Logiikka

Lyhyt kurssi

Tero Harju
Matematiikan laitos
Turun yliopisto
2007–2009

Sisältö

Kirjallisuutta

[1] S.N. Burris: *Logic for Mathematics and Computer Science*. Prentice-Hall, Upper Saddle River, NJ 1998.

[2] D. van Dalen: *Logic and Structure* (3. ed). Springer, Berlin 1994.

[3] H.D. Ebbinghaus, J. Flum & W. Thomas: *Mathematical Logic* (2. ed). Springer, Berlin 1994.

[4] H.B. Enderton: *Mathematical Introduction to Logic* (2. ed). Academic Press 2001.

[5] A. Nerode & R.A. Shore: *Logic for Applications*. Springer, New York 1993.

[6] H. Salminen & J. Väänänen: *Johdatus Logiikkaan*. Gaudeamus, Helsinki 1997.

[7] U. Schöning: *Logic for Computer Scientists*. Birkhäuser, Boston-Basel-Berlin 1989.

[8] R. Smullyan: *Forever Undecidable: a puzzle book to Gödel*. Oxford University Press, Oxford 1987.

[9] R. Smullyan: *First-Order Logic*. Dover 1995.

[10] M. Steinby: *Logiikka*. Turun yliopisto 2004.

Johdantoa

Logiikka on formaalinen teoria, jonka ensisijainen tehtävä on tutkia päättelyn oikeellisuutta. Näiden luentojen aiheena logiikka on symbolinen teoria, joka esitetään *formaalisena kielenä*, eli siinä esiintyvien osien rakenne ja merkitys ovat täsmällisesti määritellyt. Formaalisessa logiikassa päätelmät pyritään esittämään yksiselitteisen täsmällisesti. Näin ei ole yleensä laita arkisissa pohdinnoissa, joissa päätelmien teko on usein tulkinnanvaraista – esimerkiksi silloin kun johtopäätös tehdään vetoamalla samankaltaisuuteen, todennäköisyyteen tai vaillinaisesti tunnettuun tietoon.

Logiikka on laaja-alainen teoria kattaen monia erilaisia aiheita. Tässä kurssissa keskitytään erityisesti *propositio*- eli lauselogiikkaan ja johdatellaan myös vahvempaan logiikkaan eli *ensimmäisen kertaluvun logiikkaan*. Nämä kaksi logiikan lajia ovat luonnollisimmat, ja samalla tärkeimmät alat, joille lähes kaikki muut logiikat rakentuvat.

Jokainen looginen systeemi rakentuu kolmesta osa-alueesta:

1. Syntaksi määrittelee formaalisen kielen hyvinmuodostetut ilmaisut eli kaavat. Nämä muodostavat teorian *objektikielen*. Objektikielen tarkastelussa käytettyä kieltä kutsutaan *metakieleksi*, joka on yleensä matemaattisilla käsitteillä rikastettu luonnollinen kieli. On välttämätöntä erottaa toisistaan objektikieli ja metakieli samaan tapaan kuin vieraita kieliä opiskeltaessa on erotettava opittava kieli ja kieli, jolla opetetaan.

2. Semantiikka eli **malliteoria** antaa teorian kaavoille merkitykset tulkitsemalla niissä esiintyvät symbolit. Esimerkiksi propositiologiikassa tulkinta määrää kaavalle *totuusarvon*: *tosi* ja *epätosi*.

3. Todistusteoria on järjestelmä, jonka avulla kyseisen logiikan semanttisesti todet kaavat voidaan todistaa formaalisesti. Tällainen järjestelmä voi olla esimerkiksi *aksiomatisointi*, joka koostuu tietyistä *aksioomeista* ja *päättelysäännöistä*.

Merkintöjä

Nämä ovat logiikan metakielen merkintöjä.

joss on lyhenne ilmaisusta: “jos ja vain jos”

$\iff$ tarkoittaa samaa kuin “joss”

$\{0,1\}^n = \{(b_1, b_2, \ldots, b_n) \mid b_i \in \{0,1\}\}$

$\mapsto$ esittää alkion kuvautumista. (Esim. $x \mapsto x^2$)

$|A|$ on joukon A alkioiden lukumäärä

A. Propositiologiikka

1 Propositiologiikan syntaksi

Propositiologiikan perusalkiot ovat propositiot, jotka esittävät väitelauseita. Nämä ovat rakenteellisesti hyvinmuodostettuja lauseita, jotka ovat joko tosia tai epätosia. Esimerkiksi lause "Helsinki on Suomen pääkaupunki" on propositio ja samoin on "Kaikille luonnollisille luvuille n on voimassa $n > \sqrt{5}$". Edellinen on tosi, jälkimmäinen epätosi. Sensijaan, esimerkiksi lause "Tulehan tänne!" ei ole propositio, sillä käskylauseena se ei ole tosi eikä epätosi.

Edeltävät propositiot ovat *atomaarisia* sikäli, että niitä ei voi jakaa yksinkertaisempiin propositioihin. *Yhdistettyjä*, eli molekulaarisia, propositioita saadaan yhdistämällä muita propositioita *konnektiivien* avulla. Esimerkiksi "Murre on kissa ja Turku on kaupunki" on yhdistetty propositio, jossa kahta atomaarista propositiota yhdistää konnektiivi 'ja'. Formaalisessa logiikassa väitelauseet esitetään lyhykäisesti symbolein, joita konnektiivit yhdistävät.

Jokainen konnektiivi joko muuntaa proposition (kuten kielto) tai yhdistää kaksi tai useampia propositioita uudeksi propositioksi. Mahdollisia konnektiiveja on toki ääretön määrä, mutta jäljempänä otetaan käyttöön vain muutama sellainen. Osoittautuu, että semanttisesti – propositiologiikan rajoissa – kaikki mahdolliset konnektiivit voidaan lausua näiden tavallisimpien konnektiivien avulla.

Hyvin muodostetut ilmaisut

Määritellään ensin propositiologiikan syntaksi eli *hyvin muodostetut kaavat* merkkijonojen eli ilmaisujen avulla. Näiden tulkinta eli semantiikka määritellään sitten seuraavassa pykälässä.

Logiikan aakkosto koostuu peruskonnektiiveista, erityismerkeistä ja propositiokirjaimista.

- **Peruskonnektiivit** ovat

$$\neg \quad \text{negaatio}, \qquad \wedge \quad \text{konjunktio}, \qquad \vee \quad \text{disjunktio}.$$

Myöhemmin osoitetaan, että nämä konnektiivit ovat (semanttisesti) täydellisiä, eli kaikki muut konnektiivit voidaan ottaa käyttöön lyhennysmerkintöinä lausumalla ne konnektiivien $\neg$, $\wedge$, ja $\vee$ avulla. Nämä konnektiivit lausutaan myös 'ei', 'ja', 'tai' johtuen niiden semanttisesta määrittelystä.

- Logiikan aakkostoon kuuluvat myös sulkeet (ja).
- Kiinnitetään numeroituvasti ääretön joukko **propositiokirjaimia** eli **propositiomuuttujia**:

$$\mathrm{PM} = \{\, p_0, p_1, p_2, \ldots \}.$$

<u>**Määr**</u>**. 1. Propositioiden** eli **(hyvin muodostettujen) kaavojen** joukko Prop on pienin ilmaisujen joukko, joka toteuttaa seuraavat ehdot:

(1) Jokainen propositiomuuttuja $p_i \in \mathrm{PM}$ on propositio;

(2) jos P ja Q ovat propositioita, samoin ovat $(\neg P)$, $(P \vee Q)$ ja $(P \wedge Q)$.

Propositio on **yhdistetty**, jos se ei ole propositiomuuttuja.

Esim. 1. Esimerkiksi ilmaisu $((p_3 \vee p_1) \wedge (\neg p_3))$ on propositio, sillä se on saatu propositioista p_1 ja p_3 käyttäen kolmasti ehtoa (2). Toisaalta ilmaisu $(p_1 \vee p_2 \wedge p_3)$ ei ole propositio, sillä siitä puuttuu yksi sulkupari, ja on mahdotonta sanoa mistä se puuttuu. □

Metakielessä, jolla logiikan kaavoista ja tuloksista puhutaan, propositioita merkitään isoin kirjaimin $P, Q, R, \ldots$ kun taas pienet kirjaimet $p, q, r, \ldots$ edustavat propositiomuuttujia. Propositioiden joukkoja merkitään yleensä isoilla kreikkalaisilla kirjaimilla Γ, $\Delta, \ldots$

Sopimus. Ilmaisuja voidaan yksinkertaistaa jättämällä pois kaavojen uloimmat sulkeet ja mahdollisesti myös muita sulkupareja olettaen, että $\neg$ sitoo voimakkaammin kuin $\vee$ ja $\wedge$. Täten voidaan esimerkiksi propositio $((\neg p) \wedge (q \vee r))$ kirjoittaa lyhyemmin muodossa $\neg p \wedge (q \vee r)$. Huomaa, että propositiossa $\neg((p \wedge q) \vee p)$ ei ole ylimääräisiä sulkeita.

Luettavuuden takia on usein parempi jättää 'turhia' sulkeita selventämään proposition rakennetta.

Rakennepuut

Kullakin propositiolla $P \in \mathrm{Prop}$ on yksikäsitteinen rakenne, jonka propositiomuuttujat ja käytettyjen konnektiivien järjestys määräävät. Tämä rakenne voidaan ilmaista **rakennepuuna**, jonka alkiot, eli **solmut**, leimataan propositioilla. Rakennepuuta piirrettäessä solmut usein samaistetaan leimojensa kanssa, jolloin kahdella eri solmulla voi olla sama leima. Solmu yhdistetään viivalla **jälkeläisiinsä** seuraavasti: Rakennepuun **juuri** on annettu propositio P, joka ei ole minkään solmun jälkeläinen, ja

- jos puussa on solmu $\neg Q$, on sillä jälkeläinen Q,
- jos puussa on solmu $Q \wedge R$, on sillä jälkeläiset Q ja R,
- jos puussa on solmu $Q \vee R$, on sillä jälkeläiset Q ja R.

Propositiomuuttujilla $p \in \mathrm{PM}$ ei ole jälkeläisiä.

Esim. 2. Proposition $P = ((p \wedge \neg q) \vee \neg p) \wedge \neg(p \vee q)$ rakennepuu on esitetty kuvassa 1. Huomaa että

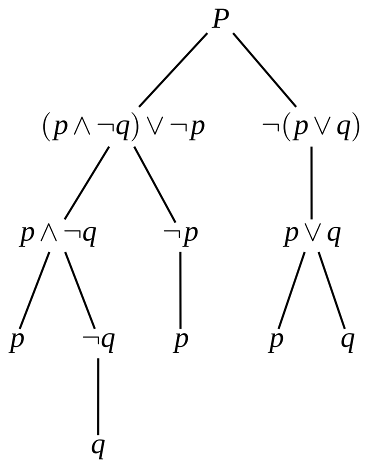
- polkujen alimmat solmut ovat propositiomuuttujia;
- millään (jälkeläis)polulla ei esiinny samaa propositiota kahdesti, vaan jos R on proposition Q jälkeläinen (useammassa polvessa), on R yksinkertaisempi kuin Q: siinä esiintyy vähemmän konnektiiveja.

□

Propositioiden määritelmä on *induktiivinen*: ensin määrätään lähtöjoukko (propositiokirjaimet) ja sitten esitetään miten muut propositiot muodostetaan jo annetuista propositioista. Niinpä propositioita koskevat väitteet voidaan usein todistaa rakenteellisella induktiolla.

Rakenteellinen induktio. Olkoon Ω jokin propositioita koskeva ominaisuus. Kaikilla propositiolla on ominaisuus Ω, jos seuraavat ehdot ovat voimassa:

1. Kaikilla propositiomuuttujilla on ominaisuus Ω.
2. Jos propositioilla P ja Q on ominaisuus Ω, niin myös propositioilla $\neg P$, $P \vee Q$ ja $P \wedge Q$ on ominaisuus Ω.



Kuva 1: Proposition $P = ((p \wedge \neg q) \vee \neg p) \wedge \neg(p \vee q)$ rakennepuu.

Todistus. Olkoon Γ niiden propositioiden joukko, joilla on ominaisuus Ω. Oletuksista seuraa, että joukko Γ toteuttaa määritelmän 1 ehdot (1) ja (2). Koska Prop on pienin nämä ehdot toteuttava osajoukko, seuraa tästä Prop $\subseteq \Gamma$. □

Olkoon Ω jokin propositioita koskeva ominaisuus. Merkitään $\Omega(P)$, jos propositiolla P on tämä ominaisuus.

Esim. 3. Olkoon Ω seuraava ominaisuus: $\Omega(P)$, jos propositiossa P esiintyvien konnektiivien lukumäärä on vähintään siinä esiintyvien propositiomuuttujien lukumäärä miinus 1. Tätä varten olkoot $k(P)$ ja $m(P)$ propositiossa esiintyvien konnektiivien ja muuttujien lukumäärät, vastaavasti.

Väite: $k(P) \geq m(P) - 1$.

Lähtökohta: Jos $P = p \in$ PM, niin $k(P) = m(P)$. Siis $\Omega(P)$ tässä tapauksessa.

Induktio-oletus: Oletetaan, että väite on voimassa propositioille Q ja R, eli $k(Q) \geq m(Q) - 1$ ja $k(R) \geq m(R) - 1$.

Induktioaskel:

(1) Jos $P = \neg Q$, niin $k(P) = k(Q) + 1 \geq m(Q) = m(P) \geq m(P) - 1$, ja siten $\Omega(P)$.

(2) Jos $P = Q \wedge R$, niin $k(P) = k(Q) + k(R) + 1 \geq m(Q) - 1 + m(R) - 1 + 1 = m(Q) + m(R) - 1 = m(P) - 1$, ja siten $\Omega(P)$.

(3) Sama päättely on voimassa propositiolle $P = Q \vee R$, ja siten $\Omega(P)$.

Täten $\Omega(P)$ on voimassa kaikille P. □

Propositioiden määritelmän induktiivisesta luonteesta seuraa myös, että niihin liittyvät käsitteet määritellään usein *rekursiivisesti*: määritellään ensin käsite propositiomuuttujille ja laajennetaan se sitten kaikille propositioille konnektiivien avulla: $\neg P$, $P \wedge Q$ ja $P \vee Q$.

Esim. 4. Proposition P **osakaavojen** joukko $\mathrm{sub}(P)$ on pienin propositiojoukko, joka toteuttaa seuraavat ehdot:

(1) jos $P = p$ on propositiomuuttuja, niin $\mathrm{sub}(P) = \{p\}$;
(2) jos $P = Q \vee R$ tai $P = Q \wedge R$, niin $\mathrm{sub}(P) = \mathrm{sub}(Q) \cup \mathrm{sub}(R) \cup \{P\}$;
(3) jos $P = \neg Q$, niin $\mathrm{sub}(P) = \mathrm{sub}(Q) \cup \{P\}$.

Todetaan vielä, että $\mathrm{sub}(P)$ koostuu tarkalleen rakennepuunsa solmujen leimoista. □

2 Propositiologiikan semantiikkaa

Propositiologiikan semantiikka perustuu totuusarvotuksille eli tulkinnoille, jotka kuvaavat mahdollisia tilanteita. Tällöin jokainen propositio saa **totuusarvon**, **tosi** tai **epätosi**, joita formalismissa merkitään symbolein 1 ja 0. Propositioiden totuusarvot määrätään antamalla ensin tulkinta propositiomuuttujille ja sitten käyttämällä konnektiivien totuustauluja yleisemmille propositioille. Näin ollen jokaisen proposition totuusarvo määräytyy yksikäsitteisesti propositiomuuttujien totuusarvoista. (*Ei-klassillisia* logiikkoja tunnetaan monenlaisia, ja jotkut niistä sallivat useampia totuusarvoja, jotka viittaavat esimerkiksi mahdollisuuteen, todennäköisyyteen tai epävarmuuteen.) Formaalisen logiikassa konnektiivien tulkinnat ovat täysin yksikäsitteiset, päinvastoin kuin luonnollisessa kielessä, jossa konnektiivien ‘ei’, ’ja’, ’tai’ merkitykset vaihtelevat eri yhteyksissä.

Totuustaulut ja tulkinnat

Proposition P totuusarvo määräytyy konnektiivien tulkinnoista ja siinä esiintyvien propositiomuuttujien totuusarvoista. Jokainen tulkinta luo ‘mahdollisen maailman’, missä asiantila P on voimassa jos ja vain jos tulkinta antaa sille totuusarvon 1. Yhdistettyjen propositioiden totuusarvot riippuvat yksikäsitteisesti propositiomuuttujien totuusarvoista.

Määr. 2. Jokainen kuvaus $v\colon \mathrm{PM} \to \{0,1\}$ on **tulkinta** eli **totuusarvotus**.

Kun totuusarvot 0 ja 1 tulkitaan luonnollisina lukuina, voidaan konnektiivien tulkinnat esittää seuraavan lauseen mukaisesti, missä rakennepuu määrää proposition totuusarvon kun propositiomuuttujat on ensin tulkittu.

Lause 1. *Jokainen tulkinta $v\colon \mathrm{PM} \to \{0,1\}$ voidaan laajentaa yksikäsitteisellä tavalla kuvaukseksi $v\colon \mathrm{Prop} \to \{0,1\}$: kun $P,Q \in \mathrm{Prop}$, niin*

(1) $v(\neg P) = 1 - v(P)$,

(2) $v(P \vee Q) = \max(v(P), v(Q))$,

(3) $v(P \wedge Q) = \min(v(P), v(Q))$.

Todistus. Rakenteellinen induktio osoittaa, että $v\colon \mathrm{PM} \to \{0,1\}$ ja ehdot (1)–(3) määräävät yksikäsitteisen arvon $v(P)$ jokaiselle propositiolle P, koska lähtökohdat $v(p)$ on määrätty jokaiselle $p \in \mathrm{PM}$. □

On selvää, että arvo $v(P)$ riippuu vain tulkinnan v rajoittumasta niille propositiomuuttujille, jotka esiintyvät propositiossa P. Näitä propositiomuuttujia on toki vain äärellinen määrä.

Lause 1 voidaan ilmaista myös **totuustaulujen** avulla, missä jokainen vaakarivi vastaa sellaista tulkintaa, jolla $v(P)$ ja $v(Q)$ saavat kyseiset arvot.

P	$\neg P$
0	1
1	0

P	Q	$P \wedge Q$	$P \vee Q$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

Esim. 5. Jos $v(P)=0$ ja $v(Q)=1$, niin $v(P\wedge Q)=0$. *Huomaa kuitenkin, että tässä $P,Q\in$ Prop voivat olla yhdistettyjä propositioita*, eli ne eivät välttämättä ole pelkkiä propositiomuuttujia. Niinpä, jos esimerkiksi $P=p\vee\neg p$, niin aina $v(P)=1$ olipa tulkinta v mikä tahansa, ja näin ollen ylläolevassa totuustaulussa tapauksessa $P\wedge Q$ kaksi ensimmäistä riviä eivät koskaan tule käyttöön tälle propositiolle. □

Seuraavassa määritellään uusia konnektiiveja alkuperäisten konnektiivien avulla määriteltyinä lyhennysmerkintöinä niin, että uudet konnektiivit saavat luonnolliset tulkintansa.

Määr. 3. Konnektiivit $\rightarrow$ (**implikaatio**) ja $\leftrightarrow$ (**ekvivalenssi**), määritellään lyhennysmerkintöinä seuraavasti:

$$P\rightarrow Q=\neg P\vee Q\,,\qquad P\leftrightarrow Q=(P\wedge Q)\vee(\neg P\wedge\neg Q)\,.$$

Lisäksi määritellään **totuusvakiot**: **falsum** ja **verum** oheisesti:

$$\bot=p_0\wedge\neg p_0\quad\text{ja}\quad\top=p_0\vee\neg p_0\,.$$

Siis olipa $v\colon$ PM $\rightarrow\{0,1\}$ mikä tulkinta tahansa, on $v(\bot)=0$ ja $v(\top)=1$. Uusia 2-paikkaisia konnektiiveja vastaavat totuustaulut ovat

P	Q	$P\rightarrow Q$	$P\leftrightarrow Q$
0	0	1	1
0	1	1	0
1	0	0	0
1	1	1	1

Sopimus. Edellä sovittuja sulkumerkkisääntöjä sovelletaan myös yleistettyihin propositioihin, joissa esiintyy näitä lyhennysmerkintöjä. Tällöin konnektiivit $\vee$ ja $\wedge$ sitovat voimakkaammin kuin konnektiivit $\rightarrow$ ja $\leftrightarrow$. Sulkeiden poistamisessa kannattaa olla jälleen varovainen proposition luettavuuden vuoksi. Ilmaisu $P\wedge Q\rightarrow R\vee P$ on hyvin muodostettu propositio tämän sopimuksen mukaan, mutta sen täydellisempi muoto $(P\wedge Q)\rightarrow(R\vee P)$ on selkeämpi.

