Sovellettu predikaattilogiikka

Antti Valmari

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

1 Johdanto

Matematiikan kursseilla keskitytään kunkin matematiikan alueen asioihin

- esim. todennäköisyyteen liittyvät käsitteet, lait ja tehtävien ratkaiseminen
- esim. joukkoihin liittyvät käsitteet, lait ja tehtävien ratkaiseminen

Tällä kurssilla keskitytään täsmällisille teorioille yleisiin asioihin

- ilmaukset ja niiden merkitykset
  - lausekkeet: tuottavat luvun, merkkijonon, ...
  - kaavat: tuottavat totuusarvon
- yleisimmät täsmällisen päättelemisen säännöt
  - emme käsittele mm. tietämyslogiikkaa

Alakohtaisia asioita käsitellään esimerkkeinä yleisten asioiden soveltamisesta

Suurin osa on maalaisjärkistä, mutta ei kaikki

- paljon pientä ja helppoa ei yhdistettynä välttämättä olekaan helppoa
  - logiikan maalaisjärkiset asiat ovat usein pikkuriikkisiä
  - kun suuri määrä niitä yhdistetään selväjärkisellä tavalla, voi kokonaisuus hämärtyä
- käsittely on usein abstraktia: $3 \rightsquigarrow x \rightsquigarrow \mathfrak{f}$ ja $\varphi \rightsquigarrow$ päättelemisestä päätteleminen
- joissakin asioissa vaistomme ohjaa meitä harhaan
  - esim. jos Jaana pitää jäätelöstä, niin Jaana ei pidä jäätelöstä

Matematiikassa ja tietojenkäsittelyssä käytetään formaalin ja luonnollisen kielen sekakieltä

- siihen, missä toinen on selvästi huonompi, käytetään toista
- välialueella käytetään kumpaa vaan
- vaikka asiaa ei formalisoitaisi, formalisoinnin osaaminen auttaa välttämään luonnollisen kielen ja päättelyn karikoita

$\Rightarrow$ on paljon asioita, joita ei kannata formalisoida, mutta kannattaa osata formalisoida

Miksi ei pelkästään luonnollista kieltä?

- luonnollinen kieli on epätarkkaa, eri ihmiset ymmärtävät samoja ilmauksia eri tavoin
- jotkin asiat paisuvat luonnollisella kielellä ilmaistuina hallitsemattoman pitkiksi
- asioissa voi olla kiemuroita, joita ei huomata normaalia puhetapaa käytettäessä
  - esim. Suomen perustuslaki 54§ 2. momentti:

    > Presidentiksi valitaan ehdokas, joka saa vaalissa enemmän kuin puolet annetuista äänistä. Jos kukaan ehdokkaista ei ole saanut enemmistöä annetuista äänistä, toimitetaan uusi vaali kahden eniten ääniä saaneen ehdokkaan välillä. Presidentiksi valitaan tällöin uudessa vaalissa enemmän ääniä saanut ehdokas. Jos on asetettu vain yksi ehdokas, hän tulee valituksi presidentiksi ilman vaalia.

  - huomaatko epätodennäköisiä mutta periaatteessa mahdollisia ongelmia?

Miksi ei pelkästään formaalia kieltä?

- vain osa asioista voidaan ilmaista kätevästi nykyisillä formalismeilla
- usein on vaikea varmistua, että formaali versio sanoo mitä haluttiin
- toisinaan ihmisille luonteva ja formalismille luonteva päättely kulkevat eri reittiä

⇒ monesti asian tekeminen formaalisti on vaivalloisempaa ja virhealttiimpaa kuin saman asian tekeminen epäformaalisti

⇒ täysin formaalit lähestymistavat ovat yleensä hyvin kömpelöitä

Olisi hyvä oppia käyttämään luonnollista kieltä formaalilla täsmällisyydellä

- monitulkintaisuuden vaaran tunnistaminen
- ilmaisujen muotoilu sellaisiksi, että riski väärin tulkitsemisesta minimoituu

Kahnemanin hitaan ja nopean päättelyn teoria 2011

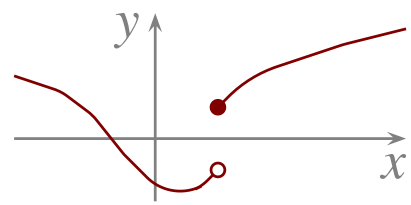
- Kahneman sai Nobelin palkinnon 2002 ihmisten päätöksentekoa koskevista töistään
- nopea päättelyjärjestelmä: vaistonvarainen, tunteellinen, yksioikoinen, tiedostamaton
- hidas päättelyjärjestelmä: harkitseva, looginen, tietoinen

