Matemaattista logiikkaa soveltajille ja uteliaille

Antti Valmari

7. joulukuuta 2022

1 Johdanto

Tämän kirjan tavoitteena on esittää matemaattisen logiikan keskeisimmät ajatukset ja joukko upeimpia tuloksia tavallista helppolukuisemmin. Kirja on tarkoitettu toisaalta auttamaan logiikan soveltamisessa käytäntöön ohjelmoinnissa, matematiikassa ja muuallakin, ja toisaalta antamaan logiikan joistakin suurista tuloksista oikea ja pätevä kuva, jossa tuloksen merkitys ei huku teknisten yksityiskohtien taakse.

Kirjan aiheen vuoksi on selvää, että asioiden ymmärtäminen edellyttää huolellista ajattelua. Kirja on kuitenkin yritetty kirjoittaa siten, että matemaattis-loogista ajattelutapaa ei tarvitse osata etukäteen, vaan sitä opitaan pikkuhiljaa matkan varrella. Asioista on runsaasti esimerkkejä. Tärkeimpiä taitoja ja asioita toistetaan sopivissa yhteyksissä, jotta ne jäisivät paremmin mieleen. Tekstin seassa on kysymyksiä ja tehtäviä. Ne on numeroitu marginaaliin. Ne ovat enimmäkseen pieniä. Niillä pyritään varmistamaan juuri luetun asian oppiminen, ja ne on tarkoitettu tehtäväksi ennen kuin jatkat lukemista. Osaan on annettu vastaus kirjan lopussa. Muitakin oikeita vastauksia saattaa olla olemassa.

Jos luet tätä kirjaa paperilta, niin mallivastausten katsomista helpottaa, jos pidät kirjanmerkkiä vastaussivulla. Ruudulta lukiessasi saat saman vaikutuksen pitämällä tekstin auki kahdessa ikkunassa, toisessa siitä kohdasta mistä luet ja toisessa mallivastausten kohdalta. Voit myös kokeilla, mitä tapahtuu, jos siirrät kursorin marginaalissa olevan numeron päälle ja klikkaat. Jos kirjan lopussa on mallivastaus, niin marginaalissa oleva numero on linkki siihen. Jos ohjelma, jolla luet, osaa seurata näitä linkkejä, niin tälläkin tavalla saat mallivastaukset näkyviin. Takaisin kysymyksen kohdalle pääset klikkaamalla mallivastauksen edessä olevaa numeroa. Etsi kirjan lopusta tehtävän 1 mallivastaus! 1

Matematiikan kirjoissa on tavallista aloittaa kunkin asian käsittely täsmällisellä määritelmällä. Täsmällisten määritelmien ymmärtäminen on kuitenkin usein vaikeaa, jollei lukijalla ole etukäteen jonkinlaista käsitystä määritelmän kohteesta sekä kokemusta matemaattisten määritelmien lukemisesta. Siksi moni käsite esitellään tässä kirjassa vähän kerrassaan ja käyttöön kytkettynä, ja sille annetaan täsmällinen määritelmä vasta myöhemmin tekstissä.

Laajalti ajatellaan, että logiikan osaamisesta on hyötyä ohjelmistoammateissa. Esimerkiksi Association for Computing Machinery:n ja IEEE Computer Society:n laatimat arvovaltaiset kansainväliset suositukset ohjelmistoalan tutkintojen sisällöiksi sisältävät propositio- ja predikaattilogiikan perusteet. Kuitenkin logiikan menestys on useissa ohjelmistoalan ammatillisista osaamistarpeista tehdyissä selvityksissä ollut vain keskinkertainen. Siinä missä monien muiden aiheiden osaaminen kasvaa työuran aikana, logiikan osaaminen vähenee. Tämä viittaa siihen, että logiikkaa on kyllä opetettu, mutta sitä ei ole onnistuttu opettamaan käytännöllisenä työkaluna.

Siksi tässä kirjassa esitetään joitakin asioita toisin kuin perinteisissä logiikan oppikirjoissa. Tämä näkyy edellä mainittuna pyrkimyksenä helppolukuisuuteen, mutta myös muun muassa implikaatioon ja päättelysääntöihin liittyvien asioiden käsittelyssä. Matematiikan tapa tulkita ja käyttää niitä eroaa formaalin logiikan tavasta. Tämä ero jää usein huomaamatta ja aiheuttaa logiikan käytäntöön soveltamista haittaavia sekaannuksia. Tässä kirjassa ero tehdään näkyväksi ja keskitytään matematiikan tapaan.

Eräs yleinen virhe ohjelmissa on kaatuminen eli suorituksen yhtäkkinen keskeytyminen sen seurauksena, että ohjelma yritti tehdä jotain mitä ei voi tai ei saa tehdä. Jakolasku, jossa jakajana on 0, on koulumatematiikasta tuttu esimerkki mahdottomasta toimenpiteestä. Ohjelman kaatumista on luontevaa käsitellä ottamalla totuusarvojen ”tosi” ja ”epätosi” lisäksi käyttöön kolmas totuusarvo ”määrittelemätön”. Siksi kirjassa on myös kolmiarvoista logiikkaa koskeva luku.

Logiikan osaamisen suurin käytännön hyöty on kolmitahoinen. Ensiksi, se auttaa ilmaisemaan asioita yksikäsitteisesti ja tarkasti. Luonnollisen kielen ilmaukset ovat usein monitulkintaisia. Monitulkintaisuus saattaa tehdä ilmauksesta hauskan, kuten uutisotsikon ”Nuori mies kaahasi lähes kahtasataa poliisia karkuun” tapauksessa. Ei kuitenkaan ole hauskaa riidellä oikeudessa vastuunjakosopimuksen tulkinnasta, eikä ole hauskaa kun ohjelma tekee väärän asian siksi, että sen tilaaja ja toimittaja ymmärsivät saman ilmauksen eri tavalla.

Monet luonnollisen kielen ilmaukset tarkoittavat todellisuudessa aivan muuta kuin niiden kirjaimellinen tulkinta olisi. Esimerkiksi ”kengät jalkaan” tarkoittaa todellisuudessa ”jalat kenkiin”. Kysymykseen ”otatko kahvia” annettu vastaus ”ilman muuta” ei tarkoita ”ilman sokeria, kermaa, maitoa, pullaa ja niin edelleen”, vaan se tarkoittaa ”totta kai”. Se puolestaan on hyvin vahva ”kyllä”, vaikka ”kai” ilmaisee usein epävarmuutta, kuten ilmauksissa ”kyllä kai” ja ”niin kai”.

Jopa matemaattisissa teksteissä on käsitteitä tai merkintöjä määriteltäessä tavallista sanoa asia eri päin kuin tarkoitetaan. Esimerkiksi eräässä oppikirjassa lukee ”Mikäli jakojäännös on nolla eli jako menee tasan, sanotaan, että luku a on jaollinen luvulla b”. Kirjaimellisesti luettuna tämä ei kiellä sanomasta muulloinkin, että a on jaollinen b:llä. Tarkemmin oikein olisi ”Mikäli sanotaan, että luku a on jaollinen luvulla b, on jakojäännös nolla eli jako menee tasan”.

Ihmisillä on taipumus tulkita näkemänsä ja kuulemansa järkevästi jopa huomaamattaan. Kun maksupäätteen ruutuun ilmestyy teksti ”lue kortti”, niin tuskin kukaan alkaa itse lukea maksukorttiaan. Sen sijaan se asetetaan tai sitä liikutetaan siten, että maksupääte voi lukea sen. Kun lääkepaketissa lukee ”käytettävä ennen 06 / 2020” ja määräaika on juuri menossa umpeen, niin Fingerpori-sarjakuvan hahmo hotkaisee paketin tyhjäksi ja joutuu ensiapuun, mutta tosielämän ihminen ei tee niin.

Tämä on yleensä eduksi. Se kääntyy haitaksi silloin, kun olisi tärkeää nähdä mitä tekstissä oikeasti lukee, kuten sopimusta tai ohjetta tarkastettaessa. Pyörätuolissa istunut mies melkein joutui vartijan ulos heittämäksi Malmin Prismasta 13.2.2017, kun hän yritti ostaa 74,50 € maksavat talvikengät antamalla kassalle Kelan myöntämän enintään 70 € arvoisen maksusitoumuksen ja 4,50 € käteistä rahaa. Kassoille annetuissa ohjeissa oli yritetty sanoa, että maksusitoumus kelpaa rahan sijaan vain maksimiarvoonsa saakka, mutta sen sijaan oli vahingossa kielletty maksusitoumuksen käyttö kokonaan, jos se ei yksinään riitä maksamaan ostosta.

Yksikäsitteisyys ja tarkkuus eivät vaadi logiikan merkintöjen käyttämistä, vaan niihin voidaan päästä myös luonnollisella kielellä. Ilmaukset ”lähes kaksisataa poliisia ajoi takaa nuorta kaahaajaa” ja ”nuori mies kaahasi poliisia karkuun lähes kahtasataa” ovat yksikäsitteiset. Malmin Prisman kassoille tehtiin uudet ohjeet. Vaikka uutinen ei asiaa kerrokaan, voimme olla varmoja että ne eivät muodostuneet loogisista kaavoista. Ensin pitää kuitenkin nähdä tavoitteiden vastaisen tulkinnan vaara. Se edellyttää kykyä ajatella ilmausten merkitystä loogisesti ja tarkasti. Tarkastellaan lauseita ”saimme hyvää ruokaa” ja ”aluksi söin salaatin”. Kummassa niistä kahdessa viimeisessä sanassa kaksi viimeistä kirjainta ovat samat? 2

Toiseksi, logiikan osaaminen auttaa ennakoimaan mitä suunnittelupäätöksistä seuraa. Eräässä yliopistossa oli ongelmana, että kovin moni ruotsin tai englannin kurssille ilmoittautunut perui ilmoittautumisensa viime hetkellä. Syyksi paljastui, että tiedot opetuksen ajankohdista kerrottiin vasta ilmoittautumisajan päätyttyä, koska kurssien järjestäjät varasivat opetustilat ilmoittautumistietojen perusteella. Opiskelijat joutuivat ilmoittautumaan tietämättä milloin opetusta annetaan. Sitten kun ajat kerrottiin, moni huomasi kielen kurssin opetuksen olevan samanaikaisesti jonkin muun heille tärkeän kurssin opetuksen kanssa, ja perui ilmoittautumisensa kielen kurssilta. Tällaisten ongelmien välttämisessä ja korjaamisessa täytyy sekä tunnistaa kaikkien osapuolten tarpeet että analysoida niiden välisiä loogisia riippuvuuksia.

Kolmanneksi, logiikan osaaminen auttaa uskomaan, että monet asiat ovat monimutkaisempia kuin miltä näyttää, ja siksi tarvitsevat pohdintaa siitä, mitä niihin sisältyy ja mitä ohjelman käyttäjä tarvitsee. Tämä on ehkä tärkeämpää kuin edelliset kaksi. On esimerkiksi helppo luulla, että tenttituloksen kirjaaminen opintosuoritusrekisteriin on niin yksinkertainen asia, että se ei tarvitse tällaista pohdintaa. Liekö syynä tämä vai jokin muu, suomalaisia yliopistoja varten ”asiakaskeskeisesti ja edelläkävijän otteella” tehty uusi ”opetuksen ja opiskelun ydinjärjestelmä” ei ensimmäisinä vuosinaan selvinnyt tilanteesta, jossa opiskelija sai tentin läpi vasta toisella yrityksellä. Moni muukin vika siinä ja muissa ohjelmissa näyttää siltä, että kukaan ei ole miettinyt kunnolla, mitä kyseessä olevan toiminnon pitää tehdä.

Matemaattisessa logiikassa on kyse paljon muustakin kuin asioiden yksikäsitteisestä ja tarkasta ilmaisemisesta sekä seurausten päättelemisestä. Logiikan tutkimus tuotti 1900-luvulla syvällisiä, osittain ennakko-odotusten vastaisia tuloksia siitä, mitä voidaan ja mitä ei voida tehdä formaaleilla järjestelmillä. Tähän kirjaan on sisällytetty joitakin tärkeimpiä tuloksia ihan vain siksi, että ne ovat hyvin kiehtovia. Käyttäen hyväksi kirjan käytännöllisten osuuksien luomaa pohjaa, niiden asiasisältö yritetään esittää täsmällisesti. Esimerkiksi Gödelin ensimmäisestä epätäydellisyyslauseesta esitetään paitsi nykyisin yleinen ”kevennetty” versio, myös Gödelin oma versio ja Rosserin siihen tekemä parannus.

??? Johdantoa täydennetään kunhan selviää, mitä kirjassa loppujen lopuksi on.

2 Propositiologiikka

Tässä luvussa käsitellään propositiologiikkaa. Se on varsin yksinkertainen logiikka, eikä sellaisenaan vastaa kovinkaan hyvin esimerkiksi arkielämän, matematiikan ja ohjelmistotekniikan ilmaisu- ja päättelytarpeita. Se on silti monesta syystä tärkeä. Se on monimutkaisempien logiikoiden perusta. Se riittää tuomaan esiin monia logiikan keskeisiä ilmiöitä. Sen merkitys tietotekniikassa on suuri monella tavalla: se on tietokoneiden laitteistotason perusta, sillä on käyttöä jokapäiväisessä ohjelmoinnissa, sille on onnistuttu kehittämään tehokkaita automaattisia päättelymenetelmiä joilla voi ratkaista vaikeita tehtäviä tietokoneella, ja monet teoreettisen tietojenkäsittelytieteen suuret tulokset kuten NP-täydellisyyden keksiminen kytkeytyvät siihen.

2.1 Monta asiaa kaavoista ja ensi askeleet päättelemisestä

Tässä alaluvussa tarkastellaan propositiologiikan kaavoja ja niiden osia, esitetään niitä koskevia lainalaisuuksia sekä aloitetaan loogisen päättelemisen harjoitteleminen. Koska kirjan on tarkoitus olla luettavissa vähäisillä matemaattisilla taustatiedoilla, tässä alaluvussa selitetään ja harjoitellaan myös yleismatemaattisia käsitteitä sitä mukaa kuin on tarvetta.

Asiat on pyritty esittämään sellaisessa järjestyksessä, että mitään ei oleteta tunnetuksi ennen kuin se on selitetty, mutta mahdollisiman moni asia selitetään yhteydessä, jossa sen tarve ja sisältö voidaan havainnollistaa. Tästä syystä tekstissä on kaavoja koskevia käsitteitä, yleismatemaattisia käsitteitä ja päättelemisen alkeita sikin sokin. Tässä alaluvussa ei ole tavoitteena muodostaa kokonaiskuvaa mistään propositiologiikan asiasta, vaan se on myöhempien alalukujen tehtävä.

Silti saattaa olla hyödyllistä lukea tämä alaluku kahteen kertaan. Ihminen voi oppia kerralla vain rajallisen määrän uusia asioita. Edellä mainitusta syystä monessa kohdassa selitetään pääasian lisäksi esimerkiksi jotain yleismatemaattista asiaa. Voi olla, että ensimmäisellä lukukerralla niistä opitaan vain toinen. Jo opittu asia ei ole uusi enää jälkimmäisellä lukukerralla, jolloin toisenkin asian oppimiselle on paremmin tilaa.

Propositiologiikassa käsitellään *väitelauseita* (*proposition*). Väitelauseella on *totuusarvo* (*truth value*), joka saattaa riippua tilanteesta. Esimerkiksi ”aurinko paistaa” on jollain paikkakunnalla jonain hetkenä tosi ja jonain toisena hetkenä epätosi.

Yleisimmin käytössä on *kaksiarvoinen* logiikka. Siinä on kaksi totuusarvoa *tosi* (*true*) ja *epätosi* (*false*). Tässä kirjassa niitä merkitään T ja F. Muita kirjallisuudessa usein esiintyviä merkintöjä ovat 1 ja 0 sekä $\top$ ja $\bot$. Suurimmassa osassa tätä kirjaa käytössä ovat vain T ja F. Luvussa **??** käytetään hieman ja luvussa 8 paljon myös kolmatta totuusarvoa. Sellainen logiikka on *kolmiarvoinen*. Tulosten, jotka pätevät kaksimutta eivät kolmiarvoisessa logiikassa, kohdalla on sanallinen maininta asiasta, jotta lukijan olisi helpompi tietää mikä pätee missäkin.

Propositiologiikassa *kaava* (*formula*) tarkoittaa väitelauseen esitystä propositiologiikan merkinnöillä. Propositiologiikassa on kahdenlaisia kaavoja: *atomi-* (*atomic*) ja *yhdistetty* (*compound*). Propositiologiikan atomikaavoja ovat tässä kirjassa F ja T sekä *propositiomuuttujat* (*propositional variable*). Propositiomuuttujina käytetään isoja kirjaimia, joissa saattaa olla lisämerkintöjä oikeassa ala- tai ylänurkassa, kuten P, Q, P' ja P_1. Esimerkeissä pyritään käyttämään kirjaimia, jotka liittyvät esimerkin sisältöön ja siten helpottavat muistamista. Voidaan esimerkiksi valita että ”aurinko paistaa” merkitään kirjaimella A ja ”menen ulos” kirjaimella U. Muualla kuin esimerkeissä suositaan kirjaimia P, Q ja R.

$\wedge$	F	T
F	F	F
T	F	T

$\wedge$	F	T
F	F	F
T	F	T

$\wedge$	F	T
F	F	F
T	F	T

Kuva 1: $(A \wedge U)$:n totuusarvo A:n totuusarvon (vasen sarake) ja U:n totuusarvon (ylin rivi) funktiona

Yhdistettyjä kaavoja muodostetaan *loogisilla konnektiiveilla* (*logical connectives*). Konnektiivi $\wedge$ yhdistää kaksi kaavaa. Se luetaan ”ja”, ja se vastaa varsin pitkälle luonnollisen kielen sanaa ”ja”. Esimerkiksi jos A ja U ovat kuten edellä, niin $A \wedge U$ tarkoittaa ”aurinko paistaa ja menen ulos”. Se on tosi jos ja vain jos sekä ”aurinko paistaa” että ”menen ulos” ovat tosi. Kuvassa 1 tämä on ilmaistu taulukkona, jonka vasemmasta reunasta valitaan A:n totuusarvo ja yläriviltä valitaan U:n totuusarvo, ja niin saatujen rivin ja sarakkeen leikkauskohdassa on $(A \wedge U)$:n totuusarvo. Keskellä kuvaa on havainnollistettu, että jos A:n totuusarvo on T ja U:n totuusarvo on F, niin $(A \wedge U)$:n totuusarvo on F.

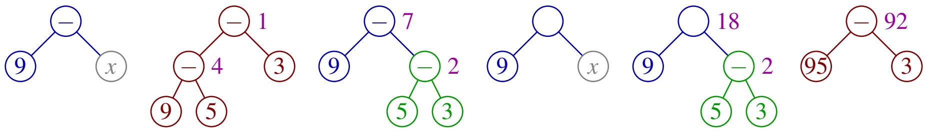
Matematiikassa käytetään usein sekä ilmauksia muotoa ”jos väite1 niin väite2” että ilmauksia muotoa ”väite1 jos ja vain jos väite2”. Kannattaa tehdä itselle selväksi niiden ero: edellinen sallii ja jälkimmäinen kieltää tilanteen, jossa väite2 pätee mutta väite1 ei päde. Esimerkiksi ”jos sekä A on tosi että U on tosi niin $A \wedge U$ on tosi” ei kerro ilmauksen $A \wedge U$ merkitystä kunnolla, koska se sallii useita erilaisia mahdollisuuksia. Se sallii muun muassa, että $A \wedge U$ on aina tosi, jopa silloinkin kun sekä A että U on epätosi. Se ei kiellä mitään muuta kuin sen, että A on tosi, U on tosi ja $A \wedge U$ on epätosi. Ilmaus ”$A \wedge U$ on tosi jos ja vain jos sekä A on tosi että U on tosi” ei kärsi tästä ongelmasta. Se sisältää myös sen vaatimuksen, että $A \wedge U$ ei ole tosi muulloin kuin silloin kun sekä A on tosi että U on tosi. Siksi fraasi ”jos ja vain jos” toistuu matematiikassa vähän väliä.

Ilmaukset tyyppiä ”$(A \wedge U)$:n totuusarvo on F” ovat kömpelöitä. Siksi otamme käyttöön merkinnän $\varphi \Leftrightarrow \psi$, missä φ:n ja ψ:n tilalla saa olla mitkä tahansa kaavat. Logiikassa on tavallista käyttää kreikkalaisia kirjaimia φ, ψ ja χ edustamaan kaavoja. Ne luetaan fii, psii ja khii. Niissäkin voi olla lisämerkintöjä oikeassa ala- tai ylänurkassa.

Symbolin $\Leftrightarrow$ merkitys vaihtelee kirjallisuudessa laajasti. Tässä kirjassa käytettävää merkitystä käsitellään perusteellisesti luvussa 2.4. Siihen saakka voit ajatella, että $\varphi \Leftrightarrow \psi$ tarkoittaa, että φ:llä ja ψ:llä on sama totuusarvo, samaan tapaan kuin koulumatematiikassa ”vasen $=$ oikea” tarkoittaa, että vasen ja oikea puoli tuottavat saman lukuarvon. Sanomme, että φ ja ψ ovat *yhtäpitävät*, ja $\varphi \Leftrightarrow \psi$ on *yhtäpitävyys*. Koska myös F on kaava, nyt ”$(A \wedge U)$:n totuusarvo on F” voidaan ilmaista $A \wedge U \Leftrightarrow$ F. Kuvan 1 oikeassa reunassa selvitetään, että jos $A \Leftrightarrow$ T ja $U \Leftrightarrow$ T, niin $A \wedge U \Leftrightarrow$ T.

Kuvan 1 taulukko ei päde pelkästään tapaukseen $A \wedge U$, vaan se pätee jokaiseen tapaukseen muotoa $\varphi \wedge \psi$ eli mille tahansa kahdelle kaavalle φ ja ψ. Kaavan $\varphi \wedge \psi$ totuusarvo voidaan laskea laskemalla ensin φ:n totuusarvo ja ψ:n totuusarvo, valitsemalla niiden mukaan rivi ja sarake, ja katsomalla lopputulos niiden leikkauskohdasta. Taulukosta huomaamme, että jos φ:n totuusarvoksi tulee F, niin lopputulos on F riippumatta ψ:n totuusarvosta. Tällöin ψ:n totuusarvoa ei tarvitse laskea — säästyy vaivaa! Esimerkiksi jos tiedetään että aurinko ei paista, niin ”aurinko paistaa ja ulkona on lämmintä” voidaan todeta epätodeksi vaikka ei otettaisi selvää, onko ulkona lämmintä.

Kun kreikkalaisen kirjaimen tilalle laitetaan kaava, on usein tarpeen lisätä sen ympärille sulkeet. Jollei ole varma että sulkeita ei tarvita, ne kannattaa laittaa varmuuden



Kuva 2: Lausekkeiden $9-x$, $9-5-3$, $9-(5-3)$, $9x$, $9(5-3)$ ja $95-3$ lausekepuut ja välitulokset

vuoksi. Sillä varmistetaan, ettei tapahdu samankaltaista virhettä kuin jos koulumatematiikan lausekkeeseen $9-x$ pannaan x:ksi $5-3$ ilman sulkeita, jolloin saadaan $9-5-3$, joka tuottaa 1. Oikein olisi $9-(5-3)$, joka tuottaa 7. Nämä lausekkeet on esitetty *lausekepuina* (*expression tree*) kuvassa 2. Kuvassa on näytetty myös välitulokset. Laskujärjestyksen ero näkyy kuvassa selvästi. Vielä hullumpi tulos tulee lausekkeella $9x$: sulkeiden kanssa $9(5-3)$ eli 18, ilman sulkeita $95-3$ eli 92.

Logiikan rakentamisen kannalta olisi yksinkertaisinta, että sulkeet laitettaisiin aina. Monissa oppikirjoissa tehdäänkin alkuun niin. Valitettavasti se aiheuttaa ihmisille haittaa. Ihmisten on vaikeampi tulkita $((a^2)+((2a)b))$ ja $((((a^2)+2)a)b)$ kuin a^2+2ab ja $(a^2+2)ab$.

Siksi sekä logiikassa että koulumatematiikassa on annettu lupa jättää sulkeita pois ja määritelty, mitä niin saatu ilmaus tarkoittaa. Esimerkiksi koulumatematiikassa $9-5-3$ tarkoittaa samaa kuin $(9-5)-3$. Sen näkee siitä, että kun lasketaan $9-5-3$, lasketaan ensin $9-5$ ja sen tuloksesta (joka on 4) vähennetään 3 (jolloin tulee 1). Lausekkeilla $9-5-3$ ja $(9-5)-3$ on täysin sama lausekepuu. Näin käyttäytyvää laskutoimitusta kutsutaan *vasemmalle liitännäiseksi* (*left-associative*).

Ohjelmointikielen C++ operaattori `+=` on *oikealle liitännäinen* (*right-associative*). Niinpä C++:ssa `x += y += 5` tarkoittaa samaa kuin `x += (y += 5)` eikä samaa kuin `(x += y) += 5`. Jos alussa $\mathtt{x} = \mathtt{y} = 0$, niin kumpikin ensin mainituista kasvattaa `y`:tä viidellä, mutta viimeksi mainittu ei kasvata.

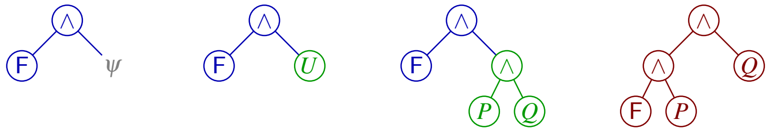
Suurin osa koulumatematiikan laskutoimituksista on vasemmalle liitännäisiä, mutta yksi tärkeä on oikealle liitännäinen — mikä? 3

Konnektiivin $\wedge$ liitännäisyyden suunta ei ole vakiintunut kirjallisuudessa. Tässä kirjasssa $\wedge$ on vasemmalle liitännäinen, eli $\varphi\wedge\psi\wedge\chi$ tarkoittaa samaa kuin $(\varphi\wedge\psi)\wedge\chi$. Siis kun lasketaan $\varphi\wedge\psi\wedge\chi$, niin välivaiheena lasketaan $\varphi\wedge\psi$ eikä $\psi\wedge\chi$.

On syytä korostaa, että logiikan näkökulmasta $\varphi\wedge\psi\wedge\chi$ on *sama kaava* kuin $(\varphi\wedge\psi)\wedge\chi$. Niillä on sama lausekepuu. Niiden ero on vain siinä, miten kaava esitetään ihmisille. Akateemisessa kirjallisuudessa tämä voidaan ilmaista sanomalla, että $\varphi\wedge\psi\wedge\chi$ on *lyhenne* (*abbreviation*) kaavalle $(\varphi\wedge\psi)\wedge\chi$. Sen sijaan $\varphi\wedge\psi\wedge\chi$ on *eri kaava* kuin $\varphi\wedge(\psi\wedge\chi)$, koska niillä on eri lausekepuu, ja laskujärjestys on eri.

Myös on hyvä pehmentää myöhemmin tulossa olevaa järkytystä huomauttamalla jo tässä vaiheessa, että itse asiassa ei $\varphi\wedge\psi\wedge\chi$ eikä $(\varphi\wedge\psi)\wedge\chi$ ole kaava. Kumpikin on *kaavaskeema* (*formula schema*), joka esittää äärettömän monta eri kaavaa, ja josta tulee kaava laittamalla kreikkalaisten kirjainten tilalle kaavat. Kreikkalaisen kirjaimen tilalle saa laittaa myös kaavaskeeman, jolloin lopputuloskin on kaavaskeema. Kaava siitä tulee vasta kun siinä ei ole yhtään kreikkalaista kirjainta. Esimerkiksi kaavaskeemaan $\varphi\wedge\varphi'$ voi laittaa φ':n tilalle $\psi\wedge\chi$, jolloin saadaan kaavaskeema $\varphi\wedge(\psi\wedge\chi)$. Eräässä myöhemmin käsiteltävässä esimerkissä siihen tullaan laittamaan φ:n tilalle $\neg\neg A$, ψ:n tilalle B ja χ:n tilalle $\neg C$, jolloin saadaan kaava $(\neg\neg A)\wedge(B\wedge(\neg C))$.

Suurimman osan aikaa kaavan ja kaavaskeeman erosta ei tarvitse välittää. Siksi on tavallista kutsua kaavaskeemoja kaavoiksi, aksioomaskeemoja aksioomiksi ja niin



Kuva 3: Kaavaskeeman $\mathsf{F} \wedge \psi$, kahden sen esittämän kaavan sekä kaavan $(\mathsf{F} \wedge P) \wedge Q$ lausekepuut

edelleen, vaikka se tarkkaan ottaen onkin väärin. Tässä kirjassa tämä asia mainitaan uudelleen sitten kun se alkaa olla tärkeä, ja siihen saakka saat unohtaa sen.

Havainnon ”jos $\varphi \Leftrightarrow \mathsf{F}$ niin $\varphi \wedge \psi \Leftrightarrow \mathsf{F}$” voi ilmaista yhtäpitävyytenä

$$\mathsf{F} \wedge \psi \;\Leftrightarrow\; \mathsf{F} \qquad [1]$$

Se pätee aina, eli se pätee jokaiselle kaavalle ψ riippumatta siitä, mitkä totuusarvot annetaan ψ:ssä esiintyville propositiomuuttujille. Jos valitsemme ψ:ksi U, saamme, että $\mathsf{F} \wedge U \Leftrightarrow \mathsf{F}$ pätee sekä silloin kun $U \Leftrightarrow \mathsf{F}$ että silloin kun $U \Leftrightarrow \mathsf{T}$. Jos valitsemme ψ:ksi $P \wedge Q$, saamme että $\mathsf{F} \wedge (P \wedge Q) \Leftrightarrow \mathsf{F}$ pätee kun P:n ja Q:n totuusarvot ovat F ja F taikka F ja T taikka T ja F taikka T ja T. Näitten ψ:ksi valintojen tuottamien kaavojen lausekepuut on näytetty kuvassa 3.

Ovatko $(P \wedge Q)$:n sulkeet tarpeen äskeisessä esimerkissä? 4

Jollei yhtäpitävyydestä ole kerrottu milloin se pätee, niin yleensä tarkoitetaan, että se pätee aina. Aina pätevää yhtäpitävyyttä voidaan kutsua *laiksi* (*law*). Propositiologiikan lakeja ilmaistaan toisinaan propositiomuuttujien avulla, esimerkiksi $\mathsf{F} \wedge P \Leftrightarrow \mathsf{F}$. Tällöin P:stä ei saa olla oletettu mitään; tähän palataan kohta. Toisinaan laki ilmaistaan kaavojen avulla, esimerkiksi $\mathsf{F} \wedge \psi \Leftrightarrow \mathsf{F}$. Tällöin ψ edustaa mitä tahansa kaavaa. Nämä kaksi tapaa ilmaisevat saman asian, mutta ovat käteviä eri tilanteissa. Emme todista yleisesti että ne ilmaisevat saman asian, mutta havainnollistamme sen syytä esimerkillämme $\mathsf{F} \wedge P \Leftrightarrow \mathsf{F}$ ja $\mathsf{F} \wedge \psi \Leftrightarrow \mathsf{F}$. Siinä jälkimmäinen seuraa edellisestä, koska edellinen pätee millä tahansa P:n totuusarvolla, joten se pätee silläkin totuusarvolla jonka ψ tuottaa. Edellinen seuraa jälkimmäisestä, koska ψ saa olla mikä tahansa kaava, ja P on kaava.

Edellä P:stä ei saa olla oletettu mitään, jotta ei syyllistyttäisi seuraavan esimerkin mukaiseen päättelyvirheeseen. Oletetaan, että kuu ei ole vihreää juustoa (tämä oletus lienee helppo hyväksyä!) ja että K tarkoittaa ”kun on vihreää juustoa”. Niinpä $K \Leftrightarrow \mathsf{F}$. Voimme päätellä $K \wedge P \Leftrightarrow \mathsf{F} \wedge P \Leftrightarrow \mathsf{F}$. Siksi $K \wedge P \Leftrightarrow \mathsf{F}$. Kun tähän sijoitetaan K:ksi φ ja P:ksi ψ, saadaan $\varphi \wedge \psi \Leftrightarrow \mathsf{F}$. Sijoittamalla sekä φ:ksi että ψ:ksi T saadaan $\mathsf{T} \wedge \mathsf{T} \Leftrightarrow \mathsf{F}$. Se ei tietenkään ole totta. Siksi on tärkeää, että kun korvataan propositiomuuttuja kaavalla, propositiomuuttujasta ei saa olla oletettu mitään.

Kuvan 1 taulukosta voi havaita kolme muutakin lakia:

$$\mathsf{T} \wedge \psi \;\Leftrightarrow\; \psi \qquad\qquad \varphi \wedge \varphi \;\Leftrightarrow\; \varphi \qquad\qquad \varphi \wedge \psi \;\Leftrightarrow\; \psi \wedge \varphi \qquad [2]$$

On oppimiselle hyödyllistä katsoa taulukosta, että nämä kolme todella pitävät aina paikkansa. Siksi tee niin! Lakia $\mathsf{T} \wedge \psi \Leftrightarrow \psi$ vastaa arjessa esimerkiksi se, että opis- 5
kelijan on kurssi läpäistäkseen suoritettava hyväksytysti sekä harjoitustyö että tentti, ja hänen harjoitustyönsä on jo hyväksytty. Niinpä kurssin läpäisemisen totuusarvo tulee olemaan sama kuin tentin hyväksymisen totuusarvo. Keksi kahdelle jälkimmäiselle laille esimerkit arkielämästä, vaikka niistä tulisikin hieman hassun kuuloisia, sillä sekin
on hyödyllistä! 6

XOR	F	T
F	F	T
T	T	F

$\vee$	F	T
F	F	T
T	T	T

Kuva 4: Poissulkeva tai eli XOR ja (molemmat salliva) tai eli $\vee$

Laista $\varphi \wedge \psi \Leftrightarrow \psi \wedge \varphi$ tarvitsee puhua niin monesti, että sille ja muille samankaltaisille on annettu nimi: ne ovat *vaihdantalakeja* (*commutative law*). Sanotaan myös, että $\wedge$ on *vaihdannainen* (*commutative*). Koulumatematiikan yhteen- ja kertolasku ovat vaihdannaisia, mutta vähennys- ja jakolasku eivät ole. Esimerkiksi $7-4=3$ mutta $4-7=-3$. Totesimme juuri, että logiikan $\wedge$ on vaihdannainen. Melkein kaikki laajalti käytetyt logiikan konnektiivit, jotka yhdistävät kaksi kaavaa, ovat vaihdannaisia, mutta luvussa 2.3 kohtaamme konnektiivin, joka ei ole.

Seuraava periaate on hyvin hyödyllinen. Se pätee laajalti myös propositiologiikan ulkopuolella. Siellä sen käyttöön liittyy varauma, josta ei vielä pitkään aikaan tarvitse tietää muuta kuin että jollei käytä symboleita $\forall$ ja $\exists$, niin siitä ei tarvitse välittää. Nämä symbolit tullaan ottamaan käyttöön luvussa 5. Niiden oikea käyttötapa seuraavassa periaatteessa ja muissa vastaavissa on vaikea selittää. Siksi lait ja periaatteet muotoillaan toistaiseksi siten, että niitä ei käytetä. Sivulla 100 tullaan kertomaan, miten niitä käytetään oikein.

> *Yhtäpitävyyttä saa soveltaa myös isomman kaavan osana olevaan kaavaan, jos $\forall$ ja $\exists$ eivät esiinny isommassa kaavassa. Siten saatu yhtäpitävyys pätee ainakin samoissa tilanteissa kuin alkuperäinen yhtäpitävyys.*

Niinpä, vaikka vielä ei ole kerrottu mitä $\neg$ ja $\vee$ tarkoittavat, $\varphi \wedge \psi \Leftrightarrow \psi \wedge \varphi$ antaa luvan päätellä $\neg(P \wedge \mathsf{T}) \vee Q \Leftrightarrow \neg(\mathsf{T} \wedge P) \vee Q$. Mikä on tässä φ:n tilalla ja mikä ψ:n tilalla? 7
Koska $\mathsf{T} \wedge \psi \Leftrightarrow \psi$, tästä voi jatkaa $\neg(\mathsf{T} \wedge P) \vee Q \Leftrightarrow \neg P \vee Q$. (Sulkeet P:n ympärillä eivät ole tarpeen.) Olemme osoittaneet $\neg(P \wedge \mathsf{T}) \vee Q \Leftrightarrow \neg P \vee Q$ (siis olemme osoittaneet, että $\neg(P \wedge \mathsf{T}) \vee Q \Leftrightarrow \neg P \vee Q$ pätee aina).

Tämä esimerkki havainnollistaa myös, että kuvasta 1 olisi voitu havaita $\varphi \wedge \mathsf{F} \Leftrightarrow \mathsf{F}$ ja $\varphi \wedge \mathsf{T} \Leftrightarrow \varphi$, mutta ilmankin pärjättiin, koska ne saa johdettua tehdyistä havainnoista. Koska ne esiteltiin tällä tavalla, niin kun seuraavan kerran näet jollekin konnektiiville ? pätevän $\mathsf{T} \mathbin{?} \varphi \Leftrightarrow \psi$ (tai $\mathsf{F} \mathbin{?} \varphi \Leftrightarrow \psi$) ja $\varphi \mathbin{?} \psi \Leftrightarrow \psi \mathbin{?} \varphi$, niin hoksaat ehkä itse, että $\varphi \mathbin{?} \mathsf{T} \Leftrightarrow \psi$ (tai $\varphi \mathbin{?} \mathsf{F} \Leftrightarrow \psi$).

Jos minkä tahansa $\Leftrightarrow$-lain vasen ja oikea puoli vaihdetaan keskenään, niin lopputuloskin on laki. Niinpä muun muassa seuraavat ovat lakeja:

$$\mathsf{F} \Leftrightarrow \mathsf{F} \wedge \psi \qquad \psi \Leftrightarrow \mathsf{T} \wedge \psi \qquad \varphi \Leftrightarrow \varphi \wedge \varphi \qquad \mathsf{F} \Leftrightarrow \varphi \wedge \mathsf{F} \qquad \varphi \Leftrightarrow \varphi \wedge \mathsf{T}$$

Sen sijaan että muistaisi jokaisen näistä erikseen, on helpompi muistaa, että jos minkä tahansa $\Leftrightarrow$-lain vasen ja oikea puoli vaihdetaan keskenään, niin lopputuloskin on laki. Ilmauksella ”laki X takaperin” tarkoitetaan sitä lakia, joka saadaan vaihtamalla lain X vasen ja oikea puoli keskenään.

Kaavojen esittäminen lausekepuina on niin tärkeä asia, että keskeytämme hetkeksi logiikan pohtimisen ja teemme yhden lausekepuuharjoituksen. Esitä $\neg(P \wedge \mathsf{T}) \vee Q$ lausekepuuna! 8

Luonnollisen kielen sanaa ”tai” käytetään kahdessa eri merkityksessä. Jos ravintolan

U	J	E	$U \wedge J$	$J \vee E$	$(U \wedge J) \vee E$	$U \wedge (J \vee E)$
F	F	F	F	F	F	F
F	F	T	F	T	T	F
F	T	F	F	T	F	F
F	T	T	F	T	T	F
T	F	F	F	F	F	F
T	F	T	F	T	T	T
T	T	F	T	T	T	T
T	T	T	T	T	T	T

Kuva 5: Yhdistetty totuustaulu kaavoille $(U \wedge J) \vee E$ ja $U \wedge (J \vee E)$

listalla lukee ”alkupalaksi parsakeitto tai savulohisalaatti”, niin tarkoitus on, että asiakas ottaa niistä vain toisen. Tällainen ”tai” on *poissulkeva tai* (*exclusive or*). Se on esitetty taulukkona kuvassa 4 vasemmalla. Jos ystäväsi sanoo ”kuulostaa hyvältä, mennään sinne jos pääruoaksi on tarjolla kanaa tai lammasta”, niin ravintola todennäköisesti kelpaa hänelle siinäkin tapauksessa, että siellä on tarjolla molempia. Tämä jälkimmäinen ”tai” ei siis ole poissulkeva vaan *molemmat salliva* (*inclusive*). Se on esitetty kuvassa 4 oikealla. Kun logiikassa käytetään sanaa ”tai” täsmentämättä kumpaa tarkoitetaan, niin tarkoitetaan molemmat sallivaa. Logiikassa ei ole vakiintunutta symbolia poissulkevalle versiolle. Elektroniikassa sen nimi on XOR.

Molemmat salliva ”tai” esitetään konnektiivilla $\vee$. Se luetaan ”tai”, ja se yhdistää kaksi kaavaa. Niinpä $A \vee U \Leftrightarrow \mathsf{T}$ kolmessa erilaisessa tilanteessa: aurinko paistaa ja en mene ulos, aurinko ei paista ja menen ulos, tai aurinko paistaa ja menen ulos. Jos aurinko ei paista ja en mene ulos, niin $A \vee U \Leftrightarrow \mathsf{F}$.

Kuten $\wedge$, myös $\vee$ on vasemmalle liitännäinen. Siis $\varphi \vee \psi \vee \chi$ tarkoittaa samaa kuin $(\varphi \vee \psi) \vee \chi$.

Edellä huomasimme neljä lakia koskien konnektiivia $\wedge$. Ne ovat hyödyllisiä, koska niillä voi *sieventää* (*simplify*) kaavoja eli muuntaa niitä yhtäpitäviksi yksinkertaisemmiksi kaavoiksi, ja koska ne todellakin pätevät aina, eli riippumatta siitä mitkä kaavat laitetaan φ:n ja ψ:n tilalle ja mitkä totuusarvot annetaan propositiomuuttujille. Saman-
kaltaiset lait pätevät myös konnektiiville $\vee$. Mitkä ne ovat? Keksi myös jokaisesta ar- 9
kielämän esimerkki! Jos olet jo huomannut viidennen ja kuudennen lain, joissa ei lue 10
$\mathsf{F} \vee \psi$ eikä $\mathsf{T} \vee \psi$ vaan toisinpäin, niin kehu itseäsi! Jollet vielä ole huomannut niitä,
niin keksi ne nyt ja sitten kehu itseäsi! 11

Tarkoittakoon J että syön jäätelön ja E että katson elokuvan. Ilmaus ”menen ulos ja syön jäätelön tai katson elokuvan” jättää epäselväksi, menenkö varmasti ulos myös siinä tapauksessa, että katson elokuvan. Kaavoissa tällaiset epäselvyydet voi välttää lisäämällä sulkeet: kaavan $(U \wedge J) \vee E$ tapauksessa on mahdollista, että en mene ulos, mutta kaavan $U \wedge (J \vee E)$ tapauksessa menen varmasti ulos. Kuvassa 5 on esitetty molempien kaavojen totuusarvot atomisten väitelauseiden ”menen ulos”, ”syön jäätelön” ja ”katson elokuvan” totuusarvojen funktiona. Siitä näkee, että lopputulokset eroavat kahdessa tilanteessa: silloin ja vain silloin kun $U \Leftrightarrow \mathsf{F}$, $E \Leftrightarrow \mathsf{T}$ ja J:n totuusarvo on joko F tai T.

Kuvan 5 taulukko on *totuustaulu* (*truth table*), eli siinä on yksi sarake kullekin propositiomuuttujalle, yksi tai useampi sarake lopputuloksille, mahdollisesti sarakkeita välituloksille, sekä rivi jokaiselle propositiomuuttujien totuusarvojen yhdistelmälle. Kuvien 1 ja 4 taulukot eivät ole totuustauluja, koska niissä toinen propositiomuuttuja juoksee vaakasuoraan. Totuustauluilla voi periaatteessa ratkaista monia propositiologiikan tehtäviä, kuten selvittää onko kaavan totuusarvo aina T ja tuottavatko kaksi kaavaa aina saman totuusarvon. Valitettavasti niillä on yksi paha vika: ne kasvavat nopeasti hallitsemattoman suuriksi, kun propositiomuuttujien määrä kasvaa.

Siksi tarvitaan muita keinoja. Yksi tehokas keino on valita jokin propositiomuuttuja, sijoittaa siihen vuorotellen F ja T ja sieventää näin syntyvät kaavat. Kun U:n tilalle sijoitetaan T kaavassa $(U \wedge J) \vee E$, saadaan $(\mathsf{T} \wedge J) \vee E$, joka sievenee kaavaksi $J \vee E$. Sama sijoitus kaavaan $U \wedge (J \vee E)$ tuottaa $\mathsf{T} \wedge (J \vee E)$ ja edelleen $J \vee E$. Koska niistä tuli sama sievennetty kaava, tuottavat ne aina saman totuusarvon. Tämä täsmää siihen, että kuvan 5 jokaisella neljällä alimmalla rivillä rivin kaksi viimeistä totuusarvoa ovat samat.

Äskeiset sievennykset voi esittää tiiviimmin muodossa ”Jos $U \Leftrightarrow \mathsf{T}$, niin $(U \wedge J) \vee E \Leftrightarrow (\mathsf{T} \wedge J) \vee E \Leftrightarrow J \vee E$ ja $U \wedge (J \vee E) \Leftrightarrow \mathsf{T} \wedge (J \vee E) \Leftrightarrow J \vee E$”. Ilmaus $\varphi \Leftrightarrow \psi \Leftrightarrow \chi$ tarkoittaa, että φ ja ψ ovat yhtäpitävät ja myös ψ ja χ ovat yhtäpitävät. Symbolilla $\Leftrightarrow$ ilmaistun yhtäpitävyyden tulee päteä kaikissa niissä tilanteissa, jotka ovat mahdollisia taustatiedot huomioon ottaen. Esimerkiksi $(U \wedge J) \vee E \Leftrightarrow (\mathsf{T} \wedge J) \vee E$ ei ole yleisesti pätevä, mutta on pätevä tässä esimerkissä, koska sen alussa oletettiin $U \Leftrightarrow \mathsf{T}$.

Tässä kirjassa kaavoista puhuttaessa ”tilanne” tarkoittaa mitä tahansa käytössä olevien muuttujien arvojen yhdistelmää. Propositiologiikan tapauksessa muuttujia ovat propositiomuuttujat, joten ”tilanne” on mikä tahansa propositiomuuttujien totuusarvojen yhdistelmä. Propositiologiikassa tilanne vastaa siis totuustaulun riviä (muuta riviä kuin otsikkorivi, joka koostuu kaavoista). Asian käsittelyn edetessä tehdään usein tilapäisiä tai pysyviä oletuksia, jotka jakavat tilanteet ”mahdollisiin” ja ”mahdottomiin”. Edellä tehtiin tilapäinen oletus, jonka mukaan U:n totuusarvo on T. Se teki kuvan 5 neljän F-alkuisen rivin esittämistä tilanteista mahdottomia ja jätti T-alkuiset mahdollisiksi. Sivulla 7 oli esimerkki, jossa K asetettiin tarkoittamaan, että kuu on vihreää juustoa. Sitten tehtiin pysyvä oletus, jonka mukaan K:n totuusarvo on aina F. Kuvassa 16 tullaan tekemään monimutkainen pysyvä oletus, joka sanoo muun muassa, että Pihtiputaan mummo ei voi olla yhtäaikaa Kuopiossa ja Rovaniemellä.

Mihin muotoon $(U \wedge J) \vee E$ ja $U \wedge (J \vee E)$ sievenevät, kun U:n tilalle sijoitetaan
F? Tarkasta, että vastauksesi täsmäävät kuvan 5 niihin riveihin, joilla $U \Leftrightarrow \mathsf{F}$. Ne eivät 12
tuota samaa totuusarvoa silloin kun $E \Leftrightarrow \mathsf{T}$. Niinpä $(U \wedge J) \vee E$ ja $U \wedge (J \vee E)$ eivät ole yhtäpitävät.

Seuraavaksi tarkastamme tällä keinolla, onko $\wedge$ *liitännäinen* (*associative*). Matemaattisen operaattorin $\textcircled{?}$ liitännäisyys tarkoittaa, että $(X \textcircled{?} Y) \textcircled{?} Z$ tuottaa aina saman tuloksen kuin $X \textcircled{?} (Y \textcircled{?} Z)$. (Se on eri asia kuin aiemmin mainitut vasemmalle ja oikealle liitännäisyys, eikä sitä pidä sekoittaa niihin.) Koulumatematiikan yhteen- ja kertolasku ovat liitännäiset, mutta vähennyslasku ei ole, sillä esimerkiksi $(9-5)-3 = 4-3 = 1$ mutta $9-(5-3) = 9-2 = 7$.

Niinpä valitsemme kolme propositiomuuttujaa P, Q ja R, joista ei ole oletettu mitään, ja sijoitamme P:n tilalle vuoron perään F ja T kaavoissa $(P \wedge Q) \wedge R$ ja $P \wedge (Q \wedge R)$. Kun $P \Leftrightarrow \mathsf{F}$, niin $(P \wedge Q) \wedge R \Leftrightarrow (\mathsf{F} \wedge Q) \wedge R \Leftrightarrow \mathsf{F} \wedge R \Leftrightarrow \mathsf{F}$ ja $P \wedge (Q \wedge R) \Leftrightarrow \mathsf{F} \wedge (Q \wedge R) \Leftrightarrow \mathsf{F}$. Siis molemmista kaavoista tuli sama tulos F. Kun $P \Leftrightarrow \mathsf{T}$, niin $(P \wedge Q) \wedge R \Leftrightarrow (\mathsf{T} \wedge Q) \wedge R \Leftrightarrow Q \wedge R$ ja $P \wedge (Q \wedge R) \Leftrightarrow \mathsf{T} \wedge (Q \wedge R) \Leftrightarrow Q \wedge R$. Nytkin molemmista kaavoista tuli sama tulos, nimittäin $Q \wedge R$. Koska kummallakin sijoituksella molemmista kaavoista tuli sama tulos, pätee $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ eli $\wedge$ on liitännäinen. Tämän lain nimi on tietenkin *liitäntälaki* (*associative law*). Kaavoilla ilmaistuna se näyttää tältä:

$$(\varphi \wedge \psi) \wedge \chi \;\Leftrightarrow\; \varphi \wedge (\psi \wedge \chi) \qquad [3]$$

kaava	Q:hun F	Q:hun T	P:hen F	P:hen T
$P \wedge (Q \vee R)$	$P \wedge R$	P	F	$Q \vee R$
$(P \wedge Q) \vee (P \wedge R)$	$P \wedge R$	$P \vee (P \wedge R)$	F	$Q \vee R$

Kuva 6: Kaksi yritystä tutkia päteekö $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

Totesimme aiemmin, että $\varphi \wedge \psi \wedge \chi$ tarkoittaa samaa kuin $(\varphi \wedge \psi) \wedge \chi$. Siksi $\wedge$:n liitäntälaki voidaan kirjoittaa myös näin:

$$\varphi \wedge \psi \wedge \chi \;\Leftrightarrow\; \varphi \wedge (\psi \wedge \chi) \qquad [4]$$

Koska $\wedge$ on liitännäinen, ei logiikan sovelluksissa ole juuri koskaan olennaista, onko se vasemmalle vai oikealle liitännäinen. Erohan on vain laskujärjestyksessä, ei laskun tuottamassa lopputuloksessa. Teoreettisisssa tarkasteluissa laskujärjestys on toisinaan tärkeä silloinkin, kun se ei vaikuta lopputulokseen. Siksi on tärkeää, että jompikumpi liitännäisyyden suunta on valittu, vaikka ei olekaan tärkeää, kumpi suunta valittiin. Kerrataanpa vielä lauseketta X ? Y ? Z esimerkkinä käyttäen: mitä tarkoittaa vasemmalle liitännäisyys, mitä tarkoittaa oikealle liitännäisyys, ja mitä tarkoittaa liitännäisyys? 13

Sijoituksen jälkeen tehtyjen sievennysten lopputulosten ei tarvitse olla samat; riittää, että ne ovat yhtäpitävät. Toisinaan ei ole helppo nähdä ovatko ne yhtäpitävät. Silloin voidaan valita jokin niissä esiintyvä propositiomuuttuja ja sijoittaa siihenkin vuoron perään F ja T. Tätä voidaan jatkaa niin pitkälle kuin tarvitaan. Valitettavasti jokainen valinta jakaa päättelyn kahteen haaraan, joten työmäärä voi kasvaa suureksi.

Siksi kenties kannattaa toimia toisin: hylätään alkuperäinen propositiomuuttujan valinta ja kokeillaan sen sijaan eri valintaa. Kuvassa 6 tutkitaan, päteekö $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$. Ensin valitaan Q. Sijoitus F tuottaa sutjakasti $P \wedge (\mathsf{F} \vee R) \Leftrightarrow P \wedge R$ ja $(P \wedge \mathsf{F}) \vee (P \wedge R) \Leftrightarrow \mathsf{F} \vee (P \wedge R) \Leftrightarrow P \wedge R$ eli saman molemmista kaavoista. Mutta T tuottaa P ja $P \vee (P \wedge R)$. Niistä ei näe helposti tuottavatko ne aina saman totuusarvon. Siksi yritetään uudelleen valitsemalla sijoituksen kohteeksi P. Nyt kummastakin alkuperäisestä kaavasta tulee F sijoituksella F ja $Q \vee R$ sijoituksella T. Niinpä $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ pätee.

Huomaa, että epäonnistuminen sijoituksella $Q \Leftrightarrow \mathsf{T}$ ei tarkoittanut, että yhtäpitävyys ei päde. Sehän pätee, koska se onnistuttiin todistamaan P:n avulla! Epäonnistuminen tarkoitti vain, että jatkaminen Q:n kanssa alkoi näyttää hankalalta, joten kokeiltiin, päästäisiinkö helpommalla vaihtamalla P:hen. Vaihtamisen sijaan olisi voitu todistaa P ja $P \vee (P \wedge R)$ yhtäpitäviksi. Sen olisi voinut tehdä vaikkapa sijoittamalla niissä P:hen vuoron perään F ja T.

Edes epäonnistuminen jokaisella propositiomuuttujalla ei todista, että yhtäpitävyys ei päde. Hyvin usein selkein ja vähiten ajatteluvirheille altis tapa todistaa, että yhtäpitävyys ei päde, on seuraava:

> *Luotettava tapa todistaa, että propositiologiikan yhtäpitävyys ei päde, on ilmoittaa propositiomuuttujille (tai osalle niistä) sellaiset arvot, että väitetyn yhtäpitävyyden eri puolilta tulee eri totuusarvot. Tällainen propositiomuuttujien arvojen yhdistelmä on* vastaesimerkki *(*counterexample*).*

Esimerkiksi edellä valinta $U \Leftrightarrow \mathsf{F}$ ja $E \Leftrightarrow \mathsf{T}$ osoitti, että $(U \wedge J) \vee E$ ja $U \wedge (J \vee E)$ eivät ole yhtäpitävät, koska sillä $(U \wedge J) \vee E \Leftrightarrow \mathsf{T}$ mutta $U \wedge (J \vee E) \Leftrightarrow \mathsf{F}$. Tämä valinta löydettiin huomaamalla, että sijoitus $U \Leftrightarrow \mathsf{F}$ tuotti eri kaavat E ja F, ja miettimällä, millä sijoituksella ne saisi tuottamaan eri totuusarvot.

Huomasithan, että tässä esimerkissä ei annettu totuusarvoa J:lle. Siksi edellä lukee "(tai osalle niistä)".

Vastaesimerkin antaminen on myös propositiologiikassa, koulumatematiikassa ja yleisemminkin luotettava tapa todistaa, että jokin kaava ei ole aina tosi tai jokin laiksi väitetty ei aina päde. Hyvin usein on annettavissa vastaesimerkki, joka lukijan on helppo tarkastaa. Muitakin keinoja saattaa olla, kuten sen osoittaminen, että väitetty asia johtaa ristiriitaan tunnettujen pätevien asioiden kanssa. Ne ovat kuitenkin usein alttiimpia päättelyvirheille ja työläämpiä kuulijoillesi ja lukijoillesi kuin hyvän vastaesimerkin antaminen. Siksi, ja koska tämä on oppikirja, käytä vastauksissasi niitä vain jos et löydä hyvää vastaesimerkkiä.

Toisinaan on helppo päästä välivaiheeseen, jossa ei konkreettisesti anneta vastaesimerkkiä, mutta on ilmeista, että sellaisia on olemassa. Näin on esimerkiksi silloin, kun ei ole tehty P:n ja Q totuusarvojen mahdollisia yhdistelmiä rajoittavia oletuksia ja on saatu $P \wedge Q \Leftrightarrow P \vee Q$. Koska tämä on oppikirja, älä tyydy tällaiseen, vaan esitä konkreettinen vastaesimerkki. Sillä vältät sen riskin, että jotain jäi sinulta huomaamatta eikä vastaesimerkkejä todellisuudessa olekaan olemassa. Jos jatkaminen konkreettiseen vastaesimerkkiin on helppoa, niin se ei ole sinulle suuri lisävaiva. Jos se on vaikeaa, niin ehkä vastauksesi on kesken tai ehkä välivaiheesi ei olekaan pätevä.

Anna vastaesimerkki yhtäpitävyydelle $P \wedge Q \Leftrightarrow P \vee Q$! 14

Jos halutaan puhua kaavaan sijoittamisesta ilman että puhutaan jostain nimenomaisesta kaavasta, voidaan käyttää esimerkiksi merkintää $\varphi(P,Q,R)$. Merkintä $\varphi(P,\mathsf{F},R)$ tarkoittaa sitä mikä saadaan sijoittamalla Q:n tilalle F kaavassa $\varphi(P,Q,R)$. Tarvittaessa täytyy lisätä sulkeet. (Ne saa lisätä muulloinkin, jos vaikka ei jaksa miettiä tarvitaanko niitä.) Jos esimerkiksi $\varphi(P)$ on $U \wedge P$, niin $\varphi(J \vee E)$ ei ole $U \wedge J \vee E$ vaan $U \wedge (J \vee E)$.

Ilmauksen $U \wedge J \vee E$ merkitys ei ole täysin vakiintunut. Monet kirjoittajat määrittelevät, että $\wedge$ lasketaan ennen kuin $\vee$. Tässäkin kirjassa tehdään niin. Silloin $U \wedge J \vee E$ tarkoittaa samaa kuin $(U \wedge J) \vee E$. Kuten edellä nähtiin, se ei ole yhtäpitävä kaavan $U \wedge (J \vee E)$ kanssa. Jotkut kuitenkin katsovat, että sulkeiden puutteen vuoksi $U \wedge J \vee E$ ei tarkoita mitään. Silloinkaan se ei tarkoita samaa kuin $U \wedge (J \vee E)$. Toisinaan tässä kirjassa käytetään sulkeita muotoa $(\varphi \wedge \psi) \vee \chi$ tai $\varphi \vee (\psi \wedge \chi)$ olevissa ilmauksissa (joissa sulkeet ovat vapaaehtoiset), jotta ne olisivat helpommat hahmottaa. Näin tehdään erityisesti silloin, kun halutaan korostaa symmetriaa lähistöllä sijaitsevien muotoa $(\varphi \vee \psi) \wedge \chi$ tai $\varphi \wedge (\psi \vee \chi)$ olevien ilmausten (joissa sulkeet ovat pakolliset) kanssa. Poista vapaaehtoiset sulkeet seuraavista yhtäpitävyyksistä:

$$\begin{aligned} P \vee (Q \wedge R) &\Leftrightarrow (P \vee Q) \wedge (P \vee R) \\ P \wedge (Q \vee R) &\Leftrightarrow (P \wedge Q) \vee (P \wedge R) \end{aligned}$$ 15

Edellä käytetyssä keinossa selvittää, päteekö $\varphi \Leftrightarrow \psi$, valittiin jokin propositiomuuttuja P ja sijoitettiin sen tilalle vuoron perään F ja T. Jos $\varphi(\mathsf{F})$ ja $\psi(\mathsf{F})$ sievenevät samaksi kaavaksi tai pystytään muuten osoittamaan yhtäpitäviksi, ja jos $\varphi(\mathsf{T})$ ja $\psi(\mathsf{T})$ sievenevät samaksi kaavaksi tai pystytään muuten osoittamaan yhtäpitäviksi, niin $\varphi \Leftrightarrow \psi$ pätee. Jos propositiomuuttujille löytyy totuusarvot joilla $\varphi(\mathsf{F})$ ja $\psi(\mathsf{F})$ tuottavat eri totuusarvot, niin $\varphi \Leftrightarrow \psi$ ei päde, ja löydetyt totuusarvot sekä $P \Leftrightarrow \mathsf{F}$ todistavat sen. Jos propositiomuuttujille löytyy totuusarvot joilla $\varphi(\mathsf{T})$ ja $\psi(\mathsf{T})$ tuottavat eri totuusarvot, niin $\varphi \Leftrightarrow \psi$ ei päde, ja löydetyt totuusarvot sekä $P \Leftrightarrow \mathsf{T}$ todistavat sen.

Kun tätä keinoa sovelletaan yhtäpitävyyteen $P \wedge \mathsf{F} \Leftrightarrow \mathsf{F}$, niin $\varphi(P)$ on $P \wedge \mathsf{F}$ ja $\psi(P)$ on F. Niistä jälkimmäinen on esimerkki siitä, että sulkeiden sisällä voi esiintyä myös propositiomuuttujia joita kaavassa itsessään ei esiinny. Kun keinoa sovelletaan yhtäpitävyyteen $P \wedge Q \Leftrightarrow Q \wedge P$, niin $\varphi(P)$ on $P \wedge Q$ ja $\psi(P)$ on $Q \wedge P$. Tämä havainnollistaa sitä, että sulkeiden sisällä ei välttämättä luetella kaikkia kaavassa esiintyviä propositiomuuttujia.

Todista $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$! 16

Tätä keinoa käyttävät todistukset voidaan esittää tiiviimmin ja selkeämmin seuraavan esimerkin mukaisesti. Siinä todistetaan $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$. Siinä näytetään vain sievennys, jossa jonkin propositiomuuttujan tilalla on F ja sievennys, jossa saman propositiomuuttujan tilalla on T. Todistuksen periaatetta ei kerrata, vaan oletetaan lukijan jo tietävän sen: koska $\Leftrightarrow$:n molemmin puolin olevat kaavat sievenivät samoiksi kun sijoitettiin F, koska ne sievenivät samoiksi kun sijoitettiin T, ja koska muita vaihtoehtoja propositiomuuttujan arvoksi ei ole kuin F ja T, tuottavat kaavat aina saman totuusarvon. Jälkimmäinen sievennys on esitetty takaperin, jolloin sievennysten yhteinen lopputulos on suunnilleen keskellä.

- $(\mathsf{F} \wedge Q) \wedge R \;\Leftrightarrow\; \mathsf{F} \wedge R \;\Leftrightarrow\; \mathsf{F} \;\Leftrightarrow\; \mathsf{F} \wedge (Q \wedge R)$
- $(\mathsf{T} \wedge Q) \wedge R \;\Leftrightarrow\; Q \wedge R \;\Leftrightarrow\; \mathsf{T} \wedge (Q \wedge R)$

Sininen väri on tarkoitettu auttamaan lukijaa näkemään nopeasti mihin F ja T on sijoitettu. Sinun ei tarvitse käyttää sitä vastauksissasi.

Esitä aiempi yhtäpitävyyden $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ todistuksesi tässä tiiviissä muodossa! 17

Äskeiset tulokset todistettiin tekemättä mitään oletuksia P:stä, Q:sta ja R:stä. Siitä seuraa, että ne pätevät aina eli ovat propositiologiikan lakeja. Aiemmin todettiin, että propositiologiikan lait saa ilmaista myös niin, että propositiomuuttujien tilalla on kaavoja edustavat symbolit. Niin saadaan

$$\varphi \wedge (\psi \vee \chi) \;\Leftrightarrow\; (\varphi \wedge \psi) \vee (\varphi \wedge \chi) \qquad \varphi \vee (\psi \wedge \chi) \;\Leftrightarrow\; (\varphi \vee \psi) \wedge (\varphi \vee \chi) \qquad [5]$$

Näitä yhtäpitävyyksiä kutsutaan *osittelulaeiksi* (*distributivity*).

Myös koulumatematiikassa on osittelulaki. Sievennä koulumatematiikan lauseke $a(b+c)$ muotoon, jossa ei esiinny yhtään (eikä)! Jos koulumatematiikan muuttujat vaihdetaan propositiologiikan muuttujiksi, niin miten juuri tekemäsi sievennöksen muut osat pitäisi vaihtaa logiikan symboleiksi, jotta tuloksena olisi [5]:n ensimmäinen laki? 18 19

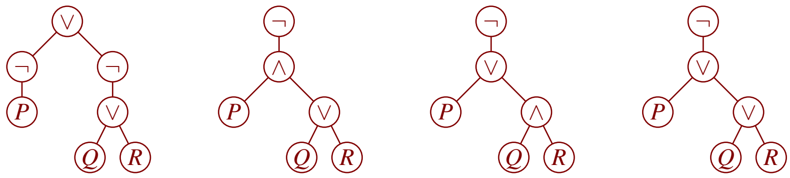
Jos samat vaihdot tehdään toisinpäin, niin mitä saadaan [5]:n toisesta laista? Onko se koulumatematiikan laki? 20

Sievennä myös $d(b+c)$ sulkeettomaan muotoon! Sitä ja vastausta [18] hyödyntämällä sievennä $(a+d)(b+c)$ sulkeettomaan muotoon! 21

Edellisessä tehtävässä käytettiin koulumatematiikan osittelulain muunnosta $(x+y)z = xz + yz$. Kirjoita sen vastine logiikalle (ei tarvitse todistaa, todistamme sen myöhemmin). Kirjoita myös sen muunnelma, jossa $\wedge$ ja $\vee$ on vaihdettu keskenään! 22

Konnektiivi $\neg$ ei yhdistä kahta kaavaa, vaan tulee yhden kaavan eteen. Se luetaan ”ei” ja se vaihtaa kaavan totuusarvon päinvastaiseksi. Niinpä $\neg A$ tarkoittaa ”aurinko ei paista”. Pätee $\neg\mathsf{F} \Leftrightarrow \mathsf{T}$ ja $\neg\mathsf{T} \Leftrightarrow \mathsf{F}$. Niistä seuraa $\neg\neg\varphi \Leftrightarrow \varphi$.

$$\neg\mathsf{F} \Leftrightarrow \mathsf{T} \qquad \neg\mathsf{T} \Leftrightarrow \mathsf{F} \qquad \neg\neg\varphi \Leftrightarrow \varphi \qquad [6]$$



Kuva 7: Lausekepuuesimerkkejä

Jos jokainen kaava on kussakin tilanteessa joko tosi tai epätosi, niin pätee myös $\varphi \vee \neg\varphi \Leftrightarrow \mathsf{T}$ ja $\varphi \wedge \neg\varphi \Leftrightarrow \mathsf{F}$. Ikävä kyllä sekä koulumatematiikassa, ohjelmoinnissa että arkielämässä on paljon tilanteita, joissa väite ei ole tosi eikä epätosi, vaan määrittelemätön. Esimerkiksi $\frac{1}{0} > 0$ on määrittelemätön, koska nollalla ei saa jakaa; ja "viimeinen auto oli sininen, ja sitä seuraava auto oli valkoinen" on määrittelemätön, koska viimeisellä autolla ei ole seuraavaa autoa. Määrittelemättömiä väitteitä voi johonkin rajaan saakka kohdella ikään kuin ne olisivat epätosia, mutta $\neg$:n kohdalla se ei enää onnistu. Esimerkiksi jos $\frac{1}{0} > 0$ olisi epätosi, niin $\neg\big(\frac{1}{0} > 0\big)$ olisi tosi, joten joko $\frac{1}{0} \leq 0$ olisi tosi tai menetettäisiin se laki, että "ei suurempi" on sama asia kuin "pienempi tai yhtäsuuri".

Suurin osa tässä kirjassa esitettävistä laeista pätee sellaisenaan myös määrittelemättömille väitteille. Muiden lakien kohdalla asiasta mainitaan tavalla tai toisella. Niinpä esitämme lait $\varphi \vee \neg\varphi \Leftrightarrow \mathsf{T}$ ja $\varphi \wedge \neg\varphi \Leftrightarrow \mathsf{F}$ seuraavasti:

$$\text{Jos } \varphi \text{ on määritelty, niin} \quad \varphi \vee \neg\varphi \Leftrightarrow \mathsf{T} \quad \text{ja} \quad \varphi \wedge \neg\varphi \Leftrightarrow \mathsf{F}\,. \qquad [7]$$

Sitä milloin kaava on määritelty aletaan käsitellä luvussa **??**. Siihen asti voit käyttää yhtäpitävyyksiä $\varphi \vee \neg\varphi \Leftrightarrow \mathsf{T}$ ja $\varphi \wedge \neg\varphi \Leftrightarrow \mathsf{F}$ kuten muitakin lakeja.

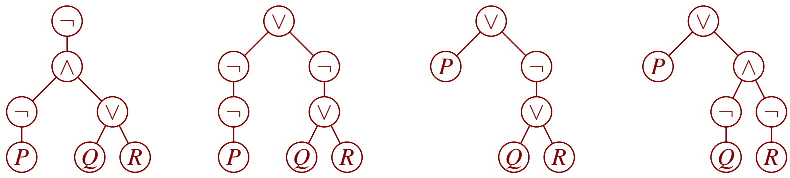
Yhtäpitävyys $\varphi \vee \neg\varphi \Leftrightarrow \mathsf{T}$ voidaan esittää lyhyemmin kaavana $\varphi \vee \neg\varphi$. Aivan kuten aina pätevää yhtäpitävyyttä voidaan kutsua laiksi, myös aina totta kaavaa voidaan kutsua laiksi. Jos φ on aina määritelty, niin $\varphi \vee \neg\varphi$ on laki. Se tunnetaan nimellä *kolmannen poissuljetun laki* (*law of excluded middle*).

Kaava $A \wedge \neg U$ tarkoittaa "aurinko paistaa ja en mene ulos". Kaavaan $\neg A \wedge U$ liittyy ongelma: tarkoittaako se "aurinko ei paista ja menen ulos" vai "ei ole niin, että aurinko paistaa ja menen ulos"? Kuten aiemmin todettiin, tällaiset epäselvyydet voi välttää lisäämällä sulkeet: $(\neg A) \wedge U$ tarkoittaa "aurinko ei paista ja menen ulos" ja $\neg(A \wedge U)$ tarkoittaa "ei ole niin, että aurinko paistaa ja menen ulos". Ikävä kyllä jos sulkeita on paljon, niin ne hankaloittavat kaavan lukemista. Siksi on sovittu, että jollei sulkeita ole, niin $\neg$ vaikuttaa vain seuraavaan atomiseen propositioon. Siis $\neg A \wedge U$ tarkoittaa samaa kuin $(\neg A) \wedge U$.

Nytpäs teemme lausekepuuharjoituksen niin päin, että tehtävänäsi ei ole piirtää vaan tulkita lausekepuita. Kirjoita jokaisesta kuvan 7 lausekepuusta kaava, jossa ei ole turhia sulkeita! 23

Luonnollisessa kielessä käytetään muitakin sanoja kuin "ja", "tai" ja "ei" konnektiiveja $\wedge$, $\vee$ ja $\neg$ vastaavassa merkityksessä. Esimerkiksi sen sijaan että sanottaisiin "en syö jäätelöä ja en katso elokuvaa", yleensä sanotaan "en syö jäätelöä enkä katso elokuvaa". "Otan kahvia ilman sokeria" tarkoittaa "otan kahvia ja en ota siihen sokeria".

Sama merkitys saatetaan ilmaista luonnollisessa kielessä joko sanalla "ja" tai sanalla "tai", riippuen siitä, miten ilmaus on rakennettu. Esimerkiksi "opiskelijat ja eläkeläiset saavat alennuksen" tarkoittaa samaa kuin "jos henkilö on opiskelija tai eläkeläinen, niin hän saa alennuksen". Tästä syystä "ja" ei aina käänny konnektiiviksi "$\wedge$" eikä "tai"



Kuva 8: Esimerkki ¬:den alas painamisesta

aina käänny konnektiiviksi ”$\vee$”, vaan ne voivat mennä päinvastoin. Mitkä luvut toteuttavat $x < 2 \vee x \geq 5$? Älä käytä vastauksessasi symbolia x, vaan sanaa ”luvut”. Ilmaise vastaus sanallisesti ensin siten, että konnektiivia $\vee$ edustaa ”tai”, ja sen jälkeen siten,
että sitä edustaa ”ja”! 24

Maalaisjärki sanoo, että jos ei ole niin että syön jäätelön tai katson elokuvan, niin en syö jäätelöä enkä katso elokuvaa. Myös vastakkainen suunta pätee: jos en syö jäätelöä enkä katso elokuvaa, niin ei ole niin että syön jäätelön tai katson elokuvan. Niinpä maalaisjärjen mukaan $\neg(J \vee E) \Leftrightarrow \neg J \wedge \neg E$. Saman voi helposti todistaa totuustaululla tai sijoittamalla J:hin vuoron perään F ja T. Myös pätee $\neg(J \wedge E) \Leftrightarrow \neg J \vee \neg E$. Tul-
kitse se jäätelön syönnin ja elokuvan katsomisen avulla! Osoita se totuustaululla tai 25
sijoittamalla F ja T! 26

Vaikka tulkitsimmekin J:n ja E:n tarkoittamaan jäätelön syömistä ja elokuvan katsomista, äskeisten yhtäpitävyyksien todistus totuustaululla tai sijoituskeinolla ei nojannut tähän tulkitaan, eikä mihinkään muuhunkaan oletuksiin J:stä ja E:stä. Siksi nekin ovat lakeja, ja siis pätevät myös kun J:n ja E:n tilalla on mielivaltaiset kaavat. Niinpä

$$\neg(\varphi \vee \psi) \;\Leftrightarrow\; \neg\varphi \wedge \neg\psi \qquad\qquad \neg(\varphi \wedge \psi) \;\Leftrightarrow\; \neg\varphi \vee \neg\psi \qquad [8]$$

Ne ovat nimeltään *De Morganin lait* (*De Morgan's laws*).

Yksi usein toistuva käyttökohde De Morganin laeille on ¬:den ”alas painaminen”. Siinä kaava muunnetaan yhtäpitävään muotoon, jossa ei ole ¬:itä muualla kuin välittömästi propositiomuuttujien edessä. Kuvassa 8 on siitä esimerkki esitettynä lausekepuilla. Sen ensimmäisessä ja kolmannessa askeleessa käytetään De Morganin lakeja, ja
toisessa [6]:sta. Esitä sama esimerkki päättelyketjuna kaavoilla ja $\Leftrightarrow$:lla! 27

Kun siirrytään propositiologiikasta yleisempään logiikkaan, tarvitaan muitakin todistamiskeinoja kuin totuustaulut sekä F:n ja T:n sijoittaminen vuoron perään johonkin propositiomuuttujaan. Siksi alamme pikkuhiljaa harjoitella lakien käyttöä todistamisessa. Ensimmäisenä esimerkkinä johdamme jälkimmäisen De Morganin lain edellisestä. Hyödynnämme sitä, että yhtäpitävyyttä saa soveltaa isomman kaavan sisällä olevaan kaavaan. Esimerkiksi koska $\neg\neg P \Leftrightarrow P$, pätee myös $\neg(\neg\neg P \wedge Q) \Leftrightarrow \neg(P \wedge Q)$. Tähän perustuu seuraavan päättelyn viimeinen askel:

$$\neg P \vee \neg Q \;\Leftrightarrow\; \neg\neg(\neg P \vee \neg Q) \;\Leftrightarrow\; \neg(\neg\neg P \wedge \neg\neg Q) \;\Leftrightarrow\; \neg(\neg\neg P \wedge Q) \;\Leftrightarrow\; \neg(P \wedge Q)$$

Missä kohdassa päättelyä käytettiin ensimmäistä De Morganin lakia? Mikä silloin oli 28
φ:n ja mikä ψ:n tilalla? 29

Vielä on kaksi päättelyaskelta tarkastamatta. Miksi ne ovat päteviä? (Tämä on help-
po!) 30

Yhtäpitävyysketju tarkoittaa, että ketjun jokainen kaava tuottaa saman totuusarvon. Niinpä ketjun ensimmäinen ja viimeinen kaava tuottavat saman totuusarvon, eli $\neg P \vee \neg Q \Leftrightarrow \neg(P \wedge Q)$. ”Sama totuusarvo” on symmetrinen käsite, joten $\neg(P \wedge Q) \Leftrightarrow$

$\neg P \vee \neg Q$. Koska emme olettaneet mitään P:stä emmekä Q:sta, saamme kirjoittaa niiden tilalle mielivaltaiset kaavat. Siksi $\neg(\varphi \wedge \psi) \Leftrightarrow \neg\varphi \vee \neg\psi$.

Kreikkalaisten kirjainten korvaaminen propositiomuuttujilla ja lopulta vaihtaminen takaisin kreikkalaisiksi kirjaimiksi saattaa tuntua turhalta päättelyn monimutkaistamiselta, ja usein se onkin sitä. Pidämme kuitenkin siitä jonkin aikaa kiinni, koska se selkeyttää siitä puhumista, mitä lakeja ja miten päättelyn aikana käytettiin. Jos esimerkiksi äskeisen päättelyn tekee P:n ja Q:n sijaan φ:llä ja ψ:llä, niin siihen tulee muun muassa päättelyaskel $\neg\neg(\neg\varphi \vee \neg\psi) \Leftrightarrow \neg(\neg\neg\varphi \wedge \neg\neg\psi)$, jossa sovellettiin De Morganin lakia $\neg(\varphi \vee \psi) \Leftrightarrow \neg\varphi \wedge \neg\psi$ siten, että φ:n tilalla oli $\neg\varphi$ ja ψ:n tilalla oli $\neg\psi$. Tällaisissa menee helposti sekaisin, koska φ ja ψ ovat kaksoisrooleissa.

Mallivastauksissa viitataan lakeihin niiden numeroilla, koska se tekee helpoksi tarkastaa, mistä laista kulloinkin on kyse. Tämän kirjan numeroinnin opettelu olisi tietenkin järjetöntä, joten sinun ei tarvitse käyttää numeroita omissa vastauksissasi. Vastauksissasi ei vaadita nimiäkään, koska vain osalla laeista on vakiintunut suomenkielinen nimi. Riittää, että tiedät lakien sisällön ja pystyt vertaamalla mallivastaukseen tarkastamaan, että olet käyttänyt todellista lakia. Johda [97] [5]:llä ja muilla aikaisemmin esitetyillä logiikan laeilla! 31

Mitä lakeja on käytetty seuraavassa sievennyksessä?

$$P \wedge (\neg P \vee Q) \;\Leftrightarrow\; (P \wedge \neg P) \vee (P \wedge Q) \;\Leftrightarrow\; \mathsf{F} \vee (P \wedge Q) \;\Leftrightarrow\; P \wedge Q$$ 32

Koska nytkään emme olettaneet mitään P:stä emmekä Q:sta, saamme korvata ne kaavoilla. Näin saadaan ensimmäinen seuraavista laeista. Johda jälkimmäinen käyttämällä lakeja (siis ei totuustaulua eikä sijoituskeinoa)! 33

Jos φ on määritelty, niin $\varphi \wedge (\neg\varphi \vee \psi) \;\Leftrightarrow\; \varphi \wedge \psi$ ja $\varphi \vee (\neg\varphi \wedge \psi) \;\Leftrightarrow\; \varphi \vee \psi$. [9]

Näillä kahdella lailla on mielenkiintoinen yhteys ohjelmointiin. Luvuissa **??** ja 8 otetaan käyttöön kolmas totuusarvo U eli "määrittelemätön". Sen voi tulkita edustavan ohjelman *kaatumista* (*crash*) eli suorituksen keskeytymistä siksi, että ohjelma yritti tehdä jotakin kiellettyä tai mahdotonta kuten laskea $\frac{1}{0}$. Monien ohjelmointikielten "ja"-operaattori toimii siten, että vasen puoli lasketaan ensin, ja jos se tuottaa F, niin palautetaan F ilman että oikeaa puolta edes yritetään laskea. Merkitsemme sitä `&&`. Siksi, kun $n = 0$,

$$\textbf{if } n \neq 0 \texttt{ \&\& } \tfrac{10}{n} < 1 \textbf{ then } \mathrm{print}(\text{"true"}) \textbf{ else } \mathrm{print}(\text{"false"})$$

tulostaa "false", mutta

$$\textbf{if } \tfrac{10}{n} < 1 \texttt{ \&\& } n \neq 0 \textbf{ then } \mathrm{print}(\text{"true"}) \textbf{ else } \mathrm{print}(\text{"false"})$$

ei tulosta mitään, vaan kaatuu yritykseen jakaa nollalla. Niinpä `&&` ei ole vaihdannainen, toisin kuin logiikan $\wedge$. Siksi $\wedge$ on sille huono vastine.

Mutta kun U otetaan käyttöön ja samaistetaan ohjelman kaatumiseen, kaavasta $\varphi \wedge (\neg\varphi \vee \psi)$ tulee erinomainen vastine ohjelmoinnin ilmaukselle φ `&&` ψ. Kun φ tuottaa F, tuottavat molemmat F. Kun φ tuottaa U, tuottavat molemmat U, mikä ohjelman tapauksessa tarkoittaa sitä, että kun φ:n laskeminen kaatuu, myös (φ `&&` ψ):n laskeminen kaatuu. Kun φ tuottaa T, tuottavat molemmat sen mitä ψ tuottaa, olipa se sitten F, U eli kaatuminen taikka T. Samaan tapaan kaavasta $\varphi \vee (\neg\varphi \wedge \psi)$ tulee erinomainen vastine monien ohjelmointikielten "tai"-operaattorille. Tämä kuvastaa tarkasti ohjelmoinnissa yleisten "ja"- ja "tai"-operaattoreiden eroa logiikan konnektiiveihin $\wedge$ ja $\vee$. Kun käytetään vain kahta totuusarvoa F ja T, [9]:n vuoksi ero ei tule näkyviin.

Olet ehkä huomannut, että jokaiselle tähän mennessä esitetylle laille on symmetrinen laki, jossa $\wedge$ ja $\vee$ on vaihdettu keskenään ja F ja T on vaihdettu keskenään, eikä muuta ole muutettu. Esimerkkejä tällaisista pareista ovat $\varphi \wedge \neg\varphi \Leftrightarrow \mathsf{F}$ ja $\varphi \vee \neg\varphi \Leftrightarrow \mathsf{T}$ sekä $\mathsf{T} \wedge \psi \Leftrightarrow \psi$ ja $\mathsf{F} \vee \psi \Leftrightarrow \psi$. Myös osittelulait ovat esimerkki, ja samoin De Morganin lait. Tämä symmetria tulee rikkoutumaan kun myöhemmin otamme käyttöön lisää konnektiiveja. Siihen asti se todella on yleispätevä. Seuraavaksi päättelemme, että niin on. Ensin tarvitsemme jossain määrin monimutkaisemman, kaavoja eikä yhtäpitävyyksiä koskevan havainnon. Kuten matematiikoilla on tapana, annamme sille numeron ja esitämme sen selvästi erottuvana niin että se löytyy helposti tarvittaessa. Koska se ei ole kovin suuri tulos, kutsumme sitä apulauseeksi. Sen todistus tulee hieman myöhemmin.

> **Apulause.** Jos φ ei sisällä muita konnektiiveja kuin $\neg$, $\wedge$ ja $\vee$, niin $\neg\varphi$ on yhtäpitävä kaavan kanssa, joka saadaan korvaamalla φ:ssä jokainen $\wedge$ $\vee$:lla ja päinvastoin, jokainen F T:lla ja päinvastoin, ja jokainen $\neg P$ P:llä ja päinvastoin. [10]

Viimeksi mainittu koskee kaavan jokaista propositiomuuttujaa P ja tarkoittaa, että jos P:n edessä on $\neg$, niin se otetaan pois, mutta jos P:n edessä ei ole $\neg$, niin siihen lisätään $\neg$. Muut alkuperäiset $\neg$ kuin propositiomuuttujien edessä olevat jäävät paikalleen. Kun tätä apulausetta käyttää, voi olla viisasta ensin lisätä $\wedge$-muotoisten osakaavojen ympärille sulkeita, jottei vahingossa muunna virheellisesti esimerkiksi $\neg(P \vee Q \wedge R)$ muotoon $\neg P \wedge \neg Q \vee \neg R$. Osoita, että $\neg(P \vee Q \wedge R) \Leftrightarrow \neg P \wedge \neg Q \vee \neg R$ ei ole pätevä! 34

Ennen kuin todistamme, että $\neg\varphi$ todella voidaan aina muuntaa tällaiseen muotoon, näytämme esimerkin. Siinä muunnamme kaavan $\neg(P \wedge \neg(\mathsf{F} \vee \neg Q))$. De Morganin laki tuottaa siitä $\neg P \vee \neg\neg(\mathsf{F} \vee \neg Q)$. Osuus $\neg P$ on sellaisenaan lopullisessa muodossa. Jotta alun perin keskellä ollut $\neg$ jäisi paikalleen, emme muunna $\neg\neg(\mathsf{F} \vee \neg Q)$ poistamalla $\neg\neg$. Sen sijaan teemme ensin tempun, joka ei muuta kaavaa, mutta helpottaa päättelymme seuraamista: vaihdamme $\neg$:n ja $\neg$:n keskenään. Se tuottaa $\neg\neg(\mathsf{F} \vee \neg Q)$. Sitten muunnamme $\neg(\mathsf{F} \vee \neg Q)$ ja lisäämme sen eteen $\neg$. De Morganin laki tuottaa $\neg\mathsf{F} \wedge \neg\neg Q$, josta saadaan $\mathsf{T} \wedge Q$. Niinpä $\neg\neg(\mathsf{F} \vee \neg Q)$ eli $\neg\neg(\mathsf{F} \vee \neg Q)$ tuottaa $\neg(\mathsf{T} \wedge Q)$, ja koko kaava tuottaa $\neg P \vee \neg(\mathsf{T} \wedge Q)$. Tarkasta, että se todella on sama kuin mikä saadaan tekemällä edellä luetellut korvaukset kaavaan $P \wedge \neg(\mathsf{F} \vee \neg Q)$! 35

Nyt todistamme, että $\neg\varphi$ todella voidaan aina muuntaa tällaiseen muotoon. Jos todistuksen jokin kohta on vaikea ymmärtää, etsi vastaava kohta edellä olleesta esimerkistä ja vertaa siihen. Kaavat muotoa $\neg\psi$ jaetaan todistuksessa kahteen tapaukseen: ψ on pelkkä propositiomuuttuja (neljäs tapaus) tai ei ole (viimeinen tapaus).

Todistus apulauseelle [10]. Tarkastelemme kaikkia tapauksia, jotka voivat tulla $\neg\varphi$:n muuntamisessa vastaan. Edustakoon P mitä tahansa propositiomuuttujaa. Oletusten vuoksi φ on jotain seuraavista muodoista: (1) F, (2) T, (3) P jonka edessä ei ole $\neg$, (4) $\neg P$, (5) $\psi \wedge \chi$, (6) $\psi \vee \chi$ sekä (7) sellainen $\neg\psi$, missä ψ on muuta kuin pelkkä propositiomuuttuja.

Kaksi ensimmäistä tapausta muuntuu väitettyyn muotoon lakien $\neg\mathsf{F} \Leftrightarrow \mathsf{T}$ ja $\neg\mathsf{T} \Leftrightarrow \mathsf{F}$ avulla. Kolmannessa tapauksessa $\neg P$ on sellaisenaan väitettyä muotoa, ja $\neg\neg P \Leftrightarrow P$ hoitaa neljännen tapauksen.

Viides tapaus saadaan De Morganin lailla $\neg(\psi \wedge \chi) \Leftrightarrow \neg\psi \vee \neg\chi$ ja muuntamalla $\neg\psi$ ja $\neg\chi$. Kuudes tapaus saadaan samaan tyyliin toisesta De Morganin laista.

Viimeisessä tapauksessa pitää muuntaa $\neg\neg\psi$. Se hoituu jättämällä ensimmäinen $\neg$ paikalleen ja muuntamalla $\neg\psi$. □

Nyt kun olemme nähneet että tällainen muuntaminen voidaan aina tehdä, meidän ei tarvitse tehdä sitä, vaan voimme kirjoittaa lopputuloksen suoraan.

P	$P \land \neg P$
F	F
T	F

F
F

P	F
F	F
T	F

Y	X	$X \land \neg Y$
F	F	F
F	T	T
T	F	F
T	T	F

X	Y	$X \land \neg Y$
F	F	F
F	T	F
T	F	T
T	T	F

Kuva 9: Totuustaulu kaavalle $P \land \neg P$, kaksi totuustaulua kaavalle F ja kaksi totuustaulua kaavalle $X \land \neg Y$

Laeista voidaan johtaa symmetrisiä lakeja seuraavien esimerkkien mukaisesti. Koska $\varphi \lor \neg\varphi \Leftrightarrow \mathsf{T}$ ja koska yhtäpitävyyttä saa soveltaa isomman kaavan sisällä olevaan kaavaan, saadaan $\neg(\varphi \lor \neg\varphi) \Leftrightarrow \neg\mathsf{T}$. Se pätee kun φ:n tilalla on mikä tahansa kaava, joten se pätee kun φ:n tilalla on $\neg P$. Niin saadaan $\neg(\neg P \lor \neg\neg P) \Leftrightarrow \neg\mathsf{T}$. Muuntamalla molemmat puolet apulauseessa [10] kuvatulla tavalla saadaan $P \land \neg P \Leftrightarrow \mathsf{F}$. Koska P:stä ei oletettu mitään, sen tilalle saa sijoittaa φ. Saadaan $\varphi \land \neg\varphi \Leftrightarrow \mathsf{F}$.

Koska $(\varphi \lor \psi) \lor \chi \Leftrightarrow \varphi \lor (\psi \lor \chi)$, pätee $\neg((\varphi \lor \psi) \lor \chi) \Leftrightarrow \neg(\varphi \lor (\psi \lor \chi))$ ja edelleen $\neg((\neg P \lor \neg Q) \lor \neg R) \Leftrightarrow \neg(\neg P \lor (\neg Q \lor \neg R))$. Muuntamalla saadaan $(P \land Q) \land R \Leftrightarrow P \land (Q \land R)$. Koska P:stä, Q:sta ja R:stä ei oletettu mitään, niiden tilalle saa sijoittaa φ, ψ ja χ. Niin saadaan $(\varphi \land \psi) \land \chi \Leftrightarrow \varphi \land (\psi \land \chi)$.

Johda laista $\mathsf{T} \land \psi \Leftrightarrow \psi$ laki $\mathsf{F} \lor \psi \Leftrightarrow \psi$! 36

Johda laista $\varphi \land \psi \Leftrightarrow \psi \land \varphi$ laki $\varphi \lor \psi \Leftrightarrow \psi \lor \varphi$! 37

Valitse jompikumpi osittelulaki ja johda siitä toinen osittelulaki! 38

Teemme tämän nyt mielivaltaiselle laille $\varphi(\chi_1, \ldots, \chi_n) \Leftrightarrow \psi(\chi_1, \ldots, \chi_n)$, missä φ ja ψ eivät sisällä muita konnektiiveja kuin $\neg$, $\land$ ja $\lor$, ja $\chi_1, \ldots, \chi_n$ ovat laissa esiintyvät mielivaltaiset kaavat. Esimerkiksi lain $\varphi \land (\neg\varphi \lor \psi) \Leftrightarrow \varphi \land \psi$ tapauksessa χ_1 on φ, χ_2 on ψ, $\varphi(\chi_1, \chi_2)$ on $\chi_1 \land (\neg\chi_1 \lor \chi_2)$ ja $\psi(\chi_1, \chi_2)$ on $\chi_1 \land \chi_2$.

Aluksi saamme $\neg\varphi(\chi_1, \ldots, \chi_n) \Leftrightarrow \neg\psi(\chi_1, \ldots, \chi_n)$. Koska $\chi_1, \ldots, \chi_n$ saavat olla mitä tahansa kaavoja, niiden tilalla saa olla $\neg P_1, \ldots, \neg P_n$, missä $P_1, \ldots, P_n$ ovat propositiomuuttujia, joita ei ole aiemmin käytetty. (Koska niitä ei ole aiemmin käytetty, voimme myöhemmin vedota siihen, että niistä ei ole oletettu mitään.) Siten saadaan $\neg\varphi(\neg P_1, \ldots, \neg P_n) \Leftrightarrow \neg\psi(\neg P_1, \ldots, \neg P_n)$. Soveltamalla sen molempiin puoliin apulausetta [10] saadaan $\varphi'(P_1, \ldots, P_n) \Leftrightarrow \psi'(P_1, \ldots, P_n)$, missä φ' ja ψ' ovat ne mitä saadaan, kun φ:ssä ja ψ:ssä korvataan jokainen $\land$ $\lor$:lla ja päinvastoin sekä jokainen F T:lla ja päinvastoin. Koska P_1:stä, $\ldots$, P_n:stä ei ole oletettu mitään, niiden tilalle saa sijoittaa $\chi_1, \ldots, \chi_n$. Se tuottaa $\varphi'(\chi_1, \ldots, \chi_n) \Leftrightarrow \psi'(\chi_1, \ldots, \chi_n)$. Se on alkuperäiselle laille $\varphi(\chi_1, \ldots, \chi_n) \Leftrightarrow \psi(\chi_1, \ldots, \chi_n)$ symmetrinen laki.

Tämä on niin hieno ja käyttökelpoinen tulos, ja sen johtamisessa oli niin paljon vaivaa, että olisi sääli, jos se hukkuisi tekstin sekaan. Siksi muotoilemme sen matemaattiseksi lauseeksi (voit unohtaa ”yhtäaikaa määritellyt” lukuun **??** saakka):

> **Lause.** Jos $\varphi(\chi_1, \ldots, \chi_n) \Leftrightarrow \psi(\chi_1, \ldots, \chi_n)$ on laki, missä φ ja ψ eivät sisällä muita konnektiiveja kuin $\neg$, $\land$ ja $\lor$, ja jos φ ja ψ ovat yhtäaikaa määritellyt, niin myös $\varphi'(\chi_1, \ldots, \chi_n) \Leftrightarrow \psi'(\chi_1, \ldots, \chi_n)$ on laki, missä φ' ja ψ' on saatu korvaamalla φ:ssä ja ψ:ssä jokainen $\land$ $\lor$:lla ja päinvastoin sekä jokainen F T:lla ja päinvastoin. Myös φ' ja ψ' ovat yhtäaikaa määritellyt. [11]

2.2 Totuusfunktiot

Kun yritetään osoittaa $P \land \neg P \Leftrightarrow \mathsf{F}$ erillisten totuustaulujen avulla, törmätään ilmiöön, jota on havainnollistettu kuvassa 9. (Ilmiö ei esiinny, jos tehdään yhdistetty totuustau-

P	Q	$\neg Q$	$P \vee \neg Q$	$\neg(P \vee \neg Q)$
F	F	T	T	F
F	T	F	F	T
T	F	T	T	F
T	T	F	T	F

P	Q	$\neg P$	$\neg P \wedge Q$
F	F	T	F
F	T	T	T
T	F	F	F
T	T	F	F

Y	X	$X \wedge \neg Y$
F	F	F
F	T	T
T	F	F
T	T	F

Kuva 10: Totuustaulut kaavoille $\neg(P \vee \neg Q)$, $\neg P \wedge Q$ ja $X \wedge \neg Y$

lu, jossa molemmat kaavat ovat samassa totuustaulussa.) Sen vasemmassa reunassa on mahdollisimman yksinkertainen totuustaulu kaavalle $P \wedge \neg P$, ja seuraavana on mahdollisimman yksinkertainen totuustaulu kaavalle F. Niiden ruskeat alueet eivät ole samanlaiset, vaikka $P \wedge \neg P$ ja F ovat yhtäpitävät. Kaavalle F saa kuitenkin ruskeilta alueilta samanlaisen totuustaulun kuin vasemmassa reunassa, jos ottaa P:n mukaan totuustauluun, vaikka se ei esiinny kaavassa F. Se on kuvassa kolmantena. Tämä esimerkki osoittaa, että toisinaan on hyödyllistä ottaa totuustauluun mukaan propositiomuuttujia, joita kaavassa ei ole.