Tavallisimmat logiikassa käytetyt konnektiivit ovat siis

konnektiivi			lue myös
negaatio	$\neg$	$\neg P$	"ei P"
konjunktio	$\wedge$	$P\wedge Q$	"P ja Q"
disjunktio	$\vee$	$P\vee Q$	"P tai Q"
implikaatio	$\rightarrow$	$P\rightarrow Q$	"jos P niin Q"
ekvivalenssi	$\leftrightarrow$	$P\leftrightarrow Q$	"P jos ja vain jos Q"

Esim. 6. Propositiolle $(p\vee q)\rightarrow\neg q$ saadaan oheinen totuustaulu:

p	q	$p\vee q$	$\neg q$	$(p\vee q)\rightarrow\neg q$
0	0	0	1	1
0	1	1	0	0
1	0	1	1	1
1	1	1	0	0

Huomaa, että proposition $(p\vee q)\rightarrow\neg q$ totuustaulu on sama kuin proposition $\neg q$, kun tätä tarkastellaan muuttujien p ja q propositiona. □

Looginen ekvivalenssi

Määr. 4. Sanotaan, että propositio P on **tosi tulkinnassa** v, jos $v(P) = 1$. Tällöin v on proposition P **malli**. Tulkinta v on propositiojoukon Γ **malli**, jos $v(P) = 1$ aina, kun $P \in \Gamma$.

Lisäksi propositio P on

- **tautologia**, merkitään $\models P$, jos se on tosi kaikissa tulkinnoissa;
- **toteutuva**, jos sillä on malli;
- **kumoutuva**, jos se on epätosi jossakin tulkinnassa;
- **toteutumaton**, jos sillä ei ole mallia.

Lisäksi sanotaan, että propositiojoukko $\Gamma \subseteq \mathrm{Prop}$ on **toteutuva**, jos sillä on malli.

Määr. 5. Propositiot P ja Q ovat (semanttisesti eli) **loogisesti ekvivalentit**, $P \equiv Q$, jos niillä on samat mallit:

$$P \equiv Q \iff v(P) = v(Q) \text{ kaikilla } v\colon \mathrm{PM} \to \{0,1\}\,.$$

Esim. 7. Seuraavasta totuustaulusta nähdään, että $P \vee Q \equiv \neg P \to Q$ kaikille propositioille P ja Q. Huomaa, että tämä on riippumatonta millaisia propositioita P ja Q ovat, eli ne voivat olla yhdistettyjä propositioita.

P	Q	$P \vee Q$	$\neg P$	$\neg P \to Q$
0	0	0	1	0
0	1	1	1	1
1	0	1	0	1
1	1	1	0	1

Siis disjunktio voidaan lausua (semanttisesti) negaation ja implikaation avulla. □

Jokainen kuvaus v voidaan luonnollisella tavalla laajentaa koskemaan propositioita, joissa esiintyy konnektiiveja $\to$, $\leftrightarrow$, $\bot$ ja $\top$. Niinpä esimerkiksi

$$\begin{aligned} v(P \to Q) &= v(\neg P \vee Q) = \max(v(\neg P), v(Q)) \\ &= \max(1 - v(P), v(Q))\,. \end{aligned}$$

Esim. 8. Ajatellaan totuusarvoja 0 ja 1 lukuina, jolloin voidaan kirjoittaa

$$v(\neg P) = 1 - v(P) \tag{1}$$
$$v(P \wedge Q) = v(P)v(Q) \tag{2}$$
$$v(P \vee Q) = v(P) + v(Q) - v(P) \cdot v(Q) \tag{3}$$
$$v(P \to Q) = 1 - v(P)(1 - v(Q)) \tag{4}$$
$$v(P \leftrightarrow Q) = 1 - (v(P) + v(Q)) + 2v(P)v(Q) \tag{5}$$

Näiden todentaminen jääköön harjoitukseksi.

Kaavojen (1)–(5) avulla propositioiden totuusarvoja voidaan laskea aritmeettisesti. Esimerkiksi,

$$\begin{aligned}
v(p \wedge (q \vee \neg p)) &= v(p) \cdot v(q \vee \neg p) \\
&= v(p) \cdot \big(v(q) + v(\neg p) - v(q) \cdot v(\neg p)\big) \\
&= v(p) \cdot \big(v(q) + 1 - v(p) - v(q) \cdot (1 - v(p))\big) \\
&= v(p) \cdot \big(v(q) + 1 - v(p) - v(q) + v(q)v(p)\big) \\
&= v(p) \cdot \big(1 - v(p) + v(q)v(p)\big) \\
&= v(p) - v(p)^2 + v(q)v(p)^2 \qquad (\text{sillä aina } v(p)^2 = v(p)) \\
&= v(q) \cdot v(p) = v(p \wedge q)
\end{aligned}$$

Näin ollen propositioilla $p \wedge (q \vee \neg p)$ ja $p \wedge q$ on sama totuusfunktio, eli ne ovat loogisesti ekvivalentit. Sama voidaan luonnollisesti, ja tässä tapauksessa helpommin, todeta totuustaulujen avulla. □

Annetun proposition P tautologisuus samoin kuin toteutuvuus voidaan selvittää sen totuustaulusta. Esimerkiksi, propositio P on tautologia tarkalleen silloin kun sitä vastaavassa totuustaulun pystyrivissä on vain ykkösiä. Totuustaulumenetelmä on mukava ja varma työkalu, kun propositiomuuttujia on vähän, mutta siitä tulee työläs, kun muuttujia on paljon. Ymmärrettävästi totuustaulu on jo ikävä kirjata, kun muuttujia on kuusi, sillä tällöin taulussa on $2^6 = 32$ riviä. Jos muuttujia on 10, tulee totuustauluun $2^{10} = 1024$ riviä, ja se on liikaa innostuneimmallekin taulukoijalle. Näitä vaikeampia tapauksia varten on kehitetty erilaisia todistusmenetelmiä.

Seuraavassa lauseessa luetellaan eräitä *tautologiakaavioita*: jokaisesta tällaisesta kaaviosta saadaan ääretön määrä tautologioita korvaamalla metakielen symbolit P, Q, ja R mielivaltaisilla propositioilla.

Esim. 9. Olkoot P, Q, ja R propositioita. Tällöin

$$\models P \vee \neg P \tag{a}$$
$$\models (P \wedge Q) \rightarrow P \tag{b}$$
$$\models P \rightarrow (Q \rightarrow P) \tag{c}$$
$$\models (P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R)) \tag{d}$$
$$\models (P \vee \bot) \leftrightarrow P \tag{e}$$
$$\models (P \wedge \top) \leftrightarrow P \tag{f}$$
$$\models P \rightarrow (P \vee Q)\,. \tag{g}$$

Nämä ovat harjoituksia. □

Lause 2. *Olkoot $P \equiv P'$ loogisesti ekvivalentit propositiot. Jos P on proposition Q osakaava, ja Q' on saatu korvaamalla yksi kaavan P esiintymä kaavalla P', niin $Q \equiv Q'$.*

Todistus. Todistetaan väite rakenteellisella induktiolla lähtien propositiosta P.

- Jos $Q = P$, niin $Q' = P'$ ja siten $Q \equiv Q'$. Oletetaan sitten, että P on proposition Q aito osakaava.
- Olkoon $Q = \neg R$, missä R on propositio. Tällöin kysytty proposition P esiintymä on proposition R osakaava. Induktio-oletuksen mukaan $R \equiv R'$, missä R' on saatu propositiosta R korvaamalla proposition P esiintymä propositiolla P'. Nyt $\neg R \equiv \neg R'$ osoittaa väitteen oikeaksi.

- Olkoon $Q = R \wedge S$, missä R ja S ovat propositioita. Tällöin kysytty proposition P esiintymä on joko proposition R tai proposition S osakaava. Sanokaamme, että edellinen toteutuu. Induktio-oletuksen mukaan $R \equiv R'$, missä R' on saatu propositiosta R korvaamalla proposition P esiintymä propositiolla P'. Nyt $R \wedge S \equiv R' \wedge S$ osoittaa väitteen oikeaksi.
- Tapaus $Q = R \vee Q$ on samanlainen kuin edellä.

Näin väite on todistettu. □

Esim. 10. Todetaan, että $(p \wedge \neg q) \vee q \equiv p \vee q$ ja siten esimerkiksi

$$((\neg p \wedge r) \vee ((p \wedge \neg q) \vee q)) \wedge q \equiv ((\neg p \wedge r) \vee (p \vee q)) \wedge q\,.$$

□

Looginen seuraus

Määr. 6. Propositio P on propositiojoukon Γ **looginen seuraus**, merkitään $\Gamma \models P$, jos jokainen joukon Γ malli on myös proposition P malli, eli

$$v(Q) = 1 \text{ kaikilla } Q \in \Gamma \implies v(P) = 1\,.$$

Jos $\Gamma = \{P_1, \ldots, P_n\}$ on äärellinen propositiojoukko, käytetään myös merkintää

$$P_1, \ldots, P_n \models P\,.$$

Vastaavasti propositiojoukko Δ on propositiojoukon Γ **looginen seuraus**, merkitään $\Gamma \models \Delta$, jos $\Gamma \models Q$ kaikilla $Q \in \Delta$.

Huomattakoon, että propositio on tautologia tarkalleen silloin kun se on tyhjän joukon looginen seuraus. Täten merkinnät $\Gamma \models P$ ja $P_1, \ldots, P_n \models P$ voidaan nähdä merkinnän $\models P$ luonnollisina yleistyksinä. Ehdon $P_1, \ldots, P_n \models P$ voimassaolo voidaan aina ratkaista muodostamalla totuustaulut propositioille $P_1, \ldots, P_n$ ja P.

Esim. 11. Todetaan, että $P \vee Q,\ P \to \neg Q \ \models\ (P \vee Q) \wedge (\neg P \vee \neg Q)$. Tätä varten muodostetaan totuustaulut:

P	Q	$P \vee Q$	$P \to \neg Q$	$(P \vee Q) \wedge (\neg P \vee \neg Q)$
0	0	0	1	0
0	1	1	1	1
1	0	1	1	1
1	1	1	0	0

Huomataan, että niillä riveillä, joissa propositiot $P \vee Q$ ja $P \to \neg Q$ kumpikin saavat totuusarvon 1, myös propositio $(P \vee Q) \wedge (\neg P \vee \neg Q)$ saa arvon 1. □

Esim. 12. Osoitetaan seuraavaksi, että *yleisesti ottaen* on $\neg P, P \to Q \not\models \neg Q$. Vastaavat totuustaulut ovat:

P	Q	$\neg P$	$P \to Q$	$\neg Q$
0	0	1	1	1
0	1	1	1	0
1	0	0	0	1
1	1	0	1	0

Nyt huomataan, että jos $v(P)=0$ ja $v(Q)=1$, niin $v(\neg P)=v(P\to Q)=1$, mutta $v(\neg Q)=0$. Huomattakoon kuitenkin, että propositiot P ja Q voidaan valita siten, että tilanne $v(P)=0$ ja $v(Q)=1$ ei toteudu. Esimerkiksi, jos $P=p\vee\neg p$ tai $Q=p\wedge\neg p$. Tällöin $\neg P, P\to Q\models\neg Q$ on voimassa. □

Looginen seurausrelaatio $\models$ ja implikaatio $\to$ ovat tietysti kaksi aivan eri asiaa, mutta niiden välillä vallitsee kuitenkin seuraava läheinen yhteys.

Lause 3. *Olkoot* $P,Q\in\mathrm{Prop}$. *Tällöin* $P\models Q \iff \models P\to Q$.

Todistus. Oletetaan ensin, että $P\models Q$, ja olkoon $v\colon \mathrm{PM}\to\{0,1\}$ jokin tulkinta. Jos $v(P)=0$, niin $v(P\to Q)=1$ riippumatta arvosta $v(Q)$. Jos taas $v(P)=1$, niin oletuksen $P\models Q$ nojalla myös $v(Q)=1$, ja tällöin $v(P\to Q)=1$, ja siten $P\to Q$ on tautologia.

Oletetaan sitten, että $\models P\to Q$. Jos v on proposition P malli, eli $v(P)=1$, niin myös $v(Q)=1$, sillä $v(P\to Q)=1$. Täten $P\models Q$. □

Lause 3 formalisoi tärkeän yhteyden pääteltävyyden ja totuuden välillä: *propositio Q voidaan päätellä propositiosta P jos ja vain jos $P\to Q$ on tautologia.* Seuraavan tuloksen (b)-kohta on lauseen 3 yleistys.

Lause 4. *Olkoot* $\Gamma\subseteq\mathrm{Prop}$ *ja* $P,Q\in\mathrm{Prop}$. *Tällöin*

(a) $\Gamma\models P \iff \Gamma\cup\{\neg P\}$ *on toteutumaton,*

(b) $\Gamma\cup\{P\}\models Q \iff \Gamma\models P\to Q$.

Todistus. Todistetaan vain ensimmäinen väite; toinen jääköön harjoitukseksi. Oletetaan ensin, että $\Gamma\models P$, ja olkoon v jokin tulkinta. Jos $v(Q)=1$ kaikilla $Q\in\Gamma$ eli v on joukon Γ malli, niin oletuksen mukaan myös $v(P)=1$, ja siten $v(\neg P)=0$. Näin ollen v ei ole joukon $\Gamma\cup\{\neg P\}$ malli. Siis $\Gamma\cup\{\neg P\}$ on toteutumaton.

Toisinpäin, jos $\Gamma\not\models P$, niin on olemassa tulkinta v siten, että $v(Q)=1$ kaikilla $Q\in\Gamma$, mutta $v(P)=0$. Siten $v(\neg P)=1$, ja v on joukon $\Gamma\cup\{\neg P\}$ malli, kuten vaadittua. □

Esim. 13. Seuraavat kaaviot esittävät eräitä tunnettuja päättelysääntöjä:

$$
\begin{aligned}
P,\ Q &\models P\wedge Q \\
P\wedge Q &\models P \\
P &\models P\vee Q \\
P,\ P\to Q &\models Q && \textbf{(Modus Ponens)} \\
\neg Q\to\neg P &\models P\to Q && \textbf{(Kontrapositio)}
\end{aligned}
$$

Nämä voidaan kaikki todistaa kuten edellä. □

On ilmeistä, että $P\equiv Q$ jos ja vain jos $P\models Q$ ja $Q\models P$. Samoin $\Gamma\equiv\Delta$ jos ja vain jos $\Gamma\models\Delta$ ja $\Delta\models\Gamma$. Taas on syytä todeta, että looginen ekvivalenttisuus ja konnektiivi $\leftrightarrow$ ovat kaksi eri asiaa, mutta niiden välillä vallitsee kuitenkin selvä yhteys. Seuraava lemma todistetaan aivan kuten lause 3.

Lause 5. *Olkoot* $P,Q\in\mathrm{Prop}$. *Tällöin* $P\equiv Q \iff \models P\leftrightarrow Q$.

Todistus. Harjoitus. □

Täydelliset konnektiivijoukot

Yleisesti ottaen, n-paikkainen *konnektiivi* on kuvaus #, joka yhdistää mitkä tahansa n propositiota $P_1, \dots, P_n$ yhdeksi propositioksi $\#(P_1, \dots, P_n)$, jonka totuusarvo määräytyy konnektiivin # totuustaulusta.

Esim. 14. Olkoon $\widehat{\cdots}$ 3-paikkainen konnektiivi, joka on määritelty oheisessa totuustaulussa:

P	Q	R	$\widehat{PQR}$	P	Q	R	$\widehat{PQR}$
0	0	0	1	1	0	0	1
0	0	1	0	1	0	1	1
0	1	0	0	1	1	0	1
0	1	1	0	1	1	1	0

Tällöin esimerkiksi $\neg((P \wedge Q) \wedge \neg(\widehat{PQR})) \wedge R$ on hyvin muodostettu propositio konnektiivien $\neg$, $\wedge$ ja $\widehat{\ }$ suhteen. Tämä uusi konnektiivi voidaan esittää peruskonnektiivien avulla:

$$\widehat{PQR} \equiv (P \wedge \neg Q) \vee (P \wedge \neg R) \vee (\neg Q \wedge \neg R)\,.$$

□

Määr. 7. Sanotaan, että konnektiivijoukko $\mathscr{K}$ on **täydellinen**, jos jokainen propositio on loogisesti ekvivalentti sellaisen proposition kanssa, jossa esiintyy vain konnektiiveja joukosta $\mathscr{K}$.

Luonnollisesti konnektiivijoukko $\{\vee, \wedge, \neg\}$ on täydellinen, sillä propositiot on määritelty näiden konnektiivien avulla.

Lause 6. *Joukot* $\{\vee, \neg\}$, $\{\wedge, \neg\}$ *ja* $\{\rightarrow, \perp\}$ *ovat täydellisiä.*

Todistus. Joukon $\{\vee, \neg\}$ täydellisyys voidaan johtaa siitä, että 'puuttuva' konnektiivi $\wedge$ on lausuttavissa ekvivalentissa muodossa $P \wedge Q \equiv \neg(\neg P \vee \neg Q)$. Joukon $\{\wedge, \neg\}$ täydellisyys nähdään samoin. Joukon $\{\rightarrow, \perp\}$ täydellisyys taas seuraa joukon $\{\vee, \neg\}$ täydellisyydestä, sillä $P \vee Q \equiv \neg P \rightarrow Q$ ja $\neg P \equiv P \rightarrow \perp$ kuten helposti todetaan. □

Lause 7. *Yhden konnektiivin joukko* $\{\,|\,\}$ *on täydellinen, missä* ***Shefferin viiva*** $|$ *on määritelty oheisessa totuustaulussa.*

P	Q	$P \mid Q$
0	0	1
0	1	1
1	0	1
1	1	0

Todistus. Harjoitus. □

3 Normaalimuodot

Duaalisuus

Duaalisuus on eräs Boolen algebrojen, jollainen propositiologiikkakin on, perusominaisuus. Siinä pätevästä kaavasta voidaan päätellä duaalinen kaava vaihtamalla sopivasti konnektiiveja pareittain. Tunnetuin Boolen algebra on joukkoalgebra, jossa käsitellään annetun joukon osajoukkoja operaatioiden $\overline{}$ (komplementti), $\cup$ ja $\cap$ yhdessä vakioiden X ja $\emptyset$ kanssa.

Lauseessa 8 on mainittu merkittävät duaalisuustulokset propositiologiikalle. Nämä voidaan todistaa helposti totuustaulujen avulla. Seuraavat ekvivalenssit on jaoteltu kahteen toistensa kanssa **duaaliseen** osaan niin, että vasen- ja oikeapuoli ovat toistensa duaaliset kaavat.

Lause 8. *Jos* $P, Q, R \in \mathrm{Prop}$, *niin*

$$
\begin{array}{lll}
(1) & P \vee Q \equiv Q \vee P & P \wedge Q \equiv Q \wedge P \\
(2) & P \vee (Q \vee R) \equiv (P \vee Q) \vee R & P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R \\
(3) & P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R) & P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R) \\
(4) & P \wedge (P \vee Q) \equiv P & P \vee (P \wedge Q) = P \\
(5) & P \vee \bot \equiv P & P \wedge \top \equiv P \\
(6) & P \vee \neg P \equiv \top & P \wedge \neg P \equiv \bot
\end{array}
$$

- Kohdan (1) ekvivalenssit ilmaisevat konnektiivien $\vee$ ja $\wedge$ **kommutatiivisuuden**.
- **Assosiatiivilakien** (2) ansiosta voidaan kirjoittaa

  $$P_1 \vee P_2 \vee \cdots \vee P_n \quad \text{ja} \quad P_1 \wedge P_2 \wedge \cdots \wedge P_n$$

  ilman ryhmitteleviä sulkeita.
- Kohdan (3) mukaan **distributiivilait** ovat voimassa propositiologiikassa.
- Kohta (4) esittää **absorptiolait**.
- Kohdat (5) ja (6) ovat **yksinkertaistussääntöjä**. Erityisesti kohdan (6) ensimmäinen tapaus on **kolmannen poissuljetun laki**.

Lause 9 (de Morgan)**.** *Kaikille propositioille P ja Q on voimassa*

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q \quad \textit{ja} \quad \neg(P \vee Q) \equiv \neg P \wedge \neg Q\,.$$

Todistus. Harjoituksia. □

Edeltäviä kaavoja voidaan käyttää hyväksi osoittamaan, että propositio on tautologia.

Esim. 15. Osoitetaan, että $(P \to (P \wedge Q)) \equiv (P \to Q)$. Tätä varten kirjoitetaan ensin auki implikaation määrittely, ja käytetään sitten edellä mainittuja ekvivalensseja.

$$
\begin{array}{rcll}
P \to (P \wedge Q) & \equiv & \neg P \vee (P \wedge Q) & \text{implikaation määrittely} \\
& \equiv & (\neg P \vee P) \wedge (\neg P \vee Q) & \text{distributiivisuus} \\
& \equiv & \top \wedge (\neg P \vee Q) & \text{kolmannen poissuljetun laki} \\
& \equiv & (\neg P \vee Q) \wedge \top & \text{kommutatiivisuus} \\
& \equiv & \neg P \vee Q & \text{yksinkertaistus} \\
& \equiv & P \to Q & \text{implikaation määrittely}
\end{array}
$$

□

Käsitellään seuraavassa propositioita, joissa on vain konnektiiveja $\neg, \wedge, \vee$.

Määr. 8. Olkoon P propositio ja P^* saatu siitä vaihtamalla jokainen propositiomuuttuja p negaatiokseen $\neg p$, jokainen konnektiivi $\wedge$ konnektiiviksi $\vee$ ja jokainen konnektiivi $\vee$ konnektiiviksi $\wedge$.

Huomaa, että edellä vain propositiomuuttujat p_i muutetaan negaatioikseen, ei yleisemmät osakaavat.

