopettaa.

Puuta tutkimalla voidaan rakentaa malli lauseelle $\exists x_0 P(x_0) \wedge \exists x_0 \forall x_1 R(x_0, x_1)$: olkoon $\mathcal{M} = \{c_0, c_1\}$ kahden alkion malli, jossa $P^{\mathcal{M}} = \{c_0\}$ ja $R^{\mathcal{M}} = \{(c_1, c_0), (c_1, c_1)\}$.

Koska muotoa $\forall x_i \varphi$ tai $\neg\exists x_i \varphi$ olevia solmuja ei koskaan merkitä, voi semanttisesta puusta mahdollisesti tulla ääretön. Näin käy esimerkiksi piirrettäessä puuta kaavalle $\forall x_1 \exists x_2 R(x_1, x_2)$:

$$
\begin{array}{c}
\forall x_1 \exists x_2 R(x_1, x_2) \\
| \\
\exists x_2 R(c_0, x_2) \checkmark \\
| \\
R(c_0, c_1) \\
| \\
\exists x_2 R(c_1, x_2) \checkmark \\
| \\
R(c_1, c_2) \\
| \\
\exists x_2 R(c_2, x_2) \checkmark \\
| \\
R(c_1, c_3) \\
\vdots
\end{array}
$$

Tämä ei sinänsä ole ongelma, lauseen toteuttaa malli, jonka alkiot muodostavat äärettömän jonon, niin että jonon jäsen on aina relaatiossa seuraavaan jäseneen.

Identiteettiin liittyy säännöt

$$
\begin{array}{c}
t = u \\
| \\
\varphi(t/x_i)
\end{array}
\qquad \text{ja} \qquad
\begin{array}{c}
u = t \\
| \\
\varphi(t/x_i)
\end{array}
$$

missä φ on jokin kaava, jolla $\varphi(u/x_i)$ esiintyy samalla haaralla kuin $t = u$, ja sekä termi t että termi u on vapaa muuttujalle x_i kaavassa φ. Kaavaa $t = u$ ei myöskään merkitä käsitellyksi, vaan sitä sovelletaan kaikkiin samalla haaralla oleviin kaavoihin, joissa u tai t esiintyy. Lisäksi identiteetin myötä saamme uuden tavan sulkea jokin oksa. Lause $\neg t = t$ ei tietenkään voi päteä millään termillä, joten jos oksalla esiintyy tämä kaava, voidaan oksa sulkea.

Semanttisessa puussa sääntöjen sovellukset saa tehdä missä järjestyksessä tahansa. Semanttinen puu on **lopullinen** kun jokaisella sen avoimella haaralla olevat merkitsemättömät kaavat ovat joko atomikaavoja, atomikaavojen negaatioita, muotoa $\forall x_i \varphi$, $\neg \exists x_i \varphi$ tai $t = u$, ja kaikki mahdolliset sääntöjen sovellukset on tehty. Kvanttoreiden takia on mahdollista tehdä lauseelle semanttinen puu, jossa on yksi ääretön haara, joka ei kuitenkaan ole lopullinen. Tällöin puusta ei voi päätellä mitään. *Lopullinen* ääretön oksa on kuitenkin aina avoin.

Kuten propositiologiikassa, sanomme lauseen ψ **semanttiseksi todistukseksi lauseista** $\varphi_1, \ldots, \varphi_n$ lauseiden $\varphi_1, \ldots, \varphi_n, \neg\psi$ sulkeutuvaa semanttista puuta. Jos lauseella ψ on semanttinen todistus lauseista $\varphi_1, \ldots, \varphi_n$, on se myös näiden looginen seuraus.

3.42 Esimerkki. $\{\exists x_0 P(x_0), \forall x_0 \forall x_1 (x_0 = x_1)\} \Rightarrow \forall x_8 P(x_8)$.

Todistus. Muodostetaan semanttinen puu kaavoille $\exists x_0 P(x_0)$, $\forall x_0 \forall x_1 (x_0 = x_1)$ ja

$\neg\forall x_8 P(x_8)$:

$$\begin{array}{c}
\exists x_0 P(x_0) \checkmark \\
| \\
\forall x_0 \forall x_1 (x_0 = x_1) \\
| \\
\neg\forall x_8 P(x_8) \checkmark \\
| \\
P(c_0) \\
| \\
\forall x_1 (c_0 = x_1) \\
| \\
\neg P(c_1) \\
| \\
c_0 = c_1 \\
| \\
P(c_1) \\
| \\
\times
\end{array}$$

Koska puun jokainen haara sulkeutuu, eivät lauseet $\exists x_0 P(x_0)$, $\forall x_0 \forall x_1 (x_0 = x_1)$ ja $\neg\forall x_8 P(x_8)$ voi toteutua samanaikaisesti. Siis $\{\exists x_0 P(x_0), \forall x_0 \forall x_1 (x_0 = x_1)\} \Rightarrow \forall x_8 P(x_8)$. $\square$

3.43 Esimerkki. Tutkitaan, toteutuuko lause $\forall x_0 \exists x_1 R(x_0, x_1) \wedge \exists x_0 \neg R(x_0, x_0)$ jossakin mallissa.

$$\begin{array}{c}
\forall x_0 \exists x_1 R(x_0, x_1) \wedge \exists x_0 \neg R(x_0, x_0) \checkmark \\
| \\
\forall x_0 \exists x_1 R(x_0, x_1) \\
| \\
\exists x_0 \neg R(x_0, x_0) \checkmark \\
| \\
\neg R(c_0, c_0) \\
| \\
\exists x_1 R(c_0, x_1) \checkmark \\
| \\
R(c_0, c_1) \\
| \\
\exists x_1 R(c_1, x_1) \checkmark \\
| \\
R(c_1, c_2) \\
| \\
\exists x_1 R(c_2, x_1) \checkmark \\
\vdots
\end{array}$$

Koska solmua $\forall x_0 \exists x_1 R(x_0, x_1)$ ei koskaan merkitä, tulee puun oksasta ääretön, mutta lopullinen. Sen perusteella voidaan rakentaa malli $\mathcal{M} = \{c_0, c_1, c_2, \ldots\}$, jossa $R^{\mathcal{M}} = \{(c_n, c_{n+1}) : n \in \mathbb{N}\}$.

3.44 Esimerkki. Osoitetaan, että $\exists x_0 P(x_0) \not\Rightarrow \forall x_0 P(x_0)$ rakentamalla semanttinen puu lauseille $\exists x_0 P(x_0)$ ja $\neg\forall x_0 P(x_0)$:

$$\begin{array}{c} \exists x_0 P(x_0) \checkmark \\ | \\ \neg\forall x_0 P(x_0) \checkmark \\ | \\ P(c_0) \\ | \\ \neg P(c_1) \end{array}$$

Näin saatu puu on lopullinen ja avoin, joten voimme todeta, että malli $\mathcal{M} = \{c_0, c_1\}$, $P^{\mathcal{M}} = \{c_0\}$, toteuttaa sekä lauseen $\exists x_0 P(x_0)$ että lauseen $\neg\forall x_0 P(x_0)$. Täten $\exists x_0 P(x_0) \not\Rightarrow \forall x_0 P(x_0)$.

3.8 Päättely

Predikaattilogiikan luonnollisessa päättelyssä kaikki vanhat propositiologiikan säännöt ovat voimassa, mutta näiden lisäksi mukaan otetaan joitakin uusia sääntöjä kvanttoreiden ja yhtäsuuruuden käsittelyä varten.

Tarkastellaan uudestaan päättelyä

$$\begin{array}{l} \text{Jokainen mies on kuolevainen.} \\ \text{Sokrates on mies.} \\ \hline \text{Sokrates on kuolevainen.} \end{array}$$

Merkitsemällä relaatiosymbolilla M miesten joukkoa, symbolilla K kuolevaisten joukkoa ja vakiosymbolilla S Sokratesta, voidaan tämä päättely nyt formalisoida paremmin kuin propositiologiikan tapauksessa. Predikaattilogiikassa vastaava luonnollinen päättely olisi

$$\dfrac{\dfrac{\forall x(M(x) \to K(x))}{M(S) \to K(S)}\,{\scriptstyle \forall E} \qquad M(S)}{K(S)}\,{\scriptstyle \to E}$$

Sääntö $\forall E$ voidaan tulkita seuraavalla tavalla: Jos tiedämme, että kaava $M(x) \to K(x)$ pätee millä tahansa muuttujan x arvolla, niin erityisesti se pätee, kun muuttujan x tilalle sijoitetaan Sokrates.