Kuvan 9 kaksi viimeistä totuustaulua havainnollistavat, että propositiomuuttujien esittämisjärjestyksellä on merkitystä. Ne esittävät samaa kavaa, mutta niiden ruskeat alueet ovat erilaiset, koska toisiaan vastaavat rivit ovat eri kohdissa. Ne ovat eri kohdissa siksi, että propositiomuuttujat ovat eri järjestyksessä.

Olemme nähneet useita esimerkkejä, joissa kaksi eri kaavaa ovat yhtäpitävät, eli ne tuottavat aina saman totuusarvon. Jos yhtäpitäville kaavoille tehdään totuustaulut, joissa on täsmälleen samat propositiomuuttujat ja ne on lueteltu samassa järjestyksessä, niin totuustaulut ovat otsikkoriviä ja välitulossarakkeita lukuun ottamatta täysin samanlaiset. Tätä on havainnollistettu kuvassa 10. Kuvassa on esimerkki myös siitä, että otsikkoriviä ja välitulossarakkeita lukuun ottamatta täysin samanlaisen totuustaulun voi tuottaa myös toisilla propositiomuuttujilla.

Kuvan 10 jokainen totuustaulu ilman otsikkoriviä ja välitulossarakkeita esittää saman kaksipaikkaisen *totuusfunktion* (*truth function*). Kaksipaikkainen totuusfunktio liittää jokaiseen kahden totuusarvon muodostamaan pariin jonkin totuusarvon. Kuvassa 10 (peräti kolmeen kertaan) esitetty totuusfunktio liittää pariin (F,T) totuusarvon T ja jokaiseen muuhun pariin (siis pareihin (F,F), (T,F) ja (T,T)) totuusarvon F. Pariin kuuluvia arvoja kutsutaan funktion *argumenteiksi* (*arguments*), ja pariin liitetty arvo on funktion *tulos* (*result*) eli funktion *arvo* (*value*). Jos kuvan 10 funktiolle annetaan nimeksi $\underline{\varphi}$, niin $\underline{\varphi}(\mathsf{F},\mathsf{T}) \Leftrightarrow \mathsf{T}$ eli $\underline{\varphi}$:n tulos argumenteilla F ja T on T. Nimessä oleva alleviivaus korostaa sitä, että nyt puhe ei ole kaavasta vaan totuusfunktiosta.

Kaksipaikkaisen totuusfunktion käsitteessä ei mikään muu ole olennaista kuin se, mikä totuusarvo on liitetty mihinkin pariin, eli mikä on totuusfunktion tulos milläkin argumenteilla. Pariin (F,F) liitettävällä totuusarvolla on kaksi eri vaihtoehtoa: F ja T. Siis kaksipaikkaisen totuusfunktion tulos argumenteilla F ja F voi olla F tai T, eikä se voi olla mitään muuta. Pariin (F,T) liitettävällä totuusarvolla on samat kaksi eri vaihtoehtoa, ja samoin pareille (T,F) ja (T,T). Kaikkiaan eri mahdollisuuksia on $2 \cdot 2 \cdot 2 \cdot 2$ eli 16. On siis olemassa täsmälleen 16 kaksipaikkaista totuusfunktiota.

Totuusfunktion argumenttien määrä voi olla mikä tahansa positiivinen kokonaisluku. Yksipaikkainen totuusfunktio liittää jokaiseen totuusarvoon jonkin totuusarvon, kolmepaikkainen totuusfunktio liittää jokaiseen totuusarvojen kolmikkoon jonkin totuusarvon ja niin edelleen. Jos valitaan jokin propositiomuuttuja edustamaan paikkaa 1, jokin toinen propositiomuuttuja edustamaan paikkaa 2 ja niin edelleen paikkaan n saakka, niin jokainen kaava, jossa ei esiinny muita propositiomuuttujia kuin juuri va-

P	F
F	F
T	F

P	P
F	F
T	T

P	$\neg P$
F	T
T	F

P	T
F	T
T	T

Kuva 11: Kaikki yksipaikkaiset totuusfunktiot, kun propositiomuuttujana on P

littuja, esittää jonkin n-paikkaisen totuusfunktion. Kuvassa 10 on ensin valittu P edustamaan paikkaa 1 ja Q paikkaa 2, ja sitten Y edustamaan paikkaa 1 ja X paikkaa 2. Tällaisia valintoja voi ilmaista merkinnöillä $\underline{\varphi}(P,Q)$ ja $\underline{\varphi}(Y,X)$.

Totuusfunktion käsite laajenee luontevasti myös nollaan paikkaan. Nollapaikkaisia totuusfunktioita on kaksi erilaista. Niitä esittävät kaavat F ja T.

Kuvassa 11 on näytetty kaikki yksipaikkaiset totuusfunktiot. Jokainen on myös esitetty mahdollisimman yksinkertaisella kaavalla. Kaavoissa käytettäväksi propositiomuuttujaksi on valittu P. Kuvan kaavat ovat F, P, $\neg P$ ja T. Niistä kahdessa P ei esiinny. Tulemme myöhemmin kohtaamaan kolmepaikkaisen totuusfunktion $\underline{\varphi}(P,Q,R)$, jota esittää kaava $\neg(P \vee R)$, jossa Q ei esiinny. Jos jotakin paikkaa edustava propositiomuuttuja ei esiinny totuusfunktiota esittävässä kaavassa, niin totuusfunktion tulos ei riipu kyseessä olevan propositiomuuttujan totuusarvosta. Päinvastainen suunta ei päde, eli totuusfunktion tulos ei välttämättä riipu kaavassa esiintyvän propositiomuuttujan totuusarvosta. Esimerkki tästä on $P \wedge \neg P$. Se voisi olla kaavan F tilalla kuvan 11 ensimmäisen totuustaulun oikeassa ylänurkassa.

Totuusfunktion argumenttien määrä voi siis olla suurempi kuin sitä esittävässä kaavassa esiintyvien propositiomuuttujien määrä. Kaava ei myöskään kerro, mitä paikkaa mikäkin propositiomuuttuja edustaa. Kun samalla kertaa puhutaan useista kaavoista, niin jollei muuta ole sanottu, niin voit olettaa, että sama propositiomuuttuja edustaa eri kaavoissa aina samaa paikkaa. Jos propositiomuuttuja esiintyy yhdessä kaavassa mutta ei toisessa, niin se esittää samaa paikkaa myös siinä kaavassa, jossa se ei esiinny. Tällä oletuksella, φ ja ψ esittävät saman totuusfunktion jos ja vain jos $\varphi \Leftrightarrow \psi$ pätee aina eli on propositiologiikan laki.

Sen totuusfunktion $\underline{\varphi}(P,Q)$, jonka esittää $\neg P \vee Q$, voi esittää monella muullakin kaavalla, kuten $\neg P \vee Q \vee$ F, $\neg P \vee Q \vee$ F $\vee$ F, $\neg P \vee Q \vee Q$ ja $\neg(P \wedge \neg Q)$. Jos totuusfunktion voi esittää jollain kaavalla, niin sen voi esittää äärettömän monella eri kaavalla. Kaavan peräänhän voi aina liittää " $\vee$ F", jolloin saadaan eri kaava esittämään samaa totuusfunktiota.

Erilaisten totuusfunktioiden määrä kasvaa rajusti kun argumenttien määrä kasvaa. Nollapaikkaisia totuusfunktioita on vain kaksi, nimittäin kaavojen F ja T esittämät. Yksipaikkaisia totuusfunktioita on neljä, ja ne on näytetty kuvassa 11. Laskimme aiemmin, että kaksipaikkaisia totuusfunktioita on 16. Kumpikin jälkimmäinen luku on edellisen neliö: $4 = 2 \cdot 2$ ja $16 = 4 \cdot 4$. Se ei ole sattumaa, vaan kuten kohta näemme, se pätee kaikille isommillekin argumenttien määrille. Niinpä kolmepaikkaisia totuusfunktioita on $16 \cdot 16 = 256$, nelipaikkaisia $256 \cdot 256 = 65\,536$, viisipaikkaisia $65\,536 \cdot 65\,536 = 4\,294\,967\,296$ ja kuusipaikkaisia $18\,446\,744\,073\,709\,551\,616$.

Totuusfunktiolle olennaista on vain, mikä tulos tulee milläkin argumenttien arvoilla. Totuusfunktiot $\underline{\varphi}(P_1,\ldots,P_n)$ ja $\underline{\psi}(P_1,\ldots,P_n)$ ovat samat, jos ja vain jos valitaanpa kukin $P_1, \ldots, P_n$ miten tahansa vaihtoehdoista F ja T, niin $\underline{\varphi}(P_1,\ldots,P_n)$ ja $\underline{\psi}(P_1,\ldots,P_n)$ tuottavat aina saman tuloksen (joka on F tai T). Saman voi sanoa kielteisen kautta: $\underline{\varphi}(P_1,\ldots,P_n)$ ja $\underline{\psi}(P_1,\ldots,P_n)$ ovat erit, jos ja vain jos on olemassa yksikin sellainen totuusarvojen valinta P_1:lle, …, P_n:lle, että $\underline{\varphi}(P_1,\ldots,P_n)$ ja $\underline{\psi}(P_1,\ldots,P_n)$ tuottavat eri totuusarvon.

P_1	P_2	$\underline{\varphi}$
F	F	F
F	T	T
T	F	F
T	T	F

P_1	$\underline{\varphi_{\mathsf{F}}}$
F	F
T	F

P_1	P_2	$\underline{\varphi}$
F	F	F
F	T	T
T	F	F
T	T	F

P_1	$\underline{\varphi_{\mathsf{T}}}$
F	T
T	F

Kuva 12: $\underline{\varphi_{\mathsf{F}}}$:n ja $\underline{\varphi_{\mathsf{T}}}$:n muodostaminen

Kaava on konkreettinen käsite: sen voi kirjoittaa sellaisenaan kynällä paperille. Totuusfunktio on abstrakti käsite: sitä ei voi sellaisenaan kirjoittaa kynällä paperille, vaan voi kirjoittaa vain sen esityksen jollakin esitystavalla. Olemme tähän mennessä esittäneet totuusfunktioita totuustaulujen avulla ja kaavojen avulla. On selvää, että jokaisen totuusfunktion voi esittää totuustaulun avulla, ja osoitamme kohta, että jokaisen totuusfunktion voi esittää kaavan avulla.

On kuitenkin myös olemassa tärkeitä abstrakteja käsitteitä, joissa esittäminen on toisinaan mahdotonta. Kouluissa puhutaan lukusuorasta, mutta ei ole olemassa esitystapaa, joka pystyy esittämään minkä tahansa lukusuoralla sijaitsevan luvun. Myös voi käydä niin, että esittäminen on mahdollista, mutta esityksillä ei voi tehdä kaikkea mitä haluttaisiin. Esimerkiksi on olemassa esitystapa, joka pystyy esittämään poikkeuksellisen paljon lukusuoran eri lukuja, mutta jossa on toisinaan mahdotonta saada selville, esittävätkö kaksi eri esitystä saman luvun. Tästä syystä on tärkeää ymmärtää ero abstraktin käsitteen ja sitä esittävän käsitteen välillä. Logiikassa ja teoreettisessa tietojenkäsittelytieteessä on hyvin paljon kyse siitä, mitä voidaan esittää ja mitä ei voida, sekä mitä esityksillä voi tehdä ja kuinka tehokkaasti.

Olkoon $\underline{\varphi}(P_1,\ldots,P_n)$ mikä tahansa n-paikkainen totuusfunktio, missä $n > 0$. Jos sen totuustaulusta poistetaan sarake P_n sekä rivit, joissa $P_n \Leftrightarrow \mathsf{T}$, niin jäljelle jää erään $(n-1)$-paikkaisen totuusfunktion totuustaulu. (Lopputulossarakkeen nimi voi nyt olla väärä, mutta emme piittaa siitä.) Tätä on havainnollistettu kuvassa 12. Merkitsemme näin saatua totuusfunktiota $\underline{\varphi_{\mathsf{F}}}(P_1,\ldots,P_{n-1})$. Alaindeksi F muistuttaa, että jäljelle jääneillä riveillä $P_n \Leftrightarrow \mathsf{F}$. Poistamalla sarake P_n sekä rivit, joissa $P_n \Leftrightarrow \mathsf{F}$, saadaan $(n-1)$-paikkainen totuusfunktio, jota merkitsemme $\underline{\varphi_{\mathsf{T}}}(P_1,\ldots,P_{n-1})$. Seuraavaksi päättelemme, että jos kaavat φ_{F} ja φ_{T} esittävät totuusfunktiot $\underline{\varphi_{\mathsf{F}}}$ ja $\underline{\varphi_{\mathsf{T}}}$, niin

$$\underline{\varphi}(P_1,\ldots,P_n) \;\Leftrightarrow\; \neg P_n \wedge \varphi_{\mathsf{F}}(P_1,\ldots,P_{n-1}) \;\vee\; P_n \wedge \varphi_{\mathsf{T}}(P_1,\ldots,P_{n-1})$$

Nimittäin kun $P_n \Leftrightarrow \mathsf{F}$, niin oikea puoli sievenee muotoon $\neg\mathsf{F} \wedge \varphi_{\mathsf{F}}(P_1,\ldots,P_{n-1}) \vee \mathsf{F} \wedge \varphi_{\mathsf{T}}(P_1,\ldots,P_{n-1})$ ja edelleen muotoon $\varphi_{\mathsf{F}}(P_1,\ldots,P_{n-1})$. Jokainen valinta, jossa kukin $P_1, \ldots, P_{n-1}$ saa totuusarvon F tai T, vastaa jotakin riviä $\underline{\varphi_{\mathsf{F}}}$:n totuustaulussa. Se tehtiin siitä $\underline{\varphi}$:n totuustaulun rivistä, jota vastaa $\underline{\varphi}(P_1,\ldots,P_{n-1},\mathsf{F})$. Siksi näissä kahdessa rivissä on sama totuusarvo tulossarakkeen kohdalla. Niinpä $\underline{\varphi}(P_1,\ldots,P_{n-1},\mathsf{F}) \Leftrightarrow \underline{\varphi_{\mathsf{F}}}(P_1,\ldots,P_{n-1})$. Samalla tavalla nähdään, että $\underline{\varphi}(P_1,\ldots,P_{n-1},\mathsf{T}) \Leftrightarrow \underline{\varphi_{\mathsf{T}}}(P_1,\ldots,P_{n-1})$ $\Leftrightarrow \neg\mathsf{T} \wedge \varphi_{\mathsf{F}}(P_1,\ldots,P_{n-1}) \vee \mathsf{T} \wedge \varphi_{\mathsf{T}}(P_1,\ldots,P_{n-1})$.

Jos $\underline{\varphi_{\mathsf{F}}}(P_1,\ldots,P_{n-1})$ ja $\underline{\varphi'_{\mathsf{F}}}(P_1,\ldots,P_{n-1})$ ovat eri totuusfunktioita, niin ne tuottavat jollakin P_1:n, $\ldots$, P_{n-1}:n totuusarvojen yhdistelmällä eri totuusarvon. Jos lisäksi valitaan $P_n \Leftrightarrow \mathsf{F}$, niin kaavat $\neg P_n \wedge \varphi_{\mathsf{F}}(P_1,\ldots,P_{n-1}) \vee P_n \wedge \varphi_{\mathsf{T}}(P_1,\ldots,P_{n-1})$ ja $\neg P_n \wedge \varphi'_{\mathsf{F}}(P_1,\ldots,P_{n-1}) \vee P_n \wedge \varphi_{\mathsf{T}}(P_1,\ldots,P_{n-1})$ tuottavat eri totuusarvon. (Varmaan arvasit, että φ'_{F} tarkoittaa mitä tahansa kaavaa, joka esittää $\underline{\varphi'_{\mathsf{F}}}$:n.) Sama pätee myös $\underline{\varphi_{\mathsf{T}}}$:lle valinnalla $P_n \Leftrightarrow \mathsf{T}$. Niinpä jokainen eri valinta $\underline{\varphi_{\mathsf{F}}}$:ksi ja/tai $\underline{\varphi_{\mathsf{T}}}$:ksi tuottaa eri totuusfunktion $\underline{\varphi}$. Siksi n-paikkaisia totuusfunktioita on yhtä paljon kuin eri tapoja valita $\underline{\varphi_{\mathsf{F}}}$ kertaa eri tapoja valita $\underline{\varphi_\mathsf{T}}$. Se puolestaan on $(n-1)$-paikkaisten totuusfunktioiden määrän neliö, koska eri tapoja valita $\underline{\varphi_\mathsf{F}}$ on yhtä paljon kuin $(n-1)$-paikkaisia totuusfunktioita, ja sama pätee $\underline{\varphi_\mathsf{T}}$:lle. Olemme lunastaneet lupauksemme osoittaa, että aina kun argumenttien määrä kasvaa yhdellä, niin totuusfunktioiden määrä neliöityy.

Erilaisten totuusfunktioiden määrä voidaan laskea myös seuraavasti. Kun argumenttien määrä kasvaa yhdellä, totuustaulun rivien määrä kaksinkertaistuu (otsikkorivi pois lukien). Niinpä jos paikkoja on n, on totuustaulussa 2^n riviä. Koska jokaiselle riville on valittava tulos kahdesta vaihtoehdosta F ja T, on eri mahdollisuuksia eli erilaisia totuusfunktioita kaikkiaan 2^{2^n}. (Neliöitymisen voi osoittaa tästä laskemalla $(2^{2^{n-1}})^2 = 2^{2\cdot 2^{n-1}} = 2^{2^n}$.)

Lause. Jokainen kaksiarvoisen logiikan totuusfunktio $\underline{\varphi}$ voidaan esittää propositiologiikan kaavalla. [12]

Todistus. Jos $\underline{\varphi}$:n argumenttien määrä on nolla, niin joko F tai T esittää sen. Muussa tapauksessa muodostetaan totuusfunktiot $\underline{\varphi_\mathsf{F}}$ ja $\underline{\varphi_\mathsf{T}}$ edellä kuvatulla tavalla, muodostetaan niille kaavat φ_F ja φ_T, ja yhdistetään ne kaavaksi $\neg P_n \wedge \varphi_\mathsf{F} \vee P_n \wedge \varphi_\mathsf{T}$. Jos $\underline{\varphi_\mathsf{F}}$ ei ole nollapaikkainen, niin siihen sovelletaan samaa menetelmää, eli muodostetaan totuusfunktiot $\underline{\varphi_\mathsf{FF}}$ ja $\underline{\varphi_\mathsf{FT}}$, niistä kaavat φ_FF ja φ_FT, ja yhdistetään ne kaavaksi $\neg P_{n-1} \wedge \varphi_\mathsf{FF} \vee P_{n-1} \wedge \varphi_\mathsf{FT}$. Tarvittaessa myös $\underline{\varphi_\mathsf{FF}}$:iin sovelletaan samaa menetelmää ja niin edelleen. □

Tämä esitystapa ei läheskään aina ole käytännöllinen, mutta silti se riittää osoittamaan, että jokainen totuusfunktio voidaan esittää.

Itse asiassa riittää, että käytettävissä on propositiomuuttujia, sulkeet, F sekä nimellä NAND tunnettu konnektiivi, jolle pätee $P \,\text{NAND}\, Q \Leftrightarrow \neg(P \wedge Q)$. Nimittäin T saadaan muodossa $\mathsf{F} \,\text{NAND}\, \mathsf{F}$, ja $\neg P_n \wedge \varphi_\mathsf{F} \vee P_n \wedge \varphi_\mathsf{T}$ muodossa $((P_n \,\text{NAND}\, P_n) \,\text{NAND}\, \varphi_\mathsf{F}) \,\text{NAND}\, (P_n \,\text{NAND}\, \varphi_\mathsf{T})$.

Sen sijaan jos käytettävissä on vain propositiomuuttujia, sulkeet, F, T, $\wedge$ ja $\vee$ (siis $\neg$ puuttuu), niin kaikkia totuusfunktioita ei voida esittää, vaan ainoastaan *kasvavat* totuusfunktiot. Ennen kuin todistamme että näin on, on meidän tutustuttava kasvavuuden käsitteeseen.

Totuusfunktio on *kasvava* (*increasing*), jos ja vain jos aina kun nolla tai useampi argumentti muuttuu F:sta T:ksi muiden argumenttien pysyessä muuttumattomina, totuusfunktion tulos joko säilyy ennallaan tai muuttuu F:sta T:ksi. Tämän voi ilmaista kaavoilla niin, että P_i ja Q_i edustavat paikassa i olevaa argumenttia ennen ja jälkeen muutoksen. Ehdon, että argumentti ei muutu tai muuttuu F:sta T:ksi, voi ilmaista kaavana $\neg P_i \vee Q_i$, sillä se tuottaa F jos ja vain jos $P_i \Leftrightarrow \mathsf{T}$ ja $Q_i \Leftrightarrow \mathsf{F}$. Niinpä kaavan $\varphi(P_1,\dots,P_n)$ esittämä totuusfunktio on kasvava, jos ja vain jos seuraava ehto pätee aina:

$$\text{Jos } \neg P_1 \vee Q_1, \dots, \neg P_n \vee Q_n, \text{ niin } \neg\varphi(P_1,\dots,P_n) \vee \varphi(Q_1,\dots,Q_n).$$

Saman voi ilmaista kielteisen kautta: totuusfunktio ei ole kasvava jos ja vain jos on olemassa ainakin yksi sellainen tapa antaa sen argumenteille totuusarvot, että kun nolla tai useampia argumentteja muutetaan F:sta T:ksi muiden argumenttien pysyessä muuttumattomina, niin totuusfunktion tulos muuttuu T:sta F:ksi. Esimerkiksi kaavan $\neg P \vee Q$ esittämä totuusfunktio ei ole kasvava, sillä $\neg\mathsf{F} \vee \mathsf{F} \Leftrightarrow \mathsf{T}$ mutta $\neg\mathsf{T} \vee \mathsf{F} \Leftrightarrow \mathsf{F}$. Tässä esimerkissä P:n totuusarvo muuttui F:sta T:ksi ja Q:n totuusarvo säilyi ennallaan, mutta kaavan tulos muuttui T:sta F:ksi.

Seuraavien kaavojen esittämät kaksipaikkaiset totuusfunktiot ovat kasvavia: F, T, P, Q, $P \wedge Q$ ja $P \vee Q$. Kaksi viimeksi mainittua on helppo tarkastaa kuvasta 13. Kun

$P \wedge Q$	F	T
F	F	F
T	F	T

$P \vee Q$	F	T
F	F	T
T	T	T

$\neg P \vee Q$	F	T
F	T	T
T	F	T

Kuva 13: Taulukoita kasvavuuden ja vähenevyyden tarkastamista varten

sen kummassa tahansa sinisessä alueessa kuljetaan alas (eli P muuttuu F:sta T:ksi), oikealle (eli Q muuttuu) tai alas oikealle (eli molemmat muuttuvat), niin tulos joko säilyy ennallaan tai muuttuu F:sta T:ksi. Kaksi ensin mainittua ovat kasvavia, koska niiden tulos ei milloinkaan muutu, joten se ei milloinkaan muutu T:sta F:ksi. Perustele, että myös kaksi keskimmäistä ovat kasvavia! 39

Jos kasvavan totuusfunktion nolla tai useampi argumentti muuttuu T:sta F:ksi, niin totuusfunktion tulos joko säilyy ennallaan tai muuttuu T:sta F:ksi. Tämän tietää siitä, että näin syntynyt muutos voidaan peruuttaa muuttamalla muuttuneet argumentit takaisin T:ksi. Kasvavuuden määritelmän mukaan tällöin totuusfunktion tulos joko säilyy ennallaan tai muuttuu F:sta T:ksi. Koska tämä oli alkuperäisen muutoksen peruutus, niin alkuperäisessä muutoksessa totuusfunktion tulos joko säilyi ennallaan tai muuttui T:sta F:ksi.

Kasvavuus on siis sitä, että aina kun nolla tai useampi argumentti muuttuu samaan suuntaan, niin totuusfunktion tulos joko säilyy ennallaan tai muuttuu samaan suuntaan. Tälle tärkeä sukulaiskäsite on vähenevyys. Aina kun nolla tai useampi argumentti muuttuu samaan suuntaan, niin vähenevän totuusfunktion tulos joko säilyy ennallaan tai muuttuu vastakkaiseen suuntaan. Siis kaavan $\varphi(P_1,\ldots,P_n)$ esittämä totuusfunktio on *vähenevä* (*decreasing*), jos ja vain jos seuraava ehto pätee aina:

$$\text{Jos } \neg P_1 \vee Q_1, \ldots, \neg P_n \vee Q_n, \text{ niin } \varphi(P_1,\ldots,P_n) \vee \neg\varphi(Q_1,\ldots,Q_n).$$

Jos P muuttuu F:sta T:ksi, niin $\neg P$ muuttuu T:sta F:ksi. Siksi seuraava pätee. Se on niin yksinkertainen todistaa, että emme tohdi kutsua sitä lauseeksi. Se on kuitenkin niin hyödyllinen, että se kannattaa esittää näkyvästi. Se pätee myös kolmiarvoisessa logiikassa, kun kasvavuus ja vähenevyys määritellään asianmukaisesti.

> **Apulause.** Jos φ:n esittämä totuusfunktio on kasvava, niin $\neg\varphi$:n esittämä on vähenevä. Jos φ:n esittämä totuusfunktio on vähenevä, niin $\neg\varphi$:n esittämä on kasvava. [13]

Niinpä seuraavien kaavojen esittämät totuusfunktiot ovat väheneviä: F, T, $\neg P$, $\neg Q$, $\neg(P \wedge Q)$ ja $\neg(P \vee Q)$. Kaavan $\neg P \vee Q$ esittämä totuusfunktio ei ole vähenevä, sillä $\neg \mathsf{T} \vee \mathsf{F} \Leftrightarrow \mathsf{F}$ mutta $\neg \mathsf{T} \vee \mathsf{T} \Leftrightarrow \mathsf{T}$. Tässä esimerkissä Q:n totuusarvo muuttui F:sta T:ksi ja P:n totuusarvo säilyi ennallaan, mutta kaavan tulos muuttui F:sta T:ksi.

Olkoon argumenttien määrä mikä tahansa. Näimme, että F:n esittämä totuusfunktio on sekä kasvava että vähenevä. Tämä voi vaikuttaa omituiselta, sillä sen tuottama totuusarvo on vakio eli se ei muutu millään tavalla, vaikka argumentteja muutettaisiin miten tahansa. Sama pätee T:n esittämälle totuusfunktiolle. Tämä ei vastaa sanojen ”kasvaa” ja ”vähetä” käyttöä luonnollisessa kielessä. On melko tavallista, että sanan merkitys matematiikassa on vain osittain sama kuin sen merkitys luonnollisessa kielessä. Matematiikassa käytetään käsitettä ”kasvaa tai ei muutu” niin usein, että sille tarvitaan lyhyt ilmaus. Myös käytetään ilmausta ”ei-vähenevä”, mutta se ei erotu kunnolla ilmauksesta ”ei vähenevä”. Ne tarkoittavat eri asiaa, sillä vaikka esimerkiksi kaavan $\neg P \vee Q$ esittämä totuusfunktio ei ole vähenevä, ei se ole ei-väheneväkään (eli kasvava).

Ilmaus ”aidosti kasvava” tarkoittaa matematiikassa sitä, että jos mikä tahansa argumentti muuttuu, niin tulos muuttuu samaan suuntaan — varmasti muuttuu eikä pysy ennallaan. Mikään vähintään kaksipaikkainen totuusfunktio ei ole aidosti kasvava, sillä se vaatisi että $\underline{\varphi}(\mathsf{F},\mathsf{F})$, $\underline{\varphi}(\mathsf{F},\mathsf{T})$ ja $\underline{\varphi}(\mathsf{T},\mathsf{T})$ saavat kaikki eri totuusarvon, mutta se ei ole mahdollista, koska eri totuusarvoja on vain kaksi. Siksi ”aidosti kasvava” on jokseenkin hyödytön käsite totuusfunktioista puhuttaessa.

Kaavan $\neg P \vee Q$ esittämä totuusfunktio ei siis ole kasvava eikä vähenevä. Se on kuitenkin *kasvava Q:n suhteen* ja *vähenevä P:n suhteen*. Se tarkoittaa, että aina kun Q muuttuu (ja mikään muu propositiomuuttuja ei muutu), niin tulos säilyy ennallaan tai muuttuu samaan suuntaan, ja aina kun P muuttuu (ja mikään muu propositiomuuttuja ei muutu), niin tulos säilyy ennallaan tai muuttuu vastakkaiseen suuntaan. Tarkasta kuvan 13 violetista alueesta, että $\neg P \vee Q$ todella toteuttaa nämä ehdot! 40

Formaalimmin sanottuna, olkoon $1 \leq i \leq n$. Kaavan $\varphi(P_1,\dots,P_n)$ esittämä totuusfunktio on kasvava paikan i suhteen, jos ja vain jos kun annetaan P_1:lle, …, P_{i-1}:lle, P_{i+1}:lle, …, P_n:lle mitkä tahansa totuusarvot, niin

$$\neg\varphi(P_1,\dots,\mathsf{F},\dots,P_n) \vee \varphi(P_1,\dots,\mathsf{T},\dots,P_n) \;,$$

missä F ja T on sijoitettu paikkaan i.

Miten tätä määritelmää pitää muuttaa, jotta saataisiin määritelmä vähenevyydelle paikan i suhteen? 41

On olemassa toinenkin kaksipaikkainen totuusfunktio, joka ei ole kasvava eikä vähenevä, mutta on vähenevä P:n suhteen ja kasvava Q:n suhteen. Piirrä sille kuvan 13 kaltainen esitys, sekä kirjoita sitä esittävä kaava! Etsi jokainen kaksipaikkainen totuus- 42
funktio, joka on kasvava P:n ja vähenevä Q:n suhteen! 43

Kaavan $P \wedge \neg Q \vee \neg P \wedge Q$ esittämä totuusfunktio ei ole kasvava eikä vähenevä P:n eikä Q:n suhteen. Jos piirrät sille kuvan 13 kaltaisen esityksen, niin voit siitä tarkastaa, että yhtä saraketta alas mennessä F muuttuu T:ksi ja toista saraketta mennessä T muuttuu F:ksi, sekä yhtä riviä oikealle mennessä F muuttuu T:ksi ja toista riviä oikealle mennessä T muuttuu F:ksi. On olemassa toinenkin kaksipaikkainen totuusfunktio, joka ei ole kasvava eikä vähenevä P:n eikä Q:n suhteen. Mikä se on? 44

Jos $1 \leq i \leq n$ ja kaavan $\varphi(P_1,\dots,P_i,\dots,P_n)$ esittämä totuusfunktio on kasvava paikan i suhteen, niin kaavan $\varphi(P_1,\dots,\neg P_i\dots,P_n)$ esittämä totuusfunktio on vähenevä paikan i suhteen. Perustele tämä päättelemällä, miten koko kaavan tulos muuttuu kun P_i muuttuu! 45

Kasvavuuden määritelmästä seuraa välittömästi, että kasvava totuusfunktio on kasvava jokaisen paikkansa suhteen: jos valitaan $P_i \Leftrightarrow \mathsf{F}$, $Q_i \Leftrightarrow \mathsf{T}$ ja $Q_j \Leftrightarrow P_j$ kun $1 \leq j \leq n \wedge j \neq i$, niin kasvavuuden määritelmän jos-osa toteutuu ja niin-osa sievenee paikan i suhteen kasvavuuden määritelmän mukaiseen muotoon. Toisin sanoen, kasvavuuden sanallinen kuvaus ”aina kun nolla tai useampi argumentti muuttuu F:sta T:ksi muiden argumenttien pysyessä muuttumattomina, totuusfunktion tulos joko säilyy ennallaan tai muuttuu F:sta T:ksi” sisältää erikoistapauksenaan ”aina kun paikassa i oleva argumentti muuttuu F:sta T:ksi muiden argumenttien pysyessä muuttumattomina, totuusfunktion tulos joko säilyy ennallaan tai muuttuu F:sta T:ksi”, ja sehän tarkoittaa kasvavuutta paikan i suhteen.

Myös päinvastainen suunta pätee, eli jos totuusfunktio on kasvava jokaisen paikkansa suhteen, niin se on kasvava. Muuttuvat argumentit voidaan käydä yksitellen läpi missä järjestyksessä tahansa. Esimerkiksi siirtyminen alas oikealle kuvan 13 ensimmäisessä tai toisessa taulukossa voidaan toteuttaa siirtymällä ensin alas ja sitten oikealle, tai ensin oikealle ja sitten alas. Koska totuusfunktio on kasvava jokaisen paikkansa suhteen, kukin argumentin muutos joko ei muuta totuusfunktion tulosta tai muuttaa sen

F:sta T:ksi. Jälkimmäinen voi tapahtua enintään kerran. Muutosten yhteisvaikutus on joko ei mikään tai tuloksen muuttuminen F:sta T:ksi. Juuri näin käy kuvan 13 ensimmäisessä ja toisessa taulukossa.

Jos sekä $\varphi_1(P_1,\ldots,P_n)$ että $\varphi_2(P_1,\ldots,P_n)$ esittää kasvavan totuusfunktion, niin myös $\varphi_1(P_1,\ldots,P_n) \land \varphi_2(P_1,\ldots,P_n)$ esittää kasvavan totuusfunktion. Tämän nähdäksemme merkitsemme $\varphi_1(P_1,\ldots,P_n)$:n tulosta Q_1:llä ja $\varphi_2(P_1,\ldots,P_n)$:n tulosta Q_2:lla, jolloin koko kaavan tulos on $Q_1 \land Q_2$. Jos jokin P_i muuttuu, niin Q_1 pysyy ennallaan tai muuttuu samaan suuntaan, ja myös Q_2 pysyy ennallaan tai muuttuu samaan suuntaan. Koska $Q_1 \land Q_2$ on kasvava, tällöin myös koko kaavan tulos pysyy ennallaan tai muuttuu samaan suuntaan. Tämä periaate toimii yleisemminkin:

> **Apulause.** Jos $\varphi_1(P_1,\ldots,P_n)$, ..., $\varphi_m(P_1,\ldots,P_n)$ ja $\psi(Q_1,\ldots,Q_m)$ esittävät kasvavia totuusfunktioita, niin myös [14]
>
> $$\psi(\varphi_1(P_1,\ldots,P_n),\ldots,\varphi_m(P_1,\ldots,P_n))$$
>
> esittää kasvavan totuusfunktion.

Koska F, T, $\land$ ja $\lor$ ovat kasvavia, seuraa edellisestä, että pelkästään niitä, sulkeita ja propositiomuuttujia käyttämällä voi muodostaa vain kasvavia totuusfunktioita. Osoitamme seuraavaksi, että niillä voi esittää jokaisen kasvavan totuusfunktion.

> **Lause.** Kaksiarvoisen logiikan minkä tahansa kasvavan totuusfunktion voi esittää kaavalla, jossa ei esiinny muita symboleita kuin propositiomuuttujia, sulkeet, F, T, $\land$ ja $\lor$. [15]

Todistus. Nollapaikkaiset kasvavat totuusfunktiot voi esittää F:lla ja T:lla. Osoitamme, että mielivaltaisen n-paikkaisen totuusfunktion $\underline{\varphi}(P_1,\ldots,P_n)$ voi esittää kaavalla $\varphi_\mathsf{F} \lor P_n \land \varphi_\mathsf{T}$, missä $\varphi_\mathsf{F}(P_1,\ldots,P_{n-1})$ ja $\varphi_\mathsf{T}(P_1,\ldots,P_{n-1})$ esittävät $\underline{\varphi}(P_1,\ldots,P_{n-1},\mathsf{F})$:n ja $\underline{\varphi}(P_1,\ldots,P_{n-1},\mathsf{T})$:n. Olkoot P_1:n, ..., P_{n-1}:n totuusarvot valittu miten tahansa.

Jos $P_n \Leftrightarrow \mathsf{F}$, niin kaava $\varphi_\mathsf{F} \lor P_n \land \varphi_\mathsf{T}$ tuottaa φ_F, kuten pitääkin.

Jos $P_n \Leftrightarrow \mathsf{T}$, niin kaavan pitäisi tuottaa φ_T, mutta se tuottaa $\varphi_\mathsf{F} \lor \varphi_\mathsf{T}$. Ratkaisemme tämän pulman osoittamalla, että $\varphi_\mathsf{F} \lor \varphi_\mathsf{T} \Leftrightarrow \varphi_\mathsf{T}$. Jos $\varphi_\mathsf{F} \Leftrightarrow \mathsf{F}$, niin $\varphi_\mathsf{F} \lor \varphi_\mathsf{T} \Leftrightarrow \mathsf{F} \lor \varphi_\mathsf{T} \Leftrightarrow \varphi_\mathsf{T}$. Jos $\varphi_\mathsf{F} \Leftrightarrow \mathsf{T}$ eli $\varphi_\mathsf{F}(P_1,\ldots,P_{n-1}) \Leftrightarrow \mathsf{T}$, niin $\underline{\varphi}(P_1,\ldots,P_{n-1},\mathsf{F}) \Leftrightarrow \mathsf{T}$. Kasvavuuden vuoksi $\underline{\varphi}(P_1,\ldots,P_{n-1},\mathsf{T}) \Leftrightarrow \mathsf{T}$ eli $\varphi_\mathsf{T}(P_1,\ldots,P_{n-1}) \Leftrightarrow \mathsf{T}$, joten $\varphi_\mathsf{F} \lor \varphi_\mathsf{T} \Leftrightarrow \mathsf{T} \Leftrightarrow \varphi_\mathsf{T}$.

Kaavat φ_F ja φ_T esittävät $(n-1)$-paikkaisia totuusfunktioita. Jos $n-1>0$, niin φ_F ja φ_T saadaan samalla tavalla neljää $(n-2)$-paikkaista totuusfunktiota esittävistä kaavoista, ja niin edelleen. □

2.3 Jossittelu on vaikeaa

Luonnollisen kielen ilmauksen ”jos ... niin ...” esittäminen logiikassa on osoittautunut ongelmalliseksi. Stanford Encyclopedia of Philosophyn vapaasti luettava nettiartikkeli ”The Logic of Conditionals” totesi vuonna 2022: ”Huolimatta sellaisten lauseiden tavattomasta yleisyydestä jokapäiväisessä keskustelussa ja päättelyssä, on hämmästyttävän vähän yksimielisyyttä siitä mikä voisi olla [jos ... niin ...-ilmausten] oikea logiikka, tai edes siitä voidaanko kaikille sellaisten ilmausten lajeille muodostaa yhtenäinen teoria.”

Formaalissa logiikassa opetetaan yleensä kaksi tärkeää ”jos ... niin ...” -käsitettä. Niissä itsessään ei ole ongelmaa, mutta kumpikaan ei vastaa sitä mitä käytetään matemaattisessa tai arkielämän päättelyssä. Jälkimmäisen käsitteen ero edellisiin jää helposti huomaamatta, mistä seuraa sekaannusta. Lisäksi ihmisillä on joissakin tapauk-

A D 4 7

Kuva 14: Wasonin hautakiveen kaiverretut kortit

sissa taipumus tulkita ”jos … niin …” tavalla, joka on varmasti väärin. Tässä alaluvussa pyritään esittämään matemaatikkojen ”jos … niin …” käytännöllisenä päättelyn työkaluna, samalla kun pyritään varmistamaan että sekaannusta formaalin logiikan käsitteisiin ei synny ja että ”jos … niin …” tulee ymmärretyksi oikein myös niissä tapauksissa, joissa luontainen intuitio johtaa harhaan.

Psykologi Peter Wason kehitti 1960-luvulla kokeen tutkimaan ihmisten päättelyä. Sen idea on seuraava. Pöydällä on neljä korttia. Koehenkilöt tietävät, että jokaisen kortin yhdellä puolella on kirjain ja toisella puolella on numero. Kuvassa 14 on näytetty Wasonin hautakiveen piirretyt kortit. Niistä yhden näkyvällä puolella lukee A, toisen D, kolmannen 4 ja neljännen 7. Tehtävänä on valita mahdollisimman vähän kortteja siten, että katsomalla niiden kääntöpuolet voidaan tarkastaa, noudattavatko kaikki neljä korttia seuraavaa sääntöä: jos kortin yhdellä puolella lukee A, niin toisella puolella lukee 4. Yritä ratkaista tämä ennen kuin luet eteenpäin! 46

Neljässä Wasonin varhaisessa tutkimuksessa yhteensä vain 5 koehenkilöä 128:sta eli noin 4 % ratkaisi tämänkaltaisen tehtävän oikein. Koe on sittemmin toistettu lukuisia kertoja erilaisina muunnelmina. Oikein ratkaisseiden osuus kasvoi huomattavasti, kun tehtävä kytkettiin arjesta tuttuihin sallittua ja kiellettyä koskeviin sääntöihin. Griggs ja Cox käyttivät versiota, jossa kunkin kortin toisella puolella lukee henkilön ikä ja toisella puolella juoma jota hän juo, ja sääntö on: jos henkilö juo olutta, niin hänen täytyy olla yli 19-vuotias. Tämän ratkaisi oikein 74 %!

Tarkastelkaamme olutversiota, kun korttien näkyvillä puolilla lukee olut, mehu, 16 ja 25. Kortin 16 henkilö on alaikäinen, joten kortti pitää kääntää sen tarkastamiseksi, että hän ei juo olutta. Olutkortti pitää kääntää sen tarkastamiseksi, ettei oluen juoja ole alaikäinen. Kortin 25 henkilö on täysi-ikäinen, joten ei tarvitse tarkastaa mitä hän juo. Mehua saa juoda kuka vaan, joten mehukorttiakaan ei tarvitse kääntää.

”Jos A, niin 4” -versiossa pitää kääntää kortit A ja 7. On tarkastettava, että A-kortin kääntöpuolella todella lukee 4, ja että 7-kortin kääntöpuolella ei lue A. D-korttia ei tarvitse kääntää, koska sääntö sallii sen toiselle puolelle minkä tahansa luvun. Myöskään 4-korttia ei tarvitse kääntää, sillä sääntö ei rikkoudu vaikka sen toisella puolella lukisikin A.

Tutkijat eivät ole päässeet yksimielisyyteen siitä, mitä näistä tuloksista voidaan päätellä. Ainakin näyttää selvältä, että abstraktina asiana, siis irrallaan konkreettisista käytännön tilanteista, ”jos … niin …” on vaikea. Sitä ei osata luonnostaan. Tässä tapauksessa vaikeus näyttää kuitenkin ulottuvan vain oikean ratkaisun keksimiseen. Kun se selitetään koehenkilöille, he ymmärtävät sen ja hyväksyvät sen oikeaksi.

Liisa Ihmemaassa -kirjan kirjoittaja Lewis Carroll (oikealta nimeltään Charles Dodgson) oli paitsi satukirjailija, myös matemaatikko. Hänellä oli pitkäaikainen kiista Oxfordin yliopiston logiikan professori John Cook Wilsonin kanssa siitä miten ”jos … niin …” toimii. Hän kysyi useiden loogikoiden kantaa, mutta asiaan ei tullut selvyyttä. Sitten hän julkaisi vuonna 1894 tiedelehdessä Mind kertomuksen, jossa hän selosti esimerkin avulla Wilsonin kannan ja oman kantansa, ja pyysi lukijoita auttamaan paradoksin purkamisessa.

Setä Jim ja setä Joe olivat menossa parturiliikkeeseen, jossa Allen, Brown ja Carr asuivat ja työskentelivät. Setä Jim toivoi että Carr olisi paikalla, koska hän oli parempi parturi kuin Allen ja Brown. Setä Joe lupasi voivansa todistaa, että Carr on paikalla. Tiedettiin, että joka hetki ainakin yksi heistä on paikalla. Niinpä

(1) Jos Carr on ulkona, niin jos Allen on ulkona, niin Brown on paikalla.

Sairastettuaan kuumeen Allen oli muuttunut niin hermostuneeksi, että ei enää mene ulos muuten kuin Brownin kanssa. Niinpä

(2) Jos Allen on ulkona, niin myös Brown on ulkona.

Setä Joe lupasi osoittaa, että Carr ei voi olla ulkona, koska jos hän on ulkona, niin päädytään ristiriitaan. Kun oletetaan että Carr on ulkona, (1) sievenee muotoon

(3) Jos Allen on ulkona, niin Brown on paikalla.

Mutta (2) ja (3) tekevät saman oletuksen ”Allen on ulkona”, ja tekevät siitä vastakkaiset johtopäätökset ”Brown on ulkona” ja ”Brown on paikalla”. Sellainen on setä Joen mukaan mahdotonta. Samalla lähtökohdalla ei voi olla kahta keskenään ristiriidassa olevaa seurausta. On päädytty ristiriitaan, joten Carr ei voi olla ulkona.

Setä Jim oli tietysti eri mieltä. Mitä veikkaat, mitä hänen mielestään voidaan päätellä oletuksesta, että Carr on ulkona? Palaamme myöhemmin siihen kumpi setä edusti 47
Carrollin ja kumpi Cook Wilsonin kantaa, ja mitä mieltä nykyloogikot ovat asiasta.

Yleisin tapa esittää ”jos ... niin ...” logiikassa on konnektiivi nimeltä *materiaalinen implikaatio* (*material implication*). Sen symbolina on yleensä joko $\rightarrow$ tai $\Rightarrow$. Tässä kirjassa käytetään $\rightarrow$, ja $\Rightarrow$ on varattu tarkoittamaan matemaatikkojen ”jos ... niin ...” -käsitettä. (Kuvassa 23 on esimerkki samankaltaisesta käytännöstä kanadalaisessa aineistossa.) Esittäminen konnektiivina tarkoittaa, että ”jos P niin Q” tuottaa totuusarvon, ja se riippuu pelkästään P:n ja Q:n totuusarvoista. Mietimme seuraavaksi esimerkin avulla, mikä tuotetun totuusarvon tulisi kulloinkin olla, jotta se täsmäisi luonnollisen kielen mukaiseen merkitykseen mahdollisimman hyvin.

Tarkoittakoon H että ruokana on hernekeittoa, I että Ilona ilahtuu, ja $H \rightarrow I$ että ”jos ruokana on hernekeittoa niin Ilona ilahtuu”. Jos ruokana on hernekeittoa mutta Ilona ei silti ilahdu, niin väitettä vastaan on selvästi rikottu. Niinpä $\mathsf{T} \rightarrow \mathsf{F}$ ei saa olla tosi. Siksi valitsemme $\mathsf{T} \rightarrow \mathsf{F} \Leftrightarrow \mathsf{F}$. Väitteeseen sopii, että ruokana on hernekeittoa ja Ilona ilahtuu. Siksi valitsemme $\mathsf{T} \rightarrow \mathsf{T} \Leftrightarrow \mathsf{T}$. Väitettä ei riko sekään, että ruokana ei ole hernekeittoa eikä Ilona ilahdu. Siksi valitsemme $\mathsf{F} \rightarrow \mathsf{F} \Leftrightarrow \mathsf{T}$. Vaikka ruokana ei olisi hernekeittoa, niin Ilona saattaa silti ilahtua jostain muusta syystä, vaikka siksi että hän onnistui tentissä. Siksi $\mathsf{F} \rightarrow \mathsf{T}$ ei saa olla epätosi, joten täytyy valita $\mathsf{F} \rightarrow \mathsf{T} \Leftrightarrow \mathsf{T}$.

Kaavalle $P \rightarrow Q$ valitut totuusarvot todellakin täsmäävät niihin, jotka Ilonan hernekeittoesimerkki tuotti. Toisin sanoen, $P \rightarrow Q$ tuottaa T jos ja vain jos $P \Leftrightarrow \mathsf{F}$ tai $Q \Leftrightarrow \mathsf{T}$. Tästä seuraa, että $P \rightarrow Q \Leftrightarrow \neg P \vee Q$. Ainoa tilanne, jossa $P \rightarrow Q$ tuottaa F on, että P on tosi mutta Q on epätosi. Sen voi ilmaista $\neg(P \rightarrow Q) \Leftrightarrow P \wedge \neg Q$. Saman saa De Morganin lailla tiedosta $P \rightarrow Q \Leftrightarrow \neg P \vee Q$.

Materiaalinen implikaatio ei kata kaikkia luonnollisen kielen ilmauksen ”jos ... niin ...” vivahteita. Esimerkiksi $S \rightarrow \neg U$ ja $U \rightarrow \neg S$ ovat yhtäpitävät: kumpikin sievenee muotoon $\neg S \vee \neg U$. Toisaalta ”jos sataa, niin en mene ulos” kuulostaa luontevalta, mutta ”jos menen ulos, niin ei sada” kuulostaa hieman omituiselta, ikään kuin voisin estää sateen menemällä ulos. Tämä johtuu siitä, että materiaalinen implikaatio ei säilytä tietoa siitä mikä on syy ja mikä on seuraus; se kiinnittää huomiota vain siihen, mitkä totuusarvojen yhdistelmät ovat mahdollisia ja mitkä eivät.

Tarkastelemme seuraavaksi esimerkkiä ”jos Ilona ei pidä hernekeitosta, niin hän pitää hernekeitosta”. Se saattaa kuulostaa omituiselta, mutta itse asiassa se tarkoittaa vain, että Ilona pitää hernekeitosta. Se tarkoittaa samaa kuin ”ei ole niin että Ilona ei pidä hernekeitosta, tai hän pitää hernekeitosta”. Se sievenee muotoon ”Ilona pitää hernekeitosta tai hän pitää hernekeitosta” ja edelleen muotoon ”Ilona pitää hernekeitosta”. Jos ”Ilona pitää hernekeitosta” merkitään P, niin tämä sievennys voidaan esittää $\neg P \rightarrow P \Leftrightarrow \neg\neg P \vee P \Leftrightarrow P \vee P \Leftrightarrow P$. Vaikka jokin ”jos ... niin ...” -ilmaus kuulostaisikin omituiselta, kannattaa kokeilla, tuleeko järkevä lopputulos jos sen tulkitsee materiaalisena implikaationa. Toisinaan ei tule, mutta usein tulee.

Edellä on perusteltu, että jos ”jos ... niin ...” halutaan esittää konnektiivina, niin paras tapa on materiaalinen implikaatio. Tästä tietysti herää ajatus, että saataisiinko parempi tulos esittämällä se jotenkin muuten kuin konnektiivina. Tulemme kehittämään tätä ajatusta, mutta pettymyksen välttämiseksi on parasta sanoa jo nyt, että syyn ja seurauksen käsitteet jäävät silloinkin pois.

Koska $P \rightarrow Q \Leftrightarrow \neg P \vee Q$ johdettiin olettamatta P:stä ja Q:sta mitään, se on laki ja sen saa yleistää kaavoille:

$$\varphi \rightarrow \psi \;\Leftrightarrow\; \neg\varphi \vee \psi \qquad [16]$$

Jos haluat muistaa vain yhden $\rightarrow$:ta koskevan lain, niin muista tämä. Sillä saadaan $\rightarrow$ aina korvattua $\neg$:llä ja $\vee$:lla, jolloin muita $\rightarrow$:ta koskevia lakeja ei välttämättä tarvita. Esimerkiksi sijoittamalla siihen vuoron perään φ:hin ja ψ:hin F ja T ja sieventämällä oikea puoli saadaan

$$\mathsf{F} \rightarrow \psi \;\Leftrightarrow\; \mathsf{T} \qquad \mathsf{T} \rightarrow \psi \;\Leftrightarrow\; \psi \qquad \varphi \rightarrow \mathsf{F} \;\Leftrightarrow\; \neg\varphi \qquad \varphi \rightarrow \mathsf{T} \;\Leftrightarrow\; \mathsf{T} \qquad [17]$$

Toisin kuin $\wedge$ ja $\vee$, $\rightarrow$ ei ole vaihdannainen, sillä $\mathsf{F} \rightarrow \mathsf{T} \Leftrightarrow \mathsf{T}$ mutta $\mathsf{T} \rightarrow \mathsf{F} \Leftrightarrow \mathsf{F}$. Se ei myöskään ole liitännäinen, koska $(\mathsf{F} \rightarrow \mathsf{F}) \rightarrow \mathsf{F} \Leftrightarrow \mathsf{T} \rightarrow \mathsf{F} \Leftrightarrow \mathsf{F}$, mutta $\mathsf{F} \rightarrow (\mathsf{F} \rightarrow \mathsf{F}) \Leftrightarrow \mathsf{F} \rightarrow \mathsf{T} \Leftrightarrow \mathsf{T}$. Koska se ei ole liitännäinen, on tärkeää määritellä, tulkitaanko $P \rightarrow Q \rightarrow R$ kuten $(P \rightarrow Q) \rightarrow R$ vai kuten $P \rightarrow (Q \rightarrow R)$, vai kielletäänkö se. Varsin yleistä on tulkita se kuten $P \rightarrow (Q \rightarrow R)$. Niin tehdään myös tässä kirjassa. Siis $\rightarrow$ on oikealle liitännäinen. Jolleivät sulkeet määrää toisin, $\rightarrow$ lasketaan vasta kun $\neg$, $\wedge$ ja $\vee$ on laskettu. Siis esimerkiksi $P \rightarrow Q \vee R \rightarrow S$ tarkoittaa samaa kuin $P \rightarrow ((Q \vee R) \rightarrow S)$.

Hyvä, ei ihan helppo harjoitus propositiologiikan kaavojen käsittelyssä on etsiä mahdollisimman lyhyt kaava, joka on tosi täsmälleen silloin kun $(P \rightarrow Q) \rightarrow R$ tuottaa eri totuusarvon kuin $P \rightarrow (Q \rightarrow R)$. Yritä löytää se! 48

Perustele, että sivuilla 22, ..., 24 ja vastauksessa 41 esitetyt kasvavuuskäsitteet voi ilmaista seuraavasti: 49

> **Apulause.** Kaavan $\varphi(P_1, \ldots, P_n)$ esittämä kaksiarvoisen logiikan totuusfunktio on kasvava, jos ja vain jos seuraava ehto pätee aina:
>
> Jos $P_1 \rightarrow Q_1, \ldots, P_n \rightarrow Q_n$, niin $\varphi(P_1, \ldots, P_n) \rightarrow \varphi(Q_1, \ldots, Q_n)$.
>
> Se on vähenevä, jos ja vain jos seuraava ehto pätee aina:
>
> Jos $P_1 \rightarrow Q_1, \ldots, P_n \rightarrow Q_n$, niin $\varphi(Q_1, \ldots, Q_n) \rightarrow \varphi(P_1, \ldots, P_n)$. [18]
>
> Olkoon $1 \leq i \leq n$. Kaavan $\varphi(P_1, \ldots, P_i, \ldots, P_n)$ esittämä kaksiarvoisen logiikan totuusfunktio on kasvava paikan i suhteen, jos ja vain jos aina $\varphi(P_1, \ldots, \mathsf{F}, \ldots, P_n) \rightarrow \varphi(P_1, \ldots, \mathsf{T}, \ldots, P_n)$. Se on vähenevä paikan i suhteen, jos ja vain jos aina $\varphi(P_1, \ldots, \mathsf{T}, \ldots, P_n) \rightarrow \varphi(P_1, \ldots, \mathsf{F}, \ldots, P_n)$.

aluksi	$\surd$	$\surd$	$\surd$	$\surd$	-	-	$\surd$	-
Carr ulkona	-	$\surd$	-	$\surd$	-	-	-	-
A	F	F	F	F	T	T	T	T
B	F	F	T	T	F	F	T	T
C	F	T	F	T	F	T	F	T

Kuva 15: Carrollin paradoksin mahdolliset ($\surd$) ja mahdottomat (-) tilanteet

Jos A, B ja C tarkoittavat, että Allen on ulkona, Brown on ulkona ja Carr on ulkona, niin Carrollin paradoksin (1), (2) ja (3) voidaan kirjoittaa seuraavasti:

(4) $C \rightarrow A \rightarrow \neg B$

(5) $A \rightarrow B$

(6) $A \rightarrow \neg B$

Lisää (4):een yhdet (vain yhdet) sulkeet niin että laskujärjestys ei muutu, mutta näkyy mahdollisimman selvästi! 50

Setä Joe väitti, että (5) ja (6) eivät voi olla yhtäaikaa totta. Kuitenkin jos sijoitamme $A \Leftrightarrow \mathsf{F}$, niin molemmista tulee T. Sijoituksella $A \Leftrightarrow \mathsf{T}$ saamme $(A \rightarrow B) \wedge (A \rightarrow \neg B)$ $\Leftrightarrow (\mathsf{T} \rightarrow B) \wedge (\mathsf{T} \rightarrow \neg B) \Leftrightarrow B \wedge \neg B \Leftrightarrow \mathsf{F}$. Siis (5) ja (6) ovat yhtäaikaa totta täsmälleen silloin kun Allen on paikalla. Niinpä nykynäkemyksen mukaan setä Jim eli Lewis Carroll oli oikeassa, ja setä Joe eli John Cook Wilson väärässä.

Etsimme seuraavaksi kaikki Carrollin paradoksissa mahdolliset tilanteet. Nyt kaavan (6) ei tarvitse toteutua, koska se ei ole osa alkuperäisiä ehtoja vaan setä Joen johtama välitulos. Jos Allen on ulkona eli A, niin (5):n vuoksi myös Brown on ulkona eli B. Silloin $A \rightarrow \neg B \Leftrightarrow \mathsf{F}$, joten Carrin täytyy olla paikalla eli $\neg C$, jotta (4) toteutuisi. Tämä päättely ei vielä todista että yhdistelmä Allen ulkona, Brown ulkona ja Carr paikalla on mahdollinen, vaan se todistaa ainoastaan että mikään muu yhdistelmä jossa Allen on ulkona ei ole mahdollinen. Mutta on helppo sijoittaa $A \Leftrightarrow \mathsf{T}$, $B \Leftrightarrow \mathsf{T}$ ja $C \Leftrightarrow \mathsf{F}$ (4):een ja (5):een ja tarkastaa, että ne molemmat tuottavat T. Tämä sijoitus voidaan ilmaista tiiviimmin muodossa $A \wedge B \wedge \neg C$.

Jos Allen on paikalla eli $A \Leftrightarrow \mathsf{F}$ eli $\neg A$, niin olemme jo nähneet, että (5) tuottaa T ja (4):n loppuosa tuottaa T. Koska aina $C \rightarrow \mathsf{T} \Leftrightarrow \mathsf{T}$, myös (4) pätee. Tämä tuottaa neljä mahdollista tilannetta: $\neg A \wedge \neg B \wedge \neg C$, $\neg A \wedge \neg B \wedge C$, $\neg A \wedge B \wedge \neg C$ ja $\neg A \wedge B \wedge C$. Carrollin paradoksissa on siis viisi mahdollista tilannetta. Ne on näytetty kuvan 15 ylimmällä rivillä. Loput kolme tilannetta $A \wedge \neg B \wedge \neg C$, $A \wedge \neg B \wedge C$ ja $A \wedge B \wedge C$ ovat mahdottomia. Tulkitse niistä jokainen Allenin, Brownin ja Carrin paikalla tai ulkona olemisena ja tarkasta, että jokainen rikkoo ainakin toista alkuperäisistä tiedoista "joka hetki ainakin yksi heistä on paikalla" ja "Allen ei mene ulos muuten kuin Brownin kanssa"! 51

Niinpä $\neg A \vee (A \wedge B \wedge \neg C)$ on tosi täsmälleen silloin kun (4) ja (5) toteutuvat. Sen alkuosa $\neg A$ täsmää niihin tilanteisiin, joissa Allen on paikalla, ja loppuosa $A \wedge B \wedge \neg C$ niihin, joissa hän on ulkona. Voimme päätellä $\neg A \vee (A \wedge B \wedge \neg C) \Leftrightarrow \neg A \vee (A \wedge (B \wedge \neg C))$ $\Leftrightarrow \neg A \vee (\neg\neg A \wedge (B \wedge \neg C)) \Leftrightarrow \neg A \vee (B \wedge \neg C)$. Mitä lakeja käytettiin tässä päättelyssä, ja mitkä olivat lakien kreikkalaisten kirjainten tilalla olevat kaavat? Johda sama tulos 52
sijoittamalla johonkin propositiomuuttujaan vuoron perään F ja T! 53

Niinpä Carrollin paradoksissa mahdolliset tilanteet voidaan esittää lyhyesti kaavalla $\neg A \vee (B \wedge \neg C)$. Siis $(C \rightarrow A \rightarrow \neg B) \wedge (A \rightarrow B) \Leftrightarrow \neg A \vee (B \wedge \neg C)$.

Setä Joe oletti, että Carr on ulkona, ja luuli johtaneensa siitä ristiriidan. Oletus, että Carr on ulkona, poistaa mahdollisista tilanteista ne, joissa C ei ole tosi, ja jättää jäljelle ne, joissa C on tosi. Kuvan 15 toinen rivi näyttää mahdolliset tilanteet tämän oletuksen ollessa voimassa. Jos oletus todella johtaisi ristiriitaan, niin yhtään mahdollista tilannetta ei jäisi jäljelle. Mutta kuten kuvasta näkyy, niitä jäi jäljelle kaksi.

Seuraavaksi käsittelemme esimerkin, jossa materiaalinen implikaatio ei selvästikään vastaa luonnollisen kielen ”jos ... niin ...” -ilmauksen merkitystä. Oletamme, että Suomen paikkakunnat sijaitsevat niin kuin ne todellisuudessa sijaitsevat. Silloin seuraava kuulostaa väärältä: ”Jos Pihtiputaan mummo on Pihtiputaalla niin hän on Kuopiossa, tai jos hän on Kuopiossa niin hän on Rovaniemellä.”

Merkitsemme P:llä että hän on Pihtiputaalla, K:lla että Kuopiossa ja R:llä että Rovaniemellä. Molempien ”jos ... niin ...” formalisointi $\rightarrow$:lla tuottaa $(P \rightarrow K) \vee (K \rightarrow R)$. Jos mummo on Kuopiossa niin $P \rightarrow K \Leftrightarrow P \rightarrow \mathsf{T} \Leftrightarrow \mathsf{T}$, joten $\vee$:n vasen puoli ja samalla koko kaava tuottaa T. Jos mummo ei ole Kuopiossa niin $K \rightarrow R \Leftrightarrow \mathsf{F} \rightarrow R \Leftrightarrow \mathsf{T}$, joten $\vee$:n oikea puoli ja samalla koko kaava tuottaa T. Siis aina $(P \rightarrow K) \vee (K \rightarrow R) \Leftrightarrow \mathsf{T}$. Niinpä materiaalisen implikaation mukaan ”jos Pihtiputaan mummo on Pihtiputaalla niin hän on Kuopiossa, tai jos hän on Kuopiossa niin hän on Rovaniemellä” on aina tosi!

Toinen tapa nähdä, että se on aina tosi, on käyttää lakia $\varphi \rightarrow \psi \Leftrightarrow \neg\varphi \vee \psi$. Sillä saadaan $(\neg P \vee K) \vee (\neg K \vee R)$. Koska $\vee$ on liitännäinen, se sievenee muotoon $\neg P \vee K \vee \neg K \vee R$. Siis mummo ei ole Pihtiputaalla tai hän on Kuopiossa tai hän ei ole Kuopiossa tai hän on Rovaniemellä. Se ei kuulosta väärältä. Osuuden ”hän on Kuopiossa tai hän ei ole Kuopiossa” vuoksi se on selvästi aina tosi.

Kuten usein ennenkään, nytkään emme vedonneet yhtäpitävyyden todistuksessa propositiomuuttujien merkitykseen. Niinpä $(P \rightarrow K) \vee (K \rightarrow R) \Leftrightarrow \mathsf{T}$ pätee riippumatta siitä, mitä P, K ja R tarkoittavat. Siksi jokainen ”jos ... niin ..., tai jos ... niin ...”, missä keskimmäiset ... ovat sama, on materiaalisen implikaation mukaan tosi. Niinpä esimerkiksi myös ”jos Aapo pitää jäätelöstä niin mummo on Kuopiossa, tai jos mummo on Kuopiossa niin Suomi voittaa jalkapallon maailmanmestaruuden” on materiaalisen implikaation mukaan tosi, vaikka sen kumpikaan osa (ennen ja jälkeen sanan ”tai”) ei kuulosta oikealta.

Ongelma ratkeaa, jos emme tulkitse ilmausta ”jos ... niin ...” konnektiivina vaan *päättelysääntönä*. Niin saadun päättelysäännön nimi on *päättelyimplikaatio*. Konnektiivi tuottaa tilanteesta riippuen F tai T. Tarkoittakoon S että mummo on Savossa. Esimerkiksi $S \rightarrow K$ tuottaa T silloin kun mummo on Kuopiossa tai ei ole Savossa (tai sekä että), ja F silloin kun mummo on Savossa mutta ei Kuopiossa. Päättelysääntö ei tuota tilanteesta riippuen F tai T, vaan on joko *pätevä* tai *epäpätevä*. Onko päättelysääntö pätevä ei riipu tilanteesta (missä mummo on), mutta voi riippua asiayhteydestä (mitä K, S ja niin edelleen tarkoittavat). Esittelemme tämän idean päättelyimplikaation avulla.

Ensin tarvitaan ”mahdollisen tilanteen” käsite. Propositiologiikan tapauksessa ”tilanne” on mikä tahansa käytössä olevien propositiomuuttujien totuusarvojen yhdistelmä. Tilanteet jaetaan mahdollisiin ja mahdottomiin erikseen kerrottujen tai muuten tiedossa olevien tosiseikkojen perusteella. Kuvassa 16 on näytetty kaikki Pihtiputaan mummolle mahdolliset ja mahdottomat tilanteet. Luettelo perustuu siihen, että ihminen ei voi olla kahdessa eri paikassa yhtäaikaa, sekä siihen, että Kuopio on Savossa mutta muuten luettelon paikkakunnat ovat erilliset. Ollessaan Kuopiossa mummo on Savossa. Mummo voi olla Savossa ilman että on samalla Kuopiossa — hän on vaikka Savonlinnassa. Mummo ei välttämättä ole missään mainituista paikoista — hän voi

	$\surd$	$\surd$	$\surd$	-	-	$\surd$	-	-	$\surd$	-	-	-	-	-	-	-
P	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T
K	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
R	F	F	T	T	F	F	T	T	F	F	T	T	F	F	T	T
S	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T

Kuva 16: Pihtiputaan mummon mahdolliset ($\surd$) ja mahdottomat (-) tilanteet

olla vaikka Jyväskylässä.

Myös koulumatematiikassa tilanne tarkoittaa mitä tahansa käytössä oleville muuttujille annettujen arvojen yhdistelmää, mutta nyt muuttujien arvot eivät (välttämättä) ole totuusarvoja vaan esimerkiksi lukuja. Koulumatematiikassakin voidaan tehdä muuttujien arvojen yhdistelmiä rajoittavia oletuksia, kuten että tarkasteltava luku on parillinen. Lisäksi koulumatematiikassa on rajoituksia sille, mitkä atomikaavat voivat olla yhtäaikaa tosi. Esimerkiksi $x \geq 5$ voi olla tosi ja $x < 2$ voi olla tosi, mutta ne eivät voi olla yhtäaikaa tosi. Siis $x \geq 5 \wedge x < 2$ ei voi olla tosi. Myöskään $x < y$ ja $y < x$ eivät voi olla yhtäaikaa tosi, vaikka kumpikin erikseen voi olla tosi. Käsittelemme tätä perusteellisemmin luvussa 3. Siihen asti luotamme siihen, että äskeiset esimerkit antavat riittävän mielikuvan siitä, mitä ”mahdollisella tilanteella” tarkoitetaan koulumatematiikassa.

Määritelmä. Jos jokaisessa mahdollisessa tilanteessa, jossa vasen puoli on tosi, myös oikea puoli on tosi, niin päättelyimplikaatio on *pätevä*. Jos yhdessäkin mahdollisessa tilanteessa vasen puoli on tosi mutta oikea puoli ei ole, niin päättelyimplikaatio on *epäpätevä*. Sellainen tilanne on *vastaesimerkki* (*counterexample*) päättelyimplikaatiolle. [19]

Yksikin vastaesimerkki riittää kumoamaan päättelysäännön. Esimerkiksi ”jos henkilö on ainakin 150 cm pitkä, niin hän pääsee kaikkiin Särkänniemen huvilaitteisiin” ei ole pätevä, koska Possujunaan päästetään vain alle 140-senttisiä.

Kuvasta 16 on helppo tarkastaa, että jokaisessa $\surd$:lla merkityssä sarakkeessa, jossa $K \Leftrightarrow \mathsf{T}$, myös $S \Leftrightarrow \mathsf{T}$. Niinpä ”jos Pihtiputaan mummo on Kuopiossa niin hän on Savossa” on pätevä päättelysääntö. Toinen sarake vasemmalta on merkitty $\surd$:lla, ja siinä $S \Leftrightarrow \mathsf{T}$ mutta $K \Leftrightarrow \mathsf{F}$. Se osoittaa, että ”jos Pihtiputaan mummo on Savossa niin hän on Kuopiossa” ei ole pätevä. Näin on siitä huolimatta, että kuvassa on myös $\surd$-merkitty sarake, jossa $S \Leftrightarrow \mathsf{T}$ ja $K \Leftrightarrow \mathsf{T}$. Yksikin vastaesimerkki riittää kumoamaan päättelysäännön. Viimeisessä $\surd$-merkityssä sarakkeessa $P \Leftrightarrow \mathsf{T}$ mutta $K \Leftrightarrow \mathsf{F}$. Se on vastaesimerkki säännölle ”jos Pihtiputaan mummo on Pihtiputaalla niin hän on Kuopiossa”, joka siis ei ole pätevä.

Siis konnektiivi tuottaa tuloksen (joka on T tai F) kussakin yksittäisessä tilanteessa erikseen, mutta päättelysääntö käy kaikki mahdolliset yksittäiset tilanteet läpi ja tuottaa niistä ikään kuin yhteenvedon (joka on ”pätevä” tai ”epäpätevä”).

Päättelysääntöjen yhdistäminen sanalla ”ja” voi olla mielekästä, kuten esimerkiksi ”jos hän on Kuopiossa niin hän ostaa kalakukon, ja jos hän on Rovaniemellä niin hän ostaa poroleikkelettä”. Se tarkoittaa sitä, että kumpikin päättelysääntö on pätevä. Ilmaus ”jos hän on Kuopiossa niin hän ostaa kalakukon, tai jos hän on Rovaniemellä niin hän ostaa poroleikkelettä” ei ehkä kuulosta mielekkäältä, mutta jos se ei ole mielekäs, niin sekin on merkki siitä, että ”jos . . . niin . . . ” ei edusta konnektiivia. Vaihtoehtoisesti sen voi tulkita tarkoittavan, että joko ”jos hän on Kuopiossa niin hän ostaa kalakukon” tai ”jos hän on Rovaniemellä niin hän ostaa poroleikkelettä” tai kumpikin on pätevä päättelysääntö.

Näimme, että ”jos Pihtiputaan mummo on Pihtiputaalla niin hän on Kuopiossa” ei ole pätevä. Myöskään ”jos hän on Kuopiossa niin hän on Rovaniemellä” ei ole pätevä. Niinpä tai-ilmauksen ”jos Pihtiputaan mummo on Pihtiputaalla niin hän on Kuopiossa, tai jos hän on Kuopiossa niin hän on Rovaniemellä” kumpikaan osa ei ole pätevä päättelysääntö. Tämä täsmää siihen, että ilmaus kuulostaa väärältä. Ratkaiseva ero materiaaliseen implikaatioon on siinä, että materiaaliselle implikaatiolle riittää, että jokaisessa mahdollisessa tilanteessa $P \rightarrow K$ on tosi tai $K \rightarrow R$ on tosi, mutta se kumpi niistä on tosi (vai peräti molemmat) saa vaihdella tilanteen vaihdellessa. Päättelyimplikaatio ei salli tällaista vaihtelua, vaan vaatii, että $P \rightarrow K$ on tosi kaikissa mahdollisissa tilanteissa tai $K \rightarrow R$ on tosi kaikissa mahdollisissa tilanteissa.

Tässä kirjassa $\Rightarrow$ on *päättelyoperaattori*, jota käytetään ilmaisemaan päättelyimplikaatiota. Niinpä $\varphi \Rightarrow \psi$ on pätevä, jos ja vain jos jokaisessa mahdollisessa tilanteessa jossa φ on tosi, myös ψ on tosi. Se on epäpätevä, jos ja vain jos sille on vastaesimerkki, eli mahdollinen tilanne, jossa φ on tosi mutta ψ ei ole. Vertaamalla tätä $\rightarrow$:n käyttäytymiseen saadaan seuraavan alkuosa:

> Kaksiarvoisen logiikan päättelysääntö $\varphi \Rightarrow \psi$ on pätevä, jos ja vain jos jokaisessa mahdollisessa tilanteessa $\varphi \rightarrow \psi$ tuottaa T. Oletuksena esiintyessään $\varphi \Rightarrow \psi$ poistaa mahdollisista tilanteista ne, joissa $\varphi \rightarrow \psi$ ei tuota T. [20]

Esimerkiksi koulumatematiikassa $x \geq 2 \Rightarrow x \geq 5$ ei ole pätevä, koska $x = 3$ on sille vastaesimerkki: $3 \geq 2$ tuottaa T mutta $3 \geq 5$ tuottaa F, joten $3 \geq 2 \rightarrow 3 \geq 5 \Leftrightarrow \mathsf{T} \rightarrow \mathsf{F} \Leftrightarrow \mathsf{F}$. Toisaalta $x \geq 5 \Rightarrow x \geq 2$ on pätevä, koska $x \geq 5 \rightarrow x \geq 2$ tuottaa F vain silloin kun $x \geq 5$ on tosi ja $x \geq 2$ on epätosi, mutta sellaista lukua ei ole, joka olisi samanaikaisesti vähintään 5 mutta ei vähintään 2.

Näimme jo, että Pihtiputaan mummon tapauksessa $K \Rightarrow S$ on pätevä mutta $S \Rightarrow K$ ei ole. Tämä vastaa sitä, että kuvassa 16 on $\surd$:lla merkitty sarake jossa $S \rightarrow K \Leftrightarrow \mathsf{F}$ (nimittäin toinen vasemmalta), mutta mikään niistä neljästä sarakkeesta, joissa $K \rightarrow S \Leftrightarrow \mathsf{F}$, ei ole merkitty $\surd$:lla. Kaikki sarakkeet, joissa $K \rightarrow S \Leftrightarrow \mathsf{F}$, edustavat mahdottomia tilanteita, eivätkä siksi tee päättelyimplikaatiota $K \Rightarrow S$ epäpäteväksi.

Matemaattisessa päättelyssä on tavallista tehdä tilapäisiä oletuksia. Mekin olemme tässä kirjassa useasti olettaneet, että jonkin propositiomuuttujan totuusarvo on F ja päätelleet jonkin aikaa; ja sitten olettaneet, että sen totuusarvo onkin T ja taas päätelleet jonkin aikaa. Sen aikaa kun oletus ”jos $P \Leftrightarrow \mathsf{F}$” on voimassa, on $P \Leftrightarrow \mathsf{F}$ pätevä päättelysääntö. Siksi on kätevää merkitä oletuksen osuus ”$P \Leftrightarrow \mathsf{F}$” sillä tavalla kuin päättelysääntöjä merkitään. Lain [29] loppuosa varmistaa, että oletuksena esiintyvä $\varphi \Leftrightarrow \psi$ tulkitaan näin, siis päättelysääntönä, joka juuri nyt astuu voimaan; eikä päättelysääntönä, jonka jossitellaan olevan jo entuudestaan voimassa. Lain [20] loppuosa tekee vastaavan asian oletuksena esiintyvälle $\varphi \Rightarrow \psi$.

Ilmausta ”Jos $\varphi \Rightarrow \psi$, niin $\chi \Rightarrow \zeta$” ei siis tulkita ”jos $\varphi \Rightarrow \psi$ on pätevä päättelysääntö, niin myös $\chi \Rightarrow \zeta$ on pätevä päättelysääntö” vaan ”jos mahdolliset tilanteet rajoitetaan niihin, joille $\varphi \Rightarrow \psi$ on pätevä päättelysääntö, niin myös $\chi \Rightarrow \zeta$ on pätevä päättelysääntö”. Havainnollistamme tätä esimerkillä ”jos $P \Rightarrow Q$, niin $Q \Rightarrow P$”. Oletamme, että kaikki neljä P:n ja Q:n totuusarvojen yhdistelmää ovat mahdollisia. Luonnollisen kielen ilmaus ”jos P:stä seuraa Q, niin Q:sta seuraa P” on väärin, koska tilanne $P \Leftrightarrow \mathsf{F}$ ja $Q \Leftrightarrow \mathsf{T}$ on sille vastaesimerkki. Saman vastaesimerkin vuoksi se on väärin myös valitsemamme tulkintatavan mukaan. Tilanne $P \Leftrightarrow \mathsf{T}$ ja $Q \Leftrightarrow \mathsf{F}$ on vastaesimerkki osuudelle $P \Rightarrow Q$. Siksi tulkintatavan ”jos $P \Rightarrow Q$ on pätevä päättelysääntö, niin ...” mukaan esimerkkimme olisikin oikein. Valitsemamme tulkintatapa vastaa siis paremmin luonnollisen kielen ilmausten merkitystä kuin hylkäämämme tulkintatapa.

Äskeisissä esimerkeissä tilapäiset oletukset olivat muotoa $\varphi \Rightarrow \psi$ tai $\varphi \Leftrightarrow \psi$. Tilapäinen oletus voi olla myös pelkkä kaava. Seuraava periaate (joskaan ei juuri tässä muodossa, vaan käyttäen $\Rightarrow$:n sijaan $\rightarrow$:ta ja puhuen todistamisesta) tunnetaan nimellä *deduktiolause* (*deduction theorem*):

Jos tilapäisen oletuksen φ vallitessa ψ on aina tosi,
niin ilman oletusta φ pätee $\varphi \Rightarrow \psi$. [21]

Todistus. Oletuksen φ lisäämisen jälkeen mahdollisia tilanteita ovat täsmälleen ne, jotka olivat mahdollisia juuri ennen lisäämistä, ja joissa lisäksi φ on tosi. Jos-osan mukaan myös ψ on niissä tosi. Niinpä jokaisessa tilanteessa, joka oli mahdollinen juuri ennen oletuksen φ lisäämistä pätee, että jos φ on siinä tosi, myös ψ on siinä tosi. Siksi [19]:n mukaan $\varphi \Rightarrow \psi$. $\square$

Edellä "päättelyimplikaatioksi" kutsuttiin sekä ilmausta muotoa $\varphi \Rightarrow \psi$, missä φ ja ψ ovat kaavoja, että päättelysääntöä, joka voidaan esittää tällaisella ilmauksella. Myös symbolia $\Rightarrow$ sellaisenaan (siis ilman kaavoja sen edessä ja perässä) saa kutsua päättelyimplikaatioksi. Mainittakoon vielä, että päättelyimplikaatio ei ole sama asia kuin looginen seuraus. Niiden eron selitys on pitkä. Asiaan palataan luvussa 2.4. Sen sijaan päättelyimplikaatiota voi aivan hyvin kutsua matemaattiseksi seuraukseksi.

Kuten aiemmin todettiin, $\varphi \Rightarrow \psi$ on pätevä jos ja vain jos sille ei ole olemassa yhtään vastaesimerkkiä, eli mahdollista tilannetta jossa φ tuottaa T mutta ψ tuottaa F. Jos ei ole olemassa mahdollista tilannetta jossa φ tuottaa T, niin ei ole olemassa mahdollista tilannetta jossa φ tuottaa T mutta ψ tuottaa F. Tästä seuraa, että jos φ ei ole tosi missään mahdollisessa tilanteessa, niin $\varphi \Rightarrow \psi$ on pätevä riippumatta siitä mikä ψ on. Toisin sanoen, mahdottomasta seuraa ihan mitä tahansa! Tämä ilmiö tunnetaan englanninkielellä nimellä *principle of explosion*.

Siis esimerkiksi "jos mummo on samanaikaisesti Pihtiputaalla ja Rovaniemellä, niin hän on Kuopiossa" on pätevä. Sille ei ole olemassa vastaesimerkkiä, koska vastaesimerkissä mummon pitäisi olla samanaikaisesti Pihtiputaalla ja Rovaniemellä, ja se on mahdotonta. Juuri ennen cup-muotoisen kilpailun loppuottelua "jos joukkue voittaa vielä yhdenkin ottelun, niin se voittaa koko kilpailun" on tietysti totta loppuotteluun osallistuville joukkueille. Mutta se on totta myös niille joukkueille, jotka ovat jo pudonneet kisasta! Ei voi käydä niin että sellainen joukkue voittaa vielä jonkin ottelun mutta silti ei voita koko kilpailua, koska se ei voi enää voittaa yhtään ottelua, koska se ei pelaa enää yhtään ottelua.

Vaikka tämä ilmiö tuottaa hullun näköisiä johtopäätöksiä, se ei tuota vääriä johtopäätöksiä. Se ei lupaa, että missään todellisessa tilanteessa mummo on samanaikaisesti monessa paikassa. Se ei lupaa, että joukkueella, joka on jo pudonnut kisasta, olisi vielä mahdollisuus voittaa. Sen tuottamat johtopäätökset koskevat vain epätodellisia tilanteita, joten ne ovat todellisuuden kannalta merkityksettömiä. Siksi se ei pilaa logiikan kykyä tuottaa luotettavia tuloksia.

Toisaalta ei voida kieltää normaalien päättelytapojen käyttöä mahdottomiin tilanteisiin, koska usein tarvitsee päätellä tilanteesta, josta ei etukäteen tiedetä, onko se mahdollinen. Voidaan esimerkiksi tietää auton sijainti, vauhti ja kulkusuunta sekä hyttysen sijainti, vauhti ja kulkusuunta, ja halutaan tietää, osuuko hyttynen autoon ja jos kyllä, niin mihin kohtaan. Laskut voivat antaa tulokseksi, että auton ja hyttysen radat eivät kohtaa. Silloin törmääminen on mahdotonta. Tulokseksi voi myös tulla että radat kohtaavat, mutta törmäys tapahtui menneisyydessä. Se on mahdoton tulos, koska törmäyksen jälkeen hyttynen ei enää kykene lentämään. Silti on tärkeää, että laskut voitiin tehdä ja niiden tuloksiin voidaan luottaa, koska juuri sillä tavalla saatiin selville, että todellisuudessa hyttynen ei törmää.

Myös on tavallista, että päättelyn lähtökohdaksi otetaan tietoisesti jotakin joka ei päde, ja päättelyn nimenomaisena tarkoituksena on osoittaa, että se ei päde. Tätä voi havainnollistaa esimerkillä, jossa Melusten lasten luokkatoveri on kutsunut heidät kylään. Luokkatoverin isä tai äiti tulee kaupasta ja päättelee, että jos Melusten lapset olisivat jo tulleet, niin täällä olisi melkoinen meteli; mutta täällä on hiljaista, joten he eivät ole vielä tulleet. Tällainen tapa päätellä kelpasi setä Joellekin. Hän oletti että Carr on ulkona, todistaakseen että Carr ei ole ulkona.

Setä Joelle ei kuitenkaan kelvannut enää se, että siitä, että myös Allen on ulkona, seuraa sekä Brown on ulkona että Brown on paikalla. Siksi setä Joe päätyi siihen väärään johtopäätökseen, että Carr ei voi olla ulkona. Setä Jimin ja nykynäkemyksen mukaan Brownin oleminen yhtäaikaa ulkona ja paikalla ei ole ristiriita, vaan osoitus siitä, että Allen ei voi olla ulkona. Tämä tulkinta pakottaa hyväksymään, että kun Carr on ulkona (mikä on mahdollista), Allenin ulkona olemisesta seuraa kaksi keskenään vastakkaista johtopäätöstä. Tämä ei ole ongelma, jos todetaan, että kun Carr on ulkona, on Allenin ulkona oleminen mahdotonta, mutta mahdottomasta saa seurata mitä tahansa.

Tästä voi jatkaa seuraavasti. Koska Brown on ulkona, niin Brown on ulkona tai kuu on vihreää juustoa. Koska lisäksi Brown ei ole ulkona, niin ”Brown on ulkona tai kuu on vihreää juustoa” voi toteutua vain siten, että kuu on vihreää juustoa. Siis siitä, että sekä Carr että Allen ovat ulkona, seuraa, että kuu on vihreää juustoa! Tämä päättely voi vaikuttaa loogiselta silmänkääntötempulta jolla huijataan lukijoita. Mutta jos se halutaan tuomita virheelliseksi, niin missä kohdassa virhe tapahtui? Loogikoiden valtavirta on tullut siihen tulokseen, että ei missään. Siinä ei ole virhettä. Se saattaa tuntua epäilyttävältä, mutta se ei tuota väärää johtopäätöstä mitään todellista tilannetta koskien. Se ei todista, että kuu on vihreää juustoa. Kun sen mukaan kuu on vihreää juustoa, ovat myös Carr ja Allen yhtäaikaa ulkona, mutta kuten aiemmin totesimme, he eivät voi olla yhtäaikaa ulkona.

Sen, että mahdottomasta seuraa mitä tahansa, todisti Soissonsin William jo 1100-luvulla. Vaikka vielä setä Joella oli vaikeuksia sen kanssa, nykyisin se on keskeisessä asemassa logiikan valtavirtaa. Usein se otetaan sellaisenaan mukaan jo lähtökohtana käytettäviin päättelysääntöihin (sen sijaan, että se johdettaisiin muista säännöistä). Mekin tulemme tekemään niin sivulla 128. On sovelluksia, joissa sitä ei voi hyväksyä. Niitä varten on kehitetty niin sanottuja parakonsistentteja logiikoita. Ne ovat kuitenkin erikoisalue. Logiikan valtavirrassa mahdottomasta todella seuraa mitä tahansa.

On siis järkevää hyväksyä, että mahdottomasta seuraa mitä tahansa. Kuten totesimme, se seuraa periaatteesta, jonka mukaan jokin on väärin jos ja vain jos sille on vastaesimerkki. Tämä periaate on yksinkertainen, selkeä ja osoittautunut luotettavaksi, joten siinä kannattaa pitäytyä. Jos virheetön päättely johtaa mahdottomaan lopputulokseen, niin se ei tarkoita, että lopputulos olisi todellinen, vaan että päättelyn lähtökohdissa on jotain mahdotonta. Siitä, että edellä johdimme, että kuu on vihreää juustoa, ei seuraa että kuu todella on vihreää juustoa, vaan että Carr ja Allen eivät voi olla yhtäaikaa ulkona.

2.4 Päättelyoperaattorit

Sivulla 32 kerrottiin, että $\Rightarrow$ on päättelyoperaattori. Merkintöjen samankaltaisuudesta olet varmaankin jo arvannut, että myös $\Leftrightarrow$ on päättelyoperaattori. Tässä alaluvussa käsittelemme päättelyaskelten ja päättelysääntöjen ilmaisemista päättelyoperaattoreilla

P	Q	1	2	3
F	F	$\surd$	-	$\surd$
F	T	$\surd$	-	$\surd$
T	F	$\surd$	$\surd$	-
T	T	$\surd$	$\surd$	-

Kuva 17: Todistuksen $P \wedge (\neg P \vee Q) \Leftrightarrow P \wedge Q$ eri vaiheissa mahdolliset tilanteet

$\Rightarrow$, $\Leftrightarrow$ ja $\Leftarrow$. Aloitamme esimerkillä, joka käyttää jo tutuksi tullutta päättelytapaa ja johon viittaamme myöhemminkin.

> Jos $P \Leftrightarrow \mathsf{T}$, niin $P \wedge (\neg P \vee Q) \Leftrightarrow \mathsf{T} \wedge (\neg \mathsf{T} \vee Q) \Leftrightarrow \neg \mathsf{T} \vee Q \Leftrightarrow \mathsf{F} \vee Q \Leftrightarrow Q \Leftrightarrow \mathsf{T} \wedge Q \Leftrightarrow P \wedge Q$. Jos $P \Leftrightarrow \mathsf{F}$, niin $P \wedge (\neg P \vee Q) \Leftrightarrow \mathsf{F} \wedge (\neg \mathsf{F} \vee Q) \Leftrightarrow \mathsf{F} \Leftrightarrow \mathsf{F} \wedge Q \Leftrightarrow P \wedge Q$. Niinpä $P \wedge (\neg P \vee Q) \Leftrightarrow P \wedge Q$.

Aluksi kaikki P:n ja Q:n totuusarvojen yhdistelmät ovat mahdollisia. Sitä esittää kuvan 17 sarake 1. ”Jos $P \Leftrightarrow \mathsf{T}$” ilmoittaa, että siitä alkaen $P \Leftrightarrow \mathsf{T}$ on pätevä päättelysääntö sanan ”jos” vaikutusalueen loppumiseen saakka. Se poistaa mahdollisista tilanteista ne, joissa P:n totuusarvo ei ole T. Nyt mahdolliset tilanteet ilmaisee kuvan 17 sarake 2. Poistetut tilanteet palaavat takaisin mahdollisiin tilanteisiin ja kaksi muuta tilannetta muuttuu mahdottomiksi kohdassa ”Jos $P \Leftrightarrow \mathsf{F}$”. Samalla $P \Leftrightarrow \mathsf{F}$ muuttuu päteväksi ja on pätevä sanaan ”Niinpä” saakka. Sillä välillä mahdolliset tilanteet ilmaisee kuvan 17 sarake 3. Sanan ”Niinpä” kohdalla sarake 1 astuu jälleen voimaan.

Osuus $P \wedge (\neg P \vee Q) \Leftrightarrow \mathsf{T} \wedge (\neg \mathsf{T} \vee Q)$ on päättelyaskel, joka käytti tilapäisesti voimassa olevaa sääntöä $P \Leftrightarrow \mathsf{T}$. Päättelyoperaattoriin $\Leftrightarrow$ perustuvaa sääntöä saa soveltaa kaavan sisällä. Tässä tapauksessa sitä sovellettiin kaavan $P \wedge (\neg P \vee Q)$ jokaiseen P:hen. Sillä johdettiin $\varphi(P) \Leftrightarrow \varphi(\mathsf{T})$, missä $\varphi(X)$ on $X \wedge (\neg X \vee Q)$.

Seuraava päättelyaskel $\mathsf{T} \wedge (\neg \mathsf{T} \vee Q) \Leftrightarrow \neg \mathsf{T} \vee Q$ käytti lakia $\mathsf{T} \wedge \psi \Leftrightarrow \psi$ siten, että ψ oli $\neg \mathsf{T} \vee Q$. Sitä seuraava askel $\neg \mathsf{T} \vee Q \Leftrightarrow \mathsf{F} \vee Q$ käytti sääntöä $\neg \mathsf{T} \Leftrightarrow \mathsf{F}$. Mihin
kaavaan $\varphi(X)$ sitä käytettiin? Vielä käytettiin lakia $\mathsf{F} \vee \psi \Leftrightarrow \psi$ siten, että ψ oli Q. Sen 54
jälkeen käytettiin erästä lakia takaperin — mitä lakia? Mihin ensimmäisen niin-osan 55
viimeinen päättelyaskel $\mathsf{T} \wedge Q \Leftrightarrow P \wedge Q$ perustuu? 56

Mitä sääntöjä käytettiin päättelyketjussa $P \wedge (\neg P \vee Q) \Leftrightarrow \mathsf{F} \wedge (\neg \mathsf{F} \vee Q) \Leftrightarrow \mathsf{F} \Leftrightarrow \mathsf{F} \wedge Q \Leftrightarrow P \wedge Q$? Käytettiinkö niitä kaavan sisällä vai koko kaavan tasolla, ja etuperin
vai takaperin? 57

Sana ”Niinpä” viittaa siihen, että kaikki tilanteet on käsitelty (sekä ne, joissa $P \Leftrightarrow \mathsf{T}$ että ne, joissa $P \Leftrightarrow \mathsf{F}$), ja aina saatiin $P \wedge (\neg P \vee Q) \Leftrightarrow P \wedge Q$. Siksi $P \wedge (\neg P \vee Q) \Leftrightarrow P \wedge Q$ on pätevä kaikissa tilanteissa, eli se on propositiologiikan laki.

Tässä esimerkissä päättely eteni pienin askelin, joten välivaiheita tuli paljon. Usein tehdään monta askelta ennen kuin seuraava välivaihe kirjoitetaan näkyviin. Esimerkin ensimmäisen päättelyketjun sijaan voidaan kirjoittaa vaikka $P \wedge (\neg P \vee Q) \Leftrightarrow \mathsf{T} \wedge (\neg \mathsf{T} \vee Q) \Leftrightarrow Q \Leftrightarrow \mathsf{T} \wedge Q \Leftrightarrow P \wedge Q$. Näin yksinkertainen päättely voidaan jopa tehdä melkein kokonaan päässälaskuna ja kirjoittaa $P \wedge (\neg P \vee Q) \Leftrightarrow Q \Leftrightarrow P \wedge Q$.

Päättelyoperaattorin $\Leftrightarrow$, sen avulla muodostettujen ilmausten $\varphi \Leftrightarrow \psi$ ja niiden tarkoittamien päättelysääntöjen nimiä ovat *yhtäpitävyys* ja *päättelyekvivalenssi*.

> **Määritelmä.** Jos jokaisessa mahdollisessa tilanteessa, jossa jompikumpi puoli on tosi, myös vastakkainen puoli on tosi, niin yhtäpitävyys on *pätevä*. Jos yhdessäkin mahdollisessa tilanteessa toinen puoli on tosi mutta toinen puoli ei ole, niin yhtäpitävyys on *epäpätevä*. Sellainen tilanne on *vastaesimerkki* (*counterexample*) yhtäpitävyydelle. [22]

Tässä yhteydessä on tärkeää huomauttaa, että toisin kuin voisi luulla, yhtäpitävyys eli päättelyekvivalenssi ei ole sama asia kuin se, mitä tarkasti kirjoitetuissa logiikan teksteissä hyvin yleisesti kutsutaan loogiseksi ekvivalenssiksi. Selitämme luvussa 3 miksi näin on, mutta sitä ennen keskitymme siihen, mitä ominaisuuksia yhtäpitävyydellä on.