Esim. 16. Jos $P = \neg(p \vee q) \wedge \neg q$, niin $P^* = \neg(\neg p \wedge \neg q) \vee \neg\neg q$, missä kaksoisnegaatio voidaan sieventää pois lauseen 2 mukaisesti: $P^* \equiv \neg(\neg p \wedge \neg q) \vee q$. □

Seuraava lause esittelee propositiologiikan yleisen duaalisuuslain.

Lause 10. *Jokaiselle propositiolle P on voimassa $\neg P \equiv P^*$.*

Todistus. Todistetaan väite (rakenteellisella) induktiolla.

- Jos $P = p \in \mathrm{PM}$, on väite selvä, sillä nyt $P^* = \neg p = \neg P$. Oletetaan sitten, että Q ja R toteuttavat väitteen: $\neg Q \equiv Q^*$ ja $\neg R \equiv R^*$.
- Oletetaan, että $P = \neg Q$, missä Q toteuttaa väitteen: $\neg Q \equiv Q^*$. Siten
$$\neg P = \neg\neg Q \equiv \neg Q^* = P^*.$$
- Oletetaan, että $P = Q \wedge R$. De Morganin lakia noudattaen saadaan
$$\neg P = \neg(Q \wedge R) \equiv \neg Q \vee \neg R \equiv Q^* \vee R^* = P^*.$$
- Oletetaan, että $P = Q \vee R$. De Morganin lakia noudattaen saadaan
$$\neg P = \neg(Q \vee R) \equiv \neg Q \wedge \neg R \equiv Q^* \wedge R^* = P^*.$$

□

Huom. Mikäli propositiossa P esiintyy konnektiivi $\to$, sanokaamme osakaavassa $Q \to R$, voidaan se kirjoittaa ensin ekvivalenttiin muotoon $\neg Q \vee R$, ja soveltaa sitten duaalisuutta.

Distributiivilait ja de Morganin lait voidaan yleistää seuraavasti.

Lause 11 (Yleistetty distributiivilaki)**.** *Jos* $P_1, \dots, P_m, Q_1, \dots, Q_n \in \mathrm{Prop}$, *niin*
$$(P_1 \vee \cdots \vee P_m) \wedge (Q_1 \vee \cdots \vee Q_n) \equiv (P_1 \wedge Q_1) \vee \cdots \vee (P_1 \wedge Q_n) \vee \cdots \vee (P_m \wedge Q_n)\,.$$

Todistus. Olkoon $v\colon \mathrm{PM} \to \{0,1\}$ tulkinta. Tällöin
$$\begin{aligned}
&v((P_1 \vee \cdots \vee P_m) \wedge (Q_1 \vee \cdots \vee Q_n)) = 1\\
&\quad\iff v(P_1 \vee \cdots \vee P_m) = 1 \text{ ja } v(Q_1 \vee \cdots \vee Q_n) = 1\\
&\quad\iff \text{ on indeksit } i \text{ ja } j\colon\ v(P_i) = 1 \text{ ja } v(Q_j) = 1\\
&\quad\iff \text{ on indeksit } i \text{ ja } j\colon\ v(P_i \wedge Q_j) = 1\\
&\quad\iff v((P_1 \wedge Q_1) \vee \cdots \vee (P_i \wedge Q_j) \vee \cdots \vee (P_m \wedge Q_n)) = 1\,.
\end{aligned}$$

□

Lause 12 (Yleistetty distributiivilaki)**.** *Jos* $P_1, \dots, P_m, Q_1, \dots, Q_n \in \mathrm{Prop}$, *niin*
$$(P_1 \wedge \cdots \wedge P_m) \vee (Q_1 \wedge \cdots \wedge Q_n) \equiv (P_1 \vee Q_1) \wedge \cdots \wedge (P_1 \vee Q_n) \wedge \cdots \wedge (P_m \vee Q_n).$$

Todistus. Väite seuraa edeltävästä tuloksesta duaalisuutta käyttäen. (Se voidaan toki myös todistaa aivan vastaavasti kuin edeltävä lause.) □

Lause 13 (Yleistetyt de Morganin lait)**.** *Jos* $P_1, \dots, P_n \in \mathrm{Prop}$*, niin*

$$\neg(P_1 \vee \cdots \vee P_n) \equiv \neg P_1 \wedge \cdots \wedge \neg P_n \quad ja \quad \neg(P_1 \wedge \cdots \wedge P_n) \equiv \neg P_1 \vee \cdots \vee \neg P_n.$$

Todistus. Lauseen 10 mukaan $\neg(P_1 \vee \cdots \vee P_n) \equiv P_1^* \wedge \cdots \wedge P_n^*$, missä $P_i^* \equiv \neg P_i$. Näin ensimmäinen väite seuraa. Toinen todistetaan samoin. □

Disjunktiivinen normaalimuoto

Määritellään tässä kappaleessa eräitä propositioiden normaalimuotoja sekä osoitetaan, että jokainen propositio voidaan algoritmisesti saattaa näihin normaalimuotoihin.

Määr. 9. **Literaali** on joko propositiomuuttuja p tai propositiomuuttujan negaatio $\neg p$. Olkoot $\ell_1, \dots, \ell_m$ literaaleja. Tällöin

- $\ell_1 \wedge \cdots \wedge \ell_m$ on **alkeiskonjunktio**.
- Jos jokainen K_i on alkeiskonjunktio, on propositio $K_1 \vee \cdots \vee K_n$ **disjunktiivisessa normaalimuodossa** (**DN-muodossa**). Kun $n = 0$, sovitaan, että $K_1 \vee \cdots \vee K_n = \bot$.

Vastaavasti määritellään konjunktiivinen normaalimuoto.

Määr. 10. Olkoot $\ell_1, \dots, \ell_m$ literaaleja. Tällöin

- $\ell_1 \vee \cdots \vee \ell_m$ on **alkeisdisjunktio**.
- Jos jokainen D_i on alkeisdisjunktio, on propositio $D_1 \wedge \cdots \wedge D_n$ **konjunktiivisessa normaalimuodossa** (**KN-muodossa**), Kun $n = 0$, sovitaan, että $D_1 \wedge \cdots \wedge D_n = \top$.

Esim. 17. Kun $p, q, r \in \mathrm{PM}$, on propositio $p \wedge \neg q \wedge r$ alkeiskonjunktio ja $\neg p \vee \neg q$ alkeisdisjunktio. Propositio $(p \wedge \neg q) \vee \neg r$ on DN-muodossa, mutta ei KN-muodossa. □

Propositiolla on yleensä useita disjunktiivisessa normaalimuodossa olevia kaavoja. Seuraavassa esitetty probleema on algoritmisesti hyvin vaikea: se on yksi niin kutsutuista *NP-täydellisistä ongelmista*.

Probleema. Annettuna propositio P määrää sen disjunktiivinen normaalimuoto, jossa on vähiten alkeiskonjunktioita.

Koska edellä viitatut optimaaliset normaalimuodot ovat haluttuja sovelluksissa, on kehitetty monia algoritmisia menetelmiä, jotka antavat hyviä – joskaan ei ehkä optimaalisia – DN-muotoja annetuille propositioille. Seuraavan lauseen todistuksessa esitetään algoritmi, jonka avulla jokainen propositio voidaan saattaa disjunktiiviseen normaalimuotoon. Konjunktiiviselle normaalimuodolle on vastaavanlainen algoritmi.

Lause 14. *Jokainen propositio on ekvivalentti disjunktiivisessa normaalimuodossa olevan proposition.*

Todistus. Olkoon P propositio. (Seuraavassa sovelletaan lausetta 2.)

(1) Jos siinä esiintyy konnektiiveja $\rightarrow$ tai $\leftrightarrow$, kirjoitetaan ne auki määrittelynsä mukaisesti: $P \rightarrow Q = \neg P \vee Q$ ja $P \leftrightarrow Q = (P \wedge Q) \vee (\neg P \vee \neg Q)$.

(2) Viedään konnektiivit $\neg$ propositiomuuttujien eteen soveltaen seuraavia muunnoksia niin kauan kuin tarpeellista:

$$\begin{aligned} \neg\neg Q &\mapsto Q, \\ \neg(Q \wedge R) &\mapsto \neg Q \vee \neg R, \\ \neg(Q \vee R) &\mapsto \neg Q \wedge \neg R. \end{aligned}$$

Tämän jälkeen siis negaatio voi esiintyä vain literaaleissa ($\neg p$).

(3) Viedään konjunktiot $\wedge$ iteratiivisesti alkeiskonjunktioihin distributiivilakien avulla:

$$Q \wedge (R \vee S) \mapsto (Q \wedge R) \vee (Q \wedge S)\,,$$
$$(R \vee S) \wedge Q \mapsto (R \wedge Q) \vee (S \wedge Q)\,.$$

□

Esim. 18. Propositiolle $P = \neg(p \vee \neg q) \wedge (\neg r \vee (p \wedge \neg q))$ saadaan DN-muoto seuraavasti:

$$\begin{aligned} P &\overset{(2)}{\equiv} (\neg p \wedge \neg\neg q) \wedge (\neg r \vee (p \wedge \neg q)) \\ &\overset{(2)}{\equiv} (\neg p \wedge q) \wedge (\neg r \vee (p \wedge \neg q)) \\ &\overset{(3)}{\equiv} ((\neg p \wedge q) \wedge \neg r) \vee ((\neg p \wedge q) \wedge (p \wedge \neg q)) \\ &\equiv (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge p \wedge \neg q) \end{aligned}$$

mikä on DN-muodossa, vaikkakin se yksinkertaistuu, sillä jälkimmäinen alkeiskonjunktio on toteutumaton. Siis

$$P \equiv (\neg p \wedge q \wedge \neg r) \vee \bot \equiv \neg p \wedge q \wedge \neg r\,.$$

Propositioiden normaalimuodot eivät ole yksikäsitteisiä ja niitä voidaan usein sieventää. □

Karnaugh'n kartat

Karnaugh'n karttojen käyttö perustuu seuraavan sievennyssäännön yleistykseen: jos p on propositiomuuttuja ja P propositio, niin

$$(p \wedge P) \vee (\neg p \wedge P) \equiv P\,. \tag{*}$$

Esim. 19. Tarkastellaan DN-muodossa olevaa kaavaa $(\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge q)$. Monistetaan, ensin sen toinen tekijä $\neg p \wedge q$. Tämä on sallittua, sillä jos P ja Q ovat propositioita, niin $P \vee Q \equiv P \vee P \vee Q$. Käytetään sitten sievennyssääntöä alku- ja loppuosaan:

$$\begin{aligned} &(\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge q) \\ &\equiv \big((\neg p \wedge \neg q) \vee (\neg p \wedge q)\big) \vee \big((\neg p \wedge q) \vee (p \wedge q)\big) \\ &\equiv \neg p \vee q \end{aligned}$$

□

Sievennyssääntöä voidaan soveltaa kahteen tai useampaan propositiomuuttujaan, jos niiden kaikki vaihtoehdot esiintyvät DN-muodossa jonkun proposition yhteydessä:

$$(p \wedge q \wedge P) \vee (\neg p \wedge q \wedge P) \vee (p \wedge \neg q \wedge P) \vee (\neg p \wedge \neg q \wedge P) \equiv P\,.$$

Edellä p ja q käyvät läpi kaikki mahdolliset $2^2 = 4$ yhdistelmää yhdessä proposition P kanssa.

Esim. 20. Tässä p, q käyvät läpi kaikki mahdollisuudet:

$$\begin{aligned} &(\neg p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \\ &\equiv (\neg q \wedge \neg r) \vee (q \wedge \neg r) \equiv \neg r \end{aligned}$$

□

<u>Esim</u>. 21. DN-muotoon saattamista voidaan käyttää osoittamaan proposition tautologisuus. Tarkastellaan **Peircen lakia** $R = ((P \to Q) \to P) \to P$. Tällöin

$$
\begin{aligned}
R &\overset{(1)}{\equiv} \neg(\neg(\neg P \vee Q) \vee P) \vee P \\
&\overset{(2)}{\equiv} \neg\neg(\neg P \vee Q) \wedge \neg P) \vee P \\
&\overset{(2)}{\equiv} ((\neg P \vee Q) \wedge \neg P) \vee P \\
&\overset{(3)}{\equiv} ((\neg P \wedge \neg P) \vee (Q \wedge \neg P)) \vee P \\
&\equiv (\neg P \vee (Q \wedge \neg P)) \vee P \\
&\equiv (\neg P \vee P) \vee (Q \wedge \neg P) \equiv \top\,.
\end{aligned}
$$

□

Karnaugh'n kartan piirtäminen tapahtuu binääristen Gray-koodien avulla: Asetetaan pituutta n olevat binäärijonot

$$b_1, b_2, \ldots, b_{2^n}$$

järjestykseen niin, että $b_1 = 00\cdots0$, ja $b_{2^n} = 100\cdots0$, ja b_i ja b_{i+1} eroavat toisistaan tarkalleen yhden bitin osalta (samoin kuin b_1 ja b_{2^n}). Tällainen jono on aina mahdollista tehdä – konstruktio on rekursiivinen. Huomaa, että myös ensimmäinen ja viimeinen binäärijono eroavat toisistaan vain yhden bitin osalta.

<u>Esim</u>. 22. Pienille arvoille seuraavat ovat Gray-koodeja:

- $n = 1$: 0, 1
- $n = 2$: 00, 01, 11, 10
- $n = 3$: 000, 001, 011, 010, 110, 111, 101, 100. □

Huom. Kurssissa rajoitutaan vain tapauksiin, joissa propositioissa on korkeintaan neljä muuttujaa, ja Gray-koodeihin joiden pituus on korkeintaan kaksi. Tapaukset, joissa on 5 tai useampia muuttujia vaativat monimuotoisempia karttoja (hyperkuutioita).

Olkoon P propositio, jossa on (korkeintaan) neljä muuttujaa. Sen **Karnaugh'n kartta** on Gray-koodin yleistyksenä taulukko, missä

- jokainen ruutu, eli **solu**, vastaa pituutta n olevaa binäärijonoa $b_4b_3b_2b_1$, joka saa proposition P totuustaulun arvon vastaavalla totuustaulun rivillä; kukin solu vastaa siis yhtä totuustaulun riviä;
- vierekkäiset solut eroavat toisistaan tarkalleen yhdessä bitissä. Vaakarivien päätysolut ovat vierekkäisiä, ja pystyrivien päätysolut ovat vierekkäisiä;
- kartan vaaka- ja pystyrivit järjestetään siis Gray-koodin mukaisesti.

<u>Esim</u>. 23. Olkoon $P = (p \vee \neg q) \wedge (r \to p) \wedge (s \to q)$. Sen Karnaugh'n kartta on piirretty kuvaan 2. □

Karnaugh'n kartan jokainen $2^t \times 2^k$ vierekkäisistä soluista koostuva suorakulmio, jonka jokaisessa solussa on arvo 1, vastaa jotain DN-muotoa, joka sievenee käytettäessä sääntöä (*) niin, että siitä poistuvat kaikki ne propositiomuuttujat, joiden arvo vaihtuu. Tämä johtuu siitä, että arvonsa vaihtavat propositiomuuttujat käyvät läpi kaikki mahdolliset variaatiot, ja loput muuttujat ovat vakioita koko suorakulmiossa.

0000	0001	0011	0010
0100	0101	0111	0110
1100	1101	1111	1110
1000	1001	1011	1010

$rs \backslash pq$	00	01	11	10
00	1	1	1	0
01	0	1	1	0
11	0	0	1	0
10	0	0	1	0

Kuva 2: Karnaugh'n kartan solukko, ja esimerkin proposition arvot.

<u>Esim</u>. 24. Tarkastellaan oheista Karnaugh'n karttaa, jossa kirjaimilla a, b, ja c merkityt solut saavat arvon 1.

$rs \backslash pq$	00	01	11	10
00	a			
01	a		b	b
11			b	b
10	c			c

Kuvassa samalla kirjaimella merkityt solut muodostavat tyypillisiä suorakulmioita, joita vastaavat alkeiskonjunktiot ovat

$$K_a = \neg p \wedge \neg q \wedge \neg r, \quad K_b = p \wedge s, \quad \text{ja} \quad K_c = \neg q \wedge r \wedge \neg s\,.$$

□

Annetun proposition P minimaaliset DN-muodot voidaan määrätä Karnaugh'n karttojen avulla seuraavasti:

(i) Merkitään totuustaulusta kuhunkin soluun proposition P vastaava arvo.

(ii) Muodostetaan proposition P kartan ykkössoluista kaikki maksimaaliset suorakulmiot.

(iii) Valitaan maksimaalisista kulmioista minimaalinen osasysteemi, joka kattaa kaikki kartan ykköset. Jokaista kulmiota vastaa alkeiskonjunktio, ja niiden disjunktio on ekvivalentti proposition P kanssa.

Huomattakoon, että tietty ykkönen voi esiintyä useassa suorakulmiossa.

<u>Esim</u>. 25. Tarkastellaan karttaa, ja sen yhtä maksimaalisten suorakulmioiden valintaa:

$rs \backslash pq$	00	01	11	10
00	1	1		1
01		1		
11	1	1	1	1
10				1

Saadaan propositio Q, joka on DN-muodossa

$$P \equiv Q = (r \wedge s) \vee (\neg q \wedge \neg r \wedge \neg s) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r)\,.$$

□

4 Kompaktisuuslause

Oletetaan tässä kappaleessa yksinkertaisuuden vuoksi, että käytössä ovat vain konnektiivit $\neg$, $\wedge$ ja $\vee$. Logiikan kompaktisuustulos kertoo, että äärettömien joukkojen toteutuvuus seuraa äärellisten osajoukkojen toteutuvuudesta. Kompaktisuuslauseella on useita seurauksia muualla matematiikassa.

Hintikan joukot

Määr. 11. Sanotaan, että propositiojoukko Γ on **äärellisesti toteutuva**, jos sen jokainen äärellinen osajoukko on toteutuva.

Lemma. 15. *Olkoon Γ äärellisesti toteutuva propositiojoukko. Tällöin kun P on propositio, $\Gamma \cup \{P\}$ tai $\Gamma \cup \{\neg P\}$ on äärellisesti toteutuva.*

Todistus. Tehdään vastaoletus, ja oletetaan, että on olemassa äärelliset osajoukot $\Sigma, \Delta \subseteq \Gamma$, joille $\Sigma \cup \{P\}$ ja $\Delta \cup \{\neg P\}$ eivät ole toteutuvia. Oletuksen mukaan on olemassa tulkinta v, joka on joukon $\Sigma \cup \Delta$ malli. Jos $v(P) = 1$, on v myös joukon $\Sigma \cup \Delta \cup \{P\}$ ja siten myös joukon $\Sigma \cup \{P\}$ malli, ja muutoin se on joukon $\Sigma \cup \Delta \cup \{\neg P\}$ ja siten myös joukon $\Delta \cup \{\neg P\}$ malli, mikä on kaivattu ristiriita. $\square$

Määr. 12. Kaavajoukko Γ on **Hintikan joukko** jos se toteuttaa seuraavat ehdot kaikille propositioille P, P_1 ja P_2.

(i) Ei ole niin, että $P \in \Gamma$ ja $\neg P \in \Gamma$;

(ii) Jos $\neg\neg P \in \Gamma$, myös $P \in \Gamma$;

(iii) Jos $P_1 \wedge P_2 \in \Gamma$, myös $P_1 \in \Gamma$ ja $P_2 \in \Gamma$;

(iv) Jos $P_1 \vee P_2 \in \Gamma$, myös $P_1 \in \Gamma$ tai $P_2 \in \Gamma$;

(v) Jos $\neg(P_1 \wedge P_2) \in \Gamma$, myös $\neg P_1 \in \Gamma$ tai $\neg P_2 \in \Gamma$;

(vi) Jos $\neg(P_1 \vee P_2) \in \Gamma$, myös $\neg P_1 \in \Gamma$ ja $\neg P_2 \in \Gamma$.

Lemma. 16 (Hintikka)**.** *Jokainen Hintikan joukko on toteutuva.*

Todistus. Olkoon Γ Hintikan joukko. Määritellään tulkinta v oheisesti:

$$v(p) = \begin{cases} 0 & \text{jos } \neg p \in \Gamma, \\ 1 & \text{muutoin.} \end{cases}$$

(Huomaa, että voi olla $p, \neg p \notin \Gamma$.) Osoitetaan rakenteellisella induktiolla, että v toteuttaa joukon Γ. Olkoon $P \in \Gamma$.

(1) Jos $P = p \in \mathrm{PM}$, on $v(P) = 1$.

(2) Olkoon $P = \neg Q$.

   (a) Jos $Q = q \in \mathrm{PM}$, niin $v(q) = 0$ ja siten $v(P) = 1$.

   (b) Jos $Q = \neg q$, missä $q \in \mathrm{PM}$, niin ehdon (ii) nojalla $q \in \Gamma$, ja tällöin myös $v(P) = 1$.

   (c) Jos $Q = P_1 \wedge P_2$, niin ehdon (v) mukaan $\neg P_1 \in \Gamma$ tai $\neg P_2 \in \Gamma$. Induktio-oletuksesta saadaan, että $v(\neg P_1) = 1$ tai $v(\neg P_2) = 1$. Nyt de Morganin kaavan nojalla $P \equiv \neg P_1 \vee \neg P_2$, ja siten $v(P) = 1$.

(d) Jos $Q = P_1 \vee P_2$, niin ehdon (vi) mukaan $\neg P_1 \in \Gamma$ ja $\neg P_2 \in \Gamma$, ja induktio-oletuksesta saadaan, että $v(\neg P_1) = 1$ ja $v(\neg P_2) = 1$. Nyt de Morganin kaavan nojalla $P \equiv \neg P_1 \wedge \neg P_2$, ja siten $v(P) = 1$.