Kuten propositiologiikassa, sanomme, että **kaava φ on pääteltävissä joukon Σ kaavoista,** $\Sigma \vdash \varphi$, jos on olemassa luonnollinen päättely, jonka kaikki oletukset löytyvät joukosta Σ, ja jonka johtopäätös on kaava φ. Mikäli $\emptyset \vdash \varphi$, merkitsemme $\vdash \varphi$.

Kvanttoreita koskevat päättelysäännöt ovat listattuna seuraavaan taulukkoon:

kvanttori	introduktio	eliminointi
$\forall$	$$\frac{\varphi}{\forall x_i \varphi}\ \forall I$$ Päättelysääntöä voi käyttää vain, jos x_i ei esiinny vapaana missään kaavan φ päättelyn hylkäämättömissä oletuksissa.	$$\frac{\forall x_i \varphi}{\varphi(t/x_i)}\ \forall E$$ Päättelysääntöä voi käyttää vain, jos t on vapaa muuttujalle x_i kaavassa φ.
$\exists$	$$\frac{\varphi(t/x_i)}{\exists x_i \varphi}\ \exists I$$ Päättelysääntöä voi käyttää vain, jos t on vapaa muuttujalle x_i kaavassa φ.	$$\frac{\exists x_i \varphi \quad \begin{matrix}[\varphi] \\ \vdots \\ \psi\end{matrix}}{\psi}\ \exists E$$ Päättelysääntöä voi käyttää vain, jos x_i ei esiinny vapaana kaavassa ψ, eikä missään kaavan ψ päättelyn hylkäämättömissä oletuksissa, paitsi mahdollisesti kaavassa φ.

Lisäksi yhtäsuuruuteen, eli identiteettiin, liittyy muutamia sääntöjä:

$=$	$$\frac{}{t = t}\ {=}1$$	$$\frac{t = u}{u = t}\ {=}2$$
	$$\frac{t_1 = t_2 \quad t_2 = t_3}{t_1 = t_3}\ {=}3$$	$$\frac{t = u \quad \varphi(t/x_i)}{\varphi(u/x_i)}\ {=}4$$ Päättelysääntöä saa käyttää vain jos termit t ja u ovat vapaita muuttujalle x_i kaavassa φ.

Kvanttoreihin liittyvien sääntöjen käyttö on kuitenkin hieman monimutkaisempaa kuin konnektiivisääntöjen käyttö. Jokaiseen sääntöön liittyy joitakin epätriviaaleja semanttisia oletuksia lauseista ja termeistä. Tästä syystä käymme seuraavaksi näitä sääntöjä läpi hieman tarkemmin.

Universaalikvanttori

Universaalikvanttorilla voidaan ilmaista, että jokin asia pätee jokaisella alkiolla. Universaalikvanttorin eliminointisääntö onkin helppo: mikäli φ pätee *millä tahansa* x, se pätee erityisesti kun muuttujan x paikalle sijoitetaan jonkin konkreettisen olion nimi eli termi.

$$\frac{\forall x_i \varphi}{\varphi(t/x_i)}\ \forall E$$

Tässä on kuitenkin vaaran paikka. Sääntöä ei saa käyttää, jos termissä t oleva muuttuja tulisi sidotuksi sijoituksessa! Tutkitaan virheellistä päättelyä

$$\frac{\forall x \exists y A(x,y)}{\exists y A(y,y)}\ {\scriptstyle \forall E}.$$

Säännön sovelluksessa on ajateltu, että koska lause $\exists y A(x,y)$ pätee millä tahansa x, pätee se erityisesti, kun muuttujan x paikalle sijoitetaan y. Tämä on kuitenkin virhe, sillä muuttuja y tulisi tällaisessa sijoituksessa sidotuksi. Jos atomikaavan $A(x,y)$ ajateltaan tarkoittavan "y on henkilön x äiti", niin edellisen päättelyn oletus sanoo, että jokaisella ihmisellä on äiti. Tästä ei tietenkään voida vetää johtopäätöstä, että jokin ihminen on itsensä äiti, mitä kaava $\exists y A(y,y)$ väittää.

Kaava $\forall x \exists y A(x,y)$ väittää, että "jokaista x kohti löytyy jokin $y\ldots$", eli *muuttujan y arvo saa riippua muuttujan x arvosta.* Edellisessä päättelyssä vikaan siis menee se, että jos muuttuja y sijoitetaan kaavaan muuttujan x tilalle ja se tulee sijoituksessa sidotuksi, ei "toista y:n arvoa" voidakaan enää valita vapaasti. Muuttujien välille syntyy yhteys, jota alkuperäisessä kaavassa ei ollut.

Universaalikvanttorin tuontisääntöä

$$\frac{\varphi}{\forall x_i \varphi}\ {\scriptstyle \forall I}$$

saa käyttää mikäli muuttuja x_i ei esiinny vapaana kaavan φ todistuksen hylkäämättömissä oletuksissa. Idea on tässäkin tuttu: kun haluamme näyttää, että jokin väite pätee *jokaisella* alkiolla, otamme mielivaltaisen alkion, josta emme oleta mitään, ja näytämme että väite pätee sillä. Koska emme tee mitään oletuksia kyseisestä alkiosta, voisi sen paikalla yhtä hyvin olla mikä tahansa alkio. Väite siis pätee kaikilla alkioilla.

3.45 Esimerkki. Näytetään, että jos jokainen kreikkalainen on ihminen, ja jokainen ihminen on kuolevainen, niin jokainen kreikkalainen on kuolevainen.

Todistus. Olkoon x mielivaltainen. Oletetaan, että x on kreikkalainen. Koska jokainen kreikkalainen on myös ihminen, niin koska x on kreikkalainen, x on ihminen. Koska jokainen ihminen taas on kuolevainen, ja x on ihminen, niin x on kuolevainen. Jos x siis on kreikkalainen, x on kuolevainen. Koska x oli mielivaltainen, väite pätee kaikilla x, eli jokainen kreikkalainen on kuolevainen.

Muotoillaan sama luonnollisena päättelynä. Käytetään predikaattisymbolia E merkkaamaan kreikkalaisia, I ihmisiä ja K kuolevaisia.

$$\dfrac{\dfrac{\dfrac{\dfrac{[E(x)]^1 \quad \dfrac{\forall y(E(y)\to I(y))}{E(x)\to I(x)}\,{\scriptstyle \forall E}}{I(x)}\,{\scriptstyle \to E} \quad \dfrac{\forall y(I(y)\to K(y))}{I(x)\to K(x)}\,{\scriptstyle \forall E}}{K(x)}\,{\scriptstyle \to E}}{E(x)\to K(x)}\,{\scriptstyle \to I,1}}{\forall x(E(x)\to K(x))}\,{\scriptstyle \forall I}$$

$\square$

Eksistenssikvanttori

Yleinen tapa osoittaa jonkin asian olemassaolo on konstruoida jokin olio ja näyttää, että se tosiaan on halutunlainen. Tämä on idea eksistenssikvanttorin tuontisäännössä:

$$\frac{\varphi(t/x_i)}{\exists x_i \varphi}\ {\scriptstyle \exists I}$$

Jos olemme näyttäneet, että termin t merkitsemällä alkiolla on jokin ominaisuus, niin tiedämme, että on olemassa jokin alkio, jolla on tämä ominaisuus.

Esimerkiksi jos Sokrates on mies, ja jokainen mies on kuolevainen, niin on olemassa ainakin yksi kuolevainen:

$$\cfrac{\cfrac{\cfrac{\forall x(M(x) \to K(x))}{M(S) \to K(S)}\ {\scriptstyle \forall E} \qquad M(S)}{K(S)}\ {\scriptstyle \to E}}{\exists x K(x)}\ {\scriptstyle \exists I}$$

Tämänkin säännön käyttöön liittyy rajoite: jos termissä t on muuttuja, joka olisi kaavassa $\varphi(t/x_i)$ kvantifioitu, ei sääntöä voida käyttää. Jos valitaan $\varphi = \forall y T(x,y)$, $t = y$ ja $x_i = x$, saadaa virheellinen päättely

$$\frac{\forall y T(y,y)}{\exists x \forall y T(x,y)}\ {\scriptstyle \exists I}$$

Jos esimerkiksi atomikaava $T(x,y)$ tulkitaan relaatioksi "x tuntee y:n", niin oletus $\forall y T(y,y)$ ilmaisee, että jokainen ihminen tuntee itsensä. Tästä ei tietystikään voida vetää johtopäätöstä, että jokin ihminen tuntisi kaikki ihmiset, mitä kaava $\exists x \forall y T(x,y)$ väittää.