Määritelmästä [22] seuraa välittömästi, että

$$\varphi \Leftrightarrow \mathsf{T} \text{ jos ja vain jos } \varphi \text{ on tosi jokaisessa mahdollisessa tilanteessa.} \qquad [23]$$

Määritelmä [22] yhtäpitävyydelle ja sen vastaesimerkeille ei puhu vasemmasta ja oikeasta puolesta, vaan jommastakummasta ja vastakkaisesta puolesta sekä toisesta ja toisesta puolesta. Määritelmän kannalta mikään ei muutu, jos vasen ja oikea puoli vaihdetaan. Toisin sanoen, yhtäpitävyys on *symmetrinen* (*symmetric*):

$$\text{Jos } \varphi \Leftrightarrow \psi\text{, niin } \psi \Leftrightarrow \varphi. \qquad [24]$$

Symmetrisyys tarkoittaa, että jokaisessa tilanteessa, jossa suhde pätee yhteen suuntaan, se pätee myös vastakkaiseen suuntaan. Yksikin tilanne, jossa suhde pätee toisinpäin mutta ei toisinpäin, estää suhdetta olemasta symmetrinen.

Yhtäpitävyyden voi tulkita myös tarkoittavan, että jokaisessa mahdollisessa tilanteessa vasen ja oikea puoli tuottavat saman totuusarvon. Käsitteen ”sama” ominaisuuksiin kuuluu, että jos vasen ja oikea puoli tuottavat saman totuusarvon, niin oikea ja vasen puoli tuottavat saman totuusarvon. Tälläkin ajattelutavalla on selvää, että yhtäpitävyys on symmetrinen.

Symmetrisyydestä seuraa, että mikä tahansa $\Leftrightarrow$-laki käännettynä takaperin on laki. Vaikka $P \Leftrightarrow \mathsf{T}$ ja $P \Leftrightarrow \mathsf{F}$ eivät ole lakeja vaan tilapäisesti voimassa olevia oletuksia, niitäkin saa $\Leftrightarrow$:n symmetrisyyden ansiosta käyttää takaperin. Missä tämän alaluvun alussa olleen esimerkin päättelyaskelissa teimme niin? 58

On tärkeää huomata, että $\Rightarrow$ ei ole symmetrinen. Esimerkiksi $\mathsf{F} \Rightarrow \mathsf{T}$ pätee mutta $\mathsf{T} \Rightarrow \mathsf{F}$ ei päde, ja $x > 3 \Rightarrow x > 1$ pätee mutta $x > 1 \Rightarrow x > 3$ ei päde (koska muun muassa $x = 2$ on sille vastaesimerkki).

Seuraaviin ja muihin samankaltaisiin kysymyksiin, jos vastaus on ”ei” niin perustele se vastaesimerkillä. ”Kyllä”-vastauksia on vaikeampi perustella vakuuttavasti, mutta sano vaikka mitä sana ”symmetrisyys” (ja myöhemmissä samankaltaisissa tehtävissä siellä käytetty sana) tarkoittaa sovellettuna kysymyksen tapaukseen.

Onko ihmisten välinen suhde ”x on y:n äiti” symmetrinen? 59

Onko ihmisten välinen suhde ”x on y:n esiäiti” symmetrinen? 60

Onko lukujen välinen suhde $x \leq y$ symmetrinen? 61

Onko lukujen välinen suhde $x < y$ symmetrinen? 62

Onko lukujen välinen suhde $x \neq y$ symmetrinen? 63

Yhtäpitävyys on myös *transitiivinen* (*transitive*):

$$\text{Jos } \varphi \Leftrightarrow \psi \text{ ja } \psi \Leftrightarrow \chi\text{, niin } \varphi \Leftrightarrow \chi. \qquad [25]$$

Sanoilla ilmaistuna [25] väittää, että jos φ ja ψ ovat todet täsmälleen samoissa mahdollisissa tilanteissa, ja jos ψ ja χ ovat todet täsmälleen samoissa mahdollisissa tilanteissa, niin myös φ ja χ ovat todet täsmälleen samoissa mahdollisissa tilanteissa. Olemme käyttäneet transitiivisuutta jo lukuisat kerrat, sillä siihen perustuu se, että yhtäpitävyyksistä muodostuvan ketjun ensimmäinen ja viimeinen kaava voidaan julistaa yhtäpitäviksi. Siis esimerkiksi kun oletuksesta $P \Leftrightarrow \mathsf{T}$ pääteltiin edellä $P \wedge (\neg P \vee Q) \Leftrightarrow$

$\mathsf{T} \land (\neg \mathsf{T} \lor Q) \Leftrightarrow \ldots \Leftrightarrow P \land Q$, niin transitiivisuus antoi luvan päätellä, että jos $P \Leftrightarrow \mathsf{T}$ niin $P \land (\neg P \lor Q) \Leftrightarrow P \land Q$. (Päätelmän $\varphi_0 \Leftrightarrow \varphi_n$ johtaminen päättelyketjusta $\varphi_0 \Leftrightarrow \varphi_1 \Leftrightarrow \ldots \Leftrightarrow \varphi_n$ käyttää transitiivisuutta $n-1$ kertaa: ensin $\varphi_0 \Leftrightarrow \varphi_1$ ja $\varphi_1 \Leftrightarrow \varphi_2$ tuottavat $\varphi_0 \Leftrightarrow \varphi_2$, sitten se ja $\varphi_2 \Leftrightarrow \varphi_3$ tuottavat $\varphi_0 \Leftrightarrow \varphi_3$ ja niin edelleen.)

Myös $\Rightarrow$ on transitiivinen.

Jos $\varphi \Rightarrow \psi$ ja $\psi \Rightarrow \chi$, niin $\varphi \Rightarrow \chi$. [26]

Todistus. Oletamme, että $\varphi \Rightarrow \psi$ ja $\psi \Rightarrow \chi$. Tarkastelemme mielivaltaista mahdollista tilannetta, jossa φ on tosi. Koska $\varphi \Rightarrow \psi$, on määritelmän [19] mukaan myös ψ tosi. Ja koska ψ on tosi ja $\psi \Rightarrow \chi$, sanoo [19] että myös χ on tosi. Olemme osoittaneet, että missä tahansa mahdollisessa tilanteessa, jossa φ on tosi, myös χ on tosi. Se tarkoittaa [19]:n mukaan, että $\varphi \Rightarrow \chi$. □

Laadi [26]:n todistusta muuttamalla todistus $\Leftrightarrow$:n transitiivisuudelle! 64

Onko ihmisten välinen suhde ”x on y:n äiti” transitiivinen? 65

Onko ihmisten välinen suhde ”x on y:n esiäiti” transitiivinen? 66

Onko lukujen välinen suhde $x \leq y$ transitiivinen? 67

Onko lukujen välinen suhde $x < y$ transitiivinen? 68

Onko lukujen välinen suhde $x \neq y$ transitiivinen? 69

Jos määrittelemme $\varphi \rightleftharpoons \psi$ tarkoittamaan $\varphi \Leftrightarrow \neg\psi$ eli että jokaisessa mahdollisessa tilanteessa φ ja ψ tuottavat eri totuusarvot, niin $\rightleftharpoons$ on symmetrinen mutta ei transitiivinen. Symmetrisyys on ilmeinen: jos $\varphi \rightleftharpoons \psi$, niin φ ja ψ tuottavat eri totuusarvot, joten ψ ja φ tuottavat eri totuusarvot, eli $\psi \rightleftharpoons \varphi$. Vastaesimerkki transitiivisuudelle saadaan valitsemalla φ:ksi F, ψ:ksi T ja χ:ksi F. Silloin $\varphi \rightleftharpoons \psi$ pätee ja $\psi \rightleftharpoons \chi$ pätee, koska ψ:n totuusarvo T on eri kuin φ:n ja χ:n totuusarvo F. Transitiivisuus vaatisi $\varphi \rightleftharpoons \chi$, mutta se ei päde, koska φ:llä ja χ:llä on sama totuusarvo F.

Yhtäpitävyys on myös *refleksiivinen* (*reflexive*), mikä tarkoittaa, että jokaisessa mahdollisessa tilanteessa jokainen kaava tuottaa itsensä kanssa saman totuusarvon. Todista, että myös päättelyimplikaatio on refleksiivinen! 70

$$\varphi \Leftrightarrow \varphi \qquad\qquad \varphi \Rightarrow \varphi \qquad [27]$$

Edellä määritelty $\rightleftharpoons$ ei ole refleksiivinen, koska φ ei tietenkään tuota eri totuusarvoa kuin se itse tuottaa.

Onko ihmisten välinen suhde ”x on y:n äiti” refleksiivinen? 71

Onko ihmisten välinen suhde ”x on y:n esiäiti” refleksiivinen? 72

Onko lukujen välinen suhde $x \leq y$ refleksiivinen? 73

Onko lukujen välinen suhde $x < y$ refleksiivinen? 74

Onko lukujen välinen suhde $x \neq y$ refleksiivinen? 75

Matematiikassa *ekvivalenssi* (*equivalence*) tarkoittaa mitä tahansa kahden olion välistä vertailuoperaatiota, joka on refleksiivinen, symmetrinen ja transitiivinen. Totesimme juuri, että yhtäpitävyydellä on nämä ominaisuudet. Sen toinen nimi ”päättelyekvivalenssi” kuvastaakin sitä, että se on päättelyssä käytettävä ekvivalenssi.

Ekvivalenssi ei välttämättä tarkoita, että verrattavat oliot olisivat täysin samat, siis että kukin olio on ekvivalentti itsensä kanssa mutta ei minkään muun olion kanssa. Se tarkoittaa ainostaan, että ne ovat jossain mielessä samanveroiset. Kun ekvivalenteille olioille tehdään sama asia, ne eivät enää välttämättä olekaan ekvivalentit. Tästä esimerkki ovat 16-vuotias Tarmo ja 17-vuotias Urho, jotka kuuluvat juoksun ikäsarjaan

alle 18-vuotiaat. Miksi on ilmiselvää, että samaan ikäsarjaan kuuluminen on ekvivalenssi? Mutta kun Tarmo ja Urho kumpikin vanhenevat vuoden, niin he eivät enää kuu- 76
lukaan samaan ikäsarjaan, sillä Tarmo on edelleen alle 18-vuotiaiden sarjassa mutta Urho ei enää ole.

Edes propositiologiikan kaavojen esittämiä totuusfunktioita vertaaville ekvivalensseille ei välttämättä päde, että kun ekvivalentteihin kaavoihin tehdään samanlainen lisäys, saadaan ekvivalentit kaavat. Saadaksemme tästä esimerkin määrittelemme kaavan ”vaikutuspaikkaluvun” tarkoittamaan niiden propositiomuuttujien määrää, joista kaavan tulos riippuu. Kaavan $\varphi(P_1,\ldots,P_n)$ tulos riippuu P_i:stä (missä $1 \leq i \leq n$), jos ja vain jos muille propositiomuuttujille P_1, ..., P_{i-1}, P_{i+1}, ..., P_n voidaan valita sellaiset totuusarvot, että $\varphi(P_1,\ldots,\mathsf{F},\ldots,P_n)$ ja $\varphi(P_1,\ldots,\mathsf{T},\ldots,P_n)$ tuottavat eri totuusarvot. On selvää, että jos määrittelemme $\varphi \rightleftharpoons \psi$ tarkoittamaan että φ:llä ja ψ:llä on sama vaikutuspaikkaluku, niin $\rightleftharpoons$ on φ:n ja ψ:n esittämien totuusfunktioiden välinen ekvivalenssi.

Sekä kaavan P että kaavan $\neg P$ vaikutuspaikkaluku on 1, koska kummankin tulos riippuu P:n totuusarvosta eikä riipu minkään muun propositiomuuttujan totuusarvosta. Siis $P \rightleftharpoons \neg P$. Lisäämällä kumpaankin $\wedge P$ saadaan $P \wedge P$, jonka vaikutuspaikkaluku myös on 1, sekä $\neg P \wedge P$, jonka vaikutuspaikkaluku on 0, koska sen tulos on aina F eikä niin ollen riipu minkään propositiomuuttujan totuusarvosta. Siis vaikka $P \rightleftharpoons \neg P$ pätee, $P \wedge P \rightleftharpoons \neg P \wedge P$ ei päde.

Millä valinnalla $\varphi(X)$ saadaan $\varphi(P)$:ksi $P \wedge P$ ja $\varphi(\neg P)$:ksi $\neg P \wedge P$? 77

Ei siis ole niin, että mitä tahansa ekvivalenssia saa soveltaa kaavan sisällä. Tulemme tässä alaluvussa huomaamaan, että päättelyimplikaatiotakin saa käyttää vain tietynlaisten kaavojen sisällä. Siitä huolimatta, kuten edellä on luvattu ja tehtykin monet kerrat, yhtäpitävyyttä saa soveltaa kaavan sisällä. (Vaikka $\forall$ ja $\exists$ kielletään alla, niitä saa käyttää, jos noudattaa sivulla 100 mainttua ehtoa. Voit unohtaa ”yhtäaikaa määritellyt” kunnes asia selitetään luvussa 3.1.)

> Jos $\forall$ ja $\exists$ eivät esiinny $\varphi(X)$:ssä, $\psi \Leftrightarrow \chi$, ja ψ ja χ ovat yhtäaikaa määritellyt, niin $\varphi(\psi) \Leftrightarrow \varphi(\chi)$, ja $\varphi(\psi)$ ja $\varphi(\chi)$ ovat yhtäaikaa määritellyt. [28]

Esimerkiksi jos $P \Leftrightarrow \mathsf{T}$, niin saa päätellä kuten päättelimme tämän alaluvun alussa:

$$P \wedge (\neg P \vee Q) \;\Leftrightarrow\; \mathsf{T} \wedge (\neg \mathsf{T} \vee Q) \;\Leftrightarrow\; \neg \mathsf{T} \vee Q \;\Leftrightarrow\; \mathsf{F} \vee Q \;\Leftrightarrow\; Q \;\Leftrightarrow\; \mathsf{T} \wedge Q \;\Leftrightarrow\; P \wedge Q$$

Kerroimme jo siellä mitä päättelyssä tapahtui, mutta nyt suhteutamme sen [28]:een. Ensimmäisessä askeleessa valittiin [28]:n $\varphi(X)$:ksi $X \wedge (\neg X \vee Q)$, ψ:ksi P ja χ:ksi T. Sitten siitä, että $\psi \Leftrightarrow \chi$ eli $P \Leftrightarrow \mathsf{T}$, johdettiin $\varphi(P) \Leftrightarrow \varphi(\mathsf{T})$ eli $P \wedge (\neg P \vee Q) \Leftrightarrow \mathsf{T} \wedge (\neg \mathsf{T} \vee Q)$. Mitkä asiat tehtiin viimeisessä askeleessa? 78

Ehkä yllättäen, jos $P \Leftrightarrow \mathsf{T}$, myös seuraavalla tavalla saa päätellä:

$$P \wedge (\neg P \vee Q) \;\Leftrightarrow\; P \wedge (\neg \mathsf{T} \vee Q) \;\Leftrightarrow\; P \wedge (\mathsf{F} \vee Q) \;\Leftrightarrow\; P \wedge Q$$

Tämä tapa on lyhyempi. Tämä esimerkki havainnollistaa, että joskus kannattaa korvata vain osa saman propositiomuuttujan esiintymistä. Mikä on $\varphi(X)$ ensimmäisessä askeleessa? 79

Sen lisäksi, että [28] sallii korvata kaavan sisällä olevia propositiomuuttujan esiintymiä kaavoilla, se sallii korvata kaavan sisällä olevia kaavoja kaavoilla. Esimerkiksi teimme sivulla 17 apupäätelmän $\neg(\mathsf{F} \vee \neg Q) \Leftrightarrow \mathsf{T} \wedge Q$, ja sen avulla johdimme $\neg P \vee \neg\neg(\mathsf{F} \vee \neg Q) \Leftrightarrow \neg P \vee \neg(\mathsf{T} \wedge Q)$. Kun tämä tulkitaan lain [28] käyttönä, niin mikä on $\varphi(X)$, mikä on ψ ja mikä on χ? 80

Yhtäpitävyyttä voi käyttää kaavan sisällä myös koulumatematiikassa ja predikaattilogiikassa. (Symbolien $\forall$ ja $\exists$ kanssa asia monimutkaistuu, mutta niitä aletaan käyttää vasta luvussa 5.) Työllisyysastetta laskettaessa otetaan huomioon heidät, joiden ikä on alle 65 vuotta mutta ei alle 15 vuotta. Jos ikää merkitään x:llä, niin ikärajat voi ilmaista kaavana $x < 65 \land \neg(x < 15)$. Koska $\neg(x < 15) \Leftrightarrow x \geq 15$, pätee $x < 65 \land \neg(x < 15) \Leftrightarrow x < 65 \land x \geq 15$. Kun tämä tulkitaan lain [28] käyttönä, niin mikä on $\varphi(X)$, mikä on ψ ja mikä on χ? 81

Se, että yhtäpitävyyttä voi käyttää propositiologiikan kaavan sisällä vaikka edellä määrittelemämme ekvivalenssia ”sama vaikutuspaikkaluku” ei voi, johtuu kahdesta seikasta: yhtäpitävyyden tarkastus palautuu yksittäisiksi, toisistaan riippumattomiksi totuusarvojen vertaamisiksi, ja kunkin konnektiivin tuottama totuusarvo riippuu vain osakaavojen tuottamista totuusarvoista. Yksityiskohdat käyvät ilmi seuraavasta todistuksesta. Se noudattaa menetelmää nimeltä *rakenteellinen induktio* (*structural induction*). Siinä väite osoitetaan ensin atomikaavoille sekä X:n tilalle tuleville kaavoille. Sitten jokaisesta konnektiivista osoitetaan, että väite pätee sillä muodostetulle kaavalle, jos se pätee sen argumentteina oleville osakaavoille.

Idea käy ehkä paremmin ilmi esimerkistä. Jos $\varphi(X)$ on $\neg X \lor (P \land X)$, niin $\varphi(\psi)$ on $\neg\psi \lor (P \land \psi)$ ja $\varphi(\chi)$ on $\neg\chi \lor (P \land \chi)$. Tarkastelemme mielivaltaista mahdollista tilannetta. Koska $\psi \Leftrightarrow \chi$, tuottaa ψ siinä saman totuusarvon kuin χ. Koska $\neg X$:n tuottama totuusarvo riippuu vain X:n totuusarvosta, tuottaa $\neg\psi$ mielivaltaisessa tilanteessamme saman totuusarvon kuin $\neg\chi$. Tietenkin P tuottaa tilanteessamme saman totuusarvon kuin P. Siksi, ja koska $\land$:n tuottama totuusarvo riippuu vain osakaavojen tuottamista totuusarvoista, tuottaa $P \land \psi$ saman totuusarvon kuin $P \land \chi$. Koska $\neg\psi$ tuottaa saman totuusarvon kuin $\neg\chi$ ja $P \land \psi$ tuottaa saman totuusarvon kuin $P \land \chi$, ja koska $\lor$:n tuottama totuusarvo riippuu vain osakaavojen tuottamista totuusarvoista, tuottaa $\neg\psi \lor (P \land \psi)$ saman totuusarvon kuin $\neg\chi \lor (P \land \chi)$.

Tämä esitettynä mielivaltaiselle $\varphi(X)$ riittää todistukseksi seuraavasta syystä. Kukin kaava koostuu äärellisestä määrästä merkkejä, joten sitä ei voi pilkkoa pienemmäksi loputtomasti. Siksi, jos olisi olemassa kaava, jolle väite ei päde, niin olisi olemassa mahdollisimman pieni sellainen kaava. Mutta mikään atomikaava ei voi olla sellainen, koska väite osoitetaan päteväksi kullekin niistä. Symbolin X tilalle tuleva kaava ei voi olla sellainen, koska väite olettaa $\psi \Leftrightarrow \chi$. Eikä mikään yhdistetty kaava $\varphi(X)$ voi olla sellainen, koska jos väite pätee $\varphi(X)$:n kaikille osakaavoille, niin todistuksen mukaan se pätee $\varphi(X)$:llekin; ja jos väite ei päde jollekin $\varphi(X)$:n osakaavalle, niin $\varphi(X)$ ei olekaan mahdollisimman pieni kaava jolle väite ei päde. Siksi ei voi olla olemassa kaavaa, jolle väite ei päde.

Olemme itse asiassa jo käyttäneet rakenteellista induktiota apulauseen [10] sekä lauseiden [12] ja [15] todistuksissa. Niissä ilmaisimme asian sanomalla, että kaavan tai totuusfunktion käsittelyssä mahdollisesti syntyvät osakaavat tai osien funktiot käsitellään samalla tavalla kuin alkuperäinen kaava tai funktio. Ohjelmoinnissa sama periaate tunnetaan nimellä *rekursio* (*recursion*).

Todistus [28]:lle propositiologiikassa. Käytämme rakenteellista induktiota.

Atomikaavojen tapaus on hyvin helppo. Jos $\varphi(X)$ on F, niin sekä $\varphi(\psi)$ että $\varphi(\chi)$ on F, joten ilmiselvästi $\varphi(\psi) \Leftrightarrow \varphi(\chi)$. Vastaava pätee jos $\varphi(X)$ on T tai muu propositiomuuttuja kuin X. Tapaukselle $\varphi(X)$ on X pätee $\varphi(\psi) \Leftrightarrow \psi \Leftrightarrow \chi \Leftrightarrow \varphi(\chi)$, koska [28] olettaa, että $\psi \Leftrightarrow \chi$.

Konnektiivin $\neg$ käsittelemiseksi olkoon $\psi \Leftrightarrow \chi$. Valitaan tarkasteltavaksi mikä tahansa mahdollinen tilanne. Siinä ψ tuottaa jonkin totuusarvon. Koska $\psi \Leftrightarrow \chi$, tuottaa χ saman totuusarvon. Koska ne tuottavat saman totuusarvon ja koska $\neg$:n tuottama totuusarvo riippuu vain $\neg$:n alaisen osakaavan tuottamasta totuusarvosta, tuottaa $\neg\psi$ saman totuusarvon kuin $\neg\chi$. Tämä päättely pätee jokaiselle mahdolliselle tilanteelle, joten $\neg\psi$ tuottaa jokaisessa mahdollisessa tilanteessa saman totuusarvon kuin $\neg\chi$. Toisin sanoen, $\neg\psi \Leftrightarrow \neg\chi$.

Nyt olkoon $\psi_1 \Leftrightarrow \chi_1$ ja $\psi_2 \Leftrightarrow \chi_2$. Jos valitaan jokin mahdollinen tilanne, ihan mikä tahansa, niin siinä tilanteessa ψ_1 tuottaa saman totuusarvon kuin χ_1 ja ψ_2 tuottaa saman totuusarvon kuin χ_2. Koska $\wedge$:n tuottama totuusarvo riippuu vain sen alaisten osakaavojen tuottamista totuusarvoista, tuottaa $\psi_1 \wedge \psi_2$ saman totuusarvon kuin $\chi_1 \wedge \chi_2$. Koska tämä pätee jokaiselle mahdolliselle tilanteelle, saamme $\psi_1 \wedge \psi_2 \Leftrightarrow \chi_1 \wedge \chi_2$. Sama päättely pätee konnektiiveille $\vee$, $\rightarrow$ ja $\leftrightarrow$. $\square$

Hupsista, todistuksessa mainittiin $\leftrightarrow$, vaikka sitä ei ole vielä esitelty! Tämä puute täytyy korjata heti.

Aivan kuten päättelyoperaattoria $\Rightarrow$ vastaa konnektiivi $\rightarrow$ nimeltä materiaalinen implikaatio, myös päättelyoperaattoria $\Leftrightarrow$ vastaa konnektiivi $\leftrightarrow$ nimeltä *materiaalinen ekvivalenssi* (*material equivalence*). Kaava $P \leftrightarrow Q$ tuottaa T jos ja vain jos P:llä ja Q:lla on sama totuusarvo. Vertaamalla tätä määritelmään [22] saadaan analogisesti [20]:n kanssa

> Kaksiarvoisen logiikan päättelysääntö $\varphi \Leftrightarrow \psi$ on pätevä, jos ja vain jos jokaisessa mahdollisessa tilanteessa $\varphi \leftrightarrow \psi$ tuottaa T. Oletuksena esiintyessään $\varphi \Leftrightarrow \psi$ poistaa mahdollisista tilanteista ne, joissa $\varphi \leftrightarrow \psi$ ei tuota T. [29]

Materiaalinen ekvivalenssi voidaan ilmaista muiden konnektiivien avulla monella tavalla:

$$\begin{aligned} \varphi \leftrightarrow \psi &\Leftrightarrow (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi) \\ &\Leftrightarrow (\neg\varphi \vee \psi) \wedge (\varphi \vee \neg\psi) \\ &\Leftrightarrow (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi) \end{aligned} \qquad [30]$$

Jos haluat muistaa vain yhden $\leftrightarrow$:a koskevan lain, niin muista vaikka $\varphi \leftrightarrow \psi \Leftrightarrow (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$. Sillä saadaan $\leftrightarrow$ aina korvattua $\neg$:llä, $\wedge$:lla ja $\vee$:lla, jolloin muita $\leftrightarrow$:a koskevia lakeja ei välttämättä tarvita. Esimerkiksi sijoittamalla siihen vuoron perään φ:hin ja ψ:hin F ja T ja sieventämällä oikea puoli saadaan

$$\mathsf{F} \leftrightarrow \psi \Leftrightarrow \neg\psi \qquad \mathsf{T} \leftrightarrow \psi \Leftrightarrow \psi \qquad \varphi \leftrightarrow \mathsf{F} \Leftrightarrow \neg\varphi \qquad \varphi \leftrightarrow \mathsf{T} \Leftrightarrow \varphi \qquad [31]$$

Johda $\neg(\varphi \leftrightarrow \psi) \Leftrightarrow \neg\varphi \leftrightarrow \psi$ [30]:n alimman lain avulla! 82

Johda $\neg(\varphi \leftrightarrow \psi) \Leftrightarrow \neg\varphi \leftrightarrow \psi$ sijoittamalla φ:n tilalle vuoron perään F ja T! Nyt ja tästä eteenpäin saat tehdä päättelyt suoraan kreikkalaisilla kirjaimilla, eli ei tarvitse käyttää tilapäisiä propositiomuuttujia. 83

Tässä kirjassa $\leftrightarrow$ on vasemmalle liitännäinen. Jolleivät sulkeet määrää toisin, se lasketaan vasta kun $\neg$, $\wedge$, $\vee$ ja $\rightarrow$ on laskettu. Siis esimerkiksi $P \leftrightarrow Q \rightarrow R \leftrightarrow S$ tarkoittaa samaa kuin $(P \leftrightarrow (Q \rightarrow R)) \leftrightarrow S$. Tutki, onko $\leftrightarrow$ vaihdannainen! Tutki, onko 84
$\leftrightarrow$ liitännäinen! 85

Koska $\leftrightarrow$:n nimi on "materiaalinen ekvivalenssi", olet varmaankin jo ajat sitten arvannut, että $\leftrightarrow$ on ekvivalenssi. Sen osoittamiseksi, että $\leftrightarrow$ on ekvivalenssi, tarkastelkaamme mitä tahansa tilannetta. Jokainen kaava tuottaa siinä itsensä kanssa saman totuusarvon. Jos φ tuottaa siinä saman totuusarvon kuin ψ, niin ψ tuottaa siinä saman totuusarvon kuin φ. Jos φ tuottaa siinä saman totuusarvon kuin ψ ja ψ tuottaa siinä saman totuusarvon kuin χ, niin φ tuottaa siinä saman totuusarvon kuin χ.

Mutta asia ei ole ihan näin yksinkertainen. Se vertailuoperaatio, jota $\leftrightarrow$ esittää, todellakin on ekvivalenssi; mutta kuten seuraavaksi näemme, $\leftrightarrow$ käyttäytyy kaavoissa eri tavalla kuin tutuimmat ekvivalenssia tarkoittavat symbolit. Ero ilmenee kun symboleita ketjutetaan. Esimerkiksi koulumatematiikassa

$$2(x+1)-x \;=\; 2x+1-x \;=\; x+1$$

tarkoittaa, että

$$2(x+1)-x \;=\; 2x+1-x \quad \text{ja} \quad 2x+1-x \;=\; x+1 \quad ,$$

joka on väärin, koska $2(x+1)-x = 2x+1-x$ on väärin (kokeile $x=0$). Myös propositiologiikan, koulumatematiikan ja predikaattilogiikan $\Leftrightarrow$:t käyttäytyvät ketjutettuina samalla tavalla:

$$\neg(P \rightarrow Q) \;\Leftrightarrow\; \neg(\neg P \vee Q) \;\Leftrightarrow\; P \wedge \neg Q$$

tarkoittaa, että

$$\neg(P \rightarrow Q) \;\Leftrightarrow\; \neg(\neg P \vee Q) \quad \text{ja} \quad \neg(\neg P \vee Q) \;\Leftrightarrow\; P \wedge \neg Q \quad ,$$

joka on oikein. Siis jos f, g ja h edustavat lausekkeita, niin $f = g = h$ tarkoittaa $f = g \wedge g = h$; ja jos φ, ψ ja χ edustavat kaavoja (niin kuin ovat koko ajan tehneet), niin $\varphi \Leftrightarrow \psi \Leftrightarrow \chi$ tarkoittaa, että sekä $\varphi \Leftrightarrow \psi$ että $\psi \Leftrightarrow \chi$ on pätevä. Mutta koska $\leftrightarrow$ ei ole matematiikan vertailuoperaattori eikä päättelyoperaattori vaan konnektiivi, sen ketjutusta ei tulkita samalla tavalla. Sen sijaan $\varphi \leftrightarrow \psi \leftrightarrow \chi$ tarkoittaa $(\varphi \leftrightarrow \psi) \leftrightarrow \chi$.

Miksi se tulkitaan niin eikä näin: $\varphi \leftrightarrow (\psi \leftrightarrow \chi)$? Aiemmin todettiin, että näiden 86
kahden vaihtoehdon välinen ero on olennainen $\rightarrow$:n tapauksessa mutta harvoin tärkeä $\wedge$:n tapauksessa. Onko se olennainen vai harvoin tärkeä $\leftrightarrow$:n tapauksessa? Miksi? 87

Näiden tulkintatapojen eron havainnollistamiseksi laskemme, minkä totuusarvon seuraavat kaavat tuottavat x:n eri arvoilla:

$$2(x+1)-x=6 \;\leftrightarrow\; 2x+1-x=6 \;\leftrightarrow\; x+1=6 \tag{7}$$

$$\big(2(x+1)-x=6 \;\leftrightarrow\; 2x+1-x=6\big) \;\wedge\; \big(2x+1-x=6 \;\leftrightarrow\; x+1=6\big) \tag{8}$$

Ratkaisemalla yhtälö $2(x+1)-x=6$ saadaan $x=4$, joten $2(x+1)-x=6$ on tosi jos ja vain jos $x=4$. Se perustelee kuvan 18 taulukon toisen sarakkeen. Kolmas ja viides sarake saadaan samalla tavalla yhtälöistä $2x+1-x=6$ ja $x+1=6$. Neljäs sarake kertoo kaavan $2(x+1)-x=6 \leftrightarrow 2x+1-x=6$ totuusarvon: T jos toisessa ja kolmannessa sarakkeessa on sama totuusarvo, ja F muutoin. Kaava (7) tuottaa T jos ja vain jos neljännessä ja viidennessä sarakkeessa on sama totuusarvo. Kaava (8) vaatii, että toisessa ja kolmannessa sarakkeessa on sama totuusarvo, ja kolmannessa ja viidennessä sarakkeessa on sama totuusarvo. Huomaamme, että (7) ja (8) eivät tuota aina samaa totuusarvoa.

Siis vaikka $\leftrightarrow$ on ekvivalenssi, sitä ei käytetä kaavoissa samalla tavalla kuin useimpia tuttuja ekvivalensseja. Tämä on tärkeää tiedostaa, jottei lukisi kaavoja väärin.

Myös on tärkeää tiedostaa, että vaikka $\varphi \leftrightarrow \psi \leftrightarrow \chi$ näyttää melkein samalta kuin $\varphi \Leftrightarrow \psi \Leftrightarrow \chi$, ne tulkitaan eri tavalla. Ensimmäinen erottava tekijä on se, että $\leftrightarrow$ tuottaa totuusarvon F tai T kullekin tilanteelle erikseen (myös mahdottomille), mutta $\Leftrightarrow$ tuottaa kaikista mahdollisista tilanteista yhteenvedon, joka on ”pätevä” tai ”epäpätevä”. Jos oletamme kaikki tilanteet mahdollisiksi esimerkissä $2(x+1)-x=6 \Leftrightarrow 2x+1-x=6$

x	$2(x+1)-x=6$	$2x+1-x=6$	$s2 \leftrightarrow s3$	$x+1=6$	(7)	(8)
4	T	F	F	F	T	F
5	F	T	F	T	F	F
muu	F	F	T	F	F	T

Kuva 18: Kaavojen (7) ja (8) totuusarvot eri tilanteissa

$\Leftrightarrow x+1=6$, niin tulos on ”epäpätevä”, koska, kuten kuvan 18 taulukon viimeisestä sarakkeesta näkyy, $x=4$ ja $x=5$ ovat vastaesimerkkejä askeleelle $2(x+1)-x=6 \Leftrightarrow 2x+1-x=6$.

Toinen erottava tekijä on se, että vaikka $\varphi \Leftrightarrow \psi$ on epäpätevä täsmälleen siinä tapauksessa että ainakin yhdessä mahdollisessa tilanteessa $\varphi \leftrightarrow \psi$ tuottaa F, ei ole niin että $\varphi \Leftrightarrow \psi \Leftrightarrow \chi$ on epäpätevä täsmälleen siinä tapauksessa että ainakin yhdessä mahdollisessa tilanteessa $\varphi \leftrightarrow \psi \leftrightarrow \chi$ tuottaa F. Esimerkiksi $x+1=2x-x \Leftrightarrow x+1=x \Leftrightarrow 1=0$ on pätevä, koska $x+1=2x-x$ tuottaa aina saman totuusarvon kuin $x+1=x$ tuottaa, ja $x+1=x$ tuottaa aina saman totuusarvon kuin $1=0$ tuottaa (ne kaikki tuottavat aina F). Silti $x+1=2x-x \leftrightarrow x+1=x \leftrightarrow 1=0$ tuottaa aina F. Sehän lasketaan (F $\leftrightarrow$ F) $\leftrightarrow$ F, joka tuottaa T $\leftrightarrow$ F, joka tuottaa F. Vielä hassumpaa on, että jos sen perään lisätään $\leftrightarrow 1=0$, niin saadaankin T, sillä ((F $\leftrightarrow$ F) $\leftrightarrow$ F) $\leftrightarrow$ F tuottaa T.

Olkoon φ jokin kaava, joka tuottaa joissakin mahdollisissa tilanteissa F ja joissakin T. Voit käyttää esimerkkinä kaavaa $x=0$. Missä tilanteissa $\varphi \leftrightarrow \varphi \leftrightarrow \ldots \leftrightarrow \varphi$ tuottaa F ja missä tilanteissa se tuottaa T? Perustele vastauksesi epämuodollisesti käyttäen ilmausta ”ja niin edelleen”! 88

Induktio (*induction*) (ilman etuliitettä) tarkoittaa samaa ideaa kuin sivulla 39 esitelty rakenteellinen induktio, mutta sovellettuna luonnollisiin lukuihin 0, 1, 2, ... tai positiivisiin kokonaislukuihin 1, 2, 3, ... Sekä induktio että rakenteellinen induktio ovat keskeisessä asemassa logiikassa. Siksi niidenkin harjoittelu on pikkuhiljaa aloitettava. Matematiikassa induktiotodistukset esitetään melkein aina tietyn mallin mukaan, josta ei käy ilmi, miksi induktio on pätevä todistusmenetelmä. Tulemme jatkossa käyttämään samaa mallia, mutta sitä ennen on hyvä varmistua, että sen pätevyyden syy sivulta 39 jää mieleen. Niinpä: perustele edellisen tehtävän vastauksesi siten, että vetoat induktion pätevyyden syyhyn! 89

Ketjutettujen ilmausten tulkinta kuten $=$ ja $\Leftrightarrow$ tulkitaan (ja siis ei kuten $\leftrightarrow$ tulkitaan) ei rajoitu ekvivalensseihin, vaan koskee useimpia tuttuja symboleita jotka esittävät *kaksipaikkaisia relaatioita* (*binary relation*), eli kahden olion vertailua tai suhdetta. Muun muassa koulumatematiikan $<$, $\leq$, $\neq$, $\geq$ ja $>$ käyttäytyvät niin. Esimerkiksi $0 \leq x < 1$ tarkoittaa samaa kuin $0 \leq x \wedge x < 1$. Joukko-opin $\subset$ ja $\subseteq$ käyttäytyvät samoin.

Myös ketjutettu $\Rightarrow$ käyttäytyy niin, mutta ketjutettu $\rightarrow$ käyttäytyy kuten ketjutettu $\leftrightarrow$. Tästä varsin dramaattinen esimerkki on

$$x=1 \;\Rightarrow\; x=2 \;\Rightarrow\; x=3\;\;,$$

jonka molemmat askeleet ovat selvästi väärin, mutta silti

$$x=1 \;\rightarrow\; x=2 \;\rightarrow\; x=3$$

on aina tosi. Koska $\rightarrow$ on oikealle liitännäinen, kaava tarkoittaa samaa kuin $x=1 \rightarrow (x=2 \rightarrow x=3)$. Jos $x \neq 1$, niin se on tosi siksi että ensimmäisen $\rightarrow$:n vasen puoli on epätosi. Jos $x=1$, niin ensimmäisen $\rightarrow$:n oikea puoli eli $x=2 \rightarrow x=3$ on tosi, koska se sievenee muotoon F $\rightarrow$ F, joka on tosi.

$\Leftrightarrow$	F	T
F	$\surd$	-
T	-	$\surd$

$\Rightarrow$	F	T
F	$\surd$	$\surd$
T	-	$\surd$

$\Leftarrow$	F	T
F	$\surd$	-
T	$\surd$	$\surd$

Kuva 19: Päättelyoperaattoreiden sallimat vasemman ja oikean puolen mahdollisessa tilanteessa tuottamien totuusarvojen yhdistelmät

Olemme tähän asti ilmaisseet osittain sanoilla ne vaatimukset, joista yhteensä muodostuu se, että kahden olion välinen vertailuoperaatio on ekvivalenssi. Nyt ilmaise ne muodossa ”vaatimuksen nimi: kaava” tai ”vaatimuksen nimi: kaava päättelyoperaattori kaava” niin, että vertailuoperaationa on $\leftrightarrow$. Älä siis todista, että $\leftrightarrow$ on ekvivalenssi, vaan vain sano se logiikan merkinnöillä. 90

Symbolin $\Leftarrow$ merkitys on helppo arvata: $\varphi \Leftarrow \psi$ tarkoittaa samaa kuin $\psi \Rightarrow \varphi$. Niinpä $\varphi \Leftarrow \psi$ on pätevä jos ja vain jos $\psi \Rightarrow \varphi$ on pätevä. Mikä on säännön $\varphi \Leftarrow \psi$ vastaesimerkki? 91

Ilmaus $\varphi \Leftrightarrow \psi$, $\varphi \Rightarrow \psi$ tai $\varphi \Leftarrow \psi$ on *päättelyaskel*, kun se esiintyy osana päättelyä, ja *päättelysääntö*, kun se kertoo jotakin jota saa käyttää päättelyssä. On tavallista mutta ei välttämätöntä, että päättelyaskel tuotetaan päättelysäännöstä laittamalla kaavoja esittävien kreikkalaisten kirjainten tilalle konkreettiset kaavat. Esimerkiksi Carrollin paradoksin yhteydessä vastauksessa 52 käytimme lakia $\varphi \vee (\neg\varphi \wedge \psi) \Leftrightarrow \varphi \vee \psi$ tuottamaan päättelyaskeleen $\neg A \vee (\neg\neg A \wedge (B \wedge \neg C)) \Leftrightarrow \neg A \vee (B \wedge \neg C)$ siten, että φ:n tilalla oli $\neg A$ ja ψ:n tilalla $B \wedge \neg C$.

Päättelyaskeleella ja päättelysäännöllä ei ole mitään eroa siltä osin, milloin ne ovat päteviä ja milloin eivät ole. Niiden pätevyysehdot on esitetty määritelmissä [19] ja [22], ja toisessa muodossa kuvassa 19. Kumpikin on pätevä, jos ja vain jos aina kun valitaan mikä tahansa mahdollinen tilanne, niin vasemman ja oikean puolen tuottamien totuusarvojen yhdistelmä on jokin kuvassa 19 symbolilla $\surd$ merkityistä. Mikä tahansa mahdollinen tilanne, jolla kuva 19 tuottaa -, on vastaesimerkki päättelyaskeleelle tai -säännölle, ja tekee siitä epäpätevän.

Päättelyoperaattoreita ei saa tässä kirjassa yliviivata (tyyliin $\not\Rightarrow$), eikä niitä sisältävien ilmausten ympärille saa panna sulkeita eikä niihin saa soveltaa konnektiiveja. Tämä kielto vähentää niiden sekaannusten riskiä, jotka voivat aiheutua siitä, että totuusarvo tuotetaan yksittäisessä tilanteessa mutta päättelyoperaattori tekee yhteenvedon kaikista mahdollisista tilanteista. Saa kirjoittaa ”$S \Rightarrow K$ tai $K \Rightarrow S$ on pätevä päättelysääntö”, mutta ei saa kirjoittaa ”$(S \Rightarrow K) \vee (K \Rightarrow S)$”. Tämä kielto ei hankaloita päättelyoperaattoreiden käyttöä siihen mihin ne on tarkoitettu, eli päättelyaskelten ja päättelysääntöjen ilmaisemiseen. Kielto on helppo muistaa ja noudattaa kun ajattelee, että päättelysääntö ei tuota totuusarvoa, vaan on pätevä tai epäpätevä.

Jollei kieltoa olisi, niin mitä $\varphi \not\Leftrightarrow \psi$ tarkoittaisi? Koska $\varphi \Leftrightarrow \psi$ tarkoittaa ”φ saa jokaisessa mahdollisessa tilanteessa saman totuusarvon kuin ψ”, pitäisikö merkinnän $\varphi \not\Leftrightarrow \psi$ tarkoittaa ”φ saa jokaisessa mahdollisessa tilanteessa eri totuusarvon kuin ψ”? Toisaalta koulumatematiikassa $x \neq y$ tarkoittaa samaa kuin $\neg(x = y)$, joten pitäisikö merkinnän $\varphi \not\Leftrightarrow \psi$ tarkoittaa samaa kuin $\neg(\varphi \Leftrightarrow \psi)$? Jälkimmäinen voidaan tulkita tarkoittamaan ”ei ole niin, että φ saa jokaisessa mahdollisessa tilanteessa saman totuusarvon kuin ψ”. Se on eri asia kuin edellinen tulkinta, koska esimerkiksi $P \wedge Q \not\Leftrightarrow P \vee Q$ on jälkimmäisen mukaan oikein ($\mathsf{T} \wedge \mathsf{F}$ tuottaa eri totuusarvon kuin $\mathsf{T} \vee \mathsf{F}$) mutta edellisen mukaan väärin ($\mathsf{T} \wedge \mathsf{T}$ tuottaa saman totuusarvon kuin $\mathsf{T} \vee \mathsf{T}$). Mutta kumpikaan näistä ei vastaa sitä, mitä $x \neq y$ ja $\neg(x = y)$ tarkoittavat koulumatematiikassa. Sitä vastaisi ”$P \wedge Q$ tuottaa eri totuusarvon kuin $P \vee Q$”. Se ei puhu jokaisesta mahdollisesta tilanteesta.

Päättelyketju on muotoa $\varphi_0 \rightleftharpoons_1 \varphi_1 \rightleftharpoons_2 \ldots \rightleftharpoons_n \varphi_n$, missä kukin φ_i on kaava ja kukin $\rightleftharpoons_i$ on päättelyoperaattori. Päättelyketjussa on oltava vähintään kaksi kaavaa, ja siis vähintään yksi päättelyoperaattori. Esimerkiksi

$$P \Leftrightarrow P \wedge P \Rightarrow (P \wedge P) \vee (P \wedge Q) \Leftrightarrow P \wedge (P \vee Q)$$

on päättelyketju. Mikä on sen n ja mikä on sen $\varphi_1 \rightleftharpoons_2 \varphi_2$? 92

Kukin $\varphi_{i-1} \rightleftharpoons_i \varphi_i$ on päättelyaskel. Onko jokainen päättelyaskel päättelyketju? Perustele! 93

Päättelyketju on pätevä jos ja vain jos sen jokainen askel on pätevä. Kunkin askeleen pätevyys määräytyy määritelmän [22] tai [19] mukaan. Onko yllä olevan esimerkin päättelyketju pätevä? Perustele! 94

Jos jokainen $\rightleftharpoons_i$ on $\Leftrightarrow$, niin transitiivisuuden vuoksi $\varphi_0 \Leftrightarrow \varphi_n$, eli ketjun ensimmäinen ja viimeinen kaava ovat yhtäpitävät. Jos kukin $\rightleftharpoons_i$ on $\Leftrightarrow$ tai $\Rightarrow$ (samassa ketjussa saa olla molempia), niin transitiivisuuden ja kohta todistettavan lain [32] vuoksi $\varphi_0 \Rightarrow \varphi_n$. Jos kukin $\rightleftharpoons_i$ on $\Leftrightarrow$ tai $\Leftarrow$ (samassa ketjussa saa olla molempia), niin transitiivisuuden ja [32]:n vuoksi $\varphi_0 \Leftarrow \varphi_n$. Mitä esimerkkimme päättelyketjusta voi päätellä tällä
tavalla? Samassa päättelyketjussa ei ole mielekästä esiintyä sekä $\Leftarrow$ että $\Rightarrow$ siksi, että 95
jos esiintyy, niin päättelyketju ei kerro mitään φ_0:n ja φ_n:n suhteesta.

Päättelyoperaattoreiden $\Leftrightarrow$ ja $\Rightarrow$ välinen suhde on seuraava:

- Jos $\varphi \Leftrightarrow \psi$, niin $\varphi \Rightarrow \psi$.
- Jos $\varphi \Leftrightarrow \psi$, niin $\psi \Rightarrow \varphi$.
- Jos $\varphi \Rightarrow \psi$ ja $\psi \Rightarrow \varphi$, niin $\varphi \Leftrightarrow \psi$.

Tämän voi ilmaista tiiviisti näin:

$$\varphi \Leftrightarrow \psi \text{ jos ja vain jos sekä } \varphi \Rightarrow \psi \text{ että } \varphi \Leftarrow \psi. \qquad [32]$$

Todistus. Ensin oletamme $\varphi \Leftrightarrow \psi$, ja todistamme sekä $\varphi \Rightarrow \psi$ että $\psi \Rightarrow \varphi$. Tarkastelemme mielivaltaista mahdollista tilannetta, jossa φ on tosi. Oletuksen $\varphi \Leftrightarrow \psi$ ja [22]:n mukaan myös ψ on siinä tosi. Niinpä [19] toteutuu, joten $\varphi \Rightarrow \psi$. Sitten tarkastelemme mielivaltaista mahdollista tilannetta, jossa ψ on tosi. Oletuksen $\varphi \Leftrightarrow \psi$ ja [22]:n mukaan myös φ on siinä tosi. Niinpä [19] toteutuu, joten $\psi \Rightarrow \varphi$.

Sitten oletamme sekä $\varphi \Rightarrow \psi$ että $\psi \Rightarrow \varphi$, ja todistamme $\varphi \Leftrightarrow \psi$. Tarkastelemme mielivaltaista mahdollista tilannetta, jossa φ on tosi tai ψ on tosi. Jos φ on siinä tosi, niin oletuksen $\varphi \Rightarrow \psi$ ja [19]:n mukaan myös ψ on siinä tosi. Jos ψ on siinä tosi, niin oletuksen $\psi \Rightarrow \varphi$ ja [19]:n mukaan myös φ on siinä tosi. Niinpä [22] toteutuu, joten $\varphi \Leftrightarrow \psi$. □

Juuri läpikäymämme todistus on kirjoitettu enimmäkseen sanallisesti. Yksi syy siihen on se, että olemme esitelleet vasta propositiologiikkaa ja hieman koulumatematiikan logiikkaa. Siksi meillä ei vielä ole käsitteitä eikä merkintöjä, joilla voisimme formalisoida ne asiat, joihin todistuksessa viitattiin ilmauksilla ”mielivaltainen mahdollinen tilanne” ja ”on siinä tosi”. Tämä ei kuitenkaan ole tärkein syy.

Sittenkään kun tarvittavat käsitteet on saatu, ei kaikkea kannata formalisoida, koska monessa tapauksessa formalisointi johtaisi pitkään, kömpelöön ja vaikeatajuiseen ilmaukseen asialle, jonka voi sanoa lyhyesti, ymmärrettävästi ja riittävän täsmällisesti luonnollisella kielellä. Esimerkiksi lauseen [11] ilmaus ”φ ja ψ eivät sisällä muita konnektiiveja kuin $\neg$, $\land$ ja $\lor$” on selvä ja täsmällinen, kun kaavojen rakenne on tuttu. Saman ilmaiseminen merkkijonojen teorian merkinnöin johtaisi pitkään kaavaan. Tästä syystä matematiikassa on tavallista esittää asiat ei täysin formaalisti, vaan formaalien merkintöjen ja luonnollisen kielen yhdistelmällä. Tämä pätee myös matemaattiseen logiikkaan.

Lisäksi logiikkaa koskevien määritelmien ja päättelyjen formalisointiin liittyy erityinen vaikeus, joka tunnetaan englanniksi nimellä *use–mention distinction*. Kun käytämme logiikan merkintöjä esittämään vaikka koulumatematiikan yhtälöiden ratkaisemista, esimerkiksi $2(x+1)-x=6 \Leftrightarrow 2x+2-x=6 \Leftrightarrow x+2=6 \Leftrightarrow x=4$, niin kaavat puhuvat luvuista, lukujen laskutoimituksista ja lukujen välisistä suhteista. Kun puheenaiheena onkin logiikka itse, kaavojen pitäisi puhua kaavoista ja päättelysäännöistä. Silloin on vaikeaa erottaa, milloin jokin symboli on puheen kohteena ja milloin sitä käytetään puhumiseen. Tämä on samankaltainen ongelma kuin seuraavissa esimerkeissä:

(9) Välimerkkejä ovat muun muassa !, ?, ,, ja ..

(10) Välimerkkejä ovat muun muassa ”!”, ”?”, ”,”, ja ”.”.

(11) Lainausmerkki on ”””.

Kohdan (9) ensimmäinen . on puheen kohteena ja toinen . on virkkeen loppuun normaalisti kuuluva piste. Tämä ei kuitenkaan ole ensi näkemältä selvää, vaan .. näyttää pikemminkin painovirheeltä. Tämä ongelma on vältetty (10):ssa pistämällä puheen kohteena olevat välimerkit lainausmerkkeihin. Ikävä kyllä siitä aiheutuu uusi ongelma, kuten (11) havainnollistaa. Tulemme käsittelemään sitä luvussa 7.

Niinpä logiikan symbolien käyttöönoton tarkoituksena ei olekaan, että lopulta formalisoisimme päättelyt täysin. Tarkoituksena on tarjota merkinnät, joilla voi kertoa lyhyesti ja täsmällisesti, minkälainen päättely on pätevää. Käytännön päättelyissä niitä käytetään toisinaan sellaisinaan, mutta usein niiden sijaan käytetään luonnollisen kielen ilmauksia kuten ”jos ja vain jos”. Tarkoituksena on, että silloinkin kun käytetään luonnollisen kielen ilmauksia, lukija (ja kirjoittaja) ymmärtävät ne siten kuin mitä vastaavat logiikan merkinnät tarkoittavat.

Kun edetään kaavojen ja päättelysääntöjen formalisoinnista päättelysääntöjen päteväksi todistamiseen, niin ongelmaksi nousee, mitä päättelykeinoja saa alun perin käyttää. Jos mitään päättelykeinoa ei saa käyttää ennen kuin se itse on todistettu oikeaksi, niin ei päästä alkuun, koska ei ole mitään, johon ensimmäinen todistus saisi vedota. Siksi on pakko hyväksyä joitakin päättelykeinoja ilman muuta perustetta kuin että ne tuntuvat oikeilta tai ne tuntuvat vastaavan luonnollisen kielen sanojen merkitystä.

Vaarana on, että vahingossa hyväksytään jotakin, joka ei olekaan ihan aina oikein. Tämä riski toteutui Gottlob Fregen (1848–1925) kohdalla. Hänen panoksensa logiikan kehitykseen on ollut valtava: predikaattilogiikka perustuu suurelta osin hänen ajatuksiinsa. Hänen järjestelmässään oli kuitenkin sisäinen ristiriita. Bertrand Russell huomasi sen ja kirjoitti siitä Fregelle vuonna 1902. Fregen uuden teoksen ”Aritmetiikan peruslait” (Grundgesetze der Arithmetik) osa 2 oli juuri silloin menossa painoon. Frege lisäsi kirjaansa hätäisesti kirjoitetun liitteen, jossa hän kuvaa ristiriidan ja esittää siihen korjauksen (joka huomattin myöhemmin kelvottomaksi). Liite alkaa näin:

> Tuskin mitään onnettomampaa voi kohdata tieteellistä kirjoittajaa kuin että yhtä hänen ajatusrakennelmansa perustaa horjutetaan sen jälkeen kun työ on valmis. Tähän tilanteeseen minut saattoi herra Bertrand Russellin kirje, juuri kun tämän osan painaminen oli valmistumaisillaan.

Mitä vähemmän hyväksytään ilman todistusta, sitä pienempi on riski, että järjestelmään jää piilevä virhe. Tulemme huomaamaan luvussa 6, että aika köyhä ”ensimmäisten päättelykeinojen” kokoelma riittää.

Tulemme myös toistuvasti huomaamaan, että formaaleilla päättelyjärjestelmillä on taipumus olla kömpelöitä. Esimerkiksi tuloksen $x+1-x=1$ johtaminen vaatii viisi askelta: $x+1-x=(x+1)+(-x)=(1+x)+(-x)=1+(x+(-x))=1+0=1$, sekä vielä lopuksi erillisen askeleen, jossa todetaan, että koska $x+1-x=\ldots=1$, pätee $x+1-x=1$. Köyhillä päättelyjärjestelmillä on taipumus olla aivan erityisen kömpelöitä. Siksi logiikan soveltamisessa ei ole eduksi saada ”ensimmäisten päättelysääntöjen” kokoelmasta mahdollisimman pieni. Parempi tavoite on saada riittävä kokoelma päättelykeinoja, joka on mahdollisimman helppo käyttää ja muistaa.

Edellä esitetyn [32]:n todistuksen ja monen muun todistuksen tehtävä tässä kirjassa ei ole olla osa täydellisesti rakennettua logiikan järjestelmää. Yksi niiden tehtävä on esimerkkinä toimimalla opettaa todistamiseen liittyviä käsitteitä ja todistamisessa käytettäviä ajatuskulkuja. Toinen tehtävä on tehdä näkyväksi asiaan liittyviä kiemuroita, jotka saattaisivat muuten jäädä huomaamatta. Esimerkiksi [32]:n todistuksemme nostaa esiin sitä, että kaavalla ei tyypillisesti ole yhtä totuusarvoa, vaan sillä on totuusarvo erikseen jokaisessa mahdollisessa tilanteessa.

Lisäksi todistukset auttavat kokonaiskuvan muodostamista paljastamalla asioiden välisiä yhteyksiä. Tulemme esimerkiksi huomaamaan, että kaikki $=$:n ominaisuudet nousevat kahdesta yksinkertaisesta periaatteesta: lausekkeen tuottama arvo on aina itsensä kanssa yhtäsuuri (siis esimerkiksi aina $3x+5=3x+5$); ja lausekkeen saa aina korvata lausekkeella, joka tuottaa jokaisessa mahdollisessa tilanteessa saman arvon kuin alkuperäinen lauseke (esimerkiksi koska $x+1-x=1$, pätee $2(x+1-x)+y<2y\vee y=x+1-x \Leftrightarrow 2\cdot 1+y<2y\vee y=1$).

Toisinaan todistuksen suurpiirteinenkin muistaminen voi auttaa saamaan oikein yksityiskohtia, jotka ovat vaikeita muistaa. Aiemmin todistimme lauseen, joka kertoo, miten mistä tahansa propositiologiikan laista, jossa on vain tiettyjä symboleita, saa toisen lain vaihtamalla symboleita tietyllä tavalla toisikseen. Jollet enää muista, mitä symboleita laissa saa esiintyä ja mikä vaihdetaan mihinkin, niin pystyt ehkä päättelemään jotakin siitä, että se todistettiin De Morganin lakien avulla.

Kyseessä on lause [11]. Se muistuttaa paljon apulausetta [10], mutta vain jälkimmäisessä on ehto että kukin P vaihdetaan $(\neg P)$:ksi ja päinvastoin. On helppo osoittaa todistusta katsomattakin, että jos tämä ehto poistetaan, niin [10] lakkaa olemasta pätevä. Osoita se! 96

Mutta miksi ehtoa ei tarvita lauseessa [11]? 97

Merkinnän venyttäminen (*abuse of notation*) tarkoittaa matematiikassa jonkin merkinnän käyttöä tavalla, joka on vastoin sääntöjä, mutta silti auttaa asian ymmärtämistä paremmin kuin sääntöjen mukainen tapa, ainakin jos lukijaa varoitetaan että kyseessä on venytetty merkintä. Kuten edellä todettiin, tiukasti sääntöjen mukainen merkintä saattaa olla pitkä, kömpelö ja vaikeatajuinen, vaikka itse asia olisi melko yksinkertainen. Venytetty merkintä saattaa tällöin olla huomattavasti lyhyempi ja yksinkertaisempi. Venyttämällä merkintää voimme ilmaista [32]:n näin:

$$(\varphi \Leftrightarrow \psi) \Leftrightarrow (\varphi \Rightarrow \psi) \wedge (\varphi \Leftarrow \psi)$$

Ilmaise [24] merkintää venyttämällä pelkillä symboleilla! 98

Ilmaise [25] merkintää venyttämällä pelkillä symboleilla! 99

Analysoimme nyt [32]:n äskeisen todistuksen siltä osin kuin se käyttää propositiologiikkaa. Todistimme ensin propositiologiikan ylittävillä keinoilla, että jos $\varphi \Leftrightarrow \psi$, niin $\varphi \Rightarrow \psi$. Todistetun asian voi ilmaista merkintöjä venyttämällä näin:

(12) $(\varphi \Leftrightarrow \psi) \Rightarrow (\varphi \Rightarrow \psi)$

Sitten todistimme propositiologiikan ylittävillä keinoilla, että jos $\varphi \Leftrightarrow \psi$, niin $\psi \Rightarrow \varphi$:

(13) $(\varphi \Leftrightarrow \psi) \Rightarrow (\psi \Rightarrow \varphi)$

Seuraavaksi sovelsimme periaatetta, jota emme ole vielä esitelleet:

$$\text{Jos } \chi_1 \Rightarrow \chi_2 \text{ ja } \chi_1 \Rightarrow \chi_3, \text{ niin } \chi_1 \Rightarrow \chi_2 \wedge \chi_3.$$

Siten saimme

(14) $(\varphi \Leftrightarrow \psi) \Rightarrow (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$

Mitkä olivat χ_1:n, χ_2:n ja χ_3:n tilalla? Mistä saatiin jos-osassa ilmaistut oletukset? 100

Seuraavaksi todistimme propositiologiikan ylittävillä keinoilla, että jos $\varphi \Rightarrow \psi$ ja $\psi \Rightarrow \varphi$, niin $\varphi \Leftrightarrow \psi$. Tämänkin voi ilmaista merkintöjä venyttämällä:

(15) $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi) \Rightarrow (\varphi \Leftrightarrow \psi)$

Lopuksi soveltamalla periaatetta "jos $\chi_1 \Rightarrow \chi_2$ ja $\chi_2 \Rightarrow \chi_1$, niin $\chi_1 \Leftrightarrow \chi_2$" saimme tavoitteemme $(\varphi \Leftrightarrow \psi) \Leftrightarrow (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$. Mikä nyt oli χ_1:n tilalla ja mikä χ_2:n? Mistä saatiin jos-osassa ilmaistut oletukset? 101

Periaate "jos $\chi_1 \Rightarrow \chi_2$ ja $\chi_2 \Rightarrow \chi_1$, niin $\chi_1 \Leftrightarrow \chi_2$" on muuten kuten (15), mutta (15):n φ ja ψ edustavat kaavoja, kun χ_1 ja χ_2 edustavat päättelysäännöistä merkintöjä venyttämällä muodostettuja kaavojen kaltaisia ilmauksia. Myöskään kun johdimme (14):n, χ_1, χ_2 ja χ_3 eivät edustaneet kaavoja vaan päättelysääntöjä. Nämä johtuvat siitä, että, kuten edellä todettiin, on eri asia soveltaa logiikkaa vaikka koulumatematiikkaan kuin soveltaa logiikkaa logiikkaan. Mitkä (15):n symbolit olivat puheen kohteena, ja mitä käytettiin puhumiseen? 102

Palauttakaamme vielä mieleen, että merkintä, jossa $\Rightarrow$ tai $\Leftrightarrow$ esiintyy sulkeiden sisällä, on venytetty merkintä. Sitä saa käyttää vain jos asian ilmaiseminen täsmällisillä merkinnöillä tai luonnollisella kielellä on liian hankalaa tai epäselvää, ja silloin pitää kertoa, että nyt käytetään venytettyä merkintää. Muualla kirjallisuudessa $\Rightarrow$ ja $\Leftrightarrow$ saattavat esiintyä sulkeiden sisällä, mutta silloin ne lähes varmasti eivät tarkoita sitä mitä ne tarkoittavat tässä kirjassa, vaan sitä mitä $\rightarrow$ ja $\leftrightarrow$ tarkoittavat tässä kirjassa.

Seuraavaksi käsittelemme $\Rightarrow$:n lakeja. Tässä on kaksi helppoa. Niillä voi vaikka johtaa siitä, että "aurinko paistaa, linnut laulavat ja syön jäätelön", että "linnut laulavat":

$$\varphi \wedge \psi \;\Rightarrow\; \varphi \qquad\qquad \varphi \wedge \psi \;\Rightarrow\; \psi \qquad [33]$$

Tarkoittakoon A että aurinko paistaa, L että linnut laulavat ja J että syön jäätelön. Miten $A \wedge L \wedge J \Rightarrow L$ voidaan päätellä [33]:n laeilla? 103

Perimmäinen syy sille, että niistä ensimmäinen pätee, on se, että $\wedge$ on otettu käyttöön tarkoittamaan, että sen kummallakin puolella oleva kaava on tosi. Silloinhan sen vasemmalla puolella oleva kaava on tosi. Toki asian voi tarkastaa vaikka yrittämällä löytää vastaesimerkin. Millainen olisi vastaesimerkki päättelyaskeleelle $\varphi \wedge \psi \Rightarrow \varphi$, ja miksi sellaisia ei ole? 104

Sama syy pätee tietenkin myös $\wedge$:n oikealla puolella olevaan kaavaan. Siksi myös $\varphi \wedge \psi \Rightarrow \psi$ on laki.

Todista [7]:n ja muiden lakien avulla, että F:stä seuraa mikä tahansa määritelty kaava! Tämän tehtävän mallivastaus havainnollistaa omalta osaltaan sitä, että logiikkaa on 105
vaikea muuttaa siten, että mahdottomasta ei seuraisi mitä tahansa. Nimittäin sellainen muutos vaatisi jonkin mallivastauksessa käytetyn lain kumoamista, mutta jokainen niistä on vahvasti perusteltu.

Myös seuraava laki on ilmeinen sanan "ja" sekä symbolin $\wedge$ merkitysten vuoksi:

$$\text{Jos } \varphi \Rightarrow \psi \text{ ja } \varphi \Rightarrow \chi \text{, niin } \varphi \Rightarrow \psi \wedge \chi. \qquad [34]$$

Sen käytöstä propositiologiikassa saadaan esimerkki olettamalla, että "jos Pihtiputaan mummo on kesällä Rovaniemellä, niin hän ostaa poroleikkelettä" ja "jos Pihtiputaan mummo on kesällä Rovaniemellä, niin hän läiskii hyttysiä". Silloin laki tuottaa "jos Pihtiputaan mummo on kesällä Rovaniemellä, niin hän ostaa poroleikkelettä ja läiskii hyttysiä". Mitkä ovat φ, ψ ja χ Pihtiputaan mummon tapauksessa? 106

Myös seuraavat kaksi lakia ovat helpot:

$$\varphi \ \Rightarrow \ \varphi \vee \psi \qquad\qquad \psi \ \Rightarrow \ \varphi \vee \psi \qquad [35]$$

Niistä ensimmäinen perustelee seuraavan päättelyketjun toisen askeleen:

$$P \ \Leftrightarrow \ P \wedge P \ \Rightarrow \ (P \wedge P) \vee (P \wedge Q) \ \Leftrightarrow \ P \wedge (P \vee Q)$$

Siitä saadaan transitiivisuudella $P \Rightarrow P \wedge (P \vee Q)$. Toisaalta [33] tuottaa $P \wedge (P \vee Q) \Rightarrow$
P. Mitä nämä yhdessä perustelevat, ja miksi? 107

Tämän kaltainen päättely esitetään toisinaan tähän tyyliin:

$$P \ \Leftrightarrow \ P \wedge P \ \Rightarrow \ (P \wedge P) \vee (P \wedge Q) \ \Leftrightarrow \ P \wedge (P \vee Q) \ \Rightarrow \ P$$

Tämän päättelyketjun ensimmäisestä ja viimeisestä kaavasta saadaan $P \Rightarrow P$, joka ei yksinään kerro mitään kiinnostavaa. Mutta ideana onkin, että jos päättelyketjun ensimmäinen ja viimeinen kaava ovat samat eikä päättelyketjussa esiinny sekä $\Rightarrow$ että $\Leftarrow$, niin päättelyketjun kaikki kaavat ovat yhtäpitävät. Niinpä esimerkkimme esittää tiiviissä muodossa todistuksen sille, että $P \wedge (P \vee Q) \Leftrightarrow P$.

Toivottavasti osasit perustella esimerkin ensimmäisen ja kolmannen askeleen! Jollet osannut, niin kertaa [2] ja [5].

Todista sijoittamalla samaan propositiomuuttujaan F ja T, että $\leftrightarrow$ on transitiivinen! 108

Kenties muistat vielä Ilonan? Jos ruokana on hernekeittoa, niin hän ilahtuu. Jos hän onnistuu tentissä, niin hän ilahtuu. Seuraava laki sallii päätellä näistä, että jos ruokana on hernekeittoa tai Ilona onnistuu tentissä, niin hän ilahtuu:

$$\text{Jos } \varphi \Rightarrow \chi \text{ ja } \psi \Rightarrow \chi \text{, niin } \varphi \vee \psi \Rightarrow \chi. \qquad [36]$$

Jos $\varphi_1 \Rightarrow \psi$ ja $\varphi_2 \Rightarrow \psi$, niin [36] sallii päätellä $\varphi_1 \vee \varphi_2 \Rightarrow \psi$. Jos myös $\varphi_3 \Rightarrow \psi$, niin
[36] sallii päätellä $(\varphi_1 \vee \varphi_2) \vee \varphi_3 \Rightarrow \psi$. Mitkä tässä ovat [36]:n φ, ψ ja χ? Koska $\vee$ on 109
vasemmalle liitännäinen, se tarkoittaa samaa kuin $\varphi_1 \vee \varphi_2 \vee \varphi_3 \Rightarrow \psi$. Tätä jatkamalla näemme, että jos $\varphi_1 \Rightarrow \psi$ ja ... ja $\varphi_n \Rightarrow \psi$, niin $\varphi_1 \vee \cdots \vee \varphi_n \Rightarrow \psi$. Mitä arvoja n voi
saada tässä? 110

Vaikka yllä oleva todistus käyttää ilmausta "tätä jatkamalla", on se täysin riittävä. Mutta koska meidän on opeteltava laatimaan induktiotodistuksia matematiikassa tavallisen mallin mukaan, muotoilemme sen sellaiseksi. Malli koostuu kahdesta osasta.

Pohjatapauksessa (*base case*) väite todistetaan pienimmälle kokonaisluvulle, jolle väite väitetään. Se on yleensä 0 tai 1. *Induktioaskeleessa* (*induction step*) oletetaan, että väite pätee mielivaltaiselle vähintään niin suurelle kokonaisluvulle kuin pohjatapauksessa, ja todistetaan, että se pätee yhtä suuremmalle kokonaisluvulle. Usein niitä merkitään joko $n-1$ ja n taikka n ja $n+1$. Oletusta, että väite pätee pienemmälle näistä, kutsutaan usein *induktio-oletukseksi* (*induction assumption* tai *induction hypothesis*).

> **Lause.** Olkoon $n \geq 1$. Jos $\varphi_1 \Rightarrow \psi$ ja ... ja $\varphi_n \Rightarrow \psi$, niin $\varphi_1 \vee \cdots \vee \varphi_n \Rightarrow \psi$.
>
> *Todistus.* Käytämme induktiota.
>
> *Pohjatapaus.* Kun $n = 1$, sievenee väite muotoon ”jos $\varphi_1 \Rightarrow \psi$, niin $\varphi_1 \Rightarrow \psi$”. Se on itsestäänselvästi tosi.
>
> *Induktioaskel.* Kun $n > 1$, niin lauseen oletusten $\varphi_1 \Rightarrow \psi$ ja ... ja $\varphi_{n-1} \Rightarrow \psi$ sekä induktio-oletuksen mukaan $\varphi_1 \vee \cdots \vee \varphi_{n-1} \Rightarrow \psi$. Lauseen oletuksen mukaan $\varphi_n \Rightarrow \psi$. Näistä [36] tuottaa $(\varphi_1 \vee \cdots \vee \varphi_{n-1}) \vee \varphi_n \Rightarrow \psi$. Koska $\vee$ on vasemmalle liitännäinen, se tarkoittaa samaa kuin $\varphi_1 \vee \cdots \vee \varphi_n \Rightarrow \psi$. $\square$

Todista induktiolla ”jos $n \geq 1$ ja $\varphi \Rightarrow \psi_1$ ja ... ja $\varphi \Rightarrow \psi_n$, niin $\varphi \Rightarrow \psi_1 \wedge \cdots \wedge \psi_n$”! 111
Todista induktiolla ”jos $n \geq 1$ ja $\varphi_0 \Rightarrow \varphi_1 \Rightarrow \ldots \Rightarrow \varphi_n$, niin $\varphi_0 \Rightarrow \varphi_n$”! 112
Millä i:n arvoilla väite $\varphi(\psi_1, \ldots, \psi_n) \Leftrightarrow \varphi(\chi_1, \ldots, \chi_i, \psi_{i+1}, \ldots, \psi_n)$ on mielekäs?
Sievennä väite suurimmalla sellaisella i:n arvolla. Kun $n = 3$, niin sievennä väite jokai-
sella mielekkäällä i:n arvolla! Todista induktiolla ”jos $n \geq 0$, $\forall$ ja $\exists$ eivät esiinny φ:ssä, 113
ja $\psi_1 \Leftrightarrow \chi_1$ ja ... ja $\psi_n \Leftrightarrow \chi_n$, niin $\varphi(\psi_1, \ldots, \psi_n) \Leftrightarrow \varphi(\chi_1, \ldots, \chi_n)$”! 114

Tapauksiin jakaminen (*proof by cases*) on matematiikassa usein käytetty todistuskeino. Siinä tehdään ensin jokin tilapäinen oletus φ_1 ja sen vallitessa todistetaan haluttu asia. Sitten oletuksesta φ_1 luovutaan, tehdään uusi tilapäinen oletus φ_2 ja sen vallitessa todistetaan haluttu asia. Näin jatketaan kunnes tilapäiset oletukset $\varphi_1, \ldots, \varphi_n$ kattavat kaikki mahdolliset tilanteet, eli $\varphi_1 \vee \cdots \vee \varphi_n \Leftrightarrow \mathsf{T}$. Olemme käyttäneet tätä menetelmää useasti, sillä todistaminen sijoittamalla F ja T vuoron perään samaan propositiomuuttujaan on tapauksiin jakamista. Toinen esimerkki on sivulla 39: ”Mutta mikään atomikaava ei voi olla sellainen, koska ...” ”Symbolin X tilalle tuleva kaava ei voi olla sellainen, koska ...” ”Eikä mikään yhdistetty kaava $\varphi(X)$ voi olla sellainen, koska ...”

Tapauksiin jakaminen on vähintään ideatasolla, ja usein myös formaalilla tasolla, perusteltavissa [36]:lla. Esimerkiksi todistuskeino, jossa propositiomuuttujaan sijoitetaan vuoron perään F ja T voidaan perustella seuraavasti. Menetelmän palauttamiseksi mieliin kertaamme tämän alaluvun alussa olleen todistuksen:

- Jos $P \Leftrightarrow \mathsf{F}$, niin $P \wedge (\neg P \vee Q) \Leftrightarrow \mathsf{F} \wedge (\neg \mathsf{F} \vee Q) \Leftrightarrow \mathsf{F} \Leftrightarrow \mathsf{F} \wedge Q \Leftrightarrow P \wedge Q$.
- Jos $P \Leftrightarrow \mathsf{T}$, niin $P \wedge (\neg P \vee Q) \Leftrightarrow \mathsf{T} \wedge (\neg \mathsf{T} \vee Q) \Leftrightarrow \ldots \Leftrightarrow \mathsf{T} \wedge Q \Leftrightarrow P \wedge Q$.

Oletuksen $P \Leftrightarrow \mathsf{T}$ tekeminen tarkoittaa, että mahdollisiksi tilanteiksi asetetaan ne, jotka olivat alun perin mahdollisia ja joissa lisäksi P on tosi. Kun siitä johdetaan $\varphi \Leftrightarrow \psi$, niin [29]:n mukaan se on sama kuin että osoitetaan, että jokaisessa alun perin mahdollisessa tilanteessa, jossa P on tosi, pätee $\varphi \leftrightarrow \psi$. Se puolestaan tarkoittaa [19]:n mukaan, että alun perin pätee $P \Rightarrow \varphi \leftrightarrow \psi$. Vastaavasti yhtäpitävyyden $\varphi \Leftrightarrow \psi$ johtaminen oletuksesta $P \Leftrightarrow \mathsf{F}$ eli $\neg P \Leftrightarrow \mathsf{T}$ on sama kuin että osoitetaan, että alun perin pätee $\neg P \Rightarrow \varphi \leftrightarrow \psi$. Niistä [36] tuottaa $P \vee \neg P \Rightarrow \varphi \leftrightarrow \psi$. Koska $P \vee \neg P$ on tosi jokaisessa mahdollisessa tilanteessa, on lopputulos [19]:n ja [29]:n mukaan sama kuin $\varphi \Leftrightarrow \psi$.

Onko tapauksiin jakamisessa tapausten suljettava toisensa pois, eli onko oltava $\varphi_1 \wedge \varphi_2 \Leftrightarrow \mathsf{F}$, $\varphi_1 \wedge \varphi_3 \Leftrightarrow \mathsf{F}$, $\varphi_2 \wedge \varphi_3 \Leftrightarrow \mathsf{F}$ ja niin edelleen? Perustele vastauksesi, mutta perustelun ei tarvitse olla hieno! 115

Ristiriitatodistus (*proof by contradiction*) eli *reductio ad absurdum* tarkoittaa väitteen todistamista osoittamalla, että jos väite ei ole jossakin mahdollisessa tilanteessa tosi, niin joudutaan mahdottomuuteen. Kun käytössä on vain kaksi totuusarvoa F ja T, "ei tosi" tarkoittaa "epätosi". Tällöin ristiriitatodistuksen periaatteen voi ilmaista muodossa "jos $\neg\varphi \Rightarrow \mathsf{F}$, niin φ". Valitettavasti kolmas totuusarvo saattaa hiipiä mukaan melkein huomaamatta esimerkiksi nollalla jakamisen tai negatiivisen luvun neliöjuuren kautta, ja ristiriitatodistus on erityisen altis siitä aiheutuville päättelyvirheille. Siksi ilmaisemme sen seuraavasti:

Jos φ on määritelty ja jos $\neg\varphi \Rightarrow \mathsf{F}$, niin φ. [37]

Emme todista sitä, vaan otamme sen yhdeksi niistä "ensimmäisistä päättelykeinoista", jotka hyväksymme ilman todistusta. Ristiriitatodistuksen perusidea säilyy pätevänä kun käyttöön otetaan kolmas totuusarvo, mutta se täytyy muotoilla monimutkaisemmin. Se tehdään luvussa **??**.

Olemme käyttäneet tätä todistusmenetelmää muun muassa sivulla 39, kun perustelimme, miksi yhtäpitävyyttä saa käyttää propositiologiikan kaavan sisällä. Oletimme, että on olemassa kaava, jonka sisällä sitä ei saakaan käyttää. Päättelimme siitä, että on olemassa mahdollisimman pieni kaava, jonka sisällä ei saa käyttää yhtäpitävyyttä. Sitten osoitimme, että mikään kaava ei voi olla sellainen: jokainen kaava joko sallii yhtäpitävyyden käytön, tai ei ole mahdollisimman pieni joka kieltää sen.

Siitä, että määritelty kaava voi saada vain kaksi totuusarvoa F ja T, seuraa myös seuraava laki:

Jos ψ on määritelty ja jos $\neg\psi \Rightarrow \neg\varphi$, niin $\varphi \Rightarrow \psi$. [38]

Todistus. Tarkastelemme mielivaltaista mahdollista tilannetta, jossa φ on tosi (eli φ tuottaa T). Jos siinä tilanteessa ψ tuottaa F, niin $\neg\psi$ tuottaa T. Oletuksen $\neg\psi \Rightarrow \neg\varphi$ mukaan myös $\neg\varphi$ tuottaa T eli φ tuottaa F. Se on ristiriidassa lähtökohtamme kanssa. Niinpä ei voi olla niin, että ψ tuottaa F. Koska on vain kaksi totuusarvoa F ja T, ψ tuottaa T. Olemme osoittaneet että jokaisessa mahdollisessa tilanteessa, jossa φ on tosi, myös ψ on tosi. Niinpä [19]:n mukaan $\varphi \Rightarrow \psi$. $\square$

Tässä todistuksessa käytettiin [37]:n periaatetta niin, että φ:n tilalla ei ollut kaava vaan osittain sanallinen ilmaus. Mikä oli φ:n tilalla? 116

Tämäkin päättelyperiaate säilyy perusidealtaan pätevänä mutta joudutaan muotoilemaan uudelleen, jos käyttöön otetaan kolmas totuusarvo edustamaan määrittelemättömiä väitteitä.

Tuloksen $\varphi \Rightarrow \psi$ johtaminen tätä lakia hyödyntämällä on *käänteinen todistus* (*proof by contraposition*). *Epäsuora todistus* (*indirect proof*) on joko ristiriitatodistus tai käänteinen todistus.

Todista lakeja käyttämällä, että mistä tahansa määritellystä kaavasta seuraa T! 117

Olemme tähän saakka todistaneet lakeja tarkastelemalla jokaista mahdollista tilannetta erikseen. Käänteisen todistuksen menetelmä sallii vaihtaa näkökulmaa ja keskittyä vastaesimerkkeihin. Niin toimien ei tarvitse tarkastella kuin yhtä mahdollista tilannetta. Esimerkkinä tästä todistamme lain [26].

Todistus. Jos $\varphi \Rightarrow \chi$ ei päde, niin on olemassa mahdollinen tilanne, jossa $\varphi \Leftrightarrow \mathsf{T}$ ja $\chi \Leftrightarrow \mathsf{F}$. Jos siinä tilanteessa $\psi \Leftrightarrow \mathsf{F}$, niin $\varphi \Rightarrow \psi$ ei päde. Muussa tapauksessa siinä tilanteessa $\psi \Leftrightarrow \mathsf{T}$, joten $\psi \Rightarrow \chi$ ei päde. Kummassakaan tapauksessa [26]:n vasen puoli ei päde. Olemme osoittaneet, että jos [26]:n oikea puoli ei päde, niin myöskään vasen puoli ei päde. Niinpä käänteisen todistuksen periaatteen mukaan jos vasen puoli pätee, niin myös oikea puoli pätee. Se tarkoittaa, että [26] pätee. □

Todista [36] käänteisen todistuksen menetelmällä! 118

Päättelyimplikaation käyttäminen kaavan sisällä on paljon monimutkaisempi asia kuin yhtäpitävyyden käyttäminen kaavan sisällä. Ei ole läheskään aina niin, että jos $\psi \Rightarrow \chi$, niin $\varphi(\psi) \Rightarrow \varphi(\chi)$. Yksinkertaisin vastaesimerkki saadaan valitsemalla $\varphi(X)$:ksi $\neg X$, ψ:ksi F ja χ:ksi T. Silloin $\psi \Rightarrow \chi$ koska $\mathsf{F} \Rightarrow \mathsf{T}$, mutta ei $\varphi(\psi) \Rightarrow \varphi(\chi)$ koska $\neg\mathsf{F} \Rightarrow \neg\mathsf{T}$ tarkoittaa samaa kuin $\mathsf{T} \Rightarrow \mathsf{F}$, joka on väärin. Koulumatemaattinen versio tästä on esimerkiksi seuraava: vaikka $x \geq 5 \Rightarrow x \geq 3$ pätee, ei $\neg(x \geq 5) \Rightarrow \neg(x \geq 3)$ päde, koska se on sama kuin $x < 5 \Rightarrow x < 3$. Muun muassa 4 on sille vastaesimerkki.

Oikeita lakeja on kaksi. (Niissäkin $\forall$:a ja $\exists$:a saa käyttää, jos noudattaa sivulla 100 mainittua ehtoa.)

Jos ψ ja χ ovat yhtäaikaa määritellyt, $\psi \Rightarrow \chi$, $\varphi(X_1,\ldots,X_i,\ldots,X_n)$ on kasvava paikan i suhteen, eivätkä $\forall$ ja $\exists$ esiinny siinä, niin $\varphi(\psi_1,\ldots,\psi,\ldots,\psi_n) \Rightarrow \varphi(\psi_1,\ldots,\chi,\ldots,\psi_n)$. [39]

Jos ψ ja χ ovat yhtäaikaa määritellyt, $\psi \Rightarrow \chi$, $\varphi(X_1,\ldots,X_i,\ldots,X_n)$ on vähenevä paikan i suhteen, eivätkä $\forall$ ja $\exists$ esiinny siinä, niin $\varphi(\psi_1,\ldots,\chi,\ldots,\psi_n) \Rightarrow \varphi(\psi_1,\ldots,\psi,\ldots,\psi_n)$. [40]

Muistele, mitä tarkoittaa kasvavuus paikan i suhteen ja sitten tarkasta sivulta 24! Muistele, mitä tarkoittaa vähenevyys paikan i suhteen ja sitten tarkasta vastauksesta 41! Tarkasta molemmat käsitteet myös apulauseesta [18]! 119

Lain [39] voi todistaa seuraavasti. Koska $\psi_1, \ldots, \psi_{i-1}$ ja $\psi_{i+1}, \ldots, \psi_n$ ovat koko todistuksen ajan samat, ei niiden näyttäminen tuo lisäarvoa vaan vain häiritsee varsinaisen asian hahmottamista. Siksi jätämme ne pois. Tehtävämme on osoittaa $\varphi(\psi) \Rightarrow \varphi(\chi)$. Toisin sanoen, tehtävämme on osoittaa, että jokaisessa mahdollisessa tilanteessa, jossa $\varphi(\psi)$ tuottaa T, myös $\varphi(\chi)$ tuottaa T. Todistuksen aikana saamme hyödyntää kahta oletusta: $\varphi(X_i)$ on kasvava paikan i suhteen, ja $\psi \Rightarrow \chi$.

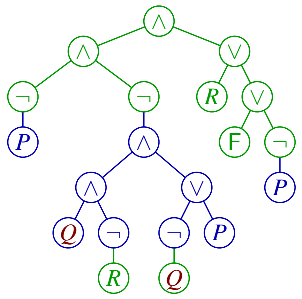
Todistus [39]:lle. Tarkastelemme mielivaltaista mahdollista tilannetta, jossa $\varphi(\psi)$ tuottaa T.

- Jos siinä tilanteessa ψ tuottaa saman totuusarvon kuin χ, niin myös $\varphi(\psi)$ tuottaa saman totuusarvon kuin $\varphi(\chi)$. Niinpä $\varphi(\chi)$ tuottaa T.
- Jos ψ tuottaa F ja χ tuottaa T, niin kasvavuuden paikan i suhteen vuoksi $\varphi(\psi) \rightarrow \varphi(\chi)$. Siitä seuraa, että $\varphi(\chi)$ tuottaa T, koska alussa tehdyn oletuksen vuoksi $\varphi(\psi)$ tuottaa tilanteessamme T.
- Muussa tapauksessa ψ tuottaa T ja χ tuottaa F. Se ei kuitenkaan ole mahdollista oletuksen $\psi \Rightarrow \chi$ vuoksi.

Niinpä jokaisessa mahdollisessa tilanteessa, joka toteuttaa oletuksen $\psi \Rightarrow \chi$ ja jossa $\varphi(\psi)$ tuottaa T, myös $\varphi(\chi)$ tuottaa T. Toisin sanoen, [39]:n oletusten vallitessa $\varphi(\psi) \Rightarrow \varphi(\chi)$. □

Todista [40]! 120

Lain [39] hyödyntämiseksi tarvitaan keino olla varma, että kaavan esittämä totuusfunktio on kasvava paikan i suhteen. Vastaava pätee laille [40] ja vähenevyydelle. Niihin on keino, joka ei toimi aina, mutta toimii niin usein että siitä on hyötyä:



Kuva 20: Lausekepuu, joka näyttää parillisen ja parittoman määrän ¬:tä alaisuudessa olevat kaavan $(\neg P \wedge \neg((Q \wedge \neg R) \wedge (\neg Q \vee P))) \wedge (R \vee (\mathsf{F} \vee \neg P))$ osat; Q on molempia

Apulause. Jos jokainen X_i:n esiintymä kaavassa $\varphi(X_1, \ldots, X_i, \ldots, X_n)$ on parillisen määrän ¬:tä alaisuudessa, missä ¬:ksi katsotaan myös $\rightarrow$ vasemman argumenttinsa osalta, eikä se ole muiden konnektiivien kuin ¬, ∧, ∨ ja $\rightarrow$ alaisuudessa, niin $\varphi(X_1, \ldots, X_i, \ldots, X_n)$:n esittämä totuusfunktio on kasvava paikan i suhteen. Jos määrä onkin pariton, niin totuusfunktio on vähenevä paikan i suhteen. [41]

Tämän lain ilmaisema ehto on riittävä mutta ei välttämätön. Esimerkiksi $X \leftrightarrow \top$ on kasvava X:n suhteen, vaikka X onkin siinä $\leftrightarrow$:n alaisuudessa. Kuvassa 20 lausekepuuna esitetyn kaavan esittämä totuusfunktio on kasvava R:n suhteen, koska kaikki R:n esiintymät ovat parillisen määrän ¬:tä alaisuudessa. Kaikki P:n esiintymät ovat parittoman määrän ¬:tä alaisuudessa, joten totuusfunktio on vähenevä P:n suhteen. Koska Q esiintyy sekä parillisen että parittoman määrän ¬:tä alaisuudessa, ei [41]:n perusteella voi sanoa, onko totuusfunktio kasvava tai vähenevä Q:n suhteen. Onko se? Onko se kasvava P:n suhteen? Onko se vähenevä R:n suhteen? 121

Apulause [41] seuraa kuvasta 13, apulauseista [13] ja [14] sekä [16]:sta. Sen voisi todistaa rakenteellisella induktiolla, mutta eiköhän sen pätevyys ole selvä ilmankin.

Kuten [28], [39] ja [40] sanovat, pätevää yhtäpitävyyttä saa soveltaa kaavan sisällä vapaasti, mutta pätevää päättelyimplikaatiota vain rajoitetusti. (Jos käyttää ∀:a tai ∃:a, niin on noudatettava sivulla 100 mainittua ehtoa.) Yhtäpitävyyden soveltaminen kaavan sisällä on usein paljon näppärämpää kuin muut keinot. Siksi $\Leftrightarrow$-lait kannattaa opiskella nimenomaan $\Leftrightarrow$-lakeina, vaikka jokaisen niistä saisikin [32]:n mukaisesti kahtena $\Rightarrow$-lakina. Yksi syy, miksi luvussa 6 esitettävä ja monet muut köyhät formaalit päättelyjärjestelmät ovat aivan erityisen kömpelöitä on se, että niistä puuttuu lupa soveltaa yhtäpitävyyttä kaavan sisällä.

Toisaalta $\Rightarrow$-lakejakin tarvitaan käytännössä. Siihen on kaksi syytä. Ensiksi, jos tarvitsee todistaa $\varphi \Rightarrow \psi$ jolle vastakkainen suunta $\varphi \Leftarrow \psi$ ei päde, niin se ei onnistu päättelyketjulla, joka ei sisällä muita päättelyoperaattoreita kuin $\Leftrightarrow$. Näin on, koska päättelyketju $\varphi_0 \Leftrightarrow \ldots \Leftrightarrow \varphi_n$ todistaa $\varphi_0 \Leftrightarrow \varphi_n$, siis sekä $\varphi_0 \Rightarrow \varphi_n$ että $\varphi_0 \Leftarrow \varphi_n$. Toiseksi, vaikka yksittäiset päättelyaskeleet onnistuvat usein näppärästi $\Leftrightarrow$-laeilla, on tavallista, että isojen $\Leftrightarrow$-muotoisten lauseiden $\Rightarrow$-suunnan todistus kulkee aivan eri reittejä kuin $\Leftarrow$-suunnan todistus. Silloin $\Leftrightarrow$-laki joudutaan todistamaan käyttäen $\Rightarrow$-lakeja. Tästä tulee myöhemmin esimerkkejä.

Tämän alaluvun lopuksi vertaamme lyhyesti tämän kirjan päättelyoperaattoreita muualla esiintyviin samankaltaisiin.

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

Kuva 21: Ote kirjan Matemaattinen logiikka sivulta 52

Kirjassa Jouko Väänänen: Matemaattinen logiikka, 29.10.2013 on useita kuvan 21 kaltaisia päättelyketjuja. Siinä Σ on tietyt ehdot täyttävä joukko kaavoja ja M on kohde, josta kaavat puhuvat. Ilmaus $M \models \varphi$ tarkoittaa, että φ on tosi M:ssä, ja $\Sigma \vdash \varphi$ tarkoittaa, että jos Σ:n sisältämät kaavat oletetaan tosiksi, niin φ voidaan todistaa. Esimerkki on peräisin induktiotodistuksesta, joka osoittaa jokaisesta kaavasta, että se on tosi M:ssä jos ja vain jos se on todistettavissa Σ:sta.

Tämän kirjan kannalta olennaista on vain, että siinä esitetään päättelyketju, jossa $\iff$:lla toisiinsa verrattavat osat eivät ole logiikan kaavoja vaan kaavoista, niiden voimassa olemisesta ja niiden todistamisesta puhuvia ilmauksia, joissa esiintyy jopa luonnollisen kielen sana ”tai”. Symbolia $\iff$ ei kirjassa esitellä, vaan se oletetaan entuudestaan tutuksi. Materiaalisen ekvivalenssin symbolina kirjassa on $\leftrightarrow$.

Kirjan Gary MacGillivray: ”Notes for Math 122, Logic and Foundations” sivulla 15 määritellään ”We use the notation $s_1 \Leftrightarrow s_2$ to denote the fact (theorem) that $s_1 \leftrightarrow s_2$ is a tautology, that is, that s_1 and s_2 are logically equivalent. Notice that $s_1 \leftrightarrow s_2$ is a statement and can in general be true or false, and $s_1 \Leftrightarrow s_2$ indicates the (higher level) fact that s_1 and s_2 always have the same truth value as each other.” Sivulla 26 on hyvin samanlainen määritelmä $\Rightarrow$:lle $\to$:n avulla. Määritelmät ovat samankaltaiset kuin tässä kirjassa, mutta ilmauksen ”jokaisessa mahdollisessa tilanteessa” tilalla on ”always”, ja tämän kirjan määritelmät toimivat myös kolmiarvoisessa logiikassa. (MacGillivray:n käsitteet ”tautology” ja ”logically equivalent” eivät ole samat kuin formaalin logiikan tautologia ja loogisesti ekvivalentti, vaan vastaavat tämän kirjan käsitettä ”laki”.)

Kuvassa 22 on johdettu [30]:n alin laki päättelyketjuna propositiologiikan lakien avulla. Ensimmäinen $\Leftrightarrow$ saadaan [30]:n keskimmäisellä lailla. Jokaiselle muulle $\Leftrightarrow$, jos siinä käytetty laki ei ollut tuttu, niin opettele se nyt! 122

Kuvassa 23 on esimerkki $\Rightarrow$:n ja $\to$:n käytöstä. Ylärivi ilmaisee sen tosiasian, että jokaisessa tilanteessa, jossa sekä $p \to q$ että p on tosi, myös q on tosi. Sen että tämä pätee näkee esimerkiksi siitä, että sijoituksella $p \Leftrightarrow \mathsf{F}$ vasemmasta puolesta tulee epätosi; ja sijoituksella $p \Leftrightarrow \mathsf{T}$ vasemmasta puolesta tulee sama kuin oikeasta, koska [16]:lla saadaan $(\mathsf{T} \to q) \land \mathsf{T} \Leftrightarrow \neg\mathsf{T} \lor q \Leftrightarrow q$.

Jos kuvan 23 alarivi ei ole pätevä, niin jossakin tilanteessa $p \to r$ ei ole tosi, mutta $(p \to q) \land (q \to r)$ on tosi eli sekä $p \to q$ että $q \to r$ on tosi. Koska $p \to r$ ei ole tosi, on p tosi mutta r ei ole. Koska sekä p että $p \to q$ ovat tosi, on ylärivin mukaan q tosi. Koska sekä q että $q \to r$ ovat tosi, on ylärivin mukaan r tosi. Niinpä r sekä ei ole että on

$$
\begin{aligned}
&p \leftrightarrow q \\
&\quad \Leftrightarrow \quad (\neg p \lor q) \land (p \lor \neg q) && \text{Known L.E.} \\
&\quad \Leftrightarrow \quad (\neg p \land (p \lor \neg q)) \lor (q \land (p \lor \neg q)) && \text{Distributive} \\
&\quad \Leftrightarrow \quad [(\neg p \land p) \lor (\neg p \land \neg q)] \lor [(q \land p) \lor (q \land \neg q)] && \text{Distributive (twice)} \\
&\quad \Leftrightarrow \quad [\mathbf{0} \lor (\neg p \land \neg q)] \lor [(q \land p) \lor \mathbf{0}] && \text{Known contradictions} \\
&\quad \Leftrightarrow \quad (\neg p \land \neg q) \lor (q \land p) && \text{Identity} \\
&\quad \Leftrightarrow \quad (p \land q) \lor (\neg p \land \neg q) && \text{Commutative } (2\times)
\end{aligned}
$$

Kuva 22: Ote kirjan Notes for Math 122, Logic and Foundations sivulta 21

- Modus Ponens: $(p \to q) \wedge p \Rightarrow q$
- Chain Rule (Law of Syllogism): $(p \to q) \wedge (q \to r) \Rightarrow p \to r$

Kuva 23: Ote kirjan Notes for Math 122, Logic and Foundations sivulta 28

tosi. Oletus, että alarivi ei ole pätevä, on johtanut ristiriitaan. Siksi alarivikin on pätevä.