(3) Olkoon $P = P_1 \wedge P_2$, jolloin ehdon (iii) nojalla $P_1 \in \Gamma$ ja $P_2 \in \Gamma$. Induktio-oletuksen nojalla $v(P_1) = 1$ ja $v(P_2) = 1$, eli myös $v(P) = 1$.

(4) Olkoon $P = P_1 \vee P_2$, jolloin ehdon (iv) nojalla $P_1 \in \Gamma$ tai $P_2 \in \Gamma$. Induktio-oletuksen nojalla $v(P_1) = 1$ tai $v(P_2) = 1$, eli myös $v(P) = 1$.

□

Seuraava lause on propositiologiikan yksi merkittävimmistä tuloksista.

Lause 17 (Kompaktisuuslause)**.** *Kaavajoukko Γ on toteutuva jos ja vain jos sen jokainen äärellinen osajoukko on toteutuva.*

Todistus. ($\Rightarrow$) Jos Γ on toteutuva, samoin ovat tietysti sen äärelliset osajoukot.

($\Leftarrow$) Oletetaan että Γ on äärellisesti toteutuva. Koskapa äärellinen joukko $\{P, \neg P\}$ ei ole toteutuva, vain toinen propositioista P ja $\neg P$ voi kuulua joukkoon Γ.

Osoitetaan ensin, että Γ sisältyy johonkin **maksimaaliseen** äärellisesti toteutuvaan joukkoon, eli sellaiseen äärellisesti toteutuvaan joukkoon, johon ei voida lisätä propositiota rikkomatta tätä ominaisuutta.

Olkoon $\mathscr{F}$ kaikkien sellaisten äärellisesti toteutuvien propositiojoukkojen Σ perhe, joille $\Gamma \subseteq \Sigma$. Jos tässä perheessä on kasvava jono $\Sigma_1 \subseteq \Sigma_2 \subseteq \dots$ myös niiden unioni $\Sigma = \cup \Sigma_{i=1}^{\infty}$ kuuluu perheeseen $\mathscr{F}$. Toden totta, se on äärellisesti toteutuva, koska jokainen sen äärellinen osajoukko on jonkin joukon Σ_i äärellinen osajoukko, ja siten toteutuva. Toisaalta, varmastikin $\Gamma \subseteq \Sigma$. Näin ollen $\Sigma \in \mathscr{F}$, ja se on jonon $\Sigma_1 \subseteq \Sigma_2 \subseteq \dots$ yläraja perheessä $\mathscr{F}$. Nyt Zornin lemman mukaan perheessä $\mathscr{F}$ on maksimaalinen alkio, sanokaamme Δ.

Todistetaan, että maksimaalinen äärellisesti toteutuva joukko Δ on Hintikan joukko. Katsotaan Hintikan ehdoista vain kolme ensimmäistä tapausta; muut menevät samankaltaisesti.

Ehto (i). Olkoon $P \in \Delta$. Jos myös $\neg P \in \Delta$, ei äärellinen osajoukko $\{P, \neg P\}$ voi olla toteutuva vastoin joukon Δ ominaisuutta. Siten Δ toteuttaa Hintikan ehdon (i).

Ehto (ii). Olkoon $\neg\neg P \in \Delta$. Luonnollisesti $\neg\neg P \equiv P$, ja siten $\Delta \cup \{P\}$ on myös äärellisesti toteutuva, sillä muutoin lemman 15 mukaan $\Delta \cup \{\neg P\}$ olisi äärellisesti toteutuva, ja $\{\neg\neg P, \neg P\}$ olisi toteutuva, mikä on mahdotonta. Maksimaalisuudesta seuraa, että $P \in \Delta$.

Ehto (iii). Olkoon $P \wedge Q \in \Delta$. Nyt lemman 15 mukaan, joko $\Delta \cup \{P\}$ tai $\Delta \cup \{\neg P\}$ on äärellisesti toteutuva, ja siten maksimaalisuuden nojalla joko $P \in \Delta$ tai $\neg P \in \Delta$. Siis jos $P \notin \Delta$, niin $\neg P \in \Delta$. Mutta äärellinen osajoukko $\{P \wedge Q, \neg P\}$ ei ole toteutuva, mikä on ristiriita. Siis $P \in \Delta$ ja aivan samoin $Q \in \Delta$.

Lemman 16 mukaan joukko Δ on toteutuva, ja siten sen osajoukko Γ on myös toteutuva.

□

Esimerkki: Hallin sovitukset

Olkoot X ja Y kaksi erillistä alkiojoukkoa (eli $X \cap Y = \emptyset$), ja $E \subseteq X \times Y$ relaatio niiden välillä. Tällöin sanotaan, että $G = (X, Y, E)$ on **2-jakoinen graafi**, jonka **pisteet** ovat joukon $X \cup Y$ alkiot ja **nuolet** ovat joukon E parit $(x, y) \in E$. Osajoukko $M \subseteq E$ on graafin G **sovitus**, jos millään kahdella nuolella $e, f \in M$ ei ole yhteistä alku- tai loppupistettä. Sovitus M

on **täydellinen**, jos jokaiselle joukon X pisteelle x on (yksikäsitteinen) piste $y \in Y$ niin, että $(x,y) \in M$.

Jos $A \subseteq X$ ja $B \subseteq Y$, ovat niiden naapurustot vastaavasti

$$\begin{aligned} N(A) &= \{y \in Y \mid (x,y) \in E \text{ jollain } x \in A\}, \\ N(B) &= \{x \in X \mid (x,y) \in E \text{ jollain } y \in B\}. \end{aligned}$$

Jos $A = \{x\}$ on yhden alkion joukko, merkitään naapurustoa yksinkertaisemmin $N(x)$.

Seuraava graafiteoreettinen tulos on peräisin Hallilta. Tämä esitetään vain mielenkiinnon vuoksi, ja sen todistus sivuutetaan.

Lause 18 (Hall)**.** *Olkoon $G = (X,Y,E)$ äärellinen 2-jakoinen graafi. Tällöin sillä on täydellinen sovitus jos ja vain jos $|A| \leq |N(A)|$ kaikilla $A \subseteq X$.*

Seuraavassa $E_A = E \cap A \times N(A)$ koostuu niistä nuolista, jotka alkavat joukosta A.

Lause 19. *Olkoon $G = (X,Y,E)$ ääretön 2-jakoinen graafi, jolle jokainen naapurusto $N(x)$ on äärellinen. Jos sen jokaisella äärellisellä osagraafilla $G_A = (A,N(A),E_A)$ on täydellinen sovitus, on graafilla G täydellinen sovitus.*

Todistus. Kullekin parille (x,y), missä $x \in X$ ja $y \in Y$, olkoon p_{xy} propositiomuuttuja. Olkoon $N(x) = \{y_1, y_2, \dots, y_m\}$ jollekin $m \geq 1$, ja määritellään seuraavat propositiot kaikille $x \in X$ ja $y \in Y$:

$$\begin{aligned} P_x &= (p_{xy_1} \vee p_{xy_2} \vee \cdots \vee p_{xy_m}) \\ Q_x &= \neg(p_{xy_1} \wedge p_{xy_2}) \wedge \neg(p_{xy_1} \wedge p_{xy_3}) \wedge \cdots \wedge \neg(p_{xy_1} \wedge p_{xy_m}) \\ &\qquad \wedge \cdots \wedge \neg(p_{xy_{m-1}} \wedge p_{xy_m}). \end{aligned}$$

Todetaan, että $v(P_x \wedge Q_x) = 1$ silloin ja vain silloin kun tarkalleen yhdelle indeksille i on $v(p_{xy_i}) = 1$. Vastaavasti, jos $y \in Y$ ja $N(y) = \{x_1, x_1, \dots, x_k\}$, niin olkoon

$$\begin{aligned} R_y &= \neg(p_{x_1y} \wedge p_{x_2y}) \wedge \neg(p_{x_1y} \wedge p_{x_3y}) \wedge \cdots \wedge \neg(p_{x_1y} \wedge p_{x_ky}) \\ &\qquad \wedge \cdots \wedge \neg(p_{x_{k-1}y} \wedge p_{x_ky}). \end{aligned}$$

Tällöin $v(R_y) = 1$ jos ja vain jos on korkeintaan yksi indeksi i, jolle $v(p_{x_iy}) = 1$. Johtopäätöksenä on, että propositiojoukko $\Gamma = \{P_x, Q_x \mid x \in X\} \cup \{R_y \mid y \in Y\}$ on toteutuva jos ja vain jos graafilla G on täydellinen sovitus.

Olkoon sitten $\Gamma_1 \subseteq \Gamma$ jokin äärellinen osajoukko, ja olkoon A siinä esiintyvien pisteiden $x \in X$ joukko. Tällöin A on varmasti äärellinen, ja oletuksen mukaan graafilla G_A on täydellinen sovitus. Niinpä, edeltävän mukaan propositiojoukko Γ_1 on toteutuva. Siis jokainen äärellinen osajoukko Γ_1 on toteutuva, ja kompaktisuuslauseen mukaan, myös Γ on toteutuva, eli graafilla G on täydellinen sovitus. $\square$

5 Aksiomatiikkaa

Aksioomat ja teoreemat

Tarkastellaan seuraavassa yksinkertaisuuden vuoksi propositioita, joissa esiintyy vain konnektiiveja $\neg$ ja $\rightarrow$. Siten konnektiivit $\wedge$, $\vee$, ja $\leftrightarrow$ ovat siten lyhennysmerkintöjä kaavoille

$$\begin{aligned} P \wedge Q &\equiv \neg(P \rightarrow \neg Q)\,, \\ P \vee Q &\equiv \neg P \rightarrow Q\,, \\ P \leftrightarrow Q &\equiv \neg((P \rightarrow Q) \rightarrow \neg(Q \rightarrow P))\,. \end{aligned}$$

Seuraavat kolme kaavaa ovat aksioomeja. Itseasiassa näitä kaavoja on ääretön määrä, sillä aksioomat ovat voimassa kaikille propositiolle.

<u>Määr</u>. 13. Kaikille propositioille P, Q ja R seuraavat ovat **aksioomeja**:

$$P \rightarrow (Q \rightarrow P) \tag{A1}$$

$$(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R)) \tag{A2}$$

$$(\neg Q \rightarrow \neg P) \rightarrow (P \rightarrow Q) \tag{A3}$$

Teoreemat määritellään induktiivisesti seuraavasti. Kaikki aksioomat ovat teoreemoja, ja jos P ja $P \rightarrow Q$ ovat teoreemoja, samoin on Q. Kyseinen päättelysääntö on nimeltään **Modus Ponens** eli **MP**. Merkitään $\vdash_{\mathrm{ax}} P$, jos P on teoreema.

Näin ollen ainoa päättelysääntö MP sanoo:

$$\left.\begin{array}{l} \vdash_{\mathrm{ax}} P \\ \vdash_{\mathrm{ax}} P \rightarrow Q \end{array}\right\} \implies \quad \vdash_{\mathrm{ax}} Q\,. \tag{MP}$$

<u>Esim</u>. 26. Osoitetaan, että $\vdash_{\mathrm{ax}} P \rightarrow P$.

1.	$P \rightarrow ((P \rightarrow P) \rightarrow P)$	(A1): $Q = (P \rightarrow P)$
2.	$(P \rightarrow ((P \rightarrow P) \rightarrow P)) \rightarrow ((P \rightarrow (P \rightarrow P)) \rightarrow (P \rightarrow P))$	(A2): $Q = (P \rightarrow P)$ ja $R = P$
3.	$((P \rightarrow (P \rightarrow P)) \rightarrow (P \rightarrow P))$	MP: 1+2
4.	$P \rightarrow (P \rightarrow P))$	(A1): $Q = P$
5.	$P \rightarrow P$	MP: 3+4

$\square$

<u>Määr</u>. 14. Olkoon $\Gamma \subseteq \mathrm{Prop}$ joukko propositioita. Proposition P **johto** (**premisseistä**) Γ on jono $Q_1, Q_2, \ldots, Q_m$, missä $Q_m = P$ ja kukin Q_i on joko aksiooma, tai $Q_i \in \Gamma$, tai se on saatu Modus Ponensilla kahdesta aikaisemmasta propositiosta Q_r ja Q_s ($r, s < i$). Merkitään

$$\Gamma \vdash_{\mathrm{ax}} P$$

jos propositiolla P on johto premisseistä Γ. Jos tässä $\Gamma = \{P_1, \ldots, P_n\}$ on äärellinen joukko, merkitään myös $P_1, \ldots, P_n \vdash_{\mathrm{ax}} P$. Jos $\Gamma \vdash_{\mathrm{ax}} P$ ei ole voimassa, merkitään $\Gamma \not\vdash_{\mathrm{ax}} P$.

Huomaa, että $\vdash_{\mathrm{ax}} P$ on sama kuin $\emptyset \vdash_{\mathrm{ax}} P$, eli edeltävä määritelmä on sopusoinnussa teoreeman määritelmän kanssa.

Esim. 27. Osoitetaan, että $P \to (Q \to R),\ P \to Q \vdash_{\text{ax}} P \to R$.

1.	$P \to (Q \to R)$	premissi
2.	$P \to Q$	premissi
3.	$(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$	(A2)
4.	$(P \to Q) \to (P \to R)$	MP: 1+3
5.	$P \to R$	MP: 2+4

□

Lause 20. *Kaikille propositiolle P ja Q on voimassa $P, \neg P \vdash_{\text{ax}} Q$.*

Todistus. Väite seuraa oheisesti:

1.	$\neg P$	premissi
2.	$\neg P \to (\neg Q \to \neg P)$	(A1)
3.	$\neg Q \to \neg P$	MP: 1+2
4.	$(\neg Q \to \neg P) \to (P \to Q)$	(A3)
5.	$P \to Q$	MP: 3+4
6.	P	premissi
7.	Q	MP: 5+6

□

Lause 21 (Kompaktisuuslause)**.** *Olkoot Γ propositiojoukko, ja P propositio. Jos $\Gamma \vdash_{\text{ax}} P$, niin on olemassa äärellinen osajoukko $\Delta \subseteq \Gamma$, jolle $\Delta \vdash_{\text{ax}} P$.*

Todistus. Koska Modus Ponensia saa käyttää vain äärellisen monta kertaa johdossa $\Gamma \vdash_{\text{ax}} P$, niin vain äärellisen monta propositiota $Q \in \Gamma$ tulee käyttöön tässä johdossa. □

Seuraava lause tunnetaan myös **deduktiolauseena**.

Lause 22 (Herbrand 1930)**.** *Olkoot Γ propositiojoukko, ja P ja Q propositioita. Tällöin*

$$\Gamma \cup \{P\} \vdash_{\text{ax}} Q \iff \Gamma \vdash_{\text{ax}} P \to Q\,.$$

Todistus. ($\Rightarrow$) Oletetaan ensin, että $\Gamma \cup \{P\} \vdash_{\text{ax}} Q$. Olkoon $Q_1, \ldots, Q_n$ kaavan $Q = Q_n$ johto premisseistä $\Gamma \cup \{P\}$, missä kukin Q_i on joko aksiooma, joukossa $\Gamma \cup \{P\}$ tai saatu Modus Ponensilla kahdesta edeltävästä johdon propositioista. Todistetaan induktiolla lukuun i nähden, että $\Gamma \vdash_{\text{ax}} P \to Q_i$. Väite seuraa kun $i = n$.

1. Jos Q_i on aksiooma tai $Q_i \in \Gamma$, saadaan johto

1.	Q_i	premissi
2.	$Q_i \to (P \to Q_i)$	(A1)
3.	$P \to Q_i$	MP: 1+2

   Jos taas $Q_i = P$, saadaan $\vdash_{\text{ax}} P \to P$ esimerkistä 26, ja siten $\Gamma \vdash_{\text{ax}} P \to Q_i$.

2. Oletetaan, että $\Gamma \vdash_{\text{ax}} P \to Q_k$ kaikilla $k < i$, ja todistetaan se tapauksessa Q_i. Kohdan (1) mukaan voidaan olettaa, että Q_i on saatu Modus Ponensilla kahdesta edeltävästä termistä, sanokaamme Q_j ja Q_k, missä siis $Q_k = Q_j \to Q_i$. Induktio-oletuksen mukaan on
$$\Gamma \vdash_{\text{ax}} P \to Q_j \quad \text{ja} \quad \Gamma \vdash_{\text{ax}} P \to (Q_j \to Q_i)\,.$$

Tällöin on äärelliset osajoukot $\Delta_1, \Delta_2 \subseteq \Gamma$ saadaan johto

	$\Delta_1 \subseteq \Gamma$	premissit
	$\vdots$ johto kaavalle (1):	
1.	$P \to Q_j$	
	$\Delta_2 \subseteq \Gamma$	premissit
	$\vdots$ johto kaavalle (2):	
2.	$P \to (Q_j \to Q_i)$	
3.	$(P \to (Q_j \to Q_i)) \to ((P \to Q_j) \to (P \to Q_i))$	(A2)
4.	$(P \to Q_j) \to (P \to Q_i)$	MP: 2+3
5.	$P \to Q_i$	MP: 1+4

Tämä todistaa, että $\Delta_1 \cup \Delta_2 \vdash_{\text{ax}} P \to Q_i$ eli myös $\Gamma \vdash_{\text{ax}} P \to Q_i$, mistä väite seuraa.

($\Leftarrow$) Oletetaan, että $\Gamma \vdash_{\text{ax}} P \to Q$, ja olkoon $\Delta \subseteq \Gamma$ äärellinen osajoukko, jolle on $\Delta \vdash_{\text{ax}} P \to Q$. Uuden premissin P myötä, Modus Ponens tuottaa $\Delta \cup \{P\} \vdash_{\text{ax}} Q$, ja siten myös $\Gamma \cup \{P\} \vdash_{\text{ax}} Q$. □

Huomaa, että edeltävä todistus ei käytä lainkaan aksioomaa (A3).

Esim. 28. Lauseen 20 mukaan $P, \neg P \vdash_{\text{ax}} Q$ kaikille P ja Q. Näin ollen lauseesta 22 saadaan $\neg P \vdash_{\text{ax}} P \to Q$, ja toiseen kertaan soveltaen, $\vdash_{\text{ax}} \neg P \to (P \to Q)$. □

Esim. 29. (a) Osoitetaan, että $\vdash_{\text{ax}} \neg\neg P \to P$ käyttäen lausetta 22.

1.	$\neg\neg P$	premissi
2.	$\neg\neg P \to (\neg P \to \neg\neg\neg P)$	Esim 28
3.	$\neg P \to \neg\neg\neg P$	MP:1+2
4.	$(\neg P \to \neg\neg\neg P) \to (\neg\neg P \to P)$	(A3)
5.	$\neg\neg P \to P$	MP:3+4
6.	P	MP:1+5

Näin ollen $\neg\neg P \vdash_{\text{ax}} P$, ja siten $\vdash_{\text{ax}} \neg\neg P \to P$. Kohdassa (2) on käytetty Esimerkin 28 tulosta, eli (2) voidaan korvata pidemmällä johdolla, joka on esitetty Esimerkissä 28.

(b) Samoin $\vdash_{\text{ax}} P \to \neg\neg P$, minkä osoittaminen jää harjoitukseksi. □

Esim. 30. Osoitetaan, että seuraavat tulokset ovat voimassa.

$$P \to Q,\ Q \to R \vdash_{\text{ax}} P \to R \tag{a}$$

$$P \to (Q \to R),\ Q \vdash_{\text{ax}} P \to R \tag{b}$$

(a) Osoitetaan, että $P \to Q,\ Q \to R,\ P \vdash_{\text{ax}} R$, jolloin väite seuraa lauseesta 22.

1.	$P \to Q$	premissi
2.	$Q \to R$	premissi
3.	P	premissi
4.	Q	MP: 1+3
5.	R	MP: 2+4

(b) Osoitetaan, että $P \to (Q \to R),\ Q, P \vdash_{\text{ax}} R$, jolloin väite seuraa lauseesta 22.

1.	$P \to (Q \to R)$	premissi
2.	P	premissi
3.	$Q \to R$	MP: 1+2
4.	Q	premissi
5.	R	MP: 3+4

□

Ristiriidattomuus ja täydellisyys

Seuraavaksi osoitetaan, että "aksiomatiikka on täydellinen tulkintaan nähden."

Määr. 15. Olkoon Γ propositiojoukko.