Eksistenssikvanttorin vientisäännössä

$$\frac{\exists x_i \varphi \qquad \begin{matrix}[\varphi] \\ \vdots \\ \psi\end{matrix}}{\psi}$$

vaatimuksena on, että muuttuja x_i ei esiinny vapaana kaavassa ψ, eikä sen päättelyyn käytetyissä oletuksissa, paitsi mahdollisesti kaavassa φ. Ideana on, että muuttujan x_i merkkaamasta alkiosta ei tiedetä mitään muuta kuin että se toteuttaa kaavan φ. Jos tällöin voidaan päätellä, että jokin muuttujaa x_i mainitsematon väite ψ pätee, ja toisaalta tiedämme, että tällainen alkio x_i on olemassa, voimme todeta, että kaavan ψ tosiaan on pädettävä.

Päätellään esimerkiksi $\neg \forall x_1 P(x_1)$ oletuksesta $\exists x_0 \neg P(x_0)$. Oletus siis sanoo, että löytyy jokin alkio, joka ei ole relaatiossa P. Nimetään tätä alkiota muuttujalla x_0, eli tiedämme, että $P(x_0)$. Edetään vastaoletuksella: jos pätisi $\forall x_1 P(x_1)$, erityisesti pätisi

$P(x_0)$. Näin saisimme ristiriidan $P(x_0) \wedge \neg P(x_0)$. Voimme siis todeta, että on pädettävä $\neg \forall x_1 P(x_1)$.

Sama luonnollisena päättelynä:

$$\dfrac{\exists x_0 \neg P(x_0) \qquad \dfrac{\dfrac{\dfrac{[\forall x_1 P(x_1)]^1}{P(x_0)}\,{\scriptstyle \forall E} \qquad [\neg P(x_0)]^2}{P(x_0) \wedge \neg P(x_0)}\,{\scriptstyle \wedge I}}{\neg \forall x_1 P(x_1)}\,{\scriptstyle \neg I,1}}{\neg \forall x_1 P(x_1)}\,{\scriptstyle \exists E,2}$$

Eksistenssikvanttorilla voidaan siis tavallaan ”ottaa kiinni” jostakin kaavan φ toteuttavasta alkiosta, eli antaa sille nimi, jolla siitä voidaan puhua.

Identiteetti[2]

Identiteettiin liittyvät säännöt tuskin kaipaavat kummempaa selittelyä. Kolme ensimmäistä sanovat, että relaatio $=$ on refleksiivinen, symmetrinen ja transitiivinen (siis ekvivalenssirelaatio). Neljäs sääntö kuvaa sitä, että mikäli kaksi asiaa ovat samat, niin niillä on kaikki samat ominaisuudet, ne siis toteuttavat kaikki samat kaavat. Säännön

$$\dfrac{}{t = t}\,{\scriptstyle =1}$$

avulla voidaan aina päätellä $t = t$ mille tahansa termille t. Tällöin ei tarvita edes oletuksia, sillä viiva kaavan $t = t$ päällä, tarkoittaa sitä, että kaava $t = t$ on tosiaan saatu päättelysäännöllä, eikä se ole oletus. Esimerkiksi päättely

$$\dfrac{\dfrac{}{x_0 = x_0}\,{\scriptstyle =1}}{\forall x_0 (x_0 = x_0)}\,{\scriptstyle \forall I}$$

osoittaa, että $\emptyset \vdash \forall x_0 (x_0 = x_0)$.

Päättelysääntöjen $= 2$ ja $= 3$ avulla voidaan esimerkiksi päätellä että jos $x_0 = x_1$ ja $x_0 = x_2$, niin $x_1 = x_2$:

$$\dfrac{\dfrac{x_0 = x_1}{x_1 = x_0}\,{\scriptstyle =2} \qquad x_0 = x_2}{x_1 = x_2}\,{\scriptstyle =3}$$

Sääntö $= 4$ on ”liha luiden ympärillä” identiteettiin liittyvässä päättelyssä. Mietitään esimerkiksi oletuksia $\forall x_0 \forall x_1 (x_0 = x_1)$, $\exists x_3 P(x_3)$ ja $\exists x_4 \neg P(x_4)$. Näistä ensimmäinen sanoo, että jos mallista valitaan kaksi alkiota millä tahansa tavalla, niin ne ovat itse asiassa sama alkio. Tämä pätee mallissa tietysti vain silloin, jos siinä ei ole kuin yksi alkio. Kaksi muuta kaavaa taas ilmaisevat, että löytyy jokin alkio joka on symbolilla P nimetyssä relaatiossa ja jokin alkio, joka ei ole. Jos mallissa kuitenkin on

[2] Kirjassa [JohLog] luonnolliseen päättelyyn ei oteta mukaan identiteettisääntöjä, vaan erityiset *identiteettiaksioomat*, jotka saa aina olettaa.

vain yksi alkio, ei tällaisia alkiota voi löytyä. Päätellään $\neg\forall x_0\forall x_1(x_0 = x_1)$ oletuksista $\exists x_3 P(x_3)$ ja $\exists x_4\neg P(x_4)$:

$$
\begin{prooftree}
\AxiomC{$\exists x_4\neg P(x_4)$}
\AxiomC{$\exists x_3 P(x_3)$}
\AxiomC{$[P(x_3)]^1$}
\AxiomC{$[\forall x_0\forall x_1(x_0 = x_1)]^2$}
\RightLabel{$\scriptstyle \forall E$}
\UnaryInfC{$\forall x_1(x_3 = x_1)$}
\RightLabel{$\scriptstyle \forall E$}
\UnaryInfC{$x_3 = x_4$}
\RightLabel{$\scriptstyle =4$}
\BinaryInfC{$P(x_4)$}
\RightLabel{$\scriptstyle \exists E,1$}
\BinaryInfC{$P(x_4)$}
\AxiomC{$[\neg P(x_4)]^3$}
\RightLabel{$\scriptstyle \wedge I$}
\BinaryInfC{$P(x_4)\wedge\neg P(x_4)$}
\RightLabel{$\scriptstyle \neg I,2$}
\UnaryInfC{$\neg\forall x_0\forall x_1(x_0 = x_1)$}
\RightLabel{$\scriptstyle \exists E,3$}
\BinaryInfC{$\neg\forall x_0\forall x_1(x_0 = x_1)$}
\end{prooftree}
$$

3.46 Esimerkki. Olkoon $L = \{E\}$ verkkojen aakkosto ja

$$T_{\mathrm{graph}} = \{\forall x\neg E(x,x), \forall x\forall y(E(x,y)\to E(y,x))\}\,.$$

Joukkoa T_{graph} sanotaan *verkkojen teoriaksi.* L-malli on siis verkko jos ja vain jos se toteuttaa joukon T_{graph} lauseet.

Osoitetaan, että jos verkon jokaisesta pisteestä menee viiva jonnekin, niin verkossa on vähintään kaksi pistettä. Siis $T_{\mathrm{graph}} \vdash \forall x\exists y E(x,y)\to\exists x\exists y\neg x = y$.

Todistus. Päättely voisi edetä esimerkiksi näin: Oletetaan, että jokaisesta pisteestä menee viiva jonnekin. Olkoon x jokin verkon piste. Tällöin pisteestä x menee siis viiva johonkin pisteeseen y. Jos pätisi $x = y$, pisteestä x menisi viiva itseensä, mutta näin ei kuitenkaan verkossa voi käydä. Siis $x \neq y$, eli verkosta löytyy kaksi eri pistettä.

Vastaava luonnollinen päättely olisi

$$
\begin{prooftree}
\AxiomC{$[\forall x\exists y E(x,y)]^3$}
\RightLabel{$\scriptstyle \forall E$}
\UnaryInfC{$\exists y E(x,y)$}
\AxiomC{$[x = y]^1$}
\AxiomC{$[E(x,y)]^2$}
\RightLabel{$\scriptstyle =4$}
\BinaryInfC{$E(x,x)$}
\AxiomC{$\forall x\neg E(x,x)$}
\RightLabel{$\scriptstyle \forall E$}
\UnaryInfC{$\neg E(x,x)$}
\RightLabel{$\scriptstyle \wedge I$}
\BinaryInfC{$E(x,x)\wedge\neg E(x,x)$}
\RightLabel{$\scriptstyle \neg I,1$}
\UnaryInfC{$\neg x = y$}
\RightLabel{$\scriptstyle \exists I$}
\UnaryInfC{$\exists y\neg x = y$}
\RightLabel{$\scriptstyle \exists I$}
\UnaryInfC{$\exists x\exists y\neg x = y$}
\RightLabel{$\scriptstyle \exists E,2$}
\BinaryInfC{$\exists x\exists y\neg x = y$}
\RightLabel{$\scriptstyle \to I,3$}
\UnaryInfC{$\forall x\exists y E(x,y)\to\exists x\exists y\neg x = y$}
\end{prooftree}
$$

□

3.47 Esimerkki. $T_{\mathrm{graph}} \vdash \neg\exists x\forall y E(x,y)$. Verkossa ei siis ole pistettä, josta menisi viiva jokaiseen pisteeseen, sillä pisteestä ei tietenkään voi mennä viivaa pisteeseen itseensä.