2.5 Propositiologiikka jämptisti ja BNF ohimennen

Koska tähänastisissa alaluvuissa on ollut sikinsokin propositiologiikkaa ja matematiikan yleisiä periaatteita, ei niistä ehkä ole muodostunut selvärajaista kokonaiskuvaa propositiologiikasta. Tässä alaluvussa korjataan tämä puute määrittelemällä propositiologiikan keskeiset käsitteet lyhyesti ja täsmällisesti. Tämä alaluku on suurelta osin aiemman kertausta, mutta osittain uudesta näkökulmasta; ja jonkin verran tulee myös uusia asioita.

Propositiologiikan kaavoissa voi esiintyä vain seuraavia symboleita:

- totuusarvovakiot F ja T
- propositiomuuttujat
- konnektiivit $\wedge$, $\vee$, $\neg$, $\to$ ja $\leftrightarrow$
- sulkeet (ja).

Propositiomuuttuja on kursivoitu iso kirjain, jossa mahdollisesti on oikeassa ylänurkassa $'$ ja mahdollisesti on oikeassa alanurkassa luonnollinen luku. Esimerkkejä ovat P, Q, P' ja P_1. Propositiomuuttujat F ja T erottaa totuusarvovakioista F ja T erilaisen kirjoitusasun ansiosta.

Propositiologiikan kaavat on määritelty kuvassa 24. Siinä käytetty tapa määritellä symbolien jonojen joukkoja tunnetaan nimellä *Backus–Naur form* ja lyhenteellä *BNF*. Kukin ”::=”:n edessä oleva sana on *välisymboli* (*non-terminal symbol*). Kukin välisymboli tuottaa nolla tai useampia symbolien jonoja seuraavasti.

Ensin valitaan ”::=”:n perästä jokin vaihtoehto. Vaihtoehdot on erotettu toisistaan ”|”:lla. Välisymbolin *Kaava* tapauksessa valittavana on vain yksi vaihtoehto, nimittäin *EkvKaava*. Välisymbolin *NegKaava* tapauksessa vaihtoehtoja on kolme, nimittäin *Peruskaava*, (*Kaava*) ja $\neg$*NegKaava*.

$$
\begin{array}{rcl}
\mathit{Kaava} & ::= & \mathit{EkvKaava} \\
\mathit{EkvKaava} & ::= & \mathit{ImplKaava} \mid \mathit{EkvKaava} \leftrightarrow \mathit{ImplKaava} \\
\mathit{ImplKaava} & ::= & \mathit{DisjKaava} \mid \mathit{DisjKaava} \to \mathit{ImplKaava} \\
\mathit{DisjKaava} & ::= & \mathit{KonjKaava} \mid \mathit{DisjKaava} \vee \mathit{KonjKaava} \\
\mathit{KonjKaava} & ::= & \mathit{NegKaava} \mid \mathit{KonjKaava} \wedge \mathit{NegKaava} \\
\mathit{NegKaava} & ::= & \mathit{Peruskaava} \mid (\mathit{Kaava}) \mid \neg \mathit{NegKaava} \\
\mathit{Peruskaava} & ::= & \mathsf{F} \mid \mathsf{T} \mid \mathit{Propositiomuuttuja} \\
\mathit{Atomikaava} & ::= & \mathit{Peruskaava} \mid (\mathit{Atomikaava})
\end{array}
$$

Kuva 24: Propositiologiikan syntaksi

rivi	välisymboli	vaihtoehdolla	riveiltä	tuottaa
1	*Peruskaava*	T		T
2	*NegKaava*	*Peruskaava*	1	T
3	*KonjKaava*	*NegKaava*	2	T
4	*Peruskaava*	*Propositiomuuttuja*		P
5	*NegKaava*	*Peruskaava*	4	P
6	*NegKaava*	$\neg$*NegKaava*	5	$\neg P$
7	*KonjKaava*	*KonjKaava* $\wedge$ *NegKaava*	3, 6	$\mathsf{T} \wedge \neg P$
8	*DisjKaava*	*KonjKaava*	7	$\mathsf{T} \wedge \neg P$
9	*ImplKaava*	*DisjKaava*	8	$\mathsf{T} \wedge \neg P$
10	*EkvKaava*	*ImplKaava*	9	$\mathsf{T} \wedge \neg P$
11	*Kaava*	*EkvKaava*	10	$\mathsf{T} \wedge \neg P$
12	*NegKaava*	(*Kaava*)	11	$(\mathsf{T} \wedge \neg P)$
13	*NegKaava*	$\neg$*NegKaava*	12	$\neg(\mathsf{T} \wedge \neg P)$
14	*KonjKaava*	*NegKaava*	13	$\neg(\mathsf{T} \wedge \neg P)$
15	*DisjKaava*	*KonjKaava*	14	$\neg(\mathsf{T} \wedge \neg P)$
16	*ImplKaava*	*DisjKaava*	15	$\neg(\mathsf{T} \wedge \neg P)$
17	*EkvKaava*	*ImplKaava*	16	$\neg(\mathsf{T} \wedge \neg P)$
18	*Kaava*	*EkvKaava*	17	$\neg(\mathsf{T} \wedge \neg P)$

Kuva 25: Kaavan $\neg(\mathsf{T} \wedge \neg P)$ tuottaminen kuvan 24 BNF-määritelmästä

Vaihtoehdosta tuotetaan symbolien jono etenemällä vasemmalta oikealle. Kunkin välisymbolin kohdalla valitaan jokin sen tuottama symbolien jono — ihan mikä tahansa. Kukin *loppusymboli* (*terminal symbol*) eli $\leftrightarrow$, $\rightarrow$, $\vee$, $\wedge$, $\neg$, (,), F, T tai propositiomuuttuja otetaan mukaan sellaisenaan. Näin saadut symbolien jonot ja loppusymbolit laitetaan peräkkäin.

Esimerkiksi kaava $\neg(\mathsf{T} \wedge \neg P)$ voidaan tuottaa vaiheittain kuten kuvassa 25. Rivillä 1 todetaan, että T on yksi *Peruskaava*n vaihtoehdoista. Koska se ei sisällä välisymboleita, se tuotetaan sellaisenaan. Rivillä 2 todetaan, että *Peruskaava* on yksi *NegKaava*n vaihtoehdoista. Sen kohdalla voidaan valita T, koska rivillä 1 todettiin, että *Peruskaava* tuottaa T:n. Koska *NegKaava* on yksi *KonjKaava*n vaihtoehdoista ja tuottaa T:n, myös *KonjKaava* tuottaa T:n. Rivit 4 ja 5 toimivat samaan tyyliin. Rivillä 6 käytetään *NegKaava*n vaihtoehtoa $\neg$*NegKaava* siten, että $\neg$ otetaan sellaisenaan (koska se on loppusymboli) ja *NegKaava*n kohdalla otetaan sen rivillä 5 tuottama P. Rivillä 7 otetaan *KonjKaava*n kohdalla sen rivillä 3 tuottama T, sitten otetaan $\wedge$ sellaisenaan, ja lopuksi *NegKaava*n kohdalla otetaan sen rivillä 6 tuottama $\neg P$.

Propositiologiikan kaavoja (*propositional formula*) ovat täsmälleen ne symbolijonot, jotka *Kaava* tuottaa. Muun muassa FT ei ole kaava, koska ainoa keino tuottaa kaava ilman että mukaan tulee $\leftrightarrow$, $\rightarrow$, $\vee$, $\wedge$, (tai $\neg$ on *Peruskaava*, eikä se tuota symbolijonoa FT.

Tuota $P \vee Q \wedge R$ kuten kuvassa 25! Seuraavissa tehtävissä perustele vastauksesi 123
lyhyesti (ei tarvitse laatia kuvan 25 kaltaista esitystä). Onko $\neg\neg(\mathsf{F})$ kaava? Onko Q) 124
kaava? 125

Yhdistettyjä kaavoja (*compound formula*) ovat ne kaavat, joissa esiintyy $\neg$, $\wedge$, $\vee$, $\rightarrow$ tai $\leftrightarrow$. Muut kaavat ovat *atomikaavoja* (*atomic formula*). Atomikaava on muuten sama kuin *Peruskaava*, mutta atomikaava voi sisältää turhia sulkeita ja *Peruskaava* ei voi. Olisi tietysti ollut tyylikkäämpää, että ne vastaisivat toisiaan täsmälleen, mutta se olisi tarvinnut vaikeaselkoisemman BNF-määritelmän.

$\neg$	
F	T
T	F

$\wedge$	F	T
F	F	F
T	F	T

$\vee$	F	T
F	F	T
T	T	T

$\rightarrow$	F	T
F	T	T
T	F	T

$\leftrightarrow$	F	T
F	T	F
T	F	T

Kuva 26: Konnektiivien edustamat totuusfunktiot

Välisymbolien *EkvKaava* ja *ImplKaava* nimien alkuosat ”Ekv” ja ”Impl” viittaavat tietysti materiaaliseen ekvivalenssiin ja materiaaliseen implikaatioon. *Disjunktio* (*disjunction*) tarkoittaa konnektiivia $\vee$ tai sillä muodostettua kaavaa muotoa $\varphi \vee \psi$. ”Disj” viittaa siihen. *Konjunktio* (*conjunction*) tarkoittaa konnektiivia $\wedge$ tai sillä muodostettua kaavaa muotoa $\varphi \wedge \psi$. *Negaatio* (*negation*) tarkoittaa konnektiivia $\neg$ tai sillä muodostettua kaavaa muotoa $\neg\varphi$.

Propositiomuuttuja on *käytössä*, jos ja vain jos se esiintyy ainakin yhdessä puheena olevassa kaavassa tai se on muuten otettu puheenaiheeksi. Esimerkiksi Carrollin paradoksissa (sivu 29) käytössä ovat propositiomuuttujat A, B ja C. Pihtiputaan mummolla ne ovat P, K, R ja S (sivut 30 ja 30). Jos puhumme kolmipaikkaisesta totuusfunktiosta, jota esittää kaava $\neg(P \vee R)$, niin vakiintuneen käytännön mukaisesti sen paikkaa 2 edustaa propositiomuuttuja Q. Silloin Q on käytössä, vaikka sitä ei kaavassa mainitakaan.

Tilanne on mikä tahansa funktio käytössä olevien propositiomuuttujien joukolta joukolle $\{\mathsf{F},\mathsf{T}\}$. Toisin sanoen, tilanne asettaa kullekin käytössä olevalle propositiomuuttujalle totuusarvon, joka on joko F tai T. Propositiomuuttujan totuusarvo voidaan valita vapaasti riippumatta siitä, mitä totuusarvoja muut propositiomuuttujat saavat. Tilanne on siis mikä tahansa käytössä olevien propositiomuuttujien totuusarvojen yhdistelmä. Jos käytössä on n propositiomuuttujaa, niin erilaisia tilanteita on 2^n kappaletta.

Kaavan totuusarvo määräytyy tilanteesta. Se lasketaan sen mukaan, mitä kuvassa 24 esitettyä muotoa kukin osakaava on. Osakaavan F totuusarvo on F ja osakaavan T totuusarvo on T. Jos osakaava on muotoa *Propositiomuuttuja*, niin sen totuusarvo on sama kuin kyseessä olevan propositiomuuttujan totuusarvo puheena olevassa tilanteessa. Jos osakaava on muotoa $\neg$*NegKaava*, *KonjKaava* $\wedge$ *NegKaava*, *DisjKaava* $\vee$ *KonjKaava*, *DisjKaava* $\rightarrow$ *ImplKaava* tai *EkvKaava* $\leftrightarrow$ *ImplKaava*, niin sen totuusarvo lasketaan sen omien osakaavojen totuusarvoista kuvan 26 mukaisesti. Muotoa (*Kaava*) olevan osakaavan totuusarvo on sama kuin sen sisältämän *Kaava*n totuusarvo.

Kuva 24 määrää konnektiivien laskujärjestyksen. Esimerkkinä tästä osoitamme, että se ei salli kaavalle $P \vee Q \wedge R$ muuta laskujärjestystä kuin sen, mikä löydettiin vastauksessa 123. Kaavan $\wedge$ on peräisin vaihtoehdosta *KonjKaava* $\wedge$ *NegKaava*, koska $\wedge$ ei esiinny kuvassa 24 missään muualla. Sen *KonjKaava* käytti vaihtoehtoa *NegKaava*, koska ainoa muu vaihtoehto *KonjKaava* $\wedge$ *NegKaava* tuottaisi kaavaan toisen $\wedge$:n, mutta kaavassa $P \vee Q \wedge R$ on vain yksi $\wedge$. Tämä *NegKaava* käytti vaihtoehtoa *Peruskaava*, koska muutoin kaavassa olisi sulkeet tai $\neg$. *Peruskaava* voi tuottaa vain F:n, T:n tai propositiomuuttujan, ja niistä vain propositiomuuttuja Q täsmää siihen, mitä kaavassa $P \vee Q \wedge R$ on $\wedge$:n edessä. Siksi edellä mainitun vaihtoehdon *KonjKaava* $\wedge$ *NegKaava* tuottama osakaava alkaa $Q\,\wedge$. Niinpä $P \vee Q \wedge R$ voidaan laskea vain niin, että $Q \wedge R$ lasketaan ensin.

Missä järjestyksessä kuvan 24 mukaan lasketaan $P \leftrightarrow Q \leftrightarrow R$? Entä $P \rightarrow Q \rightarrow R$?
Perustele vastauksesi lyhyesti (ei tarvitse laatia kuvan 25 kaltaista esitystä)! 126

Kuvasta 24 voidaan tarkastaa sekin, että $\neg$ sitoo voimakkaammin kuin muut konnektiivit. Seuraavaksi vahvin on $\wedge$ ja sitten $\vee$, sitten $\rightarrow$ ja lopuksi $\leftrightarrow$. Liitännäisyyden

	$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
vaihdannainen					
liitännäinen					
vasemmalle liitännäinen					
oikealle liitännäinen					
kasvava paikan 1 suhteen					
kasvava paikan 2 suhteen					
vähenevä paikan 1 suhteen					
vähenevä paikan 2 suhteen					

Kuva 27: Tehtävässä 127 täytettävä taulukko

suunta ei ole $\neg$:lle mielekäs käsite, koska sillä on vain yksi argumentti. Täydennä kuvan 27 taulukko siten, että $\surd$ on kyllä, - on ei, ja tyhjä tarkoittaa että kysymys ei ole mielekäs! 127

Päättely tapahtuu nollan tai useamman *oletuksen* (*assumption*) vallitessa. Oletukset jakautuvat pysyviin ja tilapäisiin.

Pysyvät oletukset ilmaisevat sen kohteen lainalaisuuksia, josta kaavoilla puhutaan. Ne ovat voimassa aina kun käsitellään sitä puheenaihetta. Esimerkiksi Carrollin paradoksissa tehtiin kaksi pysyvää oletusta (1) ja (2), jotka muotoiltiin myöhemmin kaavoina (4) ja (5). Luvuista puhuttaessa esimerkiksi se on pysyvä oletus, että kun mihin tahansa lukuun lisätään nolla, niin tulos on alkuperäinen luku. Jos kaava on tosi jokaisessa tilanteessa joka toteuttaa pysyvät oletukset, niin se on *laki*. Niinpä (4) ja (5) ovat lakeja Carrollin paradoksissa, ja $x+0=x$ on laki luvuista puhuttaessa.

Tilapäinen oletus asetetaan voimaan esimerkiksi sanoilla "oletamme, että" tai "jos", ja siitä luovutaan myöhemmin. Usein käytetty tapa johtaa $\varphi \Rightarrow \psi$ on lisätä φ oletuksiin, johtaa ψ ja hylätä φ [21]. Muita tyypillisiä syitä tilapäisten oletusten tekemiseen ovat lakien [36], [37] ja [38] tai niitä vastaavien epämuodollisten periaatteiden käyttö; siis päätteleminen jakamalla tapauksiin, johtamalla ristiriita tai käänteisellä todistuksella. Esimerkiksi Carrollin paradoksissa setä Joe oletti, että Carr on ulkona ja väitti johtaneensa siitä ristiriidan.

Pysyviä oletuksia kutsutaan varsinkin propositiologiikan ulkopuolella usein *aksioomiksi* (*axioms*). Toisinaan niitä sanotaan *ei-loogisiksi aksioomiksi* (*non-logical axioms*) erottamaan ne logiikan omista aksioomista.

Tässä kirjassa käsitellään propositiologiikan omia aksioomia hyvin vähän, koska ne ovat käyttökelpoisia logiikan tutkimiseen mutta eivät oikeastaan lainkaan logiikan soveltamiseen. Jotta kuitenkin asiasta syntyisi jonkinlainen mielikuva, näytämme esimerkkinä Jan Łukasiewiczin (1878–1956) laatiman aksioomajärjestelmän propositiologiikalle. Sitä ei tarvitse opetella!

Sen kaavoissa käytetään vain propositiomuuttujia, sulkeita ja konnektiiveja $\neg$ ja $\rightarrow$. Se riittää, koska mikä tahansa muita konnektiiveja sisältävä kaava voidaan ennen järjestelmän käyttöä muuntaa yhtäpitäväksi kaavaksi, jossa ei ole muita konnektiiveja. Nimittäin $\varphi \vee \psi \Leftrightarrow (\neg\varphi \rightarrow \psi)$, $\varphi \wedge \psi \Leftrightarrow \neg(\varphi \rightarrow \neg\psi)$ ja $\varphi \leftrightarrow \psi \Leftrightarrow ((\neg\varphi \rightarrow \psi) \rightarrow \neg(\varphi \rightarrow \neg\psi))$. Niinpä jos halutaan todistaa esimerkiksi $P \vee \neg P$, se muunnetaan muotoon $(\neg P \rightarrow \neg P)$, ja näin saatu kaava johdetaan järjestelmässä. Tässä lähestymistavassa nämä kolme yhtäpitävyyttä ovat $\wedge$:n, $\vee$:n ja $\leftrightarrow$:n formaalit määritelmät, eli ne ja vain ne (eikä siis esimerkiksi kuva 26) kertovat, mitä $\wedge$, $\vee$ ja $\leftrightarrow$ tarkoittavat.

Konnektiivin $\rightarrow$ mukana tulee täsmälleen yhdet sulkeet tyyliin $(\varphi \rightarrow \psi)$, ja muuten sulkeita ei käytetä. Päättelysääntöjä on yksi: jos on päätelty φ ja on päätelty $(\varphi \rightarrow \psi)$, niin saa päätellä ψ. Aksioomaskeemoja on kolme:

$$(\varphi \rightarrow (\psi \rightarrow \varphi)) \tag{16}$$

$$((\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))) \tag{17}$$

$$((\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)) \tag{18}$$

Esimerkkinä tämän järjestelmän käytöstä todistamme asian, jonka näkee kuvasta 26 yhdellä vilkaisulla, tai jonka voi todistaa helposti [16]:lla, [95]:lla ja [7]:llä: $P \rightarrow P$. Ensin käytämme aksioomaskeemaa (16) siten, että φ on P ja myös ψ on P. Sitten käytämme sitä uudelleen siten, että φ on P mutta ψ on $(P \rightarrow P)$. Seuraavaksi käytämme aksioomaskeemaa (17) siten, että φ on P, ψ on $(P \rightarrow P)$ ja χ on P. Lopuksi käytämme kahteen kertaan päättelysääntöä, ensin rivien 2 ja 3 ja sitten rivien 1 ja 4 kaavoihin. Kaavat on alla sisennetty siten, että kun päättelysäännöllä johdetaan φ:stä ja $(\varphi \rightarrow \psi)$:stä ψ, niin φ:t ovat päällekkäin ja ψ:t ovat päällekkäin.

1.	$(P \rightarrow (P \rightarrow P))$	(16)
2.	$(P \rightarrow ((P \rightarrow P) \rightarrow P))$	(16)
3.	$((P \rightarrow ((P \rightarrow P) \rightarrow P)) \rightarrow ((P \rightarrow (P \rightarrow P)) \rightarrow (P \rightarrow P)))$	(17)
4.	$((P \rightarrow (P \rightarrow P)) \rightarrow (P \rightarrow P))$	2, 3
5.	$(P \rightarrow P)$	1, 4

Tässä järjestelmässä voidaan todistaa kaikki vaadittuun muotoon muunnetut aina todet propositiologiikan kaavat, mutta monet todistukset ovat pitkiä ja vaikeatajuisia. Järjestelmä on aivan liian kömpelö käytännön tarpeisiin, mutta logiikan teorian tutkimusta se palvelee hyvin. (Todistus että kaikki voidaan todistaa, on liian pitkä ja vaikea tässä esitettäväksi!)

Yksi sen tärkeä piirre on, että päätteleminen on pelkistetty hyvin yksinkertaisiksi tempuiksi, jotka voidaan tarkastaa mekaanisesti miettimättä yhtään, mitä mikäkin merkitsee. C++-kielinen tietokoneohjelma, joka selviää tehtävästä, mahtuu reilusti alle 200 riviin. Siitä varmistumiseksi, että tämä järjestelmä tuottaa vain tosia kaavoja, riittää tarkastaa että sen aksioomaskeemat tuottavat vain tosia kaavoja ja että päätteleminen edellä kuvatulla säännöllä tuottaa tosista kaavoista vain tosia kaavoja. Jos käyttöön halutaan myös $\wedge$, $\vee$ ja $\leftrightarrow$, niin riittää tarkastaa, että edellä annetut yhtäpitävyydet, jotka esittävät ne $\rightarrow$:n ja $\neg$:n avulla, esittävät ne oikein. Kaiken kaikkiaan niiden ”ensimmäisten päättelykeinojen” määrä, jotka täytyy vain hyväksyä jotta mitään voitaisiin todistaa, on saatu varsin pieneksi.

Toki jokainen propositiologiikan kaava on tarkastettavissa mekaanisesti vielä paljon yksinkertaisemmin kokeilemalla kaikki siinä esiintyvien propositiomuuttujien totuusarvojen yhdistelmät. Mutta kaikkien yhdistelmien kokeileminen lakkaa onnistumasta kun siirrytään predikaattilogiikkaan, toisin kuin aksioomilla ja päättelysäännöillä todistaminen. Łukasiewiczin järjestelmä on melko pienillä lisäyksillä saatavissa toimimaan myös koulumatematiikassa ja predikaattilogiikassa. Tulemme esittämään senkaltaisen tuloksen luvussa 6, joskaan ei Łukasiewiczin järjestelmälle vaan eräälle helpommin ymmärrettävälle järjestelmälle.

Tässä kirjassa $\varphi \Rightarrow \psi$, $\varphi \Leftarrow \psi$ ja $\varphi \Leftrightarrow \psi$ ilmaisevat päättelyaskelia ja päättelysääntöjä. Ne eivät ole tilanteesta riippuen tosia tai epätosia, vaan voimassa olevista oletuksista riippuen *päteviä* tai *epäpäteviä*. Päättelyaskel tai -sääntö $\varphi \Rightarrow \psi$ on pätevä jos ja vain jos $\varphi \rightarrow \psi$ on tosi jokaisessa tilanteessa, joka toteuttaa voimassa olevat oletukset.

Muussa tapauksessa se on epäpätevä. Esimerkiksi jos x:stä ei ole oletettu mitään, niin $x \geq 0 \Rightarrow x \geq 2$ on epäpätevä. Sillä on monta vastaesimerkkiä, eli tilannetta, joka toteuttaa voimassa olevat oletukset mutta jossa $x \geq 0 \rightarrow x \geq 2$ ei ole tosi. Muun muassa $x = 1$ on sellainen. Jos on oletettu että $x < 0$, niin $x \geq 0 \Rightarrow x \geq 2$ on pätevä. Silloin sillä ei ole yhtään vastaesimerkkiä.

Vastaavasti $\varphi \Leftrightarrow \psi$ on pätevä jos ja vain jos sillä ei ole yhtään vastaesimerkkiä, eli tilannetta, joka toteuttaa voimassa olevat oletukset, mutta jossa $\varphi \leftrightarrow \psi$ ei ole tosi. Tietenkin $\varphi \Leftarrow \psi$ tarkoittaa samaa kuin $\psi \Rightarrow \varphi$.

Lisäksi $\Leftrightarrow$, $\Rightarrow$ ja $\Leftarrow$ käyttäytyvät ketjutetuissa ilmauksissa eri lailla kuin $\leftrightarrow$ ja $\rightarrow$. Tästä puhutaan jonkin verran myöhemmin tässä alaluvussa. Molemmista eroista puhuttiin perusteellisemmin muun muassa sivulla 41. Sanojen ”pätevä” ja ”epäpätevä” käyttö $\Leftrightarrow$:n, $\Rightarrow$:n ja $\Leftarrow$:n tuloksista sanojen ”tosi” ja ”epätosi” sijaan helpottaa sen mielessä pitämistä, miten $\Leftrightarrow$, $\Rightarrow$ ja $\Leftarrow$ eroavat $\leftrightarrow$:sta ja $\rightarrow$:sta.

Puhumme toisinaan päättelysäännön pätevyydestä joissakin tilanteissa. Silloin tarkoitamme, että jos voimassa olevat oletukset sallivat ne ja vain ne tilanteet, niin päättelysääntö on pätevä. Saatamme myös puhua päättelyaskeleen tai -säännön epäpätevyydestä jossakin tilanteessa. Silloin tarkoitamme, että se tilanne on vastaesimerkki sille päättelyaskeleelle tai -säännölle.

Myös ilmaus muotoa $\varphi \Rightarrow \psi$, $\varphi \Leftarrow \psi$ tai $\varphi \Leftrightarrow \psi$, joka on pätevä jokaisessa tilanteessa joka toteuttaa pysyvät oletukset, on *laki*. Esimerkiksi Pihtiputaan mummon tapauksessa $K \Rightarrow S$ on laki, koska se on hänelle aina pätevä, kuten todettiin sivulla 32.

Voimassa olevat oletukset jakavat tilanteet *mahdollisiin* ja *mahdottomiin*. Pihtiputaan mummolle mahdolliset tilanteet esitettiin kuvassa 16. Carrollin paradoksissa alun perin mahdolliset tilanteet esitettiin kuvan 15 ensimmäisellä rivillä. Ne esittää myös oletusten (4) ja (5) konjunktio, sekä sivulla 29 johdettu kaava $\neg A \vee (B \wedge \neg C)$. Kun setä Joe teki tilapäisen oletuksen, että Carr on ulkona, osa ennen sitä mahdollisista tilanteista lakkasi olemasta mahdollisia. Kuvan 15 toinen rivi esittää oletuksen voimassa ollessa mahdolliset tilanteet.

Pysyvän tai tilapäisen oletuksen voi ilmaista sanallisesti, kuvien 15 ja 16 kaltaisesti, kaavana, päättelysääntönä tai muilla keinoin. Päättelyimplikaationa $\varphi \Rightarrow \psi$ ilmaistu oletus tarkoittaa tässä kirjassa samaa kuin kaavana $\varphi \rightarrow \psi$ ilmaistu oletus. Kumpikin tekee päättelyimplikaatiosta $\varphi \Rightarrow \psi$ pätevän siksi aikaa kun oletus on voimassa. ”Jos $\varphi \Rightarrow \psi$” ei siis oleta, että $\varphi \Rightarrow \psi$ on jo voimassa, vaan se asettaa sen voimaan. Vastaavasti päättelysääntönä $\varphi \Leftrightarrow \psi$ ilmaistu oletus tarkoittaa samaa kuin kaavana $\varphi \leftrightarrow \psi$ ilmaistu oletus, ja tekee yhtäpitävyydestä $\varphi \Leftrightarrow \psi$ pätevän siksi aikaa kun oletus on voimassa. Kaavana φ ilmaistu oletus tekee yhtäpitävyydestä $\varphi \Leftrightarrow \mathsf{T}$ pätevän voimassaoloajakseen. Oletus $\varphi \Leftrightarrow \mathsf{F}$ tarkoittaa samaa kuin oletus $\neg\varphi$. Oletukset $\varphi \Leftrightarrow \mathsf{T}$ ja $\varphi \Leftrightarrow \mathsf{F}$ ovat sikäli kätevämpiä kuin samaa tarkoittavat oletukset φ ja $\neg\varphi$, että niitä voi soveltaa kaavan sisällä kuten [28] lupaa.

Carrollin paradoksin tapauksessa pysyvät oletukset voitiin ilmaista yhtenä kaavana. Se onnistuu myös Pihtiputaan mummon tapauksessa — laadi sellainen kaava! 128

Se ei kuitenkaan onnistu silloin, kun oletuksia on äärettömän monta. Esimerkiksi jokainen edellä olleista aksioomaskeemoista (16), (17) ja (18) edustaa äärettömän montaa aksioomaa, koska φ:n tilalle voi laittaa minkä tahansa kaavan, ja samoin ψ:n ja χ:n tilalle. Niinpä (16) edustaa muun muassa seuraavia aksioomia: $P \rightarrow (P \rightarrow P)$, $P \rightarrow (\neg P \rightarrow P)$, $P \rightarrow (\neg\neg P \rightarrow P)$, $P \rightarrow (\neg\neg\neg P \rightarrow P)$, ... Jo tässä on äärettömän monta aksioomaa, ja lisäksi ovat $P \rightarrow ((P \rightarrow P) \rightarrow P)$, $(P \rightarrow P) \rightarrow (P \rightarrow (P \rightarrow P))$, $(P \rightarrow P) \rightarrow ((P \rightarrow P) \rightarrow (P \rightarrow P))$ ja loputtomasti muita.

$$\begin{array}{rcl} \textit{Päättelyketju} & ::= & \textit{Kaava PäättOp Kaava} \mid \textit{Päättelyketju PäättOp Kaava} \\ \textit{PäättOp} & ::= & \Leftrightarrow \mid \Rightarrow \mid \Leftarrow \end{array}$$

Kuva 28: Päättelyketjujen syntaksi sallien $\Rightarrow$ ja $\Leftarrow$ samassa ketjussa

Siksi logiikkaa ei voida rakentaa sen varaan, että oletukset voisi ilmaista yhtenä kaavana. Niinpä formaalissa logiikassa oletukset ilmaistaan joukkona kaavoja. Tämä joukko voi olla tyhjä, äärellinen tai ääretön. Merkitsemme sitä kreikkalaisella kirjaimella Γ (iso Gamma) muunnelmineen. Esimerkiksi $\Gamma \cup \{\varphi\}$ tarkoittaa sitä joukkoa kaavoja, joka saadaan lisäämällä Γ:n sisältämiin kaavoihin φ.

Merkintä $\Gamma \models \varphi$ tarkoittaa, että jokaisessa tilanteessa, jossa jokainen Γ:n sisältämä kaava on tosi, myös φ on tosi. [42]

Tälle merkinnälle pätee kolme tärkeää periaatetta. Niitä ei tarvitse oppia vielä nyt, vaan vasta luvussa 6. On kuitenkin tärkeää saada jo nyt tuntumaa siihen, mitä $\models$ tarkoittaa. Alla lueteltujen periaatteiden läpikäynti on siihen hyvä keino. Alla myös Δ on mikä tahansa joukko kaavoja, ja $\{\varphi\}$ on se joukko, johon sisältyy φ eikä mitään muuta.

(a) $\{\varphi\} \models \varphi$
(b) Jos $\Gamma \models \varphi$, niin $\Gamma \cup \Delta \models \varphi$. [43]
(c) Jos $\Gamma \models \varphi$ ja $\Gamma \cup \{\varphi\} \models \psi$, niin $\Gamma \models \psi$.

Kohta (a) ilmaisee erään itsestäänselvyyden. Minkä? 129

Kohta (b) pätee, koska $\Gamma \cup \Delta$ sisältää kaikki Γ:n kaavat (ja mahdollisesti muitakin kaavoja). Siksi jokaisessa tilanteessa, jossa jokainen $(\Gamma \cup \Delta)$:n sisältämä kaava on tosi, myös jokainen Γ:n sisältämä kaava on tosi. Jos-osan vuoksi siinä tilanteessa myös φ on tosi. Niinpä jokaisessa tilanteessa, jossa jokainen $(\Gamma \cup \Delta)$:n sisältämä kaava on tosi, myös φ on tosi.

Kohta (c) formalisoi sen, että kahdesta päättelyaskeleesta muodostuvan päättelyketjun lopputulos seuraa alkuperäisistä oletuksista. Sillä voi siis tehdä saman kuin $\Rightarrow$:n transitiivisuudella. Todistaaksemme (c):n tarkastelemme mielivaltaista tilannetta, jossa jokainen Γ:n kaava on tosi. Osuuden $\Gamma \models \varphi$ vuoksi myös φ on siinä tosi. Niinpä jokainen $(\Gamma \cup \{\varphi\})$:n kaava on siinä tosi, joten osuuden $\Gamma \cup \{\varphi\} \models \psi$ vuoksi myös ψ on siinä tosi. Olemme osoittaneet, että jokaisessa tilanteessa, jossa jokainen Γ:n kaava on tosi, myös ψ on tosi. Toisin sanoen, $\Gamma \models \psi$.

Jos Γ ilmaisee voimassa olevat oletukset, niin $\Gamma \models \varphi$ tarkoittaa, että jokaisessa mahdollisessa tilanteessa φ on tosi. Niinpä [29]:n mukaan $\Gamma \models \varphi \leftrightarrow \psi$ tarkoittaa samaa kuin oletusten Γ vallitessa lausuttu $\varphi \Leftrightarrow \psi$; ja [20]:n mukaan $\Gamma \models \varphi \rightarrow \psi$ tarkoittaa samaa kuin oletusten Γ vallitessa lausuttu $\varphi \Rightarrow \psi$.

Lisäksi $\models$:n ja $\Rightarrow$:n välillä on suora yhteys. Määritelmän [19] mukaan $\varphi \Rightarrow \psi$ tarkoittaa, että jokaisessa mahdollisessa tilanteessa, jossa φ on tosi, myös ψ on tosi. Jos Γ ilmaisee voimassa olevat oletukset, niin myös $\Gamma \cup \{\varphi\} \models \psi$ tarkoittaa samaa, koska Γ rajoittaa tarkastelun mahdollisiin tilanteisiin, ja $\cup\ \{\varphi\}$ poimii niistä ne, joissa φ on tosi.

Merkintöjen $\Leftrightarrow$, $\Rightarrow$ ja $\Leftarrow$ eräs vahvuus logiikan soveltamisen kannalta verrattuna merkintään $\models$ on siinä, että niiden avulla voi näppärästi ilmaista useammasta kuin yhdestä askeleesta koostuvia päättelyketjuja. (Toinen suuri vahvuus on se, että $\Leftrightarrow$:a voi käyttää kaavan sisällä.) Kuva 28 esittää päättelyketjun rakenteen sellaisena kuin se määriteltiin sivulla 44. Kuvasta näkyy, että päättelyketju koostuu joko kahdesta kaavasta ja niiden

$$
\begin{array}{rcl}
\mathit{Päättelyketju} & ::= & \mathit{MolKetju} \mid \mathit{OikKetju} \mid \mathit{VasKetju} \\
\mathit{MolKetju} & ::= & \mathit{Kaava} \Leftrightarrow \mathit{Kaava} \mid \mathit{MolKetju} \Leftrightarrow \mathit{Kaava} \\
\mathit{OikKetju} & ::= & \mathit{Kaava} \Rightarrow \mathit{Kaava} \mid \mathit{MolKetju} \Rightarrow \mathit{Kaava} \mid \\
 & & \mathit{OikKetju} \Leftrightarrow \mathit{Kaava} \mid \mathit{OikKetju} \Rightarrow \mathit{Kaava} \\
\mathit{VasKetju} & ::= & \mathit{Kaava} \Leftarrow \mathit{Kaava} \mid \mathit{MolKetju} \Leftarrow \mathit{Kaava} \mid \\
 & & \mathit{VasKetju} \Leftrightarrow \mathit{Kaava} \mid \mathit{VasKetju} \Leftarrow \mathit{Kaava}
\end{array}
$$

Kuva 29: Päättelyketjujen syntaksi kieltäen $\Rightarrow$ ja $\Leftarrow$ samassa ketjussa

välissä olevasta päättelyoperaattorista, tai päättelyketjusta, jota on jatkettu päättelyoperaattorilla ja kaavalla. Päättelyoperaattoreita ovat $\Leftrightarrow$, $\Rightarrow$ ja $\Leftarrow$.

Kuvassa 29 on päättelyketju määritelty uudelleen niin, että mukana on vaatimus, että $\Rightarrow$ ja $\Leftarrow$ eivät saa esiintyä samassa päättelyketjussa. *MolKetju* on päättelyketju, jossa ei esiinny muita päättelyoperaattoreita kuin $\Leftrightarrow$. Sen määritelmä noudattaa samaa mallia kuin kuva 28. *OikKetju* sisältää ainakin yhden $\Rightarrow$:n. Miten tämän voi päätellä
kuvasta 29? Miten kuvasta 29 voidaan tuottaa *OikKetju*:n alkuosa heti ensimmäisen 130
$\Rightarrow$:n perässä olevaan kaavaan asti? *OikKetju* voi loppua siihen, tai jatkua mielivaltaisen 131
monta kertaa niin, että seuraavaksi tulee $\Leftrightarrow$ tai $\Rightarrow$ ja sen jälkeen tulee kaava. *VasKetju* on muuten samanlainen kuin *OikKetju*, mutta $\Rightarrow$:n tilalla on $\Leftarrow$.

Kuva 29 on huomattavasti monimutkaisempi kuin kuva 28. Tämä havainnollistaa sitä, että BNF:llä ei voi sanoa kaikkea näppärästi. (Itse asiassa on paljon asioita, joita BNF:llä ei voi sanoa edes kömpelösti.) Käytännön määrittelytyössä kannattaa käyttää BNF:ää esittämään ne asiat jotka sillä voi esittää selkeästi, ja käyttää sanallisia ilmauksia tai muita keinoja esittämään loput. Esimerkiksi kuvat 24 ja 28 ovat lyhyitä ja selkeitä, ja tekevät selväksi muun muassa sen, että $\Leftrightarrow$, $\Rightarrow$ ja $\Leftarrow$ eivät voi esiintyä sulkeiden sisällä eivätkä konnektiivien alaisuudessa. Se, että $\Rightarrow$ ja $\Leftarrow$ eivät saa esiintyä samassa päättelyketjussa, kannattaa ilmaista sanallisesti.

Tässä kirjassa voimassa on vahva suositus mutta ei ehdoton vaatimus, että $\Rightarrow$ ja $\Leftarrow$ eivät saa esiintyä samassa päättelyketjussa.

Kukin päättelyketjun osa, joka muodostuu kahdesta kaavasta ja niiden välissä olevasta päättelyoperaattorista, on päättelyaskel. (Kaavat pitää ottaa kokonaisina, siis ei esimerkiksi niin että ketjusta $P \vee Q \vee \mathsf{F} \Leftrightarrow P \vee Q$ poimitaan $Q \vee \mathsf{F} \Leftrightarrow P$.) Päättelyaskelten pätevyys määräytyy määritelmien [19] ja [22] mukaan. Ne käyvät kaikki mahdolliset tilanteet läpi. Kuitenkaan läheskään aina ei ole käytännöllistä tai edes mahdollista tarkastaa päättelyaskeleen pätevyyttä niin. Siksi tavallisesti päättelyaskel todetaan päteväksi jonkin lain, voimassa olevan oletuksen tai aiemmin korkeintaan samoilla oletuksilla todistetun tuloksen perusteella. Niitä saa aina soveltaa koko kaavan tasolla. Kaavan sisällä niitä saa soveltaa [28]:n, [39]:n ja [40]:n mukaisesti.

Päättelyketju on pätevä jos ja vain jos sen jokainen askel on pätevä. Esimerkiksi päättelyketjun $\varphi \Rightarrow \psi \Leftrightarrow \chi \Rightarrow \zeta$ pätevyys voidaan ilmaista $\Gamma \models (\varphi \to \psi) \wedge (\psi \leftrightarrow \chi) \wedge (\chi \to \zeta)$. Jälkimmäinen merkintä on kömpelömpi kuin edellinen siksi, että muut kaavat kuin ensimmäinen ja viimeinen joudutaan kirjoittamaan kahdesti. Tällä on suuri merkitys, koska käytännön tilanteissa kaavoina on jotain pitempää ja monimutkaisempaa kuin pelkät kreikkalaiset kirjaimet ψ ja χ.

Muotoa *MolKetju* oleva pätevä päättelyketju, jonka ensimmäinen kaava on φ_0 ja viimeinen φ_n, todistaa sekä $\varphi_0 \Leftrightarrow \varphi_n$, $\varphi_0 \Rightarrow \varphi_n$ että $\varphi_0 \Leftarrow \varphi_n$. Muotoa *OikKetju* oleva pätevä päättelyketju todistaa vain $\varphi_0 \Rightarrow \varphi_n$, ja muotoa *VasKetju* oleva vain $\varphi_0 \Leftarrow \varphi_n$.

On tavallista, että yksi päättelyketju ei riitä halutun tuloksen todistamiseen. Tällöin tarvitaan monen päättelyketjun muodostama jono. Koska tavoitteemme ei ole formalisoida käytännöllistä päättelyä kattavasti, jätämme päättelyn rakenteen esittämisen tällä tasolla luonnollisen kielen varaan. Edellä kuvatussa Łukasiewiczin järjestelmässä sekä luvussa 6 esiteltävässä järjestelmässä päättely on formalisoitu kattavasti, mutta ne eivät perustu symboleilla $\Leftrightarrow$ ja $\Rightarrow$ esitettäviin päättelyketjuihin, ja ne ovat liian kömpelöitä käytännön sovelluksiin.

On tärkeää osata itse päätellä, onko jokin todistusrakenne pätevä. Usein helppo keino siihen on epäsuora todistus vastaesimerkin avulla. Esimerkiksi ”jos $\varphi \Rightarrow \psi$ pätee, missä φ on pysyvä oletus, niin ψ pätee jokaisessa mahdollisessa tilanteessa” voidaan todistaa seuraavasti. Jos ψ ei päde jokaisessa mahdollisessa tilanteessa, niin on olemassa mahdollinen tilanne, jossa ψ ei ole tosi. Koska se tilanne on mahdollinen ja koska φ on pysyvä oletus, φ on siinä tosi. Niinpä se tilanne on [19]:n mukaan vastaesimerkki päättelyimplikaatiolle $\varphi \Rightarrow \psi$ eli esimerkkimme jos-osalle.

Osoita epäsuoralla todistuksella vastaesimerkin avulla seuraavat! 132 133 134

Jos tilapäisen oletuksen φ vallitessa ψ on aina tosi,
niin ilman oletusta φ pätee $\varphi \Rightarrow \psi$. (tämä on [21].)

Jos tilapäisen oletuksen φ vallitessa pätee $\psi \Rightarrow \chi$,
niin ilman oletusta φ pätee $\varphi \wedge \psi \Rightarrow \chi$. [44]

Jos tilapäisen oletuksen φ vallitessa pätee $\psi \Leftrightarrow \chi$,
niin ilman oletusta φ pätee $\varphi \wedge \psi \Leftrightarrow \varphi \wedge \chi$. [45]

Laki [21] voidaan johtaa [44]:stä ja aikaisemmista laeista seuraavasti. Jos χ on tosi aina φ:n vallitessa, niin [23]:n mukaan φ:n vallitessa $\chi \Leftrightarrow \mathsf{T}$. Siitä [24] ja [32] tuottavat $\mathsf{T} \Rightarrow \chi$. Lain [44] mukaan ilman oletusta φ pätee $\varphi \wedge \mathsf{T} \Rightarrow \chi$. Siitä [2], [32] ja [26] tuottavat $\varphi \Rightarrow \chi$.

Johda [45] [44]:stä! 135

2.6 Propositiologiikka tietojenkäsittelytieteessä

??? Tämä alaluku ei ole kriittisellä polulla, joten se kirjoitetaan myöhemmin (jos koskaan). Siinä on tarkoitus esitellä konjunktiivinen ja disjunktiivinen normaalimuoto, puhua esitystapojen lyhyyden teoreettisista rajoista, todistaa että muuntaminen normaalimuotojen välillä voi aiheuttaa eksponentiaalista kasvua, esitellä binääripäätöskaaviot ja SAT-solver, sekä esitellä NP-täydellisyys ja sen suhde propositiologiikkaan. Voi olla, että NP-maailma tarvitsee oman alalukunsa.

3 Logiikka koulumatematiikan työkaluna

Tässä luvussa käsitellään päättelemistä propositiologiikan ja yhtäsuuruuden eli $=$-merkin laeilla. Sovelluskohteena ovat luvut, tai tarkemmin sanoen luvuista puhuvat ilmaukset. Mukana on paljon jo koulussa käsiteltyä asiaa, kuten yhtälöiden ratkaisemista, mutta näkökulma on logiikan. Käytettävällä logiikalla ei ole vakiintunutta nimeä. Se on osa predikaattilogiikkaa sovellettuna lukuihin. Tässä luvussa tullaan myös kohtaamaan syvällinen lukujen määrään liittyvä omituisuus, joka aiheutti matemaatikoille paljon päänvaivaa 1800-luvun lopulla.

3.1 Loogista yhtälö(parien) ratkaisemista

Tässä alaluvussa käsittelemme yhtäsuuruuden $=$ lakeja logiikassa. Myös pohdimme predikaattilogiikan lakien olemusta sekä jakoa logiikan omiin ja puheenaiheen lakeihin. Esimerkkeinä, joista pohdinta nousee, tarkastelemme yhtälöiden ja yhtälöparien ratkaisemista päättelynä logiikan merkintöjä käyttäen.

Yhtälö $3x-12=0$ voidaan ratkaista seuraavasti:

$$3x-12=0 \ \Leftrightarrow\ 3x=12 \ \Leftrightarrow\ x=\tfrac{12}{3}=4\,,\ \text{joten}\ 3x-12=0 \ \Leftrightarrow\ x=4\,.$$

Ensin siirrettiin vakiotermi toiselle puolelle etumerkki vaihtaen. Rutinoitunut yhtälöiden ratkaisija osaa ulkoa, että niin saa tehdä. Voisimme esittää sen lakina, missä a ja b edustavat lukusuoran lukuja:

$$a-b=0 \ \Leftrightarrow\ a=b$$

Päättelyaskel $3x-12=0 \Leftrightarrow 3x=12$ saadaan siitä valitsemalla a:ksi $3x$ ja b:ksi 12.

Tämä laki ei kuitenkaan riitä pitkälle. Se ei selviä edes päättelyaskeleesta $3x-8=4 \Leftrightarrow 3x=12$. Siitä selviää yleisempi laki $a-b=c \Leftrightarrow a=c+b$, mutta ei sekään yksinään. Lisäksi tarvitaan kyky laskea paljonko on $4+8$. Yhdessä niillä saadaan $3x-8=4 \Leftrightarrow 3x=4+8 \Leftrightarrow 3x=12$, josta [25] tuottaa $3x-8=4 \Leftrightarrow 3x=12$. Tämä esimerkki havainnollistaa, että käytännön päättelyaskelissa käytetään usein useampaa kuin yhtä lakia tai tietoa.

Yhtäpitävyys $3x=4+8 \Leftrightarrow 3x=12$ perustuu siihen, että kun luku sijoitetaan kaavaan, lopputuloksen totuusarvo voi riippua vain sijoitetun luvun lukuarvosta, ei sen esitysmuodosta (tämän varmistamiseksi pitää toisinaan lisätä esitysmuodon ympärille sulkeet). Tässä $4+8$ ja 12 ovat saman luvun eri esitysmuotoja. Niinpä kun ne sijoitetaan samaan kaavaan $3x=y$ saman muuttujan y tilalle, niin lopptuloksilla $3x=4+8$ ja $3x=12$ on sama totuusarvo.

Päättelyaskeleen $3x-8=4 \Leftrightarrow 3x=12$ saa perustella myös muodossa $3x-8=4 \Leftrightarrow 3x=4+8=12$. Se on sekä lyhyempi että helppolukuisempi kuin edellinen muoto, joten sitä kannattaa suosia, jos päättely on tarkoitettu ihmisten luettavaksi. Siitä huolimatta se on logiikan näkökulmasta monimutkaisempi kuin edellinen muoto. Vaikka lopputulos $3x-8=4 \Leftrightarrow 3x=12$ näyttää sen välittömältä seuraukselta, sen poimiminen vaatii useita alimman tason päättelyaskelia (näytämme myöhemmin, millaisia). Niin vaatii myös tietojen $3x-8=4 \Leftrightarrow 3x=4+8$ ja $4+8=12$ yhdistäminen yhtäpitävyydeksi $3x-8=4 \Leftrightarrow 3x=4+8=12$. Kokenut päättelijä ei kuitenkaan tee niitä päättelyaskelia, vaan näkee lopputuloksen suoraan. Hänellä on ikään kuin oikoteitä.

Päättelemisessä tulee vastaan niin paljon erilaisia tapauksia, että olisi toivotonta yrittää opetella jokaista varten sopiva laki tai oikotie ulkoa. Sitäpaitsi monet oikotiet on melkein mahdoton ilmaista ulkoa opetteluun sopivassa muodossa. Niiden osaaminen on osittain vaistonvaraista. Ehkä seuraava harjoitus havainnollistaa tätä.

Ihmiset kirjoittavat harvoin $1x+-5$. Sen sijaan he yleensä kirjoittavat $x-5$. Olkoot a ja b kokonaislukuja. Ilmaise säännöt miten $ax+b$ yleensä kirjoitetaan eri tapauksissa. Oleta, että "kirjoita x" kirjoittaa kirjaimen x, "kirjoita $+$" kirjoittaa plusmerkin, ja niin edelleen. Oleta, että jos $a \geq 0$, niin "kirjoita_lukuna a" kirjoittaa a:n esityksen numerojonona ilman etumerkkiä (esimerkiksi 12), ja jos $a < 0$ niin se kirjoittaa etumerkiksi $-$ (esimerkiksi -12); ja samoin b:lle! 136

Onneksi moninaiset tapaukset voi ratkaista yhdistelemällä pientä määrää lakeja, ja onneksi oikoteitä oppii itsestään kun harjoittelee. Lakeja voi myös johtaa toisistaan. Aluksi päätteleminen sujuu kömpelösti, mutta harjoittelemalla ja lukemalla muiden päättelyitä oppii oikoteitä ja ratkaisustrategioita. Johda $a-b=0 \Leftrightarrow a=b$ laista $a-b=c \Leftrightarrow a=c+b$ ja eräästä yleisesti tunnetusta muusta tiedosta! 137

Toisinaan tarvitaan päättelyaskel, jonka saisi suoraan laista $a+b=c \Leftrightarrow a=c-b$. Lienee selvää, että tätä lakia ei kannata opetella erikseen ulkoa, koska sen saa jo tutuksi tulleesta laista $a-b=c \Leftrightarrow a=c+b$ sijoittamalla b:n tilalle $-b$. Rutinoitunut päättelijä tietää, että tässä tapauksessa sen voi tehdä korvaamalla jokainen $+b$ lausekkeella $-b$ ja päinvastoin, ja pystyy siksi kirjoittamaan tuloksen suoraan. Mutta hän tietää myös, että on muita tapauksia, joissa tällainen korvaaminen ei ole oikein. Esimerkiksi jos lausekkeeseen $1+b^2$ pitää sijoittaa b:n tilalle $-b$, niin edellä kuvattu korvaaminen tuottaisi väärän tuloksen $1-b^2$. Tämä havainnollistaa sitä, että rutinoituneen päättelijän käyttämä sääntökokoelma on monimutkainen ja ehkä osittain tiedostamaton.

Jos matematiikkoa pyydettäisiin näyttämään yksityiskohtaisesti mutta tiiviisti miten yhtäpitävyydestä $a-b=c \Leftrightarrow a=c+b$ voidaan johtaa $a+b=c \Leftrightarrow a=c-b$ sijoittamalla b:n tilalle $-b$, hän kirjoittaisi kenties suunnilleen seuraavasti:

$$a+b=a+(--b)=a-(-b)=c \;\Leftrightarrow\; a=c+(-b)=c-b \tag{19}$$

Ensimmäisen yhtäsuuruuden kohdalla käytettiin sitä, että jokaiselle luvulle b pätee $b=--b$, sekä sitä, että yhtäsuuruutta (tässä tapauksessa $b=--b$) saa käyttää isomman lausekkeen sisällä (tässä tapauksessa $a+b$), jos lauseke on määritelty. Siis $b=--b \Rightarrow a+b=a+(--b)$. Jos lauseke ei ole määritelty, niin yhtäsuuruuden käyttäminen sen sisällä tuottaisi virheellisen yhtäsuuruuden. Esimerkiksi yhtäsuuruuden $x=x$ käyttäminen lausekkeen $\frac{1}{x}$ sisällä tuottaisi $x=x \Rightarrow \frac{1}{x}=\frac{1}{x}$. Se on väärin, koska kun $x=0$, siinä tuotetaan todesta lähtökohdasta $0=0$ virheellinen johtopäätös $\frac{1}{0}=\frac{1}{0}$. Koska nollalla ei saa jakaa, ei $\frac{1}{0}=\frac{1}{0}$ ole tosi.

Määrittelemättömien lausekkeiden käsittely on jossain määrin monimutkainen asia. Esimerkiksi nollalla jakaminen ja negatiivisen luvun neliöjuuri eivät ole määriteltyjä. Tässä kirjassa noudatetaan sitä matematiikan yleistä käytäntöä, että

> Jos lausekkeen osa on määrittelemätön, niin koko lauseke on määrittelemätön. Vertailu on määritelty jos ja vain jos sen molemmat puolet on määritelty. [46]

Siis esimerkiksi koska $\frac{1}{0}$ on määrittelemätön, ovat $\frac{1}{x}+1$ ja $\frac{1}{x}+1>0$ määrittelemättömiä kun $x=0$. Asiaa käsitellään perusteellisemmin luvussa **??**. Siihen saakka voit unohtaa sen muuten, mutta [46]:tta tullaan käyttämään, ja jotta et oppisi lakeja ja sääntöjä väärin, kannattaa opetella myös mitä niissä sanotaan määrittelemättömyydestä. Kannattaa muistaa muun muassa, että vaikka $0a$ on aina 0 (missä a on muuttuja), ei $0f$ ole aina 0 (missä f on lauseke). Esimerkiksi $0 \cdot \frac{1}{0}$ ei ole 0 vaan määrittelemätön.

Lähtökohdaksi annetusta laista $a-b=c \Leftrightarrow a=c+b$ saadaan $a-(-b)=c \Leftrightarrow a=c+(-b)$ sijoittamalla b:n tilalle $-b$ ja tekemättä mitään jatkokäsittelyä. (Sulkeet

$-b$:n ympärillä eivät tässä tapauksessa olisi välttämättömät. Niillä yritetään lisätä selkeyttä.) Koska lähtökohta on laki, se pätee riippumatta siitä, mikä luku on b:n tilalla. Siksi siihen saa sijoittaa b:n tilalle aina määritellyn lausekkeen, sillä aina määritelty lauseke tuottaa aina luvun. Kuten myöhemmin perustellaan, $-b$ on aina määritelty lauseke (siitä huolimatta, että sijoittamalla siihen b:n tilalle $\frac{1}{0}$ syntyy määrittelemätön lauseke $-\frac{1}{0}$).

Ilmaise (19):ssa toisen ja viimeisen $=$:n kohdalla käytetty $+$:n ja $-$:n ominaisuus lakina. Käytä muuttujana ensisijaisesti a:ta ja toissijaisesti b:tä. Johda sopivalla sijoituksella laistasi $a + (- - b) = a - (-b)$! 138

Yhtäsuuruusketjun (19) tarkkuustasolla ei tarvitsisi opetella kovin montaa lukujen lakia. Mutta päättelyihin tulisi suuri määrä yksityiskohtia, joiden seasta olisi vaikea löytää olennaiset asiat ja jotka tekisivät päättelyistä toivottoman pitkiä. Siksi käytännön päättelyissä käytetään oikoteitä. Lisäksi, vaikka (19) on melko yksityiskohtainen lukujen lakien osalta, se ei ole yksityiskohtainen logiikan lakien osalta. Kohta näemme, että jos se avataan logiikan lakien osalta, niin se pitenee huomattavasti. Siksi myös logiikan puolella tarvitaan — ja (19):ssa käytettiin — oikoteitä.

Toisinaan oikotie voidaan muotoilla selkeäksi ytimekkääksi (apu)lauseeksi, kuten [10], [11], [13], [14], [18] ja [41]. Valitettavasti tämä pätee vain osaan tärkeitä oikoteitä. Monet oikotiet opitaan ilman että niitä puetaan koskaan sanoiksi, näkemällä toisten käyttävän niitä tai huomaamalla omissa päätelmissä, että tietynlaisissa tapauksissa tulee aina tietynlainen tulos. Esimerkiksi kun riittävän monesti sijoittaa b:n tilalle $(-b)$ ja sen jälkeen poistaa tarpeettomat sulkeet, korvaa $+-$:kset $-$:lla ja $--$:kset $+$:lla, poistaa etumerkki-$+$:t ja niin edelleen, niin oppii ulkoa, mitä eri tapauksia esiintyy ja mitä niistä tulee lopputuloksiksi.

Käytännössä käytettävien sääntöjen kokoelma on siis monimutkainen ja vaikea pukea sanoiksi. Jos on epävarma mitä jossakin tilanteessa pitää tulla tulokseksi, niin on hyödyllistä kyetä tekemään sama päätelmä muilla periaatteilla. Esimerkiksi jos on epävarma, pitääkö etumerkki vaihtaa kun termi siirretään toiselle puolelle, niin asia selviää jos osaa päätellä seuraavasti:

$$\begin{aligned} 3x - 12 &= 0 && \text{lisätään molemmille puolille 12} \\ 3x - 12 + 12 &= 0 + 12 && \text{lasketaan } -12 + 12 = 0,\ 3x + 0 = 3x \text{ ja } 0 + 12 = 12 \\ 3x &= 12 \end{aligned}$$

Kovin monta kertaa tätä ei tarvitse tehdä, sillä ennen pitkää mieleen painuu, että etumerkki pitää vaihtaa. Voidakseen tehdä tämän pitää muistaa, että yhtäsuuruuden molemmille puolille saa lisätä saman luvun. Mutta alun perin on helpompi muistaa pelkästään se kuin sekä se että kun termi siirretään puolelta toiselle, niin etumerkki pitää vaihtaa.

Matemaatikot ovat tunnistaneet noin viisitoista lakia, joihin suuri osa lukusuoran lukujen ominaisuuksista on palautettavissa. (Lakien tarkka määrä riippuu siitä, miten lakikokoelma esitetään.) Tulemme käymään nämä lait läpi kuvien 35 ja 36 yhteydessä sekä luvussa 3.5. Vaikka tämä kokoelma ei yksinään riitä käytännön päättelytyöhön, se on silti hyödyllistä tuntea ja on hyödyllistä nähdä, miten erilaiset päättelyt palautuvat sen lakeihin. Matemaatikot ovat tunnistaneet noin seitsemän lakia, joihin suuri osa luonnollisten lukujen ominaisuuksista on palautettavissa. Vastaavanlaiset kokoelmat on tunnistettu monille muille matematiikan osa-alueille, kuten joukoille, vektoreille ja merkkijonoille. Samaa ajattelutapaa voi hyödyntää ohjelmoinnissa, kun määritellään tietorakenteen tuottamaa palvelua.

Teoreettiselta kannalta tällaisilla kokoelmilla on suuri merkitys. Ne tekevät mahdolliseksi tunnistaa matematiikan eri osa-alueiden välisiä yhteyksiä ja soveltaa yhdellä alueella saavutettuja tuloksia toiselle alueelle. Ne tekevät mahdolliseksi tutkia minkälaisia matemaattisia järjestelmiä ylipäänsä voi olla olemassa.

Kumpikaan edellä käytetyistä laeista $a = --a$ ja $a + -b = a - b$ ei kuulu lukusuoran lukujen peruslakien kokoelmaan. Sen sijaan $a = --a$ voidaan johtaa kokoelman laeista. Niinpä käytännön päättelemisen kannalta se on selkeäksi ytimekkääksi laiksi muotoiltu oikotie. Usein se esitetään toisinpäin eli muodossa $--a = a$, mutta tämä ei ole olennainen ero, sillä, kuten hyvin tiedetään, $=$ on symmetrinen. Seuraavassa laissa ei käytetä lukuja esittäviä muuttujia a ja b, vaan lausekkeita esittäviä symboleita f ja g syistä, jotka kerrotaan pian:

Jokaiselle lausekkeelle f ja g pätee $f = g \Leftrightarrow g = f$. [47]

Niinpä $a = --a \Leftrightarrow --a = a$.

Laki [47] on pätevä siinäkin tapauksessa, että f tai g tai molemmat olisi määrittelemättömiä. Silloin sen kumpikaan puoli ei ole tosi, mutta kuten [22] määrittelee, se on silti pätevä. Esimerkiksi $\frac{1}{x} = 2 \Leftrightarrow 2 = \frac{1}{x}$ on pätevä jokaisella x:n arvolla, 0 mukaan lukien. Muuttujien avulla muotoiltua lakia käytettäessä joudutaan tyypillisesti ensin sijoittamaan muuttujien tilalle jotakin. Muuttujien tilalle saa sijoittaa vain jokaisessa mahdollisessa tilanteessa määriteltyjä lausekkeita. (Se tarkoittaa, että lauseke on määritelty voimassa olevien pysyvien ja tilapäisten oletusten vallitessa.) Siitä varmistuminen, että ne todella on määritelty, on työvaihe, jota ei tarvita kun käytetään [47]:ää. Lisäksi muuttujien avulla muotoillusta laista $a = b \Leftrightarrow b = a$ ei voitaisi johtaa $\frac{1}{x} = 2 \Leftrightarrow 2 = \frac{1}{x}$ ilman oletusta $x \neq 0$, mutta [47]:stä voi. Nämä tekevät [47]:stä helpomman käyttää ja yleispätevämmän kuin vastaava muuttujilla ilmaistu laki olisi.

Formaalissa logiikassa ei yleensä oteta huomioon mahdollisuutta, että lauseke voisi olla määrittelemätön. Silti sielläkin [47]:ää vastaava laki muotoillaan usein lausekkeille eikä muuttujille. Tämä johtuu siitä, että päättelysäännöt pyritään muotoilemaan merkkijonojen käsittelytempuiksi, joita voi tehdä tietämättä mitään siitä, mitä merkkijonot esittävät tai tarkoittavat. Alun perin tavoitteena oli luoda matematiikalle perusta, joka ei olisi altis ihmisten välisille mielipide-eroille sen suhteen onko jokin päättely pätevä, tai ainakin jossa mielipide-erot voitaisiin palauttaa yksittäisiin selvärajaisiin kannanottoihin. Tietokoneiden keksimisen jälkeen saatiin se lisähyöty, että merkkijonojen käsittelytemppujen jonoina esitettyjä päättelyitä voidaan tarkastaa ja jopa laatia automaattisesti, ilman ihmisen apua.

Tällaisia mielipide-eroja on todella ollut, ja saattaa olla edelleenkin. Esimerkiksi norjalainen matemaatikko Thoralf Skolem (1887–1963) ei uskonut, että hänen itsensä mukaan nimetyn Löwenheim–Skolemin lauseen niin sanottu ”ylöspäin”-väite on pätevä, koska hän ei uskonut, että ylinumeroituva joukko on mielekäs käsite.

Myös $a - b = a + -b$ esitetään tyypillisesti näinpäin. Toisin kuin $--a = a$, sitä ei voi johtaa lukusuoran lukujen peruslaeista! Tämä johtuu siitä, että vaikka peruslait kertovat riittävästi siitä, mitä etumerkki-$-$ tarkoittaa, vähennyslasku-$-$:sta ne eivät kerro yhtään mitään. Sen sijaan vähennyslasku-$-$ ajatellaan *lyhenteeksi* (*abbreviation*). Ajatuksena on, että aitojen logiikan kaavojen lisäksi käytössä on toinen, ihmisille helppolukuisempi esitystapa, jonka ilmauksista saadaan aitoja logiikan kaavoja yksinkertaisilla muunnoksilla. Paremman nimen puutteessa kutsukaamme tätä esitystapaa *selkokaavoiksi* (vaikka eivät nekään aina kovin selkeitä ole). Vähennyslasku-$-$ ei esiinny aidoissa logiikan kaavoissa, mutta voi esiintyä selkokaavoissa.

Voi ajatella, että selkokaavan ilmaus $a-b$ edustaa aidon logiikan kaavan ilmausta $a+(-b)$. Tämä auttaa ymmärtämään mistä on kyse, mutta ei ole tarkkaan ottaen oikein, sillä tyypillisesti myös $a+b$ on lyhenne, ja kaikki lyhenteet auki purettuina $a+(-b)$ edustaa jotain sen kaltaista kuin $f_1^2(v_1, f_1^1(v_2))$. Näin on muun muassa siksi, että eräät logiikan keskeisimmistä tuloksista edellyttävät, että aidon logiikan kaavakieli on käsiteltävissä koneellisesti. Matematiikan tavallisista merkinnöistä ei ole helppo perustella, että ne ovat käsiteltävissä koneellisesti. Siksi aidon logiikan kaavakieli on suunniteltu erilaiseksi. Onneksi sen jälkeen, kun koneellinen käsiteltävyys on todettu, voidaan aito kaavakieli unohtaa ja siirtyä käyttämään selkokaavoja. Siksi logiikan kirjassakin voi lukea, että $a-b$ on lyhenne lausekkeesta $a+(-b)$, vaikka periaatteessa tarkoitetaankin, että se on lyhenne jostain sekavamman näköisestä.

Se, mitkä ilmaukset kuuluvat aitoihin kaavoihin ja mitkä vain selkokaavoihin, vaihtelee eri lähteissä. Esimerkiksi $\varphi \vee \psi$ saattaa kuulua aitoihin kaavoihin tai olla lyhenne kaavalle $\neg(\neg\varphi \wedge \neg\psi)$. (Tarkemmin sanoen, se mikä saadaan laittamalla φ:n ja ψ:n tilalle kaavat ilmauksessa $\varphi \vee \psi$, saattaa kuulua aitoihin kaavoihin tai olla lyhenne sille kaavalle, joka saadaan laittamalla edellä mainitut kaavat φ:n ja ψ:n tilalle ilmauksessa $\neg(\neg\varphi \wedge \neg\psi)$. Kuten sivulla 6 kerrottiin, φ:tä ja niin edelleen sisältävät kaavoilta näyttävät ilmaukset eivät ole kaavoja vaan kaavaskeemoja.)

Tästä kenties sekavalta vaikuttavasta aiheesta riittää tietää kaksi asiaa. Pitää tietää mitä ”lyhenne” tarkoittaa, jotta ymmärtää sen kun se tulee tekstissä vastaan, ja jotta ymmärtää miksi osa käytännössä tärkeistä merkinnöistä puuttuu peruslaeista. Jokaisesta käytännössä tärkeästä lyhenteestä pitää tietää, miten se puretaan auki johonkin muotoon. Kuitenkaan varsinkaan käytännön sovelluksissa ei yleensä tarvitse muistaa, että se on lyhenne. Käytännön päättelyssä ei ole olennaista tehdä eroa selkokaavojen ja aitojen kaavojen välille. Siksi käytännön päättelyn kannalta ei ole väliä esimerkiksi sillä, onko vähennyslasku-— käytössä vain selkokaavoissa vai myös aidoissa kaavoissa, ja onko $a-b=a+(-b)$ lyhenteen purkuohje vai lukuja koskeva laki. Tulkitaanpa se kummalla tavalla tahansa, se on käytännössä tärkeä ja sitä voi käyttää kuten lakia.

Jokaiselle luvulle a ja b pätee $a-b \;=\; a+-b$. [48]

Lukusuoran lukujen, merkkijonojen ja niin edelleen lakikokoelmista erillisenä asiana myös loogiselle päättelylle on omia lakikokoelmiaan. Valtaosa matemaattisesta päättelystä perustuu viime kädessä niin sanottuun ensimmäisen kertaluvun predikaattilogiikkaan, joko suoraan tai siten, että päättely perustuu joukko-oppiin, joka puolestaan käyttää ensimmäisen kertaluvun predikaattilogiikkaa. Siksi ensimmäisen kertaluvun predikaattilogiikka tulee olemaan keskeisessä asemassa tämän kirjan loppuosassa. Yksi syy ensimmäisen kertaluvun predikaattilogiikan suosioon on se, että sille on useita erilaisia *eheitä* (*sound*) *täydellisiä* (*complete*) päättelyjärjestelmiä. Eheys tarkoittaa, että päättelyjärjestelmä ei voi tuottaa tosista lähtökohdista epätosia johtopäätöksiä. Täydellisyys tarkoittaa, että kaikki mikä vääjäämättä seuraa päättelyn lähtökohdista, on myös todistettavissa.

Kun edellä yhtäpitävyydestä $a-b=c \Leftrightarrow a=c+b$ johdettiin $a+b=c \Leftrightarrow a=c-b$, niin lukujen lakien käyttö esitettiin melko yksityiskohtaisesti, mutta logiikan lakien käyttö esitettiin rutinoituneen päättelijän oikoteitä käyttäen. Niin on tarkoituksenmukaista, sillä, kuten edellä vihjattiin, ilman oikoteitä päättelyyn tulisi paljon yksityiskohtia. Kuten lukusuoran lukujen lakienkin tapauksessa, vaikka käytännön päättely perustuu oikoteihin, on hyödyllistä tarvittaessa osata käyttää myös päättelyn peruslakeja, jos vaikka on epävarma muistaako oikotien oikein.

$$
\begin{array}{rcl}
1 & & a+b=c \\
2 & \Leftrightarrow & a-(-b)=a+(--b)\land a+(--b)=a+b\land a+b=c \\
3 & \Leftrightarrow & a+b=a+(--b)\land a+(--b)=a-(-b)\land a-(-b)=c \\
4 & \Leftrightarrow & a-(-b)=c \\
5 & \Leftrightarrow & a=c+(-b) \\
6 & \Leftrightarrow & a=c+(-b)\land c+(-b)=c-b \\
7 & \Leftrightarrow & a=c-b\land c-b=c+(-b) \\
8 & \Leftrightarrow & a=c-b
\end{array}
$$

Kuva 30: Päättelyn (19) päävaiheet jonkin verran avattuina

Kun $n \geq 3$, on $f_1 = f_2 = \ldots = f_n$ lyhenne kaavalle $f_1 = f_2 \land \ldots \land f_{n-1} = f_n$. Siksi $a+b=a+(--b)=a-(-b)=c$ on lyhenne kaavalle $a+b=a+(--b)\land a+(--b)=a-(-b)\land a-(-b)=c$, ja $a=c+(-b)=c-b$ kaavalle $a=c+(-b)\land c+(-b)=c-b$. Tämän tietäen (19):n päävaiheet (mutta ei kaikkia yksityiskohtia) voidaan esittää kuten kuvassa 30.

Tämän päättelyn yksityiskohtien ymmärtäminen helpottuu, jos jätämme rivit 2, 3 ja 4 viimeisiksi. Kuten todettiin pian (19):n jälkeen, sijoittamalla $-b$ lausekkeen b tilalle lähtökohdaksi annettuun lakiin $a-b=c \Leftrightarrow a=c+b$ saadaan $a-(-b)=c \Leftrightarrow a=c+(-b)$. Sillä päästään riviltä 4 riville 5. Sen varmistamiseksi, että ei tapahdu samankaltaista virhettä kuin edellä esimerkissä $1-b^2$, on $-b$:n ympärille laitettu sulkeet. Sulkeiden laittaminen sijoitettavan lausekkeen ympärille ei ole koskaan väärin, mutta niiden pois jättäminen on toisinaan väärin. Niinpä sulkeet kannattaa laittaa, jollei ole varma, että niitä ei tarvita. (Tässä tapauksessa niitä ei olisi tarvittu.)

Koska $c+(-b)=c-b$ on aina tosi, on $a=c+(-b)\land c+(-b)=c-b$ tosi täsmälleen niissä mahdollisissa tilanteissa, joissa $a=c+(-b)$ on tosi. Niinpä [22]:n mukaan rivien 5 ja 6 välinen yhtäpitävyys on pätevä. Tällainen päättely vetoaa kaavojen merkitykseen eikä päättelysääntöihin. Päättelysääntöjä käyttämällä rivi 6 saadaan rivistä 5 yhtäpitävyydellä $\varphi \Leftrightarrow \varphi \land \mathsf{T}$. Käytännön päättelytyössä saa käyttää kumpaa tahansa tapaa. Yhtäpitävyyden $\varphi \Leftrightarrow \varphi \land \mathsf{T}$ saa olettaa tunnetuksi. Jos haluaa johtaa sen edellä olleista numeroiduista laeista, niin sen saa [25]:lla ja [24]:lla siitä, että $\varphi \land \mathsf{T} \Leftrightarrow \mathsf{T} \land \varphi \Leftrightarrow \varphi$ [2].

Kun aiemmin puhuttiin transitiivisuudesta, niin kenties huomasit tai tiesit entuudestaan, että myös $=$ on transitiivinen. Tämäkin laki kannattaa muotoilla lausekkeille eikä muuttujille:

Jokaiselle lausekkeelle f, g ja h pätee $\; f=g\land g=h \;\Rightarrow\; f=h\,.$ [49]

Soveltamalla sitä riviin 6 saadaan $a=c-b$. Rivistä 6 voidaan poimia $c+(-b)=c-b$ [33]:lla ja kääntää se takaperin $=$:n symmetrisyydellä [47]. Näin saadut kaksi kaavaa voidaan yhdistää rivin 7 kaavaksi [34]:llä. Olemme perusteelleet, että rivin 6 kaava $\Rightarrow$ rivin 7 kaava.

Perustele, että rivin 7 kaava $\Rightarrow$ rivin 6 kaava! 139

Nyt kun molemmat suunnat on perusteltu, rivien 6 ja 7 välille voi kirjoittaa $\Leftrightarrow$ [32]. Koska $c-b=c+(-b)$ on aina tosi, rivi 8 saadaan [2]:lla ja [25]:lla.

Rivit 2, 3 ja 4 voidaan perustella samaan tapaan kuin 6, 7 ja 8 siitä, että sekä $a-(-b)=a+(--b)$ että $a+(--b)=a+b$ on aina tosi. Jälkimmäinen seuraa tietenkin lukujen laista $--b=b$. Mutta jotta emme joutuisi pohtimaan liian montaa logiikan peruslakia yhtäaikaa, lykkäämme sen selittämisen tehtäväksi 147.

Rivien 2, 3 ja 4 perustelemisessa joudutaan kummassakin suunnassa käyttämään [49]:ä kahdesti. Se lisää myös [33]:n ja [34]:n käyttöä. Käytännön päättelytyössä ei

$$
\begin{array}{rcl}
1 & & a+b=c \\
2 & \Leftrightarrow & a+(--b)=c \\
3 & \Leftrightarrow & a-(-b)=c \\
4 & \Leftrightarrow & a=c+(-b) \\
5 & \Leftrightarrow & a=c-b
\end{array}
$$

Kuva 31: Päättely $a+b=c \Leftrightarrow a=c-b$ lyhyesti logiikan laeilla

kuitenkaan kannata käsitellä yhtäsuuruusketjua käyttämällä [49]:ä monesti, vaan on selvää, että voi ja kannattaa hypätä ketjun alusta suoraan ketjun loppuun seuraavan oikotien mukaisesti:

$$\text{Jos } n \geq 2 \text{ ja } f_1, \ldots, f_n \text{ ovat lausekkeita, niin } f_1 = f_2 = \ldots = f_n \;\Rightarrow\; f_1 = f_n\,. \qquad [50]$$

Kuten [47], myös [49] ja [50] ovat päteviä siinäkin tapauksessa, että yksi tai useampi niiden lausekkeista olisi määrittelemätön. Jos f, g tai h on määrittelemätön, niin $f=g$, $g=h$ tai kumpikaan ei ole tosi. Silloin [49]:n vasen puoli ei ole tosi, joten [19] ei vaadi sen oikeankaan puolen olevan tosi, joten ei ole väliä onko oikea puoli määritelty. Vastaava pätee [50]:lle.

Lait [47], [49] ja [50] ovat yleisiä logiikan lakeja, jotka koskevat muitakin puheenaiheita kuin lukuja. Niiden f, g, h ja $f_1, \ldots, f_n$ voivat edustaa vaikka merkkijonoja.

Juuri läpikäydyn päättelyn monimutkaisuus johtuu osittain siitä, että se pyrki noudattamaan (19):n rakennetta. Jos tästä tavoitteesta luovutaan, niin todistus voidaan esittää logiikan peruslakeja käyttäen melko lyhyesti, vaikka ei aivan yhtä helppolukuisesti. Se on kuvassa 31.

Aluksi käytetään aiemminkin mainittua tosiasiaa, että kun luku sijoitetaan kaavaan, lopputuloksen totuusarvo voi riippua vain sijoitetun luvun lukuarvosta, ei sen esitysmuodosta. Esitämme laista ensin yksinkertaistetun version, ja annamme numeron vasta lopulliselle versiolle.

> Jos $\forall$ ja $\exists$ eivät esiinny $\varphi(x)$:ssä ja jos jokaisessa mahdollisessa tilanteessa $f=g$, niin $\varphi(f) \Leftrightarrow \varphi(g)$.

Lakia sovellettaessa f ja g voivat olla hyvinkin erinäköiset, vaikka $3x-8$ ja 4. Jos voimassa olevat pysyvät ja tilapäiset oletukset sallivat muuttujien saada sellaisen arvojen yhdistelmän, että $f \neq g$, niin on olemassa mahdollinen tilanne jossa $f=g$ ei ole tosi, joten lain jos-osa ei ole tosi eikä lakia voi käyttää. Yksinkertaistetussa versiossamme käy samoin myös jos oletukset sallivat f:n tai g:n olla määrittelemätön. Muussa tapauksessa jokaisessa mahdollisessa tilanteessa f ja g todellakin esittävät samaa lukuarvoa erinäköisyydestään huolimatta.

Rivien 1 ja 2 yhtäpitävyys saadaan valitsemalla $\varphi(x)$:ksi $a+x=c$, f:ksi b ja g:ksi $--b$. Koska $b=--b$ on lukusuoran lukujen laki, se pätee jokaisessa mahdollisessa tilanteessa. Näillä valinnoilla uusi lakimme tuottaa $a+b=c \Leftrightarrow a+(--b)=c$.

Sitten valitsemme $\varphi(x)$:ksi $x=c$ ja hyödynnämme yhtäsuuruutta $a+(--b)=a-(-b)$, joka pätee jokaisessa mahdollisessa tilanteessa, koska se saadaan laista $a+(-b)=a-b$ sijoittamalla b:n tilalle $-b$. Niin saamme $a+(--b)=c \Leftrightarrow a-(-b)=c$, joten rivi 3 on perusteltu. Mikä tässä päättelyssä oli lakimme f ja mikä oli g? 140

Rivi 4 saadaan rivistä 3 sijoittamalla b:n tilalle $-b$ alun perin lähtökohdaksi annettuun yhtäpitävyyteen $a-b=c \Leftrightarrow a=c+b$. Kuten tähänkin asti, siten saadaan $a-(-b)=c \Leftrightarrow a=c+(-b)$.

Johda rivien 4 ja 5 yhtäpitävyys! 141

Lopullinen tavoite on rivien 1 ja 5 yhtäpitävyys. Se seuraa [25]:lla.

Lakimme ei ole rajoittunut pelkästään lukuihin, vaan on yleispätevä periaate logiikassa. Tässä alaluvussa f ja g tuottavat (tarkemmin sanoen, f:n ja g:n edustamat lausekkeet tuottavat) tuloksikseen lukuja, mutta lakimme sallii niiden tuottavan mitä tahansa mistä kulloinkin on puhe.

Päättelyaskeleen $a+b=c \Leftrightarrow a+(--b)=c$ rakenne voidaan ilmaista merkintöjä venyttämällä seuraavasti. Koska valintojemme ja sen, että $b=--b$, ansiosta $f=b=--b=g$, ja koska $\varphi(x)$ on $a+x=c$, tuottavat valintamme ja lakimme $a+b=c \Leftrightarrow \varphi(b) \Leftrightarrow \varphi(f) \Leftrightarrow \varphi(g) \Leftrightarrow \varphi(--b) \Leftrightarrow a+(--b)=c$. Tämä on merkintöjen venyttämistä siksi, että lakimme ja hyvin monet muutkin säännöt logiikassa ovat itse asiassa sääntöskeemoja. Vaikka lakimme f:ää ja g:tä saatetaan sanoa lausekkeiksi, ne eivät ole vaan edustavat lausekkeita. Samoin φ ei ole kaava, vaan se edustaa jotain kaavaa riippuen siitä, mitä sen perässä on sulkeissa. Niinpä lakimme sovelluksissa ei ole f:ää, g:tä ja φ:tä, vaan niiden tilalla on ne mitä ne edustavat.

Tästä syystä esimerkiksi $--b=g$ ei edellä tarkoita että g on yhtäsuuri kuin $--b$, vaan muistuttaa siitä, että g edustaa lauseketta $--b$. Se, mikä edellä esitettiin $--b=g$, on formaalin logiikan näkökulmasta $--b=--b$. Näin on siksi, että formaalin logiikan kaavoissa ei ole g:tä vaan se mitä g edustaa, joka on tässä tapauksessa $--b$. Samoin siellä ei ole $\varphi(--b)$:tä vaan se mitä $\varphi(--b)$ edustaa ja niin edelleen. Mikään jossa lakimme f, g tai φ esiintyy kirjaimellisesti ei ole logiikan ilmaus, vaan edustaa logiikan ilmausta. Niinpä $a+b=c \Leftrightarrow \varphi(b) \Leftrightarrow \varphi(f) \Leftrightarrow \varphi(g) \Leftrightarrow \varphi(--b) \Leftrightarrow a+(--b)=c$ on formaalin logiikan näkökulmasta $a+b=c \Leftrightarrow a+b=c \Leftrightarrow a+b=c \Leftrightarrow a+(--b)=c \Leftrightarrow a+(--b)=c \Leftrightarrow a+(--b)=c$. Formaalin logiikan näkökulmasta lakimme on ääretön kokoelma päättelysääntöjä, joista yksi on ”jos jokaisessa mahdollisessa tilanteessa $b=--b$, niin $a+b=c \Leftrightarrow a+(--b)=c$”. Kaikki muu venytetyssä merkinnässämme kertoo siitä, että tästä kokoelmasta valittiin juuri tämä konkreettinen päättelysääntö.

Jos f ja g olisivat muuttujia eivätkä lauseketta edustavia symboleita, niin valitsemalla $\varphi(x)$:ksi $a+x=c$ saataisiin laistamme vain yksi konkreettinen päättelysääntö, nimittäin ”jos $f=g$, niin $a+f=c \Leftrightarrow a+g=c$”. Siinä f ja g olisivat kirjaimellisesti f ja g, eivätkä jotain, jonka tilalle voisi laittaa eri lausekkeita. Koska ne olisivat muuttujia, niille voisi antaa eri lukuarvoja, mutta se on eri asia kuin niiden korvaaminen eri lausekkeilla. Sellainen laki ei antaisi lupaa päätellä $\varphi(b) \Leftrightarrow \varphi(f)$ eikä $\varphi(g) \Leftrightarrow \varphi(--b)$, eikä niin ollen pystyisi hoitamaan sitä tehtävää, joka sillä on päättelyjärjestelmässämme.

Jos ajattelutapa $a+b=c \Leftrightarrow \varphi(b) \Leftrightarrow \varphi(f) \Leftrightarrow \varphi(g) \Leftrightarrow \varphi(--b) \Leftrightarrow a+(--b)=c$ auttaa soveltamaan lakiamme oikein, niin kyllä niin saa ajatella, vaikka se onkin merkintöjen venyttämistä.

Lakimme ilmaisemiseksi tarvitaan jokin muuttuja. Edellä se oli x. Jos samanniminen muuttuja on jo muussa tehtävässä, niin voi syntyä sekaannusta. Esimerkiksi yhtäsuuruudesta $3-3=0$ pitäisi voida johtaa $x+(3-3)=5 \Leftrightarrow x+0=5$. Se ei onnistu valitsemalla lakimme f:ksi $3-3$, g:ksi 0 ja $\varphi(x)$:ksi $x+x=5$, koska siten $\varphi(3-3)$:sta ja $\varphi(0)$:sta tulisi $(3-3)+(3-3)=5$ ja $0+0=5$, ja johtopäätökseksi tulisi $(3-3)+(3-3)=5 \Leftrightarrow 0+0=5$ eikä $x+(3-3)=5 \Leftrightarrow x+0=5$. Näin kävisi, koska x:ää käytettiin kahdessa eri merkityksessä, jotka menivät sekaisin: muuttujana jonka oli tarkoitus esiintyä sijoituksien $\varphi(f)$ ja $\varphi(g)$ lopputuloksissa $x+(3-3)=5$ ja $x+0=5$, sekä symbolina jonka tilalle f ja g eli $3-3$ ja 0 sijoitettiin.

Tämä ongelma on matematiikassa yleinen. Onneksi ei ole olennaista, minkänimisiä ovat ne laeissa käytettävät symbolit, joiden tilalle lakeja käytettäessä laitetaan jotakin. Siksi lakiamme käytettäessä x:n tilalla saa käyttää mitä tahansa muuttujaa, joka ei aiheuta sekaannusta. Niinpä valitsemalla lakimme f:ksi $3-3$, g:ksi 0 ja $\varphi(a)$:ksi $x+a=5$ saadaan $x+(3-3)=5 \Leftrightarrow x+0=5$, kuten pitääkin.

Edellä käytetty tapa ilmaista valintamme ei saa niitä erottumaan tekstistä kovin hyvin. Siksi sallimme ilmaista ne myös näin: $f := 3-3$, $g := 0$ ja $\varphi(a) :\Leftrightarrow x+a=5$. Symbolit $:\Leftrightarrow$ ja $:=$ tarkoittavat ”saa merkityksekseen”. Ensimmäistä käytetään kaavoista ja jälkimmäistä lausekkeista. Millä valinnoilla yhtäsuuruudesta $8-3=5$ saadaan
$(x+3)-3=8-3 \Leftrightarrow (x+3)-3=5$? Millä valinnoilla yhtäsuuruudesta $x=2a-3$ 142
saadaan $3a-2x=2 \Leftrightarrow 3a-2(2a-3)=2$? 143

On tärkeää muistaa, että lakimme on yksisuuntainen: siitä, että $\varphi(f) \Leftrightarrow \varphi(g)$, ei välttämättä seuraa, että $f=g$. Keksi mahdollisimman yksinkertainen esimerkki, jossa
$\varphi(f) \Leftrightarrow \varphi(g)$ pätee aina, mutta $f=g$ ei koskaan! 144

Jos f tai g on määrittelemätön jossakin mahdollisessa tilanteessa, niin lakimme jos-osa ei ole tosi, joten [19] ei rikkoudu vaikka niin-osakaan ei olisi tosi. Niinpä lakimme on myös määrittelemättömille lausekkeille pätevä (eli ei tuota väärää johtopäätöstä), mutta samalla hyödytön (eli ei tuota mitään johtopäätöstä). Luvussa 8 esitettävästä teoriasta voidaan johtaa, että jos sekä f että g on määrittelemätön, niin $\varphi(f)$ ja $\varphi(g)$ tuottavat saman totuusarvon. Tämä tarjoaa mahdollisuuden lieventää lakimme jos-osan ehtoa. Se tekee laistamme hyödyllisen entistä useammassa tapauksessa. Lisäksi lain tuottamaan johtopäätökseen voidaan lisätä uusi tieto. Sekin lisää laistamme saatavaa hyötyä.

> Jos $\forall$ ja $\exists$ eivät esiinny $\varphi(x)$:ssä ja jos jokaisessa mahdollisessa tilanteessa $f=g$ tai sekä f että g on määrittelemätön, niin $\varphi(f) \Leftrightarrow \varphi(g)$ ja $\varphi(f)$ ja $\varphi(g)$ ovat yhtäaikaa määritellyt. [51]

Tällekin laille pätee asia, jonka olemme maininneet jo monesti: se kieltää käyttämästä φ:ssä $\forall$:a ja $\exists$:a, mutta kyllä niitä saa käyttää, kunhan noudattaa sivulla 99 mainittua ehtoa, joka on liian monimutkainen nyt käsiteltäväksi.

Vaikka joudumme jättämään yksityiskohdat lukuun 8, voidaan perussyy siihen, miksi lakimme laajennos on pätevä, ymmärtää jo nyt. Ensin pitää puhua hitunen kaavojen rakenteesta. Tämän alaluvun logiikan *atomikaavoja* ovat F, T sekä ilmaukset muotoa $f=g$, $f \neq g$ ja (atomikaava) eli sulkeisiin pantu atomikaava. Myöhemmin tässä luvussa atomikaavoihin lisätään $f<g$ ja niin edelleen. Yhdistetyt kaavat muodostetaan atomikaavoista kuten propositiologiikassa eli kuvan 24 mukaisesti.

Yhteenlaskun tuottama luku ei riipu siitä, millä tavalla yhteenlaskettavat luvut on tuotettu, vaan ainoastaan yhteenlaskettavien lukujen lukuarvoista. Vaikka f ja g olisivat miten erilaiset tahansa, niin jos f tuottaa saman luvun kuin g, niin $f+2$ tuottaa saman luvun kuin $g+2$. Sama pätee muihinkin laskutoimituksiin. Se yleistyy rakenteellisella induktiolla kaikkiin määriteltyihin lausekkeisiin: jos $f=g$ niin $f+2=g+2$, koska $f+2=g+2$ niin $3(f+2)=3(g+2)$ ja niin edelleen. Vastaava pätee vertailuihin kuten $\leq$ sekä konnektiiveihin ja kvanttoreihin kuten $\wedge$ ja $\forall$, mutta niissä tuotoksena on totuusarvo.

Luvussa 8 tämä periaate laajennetaan määrittelemättömiin lausekkeisiin. Toisin sanoen, vaikka f ja g olisivat erilaiset, niin f:n tuottama määrittelemätön katsotaan laskutoimituksissa ja vertailuissa täysin samanveroiseksi kuin g:n tuottama määrittelemätön. Siksi jos $f=g$ tai sekä f että g on määrittelemätön, niin kukin $\varphi(f)$:n atomikaava tuottaa saman totuusarvon kuin vastaava $\varphi(g)$:n atomikaava. Niinpä esimerkiksi

$3(f+2) \geq 4$ tuottaa saman kolmiarvoisen logiikan totuusarvon kuin $3(g+2) \geq 4$ sekä silloin kun $f = g$, että silloin kun sekä f että g on määrittelemätön.

Tästä *ei* seuraa, että kun sekä f että g ovat määrittelemättömät niin $f = g$, vaan muun muassa, että kun f ja g ovat määrittelemättömät niin $f = f$ ja $g = f$ tuottavat saman totuusarvon. Kuten [46] sanoo, kun f tai g tai molemmat on määrittelemätön, niin jokainen vertailu $f < g$, $f = g$ ja niin edelleen on määrittelemätön. Luvussa 8 se esitetään totuusarvolla U eli *määrittelemätön* (*undefined*).

Konnektiivien ja kvanttorien määritelmistä seuraa, että kaavojen $\neg\psi$, $\psi \wedge \chi$, $\forall x : \psi$ ja niin edelleen totuusarvot riippuvat vain ψ:n ja χ:n totuusarvoista, eli millään muilla ψ:n ja χ:n ominaisuuksilla ei ole vaikutusta. Siitä seuraa rakenteellisella induktiolla, että kaavan totuusarvo riippuu vain sen atomikaavojen totuusarvoista ja kaavan rakenteesta. Siksi jos $f = g$ tai sekä f että g on määrittelemätön, niin kukin $\varphi(f)$:n atomikaava tuottaa saman totuusarvon kuin vastaava $\varphi(g)$:n atomikaava, ja siksi $\varphi(f)$ tuottaa saman totuusarvon kuin $\varphi(g)$. Esimerkiksi vaikka $x^3 \neq x$ kaikilla muilla x:n arvoilla paitsi -1, 0 ja 1, silti $\frac{1}{x^3} = 1 \Leftrightarrow \frac{1}{x} = 1$. Jos $x = 1$, niin sen molemmat puolet tuottavat T. Jos $x = 0$, niin sen molemmat puolet tuottavat U. Muilla x:n arvoilla sen molemmat puolet tuottavat F.

Tästä seuraa, että lakia $a + 0 = a$ ja monia muita yhtäsuuruuksina esitettyjä lakeja voi käyttää [51]:ssä murehtimatta, onko muuttujan tilalle tuleva lauseke määritelty vai ei. Kun johdetaan esimerkiksi $\frac{1}{x} + 0 = x - 1 \Leftrightarrow \frac{1}{x} = x - 1$, niin tapausta $x = 0$ ei tarvitse käsitellä erikseen, vaikka lakiin $a + 0 = a$ ei saa sijoittaa a:ksi $\frac{1}{0}$. Kun $x \neq 0$, niin [51]:n jos-osasta toteutuu $f = g$, ja kun $x = 0$, niin siitä toteutuu se, että sekä f että g on määrittelemätön. Tämä ylellisyys koskee jokaista yhtäsuuruutena esitettyä lakia, jonka molemmilla puolilla esiintyvät samat muuttujat. Se ei koske esimerkiksi lakia $0 = a - a$, koska a esiintyy siinä vain toisella puolella. Muutoinhan voitaisiin "todistaa" $\frac{1}{0} - \frac{1}{0} = 0$ valitsemalla $\varphi(x)$:ksi $x = 0$ ja päättelemällä $\mathsf{T} \Leftrightarrow 0 = 0 \Leftrightarrow \frac{1}{0} - \frac{1}{0} = 0$.

Koska $\psi \Leftrightarrow \chi$ vaatii vain, että joko molemmat puolet tai ei kumpikaan puoli on tosi [22], se sallii sekä sen, että molemmilta puolilta tulee sama totuusarvo, että sen, että toiselta puolelta tulee F ja toiselta U. Niinpä $\psi \Leftrightarrow \chi$ ei sisällä kaikkea sitä, mikä voidaan luvata, kun [51]:n jos-osa pätee. Lisätieto, että ei voi olla niin että toiselta puolelta tulee F ja toiselta U, saadaan sanomalla, että $\varphi(f)$ ja $\varphi(g)$ ovat yhtäaikaa määritellyt. Näin ilmaistuna tieto on käytettävissä matematiikan normaalissa käytännössä, jossa ei puhuta kolmannesta totuusarvosta U mutta puhutaan siitä, että jokin on tai ei ole määritelty.

Loogisen päättelemisen tärkein tehtävä on tuottaa tosista lähtökohdista tosia johtopäätöksiä. Jos jokin kaava ei jossakin tilanteessa ole tosi, niin pääsääntöisesti ei ole olennaista, onko se epätosi vai määrittelemätön. Se muuttuu olennaiseksi, kun yhtäpitävyyttä käytetään isomman kaavan sisällä, jossa esiintyy muitakin konnektiiveja kuin $\wedge$ ja $\vee$. Esimerkiksi $x \neq 0 \Leftrightarrow \frac{1}{x} \neq 0$ on pätevä. Sijoittamalla sen kumpikin puoli X:n tilalle kaavaan $\neg X$ saataisiin $\neg(x \neq 0) \Leftrightarrow \neg\left(\frac{1}{x} \neq 0\right)$. Koska $f \neq g \Leftrightarrow \neg(f = g)$ riippumatta siitä, ovatko f ja g määritellyt, saataisiin $x = 0 \Leftrightarrow \neg\neg(x = 0) \Leftrightarrow \neg(x \neq 0) \Leftrightarrow \neg\left(\frac{1}{x} \neq 0\right) \Leftrightarrow \neg\neg\left(\frac{1}{x} = 0\right) \Leftrightarrow \frac{1}{x} = 0$. Siitä $\Leftrightarrow$:n transitiivisuus tuottaisi $x = 0 \Leftrightarrow \frac{1}{x} = 0$. Sijoittamalla x:ksi 0 saataisiin $\frac{1}{0} = 0$.