- Γ on **ristiriitainen**, jos on olemassa propositio P, jolle $\Gamma \vdash_{\text{ax}} P$ ja $\Gamma \vdash_{\text{ax}} \neg P$; muutoin Γ on **ristiriidaton**.
- Γ on **täydellinen**, jos jokaiselle propositiolle P, joko $\Gamma \vdash_{\text{ax}} P$ tai $\Gamma \vdash_{\text{ax}} \neg P$.
- Γ on **teoria**, jos se on suljettu johtamiseen nähden, eli jokaiselle propositiolle P,

$$\Gamma \vdash_{\text{ax}} P \implies P \in \Gamma.$$

Lause 23. *Jos propositiojoukon Γ jokainen äärellinen osajoukko on ristiriidaton, niin myös Γ on ristiriidaton.*

Todistus. Tehdään vastaoletus, että Γ on ristiriitainen, jolloinka on propositio P, jolle $\Gamma \vdash_{\text{ax}} P$ ja $\Gamma \vdash_{\text{ax}} \neg P$. Kompaktisuuslauseen mukaan on joukon Γ äärelliset osajoukot Γ_1 ja Γ_2 niin, että $\Gamma_1 \vdash_{\text{ax}} P$ ja $\Gamma_2 \vdash_{\text{ax}} \neg P$. Mutta nyt $\Gamma_1 \cup \Gamma_2 \vdash_{\text{ax}} P$ ja $\Gamma_1 \cup \Gamma_2 \vdash_{\text{ax}} \neg P$, joten äärellinen osajoukko $\Gamma_1 \cup \Gamma_2$ olisikin ristiriitainen. Tämä todistaa väitteen. □

Lause 24 (Terveys)**.** *Jokainen teoreema on tautologia, eli*

$$\vdash_{\text{ax}} P \implies \models P.$$

Todistus. Todetaan ensin esimerkiksi totuustaulujen avulla, että kaikki aksioomat ovat tautologioita, ja sitten että Modus Ponens säilyttää tautologisuuden: jos $\models P$ ja $\models P \to Q$, niin $\models Q$. Näin ollen väite seuraa teoreeman määritelmästä. □

Toiseen suuntaan todistus on huomattavasti hankalampi.

Lemma. 25. *Jos $\Gamma \vdash_{\text{ax}} P$ ja $\Gamma \cup \{P\} \vdash_{\text{ax}} Q$, niin $\Gamma \vdash_{\text{ax}} Q$.*

Todistus. Olkoot $P_1, \ldots, P_n$ johto propositiolle $P = P_n$ premisseistä Γ, ja $P, Q_1, \ldots, Q_k$ johto propositiolle $Q = Q_k$ premisseistä $\Gamma \cup \{P\}$. Tällöin $P_1, P_2, \ldots, P_n, Q_1, Q_2, \ldots, Q_k$ on johto propositiolle Q premisseistä Γ. □

Lemma. 26. *Jos propositiojoukko Γ on ristiriitainen, niin $\Gamma \vdash_{\text{ax}} Q$ kaikille $Q \in$ Prop.*

Todistus. Oletetaan, että $\Gamma \vdash_{\text{ax}} P$ ja $\Gamma \vdash_{\text{ax}} \neg P$. Lauseen 20 mukaan $P, \neg P \vdash_{\text{ax}} Q$, jolloin myös $\Gamma \cup \{P, \neg P\} \vdash_{\text{ax}} Q$, mistä väite saadaan edeltävän lemman mukaan. □

Edeltävän tuloksen seurauksena saadaan

Lemma. 27. *Olkoon Γ propositiojoukko.*

(a) *Γ on ristiriidaton jos ja vain jos on olemassa propositio P niin, että $\Gamma \nvdash_{\text{ax}} P$.*

(b) *Jos $\Gamma \nvdash_{\text{ax}} P$, niin $\Gamma \cup \{\neg P\}$ on ristiriidaton.*

Todistus. Kohta (a) jääköön harjoitukseksi. Kohdassa (b) oletetaan, että $\Gamma \cup \{\neg P\}$ on ristiriitainen, ja olkoon Q jokin aksiooma. Tällöin

$$\begin{aligned}
& \Gamma \cup \{\neg P\} \vdash_{\text{ax}} \neg Q && \text{lause 26} \\
\Longrightarrow\ & \Gamma \vdash_{\text{ax}} \neg P \to \neg Q && \text{lause 22} \\
\Longrightarrow\ & \Gamma \vdash_{\text{ax}} Q \to P && \text{(A3)+MP} \\
\Longrightarrow\ & \Gamma \cup \{Q\} \vdash_{\text{ax}} P && \text{lause 22,}
\end{aligned}$$

mistä saadaan $\Gamma \vdash_{\text{ax}} P$, koska Q on aksiooma. □

Lemma. 28. *Propositiojoukko Γ on täydellinen ja ristiriidaton teoria jos ja vain jos on olemassa tulkinta v niin, että $\Gamma = \{P \mid v(P) = 1\}$.*

Todistus. (1) Oletetaan ensin, että $\Gamma = \{P \mid v(P) = 1\}$. Todetaan, että jokainen aksiooma R on tautologia, ja siten $R \in \Gamma$. Lisäksi Modus Ponens säilyttää totuusarvon 1, eli jos $v(P) = 1$ ja $v(P \to Q) = 1$, niin myös $v(Q) = 1$. Näin ollen jos $\Gamma \vdash_{\text{ax}} Q$, niin myös $v(Q) = 1$ eli $Q \in \Gamma$, ja siten Γ on teoria. Helposti todetaan, että Γ on ristiriidaton ja täydellinen.

(2) Oletetaan sitten, että Γ on täydellinen ja ristiriidaton teoria. Määritellään tulkinta $v\colon \text{PM} \to \{0,1\}$ oheisesti:

$$v(p) = 1 \iff p \in \Gamma \quad (\text{ kun } p \in \text{PM}).$$

Huomaa, että koska Γ on täydellinen ja ristiriidaton, joko $p \in \Gamma$ tai $\neg p \in \Gamma$ jokaiselle propositiokirjaimelle p. Todistetaan väite $\Gamma = \{P \mid v(P) = 1\}$ induktiivisesti.

(1) Kun $p \in \text{PM}$, niin $v(p) = 1$ jos ja vain jos $p \in \Gamma$, määritelmän mukaan.

(2) Olkoon $P = \neg Q$. Tällöin

$$\begin{aligned}
v(P) = 0 &\iff v(Q) = 1 && \\
&\iff Q \in \Gamma && \text{induktio-oletus} \\
&\iff P = \neg Q \notin \Gamma && \text{ristiriidattomuus / täydellisyys}
\end{aligned}$$

Siis $v(P) = 1$ jos ja vain jos $P \in \Gamma$.

(3) Olkoon $P = Q \to R$. Nyt

$$\begin{aligned}
v(P) = 0 &\iff v(Q) = 1 \text{ ja } v(R) = 0 && \\
&\iff Q \in \Gamma \text{ ja } R \notin \Gamma && \text{induktio-oletus} \\
&\iff P \notin \Gamma, &&
\end{aligned}$$

Missä viimeinen ekvivalenssi on voimassa, koskapa jos $Q \in \Gamma$, niin $Q \to R \in \Gamma$ jos ja vain jos $\Gamma \vdash_{\text{ax}} R$ (MP) ja siis $R \in \Gamma$, sillä Γ on teoria. □

Lemma. 29. *Olkoon P propositio, joka ei ole teoreema, eli $\nvdash_{\text{ax}} P$. Tällöin on olemassa täydellinen ja ristiriidaton teoria Γ niin, että $P \notin \Gamma$.*

Todistus. Olkoon $P_0, P_1, \ldots$ listaus kaikista propositioista. Tällainen listaus on mahdollinen, koska propositioita on numeroituva määrä. Määritellään $\Gamma_0 = \{\neg P\}$ ja kun $n \geq 0$:

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{P_n\} & \text{jos } \Gamma_n \cup \{P_n\} \text{ on ristiriidaton}, \\ \Gamma_n & \text{muutoin.} \end{cases}$$

Selvästi Γ_0 on ristiriidaton, sillä ehdosta $\nvdash_{\text{ax}} P$ seuraa, että $\{\neg P\}$ on ristiriidaton lemman 27 mukaan. Nyt $\Gamma_0 \subseteq \Gamma_1 \subseteq \ldots$ on nouseva jono ristiriidattomia propositiojoukkoja. Kompaktisuuslauseen mukaan niiden unioni

$$\Gamma = \bigcup_{n \geq 0} \Gamma_n$$

on myös ristiriidaton, sillä jokainen joukon Γ äärellinen osajoukko on jonkin joukon Γ_n äärellinen osajoukko.

Joukko Γ on myös täydellinen, sillä jos $\Gamma \nvdash_{\text{ax}} R$, niin $\Gamma \cup \{\neg R\}$ on ristiriidaton kuten lemma 27 kertoo. Mutta $\neg R = P_n$ jollain indeksillä n, ja siis $\Gamma_n \cup \{P_n\}$ on ristiriidaton, ja siten joukon Γ määrittelyn mukaan $\neg R \in \Gamma$. Lopuksi, on selvää, että Γ on teoria, sillä jos $\Gamma \vdash_{\text{ax}} R$, niin $\Gamma \cup \{R\}$ on ristiriidaton. (Jos $\Gamma \cup \{R\} \vdash_{\text{ax}} Q$ jollain Q, niin myös $\Gamma \vdash_{\text{ax}} Q$.) Siten $R \in \Gamma$ kuten edellä. $\square$

Lause 30 (Täydellisyyslause)**.** *Jokainen tautologia on todistuva, eli*

$$\models P \implies \vdash_{\text{ax}} P.$$

Näin ollen $\vdash_{\text{ax}} P \iff \models P$.

Todistus. Todistetaan väite kontrapositiolla. Oletetaan, että $\nvdash_{\text{ax}} P$. Lemman 29 mukaan on olemassa täydellinen ja ristiriidaton teoria Γ niin, että $P \notin \Gamma$. Lemma 28 sanoo, että on tulkinta v, jolle $Q \in \Gamma$ jos ja vain jos $v(Q) = 1$. Erityisesti, $v(P) = 0$, ja siten P on kumoutuva, eli se ei ole tautologia. Siis jos P on tautologia, on se teoreema.

Viimeinen väite saadaan yhdistämällä edeltävä lauseen 24 kanssa. $\square$

Lause 31 (Ristiriidattomuus)**.** *Jos $\vdash_{\text{ax}} P$, niin $\vdash_{\text{ax}} \neg P$ ei ole voimassa.*

Todistus. Tiedetään jo että jokainen teoreema on tautologia, joten vain toinen, P tai $\neg P$, voi olla teoreema. $\square$

B. Ensimmäisen kertaluvun logiikkaa

Tässä osiossa pyritään esittämään etupäässä matemaattisten rakenteiden teoriaa, johon tarvitaan propositiologiikkaa paljon voimakkaammat loogiset työkalut.

Matemaattinen rakenne (tai struktuuri) koostuu alkiojoukosta A ja sitä koskevista operaatioista. Tällainen rakenne on esimerkiksi *Abelin ryhmä* $(A,+,-,0)$, missä $+$ on operaatio $+\colon A\times A\to A$, joka yhdistää kaksi alkiota $a,b\in A$ yhdeksi alkioksi $a+b$ ja $-$ on operaatio $-\colon A\to A$, joka muuttaa alkion etumerkin, $0\in A$ on vakio (ryhmän nolla-alkio). Seuraavat ehdot tekevät tästä Abelin ryhmän: kaikilla $a,b,c\in A$,

$$
\begin{aligned}
&a+b=b+a,\\
&(a+b)+c=a+(b+c),\\
&0+x=x,\\
&-x+x=0.
\end{aligned}
$$

Kokonaisluvut muodostavat ryhmän yhteenlaskun suhteen, ja tällöin rakenne on $(\mathbb{Z},+,-,0)$ (mikä usein kirjoitetaan yksinkertaisemmin $(\mathbb{Z},+)$).

Toisaalta esimerkiksi *kunta* on rakenne $(K,\cdot,+,-,0,1)$, missä operaatiota $\cdot,+,-$ toteuttavat kuntaehdot, ja 0 ja 1 ovat vakioita. Esimerkiksi rationaaliluvut muodostavat kunnan $(\mathbb{Q},\cdot,+,-,0,1)$ tavanomaisten operaatioiden suhteen.

Propositiologiikan rakennusaineet ovat propositiomuuttujat, joista monimutkaisemmat propositiot kootaan konnektiivien avulla. Propositiomuuttujilla ei ole sisäistä rakennetta ja sikäli propositiologiikan ei ole tarpeeksi ilmaisuvoimainen kattamaan matemaattisten teorioiden – eikä myöskään arkilogiikan – formalisoinnin vaatimuksia. Erityisesti propositiologiikassa ei voida ilmaista, että jokin ominaisuus on voimassa joillekin tai kaikille yksilöille.

Esimerkiksi syllogismia

Kaikki ihmiset ovat kuolevaisia
Sokrates on ihminen
$\therefore$ *Sokrates on kuolevainen,*

ei voida formalisoida mielekkäällä tavalla propositiologiikan avulla vaikka päättelykaavio ilmeisestikin on oikea.

Ensimmäisen kertaluvun logiikka täydentää päättelyjä mahdollistamalla

- yksilösymbolit (kuten ‘Sokrates’, joka on sama sekä johtopäätöksessä ja premississä);
- yksilöiden ominaisuudet (kuten ‘kuolevainen’);
- ilmaisut yksilöiden välisille suhteille;
- ilmaisemisen, että jokin ominaisuus tai suhde koskee kaikkia yksilöitä tai, että on olemassa tietyn ominaisuuden omaava yksilö.

Edeltävä syllogismi saa seuraavan muodon:

$$
\begin{gathered}
\forall x(I(x)\to K(x))\\
I(s)\\
\therefore\ K(s),
\end{gathered}
$$

missä tulkinnat ovat $I\mapsto$ “Olla ihminen”, $K\mapsto$ “Olla kuolevainen”, $s\mapsto$ “Sokrates”.

Seuraavassa yllä esitetyt vaatimukset täyttävä yleisempi logiikka muotoillaan ajatellen lähinnä matematiikan tarpeita, minkä takia sallitaan myös funktiosymbolit.

1 Syntaksi

Ensimmäisen kertaluvun kielet

1. kertaluvun kielen aakkosto jaetaan kahteen osaan: loogiseen aakkostoon ja symboliaakkostoon, joista edellinen on kiinteä, eli sama kaikille rakenteille. Sensijaan, sovellusten ja esimerkkien takia, symboliaakkosto riippuu kulloinkin tarkasteltavista rakenteista, ja sitä tullaan kutsumaan lyhykäisesti **aakkostoksi**.

Määr. 16. Looginen aakkosto koostuu seuraavista symboleista:

- **(yksilö)muuttujat** $x_0, x_1, x_2, \ldots$, joiden joukkoa merkitään $X = \{x_0, x_1, \ldots\}$. Muuttujia merkitään (metakielessä) yleensä kirjaimin x, y, z;
- **konnektiivit** $\neg$, $\vee$ ja $\wedge$ (ja $\rightarrow$, $\leftrightarrow$ lyhennysmerkintöinä);
- **kvanttorit** $\forall$, $\exists$ (**universaali-** ja **eksistenssikvanttori**);
- **yhtäsuuruusmerkki** $=$; **sulkumerkit** (ja); **pilkku** , .

Määr. 17. Symboliaakkosto, eli **aakkosto**, koostuu kolmesta alkiovieraasta joukosta

$$S = Fun \cup Rel \cup Con,$$

missä

- Fun on **funktiosymbolien** joukko. Funktiosymboleina käytetään yleensä kirjaimia f, g, h, ja konkreettisissa sovelluksissa myös esimerkiksi $+$, $\cdot$, $*$, $\circ$.
- Rel on **relaatio-** eli **predikaattisymbolien** joukko. Relaatiosymboleina käytetään yleensä kirjaimia p, q, r, ja konkreettisissa sovelluksissa myös esimerkiksi $<$, $\leq$, $|$.
- Con on **vakiosymbolien** joukko. Vakiosymboleina käytetään yleensä kirjaimia c ja d, ja konkreettisissa tilanteissa myös esimerkiksi 0, 1, e.

Jokaisella funktio- ja relaatiosymbolilla on yksikäsitteisesti määrätty **paikkaluku**, joka on positiivinen kokonaisluku. Merkitään n-paikkaisten symbolien joukkoja vastaavasti kirjaimin Fun_n ja Rel_n, jolloin

$$Fun = \bigcup_{n>0} Fun_n \quad \text{ja} \quad Rel = \bigcup_{n>0} Rel_n .$$

Konkreettisissa esimerkeissä aakkosto S on yleensä äärellinen, ja S voidaan esittää jonona $S = (f_1, \ldots, f_n, r_1, \ldots, r_k, c_1, \ldots, c_m)$, missä $Fun = \{f_1, \ldots, f_n\}$, $Rel = \{r_1, \ldots, r_k\}$ ja $Con = \{c_1, \ldots, c_m\}$

Esim. 31. (1) Tavallisissa lukujärjestelmissä, kuten (kokonaislukujen ja luonnollisten lukujen) aritmetiikassa, aakkostona on

$$Ar = (+, *, \sigma, <, 0),$$

missä $+$, $*$ ja σ ovat 2-paikkaisia funktiosymboleja, $<$ on 2-paikkainen relaatiosymboli, ja 0 on vakiosymboli. (Tässä σ esittää seuraajafunktiota $n \mapsto n+1$.)

(2) Joukko-opin aakkosto koostuu yhdestä relaatiosymbolista $\in$.

(3) Ryhmäteoriassa tarvittava aakkosto koostuu yhdestä funktiosymbolista $\circ$ ja yhdestä vakiosymbolista e.

(4) Sukutaulujen 'teoriaa' varten tarvitaan aakkosto, jossa on kaksi 2-paikkaista relaatiosymbolia i ja ä, ja ehkäpä kaksi vakiosymbolia *adam* ja *eve*. $\square$

Ensimmäisen kertaluvun kielet koostuvat termeistä ja kaavoista, joilla on eri roolit: *Termit tullaan tulkitsemaan konkreettisten struktuurien alkioiksi, kun taas kaavat edustavat väitelauseita, jotka jokaisessa tulkinnassa ovat joko tosia tai epätosia.*

<u>Määr</u>. 18. Termit *yli* aakkoston S määritellään induktiivisesti:

(T1) jokainen muuttuja $x \in X$ ja vakiosymboli $c \in Con$ on termi;

(T2) $f(t_1, \ldots, t_m)$ on termi, kun f on m-paikkainen funktio ja $t_1, \ldots, t_m$ ovat termejä.

Termejä merkitään yleensä kirjaimin t ja s.

Huomaa, että termi on aina jonkun aakkoston S suhteen. Termissä ei esiinny konnektiiveja, ei kvanttoreita, eikä relaatiosymboleja.

<u>Esim</u>. 32. (1) Aritmetiikan aakkostossa Ar, termejä ovat esimerkiksi 0, $\sigma(0)$, $+(x, \sigma(0))$, $*(y, +(+(x,y), \sigma(0)))$ ja $\sigma(*(x,y))$. Huomaa, että termeissä ei esiinny relaatiosymbolia $<$.

Binääriset eli 2-paikkaiset funktiosymbolit kirjoitetaan usein käyttäen **infix-merkintää**, missä funktiosymboli kirjoitetaan operandien väliin. Niinpä esimerkiksi ylläoleva termi $t = *(y, +(+(x,y), \sigma(0)))$ saa tutumman näköisen muodon $y * ((x+y) + \sigma(0))$.

(2) Joukko-opissa termeinä ovat vain muuttujat, sillä joukko-opin aakkostossa ei ole funktiosymboleja eikä vakioita.

(3) Ryhmäteorian termejä ovat esimerkiksi e, $x \circ x$ ja $(x \circ e) \circ y$, missä on käytetty infix-merkintää. $\square$

<u>Määr</u>. 19. Jos t on termi, jonka muuttujat ovat joukossa $\{y_1, y_2, \ldots, y_n\}$, niin merkitään

$$t = t(y_1, y_2, \ldots, y_n).$$

Lisäksi, jos $t_1, t_2, \ldots, t_n$ ovat termejä, olkoon $t(t_1, t_2, \ldots, t_n)$ saatu termistä t korvaamalla jokainen muuttujan y_i esiintymä termillä t_i, kun $i = 1, 2, \ldots, n$.

<u>Lause</u> 32. *Olkoot $t = t(y_1, y_2, \ldots, y_n)$ ja $t_1, t_2, \ldots, t_n$ termejä aakkostossa S. Tällöin myös $t(t_1, t_2, \ldots, t_n)$ on termi.*

Todistus. Todistus on esimerkki induktiosta termien hierarkiseen rakenteeseen nähden.

(T1) Induktion lähtökohtana ovat termit, jotka ovat vakioita ja muuttujia. Jos $t = c$ on vakio, niin $t(t_1, \ldots, t_n) = c$. Jos taas $t = x$ on muuttuja, niin $t(t_1, \ldots, t_n) = x$, jos $x = y_i$ jollain i, ja $t(t_1, \ldots, t_n) = t$ muutoin.

(T2) Oletetaan, että f on m-paikkainen funktiosymboli, ja $t = f(s_1, s_2, \ldots, s_m)$, missä jokainen $s_i = s_i(y_1, \ldots, y_n)$ on termi, joille väite pätee induktio-oletuksen mukaan, ja siten jokainen $s_i(t_1, \ldots, t_n)$ on termi. Nyt

$$t(t_1, t_2, \ldots, t_n) = f(s_1(t_1, t_2, \ldots, t_n), s_2(t_1, t_2, \ldots, t_n), \ldots, s_m(t_1, t_2, \ldots, t_n)),$$

on termi induktio-oletuksen ja termien määrittelyn nojalla. $\square$

<u>Määr</u>. 20. Kaavat *yli* aakkoston S määritellään oheisesti:

(K1) jos r on n-paikkainen relaatiosymboli ja $t_1, \ldots, t_n$ termejä, niin $r(t_1, \ldots, t_n)$ on kaava;

(K2) jos s ja t ovat termejä, on $(s = t)$ kaava;

(K3) jos φ ja ψ ovat kaavoja, samoin ovat $(\neg\varphi)$, $(\varphi \wedge \psi)$ ja $(\varphi \vee \psi)$;

(K4) jos φ on kaava ja x on muuttuja, ovat $(\forall x\, \varphi)$ ja $(\exists x\, \varphi)$ kaavoja.