Todistus.

$$
\dfrac{\dfrac{\dfrac{[\exists x\forall yE(x,y)]^2 \qquad \dfrac{\dfrac{\dfrac{[\forall yE(x,y)]^1}{E(x,x)}{\scriptstyle \forall E} \quad \dfrac{\forall x\neg E(x,x)}{\neg E(x,x)}{\scriptstyle \forall E}}{E(x,x)\wedge\neg E(x,x)}{\scriptstyle \wedge I}}{\neg y=y}{\scriptstyle \neg I}}{\neg y=y}{\scriptstyle \exists E,1} \qquad \dfrac{}{y=y}{\scriptstyle =1}}{y=y\wedge\neg y=y}{\scriptstyle \wedge I}}{\neg\exists x\forall yE(x,y)}{\scriptstyle \neg I,2}
$$

Tässä päättelyssä kaavan $\neg y=y$ tuonti on tekninen kikka. Päättelyssä päällimmäisenä ideana on muoto

$$
\dfrac{\dfrac{[\exists x\forall yE(x,y)]^2 \qquad \dfrac{\begin{matrix}[\forall yE(x,y)]^1 & \forall x\neg E(x,x)\\ \vdots & \vdots\end{matrix}}{\text{ristiriita}}}{\text{ristiriita}}{\scriptstyle \exists E,1}}{\neg\exists x\forall yE(x,y)}{\scriptstyle \neg I,2}
$$

Halutuksi ristiriidaksi ei kuitenkaan voida valita kaavaa $E(x,x)\wedge\neg E(x,x)$, sillä muuttuja x esiintyy tässä vapaana, joten sääntöä $\exists E$ ei voida soveltaa. □

3.9 Predikaattilogiikan eheys- ja täydellisyyslauseet

Kuten propositiologiikassa, eheys- ja täydellisyyslauseet osoittavat, että päättelymme tekee juuri sen, mitä haluammekin sen tekevän: todistaa kaikki totuudet eikä mitään muuta.

Eheyslause

3.48 Lemma. Olkoon $\mathcal{M}$ L-malli, s tulkintajono, x_i muuttuja ja t sekä t' termejä. Tällöin $s(t(t'/x_i)) = s(s(t')/x_i)(t)$.

Todistus. Jos $t = x_i$, $s(t(t'/x_i)) = s(t') = s(s(t')/x_i)(t)$. Jos $t = x_j$ jollakin $j \neq i$, $s(t(t'/x_i)) = s(x_j) = s(s(t')/x_i)(t)$. Jos $t = c$ jollakin $c \in L$, $s(t(t'/x_i)) = c^{\mathcal{M}} = s(s(t')/x_i)(t)$. □

3.49 Lemma. Olkoon φ L-kaava, x_i muuttuja ja t termi, ja oletetaan, että termi t on vapaa muuttujalle x_i kaavassa φ. Tällöin millä tahansa L-mallilla $\mathcal{M}$ ja tulkintajonolla s

$$\mathcal{M} \models_s \varphi(t/x_i) \quad \text{jos ja vain jos} \quad \mathcal{M} \models_{s(s(t)/x_i)} \varphi.$$

Todistus. Todistetaan väite induktiolla kaavan φ rakenteen suhteen.

1. Oletetaan aluksi, että φ on atomikaava, eli joko muotoa $t_1 = t_2$ tai $R(t_1, \ldots, t_n)$.

   Jos $\varphi = t_1 = t_2$,

$$\begin{aligned} \mathcal{M} \models_s \varphi(t/x_i) &\iff s(t_1(t/x_i)) = s(t_2(t/x_i)) \\ &\iff s(s(t)/x_i)(t_1) = s(s(t)/x_i)(t_2) \\ &\iff \mathcal{M} \models_{s(s(t)/x_i)} \varphi. \end{aligned}$$

   Jos taas $\varphi = R(t_1, \ldots, t_n)$,

$$\begin{aligned} \mathcal{M} \models_s \varphi(t/x_i) &\iff (s(t_1(t/x_i)), \ldots, s(t_n(t/x_i))) \in R^{\mathcal{M}} \\ &\iff (s(s(t)/x_i)(t_1), \ldots, s(s(t)/x_i)(t_n)) \in R^{\mathcal{M}} \\ &\iff \mathcal{M} \models_{s(s(t)/x_i)} \varphi. \end{aligned}$$

2. Todistetaan konnektiiveihin liittyvistä induktioaskelista ainoastaan $\neg$ ja $\wedge$. Muut voidaan todistaa samoin. Jos $\varphi = \neg\psi$,

$$\begin{aligned} \mathcal{M} \models_s \varphi(t/x_i) &\iff \mathcal{M} \models_s (\neg\psi)(t/x_i) \\ &\iff \mathcal{M} \models_s \neg\psi(t/x_i) \\ &\iff \mathcal{M} \not\models_s \psi(t/x_i) \\ &\overset{\text{i.o.}}{\iff} \mathcal{M} \not\models_{s(s(t)/x_i)} \psi \\ &\iff \mathcal{M} \models_{s(s(t)/x_i)} \varphi. \end{aligned}$$

   Jos $\varphi = \psi \wedge \theta$,

$$\begin{aligned} \mathcal{M} \models_s \varphi(t/x_i) &\iff \mathcal{M} \models_s (\psi \wedge \theta)(t/x_i) \\ &\iff \mathcal{M} \models_s \psi(t/x_i) \wedge \theta(t/x_i) \\ &\iff \mathcal{M} \models_s \psi(t/x_i) \text{ ja } \mathcal{M} \models_s \theta(t/x_i) \\ &\overset{\text{i.o.}}{\iff} \mathcal{M} \models_{s(s(t)/x_i)} \psi \text{ ja } \mathcal{M} \models_{s(s(t)/x_i)} \theta \\ &\iff \mathcal{M} \models_{s(s(t)/x_i)} \varphi. \end{aligned}$$

3. Oletetaan nyt, että $\varphi = \forall x_j \psi$ ja oletetaan, että väite pätee kaavalle ψ. Jos $x_i = x_j$, ei muuttuja x_i esiinny vapaana kaavassa φ, joten $\varphi(t/x_i) = \varphi$. Tällöin tulkintajonon muuttujalle x_i antama arvo ei myöskään vaikuta kaavan φ totuuteen, eli

$$\begin{aligned} \mathcal{M} \models_s \varphi(t/x_i) &\iff \mathcal{M} \models_s \varphi \\ &\iff \mathcal{M} \models_{s(s(t)/x_i)} \varphi. \end{aligned}$$

   Jos $x_i \neq x_j$, koska termi t on vapaa muuttujalle x_i kaavassa φ, ei termissä t voi esiintyä muuttujaa x_j. Lisäksi termi t on vapaa muuttujalle x_i myös kaavassa ψ.

Tällöin

$$\begin{aligned}
\mathcal{M} \models_s \varphi(t/x_i) &\iff \mathcal{M} \models_s \forall x_j(\psi(t/x_i)) \\
&\iff \text{jokaisella } a \in \mathcal{M},\ \mathcal{M} \models_{s(a/x_j)} \psi(t/x_i) \\
&\overset{\text{i.o.}}{\iff} \text{jokaisella } a \in \mathcal{M},\ \mathcal{M} \models_{s(a/x_j)(s(a/x_j)(t)/x_i)} \psi \\
&\iff \text{jokaisella } a \in \mathcal{M},\ \mathcal{M} \models_{s(a/x_j)(s(t)/x_i)} \psi \\
&\iff \text{jokaisella } a \in \mathcal{M},\ \mathcal{M} \models_{s(s(t)/x_i)(a/x_j)} \psi \\
&\iff \mathcal{M} \models_{s(s(t)/x_i)} \varphi.
\end{aligned}$$

Eksistenssikvanttoria koskeva induktioaskel voidaan todistaa samoin.