Täsmää arkisiin havaintoihin:

- moni asia vaatii aluksi vaivalloista miettimistä, mutta automatisoituu kokemuksen myötä
- usein asiantuntija osaa tehdä, mutta ei (enää) osaa selittää miksi tekee niin kuin tekee
- selitys: nopeaan päättelyjärjestelmään kehittyy lisää sääntöjä, yhden jos toisen asian päätteleminen siirtyy hitaasta päättelyjärjestelmästä nopeaan

Paljon asioita menee nopeaan järjestelmään käymättä ensin hitaassa

- esim. tuskin kukaan viisivuotias on oppinut äidinkielensä lauserakenteet kielioppia miettimällä
- esim. monilla on vahva intuitio jatkuvuudesta, mutta silti se onnistuttiin määrittelemään kunnolla vasta 1800-luvulla



- mitkä kortit on käännettävä säännön ”jos toisella puolella on vokaali, niin toisella puolella on parillinen luku” tarkastamiseksi?
  - Wason ja Shapiro 1971: 4 % ratkaisi tämän kaltaisen oikein

A D 4 7

- mitkä kortit on käännettävä säännön ”alle 18-vuotias ei juo alkoholia” tarkastamiseksi?
  - Cox ja Griggs 1982: 74 % ratkaisi tämän kaltaisen oikein

olut mehu 16 25

Ihmiskunnalle on ollut vaikeaa keksiä, mitä ”jos . . . niin . . .” tarkoittaa

- 1894: Lewis Carroll julkaisi seuraavan päättelyn, josta oli ollut erimielisyyttä

  Allen, Brown ja Carr asuvat ja työskentelevät parturitalossa
  (1) joka hetki ainakin yksi heistä on paikalla
  (2) Allen ei mene ulos muuten kuin Brownin kanssa
  Niinpä kun Carr on ulkona, niin
  (3) jos Allen on ulkona, niin Brown on paikalla — koska (1)
  (4) jos Allen on ulkona, niin Brown on ulkona — koska (2)

  - mm. Oxfordin logiikan professori John Cook Wilsonin mielestä (3) ja (4) ovat ristiriidassa, joten Carr ei voi olla ulkona
  - mm. Carroll oli eri mieltä

- Stanford Encyclopedia of Philosophy 2021:

  Logics of conditionals deal with inferences involving sentences of the form “if A, (then) B” of natural language. Despite the overwhelming presence of such sentences in everyday discourse and reasoning, there is surprisingly little agreement about what the right logic of conditionals might be, or even about whether a unified theory can be given for all kinds of conditionals.

- esim. Jos Kaino on Lontoossa niin hän on Pariisissa, tai
  jos hän on Pariisissa niin hän on Jyväskylässä

Myös matematiikassa ja tietojenkäsittelyssä tarvitaan molempia päättelyjärjestelmiä

- kaiken tekeminen hitaalla järjestelmällä olisi liian hidasta ja työlästä
- nopea järjestelmä pystyy vain tuttua muotoa oleviin päätelmiin
- nopea järjestelmä johtaa toisinaan pahasti harhaan

Esimerkki

- voiko kokonaisluku olla itseään suuremman kokonaisluvun monikerta?
  - voi, esim. $0 < 1$ mutta $0 = 1 \cdot 0$, ja $-2 < -1$ mutta $-2 = (-1) \cdot 2$
- voiko positiivinen kokonaisluku olla itseään suuremman kokonaisluvun monikerta?
  - onko olemassa sellaiset kokonaisluvut n, m ja k, että $0 < n < m$ ja $n = mk$?
- ennen kuin päättelyrutiini on kehittynyt, voidaan tarvita monta välivaihetta
  - koska $0 < n < m$, pätee $m > 0$
  - positiivisella kertominen säilyttää $\leq$, eli jos $a \leq b$ ja $m > 0$, niin $ma \leq mb$
  - jos $k \leq 0$, niin koska $m > 0$ pätee $mk \leq m \cdot 0 = 0 < n$, joten $mk < n$ joten $mk \neq n$
  - jos $k \geq 1$, niin koska $m > 0$ pätee $mk \geq m \cdot 1 = m > n$, joten $mk > n$ joten $mk \neq n$
  - muita tapauksia ei ole, koska jos $k > 0$ niin $k \geq 1$, koska k on kokonaisluku

$\Rightarrow$ ei voi

- kun päättelyrutiini on vahva, riittää esim.
  - jos $k \leq 0$, niin $mk \leq 0 < n$
  - muutoin $k \geq 1$, joten $mk \geq m > n$