Huomaa, että kaava on aina jonkun aakkoston suhteen. Merkitään kaavoja yleensä pienillä kreikkalaisilla kirjaimilla φ, ψ, tai η. Usein kaavoja yksinkertaistetaan jättämällä pois sulkeita noudattaen samoja sääntöjä kuin propositiologiikassa. Lisäksi sovitaan, että molemmat kvanttorit sitovat voimakkaammin kuin konnektiivit.

Esim. 33. (1) Aakkostossa Ar kaavoja ovat esimerkiksi $x = 0$, $\forall x \neg(x * y < \sigma(y))$, ja $\forall x \exists y \exists z \exists k((x < k) \to y * y + z * z = k * k)$, missä x, y, z, k ovat muuttujia.

(2) Ilmaisu $\forall z \exists x\,(x \in y \wedge y \in z)$ on joukko-opillinen kaava.

(3) Ilmaisu $\forall x \exists y (x \circ y = e)$ on ryhmäteoreettinen kaava. □

Vapaat ja sidotut muuttujat

Määr. 21. Olkoon φ jokin kaava (yli aakkoston S).

- Sanotaan, että muuttujan x **esiintymä** kaavassa φ on **sidottu**, jos se on jossain muotoa $\forall x\,\psi$ tai $\exists x\,\psi$ olevassa osakaavassa, ja muutoin se on **vapaa esiintymä**.
- Sanotaan, että φ on **suljettu kaava**, jos siinä ei ole vapaita muuttujia. Vastaavasti, kaava on **avoin**, jos siinä ei esiinny lainkaan kvanttoreita.

Esim. 34. Olkoot $f \in Fun_2$, $r \in Rel_2$ ja $c \in Con$. Tällöin kaavassa

$$\varphi = \forall x\, r(x, c) \vee \exists y\,(f(x, y) = c)$$

muuttuja x esiintyy sekä sidottuna että vapaana. Esiintymä osakaavassa $\forall x\, r(x, c)$ on sidottu, mutta esiintymä osakaavassa $\exists y\,(f(x, y) = c)$ on vapaa. Kaava

$$\forall x \exists y (r(x, y) \vee (f(x, y) = c))$$

on suljettu. Kaava $f(c, c) = c$ on sekä suljettu että avoin. □

Määr. 22. Jos kaavan φ (aakkostossa S) vapaat muuttujat ovat joukossa $\{y_1, y_2, \ldots, y_n\}$, merkitään

$$\varphi = \varphi(y_1, y_2, \ldots, y_n).$$

Lisäksi, jos $t_1, t_2, \ldots, t_n$ ovat termejä, olkoon $\varphi(t_1, t_2, \ldots, t_n)$ saatu kaavasta φ korvaamalla jokainen muuttuja y_i termillä t_i, kun $i = 1, 2, \ldots, n$.

Vastaavasti kuin lauseen 32 todistuksessa, voidaan induktiivisesti todistaa seuraava tulos.

Lause 33. *Olkoot $\varphi = \varphi(y_1, y_2, \ldots, y_n)$ kaava ja $t_1, t_2, \ldots, t_n$ termejä aakkostossa S. Tällöin myös $\varphi(t_1, t_2, \ldots, t_n)$ on kaava.*

Todistus. Harjoitustehtävä. □

Ensimmäisen kertaluvun teorioita

Määr. 23. Ensimmäisen kertaluvun teoria (1.kl teoria) $\mathscr{T}$ koostuu aakkostosta S ja suljettujen kaavojen joukosta. Näitä kaavoja kutsutaan teorian **aksioomeiksi**.

Esim. 35. Ryhmiä koskeva 1.kl teorian $\mathscr{G}$ aakkostona on $(\circ, e)$, missä $\circ$ on 2-paikkainen funktiosymboli ja e on vakiosymboli. Teorian $\mathscr{G}$ aksioomat ovat seuraavat suljetut kaavat:

$$\begin{aligned}
&\forall x \forall y \forall z\,(x \circ (y \circ z) = (x \circ y) \circ z) \\
&\forall x\,(x \circ e = x \;\wedge\; e \circ x = x) \\
&\forall x \exists y\,(x \circ y = e \;\wedge\; y \circ x = e)\,.
\end{aligned}$$

□

Esim. 36. **Ekvivalenssirelaatioiden teorian** $\mathscr{E}$ aakkostossa on yksi 2-paikkainen relaatio $\approx$. Sen aksioomat ovat

$$\begin{aligned}
&\forall x\,(x \approx x)\\
&\forall x \forall y\,(x \approx y \rightarrow y \approx x)\\
&\forall x \forall y \forall z\,((x \approx y \wedge y \approx z) \rightarrow x \approx z)\,.
\end{aligned}$$

□

Esim. 37. **Lukuteorian** $\mathscr{L}$ aakkostona on Ar. Sen aksioomat ovat seuraavat:

$$\begin{aligned}
&\forall x\,(\neg(\sigma(x) = 0))\\
&\forall x \forall y\,(\sigma(x) = \sigma(y) \rightarrow x = y)\\
&\forall x\,(x + 0 = x)\\
&\forall x \forall y\,(x + \sigma(y) = \sigma(x + y))\\
&\forall x\,(x * 0 = 0)\\
&\forall x \forall y\,(x * \sigma(y) = (x * y) + x)\\
&\forall x\,(\neg(x < 0))\\
&\forall x \forall y\,(x < \sigma(y) \leftrightarrow (x < y \ \vee \ x = y))\\
&\forall x \forall y\,(x < y \ \vee \ x = y \ \vee y < x)
\end{aligned}$$

□

Esim. 38. **Joukko-opin teoriassa** (Zermelo-Fraenkel joukko-oppi) on kaikkiaan yhdeksän aksioomaa, joita emme tässä luettele. Aksioomien joukossa ovat mm. seuraavat suljetut kaavat:

$$\exists x\,(x = x) \quad \text{ja} \quad \forall x \forall y\,(\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

□

2 Semantiikkaa

Ensimmäisen kertaluvun logiikan semantiikka on luonnollisesti mutkikkaampaa kuin propositiologiikan semantiikka, sillä konnektiivien lisäksi on tulkittava myös sekä kvanttorit että aakkoston funktio-, relaatio- ja vakiosymbolit. Lisäksi on vielä sanottava mitä alkioita muuttujat edustavat. Niinpä kaavojen tulkinta totuustaulujen avulla ei ole hyvä ratkaisu, sillä esimerkiksi kaavan $x > 7$ totuuden tarkistaminen vaatii äärettömän monta totuustaulun riviä, kun x käy läpi luonnolliset luvut.

Struktuurit

Määr. 24. **Struktuuri** $\mathscr{A}$ on järjestetty pari (A, S), missä S on aakkosto ja A on epätyhjä joukko (struktuurin $\mathscr{A}$ **universumi** tai **alkiojoukko**), ja jokaiseen

- funktiosymboliin $f \in Fun_m$ on liitetty m-paikkainen funktio $f^{\mathscr{A}} : A^m \rightarrow A$,
- relaatiosymboliin $r \in Rel_n$ on liitetty n-paikkainen relaatio $r^{\mathscr{A}} \subseteq A^n$ ja
- vakiosymboliin $c \in Con$ on liitetty alkio $c^{\mathscr{A}} \in A$,
- symboli $=$ tulkitaan aina alkioiden yhtäsuuruudeksi.

<u>Esim</u>. 39. Olkoon $Ar = (+, *, \sigma, <, 0)$ on aritmetiikan aakkosto.

(1) Aakkoston Ar eräs struktuuri on

$$\mathscr{N} = (\mathbb{N}, +, \cdot, \sigma, <, 0),$$

missä universumina on luonnollisten lukujen joukko $\mathbb{N} = \{0, 1, \dots\}$. Tässä $+^{\mathscr{N}} = +$ on tavallinen yhteenlasku, $*^{\mathscr{N}} = \cdot$ on kertolasku, $\sigma^{\mathscr{N}}$ on **seuraajafunktio** $n \mapsto n+1$, $<^{\mathscr{N}} = <$ on pienemmyysrelaatio ja $0^{\mathscr{N}} = 0$.

(2) Vastaavasti $\mathscr{Z}$ ja $\mathscr{R}$ ovat struktuureja, joiden universumeina ovat kokonaislukujen joukko $\mathbb{Z}$ reaalilukujen joukko ja $\mathbb{R}$. □

Tulkinnat

Tarkastellaan struktuuria $\mathscr{A} = (A, S)$, ja sen termiä t, jonka muuttujat kuuluvat joukkoon $\{y_1, \dots, y_n\}$, eli $t = t(y_1, \dots, y_n)$. Kun $a_1, a_2, \dots, a_n \in A$ ovat universumin A alkioita, on

$$t^{\mathscr{A}}(a_1, a_2, \dots, a_n) \in A$$

saatu termistä t korvaamalla jokainen esiintymä y_i alkiolla a_i.

Termin arvo on siis aina yksikäsitteinen määrittelyjoukon A alkio.

Jokaisen (suljetun) kaavan totuus riippuu annetusta struktuurista, eli symbolien ja syntaksin tulkinnoista.

<u>Määr</u>. 25. (1. kertaluvun) **tulkinta** on järjestetty pari $I = (\mathscr{A}, \alpha)$, joka koostuu struktuurista (A, S) ja (muuttujien) **arvotuksesta** $\alpha \colon X \to A$. Termin t **arvo** $t^{\mathscr{A}}[\alpha]$ määritellään seuraavasti: kun $t = t(y_1, y_2, \dots, y_n)$, niin

$$t^{\mathscr{A}}[\alpha] = t^{\mathscr{A}}(a_1, a_2, \dots, a_n) \quad (\in A),$$

missä $a_i = \alpha(y_i)$ kullekin i.

Yhtäsuuruussymboli tulkitaan aina alkioiden yhtäsuuruutena:

$$t = s \implies t^{\mathscr{A}} = s^{\mathscr{A}}.$$

Termien arvot määräytyvät rakenteellisella induktiolla:

- jos $t = x \in X$, niin $t^{\mathscr{A}}[\alpha] = \alpha(x)$;
- jos $t = c \in Con$, niin $t^{\mathscr{A}}[\alpha] = c^{\mathscr{A}}$;
- jos $t = f(t_1, \dots, t_m)$, niin $t^{\mathscr{A}}[\alpha] = f^{\mathscr{A}}(t_1^{\mathscr{A}}[\alpha], \dots, t_m^{\mathscr{A}}[\alpha])$.

Seuraavaksi tarkastellaan 1. kertaluvun kaavojen totuusarvoja. Tätä varten otetaan käyttöön merkintä: jos $I = (\mathscr{A}, \alpha)$ on tulkinta, $a_1, a_2, \dots, a_n \in A$ ja $y_1, y_2, \dots, y_n \in X$, niin

$$I[a_1/y_1, \dots, a_n/y_n] = (\mathscr{A}, \alpha')$$

on tulkinta, missä

$$\alpha'(y) = \begin{cases} a_i & \text{jos } y = y_i \ (i = 1, 2, \dots, n), \\ \alpha(y) & \text{jos } y \notin \{y_1, y_2, \dots, y_n\}. \end{cases}$$

<u>Määr</u>. 26. Kaavojen totuusarvot tulkinnassa $I = (\mathscr{A}, \alpha)$ määritellään rekursiivisesti. Merkintä $I \models \varphi$ tarkoittaa, että kaava φ on **tosi tulkinnassa** I. Olkoot r relaatiosymboli, s ja t termejä, ja φ ja ψ kaavoja:

$$
\begin{array}{lcl}
I \models r(t_1,\dots,t_n) & \iff & r^{\mathscr{A}}(I(t_1),\dots,I(t_n)) \text{ on voimassa} \\
I \models s = t & \iff & I(s) = t^{\mathscr{A}}[\alpha] \\
I \models \varphi \vee \psi & \iff & I \models \varphi \text{ tai } I \models \psi \\
I \models \varphi \wedge \psi & \iff & I \models \varphi \text{ ja } I \models \psi \\
I \models \neg\varphi & \iff & I \not\models \varphi \\
I \models \forall x\,\varphi & \iff & I[a/x] \models \varphi \text{ kaikilla arvoilla } a \in A \\
I \models \exists x\,\varphi & \iff & I[a/x] \models \varphi \text{ jollakin arvolla } a \in A
\end{array}
$$

Jos $I \models \varphi$, sanotaan, että φ on **tosi tulkinnassa** I tai, että I on kaavan φ **malli**. Merkintä $I \not\models \varphi$ tarkoittaa, että φ on **epätosi tulkinnassa** I. Sanotaan myös, että tulkinta $I = (\mathscr{A}, \alpha)$ on kaavajoukon Γ **malli** tai että I **toteuttaa** kaavajoukon Γ, jos $I \models \varphi$ aina, kun $\varphi \in \Gamma$. Tämä merkitään $I \models \Gamma$.

__Esim__. **40.** Ar-kaava $\exists x(x < y)$ on tosi tulkinnassa $I = (\mathscr{N}, \alpha)$ tarkalleen silloin, kun muuttujien arvotus $\alpha \colon X \to \mathbb{N}$ toteuttaa ehdon $0 < \alpha(y)$, sillä

$$
\begin{aligned}
I \models \exists x(x < y) &\iff \text{jollakin } a \in \mathbb{N} : I[a/x] \models x < y \\
&\iff \text{jollakin } a \in \mathbb{N} : a < \alpha(y) \\
&\iff 0 < \alpha(y).
\end{aligned}
$$

□

Seuraavan lemman mukaan toteutuvuus $I \models \varphi$ arvotuksen α osalta riippuu vain sen kaavan φ vapaille muuttujille antamista arvoista. Todistuksen voi helposti muotoilla induktiolla.

__Lemma__. **34.** *Olkoot $I_1 = (\mathscr{A} = \alpha)$ ja $I_2 = (\mathscr{A}, \beta)$ kaksi tulkintaa samalle struktuurille $\mathscr{A}$. Jos φ on kaava, jolle $\alpha(x) = \beta(x)$ aina, kun x on vapaa kaavassa φ, niin*

$$I_1 \models \varphi \iff I_2 \models \varphi\,.$$

Erityisesti jos φ on suljettu, on sen totuusarvo tulkinnassa $I = (\mathscr{A}, \alpha)$ riippumaton muuttujien arvotuksesta α.

Jos φ on suljettu kaava ja $I \models \varphi$, voidaan kirjoittaa $\mathscr{A} \models \varphi$. Tällöin φ on **tosi** struktuurissa $\mathscr{A}$ ja $\mathscr{A}$ on kaavan φ **malli**. Nämä sanonnat ulotetaan luonnollisella tavalla koskemaan myös suljettujen kaavojen joukkoja. Jos struktuuri $\mathscr{A}$ on suljettujen kaavojen joukon Γ malli, kirjoitetaan $\mathscr{A} \models \Gamma$.

__Esim__. **41.** Konnektiivi $\to$ määritellään kaavoille kuten propositiologiikassa:

$$I \models \varphi \to \psi \iff I \models \neg\varphi \ \text{ tai } I \models \psi\,.$$

Esimerkiksi suljettu Ar-kaava $\forall x \forall y(x < y \to \exists z(x < z \wedge z < y))$ on tosi struktuurissa $\mathscr{R}$, mutta epätosi struktuurissa $\mathscr{N}$. □

Otetaan vielä käyttöön seuraavat määritelmään 26 liittyvät tärkeät käsitteet.

__Määr__. **27.** Tarkastellaan S aakkosto. Sanotaan, että sen kaava φ on

- **loogisesti tosi**, merkitään $\models \varphi$, jos se on tosi kaikissa tulkinnoissa;
- **toteutuva**, jos sillä on ainakin yksi malli;
- **kumoutuva**, jos se on epätosi ainakin yhdessä tulkinnassa;

- **toteutumaton**, jos se on epätosi kaikissa tulkinnoissa.

Vastaavasti kaavajoukko on **toteutuva**, jos sillä on malli; muutoin se on **toteutumaton**.

Esim. 42. Suljettu *Ar*-kaava

$$\forall x((0 < x) \to \exists y_1 \exists y_2 \exists y_3 \exists y_4 (x = y_1 * y_1 + y_2 * y_2 + y_3 * y_3 + y_4 * y_4)),$$

on toteutuva, sillä se on tosi aritmetiikassa: jokainen positiivinen luku voidaan ilmaista neljän neliön summana. □

Huom. *Luonnollisten lukujen teoria $\mathscr{N}$ on algoritmisesti ratkeamaton*, eli ei ole olemassa algoritmia, joka määräisi kullekin suljetulle kaavalle φ, onko $\mathscr{N} \models \varphi$ vai $\mathscr{N} \not\models \varphi$.

3 Looginen seuraus ja ekvivalenssi

Looginen seuraus

Loogisen seurauksen käsitteen määrittely perustuu taas malleihin.

Määr. 28. Olkoon S aakkosto. Sanotaan, että sen kaava φ on kaavajoukon Γ **looginen seuraus**, merkitään $\Gamma \models \varphi$, jos jokainen joukon Γ malli on myös kaavan φ malli. Jos $\Gamma = \{\psi_1, \dots, \psi_n\}$ on äärellinen, niin kirjoitetaan yleensä $\psi_1, \dots, \psi_n \models \varphi$. Vastaavasti kaavajoukko Δ on kaavajoukon Γ **looginen seuraus**, mikä merkitään $\Gamma \models \Delta$, jos jokainen joukon Γ malli on joukon Δ malli.

Määr. 29. Aakkoston S kaavat φ ja ψ ovat **loogisesti ekvivalentit**, merkitään $\varphi \equiv \psi$, jos niillä on tarkalleen samat mallit. Vastaavasti ovat kaksi kaavajoukkoa Γ ja Δ keskenään **loogisesti ekvivalentit**, ja kirjoitetaan $\Gamma \equiv \Delta$, jos niillä on samat mallit.

Huomattakoon, että kun kyse on pelkästään suljetuista kaavoista (kuten 1.kl teorioiden yhteydessä), riittää ehdon $\Gamma \models \Delta$ toteamiseen tarkastella struktuureja, joissa joukon Γ lauseet ovat tosia.

Aivan kuten propositiologiikassakin, relaatiota $\models$ voidaan käyttää päättelysääntöjen formalisoimiseen ja niiden terveyden tutkimiseen.

Esim. 43. Jos otetaan käyttöön predikaatit $i(x) =$ ”x on ihminen” ja $k(x) =$ ”x on kuolevainen”, sekä vakion c (Sokrates), voidaan esimerkin

Kaikki ihmiset ovat kuolevaisia
Sokrates on ihminen
$\therefore$ *Sokrates on kuolevainen*

avulla esitetty päättelysääntö kirjoittaa yleisenä formaalisena päättelysääntönä:
jos $\forall x(i(x) \to k(x))$ ja $i(c)$, niin myös $k(c)$. Hieman formaalisemmin

$$\forall x(i(x) \to k(x)), i(c) \models k(c).$$

□

Jonkin epäterveen päättelyn virheellisyys voidaan tietysti myös todistaa täsmällisesti formalisoimalla ensin ko. päättely loogisena seurausrelaationa.

<u>Esim</u>. 44. Olkoot p,q ja r 1-paikkaisia relaatiosymboleja aakkostossa S, ja olkoot

$$\begin{aligned}\varphi_1 &= \forall x(p(x) \to \neg q(x))\,,\\ \varphi_2 &= \forall x(r(x) \to p(x))\,,\\ \psi &= \forall x(r(x) \to \neg q(x))\,.\end{aligned}$$

Osoitetaan, että ψ on kaavojen φ_1 ja φ_2 looginen seuraus, eli $\varphi_1, \varphi_2 \models \psi$. Koska kyseiset kaavat ovat S-lauseita, riittää tarkastella struktuureja ilman muuttujien tulkintoja α. Oletetaan, että $\mathscr{A} = (A,S)$ on struktuuri, missä $\mathscr{A} \models \varphi_1$ ja $\mathscr{A} \models \varphi_2$, mutta $\mathscr{A} \not\models \psi$.

Jälkimmäisestä seuraa, että on olemassa alkio $c \in A$, jolle $r^{\mathscr{A}}(c) \to \neg q^{\mathscr{A}}(c)$ ei ole tosi, ja siten $r^{\mathscr{A}}(c)$ on tosi, mutta $\neg q^{\mathscr{A}}(c)$ ei ole, ja siis $q^{\mathscr{A}}(c)$ on tosi.

Koskapa $r^{\mathscr{A}}(c)$ on tosi ja $\mathscr{A} \models \varphi_2 = (\forall x)(r(x) \to p(x))$, välttämättä myös $p^{\mathscr{A}}(c)$ on tosi. Nyt ehdosta $\mathscr{A} \models \varphi_1 = (\forall x)(p(x) \to \neg q(x))$ seuraa, että $\neg q^{\mathscr{A}}(c)$ on tosi, mikä on ristiriita. Näin väite on todistettu. □

Seuraavat huomiot todistetaan kuten vastaavat väitteet propositiologiikassa.

<u>Lemma</u>. 35. *Olkoot φ ja ψ kaavoja aakkostossa S ja Γ on jokin kaavajoukko. Tällöin*

(a) $\Gamma \models \varphi \iff \Gamma \cup \{\neg\varphi\}$ *on toteutumaton, ja*

(b) $\Gamma \cup \{\varphi\} \models \psi \iff \Gamma \models \varphi \to \psi$.