Tästä syystä [28]:n jos-osa vaatii ei pelkästään $\psi \Leftrightarrow \chi$, vaan myös että ψ ja χ ovat yhtäaikaa määritellyt. Yhdessä ne takaavat, että ψ:llä on aina sama kolmiarvoisen logiikan totuusarvo kuin χ:llä. Kuten edellä, siitä seuraa rakenteellisella induktiolla, että $\varphi(\psi)$:llä on aina sama kolmiarvoisen logiikan totuusarvo kuin $\varphi(\chi)$:llä.

Niinpä, vaikka päättelyn lopputuloksessa ei olisikaan olennaista erottaa epätotta ja määrittelemätöntä toisistaan, se saattaa olla tarpeen välivaiheessa, jotta voitaisiin käyt-

tää lakia, jonka jos-osa vaatii niitten erottamista. Sellaisia lakeja ovat [28]:n lisäksi ainakin [11], [39] ja [40]. Siksi joihinkin lakeihin, jotka tuottavat muotoa $\psi \Leftrightarrow \chi$ olevan johtopäätöksen, on tässä kirjassa lisätty johtopäätökseen maininta, että ψ ja χ ovat yhtäaikaa määritellyt. Selkeyden vuoksi maininta on kuitenkin jätetty pois sellaisista laeista kuten [5], joissa ei lue mitään muuta kuin kaksi kaavaa ja niiden välissä $\Leftrightarrow$.
Miksi tämä ei koskaan tee niistä virheellisiä? Se vähentää niiden hyödyllisyyttä kol- 145
miarvoisen logiikan päättelyissä, mutta ennen lukua 8 siitä aiheutuu haittaa vain vähän, ja luvussa 8 asia käsitellään uudelleen.

Edellä yhtälön $3x - 12 = 0$ ratkaisemisen ensimmäinen päättelyaskel oli $3x - 12 = 0 \Leftrightarrow 3x = 12$. Totesimme, että tämä askel voidaan johtaa laista $a - b = 0 \Leftrightarrow a = b$ tai hieman yleisemmästä laista $a - b = c \Leftrightarrow a = c + b$. Kumpikin on kuitenkin seuraus vielä yleisemmistä periaatteista, joihin tutustumme seuraavaksi.

Jos x:llä on sellainen arvo, että $3x - 12$ ja 0 tuottavat saman luvun, niin myös $(3x - 12) + 12$ ja $0 + 12$ tuottavat saman luvun, koska kumpikin niistä lisää 12 samaan lukuun. Tämän voi ilmaista $3x - 12 = 0 \Rightarrow (3x - 12) + 12 = 0 + 12$. Sama ajatus tietysti pätee mille tahansa kahdelle lausekkeelle f ja g: jos ne tuottavat saman luvun, niin myös $f + 12$ ja $g + 12$ tuottavat saman luvun. Siis $f = g \Rightarrow f + 12 = g + 12$. Yleisemmin, kun samoille luvuille tehdään samat laskutoimitukset, niin saadaan samat tulokset. Esimerkiksi $f = g \Rightarrow 1 - 5f = 1 - 5g$ ja $f = g \Rightarrow (f + 6)^2 = (g + 6)^2$. Ei kuitenkaan päde $f = g \Rightarrow \frac{f}{0} = \frac{g}{0}$, koska nollalla ei saa jakaa.

Merkitsemme $h(a)$:lla sitä lauseketta, jonka osaksi f ja g sijoitetaan. (Jos a on jo varattu muuhun käyttöön, tai vaikka ei olisikaan, niin sen tilalla saa käyttää muuta muuttujaa.) Edellä olleissa esimerkeissä $h(a)$ oli $a + 12$, $1 - 5a$, $(a + 6)^2$ ja $\frac{a}{0}$. Jotta $h(f) = h(g)$ voisi olla tosi, täytyy $h(f)$:n ja $h(g)$:n olla määritellyt. (Kuten [46] sanoo, mikään vertailu, jonka toinen tai molemmat osapuolet on määrittelemätön, ei ole tosi. Se ei ole myöskään epätosi, vaan määrittelemätön.) Riittää vaatia, että $h(f)$ on määritelty, koska kun g tuottaa saman luvun kuin f, tuottaa $h(g)$ saman tuloksen kuin $h(f)$.

Jos $h(f)$ on määritelty ja $f = g$, niin $h(f) = h(g)$. [52]

Jos $h(x)$ on aina määritelty, niin laki lyhenee muotoon

$$f = g \;\Rightarrow\; h(f) = h(g) \; .$$

On tärkeää muistaa, että tämä laki on yksisuuntainen. Se ei lupaa $f = g \Leftrightarrow h(f) = h(g)$. Jos valitaan f:ksi x, g:ksi -2 ja $h(a)$:ksi ax, niin kaksisuuntaisena laki tuottaisi $x = -2 \Leftrightarrow xx = -2x$. Se ei ole oikein, koska kun $x = 0$ niin $x = -2$ on epätosi vaikka $xx = -2x$ on tosi, sillä $0 \cdot 0 = -2 \cdot 0 = 0$.

Kuten totesimme, jos f on $3x - 12$, g on 0 ja $h(a)$ on $a + 12$, niin [52] tuottaa $3x - 12 = 0 \Rightarrow (3x - 12) + 12 = 0 + 12$. Tutuilla lukujen laeilla saadaan $(3x - 12) + 12 = 3x$ ja $0 + 12 = 12$, joten $3x - 12 = 0 \Rightarrow (3x - 12) + 12 = 0 + 12 \Leftrightarrow 3x = 12$.

Osoita [52]:lla $3x = 12 \Rightarrow x = 4$! 146

Johda $a + (--b) = a + b$ [52]:lla laista $--b = b$! 147

Oletamme, että $|x| - 1 \geq 0$. Osoita [52]:lla $3\sqrt{|x| - 1} = x + 1 \Rightarrow 9|x| = x^2 + 2x + 10$! 148

Koska [52] on yksisuuntainen, emme ole vielä osoittaneet $3x - 12 = 0 \Leftrightarrow 3x = 12$ vaan vasta $3x - 12 = 0 \Rightarrow 3x = 12$. Vielä täytyy osoittaa $3x = 12 \Rightarrow 3x - 12 = 0$. Sekin onnistuu [52]:lla: valitaan f:ksi $3x$, g:ksi 12 ja $h(a)$:ksi $a - 12$. Siten saadaan $3x = 12 \Rightarrow 3x - 12 = 12 - 12 \Leftrightarrow 3x - 12 = 0$.

Viimeistele väitteen $3x - 12 = 0 \Leftrightarrow x = 4$ todistus! 149

$$
\begin{array}{llcl}
1 & a+b=c & \Rightarrow & (a+b)+(-b)=c+(-b) \\
2 & & \Leftrightarrow & a=c+(-b) \\
3 & & \Leftrightarrow & a=c-b \\
4 & a+b=c & \Rightarrow & a=c-b \\
5 & a=c-b & \Rightarrow & a+b=(c-b)+b \\
6 & & \Leftrightarrow & a+b=c \\
7 & a=c-b & \Rightarrow & a+b=c \\
8 & a+b=c & \Leftrightarrow & a=c-b
\end{array}
$$

Kuva 32: Liittyy tehtävään 150

Kuvassa 32 on johdettu $a+b=c \Leftrightarrow a=c-b$ vetoamatta muihin lukujen yhtäpitävyyksiin mutta olettaen kaikki lukujen yhtäsuuruudet tunnetuiksi. Kerro mitä logiikan lakeja ja miten kullakin rivillä on käytetty! 150

Olemme tässä alaluvussa tähän mennessä todenneet, että päätteleminen pelkästään logiikan ja lukujen peruslakeja sekä laeiksi muotoiltuja oikoteitä käyttäen johtaa usein pitkiin päättelyketjuihin, joissa olennainen saattaa hukkua pikkutarkkojen yksityiskohtien alle. Siksi käytännön päättelyssä käytetään paljon myös sellaisia oikoteitä, joita ei ole opittu tietoisesti lakeina, vaan tiedostamattomasti kokemuksen kautta. Silti, jotta päättely olisi pätevää, sen täytyy olla ainakin periaatteessa palautettavissa peruslakeihin. Peruslait jakautuvat kahteen ryhmään: puheenaiheen peruslait (esimerkiksi lukusuoran lukujen peruslait tai merkkijonojen peruslait) ja loogisen päättelyn peruslait.

Tämän alaluvun jatkossa keskitymme logiikan peruslakien käyttämiseen yhtälöiden ratkaisemisessa sellaisinaan ja oikoteiden kautta. Lukusuoran lukujen käsittelyn oletamme tutuksi, eli tämän alaluvun jatkossa emme näpertele sellaisten asioiden kanssa kuin miksi $--a=a$ tai $3x-12+12=3x$. Nyt näpertelemme logiikan peruslakien kanssa! Ne voi esittää monella tavalla. Ne voi jakaa viiteen ryhmään.

Lait, jotka ilmaisevat miten päättelyn saa koota yksittäisistä päättelyaskelista. Matematiikassa niitä ei yleensä formalisoida, vaan käytetään sanallisia ilmauksia tyyliin ”olettakaamme, että”, ”siksi”, ”niinpä” ja ”muussa tapauksessa”. Tässä kirjassa ne on esitetty toisaalta sanallisesti ja toisaalta $\Rightarrow$:n ja $\Leftrightarrow$:n lakeina. Matemaattisessa logiikassa niitä esitetään usein symbolin $\vdash$ avulla.

Propositiologiikan lait. Niin kauan kun pysytään propositiologiikassa, on kaikki tarpeellinen periaatteessa kuvassa 26 tai sen myös U:ta käyttävässä vastineessa. Monet luvussa 2 esitetyt kaavat ja lait kuten [2], [10] ja [16] ovat kuitenkin todella hyödyllisiä oikoteitä.

Vielä tärkeämpiä ne ovat koulumatematiikassa ja predikaattilogiikassa. Niissä ei juuri koskaan voida kokeilla kaikkia muuttujien arvojen yhdistelmiä, koska mahdollisia arvoja on paljon (usein äärettömästi). Atomikaavojen totuusarvojen yhdistelmiä on vähemmän, mutta niiden kokeilemista vaikeuttaa se, että niistä pitää karsia mahdottomat (esimerkiksi on mahdotonta, että $x>3$ on tosi mutta $x>2$ on epätosi). Siksi koulumatematiikassa ja predikaattilogiikassa on usein liian hankalaa päätellä suoraan kuvaan 26 perustuen. Silti sitä ei kannata heittää pois työkalupakista, koska toisinaan se on kätevää.

Yhtäsuuruuden lait. Yhtäsuuruutta merkitään $=$. Sen lait voidaan esittää joko logiikan tai puheenaiheen lakeina. Tässä kirjassa ne esitetään logiikan lakeina. Se lienee yleisempi käytäntö, ja joka tapauksessa se on tämän kirjan kannalta kätevämpi.

Matematiikassa on tapana kertoa, että yhtäsuuruus on refleksiivinen, symmetrinen ja transitiivinen. Lisäksi saatetaan mainita, että kun yhtäsuuria käytetään saman lausekkeen tai kaavan osina, saadaan samat lopputulokset. Mainittiinpa se tai ei, sitä käytetään vähän väliä. Matematiikassa nämä lait on tapana muotoilla muuttujien avulla.

Muut yhtäsuuruuden tärkeät lait olemme jo maininneet tässä kirjassa, mutta refleksiivisyyttä emme. Siksi mainitsemme sen nyt. Jos-osan ehdolla ylläpidetään periaatetta [46], että mikään vertailu, jonka toinen tai molemmat puolet on määrittelemätön, ei ole tosi. Ilman sitä [53]:lla voitaisiin johtaa väärä tulos $\frac{1}{0} = \frac{1}{0}$.

Jos f on määritelty, niin $f = f$. [53]

Formaalissa logiikassa $=$:n lait muotoillaan usein lausekkeiden avulla, koska formaali looginen päättely ei pohjimmiltaan käsittele esimerkiksi lukuja, vaan merkkijonoja, jotka ilmaisevat lukuja ja lukujen ominaisuuksia. Tässä kirjassa $=$:n lait ovat [53], [47], [49], [52] ja [51]. Niiden muotoiluun on vaikuttanut pyrkimys olla huolellinen määrittelemättömien lausekkeiden kanssa. Yhtäsuuruuden laeiksi riittäisivät [53] ja [51] kahdestaan, sillä loput kolme voi johtaa niistä.

Todistus [47]:lle. Osoitamme ensin $f = g \Rightarrow g = f$ olettamalla $f = g$ ja johtamalla $g = f$. Koska $f = g$, on [46]:n mukaan f määritelty, joten [53]:n mukaan $f = f$ on tosi. Oletuksen ansiosta jokaisessa mahdollisessa tilanteessa $f = g$. Siksi valitsemalla $\varphi(x)$:ksi $x = f$ [51] tuottaa $f = f \Leftrightarrow g = f$. Koska $f = f$ on tosi, myös $g = f$ on tosi.

Vaihtamalla f:n ja g:n roolit saadaan $g = f \Rightarrow f = g$. Niinpä [32] tuottaa $f = g \Leftrightarrow g = f$. □

Tämä on helppo, tai ainakin lyhyt. Todista [49] laeista [53] ja [51]! 151

Todista [52] laeista [53] ja [51]! 152

Kvanttorien lait. Kvanttorit käsitellään varsinaisesti vasta luvussa 5. Silti niistä täytyy puhua jonkin verran jo nyt, koska matematiikassa, jopa koulumatematiikassa, niitä käytetään melkein koko ajan, vaikkakin hyvin usein ikään kuin piilevästi. Kvanttoreita ovat $\forall$ ja $\exists$. Kaavasta, jossa esiintyy muuttujia mutta ei kvanttoreita, ei ilman asiayhteyttä välttämättä näe, esittääkö se lakia, ratkaistavaksi tarkoitettua yhtälöä, väitettä että jokin asiantila vallitsee (esimerkiksi että lämpötila on 21 astetta) vai jotakin muuta. Jos tarkoitetaan lakia, niin kaavan yhteydessä saattaa lukea esimerkiksi, että se pätee jokaisella x:n arvolla.

Kvanttori $\forall$ vastaa ilmausta ”jokaisella” ja $\exists$ ”ainakin yhdellä”. Esimerkiksi se tosiasia, että ei ole olemassa suurinta lukua, voidaan ilmaista kaavalla, joka sanoo, että otetaanpa mikä tahansa luku, niin on olemassa sitä suurempi luku: $\forall x : \exists y : y > x$. Kvanttoreita käytettäessä esimerkiksi [48] voitaisiin ilmaista $\forall a : \forall b : a - b = a + -b$. Matematiikassa on kuitenkin tavallista kirjoittaa pelkästään $a - b = a + -b$ ja joko ilmaista sanallisesti tai jättää kokonaan ilmaisematta, että tarkoitetaan, että valitaanpa a:lle ja b:lle mitkä tahansa lukuarvot, niin $a - b = a + -b$ on tosi.

Myös logiikassa $\forall$:n voi usein jättää pois, kun tarkoitetaan, että kaava pätee jokaisella muuttujan arvolla. Itse asiassa on tavallista valita yhdeksi logiikan peruslaeista laki, josta seuraa muun muassa, että jos $\forall x : \varphi(x)$ on tosi, niin myös $\varphi(x)$ on tosi. Tämä peruslaki sanoo, että x:n tilalle saa sijoittaa minkä tahansa määritellyn lausekkeen f, kunhan varoo sekoittamasta toisiinsa muuttujia, joilla on sama nimi mutta eri merkitys $\varphi(x)$:ssä kuin f:ssä (asiaan palataan sivulla 99).

Eräs toinen laki sanoo, että jos $\varphi(x)$ voidaan johtaa tekemättä mitään x:n arvoa koskevia oletuksia, niin $\forall x : \varphi(x)$ on tosi. Olettamatta x:stä mitään voidaan johtaa mitäänsanomattomia kaavoja, kuten $x = x$ ja $x^2 \geq 0$, mutta myös vähemmän ilmeisiä kaavoja, kuten $(x+1)^5 \geq 5x+1$ tai $\sin 2x = 2 \sin x \cos x$. Sen, että näin johdettu $\varphi(x)$ pätee jokaiselle luvulle, näkee siitä, että jos valitaan mikä tahansa konkreettinen luku, vaikka 1863, johtamisen voisi toistaa niin että x:n tilalla olisi se luku. Jokainen johtamisessa käytetty päättelyaskel olisi pätevä 1863:lle, koska se oli pätevä x:lle, jonka arvo voi olla mikä tahansa luku, koska siitä ei oletettu mitään.

Kun näitä lakeja käytetään peräkkäin, niin saadaan, että jos $\varphi(x)$ ei sisällä $\forall$:a eikä $\exists$:a ja se voidaan johtaa tekemättä mitään x:n arvoa koskevia oletuksia, niin x:n tilalle saa sijoittaa minkä tahansa määritellyn lausekkeen, ja tulos on tosi. Määritellyn lausekkeen sijoittaminen muuttujan tilalle on niin yleinen toimenpide matematiikassa, että sille, että se on matemaattisesti oikein, ei välttämättä edes osaa kaivata perustelua. Kaipasitpa perustelua tai et, nyt olet sellaisen nähnyt (paitsi jos hyppäsit edellisten rivien yli).

Tähän periaatteeseen viitattiin jo sivulla 7, kun puhuttiin propositiosymboleiden korvaamisesta kaavoilla (tai kaavoja edustavilla kreikkalaisilla kirjaimilla, kuten φ). Sen, että x:n arvosta ei ole oletettu mitään, voi formaalissa logiikassa varmistaa käyttämällä x:n tilalla muuttujaa, jota ei ole siihen mennessä käytetty lainkaan. Matematiikassa se hoidetaan usein sillä, että lukija vaan jotenkin hiljaisesti tietää, että tässä esiintyvä a tai x on eri muuttuja kuin mikään aiemmin esiintynyt a tai x.

Määrittelemättömyyden lait. Osa koulumatematiikan laskutoimituksista on joissakin tilanteissa määrittelemättömiä: nollalla ei saa jakaa, negatiivisella luvulla ei ole neliöjuurta, nollavektorilla ei ole suuntaa, ei ole olemassa suurinta lukua ja niin edelleen. Kun jokaiselle lausekkeessa esiintyvälle muuttujalle annetaan jokin arvo, niin lauseke joko tuottaa jonkin arvon tai on määrittelemätön. Kuten [46] sanoo, lauseke on määrittelemätön, jos ja vain jos se sisältää määrittelemättömän laskutoimituksen. Esimerkiksi jos x:lle annetaan arvo 3, niin $\frac{4}{x-1} + x$ tuottaa arvon 5, koska $\frac{4}{3-1} + 3 = \frac{4}{2} + 3 = 2 + 3 = 5$. Mutta jos x:lle annetaan arvo 1, niin lasku alkaa $\frac{4}{1-1} + 1 = \frac{4}{0} + 1$ ja loppuu siihen, koska nollalla ei voi jakaa. Toisin sanoen, kun $x = 1$, on $\frac{4}{x-1} + x$ määrittelemätön, koska se sisältää $\frac{4}{x-1}$:n, jossa jaetaan nollalla.

Määrittelemättömien lausekkeiden käsittelyyn matemaattisissa tieteissä ja tekniikassa ei ole yhtenäistä linjaa. Logiikan valtavirrassa niitä ei käsitellä lainkaan, vaan oletetaan, että jokainen laskutoimitus tuottaa aina määritellyn lopputuloksen. Matematiikassa ne käsitellään tavallisesti sanallisilla säännöillä, joita ei formalisoida. Ohjelmoinnissa niitä käsitellään vaihtelevin tavoin. Esimerkiksi numeerisessa laskennassa hyvin usein käytettävän standardin IEEE 754 mukaan jos f tai g tai molemmat ovat määrittelemättömiä, niin $f < g$, $f \leq g$, $f = g$, $f \geq g$ ja $f > g$ tuottavat epätosi, mutta $f \neq g$ tuottaa tosi.

Tässä kirjassa on pyritty tunnistamaan ja formalisoimaan matemaatikkojen käyttämät säännöt. Kuten kohta näemme, määrittelemättömien lausekkeiden käsittelyyn riittää usein tavallinen kaksiarvoinen logiikka täydennettynä pienellä määrällä määrittelemättömyyteen viittavia ehtoja ja päättelykeinoja. Niitä on jo mainittu aiemmissa laeissa, kuten [51], [52] ja [53]. Tämä lähestymistapa ei kuitenkaan aina riitä. Aihepiiri on ollut sekä loogikoiden että ohjelmoinnin teoreetikkojen aktiivisen tutkimuksen kohteena. Luvussa 8 esitetään tuore kolmiarvoiseen logiikkaan perustuva käsittelytapa, joka pystyy todistamaan kaiken sen mikä pitääkin pystyä eikä mitään liikaa, perustelee edellä mainitut kaksiarvoista logiikkaa käyttävät keinot, ja näyttää vastaavan matematiikkojen käyttämiä julkilausumattomia sääntöjä.

Päätellä voi paitsi lakeja käyttämällä, myös vetoamalla kaavojen tulkintaan eli niissä esiintyvien symboleiden merkitykseen. Tulkintaan vetoamallahan monet laitkin perustellaan! Tämä pätee varsinkin niihin, jotka valitaan osaksi ”ensimmäisiä päättelykeinoja”, eli joita ei perustella johtamalla aikaisemmin esitetyistä laeista. Edellä on moneen kertaan perusteltu lakeja pohdiskelemalla mahdollisia tilanteita. Yhtä pätevää kuin soveltaa lakia, on soveltaa sitä tulkintaan vetoavaa päättelyä, jolla laki itse perusteltiin.

Kun $f = g$ tulkitaan tarkoittamaan, että f ja g ovat määritellyt ja esittävät saman olion, niin $=$:n lait ovat ilmeiset. Niitä ei tarvitse erikseen painaa mieleen, vaan maalaisjärki sanoo muun muassa, että jos f esittää samaa kuin g, niin g esittää samaa kuin f, $h(f)$ esittää samaa kuin $h(g)$ ja $\varphi(f)$ esittää samaa kuin $\varphi(g)$. Yleisemmin, kun samoille olioille tehdään sama temppu, niin saadaan sama lopputulos. Kaksi asiaa on kuitenkin otettava huomioon.

Ensiksi, toisinaan on tarpeen olla tarkkana, että ”sama temppu” todellakin tehdään samoille olioille eikä vain niiden eri esitysmuodoille. Esimerkiksi $2^2 = (-2)^2$ on oikein, koska sen molemmat puolet esittävät samaa lukua 4. Mutta kun kummastakin poistetaan ^{2}, niin lopputulokset 2 ja (-2) eivät esitäkään samaa lukua. Osuuden ^{2} poistaminen ei ole lukuja käsittelevä temppu, vaan vain lukujen esitysmuotoja käsittelevä temppu. Siksi lopputulokset eivät välttämättä edusta samaa lukua. Vastaava lukuja käsittelevä temppu on neliöjuuren ottaminen. Sen tuottamat lopputulokset edustavat samaa lukua: $\sqrt{2^2} = \sqrt{4} = 2$ ja $\sqrt{(-2)^2} = \sqrt{4} = 2$.

Lauseketta muuttujan tilalle sijoitettaessa on toisinaan lisättävä sulkeet juuri siksi, että se mikä ennen sijoitusta kohdistui puheena olevaan muuttujaan, kohdistuisi jatkossa sijoitettavan lausekkeen esittämään arvoon eikä vain lausekkeeseen itseensä. Esimerkiksi kun a:han sijoitetaan $x+1$ lausekkeessa $2a$, pitää kakkosella kertomisen kohdistua lausekkeen $x+1$ tuottamaan arvoon, joten $2x+1$ on väärin mutta $2(x+1)$ oikein. Vastaava pätee kun sijoitetaan kaava propositiomuuttujaan: jos $\varphi(X)$ on $x \geq 2 \wedge X$ ja X:n tilalle sijoitetaan $y < 2 \vee y = 5$, niin $x \geq 2 \wedge y < 2 \vee y = 5$ on väärin mutta $x \geq 2 \wedge (y < 2 \vee y = 5)$ on oikein.

Kaikki kynällä ja paperilla tai tietokoneella tapahtuva lukujen, lausekkeiden ja kaavojen käsittely on viime kädessä esitysmuotojen käsittelyä. Se voidaan kuitenkin tulkita lukujen käsittelyksi, jos lopputuloksen esittämä luku riippuu vain siitä, mitä lukuja lähtötiedot esittävät, eikä siitä, mikä saman luvun eri esitystavoista on lähtötietona. Tämä ajatus yleistyy moniin abstrakteihin käsitteisiin ja on matematiikassa laajassa käytössä. Sitä tarkoitetaan, kun jokin käsite määritellään niin sanottuna ekvivalenssiluokkana. Mutta nyt ei ole oikea aika paneutua siihen.

Toiseksi, toisinaan $=$ ei ole oikea symboli ilmaisemaan ”esittää samaa”. Tästä tärkeä esimerkki on, että sitä näkee vain harvoin käytettävän kaavojen tuottamien totuusarvojen samuuden ilmaisemiseen. Koska $=$ voi esiintyä myös kaavan sisällä, on selkeämpää verrata totuusarvoja jollain muulla symbolilla. Mikään symboli ei ole saavuttanut ylivoimaista suosiota, mutta $\Leftrightarrow$ on jossain määrin yleinen.

Toinen esimerkki on määrittelemättömien lausekkeiden käsittely tässä kirjassa ja usein matematiikassa. Määrittelemätön käyttäytyy lausekkeissa ja kaavoissa samalla tavalla riippumatta siitä, miten se on saatu aikaan. Jos $h(x)$ on lauseke ja f on mikä tahansa määrittelemätön lauseke, niin [46]:n mukaan $h(f)$ on määrittelemätön. Esimerkiksi jos $h(x)$ on $2x+1$, niin, koska sekä $\frac{1}{0}$ että $\sqrt{-1}$ on määrittelemätön, myös sekä $2 \cdot \frac{1}{0} + 1$ että $2\sqrt{-1}+1$ on määrittelemätön. Edelleen, jos $\varphi(x)$ on kaava ja sekä f

että g on määrittelemätön lauseke, niin $\varphi(f)$ ja $\varphi(g)$ joko tuottavat saman totuusarvon tai molemmat ovat määrittelemättömiä. Esimerkiksi kun $\varphi(x)$ on $x = 1 \vee 1 = 1$, niin sekä $\varphi\left(\frac{1}{0}\right)$ että $\varphi\left(\sqrt{-1}\right)$ tuottavat T. Kun $\varphi(x)$ on $x = 1 \wedge 1 = 1$, niin sekä $\varphi\left(\frac{1}{0}\right)$ että $\varphi\left(\sqrt{-1}\right)$ ovat määrittelemättömiä.

Niinpä voidaan aivan hyvin ajatella, ja usein ajatellaankin, että $\frac{1}{0}$ ja $\sqrt{-1}$ tuottavat saman tuloksen. Silti $\frac{1}{0} = \sqrt{-1}$ katsotaan vääräksi. Lausekkeiden $\frac{1}{0}$ ja $\sqrt{-1}$ tulokset ovat jossakin hyvin toimivassa mielessä samat (lausekkeissa ja kaavoissa ne voi vaihtaa keskenään, eikä lopputulos muutu), mutta tätä samuutta ei merkitä $=$:lla. Syynä on se, että jos sallittaisiin merkitä $\frac{1}{0} = \sqrt{-1}$, niin joko voitaisiin johtaa vääriä tuloksia tai jouduttaisiin muuttamaan monta lakia monimutkaisemmiksi. Tämän kirjan käytäntö, joka on myös usein matematiikan käytäntö, on varsin onnistunut yritys valita pienimmän riesan tie. Siinä määrittelemätön lauseke ei ole $=$:n esittämässä mielessä yhtäsuuri minkään lausekkeen kanssa, ei edes itsensä kanssa, mutta $=$:n ulkopuolisessa mielessä jokainen määrittelemätön lauseke on samanveroinen.

Kuvittele, että lausekkeisiin $\frac{1}{0}$ ja $\sqrt{-1}$ saa soveltaa kaikkia samoja lakeja kuin määriteltyihin lausekkeisiin. Johda oletuksesta $\frac{1}{0} = \sqrt{-1}$ ja tutuista lukujen ja logiikan laeista $\frac{1}{0} = -1$, $\frac{1}{0} = 1$ ja $-1 = 1$! 153

Seuraavassa esimerkissä ratkaistaan toisen asteen yhtälö neliöksi täydentämällä.

$$\begin{array}{lll}
1 & x^2+4x-12=0 & \Leftrightarrow\ x^2+4x+0-12=0\ \Leftrightarrow\ x^2+4x+(4-4)-12=0 \\
2 & & \Leftrightarrow\ (x^2+4x+4)+(-4-12)=0\ \Leftrightarrow\ (x+2)^2-16=0 \\
3 & & \Leftrightarrow\ (x+2)^2=16\ \Leftrightarrow\ x+2=-4 \vee x+2=4 \\
4 & & \Leftrightarrow\ x=-6 \vee x=2
\end{array}$$

Rivillä 1 sovellettiin ensin lakia $a+0=a$ ja [51]:ää. Mitkä olivat a ja [51]:n f, g ja φ, ja miksi juuri ne? 154

Jos a olisi ollut jälkimmäinen x, niin mikä olisi tullut tulokseksi? 155

Myös rivin 1 lopussa sovellettiin [51]:ää. Mitkä olivat f, g ja φ? 156

Toisen rivin alussa laskujärjestys vaihdettiin käyttämällä lakia [48] ja lukujen liitäntälakia. Ensin mainittua olemme jo pohtineet, ja jälkimmäistä käsitellään alaluvussa 3.2. Lupa soveltaa niitä lausekkeen sisällä tulee [52]:sta. Niin saatiin $x^2+4x+(4-4)-12 = (x^2+4x+4)+(-4-12)$, josta [51] tuotti $x^2+4x+(4-4)-12=0 \Leftrightarrow (x^2+4x+4)+(-4-12)=0$. Kuten varmaan on käynyt ilmeiseksi, [51]:ää ja [52]:aa käytetään vähän väliä. Jatkossa niiden käyttöä ei mainita paitsi jos mainitsemiseen on erityinen syy. Toisen rivin loppu seuraa lukujen laeista. Sitten lisättiin molemmille puolille 16. Olemme jo käsitelleet juurta jaksain, miten se purkautuu alemman tason lakien käytöksi. Palaamme kohta rivin 3 jälkimmäiseen vaiheeseen. Miten rivi 4 seuraa yhtäpitävyyksistä $x+2=-4 \Leftrightarrow x=-6$ ja $x+2=4 \Leftrightarrow x=2$? 157

Rivin 3 loppu seuraa tietenkin oikotielaista $a^2=b^2 \Leftrightarrow a=b \vee a=-b$. Sen suunta $\Leftarrow$ seuraa [36]:lla siitä, että [52]:n mukaan $a=b \Rightarrow a^2=b^2$, ja siitä, että [52]:n ja lukujen lakien mukaan $a=-b \Rightarrow a^2=(-b)^2=b^2$. Suunta $\Rightarrow$ seuraa kohta esitettävällä päättelyllä laista nimeltä *tulon nollasääntö* (*zero-product property*):

$$fg=0 \text{ jos ja vain jos } f=0 \text{ ja } g \text{ on määritelty, tai } g=0 \text{ ja } f \text{ on määritelty.} \qquad [54]$$

Tulon nollasääntö ei ole peruslaki, mutta kannattaa silti muistaa erikseen, koska sillä on suuri käytännön merkitys. Todistamme sen lukujen peruslaeista sivulla 91.

Jos $a^2=b^2$, niin $(a+b)(a-b)=a^2-b^2=0$. Tulon nollasäännön mukaan $a+b=0 \vee a-b=0$. Siitä seuraa $a=-b \vee a=b$.

Tässä esimerkissä käytettiin $\vee$:ta ilmaisemaan, että yhtälöllä on kaksi juurta. On tavallista ilmaista välivaihe $x+2=-4 \vee x+2=4$ muodossa $x+2=\pm 4$. Symbolia $\pm$ voi käyttää huoletta, jos se esiintyy kaavassa vain yhden kerran. Jos se esiintyy useasti, niin voi olla tarpeen selventää mitä tarkoitetaan. Esimerkiksi $a \pm b \pm c = d$ voi tarkoittaa joko $a+b+c=d \vee a-b-c=d$ tai $a+b+c=d \vee a+b-c=d \vee a-b+c=d \vee a-b-c=d$. Lopullinen vastaus $x=-6 \vee x=2$ on paras ilmaista $\vee$:n avulla.

Tämäkin esimerkki havainnollistaa, että [52] on yksisuuntainen: siitä, että $h(f)=h(g)$, ei tavallisesti voi päätellä, että $f=g$. Jos kuitenkin on varmaa, että $h(x)$ ei voi saada samaa arvoa kahdesti, niin saa päätellä, että $f=g$. Riittää, että $h(x)$ ei voi saada samaa arvoa kahdesti niillä x:n arvoilla, jotka f tai g voi tuottaa mahdollisissa tilanteissa.

Jos tiedetään, että $(x^2+2)x=(4x-1)x$ niin voidaanko päätellä $x^2+2=4x-1$? 158

Jos tiedetään, että $(x^2+2)x=(x^2+2)y$ niin voidaanko päätellä $x=y$? 159

Seuraavaksi ratkaisemme yhtälöparin

$$\begin{aligned} 2x-y &= 3 \\ 3x-2y &= 2 \end{aligned}$$

Yhtälöpari tarkoittaa kahta yhtälöä, joille on löydettävä kaikki ne muuttujien arvojen yhdistelmät, joilla yhtälöt ovat yhtä aikaa totta. On siis löydettävä ne x:n ja y:n arvojen yhdistelmät, joilla $2x-y=3 \wedge 3x-2y=2 \Leftrightarrow \mathsf{T}$. Joudumme viittaamaan kaavaan $2x-y=3 \wedge 3x-2y=2$ useasti. Annamme sille nimen *lähtökohta*, jotta viittaukset siihen erottuisivat selvästi. Siis

$$\textit{lähtökohta} \;\Leftrightarrow\; 2x-y=3 \wedge 3x-2y=2$$

Aluksi poimimme yhtälöparista ensimmäisen yhtälön ja ratkaisemme siitä y:n x:n funktiona. Askel, jossa ratkaistava yhtälö poimitaan yhtälöparista, jätetään tyypillisesti kirjoittamatta. Se vie tilaa ja se on tottuneelle lukijalle asiayhteyden vuoksi selvä. Nyt kuitenkin kirjoitamme sen näkyviin, jotta voisimme kommentoida sitä. Se on alla ensimmäisenä:

$$\textit{lähtökohta} \;\Rightarrow\; 2x-y=3 \;\Leftrightarrow\; -y=-2x+3 \;\Leftrightarrow\; y=2x-3 \tag{20}$$

Koska sana "*lähtökohta*" edustaa alkuperäistä yhtälöparia, ensimmäinen askel on oikeasti $2x-y=3 \wedge 3x-2y=2 \Rightarrow 2x-y=3$. Se käyttää [33]:n ensimmäistä lakia. Ei olisi oikein kirjoittaa siihen $\Rightarrow$:n tilalle $\Leftrightarrow$, koska muun muassa $x=2 \wedge y=1$ on sille vastaesimerkki: $3 \cdot 2 - 2 \cdot 1 = 2$ ei ole tosi mutta $2 \cdot 2 - 1 = 3$ on tosi, joten $\Rightarrow$:n vasen puoli ei ole mutta oikea puoli on tosi. Toisessa askeleessa molemmilta puolilta vähennettiin $2x$. Perustele $-y=-2x+3 \Rightarrow y=2x-3$ ja $-y=-2x+3 \Leftarrow y=2x-3$! 160

Transitiivisuuden nojalla saamme (20):stä

$$\textit{lähtökohta} \;\Rightarrow\; y=2x-3 \tag{21}$$

Seuraava tavoitteemme on sijoittaa näin saatu y:n lauseke y:n tilalle jälkimmäiseen yhtälöön, ja ratkaista niin syntyneestä yhtälöstä x. Sitä varten ensin poimimme yhtälöparista jälkimmäisen yhtälön käyttäen [33]:n toista lakia:

$$\textit{lähtökohta} \;\Rightarrow\; 3x-2y=2 \tag{22}$$

Koska (21):n mukaan $y=2x-3$, tuottaa [51] $3x-2y=2 \Leftrightarrow 3x-2(2x-3)=2$. Nyt voidaan ratkaista x lukujen laeilla, vähentämällä molemmilta puolilta 6 ja ottamalla molemmista puolista vastaluku: $3x-2(2x-3)=2 \Leftrightarrow -x+6=2 \Leftrightarrow -x=-4 \Leftrightarrow$

$x = 4$. Ei ole olemassa vakiintunutta kätevää tapaa ilmaista tätä päättelyä kokonaan kaavakielellä, mutta kun on ensin ilmaistu että tiedetään tai oletetaan $y = 2x-3$, niin suurimman osan voi ilmaista seuraavasti:

$$\begin{aligned} \textit{lähtökohta} \ &\Rightarrow\ 3x-2y=2 \ \Rightarrow\ 3x-2(2x-3)=2 \\ &\Leftrightarrow\ -x+6=2 \ \Leftrightarrow\ -x=-4 \ \Leftrightarrow\ x=4 \end{aligned}$$

Miksi se ei ole oikein ilmman tietoa tai oletusta $y = 2x-3$? 161

Formaalissa logiikassa saman voi perustella esimerkiksi [43](c):llä. Jos Γ sisältää lukujen lait ja alkuperäisen yhtälöparin, niin siitä seuraa $y = 2x-3$, kuten edellä nähtiin. Sen voi ilmaista $\Gamma \models y = 2x-3$. Juuri äsken totesimme, että lukujen laeista, alkuperäisestä yhtälöparista ja oletuksesta $y = 2x-3$ seuraa $x = 4$. Miten sen voi ilmaista [43](c):n merkinnöillä? Minkä johtopäätöksen [43](c) tuottaa, ja miten sen voi ilmaista 162
$\Rightarrow$:ta ja/tai $\Leftrightarrow$:a käyttäen? 163

Kirjoittamalla hieman enemmän melkein sama päättely voidaan ilmaista kaavakielellä ilman, että tarvitsee erikseen mainita mitään oletuksia:

$$\begin{aligned} \textit{lähtökohta} \ &\Rightarrow\ y=2x-3 \wedge 3x-2y=2 \ \Rightarrow\ 3x-2(2x-3)=2 \\ &\Leftrightarrow\ -x+6=2 \ \Leftrightarrow\ -x=-4 \ \Leftrightarrow\ x=4 \end{aligned} \tag{23}$$

Ensimmäinen askel seuraa (21):stä, (22):sta ja [34]:stä. Olemme jo nähneet, että oletuksen $y = 2x-3$ vallitessa $3x-2y = 2 \Leftrightarrow 3x-2(2x-3) = 2$, joten [32] ja [44] tuottavat toisen askeleen. Loput kolme askelta on jo perusteltu. Voisiko (23):n toisessa askeleessa olla $\Leftrightarrow$ eikä $\Rightarrow$, sillä sen perustelussakin on $\Leftrightarrow$? Miksi (23):n ensimmäisessä 164
askeleessa on $\Rightarrow$ eikä $\Leftrightarrow$? 165

Toinen askel saadaan äskeistä helpommin seuraavalla lailla, joka on yksinkertaisempi kuin [51]:

Jos $\forall$ ja $\exists$ eivät esiinny $\varphi(x)$:ssä, niin $f = g \wedge \varphi(f) \ \Leftrightarrow\ f = g \wedge \varphi(g)$. [55]

Kuten monesti aiemminkin, $\forall$ ja $\exists$ sallitaan sivulla 99 kerrottavalla ehdolla. Toinen askel saadaan tästä ja [33]:sta näin:

$$y = 2x-3 \wedge 3x-2y=2 \ \Leftrightarrow\ y = 2x-3 \wedge 3x-2(2x-3)=2 \ \Rightarrow\ 3x-2(2x-3)=2$$

Todistus [55]:lle. Valitaan tarkasteltavaksi mikä tahansa mahdollinen tilanne. Jos $f = g$ ei ole siinä tosi, niin kumpikaan niin-osan puoli ei ole tosi. Muutoin $f = g$ on tosi. Niinpä $\varphi(f)$ ja $\varphi(g)$ käsittelevät samaa arvoa ja siksi tuottavat saman totuusarvon. Jos se on T, niin niin-osan molemmat puolet ovat tosi. Muussa tapauksessa niin-osan kumpikaan puoli ei ole tosi, koska $f = g \wedge \varphi(x)$ on tosi vain kun sekä $f = g$ että $\varphi(x)$ on tosi. □

Perustele seuraava! 166

$$\textit{lähtökohta} \ \Rightarrow\ x=4 \wedge y=2x-3 \ \Leftrightarrow\ x=4 \wedge y=2\cdot 4-3 \ \Leftrightarrow\ x=4 \wedge y=5 \tag{24}$$

Tämä saattaa näyttää valmiilta lopputulokselta, mutta se ei vielä ole valmis. Nimittäin kaikki minkä olemme tähän asti tehneet tämän yhtälöparin ratkaisemiseksi olisi ollut pätevää myös siinä tapauksessa, että mukana olisi ollut myös kolmas yhtälö $x-y=5$. Selvästikään $x = 4 \wedge y = 5$ ei toteuta yhtälöä $x-y = 5$. Mistä sitten tiedämme, että se toteuttaa molemmat alkuperäiset yhtälöt? Tähänastinen päättelymme ei sitä osoita. Se, minkä tähänastinen päättelymme osoittaa, on että mikään muu x:n ja y:n arvojen yhdistelmä kuin $x = 4 \wedge y = 5$ ei toteuta alkuperäistä yhtälöparia. Mitä vielä on tehtävä, jotta yhtälöpari olisi ratkaistu? Miten sen voi tehdä? 167

$$
\begin{array}{rcl}
1 & & 2x-y=3 \ \wedge\ 3x-2y=2 \\
2 & \Leftrightarrow & y=2x-3 \ \wedge\ 3x-2y=2 \\
3 & \Leftrightarrow & y=2x-3 \ \wedge\ 3x-2(2x-3)=2 \\
4 & \Leftrightarrow & y=2x-3 \ \wedge\ x=4 \\
5 & \Leftrightarrow & x=4 \ \wedge\ y=2x-3 \\
6 & \Leftrightarrow & x=4 \ \wedge\ y=2\cdot 4-3 \\
7 & \Leftrightarrow & x=4 \ \wedge\ y=5
\end{array}
$$

Kuva 33: Yhtälöparin ratkaiseminen pelkästään $\Leftrightarrow$:lla

Edellisessä vastauksessa tehty temppu oli helppo. Kuitenkin esimerkiksi epäyhtälöryhmän tapauksessa sama asia on paljon työläämpi. Sitä ei tarvitse tehdä, jos alkuperäisestä (epä)yhtälöryhmästä lopulliseen vastaukseen on päättelyketju, jossa ei esiinny $\Rightarrow$:ta vaan ainoastaan $\Leftrightarrow$:a. Sen esivalmisteluissa saa esiintyä $\Rightarrow$:ta, mutta siinä itsessään ei saa.

Esimerkkimme tapauksessa sen voi tehdä kuten kuvassa 33. Rivillä 1 toistettiin alkuperäinen yhtälöpari. Rivillä 2 käytettiin (20):ssä johdettua yhtäpitävyyttä $2x-y=3$
$\Leftrightarrow y=2x-3$ ja [28]:a. Mikä oli [28]:n $\varphi(X)$? Ensimmäinen (20):n askel *lähtökohta* 168
$\Rightarrow 2x-y=3$ ei ole tarpeen. Rivillä 3 sovellettiin [55]:ttä — miten? Rivillä 4 käytettiin 169
tavallisen yhtälön ratkaisemisen tuottamaa yhtäpitävyyttä $3x-2(2x-3)=2 \Leftrightarrow x=4$
ja [28]:a. Rivillä 5 käytettiin [2]:ta. Mitä tehtiin rivillä 6? Jos rivi 7 tulkitaan [51]:n 170
käyttämiseksi, niin mikä oli $\varphi(a)$? 171

3.2 Lukusuoran lukujen lakeja

Tässä alaluvussa pohdimme lukusuoran lukujen lakeja sekä hieman muitakin järjestelmiä, jotka noudattavat useimpia samoja lakeja. Aloitamme pohtimalla lukujen ja lausekkeiden käsitteitä ja suhdetta toisiinsa.

Luku on abstrakti käsite. Osalla luvuista on oma merkki tai merkkiyhdistelmä, mutta ei jokaisella. Esimerkiksi luvulla kolme on oma numeromerkki 3, ja luvun tuhatviisikymmentäkaksi esittää neljän numeromerkin yhdistelmä 1052. Ympyrän kehän ja halkaisijan pituuksien suhdetta (suunnilleen 3,14) esittävän luvun merkki on π.

Moni muu luku voidaan ilmaista vain epäsuorasti. Esimerkiksi sillä positiivisella luvulla, jonka neliö on 2, ei ole omaa merkkiä eikä merkkiyhdistelmää, mutta sen voi ilmaista lausekkeella $\sqrt{2}$. Siinä 2 on luvun kaksi merkki ja $\sqrt{\ }$ on erään laskutoimituksen merkki. Edes luvulla miinus yksi ei ole omaa merkkiä eikä merkkiyhdistelmää, vaan -1 on lauseke, joka koostuu luvun yksi merkistä ja sen laskutoimituksen merkistä, joka tuottaa luvusta sen vastaluvun. Sen, että -1 todellakin on lauseke eikä lukua miinus yksi tarkoittava kahden merkin merkkiyhdistelmä, näkee siitä, että $-1^2=-1$. Se siis lasketaan $-1^2=-(1^2)=-1$ eikä $-1^2=(-1)^2=1$. Huomaa ero: 21^2 ei lasketa
$2(1^2)=21$ vaan $(21)^2=441$. Piirrä lausekkeiden -1^2, $(-1)^2$ ja 21^2 lausekepuut! 172

Numeromerkkejä ovat 0, 1, 2, 3, 4, 5, 6, 7, 8 ja 9. Luonnolliset luvut ovat 0, 1, 2, $\ldots$, 10, 11, $\ldots$. Siis luonnolliset luvut ovat täsmälleen ne luvut, jotka voidaan ilmaista äärellisinä numeromerkkien jonoina. Luvun miinus sataviisi voi ilmaista lausekkeella -105, ja sama periaate toimii jokaiselle negatiiviselle kokonaisluvulle. Niinpä jokainen kokonaisluku voidaan ilmaista lausekkeella. *Rationaaliluvut* (*rational numbers*) $\mathbb{Q}$ ovat ne luvut, jotka voi ilmaista jakolaskuna, jonka osoittaja on kokonaisluku ja nimittäjä on positiivinen kokonaisluku. Esimerkkejä ovat $\frac{2}{3}$, $-\frac{120}{7}$ ja 1052 eli $\frac{1052}{1}$. Niinpä jokainen rationaaliluku voidaan ilmaista lausekkeena.

lauseke	tuotti	rikottu
`(1+-1)+1e-17`	10^{-17}	
`1+(-1+1e-17)`	0	[57]
`1-49*1./49`	$1{,}11022 \cdot 10^{-16}$	[63]
`0.0204082*(0.333333+0.666667) - (0.0204082*0.333333 + 0.0204082*0.666667)`	$-3{,}46945 \cdot 10^{-18}$	[65]

Kuva 34: Lauseke, sen tyypillä `double` tuottama arvo ja kuvan 35 laki, jota tulos rikkoo

Tulemme huomaamaan luvussa 3.5, että suurinta osaa lukusuoran luvuista ei voi ilmaista lainkaan, ei edes epäsuorasti! Tarkemmin sanoen, ei ole mahdollista suunnitella merkintäjärjestelmää, joka käyttää äärellistä valikoimaa erilaisia merkkejä, ja jossa jokainen lukusuoran luku voidaan esittää laittamalla äärellinen määrä merkkejä peräkkäin. Tämä seuraa Georg Cantorin 1800-luvun lopulla tekemistä keksinnöistä. Siis vaikka rationaalilukuja on lukusuoralla kaikkialla tiheässä, ne kattavat vain mitättömän pienen osan lukusuoran luvuista! Tämä tulos on hyvin kummallinen. Sitä vastustettiin aluksi jyrkästi, mutta sittemmin matematiikot ovat hyväksyneet sen jokseenkin yksimielisesti, ja se on nykyisin tärkeä osa matematiikkaa ja matemaattista logiikkaa. Miksi desimaaliluvut ei ole edellä kuvattujen vaatimusten mukainen merkintäjärjestelmä? 173

Tästä syystä useimmissa nykyaikaisissa tietokoneissa on kaksi erillistä ryhmää lukujärjestelmiä. Toiset käsittelevät vain kokonaislukuja. Niitä käytetään muun muassa kertomaan missä kohdassa muistia jokin tieto sijaitsee sekä laskemaan kuinka monta kertaa jokin toimenpide on toistettava. Niitä voi käyttää myös esittämään puhelinnumeroita, päivämääriä, sentteinä ilmaistuja rahasummia ja niin edelleen. Koska kokonaisluvun esittämiseen on varattu kiinteä määrä bittejä (tyypillisesti 8, 16, 32 tai 64), voidaan esittää vain äärellinen määrä eri kokonaislukuja. Siksi ei voida esittää miten suuria positiivisia ja miten pieniä negatiivisia kokonaislukuja tahansa. Yleisimmät järjestelmät esittävät kokonaisluvut $-2^{b-1}, \ldots, 2^{b-1}-1$ (etumerkillinen) tai $0, \ldots, 2^b - 1$ (etumerkitön), missä b on 8, 16, 32 tai 64. Jollei laskun välivaihe tai lopputulos ole liian suuri eikä liian pieni, niin se on aina täysin tarkka. Pyöristysvirheitä ei siis tapahdu.

Toinen ryhmä lukujärjestelmiä on niitä tarpeita varten, joihin kokonaisluvut eivät riitä. Niiden nimi on *liukuluvut* (*floating point number*). Ne muistuttavat melko paljon desimaalilukuja. Liukuluvuillekin on varattu kiinteä määrä bittejä, joten nekään eivät voi olla miten suuria tai pieniä tahansa — eivätkä miten tarkkoja tahansa, eivätkä miten lähellä nollaa tahansa olematta tasan nolla. Suurin ja pienin mahdollinen liukuluku ovat tyypillisesti noin $\pm 10^{38}$ (tyyppi `float`) tai $\pm 10^{308}$ (tyyppi `double`). Pyöristysvirheitä tapahtuu. Liukulukujen tarkkuus vastaa tyypillisesti joko suunnilleen seitsemää (`float`) tai kuuttatoista (`double`) desimaalia. Esimerkiksi tietokoneella, jolla tämä kirja kirjoitettiin, saatiin kuvassa 34 näytetyt tulokset tyypillä `double`. Pienin positiivinen liukuluku on tyypillisesti noin 10^{-45} (`float`) tai 10^{-323} (`double`), mutta niin lähellä nollaa tarkkuus on kehno, koska esimerkiksi sen puolikasta tai neljää kolmasosaa ei voida esittää. Liukuluvut ovat kaikkiaan melko monimutkainen asia. Useimmissa tietokoneissa niiden käsittely noudattaa standardia nimeltä IEEE 754.

Tietokoneohjelmilla voidaan toteuttaa laajempia lukualueita ja parempi tarkkuus. Esimerkiksi rationaaliluvuille voidaan ohjelmoida toteutus, joka esittää ne täysin tarkasti eikä tee yhteen-, vähennys-, kerto- ja jakolaskuissa pyöristysvirheitä. Sen ja muiden vastaavien toteutusten ongelmana on, että tarvittavan muistin ja laskenta-ajan määrällä on taipumusta kasvaa laskujen edetessä liian suureksi. Siksi niitä käytetään vain poikkeustapauksissa.

Lauseke (*expression*) on tekstuaalinen ilmaus. Emme määrittele lausekkeen rakennetta viimeisen päälle, vaan luotamme siihen, että se on melko tuttu jo koulusta. Logiikan tarpeita ajatellen on kuitenkin hyvä mainita pari asiaa. Lausekkeessa voi esiintyä *vakioita* (*constant*) kuten 3810 ja π; *muuttujia* (*variable*) kuten x ja a_2; laskutoimituksia kuten $+$ ja log (10-kantainen logaritmi); sekä tietenkin sulkeita (ja). Muuta lausekkeessa ei voi olla. Kukin lauseke voidaan esittää merkkijonolla, eli äärellisellä määrällä äärellisestä valikoimasta poimittuja merkkejä pantuna peräkkäin. Vaikka esimerkiksi $\frac{\sqrt{a_2+x}}{x+1}$ ei esitä asioita pelkästään peräkkäin, se on kuitenkin tuotettu tähän kirjaan eräällä merkkijonolla (nimittäin `\frac{\sqrt{a_2+x}}{x+1}`).

Tässä luvussa lausekkeet käsittelevät lukuja, mutta myöhemmin tässä kirjassa ne voivat käsitellä muutakin, esimerkiksi merkkijonoja. Sitä ennakoiden, tässä luvussa käytetään toisinaan sanaa ”arvo” sanan ”luku” sijaan, kun puhutaan siitä mitä lauseke käsittelee ja tuottaa. Kun siirrytään luvuista muihin puheenaiheisiin, yleensä vakiot ja laskutoimitukset vaihtuvat toisiin, mutta lausekkeen yleinen rakenne säilyy: siinä voi olla vakioita, muuttujia, laskutoimituksia ja sulkeita, eikä muuta. Sitä mitä tässä kirjassa kutsutaan laskutoimitukseksi, on logiikassa tapana kutsua funktioksi tai funktiosymboliksi.

Logiikassa on tapana käyttää sanaa *termi* (*term*) tarkoittamaan sitä, mitä tässä kirjassa kutsutaan lausekkeeksi. Tässä kirjassa valittiin toisin, koska aika yleisesti ”termillä” tarkoitetaan tiettyä muotoa olevia lausekkeita, kuten 5, x, $5x$, x^3 tai $5x^3y$, mutta ei $5+x$. Tarkka määritelmä vaihtelee. Melko yleisen käytännön mukaan termi on monimutkaisimmillaan vakiolauseke kertaa muuttuja korotettuna potenssiin vakiona ilmaistu luonnollinen luku kertaa … kertaa muuttuja korotettuna potenssiin vakiona ilmaistu luonnollinen luku. Tarpeettomia osia kuten ykkösellä kertomisen voi jättää pois. Tällaiset termit voi määritellä BNF:llä näin:

$$\begin{array}{rcl} \textit{Termi} & ::= & \textit{Vakiolauseke} \mid \textit{Potenssi} \mid \textit{Termi Potenssi} \\ \textit{Potenssi} & ::= & \textit{Muuttuja} \mid \textit{Muuttuja}\,\hat{}\;\textit{LuonnLuku} \end{array}$$

Vakiolauseke (*ground term*) tarkoittaa lauseketta jossa ei esiinny muuttujia. Esimerkiksi 3, -3 ja $\frac{2}{3}$ ovat vakiolausekkeita. Luonnollinen luku on epätyhjä jono numeromerkkejä eli merkkejä 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Luonnollisen luvun sisällä ei saa olla tyhjää.
Mitä termi voi yksinkertaisimmillaan olla äskeisen BNF:n mukaan? Usein vaaditaan, 174
että muuttujat esiintyvät aakkosjärjestyksessä eikä sama muuttuja toistu. Sitä ei ole helppo ilmaista BNF:llä. Toisaalta toisinaan sallitaan esimerkiksi, että vakiolauseke voi esiintyä muuallakin kuin alussa.

Koska edellä mainitut eksponentit pitää ilmaista vakioina, on x^3 termi, mutta x^n ei ole. Kun sanotaan että x^n on termi, niin tarkoitetaan jotain niistä termeistä, jotka saadaan vaihtamalla n:n tilalle jokin vakiona ilmaistu luonnollinen luku. Niinpä x^3 *on* termi, mutta x^n ei ole vaan *edustaa* termiä, samaan tapaan kuin esimerkiksi kaavaskeema edustaa kaavaa. Tämä olemisen ja edustamisen välinen ero on tärkeä formaalissa logiikassa. Siihen tullaan jatkossa palaamaan muutamaan kertaan.

Palatkaamme puhumaan luvuista. Aivan kuten propositiologiikassa tilanne on mikä tahansa propositiomuuttujille annettujen totuusarvojen yhdistelmä, nyt *tilanne* on mikä tahansa muuttujille annettujen arvojen yhdistelmä, missä muuttujat saavat arvoikseen lukuja. Kun lausekkeen muuttujille on annettu arvot, lauseke joko tuottaa luvun tai sisältää määrittelemättömän laskutoimituksen kuten nollalla jakamisen. Jos lauseke ei missään tilanteessa sisällä määrittelemätöntä laskutoimitusta, niin se esittää funktiota joka ottaa paikkalukunsa ilmaiseman määrän lukuja ja tuottaa luvun, aivan kuten jokainen propositiologiikan kaava esittää funktiota joka ottaa paikkalukunsa ilmaiseman määrän totuusarvoja ja tuottaa totuusarvon (katso luku 2.2).

Mutta toisin kuin propositiologiikassa jossa jokainen totuusfunktio voidaan esittää kaavalla, ei ole mahdollista esittää jokaista lukujen funktiota lausekkeella. Se ei onnistu edes jokaiselle funktiolle, joka ottaa yhden luonnollisen luvun ja tuottaa tulokseksi 0 tai 1. Tämäkin seuraa Cantorin tuloksista.

Kuten hyvin tiedetään, niin jos f ja g edustavat lausekkeita, niin $f = g$ tarkoittaa, että f:n edustama lauseke ja g:n edustama lauseke tuottavat saman arvon. Esimerkiksi $1+2 = 3$ tarkoittaa, että $1+2$ ja 3 tuottavat saman luvun. Siksi $1+2 = 3$ on totta, vaikka $1+2$ on eri lauseke kuin 3. Yhtäsuuruus $x+3 = 8$ on tosi kun $x = 5$, ja epätosi muulloin. Yhtäsuuruus on mielekäs käsite muillekin puheenaiheille kuin luvuille, joten nykyisin yleensä (mutta ei aina) katsotaan, että $=$ on logiikan eikä lukujen symboli ja sen lait [53], [51] ja niin edelleen ovat logiikan yleisiä lakeja.

Ilmaus $f \neq g$ tarkoittaa samaa kuin $\neg(f = g)$. Symboli $\neq$ katsotaan yleensä vain selkokaavojen (siis ei aitojen kaavojen) symboliksi. Siksi sitä ei yleensä katsota logiikan symboliksi mutta ei myöskään puheenaiheen symboliksi. Tämä ei ole olennaista. Voit käyttää symbolia $\neq$ ikään kuin se olisi logiikan symboli ja yhtäpitävyyttä $f \neq g \Leftrightarrow \neg(f = g)$ ikään kuin se olisi logiikan laki.

Suuruusjärjestys ei ole mielekäs käsite kaikille puheenaiheille. Siksi $<$ ei ole logiikan symboli eivätkä sen lait ole logiikan yleisiä lakeja, vaan se määritellään erikseen niille puheenaiheille joille se on hyödyllinen ja jätetään määrittelemättä muille. Tämä on tärkeä ero symbolien $=$ ja $<$ välillä.

Luvussa 2 otettiin käyttöön propositiomuuttujia. Ne saavat arvoikseen totuusarvoja. Luvussa 2 ei ollut muunlaisia muuttujia, mutta siellä käytettiin kreikkalaisia kirjaimia edustamaan kaavoja tavalla, joka muistuttaa muuttujia. Sekaannusten välttämiseksi emme kutsuneet niitä muuttujiksi.

Tämän luvun logiikan muuttujat saavat arvoikseen lukuja. Tämänkään luvun kaavoissa ei ole muunlaisia muuttujia. Propositiomuuttujia saattaa vilahtaa viittauksissa propositiologiikan lakeihin kuten X kaavassa [28], mutta tämän luvun logiikan kaavoihin saakka niitä ei päädy. Tässäkin luvussa tarvitaan kreikkalaisia kirjaimia edustamaan kaavoja. Lisäksi tarvitaan jotakin edustamaan lausekkeita. Olemme käyttäneet ja käytämme jatkossakin siihen enimmäkseen kirjaimia f, g ja h. Lausekkeita edustavat kirjaimet eivät ole muuttujia. Voidaksemme puhua kätevästi niistä sekä kaavoja edustavista kreikkalaisista kirjaimista, kutsumme molempia *skeemaparametreiksi*. Englanninkielisessä kirjallisuudessa käytetään muun muassa nimiä *metavariable*, *metalinguistic variable* ja *syntactical variable*.

Mitkä [48]:n symbolit ovat muuttujia, ja mitkä skeemaparametreja? 175

Mitkä [51]:n symbolit ovat muuttujia, ja mitkä skeemaparametreja? 176

Mitkä [52]:n symbolit ovat muuttujia, ja mitkä skeemaparametreja? 177

Ilmaus ”jos f ja g edustavat lausekkeita, niin $f = g$ tarkoittaa, että f:n edustama lauseke ja g:n edustama lauseke tuottavat saman arvon” on jossain määrin kömpelö. Siksi usein sanotaan yksinkertaisemmin ”jos f ja g ovat lausekkeita, niin $f = g$ tarkoittaa, että f ja g tuottavat saman arvon”. Samoin sen sijaan että sanottaisiin ”φ edustaa kaavaa”, usein sanotaan ”φ on kaava”. Tällainen yksinkertaistaminen on tavallista matematiikassa ja logiikassa. Haittana on, että saattaa jäädä hämäräksi, milloin jokin ilmaus pitää tulkita kirjaimellisesti ja milloin sen pitää ajatella edustavan jotakin.

Jotkin vaikeasti ymmärrettävät asiat avautuvat miettimällä, mitkä ilmaukset ovat sitä mitä niiden sanotaan olevan ja mitkä vain edustavat sitä. Käsittelemme tästä esimerkkinä *Berryn paradoksin*. Luonnollisia lukuja voi ilmaista muutenkin kuin nume-

Jokaiselle luvulle a, b ja c pätee:

[56]	$a+b=b+a$	[61]	$(ab)c=a(bc)$
[57]	$(a+b)+c=a+(b+c)$	[62]	$a\cdot 1=a$
[58]	$a+0=a$	[63]	$a\neq 0 \;\Rightarrow\; a\cdot\frac{1}{a}=1$
[59]	$a+-a=0$	[64]	$0\neq 1$
[60]	$ab=ba$	[65]	$a(b+c)=ab+ac$

Kuva 35: Kunta-aksioomat

romerkkien jonoina. Esimerkiksi ”pienin luonnollinen luku, jonka neliö on suurempi kuin 10” on 4. Sellainen ilmaus saattaa olla lyhyempi kuin vastaava numeromerkkien jono. Esimerkiksi luvun 387420489 ilmaisemiseen numeromerkkien jonona tarvitaan 9 merkkiä, mutta jos potenssilasku katsotaan merkiksi, niin sen voi ilmaista kolmella merkillä lausekkeella 9^9. ”Ykkönen ja sata nollaa” on paljon lyhyempi kuin sama luku (jonka nimi on googol) ilmaistuna numeromerkkien jonona. Mutta

(25) pienin luonnollinen luku, jonka ilmaisemiseen tarvitaan vähintään 77 merkkiä

vaikuttaa paradoksilta, koska (25) ilmaisee sen 76 merkillä: p, i, e, n, . . . , ä.

Paradoksi purkautuu, kun hoksaa, että ”pienin . . . merkkiä” ei ole luku vaan ilmaus, joka on edustavinaan mutta ei todellisuudessa edusta lukua. Se ei siis ole sen ristiriitaisempi kuin ”pienin luonnollinen luku, joka on itseään suurempi”, josta näkee heti, että se on edustavinaan mutta ei todellisuudessa edusta lukua.

Alaluvussa 3.1 keskityimme logiikan lakeihin ja oletimme lukujen lait tunnetuiksi. Seuravaaksi käsiteltävässä esimerkissä sekä lukujen että logiikan lakien käyttö näytetään yksityiskohtaisella tasolla. Esimerkissä ratkaistaan yhtälö $x+3=8$. Käytännön työssä yhtälöiden ratkaiseminen etenee paljon pitemmin loikin kuin tässä esimerkissä. Nyt kuitenkaan tavoitteena ei ole opetella yhtälöiden ratkaisemista, vaan ratkaisuprosessi on vain esimerkki, jonka avulla havainnollistetaan miten tutut päättelykeinot perustuvat sekä lukujen että logiikan lakeihin sekä nostetaan esiin uusia käsiteltäviä asioita. Käsittelemme esimerkin lopusta alkuun, koska sen helpoin askel on lopussa ja monimutkaisin heti alussa.

(26) $$\begin{aligned} x+3=8 &\Leftrightarrow (x+3)-3=8-3 \Leftrightarrow (x+3)-3=5 \\ &\Leftrightarrow x+(3-3)=5 \Leftrightarrow x+0=5 \Leftrightarrow x=5 \end{aligned}$$

Viimeinen askel $x+0=5 \Leftrightarrow x=5$ voidaan johtaa [51]:llä yhtäsuuruudesta $x+0=x$ valitsemalla $f:=x+0$, $g:=x$ ja $\varphi(a):\Leftrightarrow a=5$. Tällöin $\varphi(f)$ on $\varphi(x+0)$ eli $x+0=5$, ja $\varphi(g)$ on $\varphi(x)$ eli $x=5$. Koska $\forall$ ja $\exists$ loistavat poissaolollaan ja koska $x+0=x$ eli $f=g$, [51] tuottaa $\varphi(f)\Leftrightarrow\varphi(g)$ eli $\varphi(x+0)\Leftrightarrow\varphi(x)$ eli $x+0=5\Leftrightarrow x=5$.

Yhtäsuuruus $x+0=x$ tuli tietysti siitä, että kun mihin tahansa lukuun lisätään nolla, niin se ei muutu miksikään. Tämä ominaisuus on valittu yhdeksi lukujen peruslaeista. Se on numero [58] kuvassa 35. Laista [58] saadaan $x+0=x$ valitsemalla $a:=x$. Kuvaan 35 on koottu kaikki tässä alaluvussa käytettävät lukusuoran lukujen peruslait. Lukusuoran luvuilla on myös muita peruslakeja. Niihin paneudutaan luvuissa 3.3 ja 3.5.

Kuvan 35 lakikokoelmaa kutsutaan kunta-aksioomiksi siksi, että on olemassa muitakin hyödyllisiä järjestelmiä kuin lukusuoran luvut, jotka toteuttavat sen. Siksi se on sellaisenaankin tärkeä. Matemaatikot tarkoittavat *kunnalla* (*field*) mitä tahansa järjestelmää, joka noudattaa kaikkia kuvan 35 lakeja.

Laki $a+0=a$ voi näyttää itsestäänselvältä, mutta siihen ja lukujen lakeihin yleisemminkin liittyy kiemura, joka yleensä selitetään vain luonnollisella kielellä, ja jonka kohtasimme jo luvussa 3.1. Nimittäin jos sijoitetaan a:n tilalle esimerkiksi $\frac{1}{x}$, niin $a+0=a$ tuottaa $\frac{1}{x}+0=\frac{1}{x}$. Kun $x=0$, se ei ole oikein, koska nollalla ei saa jakaa. Edes $\frac{1}{0}=\frac{1}{0}$ ei ole oikein. Kunta-aksioomat pätevät kaikille lukusuoran luvuille, mutta tämä lupaus ei koske $\frac{1}{0}$:aa, koska se ei edusta lukusuoran lukua. Siksi laista $a+0=a$ ei voi johtaa $\frac{1}{0}+0=\frac{1}{0}$. Myöskään $\frac{1}{0}+0$ ei edusta lukusuoran lukua. Sanomme, että $\frac{1}{0}$ ja $\frac{1}{0}+0$ eivät ole määriteltyjä, ja että $\frac{1}{x}$ ja $\frac{1}{x}+0$ eivät ole määriteltyjä kun $x=0$.

Tätä ongelmaa lievittää jonkin verran sivulla 72 tehty huomautus, jonka mukaan sellaisia yhtäsuuruuksia, jonka molemmilla puolilla esiintyvät täsmälleen samat muuttujat, saa käyttää [51]:ssä tarkastamatta, ovatko muuttujien tilalle tulevat lausekkeet määritellyt. Laki $a+0=a$ täyttää tämän ehdon, mutta esimerkiksi $a-a=0$ ja $0a=0$ eivät täytä.

Myöskään muun muassa $\sqrt{-1}$, $\log 0$ (nollan logaritmi) ja $\log(-1)$ eivät edusta lukusuoran lukuja. On olemassa lukusuoran lukuja laajempi kunta nimeltä ”kompleksiluvut” jossa $\sqrt{-1}$ edustaa lukua, mutta siinäkään $\frac{1}{0}$ ja $\log 0$ eivät edusta lukuja. Kun käytössä on (vain) lukusuoran luvut, kunta-aksioomia ei saa soveltaa nollalla jakamisen lopputulokseen, negatiivisten lukujen neliöjuuriin ja niin edelleen, koska ne eivät edusta lukusuoran lukuja. Lukusuoran luvuista puhuttaessa ne ovat määrittelemättömiä.

Tämä ongelma ei kuitenkaan nouse esiin käyttötapauksessamme $x+0=x$, sillä siinä a:n tilalla ei ole mitään jakolaskua, neliöjuurta tai muutakaan mahdollisesti määrittelemätöntä laskutoimitusta sisältävää, vaan pelkkä x. Kannattaa muistaa ero: muuttujat ovat aina määriteltyjä, mutta muuttujan tilalle laitettava lauseke saattaa olla määrittelemätön. Esimerkiksi x on aina määritelty, mutta $\frac{1}{x}$, $\sqrt{x}$ ja $\log x$ eivät ole. Kun muuttujan tilalle sijoitetaan lauseke, täytyy varmistua siitä, että se on määritelty (ellei erikseen ole annettu lupaa jättää varmistautumatta, kuten [51]:ssä, jossa f:n ja g:n sallitaan olla määrittelemättömiä, vaikka ne sijoitetaan $\varphi(x)$:n muuttujaan x).

Esimerkkimme toiseksi viimeisen askeleen $x+(3-3)=5 \Leftrightarrow x+0=5$ johtaminen voidaan aloittaa käyttämällä vähennyslaskun määritelmää [48]. Valinnalla $a:=3$ ja $b:=3$ siitä saadaan $3-3=3+-3$. Nämä valinnat eivät voi aiheuttaa määrittelemättömiä lausekkeita, koska 3 ei millään muuttujien arvoilla sisällä kiellettyjä laskutoimituksia, koska se ei sisällä mitään laskutoimituksia. Sitten johdamme [59]:llä $3+-3=0$ valinnalla $a:=3$. Kuten jo todettiin, 3 on aina määritelty. Saadut yhtäsuuruudet voi ketjuttaa näin: $3-3=3+-3=0$. Niistä saadaan $3-3=0$, koska $=$ on transitiivinen [49]. Siitä johdettiin $x+(3-3)=5 \Leftrightarrow x+0=5$ jo sivulla 71.

Seuraavana on vuorossa $(x+3)-3=5 \Leftrightarrow x+(3-3)=5$. Strategia lienee jo tullut tutuksi: ensin johdetaan $(x+3)-3=x+(3-3)$ ja sitten käytetään [51]:stä. Liitäntälaki [57] näyttää sopivalta ensin mainitun johtamiseen. Mutta välittömästi sitä ei voi käyttää, koska lausekkeessa $(x+3)-3$ on $-$ kohdassa jossa [57]:ssä on $+$. Siksi johdamme ensin $(x+3)-3=(x+3)+-3$. Tai tarkemmin sanoen, sinä johdat. Johda se, ja muista varoa määrittelemättömiä laskutoimituksia! 178

Nyt käytä [57]:ää! 179

Sen hokeminen, että 3 on aina määritelty, x on aina määritelty ja niin edelleen, alkaa ennemmin tai myöhemmin tuntua hyödyttömältä ja turhauttavalta — on ehkä alkanut jo. Siksi tästä eteenpäin lukuvakioista, muuttujista, yhteenlaskusta, vähennyslaskusta, vastaluvun tuottamisesta ja kertolaskusta ei tarvitse sanoa, että ne ovat aina määriteltyjä. Kuitenkin kun käytetään lakia, jossa on erikseen kirjattuna ehto, että jokin lauseke on määritelty, niin jotta näkyisi, että ehto on huomattu ja tarkastettu, kannattaa sanoa vaikka että ehto on selvästi tosi.

Seuraava tavoitteemme on johtaa $x+(3+-3)=x+(3-3)$. Käyttämällä [48]:aa siten, että $a := 3$ ja $b := 3$, saamme $3-3=3+-3$. Se saadaan käännettyä takaperin käyttämällä $=$:n symmetrisyyttä [47]. Siitä valinnalla $f := 3+-3$, $g := 3-3$ ja $h(a) := x+a$ [52] tuottaa $x+(3+-3)=x+(3-3)$. (Nyt kirjoitettiin $h(a)$ eikä $h(x)$, koska muuten x:t olisivat menneet sekaisin ja olisi tullut $(3+-3)+(3+-3) = (3-3)+(3-3)$.)

Viimeistele askeleen $(x+3)-3=5 \Leftrightarrow x+(3-3)=5$ todistus! 180

Edellä käytetyt logiikan lait olivat [47], [49], [51] ja [52]. Myös [28] on usein hyödyllinen. Niiden numeroita ja sanamuotoa ei tarvitse muistaa, vaan riittää että osaa päätellä niiden mukaisesti. Niiden ilmaisemat päättelyperiaatteet ovat niin itsestäänselviä, että voi olla vaikea edes huomata käyttävänsä niitä. Kannattaa hankkia vahva rutiini niiden käytössä, sillä käytännön päättelytyössä niitä käytetään tiuhaan. Rutiini syntyy itsestään, kun laskee paljon.

Kokeneella laskijalla saattaa olla valmiina mielessään liitäntälain muunnos $(a+b)-c=a+(b-c)$, jolla hän voi välittömästi johtaa $(x+3)-3=x+(3-3)$. Tällaisia muunnoksia jää mieleen kun laskee paljon. Niitä ei kannata alkaa opetella tietoisesti, sillä siitä tulisi liikaa opeteltavaa. On parempi opetella johtamaan niitä tarvittaessa.

Lain $(a+b)-c=a+(b-c)$ johtamiseksi riittää $(a+b)-c=(a+b)+-c = a+(b+-c)=a+(b-c)$. Jos tarvitaan enemmän perusteluja, niin voi mainita, että ensimmäinen ja viimeinen yhtäsuuruus perustuvat vähennyslaskun määritelmään ja keskimmäinen yhteenlaskun liitännäisyyteen (ne ovat [48] ja [57]). Ei tarvitse kertoa, mitä laitettiin lakien muuttujien tilalle, paitsi jos se on erityisen vaikea nähdä. Koska lakeja [28], [47], [49], [51] ja [52] käytetään lukuisissa päättelyissä vähän väliä, on tapana, että niiden käyttöä ei mainita. Jos kuitenkin on hankala nähdä miten [51]:tä käytettiin, voi olla hyvä kertoa mikä oli $\varphi(x)$, ja vastaavasti [28]:lle $\varphi(X)$. Tietenkin [51]:n olettama $f=g$ tai sekä f että g on määrittelemätön, [28]:n olettama $\psi \Leftrightarrow \chi$ ja ne ovat yhtäaikaa määritellyt, ja muidenkin lakien olettamat täytyy perustella, mikäli ne eivät ole itsestäänselvät.

Siis saa jättää sanomatta, että $b-c=b+-c$ käännettiin viimeisessä askeleessa takaperin [47]:llä, jonka jälkeen sitä sovellettiin lausekkeen $a+(b+-c)$ sisällä [52]:n luvalla. Myös saa jättää sanomatta, että [49]:n mukaan yhtäsuuruusketjusta $(a+b)-c = \ldots = a+(b-c)$ seuraa $(a+b)-c=a+(b-c)$. Lukujen lakien [48] ja [57] käyttö erottaa tämän päättelyn monista muista samankaltaisista, joten ne tulee mainita, jos päättelyn yhtäsuuruuksille kysytään perusteluja.

Johda laki muotoa $(a-b)-c=a\pm(b\pm c)$, missä kukin $\pm$ on joko $+$ tai $-$! Saat käyttää kaikkia tässä kirjassa jo esitettyjä lakeja sekä lakia $-(a+b)=-a-b$. 181

Johda laki muotoa $(a-b)+c=a\pm(b\pm c)$, missä kukin $\pm$ on joko $+$ tai $-$! Saat käyttää kaikkia tässä kirjassa jo esitettyjä lakeja sekä lakia $--a=a$. 182

Sitä edeltävä askel $(x+3)-3=8-3 \Leftrightarrow (x+3)-3=5$ johdettiin vastauksessa 142 siitä, että $8-3=5$. Käytännön työssä $8-3=5$ saadaan päässälaskuna, eikä sitä tarvitse sen kummemmin perustella. Lukujen lakien kannalta on kuitenkin mielenkiintoista purkaa se osiin. Se havainnollistaa sitä, että jopa näin yksinkertaisia asioita voidaan palauttaa vielä yksinkertaisempiin perusasioihin. Samalla se korostaa sitä jo havaittua tosiasiaa, että kaiken palauttaminen perusasioihin tekee päättelemisestä tolkuttoman kömpelöä. Lisäksi se tarjoaa mahdollisuuden kerrata edellä esitettyjen lakien käyttöä.

Yhtäsuuruuden $8-3=5$ johtamiseksi johdamme ensin $8=5+3$. Se seuraa siitä, että numeromerkkien määritelmistä $2=1+1$, $3=2+1$ ja niin edelleen sekä [52]:sta,

[57]:stä ja [47]:stä voidaan johtaa $8 = 7+1 = (6+1)+1 = ((5+1)+1)+1 = (5+(1+1))+1 = (5+2)+1 = 5+(2+1) = 5+3$.

Perustele hyvin yksityiskohtaisesti $(6+1)+1 = ((5+1)+1)+1$! 183

Perustele hyvin yksityiskohtaisesti $((5+1)+1)+1 = (5+(1+1))+1$! 184

Missä päättelyaskelissa käytettiin [47]:ää, ja mitä sillä tehtiin? 185

Johda $8-3 = 5$ käyttäen juuri johdettua yhtäsuuruutta $8 = 5+3$. Riittää esittää yhtäsuuruusketju, jonka yhtäsuuruudet ovat perusteltavissa tähän mennessä esitetyillä laeilla. Yhtäsuuruuksien perusteluja ei tarvitse esittää. 186

Kuinka monta kertaa käytettiin [49]:ää, kun johdettiin $8 = 5+3$ ja $8-3 = 5$? 187

Esimerkkimme ensimmäinen askel $x+3 = 8 \Leftrightarrow (x+3)-3 = 8-3$ saadaan välivaiheen $(x+3)+-3 = 8+-3$ kautta. Käyttämällä [48]:aa takaperin kahdesti saadaan $(x+3)+-3 = 8+-3 \Leftrightarrow (x+3)-3 = 8-3$. Yhtäpitävyys $x+3 = 8 \Leftrightarrow (x+3)+-3 = 8+-3$ saadaan seuraavalla lailla valinnalla $f := x+3$, $g := 8$ ja $h := -3$. Voidaksemme ilmaista lain näppärästi tarvitsemme merkinnän tarkoittamaan, että lauseke on määritelty. Siihen ei ole vakiintunutta merkintää matematiikassa eikä logiikassa. Tässä kirjassa siihen käytetään merkintää $\lceil f \rfloor$. Vastaavasti tässä kirjassa $\neg\lceil f \rfloor$ tarkoittaa, että f on määrittelemätön.

$$\lceil h \rfloor \wedge f = g \;\Leftrightarrow\; f+h = g+h \qquad [66]$$

Lain ehto $\lceil h \rfloor$ tarvitaan estämään esimerkiksi virheellisen tuloksen $0+\frac{1}{0} = 0+\frac{1}{0}$ johtaminen päättelyketjulla $0 = 0 \Leftrightarrow 0+\frac{1}{0} = 0+\frac{1}{0}$. Oikealla puolella ei tarvita ehtoa $\lceil h \rfloor$, koska jos h on määrittelemätön, niin [46]:n mukaan myös $f+h$ ja $g+h$ ovat määrittelemättömät, joten oikea puoli vertaa kahta määrittelemätöntä lauseketta ja vasen puoli tuottaa F. (Tässä kirjassa $\mathsf{F} \wedge f = g \Leftrightarrow \mathsf{F}$ ja $\mathsf{T} \vee f = g \Leftrightarrow \mathsf{T}$ vaikka f tai g olisi määrittelemätön.) Niinpä kumpikaan puoli ei ole tosi, joten [22] ei rikkoudu. Kummallakaan puolella ei tarvita ehtoja $\lceil f \rfloor$ ja $\lceil g \rfloor$, koska jos toinen tai molemmat niistä ei päde, niin sekä $f = g$ että $f+h = g+h$ sisältää määrittelemättömän lausekkeen, joten kumpikaan niistä ei ole tosi.

Laki [66] ei ole peruslaki, vaan se seuraa kunta-aksioomista ja logiikan yleisistä laeista. Yksi syy kunta-aksioomien tärkeyteen on, että hyvin suuri osa yhteen-, vähennys-, kerto- ja jakolaskun ominaisuuksista todellakin on todistettavissa ilman muita oletuksia kuin kunta-aksioomat ja logiikan yleiset lait. Suunta $\Rightarrow$ ei tarvitse edes kunta-aksioomia, sillä sekin on vain ilmentymä siitä [52]:n ilmaisemasta yleisestä periaatteesta, että kun yhtäsuurille arvoille tehdään sama asia, jonka lopputulos on määritelty, niin lopputuloksetkin ovat yhtäsuuret. Johda suunta $\Rightarrow$ [52]:sta! 188

On tärkeää tiedostaa, että tämä yleinen periaate ei ole kaksisuuntainen: siitä, että lopputulokset ovat yhtäsuuret, ei välttämättä seuraa, että alkuperäiset arvot ovat yhtäsuuret. Esimerkiksi $5 \cdot 0 = 0 = 4 \cdot 0$ mutta $5 \neq 4$, ja $(-3)^2 = 9 = 3^2$ mutta $-3 \neq 3$. Se, että poistetaan kumpikin "$\cdot\, 0$" yhtäsuuruudesta $5 \cdot 0 = 4 \cdot 0$ ei ole saman asian tekemistä yhtäsuurille arvoille, sillä sellainen poistaminen kohdistuu lausekkeisiin eikä niiden tuottamiin lukuihin, eivätkä $5 \cdot 0$ ja $4 \cdot 0$ ole sama lauseke. Siitä, että $x \cdot 2 = 4 \cdot 2$ voi päätellä, että $x = 4$, koska se onnistuu tempulla, joka käsittelee lausekkeiden tuottamia lukuja ja tuottaa määritellyn lopputuloksen: jaetaan kumpikin puoli 2:lla. Mutta siitä, että $5 \cdot 0 = 4 \cdot 0$ ei voi samalla tavalla päätellä, että $5 = 4$, koska vastaava temppu eli kummankin puolen jakaminen nollalla ei tuota määriteltyjä lopputuloksia.

Siksi [66]:n suunta $\Leftarrow$ tarvitsee kunta-aksioomia. Niissä tilanteissa, joissa f, g ja h ovat määritellyt, [57]:llä, [59]:llä ja [58]:lla saadaan $(f+h)+-h = f+(h+-h) = f+0 = f$ ja samoin $(g+h)+-h = g$. Niinpä $f+h = g+h \Rightarrow (f+h)+-h = (g+h)+-h$

$\Leftrightarrow f = g$, missä ensimmäinen askel saadaan [52]:lla ja jälkimmäinen juuri johdetuista yhtäsuuruuksista [51]:llä. Jälkimmäinen askel sisältää kaksi [51]:n käyttöä, mutta koska ne vaikuttavat eri kohdissa kaavaa, ne voi esittää yhtenä askeleena luettavuuden kärsimättä. Loput tilanteet eli ne, joissa ainakin yksi f:stä, g:stä ja h:sta ei ole määritelty, onkin jo käsitelty, nimittäin heti [66]:n perässä.

Todista kunta-aksioomilla ja tiedolla $2 \neq 0$, että $(x \cdot 2) \cdot \frac{1}{2} = x$! 189

Todista kunta-aksioomilla, että $x \cdot 2 = 4 \cdot 2 \Rightarrow x = 4$! 190

Yleinen periaate siis on, että

> *Kun samanlaisille kohteille tehdään sama, määritelty asia, niin lopputuloksetkin ovat samanlaiset; mutta lopputulosten samanlaisuudesta ei välttämättä seuraa alkuperäisten samanlaisuus. Tätä käytettäessä on tärkeää varmistua, että asia joka tehdään todellakin tehdään samanlaisille kohteille, eikä niiden erilaisille esitysmuodoille.*

Analysoi seuraava päättely edellä olevan periaatteen valossa: Selvästi $\frac{4+2}{2} = \frac{6}{2} = 3 = \frac{3}{1} = \frac{1+2}{1}$, joten $\frac{4+2}{2} = \frac{1+2}{1}$. Poistamalla molemmilta puolilta "$+2$" saadaan $\frac{4}{2} = \frac{1}{1}$, joten $2 = \frac{4}{2} = \frac{1}{1} = 1$. Niinpä $2 = 1$. 191

Samanlaisuus voi olla muutakin kuin lukujen yhtäsuuruutta. Se voi olla vaikka että kaksi propositiologiikan kaavaa tuottaa saman totuusarvon. Jos totuusarvot ovat (vain) F ja T, niin P:llä ja Q:lla on sama totuusarvo jos ja vain jos $P \leftrightarrow Q$ on tosi. Siis $\leftrightarrow$ on $=$:n roolissa. Seuraavaksi harjoittelemme tässä asetelmassa sen tunnistamista, seuraako lopputulosten samanlaisuudesta alkuperäisten samanlaisuus. Todista seuraavista ne, jotka pätevät, ja anna muille vastaesimerkit:

$$P \leftrightarrow Q \;\Leftrightarrow\; \neg P \leftrightarrow \neg Q$$ 192

$$P \leftrightarrow Q \;\Leftrightarrow\; P \wedge R \leftrightarrow Q \wedge R$$ 193

$$P \leftrightarrow Q \;\Leftrightarrow\; (P \rightarrow R) \leftrightarrow (Q \rightarrow R)$$ 194

$$P \leftrightarrow Q \;\Leftrightarrow\; (P \leftrightarrow R) \leftrightarrow (Q \leftrightarrow R)$$ 195

Olemme nyt saaneet valmiiksi päättelyn $x + 3 = 8 \Leftrightarrow \ldots \Leftrightarrow x = 5$. Kuten edellä on sanottu, käytännön päättelytyössä tämä päätelmä tehtäisiin huomattavasti nopeammin, jopa suoraan päässälaskuna $x + 3 = 8 \Leftrightarrow x = 5$. Käytännön päättelytyössä käytetään monia oikoteitä, joista osa opetetaan ja osan hoksaa kokemuksen myötä.

Eräs kouluissa opetettava oikotie on samanmuotoisten termien yhdistäminen. Termit ovat samanmuotoiset, jos ja vain jos jokainen muuttuja, joka esiintyy jommassa kummassa niistä, esiintyy yhtä monta kertaa myös toisessa niistä, missä kukin muotoa x^n oleva ilmaus lasketaan n:ksi esiintymäksi. (Toisinaan esitetty määritelmä "niiden kirjainosat ovat samat" jättää esimerkiksi x^2x^3 ja x^5 erimuotoisiksi, vastoin samanmuotoisten termien yhdistämisen tarkoitusta.)

Esimerkiksi lausekkeessa $2x + 7 - 3y^2 + 6x + y - 9 - x + 4y^2$ on neljä ryhmää samanmuotoisia termejä. Termit $2x$, $6x$ ja $-x$ yhdistämällä tulee $7x$; termeistä 7 ja -9 tulee -2; termeistä $-3y^2$ ja $4y^2$ tulee y^2; ja termi y on ainoa ryhmässään, joten se jää sellaiseksi. Yhdistetyt termit lasketaan yhteen jossain sopivalta tuntuvassa järjestyksessä, ja etumerkki-miinukset muutetaan vähennyslaskuiksi paitsi aivan alussa. Näin saadaan $y^2 + y + 7x - 2$ tai vaikka $-2 + 7x + y + y^2$.

Samanmuotoiset termit voi yhdistää kunta-aksioomia ja vakioiden laskusääntöjä käyttäen, mutta se on kovin kömpelöä. Esimerkiksi [60]:llä, [60]:llä, [65]:llä, sillä että $2 + 6 = 8$ ja [60]:llä saadaan $2x + 6x = 2x + x \cdot 6 = x \cdot 2 + x \cdot 6 = x(2+6) = x \cdot 8 = 8x$.

Kömpelöä tässä oli se, että $2x$, $6x$ ja $x \cdot 8$ piti kääntää toisinpäin, jotta päästiin käyttämään [65]:ä. Jotta meidän ei tarvitsisi tehdä niin uudelleen ja uudelleen, todistamme [65]:n muunnelman, jossa yhteinen tekijä on viimeisenä: $(a+b)c = ac+bc$. Se saadaan [60]:llä, [65]:llä, [60]:llä ja [60]:llä näin: $(a+b)c = c(a+b) = ca+cb = ca+bc = ac+bc$. Käyttäen sitä takaperin saadaan kätevämmin $2x+6x = (2+6)x = 8x$.

Tietenkin $2x+6x-x = 7x$ lasketaan käytännössä päässälaskuna tavalla, joka auki kirjoitettuna olisi $2x+6x-x = (2+6-1)x = 7x$. Jos kaikki halutaan palauttaa kunta-aksioomiin, niin pitää perustella, että sulkeiden sisällä saa olla kolme yhteenlaskettavaa, sillä [65]:ssä ja sille johtamassamme toisinpäisessä versiossa niitä ei ole kolme vaan kaksi. Näin se käy: $(a+b+c)x = ((a+b)+c)x = (a+b)x+cx = (ax+bx)+cx = ax+bx+cx$. Tämän ensimmäisessä ja viimeisessä askeleessa ei tapahdu logiikan näkökulmasta mitään, vaan ne vain palauttavat ihmislukijoiden mieleen, että $a+b+c$ on sama lauseke kuin $(a+b)+c$ ja $(ax+bx)+cx$ on sama lauseke kuin $ax+bx+cx$, koska $+$ on vasemmalle liitännäinen. Toisessa askeleessa käytetään [65]:lle johtamaamme muunnelmaa koko lausekkeen tasolla, ja kolmannessa askeleessa lausekkeen sisällä. Lupa käyttää sitä lausekkeen sisällä tulee tietenkin [52]:sta.

Jonain päivänä sulkeiden sisällä saattaakin olla neljä tai viisi yhteenlaskettavaa. Tarvitaan siis yleinen lause muotoa $(a_1+\ldots+a_n)b = a_1b+\ldots+a_nb$. Se voidaan ”todistaa” induktiolla siten, että pohjatapaus $n = 1$ on $(a_1)b = a_1b$, joka on tietenkin tosi, ja induktioaskel on $(a_1+\ldots+a_n+a_{n+1})b = ((a_1+\ldots+a_n)+a_{n+1})b = (a_1+\ldots+a_n)b+a_{n+1}b = (a_1b+\ldots+a_nb)+a_{n+1}b = a_1b+\ldots+a_nb+a_{n+1}b$. Perustele tämän päättelyn jokainen yhtäsuuruus! 196

Mutta tätä ”todistusta” ei voi esittää formaalissa logiikassamme, sillä siinä ei ole symbolia ”. . .” eikä mitään muutakaan keinoa kirjoittaa lauseketta, jossa yhteenlaskettavien määrä riippuu n:stä! Tämä ”todistus” on itse asiassa todistusskeema, joka edustaa ääretöntä määrää formaalin logiikan todistuksia, yhtä kullekin positiiviselle kokonaisluvulle n. Ensimmäinen sen edustamista todistuksista todistaa $(a_1)b = a_1b$, toinen $(a_1+a_2)b = a_1b+a_2b$, kolmas $(a_1+a_2+a_3)b = a_1b+a_2b+a_3b$ ja niin edelleen. (Formaalissa logiikassa saa kirjoittaa alaindeksoituja muuttujia kuten a_3, kunhan indeksinä on numeromerkkien jono eikä mitään muuta.) Muut kuin ensimmäinen todistus sisältävät edellisen todistuksen ja induktioaskeltamme muistuttavan mutta kokonaan auki kirjoitetun vaiheen, jolla tulos laajennetaan yhtä pitempiin lausekkeisiin.

Tulos voidaan esittää formaalisti summamerkintää käyttäen: $(\sum_{i=1}^{n} a_i)b = \sum_{i=1}^{n} a_ib$. Mutta se jättää epäformaaliksi sen, että $a_1+\ldots+a_n = \sum_{i=1}^{n} a_i$ ja sen, että $a_1b+\ldots+a_nb = \sum_{i=1}^{n} a_ib$, koska niissä esiintyy epäformaali symboli ”. . .”. Käytäntö on osoittanut, että ilmaus $(a_1+\ldots+a_n)b = a_1b+\ldots+a_nb$ on ihmislukijoille riittävän selvä, eikä $(\sum_{i=1}^{n} a_i)b = \sum_{i=1}^{n} a_ib$ ole ainakaan helpompi ymmärtää. Käytännön päättelytyössä pyritään käyttämään ihmisille luontevia ajatustapoja, eivätkä ne kaikki ole sellaisinaan helposti formalisoitavissa. Siksi matematiikassa ja logiikassa on tavallista, että jotakin asiaa ei tehdä formaalisti, vaan ainoastaan perustellaan, että se olisi tehtävissä formaalisti jos jaksettaisiin nyhrätä valtava määrä yksityiskohtia.

Lauseke $2x+6x-x$ ei ole [65]:lle eikä sen tähän mennessä esittämillemme muunnelmille sopivassa muodossa, vaan $-$ pitää muuttaa $+-$:ksi. Siis lasku $2x+6x-x = (2+6-1)x = 7x$ olisi yksityiskohtaisemmin esitettynä $2x+6x-x = 2x+6x+-x = 2x+6x+(-1)x = (2+6+-1)x = 7x$. Siitä näkyy, että laskussa käytettiin tietoa $(-1)x = -x$. Se saadaan seuraavalla päättelyllä. Sen yhtä vaille jokainen askel muodostuu yhden kunta-aksiooman käytöstä joko lausekkeen sisällä tai koko lausekkeen tasolla. Mikä on tämä yksi askel? 197

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

Puuttuvan askeleen voi johtaa seuraavasti. Näytämme käytetyt kunta-aksioomat ja välituloksen käytön =-merkin alaindekseillä. Koska

$$a\cdot 0+a =_{[56]} a+a\cdot 0 =_{[62]} a\cdot 1+a\cdot 0 =_{[65]} a(1+0) =_{[58]} a\cdot 1 =_{[62]} a\,, \tag{27}$$

saamme

$$a\cdot 0 =_{[58]} a\cdot 0+0 =_{[59]} a\cdot 0+(a+-a) =_{[57]} (a\cdot 0+a)+-a =_{(27)} a+-a =_{[59]} 0\,.$$

Siis jokaiselle luvulle a pätee $a\cdot 0=0$. Siksi $x\cdot 0+-x=0+-x$.