  $\Rightarrow$ aina $mk \neq n$

Formaalit päättelyjärjestelmät ovat yleensä liian pikkutarkkoja käytännön työhön

- esimerkki lausekkeen sieventämisestä suoraan reaalilukujen aksioomilla yms.:

$$2x+2-x-2 = ((2x+2)+-x)+-2 = (2x+(2+-x))+-2 =$$
$$(2x+(-x+2))+-2 = ((2x+-x)+2)+-2 = ((2x+(-1)x)+2)+-2 =$$
$$((2+-1)x+2)+-2 = (1x+2)+-2 = (x+2)+-2 = x+(2+-2) = x+0 = x$$

- käytännössä
  - käytettäisiin vähennyslaskua $-$ eikä vastaluvun yhteenlaskua $+-$
  - poimittaisiin samanmuotoiset termit ja yhdistettäisiin ne samantien:
    $2x-x=(2-1)x=1x=x$ ja $2-2=0$
  - laskettaisiin $x+0=x$ samantien: $2x+2-x-2=x$

Kurssilla puretaan käytännön täsmällisessä päättelemisessä tyypillisiä loikkia osiin, jotta

- näkyisi, miksi ne ovat oikein
- päättelemisessä tarvittavat asiat olisi helpompi muistaa
  - on helpompaa muistaa pieni määrä perussääntöjä ja osata rakentaa niistä pitempiä loikkia, kuin muistaa suuri määrä pitempien loikkien sääntöjä
  - jos joutuu rakentamaan saman pitemmän loikan säännön useasti, niin se jää lopulta itsestään mieleen
- opittaisiin ymmärtämään ja tarkastamaan kirjallisuudessa esiintyviä päättelyitä
- oma päättelytaito monipuolistuisi
- täsmällisen päättelyn perimmäiset säännöt tulisivat tutuiksi

Asiat pyritään esittämään yhteydessä sovelluksiin

- ongelma: täysin auki purettu päättely sisältää yleensä valtavasti tylsiä yksityiskohtia
  - useimmista niistä selviää vaivattomasti
  - ne on kuitenkin aina hoidettava, koska muuten toisinaan syntyisi päättelyvirheitä
  - jos ne aina mainittaisiin, niin kulloinenkin pääasia hukkuisi epäolennaisuuksien alle
- esimerkki
  - usein on tarkastettava, että ei synny nollalla jakamista eikä negatiivisen neliöjuurta

  $\Rightarrow$ lukuisiin päättelyaskeliin kuuluisi maininta ”ei sisällä jakolaskuja, neliöjuuria tms.”
  - kurssin esimerkeissä tarkastaminen mainitaan muutaman kerran jotta sen tarve jäisi mieleen, mutta sen jälkeen jätetään pois häiritsemästä pääasiaa
- toinen esimerkki
  - tarvitaan vähän väliä sitä, että yhtäsuuren saa tietyin ehdoin korvata yhtäsuurella kaavan sisällä
  - tämäkin näytetään esimerkeissä monesti, mutta ei loputtomasti

$\Rightarrow$ esimerkeissä ei tuoda esiin kaikkia sääntöjen käyttöjä, vaan vain esimerkin tavoitteen kannalta hyödylliset

- esimerkeissä voidaan käyttää aiemmista opinnoista tuttuja asioita, joiden looginen perusta on vielä esittämättä

2 Muutamia symboleita ja käsitteitä

"$\wedge$" tarkoittaa "ja"

- $vasen \wedge oikea$ on tosi jos ja vain jos sekä $vasen$ että $oikea$ on tosi
- $vasen \wedge oikea$ on epätosi jos ja vain jos $vasen$ tai $oikea$ tai molemmat on epätosi
- esim. (Jyväskylä on Suomessa) $\wedge$ (Oslo on Tanskassa) on epätosi
- esim. (Jyväskylä on Suomessa) $\wedge$ (Oslo on Norjassa) on tosi
- esim. (Jyväskylä on Ruotsissa) $\wedge$ (Oslo on Norjassa) on epätosi
- esim. (Jyväskylä on Ruotsissa) $\wedge$ (Oslo on Tanskassa) on epätosi

"$\vee$" tarkoittaa "tai"

- $vasen \vee oikea$ on tosi jos ja vain jos $vasen$ tai $oikea$ tai molemmat on tosi
- $vasen \vee oikea$ on epätosi jos ja vain jos sekä $vasen$ että $oikea$ on epätosi
- esim. (Jyväskylä on Suomessa) $\vee$ (Oslo on Tanskassa) on tosi
- esim. (Jyväskylä on Suomessa) $\vee$ (Oslo on Norjassa) on tosi
- esim. (Jyväskylä on Ruotsissa) $\vee$ (Oslo on Norjassa) on tosi
- esim. (Jyväskylä on Ruotsissa) $\vee$ (Oslo on Tanskassa) on epätosi