(c) $\Gamma \models \varphi \to \psi$ *ja* $\Gamma \models \psi \implies \Gamma \models \psi$.

Kohta (b) on *Modus Ponens* ja kohdan (c) mukaan on $\varphi \models \psi \Leftrightarrow\, \models \varphi \to \psi$.

<u>Lemma</u>. 36. *Olkoot φ ja ψ kaavoja ja Γ ja Δ ovat kaavojen joukkoja yli aakkoston S. Tällöin*

(a) $\varphi \equiv \psi \iff\, \models \varphi \leftrightarrow \psi$.

(b) $\varphi \equiv \psi \iff \varphi \models \psi$ *ja* $\psi \models \varphi$.

(c) $\Gamma \equiv \Delta \iff \Gamma \models \Delta$ *ja* $\Delta \models \Gamma$.

Todistus. Harjoitustehtävä. (Jokainen väite seuraa määritelmästä.) □

Koska konnektiivit tulkitaan samoin kuin propositiologiikassa, ovat kaikki propositiologiikan yleiset ekvivalenssit voimassa myös predikaattilogiikassa. Täten on esimerkiksi kaikille kaavoille φ ja ψ voimassa $\varphi \vee \varphi \equiv \varphi$, $\varphi \wedge \psi \equiv \psi \wedge \varphi$, $\varphi \vee \psi \equiv \neg\varphi \to \psi$ jne. Se, että φ ja ψ nyt ovat kaavoja eivätkä propositioita, ei vaikuta asiaan, sillä vain niiden totuusarvoilla on merkitystä.

<u>Lause</u> 37. *Olkoot φ kaava sekä x ja y muuttujia. Tällöin*
(a) $\forall x \forall y\, \varphi \equiv \forall y \forall x\, \varphi$ *ja* $\exists x \exists y\, \varphi \equiv \exists y \exists x\, \varphi$.
(b) $\neg\forall x\, \varphi \equiv \exists x \neg\varphi$ *ja* $\neg\exists x\, \varphi \equiv \forall x \neg\varphi$.
(c) $\forall x(\varphi \wedge \psi) \equiv \forall x\, \varphi \wedge \forall x\, \psi$ *ja* $\exists x(\varphi \vee \psi) \equiv \exists x\, \varphi \vee \exists x\, \psi$.

Todistus. (a) Olkoon $I = (\mathscr{A}, \alpha)$ tulkinta, missä $\mathscr{A} = (A,S)$. Tällöin

$$\begin{aligned}I \models \forall x \forall y\, \varphi &\iff \text{kaikilla } a \in A : I[a/x] \models \forall y\, \varphi\\ &\iff \text{kaikilla } a \in A,\ \text{kaikilla } b \in A : I[a/x, b/y] \models \varphi\\ &\iff \text{kaikilla } b \in A,\ \text{kaikilla } a \in A : I[a/x, b/y] \models \varphi\\ &\iff \text{kaikilla } b \in A : I[b/y] \models \forall x\, \varphi\\ &\iff I \models \forall y \forall x\, \varphi,\end{aligned}$$

mistä ensimmäinen ekvivalenssi seuraa. Toinen väite voidaan todistaa aivan vastaavasti.

(b) Todistetaan tapauksen ensimmäinen väite; toinen jää harjoitukseksi. Olkoon $I = (\mathscr{A}, \alpha)$ jokin tulkinta. Tällöin

$$\begin{aligned} I \models \neg\forall x\,\varphi &\iff I \not\models \forall x\,\varphi \\ &\iff \text{jollakin } a \in A : I[a/x] \not\models \varphi \\ &\iff \text{jollakin } a \in A : I[a/x] \models \neg\varphi \\ &\iff I \models \exists x \neg\varphi. \end{aligned}$$

(c) Todistetaan ensimmäinen tapaus; toinen on harjoitus. Jos $I = (\mathscr{A}, \alpha)$ on tulkinta, niin

$$\begin{aligned} I \models \forall x(\varphi \wedge \psi) &\iff \text{kaikilla } a \in A : I[a/x] \models \varphi \wedge \psi \\ &\iff \text{kaikilla } a \in A : I[a/x] \models \varphi \text{ ja } I[a/x] \models \psi \\ &\iff \text{kaikilla } a \in A : I[a/x] \models \varphi \text{ ja kaikilla } a \in A : I[a/x] \models \psi \\ &\iff I \models \forall x\,\varphi \text{ ja } I \models \forall x\,\psi \\ &\iff I \models \forall x\,\varphi \wedge \forall x\,\psi\,. \end{aligned}$$

□

Se, että jokin ekvivalenssilaki ei ole yleisesti voimassa osoitetaan vastaesimerkillä.

<u>Esim</u>. 45. (1) Yleisesti ottaen $\forall x(\varphi \vee \psi) \not\equiv \forall x\,\varphi \vee \forall x\,\psi$. Tämä nähdään esimerkiksi valitsemalla $S = Ar$, ja siinä φ olkoon $(0 < x)$ ja ψ olkoon $(0 = x)$. Tällöin

$$\mathscr{N} \models \forall x((0 < x) \vee (0 = x))\,,$$

mutta

$$\mathscr{N} \not\models \forall x(0 < x) \vee \forall x(0 = x)\,.$$

Samoilla valinnoilla voidaan todeta myös, että $\exists x(\varphi \wedge \psi) \not\equiv \exists x\,\varphi \wedge \exists x\,\psi$.

(2) Kahden erityyppisen kvanttorin järjestystä ei yleensä voi vaihtaa. Jos valitaan $S = Ar$, niin ilmeisestikin $\forall x \exists y(x < y) \not\equiv \exists y \forall x(x < y)$. □

<u>Esim</u>. 46. Vaikka yleensä onkin $\forall x(\varphi \vee \psi) \not\equiv \forall x\,\varphi \vee \forall x\,\psi$, on kuitenkin

$$\forall x\,\varphi \vee \forall x\,\psi \models \forall x(\varphi \vee \psi)$$

aina voimassa. Jos nimittäin $I = (\mathscr{A}, \alpha)$ on tulkinta, niin

$$\begin{aligned} I \models \forall x\,\varphi \vee \forall x\,\psi \quad &\iff \quad I \models \forall x\,\varphi \text{ tai } I \models \forall x\,\psi \\ &\iff \quad \text{kaikilla } a \in A : I[a/x] \models \varphi \text{ tai kaikilla } a \in A : I[a/x] \models \psi \\ &\implies \quad \text{kaikilla } a \in A : I[a/x] \models \varphi \vee \psi \\ &\iff \quad I \models \forall x(\varphi \vee \psi). \end{aligned}$$

□

Ensimmäisen kertaluvun ominaisuudet

Tarkastellaan nyt lyhykäisesti joidenkin matemaattisten käsitteiden formalisointi 1. kertaluvun logiikassa.

Määr. 30. Struktuurien perhe **K** on **aksiomatisoituva** (tai **elementaarinen**), jos on olemassa suljettujen kaavojen joukko Γ niin, että

$$\mathbf{K} = \{\mathscr{A} \mid \mathscr{A} \models \Gamma\}.$$

Tällöin Γ **määrittelee** (tai **aksiomatisoi**) luokan **K** ja, Γ on perheen **K aksioomajoukko**. Jos **K** voidaan määritellä äärellisellä kaavajoukolla, on se **äärellisesti aksiomatisoituva**.

Struktuureja koskeva ominaisuus Ω on **elementaarinen** (tai **1. kertaluvun ominaisuus**) luokassa **K**, jos on olemassa sellainen suljettujen kaavojen joukko Δ, että perheeseen **K** kuuluvalla struktuurilla $\mathscr{A}$ on ominaisuus Ω jos ja vain jos $\mathscr{A} \models \Delta$.

Monet tunnetut algebraluokat, kuten ryhmien, renkaiden tai Boolen algebrojen luokat, määritellään identiteeteillä, joista kukin voidaan kirjoittaa muotoa

$$\forall x_1 \cdots \forall x_n (s(x_1, \dots, x_n) = t(x_1, \dots, x_n))$$

olevana kaavana (kunhan aakkosto S sisältää termien s ja t funktio- ja vakiosymbolit). Näin ollen nämä algebraluokat ovat (äärellisesti) aksiomatisoituvia määritelmiensä nojalla.

Lause 38. *Jokainen äärellisesti aksiomatisoituva struktuurien luokka voidaan määritellä yhdellä suljetulla kaavalla.*

Todistus. Todetaan, että jos $\Gamma = \{\varphi_1, \dots, \varphi_n\}$ on äärellinen joukko, niin

$$\mathscr{A} \models \Gamma \iff \mathscr{A} \models \varphi_1 \wedge \ldots \wedge \varphi_n$$

kullakin $\mathscr{A}$. $\square$

Esim. 47. Ryhmiä koskevan esimerkin 35 mukaan ryhmät muodostavat aksiomatisoituvan struktuurien luokan. Kommutatiivisuus on elementaarinen ominaisuus (ryhmien luokassa), sillä se voidaan määritellä kaavalla $\forall x \forall y (x \circ y = y \circ x)$. $\square$

Esim. 48. **Graafiteorian** aakkosto koostuu yhdestä 2-paikkaisesta relaatiosta $\sim$. Tällöin jos $x \sim y$, niin x ja y ovat **vierekkäisiä**. (Graafien mallissa xy on tällöin **viiva**, ja se voidaa piirtää sellaisena.) Nyt **graafien luokka** koostuu struktuureista G, joille seuraavat aksioomat ovat voimassa:

$$\forall x \forall y (x \sim y \rightarrow y \sim x) \tag{G1}$$

$$\forall x \neg (x \sim x) \tag{G2}$$

Seuraava kaava ilmaisee ominaisuuden, että graafissa G ei ole 'kolmioita'

$$\forall x \forall y \forall z \big(((x \sim y) \wedge (y \sim z)) \rightarrow ((x = z) \vee \neg (x \sim z)) \big) .$$

Sanotaan, että graafi G on **yhtenäinen**, jos jokainen sen pari (u, v), missä $u \neq v$, on yhdistetty jonolla viivoja $u = u_0 \sim u_1 \sim \ldots \sim u_n = v$. Ominaisuus "graafi G on yhtenäinen" *ei ole elementaarinen kertaluvun ominaisuus.* Tämä seuraa 1. kertaluvun logiikan kompaktisuuslauseesta. $\square$

Esim. 49. Olkoon $n \geq 1$, ja tarkastellaan seuraavia elementaarinen ominaisuuksia.

- Struktuurissa on enintään n alkiota. Tämä voidaan ilmaista suljetulla kaavalla

$$\varphi_{\leq n} = \forall x_0 \cdots \forall x_n ((x_0 = x_1) \vee \cdots \vee (x_0 = x_n) \vee \cdots \vee (x_{n-1} = x_n)).$$

  Siis $\mathscr{A} \models \varphi_{\leq n} \iff |A| \leq n$.

- Struktuurissa on vähintään n alkiota. Tämä voidaan ilmaista suljetulla kaavalla

$$\varphi_{\geq n} = \exists x_1 \cdots \exists x_n (\neg(x_1 = x_2) \wedge \cdots \wedge \neg(x_1 = x_n) \wedge \cdots \wedge \neg(x_{n-1} = x_n)).$$

  Siis $\mathscr{A} \models \varphi_{\geq n} \iff |A| \geq n$.

- Struktuurissa on tarkalleen n alkiota. Tämä voidaan ilmaista suljetulla kaavalla

$$\varphi_{=n} = \varphi_{\leq n} \wedge \varphi_{\geq n}.$$

  Siis $\mathscr{A} \models \varphi_{=n} \iff |A| = n$.

Koska näissä lauseissa esiintyy vain loogisen aakkoston symboleja, ovat ‘enintään n’, ‘vähintään n’ tai ‘tarkalleen n’ alkiota sisältävien struktuurien luokat äärellisesti aksiomatisoituvia.

Kaavajoukko $\Phi_\infty = \{\varphi_{\geq n} \mid n \geq 1\}$ määrittelee äärettömien struktuurien luokan, joten tämä on aksiomatisoituva. Äärettömyys on siis elementaarinen ominaisuus. Tästä seuraa myös, että äärettömien ryhmien luokka on aksiomatisoituva. Äärettömien struktuurien luokka ei kuitenkaan ole äärellisesti aksiomatisoituva. Voidaan myös osoittaa, että äärellisten struktuurien luokka ei ole edes aksiomatisoituva. □

Määr. 31. Annettu suljettujen kaavojen joukko Γ on **riippumaton**, jos mikään sen kaavoista ei ole sen muiden kaavojen looginen seuraus.

Ilmeisestikin struktuuriluokan **K** aksioomajoukko Γ on riippumaton, jos mikään sen aito osajoukko ei määrittele luokkaa **K**. Kaavajoukon Γ riippumattomuus voidaan osoittaa konstruoimalla kutakin joukon Γ kaavaa φ kohti joukon $\Gamma \setminus \{\varphi\}$ malli, jossa φ ei ole voimassa.

Esim. 50. Ekvivalenssirelaatiot muodostavat aksiomatisoituvan struktuuriluokan esimerkin 36 mukaan. Helpohkosti osoitetaan myös, että tässä esitetty aksioomajoukko on riippumaton. Esimerkiksi $\varphi_1, \varphi_3 \not\models \varphi_2$, nähdään tarkastelemalla struktuuria $\mathscr{A} = (\{a,b\}, \rho)$, missä relaationa on $\rho^{\mathscr{A}} = \{(a,a),(b,b),(a,b)\}$. □

Tarkastellaan vielä toista esimerkkiä äärellisesti aksiomatisoituvasta relaatioiden struktuurien luokasta.

Esim. 51. Joukon A **osittaisella järjestyksellä** tarkoitetaan sen relaatiota, joka on refleksiivinen, **antisymmetrinen** ja transitiivinen. Jos S_{os} on binäärisestä relaatiosymbolista r koostuva aakkosto, on siis struktuuri $\mathscr{A} = (A, r)$ **osittain järjestetty joukko**, jos se toteuttaa suljetut kaavat

$$\begin{aligned}
&\forall x\, r(x,x) && \text{(refleksiivisyys)}\\
&\forall x \forall y\, (r(x,y) \wedge r(y,x) \to (x = y)) && \text{(antisymmetrisyys)}\\
&\forall x \forall y \forall z\, (r(x,y) \wedge r(y,z) \to r(x,z)) && \text{(transitiivisuus)}.
\end{aligned}$$

Täten osittain järjestettyjen joukkojen luokka on äärellisesti aksiomatisoituva. □

Elementaarinen osajoukot ja relaatiot

Tarkastellaan nyt annetun struktuurin $\mathscr{A} = (A, S)$ alkioiden ominaisuuksia ja alkioden välisiä relaatioita, jotka voidaan määritellä kaavoilla aakkostossa S.

Määr. 32. Olkoon $\varphi = \varphi(y_1, \ldots, y_k)$ kaava yli aakkoston S, jonka vapaat muuttujat ovat joukossa $\{y_1, \ldots, y_k\}$, ja olkoon $\mathscr{A} = (A, S)$ jokin struktuuri. Tällöin merkintä

$$\mathscr{A} \models \varphi(a_1, \ldots, a_n)$$

tarkoittaa samaa kuin $I[a_1/y_1, a_2/y_2, \ldots, a_n/y_n] \models \varphi$ missä $I = (\mathscr{A}, \alpha)$.

Määr. 33. Olkoon $\varphi = \varphi(y_1, \ldots, y_k)$ kaava yli aakkoston S, missä kaavan φ vapaat muuttujat ovat joukossa $\{y_1, \ldots, y_k\}$, ja olkoon $\mathscr{A} = (A, S)$ jokin struktuuri. Määritellään kaavan φ **määrittelemä relaatio**:

$$r_{\mathscr{A}}(\varphi) = \{(a_1, \ldots, a_k) \in A^k \mid \mathscr{A} \models \varphi(a_1, \ldots, a_k)\} \ (\subseteq A^k)$$

Yleisemmin, jos Γ on jokin sellaisten kaavojen joukko, joiden vapaat muuttujat ovat joukossa $\{y_1, \ldots, y_k\}$, määrittelee Γ struktuurissa $\mathscr{A}$ relaation

$$r_{\mathscr{A}}(\Gamma) = \{(a_1, \ldots, a_k) \in A^k \mid \mathscr{A} \models \varphi(a_1, \ldots, a_k) \text{ kaikilla } \varphi \in \Gamma\}.$$

Relaatiota, joka tällä tavoin voidaan määritellä kaavajoukon avulla, kutsutaan **elementaariseksi struktuurin $\mathscr{A}$ relaatioksi**.

Jos $k = 1$, määritellään $r_{\mathscr{A}}(\Gamma)$ yleensä joukon A:n osajoukkona

$$\{a \in A \mid \mathscr{A} \models \varphi(a) \text{ kaikilla } \varphi \in \Gamma\},$$

ja tämä on joukon Γ **määrittelemä osajoukko**, sekä vastaavasti struktuurin **elementaariset osajoukot**. Kaava $\varphi = \varphi(y_1, \ldots, y_k)$ voidaan siis tulkita annetun struktuurin $\mathscr{A} = (A, S)$ alkioiden väliseksi ehdoksi.

Esim. 52. Annetun osittain järjestetyn joukon $\mathscr{A} = (A, \leq)$ kahden alkion keskinäinen **vertailukelvottomuus** on elementaarinen relaatio, sillä se voidaan määritellä kaavalla

$$\varphi(x, y) = \neg(x \leq y \lor y \leq x).$$

Vastaavasti **maksimaalisuus** ja **minimaalisuus** ovat struktuurin $\mathscr{A}$ alkioiden elementaarisia ominaisuuksia; maksimaalisten ja minimaalisten alkioiden joukot voidaan määritellä vastaavasti kaavoilla

$$\varphi_{\max}(x) = \forall y(x \leq y \to x = y) \quad \text{ja} \quad \varphi_{\min}(x) = \forall y(y \leq x \to y = x).$$

□

Esim. 53. Seuraavassa on esimerkkejä struktuurin $\mathscr{N} = (\mathbb{N}, +, \cdot, \sigma, <, 0)$ elementaarisista osajoukoista ja relaatioista.

(a) Jokainen luonnollisen lukujen joukon $\mathbb{N}$ äärellinen osajoukko on elementaarinen struktuurissa $\mathscr{N}$. Esimerkiksi tyhjän joukon määrittelee kaava $\neg(x = x)$, ja joukon $A = \{0, 2, 3\}$ määrittelee kaava

$$\varphi_A(x) = (x = 0) \lor (x = \sigma(\sigma(0))) \lor (x = \sigma(\sigma(\sigma(0)))).$$

(b) Parillisten luonnollisten lukujen joukon määrittelee struktuurin $\mathscr{N}$ kaava $\varphi_2(x) = \exists y(x = y + y)$. Yleisemmin

$$\varphi_n = \exists y(x = (y + (\ldots + (y + (y + y))\ldots))) \qquad (n \text{ kappaletta})$$

määrittelee luvulla n jaollisten lukujen joukon.

(c) Alkulukujen joukon määrittelee kaava

$$\varphi_{alk}(x) = \neg(x = 0) \land \neg(x = \sigma(0)) \land \forall y \forall z((x = y \cdot z) \to (x = y) \lor (x = z)).$$

(d) Jaollisuusrelaation $x|y$ määrittelee kaava

$$\varphi_|(x,y) = \exists z(x \cdot z = y).$$

(e) Luvun 2 potenssien joukon $\{2^n | n \geq 0\} = \{1, 2, 4, 8, \ldots\}$ määrittelee kaava

$$\varphi_{2^n}(x) = \forall y(\varphi_|(y,x) \to (y = \sigma(0)) \lor \varphi_|(\sigma(\sigma(0)), y)),$$

jossa on käytetty hyväksi edellä määriteltyä kaavaa $\varphi_|(x,y)$.

(f) Joukon $\mathbb{N}$ 3-paikkainen relaatio “x on lukujen y ja z suurin yhteinen tekijä”, missä oletetaan, että ainakin toinen luvuista y ja z eriää nollasta, voidaan määritellä kaavalla

$$\begin{aligned}\varphi_{syt}(x,y,z) = (\neg(y = 0) \lor \neg(z = 0)) \land \varphi_|(x,y) \land \varphi_|(x,z)\\ \land \forall u(\varphi_|(u,y) \land \varphi_|(u,z) \to \varphi_|(u,x)).\end{aligned}$$

Vastaavasti voidaan osoittaa, että relaatio ‘$x = \text{pyj}(y,z)$’ on elementaarinen.

(g) Joukon $\mathbb{N}$ tavallinen $\leq$-relaatio voidaan määritellä struktuurissa $\mathscr{N}$ kaavalla

$$\varphi_{\leq}(x,y) = \exists z(x + z = y)$$

käyttämättä relaatiota $<$. □

Edellä on esitetty vain positiivisia esimerkkejä elementaarisuudesta. Tämä johtuu tietysti siitä, että käytettävissä ei ole teoriaa, jonka avulla voidaan todistaa, että jokin struktuuriluokka, struktuurin osajoukko tai relaatio ei ole elementaarinen. Elementaarisen määriteltävyyden rajojen etsiminen on monessa yhteydessä tärkeä ja vaativa tehtävä.