□

Predikaattilogiikan eheyslauseen todistus on rakenteeltaan samanlainen kuin propositiologiikan eheyslauseen. Tärkein osa todistusta on seuraava lemma, jota propositiologiikassa vastasi lemma 2.37. Koska konnektiiveihin liittyvät päättelysäännöt ovat molemmissa logiikoissa täysin samat, niihin liittyvät induktioaskeleet ovat käytännössä samat kuin lemmassa 2.37.

3.50 Lemma. Olkoon $\mathcal{P}$ päättely, jonka oletusten joukko on $\Sigma_{\mathcal{P}}$ ja johtopäätös φ. Tällöin $\Sigma_{\mathcal{P}} \Rightarrow \varphi$.

Todistus. Jos päättely $\mathcal{P}$ on triviaali päättely, jonka ainut oletus on φ ja johtopäätös φ. Jos $\mathcal{M}$ toteuttaa tulkintajonolla s kaikki joukon $\Sigma_{\mathcal{P}}$ oletukset, niin se toteuttaa kaavan φ. Siis $\Sigma_{\mathcal{P}} \Rightarrow \varphi$. Konnektiiveihin liittyviin päättelyaskeliin liittyvät induktioaskeleet voidaan todistaa kuten lemmassa 2.37.

Osoitettavaksi jää kvanttoreihin ja identiteettiin liittyvät induktioaskeleet.

$\boxed{\forall I}$ Oletetaan siis, että väite pätee päättelylle $\begin{array}{c}\mathcal{P}\\ \psi\end{array}$. Olkoon $\mathcal{Q}$ päättely $\dfrac{\begin{array}{c}\mathcal{P}\\ \psi\end{array}}{\forall x_i\psi}$, missä x_i ei esiinny vapaana päättelyn $\mathcal{P}$ oletuksissa.

Päättelyissä $\mathcal{P}$ ja $\mathcal{Q}$ on samat oletukset. Olkoon $\mathcal{M}$ malli ja s tulkintajono, jotka toteuttavat kaikki päättelyn $\mathcal{Q}$ oletukset. Olkoon $a \in \mathcal{M}$ mielivaltainen. Koska x_i ei esiinny vapaana päättelyn $\mathcal{P}$ oletuksissa, myös tulkintajono $s(a/x_i)$ toteuttaa ne, joten induktio-oletuksen nojalla $\mathcal{M} \models_{s(a/x_i)} \psi$. Siis millä tahansa $a \in \mathcal{M}$

$$\mathcal{M} \models_{s(a/x_i)} \psi,$$

joten $\mathcal{M} \models_s \forall x_i\psi$. Siis väite pätee myös päättelylle $\mathcal{Q}$.

$\boxed{\forall E}$ Oletetaan, että väite pätee päättelylle $\begin{array}{c}\mathcal{P}\\ \forall x_i\varphi\end{array}$. Olkoon $\mathcal{Q}$ päättely $\dfrac{\begin{array}{c}\mathcal{P}\\ \forall x_i\varphi\end{array}}{\varphi(t/x_i)}$, missä t on vapaa muuttujalle x_i kaavassa φ. Oletetaan, että $\mathcal{M}$ ja s toteuttavat kaikki päättelyn $\mathcal{Q}$ oletukset. Nämä ovat samat kuin päättelyn $\mathcal{P}$ oletukset, joten induktio-oletuksen nojalla $\mathcal{M} \models_s \forall x_i \varphi$. Siis millä tahansa $a \in \mathcal{M}$, $\mathcal{M} \models_{s(a/x_i)} \varphi$, erityisesti

$$\mathcal{M} \models_{s(s(t)/x_i)} \varphi.$$

Koska t on vapaa muuttujalle x_i kaavassa φ, lemman 3.49 nojalla $\mathcal{M} \models_s \varphi(t/x_i)$, joten väite pätee myös päättelylle $\mathcal{Q}$.

$\boxed{\exists I}$ Oletetaan, että väite pätee päättelylle $\begin{array}{c}\mathcal{P}\\ \psi\end{array}$, missä t on vapaa muuttujalle x_i kaavassa φ. Olkoon $\mathcal{Q}$ päättely $\begin{array}{c}\mathcal{P}\\ \varphi(t/x_i) \\ \hline \exists x_i \varphi\end{array}$. Oletetaan, että $\mathcal{M}$ ja s toteuttavat kaikki päättelyn $\mathcal{Q}$ oletukset. Nämä ovat samat kuin päättelyn $\mathcal{P}$ oletukset, joten induktio-oletuksen nojalla $\mathcal{M} \models_s \varphi(t/x_i)$. Koska t on vapaa muuttujalle x_i kaavassa φ, lemman 3.49 nojalla $\mathcal{M} \models_{s(s(t)/x_i)} \varphi$. Täten $\mathcal{M} \models_s \exists x_i \varphi$, joten väite pätee päättelylle $\mathcal{Q}$.

$\boxed{\exists E}$ Oletetaan, että väite pätee päättelyille $\begin{array}{c}\mathcal{P}\\ \exists x_i \varphi\end{array}$ ja $\begin{array}{c}\varphi\\ \mathcal{Q}\\ \psi\end{array}$, missä x_i ei esiinny vapaana kaavassa ψ eikä päättelyn $\mathcal{Q}$ oletuksissa kaavaa φ lukuunottamatta. Olkoon $\mathcal{R}$ päättely $\begin{array}{cc} & [\varphi] \\ \mathcal{P} & \mathcal{Q} \\ \exists x_i \varphi & \psi \\ \hline \multicolumn{2}{c}{\psi}\end{array}$. Oletetaan, että $\mathcal{M}$ ja s toteuttavat kaikki päättelyn $\mathcal{R}$ oletukset. Erityisesti ne toteuttavat kaikki päättelyn $\mathcal{P}$ oletukset, joten induktio-oletuksen nojalla myös kaava $\exists x_i \varphi$ toteutuu. Löytyy siis jokin $a \in \mathcal{M}$, jolla $\mathcal{M} \models_{s(a/x_i)} \varphi$. Koska x_i ei esiinny vapaana päättelyn $\mathcal{Q}$ oletuksissa, myös $s(a/x_i)$ toteuttaa ne. Tulkintajono $s(a/x_i)$ toteuttaa siis kaikki päättelyn $\mathcal{Q}$ oletukset, joten induktio-oletuksen nojalla $\mathcal{M} \models_{s(a/x_i)} \psi$. Koska x_i ei esiinny vapaana kaavassa ψ, $\mathcal{M} \models_s \psi$, joten väite pätee myös päättelylle $\mathcal{R}$.

$\boxed{=1}$ Millä tahansa termillä t, mallilla $\mathcal{M}$ ja tulkintajonolla s, $\mathcal{M} \models_s t = t$, joten päättelyn $\begin{array}{c}\hline t = t\end{array}$ oletuksista (joita ei ole) seuraa loogisesti $t = t$.

$\boxed{=2}$ Oletetaan, että väite pätee päättelylle $\begin{array}{c}\mathcal{P}\\ t = u\end{array}$. Olkoon $\mathcal{Q}$ päättely $\begin{array}{c}\mathcal{P}\\ t = u \\ \hline u = t\end{array}$. Oletetaan, että $\mathcal{M}$ ja s toteuttavat päättelyn $\mathcal{Q}$ oletukset. Nämä ovat samalla päättelyn $\mathcal{P}$ oletukset, joten induktio-oletuksen nojalla $\mathcal{M} \models_s t = u$, eli $s(t) = s(u)$. Tällöin tietysti $s(u) = s(t)$, joten $\mathcal{M} \models_s u = t$.

$\boxed{=3}$ Oletetaan, että väite pätee sekä päättelylle $\begin{array}{c}\mathcal{P}\\ t_1 = t_2\end{array}$, että päättelylle $\begin{array}{c}\mathcal{Q}\\ t_2 = t_3\end{array}$. Olkoon $\mathcal{R}$ päättely $\begin{array}{cc}\mathcal{P} & \mathcal{Q} \\ t_1 = t_2 & t_2 = t_3 \\ \hline \multicolumn{2}{c}{t_1 = t_3}\end{array}$. Oletetaan, että $\mathcal{M}$ ja s toteuttavat päättelyn $\mathcal{R}$ oletukset. Siispä päättelyiden $\mathcal{P}$ ja $\mathcal{Q}$ oletukset toteutuvat, joten induktio-oletuksen nojalla $\mathcal{M} \models_s t_1 = t_2$ ja $\mathcal{M} \models_s t_2 = t_3$. Siis $s(t_1) = s(t_2)$ ja $s(t_2) = s(t_3)$, joten $s(t_1) = s(t_3)$, joten $\mathcal{M} \models_s t_1 = t_3$. Siis väite pätee myös päättelylle $\mathcal{R}$.