Koska $\frac{1}{0}$ ei edusta lukua, on $0\cdot\frac{1}{0}=1$ määrittelemätön. Siksi se ei ole tosi, joten se ei saa olla johdettavissa [63]:sta. Siksi [63]:ssa on ehto $a\neq 0$. Osoitamme seuraavaksi, että ehto $a\neq 0$ tarvittaisiin, vaikka $\frac{1}{0}$ edustaisi lukua. Siitä, että jokaiselle luvulle a pätee $a\cdot 0=0$ saadaan [60]:llä, että jokaiselle luvulle a pätee myös $0a=0$. Niinpä jos $\frac{1}{0}$ edustaisi lukua, niin pätisi $0\cdot\frac{1}{0}=0$. Koska [64]:n mukaan $0\neq 1$, ei voisi olla $0\cdot\frac{1}{0}=1$. Siksi ehto $a\neq 0$ olisi välttämätön [63]:ssa, vaikka $\frac{1}{0}$ edustaisi lukua. Koska ehto on välttämätön sekä silloin kun $\frac{1}{0}$ ei edusta lukua että silloin kun se edustaa lukua, ei nollalla jakamista saa mitenkään noudattamaan samoja lakeja kuin muut jakolaskut. Tästä syystä nollalla jakaminen on jätetty määrittelemättä.

Olemme perustelleet, että kunta-aksioomilla voi johtaa $2x+6x-x=7x$. Sitä ei kuitenkaan voi soveltaa alkuperäiseen lausekkeeseemme $2x+7-3y^2+6x+y-9-x+4y^2$ sellaisenaan, vaan ensin termit $2x$, $6x$ ja $-x$ pitää siirtää toistensa viereen. Se onnistuu käyttämällä [56]:ta ja [57]:ää, mutta on niin työlästä, että näytämme vain osan:

$$\begin{aligned}2x+7-3y^2+6x &= ((2x+7)-3y^2)+6x = (2x+(7-3y^2))+6x\\ = 2x+((7-3y^2)+6x) &= 2x+(6x+(7-3y^2)) = (2x+6x)+(7-3y^2)\end{aligned}$$

Kunta-aksioomista voidaan sentään jotakin johtaa helposti. Esimerkiksi se saadaan hyvin helposti, että 0 on yksikäsitteinen. ”Vaihtoehtoinen nolla” olisi mikä tahansa muu sellainen luku o, että jokaisella luvulla a pätee $a+o=a$. Laeilla [58] ja [56] sekä o:n perusominaisuudella saadaan $o=o+0=0+o=0$, joten $o=0$ eli ”vaihtoehtoisia nollia” ei ole.

Todista, että myös kunkin luvun vastaluku on yksikäsitteinen! Se onnistuu seitsemän =:n ketjulla. 198

Johda $--a=a$ käyttämällä vain kunta-aksioomia sellaisinaan! Se onnistuu kuudella askeleella. 199

Esitelimme aiemmin tulon nollasäännön [54]. Silloin lykkäsimme sen todistuksen sivulle 91. Mutta nythän olemme jo sivulla 91! On siis aika pitää lupaus ja todistaa tulon nollasääntö. Onneksi se on helppoa. Muistathan, että $\lceil f\rfloor$ tarkoittaa, että lauseke f on määritelty.

$$fg=0 \;\Leftrightarrow\; (f=0\wedge\lceil g\rfloor)\vee(g=0\wedge\lceil f\rfloor)$$

Todistus. Jos $\neg\lceil f\rfloor$, niin $fg=0$ ei ole määritelty, $f=0$ ei ole määritelty eikä $g=0\wedge\lceil f\rfloor$ ole tosi, joten tulon nollasäännön kumpikaan puoli ei ole tosi, joten yhtäpitävyys pätee. Vastaava pätee jos $\neg\lceil g\rfloor$, joten myös silloin yhtäpitävyys pätee. Jäljellä on tapaus, jossa sekä f että g on määritelty. Silloin niiden tilalla voidaan käyttää niiden tuottamia arvoja a ja b. Osoitamme kummankin suunnan erikseen.

Suunta $\Leftarrow$. Olemme jo osoittaneet, että jokaiselle luvulle x pätee $x\cdot 0=0$ ja $0x=0$. Siksi jos $a=0\wedge\lceil b\rfloor$ niin $ab=0b=0$, ja jos $b=0\wedge\lceil a\rfloor$ niin $ab=a\cdot 0=0$.

Suunta $\Rightarrow$. Jos $b = 0$, niin $a = 0 \vee b = 0$. Muussa tapauksessa $b \neq 0$, joten [62], [63], [61], oletus $ab = 0$ ja $0x = 0$ tuottavat $a = a \cdot 1 = a(b \cdot \frac{1}{b}) = (ab)\frac{1}{b} = 0 \cdot \frac{1}{b} = 0$, joten $a = 0$, joten $a = 0 \vee b = 0$. Koska muuttujat ovat aina määriteltyjä, molemmissa tapauksissa $(a = 0 \wedge \lceil b \rfloor) \vee (b = 0 \wedge \lceil a \rfloor)$. □

Polynomi (*polynomial*) on lauseke, jossa ei esiinny muuta kuin määriteltyjä vakiolausekkeita; muuttujia; yhteen-, vähennys- ja kertolaskuja; vastaluvun ottamista; jakamista määritellyllä vakiolausekkeella jonka tuottama luku ei ole 0; sekä korottamista potenssiin, missä eksponentti on vakiona ilmaistu luonnollinen luku. Tällainen potenssiin korottaminen voidaan tulkita peräkkäisinä kertolaskuina: esimerkiksi $x^3 = xxx$ ja $(x+y)^2 = (x+y)(x+y)$.

Kuten on tavallista matematiikassa, puhetavan yksinkertaistamiseksi kutsumme jatkossa ”vakioksi” sekä määriteltyä vakiolauseketta että sen tuottamaa arvoa. *Vakiopolynomi* on vakio (tarkemmin sanoen, vakiopolynomi on määritelty vakiolauseke). *Nollapolynomi* on 0 (tarkemmin sanoen, nollapolynomi on määritelty vakiolauseke, jonka tuottama arvo on 0 — siis esimerkiksi 0 tai $\left(\sqrt{2}\right)^2 - 2$). *Yhden muuttujan polynomi* (*univariate polynomial*) on polynomi, jossa esiintyy korkeintaan yhtä muuttujaa. Yhden muuttujan polynomin $P(x)$ *nollakohta* on sellainen arvo a, että $P(a) = 0$.

Kouluissa polynomissa esiintyvät vakiot ja polynomin muuttujien saamat arvot ovat lukuja, mutta yleisemmin matematiikassa ne voivat olla muutakin. Missä tahansa kunnassa on mielekästä tutkia polynomeja, joiden vakiot ja muuttujien arvot ovat peräisin siitä kunnasta. Tämä johtuu siitä, että kunta-aksioomista seuraa, että jokainen polynomi voidaan esittää summana, jonka jokainen yhteenlaskettava on termi sellaisena kuin ”termi” määriteltiin sivulla 83, ja samanmuotoiset termit on yhdistetty. Jokainen yhden muuttujan x polynomi voidaan esittää joko nollapolynomina tai muodossa $a_nx^n + \ldots + a_2x^2 + a_1x + a_0$, missä jokainen a_i on vakio (tarkemmin sanoen määritelty vakiolauseke) ja $a_n \neq 0$ (siis a_n:n tuottama arvo ei ole 0). Arvoja a_i kutsutaan *kertoimiksi* (*coefficient*). Jos $a_n \neq 0$, niin polynomin *aste* (*degree*) on n. Nollapolynomin asteeksi määritellään tässä kirjassa ja usein (mutta ei aina) muuallakin -1.

Myös yhtälön ja sen ratkaisemisen käsitteet yleistyvät kaikkiin kuntiin. Yhtälön *juuri* (*root*) tarkoittaa arvoa, joka toteuttaa yhtälön. Yhtälön ratkaiseminen tarkoittaa sen kaikkien juurten etsimistä. Jos $A(x)$ ja $B(x)$ ovat yhden muuttujan polynomeja, niin yhtälön $A(x) = B(x)$ juuret ovat samat kuin polynomin $A(x) - B(x)$ nollakohdat. Yhtälön $A(x) = B(x)$ aste on sama kuin polynomin $A(x) - B(x)$ aste.

Kunta-aksioomista seuraa, että jos $P(x)$ on yhden muuttujan polynomi, a on sen nollakohta eikä $P(x)$ ole nollapolynomi, niin on olemassa sellainen yhden muuttujan polynomi $Q(x)$, että $P(x) = (x-a)Q(x)$. Lisäksi $Q(x)$:n aste on yhtä pienempi kuin $P(x)$:n aste, ja $Q(x)$:n korkeimman asteen termin kerroin on sama kuin $P(x)$:n (siis jos $P(x) = a_nx^n + \ldots + a_0$ ja $Q(x) = b_mx^m + \ldots + b_0$ missä $a_n \neq 0$ ja $b_m \neq 0$, niin $m = n - 1$ ja $b_m = a_n$). Jos $P(x)$:n kertoimet ja a tunnetaan, niin $Q(x)$ saadaan laskemalla. Tulon nollasäännön vuoksi $P(x)$:n muut nollakohdat kuin a ovat $Q(x)$:n nollakohtia. Niinpä jos yhtälölle $P(x) = 0$ löydetään jollain tavalla yksi juuri, niin loput juuret saadaan laskemalla $Q(x)$ ja etsimällä sen nollakohdat.

Ratkaisemme tästä esimerkkinä yhtälön $x^3 - 3x^2 - x + 6 = 0$ lukusuoran lukujen kunnassa. Jos yhden muuttujan polynomin kertoimet ovat kokonaislukuja, niin melko usein ainakin yksi nollakohta löytyy kokeilemalla vakiotermin kaikki tekijät ja niiden vastaluvut. (Tämä johtuu siitä, että tehtävät laaditaan melko usein siten, että ainakin yksi juuri on kokonaisluku, ja lukujen jaollisuusominaisuuksista seuraa, että mikään muu kokonaisluku kuin edellä mainitut ei voi olla kokonaislukukertoimisen yhden muuttujan polynomin nollakohta.) Polynomi $x^3 - 3x^2 - x + 6$ on kokonaislukukertoiminen.

Sen vakiotermi on 6, ja sen tekijät vastalukuineen ovat 1, -1, 2, -2, 3, -3, 6 ja -6. Niistä 2 on nollakohta.

Laske $Q(x)$ siitä, että $x^3 - 3x^2 - x + 6 = (x-2)Q(x)$! Tee se täsmäyttämällä kummankin puolen vakiotermit, ensimmäisen asteen termit ja niin edelleen. 200

Siis $x^3 - 3x^2 - x + 6 = (x-2)(x^2 - x - 3)$. Polynomin $x^2 - x - 3$ nollakohdat saadaan toisen asteen yhtälön ratkaisukaavalla. Ne ovat $\frac{1-\sqrt{13}}{2}$ ja $\frac{1+\sqrt{13}}{2}$. Niinpä yhtälön $x^3 - 3x^2 - x + 6 = 0$ juuret ovat 2, $\frac{1-\sqrt{13}}{2}$ ja $\frac{1+\sqrt{13}}{2}$.

Kehittämällä tätä ajatuskulkua hieman pitemmälle saamme seuraavan lauseen:

Lause. Olkoon n luonnollinen luku. Jokaisessa kunnassa pätee: n:nnen asteen yhtälöllä on enintään n juurta. [67]

Todistus. Olkoon $P_n(x)$ n:nnen asteen polynomi, ja c sen korkeimman asteen termin kerroin. Asteen määritelmän mukaan $c \neq 0$. Jos $P_n(x)$:llä on ainakin yksi nollakohta a, niin edellä todetun mukaan on olemassa sellainen polynomi $P_{n-1}(x)$, että $P_n(x) = (x-a)P_{n-1}(x)$, $P_{n-1}(x)$:n aste on $n-1$ ja sen korkeimman asteen termin kerroin on c. Tulon nollasäännön mukaan kaikki muut $P_n(x)$:n nollakohdat kuin a ovat $P_{n-1}(x)$:n nollakohtia. Jos niitä on, niin samaa ajatusta voidaan soveltaa $P_{n-1}(x)$:ään tuottaen $P_{n-2}(x)$ ja niin edelleen. Tämä loppuu viimeistään, kun jäljellä on pelkkä vakiotermi $P_0(x) = c$. Sillä ei ole nollakohtia. □

Miksi [67]:n kannalta on tärkeää, että nollapolynomin asteeksi määriteltiin -1 eikä sama kuin muiden vakiopolynomien aste eli 0? 201

Edellä yhden muuttujan polynomi jaettiin kahteen tekijään, joista toinen on muotoa $x - a$. Yhden muuttujan polynomeja voi kuitenkin jakaa paljon yleisemmin. Sen käsittelemistä varten tarvitsemme aputuloksen.

Apulause. Jos $A(x) = a_n x^n + \ldots + a_0$ ja $B(x) = b_m x^m + \ldots + b_0$, missä $a_n \neq 0$, $b_m \neq 0$ ja $n \geq m$, niin $A(x) - \frac{a_n}{b_m} x^{n-m} B(x)$ on polynomi, jonka aste on pienempi kuin n. [68]

Todistus. Koska $b_m \neq 0$ on $\frac{a_n}{b_m}$ määritelty vakio, ja koska $n \geq m$ on x^{n-m}:n eksponentti luonnollinen luku. Osittelulailla, kertolaskun vaihdannaisuudella ja liitännäisyydellä, koska x^n tarkoittaa kertolaskua $xx \cdots x$ missä x toistuu n kertaa, samanmuotoiset termit yhdistämällä ja koska $(a_n - \frac{a_n b_m}{b_m})x^n = (a_n - a_n)x^n = 0x^n = 0$ ja $0 + \ldots = \ldots$ saadaan

$$\begin{aligned} A(x) - \tfrac{a_n}{b_m} x^{n-m} B(x) &= A(x) - \tfrac{a_n}{b_m} x^{n-m} (b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0) \\ &= (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0) - (\tfrac{a_n b_m}{b_m} x^n + \tfrac{a_n b_{m-1}}{b_m} x^{n-1} + \ldots + \tfrac{a_n b_0}{b_m} x^{n-m}) \\ &= (a_{n-1} - \tfrac{a_n b_{m-1}}{b_m}) x^{n-1} + \ldots + (a_{n-m} - \tfrac{a_n b_0}{b_m}) x^{n-m} + a_{n-m-1} x^{n-m-1} + \ldots + a_0 \end{aligned}$$

□

Minkä tahansa kokonaisluvun voi jakaa millä tahansa nollasta poikkeavalla kokonaisluvulla niin että tulokseksi saadaan osamäärä ja jakojäännös. Jakojäännös on vähintään 0 ja pienempi kuin jakajan itseisarvo. Myös minkä tahansa yhden muuttujan polynomin voi jakaa millä tahansa muulla yhden muuttujan polynomilla kuin nollapolynomilla. Tulokseksi saadaan kaksi yhden muuttujan polynomia, joita kutsutaan osamääräksi ja jakojäännökseksi. Jakojäännöksen aste on pienempi kuin jakajan aste. Jako menee tasan jos ja vain jos jakojäännös on nollapolynomi. Tämäkin tulos seuraa kunta-aksioomista. Siksi se pätee kaikissa kunnissa. Sitä kutsutaan yhden muuttujan polynomien *jakoyhtälöksi*.

Lause. Jos $A(x)$ ja $B(x)$ ovat yhden muuttujan polynomeja eikä $B(x)$ ole nollapolynomi, niin on olemassa sellaiset yhden muuttujan polynomit $Q(x)$ ja $R(x)$, että $A(x) = B(x)Q(x) + R(x)$ ja $R(x)$:n aste on pienempi kuin $B(x)$:n aste. [69]

Todistus. Induktion pohjatapaus: jos $A(x)$:n aste on pienempi kuin $B(x)$:n aste, niin jakoyhtälö toteutuu valinnoilla $Q(x) = 0$ ja $R(x) = A(x)$.

Induktioaskel: Muussa tapauksessa $A(x)$:n aste on vähintään sama kuin $B(x)$:n aste, joten $A(x)$ ei ole nollapolynomi. Apulauseen [68] mukaan $A(x) - \frac{a_n}{b_m}x^{n-m}B(x)$ on polynomi, joka on pienempää astetta kuin $A(x)$. Induktio-oletuksen mukaan on olemassa sellaiset $Q'(x)$ ja $R(x)$, että $A(x) - \frac{a_n}{b_m}x^{n-m}B(x) = B(x)Q'(x) + R(x)$ ja $R(x)$:n aste on pienempi kuin $B(x)$:n aste. Niinpä $A(x) = B(x)\big(\frac{a_n}{b_m}x^{n-m} + Q'(x)\big) + R(x)$, joten lause toteutuu valinnalla $Q(x) = \frac{a_n}{b_m}x^{n-m} + Q'(x)$. □

Tulokset kuten [54], [67] ja [69], jotka voidaan johtaa käyttäen pelkästään kunta-aksioomia ja logiikan yleisiä lakeja, pätevät kaikissa kunnissa. Tämä on hyödyllistä, koska on olemassa paljon muitakin tärkeitä kuntia kuin lukusuorat luvut.

Kaikkein pienin kunta saadaan kokonaislukujen parillisuudesta ja parittomuudesta. Voidaan todistaa, että kahden kokonaisluvun summan parillisuus / parittomuus riippuu vain yhteenlaskettavien parillisuudesta / parittomuudesta, ja sama pätee kahden kokonaisluvun tulolle. Esimerkiksi parillinen plus pariton on aina pariton. Se on merkitty valmiiksi alla olevaan taulukkoon, jossa ”nen” tarkoittaa, että luku on parillinen, ja ”ton” että se on pariton. Täydennä taulukot! 202

+	nen	ton
nen		ton
ton		

·	nen	ton
nen		
ton		

Tämän pienempää kuntaa ei voi olla, koska [64]:n vuoksi jokaisessa kunnassa on ainakin kaksi eri alkiota, nimittäin 0 ja 1. Nähdäksemme, että tämä todellakin on kunta, kirjoitamme taulukot uudelleen niin että ”nen” korvataan 0:lla ja ”ton” 1:llä:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Ensimmäisestä taulukosta on helppo katsoa, että $0+1 = 1+0$ ja $1+0 = 0+1$. Sen, että $0+0 = 0+0$ ja $1+1 = 1+1$, tietää taulukkoa katsomattakin. Muita tapauksia ei ole. Siksi aina $a+b = b+a$, eli [56] pätee. Aksiooma [60] voidaan tarkastaa vastaavasti toisesta taulukosta. Miten voidaan mistä tahansa samankaltaisesta taulukosta katsoa, toteuttaako se vaihdantalain? 203

Edellä olevista taulukoista on helppo tarkastaa myös, että jokaiselle luvulle a pätee $a+0 = a$ ja $a \cdot 1 = a$, eli että [58] ja [62] pätevät. Miten nähdään helposti, että aina $a \cdot 1 = a$? Tulemme jatkossa tarvitsemaan myös, että jokaiselle luvulle a pätee $0+a = a$, 204
$1a = a$, $0a = 0$ ja $a \cdot 0 = 0$. Nekin on helppo tarkastaa taulukoista. Kaksi ensimmäistä saa vaihtoehtoisesti jo tarkastetuilla laeilla [58] ja [56] sekä [62] ja [60]. Miten nähdään helposti, että aina $0a = a$? 205

Jos $a = 0$, niin $(a+b)+c = (0+b)+c = b+c = 0+(b+c) = a+(b+c)$. Vastaava pätee myös kun $b = 0$ tai $c = 0$. Koska muita alkioita ei ole kuin 0 ja 1, on jäljellä enää yksi tapaus, nimittäin $a = b = c = 1$. Taulukon mukaan $1+1 = 0$, joten $(1+1)+1 = 0+1 = 1 = 1+0 = 1+(1+1)$. Niinpä [57] pätee.

Samaan tyyliin [61] pätee, koska jos $a = 0 \vee b = 0 \vee c = 0$ niin $(ab)c = 0 = a(bc)$, ja $(1 \cdot 1) \cdot 1 = 1 = 1(1 \cdot 1)$, eikä nytkään muita tapauksia ole.

Aksiooma [64] seuraa siitä, että 0 ja 1 ilmoitettiin eri alkioiksi eikä missään ole vedottu siihen, että ne olisivat sama alkio.

Laki [59] vaatii, että jokaisella luvulla on vastaluku. Miten sen voi tarkastaa? 206

Tarkasta [65]! 207

Mitä vielä pitää tehdä, että on tarkastettu, että edellä olevat taulukot muodostavat kunnan? Tee se! 208

Sama kunta voidaan löytää myös propositiologiikasta jopa kahdella tavalla. Miten? 209

Tämä järjestelmä on esimerkki kunnasta, jossa $1 + 1 = 0$. Koska sellainen kunta on olemassa, ei kunta-aksioomista seuraa, että $1 + 1 \neq 0$. Siksi tehtävässä 189 oli pakko olettaa erikseen, että $2 \neq 0$.

Tässä kunnassa on siis kaksi alkiota. Se on esimerkki äärellisestä kunnasta. Kunta on äärellinen, jos ja vain jos siinä on äärellinen määrä alkioita. Äärellisiä kuntia käytetään paljon salausmenetelmissä sekä digitaalisessa tietoliikenteessä. On olemassa 3-alkioinen kunta, 4-alkioinen kunta ja 5-alkioinen kunta, mutta ei 6-alkioista kuntaa. Nimittäin on olemassa äärellinen kunta, jossa on n alkiota, jos ja vain jos n on muotoa alkuluku potenssiin positiivinen kokonaisluku. Mikä on kolmanneksi pienin sellainen positiivinen kokonaisluku n, että ei ole olemassa kuntaa, jossa on n alkiota? 210

Kunnassa on helppo todistaa, että $a+x = a+y \Rightarrow x = y$ ja $x+a = y+a \Rightarrow x = y$. Todista ne. Kussakin askeleessa saat käyttää vain logiikan yleisiä lakeja sekä enintään yhtä kunta-aksioomaa, mutta saat käyttää samaa aksioomaa monesti samassa askeleessa. Käyttämiäsi logiikan lakeja ja kunta-aksioomia ei tarvitse mainita. 211

Miten edellisen tehtävän tulokset näkyvät äärellisen kunnan yhteenlaskutaulussa? 212

Kolmialkioisia kuntia on täsmälleen yksi. Anna sen yhteenlasku- ja kertotaulu! Ei tarvitse tarkastaa kunta-aksioomien toteutumista, vaan riittää, että perustelet, että mikään muu yhteenlaskutaulu ja mikään muu kertotaulu eivät voi olla oikein. 213

Lukusuoran lukujen kunta on ääretön, eli siinä on äärettömästi alkioita. Lukusuoran lukujen sisällä on monia äärettömiä kuntia, pienimpänä rationaaliluvut. On myös olemassa äärettömiä kuntia, jotka eivät sisällä rationaalilukujen kuntaa.

Eräs tekniikassa ja luonnontieteissä hyvin tärkeä ääretön kunta on *kompleksiluvut* (*complex numbers*). Se saadaan ottamalla käyttöön uusi, lukusuoran ulkopuolinen luku i, jolle pätee $ii = -1$ (eli $i^2 = -1$), ja hyväksymällä luvuiksi yhdistelmät muotoa $a+bi$, missä a ja b ovat lukusuoran lukuja. Pätee $(a+bi)+(c+di) = (a+c)+(b+d)i$, $-(a+bi) = (-a)+(-b)i$, $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$ ja $\frac{1}{a+bi} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$. Koska tulos, että n:nnen asteen polynomilla on korkeintaan n nollakohtaa pätee kaikissa kunnissa, se pätee myös kompleksilukujen kunnassa. Kompleksiluvuilla jokaisella muulla polynomilla kuin vakiopolynomeilla on nollakohta.

3.3 Suuruusjärjestys ja epäyhtälöt

Tässä alaluvussa on tällä hetkellä vain reaalilukujen järjestysaksioomat ilman taustojen pohdintaa tai esimerkkejä niiden käyttämisestä päättelemisessä. Ehkä joskus tätä alalukua ehditään muokata niin, että se muodostaa mielekkään kokonaisuuden.

Reaalilukujen järjestysaksioomat on näytetty kuvassa 36. Ne määrittelevät relaation $<$. Muut kolme tuttua järjestysrelaatiota voi määritellä vaikka näin:

$$a > b \Leftrightarrow b < a \qquad a \leq b \Leftrightarrow a < b \vee a = b \qquad a \geq b \Leftrightarrow b < a \vee a = b$$

Jokaiselle luvulle a, b ja c pätee:

[70] täsmälleen yksi seuraavista: $a < b$, $a = b$ ja $b < a$
[71] $a < b \land b < c \;\Rightarrow\; a < c$
[72] $a < b \;\Rightarrow\; a + c < b + c$
[73] $0 < a \land 0 < b \;\Rightarrow\; 0 < ab$

Kuva 36: Lukusuoran lukujen järjestysaksioomat

Reaaliluvuilla pätee myös $a \leq b \Leftrightarrow \neg(b < a)$ ja $a \geq b \Leftrightarrow \neg(a < b)$.

Vahtoehtoisesti voidaan määritellä ensiksi $\leq$ seuraavasti:

$$a = b \;\Leftrightarrow\; a \leq b \land b \leq a \qquad a \leq b \lor b \leq a \qquad a \leq b \land b \leq c \;\Rightarrow\; a \leq c$$

Niistä saadaan $<$ yhtäpitävyydellä $a < b \Leftrightarrow a \leq b \land \neg(a = b)$.

3.4 Kokonaislukujen ominaisuuksia

Tässä alaluvussa on tällä hetkellä vain asioita, joita tarvitaan myöhemmin. Siksi tämä alaluku on sekalainen kokoelma yksittäisiä tosiasioita. Ehkä joskus tätä alalukua ehditään muokata niin, että se muodostaa mielekkään kokonaisuuden.

Kokonaislukujen joukkoa merkitään $\mathbb{Z}$ ja luonnollisten lukujen joukkoa $\mathbb{N}$. Luonnollisia lukuja ovat 0, 1, 2 ja niin edelleen, ja kokonaislukuja ovat kaikki luonnolliset luvut ja niiden vastaluvut, siis $\ldots\ -2, -1, 0, 1, 2, \ldots$. Niinpä luonnolliset luvut ovat nolla ja positiiviset kokonaisluvut. (Joillakin matematiikan aloilla nolla jätetään pois luonnollisista luvuista. Tietojenkäsittelytieteessä ja matemaattisessa logiikassa nolla on lähes aina mukana luonnollisissa luvuissa.)

Kokonaisluvuilla pätee $a < b \Leftrightarrow a + 1 \leq b$. Reaaliluvuilla se ei päde.

Jos m ja n ovat kokonaislukuja ja $n \neq 0$, niin on olemassa yksikäsitteiset kokonaisluvut $m \operatorname{div} n$ ja $m \bmod n$, joita kutsutaan nimillä *osamäärä* (*quotient*) ja *jakojäännös* (*remainder*), ja joille pätee *jakoyhtälö*:

Jos $m \in \mathbb{Z}$, $n \in \mathbb{Z}$ ja $n \neq 0$, niin $m \;=\; n(m \operatorname{div} n) + (m \bmod n)$ ja $0 \leq m \bmod n < |n|$. [74]

Jakoyhtälön todistamiseksi täytyy osoittaa, että ehdot täyttävät $m \operatorname{div} n$ ja $m \bmod n$ ovat olemassa ja yksikäsitteiset. Yksikäsitteisyyden todistamme lopuksi. Muun todistamme ensin ei-negatiivisille m ja positiivisille n, sitten laajennamme sen negatiivisille m ja lopuksi myös negatiivisille n. Vetoamme ensimmäisen tapauksen todistuksessa seuraavaan tietokoneohjelmaan, josta todistamme, että jos $m \geq 0$ ja $n > 0$, niin se laskee jakoyhtälön toteuttavat $m \operatorname{div} n$ ja $m \bmod n$:

```
1  r := m; q := 0
2  while r ≥ n do r := r − n; q := q + 1
```

Todistus. Kun ohjelma on lopettanut, missä muuttujassa on $m \operatorname{div} n$ ja missä $m \bmod n$? 214
Miksi on varmaa, että m:n ja n:n arvot eivät muutu ohjelman suorituksen aikana? 215

Osoitamme, että aina rivin 2 alussa pätee $m = nq + r$.

- Kun riville 2 tullaan ensimmäisen kerran, se pätee, koska silloin rivin 1 vuoksi $r = m$ ja $q = 0$, joten $nq + r = 0 + r = m$.

- Kun riville 2 tullaan myöhemmin, se tapahtuu suorittamalla rivi 2. Olkoot q ja r arvot rivin 2 suorituksen alussa ja q' ja r' rivin 2 lopussa. Ohjelman koodin mukaan $r' = r - n$ ja $q' = q + 1$. Jos $m = nq + r$, saamme $nq' + r' = n(q+1) + (r-n) = nq+n+r-n = nq+r = m$, joten $nq' + r' = m$. Rivin 2 lopusta siirrytään rivin 2 alkuun muuttamatta muuttujien arvoja, joten jos $m = nq + r$ pätee rivin 2 alussa, niin se pätee myös kun suoritus on seuraavan kerran rivin 2 alussa.

- Olemme osoittaneet, että $m = nq + r$ pätee kun suoritus on ensimmäisen kerran rivin 2 alussa; ja että jos se pätee jollakin kerralla kun suoritus on rivin 2 alussa, niin se pätee seuraavallakin kerralla. Niistä yhdessä seuraa, että $m = nq + r$ pätee aina kun suoritus on rivin 2 alussa.

Olemme osoittaneet, että jakoyhtälön alkuosa pätee aina rivin 2 alussa. Jos ohjelma lopettaa, niin se pätee myös ohjelman lopussa, koska ainoa tapa lopettaa on todeta rivillä 2, että **while**-silmukan ehto ei päde, ja siirtyä suoraan loppuun tekemättä mitään muuta. Vielä tarvitsee osoittaa, että ohjelma varmasti lopettaa, ja että silloin myös jakoyhtälön loppuosa pätee.

Osoitamme seuraavaksi, että ohjelma lopettaa joskus. Sitä varten ei tarvitse laskea **while**-silmukan kierrosten määrää tarkasti, vaan riittää perustella, että ennemmin tai myöhemmin **while**-silmukan ehto $r \geq n$ ei päde. Koska $n > 0$, pienenee r joka kierroksella ainakin ykkösellä. Siksi viimeistään m kierroksen jälkeen $r \leq 0 < n$, jolloin **while**-silmukan ehto ei päde.

Osoita, että aina rivin 2 alussa $r \geq 0$! 216

Ohjelman lopetettua pätee kaikki se mikä pätee aina rivin 2 alussa ja lisäksi **while**-silmukan ehdon $r \geq n$ negaatio. Siksi ohjelman lopetettua pätee $m = nq + r$, $r \geq 0$ ja $r < n$. Niinpä ohjelman lopetettua jakoyhtälö pätee. □

Muuta ohjelma sellaiseksi, että se tuottaa oikean vastauksen myös kun $m < 0$ ja $n > 0$ (siis m saa olla mikä tahansa kokonaisluku, mutta n on positiivinen)! Todista muutettu 217
ohjelma oikeaksi lyhyesti. Siinä määrin kuin mahdollista, yksityiskohtien esittämisen sijaan vetoa samankaltaisuuteen jo tehtyjen päätelmien kanssa! 218

Mitä muutettu ohjelma tekee, jos $n \leq 0$? 219

Negatiivisilla n toimii ohjelma, joka on muuten samanlainen kuin muutettu ohjelma, mutta rivin 2 **while**-silmukan ehtona on $r < 0$ ja rivin 3 **while**-silmukan ehtona on $r \geq -n$. Rivillä 2 r kasvaa, koska siitä vähennetään negatiivinen luku. Riviltä poistutaan kun r on tarpeeksi suuri. Rivillä 3 r vähenee. Riviltä poistutaan kun r on tarpeeksi pieni, mikä tässä tapauksessa tarkoittaa $r < -n$, koska jakoyhtälön loppu vaatii että $r < |n|$, ja nyt $|n| = -n$ koska $n < 0$. Koska tämä ohjelma toimii oikein kun $n < 0$, toteutuu jakoyhtälö myös negatiivisilla n.

Lopuksi osoitamme, että q ja r ovat yksikäsitteiset. Olkoon $nq + r = m = nq' + r'$. Lisäämällä molemmille puolille $-nq - r'$ ja käyttämällä osittelulakia saadaan $r - r' = n(q' - q)$. Jos $q = q'$, niin $r - r' = n(q' - q) = 0$. Silloin myös $r = r'$, joten $(q, r) = (q', r')$. Muussa tapauksessa $q \neq q'$. Silloin $|q' - q| \geq 1$ ja $|r - r'| = |n||q' - q| \geq |n|$. Toisaalta [74]:n mukaan $-r' \leq 0$ ja $r < |n|$, joten $r - r' < |n|$; ja $r \geq 0$ ja $-r' > -|n|$, joten $r - r' > -|n|$. Siksi $|r - r'| < |n|$. Olemme johtaneet sekä $|r - r'| \geq |n|$ että $|r - r'| < |n|$. Se on ristiriita, joten ei voi olla $q \neq q'$.

Jos $k \in \mathbb{Z}$, niin jakoyhtälön mukaan

$$m + kn = n(m \operatorname{div} n) + (m \bmod n) + kn = n((m \operatorname{div} n) + k) + (m \bmod n)$$

joten $(m + kn) \operatorname{div} n = (m \operatorname{div} n) + k$ ja $(m + kn) \bmod n = m \bmod n$.

Lasku m jaettuna n:llä *menee tasan* eli m on n:n *monikerta* jos ja vain jos $m \bmod n = 0$. Osoita, että jos $n > 0$, niin jokin luvuista m, $m+1$, $m+2$, $\ldots$, $m+n-1$ on n:n monikerta! 220

3.5 Täydellisyysaksiooma

Tätä alalukua ei ole vielä ehditty kirjoittaa. Sen sijaan lue

- `http://users.jyu.fi/~ava/t_0mitta.html` ja
- `http://users.jyu.fi/~ava/t_taydellisyysaksiooma.html`

4 Joukko-oppia

??? Tässä luvussa on tarkoitus kertoa joukko-opin peruskäsitteitä sekä äärettömien joukkojen (yli)numeroituvuudesta sen verran kuin kirjan lopussa tarvitaan.

5 Ensimmäisen kertaluvun predikaattilogiikka

Tämän kirjan loppuosassa keskitytään niin sanottuun ensimmäisen kertaluvun logiikkaan. Se tarkoittaa predikaattilogiikkaa, jossa muuttujat voivat saada arvoikseen vaikka lukuja, mutta ei niistä muodostettuja muita olioita kuten relaatioita ja funktioita. Niin sanotuissa korkeamman kertaluvun logiikoissa muuttujat voivat saada arvoikseen myös relaatioita ja funktioita. Ensimmäisen kertaluvun logiikalla on erittäin hyödyllisiä ominaisuuksia jotka puuttuvat korkeamman kertaluvun logiikoilta. Siksi se predikaattilogiikka, jota eniten käytetään, on nimenomaan ensimmäisen kertaluvun. Silti korkeamman kertaluvun logiikat eivät ole pelkkä akateeminen kuriositeetti, vaan jotkut käyttävät sovelluksissa niitäkin.

5.1 Kvanttorit

Tämänkin alaluvun kirjoittaminen on kesken.

Kaava $\forall x : \varphi$ tarkoittaa, että φ pätee, sijoitetaanpa x:ään mikä tahansa puheenaiheen piiriin kuuluva arvo. Esimerkiksi reaalilukujen tapauksessa $\forall x : x^2 \geq 0$ tarkoittaa väitettä, että jokaisen reaaliluvun neliö on ei-negatiivinen. Se on tosi väite. Kaava $\exists x : \varphi$ tarkoittaa, että on olemassa ainakin yksi sellainen arvo, että kun se sijoitetaan x:n tilalle φ:ssä, saadaan tosi kaava. Esimerkiksi $\exists x : x^2 = 2$ on tosi reaaliluvuille (koska $\sqrt{2}$ ja $-\sqrt{2}$ toteuttavat $x^2 = 2$), mutta ei ole tosi kokonaisluvuille (minkään kokonaisluvun neliö ei ole 2). Symbolin $\forall$ nimi on *kaikkikvanttori* (*universal quantifier*), ja $\exists$ on *olemassaolokvanttori* (*existential quantifier*).

Kaavojen muotoa $\forall x : \exists y : \varphi$ ymmärtämistä saattaa auttaa ajatella niitä peleinä. Ensimmäisen pelaajan on valittava x:n arvo ja toisen pelaajan on valittava y:n arvo. Kaava on tosi jos ja vain jos valitsipa ensimmäinen pelaaja x:ksi minkä arvon tahansa, pystyy toinen pelaaja aina valitsemaan sellaisen y:n, että φ on tosi. Kaava on epätosi jos ja vain jos ensimmäinen pelaaja voi valita sellaisen x, että mikään valinta y:ksi ei saa φ:stä totta. Esimerkiksi $\forall x : \exists y : y > x$ on luonnollisilla luvuilla tosi, sillä valitseepa ensimmäinen pelaaja minkä luonnollisen luvun tahansa, pystyy toinen pelaaja valitsemaan sitä suuremman luonnollisen luvun (hän voi valita vaikka $x+1$). Sen sijaan

$\forall x : \exists y : y < x$ on luonnollisilla luvuilla epätosi, sillä jos ensimmäinen pelaaja valitsee 0, ei mikään valinta kelpaa y:ksi, sillä mikään luonnollinen luku ei ole pienempi kuin nolla.

Muuttujan x esiintymä kaavassa on *sidottu* (*bound*), jos ja vain jos se sijaitsee osakaavassa muotoa $\forall x : \ldots$ tai $\exists x : \ldots$. Esiintymä on *vapaa* (*free*), jos ja vain jos se ei ole sidottu. Esimerkiksi x esiintyy vapaana ja y sidottuna kaavassa $\exists y : 0 < y < x$. Usein sana "esiintyä" jätetään pois, eli puhutaan vapaista ja sidotuista muuttujista.

On hyödyllistä ajatella, että jokainen kvanttori luo uuden muuttujan, joka on eri kuin kaikki vapaat muuttujat ja kaikki muiden kvanttorien luomat muuttujat, vaikka sillä sattuisi olemaan sama nimi. Esimerkiksi $(\exists x : (\forall x : x^2 \neq 2) \vee x^2 = 2) \wedge x \neq 1 \wedge (\forall x : x^2 > 0 \vee x = 0) \vee x = 1$ sisältää neljä eri muuttujaa, joiden nimi on x. Vapaa x esiintyy osakaavoissa $x \neq 1$ ja $x = 1$. Yksi sidottu x esiintyy kohdissa $\exists x : (\ldots) \vee x^2 = 2$, mutta $\ldots$:n kohdalla olevan osakaavan x:t ovat toinen, eri sidottu x. Kolmas sidottu x esiintyy osakaavassa $\forall x : x^2 > 0 \vee x = 0$.

Usein kannattaa selvyyden vuoksi antaa saman kaavan eri muuttujille eri nimet, mutta tämä ei ole ehdoton sääntö, koska nimistä saattaa tulla pulaa, ja toisinaan saman nimen käyttö samankaltaisissa osakaavoissa saattaa selkeyttää kaavaa. Esimerkiksi "on olemassa parillinen luku ja on olemassa pariton luku" on luontevaa ilmaista $(\exists n : \exists k : n = 2k) \wedge (\exists n : \exists k : n = 2k+1)$. Mitkä seuraavista kaavoista ovat tosia kokonaisluvuilla?

$$(\exists n : \exists k : n = 2k) \wedge (\exists n : \exists k : n = 2k+1)$$ 221

$$\exists n : ((\exists k : n = 2k) \wedge (\exists k : n = 2k+1))$$ 222

$$\exists n : ((\exists k : n = 2k) \wedge (\exists k : n = 3k))$$ 223

Kaava on *suljettu* (*closed*), jos ja vain jos siinä ei ole vapaita muuttujien esiintymiä. Kaava on *avoin* (*open*), jos ja vain jos se ei ole suljettu. Esimerkiksi $\exists y : 0 < y < x$ on avoin, koska x esiintyy siinä vapaana, mutta $\forall x : x > 0 \rightarrow \exists y : 0 < y < x$ on suljettu. Suljetun kaavan totuusarvo riippuu vain puheenaiheesta. Esimerkiksi $\forall x : x > 0 \rightarrow \exists y : 0 < y < x$ on reaaliluvuilla tosi (koska esimerkiksi $\frac{x}{2}$ kelpaa y:ksi) ja kokonaisluvuilla epätosi (koska kun $x = 1$, niin $x > 0$ mutta ei ole olemassa kokonaislukua y jolle $0 < y < 1$). Avoimen kaavan totuusarvo voi lisäksi riippua vapaiden muuttujien arvoista. Esimerkiksi reaaliluvuilla $\exists y : 0 < y < x$ on tosi kun $x = 1$ (perustele!) mutta epätosi 224
kun $x = 0$ (perustele!). 225

Lauseke f on *sijoitettavissa muuttujaan x kaavassa $\varphi(x)$* (*substitutable / free for x in $\varphi(x)$*) jos ja vain jos mikään f:ssä esiintyvistä muuttujista ei joudu sidotuksi $\varphi(f)$:ssä. Jollei tämä ehto toteudu, niin f:n sijoittaminen x:n tilalle toteen kaavaan $\varphi(x)$ voi johtaa epätoteen lopputulokseen. Esimerkiksi aina todesta kaavasta $\exists y : y > x$ (on olemassa luku, joka on suurempi kuin x) tulee epätosi, jos x:n tilalle sijoitetaan y, koska siitä tulee $\exists y : y > y$ (on olemassa luku, joka on itseään suurempi). Tämä on jälleen esimerkki siitä, että täytyy varoa sekoittamasta toisiinsa eri muuttujia, joilla on sama nimi.

Ehkä havainnollisempi esimerkki saadaan kokonaisluvuilla kaavasta $x > 1 \rightarrow \exists y : 0 < y < x$. Se on tosi kun $x = 2$, mutta kun siihen sijoitetaan x:n tilalle y, saadaan $y > 1 \rightarrow \exists y : 0 < y < y$, joka ei ole tosi kun $y = 2$. Kaavassa $x > 1 \rightarrow \exists y : 0 < y < x$ molemmat x ovat saman vapaan muuttujan x esiintymiä, ja molemmat y ovat saman sidotun muuttujan y esiintymiä. Kaavassa $y > 1 \rightarrow \exists y : 0 < y < y$ vain ensimmäinen y on vapaan muuttujan y esiintymä, ja muut kolme y:tä ovat sidotun muuttujan y esiintymiä, joka on eri muuttuja kuin vapaana esiintyvä y. Ennen sijoitusta kaavan viimeinen muuttuja oli sama kuin ensimmäinen, mutta sijoituksen jälkeen ei, koska se sekottui toiseen samannimiseen muuttujaan (sidottu y).

Millä x:n arvoilla $x > 1 \rightarrow \exists y : 0 < y < x$ on tosi kokonaislukujen tapauksessa? 226
Millä y:n arvoilla $y > 1 \rightarrow \exists y : 0 < y < y$ on tosi kokonaislukujen tapauksessa? 227
Perustele tehtävän 226 vastaus! 228
Perustele tehtävän 227 vastaus! 229

Jos f ei ole sijoitettavissa muuttujaan x kaavassa $\varphi(x)$, niin ongelma korjaantuu vaihtamalla sidottujen muuttujien nimiä $\varphi(x)$:ssä. Nimittäin

Jos y ei esiinny $\varphi(x)$:ssä, niin $\forall x : \varphi(x) \Leftrightarrow \forall y : \varphi(y)$ ja $\exists x : \varphi(x) \Leftrightarrow \exists y : \varphi(y)$. [75]

Tämä laki on helppo muistaa ajattelemalla, että kvantifioidun muuttujan nimi ei ole tärkeä, tärkeää on vain että muuttuja ei sekoitu muihin muuttujiin. Lain [75] y tulee x:n niiden ja vain niiden esiintymien tilalle, jotka ovat vapaita $\varphi(x)$:ssä. Muut x:n esiintymät tarkoittavat eri muuttujaa kuin vapaana esiintyvä x, joten on oikein, että y ei tule niiden tilalle. Vapaan muuttujan x tilalle tuleva y ei voi sekoittua muihin $\varphi(x)$:ssä esiintyviin muuttujiin nimeltä y, koska oletuksen mukaan sellaisia ei ole.

Vastaavasti kaava ψ on sijoitettavissa X:ään kaavaskeemassa $\varphi(X)$ jos ja vain jos mikään ψ:ssä vapaana esiintyvistä muuttujista ei joudu sidotuksi $\varphi(\psi)$:ssä. Nytkin, jos ψ ei ole sijoitettavissa X:ään $\varphi(X)$:ssä, niin $\varphi(X)$ voidaan [75]:llä muuttaa yhtäpitäväksi kaavaksi, jossa ψ on sijoitettavissa X:ään.

Peräkkäisten samanlaisten kvanttorien järjestyksellä ei ole väliä:

$$\forall x : \forall y : \varphi \Leftrightarrow \forall y : \forall x : \varphi \qquad \exists x : \exists y : \varphi \Leftrightarrow \exists y : \exists x : \varphi \qquad [76]$$

Kvanttorien De Morganin lait ovat todella hyödyllisiä. Ne on helppo muistaa ajattelemalla tyyliin ”jos ei ole niin, että kaikki jäätelöt ovat hyviä, niin on olemassa paha jäätelö, ja jos on olemassa paha jäätelö, niin ei ole niin, että kaikki jäätelöt ovat hyviä.”

$$\neg\forall x : \varphi \Leftrightarrow \exists x : \neg\varphi \qquad \neg\exists x : \varphi \Leftrightarrow \forall x : \neg\varphi \qquad [77]$$

Seuraavat on melkeinpä helpompi keksiä ja perustella kun niitä sattuu tarvitsemaan, kuin muistaa. Niistä ensimmäinen sanoo esimerkiksi, että ”jokaisena päivänä aurinko paistaa ja linnut laulavat, jos ja vain jos jokaisena päivänä aurinko paistaa ja jokaisena päivänä linnut laulavat”. Viides sanoo esimerkiksi, että ”vesi on märkää ja jokaisena päivänä aurinko paistaa, jos ja vain jos jokaisena päivänä vesi on märkää ja aurinko paistaa”. Tässä esimerkissä se, että x ei esiinny vapaana φ:ssä, vastaa sitä, että ilmauksessa ”vesi on märkää” ei ole muuttujaa, joka saa arvokseen päivämäärän (toisin kuin ilmauksessa ”tänään aurinko paistaa”, jossa ”tänään” on sellainen muuttuja).

$$\forall x : \varphi \wedge \psi \Leftrightarrow (\forall x : \varphi) \wedge (\forall x : \psi) \qquad \exists x : \varphi \vee \psi \Leftrightarrow (\exists x : \varphi) \vee (\exists x : \psi) \qquad [78]$$

Jos x ei esiinny vapaana φ:ssä, niin

$$\begin{array}{cc} \forall x : \varphi \Leftrightarrow \varphi & \exists x : \varphi \Leftrightarrow \varphi \\ \varphi \wedge \forall x : \psi \Leftrightarrow \forall x : \varphi \wedge \psi & \varphi \vee \forall x : \psi \Leftrightarrow \forall x : \varphi \vee \psi \\ \varphi \wedge \exists x : \psi \Leftrightarrow \exists x : \varphi \wedge \psi & \varphi \vee \exists x : \psi \Leftrightarrow \exists x : \varphi \vee \psi \end{array} \qquad [79]$$

Seuraavasta laista on tärkeää muistaa, että se on yksisuuntainen. On eri asia että jokainen oppilas pitää jostain oppiaineesta kuin että jostain oppiaineesta pitää jokainen oppilas. Jos yksi pitää matematiikasta ja vain siitä, toinen liikunnasta ja vain siitä, ja kolmas pitää molemmista, eikä muita oppilaita eikä oppiaineita ole, niin jokainen oppilas pitää jostain oppiaineesta, mutta ei ole oppiainetta josta jokainen oppilas pitää. Jos jokainen oppilas pitää äidinkielestä, niin jostain oppiaineesta pitää jokainen oppilas. On totta että $\forall y : \exists x : x > y$, mutta $\exists x : \forall y : x > y$ ei ole tosi.

$$\exists x : \forall y : \varphi \Rightarrow \forall y : \exists x : \varphi \qquad [80]$$

Onko $\exists x : \forall y : \varphi \Rightarrow \forall x : \exists y : \varphi$ pätevä jokaisella kaavalla φ? Perustele! 230

Onko $\forall x : \exists y : \varphi \Rightarrow \exists x : \forall y : \varphi$ pätevä jokaisella kaavalla φ? Perustele! 231

Oletetaan, että Jessi syö lomansa jokaisena aurinkoisena päivänä jäätelön. Siitä voi päätellä, että jos jokainen Jessin lomapäivä on aurinkoinen, niin Jessi syö lomansa jokaisena päivänä jäätelön; ja että jos jokin Jessin lomapäivä on aurinkoinen, niin Jessi syö lomansa jonain päivänä jäätelön. Tämä on esimerkki seuraavasta laista.

Jos $\varphi \Rightarrow \psi$, niin $\forall x : \varphi \;\Rightarrow\; \forall x : \psi$ ja $\exists x : \varphi \;\Rightarrow\; \exists x : \psi$. [81]

Päteekö $\exists x : \varphi \wedge \psi \;\Leftrightarrow\; (\exists x : \varphi) \wedge (\exists x : \psi)$? Perustele! 232

Päteekö $\exists x : \varphi \vee \psi \;\Leftrightarrow\; (\exists x : \varphi) \vee (\exists x : \psi)$? Perustele! 233

Seuraavaa lakia käytetään matematiikassa vähän väliä siten, että $\forall$ ei ole kirjoitettu näkyville, vaan jollain muulla tavalla on ilmoitettu, että x edustaa mielivaltaista lukua.

Jos f on määritelty ja sijoitettavissa x:ään $\varphi(x)$:ssä, niin $\forall x : \varphi(x) \;\Rightarrow\; \varphi(f)$. [82]

Esimerkiksi kun sivulla 91 johdettiin $(7-3y^2)+6x = 6x+(7-3y^2)$, niin se tapahtui sijoittamalla [56]:een a:n tilalle $7-3y^2$ ja b:n tilalle $6x$, eli päättelyketjuna $\forall a : \forall b : a+b = b+a \Rightarrow \forall b : (7-3y^2)+b = b+(7-3y^2) \Rightarrow (7-3y^2)+6x = 6x+(7-3y^2)$. Se, että a ja b edustavat mielivaltaisia lukuja, oli sanottu kuvan 35 yläreunassa.

Matematiikassa on tavallista myös tavalla tai toisella ilmaista (tai olettaa, että on sanomattakin selvää) että x edustaa mielivaltaista eli mitä tahansa lukua; päätellä ajatellen, että x edustaa jotakin, koko päättelyn ajan samaa lukua; ja katsoa niin saatu tulos päteväksi kaikille luvulle. Tällainen toiminta vastaa seuraavaa logiikan lakia:

Jos $\varphi(x)$ johdetaan tekemättä mitään oletuksia x:stä, niin $\forall x : \varphi(x)$. [83]

Esimerkiksi voidaan olettaa, että a ja b ovat mitkä tahansa luvut, laskea vähennyslaskun määritelmällä ja kunta-aksioomilla $(a+b)(a-b) = (a+b)(a+-b) = (a+b)a+(a+b)(-b) = aa+ba+a(-b)+b(-b) = \ldots = aa+(b+-b)a+-bb = a^2+0-b^2 = a^2-b^2$, ja julistaa että kaikilla luvuilla a ja b pätee $(a+b)(a-b) = a^2-b^2$ eli että $\forall a : \forall b : (a+b)(a-b) = a^2-b^2$.

Seuraava on välitön seuraus siitä mitä $\exists$ tarkoittaa. Koska $\varphi(x)$ toteutuu f:n tuottamalla arvolla, niin se toteutuu jollakin arvolla.

Jos f on määritelty ja sijoitettavissa x:ään $\varphi(x)$:ssä, niin $\varphi(f) \;\Rightarrow\; \exists x : \varphi(x)$. [84]

(Luvussa 8 tullaan näkemään, että jos käytössä ei ole muita konnektiiveja ja kvanttoreita kuin $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\forall$ ja $\exists$, niin ei tarvita oletusta, että f on määritelty.) Olettaen, että $\exists x : \varphi(x)$ on määritelty, johda [84] De Morganin lailla [82]:sta! 234

Matematiikassa on tavallista antaa nimi jollekin jonka on todettu olevan olemassa, käyttää sitä vähän aikaa päättelyssä ja johtaa lopulta tulos jossa tätä nimeä ei enää käytetä. Esimerkiksi voidaan todistaa, että jos $n \in \mathbb{Z}$, niin $n^2 \bmod 4$ on joko 0 tai 1.

> Kokonaisluku n on joko parillinen tai pariton. Jos n on parillinen, niin on olemassa sellainen $k \in \mathbb{Z}$ että $n = 2k$. Silloin $n^2 \bmod 4 = (4k^2) \bmod 4 = 0$. Jos n on pariton, niin on olemassa sellainen $k \in \mathbb{Z}$ että $n = 2k+1$. Silloin $n^2 \bmod 4 = (4k^2+4k+1) \bmod 4 = 1$. Niinpä $n^2 \bmod 4 = 0 \vee n^2 \bmod 4 = 1$.

Tässä päättelyssä k otettiin kahdesti käyttöön edustamaan jotakin lukua jonka tiedettiin olevan olemassa, ja k esiintyi välivaiheissa mutta ei enää lopputuloksessa. Seuraava laki ilmaisee tämän periaatteen.

Jos $\varphi(y) \Rightarrow \psi$ eikä y esiinny oletuksissa, $(\exists x : \varphi(x))$:ssä eikä ψ:ssä, niin $\exists x : \varphi(x) \Rightarrow \psi$. [85]

Matematiikassa käytetään usein seuraavia lyhennemerkintöjä. Ne ovat käteviä selventämään, mistä joukosta x saa arvonsa.

$$\forall x \in A : \varphi \;\Leftrightarrow\; \forall x : x \in A \to \varphi \qquad\qquad \exists x \in A : \varphi \;\Leftrightarrow\; \exists x : x \in A \land \varphi \qquad [86]$$

Esimerkiksi

$$\forall x \in \mathbb{R} : \forall y \in \mathbb{R} : x < y \to \exists z \in \mathbb{Q} : x < z < y$$

ilmaisee sen ehkä yllättävän tosiasian, että minkä tahansa kahden eri reaaliluvun välissä on rationaaliluku. Mitkä seuraavista ovat tosi? Perustele!

$\forall x \in \mathbb{N} : \exists y \in \mathbb{Q} : x < y < x+1$ 235

$\forall x \in \mathbb{Q} : \exists y \in \mathbb{N} : x \leq y < x+1$ 236

$\forall x \in \mathbb{Q} : \exists y \in \mathbb{Z} : x \leq y < x+1$ 237

$\forall x \in \mathbb{Q} : \exists y \in \mathbb{Z} : x < y < x+1$ 238

Merkintöjä $\forall x \in A : \ldots$ ja $\exists x \in A : \ldots$ käytetään usein samaan tapaan kuin ohjelmointikielten tyyppimäärittelyjä kuten `int n;` ja `double x;`. Niissä yhdistetään varsinaisen puheenaiheen merkintöjä joukko-opin merkintöihin, joten ne eivät ole tulkittavissa tavallisessa predikaattilogiikassa vaan tulkinta vaatisi laajennetun logiikan, joka voi puhua yhtäaikaa esimerkiksi luvuista ja lukujoukoista. Yleensä tällaista laajennettua logiikkaa ei esitetä. Siksi, vaikka $\forall x \in A : \ldots$ ja $\exists x \in A : \ldots$ näyttävät formaaleilta kaavoilta, ne ovat yleensä epämuodollisia ilmauksia. Tämä ei kuitenkaan ole iso ongelma, koska niitä käytetään matematiikassa yleensä siten, että joukkoja koskevat ilmaukset ovat yksinkertaisia ja tarkoitettu merkitys on selvä.

Seuraavat merkinnät ovat melko harvinaisia, mutta hyödyllisiä varsinkin tietokoneohjelmien taulukoista puhuttaessa. Niitä kannattaa käyttää siten, että φ ilmoittaa mitä arvoja taulukon indeksinä käytettävä muuttuja voi saada. Esimerkiksi $\forall i; 1 \leq i < n : A[i] \leq A[i+1]$ sanoo, että taulukko A on kasvavassa suuruusjärjestyksessä indeksistä 1 alkaen indeksiin n saakka. Se sanoo sen sanomalla, että otetaanpa tarkasteltavaksi mikä tahansa muu indeksi tältä väliltä paitsi viimeinen, niin siinä kohdassa oleva alkio on enintään yhtäsuuri kuin seuraavassa kohdassa oleva alkio.

$$\forall x; \varphi : \psi \;\Leftrightarrow\; \forall x : \varphi \to \psi \qquad\qquad \exists x; \varphi : \psi \;\Leftrightarrow\; \exists x : \varphi \land \psi \qquad [87]$$

5.2 Esimerkki: suunnatut graafit

Tässä alaluvussa johdatellaan esimerkin avulla predikaattilogiikan tärkeimpiin käsitteisiin ja annetaan maistiainen alan suurista tuloksista. Jotta teksti olisi helpompi lukea, joidenkin käsitteiden tarkat määritelmät ohitetaan ja korvataan sanallisilla kuvauksilla ja esimerkeillä, joista tämän alaluvun kannalta olennainen toivottavasti välittyy riittävän tarkasti. Näin tehdään vain teknisluontoisten yksityiskohtien osalta — muilta osin pyritään täyteen matemaattiseen tarkkuuteen. Lukijan oletetaan osaavan lukea kvanttoreita $\forall$ ja $\exists$ sisältäviä kaavoja, mutta ei oleteta tietävän sen enempää predikaattilogiikasta. Tähän on yksi poikkeus: eräässä tehtävässä oletetaan, että lukija tietää, että $\neg\exists x : \varphi(x)$ tarkoittaa samaa kuin $\forall x : \neg\varphi(x)$.

Suunnattu graafi (*directed graph*) koostuu *solmuista* (*vertex*) ja *kaarista* (*edge*). Kaari alkaa solmusta ja päättyy solmuun. Kuvassa 37 on kaksi esimerkkiä. Vasemmanpuoleisen esimerkin solmut ovat 1, 2, 3 ja 4. Solmusta 1 on kaari solmuun 2, solmuista 2 ja 4 on kaaret solmuun 3, ja muita kaaria ei ole.

Kuva 37: Kaksi suunnattua graafia

Sen, että solmusta u on kaari solmuun v, merkitsemme $u \rightsquigarrow v$. (Tavallisesti siihen käytetään symbolia $\rightarrow$, mutta se on myös propositiologiikan symboli, joten sekaannusten välttämiseksi emme käytä sitä.) Saman asian voi sanoa sanallisesti myös ”v on u:n seuraaja” ja ”u on v:n edeltäjä”. Merkintää voi ketjuttaa: $v_1 \rightsquigarrow v_2 \rightsquigarrow \cdots \rightsquigarrow v_n$ tarkoittaa $v_1 \rightsquigarrow v_2 \wedge v_2 \rightsquigarrow v_3 \wedge \cdots \wedge v_{n-1} \rightsquigarrow v_n$. Kuvan 37 oikeanpuoleiselle esimerkille pätee muun muassa $3 \rightsquigarrow 1 \rightsquigarrow 2 \rightsquigarrow 3 \rightsquigarrow 1$.

Polku (*path*) tarkoittaa sellaista jonoa $v_1 v_2 \cdots v_n$ solmuja, että $v_1 \rightsquigarrow v_2 \rightsquigarrow \cdots \rightsquigarrow v_n$. Toisin sanoen, polun jokaisesta muusta solmusta kuin viimeisestä on kaari polulla seuraavaan solmuun. Myös yksittäinen solmu kelpaa poluksi. Polku voi olla toiseen tai molempiin suuntiin ääretön. Merkintä $u \rightsquigarrow^* v$ tarkoittaa, että solmusta u on polku solmuun v. (Sanojen ”polku” ja ”path” merkitys vaihtelee kirjallisuudessa. Osassa lähteistä ne ovat kaarten tai solmujen ja kaarten jonoja. Osa lähteistä kieltää solmuja toistumasta polulla. Nämä erot eivät onneksi vaikuta käsitteeseen $u \rightsquigarrow^* v$.)

Kuvan 37 vasemmanpuoleisessa esimerkissä on kahdeksan polkua. Mitkä ne ovat? 239
Oikeanpuoleisessa esimerkissä on äärettömän monta polkua.

Kuvitelkaamme laatikkoa, jossa on piilossa suunnattu graafi. Sen solmujen niminä ovat luvut $1, 2, \ldots$ niin pitkälle kuin solmuja riittää. Laatikolle voi toistuvasti näppäillä kaksi positiivista kokonaislukua u ja v ja painaa nappia, jolloin laatikko vastaa ”kyllä” tai ”ei” sen mukaan päteekö $u \rightsquigarrow v$. Käyttäjä ei tiedä, paljonko solmuja on, mutta tietää, että niitä on ainakin yksi. Jos näppäilty u tai v on suurempi kuin minkään solmun nimi, niin laatikko vastaa ikään kuin sen sijaan olisi näppäilty 1. Käyttäjä ei siis tiedä etukäteen tarkoittaako esimerkiksi 7 samaa vai eri solmua kuin 1.

Tehtävänä on selvittää, päteekö $1 \rightsquigarrow^* 2$ eli onko piilotetussa suunnatussa graafissa polkua solmusta 1 solmuun 2. Tehtävää voi yrittää ratkaista monella eri tavalla. Voidaan esimerkiksi ensin kysyä, päteekö $1 \rightsquigarrow 2$. Jollei päde, voidaan kysyä päteekö $1 \rightsquigarrow 3$ ja niin edelleen. Jos sekään ei päde eikä $1 \rightsquigarrow 4$ päde mutta $1 \rightsquigarrow 5$ pätee, niin voidaan jatkaa kysymällä päteekö $5 \rightsquigarrow 2$. Kenties siihenkin laatikko vastaa ”ei”, mutta vastaa ”kyllä” kyselyihin $5 \rightsquigarrow 3$ ja $3 \rightsquigarrow 2$, jolloin on löytynyt polku 1 5 3 2.

Jos $1 \rightsquigarrow^* 2$ pätee, niin polku löytyy kyselemällä riittävän kauan tarpeeksi systemaattisesti. Eräs toimiva tapa alkaa merkitsemällä solmu 1 saavutetuksi. Sitten toistetaan seuraavaa, kunnes saavutetaan solmu 2. Valitaan sellaiset u ja v, että u on saavutettu, v ei ole vielä saavutettu, ei ole vielä kysytty päteekö $u \rightsquigarrow v$, ja v on mahdollisimman pieni. Kysytään, päteekö $u \rightsquigarrow v$. Jos pätee, niin merkitään v saavutetuksi.

Miksi vaaditaan, että v on mahdollisimman pieni? 240

Jos $1 \rightsquigarrow^* 2$ ei päde, niin millään kyselytavalla ei voi saada varmuutta siitä, että se ei päde. Vaikka kysyttäisiin kaikki $u \rightsquigarrow v$ missä u ja v ovat enintään 1 000 000, niin jäljelle jää mahdollisuus, että $1 \rightsquigarrow 1\,000\,001 \rightsquigarrow 2$. Tämä on esimerkki siitä yleisestä periaatteesta, että jos mahdollisuuksia on äärettömästi, niin kokeilemalla niitä yksi kerrallaan (tai mikään äärellinen määrä kerrallaan) ei koskaan voida käydä läpi niitä kaikkia. Tällä on suuri merkitys matematiikassa, logiikassa, teoreettisessa tietojenkäsittelytieteessä ja ohjelmien testaamisessa.

Äärettömän montaa tapausta koskevaa tietoa on usein mahdollista saada muilla keinoin. Tiedämme esimerkiksi, että $0x = 0$ pätee jokaiselle luvulle x, vaikka ihmiskunta ei ole yhteensäkään kokeillut edes jokaista luonnollista lukua x:n arvona. Sellaisilla keinoilla voi muun muassa vähentää huomattavasti sitä riskiä, että ohjelmassa, algoritmissa tai muussa sellaisessa on vakava virhe. Olennaista ei ole mikään yksittäinen asia vaan matemaattisen päättelemisen taito yleensä. Siksi monissa yliopistoissa opetetaan matemaattista todistamista myös ohjelmoinnin opiskelijoille.

Vuoden 1900 molemmin puolin matemaatikot yrittivät laajentaa tällaiset menetelmät kattamaan matematiikan tärkeimmät osat kokonaan. Heidän pettymyksekseen 1930-luvulla se todistettiin mahdottomaksi. Nämäkin tulokset vaikuttavat ohjelmointiin ja siksi niitäkin opetetaan myös ohjelmoinnin opiskelijoille. Tämän alaluvun lopussa esitetään eräs kaikkein lyhyimmistä ja helpoimmin ymmärrettävistä mahdottomuustodistuksista.

Seuraava kaava sanoo, että täsmälleen yhdestä solmusta on kaari solmuun v eli että v:llä on täsmälleen yksi edeltäjä. Auki luettuna se sanoo ”on olemassa sellainen u, että u:sta on kaari v:hen ja jokainen solmu, josta on kaari v:hen, on u”:

(28) $\exists u : u \rightsquigarrow v \wedge \forall w : (w \rightsquigarrow v) \rightarrow w = u$

Onko tämä kaava tosi vai ei, riippuu siitä, mistä suunnatusta graafista on puhe, ja mikä sen solmuista valitaan v:ksi. Se on tosi kuvan 37 vasemmanpuoleisen esimerkin solmulle 2 mutta epätosi solmuille 1, 3 ja 4. Se on tosi kuvan 37 oikeanpuoleisen esimerkin jokaiselle solmulle.

Kirjoita kaava, joka sanoo, että ei ole olemassa solmua, josta on kaari v:hen ja joka ei ole u. Sitten muokkaa se logiikan lakeja käyttäen mahdollisimman samanlaiseksi (28):n kanssa! 241

Silmukka (*cycle*) tarkoittaa sellaista polkua $v_1 \cdots v_n$, että $v_n \rightsquigarrow v_1$. (Sanojen ”silmukka” ja ”cycle” merkitys vaihtelee kirjallisuudessa samaan tapaan kuin sanojen ”polku” ja ”path”.) Kirjoita kaava, joka sanoo, että u on silmukassa! 242

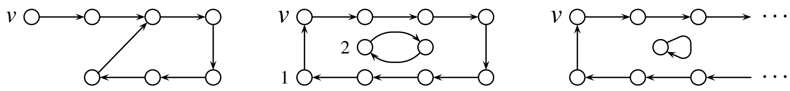
Muuttujan x esiintymä kaavassa on *sidottu* (*bound*), jos ja vain jos se sijaitsee osakaavassa muotoa $\forall x : \ldots$ tai $\exists x : \ldots$. Esiintymä on *vapaa* (*free*), jos ja vain jos se ei ole sidottu. Esimerkiksi v esiintyy vapaana ja u sidottuna kaavassa $\exists u : u \rightsquigarrow v$. Kaava on *suljettu* (*closed*), jos ja vain jos siinä ei ole vapaita muuttujien esiintymiä. Kaava on *avoin* (*open*), jos ja vain jos se ei ole suljettu. Esimerkiksi $\exists u : u \rightsquigarrow v \wedge \forall w : (w \rightsquigarrow v) \rightarrow w = u$ on avoin, koska v esiintyy siinä vapaana, mutta $\forall v : \exists u : u \rightsquigarrow v \wedge \forall w : (w \rightsquigarrow v) \rightarrow w = u$ on suljettu. Usein sana ”esiintyä” jätetään pois, eli puhutaan vapaista ja sidotuista muuttujista. Suunnatuista graafeista puhuvan suljetun kaavan totuusarvo voi riippua vain suunnatusta graafista, josta on puhe. Avoimen kaavan totuusarvo voi lisäksi riippua siitä, mitkä solmut valitaan vapaiden muuttujien arvoiksi.

Sidottu muuttuja ei ole sama kuin muualla esiintyvä samanniminen muuttuja. Esimerkiksi kaavassa $\exists u : (v \rightsquigarrow u \wedge \exists v : u \rightsquigarrow v)$ jälkimmäinen v on eri muuttuja kuin ensimmäinen v. Samasta syystä kuvan 38 v on eri muuttuja kuin mikään sidottu v.

Mitä $\exists u : (v \rightsquigarrow u \wedge \exists v : u \rightsquigarrow v)$ sanoo? Mille kuvien 37 ja 38 solmuille se on tosi? 243

Loogisia symboleita (*logical symbols*) ovat muuttujat, F, T, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\forall\,:$, $\exists\,:$, (,) ja $=$. (Tarkka luettelo vaihtelee hieman kirjallisuudessa.) Kaikki muut kaavoissa esiintyvät symbolit kuten 1, $+$ ja $\leq$ ovat *ei-loogisia symboleita* (*non-logical symbols*). Suunnattujen graafien esimerkissämme ei-loogisia symboleita ovat $\rightsquigarrow$ ja $\rightsquigarrow^*$.

Tulkinta (*interpretation*) kertoo minkälaisia arvoja muuttujat voivat saada ja antaa jokaiselle ei-loogiselle symbolille merkityksen. Täsmennämme sivulla 124, millaisia merkitykset voivat olla; tässä alaluvussa tyydymme esimerkkien luomaan mielikuvaan. Esimerksi alakoulussa muuttujat saavat arvoikseen luonnollisia lukuja, ja 1, $+$ ja $<$ tulkitaan tarkoittamaan lukua yksi, yhteenlaskua ja vertailua pienempi kuin. Suunnattujen



Kuva 38: Kolme suunnattua graafia

graafien esimerkissämme muuttujat saavat arvoikseen solmuja, ja solmujen joukko yhdessä $\rightsquigarrow$:n tulkinnan kanssa ratkaisee mistä suunnatusta graafista on kyse. Esimerkiksi jos solmut ovat 1, 2, 3 ja 4 ja $\rightsquigarrow$ tulkitaan siten, että $1 \rightsquigarrow 2$, $2 \rightsquigarrow 3$ ja $4 \rightsquigarrow 3$ ovat tosi mutta $1 \rightsquigarrow 1$, $1 \rightsquigarrow 3$, $1 \rightsquigarrow 4$, $2 \rightsquigarrow 1$ ja niin edelleen eivät ole, niin kyse on kuvan 37 vasemmanpuoleisesta suunnatusta graafista.

Mille suunnatuille graafeille kuvissa 37 ja 38 pätee $\forall u : \exists v : u \rightsquigarrow^* v \rightsquigarrow u$? Mille
pätee $\forall u : \neg\exists v : u \rightsquigarrow^* v \rightsquigarrow u$? Mille ei päde kumpikaan? 244

Vakiintuneen matemaattisen käytännön mukaisesti sallimme myös symbolit $\neq$, $\not\rightsquigarrow$ ja $\not\rightsquigarrow^*$ siten, että $u \neq v$, $u \not\rightsquigarrow v$ ja $u \not\rightsquigarrow^* v$ tarkoittavat samaa kuin $\neg(u = v)$, $\neg(u \rightsquigarrow v)$ ja $\neg(u \rightsquigarrow^* v)$. Siis esimerkiksi symbolin $\rightsquigarrow$ tulkinta voi vaihdella, mutta valitaan mikä tulkinta tahansa, niin $u \not\rightsquigarrow v$ tarkoittaa samaa kuin $\neg(u \rightsquigarrow v)$.

Kuinka monta sellaista suunnattua graafia on olemassa, joille pätee $1 \neq 2 \wedge (\forall v :$
$v = 1 \vee v = 2) \wedge 1 \rightsquigarrow 1 \not\rightsquigarrow 2$? Kuinka monta sellaista suunnattua graafia on olemassa, 245
joille pätee $(\forall v : v = 1 \vee v = 2) \wedge (\forall v : v \not\rightsquigarrow v)$? Onko ehto $1 \neq 2$ tarpeen tehtävässä 245? 246
Perustele! 247

Logiikan yleisiin pelisääntöihin kuuluu, että ellei erikseen ole sanottu toisin, niin puheenaihe ei voi olla tyhjä. Se tarkoittaa, että täytyy olla olemassa ainakin yksi arvo, jonka muuttujat voivat saada. Suunnattujen graafien esimerkissämme se tarkoittaa, että solmuja on ainakin yksi.

Tyhjälle puheenaiheelle eivät päde kaikki samat lait kuin epätyhjille. Esimerkiksi jos solmuja on ainakin yksi, niin toinen tai molemmat kaavoista $\forall u : \exists v : u \rightsquigarrow^* v \rightsquigarrow u$ ja $\forall u : \neg\exists v : u \rightsquigarrow^* v \rightsquigarrow u$ on epätosi, mutta jos solmuja ei ole yhtään, niin ne molemmat ovat tosi. Siksi tyhjä puheenaihe mutkistaisi asioita, jos se käsiteltäisiin yhdessä muiden tapausten kanssa. Toisaalta se on helppo tarvittaessa miettiä erikseen, koska siinä jokainen kaava muotoa $\forall x : \ldots$ on tosi ja jokainen kaava muotoa $\exists x : \ldots$ on epätosi. Kun tämän tietää, niin tyhjiin puheenaiheisiin liittyy vain yksi vaikea asia: sen muistaminen, että ne täytyy käsitellä erikseen.

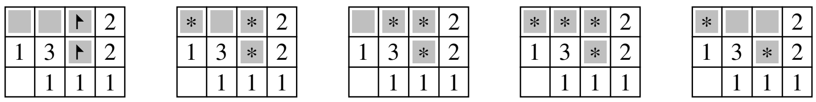
Puheenaiheen ominaisuuksia voi määritellä asettamalla *aksioomia* (*axiom*). Aksioomaksi kelpaa vain suljettu kaava, joka on tosi jokaiselle kohteelle, jonka on tarkoitus kuulua tarkastelun piiriin. Voimme niin halutessamme asettaa aksioomat, jotka sanovat, että jokaisella solmulla on täsmälleen yksi edeltäjä, ja jokaisella solmulla on täsmälleen yksi seuraaja:

(29) $\forall v : \exists u : u \rightsquigarrow v \wedge \forall w : (w \rightsquigarrow v) \rightarrow w = u$

(30) $\forall v : \exists u : v \rightsquigarrow u \wedge \forall w : (v \rightsquigarrow w) \rightarrow w = u$

Silmukka on *toistoton* (*simple*), jos ja vain jos mikään muu solmu paitsi viimeinen ei ole sama kuin aiempi solmu.

Jos (29) ja (30) asetetaan aksioomiksi, niin tarkasteltavana ovat ne ja vain ne suunnatut graafit, jotka muodostuvat ainakin yhdestä toistottomasta silmukasta ja/tai ainakin yhdestä molempiin suuntiin päättymättömästä solmujonosta. Kuvassa 38 on esimerkki sekä keskellä että oikealla. Nimittäin kuten edellä todettiin, on ainakin yksi solmu v. Sillä on täsmälleen yksi seuraaja, jolla on täsmälleen yksi seuraaja ja niin edelleen.



Kuva 39: Miinapelin tilanne, kaksi sen mallia ja kaksi muuta tulkintaa

Seuraaja tai seuraajan seuraaja tai … voi olla v, mutta se ei voi olla v:n seuraaja eikä sen seuraaja eikä …, koska muuten rikottaisiin sitä, että jokaisella solmulla on täsmälleen yksi edeltäjä. Kuvan 38 vasemmanpuoleinen esimerkki havainnollistaa tätä. Seuraajien ketju ei välttämättä palaa v:hen vaan voi jatkua äärettömästi. Siinä tapauksessa v:n edeltäjien ketju jatkuu takaperin äärettömästi, kuten kuvan 38 oikeanpuoleisessa esimerkissä.

Mikä vika on ilmauksessa ”ne ja vain ne suunnatut graafit, jotka muodostuvat yhdestä silmukasta ja ainakin yhdestä molempiin suuntiin päättymättömästä solmujonosta”? 248

Seuraava kaava sanoo, että suunnatussa graafissa on ainakin neljä solmua:

$$\exists v_1 : \exists v_2 : \exists v_3 : \exists v_4 : v_1 \neq v_2 \wedge v_1 \neq v_3 \wedge v_1 \neq v_4 \wedge v_2 \neq v_3 \wedge v_2 \neq v_4 \wedge v_3 \neq v_4$$

Laittamalla sen eteen $\neg$ saadaan kaava, joka sanoo, että solmuja on enintään kolme. Asettamalla niiden kaltaisia kaavoja aksioomiksi voidaan rajoittua vaikka niihin suunnattuihin graafeihin, joissa on vähintään 10 mutta enintään 20 solmua.

On melko tavallista käyttää äärettömän montaa aksioomaa. Niin tehdään muun muassa sekä luonnollisten lukujen tapauksessa että reaalilukujen tapauksessa. Koska äärettömän monen aksiooman kirjoittamiseen sellaisinaan ei ihmisikä riitä, on ääretön aksioomajoukko esitettävä jollakin muulla, äärellisellä keinolla. Keinon on oltava sellainen, että aksioomajoukon käyttäjälle (ihminen tai tietokone) ei ole koskaan epäselvää, onko jokin merkkijono aksioomajoukkoon kuuluva aksiooma vai eikö ole.

Sekä ihminen että tietokone pystyy tarkastamaan, onko annettu merkkijono muotoa

$$(31) \quad \exists v_1 : \exists v_2 : \ldots \exists v_n : v_1 \neq v_2 \wedge v_1 \neq v_3 \wedge \cdots \wedge v_1 \neq v_n \wedge \cdots \wedge v_{n-1} \neq v_n,$$

missä $\wedge$:lla toisistaan erotetut vertailut ovat täsmälleen ne $v_i \neq v_j$, joissa $1 \leq i < j \leq n$. Niinpä, jos halutaan, voidaan päättää, että jokainen tällainen kaava on aksiooma. Lyhyimmästä alkaen ne sanovat: ”solmuja on ainakin 2”, ”solmuja on ainakin 3”, ”solmuja on ainakin 4”, …. Yhdessä ne vaativat, että solmuja on äärettömän monta.

Aksioomien *malli* (*model*) tarkoittaa tulkintaa, joka toteuttaa jokaisen aksiooman (tähän palataan sivulla 125). Kuvan 37 vasemmanpuoleinen suunnattu graafi ei ole mutta oikeanpuoleinen on aksioomien (29) ja (30) malli. Kuvan 38 vasemmanpuoleinen suunnattu graafi ei ole mutta muut kaksi ovat aksioomien (29) ja (30) malleja. Näistä viidestä suunnatusta graafista vain kuvan 38 oikeanpuoleinen on sen aksioomajoukon malli, jonka aksioomat sanovat, että solmuja on ainakin 2, solmuja on ainakin 3, solmuja on ainakin 4, ….

Jos emme nirsoile sen kanssa että väitteet pitää esittää nimenomaan kaavoina, niin voimme soveltaa tulkinnan ja mallin käsitteitä myös miinapeliin. Tulkinta on mikä tahansa tapa laittaa tai jättää laittamatta miina kuhunkin avaamattomaan ruutuun, ja malli on tulkinta, joka täsmää pelitilanteessa näkyvissä oleviin lukuihin. Kuvassa 39 on miinapelin pelitilanne ja neljä sen tulkintaa. Tulkinnoista kaksi ensimmäistä ovat ja kaksi seuraavaa eivät ole pelitilanteen malleja.

Kaava φ on aksioomien *looginen seuraus* (*logical consequence*), jos ja vain jos se on tosi aksioomien jokaisessa mallissa jokaisella vapaiden muuttujien arvojen yhdistelmällä. Luonnollisten lukujen aksioomilla on valtavasti loogisia seurauksia, kuten

$1+2=3$, $\forall x : \forall y : x+y=y+x$ ja $\forall x : x+y=y+x$. Aksioomalla $\forall u : \forall v : \neg(u \rightsquigarrow v \rightsquigarrow u)$ on loogisena seurauksena $w \not\rightsquigarrow w$. Sijoita u:ksi ja v:ksi w kaavassa $\neg(u \rightsquigarrow v \rightsquigarrow u)$, ja sievennä lopputulos mahdollisimman yksinkertaiseksi! 249

Voidaan ajatella, että aksioomat ilmaisevat ne suljettuina kaavoina ilmaistavissa olevat perusasiat jotka puheenaiheesta tiedetään tai oletetaan, ja loogiset seuraukset ovat kaikki se kaavoina ilmaistavissa oleva, joka on vääjäämättä totta silloin kun aksioomat ovat totta. Se, että täsmälleen yhdessä liputtamattomassa avaamattomassa ruudussa on miina, on miinapelin sääntöjen ja kuvassa 39 esitetyn miinapelin tilanteen looginen seuraus. Sen sijaan ei ole looginen seuraus, että vasemmassa ylänurkassa on miina, koska näkyvät luvut ovat oikein myös siinä tapauksessa, että miina onkin viereisessä ruudussa.

On mahdollista, että aksioomajoukolla ei ole lainkaan malleja. Sen saa aikaan esimerkiksi asettamalla sekä aksiooman, joka sanoo että solmuja on ainakin 10, että aksiooman, joka sanoo että solmuja on enintään 5. Yksinkertaisin aksioomajoukko, jolla ei ole mallia, on $\{\mathsf{F}\}$. Esitä mahdollisimman yksinkertainen aksioomajoukko, joka ei käytä symboleita F ja T, ja jolla ei ole mallia! 250

Malliton aksioomajoukko on sovellusten kannalta hyödytön. Se ei kuvaa mitään olemassa olevaa kohdetta, ja jokainen kaava on sen looginen seuraus — jopa F. Malliton aksioomajoukko voi syntyä vahingossa, jos aksioomien valitsemisessa tapahtuu virhe. On osoittautunut, että toisinaan on hyvin vaikeaa ottaa selville, onko aksioomajoukolla mallia!

Kun on asetettu aksioomajoukko jolla on ainakin yksi malli, ja lisäksi on valittu kaava φ, niin on mahdotonta, että sekä φ että $\neg\varphi$ olisi looginen seuraus. Tämän näkee valitsemalla tarkasteltavaksi aksioomajoukon jonkin mallin ja vapaiden muuttujien arvojen jonkin yhdistelmän, mitkä tahansa. Jos φ ei ole niissä tosi, niin φ ei ole looginen seuraus. Muussa tapauksessa φ on niissä tosi, jolloin $\neg\varphi$ on epätosi eikä niin ollen ole looginen seuraus.

Niinpä mallillisen aksioomajoukon tapauksessa on vain kolme mahdollisuutta:

- φ on ja $\neg\varphi$ ei ole aksioomajoukon looginen seuraus. Jokainen tulkinta, joka toteuttaa jokaisen aksiooman, toteuttaa jokaisella vapaiden muuttujien arvojen yhdistelmällä myös φ:n.

- $\neg\varphi$ on ja φ ei ole aksioomajoukon looginen seuraus. Jokaisella tulkinnalla, joka toteuttaa jokaisen aksiooman, ja jokaisella vapaiden muuttujien arvojen yhdistelmällä φ on epätosi.

- Kumpikaan ei ole aksioomajoukon looginen seuraus. On olemassa joko sekä sellainen aksioomajoukon toteuttava tulkinta ja vapaiden muuttujien arvojen yhdistelmä, jolla φ on tosi, että sellainen, jolla φ on epätosi; tai sellainen, jolla φ on määrittelemätön.

Jos φ on jossakin mallissa jollakin vapaiden muuttujien arvojen yhdistelmällä määrittelemätön, niin alin vaihtoehto toteutuu. Esimerkiksi kumpikaan kaavoista $x \cdot \frac{1}{x} = 1$ ja $x \cdot \frac{1}{x} \neq 1$ ei ole reaalilukujen aksioomien sekä jakolaskun ja $\neq$:n määritelmien looginen seuraus, koska kumpikin on määrittelemätön, kun $x = 0$. Sen sijaan $x \neq 0 \rightarrow x \cdot \frac{1}{x} = 1$ on niiden looginen seuraus.

Jos φ on aina määritelty, niin alin vaihtoehto voi toteutua kahdella eri tavalla. Havainnollistamme niitä suunnatuilla graafeilla. Kuvan 38 keskimmäinen esimerkki toteuttaa aksioomat (29) ja (30). Avoin kaava $\neg\exists v : u \rightsquigarrow v \rightsquigarrow u$ on tosi sen solmulle 1, mutta ei solmulle 2. Sen totuusarvo riippuu siis siitä, mikä solmu valitaan vapaan muuttujan

u arvoksi. Siksi se ei ole (29):n ja (30):n looginen seuraus. Myös kuvan 37 oikeanpuoleinen esimerkki toteuttaa aksioomat (29) ja (30). Suljettu kaava $\neg\exists u : \exists v : u \rightsquigarrow v \rightsquigarrow u$ on sille tosi, mutta ei ole tosi kuvan 38 keskimmäiselle esimerkille. Sen totuusarvo riippuu siis siitä, mitä (29):n ja (30):n toteuttavaa suunnattua graafia tarkastellaan. Siksi se ei ole (29):n ja (30):n looginen seuraus.

Kaavan totuusarvon riippuminen vapaille muuttujille annettavista arvoista on tuttua koulumatematiikasta. Esimerkiksi $x \geq 0$ on tietenkin tosi silloin kun x on nolla tai positiivinen, ja epätosi kun x on negatiivinen. Sen sijaan kaavan totuusarvon riippuminen aksioomien mallista lienee oudompi asia, koska symbolien 1, $+$, $\geq$ ja niin edelleen merkitys on koulumatematiikassa kiinteä eikä aksioomien salliman liikkumatilan verran vaihteleva. Tosin koulumatematiikassakin on saman kaltainen ilmiö siinä muodossa, että suljetun kaavan totuusarvo saattaa riippua puheenaiheesta. Esimerkiksi $\forall x : x > 0 \rightarrow x \geq 1$ on tosi kokonaisluvuille mutta ei ole tosi reaaliluvuille.

On tärkeää muistaa, että vaikka sekä aksioomat että suljettu kaava vastaisivat käsitystä siitä, miten asian pitäisi olla, kaava ei silti välttämättä ole aksioomien looginen seuraus. Aksioomilla voi olla tarkoitetun mallin lisäksi toinen malli, jossa kaava ei olekaan tosi. Tämä muistuttaa sitä, että syytetyn tuomitsemiseksi rikoksesta ei riitä, että kaikki tiedossa olevat tosiasiat sopivat kunnolla häneen. Tarvitaan myös, että ne eivät sovi kunnolla keneenkään muuhun.

Käsitteelle $u \rightsquigarrow^* v$ pätee muun muassa

(32) $\forall v : v \rightsquigarrow^* v$ (jokaisesta solmusta on polku itseensä), ja

(33) $\forall u : \forall v : \forall w : (u \rightsquigarrow^* v \rightsquigarrow w) \rightarrow (u \rightsquigarrow^* w)$
(jos u:sta on polku v:hen ja v:stä kaari w:hen, niin u:sta on polku w:hen).

Jos asetamme nämä kaksi kaavaa aksioomiksi, niin mistä tahansa polusta $v_1 \cdots v_n$ voidaan todistaa, että se on polku. Aksiooman (32) mukaan v_1 on polku eli $v_1 \rightsquigarrow^* v_1$. Jos polkumme ei lopu siihen, niin $v_1 \rightsquigarrow v_2$. Aksioomasta (33) saadaan $(v_1 \rightsquigarrow^* v_1 \rightsquigarrow v_2) \rightarrow (v_1 \rightsquigarrow^* v_2)$. Siitä seuraa $v_1 \rightsquigarrow^* v_2$, koska $v_1 \rightsquigarrow^* v_1$ ja $v_1 \rightsquigarrow v_2$ on jo todettu todeksi. Jos polkumme ei lopu siihenkään, niin $v_2 \rightsquigarrow v_3$. Aksioomasta (33) saadaan $(v_1 \rightsquigarrow^* v_2 \rightsquigarrow v_3) \rightarrow (v_1 \rightsquigarrow^* v_3)$. Siitä seuraa $v_1 \rightsquigarrow^* v_3$, koska $v_1 \rightsquigarrow^* v_2$ ja $v_2 \rightsquigarrow v_3$ on jo todettu todeksi. Tätä voidaan jatkaa kunnes koko polku on käyty läpi.

Sen sijaan aksioomat (32) ja (33) eivät riitä osoittamaan, että jostakin solmusta jonnekin ei ole polkua. Nimittäin ne eivät kerro, että $u \rightsquigarrow^* v$ ei voi toteutua millään muulla kuin aksioomien (32) ja (33) ilmaisemalla tavalla. Sen huomataksemme kuvittelemme seuraavaksi, että laatikoltamme voi kysellä myös päteekö $u \rightsquigarrow^* v$, mutta tämä toiminto on mahdollisesti rikki.

Jos laatikko vastaa ”ei” kysymykseen ”päteekö $7 \rightsquigarrow^* 7$”, niin paljastuu, että se on rikki, koska vastaus on vastoin aksioomaa (32). Jos se vastaa ”kyllä” kysymyksiin ”päteekö $1 \rightsquigarrow^* 2$” ja ”päteekö $2 \rightsquigarrow 3$” mutta ”ei” kysymykseen ”päteekö $1 \rightsquigarrow^* 3$”, niin silloinkin se on varmasti rikki, koska aksiooma (33) ei toteudu. Se on rikki myös jos se vastaa ”kyllä” kysymyksiin ”päteekö $1 \rightsquigarrow 2$”, ”päteekö $2 \rightsquigarrow 3$” ja ”päteekö $3 \rightsquigarrow 4$” mutta ”ei” kysymykseen ”päteekö $1 \rightsquigarrow^* 4$”, koska, kuten aiemmin nähtiin, aksioomat (32) ja (33) riittävät osoittamaan, että jos $1 \rightsquigarrow 2 \rightsquigarrow 3 \rightsquigarrow 4$ niin $1 \rightsquigarrow^* 4$. Mikä tahansa vastausten jono, joka on ristiriidassa minkä tahansa aksioomista (32) ja (33) virheettömällä päättelyllä johdettavissa olevan tuloksen kanssa, paljastaa, että laatikkomme on rikki.

Entä jos laatikkomme vastaa ”ei” jokaiseen kysymykseen ”päteekö $u \rightsquigarrow v$”, ja ”kyllä” jokaiseen kysymykseen ”päteekö $u \rightsquigarrow^* v$”? Silloin se on rikki, koska sen mukaan

$1 \rightsquigarrow^* 2$, vaikka solmusta 1 ei ole kaarta mihinkään muuhun solmuun, ja solmu 2 on eri kuin solmu 1 jos solmuja on ainakin kaksi. (Jos solmuja on vain yksi, niin ”kyllä” on oikea vastaus kysymykseen ”päteekö $1 \rightsquigarrow^* 2$” siksi, että liian suuria solmun numeroita piti käsitellä ikään kuin niiden tilalla olisi 1, ja $1 \rightsquigarrow^* 1$ on tosi.)

Silti sen vastaukset eivät koskaan ole ristiriidassa aksioomien (32) ja (33) kanssa. Näin on siksi, että kaavat, jotka saadaan laittamalla aksioomissa (32) ja (33) jokaisen osakaavan muotoa $x \rightsquigarrow^* y$ tilalle T, ovat totta mille tahansa suunnatulle graafille:

- $\forall v : \mathsf{T}$
- $\forall u : \forall v : \forall w : (\mathsf{T} \wedge v \rightsquigarrow w) \rightarrow \mathsf{T}$

Ensimmäinen niistä vastaa sitä, että laatikko vastaa T jokaiseen kysymykseen ”päteekö $v \rightsquigarrow^* v$”. Niin vastaisi ehjäkin laatikko, joten tämä ei voi paljastaa rikkinäisyyttä. Vastaukset voivat olla ristiriidassa aksiooman (33) kanssa vain siten, että niiden mukaan $u \rightsquigarrow^* v$ ja $v \rightsquigarrow w$ ovat tosi mutta $u \rightsquigarrow^* w$ ei ole. Tällaista vastausten jonoa ei kuitenkaan voi syntyä, koska rikkinäinen laatikkomme vastaa ”kyllä” jokaiseen kysymykseen ”päteekö $u \rightsquigarrow^* w$”. Se ei jää kiinni vääristä vastauksistaan, koska se vastaa väärin niin johdonmukaisesti, että vastaukset eivät koskaan ole ristiriidassa keskenään.

Sitäpaitsi tässäkin pätee se, että jos kyselijä jaksaa kysellä vain solmuun 1 000 000 saakka, niin mikään rikkinäisen laatikon vastaus ei eroa sellaisen ehjän laatikon vastauksesta, joka vastaa kysymykseen ”päteekö $u \rightsquigarrow v$” kyllä jos ja vain jos $u = 1\,000\,001$ tai $v = 1\,000\,001$.

Tämä osoittaa, että aksioomat (32) ja (33) eivät riitä erottamaan, tarkoittaako $u \rightsquigarrow^* v$ sitä, että u:sta on polku v:hen, vai onko $u \rightsquigarrow^* v$ aina tosi. Olemme löytäneet aksioomille (32) ja (33) kaksi erilaista mallia. Kummassakin $u \rightsquigarrow v$ tarkoittaa, että u:sta on kaari v:hen. Toisessa $u \rightsquigarrow^* v$ tarkoittaa, että u:sta on polku v:hen, ja toisessa $u \rightsquigarrow^* v$ on aina tosi. Jos tarkoitus on rajata $u \rightsquigarrow^* v$ tarkoittamaan, että u:sta on polku v:hen, niin aksioomat (32) ja (33) hoitavat yhden puolen asiasta: ne takaavat, että $u \rightsquigarrow^* v$ on tosi aina kun pitääkin. Ne jättävät hoitamatta toisen puolen: ne eivät takaa, että $u \rightsquigarrow^* v$ on epätosi silloin kun sen ei pidä olla tosi.

Matematiikassa on tämänkaltaisissa tilanteissa tavallista määritellä täsmällisesti kaikki mikä kuuluu mukaan, ja sanoa sanallisesti tai luottaa että asiayhteyden vuoksi on selvää, että mikään muu ei kuulu mukaan. Esimerkiksi propositiologiikan kaavat määritellään tyypillisesti luettelemalla atomikaavat; kertomalla, miten kaavoista voidaan muodostaa suurempia kaavoja $\neg$:llä, $\wedge$:lla ja niin edelleen; ja sanomalla tai jättämällä sanomatta, että mikään muu ei ole kaava.

Sen tuloksen kannalta, johon olemme tähtäämässä, on kuitenkin hyödyllistä miettiä, miten voitaisiin ilmaista aksioomina, että $u \rightsquigarrow^* v$ on tosi ainoastaan kun u:sta on polku v:hen. Aloitamme esittämällä melko luontevan ehdotuksen ja toteamalla, että se ei toimi.