4 Aksiomatiikkaa

Teoreemat

Tarkastellaan tässä luvussa **predikaattilogiikan** aksiomatiikkaa, toisin sanoen, oletetaan, että aakkostoon kuuluu vain relaatiosymboleja ja vakiosymboleja, mutta ei lainkaan funktiosymboleja. Lisäksi, yksinkertaisuuden nimissä, jätetään looginen symboli $=$ pois aksiomatiikasta. Erityisesti *jokainen termi on joko muuttuja tai vakiosymboli*.

Määr. 34. Olkoon φ kaava, x muuttuja ja t termi. Tällöin $\varphi(t/x)$ on kaava, jossa jokainen muuttujan x vapaa esiintymä on korvattu termillä t.

Määr. 35. Olkoon φ kaava ja x, y muuttujia. Sanotaan, että φ **hyväksyy sijoituksen** $x \mapsto y$, jos kaavassa φ ei ole muuttujan x vapaata esiintymää, joka muuttuu sidotuksi muuttujan y esiintymäksi kaavassa $\varphi(y/x)$.

Esim. 54. Kun $p,q \in Rel_1$, niin $\exists x\,(p(x) \to \neg q(x))$ hyväksyy sijoituksen $x \mapsto y$, ja tuloksena on $\exists y\,(p(y) \to \neg(y))$. Toisaalta kaava $\forall x\,(p(x) \to \forall y\, q(x))$ ei hyväksy sijoitusta $x \mapsto y$, koska y sitoutuisi loppuosassa. □

Määr. 36. Kaikille kaavoille φ, ψ ja η seuraavat ovat **aksioomeja**:

$$\varphi \to (\psi \to \varphi) \tag{P1}$$

$$(\varphi \to (\psi \to \eta)) \to ((\varphi \to \psi) \to (\varphi \to \eta)) \tag{P2}$$

$$(\neg\psi \to \neg\varphi) \to (\varphi \to \psi) \tag{P3}$$

$$\forall x\,(\varphi \to \psi) \to (\forall x\,\varphi \to \forall x\,\psi) \tag{P4}$$

$$\forall x\,\varphi \to \varphi(t/x) \qquad \text{jos } \varphi \text{ hyväksyy sijoituksen } x \mapsto t \tag{P5}$$

$$\varphi \to \forall x\,\varphi \qquad \text{jos } x \text{ ei ole vapaana kaavassa } \varphi \tag{P6}$$

$$\forall x\,\varphi \qquad \text{jos } \varphi \text{ on aksiooma, jossa } x \text{ on vapaa} \tag{P7}$$

Teoreemat määritellään induktiivisesti: Kaikki aksioomat ovat teoreemoja, ja jos φ ja $\varphi \to \psi$ ovat teoreemoja, samoin on ψ. Tämä päättelysääntö on **Modus Ponens** eli **MP**. Merkitään $\vdash_{\text{ax}} P$, jos P on teoreema.

Vastaavasti, jos Γ on kaavajoukko, asetetaan $\Gamma \vdash_{\text{ax}} \varphi$, jos φ voidaan johtaa aksioomeista ja joukon Γ kaavoista käyttäen päättelysääntöä MP.

Huom. Aksioomat (P1)–(P3) ovat samat kuin propositiologiikan aksioomat (A1)–(A3), joten jokaista propositiologiikan johtoa $\vdash_{\text{ax}} P$ vastaa predikaattilogiikan johto $\vdash_{\text{ax}} \varphi$, missä jokainen johdon aksioomeissa esiintyvä propositiosymboli on korvattu kaavasymbolilla ($P_i \mapsto \varphi_i$). Tällöin sanotaan, että φ on (propositiologiikan mukainen) **tautologia**. Näin ollen, kun P on propositiologiikan tautologia, on sillä täydellisyyslauseen nojalla jokin johto aksioomeista (A1)–(A3) käsin, ja siten myös kaavalla φ on johto predikaattilogiikassa.

Lause 39. *Olkoon P propositiologiikan tautologia. Jos φ on saatu propositiosta P korvaamalla jokainen propositiomuuttuja kaavalla, niin $\vdash_{\text{ax}} \varphi$.*

Esim. 55. Propositio $(p_1 \to (\neg p_2 \vee \neg p_1)) \to p_2$ on tautologia, ja siten se on johdettavissa aksiomaattisesti propositiologiikassa. Sama johto tuottaa johdon predikaattilogiikassa, kun propositiomuuttujien tilalle sijoitetaan kaavat. Täten, kun sijoitetaan $p_1 \mapsto \forall x\, r(x,y)$ ja $p_2 \mapsto \exists y\, q(y)$, saadaan $\vdash_{\text{ax}} (\forall x\, r(x,y) \to (\neg\exists y\, q(y) \vee \neg\forall x\, r(x,y))) \to \exists y\, q(y)$. □

Lause 40 (Spesialisointi)**.** *Oletetaan, että $\Gamma \vdash_{\text{ax}} \forall x\,\varphi$ ja että φ hyväksyy sijoituksen $x \mapsto t$, missä t on termi. Tällöin $\Gamma \vdash_{\text{ax}} \varphi(t/x)$.*

Todistus.

1.	$\forall x\,\varphi$	premissi
2.	$\forall x\,\varphi \to \varphi(t/x)$	(P5)
3.	$\varphi(t/x)$	MP: 1+2

□

Lause 41 ($\exists$-sääntö)**.** *Oletetaan, että $\Gamma \vdash_{\text{ax}} \varphi(t/x)$ ja että φ hyväksyy sijoituksen $x \mapsto t$, missä t on termi. Tällöin $\Gamma \vdash_{\text{ax}} \exists x\,\varphi(x)$.*

Todistus.

1.	$\varphi(t/x)$	premissi
2.	$\forall x \neg\varphi \to \neg\varphi(t/x)$	(P5)
3.	$\varphi(t/x) \to \neg\forall x \neg\varphi$	lause 39
4.	$\neg\forall x \neg\varphi$	MP: 1+3
5.	$\exists x\, \varphi$	(sama)

□

Lause 42 (Yleistyslaki)**.** *Olkoon* $\Gamma \vdash_{\text{ax}} \varphi$*. Jos* x *ei ole vapaa missään joukon* Γ *kaavassa, niin* $\Gamma \vdash_{\text{ax}} \forall x\, \varphi$.

Todistus. Jokaisen kaavan johto on äärellinen, ja siten olkoon $\psi_1, \psi_2, \ldots, \psi_n$ kaavan φ johto premisseistä Γ. Tässä siis kukin ψ_i on premissi, aksiooma tai saatu päättelysäännöllä MP kahdesta aikaisemmasta kaavasta, ja $\psi_n = \varphi$.

Osoitetaan induktiivisesti, että myös $\forall x\, \psi_1, \ldots, \forall x\, \psi_n$ on myös kelvollinen johto kaavalle $\forall x\, \psi_n = \forall x\, \varphi$.

(1.1) Jos ψ_i on aksiooma, missä x on vapaa, on myös $\forall x\, \psi_i$ aksiooma, (P7).

(1.2) Jos ψ_i on aksiooma tai premissi, missä x ei ole vapaana, niin saadaan seuraava johto:

1.	ψ_i	premissi
2.	$\psi_i \to \forall x\, \psi_i$	(P6)
3.	$\forall x\, \psi_i$	MP:1+2

(2) Oletetaan sitten, että $\forall x\, \psi_1, \ldots, \forall x\, \psi_{n-1}$ on kelvollinen johto. Jos ψ_n on aksiooma tai premissi, on edeltävän mukaan väite selvä. Oletetaan , että MP tuottaa kaavan ψ_n kaavoista ψ_k ja $\psi_j = \psi_k \to \psi_n$. Tällöin

	$\ldots$	
1.	$\forall x\, \psi_j$	induktio-oletus
	$\ldots$	
2.	$\forall x\, (\psi_j \to \psi_n)$	induktio-oletus
3.	$\forall x\, (\psi_j \to \psi_n) \to (\forall x\, \psi_j \to \forall x\, \psi_n)$	(P4)
4.	$\forall x\, \psi_j \to \forall x\, \psi_n$	MP: 2+3
3.	$\forall x\, \psi_n$	MP: 1+4

□

Lause 43 (Deduktiolause)**.** *Olkoon* Γ *kaavajoukko. Tällöin*

$$\Gamma \cup \{\varphi\} \vdash_{\text{ax}} \psi \iff \Gamma \vdash_{\text{ax}} \varphi \to \psi$$

Erityisesti, jos $\varphi_1, \varphi_2, \ldots, \varphi_{n+1} \vdash_{\text{ax}} \varphi$*, niin* $\vdash_{\text{ax}} (\varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_n) \to \varphi$.

Todistus. Tämän todistus on sama kuin propositiologiikassa, sillä siellä tarvittiin vain kahta ensimmäistä aksioomaa. □

Gödelin täydellisyyslause

Lause 44 (Terveys). *Jos* $\vdash_{\text{ax}} \varphi$*, niin* $\models \varphi$*.*

Todistus. Tätä varten täytyy osoittaa, että aksioomat ovat loogisesti tosia, ja että MP säilyttää tämän ominaisuuden. Todistus on pitkä, mutta suoraviivainen. Aksioomat (P1)–(P3) ovat loogisesti tosia lauseen 39 mukaisesti ja se, että MP säilyttää loogisesti totuuden seuraa kuten propositiologiikassa.

Osoitetaan esimerkkinä, että aksiooma (P4) on loogisesti tosi. Käytetään tähän deduktiolausetta. Oletetaan, että $I = (\mathscr{A}, \alpha)$ on tulkinta (universumina A) niin, että $I \models \forall x (\varphi \to \psi)$ ja $I \models \forall x \varphi$. Siis kaikille $a \in A$ on $I[a/x] \models \varphi \to \psi$ ja $I[a/x] \models \varphi$. Nyt, lauseen 35 mukaan kaikilla $a \in A$ on $I[a/x] \models \psi$, ja siten $I \models \forall x \psi$. Kaiken kaikkiaan $\forall x (\varphi \to \psi),\ \forall x \varphi \models \forall x \psi$, mistä deduktiolauseen avulla saadaan väite: $\models \forall x (\varphi \to \psi) \to (\forall x \varphi \to \forall x \psi)$. $\square$

Toiseen suuntaan todistus on hankalampi. Alunperin väitteen "$\models \varphi \implies \vdash_{\text{ax}} \varphi$" todistuksen esitti K. Gödel vuonna 1929. Nykyisin käytetään mieluummin Henkinin todistusta vuodelta 1949.

Määr. 37. Kaavajoukko Γ on **ristiriidaton**, jos ei ole olemassa kaavaa φ, jolle $\Gamma \vdash_{\text{ax}} \varphi$ ja $\Gamma \vdash_{\text{ax}} \neg\varphi$.

Lause 45. *Jos kaavajoukolla* Γ *on malli, on se ristiriidaton.*

Todistus. Ajatellaan, että Γ on ristiriitainen, jolloinka on olemassa kaava φ niin, että $\Gamma \vdash_{\text{ax}} \varphi$ ja $\Gamma \vdash_{\text{ax}} \neg\varphi$. Olkoot $\varphi_1, \ldots, \varphi_n \in \Gamma$ niin, että

$$\varphi_1, \varphi_2, \ldots, \varphi_i \ (= \varphi) \quad \text{ja} \quad \varphi_{i+1}, \varphi_{i+2}, \ldots, \varphi_n \ (= \neg\varphi)$$

ovat vastaavat johdot. Deduktiolauseen mukaan saadaan

$$\vdash_{\text{ax}} (\varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_i) \to \varphi\,,$$
$$\vdash_{\text{ax}} (\varphi_{i+1} \wedge \varphi_{i+2} \wedge \ldots \wedge \varphi_n) \to \neg\varphi\,,$$

ja kun $\psi = (\varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_n)$, saadaan siis $\vdash_{\text{ax}} \psi \to \varphi$ ja $\vdash_{\text{ax}} \psi \to \neg\varphi$. Päätellään, että $\vdash_{\text{ax}} \neg\psi$, sillä $(\psi \to \varphi) \wedge (\psi \to \neg\varphi) \to \neg\psi$ on (propositiologiikan mukainen) tautologia.

Olkoon $I = (\mathscr{A}, \alpha)$ kaavajoukon Γ malli. Lauseen 44 nojalla $\models \neg\psi$, ja siten $I \not\models \psi$. Näin ollen on indeksi k, jolle $I \not\models \varphi_k$. Mutta nyt I ei ole joukon Γ malli, koskapa $\varphi_k \in \Gamma$. $\square$

Lause 46. *Olkoon* Γ *ristiriitainen kaavajoukko. Tällöin* $\Gamma \vdash_{\text{ax}} \varphi$ *kaikille kaavoille* φ*.*

Todistus. Todistus on sama kuin propositiologiikassa. $\square$

Lause 47. *Olkoot* Γ *suljettujen kaavojen joukko ja* φ *suljettu kaava. Jos* $\Gamma \nvdash_{\text{ax}} \neg\varphi$*, niin* $\Gamma \cup \{\varphi\}$ *on ristiriidaton.*

Todistus. Jos $\Gamma \cup \{\varphi\}$ on ristiriitainen, niin edeltävän tuloksen mukaan $\Gamma \cup \{\varphi\} \vdash_{\text{ax}} \neg\varphi$. Tällöin deduktiolauseesta saadaan $\Gamma \vdash_{\text{ax}} \varphi \to \neg\varphi$. Toisaalta $(\varphi \to \neg\varphi) \to \neg\varphi$ on (propositiologiikan mukainen) tautologia, ja siten lauseen 39 mukaan $\vdash_{\text{ax}} (\varphi \to \neg\varphi) \to \neg\varphi$, mistä MP tuottaa $\Gamma \vdash_{\text{ax}} \neg\varphi$, ja tämä osoittaa väitteen oikeaksi. $\square$

Määr. 38. Suljettujen kaavojen joukko Γ on **täydellinen**, jos aina kun φ on suljettu kaava, joko $\Gamma \vdash_{\text{ax}} \varphi$ tai $\Gamma \vdash_{\text{ax}} \neg\varphi$.

Määr. 39. Kaavajoukko Γ on joukon Δ **laajennus**, jos kaikille φ on $\Delta \vdash_{\text{ax}} \varphi \implies \Gamma \vdash_{\text{ax}} \varphi$.

Lause 48 (Lindenbaumin lemma)**.** *Olkoon Γ ristiriidaton suljettujen kaavojen joukko. Tällöin se voidaan laajentaa täydelliseksi ristiriidattomaksi suljettujen kaavojen joukoksi.*

Todistus. Olkoon $\varphi_1, \varphi_2, \ldots$ kaikkien suljettujen kaavojen jono – tällainen listaus voidaan tehdä. Määritellään kaavajoukot $\Delta_0 \subseteq \Delta_1 \subseteq \ldots$ induktiivisesti:

(0) $\Delta_0 = \Gamma$.

$(n+1)$ Oletetaan, että $\Delta_0, \ldots, \Delta_n$ on jo määritelty. Tällöin

$$\Delta_{n+1} = \begin{cases} \Delta_n \cup \{\varphi_{n+1}\} & \text{jos } \Delta_n \nvdash_{\text{ax}} \neg\varphi_{n+1} \\ \Delta_n & \text{muutoin.} \end{cases}$$

(a) Osoitetaan, että jokainen Δ_n on ristiriidaton. Oletuksen mukaan $\Delta_0 = \Gamma$ on ristiriidaton. Oletetaan, että Δ_n on ristiriidaton, ja osoitetaan, että samoin on Δ_{n+1}. Kun $\Delta_{n+1} = \Delta_n$ on asia selvä, ja muutoin $\Delta_n \nvdash_{\text{ax}} \neg\varphi_{n+1}$, ja väite seuraa lauseesta 47.

(b) Olkoon $\Delta = \cup_{n \geq 0} \Delta_n$. Tällöin Δ on ristiriidaton, sillä jokainen johto on äärellisen mittainen: jos $\Delta \vdash_{\text{ax}} \varphi$ ja $\Delta \vdash_{\text{ax}} \neg\varphi$, niin $\Delta_n \vdash_{\text{ax}} \varphi$ ja $\Delta_n \vdash_{\text{ax}} \neg\varphi$ tarpeeksi suurella n.

(c) Osoitetaan vielä, että Δ on täydellinen. Tätä varten olkoon φ_n suljettu kaava, jolle $\varphi_n \notin \Delta$. Tällöin määritelmän mukaan $\Delta_n \vdash_{\text{ax}} \neg\varphi_n$, ja siis $\neg\varphi_n \in \Delta$. □

Lause 49 (Henkin)**.** *Olkoon Γ ristiriidaton suljettujen kaavojen joukko. Tällöin sillä on (numeroituva) malli.*

Todistus. Todistus on pitkähkö, ja se sivuutetaan. Henkinin todistus perustuu uusien vakiosymbolien tuottamiseen. □

Lauseiden 45 ja lauseen 49 nojalla on saatu:

Lause 50. *Olkoon Γ suljettujen kaavojen joukko. Tällöin Γ on ristiriidaton jos ja vain jos sillä on malli.*

Lause 51. *Olkoon Γ jokin suljettujen kaavojen joukko, ja olkoon φ suljettu kaava. Tällöin*

$$\Gamma \models \varphi \implies \Gamma \vdash_{\text{ax}} \varphi.$$

Todistus. Oletetaan, että $\Gamma \models \varphi$, ja olkoon $\Delta = \Gamma \cup \{\neg\varphi\}$. Nyt $\Delta \models \varphi$, sillä jokainen joukon Δ malli on myös joukon Γ malli, ja siten oletuksen mukaan kaavan φ malli. Mutta Δ on ristiriitainen, joten sillä ei ole mallia. Näin ollen $\Delta \vdash_{\text{ax}} \varphi$ (lause 46), ja siten deduktiolauseen mukaan $\Gamma \vdash_{\text{ax}} \neg\varphi \to \varphi$. Koska $(\neg\varphi \to \varphi) \to \varphi$ on (propositiologiikan mukainen) tautologia, tuottaa MP tuloksen $\Gamma \vdash_{\text{ax}} \varphi$ kuten vaadittua. □

Seuraava tulos on logiikan eräs merkittävimmistä tuloksista.

Lause 52 (Gödelin täydellisyyslause)**.** *Jos φ on suljettu loogisesti tosi kaava, niin $\Gamma \vdash_{\text{ax}} \varphi$. Näin ollen*

$$\models \varphi \iff \vdash_{\text{ax}} \varphi\,.$$

Todistus. Olkoon $\models \varphi$ eli φ on loogisesti tosi, jolloinka jokainen tulkinta I on kaavan φ malli. Lauseen 51 mukaan $\vdash_{\text{ax}} \varphi$. □

Liite: Boolen algebrat

Kun propositioita tarkastellaan 'modulo looginen ekvivalenttisuus', toteuttavat ne monia laskulakeja, joita voidaan käyttää niiden sieventämiseen ja normaalimuotojen määrittelyyn. Erityisesti ne muodostavat ns. Boolen algebran, jossa disjunktio, konjunktio ja negaatio esiintyvät operaatioina.

Määr. 40. Boolen algebra $\mathscr{B} = (B, \vee, \wedge, ', 0, 1)$ koostuu epätyhjästä joukosta B, binäärisistä operaatioista $\vee$ ja $\wedge$, unaarisesta operaatiosta $'$, sekä vakioista 0 ja 1 vakiota siten, että seuraavat ehdot ovat voimassa kaikille $x, y, z \in B$:

(B1)	$x \vee (y \vee z) = (x \vee y) \vee z$;	(B2)	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$;
(B3)	$x \vee y = y \vee x$;	(B4)	$x \wedge y = y \wedge x$;
(B5)	$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$;	(B6)	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$;
(B7)	$x \vee 0 = x$;	(B8)	$x \wedge 1 = x$;
(B9)	$x \vee x' = 1$;	(B10)	$x \wedge x' = 0$.

Jos $a, b \in B$, on $a \vee b$ niiden **yhdiste**, $a \wedge b$ niiden **kohtaus**, ja a' on alkion a **komplementti**. Alkio 0 on $\mathscr{B}$:n **nolla-alkio** ja 1 on sen **ykkösalkio**.

Esim. 56. Olkoon U jokin joukko, ja $\wp(U)$ sen kaikkien osajoukkojen muodostama joukko. Tällöin $\wp(U)$ muodostaa Boolen algebran yhdessä operaatioiden $\cup$, $\cap$, $'$ (komplementti: $A' = U \setminus A$), ja vakioiden $\emptyset, U$ kanssa. Helposti todetaan, että Boolen algebrojen ehdot (B1) – (B10) ovat voimassa. □

Esim. 57. Kun propositiologiikan konnektiivit $\neg$, $\vee$, $\wedge$ ja $\neg$ tulkitaan joukon $\{0, 1\}$ operaatioina, saadaan *totuusarvojen Boolen algebra* $(\mathbb{B}_2 = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$. Tällöin siis esimerkiksi $0 \vee 1 = 1$ ja $0 \wedge 1 = 0$. Identiteetit (B1) – (B10) voidaan todentaa totuustaulujen avulla. □

Boolen algebran määrittelevät identiteetit esiintyvät *duaaleina pareina*:

(B1)&(B2), (B3)&(B4), (B5)&(B6), (B7)&(B8), (B9)&(B10),

jotka saadaan toisistaan vaihtamalla vaihdetaan keskenään $\vee$ ja $\wedge$, sekä 0 ja 1. Erityisesti jokaisen Boolen algebran tuloksen todistus muuttuu vastaavaksi duaalin tuloksen todistukseksi.