"$\neg$" tarkoittaa "ei"

- $\neg\,oikea$ on tosi jos ja vain jos $oikea$ on epätosi
- $\neg\,oikea$ on epätosi jos ja vain jos $oikea$ on tosi
- esim. $\neg$ (Jyväskylä on Suomessa) on epätosi
- esim. $\neg$ (Jyväskylä on Ruotsissa) on tosi

"T" tarkoittaa "tosi"

"F" tarkoittaa "epätosi"

Pikaesittely: *propositiologiikka* (*propositional logic*)

- *propositio* on totuusarvon saava vakio tai muuttuja
- esim. "Jyväskylä on Suomessa" on tosi propositiovakio
- esim. S eli "sataa" on propositiomuuttuja
- propositiologiikan kaavat muodostuvat propositioista ja symboleista $\neg$, $\wedge$, $\vee$, $\rightarrow$ ja $\leftrightarrow$
- kaavoja voi verrata symboleilla $\Leftrightarrow$, $\Rightarrow$, $\Leftarrow$ ja $\equiv$

Pikaesittely: *predikaattilogiikka* (*predicate logic*)

- propositiot on korvattu esim. lukuja tuottavien lausekkeiden vertailuilla
  - esim. $x^2 < 2y - 3$
- muuttujien käsittelemiseksi on symbolit $\forall$ ja $\exists$

Määritelmän määritelmä

yleispätevät asiat ovat **tummansinisellä**

- *määritelmä* tarkoittaa ilmausta, joka kertoo jonkin symbolin tai ilmauksen merkityksen

esimerkit yms. ovat **ruskealla**

- esim. *pääkaupunki* tarkoittaa sitä kaupunkia, jossa ylimmät hallintoelimet sijaitsevat
- esim. $\sqrt{x}$ tarkoittaa pienintä ei-negatiivista lukua, jolle pätee $\left(\sqrt{x}\right)^2 = x$

Tilapäinen määritelmä: *kaava* on mikä tahansa, joka tuottaa totuusarvon

- esim. $x^2 + 10 > 7x$ on kaava, mutta $x^2 + 10$ ei ole kaava, koska se tuottaa luvun
- kaavojen rakenne määritellään luvussa 5
- kaavan tuottama totuusarvo voi riippua tilanteesta
  - esim. tänään sataa
  - esim. $x^2 + 10 > 7x$
- *kaava on tosi* tarkoittaa samaa kuin *kaava tuottaa* T
- *kaava on epätosi* tarkoittaa samaa kuin *kaava tuottaa* F

Tällä kurssilla *tilanne* tarkoittaa muuttujien arvojen yhdistelmää

- esim. tänään voi olla 6.12.1917, 1.1.2024, ...
- esim. $x < y$ on tosi jos $x = 0 \land y = 1$, mutta epätosi jos $x = 1 \land y = 1$

Väittämiä esitetään ja päätelmiä tehdään eritasoisten *oletusten* alaisuudessa

- Torikatu on tärkeä joukkoliikennekatu on totta Oulussa mutta ei Jyväskylässä
- jos $x > 0$ niin $x \geq 1$ on pätevä jos puhutaan kokonaisluvuista, mutta ei ole jos puhutaan reaaliluvuista
- jos olen menossa pyörällä Harjun näkötornille, niin
  - jos en pue sadevaatteita ja alkaa sataa, niin kastun sateesta
  - jos puen sadevaatteet, niin kastun hiestä

  $\Rightarrow$ jos alkaa sataa, niin kastun joka tapauksessa
- kokonaisluvuilla
  - jos $n \leq 0$, niin $n^2 \geq n$, koska aina $n^2 \geq 0$
  - muussa tapauksessa $n \geq 1$, joten $n^2 = n \cdot n \geq 1 \cdot n = n$

  $\Rightarrow$ aina $n^2 \geq n$
- voi jopa olla, että tehdyt oletukset ovat tarkoituksellisesti mahdottomat
  - jos kassakaappi olisi räjäytetty viimeistään kun vahtimestari lähti töistä, niin vahtimestari olisi kuullut räjähdyksen

  $\Rightarrow$ kassakaappi räjäytettiin sen jälkeen kun vahtimestari lähti töistä
- esim. sivulla 6 pääteltiin kokonaisluvuilla pitkään oletuksesta $0 < n < m \wedge n = mk$ sen osoittamiseksi, että se on mahdoton