$\boxed{=4}$ Oletetaan, että väite pätee sekä päättelylle $\begin{array}{c}\mathcal{P}\\ t=u\end{array}$, että päättelylle $\begin{array}{c}\mathcal{Q}\\ \varphi(t/x_i)\end{array}$, ja sekä termi t että termi u on vapaa muuttujalle x_i kaavassa φ. Olkoon $\mathcal{R}$ päättely $\dfrac{\begin{array}{cc}\mathcal{P} & \mathcal{Q}\\ t=u & \varphi(t/x_i)\end{array}}{\varphi(u/x_i)}$, ja oletetaan, että $\mathcal{M}$ ja s toteuttavat päättelyn $\mathcal{R}$ oletukset. Siis sekä päättelyn $\mathcal{P}$ että päättelyn $\mathcal{Q}$ oletukset toteutuvat, joten induktio-oletuksen nojalla $\mathcal{M} \models_s t = u$ ja $\mathcal{M} \models_s \varphi(t/x_i)$. Lemman 3.49 nojalla $\mathcal{M} \models_{s(s(t)/x_i)} \varphi$. Koska $s(t) = s(u)$, $\mathcal{M} \models_{s(s(u)/x_i)} \varphi$, ja edelleen lemman 3.49 nojalla $\mathcal{M} \models_s \varphi(t/x_i)$, joten väite pätee päättelylle $\mathcal{R}$.

$\square$

Predikaattilogiikan eheyslause. *Jos* $\Sigma \vdash \varphi$, *niin* $\Sigma \Rightarrow \varphi$.

Todistus. Oletetaan, että $\Sigma \vdash \varphi$. Siis on olemassa luonnollinen päättely $\mathcal{P}$, jonka oletusten joukko $\Sigma_{\mathcal{P}}$ sisältyy joukkoon Σ. Olkoon $\mathcal{M}$ malli ja s tulkintajono, ja oletetaan, että jokainen joukon Σ kaava toteutuu mallissa $\mathcal{M}$ tulkintajonolla s. Erityisesti joukon $\Sigma_{\mathcal{P}}$ kaavat toteutuvat, ja φ on niiden looginen seuraus, joten $\mathcal{M} \models_s \varphi$. $\square$

A Disjunktiivinen normaalimuoto

Normaalimuodolla tarkoitetaan tiettyjä syntaktisia ehtoja täyttävää lausetta. Yleensä jokaista lausetta kohti on olemassa ekvivalentti normaalimuotoinen lause, ja lauseiden semantiikka tutkittaessa ei tietysti ole väliä, mitä ekvivalenteista lauseista käytetään. Normaalimuodon etuna saattaa olla esimerkiksi yksinkertaisempi rakenne, jolloin lauseen käsittely algoritmisesti saattaa vaatia vähemmän aikaa tai yksinkertaisemman algoritmin.

Käytämme kappaleessa 2.7 sovittuja lyhenteitä.

A.1 Disjunktiivinen normaalimuoto

A.1 Määritelmä. Propositiolausetta, joka on joko yksittäinen propositiosymboli tai yksittäisen propositiosymbolin negaatio, sanotaan **literaaksi**. Propositiolauseen sanotaan olevan **disjunktiivisessä normaalimuodossa**, mikäli se on muodostettu disjunktiolla lauseista, jotka on muodostettu konjunktiolla literaaleista.

Edellisessä määritelmässä sallitaan ”surkastuneet konjunktiot ja disjunktiot”, eli tilanteet, jossa konjunkteja tai disjunkteja on vain yksi. Tällöin siis ”konjunktio” tai ”disjunktio” tästä lauseesta on vain lause itse.

A.2 Esimerkki. Seuraavat lauseet ovat disjunktiivisessa normaalimuodossa.

$$\begin{array}{ll}
(p_0 \wedge \neg p_1) \vee (p_1 \wedge \neg p_0) & p_0 \vee \neg p_4 \vee (p_5 \wedge \neg p_1) \\
(p_1 \wedge p_2) \vee (\neg p_5 \wedge p_5) \vee (p_6 \wedge p_6 \wedge p_6) & (p_9 \wedge \neg p_7) \vee p_7 \vee (p_0 \wedge \neg p_7) \\
(p_0 \wedge p_0 \wedge p_0) \vee (\neg p_0 \wedge \neg p_0) & p_0 \wedge \neg p_3
\end{array}$$

A.3 Lause. Jokaista propositiologiikan lausetta B kohti on olemassa disjunktiivisessa normaalimuodossa oleva lause A, jolla $A \Leftrightarrow B$.

Todistus. Olkoon B propositiologiikan lause. Olkoon n suurin luku, jolla symboli p_{n-1} esiintyy lauseessa B. Olkoon T_B lauseen B n-paikkainen totuusfunktio. Lauseen 2.24 todistuksessa konstruoitiin lause A, joka on disjunktiivisessa normaalimuodossa, ja jolla $T_A = T_B$. Tällöin $A \Leftrightarrow B$. □

Propositiolauseen kanssa ekvivalentteja disjunktiivisessa normaalimuodossa olevia propositiolauseita on tietysti useita. Jos esimerkiksi lause A on disjunktiivisessa normaalimuodossa, niin myös lause $A \vee A$ on. Tietysti $A \Leftrightarrow A \vee A$.

A.4 Esimerkki. Seuraavassa taulukossa on annettu joitakin propositiologiikan lauseita, ja niiden kanssa ekvivalentteja disjunktiivisessa normaalimuodossa olevia lauseita.

Lause	Disjunktiivinen normaalimuoto
$(p_0 \to p_1)$	$\neg p_0 \vee p_1$
$\neg(p_0 \to p_1)$	$p_0 \wedge \neg p_1$
$(p_1 \leftrightarrow p_2)$	$(p_1 \wedge p_2) \vee (\neg p_1 \wedge \neg p_2)$
$(p_0 \wedge (p_1 \vee p_2))$	$(p_0 \wedge p_1) \vee (p_0 \wedge p_2)$
$(p_0 \leftrightarrow (p_1 \leftrightarrow \neg p_2))$	$(p_0 \wedge p_1 \wedge \neg p_2) \vee (p_0 \wedge \neg p_1 \wedge p_2) \vee (\neg p_0 \wedge p_1 \wedge p_2) \vee (\neg p_0 \wedge \neg p_1 \wedge p_2)$

A.2 Sovelluksia tietojenkäsittelytieteeseen

Yleisessä tapauksessa voi olla hyvinkin työlästä selvittää, onko jokin propositiolause ristiriita. Eräs tapa tehdä tämä, on totuustaulu. Totuustaulusta voi kuitenkin tulla valtava suhteellisen yksinkertaisillakin propositiolauseilla, jos niissä esiintyy monta eri propositiosymbolia. Esimerkiksi lauseen

$$((p_0 \wedge (p_1 \to \neg(p_2 \vee p_3))) \to (p_6 \vee (\neg p_4 \leftrightarrow p_5)))$$

totuustaulussa olisi jo $2^7 = 128$ riviä. Pahimmassa tapauksessa totuustaulun piirtämiseen menee siis eksponentiaalinen määrä aikaa suhteessa lauseen pituuteen. Tätä voi tietysti optimoida, eihän koko totuustaulua välttämättä tarvitse piirtää, jos huomataan, että jollakin taulun rivillä lause toteutuu. Toinen tapa ratkaista ongelma on piirtää lauseen semanttinen puu, mutta pahimmassa tapauksessa tämäkin vie eksponentiaalisen määrän aikaa.

Onkin tunnettua, että ongelma "selvitä, toteutuuko lause A jollakin totuusjakaumalla", tuttavallisemmin SAT, on NP-täydellinen, eli käytännössä nykymenetelmin hyvin hankala ratkaista. Yleisessä tapauksessa polynomiaikaisesti tähän kysymykseen oikein vastaava algoritmi olisikin vastaus P=NP -ongelmaan, jonka ratkaisusta Clay -instituutti on luvannut miljoonan dollarin Millenium -palkinnon.