Kirjoita kaava, joka sanoo, että jos u:sta on polku v:hen, niin joko u ja v ovat sama
solmu tai u:sta on polku v:n johonkin edeltäjään! Jokaiselle solmujen määrälle $n >$ 251
1 on olemassa suunnattu graafi, jossa ei ole jokaisesta solmusta jokaiseen solmuun
polkua, mutta jolle (32), (33) ja kaavasi pätevät vaikka $u \rightsquigarrow^* v$ tuottaisi aina T. Kuvaile
jokaiselle $n > 1$ jokin sellainen! 252

Seuraava kaava $u \rightsquigarrow^3 v$ sanoo, että u:sta on polku v:hen jossa on enintään kolme kaarta:

$$u = v \vee \exists v_1 : u \rightsquigarrow v_1 \wedge (v_1 = v \vee \exists v_2 : v_1 \rightsquigarrow v_2 \wedge (v_2 = v \vee \exists v_3 : v_2 \rightsquigarrow v_3 \wedge v_3 = v)) \tag{34}$$

Samalla periaatteella voidaan kirjoittaa mikä tahansa kaavoista $u \rightsquigarrow^0 v$, $u \rightsquigarrow^1 v$, $u \rightsquigarrow^2 v$, ... Niille suunnatuille graafeille, joissa on enintään neljä solmua, $u \rightsquigarrow^* v$ saadaan takaamaan polun olemassaolo lisäämällä seuraava aksiooma:

(35) $\forall u : \forall v : (u \rightsquigarrow^* v) \rightarrow (u \rightsquigarrow^3 v)$

Jotta rikkinäinen laatikkomme saataisiin kiinni sen rikkomisesta, tarvitaan vielä tieto, että nelosta suuremmilla solmujen numeroilla ei ole merkitystä (koska solmuja on enintään neljä). Sen sanomisessa ei tarvitse varoa käyttämästä liian suurta solmun numeroa, koska laatikkomme tulkitsee niiden tarkoittavan solmua 1. Lisäksi solmuja täytyy olla ainakin kaksi, sillä jos niitä on vain yksi, niin jokainen $u \rightsquigarrow^* v$ pätee, koska u ja v tarkoittavat samaa solmua. Koska solmut numeroidaan ykkösestä alkaen, on siis oltava $1 \neq 2$.

(36) $\forall v : v = 1 \vee v = 2 \vee v = 3 \vee v = 4$

(37) $1 \neq 2$

Jos $1 \rightsquigarrow^3 2$, niin (34):n mukaan $1 = 2$ tai $\exists v_1 : 1 \rightsquigarrow v_1$. Aksiooma (37) sulkee pois mahdollisuuden $1 = 2$. Aksiooma (36) ja $\exists v_1 : 1 \rightsquigarrow v_1$ tuottavat, että jokin kaavoista $1 \rightsquigarrow 1$, $1 \rightsquigarrow 2$, $1 \rightsquigarrow 3$ ja $1 \rightsquigarrow 4$ on tosi. Mutta laatikkomme väittää, että mikään niistä ei ole tosi. Niinpä laatikon antamien tietojen perusteella $1 \rightsquigarrow^3 2$ ei ole tosi. Rikkinäinen laatikkomme väittää, että $1 \rightsquigarrow^* 2$ on tosi. Nämä ovat ristiriidassa aksiooman (35) kanssa, joten rikkinäisyys paljastuu.

Aksioomilla (32), (33) ja $\forall u : \forall v : (u \rightsquigarrow^* v) \rightarrow (u \rightsquigarrow^9 v)$ saadaan $u \rightsquigarrow^* v$ määriteltyä tyhjentävästi mille tahansa suunnatulle graafille, jossa on enintään 10 solmua. Sama periaate toimii mille tahansa solmujen maksimimäärälle. Tällainen määritelmä on kuitenkin käyttökelvoton silloin, kun solmuja saa olla äärettömästi, tai kun solmujen määrän tiedetään olevan äärellinen mutta sille ei tiedetä ylärajaa. Siksi jatkamme paremman määritelmän etsintää.

Aiemmin pystyimme määrittelemään, että suunnatussa graafissa on äärettömästi solmuja, asettamalla aksioomaksi jokaisen kaavoista ”solmuja on ainakin 2”, ”solmuja on ainakin 3”, ... (31). Jos samaa kikkaa yritetään aksioomalle (35), niin saadaan tulokseksi, että jos u:sta on polku v:hen, niin u:sta on polku v:hen jossa on enintään 0 kaarta, ja u:sta on polku v:hen jossa on enintään 1 kaari, ja u:sta on polku v:hen jossa on enintään 2 kaarta, ... Se ei sano sitä mitä tarvitaan, vaan se sanoo, että $u = v$. Tarvittaisiin keino sanoa, että jos u:sta on polku v:hen, niin u:sta on polku v:hen jossa on enintään 0 kaarta, tai u:sta on polku v:hen jossa on enintään 1 kaari, tai u:sta on polku v:hen jossa on enintään 2 kaarta, ...

Valmisteluna tulossa olevaan yksityiskohtaan ja kertauksena vanhasta asiasta: jos puhutaan kokonaisluvuista, niin milloin $x^2 = 9$ on tosi, milloin $\exists x : x^2 = 9$ on tosi ja milloin $\exists x : x^2 = 8$ on tosi? 253

Käsite $u \rightsquigarrow^* v$ voidaan määritellä tyhjentävästi käyttämällä apuna joukko-oppia. Alla olevan kaavan ylärivin ulompi sulkeissa oleva osuus määrittelee A:n sellaiseksi joukoksi, että u kuuluu siihen, ja jokaisen siihen kuuluvan solmun jokainen seuraaja kuuluu siihen. Alarivi tekee A:sta mahdollisimman pienen sellaisen joukon sanomalla, että A on jokaisen sellaisen joukon osajoukko. Kuten kohta todistamme, näistä seuraa, että A on täsmälleen niiden solmujen joukko, joihin on polku u:sta. Ylärivin alku sanoo, että v kuuluu siihen. Tämä tekee koko kaavasta toden tai epätoden sen mukaan, onko v:hen polku u:sta. Jotta A olisi se joukko jolla on edellä kuvatut ominaisuudet, eikä jokin ulkopuolelta annettava joukko josta kaava testaa onko sillä edellä kuvatut ominaisuudet, tarvitaan alkuun $\exists A$ (vertaa tehtävä 253).

$$\exists A : v \in A \wedge (u \in A \wedge \forall w_1 : \forall w_2 : w_1 \in A \wedge (w_1 \rightsquigarrow w_2) \rightarrow w_2 \in A) \wedge$$
$$(\forall B : (u \in B \wedge \forall w_1 : \forall w_2 : w_1 \in B \wedge (w_1 \rightsquigarrow w_2) \rightarrow w_2 \in B) \rightarrow A \subseteq B)$$

Tällä määritelmällä on se huono puoli, että toisin kuin kaikki aikaisemmin tässä alaluvussa esitetyt kaavat, se puhuu sekä solmuista että joukoista. Kun sen pohjalta päätellään, tarvitaan myös joukkojen lakeja. Siitä huolimatta tämänkaltaiset määritelmät ovat matematiikassa yleisiä, joskaan ei näin auki kirjoitettuina, vaan sanallisesti ilmaistuina tyyliin "pienin joukko, joka ..." tai "ne jotka voidaan muodostaa näillä säännöillä, ja vain ne".

Edellä luvattiin osoittaa, että jos $\exists A : v \in A \wedge$ jätetään pois, niin A on niiden solmujen w joukko, joille $u \rightsquigarrow^* w$. Osoitamme ensin, että jos $u \rightsquigarrow^* w$, niin $w \in A$. Teemme sen johtamalla ristiriidan oletuksesta, että $u \rightsquigarrow^* w$ mutta $w \notin A$. Koska $u \rightsquigarrow^* w$, on u:sta polku w:hen. Koska $w \notin A$, ja koska A:n määritelmän mukaan $u \in A$, on jossakin kohdassa tätä polkua sellainen kaari $w_1 \rightsquigarrow w_2$, että $w_1 \in A$ ja $w_2 \notin A$. Mutta se on ristiriidassa A:n määritelmän kohdan $\forall w_1 : \forall w_2 : w_1 \in A \wedge (w_1 \rightsquigarrow w_2) \rightarrow w_2 \in A$ kanssa.

Enää tarvitsee osoittaa, että jos $w \in A$, niin $u \rightsquigarrow^* w$. Olkoon B niiden solmujen w joukko, joille $u \rightsquigarrow^* w$. Aksiooman (32) mukaan $u \rightsquigarrow^* u$, joten $u \in B$. Jos $w_1 \in B$ ja $w_1 \rightsquigarrow w_2$, niin $u \rightsquigarrow^* w_1 \rightsquigarrow w_2$, joten aksiooman (33) mukaan $u \rightsquigarrow^* w_2$ eli $w_2 \in B$. Niinpä B toteuttaa sen ehdon, joka sille asetetaan edellä olevassa kaavassa sulkeissa. Siksi kaavan alarivin vuoksi $A \subseteq B$. Niinpä jos $w \in A$, niin $w \in B$, joten $u \rightsquigarrow^* w$.

Aksioomien lisäksi tarvitaan *päättelyjärjestelmä* (*proof system*). Aksioomat ovat tapauskohtaisia. Ne puhuvat esimerkiksi luonnollisista luvuista, suunnatuista graafeista tai merkkijonoista. Päättelyjärjestelmä koostuu päättelysäännöistä, jotka ovat yleisiä logiikan lainalaisuuksia. Yksinkertainen esimerkki päättelysäännöstä on "jos $\varphi \wedge \psi$, niin φ". Toinen esimerkki on "jos f ja g ovat sijoitettavissa muuttujaan x kaavassa $\varphi(x)$, niin aina kun $f = g$ tai sekä f että g on määrittelemätön, tuottaa $\varphi(f)$ saman totuusarvon kuin $\varphi(g)$".

Melko vaikeatajuinen esimerkki on "Jos ψ voidaan johtaa joukon $\Gamma \cup \{\varphi(y)\}$ sisältämistä kaavoista eikä y esiinny Γ:ssa, kaavassa $\exists x : \varphi(x)$ eikä ψ:ssä, ja jos joukon $\Gamma \cup \{\exists x : \varphi(x)\}$ sisältämät kaavat pätevät, niin ψ pätee". Se sallii antaa nimen y sille arvolle, jonka $\exists x : \varphi(x)$ lupaa olevan olemassa, ja jatkaa päättelyä ikään kuin $\varphi(y)$ olisi johdettu. Muuttujalle y asetetut ehdot estävät y:n sekoittumisen muihin samannimisiin muuttujiin.

Matemaattisessa päättelyssä tehdään usein niin. Niin tehtiin esimerkiksi kun edellä todettiin "on jossakin kohdassa tätä polkua sellainen kaari $w_1 \rightsquigarrow w_2$, että $w_1 \in A$ ja $w_2 \notin A$", ja johdettiin siitä ristiriita A:n määritelmän kanssa. Väite, että sellainen kaari on olemassa, vastaa kaavaa $\exists u_1 : \exists u_2 : \varphi(u_1, u_2)$, missä $\varphi(u_1, u_2)$ on $u_1 \rightsquigarrow u_2 \wedge u_1 \in A \wedge u_2 \notin A$. Osuus "$w_1 \rightsquigarrow w_2$, että $w_1 \in A$ ja $w_2 \notin A$" vastaa kaavaa $\varphi(w_1, w_2)$. Siitä johdettiin ristiriita eli F. Se vastaa ψ:tä, eivätkä w_1 ja w_2 esiinny siinä.

Päättelyjärjestelmistä pyritään tekemään *eheitä* (*sound*) eli sellaisia, että ne eivät voi tuottaa tosista lähtökohdista epätosia johtopäätöksiä. Siitä seuraa, että päättelyjärjestelmä saa tuottaa vain aksioomien loogisia seurauksia. Nimittäin jos φ ei ole aksioomien looginen seuraus, niin on olemassa tulkinta ja vapaiden muuttujien arvojen yhdistelmä joille φ ei päde mutta jokainen aksiooma pätee. Sen näkökulmasta aksioomat ovat todet mutta φ ei ole. Jos aksioomajoukkoa ei ole tarkoitettu käytettäväksi sille tulkinnalle vaan vain sellaisille, joille φ pätee, niin täytyy lisätä aksioomia, jotka sulkevat sen pois mutta jättävät jäljelle *tarkoitetut tulkinnat* (*intended interpretation*). Juuri tätä teimme, kun lisäsimme aksioomia sulkeaksemme pois sen tulkinnan, jonka mukaan $u \rightsquigarrow^* v$ on tosi jokaiselle u ja v, menettämättä sitä tulkintaa, että $u \rightsquigarrow^* v$ tarkoittaa, että u:sta on polku v:hen.

Epäeheitä päättelyjärjestelmiä voidaan pohtia esimerkiksi sen ilmiön tutkimiseksi, että sama ihminen saattaa samanaikaisesti uskoa keskenään ristiriitaisiin asioihin. Tyypillisissä logiikan sovelluksissa epäeheä päättelyjärjestelmä on kuitenkin hyödytön.

Eheäkin päättelyjärjestelmä voi olla hyödytön, kuten se päättelyjärjestelmä, joka ei tuota mitään johtopäätöksiä. Se on kuin henkilö, joka vastaa jokaiseen kysymykseen "en ota kantaa". Vähän parempi mutta silti aika hyödytön päättelyjärjestelmä on se, joka tuottaa jokaisen aksiooman mutta ei mitään muuta. Se tekee vain tyhjänpäiväisiä johtopäätöksiä tyyliin "koska aurinko paistaa, niin aurinko paistaa".

Onneksi on olemassa paljon parempia päättelyjärjestelmiä. Mitä enemmän aksioomien loogisia seurauksia päättelyjärjestelmä todistaa, sitä hyödyllisempi se on — kunhan se ei todista mitään muuta. Ihannetapauksessa se todistaa kaikki aksioomien loogiset seuraukset eikä muuta. Tämä ihanne voi kuulostaa kaukaiselta, mutta sekä propositiologiikalle että niin sanotulle ensimmäisen kertaluvun predikaattilogiikalle on sellaisia päättelyjärjestelmiä. Tämä on merkittävää, koska ensimmäisen kertaluvun predikaattilogiikka on hyvin laajassa käytössä. Itse asiassa eräs suurimmista syistä, joiden vuoksi se on hyvin laajassa käytössä, on että sille on sellaisia päättelyjärjestelmiä.

Nyt on tullut aika kertoa, että on olemassa ensimmäisen ja korkeamman (eli toisen, kolmannen ja niin edelleen) kertaluvun predikaattilogiikoita. Tässä kirjassa korkeamman kertaluvun predikaattilogiikoista tarvitsee tietää vain sen verran, että kykenee tunnistamaan, onko kaava ensimmäistä kertalukua. Ensimmäisen kertaluvun predikaattilogiikassa muuttujat saavat arvoikseen vain puheenaiheen arvoja, kuten lukuja, merkkijonoja tai suunnatun graafin solmuja. Korkeamman kertaluvun predikaattilogiikoissa voidaan käyttää myös esimerkiksi muuttujia, jotka saavat arvoikseen lukujen funktioita. Muun muassa $(\exists P : P(x) \land \neg P(y)) \rightarrow x \neq y$ on toista kertalukua. Sen P saa arvoikseen puheenaiheen arvojen ominaisuuksia. Se sanoo, että jos x:n ja y:n arvot eroavat toisistaan jonkin — minkä tahansa — ominaisuuden suhteen, niin x:n arvo on eri kuin y:n arvo.

Käyttäen luonnollisten lukujen teoriaa apuna $u \rightsquigarrow^* v$ voidaan määritellä toisen kertaluvun kaavalla $\exists n : \exists V : u = V(1) \land v = V(n) \land \forall i : 1 \leq i < n \rightarrow (V(i) \rightsquigarrow V(i+1))$. Saman voi esittää ihmisille ehkä helppolukuisemmin seuraavasti:

$$\exists n : \exists v_1 : \ldots \exists v_n : u = v_1 \land v = v_n \land \forall i : 1 \leq i < n \rightarrow (v_i \rightsquigarrow v_{i+1})$$

Päätteleminen koostuu askelista. Tyypillisessä askeleessa tuotetaan aksioomista ja/tai aiemmin johdetuista kaavoista kaava, tai valmistellaan sellaisen tuottamista esimerkiksi asettamalla jokin kaava tilapäiseksi oletukseksi. Jälkimmäisestä oli edellä esimerkki, jossa kaavan $(u \rightsquigarrow^* w) \rightarrow w \in A$ johtamiseksi asetettiin oletus $(u \rightsquigarrow^* w) \land w \notin A$, josta sittemmin johdettiin ristiriita. Yksittäinen askel voi käyttää vain rajallista tietomäärää. Päättely ei saa jatkua loputtomasti. Siksi, vaikka aksioomia saattaa olla äärettömästi, kukin päättely käyttää vain äärellistä määrää aksioomia. Tämä on jatkossa tärkeää.

Jatkamme suunnattujen graafien tarkastelua. Asetamme aksioomiksi seuraavat:

(38) sen, joka sanoo, että jokaisella solmulla on täsmälleen yksi seuraaja (se oli edellä numero (30)),

(39) ne, joihin viittasimme edellä ilmauksilla "solmuja on ainakin 2", "solmuja on ainakin 3", "solmuja on ainakin 4", ... (31), sekä

(40) jonkin (minkä tahansa) kokoelman aksioomia, joka määrittelee käsitteen $u \rightsquigarrow^* v$ oikein ja tarkasti.

Osoitamme seuraavaksi, että $\exists u : \exists v : \neg(u \rightsquigarrow^* v)$ on näiden aksioomien looginen seuraus. Otamme tarkasteltavaksi minkä tahansa solmun v. Aksiooman (38) mukaan sillä on täsmälleen yksi seuraaja, seuraajan seuraaja ja niin edelleen. Jos tämä polku ei palaa takaisin v:hen, niin v:lle ja sen seuraajalle u pätee $\neg(u \rightsquigarrow^* v)$. Muussa tapauksessa tämä polku sisältää vain äärellisen määrän eri solmuja, joten (39):n vuoksi on olemassa ainakin yksi solmu w, joka ei ole sillä. Sille pätee $\neg(u \rightsquigarrow^* w)$.

Jos käytössä oleva päättelyjärjestelmä todistaa kaikki aksioomien loogiset seuraukset, niin se todistaa $\exists u : \exists v : \neg(u \rightsquigarrow^* v)$. Koska kukin päättely käyttää vain äärellistä määrää aksioomia, on olemassa sellainen luku n, että kaavan $\exists u : \exists v : \neg(u \rightsquigarrow^* v)$ todistus ei käytä mitään aksioomista "solmuja on ainakin n", "solmuja on ainakin $n+1$", "solmuja on ainakin $n+2$", ... Päättely menee siis läpi, vaikka nämä aksioomat poistettaisiin. Poistamme ne.

Yksittäinen n:stä solmusta koostuva silmukka toteuttaa kaikki jäljelle jääneet aksioomat. Se ei silti toteuta kaavaa $\exists u : \exists v : \neg(u \rightsquigarrow^* v)$, koska mistä tahansa silmukan solmusta pääsee silmukkaa pitkin kulkemalla mihin tahansa silmukan solmuun. Päättelyjärjestelmämme siis todistaa vain jäljelle jääneitä aksioomia käyttäen kaavan, joka ei ole niiden looginen seuraus. Toisin sanoen, päättelyjärjestelmämme ei ole eheä.

Tämä esimerkki osoittaa, että on mahdotonta toteuttaa yhtäaikaa kaikki neljä seuraavista:

- Kaavojen kieli kattaa ainakin ensimmäisen kertaluvun kaavat, ja aksioomien joukko voi olla ääretön.
- Päättelyjärjestelmä on eheä.
- Päättelyjärjestelmä todistaa kaikki aksioomien loogiset seuraukset.
- Käsite $u \rightsquigarrow^* v$ voidaan määritellä oikein ja tyhjentävästi päättelyjärjestelmän mahdollistamilla keinoilla.

Kuten edellä mainittiin, ensimmäisen kertaluvun predikaattilogiikalle on olemassa eheitä päättelyjärjestelmiä, jotka todistavat aksioomien kaikki loogiset seuraukset. Edellä $u \rightsquigarrow^* v$ määriteltiin oikein ja tyhjentävästi joukko-opin avulla ensimmäisen kertaluvun aksioomilla. Näistä ei synny ristiriitaa, sillä joukkoja käyttävää määritelmäämme käsitteelle $u \rightsquigarrow^* v$ voi käyttää päättelyssä vasta kun on riittävän hyvin määritelty, mitä joukot ovat. Niinpä näistä syntyy ristiriidan sijaan havainto, että joukko-oppia ei voi määritellä oikein ja tyhjentävästi ensimmäisen kertaluvun aksioomilla.

Edellä esitetty joukko-oppia hyödyntävä käsitteen $u \rightsquigarrow^* v$ määritelmä voidaan helposti muuttaa toisen kertaluvun kaavaksi, joka ei puhu joukoista vaan pelkästään solmuista. Myös se määrittelee käsitteen oikein ja tyhjentävästi. Muunnos perustuu siihen, että toisen kertaluvun muuttuja, joka saa arvoikseen puheenaiheen arvojen ominaisuuksia, on melkein sama asia kuin ensimmäisen kertaluvun muuttuja, joka saa arvoikseen puheenaiheen arvoista muodostettuja joukkoja. Kirjoita muunnoksen lopputulos! Niin- 254
pä toiselle (ja korkeammille) kertaluvuille ei voi olla olemassa eheää päättelyjärjestelmää, joka todistaisi kaikki loogiset seuraukset.

Ainoa näissä johtopäätöksissä käytetty tosiasia, jota emme todistaneet, on että ensimmäisen kertaluvun predikaattilogiikalle on olemassa eheitä kaikki loogiset seuraukset todistavia päättelyjärjestelmiä. Sitä ei ole helppo todistaa! Mutta ilman sitäkin voimme päätellä, että joukkoja eikä edes käsitettä $u \rightsquigarrow^* v$ ei voi määritellä oikein ja tyhjentävästi sellaisessa eheässä päättelyjärjestelmässä, joka kattaa ensimmäisen kertaluvun predikaattilogiikan ja pystyy todistamaan kaikki loogiset seuraukset. Tämä on hyvin suuri rajoitus matematiikassa.

Parhaat tarjolla olevat ainakin ensimmäisen kertaluvun predikaattilogiikan kattavat vaihtoehdot ovat siis

- Eheässä päättelyjärjestelmässä voidaan johtaa kaikki loogiset seuraukset, mutta käsitettä $u \rightsquigarrow^* v$ ei voi määritellä oikein ja tyhjentävästi. Jos määritteleminen onnistuu apukäsitteen kuten joukkojen avulla, niin tätä apukäsitettä ei voi määritellä oikein ja tyhjentävästi.
- Käsitteen $u \rightsquigarrow^* v$ voi määritellä oikein ja tyhjentävästi, mutta eheässä päättelyjärjestelmässä ei voida johtaa kaikkia loogisia seurauksia.

Tämä alaluku on pitkähkö, koska asioita pyrittiin havainnollistamaan esimerkeillä ja koska jouduttiin esittelemään monta käsitettä, kuten malli. Varsinainen rajoituksen todistus oli kuitenkin lyhyt, eikä se vaatinut muuta kuin yleistä todistusten ymmärtämisen taitoa sekä hieman sen hahmottamista, minkälaisia suunnattuja graafeja käytetyt aksioomat sallivat ja mitä polkuja niissä on.

5.3 Ensimmäisen kertaluvun teoriat

Ensimmäisen kertaluvun teoria (*first-order theory*) yksilöidään ilmoittamalla kaksi asiaa: *ei-loogiset symbolit* (*non-logical symbols*) ja *aksioomat* (*axioms*). Tässä alaluvussa keskitytään niihin ja miten niistä syntyy teoria.

Asiasta on ehkä helpoin päästä jyvälle aloittamalla niistä kohteista, joista puhumiseen teorioita usein käytetään. Tällaista kohdetta kutsutaan nimellä *struktuuri* (*structure*). Siinä on kolme osaa:

- Epätyhjä joukko, jota kutsutaan englanniksi nimellä *domain of discourse* ja merkitään toisinaan symbolilla $\mathbb{D}$. Paremman suomenkielisen nimen puutteessa kutsumme sitä *puheenaiheen joukoksi*. Tutuimpia esimerkkejä ovat luonnolliset luvut $\mathbb{N}$ ja reaaliluvut $\mathbb{R}$. Muita erityisen valaisevia esimerkkejä ovat merkkijonot Σ^* (kun merkkien joukko Σ on ennalta sovittu, esimerkiksi kaikki 8-bittiset tavut) ja epätyhjän suunnatun graafin G solmujen joukko V (kun G on ennalta sovittu).
- Nolla tai useampia *funktioita* (*function*). Ne ovat laskutoimituksia tai muita temppuja, jotka ottavat jonkin kiinteän määrän puheenaiheen joukon alkioita ja tuottavat puheenaiheen joukon alkion. Luonnollisten lukujen tapauksessa tuttuja funktioita ovat yhteenlasku ja kertolasku. Kumpikin ottaa kaksi lukua ja tuottaa yhden luvun. Reaalilukujen tapauksessa vastaluku ottaa ja tuottaa yhden luvun. *Peräkkäin laittaminen* (*concatenation* tai *juxtaposition*) ottaa kaksi merkkijonoa ja tuottaa yhden merkkijonon, esimerkiksi merkkijonoista `yli` ja `opisto` tulee `yliopisto`. Suunnattujen graafien esimerkissämme ei ollut funktioita lainkaan. Millä nimellä kutsutaan funktion ottamien arvojen määrää? 255
- Nolla tai useampia *relaatioita* (*relation*). Relaatio ottaa jonkin kiinteän määrän puheenaiheen joukon alkioita ja tuottaa totuusarvon. Reaalilukujen teorioissa käytetään usein kaksipaikkaista relaatiota $\leq$. Suunnattujen graafien esimerkissämme käytimme kaksipaikkaisia relaatioita $\rightsquigarrow$ ja $\rightsquigarrow^*$. Ne riippuivat siitä, mistä suunnatusta graafista on kyse — mutta suunnattujen graafien teoriamme ei olekaan kaikkien suunnattujen graafien teoria, vaan jokaisella suunnatulla graafilla on oma teoriansa! Mikä on suunnattujen graafien teoriamme $\mathbb{D}$? Mikä olisi 256
kaikkien suunnattujen graafien teorian $\mathbb{D}$? Yhtäsuuruus $=$ ajatellaan tyypillisesti 257

logiikan kalustoon kuuluvaksi, eikä sitä mainita teorian relaatioissa, vaikka sitä kutsutaankin relaatioksi.

Termiä ”domain of discourse” käytetään toisinaan tarkoittamaan koko struktuuria ja toisinaan pelkästään joukkoa $\mathbb{D}$. Itse asiassa jopa sanaa ”joukko” käytetään usein molemmilla tavoilla. Esimerkiksi kun sanotaan ”reaalilukujen joukko”, niin melkein poikkeuksetta ajatellaan myös sen yhteen- ja kertolaskua, vastalukuja ja käänteisarvoja sekä suuruusjärjestystä tuttuine ominaisuuksineen. Siksi mekin otamme vapauden käyttää sanaa ”puheenaihe” tarkoittamaan joko koko struktuuria tai pelkästään joukkoa $\mathbb{D}$.

Ensimmäinen vaihe ensimmäisen kertaluvun teorian rakentamisessa on *ei-loogisten symbolien* (*non-logical symbols*) valinta. Niitä voi olla kolmenlaisia:

- *Vakiosymboli* (*constant symbol*) tarkoittaa jotakin $\mathbb{D}$:n alkiota. Esimerkiksi 0 ja 1 tarkoittavat tyypillisesti lukuja nolla ja yksi, ja reaaliluvuista puhuttaessa π tarkoittaa usein lukua $4(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\ldots)$. Merkkijonoista puhuttaessa ε tarkoittaa usein tyhjää merkkijonoa.

- *Funktiosymboli* (*function symbol*) tarkoittaa jotakin funktiota. Formaalissa logiikassa funktion käyttö esitetään yleensä muodossa $f(g_1,\ldots,g_n)$, missä n on funktion paikkaluku ja g_1, …, g_n ovat lausekkeita. Esimerkeissä käytetään usein puheenaiheen alalla vakiintuneita merkintätapoja. Esimerkiksi $\cdot(a,+(b,1))$ esitetään tyypillisesti $a\cdot(b+1)$ tai $a(b+1)$.

- *Relaatiosymboli* (*relation symbol*) tarkoittaa jotakin relaatiota. Formaalissa logiikassa relaation käyttö esitetään yleensä muodossa $R(f_1,\ldots,f_n)$, missä n on relaation paikkaluku ja f_1, …, f_n ovat lausekkeita. Esimerkeissä käytetään usein puheenaiheen alalla vakiintuneita merkintätapoja. Esimerkiksi $\leq(a,+(b,1))$ esitetään tyypillisesti $a\leq b+1$. Symboli $=$ ei kuulu tähän kohtaan vaikka myös sitä kutsutaan relaatiosymboliksi, koska se katsotaan loogiseksi symboliksi, ja tässä luetellaan vain ei-loogiset symbolit.

Vakio-, funktio- ja relaatiosymbolien ja niiden paikkalukujen muodostaman kokonaisuuden nimi englanniksi on *signature* tai *vocabulary*. Suomeksi käytössä on muun muassa ”aakkosto” ja ”kieli”, mutta koska kummallakin on muu vakiintunut merkitys tietojenkäsittelytieteessä ja matematiikassa, käytämme tässä kirjassa niiden sijaan sanaa *sanasto*. (Sanoja ”aakkosto” ja ”kieli” käytetään esimerkiksi äärellisten automaattien teoriassa seuraavasti. Aakkosto on mikä tahansa epätyhjä äärellinen joukko, esimerkiksi $\{\mathtt{a},\mathtt{b},\ldots,\mathtt{ö}\}$. Merkkijono on mikä tahansa äärellinen määrä aakkostosta poimittuja alkioita laitettuna peräkkäin, esimerkiksi `logiikka`. Kieli on mikä tahansa joukko merkkijonoja.)

Vakiosymboleita, funktiosymboleita ja relaatiosymboleita voi olla mikä tahansa määrä. Niitä ei tarvitse olla lainkaan. Tietojenkäsittelytieteessä ja aika usein muuallakin on tavallista vaatia, että kutakin niistä on korkeintaan numeroituvasti äärettömän monta. Esimerkiksi luonnollisten lukujen teorioissa voidaan sallia vakiosymboleina kaikki numerojonoina esitetyt luonnolliset luvut kuten 3810, jolloin vakiosymboleita on numeroituvasti äärettömän monta. Jos tyydytään vakiosymboleihin 0 ja 1, niin suuremmat lukuvakiot joudutaan ilmaisemaan esimerkiksi tyyliin $1+1+\ldots+1$.

Kaavoja muodostettaessa saa käyttää ei-loogisten symbolien lisäksi loogisia symboleita. Tässä kirjassa ne ovat muuttujasymbolit, $=$, (,), F, T, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\forall$: ja $\exists$:. Loogisten symbolien kokoelma vaihtelee eri lähteissä muun muassa sen mukaan tarvitseeko kirjoittaja symbolia $\leftrightarrow$, katsooko hän symbolin $=$ loogiseksi vai ei-loogiseksi, ja katsooko hän sulkeet (ja) loogisiksi symboleiksi, välimerkeiksi vai joksikin muuksi. Myös muuttujasymboleiden tarkka esitystapa vaihtelee. Muuttujasymboleita täytyy olla äärettömästi, jotta ne eivät loppuisi kesken pitkiäkään kaavoja kirjoitettaessa. Tietojenkäsittelytieteessä ja aika usein muuallakin niitä on tavallisesti numeroituvasti äärettömästi. Ensimmäisen kertaluvun predikaattilogiikassa muuttujasymbolit saavat arvonsa joukosta $\mathbb{D}$ eli puheenaiheen alkioiden joukosta.

Matematiikassa on tavallista ottaa käyttöön uusia symboleita sitä mukaa kuin tarvitaan. Formaalissa logiikassa on kuitenkin olennaista kiinnittää sanasto (eli käytössä olevien vakio-, funktio- ja relaatiosymbolien luettelo paikkalukuineen) teoriaa rakennettaessa, koska se vaikuttaa kahteen tärkeään asiaan: mitä teorian kaavoilla voi ilmaista ja kuinka kattavasti kaavojen totuusarvoja voi selvittää.

Esimerkiksi luonnolliset luvut sanastolla 0, 1 ja + (niin sanotun *Presburger-aritmetiikan* sanasto) on olennaisesti eri asia kuin luonnolliset luvut sanastolla 0, 1, + ja $\cdot$ (niin sanotun *Peanon aritmetiikan sanasto*). Ensimmäiselle on mutta jälkimmäiselle ei ole olemassa algoritmia, jolla minkä tahansa suljetun kaavan totuusarvon voi selvittää. Toisaalta väite $x \cdot y = z$ on sellaisenaan ilmaistavissa Peanon aritmetiikan kaavana, mutta ei ole olemassa mitään keinoa ilmaista sitä Presburger-aritmetiikan kaavana. Sen sijaan väite $3 \cdot y = z$ voidaan ilmaista myös Presburger-aritmetiikan kaavana, nimittäin $y + y + y = z$.

Kaavat $\forall x : x \cdot 0 = 0$ ja $\forall x : \forall y : x \cdot (y+1) = x \cdot y + x$ määrittelevät luonnollisten lukujen kertolaskun olettaen, että yhteenlasku on käytettävissä. Jotta huomaisit että ne todella määrittelevät sen, kirjoita rekursiivinen ohjelma, joka laskee kertolaskun tällä periaatteella. Käytä lauseketta $y - 1$ tuottamaan se luku y', jolle $y' + 1 = y$. Testaa ohjelmaasi kaikilla tapauksilla joissa $x \leq 2$ ja $y \leq 2$, sekä muutamilla muilla tapauksilla! 258
Miksi tämä kertolaskuohjelma on huono käytännön tarpeisiin? Miksi kertolaskua ei voi 259
ilmaista Presburger-aritmetiikassa näillä kaavoilla? 260

Kuitenkaan luonnolliset luvut sanastolla 0, 1, + ja $\leq$ ei ole olennaisesti eri asia kuin luonnolliset luvut sanastolla 0, 1 ja +. Se johtuu siitä, että minkä tahansa kaavan $f \leq g$ voi korvata kaavalla $\exists x : f + x = g$, missä x on jokin muuttujasymboli, joka ei esiinny lausekkeessa f eikä g. Koska lausekkeet ovat aina äärellisen pituisia, voivat f ja g sisältää yhteensä vain äärellisen määrän merkkejä, joten niissä voi esiintyä yhteensä vain äärellinen määrä muuttujasymboleita. Koska edellä vaadittiin että muuttujasymboleita on äärettömästi, on aina olemassa muuttujasymboli, joka ei esiinny f:ssä ja g:ssä ja niin ollen kelpaa x:ksi. Siksi luonnollisten lukujen tapauksessa, jos + on käytettävissä, niin symbolia $\leq$ voi käyttää selkokaavoissa murehtimatta, saako sitä käyttää aidoissa kaavoissa — vaikka ei saisi, niin $f \leq g$ voidaan aina tulkita lyhenteeksi jostakin kaavasta muotoa $\exists x : f + x = g$.

Miksi edellä kuvattu tapa korvata $\leq$ muilla symboleilla ei toimi kokonaisluvuilla sanastolla 0, 1, + ja $\cdot$? 261

Miten $\leq$ voidaan korvata reaaliluvuilla sanastolla 0, 1, + ja $\cdot$? 262

Miksi edellisen vastauksen tapa ei toimi kokonaisluvuilla? 263

On vaikea löytää keinoa korvata $\leq$ kokonaisluvuilla sanastolla 0, 1, + ja $\cdot$. Esimerkiksi ajatus $\exists x : (x \text{ on ei-negatiivinen}) \wedge f + x = g$ vaatii, että pitäisi voida ilmaista ilman symbolia $\leq$ kaavana se, minkä $0 \leq x$ ilmaisee. Jos ehdimme ja muistamme, niin palaamme myöhemmin siihen, onko se mahdollista.

Ehkä yllättäen, luonnolliset luvut sanastolla 0, 1, +, $\cdot$ ja ^ (potenssiin korotus) ei ole olennaisesti eri asia kuin sama ilman potenssiin korotusta. Se johtuu siitä, että on olemassa keino ilmaista väite $x^y = z$ sanastolla 0, 1, + ja $\cdot$. Se on aivan liian monimutkainen tässä esitettäväksi!

[88]	$\forall x : \neg(x+1=0)$	[92]	$\forall x : x \cdot 0 = 0$
[89]	$\forall x : \forall y : x+1=y+1 \rightarrow x=y$	[93]	$\forall x : \forall y : x \cdot (y+1) = x \cdot y + x$
[90]	$\forall x : x+0=x$	[94]	$\varphi(0) \wedge (\forall x : \varphi(x) \rightarrow \varphi(x+1))$
[91]	$\forall x : \forall y : x+(y+1)=(x+y)+1$		$\rightarrow \forall x : \varphi(x)$

Kuva 40: Peanon aritmetiikan aksioomat (ilman seuraajafunktiota)

Toinen ja samalla viimeinen vaihe ensimmäisen kertaluvun teorian rakentamisessa on aksioomien valinta. Aksioomat ovat joukko suljettuja kaavoja, jotka yhdessä kuvaavat puheenaiheen ominaisuudet virheettömästi ja mahdollisimman kattavasti. Esimerkiksi Peanon aritmetiikassa asetetaan yleensä kuvassa 40 näytetyt aksioomat. Jotta kaavoja olisi helpompi lukea, omaksumme nytkin käytännön, jonka mukaan sulkeet saa jättää pois, jos se ei muuta laskujärjestystä olettaen että kertolaskut lasketaan ennen yhteenlaskuja ja samanlaiset laskut lasketaan vasemmalta oikealle. Siis esimerkiksi $f+g+h$ tarkoittaa samaa kuin $(f+g)+h$, mutta $0 \cdot f+g+h$ ei tarkoita samaa kuin $0 \cdot (f+g)+h$ vaan samaa kuin $((0 \cdot f)+g)+h$.

Näimme tehtävässä [258], että [92] ja [93] määrittelevät kertolaskun, kun yhteenlasku on käytettävissä. Samaan tapaan voidaan havaita, että [90] ja [91] määrittelevät yhteenlaskun, kun ykkösen lisääminen on käytettävissä. Numero [94] ei ole yksi aksiooma vaan aksioomaskeema, josta saadaan äärettömän monta eri aksioomaa laittamalla φ:n tilalle mikä tahansa kaava. Se ilmaisee luonnollisten lukujen induktioperiaatteen: jos kaava pätee nollalle ja jos sen voimassaolo periytyy jokaiselta luonnolliselta luvulta seuraavalle luonnolliselle luvulle, niin se pätee jokaiselle luonnolliselle luvulle. Kerromme seuraavaksi, miten [88] ja [89] takaavat tutun äärettömän monesta eri luvusta muodostuvan jonon 0, 1, 2, ... olemassaolon.

Luonnollisia lukuja ovat ainakin

(41) $\quad 0,\ 0+1,\ 0+1+1,\ 0+1+1+1,\ \ldots$

Aksiooman [88] vuoksi mikään muu niistä ei ole yhtäsuuri kuin 0. Myöskään esimerkiksi $0+1+1$ ei ole yhtäsuuri kuin $0+1+1+1+1$ (eli $2 \neq 4$), koska jos $0+1+1 = 0+1+1+1+1$ niin [89]:n vuoksi $0+1 = 0+1+1+1$ ja uudelleen [89]:n vuoksi $0 = 0+1+1$, mistä [47]:llä saadaan $0+1+1=0$, joka on vastoin aksioomaa [88]. Sama päättelytapa toimii mille tahansa kahdelle eri lausekkeelle muotoa $0+1+\ldots+1$, joten jonon (41) luvut ovat kaikki eri lukuja. Luonnollisia lukuja on siis äärettömän monta.

Tämä päättely ei ota kantaa siihen, onko Peanon aritmetiikan aksioomien mukaan olemassa muitakin luonnollisia lukuja kuin jonon (41) tuottamat. On helppo nähdä, että esimerkiksi $0+1+0$ ei ole muu luku, koska [90]:n mukaan $0+1+0=0+1$, ja $0+1$ on jonossa (41). Koska Peanon aritmetiikan tarkoituksena on olla luonnollisten lukujen teoria, ja koska alakoulusta saakka luonnollisiin lukuihin ovat kuuluneet vain 0, 1, 2, ja niin edelleen, haluamme, että Peanon aritmetiikan aksioomat takaavat, että muita luonnollisia lukuja ei ole. Tulemme huomaamaan, että se on syvällinen kysymys, mutta aika paljon siihen suuntaan voidaan saavuttaa.

Voidaan esimerkiksi todistaa, että $\forall x : 0+x=x$. Tehtävää vaikeuttaa se, että vielä ei saa vedota yhteenlaskun vaihdantalakiin, koska Peanon aritmetiikan aksioomissa ei ole yhteenlaskun vaihdantalakia. Aksiomaattisen menetelmän ideaan kuuluu, että todistuksissa ei saa käyttää mitään muuta kuin aksioomia, logiikan yleisiä lakeja sekä näitä rajoituksia noudattaen todistettuja väitteitä. Tarkoitushan on, että aksioomat määrittelevät puheenaiheen (virheettömästi ja) mahdollisimman tyhjentävästi. Tätä ei ole saavutettu, jos todistuksissa joudutaan käyttämään informaatiota, joka ei palaudu aksioomiin logiikan keinoilla.

Todistamme kaavan $\forall x : 0+x = x$ valitsemalla [94]:n $\varphi(x)$:ksi $0+x = x$. Valitsemalla [90]:n x:ksi 0 saadaan $0+0 = 0$ eli $0+0 = 0$ eli $\varphi(0)$. Aksioomasta [91] saadaan $0+(x+1) = (0+x)+1$. Jos $\varphi(x)$ pätee eli jos $0+x = x$, niin [52]:n mukaan $(0+x)+1 = x+1$. Niistä [49] tuottaa $0+(x+1) = x+1$. Se on $\varphi(x+1)$. Olemme siis oletuksesta $\varphi(x)$ todistaneet $\varphi(x+1)$. Lakien [21] ja [20] mukaan siitä seuraa, että $\varphi(x) \rightarrow \varphi(x+1)$ pätee ilman että x:stä oletetaan mitään. Niinpä [83] tuottaa $\forall x : \varphi(x) \rightarrow \varphi(x+1)$. Olemme osoittaneet $\varphi(0) \wedge (\forall x : \varphi(x) \rightarrow \varphi(x+1))$. Siitä [16] ja [94] tuottavat $\forall x : \varphi(x)$ eli $\forall x : 0+x = x$.

Jatkossa [94]:ää käytettäessä riittää todistaa $\varphi(0)$ ja todistaa $\varphi(x+1)$ oletuksesta $\varphi(x)$, tekemättä lisäksi muita oletuksia kuin todistettavassa väitteessä "jos ..., niin $\forall x : \varphi(x)$" alun perin mainittuja. Vaikka edellä perusteltiin, miksi [94] tuottaa niistä $(\forall x : \varphi(x))$:n, sitä ei tarvitse jatkossa perustella, koska sen oletetaan olevan yleisesti tunnettu. Myöskään ei tarvitse viitata logiikan yleisiin lakeihin kuten [47], [52] ja [83] (kuitenkin, jos on erityisen vaikea nähdä miten lakia on käytetty, on hyvä kertoa miten sitä on käytetty). Seuraavissa tehtävissä saa käyttää myös kaikkea mikä siihen mennessä on todistettu Peanon aritmetiikan aksioomista.

Todista Peanon aritmetiikan aksioomista $\forall x : 0 \cdot x = 0$! 264

Todista Peanon aritmetiikan aksioomista $\forall x : 1 \cdot x = x$! 265

Todista Peanon aritmetiikan aksioomista $\forall x : x \cdot 1 = x$! 266

Edellä osoitetuista tuloksista seuraa, että mistä tahansa Peanon aritmetiikan vakiolausekkeesta eli lausekkeesta, jossa ei esiinny muuta kuin 0, 1, +, ·, (ja), voidaan johtaa yhtäsuuri vakiolauseke, jossa ei esiinny yhteen- eikä kertolaskuja jonka ainakin toinen osapuoli on 0. Sellainen lauseke on joko pelkkä 0 tai 0 ei esiinny siinä lainkaan. Johda sellainen lauseke lausekkeesta $((0\cdot 1)+1)\cdot(1+1)+(1+1)\cdot 0$! Näytä jokainen välivaihe, mutta ei tarvitse kertoa, mitä aksioomia ja johdettuja tuloksia käytit. 267

Vakiolausekkeesta, jossa 0 ei esiinny, voidaan edellä osoitettujen tulosten ja [93]:n avulla sieventää kaikki kertolaskut pois. Tee niin lausekkeelle $(1+1)\cdot((1+1)+1)$, ja tällä kertaa kerro, mitä lakia tai tulosta käytit missäkin askeleessa! 268

Näiden sievennösten jälkeen jäljellä on pelkkä 0 tai lauseke, jossa on vain symboleita 1, +, (ja). Symbolit (voidaan siirtää vasempaan reunaan [91]:n avulla. Tee niin lausekkeelle $(1+(1+1))+((1+1)+1)$! 269

Koska $(1+1)+1 = 1+1+1$, $((1+1)+1)+1 = 1+1+1+1$ ja niin edelleen, saadaan jokainen vakiolauseke sievennettyä muotoon 0 tai $1+\ldots+1$. Niinpä jokainen luku, jonka voi kirjoittaa Peanon aritmetiikan sanastolla, on jonossa (41). Tämä ei kuitenkaan sulje pois sitä mahdollisuutta, että Peanon aritmetiikan aksioomat sallisivat lukuja, joita ei voi kirjoittaa Peanon aritmetiikan sanastolla. Tämä ei ole tuulesta temmattu epäilys, sillä kuten totesimme sivulla 82, reaaliluvuilla tilanne on tämän kaltainen, ja jopa paljon pahempi: valitaanpa mikä tahansa merkintäjärjestelmä, suurin osa reaaliluvuista jää vaille esitystapaa.

Luonnollisen luvun x *seuraaja* (*successor*) on $x+1$. Peanon aritmetiikan sanastona käytetään toisinaan symboleita 0, +, · ja s, missä $s(x)$ tarkoittaa luvun x seuraajaa. Niin tehdään osittain historiallisista syistä ja osittain halusta korostaa seuraajafunktion roolia. Symbolit 1, 2, 3 ja niin edelleen ovat silloin lyhennemerkintöjä lausekkeille $s(0)$, $s(s(0))$, $s(s(s(0)))$ ja niin edelleen, ja esimerkiksi [91] kirjoitetaan muodossa $\forall x : \forall y : x+s(y) = s(x+y)$. Tämä ei ole olennainen ero edellä esitettyyn, sillä $s(x)$ ja $x+1$ on helppo vaihtaa toisikseen kummin päin tahansa missä tahansa kaavassa, eikä edelläkään ollut vakiosymboleita 2, 3 ja niin edelleen, vaan ne olivat lyhennemerkintöjä lausekkeille $1+1$, $1+1+1$ ja niin edelleen.

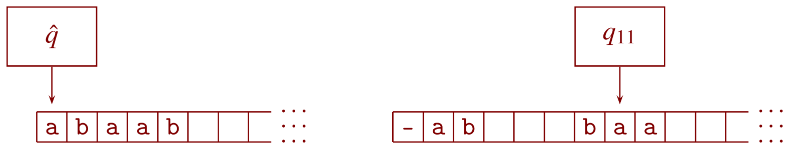
Aksioomaskeema [94] tuottaa vain ensimmäisen kertaluvun aksioomia. Giuseppe Peanon vuonna 1889 esittämissä alkuperäisissä aksioomissa sen tilalla oli jotakin, jonka voi nykykielellä ilmaista joukkojen avulla: jokainen joukko, joka sisältää 0:n sekä jokaisen sisältämänsä luvun seuraajan, sisältää kaikki luonnolliset luvut. Tällä tavalla Peano sulki pois muut kuin jonon (41) luvut. Nykynäkökulmasta tässä on kuitenkin se huono puoli, että se tuo aksioomiin joukon käsitteen, jolloin myös päättelysääntöihin täytyy lisätä joukkoja koskevia sääntöjä. Jonkin verran kevyempi ratkaisu on esittää sama ajatus toisen kertaluvun predikaattilogiikalla: $\forall P : P(0) \land (\forall x : P(x) \rightarrow P(x+1)) \rightarrow \forall x : P(x)$. Tämäkään ajatus ei ole ongelmaton, koska toisen kertaluvun logiikalle ei ole olemassa yhtä kattavia päättelyjärjestelmiä kuin ensimmäisen kertaluvun logiikalle.

Siksi nykyisin suositaan aksioomaskeemaa [94]. Se esittää ensimmäisen kertaluvun keinoin melkein saman ajatuksen. Sen sijaan että se puhuisi kaikista joukoista joissa on nolla sekä jokaisen sisältämänsä luvun seuraaja, se puhuu vain niistä sellaisista joukoista, jotka voidaan ilmaista kaavoina. Siksi on periaatteessa mahdollista, että se ei rajaa luonnollisia lukuja tarkasti, vaan sallii ”ylimääräisiä” lukuja, kunhan myös jokaisen ”ylimääräisen” luvun seuraaja on mukana. Tästä ei olisi suurta haittaa, jos minkään kaavan totuusarvo ei riippuisi siitä, onko ”ylimääräisiä” lukuja mukana vai ei. Haittaa tulisi vasta sitten, jos aksioomat ja päättelyjärjestelmä todistaisivat jonkin kaavan, joka ei ole luonnollisille luvuille tosi, tai jättäisivät todistamatta jonkin kaavan, joka on luonnollisille luvuille tosi.

Kurt Gödel julkaisi vuonna 1931 tuloksen, josta seuraa, että tilanne on juuri tämä ja itse asiassa paljon pahempi. Valitaan ihan mikä tahansa erään järkevyysehdon täyttävä kaavojen todennusmenetelmä, niin se ilmoittaa todeksi jonkin kaavan, joka ei ole luonnollisille luvuille tosi, tai jättää ilmoittamatta todeksi jonkin kaavan, joka on luonnollisille luvuille tosi. Tässä todennusmenetelmän käsite on hyvin yleinen. Se kattaa ensimmäisen kertaluvun logiikan, korkeamman kertaluvun logiikat ja jopa kaikki sellaiset ”järkevyysehdon” täyttävät todennusmenetelmät, jotka eivät lainkaan muistuta meille tuttua logiikkaa. Se kattaa Peanon aritmetiikan aksioomat, mitkä tahansa muut ”järkevyysehdon” täyttävät aksioomajärjestelmät, sekä sellaiset ”järkevyysehdon” täyttävät todennusmenetelmät, jotka eivät perustu aksioomiin.

”Järkevyysehto” on, että täytyy olla olemassa objektiivinen keino tarkastaa, että esitetty päättely tai muu todennus noudattaa päättelyjärjestelmän tai todennusmenetelmän kaikkia muotoseikkoja. Tarkastettavana muotoseikkana voi olla muun muassa, että kun muuttujan tilalle sijoitetaan lauseke, on sen ympärille tarvittaessa lisättävä sulkeet. ”Järkevyysehto” kieltää esimerkiksi sellaiset todistukset, joiden yhtenä vaiheena on ”sen, että tästä kaavasta seuraa tuo kaava näkee seuraavana yönä unessa, kun ennen nukkumaan menoa syö teelusikallisen kärpässientä”, taikka ”tämä kaava on aksiooma, jos ja vain jos valtiomme kunnioitettu suuri johtaja, kansakuntamme valo ja ajatusten valtameri, sanoo niin”. Kun logiikassa vaaditaan että jokin on ”effective”, niin tarkoitetaan, että se on tässä mielessä järkevä.

Ennen 1930-lukua tälle käsitteelle ei ollut täsmällistä määritelmää. Gödel tarvitsi sellaista omissa tutkimuksissaan ja ehdotti vuonna 1934 niin sanottuja yleisiä rekursiivisia funktioita. Alan Turing ehdotti 1936 sitä, mikä nykyisin tunnetaan Turingin koneina, ja perusteli vakuuttavasti niiden olevan hyvin kattava käsite. Alonzo Churchin ehdotus vuodelta 1936 oli λ-kalkyyli. Osoittautui, että nämä kolme näennäisesti hyvin erilaista määritelmää tuottavat täysin saman käsitteen. Niinpä ei ole väliä, mitä niistä käytetään. Ehdotusta, että ”effective” määritellään tarkoittamaan jotakin niistä kutsutaan nykyisin *Church–Turingin teesiksi* (*Church–Turing thesis*). Myöhemmin



Kuva 41: Turingin kone alussa ja kesken laskennan

on havaittu, että moni muukin määritelmä johtaa samaan käsitteeseen. Siksi Church–Turingin teesi on nykyisin erittäin vahvalla pohjalla.

Church–Turingin teesi ei ole matemaattinen lause, vaan ehdotus, mikä tarkka ja täsmällinen matemaattinen käsite kannattaisi valita sumean käsitteen ”effective” vastineeksi matematiikassa. Tarkkojen määritelmien tarvetta voi havainnollistaa esimerkillä pikkulapsesta, joka ei halua syödä ruokaansa. Koska on karkkipäivä, hänen vanhempansa lupaa, että hän saa karkkia sitten kun lautanen on tyhjä. Lapsi kaataa lautasensa sisällön lattialle ja sanoo ”nyt lautanen on tyhjä.” Lapset voi ja pitää opettaa siihen, että vaikka sitä ei erikseen sanottaisikaan, mikä tahansa tapa tyhjentää lautanen ei kelpaa, vaan vain sellaiset, jotka vastaavat ruoan tarkoitusta ja hyviä käytöstapoja.

Matematiikalle (eikä tietokoneille) ei kuitenkaan voi opettaa vastaavaa, koska ne eivät tiedä asioiden tarkoitusta eivätkä osaa käytöstapoja. Niiden kannalta merkitystä on vain sillä, mitä määritelmät sanovat. Jos määritelmät sallivat järjettömiä lopputuloksia, niin matematiikka ja tietokoneet tuottavat järjettömiä lopputuloksia.

Turingin kone on yksinkertainen laskentalaite. Se on tarkoitettu teoreettisiin tarkasteluihin eikä oikeaksi käytännön tietokoneeksi. Sen muistina on yksi tai useampi ääretön, ruutuihin jaettu nauha. Turingin koneesta on muunnelmia muun muassa sen mukaan kuinka monta nauhaa on ja ovatko ne oikealle vai molempiin suuntiin äärettömiä. Turingin koneella on jokaista nauhaa varten yksi luku / kirjoituspää, joka on joka hetki jonkin ruudun kohdalla. Lisäksi Turingin koneella on ohjausyksikkö, jolla on äärellinen määrä sisäisiä tiloja. Kuvassa 41 on havainnollistettu Turingin konetta jolla on yksi, oikealle mutta ei vasemmalle ääretön nauha.

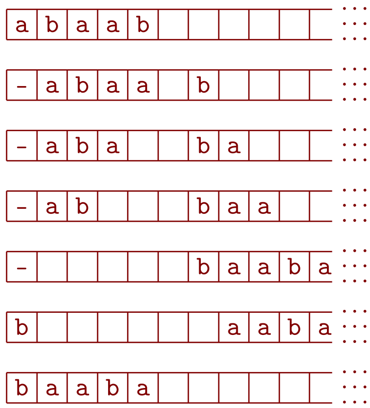
On sovittu jokin epätyhjä äärellinen joukko Γ, jota kutsutaan *aakkostoksi* (*alphabet*). Se voi olla vaikka $\{\texttt{a}, \ldots, \texttt{z}, \text{␣}\}$. Symboli ␣ edustaa tyhjää ruutua. Joka hetki kukin ruutu sisältää täsmälleen yhden merkin tästä aakkostosta. Vain äärellisessä määrässä ruutuja on muu merkki kuin ␣, mutta tämä määrä voi kasvaa rajatta koneen toiminnan edetessä.

Turingin koneen syöte on äärellinen merkkijono. Aluksi nauhan alussa on Turingin koneen syöte, nauha on muuten tyhjä, luku / kirjoituspää on nauhan ensimmäisen merkin kohdalla, ja ohjausyksikkö on tilassa jota kutsutaan *alkutilaksi* (*initial state*). Tästäkin on muunnelmia, mutta aika yleistä on, että jokin Γ:n osajoukko Σ on nimetty syöteaakkostoksi, ja syöte saa sisältää vain sen alkioita. Tyhjän merkki ␣ ei kuulu syöteaakkostoon.

Turingin koneen askel koostuu kolmesta vaiheesta. Ensin kone katsoo, mikä merkki on luku / kirjoituspään kohdalla nauhalla. Sitten kone kirjoittaa samaan kohtaan uuden merkin (joka voi olla sama kuin vanha merkki), sekä vaihtaa sisäistä tilaansa (tai jättää vaihtamatta). Lopuksi luku / kirjoituspää siirtyy yhden askeleen verran vasemmalle tai oikealle, tai pysyy paikallaan. Turingin kone tekee tällaisia askelia niin pitkään kuin mahdollista.

Ohjausyksikkö toimii taulukon mukaan, jossa on kahta vaille jokaiselle sisäiselle tilalle ja jokaiselle aakkoston merkille lueteltu, minkä uuden merkin kone kirjoittaa

q_1	␣	q_{23}	␣	|	tyhjällä syötteellä lopeta heti
q_1	a	q_2	-	>	kirjoita reunamerkki, ota a mukaan
q_1	b	q_3	-	>	kirjoita reunamerkki, ota b mukaan
q_2	␣	q_4	␣	>	ohita yksi tyhjä a mukana
q_2	a	q_2	a	>	kirjoita a, ota a mukaan
q_2	b	q_3	a	>	kirjoita a, ota b mukaan
q_3	␣	q_5	␣	>	ohita yksi tyhjä b mukana
q_3	a	q_2	b	>	kirjoita b, ota a mukaan
q_3	b	q_3	b	>	kirjoita b, ota b mukaan
q_4	␣	q_6	a	<	kirjoita a, lähde paluumatkalle
q_5	␣	q_6	b	<	kirjoita b, lähde paluumatkalle
q_6	␣	q_6	␣	<	ohita osien välinen tyhjä alue
q_6	-	q_{12}	-	>	siirrä merkkijono vasempaan reunaan
q_6	a	q_7	␣	>	lähde viemään a käännetyn loppuun
q_6	b	q_8	␣	>	lähde viemään b käännetyn loppuun
	...		...		
q_{21}	␣	q_{23}	a	>	kirjoita a ja lopeta tuloksen perässä
q_{22}	␣	q_{23}	b	>	kirjoita b ja lopeta tuloksen perässä



Kuva 42: Merkkijonon kääntö takaperin Turingin koneella

nauhalle, mihin sisäiseen tilaan kone siirtyy ja mihin suuntaan luku / kirjoituspää siirtyy. Ne kaksi tilaa, joille tämä on jätetty määrittelemättä, edustavat vastauksia ”kyllä” ja ”ei”. Ohjausyksikön joutuessa jompaankumpaan niistä kone pysähtyy. Se pysähtyy myös, jos luku / kirjoituspää on nauhan vasemmassa reunassa ja sen pitäisi siirtyä vasemmalle. Silloin vastaus on ”ei”. Näistäkin yksityiskohdista on muunnelmia. Esimerkiksi nauhan vasemmasta reunasta putoaminen voidaan estää sillä, että nauhalla on alkumerkki, jonka tilalle ei voi kirjoittaa muuta, jota ei voi kirjoittaa muualle, ja jonka kohdalla luku / kirjoituspää ei voi siirtyä vasemmalle.

Kuvassa 42 on osa sellaisen Turingin koneen ohjausyksikön taulukosta, joka kääntää takaperin merkkijonon syöteaakkostosta $\{\mathtt{a},\mathtt{b}\}$. Kuvassa on myös havainnollistettu koneen toimintaa. Jos syöte on tyhjä, kone lopettaa heti siirtymällä lopputilaan q_{23}. Muussa tapauksessa kone ottaa vasemmanpuoleisimman merkin muistiin sisäiseen tilaansa, kirjoittaa sen tilalle - ja siirtyy oikealle. Sen jälkeen se toistuvasti ottaa luku / kirjoituspään alla olevan merkin muistiin, kirjoittaa sen tilalle edellisen muistiin ottamansa merkin ja siirtyy oikealle kunnes se kohtaa tyhjän ruudun. Tilassa q_2 se on matkalla oikealle muistissaan a, ja tilassa q_3 se on matkalla oikealle muistissaan b. Kohdattuaan tyhjän ruudun se siirtyy vielä yhden ruudun oikealle ja kirjoittaa muistiin ottamansa merkin sinne (q_4 ja q_5). Näin se tulee siirtäneeksi merkkijonon oikeanpuoleisimman merkin kaksi ruutua oikealle ja muut merkit yhden ruudun oikealle.

Sitten se palaa takaisin vasemmalle kunnes kohtaa epätyhjän merkin. Jos se on a tai b, niin kone ottaa sen mukaansa, kirjoittaa sen tilalle ␣, kulkee oikealle tyhjän alueen yli ja epätyhjän alueen yli, ja kirjoittaa mukaansa ottamansa merkin sinne. Sitten se lähtee uudelleen vasemmalle ja ohittaa ensin epätyhjän ja sitten tyhjän alueen. Se ottaa mukaansa seuraavan merkin a tai b, ja vie sen oikealle tyhjän alueen yli ja epätyhjän alueen jatkoksi. Se jatkaa tätä kunnes haettavan merkin tilalla onkin -. Silloin se on kopioinut koko syötteen oikealle ja samalla kääntänyt sen takaperin.

Seuraavaksi se siirtää samankaltaisilla keinoilla merkkijonon nauhan vasempaan reunaan. Aina siirrettävän merkin hakiessaan se tarkastaa, onko sen jälkeen tyhjä ruutu. Sitten kun on, se siirtää vielä tämän merkin kiinni jo siirrettyyn merkkijonoon, mutta ei enää palaa hakemaan uutta merkkiä vaan siirtyy yhden ruudun oikealle ja lopettaa.

Turingin koneita käytetään sen tutkimiseen, mitä osittaisia funktioita merkkijonoilta merkkijonoille tai merkkijonoilta totuusarvoille voidaan ja ei voida laskea, ja kuinka nopeasti ne voidaan laskea. Kuten esimerkistä varmaan kävi ilmi, Turingin koneita on työläs laatia, ja pienenkin asian laskeminen saattaa vaatia Turingin koneelta paljon toimenpiteitä. Tästä huolimatta Turingin koneilla voi laskea minkä tahansa osittaisen funktion minkä oikeallakin tietokoneella. Myöskään Turingin koneen nopeusero oikeisiin tietokoneisiin verrattuna ei ole niin suuri kuin miltä ehkä näyttää. Kaiken minkä voi laskea oikealla tietokoneella polynomiajassa, voi laskea myös Turingin koneella polynomiajassa.

Alan Turing osoitti, että on olemassa *universaali Turingin kone* (*universal Turing machine*), joka pystyy matkimaan mitä tahansa Turingin konetta. Sille annetaan kaksiosainen syöte, jonka toinen osa esittää matkittavan Turingin koneen ohjausyksikön ja toinen osa on matkittavan Turingin koneen syöte. Matkittavan Turingin koneen ohjausyksikön esittävä osa on periaatteessa tietokoneohjelma.

Lisäksi Turingin koneilla on yksi ylivoimainen etu oikeisiin tietokoneisiin verrattuna: Turingin koneen muisti ei koskaan lopu kesken. Oikealla tietokoneella ei voi laskea miten suurta tehtävää tahansa, mutta Turingin koneella voi. Oikean tietokoneen keskusmuistia voi laajentaa vain niin kauan kuin osoiteavaruudessa riittää tilaa. Sen jälkeen voidaan hankkia lisää kiintolevyasemia. Jos kuitenkin niitä hankitaan lisää ja lisää, niin tarvitaan aina vain pitempi luku ilmoittamaan mistä kiintolevyasemasta tieto haetaan tai mille talletetaan. Jossain vaiheessa tietokone ei enää kykene esittämään niin suurta lukua. Tämä ongelma voidaan välttää laittamalla kiintolevyasemat jonoon ja viittaamalla niihin lukujen sijaan sanoilla ”seuraava” ja ”edellinen”. Mutta siinä vaiheessa järjestelmästämme on tullut Turingin kone, jonka nauhan ruutuja ovat kiintolevyasemat!

Algoritmien analyysissa ajatellaan tavallisesti, että esimerkiksi yhteenlasku, kahden luvun suuruusjärjestyksen vertaaminen ja taulukon indeksointi vievät kukin vakioajan. Siis esimerkiksi testi onko $A[0] = 1$ vie saman ajan kuin testi onko $A[1000000] = 1234567$. Tämä oletus on realistinen vain jos lukujen ja taulukoiden koolla on yläraja. Algoritmien analyysissa käytettävät O-merkintä, Θ-merkintä ja niin edelleen keskittyvät siihen, kuinka paljon aikaa tai muistia kuluu jos syöte on jotakin rajaa suurempi. Siksi, jos ollaan aivan tarkkoja, niiden käyttö olettaa, että syöte voi olla miten suuri tahansa. Nämä kaksi oletusta eivät todellisuudessa voi olla yhtäaikaa voimassa! Oikeissa tietokoneissa testi onko $A[0] = 1$ vie saman ajan kuin testi onko $A[1000000] = 1234567$, mutta oikean tietokoneen syöte ei voi olla miten suuri tahansa. Turingin koneilla tilanne on päinvastainen: syöte voi olla miten suuri tahansa, mutta yhteenlasku ja niin edelleen vievät sitä pitemmän ajan, mitä isompia lukuja käsitellään.

Niinpä tavallisen algoritmien suorituskykyanalyysin tulos on vain likiarvo siitä, mitä oikeasti tapahtuu. Se on kuitenkin hyvin usein erittäin hyvä likiarvo, paljon parempi kuin muilla keinoilla voidaan saavuttaa ainakaan yhtä helposti. (Jos haluat tutustua tapauksiin joissa se onkin hyvin huono likiarvo, niin lue Wikipedian sivu ”Galactic algorithm”.)

Turingin koneilla vastaavaa likimääräisyyttä ei synny, koska Turingin koneen syöte voi olla miten suuri tahansa. Toisaalta suoritusaikaa kuvaavasta funktiosta tulee Turingin koneilla melkein aina jonkin verran nopeammin kasvava kuin tavallisessa algoritmianalyysissa, koska Turingin kone joutuu kulkemaan nauhaa edestakaisin siinä missä tavallinen tietokone voi osoittaa mitä tahansa muistipaikkaa vakioajassa, ja Turingin koneiden tapauksessa muun muassa yhteenlasku kestää sitä kauemmin mitä isompia luvut ovat, toisin kuin tavallisessa algoritmianalyysissa. Tällä nopeuserolla on merkitystä kun puhutaan esimerkiksi neliöllisistä algoritmeista, mutta ei ole kun puhutaan polynomiaalisista tai sitä hitaammista algoritmeista.

Aivan hyvin voi ajatella, että Turingin koneella voidaan laskea kaikki se ja vain se, mitä tavallisella ohjelmointikielellä voisi laskea, jos muisti ei koskaan loppuisi kesken, kokonaislukujen sanapituus olisi rajaton ja vuorovaikutus käyttäjän kanssa olisi rajoitettu siihen, että käyttäjä antaa syötteeksi merkkijonon ja saa vastaukseksi joko merkkijonon tai merkkivalon ”kyllä” tai ”ei” syttymisen — ellei kone jää ikuiseen silmukkaan.

Kuten tavallinenkin tietokone, myös Turingin kone voi jäädä ikuiseen silmukkaan. Siksi Turingin kone ei välttämättä laske funktiota syötteeltä tulokselle, vaan osittaisen funktion. Niillä syötteillä joilla Turingin kone lopulta pysähtyy, funktion arvo on nauhan sisältö koneen pysähdyttyä. (On erilaisia määritelmiä sille, mitä ”nauhan sisältö” tarkalleen ottaen tarkoittaa tässä. Se voi esimerkiksi loppua viimeiseen epätyhjään ruutuun, ensimmäisen tyhjän ruudun eteen tai luku / kirjoituspään sijainnin eteen. Missä tapauksessa kaksi ensimmäistä näistä eivät tarkoita samaa?) Niillä syötteillä joilla Turingin kone ei pysähdy, funktion arvoa ei ole määritelty. *Osittainen rekursiivinen funktio* (*partial recursive function*) on osittainen funktio, jonka voi laskea Turingin koneella.

Kaikkein alkeellisin mutta samalla erittäin tärkeä tapa tuottaa tulos Turingin koneella on syötteiden jako kahteen joukkoon: niihin joilla annettu Turingin kone pysähtyy, ja niihin joilla se ei pysähdy. *Rekursiivisesti lueteltava joukko* (*recursively enumerable set*) tarkoittaa mitä tahansa joukkoa merkkijonoja, jolle on olemassa Turingin kone, joka pysähtyy joukon alkioille ja laskee ikuisesti muille merkkijonoille. Joillekin rekursiivisesti lueteltaville joukoille, mutta ei jokaiselle, on olemassa myös Turingin kone, joka laskee ikuisesti joukon alkioille ja pysähtyy muille merkkijonoille. Niinpä rekursiivinen lueteltavuus ei ole symmetrinen ”kyllä”:n ja ”ei”:n suhteen.

Tätä epäsymmetrisyyttä voi havainnollistaa Lothar Collatzin vuonna 1937 esittämän ajatusleikin avulla. Aloitetaan jostakin positiivisesta kokonaisluvusta. Jos se on parillinen, niin se jaetaan kahdella. Muussa tapauksessa se kerrotaan kolmella ja lisätään tulokseen yksi. Näin saadulle luvulle tehdään sama ja niin edelleen, kunnes tuloksena on 1. Aloitetaan esimerksi luvusta 6. Se on parillinen, joten se jaetaan kahdella ja saadaan 3. Se on pariton, joten se kerrotaan kolmella ja lisätään 1, jolloin saadaan 10. Se on parillinen, joten se jaetaan kahdella ja saadaan 5. Se on pariton, joten se kerrotaan kolmella ja lisätään 1, jolloin saadaan 16. Se on parillinen, joten se jaetaan kahdella ja saadaan 8. Se on parillinen, joten se jaetaan kahdella ja saadaan 4. Se on parillinen, joten se jaetaan kahdella ja saadaan 2. Se on parillinen, joten se jaetaan kahdella ja saadaan 1 ja lopetetaan.

Tämä prosessi voidaan helposti ohjelmoida tietokoneelle. Niinpä suoraan määritelmästä seuraa, että niiden kokonaislukujen joukko, joille Collatzin prosessi pysähtyy, on rekursiivisesti lueteltava. Jos lähtökohdaksi valitulla luvulla prosessi pysähtyy, niin siitä on mahdollista saada varma tieto jatkamalla niin kauan kunnes se pysähtyy. Jos kuitenkin yrittää tätä mutta se ei pysähdykään, niin joutuu jatkamaan ja jatkamaan loputtomiin. Jos on jatkanut jo kauan ja prosessi vain poukkoilee ylös alas, niin mistä voi tietää, kannattaako jatkaa? Luvulla 27 jono alkaa 27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214, 107, 322, 161, 484, ... Jaksatko jatkaa niin kauan, kunnes se pysähtyy? Entä jos se ei koskaan pysähdykään?

Rekursiivinen joukko (*recursive set*) tarkoittaa mitä tahansa joukkoa merkkijonoja, jolle on olemassa Turingin kone, joka vastaa ”kyllä” joukon alkioille ja ”ei” muille merkkijonoille. Voidaan osoittaa, että tämä on sama asia kuin että on olemassa sekä Turingin kone, joka pysähtyy joukon alkioille ja laskee ikuisesti muille merkkijonoille, että Turingin kone, joka laskee ikuisesti joukon alkioille ja pysähtyy muille merkkijonoille. Niinpä joukko on rekursiivinen jos ja vain jos sekä se itse että sen komplementti on rekursiivisesti lueteltava. Rekursiivisuus on siis symmetrinen ”kyllä”:n ja ”ei”:n suhteen.

Edellä todettiin, että tarvitaan ”järkevyysehto”, joka kieltää muun muassa sellaiset todistukset, joiden yhtenä vaiheena on ”sen, että tästä kaavasta seuraa tuo kaava näkee seuraavana yönä unessa, kun ennen nukkumaan menoa syö teelusikallisen kärpässientä”. Nykyisin ”järkevyysehtona” käytetään tilanteesta riippuen joko vaatimusta, että todistusten tai todennusten joukon pitää olla rekursiivisesti lueteltava, tai vaatimusta, että sen pitää olla rekursiivinen. Toisin sanoen, päättelyjärjestelmän tai muun todennusmenetelmän pitää olla sellainen, että on olemassa tietokoneohjelma (tai ainakin sellainen voitaisiin tehdä), joka tarkastaa, noudattaako sille syötteeksi annettu merkkijono päättelyjärjestelmän tai muun todennusmenetelmän sääntöjä pilkuntarkasti. Ohjelman pitää antaa vastauksensa joko muodossa ”kyllä” tai ”ei”, tai pysähtymällä jos syötemerkkijono noudattaa sääntöjä ja laskemalla ikuisesti jos se ei noudata.

”Järkevyysehtoa” tarvitaan myös kun halutaan käyttää ääretöntä joukkoa aksioomia. Jotta ääretöntä aksioomajoukkoa voitaisiin käytännössä käyttää, se täytyy esittää jollain sellaisella äärellisellä tavalla, että mistä tahansa aksioomasta voidaan äärellisellä työllä varmistua, että se todella on aksiooma. Toisin sanoen, aksioomien joukon pitää olla rekursiivisesti lueteltava. Jollei tämä ehto toteudu, niin todistusta, joka käyttää sellaista aksioomaa, ei voi tarkastaa, koska ei voida todentaa, että aksioomaksi väitetty merkkijono todella on aksiooma.

Ääriesimerkki tästä on asettaa aksioomaksi jokainen puheenaiheessa tosi suljettu kaava ja vain ne. Todistamisessa ei silloin koskaan tarvita kuin korkeintaan kolme askelta: kaavan muuttaminen suljetuksi lisäämällä sen eteen jokaista siinä vapaana esiintyvää muuttujaa x kohti $\forall x:$, niin saadun kaavan todentaminen aksioomaksi, ja lisättyjen $\forall x:$ poistaminen [82]:lla. Tätä ei kuitenkaan voida käytännössä toteuttaa, jollei ole olemassa keinoa todeta tutkittavaa suljettua kaavaa aksioomaksi.

Edellä on käytetty aksioomaskeemoja esittämään äärettömiä aksioomien joukkoja. Esimerkiksi [94] tekee niin. Luvussa 5.2 käytimme ääretöntä aksioomien joukkoa ”solmuja on ainakin 2”, ”solmuja on ainakin 3”, ”solmuja on ainakin 4”, ..., jossa kukin aksiooma on muotoa (31). Vaikka tätä joukkoa ei voi esittää yhtä yksinkertaisena skeemana kuin [94], ihmiset pystyvät silti itse tarkastamaan tai tekemään tietokoneohjelman joka tarkastaa kuuluuko annettu merkkijono siihen. Reaalisuljettujen kuntien teoriassa on jokaista parittoman asteista polynomia varten aksiooma, joka sanoo, että sillä on nollakohta. Sääntö tai tietokoneohjelma, joka tunnistaa onko merkkijono tällainen aksiooma, saattaa olla työläs kirjoittaa, mutta silti on selvää, että sellainen voidaan kirjoittaa. Niinpä jokainen tähän mennessä käyttämämme aksioomaskeema tuottaa rekursiivisesti lueteltavan joukon aksioomia. Tästedes voimme käyttää skeemojen tilalla mitä tahansa tapaa josta pystymme perustelemaan, että sekin tuottaa rekursiivisesti lueteltavan joukon aksioomia.

Eri lähteissä esiintyy jonkin verran vaihtelevuutta predikaattilogiikan käsitteiden nimityksissä. Seuraavassa on esitelty yksi käsitteistö, joka pyrkii olemaan sisäisesti johdonmukainen ja vastaamaan usein käytettyjä nimityksiä.

Kuten edellä kerrottiin, *sanasto* (*signature* tai *vocabulary*) on luettelo ei-loogisia symboleita lajitietoineen ja paikkalukuineen. Lajina voi olla vakio-, funktio- tai relaatiosymboli, ja paikkaluku tarvitaan vain jälkimmäisille. Esimerkiksi reaalisuljettujen kuntien sanastoksi valitaan yleensä vakiosymbolit 0 ja 1, kaksipaikkaiset funktiosymbolit $+$ ja $\cdot$ (kertolasku), sekä kaksipaikkainen relaatiosymboli $\leq$.

Tulkinta (*interpretation*) koostuu epätyhjästä joukosta sekä siitä, että jokaiselle sanaston symbolille annetaan arvo tämän joukon avulla. Tätä joukkoa merkitään toisinaan symbolilla $\mathbb{D}$. Vakiosymbolin arvo on tietenkin tämän joukon alkio, funktiosymbolin arvo on funktio ja relaatiosymbolin arvo on relaatio. *Tarkoitettu tulkinta* (*intended interpretation*) on esimerkiksi se tulkinta, johon kyseisessä asiayhteydessä viitataan esimerkiksi puhumalla ”reaaliluvuista” tai ”luonnollisista luvuista”.

Looginen *kieli* (*language*) on kaikki kaavat, jotka voidaan kirjoittaa valitulla sanastolla ja logiikan symboleilla. Logiikan symboleita ovat muuttujasymbolit, (,), =, F, T, konnektiivit ja kvanttorit tarpeellisine välimerkkeineen. Muut atomikaavat kuin F ja T kirjoitetaan yleensä joko sovellusalueesta tutulla syntaksilla tai muodossa $\mathit{termi} = \mathit{termi}$ tai muodossa $\mathit{relaatiosymboli}(\mathit{termi},\ldots,\mathit{termi})$, missä *termi* on vakiosymboli, muuttujasymboli tai muotoa $\mathit{funktiosymboli}(\mathit{termi},\ldots,\mathit{termi})$. Atomikaavoista ylöspäin tässä kirjassa noudatetaan kuvassa 24 esitettyä syntaksia, paitsi että ylin rivi muuttuu muotoon

$$\mathit{Kaava} \quad ::= \quad \mathit{EkvKaava} \mid \forall\, \mathit{Muuttuja} : \mathit{Kaava} \mid \exists\, \mathit{Muuttuja} : \mathit{Kaava}$$

Sijoitus (*assignment*) antaa jokaiselle vapaalle muuttujalle arvon tulkinnan ilmoittamasta joukosta. Kun tulkinta ja sijoitus on valittu, on jokaisella kaavalla yksikäsitteinen totuusarvo. Suljetun kaavan totuusarvo määräytyy ilman sijoitustakin.

Jos φ on suljettu kaava ja M on tulkinta, niin ilmaus M on φ:n *malli* (*model*) ja merkintä $M \models \varphi$ tarkoittavat, että φ on tosi M:ssä. Jos lisäksi Γ on joukko suljettuja kaavoja, niin $M \models \Gamma$ tarkoittaa, että jokainen $\varphi \in \Gamma$ on tosi M:ssä. Tällöin M on Γ:n malli. Jos φ on kaava, M on tulkinta ja ν on sijoitus, niin $M, \nu \models \varphi$ tarkoittaa, että φ on tosi M:ssä ν:n mukaisilla vapaiden muuttujien arvoilla. Tällöin M, ν on φ:n malli. Jos lisäksi Γ on joukko kaavoja, niin $M, \nu \models \Gamma$ tarkoittaa, että jokainen $\varphi \in \Gamma$ on tosi M:ssä ν:n mukaisilla vapaiden muuttujien arvoilla. Tällöin M, ν on Γ:n malli.

Kaava φ on kaavajoukon Γ *looginen seuraus* (*logical consequence*), merkitään $\Gamma \models \varphi$, jos ja vain jos jokainen Γ:n malli on myös φ:n malli. Siis φ on Γ:n looginen seuraus jos ja vain jos aina kun ei-loogisten symbolien tulkinta ja vapaiden muuttujien arvot on valittu siten, että jokainen Γ:n kaava on tosi, myös φ on tosi. Kun arvioidaan onko φ looginen seuraus, niin ei-loogisten symbolien tulkinnasta ja vapaiden muuttujien arvoista oletetaan vain se, mikä on kerrottu Γ:ssa.

Esimerkiksi $x > 2 \Rightarrow x > 1$ ei ole looginen seuraus, koska se ei ole totta muun muassa silloin kun $>$ tulkitaan tarkoittamaan ”erisuuri” ja 1 ja 2 tulkitaan normaalisti, koska 1 on erisuuri kuin 2 mutta 1 ei ole erisuuri kuin 1. Sen sijaan $x > 2 \wedge 2 > 1 \wedge \forall x : \forall y : \forall z : x > y \wedge y > z \rightarrow x > z \Rightarrow x > 1$ on looginen seuraus, koska sen vasen puoli rajoittaa malleja niin paljon, että jäljelle ei jää sellaisia, joissa vasen puoli pätee mutta oikea puoli ei päde. Myös $x > 1 \wedge 1 > 2 \wedge \forall x : \forall y : \forall z : x > y \wedge y > z \rightarrow x > z \Rightarrow x > 2$ on looginen seuraus, mutta $x > 1 \wedge 1 > 2 \Rightarrow x > 2$ ei ole.

Päättelyjärjestelmä (*proof system*) kertoo, miten kaavojen joukoista saa johtaa kaavoja. Sitä, että joukosta Γ voidaan johtaa φ, merkitään $\Gamma \vdash \varphi$.

Päättelyjärjestelmä on *eheä* (*sound*), jos ja vain jos siinä voi johtaa vain sellaisia kaavoja, jotka seuraavat loogisesti lähtökohdista. Toisin sanoen eheys tarkoittaa sitä, että jos $\Gamma \vdash \varphi$, niin $\Gamma \models \varphi$. Eheydestä seuraa, että päättelyjärjestelmä tuottaa tosista lähtökohdista vain tosia lauseita. Päättelyjärjestelmän eheys on yleensä helppo todistaa. Eheyden todistukset ovat yleensä hyvin epämuodollisia ja vetoavat intuitioon, koska ne eivät itse asu formaaleissa teorioissa vaan formaalien teorioiden ja ihmisten ajattelun rajalla.

Sanaa *teoria* (*theory*) käytetään logiikassa tyypillisesti kahdessa eri merkityksessä. Sillä voidaan tarkoittaa kaikkien puheenaihetta koskevien tosien kaavojen joukkoa. Tämä joukko riippuu paitsi tietenkin puheenaiheesta, myös valitusta sanastosta ja logiikasta (ensimmäisen kertaluvun, toisen kertaluvun, ...), koska ne määräävät, mitä kaavoja voi kirjoittaa.

Toisessa käyttötavassa teoria eritellään antamalla sanasto ja joukko suljettuja kaavoja. Tätä joukkoa kutsutaan usein *aksioomiksi* (*axioms*). Teorian malli on tulkinta, joka toteuttaa jokaisen aksiooman. Tavallisesti on sovittu jokin päättelyjärjestelmä, jolla aksioomista voidaan johtaa lisää kaavoja. Jos tämä päättelyjärjestelmä on eheä ja jos jokainen aksiooma on puheenaiheessa tosi, niin myös teoria on eheä eli tuottaa vain puheenaiheessa tosia kaavoja.

Kaavojen toteamiseen puheenaiheessa tosiksi on käytössä muitakin menetelmiä kuin niiden johtaminen aksioomista päättelyjärjestelmässä. Esimerkiksi moni alakoululainen osaa todeta kaavan $12 + 25 = 36$ epätodeksi ja kaavan $12 + 25 = 37$ todeksi laskemalla 12 ja 25 yhteen kynällä ja paperilla ja huomaamalla, että tulos ei ole 36 mutta on 37. *Todennusmenetelmä* tarkoittaa tässä kirjassa mitä tahansa hyvin määriteltyä menetelmää, jolle voi antaa mielivaltaisen merkkijonon ja joka ilmoittaa tai jättää ilmoittamatta sen todeksi kaavaksi. (Logiikassa sille ei ole vakiintunutta sanaa.) Todennusmenetelmä voi siis olla aksioomien ja päättelyjärjestelmän yhdistelmä; pelkkiä lukuvakioita ja niiden laskutoimituksia sisältävän kaavan tarkastaminen alakoulussa opetetuin keinoin; tietokoneohjelma, joka saa syötteekseen merkkijonon ja vastaa tai ei vastaa ”tosi”; tai jokin muu hyvin määritelty menetelmä.

Todennusmenetelmä on *eheä* (*sound*), jos ja vain jos se todentaa vain puheenaiheessa tosia kaavoja. Todennusmenetelmä on *ristiriitainen* (*inconsistent*) jos ja vain jos jollekin kaavalle φ se todentaa sekä φ:n että $\neg\varphi$:n. Jokainen eheä todennusmenetelmä on ristiriidaton, koska sekä φ että $\neg\varphi$ eivät voi olla yhtäaikaa tosi. Toisinpäin ei päde: todennusmenetelmä voi olla ristiriidaton mutta epäeheä todentamalla väärän kaavoista φ ja $\neg\varphi$. Esimerkiksi reaaliluvuille tarkoitettu todennusmenetelmä, joka toimii muuten täysin oikein mutta tulkitsee symbolin $\leq$ (ja siitä johdetut symbolit $<$, $\geq$ ja $>$) väärinpäin, on ristiriidaton (koska se on vain merkintätavan muunnos ”oikeasta” reaalilukujen teoriasta) mutta epäeheä (koska se todentaa esimerkiksi kaavan $1 \leq 0$).

Eheys viittaa malleihin tai puheenaiheeseen. Se puhuu siitä, että kaava on tai ei ole tosi jossakin tulkinnassa ja sijoituksessa, tai siitä, että kaava on tai ei ole tosi puheenaiheessa. Ristiriidattomuus ei viittaa malleihin eikä puheenaiheeseen, vaan siihen mitä aksioomista voidaan johtaa päättelyjärjestelmässä tai mitä jokin muu todennusmenetelmä ilmoittaa todeksi. Niin sanotussa parakonsistentissa logiikassa hyväksytään ristiriitaisia järjestelmiä, mutta logiikan valtavirrassa ristiriidattomuus on ehdoton tavoite. Ristiriidattomuus takaa, että kaavat puhuvat *jostakin asiasta* oikein, mutta se ei takaa, että ne puhuvat oikein nimenomaan *siitä asiasta*, josta oli tarkoitus puhua.

Päättelyjärjestelmä on *täydellinen* (*complete*), jos ja vain jos se johtaa jokaisen loogisen seurauksen. Toisin sanoen, jos φ on kaava ja Γ on joukko kaavoja, niin täydellisyys vaatii, että jos $\Gamma \models \varphi$, niin $\Gamma \vdash \varphi$. Joukko aksioomia on *täydellinen* (*complete*), jos ja vain jos ei ole olemassa suljettua kaavaa, joka on tosi aksioomien jossakin mallissa mutta ei kaikissa malleissa. Täydellisellä aksioomien joukolla voi siis olla eri malleja, mutta jokainen niistä on samaa mieltä kunkin suljetun kaavan totuusarvosta. Todennusmenetelmä on *täydellinen* (*complete*), jos ja vain jos se todentaa kaikki puheenaihetta koskevat todet kaavat. Jos aksioomien joukko ja päättelyjärjestelmä ovat täydelliset, niin myös niiden yhdessä muodostama todennusmenetelmä on täydellinen.

Koska tyypillisesti hyväksytään periaate, että mahdottomasta seuraa mitä tahansa, laaditaan päättelyjärjestelmät tyypillisesti sellaisiksi, että ristiriidasta voi johtaa minkä tahansa kaavan. Siksi ristiriitainen aksioomien ja tyypillisen päättelyjärjestelmän yhdistelmä johtaa jokaisen kaavan. Niinpä se on täydellinen. Silti sitä ei voi käyttää selvittämään mistään kaavasta φ päteekö se vai ei, koska se todistaa sekä φ että $\neg\varphi$. Siksi täydellisyys on harvoin hyödyllinen muutoin kuin samanaikaisesti ristiriidattomuuden kanssa. Valitettavasti suurelle osalle mielenkiintoisia puheenaiheita on mahdotonta löytää ristiriidaton täydellinen todennusmenetelmä.

Yleisesti ottaen ristiriitaisuus voi johtua virheellisistä aksioomista tai virheellisistä päättelysäännöistä, ja epätäydellisyys voi johtua aksioomien tai päättelysääntöjen puutteesta. Ensimmäisen kertaluvun teorioiden kohdalla tilanne on parempi. Niille on useita eheitä ristiriidattomia täydellisiä päättelyjärjestelmiä, aika yksinkertaisiakin. Luvussa 6 esitellään niistä yksi. Siksi ensimmäisen kertaluvun tapauksessa ongelmana on ”vain” löytää ristiriidaton täydellinen aksiomatisointi, eli sellainen, että se luonnehtii puheenaiheen tarkasti. Jos siinä onnistutaan, niin siitä voidaan johtaa kaikki loogiset seuraukset eikä muuta.

Todennusmenetelmä on *rekursiivisesti lueteltava* (*recursively enumerable*), jos ja vain jos se on esitettävissä tietokoneohjelmana, joka pysähtyy kaavoille jotka se todentaa ja laskee ikuisesti muille syötemerkkijonoille. Jos todennusmenetelmä on eheä, täydellinen ja rekursiivisesti lueteltava, niin mistä tahansa suljetusta kaavasta φ voidaan selvittää onko se tosi, laittamalla yksi Turingin kone todentamaan φ ja toinen Turingin kone todentamaan $\neg\varphi$ ja odottamalla, kunnes jompikumpi niistä pysähtyy. Täydellisyyden vuoksi ainakin toinen niistä lopulta pysähtyy. Eheyden vuoksi vain se voi pysähtyä, jonka käsittelemä kaava on tosi. Esimerkiksi reaalisuljetuille kunnille tunnetaan tällainen todennusmenetelmä. Valitettavasti se on joillekin kaavoille hyvin hidas, ja on todistettu, että tätä ei voi välttää. Gödel todisti vuonna 1931, että luonnollisille luvuille Peanon aritmetiikan sanastolla ei voi olla olemassa tällaista todennusmenetelmää.

5.4 Ensimmäisen kertaluvun logiikan suuria tuloksia

Tässä alaluvussa oletetaan valituksi jokin eheä täydellinen ensimmäisen kertaluvun päättelyjärjestelmä.

Leon Henkin esitti mallin olemassaololauseen väitöskirjassaan 1947 ja julkaisi sen tieteellisessä lehdessä vuonna 1949. Mallin olemassaololause sanoo, että jokaisella ensimmäisen kertaluvun ristiriidattomalla aksioomajärjestelmällä on malli. Sen todistus on monimutkainen, mutta voimme esittää sen suuren linjan.

Ideana on ensin lisätä järjestelmään aksioomia niin että siitä tulee lopulta täydellinen. Jokaisesta suljetusta kaavasta φ kokeillaan vuoron perään, tekisikö sen lisääminen aksioomiin aksioomajärjestelmästä ristiriitaisen. Jollei tee, niin φ lisätään, muussa tapauksessa $\neg\varphi$ lisätään. Tämä kokeileminen ja lisääminen ei ole konkreettista toimintaa, vaan kuvitteellinen päättymätön prosessi, josta täydellinen aksioomien joukko tulee ikään kuin raja-arvona. Tämä vaihe tunnetaan nimellä Lindenbaumin lemma Adolf Lindenbaumin mukaan, joka kuoli toisen maailmansodan seurauksena vuonna 1941.

Aina kun lisätään aksiooma muotoa $\exists x : \varphi(x)$, otetaan käyttöön uusi vakiosymboli c ja lisätään myös aksiooma $\varphi(c)$. Näin saadaan varmistettua nimi sille arvolle, jonka $\exists x : \varphi(x)$ väittää olevan olemassa. Vastaavasti aina kun lisätään aksiooma muotoa $\neg\forall x : \varphi(x)$, otetaan käyttöön uusi vakiosymboli c ja lisätään myös aksiooma $\neg\varphi(c)$. Näitä lisättäviä vakiosymboleita kutsutaan *Henkin-todistajiksi* (*Henkin witness*).

Lopuksi näin täydennetyn aksioomien joukon ohjaamana muodostetaan malli. Sitä varten niputetaan yhteen kaikki sellaiset vakiolausekkeet f ja g, joille $f = g$ on aksiooma. Muodostettavan mallin $\mathbb{D}$ on näiden nippujen joukko. Kaavojen ohjaamana saadaan selville, mitä minkäkin funktio- ja relaatiosymbolin pitää tuottaa milläkin argumenttien arvoilla.

Jos lähtökohtana käytetyn aksioomajärjestelmän sanasto on äärellinen, niin tällä tavalla syntyvä malli on äärellinen tai numeroituvasti ääretön. Sama pätee jos lähtökohtana käytetyn aksioomajärjestelmän sanasto on numeroituvasti ääretön. Käytännön aksioomajärjestelmät noudattavat tätä ehtoa melkein poikkeuksetta. Muun muassa reaalisuljettujen kuntien teorian sanasto on äärellinen, eihän siinä ole kuin viisi symbolia: 0, 1, $+$, $\cdot$ ja $\leq$. Niinpä sillä on numeroituva malli, vaikka reaalilukujen joukko on ylinumeroituva! Tämä kummallinen tilanne on mahdollinen muun muassa siksi, että ensimmäisen kertaluvun kaavoilla ei voi ilmaista niitä reaalilukujen joukon ominaisuuksia, jotka aiheuttavat ylinumeroituvuuden.

Gödelin täydellisyyslause sanoo, että jos Γ on joukko ensimmäisen kertaluvun aksioomia ja φ on niiden looginen seuraus, niin φ voidaan todistaa Γ:sta. (Siis jos $\Gamma \models \varphi$, niin $\Gamma \vdash \varphi$.) Se on helppo todistaa mallin olemassaololauseesta. Oletetaan, että φ:tä ei voi todistaa Γ:sta. Tällöin $\Gamma \cup \{\neg\varphi\}$ on ristiriidaton, koska jos se olisi ristiriitainen, niin tämän ristiriidan todistus olisi epäsuora todistus φ:lle. Niinpä sillä on Henkinin lauseen mukaan malli. Mutta se on Γ:n malli joka ei ole φ:n malli, joten φ ei ole Γ:n looginen seuraus.

Gödelin oma todistus vuodelta 1929 oli erilainen, tulokseltaan hieman heikompi ja vieläkin vaikeatajuisempi kuin mallin olemassaololauseen todistus. Tulos kulkee silti Gödelin nimissä, koska Gödel oli ensimmäinen joka todisti suurimman osan nykyisestä täydellisyyslauseesta.