Mikäli lause A on disjunktiivisessä normaalimuodossa, ongelma kuitenkin yksinkertaistuu huomattavasti. Lause $A = A_1 \vee A_2 \vee \ldots \vee A_n$ nimittäin toteutuu jos ja vain jos jokin disjunkteista A_i toteutuu. Tällainen disjunkti $A_i = q_1 \wedge q_2 \wedge \ldots \wedge q_m$, missä $q_1, \ldots, q_m$ ovat literaaleja, taas toteutuu täsmälleen siinä tapauksessa, että se ei sisällä minkään konjunktina olevan propositiosymbolin negaatiota. Tämä syntaktinen kriteerio voidaan tarkistaa helposti polynomiajassa.

Eräs tapa ratkaista SAT on tietysti muuttaa lause A ensin ekvivalentiksi disjunktiivisessa normaalimuodossa olevaksi lauseeksi, ja tarkistaa sitten, löytyykö mistään disjunktista sekä propositiosymbolia, että sen negaatiota. Tällä ratkaisulla ei kuitenkaan miljoonia vielä tienata, sillä lauseen muuttamista disjunktiiviseen normaalimuotoon ei yleisesti voida tehdä alle eksponentiaalisessa ajassa.

B Rakenteellinen induktio ja rekursio

Tässä kappaleessa tutustumme tarkemmin *rakenteelliseen induktioon*, johon törmää jatkuvasti matemaattisessa logiikassa. Rakenteellisella induktiolla ja rekursiolla on sovelluksia myös teoreettisessa tietojenkäsittelytieteessä sekä diskreetissä matematiikassa.

B.1 Induktio

Olkoon X joukko, ja $\mathcal{F}$ joukko funktioita, joista jokaisen maalijoukko on X, ja lähtöjoukko X^n jollakin $n > 0$. Tällöin sanotaan, että $\mathcal{F}$ on **joukon X funktioperhe**.

B.1 Määritelmä. Olkoon X joukko ja $\mathcal{F}$ joukon X funktioperhe. Joukon $A \subset X$ **$\mathcal{F}$-kuva** $\mathcal{F}A$ on joukko

$$A \cup \bigcup_{f \in \mathcal{F}} \left\{ f(a) \colon a \in A^{\#f} \right\},$$

missä $\#f$ tarkoittaa funktion f paikkalukua, eli $\#f = n \iff f \colon X^n \to X$. Joukon A **$\mathcal{F}$-sulkeuma** $\mathrm{cl}_{\mathcal{F}}(A)$ on joukko

$$\bigcup_{n \in \mathbb{N}} A_n,$$

missä $A_0 = A$ ja $A_{n+1} = \mathcal{F}A_n$.

Joukon A $\mathcal{F}$-sulkeuma on siis pienin joukon X osajoukko, joka sisältää joukon A, ja on suljettu kaikkien joukon $\mathcal{F}$ funktioiden suhteen. $\mathcal{F}$-sulkeuman käsite on hyvin luonnollinen. Muutama esimerkki:

B.2 Esimerkki. Olkoon $X = \mathbb{R}$, $S \colon \mathbb{R} \to \mathbb{R}$, $S(x) = x + 1$, ja $\mathcal{F} = \{S\}$. Tällöin joukon $\{0\}$ $\mathcal{F}$-sulkeuma on

$$\{0\} \cup \{0, 1\} \cup \{0, 1, 2\} \cup \ldots = \mathbb{N}.$$

B.3 Esimerkki. Olkoon G ryhmä. Olkoon $f \colon G^2 \to G$, $f(x, y) = x \cdot y$, $g \colon G \to G$, $g(x) = x^{-1}$ ja $\mathcal{F} = \{f, g\}$. Tällöin minkä tahansa osajoukon $\mathcal{F}$-sulkeuma on täsmälleen kyseisen joukon virittämä aliryhmä.

B.4 Esimerkki. Olkoon V reaalikertoiminen vektoriavaruus. Olkoon $f \colon V^2 \to V$ vektoreiden yhteenlasku ja olkoon jokaisella $a \in \mathbb{R}$ $g_a \colon \mathbb{R} \to \mathbb{R}$ skalaarikertolasku alkiolla a, eli $g_a(x) = ax$. Olkoon nyt $\mathcal{F} = \{f\} \cup \{g_a \colon a \in \mathbb{R}\}$. Tällöin minkä tahansa osajoukon $\mathcal{F}$-sulkeuma on kyseisen joukon virittämä aliavaruus.

B.5 Esimerkki. Olkoon M kaikkien symboleista $), (, \neg, \wedge, \vee, \to, \leftrightarrow$ sekä propositiosymboleista muodostettavien äärellisten merkkijonojen joukko. Määritellään seuraavat funktiot:

$$\begin{array}{ll}
f_\neg \colon M \to M & f_\neg(A) = \neg A \\
f_\wedge \colon M^2 \to M & f_\wedge(A, B) = (A \wedge B) \\
f_\vee \colon M^2 \to M & f_\vee(A, B) = (A \vee B) \\
f_\to \colon M^2 \to M & f_\to(A, B) = (A \to B) \\
f_\leftrightarrow \colon M^2 \to M & f_\leftrightarrow(A, B) = (A \leftrightarrow B)
\end{array}$$

Olkoon $\mathcal{F} = \{f_\neg, f_\wedge, f_\vee, f_\to, f_\leftrightarrow\}$ ja $P \subset M$ kaikkien propositiosymboleiden joukko. Tällöin joukon P $\mathcal{F}$-sulkeuma on kaikkien propositiolauseiden joukko.

Rakenteellinen induktio. *Olkoon X joukko, $\mathcal{F}$ sen funktioperhe ja $A \subset X$. Oletetaan, että $Y \subset \mathrm{cl}_{\mathcal{F}}(A)$ on sellainen, että $A \subset Y$ ja jokaisella $f \in \mathcal{F}$, $\#f = n$, jos $a_1, \ldots, a_n \in Y$, niin $f(a_1, \ldots, a_n) \in Y$. Tällöin $Y = \mathrm{cl}_{\mathcal{F}}(A)$.*

Todistus. Riittää näyttää, että $\mathrm{cl}_{\mathcal{F}}(A) \subset Y$. $\mathcal{F}$-sulkeuman määritelmän nojalla

$$\mathrm{cl}_{\mathcal{F}}(A) = \bigcup_{n \in \mathbb{N}} A_n,$$

missä $A_0 = A$ ja $A_{n+1} = \mathcal{F}A_n$. Näytetään induktiolla, että $A_n \subset Y$ jokaisella $n \in \mathbb{N}$.

Oletuksen nojalla $A_0 \subset Y$, joten alkuaskel on selvä. Oletetaan sitten, että $A_n \subset Y$. Olkoon $a \in A_{n+1} = \mathcal{F}A_n$. Tällöin siis löytyy funktio $f \in \mathcal{F}$, $\#f = m$ ja alkiot $a_1, \ldots, a_m \in A_n$, joilla $a = f(a_1, \ldots, a_m)$. Induktio-oletuksen nojalla $A_n \subset Y$, joten oletuksen nojalla $a \in Y$. Siis $A_{n+1} \subset Y$.

Induktioperiaatteen nojalla $A_n \subset Y$ jokaisella $n \in \mathbb{N}$, joten $\mathrm{cl}_{\mathcal{F}}(A) \subset Y$. □

B.6 Esimerkki. Olkoon G ryhmä, $f\colon G^2 \to G$ ryhmän laskutoimitus, $g\colon G \to G$, $g(x) = x^{-1}$ ja $\mathcal{F} = \{f, g\}$. Olkoon $A \subset G$ sellainen osajoukko, että jokaisella $a \in A$ ja $x \in G$ pätee $ax = xa$. Tällöin joukon A virittämä aliryhmä on vaihdannainen.

Todistus. Koska joukon A virittämä aliryhmä on $\mathrm{cl}_{\mathcal{F}}(A)$, voimme käyttää rakenteellista induktiota. Olkoon $X = \{x \in \mathrm{cl}_{\mathcal{F}}(A)\colon ax = xa \text{ jokaisella } a \in \mathrm{cl}_{\mathcal{F}}(A)\}$. Oletuksen nojalla $A \subset X$.

Olkoon $x \in X$ ja $a \in \mathrm{cl}_{\mathcal{F}}(A)$. Koska $ax = xa$, niin kertomalla alkiolla x^{-1} saadaan $x^{-1}a = ax^{-1}$, eli $ag(x) = g(x)a$, joten $g(x) \in X$.

Olkoon sitten $x, y \in X$ ja $a \in \mathrm{cl}_{\mathcal{F}}(A)$. Koska $ay = ya$, niin $xay = xya$, ja koska $xa = ax$, niin $axy = xya$, eli $af(x,y) = f(x,y)a$, joten $f(x,y) \in X$.

Siis rakenteellisen induktion nojalla $X = \mathrm{cl}_{\mathcal{F}}(A)$, eli kaikki joukon X alkiot kommutoivat keskenään. □

B.2 Rekursio

Induktio ja rekursio kulkevat aina käsikkäin. Siinä missä induktio on tapa todistaa asioita, rekursio on tapa määritellä asioita. Myös luonnollisten lukujen rekursiiviset määritelmät yleistyvät rakenteellisiksi.

Esimerkiksi propositiologiikan lauseiden totuus määritellään rekursiivisesti: lauseen $(p_0 \to \neg p_1)$ totuusarvo jollakin totuusjakaumalla riippuu lauseiden p_0 ja $\neg p_1$ totuusarvoista samalla jakaumalla, ja lauseen $\neg p_1$ totuusarvo riippuu lauseen p_1 totuusarvosta.

Tutkitaan seuraavaa tilannetta: X on joukko, ja $\mathcal{F}$ sen funktioperhe. Olkoon $A \subset X$ ja oletetaan että $\mathrm{cl}_{\mathcal{F}}(A) = X$. Olkoon Y jokin joukko. Haluamme määritellä funktion $f\colon X \to Y$ rekursiivisesti, eli tiedämme, mitä funktion arvojen tulee olla joukon A alkioilla, ja että miten joukon $\mathcal{F}$ funktioiden soveltaminen vaikuttaa näihin arvoihin.

B.7 Esimerkki. Määritellään funktio $f\colon \mathbb{N} \to \mathbb{N}$ seuraavasti:

1. $f(0) = 1$
2. $f(n+1) = 2 \cdot f(n)$

Sama hieman monimutkaisemmin ilmaistuna: Olkoon $X = \mathbb{N}$, $\mathcal{F} = \{S\}$, missä $S(n) = n+1$, ja $A = \{0\}$.

1. $f(a) = 1$ jokaisella $a \in A$
2. Mikäli $f(n) = y$, niin $f(S(n)) = 2y$

Näin saatu funktio f on tietysti funktio $f(n) = 2^n$.

B.8 Esimerkki. Olkoot M, $\mathcal{F}$ ja P kuten esimerkissä B.5. Olkoon $v\colon \mathbb{N} \to \{0,1\}$ mielivaltainen funktio. Määritellään funktio $t\colon \mathrm{cl}_{\mathcal{F}}(P) \to \{0,1\}$ rekursiivisesti:

1. $t(p_i) = v(i)$ jokaisella $p_i \in P$
2. $t(f_\neg(A)) = 1 - t(A)$
3. $t(f_\wedge(A,B)) = 1$ jos $t(A) = t(B) = 1$, muulloin $t(f_\wedge(A,B)) = 0$
4. $t(f_\vee(A,B)) = 0$ jos $t(A) = t(B) = 0$, muulloin $t(f_\vee(A,B)) = 1$
5. $t(f_\to(A,B)) = 0$ jos $t(A) = 1$ ja $t(B) = 0$, muulloin $t(f_\to(A,B)) = 1$
6. $t(f_\leftrightarrow(A,B)) = 1$ jos $t(A) = t(B)$, muulloin $t(f_\leftrightarrow(A,B)) = 0$

Näin määritellyn funktion arvo $t(A)$ on tietysti lauseen A totuusarvo jakaumalla v, jota olemme tottuneet merkkaamaan $v[A]$, tämä uusi määritelmä on vain hieman formaalimpi.

Määritellään toinenkin funktio $r\colon \mathrm{cl}_{\mathcal{F}}(P) \to \mathbb{N}$ rekursiivisesti:

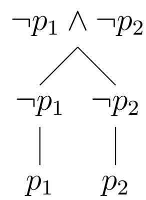
1. $r(A) = 0$ jokaisella $A \in P$.
2. $r(f_\neg(A)) = 1 + r(A)$
3. $r(f_\wedge(A,B)) = r(f_\vee(A,B)) = r(f_\to(A,B)) = r(f_\leftrightarrow(A,B)) = 1 + \max(r(A), r(B))$

Funktion r arvo yksittäisillä symboleilla on siis nolla ja aina kun sovelletaan jotakin konnektiivia, funktion r arvo kasvaa yhdellä. $r(A)$ on siis suurin lauseessa A olevien sisäkkäisten konnektiivien lukumäärä, eli lauseen A jäsennyspuun korkeus.

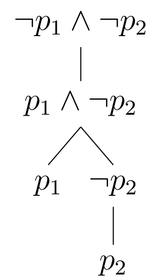
Rekursiivisissa määritelmissä on oleellista, että joko jäsennyspuut ovat yksikäsitteisiä, tai että eri jäsennykset antavat määriteltävälle funktiolle saman arvon. Varoittava esimerkki seuraa. Olkoon X kaikkien symboleista $\neg$ ja $\wedge$ sekä propositiosymboleista $p_i\colon i \in \mathbb{N}$ koostuvien merkkijonojen joukko. Määritellään *porpositiolauseiden* joukko A seuraavasti:

1. propositiosymbolit p_i ovat porpositiolauseita
2. mikäli A on porpositiolause, niin $\neg A$ on porpositiolause
3. mikäli A ja B ovat porpositiolauseita, niin $A \wedge B$ on porpositiolause

Porpositiolauseita ovat esimerkiksi $p_0, p_6, p_0 \wedge p_{12}$, sekä $\neg\neg p_0 \wedge \neg p_6 \wedge p_0$. Nyt jäsennyspuut eivät kuitenkaan ole yksikäsitteisiä. On esimerkiksi epäselvää, onko porpositiolauseen $\neg p_1 \wedge \neg p_2$ alussa oleva negaatio symbolin p_1 edessä, vai porpositiolauseen $p_1 \wedge \neg p_2$ edessä. Lauseen voi siis jäsentää ainakin kahdella eri tavalla:



tai



Yritetään esimerkiksi määritellä esimerkin B.8 kaltainen funktio r, joka kertoo kunkin lauseen suurimman *sisäkkäisten* konnektiivien määrän:

1. $r(A) = 0$ jos $A = p_i$ jollakin $i \in \mathbb{N}$
2. $r(\neg A) = 1 + r(A)$
3. $r(A \wedge B) = 1 + \max(r(A), r(B))$

Määritelmä ei kuitenkaan toimi: Porpositiolauseen $\neg p_1 \wedge \neg p_2$ vasemmanpuoleisen jäsennyspuun mukaan arvon $r(\neg p_1 \wedge \neg p_2)$ tulisi olla 2, sillä $r(\neg p_1) = r(\neg p_2) = 1$, eli $\max(r(\neg p_1), r(\neg p_2)) = 1$. Oikeanpuoleisen jäsennyspuun tulos on kuitenkin ristiriidassa tämän kanssa. Koska $r(\neg p_2) = 1$, $r(p_1 \wedge \neg p_2) = 2$, joten arvon $r(\neg p_1 \wedge \neg p_2)$ tulisi olla 3. Siis määritelmä ei anna porpositiolauseelle $\neg p_1 \wedge \neg p_2$ yksikäsitteistä arvoa funktiossa r.

Tämä ongelma poistuu, jos rakennepuut ovat yksikäsitteisiä, kuten esimerkiksi propositiolauseiden määritelmässä. Vaikka rakennepuut eivät olisi yksikäsitteisiä, joissain tapauksissa rekursiivinen määritelmä saattaa silti toimia. Jos nimittäin voidaan todistaa, että määritelmä antaa funktiolle saman arvon riippumatta siitä, mitä jäsennyspuuta käytetään, määritelmä toimii. Esimerkkinä: määritellään funktio k porpositiolauseiden joukosta luonnollisten lukujen joukkoon, niin että $k(A)$ on kaikkien lauseessa A olevien konnektiivien määrä. Siis:

1. $r(A) = 0$ aina kun $A = p_i$ jollakin i
2. $r(\neg A) = 1 + r(A)$
3. $r(A \wedge B) = 1 + r(A) + r(B)$ (lauseessa $A \wedge B$ on siis kaikki lauseen A konnektiivit, kaikki lauseen B konnektiivit sekä näiden lisäksi yksi uusi konnektiivi $\wedge$.)

Tällöin minkä tahansa porpositiolauseen kaikki eri jäsennyspuut antavat funktiolle k saman arvon.

Viitteet

[JohLog] Hannele Salminen, Jouko Väänänen. Johdatus logiikkaan. Gaudeamus Helsinki University Press 1992.