Kompaktisuuslause sanoo, että ensimmäisen kertaluvun aksioomajärjestelmällä on malli jos ja vain jos sen jokaisella äärellisellä osajoukolla on malli. Toinen suunta on triviaali: alkuperäisen aksioomajärjestelmän malli on tietenkin myös jokaisen sen osajoukon malli. Toisinpäin, jos alkuperäisellä aksioomajärjestelmällä ei ole mallia, niin Henkinin mallin olemassaololauseen mukaan siitä voidaan johtaa ristiriita. Koska todistukset ovat äärellisiä, tämä ristiriidan todistus käyttää vain äärellistä määrää aksioomia. Sen käyttämät aksioomat muodostavat alkuperäisen aksioomajärjestelmän äärellisen osajoukon. Koska siitä voidaan johtaa F, koska päättelyjärjestelmämme oletettiin eheäksi ja koska F ei ole tosi missään mallissa, ei sillä ole mallia.

Lisää tekstiä tulossa ...

???

6 Gödelin täydellisyyslause

??? *Luonnollinen päättely* (*natural deduction*)

Myös predikaattilogiikan kompaktisuuslause ja alaspäin Löwenheim-Skolem, sekä niiden käyttö osoittamaan, että saavutettavuus ei ole ilmaistavissa 1. kertaluvun logiikassa.

7 Gödelin ensimmäinen epätäydellisyyslause

8 Määrittelemättömät termit kolmiarvoisella logiikalla

???

Tehtävien vastauksia

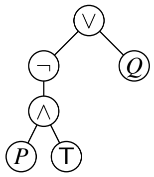
1. Tehtävän 1 mallivastaus on tässä. Tuossa on linkki takaisin tehtävän 1 kysymyksen kohdalle.

2. Voi ajatella niin, että sanassa ”hyvää” kaksi viimeistä kirjainta ovat sama (nimittäin ”ä”) ja myös sanassa ”ruokaa” kaksi viimeistä kirjainta ovat sama (nimittäin ”a”). Vaihtoehtoisesti voi ajatella, että sanojen ”söin” ja ”salaatin” viimeinen kirjain on sama (nimittäin ”n”) ja toiseksi viimeinen kirjain on sama (nimittäin ”i”). Tarkoitus oli, että huomaisit molemmat ajattelutavat ja hoksaisit, että ”kahdessa viimeisessä sanassa kaksi viimeistä kirjainta ovat samat” on monikäsitteinen.

3. Potenssilasku. Sen näkee vaikka siitä, että 2^{3^2} lasketaan kuten $2^{(3^2)} = 2^9 = 512$ eikä kuten $(2^3)^2 = 8^2 = 64$.

4. Jos ollaan ihan tarkkoja, niin oikea vastaus on ”kyllä”. Edellä päätettiin, että $\mathsf{F} \wedge P \wedge Q$ tarkoittaa samaa kuin $(\mathsf{F} \wedge P) \wedge Q$, eikä siis samaa kuin $\mathsf{F} \wedge (P \wedge Q)$. Toisaalta, kuten myöhemmin todistamme, $(\varphi \wedge \psi) \wedge \chi$ tuottaa aina saman totuusarvon kuin $\varphi \wedge (\psi \wedge \chi)$, ovatpa φ, ψ ja χ mitkä tahansa kaavat. Siksi esimerkistä seuraa välittömästi, että myös $\mathsf{F} \wedge P \wedge Q \Leftrightarrow \mathsf{F}$ pätee aina. Niinpä vastaus ”ei” ei ole suuresti väärin, vaan vain pikkuisen väärin.

7. φ:n tilalla on P ja ψ:n tilalla on T.

8. 

9. $\mathsf{T} \vee \psi \Leftrightarrow \mathsf{T}$ $\quad \mathsf{F} \vee \psi \Leftrightarrow \psi$ $\quad \varphi \vee \psi \Leftrightarrow \psi \vee \varphi$ $\quad \varphi \vee \varphi \Leftrightarrow \varphi$ [95]

11. $\varphi \vee \mathsf{F} \Leftrightarrow \varphi$ $\quad \varphi \vee \mathsf{T} \Leftrightarrow \mathsf{T}$ [96]

12. E ja F.

U	J	E	$U \wedge J$	$J \vee E$	$(U \wedge J) \vee E$	$U \wedge (J \vee E)$
F	F	F	F	F	F	F
F	F	T	F	T	T	F
F	T	F	F	T	F	F
F	T	T	F	T	T	F

13. Vasemmalle liitännäisyys: $X ? Y ? Z$ tarkoittaa samaa kuin $(X ? Y) ? Z$.

    Oikealle liitännäisyys: $X ? Y ? Z$ tarkoittaa samaa kuin $X ? (Y ? Z)$.

    Liitännäisyys: valitaanpa X:n, Y:n ja Z:n arvot miten tahansa, niin $(X ? Y) ? Z$ ja $X ? (Y ? Z)$ tuottavat saman arvon.

14. Vastaukseksi kelpaa P tosi ja Q epätosi. Vastaukseksi kelpaa myös P epätosi ja Q tosi.

15. $P \vee Q \wedge R \;\Leftrightarrow\; (P \vee Q) \wedge (P \vee R)$
    $P \wedge (Q \vee R) \;\Leftrightarrow\; P \wedge Q \vee P \wedge R$

16. Jos $P \Leftrightarrow \mathsf{F}$, niin $P \vee (Q \wedge R) \Leftrightarrow \mathsf{F} \vee (Q \wedge R) \Leftrightarrow Q \wedge R$ ja $(P \vee Q) \wedge (P \vee R) \Leftrightarrow (\mathsf{F} \vee Q) \wedge (\mathsf{F} \vee R) \Leftrightarrow Q \wedge R$, joten sama tuli. Jos $P \Leftrightarrow \mathsf{T}$, niin $P \vee (Q \wedge R) \Leftrightarrow \mathsf{T} \vee (Q \wedge R) \Leftrightarrow \mathsf{T}$ ja $(P \vee Q) \wedge (P \vee R) \Leftrightarrow (\mathsf{T} \vee Q) \wedge (\mathsf{T} \vee R) \Leftrightarrow \mathsf{T} \wedge \mathsf{T} \Leftrightarrow \mathsf{T}$, joten sama tuli.

17.
   - $\mathsf{F} \vee (Q \wedge R) \;\Leftrightarrow\; Q \wedge R \;\Leftrightarrow\; (\mathsf{F} \vee Q) \wedge (\mathsf{F} \vee R)$
   - $\mathsf{T} \vee (Q \wedge R) \;\Leftrightarrow\; \mathsf{T} \;\Leftrightarrow\; \mathsf{T} \wedge \mathsf{T} \;\Leftrightarrow\; (\mathsf{T} \vee Q) \wedge (\mathsf{T} \vee R)$

18. $a(b+c) = ab + ac$

19. Kertolasku pitää vaihtaa $\wedge$:ksi, yhteenlasku $\vee$:ksi ja $=$ $\Leftrightarrow$:ksi.

20. Saadaan $a + bc = (a+b)(a+c)$. Se ei ole koulumatematiikan laki, koska esimerkiksi sijoittamalla $a = b = c = 1$ saadaan $a + bc = 2$ mutta $(a+b)(a+c) = 4$.

21. Ensin saadaan $db + dc$, ja sitten $(a+d)(b+c) = a(b+c) + d(b+c) = ab + ac + db + dc$.

22. $(\varphi \vee \psi) \wedge \chi \;\Leftrightarrow\; (\varphi \wedge \chi) \vee (\psi \wedge \chi) \qquad (\varphi \wedge \psi) \vee \chi \;\Leftrightarrow\; (\varphi \vee \chi) \wedge (\psi \vee \chi)$ [97]

23. $\neg P \vee \neg(Q \vee R)$, $\neg(P \wedge (Q \vee R))$, $\neg(P \vee Q \wedge R)$ ja $\neg(P \vee (Q \vee R))$.

24. Ne luvut, jotka ovat pienempiä kuin kaksi tai vähintään viisi. Kakkosta pienemmät luvut ja vähintään viitosen suuruiset luvut.

25. ”Ei ole niin, että syön jäätelön ja menen elokuviin” tarkoittaa samaa kuin ”en syö jäätelöä tai en mene elokuviin”.

26.
   - $\neg(\mathsf{F} \wedge E) \;\Leftrightarrow\; \neg\mathsf{F} \;\Leftrightarrow\; \mathsf{T} \;\Leftrightarrow\; \mathsf{T} \vee \neg E \;\Leftrightarrow\; \neg\mathsf{F} \vee \neg E$
   - $\neg(\mathsf{T} \wedge E) \;\Leftrightarrow\; \neg E \;\Leftrightarrow\; \mathsf{F} \vee \neg E \;\Leftrightarrow\; \neg\mathsf{T} \vee \neg E$

27. $\neg(\neg P \wedge (Q \vee R)) \;\Leftrightarrow\; \neg\neg P \vee \neg(Q \vee R) \;\Leftrightarrow\; P \vee \neg(Q \vee R) \;\Leftrightarrow\; P \vee (\neg Q \wedge \neg R)$

28. $\neg\neg(\neg P \vee \neg Q) \Leftrightarrow \neg(\neg\neg P \wedge \neg\neg Q)$

29. φ:n tilalla oli $\neg P$ ja ψ:n tilalla oli $\neg Q$.

30. Ensimmäinen askel soveltaa lakia $\neg\neg\varphi \Leftrightarrow \varphi$ takaperin koko alkuperäiseen kaavaan. Kolmas askel soveltaa sitä (etuperin) kaavaan Q, joka on isomman kaavan sisällä.

31. Osoitamme tulokset ensin P:lle, Q:lle ja R:lle:

$$\begin{array}{lll}
 & (P \vee Q) \wedge R & \\
\Leftrightarrow & R \wedge (P \vee Q) & [2] \\
\Leftrightarrow & (R \wedge P) \vee (R \wedge Q) & [5] \\
\Leftrightarrow & (R \wedge P) \vee (Q \wedge R) & [2] \\
\Leftrightarrow & (P \wedge R) \vee (Q \wedge R) & [2]
\end{array}
\qquad
\begin{array}{lll}
 & (P \wedge Q) \vee R & \\
\Leftrightarrow & R \vee (P \wedge Q) & [95] \\
\Leftrightarrow & (R \vee P) \wedge (R \vee Q) & [5] \\
\Leftrightarrow & (R \vee P) \wedge (Q \vee R) & [95] \\
\Leftrightarrow & (P \vee R) \wedge (Q \vee R) & [95]
\end{array}$$

Koska P:stä, Q:sta ja R:stä ei oletettu mitään, niiden tilalla saa olla mielivaltaiset kaavat φ, ψ ja χ, joten $(\varphi \vee \psi) \wedge \chi \Leftrightarrow (\varphi \wedge \chi) \vee (\psi \wedge \chi)$ ja $(\varphi \wedge \psi) \vee \chi \Leftrightarrow (\varphi \vee \chi) \wedge (\psi \vee \chi)$.

32. Osittelulakia sekä lakeja $\varphi \wedge \neg\varphi \Leftrightarrow \mathsf{F}$ ja $\mathsf{F} \vee \psi \Leftrightarrow \psi$.

33. Osoitamme ensin $P \vee (\neg P \wedge Q) \Leftrightarrow P \vee Q$:

$$\begin{array}{lll}
 & P \vee (\neg P \wedge Q) & \text{osittelulaki} \\
\Leftrightarrow & (P \vee \neg P) \wedge (P \vee Q) & \varphi \vee \neg\varphi \Leftrightarrow \mathsf{T} \\
\Leftrightarrow & \mathsf{T} \wedge (P \vee Q) & \mathsf{T} \wedge \varphi \Leftrightarrow \varphi \\
\Leftrightarrow & P \vee Q &
\end{array}$$

Koska P:stä ja Q:sta ei oletettu mitään, niiden tilalla saa olla mielivaltaiset kaavat φ ja ψ, joten $\varphi \vee (\neg\varphi \wedge \psi) \Leftrightarrow \varphi \vee \psi$.

34. P tosi ja R epätosi on vastaesimerkki.

36. Laista $\mathsf{T} \wedge \psi \Leftrightarrow \psi$ saadaan $\neg(\mathsf{T} \wedge \psi) \Leftrightarrow \neg\psi$ lisäämällä molemmille puolille $\neg$. Valitsemalla ψ:ksi $\neg P$ saadaan $\neg(\mathsf{T} \wedge \neg P) \Leftrightarrow \neg\neg P$, josta apulause [10] tuottaa $\mathsf{F} \vee P \Leftrightarrow P$. Koska P:stä ei oletettu mitään, sen tilalla saa olla mielivaltainen kaava ψ, joten $\mathsf{F} \vee \psi \Leftrightarrow \psi$.

37. Laista $\varphi \wedge \psi \Leftrightarrow \psi \wedge \varphi$ saadaan $\neg(\varphi \wedge \psi) \Leftrightarrow \neg(\psi \wedge \varphi)$ lisäämällä molemmille puolille $\neg$. Valitsemalla φ:ksi ja ψ:ksi $\neg P$ ja $\neg Q$ saadaan $\neg(\neg P \wedge \neg Q) \Leftrightarrow \neg(\neg Q \wedge \neg P)$, josta apulause [10] tuottaa $P \vee Q \Leftrightarrow Q \vee P$. Koska P:stä ja Q:sta ei oletettu mitään, niiden tilalla saa olla mielivaltaiset kaavat φ ja ψ, joten $\varphi \vee \psi \Leftrightarrow \psi \vee \varphi$.

38. Laista $\varphi \wedge (\psi \vee \chi) \Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$ saadaan $\neg(\varphi \wedge (\psi \vee \chi)) \Leftrightarrow \neg((\varphi \wedge \psi) \vee (\varphi \wedge \chi))$ lisäämällä molemmille puolille $\neg$. Valitsemalla φ:ksi, ψ:ksi ja χ:ksi $\neg P$, $\neg Q$ ja $\neg R$ saadaan $\neg(\neg P \wedge (\neg Q \vee \neg R)) \Leftrightarrow \neg((\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R))$, josta apulause [10] tuottaa $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$. Koska P:stä, Q:sta ja R:stä ei oletettu mitään, niiden tilalla saa olla mielivaltaiset kaavat φ, ψ ja χ, joten $\varphi \vee (\psi \wedge \chi) \Leftrightarrow (\varphi \vee \psi) \wedge (\varphi \vee \chi)$.

39. Kaavan P tapauksessa P tulkitaan välillä totuusfunktion tulosta esittäväksi kaavaksi ja välillä totuusfunktion argumenttia esittäväksi propositiomuuttujaksi. Sen totuusarvo ei kuitenkaan riipu siitä, kumpaa tulkintaa käytetään. Koska totuusfunktio on kaksipaikkainen, tarvitaan myös Q. Kun Q muuttuu F:sta T:ksi, P (tulkittuna kaavaksi) ei muutu, koska Q ei esiinny kaavassa P. Kun P (tulkittuna argumentiksi) muuttuu F:sta T:ksi, niin P (tulkittuna kaavaksi) muuttuu F:sta T:ksi.

    Jos tämä on hankala hahmottaa, niin tee kuvan 13 kaltainen taulukko ja totea, että kun siinä mennään oikealle niin totuusarvo ei muutu, ja kun mennään alas, niin totuusarvo muuttuu F:sta T:ksi.

    Kaava Q voidaan käsitellä samalla tavalla vaihtaen keskenään P:n ja Q:n roolit sekä suunnat alas ja oikealle.

41. ”kasvava” $\rightsquigarrow$ ”vähenevä” ja ”$\neg\varphi(P_1,\ldots,\mathsf{F},\ldots,P_n) \vee \varphi(P_1,\ldots,\mathsf{T},\ldots,P_n)$” $\rightsquigarrow$ ”$\varphi(P_1,\ldots,\mathsf{F},\ldots,P_n) \vee \neg\varphi(P_1,\ldots,\mathsf{T},\ldots,P_n)$”

42.

$\neg P \wedge Q$	F	T
F	F	T
T	F	F

43. Niitä esittävät F, T, P, $\neg Q$, $P \wedge \neg Q$ ja $P \vee \neg Q$.

44. Sitä esittää $P \wedge Q \vee \neg P \wedge \neg Q$.

45. Kun P_i muuttuu F:sta T:ksi, niin $\neg P_i$ muuttuu T:sta F:ksi. Koska φ on kasvava paikan i suhteen, muuttuu $\varphi(P_1,\ldots,\neg P_i,\ldots,P_n)$ samaan suuntaan kuin $\neg P_i$, eli T:sta F:ksi.

46. Vastaus tulee tekstissä hieman myöhemmin. Siis jatka lukemista.

47. Allen on paikalla.

48. $\neg(P \vee R)$

49. Muunnetaan ensin apulauseen [18] jokainen $\psi \rightarrow \chi$ muotoon $\neg\psi \vee \chi$. Sen jälkeen ensimmäinen ja kolmas tulos seuraavat suoraan kasvavuuden ja paikan i suhteen kasvavuuden määritelmistä sivuilta 22 ja 24. Toinen ja neljäs tulos saadaan vastaavalla tavalla sivulta 23 ja vastauksesta 41 soveltamalla lisäksi $\vee$:n vaihdannaisuutta.

50. $C \rightarrow (A \rightarrow \neg B)$

52. Ensin johdettiin $\neg A \vee (A \wedge (B \wedge \neg C))$ käyttämällä liitäntälakia $\varphi \wedge \psi \wedge \chi \Leftrightarrow \varphi \wedge (\psi \wedge \chi)$ siten, että φ:n tilalla oli A, ψ:n tilalla B ja χ:n tilalla $\neg C$. Siitä johdettiin $\neg A \vee (\neg\neg A \wedge (B \wedge \neg C))$ käyttämällä lakia $\neg\neg\varphi \Leftrightarrow \varphi$ takaperin siten, että φ:n tilalla oli A. Lopuksi käytettiin lakia $\varphi \vee (\neg\varphi \wedge \psi) \Leftrightarrow \varphi \vee \psi$ siten, että φ:n tilalla oli $\neg A$ ja ψ:n tilalla $B \wedge \neg C$. Niin saatiin $\neg A \vee (B \wedge \neg C)$.

53.
- $\neg\mathsf{F} \vee (\mathsf{F} \wedge B \wedge \neg C) \Leftrightarrow \mathsf{T} \vee (\mathsf{F} \wedge B \wedge \neg C) \Leftrightarrow \mathsf{T} \Leftrightarrow \mathsf{T} \vee (B \wedge \neg C) \Leftrightarrow \neg\mathsf{F} \vee (B \wedge \neg C)$
- $\neg\mathsf{T} \vee (\mathsf{T} \wedge B \wedge \neg C) \Leftrightarrow \neg\mathsf{T} \vee (B \wedge \neg C)$

54. $X \vee Q$

55. $\mathsf{T} \wedge \psi \Leftrightarrow \psi$

56. Sääntöä $P \Leftrightarrow \mathsf{T}$ käytettiin takaperin kaavaan $X \wedge Q$.

57. Ensin käytettiin tilapäisesti voimassa olevaa sääntöä $P \Leftrightarrow \mathsf{F}$ etuperin kaavan sisällä. Sitten käytettiin lakia [1] eli $\mathsf{F} \wedge \psi \Leftrightarrow \mathsf{F}$ etuperin koko kaavan tasolla, ja seuraavaksi samaa lakia takaperin koko kaavan tasolla. Lopuksi käytettiin takaperin sääntöä $P \Leftrightarrow \mathsf{F}$ kaavan sisällä.

58. Askelissa $\mathsf{T} \wedge Q \Leftrightarrow P \wedge Q$ ja $\mathsf{F} \wedge Q \Leftrightarrow P \wedge Q$.

59. Ei ole. Esimerkiksi Jenni Haukio on Aaro Niinistön äiti, mutta Aaro Niinistö ei ole Jenni Haukion äiti.

60. Ei ole. Esimerkiksi Jenni Haukio on Aaro Niinistön esiäiti, mutta Aaro Niinistö ei ole Jenni Haukion esiäiti.

61. Ei ole. Esimerkiksi $2 \leq 3$ mutta $3 \not\leq 2$.

62. Ei ole. Esimerkiksi $2 < 3$ mutta $3 \not< 2$.

63. On. Kaikille luvuille x ja y pätee, että jos x on erisuuri kuin y, niin y on erisuuri kuin x. Tämä voi kuulostaa tyhjältä sanahelinältä. Mutta jos vaihdetaan sanan ”erisuuri” tilalle ”pienempi”, niin saadaan ”… jos x on pienempi kuin y, niin y on pienempi kuin x”, joka on selvästi väärin. Siksi alkuperäinen ilmaus ei ole tyhjää sanahelinää, vaan kertoo ominaisuuden, joka on käsitteellä ”erisuuri” mutta ei ole käsitteellä ”pienempi”.

64. *Todistus.* Oletamme, että $\varphi \Leftrightarrow \psi$ ja $\psi \Leftrightarrow \chi$.

    Tarkastelemme mielivaltaista mahdollista tilannetta, jossa φ on tosi. Koska $\varphi \Leftrightarrow \psi$, on [22]:n mukaan myös ψ tosi. Ja koska $\psi \Leftrightarrow \chi$ ja ψ on tosi, sanoo [22] että myös χ on tosi. Olemme osoittaneet, että missä tahansa mahdollisessa tilanteessa, jossa φ on tosi, myös χ on tosi.

Sitten tarkastelemme mielivaltaista mahdollista tilannetta, jossa χ on tosi. Koska $\psi \Leftrightarrow \chi$, on [22]:n mukaan myös ψ tosi. Ja koska $\varphi \Leftrightarrow \psi$ ja ψ on tosi, sanoo [22] että myös φ on tosi. Olemme osoittaneet, että missä tahansa mahdollisessa tilanteessa, jossa χ on tosi, myös φ on tosi.

Osoittamamme kaksi asiaa yhdessä tarkoittavat [22]:n mukaan, että $\varphi \Leftrightarrow \chi$. $\square$

65. Ei ole. Esimerkiksi Ritva Haukio on Jenni Haukion äiti ja Jenni Haukio on Aaro Niinistön äiti, mutta Ritva Haukio ei ole Aaro Niinistön äiti.

66. On. Kenen tahansa henkilön esiäidin esiäiti on henkilön itsensä esiäiti.

67. On. Kaikille luvuille x, y ja z pätee, että jos $x \leq y$ ja $y \leq z$, niin $x \leq z$.

68. On. Kaikille luvuille x, y ja z pätee, että jos $x < y$ ja $y < z$, niin $x < z$.

69. Ei ole. Esimerkiksi $1 \neq 2$ ja $2 \neq 1$, mutta silti ei $1 \neq 1$.

70. On itsestäänselvää, että jokaisessa mahdollisessa tilanteessa, jossa φ on tosi, myös φ on tosi. Vaikka se onkin itsestäänselvää, siitä seuraa että määritelmä [19] toteutuu, joten $\Rightarrow$ on refleksiivinen.

71. Ei ole. Esimerkiksi Aaro Niinistö ei ole oma äitinsä.

72. Ei ole. Esimerkiksi Aaro Niinistö ei ole oma esiäitinsä.

73. On. Alin viiva symbolissa $\leq$ kertoo, että jos vasen ja oikea puoli ovat yhtäsuuret, niin suhde pätee.

74. Ei ole. Esimerkiksi $1 < 1$ ei päde.

75. Ei ole. Esimerkiksi $1 \neq 1$ ei päde.

76. Pitää tarkastaa refleksiivisyys, symmetrisyys ja transitiivisuus. Kun kirjoittaa mitä niiden määritelmät vaativat, niin jokaisesta tulee väite, joka on samaan ikäsarjaan kuuluville selvästi tosi.

    - Refleksiivisyys: jokainen kuuluu itsensä kanssa samaan ikäsarjaan.
    - Symmetrisyys: jos henkilö x kuuluu samaan ikäsarjaan kuin y, niin y kuuluu samaan ikäsarjaan kuin x.
    - Transitiivisuus: jos x kuuluu samaan ikäsarjaan kuin y ja y kuuluu samaan ikäsarjaan kuin z, niin x kuuluu samaan ikäsarjaan kuin z.

77. $X \land P$

78. Ensin oletuksesta $P \Leftrightarrow \mathsf{T}$ johdettiin $\Leftrightarrow$:n symmetrisyyden perusteella $\mathsf{T} \Leftrightarrow P$. Sitten valittiin lain [28] $\varphi(X)$:ksi $X \land Q$ ja johdettiin $\varphi(\mathsf{T}) \Leftrightarrow \varphi(P)$ eli $\mathsf{T} \land Q \Leftrightarrow P \land Q$.

79. $P \land (\neg X \lor Q)$

80. $\varphi(X)$ on $\neg P \lor \neg X$, ψ on $\neg(\mathsf{F} \lor \neg Q)$ ja χ on $\mathsf{T} \land Q$.

81. $\varphi(X)$ on $x < 65 \land X$, ψ on $\neg(x < 15)$ ja χ on $x \geq 15$.

82. $\neg(\varphi \leftrightarrow \psi) \;\Leftrightarrow\; \neg((\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi))$
$\Leftrightarrow\; (\neg\varphi \vee \neg\psi) \wedge (\varphi \vee \psi)$
$\Leftrightarrow\; (\neg\varphi \wedge \varphi) \vee (\neg\varphi \wedge \psi) \vee (\neg\psi \wedge \varphi) \vee (\neg\psi \wedge \psi)$
$\Leftrightarrow\; \mathsf{F} \vee (\neg\varphi \wedge \psi) \vee (\neg\psi \wedge \varphi) \vee \mathsf{F}$
$\Leftrightarrow\; (\neg\varphi \wedge \psi) \vee (\neg\neg\varphi \wedge \neg\psi)$
$\Leftrightarrow\; \neg\varphi \leftrightarrow \psi$

83.
- $\neg(\mathsf{F} \leftrightarrow \psi) \;\Leftrightarrow\; \neg\neg\psi \;\Leftrightarrow\; \psi \;\Leftrightarrow\; \mathsf{T} \leftrightarrow \psi \;\Leftrightarrow\; \neg\mathsf{F} \leftrightarrow \psi$
- $\neg(\mathsf{T} \leftrightarrow \psi) \;\Leftrightarrow\; \neg\psi \;\Leftrightarrow\; \mathsf{F} \leftrightarrow \psi \;\Leftrightarrow\; \neg\mathsf{T} \leftrightarrow \psi$

84. On vaihdannainen. Sen näkee sieventämällä $\varphi \leftrightarrow \psi \Leftrightarrow (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi) \Leftrightarrow (\psi \wedge \varphi) \vee (\neg\psi \wedge \neg\varphi) \Leftrightarrow \psi \leftrightarrow \varphi$, missä keskimmäinen ”$\Leftrightarrow$” käyttää kahdesti $\wedge$:n vaihdannaisuutta. Toinen keino on sijoittaa vuoron perään F ja T ja sieventää: $\mathsf{F} \leftrightarrow \psi \Leftrightarrow \neg\psi \Leftrightarrow \psi \leftrightarrow \mathsf{F}$ ja $\mathsf{T} \leftrightarrow \psi \Leftrightarrow \psi \Leftrightarrow \psi \leftrightarrow \mathsf{T}$, joten $\varphi \leftrightarrow \psi \Leftrightarrow \psi \leftrightarrow \varphi$.

85. On liitännäinen. Poistamalla kumpikin $\leftrightarrow$ tulee pitkä kaava, mutta F ja T sijoittamalla tulos saadaan näppärästi lain $\neg(\varphi \leftrightarrow \psi) \Leftrightarrow \neg\varphi \leftrightarrow \psi$ avulla:
- $(\mathsf{F} \leftrightarrow \psi) \leftrightarrow \chi \;\Leftrightarrow\; \neg\psi \leftrightarrow \chi \;\Leftrightarrow\; \neg(\psi \leftrightarrow \chi) \;\Leftrightarrow\; \mathsf{F} \leftrightarrow (\psi \leftrightarrow \chi)$
- $(\mathsf{T} \leftrightarrow \psi) \leftrightarrow \chi \;\Leftrightarrow\; \psi \leftrightarrow \chi \;\Leftrightarrow\; \mathsf{T} \leftrightarrow (\psi \leftrightarrow \chi)$

86. Koska edellä sanottiin, että $\leftrightarrow$ on vasemmalle liitännäinen.

87. Harvoin tärkeä, koska $\leftrightarrow$ on liitännäinen.

88. Jos φ tuottaa T, niin myös $\varphi \leftrightarrow \ldots \leftrightarrow \varphi$ tuottaa T. Jos φ tuottaa F, niin $\varphi \leftrightarrow \ldots \leftrightarrow \varphi$ tuottaa T tai F sen mukaan, esiintyykö φ kaavassa parillisen vai parittoman määrän kertoja.

Niissä tilanteissa, joissa $\varphi \Leftrightarrow \mathsf{T}$, pätee

$$\begin{array}{lclclcl}
\varphi \leftrightarrow \varphi & \Leftrightarrow & \varphi \leftrightarrow \varphi & \Leftrightarrow & \mathsf{T} \leftrightarrow \mathsf{T} & \Leftrightarrow & \mathsf{T} \\
\varphi \leftrightarrow \varphi \leftrightarrow \varphi & \Leftrightarrow & (\varphi \leftrightarrow \varphi) \leftrightarrow \varphi & \Leftrightarrow & \mathsf{T} \leftrightarrow \mathsf{T} & \Leftrightarrow & \mathsf{T} \\
\varphi \leftrightarrow \varphi \leftrightarrow \varphi \leftrightarrow \varphi & \Leftrightarrow & (\varphi \leftrightarrow \varphi \leftrightarrow \varphi) \leftrightarrow \varphi & \Leftrightarrow & \mathsf{T} \leftrightarrow \mathsf{T} & \Leftrightarrow & \mathsf{T} \\
\varphi \leftrightarrow \varphi \leftrightarrow \varphi \leftrightarrow \varphi \leftrightarrow \varphi & \Leftrightarrow & (\varphi \leftrightarrow \varphi \leftrightarrow \varphi \leftrightarrow \varphi) \leftrightarrow \varphi & \Leftrightarrow & \mathsf{T} \leftrightarrow \mathsf{T} & \Leftrightarrow & \mathsf{T}
\end{array}$$

ja niin edelleen. Niissä tilanteissa, joissa $\varphi \Leftrightarrow \mathsf{F}$, pätee

$$\begin{array}{lclclcl}
\varphi \leftrightarrow \varphi & \Leftrightarrow & \varphi \leftrightarrow \varphi & \Leftrightarrow & \mathsf{F} \leftrightarrow \mathsf{F} & \Leftrightarrow & \mathsf{T} \\
\varphi \leftrightarrow \varphi \leftrightarrow \varphi & \Leftrightarrow & (\varphi \leftrightarrow \varphi) \leftrightarrow \varphi & \Leftrightarrow & \mathsf{T} \leftrightarrow \mathsf{F} & \Leftrightarrow & \mathsf{F} \\
\varphi \leftrightarrow \varphi \leftrightarrow \varphi \leftrightarrow \varphi & \Leftrightarrow & (\varphi \leftrightarrow \varphi \leftrightarrow \varphi) \leftrightarrow \varphi & \Leftrightarrow & \mathsf{F} \leftrightarrow \mathsf{F} & \Leftrightarrow & \mathsf{T} \\
\varphi \leftrightarrow \varphi \leftrightarrow \varphi \leftrightarrow \varphi \leftrightarrow \varphi & \Leftrightarrow & (\varphi \leftrightarrow \varphi \leftrightarrow \varphi \leftrightarrow \varphi) \leftrightarrow \varphi & \Leftrightarrow & \mathsf{T} \leftrightarrow \mathsf{F} & \Leftrightarrow & \mathsf{F}
\end{array}$$

ja niin edelleen.

89. Olkoon ψ_n se kaava muotoa $\varphi \leftrightarrow \ldots \leftrightarrow \varphi$, jossa φ esiintyy n kertaa ($n > 0$). Koska $\leftrightarrow$ on vasemmalle liitännäinen, on ψ_n sama kuin $\psi_{n-1} \leftrightarrow \varphi$, kun $n > 1$. (Esimerkiksi $\psi_3 \Leftrightarrow (\varphi \leftrightarrow \varphi) \leftrightarrow \varphi \Leftrightarrow \psi_2 \leftrightarrow \varphi$.)

Tarkastelemme aluksi tilanteita, joissa φ tuottaa T. Osoitamme, että mikään n ei voi olla pienin sellainen positiivinen kokonaisluku, että ψ_n ei tuota T. Ykkönen ei ole sellainen, koska ψ_1 on sama kuin φ ja φ tuottaa T. Jäljellä on tapaus $n > 1$. Jos ψ_{n-1} tuottaa T, niin $\psi_n \Leftrightarrow \psi_{n-1} \leftrightarrow \varphi \Leftrightarrow \mathsf{T} \leftrightarrow \mathsf{T} \Leftrightarrow \mathsf{T}$, joten myös ψ_n tuottaa T. Jos ψ_{n-1} ei tuota T, niin n ei ole pienin, jolla ψ_n ei tuota T. Ei siis ole olemassa pienintä positiivista kokonaislukua n jolla ψ_n ei tuota T. Siksi jokainen ψ_n tuottaa T.

Jäljellä ovat tilanteet, joissa φ tuottaa F. Meidän on todistettava, että jos n on pariton, niin ψ_n tuottaa F, ja jos n on parillinen, niin ψ_n tuottaa T. Todistamme sen osoittamalla, että ei ole olemassa pienintä n, jolla ψ_n poikkeaisi tästä säännöstä. Ykkönen ei ole sellainen, koska 1 on pariton ja ψ_1 eli φ tuottaa F. Jos $n > 1$ ja ψ_{n-1} noudattaa sääntöä, niin $\psi_n \Leftrightarrow \psi_{n-1} \leftrightarrow \varphi \Leftrightarrow \psi_{n-1} \leftrightarrow \mathsf{F}$, joten ψ_n tuottaa eri totuusarvon kuin ψ_{n-1}. Mutta juuri niin pitää ollakin, koska myös n:n parillisuus tai parittomuus on eri kuin $(n-1)$:n. Jos $n > 1$ ja ψ_{n-1} rikkoo sääntöä, niin n ei olekaan pienin, jolla sääntö ei päde.

90. Refleksiivisyys: $\varphi \leftrightarrow \varphi$ (vastaukseksi kelpaa myös $\varphi \leftrightarrow \varphi \Leftrightarrow \mathsf{T}$)

    Symmetrisyys: $\varphi \leftrightarrow \psi \Rightarrow \psi \leftrightarrow \varphi$

    Transitiivisuus: $(\varphi \leftrightarrow \psi) \wedge (\psi \leftrightarrow \chi) \Rightarrow \varphi \leftrightarrow \chi$

91. Mahdollinen tilanne, jossa φ ei ole tosi mutta ψ on tosi.

92. $n = 3$ ja $\varphi_1 \rightleftharpoons_2 \varphi_2$ on $P \wedge P \Rightarrow (P \wedge P) \vee (P \wedge Q)$.

93. On. Päättelyaskel toteuttaa päättelyketjun määritelmän: se on vaadittua muotoa, ja siinä on vähintään kaksi kaavaa.

94. On. Sijoittamalla P:hen vuoron perään F ja T on helppo tarkastaa, että esimerkin jokaisella kaavalla on sama totuusarvo kuin P:llä. Niinpä kummallekin $\Leftrightarrow$:lle pätee että jos sen jompikumpi puoli on tosi, niin myös vastakkainen puoli on tosi; ja $\Rightarrow$:lle pätee että jos sen vasen puoli on tosi, niin myös oikea puoli on tosi.

95. $P \Rightarrow P \wedge (P \vee Q)$

96. Esimerkiksi valitsemalla φ:ksi P saataisiin $\neg P$ muka muunnettua muotoon P. Se ei ole yhtäpitävä $(\neg P)$:n kanssa, koska esimerkiksi $\neg\mathsf{T}$ ei ole T vaan F.

97. Siksi, että lopulliset $\chi_1, \ldots, \chi_n$ eivät ole samat kuin alkuperäiset, vaan kukin lopullinen on saatu alkuperäisestä lisäämällä eteen tai poistamalla edestä $\neg$. Koska alkuperäiset χ_i saavat edustaa mitä tahansa kaavoja, ne saavat edustaa myös niitä kaavoja, jotka saadaan lisäämällä kunkin lopputulokseen halutun kaavan eteen $\neg$. Lähellä todistuksen alkua tehtiin niin. Lisätyt $\neg$:t katosivat myöhemmin, kun todistuksessa sovellettiin apulausetta [10].

98. $(\varphi \Leftrightarrow \psi) \Rightarrow (\psi \Leftrightarrow \varphi)$

99. $(\varphi \Leftrightarrow \psi) \wedge (\psi \Leftrightarrow \chi) \Rightarrow (\varphi \Leftrightarrow \chi)$

100. χ_1:n, χ_2:n ja χ_3:n tilalla olivat $\varphi \Leftrightarrow \psi$, $\varphi \Rightarrow \psi$ ja $\psi \Rightarrow \varphi$. Oletukset saatiin (12):stä ja (13):stä.

101. χ_1:n tilalla oli $\varphi \Leftrightarrow \psi$ ja χ_2:n tilalla oli $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$. Oletukset saatiin (14):sta ja (15):sta.

102. Tämän väriset olivat puheen kohteena ja tämän värisiä käytettiin puhumiseen:

$$(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi) \Rightarrow (\varphi \Leftrightarrow \psi)$$

103. Koska $\wedge$ on vasemmalle liitännäinen, $A \wedge L \wedge J$ tarkoittaa $(A \wedge L) \wedge J$. Soveltamalla ensin vasemmanpuoleista ja sitten oikeanpuoleista lakia saadaan $(A \wedge L) \wedge J \Rightarrow A \wedge L \Rightarrow L$.

104. Vastaesimerkki olisi mahdollinen tilanne, jossa $\varphi \wedge \psi$ on tosi, mutta φ ei ole tosi. Sellaista ei voi olla, koska $\wedge$:n merkityksen mukaan jos $\varphi \wedge \psi$ on tosi, niin sekä φ että ψ ovat tosia.

105. Olkoon φ mielivaltainen määritelty kaava. Toinen [7]:n laeista takaperin on $\mathsf{F} \Leftrightarrow \varphi \wedge \neg\varphi$, josta [32] ja [33] tuottavat $\mathsf{F} \Rightarrow \varphi \wedge \neg\varphi \Rightarrow \varphi$. Koska $\Rightarrow$ on transitiivinen, $\mathsf{F} \Rightarrow \varphi$.

106. ”Pihtiputaan mummo on kesällä Rovaniemellä”, ”hän ostaa poroleikkelettä” ja ”hän läiskii hyttysiä”.

107. Niistä yhdessä saadaan [32]:lla $P \Leftrightarrow P \wedge (P \vee Q)$.

108. [31]:n, [35]:n ja [30]:n nojalla

- $(\varphi \leftrightarrow \mathsf{F}) \wedge (\mathsf{F} \leftrightarrow \chi) \;\Leftrightarrow\; \neg\varphi \wedge \neg\chi \;\Rightarrow\; (\varphi \wedge \chi) \vee (\neg\varphi \wedge \neg\chi) \;\Leftrightarrow\; \varphi \leftrightarrow \chi$
- $(\varphi \leftrightarrow \mathsf{T}) \wedge (\mathsf{T} \leftrightarrow \chi) \;\Leftrightarrow\; \varphi \wedge \chi \;\Rightarrow\; (\varphi \wedge \chi) \vee (\neg\varphi \wedge \neg\chi) \;\Leftrightarrow\; \varphi \leftrightarrow \chi$

109. $\varphi_1 \vee \varphi_2$, φ_3 ja ψ.

110. n on positiivinen kokonaisluku.

111. *Todistus.* Käytämme induktiota.

Pohjatapaus. Kun $n = 1$, sievenee väite muotoon ”jos $\varphi \Rightarrow \psi_1$, niin $\varphi \Rightarrow \psi_1$”. Se on itsestäänselvästi tosi.

Induktioaskel. Kun $n > 1$, niin lauseen oletusten $\varphi \Rightarrow \psi_1$ ja … ja $\varphi \Rightarrow \psi_{n-1}$ sekä induktio-oletuksen mukaan $\varphi \Rightarrow \psi_1 \wedge \cdots \wedge \psi_{n-1}$. Lauseen oletuksen mukaan $\varphi \Rightarrow \psi_n$. Näistä [34] tuottaa $\varphi \Rightarrow (\psi_1 \wedge \cdots \wedge \psi_{n-1}) \wedge \psi_n$. Koska $\wedge$ on vasemmalle liitännäinen, se tarkoittaa samaa kuin $\varphi \Rightarrow \psi_1 \wedge \cdots \wedge \psi_n$. □

112. *Todistus.* Käytämme induktiota.

Pohjatapaus. Kun $n = 1$, sievenee väite muotoon ”jos $\varphi_0 \Rightarrow \varphi_1$, niin $\varphi_0 \Rightarrow \varphi_1$”. Se on itsestäänselvästi tosi.

Induktioaskel. Kun $n > 1$, niin $\varphi_0 \Rightarrow \varphi_1 \Rightarrow \ldots \Rightarrow \varphi_n$ tarkoittaa samaa kuin $\varphi_0 \Rightarrow \varphi_1 \Rightarrow \ldots \Rightarrow \varphi_{n-1}$ ja $\varphi_{n-1} \Rightarrow \varphi_n$. Induktio-oletus tuottaa edellisestä $\varphi_0 \Rightarrow \varphi_{n-1}$. Siitä ja jälkimmäisestä [26] tuottaa $\varphi_0 \Rightarrow \varphi_n$. □

113. Väite on mielekäs, kun $0 \le i \le n$. Kun $i = n$, se sievenee muotoon $\varphi(\psi_1, \ldots, \psi_n) \Leftrightarrow \varphi(\chi_1, \ldots, \chi_n)$. Kun $n = 3$, eri muodot ovat

i	väite
0	$\varphi(\psi_1, \psi_2, \psi_3) \;\Leftrightarrow\; \varphi(\psi_1, \psi_2, \psi_3)$
1	$\varphi(\psi_1, \psi_2, \psi_3) \;\Leftrightarrow\; \varphi(\chi_1, \psi_2, \psi_3)$
2	$\varphi(\psi_1, \psi_2, \psi_3) \;\Leftrightarrow\; \varphi(\chi_1, \chi_2, \psi_3)$
3	$\varphi(\psi_1, \psi_2, \psi_3) \;\Leftrightarrow\; \varphi(\chi_1, \chi_2, \chi_3)$

114. *Todistus.* Todistamme induktiolla i:n arvoilla 0, …, n, että $\varphi(\psi_1,\dots,\psi_n) \Leftrightarrow \varphi(\chi_1,\dots,\chi_i,\psi_{i+1},\dots,\psi_n)$. Lauseen väite seuraa tapauksesta $i = n$.

   Pohjatapaus. Kun $i = 0$, sievenee väite muotoon $\varphi(\psi_1,\dots,\psi_n) \Leftrightarrow \varphi(\psi_1,\dots,\psi_n)$. Se on tosi $\Leftrightarrow$:n refleksiivisyyden vuoksi.

   Induktioaskel. Olkoon $1 \le i \le n$. Induktio-oletus on

$$\varphi(\psi_1,\dots,\psi_n) \;\Leftrightarrow\; \varphi(\chi_1,\dots,\chi_{i-1},\psi_i,\dots,\psi_n)$$

   Laki [28] tuottaa $\varphi(\chi_1,\dots,\chi_{i-1},\psi_i,\dots,\psi_n) \Leftrightarrow \varphi(\chi_1,\dots,\chi_i,\psi_{i+1},\dots,\psi_n)$. Transitiivisuus tuottaa näistä $\varphi(\psi_1,\dots,\psi_n) \Leftrightarrow \varphi(\chi_1,\dots,\chi_i,\psi_{i+1},\dots,\psi_n)$. □

115. Ei ole. Koska $\mathsf{T} \vee \mathsf{T} \Leftrightarrow \mathsf{T}$, sallii [36] saman mahdollisen tilanteen sisältyvän useampaan kuin yhteen tapaukseen. Muuallakaan todistusmenetelmän kuvauksessa ei vaadita, että tapaukset ovat toisensa poissulkevia. Kun mahdollisesta tilanteesta on kerran todistettu, että väite pätee siinä, ei saman todistaminen uudelleen kumoa sitä.

116. Siinä tilanteessa ψ ei tuota F.

117. Olkoon ψ mielivaltainen määritelty kaava. Koska myös vastauksen 105 φ on mielivaltainen määritelty kaava, voidaan sen tilalle laittaa $\neg\psi$. Niin saadaan $\neg\mathsf{T} \Leftrightarrow \mathsf{F} \Rightarrow \neg\psi$. Siitä transitiivisuus ja [38] tuottavat $\psi \Rightarrow \mathsf{T}$.

118. *Todistus.* Jos $\varphi \vee \psi \Rightarrow \chi$ ei päde, niin on olemassa mahdollinen tilanne, jossa $\varphi \vee \psi \Leftrightarrow \mathsf{T}$ ja $\chi \Leftrightarrow \mathsf{F}$. Jos siinä tilanteessa $\varphi \Leftrightarrow \mathsf{T}$, niin $\varphi \Rightarrow \chi$ ei päde. Muussa tapauksessa, koska $\varphi \vee \psi \Leftrightarrow \mathsf{T}$, siinä tilanteessa $\psi \Leftrightarrow \mathsf{T}$, joten $\psi \Rightarrow \chi$ ei päde. Olemme osoittaneet, että jos [36]:n oikea puoli ei päde, niin myöskään vasen puoli ei päde. Niinpä käänteisen todistuksen periaatteen mukaan jos vasen puoli pätee, niin myös oikea puoli pätee. Se tarkoittaa, että [36] pätee. □

120. *Todistus [40]:lle.* Tarkastelemme mielivaltaista mahdollista tilannetta, jossa $\varphi(\chi)$ tuottaa T.

   - Jos siinä tilanteessa ψ tuottaa saman totuusarvon kuin χ, niin myös $\varphi(\psi)$ tuottaa saman totuusarvon kuin $\varphi(\chi)$. Niinpä $\varphi(\psi)$ tuottaa T.
   - Jos ψ tuottaa F ja χ tuottaa T, niin vähenevyyden paikan i suhteen vuoksi $\varphi(\chi) \rightarrow \varphi(\psi)$. Siitä seuraa, että $\varphi(\psi)$ tuottaa T, koska alussa tehdyn oletuksen vuoksi $\varphi(\chi)$ tuottaa tilanteessamme T.
   - Muussa tapauksessa ψ tuottaa T ja χ tuottaa F. Se ei kuitenkaan ole mahdollista oletuksen $\psi \Rightarrow \chi$ vuoksi.

   Niinpä jokaisessa mahdollisessa tilanteessa, joka toteuttaa oletuksen $\psi \Rightarrow \chi$ ja jossa $\varphi(\chi)$ tuottaa T, myös $\varphi(\psi)$ tuottaa T. Toisin sanoen, [40]:n oletusten vallitessa $\varphi(\chi) \Rightarrow \varphi(\psi)$. □

121. Se ei ole kasvava P:n suhteen, mutta muihin kysymyksiin vastaus on ”kyllä”. Sijoittamalla $P \Leftrightarrow \mathsf{T}$ sievenee kaava nopeasti F:ksi. Sijoittamalla $P \Leftrightarrow \mathsf{F}$ sievenee kaava muotoon $\neg((Q \wedge \neg R) \wedge \neg Q) \Leftrightarrow \neg\mathsf{F} \Leftrightarrow \mathsf{T}$. Niinpä kaava on yhtäpitävä kaavan $\neg P$ kanssa. Se ei ole kasvava P:n suhteen koska $\neg\mathsf{F} \Leftrightarrow \mathsf{T}$ mutta $\neg\mathsf{T} \Leftrightarrow \mathsf{F}$. Se on sekä kasvava että vähenevä Q:n ja R:n suhteen, koska sen tulos ei riipu niistä ollenkaan.

122. [97], [5], [7] ja joko [2] tai [6], [95] ja [96] sekä [2] ja [95].

123.

rivi	välisymboli	vaihtoehdolla	riveiltä	tuottaa
1	*Peruskaava*	*Propositiomuuttuja*		Q
2	*NegKaava*	*Peruskaava*	1	Q
3	*KonjKaava*	*NegKaava*	2	Q
4	*Peruskaava*	*Propositiomuuttuja*		R
5	*NegKaava*	*Peruskaava*	4	R
6	*KonjKaava*	*KonjKaava* $\wedge$ *NegKaava*	3, 5	$Q \wedge R$
7	*Peruskaava*	*Propositiomuuttuja*		P
8	*NegKaava*	*Peruskaava*	7	P
9	*KonjKaava*	*NegKaava*	8	P
10	*DisjKaava*	*KonjKaava*	9	P
11	*DisjKaava*	*DisjKaava* $\vee$ *KonjKaava*	10, 6	$P \vee Q \wedge R$
12	*ImplKaava*	*DisjKaava*	11	$P \vee Q \wedge R$
13	*EkvKaava*	*ImplKaava*	12	$P \vee Q \wedge R$
14	*Kaava*	*EkvKaava*	13	$P \vee Q \wedge R$

124. On. Sen voi tuottaa tuottamalla *Peruskaava*sta F, tuottamalla sama *NegKaava*sta vaihtoehdolla *Peruskaava*, sitten *KonjKaava*sta ja niin edelleen kunnes se on tuotettu *Kaava*sta, sitten tuottamalla *NegKaava*sta (F) vaihtoehdolla (*Kaava*), *NegKaava*sta $\neg(\mathsf{F})$ vaihtoehdolla $\neg$*NegKaava*, *NegKaava*sta $\neg\neg(\mathsf{F})$ vaihtoehdolla $\neg$*NegKaava*, ja ylentämällä se *KonjKaava*ksi ja niin edelleen kunnes se on tuotettu *Kaava*sta.

125. Ei ole. Ainoa keino saada) mukaan on vaihtoehto (*Kaava*), mutta sen mukana tulee myös (, joten sen avulla ei voi tuottaa Q).

126. Valitsemalla *Peruskaava*ksi *Propositiomuuttuja* ja muiksi välisymboleiksi aina ensimmäinen vaihtoehto nähdään, että sekä *EkvKaava* että *ImplKaava* pystyy tuottamaan minkä tahansa propositiomuuttujan. Ainoa keino saada kaavaan $\leftrightarrow$ on vaihtoehto *EkvKaava* $\leftrightarrow$ *ImplKaava*. *ImplKaava* ei voi käyttää sitä muuten kuin vaihtoehdon (*Kaava*) kautta. Se tuottaa kaavaan myös sulkeet. Kaavassa $P \leftrightarrow Q \leftrightarrow R$ ei ole sulkeita, joten se voidaan tuottaa vain vaihtoehdolla *EkvKaava* $\leftrightarrow$ *ImplKaava*, missä *ImplKaava* tuottaa R ja *EkvKaava* tuottaa $P \leftrightarrow Q$. Siksi $P \leftrightarrow Q$ lasketaan ensin.

Vastaavasti $P \rightarrow Q \rightarrow R$ voidaan tuottaa vain vaihtoehdolla *DisjKaava* $\rightarrow$ *ImplKaava*, missä *DisjKaava* tuottaa P ja *ImplKaava* tuottaa $Q \rightarrow R$. Nimittäin *DisjKaava*n tuotokseen voidaan saada $\rightarrow$ vain vaihtoehdon (*Kaava*) kautta, jolloin kaavassa olisi sulkeet. Siksi $Q \rightarrow R$ lasketaan ensin.

127.

	$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
vaihdannainen		$\surd$	$\surd$	-	$\surd$
liitännäinen		$\surd$	$\surd$	-	$\surd$
vasemmalle liitännäinen		$\surd$	$\surd$	-	$\surd$
oikealle liitännäinen		-	-	$\surd$	-
kasvava paikan 1 suhteen	-	$\surd$	$\surd$	-	-
kasvava paikan 2 suhteen		$\surd$	$\surd$	$\surd$	-
vähenevä paikan 1 suhteen	$\surd$	-	-	$\surd$	-
vähenevä paikan 2 suhteen		-	-	-	-

128. $\neg(P \wedge R) \wedge \neg(P \wedge S) \wedge \neg(R \wedge S) \wedge (K \rightarrow S)$

129. Jokaisessa tilanteessa, jossa φ on tosi, myös φ on tosi.

130. Kumpikin kahdesta ensimmäisestä vaihtoehdosta tuottaa $\Rightarrow$:n *OikKetju*un. Loppuja vaihtoehtoja voidaan käyttää vain pidentämään jo tuotettuja *OikKetju*ja. Ei siis ole mitään keinoa tuottaa ensimmäisen kerran *OikKetju*a, jossa ei ole $\Rightarrow$:ta.

131. Jos $\Rightarrow$ on ketjun ensimmäinen päättelyoperaattori, niin ketjun alku saadaan vaihtoehdolla *Kaava* $\Rightarrow$ *Kaava*. Muussa tapauksessa ketjun alku saadaan vaihtoehdolla *MolKetju* $\Rightarrow$ *Kaava*, missä *MolKetju* tuottaa kaiken mikä on ensimmäisen $\Rightarrow$:n edellä.

132. Jos jossain mahdollisessa tilanteessa $\varphi \Rightarrow \psi$ ei päde, niin [19]:n mukaan φ on siinä tosi mutta ψ ei ole. Koska φ on siinä tosi, se on mahdollinen tilanne myös tilapäisen oletuksen φ vallitessa. Niinpä se tilanne on vastaesimerkki jos-osalle.

133. Jos jossain mahdollisessa tilanteessa $\varphi \wedge \psi \Rightarrow \chi$ ei päde, niin [19]:n mukaan φ ja ψ ovat siinä todet mutta χ ei ole. Koska φ on siinä tosi, se on mahdollinen tilanne myös oletuksen φ vallitessa. Niinpä se kuuluu niihin tilanteisiin, joissa jos-osa olettaa $\psi \Rightarrow \chi$. Mutta se on sille vastaesimerkki, koska ψ on siinä tosi mutta χ ei ole. Niinpä jos-osa ei päde.

134. Jos jossain mahdollisessa tilanteessa $\varphi \wedge \psi \Leftrightarrow \varphi \wedge \chi$ ei päde, niin [22]:n mukaan toinen kaavoista $\varphi \wedge \psi$ ja $\varphi \wedge \chi$ on siinä tosi, mutta toinen ei ole. Tämä on mahdollista vain siten, että φ on siinä tosi (koska muutoin kumpikaan kaavoista ei ole siinä tosi), ja toinen mutta ei molemmat ψ:stä ja χ:stä on siinä tosi. Koska φ on siinä tosi, se on mahdollinen tilanne myös oletuksen φ vallitessa. Niinpä se kuuluu niihin tilanteisiin, joissa jos-osa olettaa $\psi \Leftrightarrow \chi$. Mutta se on sille vastaesimerkki, koska toinen ψ:stä ja χ:stä on siinä tosi mutta toinen ei ole. Niinpä jos-osa ei päde.

135. Jos φ:n vallitessa pätee $\psi \Leftrightarrow \chi$, niin [32]:n mukaan φ:n vallitessa pätee $\psi \Rightarrow \chi$. Niinpä [44]:n mukaan ilman oletusta φ pätee $\varphi \wedge \psi \Rightarrow \chi$. Toisaalta [33]:n mukaan $\varphi \wedge \psi \Rightarrow \varphi$. Niistä [34] tuottaa $\varphi \wedge \psi \Rightarrow \varphi \wedge \chi$. Samaan tapaan voidaan osoittaa $\varphi \wedge \psi \Leftarrow \varphi \wedge \chi$. Niistä [32] tuottaa $\varphi \wedge \psi \Leftrightarrow \varphi \wedge \chi$.

136. Jos $a = 0$, niin kirjoita_lukuna b ja lopeta. Muussa tapauksessa jatka. Jos $a = -1$, niin kirjoita $-$; ja jos a ei ole 1 eikä -1, niin kirjoita_lukuna a. Kirjoita x. Jos $b > 0$, niin kirjoita $+$. Jos $b \neq 0$, niin kirjoita_lukuna b. Lopeta.

137. Valitsemalla $c = 0$ saadaan $a - b = 0 \Leftrightarrow a = 0 + b = b$, missä viimeinen $=$ perustuu siihen, että jokaiselle luvulle b pätee $0 + b = b$. Siitä voidaan poimia $a - b = 0 \Leftrightarrow a = b$.

138. Laki on $a + (-b) = a - b$. Sijoittamalla b:n tilalle $-b$ saadaan $a + (--b) = a - (-b)$.

139. Rivistä 7 saadaan [49]:llä $a = c + (-b)$ sekä [33]:lla ja [47]:lla $c + (-b) = c - b$. Niistä [34] tuottaa rivin 6 kaavan.

140. $a + (--b)$ ja $a - (-b)$

141. Koska $c + (-b) = c - b$ pätee aina, rivien 4 ja 5 yhtäpitävyys saadaan valitsemalla $\varphi(x)$:ksi $a = x$, f:ksi $c + (-b)$ ja g:ksi $c - b$.

142. $f := 8-3$, $g := 5$ ja $\varphi(a) :\Leftrightarrow (x+3)-3 = a$.

143. $f := x$, $g := 2a-3$ ja $\varphi(y) :\Leftrightarrow 3a-2y = 2$. (Myös $\varphi(x) :\Leftrightarrow 3a-2x = 2$ kelpaa.)

144. Valitaan f:ksi 0, g:ksi 1 ja φ:ksi $\top$. Tämä vastaus ei ole huijausta, mutta siltä varalta että se tuntuu sinusta huijaukselta, saat toisenkin vastauksen: valitaan f:ksi 0, g:ksi 1 ja $\varphi(x)$:ksi $0x = 0$.

145. Ennen poistamista laki on muotoa ”tulos1 ja tulos2”, missä tulos1 on ”$\psi \Leftrightarrow \chi$” ja tulos2 on ”$\psi$ ja χ ovat yhtäaikaa määritellyt”. Siitä, että sekä tulos1 että tulos2 pätee, seuraa että tulos1 pätee.

146. Valitsemalla f:ksi $3x$, g:ksi 12 ja $h(a)$:ksi $\frac{a}{3}$ saadaan $3x = 12 \Rightarrow \frac{3x}{3} = \frac{12}{3} \Leftrightarrow x = 4$.

147. Valitsemalla f:ksi $--b$, g:ksi b ja $h(x)$:ksi $a+x$ saadaan $--b = b \Rightarrow a+(--b) = a+b$.

148. Valitsemalla f:ksi $3\sqrt{|x|-1}$, g:ksi $x+1$ ja $h(a)$:ksi a^2 saadaan

$$3\sqrt{|x|-1} = x+1 \;\Rightarrow\; \left(3\sqrt{|x|-1}\right)^2 = (x+1)^2 \;\Leftrightarrow\; 9(|x|-1) = x^2+2x+1.$$

Valitsemalla f:ksi $9(|x|-1)$, g:ksi x^2+2x+1 ja $h(a)$:ksi $a+9$ saadaan

$$9(|x|-1) = x^2+2x+1 \;\Rightarrow\; 9(|x|-1)+9 = x^2+2x+1+9 \;\Leftrightarrow\; 9|x| = x^2+2x+10.$$

Niistä yhdessä saadaan $3\sqrt{|x|-1} = x+1 \;\Rightarrow\; 9|x| = x^2+2x+10$.

Toinen tapa: valitsemalla f:ksi $3\sqrt{|x|-1}$, g:ksi $x+1$ ja $h(a)$:ksi a^2+9 saadaan

$$\begin{aligned} 3\sqrt{|x|-1} = x+1 \;&\Rightarrow\; \left(3\sqrt{|x|-1}\right)^2+9 = (x+1)^2+9 \\ \Leftrightarrow\; 9(|x|-1)+9 = x^2+2x+1+9 \;&\Leftrightarrow\; 9|x| = x^2+2x+10. \end{aligned}$$

149. Osoittamatta on enää $x = 4 \Rightarrow 3x = 12$. Valitsemalla [52]:n f:ksi x, g:ksi 4 ja $h(a)$:ksi $3a$ saadaan $x = 4 \Rightarrow 3x = 3 \cdot 4 \Leftrightarrow 3x = 12$.

150.

	laki	f tai rivi	g tai rivi	$h(x)$ tai $\varphi(x)$
1	[52]	$a+b$	c	$x+(-b)$
2	[51]	$(a+b)+(-b)$	a	$x = c+(-b)$
3	[51]	$c+(-b)$	$c-b$	$a = x$
4	[32] [26]	1	3	
5	[52]	a	$c-b$	$x+b$
6	[51]	$(c-b)+b$	c	$a+b = x$
7	[32] [26]	5	6	
8	[32]	4	7	

151. *Todistus [49]:lle.* Olettamalla $g = h$ ja valitsemalla $\varphi(x)$:ksi $f = x$ [51] tuottaa $f = g \Leftrightarrow f = h$. Niinpä olettamalla sekä $f = g$ että $g = h$ saadaan $f = h$. $\square$

152. *Todistus [52]:lle.* Riittää osoittaa, että jos-osan sallimissa tilanteissa pätee $h(f) = h(g)$. Niissä $h(f)$ on määritelty ja $f = g$. Koska $h(f)$ on määritelty, [53]:n mukaan $h(f) = h(f)$. Koska $f = g$, valitsemalla $\varphi(x)$:ksi $h(f) = h(x)$ [51] tuottaa $h(f) = h(f) \Leftrightarrow h(f) = h(g)$. Niinpä $h(f) = h(g)$. $\square$

153. Neliöimällä oletuksen $\frac{1}{0} = \sqrt{-1}$ molemmat puolet eli valitsemalla [52]:n $h(x)$:ksi x^2 saadaan $\left(\frac{1}{0}\right)^2 = \left(\sqrt{-1}\right)^2$. Lukujen laeilla vasen puoli sievenee $\left(\frac{1}{0}\right)^2 = \frac{1}{0} \cdot \frac{1}{0} = \frac{1 \cdot 1}{0 \cdot 0} = \frac{1}{0}$ ja oikea puoli sievenee $\left(\sqrt{-1}\right)^2 = -1$, joten $\frac{1}{0} = -1$. Neliöimällä uudelleen saadaan $\frac{1}{0} = 1$. Yhtäsuuruuden symmetrisyys ja transitiivisuus tuottavat $-1 = 1$.

154. a ja f olivat x^2+4x, g oli x^2+4x+0 ja $\varphi(x)$ oli $x-12=0$. Tämä johtuu siitä, että $a+b+c$ tarkoittaa samaa kuin $(a+b)+c$. Niinpä $x^2+4x-12 = (x^2+4x)-12 = ((x^2+4x)+0)-12 = x^2+4x+0-12$.

155. $x^2+4x-12=0 \Leftrightarrow x^2+4(x+0)-12=0$

156. Nyt pitää vaihtaa $\varphi(x)$:n tilalle vaikka $\varphi(a)$, koska muuten x on kahdessa eri roolissa jotka menevät sekaisin. Tällä merkinnällä f, g ja $\varphi(a)$ ovat 0, $4-4$ ja $x^2+4x+a-12=0$.

157. Käyttämällä [28]:ä kahdesti, esimerkiksi ensin niin että ψ on $x+2=-4$, χ on $x=-6$ ja $\varphi(X)$ on $X \vee x+2=4$ tuottaen $x=-6 \vee x+2=4$, ja sitten niin että ψ on $x+2=4$, χ on $x=2$ ja $\varphi(X)$ on $x=-6 \vee X$.

158. Ei voida, koska kun $x=0$, on $(x^2+2)x = (4x-1)x$ mutta $x^2+2 \neq 4x-1$.

159. Kyllä voidaan. Pätee $(x^2+2)x = (x^2+2)y \Leftrightarrow (x^2+2)x-(x^2+2)y = 0 \Leftrightarrow (x^2+2)(x-y)=0 \Leftrightarrow x^2+2=0 \vee x-y=0$, missä viimeinen askel seuraa tulon nollasäännöstä. Koska $x^2 \geq 0$ ja $2>0$, on $x^2+2=0$ mahdoton. Jäljelle jää vain $x-y=0$. Se tarkoittaa samaa kuin $x=y$.

160. Kumpikin suunta saadaan [52]:lla ja lukujen laeilla valitsemalla $h(x)$:ksi $-x$.

161. Ilman sitä $3x-2y=2 \Rightarrow 3x-2(2x-3)=2$ ei ole oikein. Sen näkee esimerkiksi sijoituksella $x=y=2$. Sillä $3x-2y=2$ on tosi mutta $3x-2(2x-3)=2$ ei ole.

162. $\Gamma \cup \{(y=2x-3)\} \models x=4$

163. $\Gamma \models x=4$ ja *lähtökohta* $\Rightarrow x=4$

164. Ei voisi, koska $\Leftrightarrow$ ei olisi oikein. Esimerkiksi $x=4 \wedge y=0$ on vastaesimerkki: sillä $3x-2(2x-3)=2$ pätee, mutta $y=2x-3 \wedge 3x-2y=2$ ei päde.

165. Tällä kertaa syynä ei ole se, että $\Leftrightarrow$ olisi väärin. Se nimittäin on oikein. Syynä on se, että emme ole perustelleet, että se olisi oikein. Se johdettiin [34]:llä, eikä [34] anna lupaa kirjoittaa $\Leftrightarrow$. Siis emme uskaltaneet väittää *lähtökohta* $\Leftarrow y=2x-3 \wedge 3x-2y=2$, koska emme olleet tarkastaneet, onko se pätevä. Emme olleet tarkastaneet onko se pätevä, koska yhtälöparimme ratkaiseminen ei ainakaan vielä tarvitse sitä tietoa, joten sen tarkastaminen olisi ollut turhaa.

166. Ensimmäinen askel saadaan (23):lla, transitiivisuudella, (21):llä ja [34]:llä. Toinen askel saadaan [55]:llä siitä, että $x=4$. Kolmas askel saadaan [51]:llä siitä, että $2\cdot 4-3=5$ valitsemalla $\varphi(a)$:si $x=4 \wedge y=a$.

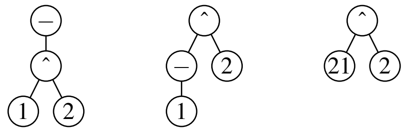
167. On perusteltava, että *lähtökohta* $\Leftarrow x=4 \wedge y=5$. Sen voi tehdä sijoittamalla alkuperäiseen yhtälöpariin $x=4$ ja $y=5$. Niin saadaan $2\cdot 4-5=3 \wedge 3\cdot 4-2\cdot 5=2$. Se on tosi, joten *lähtökohta* $\Leftarrow x=4 \wedge y=5$. Koska on jo perusteltu *lähtökohta* $\Rightarrow x=4 \wedge y=5$, [32] tuottaa *lähtökohta* $\Leftrightarrow x=4 \wedge y=5$, eli yhtälöparilla on yksi juuri, nimittäin $x=4 \wedge y=5$.

168. $X \wedge 3x - 2y = 2$

169. f on y, g on $2x-3$ ja $\varphi(a)$ on $3x - 2a = 2$.

170. Rivillä 6 sovellettiin [55]:tä siten, että f on x, g on 4 ja $\varphi(a)$ on $y = 2a-3$.

171. $x = 4 \wedge y = a$

172. 

173. Se ei noudata ehtoa, että merkkejä saa laittaa peräkkäin vain äärellisen määrän. Esimerkiksi luvun $\frac{1}{3}$ desimaaliesitys $0{,}333\ldots$ sisältää äärettömän määrän kolmosia.

174. Yksinkertaisimmillaan termi voi olla pelkkä vakio tai pelkkä muuttuja.

175. a ja b ovat muuttujia.

176. x on muuttuja, ja φ, f ja g ovat skeemaparametreja.

177. f, g ja h ovat skeemaparametreja.

178. Sen tuottaa [48] valinnalla $a := x+3$ ja $b := 3$. On jo todettu, että 3 ei sisällä määrittelemättömiä laskutoimituksia. Myöskään $x+3$ ei sisällä määrittelemättömiä laskutoimituksia, koska ainoa sen sisältämä laskutoimitus on yhteenlasku, ja yhteenlasku on aina määritelty.

179. Valinnalla $a := x$, $b := 3$ ja $c := -3$ [57] tuottaa $(x+3) + -3 = x + (3 + -3)$. Niistä x ja 3 eivät sisällä laskutoimituksia. Lauseke -3 sisältää laskutoimituksen $-$ jolla luvusta tuotetaan sen vastaluku, mutta se on aina määritelty.

180. Olemme johtaneet $(x+3)-3 = (x+3) + -3 = x + (3 + -3) = x + (3-3)$. Siitä $=$:n transitiivisuus tuottaa $(x+3)-3 = x+(3-3)$. Siitä saadaan [51]:llä $(x+3)-3 = 5 \Leftrightarrow x+(3-3) = 5$ siten, että $f := (x+3)-3$, $g := x+(3-3)$ ja $\varphi(a) :\Leftrightarrow a = 5$.

181. $(a-b)-c = (a+-b)-c = a+(-b-c) = a+-(b+c) = a-(b+c)$. Yhtäsuuruuksien perustelut: [48], aiemmin johdettu $(a+b)-c = a+(b-c)$, tehtävässä annettu $-(a+b) = -a-b$ takaperin sekä [48] takaperin.

182. $(a-b)+c = (a-b) + --c = (a-b) - -c = a-(b+-c) = a-(b-c)$. Yhtäsuuruuksien perustelut: tehtävässä annettu $--a = a$ takaperin, [48] takaperin, edellisessä tehtävässä johdettu laki sekä [48] takaperin.

183. Numeromerkin 6 määritelmän mukaan $6 = 5+1$. Valinnalla $f := 6$, $g := 5+1$ ja $h(x) := (x+1)+1$ [52] tuottaa siitä $(6+1)+1 = ((5+1)+1)+1$.

184. [57]:n mukaan $(5+1)+1 = 5+(1+1)$. Valinnalla $f := (5+1)+1$, $g := 5+(1+1)$ ja $h(x) := x+1$ [52] tuottaa siitä $((5+1)+1)+1 = (5+(1+1))+1$.

185. Sillä käännettiin $2 = 1+1$ ja $3 = 2+1$ takaperin päättelyaskelissa $(5+(1+1))+1 = (5+2)+1$ ja $5+(2+1) = 5+3$.

186. $8-3=8+-3=(5+3)+-3=5+(3+-3)=5+0=5$.

187. Kuusi kertaa yhtäsuuruusketjussa $8=\ldots=5+3$ ja neljä kertaa ketjussa $8-3=\ldots=5$, eli kaikkiaan 10 kertaa.

188. Aluksi oletamme $\lceil h\rfloor\wedge f=g$. Sen f ja g ovat samalla [52]:n f ja g, ja [52]:n $h(f)$ on $f+h$. Voidaksemme käyttää [52]:ta on meidän todistettava sen oletus, eli että $f=g$ ja $h(f)$ on määritelty. Ensimmäinen niistä pätee siksi, että se on todistettavan väitteemme oletuksissa. Jälkimmäinen pätee, koska [46]:n mukaan $f=g$ lupaa että f on määritelty; h oletettiin määritellyksi; ja yhteenlasku on aina määritelty. Siksi $f+h$ on määritelty. Nyt [52]:n oletukset on osoitettu, joten sen johtopäätös $h(f)=h(g)$ on käytettävissä. Koska $h(f)$ on nyt $f+h$, on $h(g)$ nyt $g+h$ ja [52]:n tuottama johtopäätös eli $h(f)=h(g)$ on $f+h=g+h$. Olemme oletuksesta $\lceil h\rfloor\wedge f=g$ johtaneet $f+h=g+h$, joten $\lceil h\rfloor\wedge f=g\Rightarrow f+h=g+h$.

189. Lakien [61], [63] (koska $2\neq 0$) ja [62] mukaan $(x\cdot 2)\cdot\frac{1}{2}=x\cdot(2\cdot\frac{1}{2})=x\cdot 1=x$.

190. Tehtävästä 189 saatiin $(x\cdot 2)\cdot\frac{1}{2}=x$. Sijoittamalla x:ksi 4 saadaan $(4\cdot 2)\cdot\frac{1}{2}=4$. Laki [52], ne ja [51] tuottavat $x\cdot 2=4\cdot 2\Rightarrow(x\cdot 2)\cdot\frac{1}{2}=(4\cdot 2)\cdot\frac{1}{2}\Leftrightarrow x=4$.

191. Lopputulos on kiistatta väärin, joten päättelyssä täytyy olla virhe. Tarkastamalla kaikki yhtäsuuruudet huomataan, että ainoa väärä on $\frac{4}{2}=\frac{1}{1}$. Niinpä ei ollut oikein poistaa molemmilta puolilta ”$+2$”. Sellainen poistaminen ei kohdistu lausekkeiden $\frac{4+2}{2}$ ja $\frac{1+2}{1}$ tuottamiin arvoihin (jotka ovat samat), vaan niiden esitysmuotoihin (jotka eroavat toisistaan sekä jakoviivan päällä että sen alla).

192. [31]:n mukaan $\mathsf{F}\leftrightarrow\psi\Leftrightarrow\neg\psi$ ja $\mathsf{T}\leftrightarrow\psi\Leftrightarrow\psi$, joten

- $\mathsf{F}\leftrightarrow Q\ \Leftrightarrow\ \neg Q\ \Leftrightarrow\ \mathsf{T}\leftrightarrow\neg Q\ \Leftrightarrow\ \neg\mathsf{F}\leftrightarrow\neg Q$
- $\mathsf{T}\leftrightarrow Q\ \Leftrightarrow\ Q\ \Leftrightarrow\ \neg\neg Q\ \Leftrightarrow\ \mathsf{F}\leftrightarrow\neg Q\ \Leftrightarrow\ \neg\mathsf{T}\leftrightarrow\neg Q$

193. $P\Leftrightarrow\mathsf{T}$, $Q\Leftrightarrow\mathsf{F}$ ja $R\Leftrightarrow\mathsf{F}$.

194. $P\Leftrightarrow\mathsf{T}$, $Q\Leftrightarrow\mathsf{F}$ ja $R\Leftrightarrow\mathsf{T}$.

195. Tehtävän [192] ja [31]:n mukaan

- $P\leftrightarrow Q\ \Leftrightarrow\ \neg P\leftrightarrow\neg Q\ \Leftrightarrow\ (P\leftrightarrow\mathsf{F})\leftrightarrow(Q\leftrightarrow\mathsf{F})$
- $P\leftrightarrow Q\ \Leftrightarrow\ (P\leftrightarrow\mathsf{T})\leftrightarrow(Q\leftrightarrow\mathsf{T})$

196. Ensimmäinen ja viimeinen seuraavat siitä, että yhteenlasku on vasemmalle liitännäinen. Toinen käyttää [65]:lle johtamaamme muunnelmaa ja kolmas induktio-oletusta.

197. $x\cdot 0+-x\ =\ 0+-x$

198. Luvun a ”vaihtoehtoinen vastaluku” olisi muu sellainen luku a', että $a+a'=0$. Sellaista ei ole olemassa, koska [58], [59], [57], [56], a':n perusominaisuus, [56] ja [58] tuottavat $a'=a'+0=a'+(a+-a)=(a'+a)+-a=(a+a')+-a=0+-a=-a+0=-a$.

199. [58], [59], [56], [57], [59] ja [58] tuottavat $--a=--a+0=--a+(a+-a)=(a+-a)+--a=a+(-a+--a)=a+0=a$.

200. Koska alkuperäinen polynomi on kolmatta astetta, on $Q(x)$ toista astetta. Niinpä se on muotoa $a_2x^2+a_1x+a_0$. Tällöin $(x-2)Q(x) = (x-2)a_2x^2+(x-2)a_1x+(x-2)a_0 = (a_2x^3-2a_2x^2)+(a_1x^2-2a_1x)+(a_0x-2a_0) = a_2x^3+(a_1-2a_2)x^2+(a_0-2a_1)x-2a_0$. Koska sen pitää olla yhtäsuuri kuin x^3-3x^2-x+6, pitää valita a_2, a_1 ja a_0 siten, että $a_2 = 1$, $a_1-2a_2 = -3$ eli $a_1 = -3+2a_2 = -3+2\cdot 1 = -1$, $a_0-2a_1 = -1$ eli $a_0 = -1+2a_1 = -1+2\cdot -1 = -3$ ja $-2a_0 = 6$ eli $a_0 = -3$. Niinpä $Q(x) = x^2-x-3$.

201. Jos nollapolynomin asteeksi olisi määritelty 0, väittäisi [67] että yhtälöllä $0 = 0$ olisi nolla juurta. Todellisuudessa jokainen kunnan alkio on sen juuri, joten sillä on yhtä monta juurta kuin kunnassa on alkioita eli ainakin kaksi.

202.

+	nen	ton
nen	nen	ton
ton	ton	nen

·	nen	ton
nen	nen	nen
ton	nen	ton

203. Katsomalla, onko taulukko symmetrinen vasemmasta yläkulmasta oikeaan alakulmaan vievän lävistäjän suhteen.

	♡	♠	♣
♡	♠	♡	♣
♠	♡	♡	♣
♣	♣	♣	♠

204. Taulukon $\cdot$ otsikkosarake ja sarake, jonka otsikkona on 1, ovat otsikkoriviä lukuun ottamatta samanlaiset.

·	0	1
0	0	0
1	0	1

205. Taulukon $\cdot$ rivillä, jonka alussa on 0, on jokaisessa sarakkeessa 0.

·	0	1
0	0	0
1	0	1

206. Tarkastamalla, että vasemmanpuoleisen taulukon jokaisella rivillä esiintyy 0 muuallakin kuin ensimmäisessä sarakkeessa. Toinen tapa: taulukosta näkee, että $0+0=0$ ja $1+1=0$, joten $-0=0$ ja $-1=1$.

207. Olemme jo tarkastaneet, että $0=0+0$ ja että jokaiselle luvulle x pätee $0x=0$ ja $1x=x$. Siksi $0(b+c)=0=0+0=0b+0c$ ja $1(b+c)=b+c=1b+1c$. Koska muita alkioita ei ole kuin 0 ja 1, on kaikki tapaukset käsitelty.

208. Tarkastamatta on enää [63] eli että jokaisella nollasta poikkeavalla luvulla on käänteisarvo. Ainoa nollasta poikkeava luku on 1. Se on itse oma käänteisarvonsa, koska $1\cdot 1=1$.

209. 0 on F, 1 on T, $+$ on XOR ja $\cdot$ on $\wedge$; tai 0 on T, 1 on F, $+$ on $\leftrightarrow$ ja $\cdot$ on $\vee$.

210. 10

211. $a+x=a+y \Rightarrow x+a=y+a \Rightarrow (x+a)+-a=(y+a)+-a \Rightarrow x+(a+-a)=y+(a+-a) \Rightarrow x+0=y+0 \Rightarrow x=y$.

212. Otsikkorivin ja -sarakkeen ulkopuolella mikään arvo ei voi esiintyä kahdesti samalla rivillä eikä kahdesti samassa sarakkeessa.

213. Yhteenlaskutaulu saadaan hyvälle alulle sillä, että jokaisella a pätee $0+a=a+0=a$. Loput arvot saadaan siitä, että sama arvo ei saa toistua samalla rivillä eikä samassa sarakkeessa. Esimerkiksi keskirivin oikeaan reunaan tulee laittaa

0, jottei keskiriville tulisi kahta ykköstä eikä viimeiseen sarakkeeseen kahta kakkosta. Kertotaulu saadaan siitä, että jokaisella a pätee $0a = a \cdot 0 = 0$, $1a = a \cdot 1 = a$ ja että on oltava olemassa sellainen arvo $\frac{1}{2}$, että $2 \cdot \frac{1}{2} = 1$.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

214. m div n on q:ssa ja m mod n on r:ssä.

215. Muuttujiin m ja n ei sijoiteta ohjelmassa.

216. Kun riville 2 tullaan ensimmäisen kerran, pätee $r = m$, ja alussa oletettiin $m \geq 0$. Kun riville 2 tullaan uudelleen, r sai arvonsa sijoituksesta $r := r - n$. Juuri sitä ennen testattiin että $r \geq n$, joten sijoituksen jälkeen $r \geq n - n = 0$.

217.

1 $r := m$; $q := 0$
2 **while** $r \geq n$ **do** $r := r - n$; $q := q + 1$
3 **while** $r < 0$ **do** $r := r + n$; $q := q - 1$

218. Jos $m \geq 0$, niin rivin 3 alkuun saakka kaikki on kuten edellisessä todistuksessa. Niinpä jakoyhtälö pätee rivin 3 alussa. Siksi $r \geq 0$, joten rivin 3 alusta siirrytään suoraan loppuun muuttamatta muuttujien arvoja. Niinpä jakoyhtälö pätee myös lopussa.

Muussa tapauksessa $m < 0$. Siksi rivin 1 lopussa $r < 0$. Koska $n > 0$, ei $r \geq n$ päde, joten riviltä 2 siirrytään riville 3 muuttamatta muuttujien arvoja. Samaan tapaan kuin edellisessä todistuksessa, $m = nq + r$ pätee aina rivin 3 alussa. Koska $n > 0$, r kasvaa joka kierroksella ja lopulta ohjelma lopettaa tilanteessa, jossa $m = nq + r$ ja $r \geq 0$. Silloin $r < n$, koska riville 3 alun perin tultaessa päti $r < 0 < n$ ja jos rivillä 3 r:ää kasvatetaan, niin sitä ennen on testattu että $r < 0$, joten kasvatuksen jälkeen $r < n$. Jakoyhtälön kaikki osat on nyt perusteltu.

219. Jos $m \geq n$, niin se jää ikuiseen silmukkaan rivillä 2. Muussa tapauksessa se jää ikuiseen silmukkaan rivillä 3.

220. Jos m on n:n monikerta, niin väite pätee. Muussa tapauksessa jakoyhtälön [74] mukaan $0 < m \bmod n < n$, sillä $|n| = n$ koska $n > 0$. Siksi $-n < -(m \bmod n) < 0$. Lisäämällä jokaiseen verrattavaan $m + n$ saadaan $m < m - (m \bmod n) + n < m + n$. Jakoyhtälön mukaan $m - (m \bmod n) = n(m \operatorname{div} n)$. Niinpä $m < n((m \operatorname{div} n) + 1) < m + n$, joten $n((m \operatorname{div} n) + 1)$ on luvattu luku.

221. On tosi. Esimerkiksi $6 = 2 \cdot 3$ ja $11 = 2 \cdot 5 + 1$.

222. Ei ole tosi. Se väittää, että on olemassa kokonaisluku, joka on yhtäaikaa parillinen ja pariton.

223. On tosi. Esimerkiksi $12 = 2 \cdot 6 = 3 \cdot 4$.

224. Esimerkiksi $\frac{1}{2}$ kelpaa y:ksi.

225. Ei ole olemassa reaalilukua, jolle $0 < y < 0$, koska sen pitäisi olla yhtäaikaa suurempi ja pienempi kuin 0, mikä on vastoin [70]:ää.

226. Kaikilla.

227. $y \leq 1$

228. Kun $x > 1$, luku 1 kelpaa y:ksi, joten $\rightarrow$:n oikea puoli ja samalla koko kaava on tosi. Muulloin kaava on tosi, koska $\rightarrow$:n vasen puoli $x > 1$ on epätosi.

229. Koska $y < y$ on mahdoton, on $\rightarrow$:n oikea puoli aina epätosi. Siksi kaava sievenee muotoon $\neg(y > 1)$ eli $y \leq 1$.

230. Ei ole. Esimerkiksi $\exists x : \forall y : x = 0$ on tosi, mutta $\forall x : \exists y : x = 0$ ei ole. Siltä varalta, että sinua häiritsee se, että tässä vastauksessa y ei esiinny φ:ssä, saat toisenkin vastauksen: $\exists x : \forall y : x = 0 \wedge y = y$ on tosi, mutta $\forall x : \exists y : x = 0 \wedge y = y$ ei ole.

231. Ei ole. Esimerkiksi $\forall x : \exists y : y = 0$ on tosi, mutta $\exists x : \forall y : y = 0$ ei ole.

232. Ei. Esimerkiksi $(\exists x : x > 0) \wedge (\exists x : x < 0)$ pätee, mutta $\exists x : x > 0 \wedge x < 0$ ei päde.

233. Kyllä. Jos jollain x:n arvolla φ on tosi, niin sillä myös $\varphi \vee \psi$ on tosi, joten vasen puoli eli $\exists x : \varphi \vee \psi$ on tosi. Silloin myös $\exists x : \varphi$ ja samalla oikea puoli ovat tosi, joten molemmat puolet ovat tosi. Samalla tavalla saadaan, että jos jollain x:n arvolla ψ on tosi, niin molemmat puolet ovat tosi. Muussa tapauksessa sekä φ että ψ ovat jokaisella x:n arvolla epätosi, joten $\exists x : \varphi$ ja $\exists x : \psi$ ja samalla oikea puoli ovat epätosi. Silloin myös $\varphi \vee \psi$ on jokaisella x:n arvolla epätosi, joten molemmat puolet ovat epätosi.

234. Jos $\exists x : \varphi(x)$ ei päde, niin, koska se on määritelty, $\neg\exists x : \varphi(x)$ pätee. De Morganin lain mukaan $\forall x : \neg\varphi(x)$ pätee. Lain [82] oletus, että f on määritelty, on myös [84]:n oletus. Se, että f on sijoitettavissa x:ään $(\neg\varphi(x))$:ssä seuraa siitä, että f on sijoitettavissa x:ään $\varphi(x)$:ssä eikä $\neg$:n lisääminen $\varphi(x)$:n eteen muuta niiden muuttujien joukkoa, jotka ovat sidotut x:n vapaiden esiintymien kohdalla. Niinpä [82]:sta saadaan $\neg\varphi(f)$. Se on ristiriidassa oletuksen $\varphi(f)$ kanssa, joten $\varphi(f) \Rightarrow \exists x : \varphi(x)$.

235. On tosi. Esimerkiksi $x + \frac{1}{2}$ kelpaa y:ksi. Se on rationaaliluku, koska sen voi esittää muodossa $\frac{2x+1}{2}$, missä $2x+1$ on kokonaisluku koska x on luonnollinen luku, ja 2 on positiivinen kokonaisluku. Selvästi $x < x + \frac{1}{2} < x + 1$.

236. Ei ole tosi. Koska kaavan alussa on $\forall x \in \mathbb{Q} :$, pitää sen jälkeen väitetyn asian päteä myös kun $x = -1$, sillä $-1 = \frac{-1}{1} \in \mathbb{Q}$ eli -1 on rationaaliluku. Silloin kaavan vaatimus $y < x + 1$ tarkoittaa $y < 0$. Mikään $y \in \mathbb{N}$ ei toteuta sitä, koska luonnolliset luvut ovat määritelmän mukaan nolla ja positiiviset kokonaisluvut.

237. On tosi. Valitaan mikä tahansa $x \in \mathbb{Q}$, niin se on rationaalilukujen määritelmän mukaan muotoa $\frac{m}{n}$, missä m ja n ovat kokonaislukuja ja $n > 0$. Tehtävän 220 mukaan jokin luvuista $m, m+1, \ldots, m+n-1$ on n:n monikerta. Merkitsemme sitä k:lla. Sille pätee $x = \frac{m}{n} \leq \frac{k}{n} < \frac{m+n}{n} = \frac{m}{n} + 1 = x + 1$, missä $\frac{k}{n}$ on kokonaisluku ja siis kelpaa y:ksi.

238. Ei ole tosi. Koska kaavan alussa on $\forall x \in \mathbb{Q} :$, pitää sen jälkeen väitetyn asian päteä myös kun $x = 0$, sillä $0 = \frac{0}{1} \in \mathbb{Q}$ eli 0 on rationaaliluku. Sillä valinnalla kaavan loppuosa väittää, että on olemassa luonnollinen luku, joka on nollaa suurempi ja ykköstä pienempi. Sellaista ei ole, joten kaava ei ole tosi.

239. 1, 1 2, 1 2 3, 2, 2 3, 3, 4 ja 4 3.

240. Ilman sitä kysely voisi harhautua tutkimaan aina vain suurempia ja suurempia solmujen numeroita ja jättää polun löytämättä. Se voisi esimerkiksi kaaren $1 \rightsquigarrow 5$ löydyttyä jatkaa ”päteekö $1 \rightsquigarrow 6$”, ”päteekö $1 \rightsquigarrow 7$”, ... Koska käyttäjä ei tiedä paljonko solmuja on, hän ei osaa lopettaa kun v saavuttaa solmujen määrän.

241. $\neg\exists w : (w \rightsquigarrow v) \wedge w \neq u \;\Leftrightarrow\; \forall w : \neg(w \rightsquigarrow v) \vee w = u \;\Leftrightarrow\; \forall w : (w \rightsquigarrow v) \rightarrow w = u$

242. $\exists v : u \rightsquigarrow^* v \rightsquigarrow u$

243. Kaava sanoo, että v:stä alkaa kaksi kaarta pitkä polku. Se on tosi jokaiselle muulle kuvien 37 ja 38 solmulle paitsi kuvan 37 vasemman puolen solmuille 2, 3 ja 4.

244. Kuvan 37 oikeanpuoleiselle ja kuvan 38 keskimmäiselle. Kuvan 37 vasemmanpuoleiselle. Kuvan 38 reunimmaisille.

245. Neljä: $2 \rightsquigarrow 1$ pätee tai ei päde, ja $2 \rightsquigarrow 2$ pätee tai ei päde.

246. Viisi: yksi jolle $1 = 2$ ja $1 \not\rightsquigarrow 1$, eli yksi solmu ilman kaaria; ja neljä joille $1 \neq 2$, $1 \not\rightsquigarrow 1$ ja $2 \not\rightsquigarrow 2$ pätevät, $1 \rightsquigarrow 2$ pätee tai ei päde, ja $2 \rightsquigarrow 1$ pätee tai ei päde.

247. Ei ole. Vaikka se jätettäisiin pois, olisivat 1 ja 2 eri solmu, koska 1:stä on kaari 1:een mutta ei 2:een.

248. Sellaisia suunnattuja graafeja ei ole olemassa, koska jos suunnatussa graafissa on silmukka, niin siinä on äärettömän monta silmukkaa. Jos esimerkiksi $v_1v_2v_3v_4$ on silmukka, niin myös $v_1v_2v_3v_4v_1v_2v_3v_4$, $v_1v_2v_3v_4v_1v_2v_3v_4v_1v_2v_3v_4$ ja niin edelleen ovat silmukoita.

249. $\neg(w \rightsquigarrow w \rightsquigarrow w) \;\Leftrightarrow\; \neg(w \rightsquigarrow w \wedge w \rightsquigarrow w) \;\Leftrightarrow\; \neg(w \rightsquigarrow w) \;\Leftrightarrow\; w \not\rightsquigarrow w$

250. $\{\exists v : v \neq v\}$

251. $(u \rightsquigarrow^* v) \rightarrow u = v \vee \exists w : u \rightsquigarrow^* w \rightsquigarrow v$

252. Jokaisesta solmusta on kaari itsensä ja muita kaaria ei ole. (Mikä tahansa sellainen suunnattu graafi kelpaa vastaukseksi, jossa jokaisella solmulla on edeltäjä, mutta silti ei ole jokaisesta solmusta jokaiseen solmuun polkua.)

253. $x^2 = 9$ on tosi silloin kun $x = 3$ tai $x = -3$. $\exists x : x^2 = 9$ on tosi aina. $\exists x : x^2 = 8$ ei ole tosi koskaan.

254. $$\begin{array}{l} \exists A : A(v) \wedge \\ \quad (A(u) \wedge \forall w_1 : \forall w_2 : A(w_1) \wedge (w_1 \rightsquigarrow w_2) \rightarrow A(w_2)) \wedge \\ (\forall B : (B(u) \wedge \forall w_1 : \forall w_2 : B(w_1) \wedge (w_1 \rightsquigarrow w_2) \rightarrow B(w_2)) \rightarrow \forall w : A(w) \rightarrow B(w)) \end{array}$$

255. Paikkaluku, englanniksi arity.

256. Puheena olevan suunnatun graafin solmujen joukko V.

257. Kaikkien suunnattujen graafien joukko.

258. $\mathsf{kertolasku}(x, y)\{$
   if $y = 0$ **then return** 0 **else return** $\mathsf{kertolasku}(x, y-1) + x$
$\}$

259. Se on paljon hitaampi ja vie paljon enemmän muistia kuin tietokoneen laitteistossa valmiina oleva kertolasku tai kouluissa opetettu allekkain kertominen.

260. Kaavoissa käytetään symbolia $\cdot$, jota Presburger-aritmetiikan sanastossa ei ole.

261. Kaava $\exists x : f + x = g$ ei toimi, koska se ei takaa että $f \leq g$, koska kokonaislukujen tapauksessa x voi olla myös negatiivinen. Esimerkiksi $\exists x : 1 + x = 0$ on tosi koska voidaan valita $x = -1$, mutta $1 \leq 0$ ei ole tosi.

262. $f \leq g \;\Leftrightarrow\; \exists x : f + x \cdot x = g$

263. Kaava $\exists x : f + x \cdot x = g$ ei kokonaisluvuilla ilmaise $f \leq g$, koska esimerkiksi $0 \leq 2$ on tosi, mutta ei ole olemassa sellaista kokonaislukua x että $0 + x^2 = 2$.

264. Väite saadaan [94]:llä. Nyt $\varphi(x)$ on $0 \cdot x = 0$. Kaava $\varphi(0)$ eli $0 \cdot 0 = 0$ saadaan [92]:sta sijoittamalla x:ksi 0. Aksioomien [93], [90] ja oletuksen $0 \cdot x = 0$ mukaan $0 \cdot (x+1) = 0 \cdot x + 0 = 0 \cdot x = 0$, joten $\varphi(x)$:stä seuraa $0 \cdot (x+1) = 0$ eli $\varphi(x+1)$.

265. Väite saadaan [94]:llä. Nyt $\varphi(x)$ on $1 \cdot x = x$. Kaava $\varphi(0)$ eli $1 \cdot 0 = 0$ saadaan [92]:lla. Oletus $1 \cdot x = x$ tuottaa $1 \cdot x + 1 = x + 1$ ja [93] tuottaa $1 \cdot (x+1) = 1 \cdot x + 1$, joten $1 \cdot (x+1) = x + 1$ eli $\varphi(x+1)$.

266. Osoitimme edellä $\forall x : 0 + x = x$. Siitä saadaan yhtäsuuruusketjun $x \cdot 1 = x \cdot (0+1)$ $= x \cdot 0 + x = 0 + x = x$ ensimmäinen ja viimeinen askel. Toinen ja kolmas askel saadaan [93]:lla ja [92]:lla.

267. $((0 \cdot 1) + 1) \cdot (1+1) + (1+1) \cdot 0 \;=\; ((0 \cdot 1) + 1) \cdot (1+1) + 0$
$= \; ((0 \cdot 1) + 1) \cdot (1+1) \;=\; (0+1) \cdot (1+1) \;=\; 1 \cdot (1+1)$

268. [93]:lla, uudelleen [93]:lla ja tehtävän [266] tuloksella saadaan
$(1+1) \cdot ((1+1)+1) \;=\; ((1+1) \cdot (1+1)) + (1+1)$
$= \; ((1+1) \cdot 1 + (1+1)) + (1+1) \;=\; ((1+1) + (1+1)) + (1+1)$

269. $(1 + (1+1)) + ((1+1)+1) \;=\; ((1+1)+1) + ((1+1)+1)$
$= \; (((1+1)+1) + (1+1)) + 1 \;=\; ((((1+1)+1)+1)+1)+1$

270. Jos nauhalla on jossakin kohdassa tyhjän ruudun perässä epätyhjä ruutu.