Tilanne on *mahdollinen*, jos ja vain jos se toteuttaa tehdyt oletukset

- esim. Carrollin parturiesimerkissä
  - Allen paikalla, Brown ulkona ja Carr paikalla on mahdollinen
  - Allen ulkona, Brown paikalla ja Carr ulkona on mahdoton
- kun väitetään, että jokin kaava pätee, niin tyypillisesti tarkoitetaan, että se on tosi jokaisessa mahdollisessa tilanteessa
- esim. jos $x \geq 0$, niin $\left(\sqrt{x}\right)^2 = x$
  - ei väitä, että $\left(\sqrt{-1}\right)^2 = -1$, koska $x = -1$ rikkoo oletusta $x \geq 0$
  - väittää, että $\left(\sqrt{7}\right)^2 = 7$, $\left(\sqrt{\frac{2}{5}}\right)^2 = \frac{2}{5}$, ...

Kaava voidaan kirjoittaa ilman tarkoitusta väittää, että se pätee

- esim. oletuksen ilmaisemiseksi: jos $x \geq 0$, niin ...
  - tarkastelu rajoitetaan niihin tilanteisiin, joissa kaava on tosi

  $\Rightarrow$ siitä eteenpäin kunnes oletuksesta luovutaan, mahdollisia ovat vain sellaiset tilanteet, joissa kaava on tosi
- esim. ratkaistavan tehtävän ilmaisemiseksi: ratkaise yhtälöpari $2x - y = 3 \wedge 3x - 2y = 2$
  - ratkaisijan pitää etsiä ne tilanteet, joissa kaava on tosi

Yhtäpitävyys

- olkoot *vasen* ja *oikea* kaavoja

  Vasen $\Leftrightarrow$ *oikea* tarkoittaa, että jokaisessa mahdollisessa tilanteessa, jossa *vasen* on tosi, myös *oikea* on tosi, ja päinvastoin. [1]

- siis ei saa olla olemassa sellaista muuttujien arvojen yhdistelmää, joka toteuttaa tehdyt oletukset, ja jossa toinen puoli on ja toinen ei ole tosi
- esim. $x^2+10>7x \;\Leftrightarrow\; x<2 \vee x>5$
- esim. jos $x<2$, niin $x^2=9 \;\Leftrightarrow\; x=-3 \vee x=3 \;\Leftrightarrow\; x=-3$
  - jos $x=-3$, niin sekä $x^2=9$ että $x=-3 \vee x=3$ että $x=-3$ on tosi
  - jos $x<-3$ tai $-3<x<2$, niin mikään niistä ei ole tosi
  - kun $x=3$ ei $x<2$ toteudu, joten ei haittaa että $x=-3 \vee x=3$ mutta ei $x=-3$
- *vasen* $\Leftrightarrow$ *oikea* ei ole tosi eikä epätosi, vaan *pätevä* tai *epäpätevä*
  - jos on olemassa yksikin muuttujien arvojen yhdistelmä, joka toteuttaa voimassa olevat oletukset, ja jolla toinen puoli on tosi mutta toinen ei ole, niin se on epäpätevä
  - muussa tapauksessa se on pätevä
- *vasen* $\Leftrightarrow$ *oikea* *ei ole kaava*, vaan *vertaa kahta kaavaa*
  - analogia: x^2+10 tuottaa lukuja ja $7x$ tuottaa lukuja, mutta $x^2+10>7x$ ei tuota vaan vertaa lukuja
- *vasen* $\Leftrightarrow$ *oikea* on *yhtäpitävyys* (ja vain se on yhtäpitävyys)

Yhtäpitävyysketju

$kaava_1 \Leftrightarrow kaava_2 \Leftrightarrow \ldots \Leftrightarrow kaava_n$ tarkoittaa, että
$kaava_1 \Leftrightarrow kaava_2$ ja $kaava_2 \Leftrightarrow kaava_3$ ja ... ja $kaava_{n-1} \Leftrightarrow kaava_n$.

- jokaisessa mahdollisessa tilanteessa, jossa jokin $kaava_i$ on tosi, on jokainen $kaava_i$ tosi

Yhtäpitävyyden päättelysääntöjä

jos on päätelty	niin saa päätellä
$vasen \Leftrightarrow oikea$	$oikea \Leftrightarrow vasen$
$kaava_1 \Leftrightarrow kaava_2 \Leftrightarrow \ldots \Leftrightarrow kaava_n$	$kaava_1 \Leftrightarrow kaava_n$
	$kaava \Leftrightarrow kaava$

[2]

- ensimmäinen seuraa [1]:n osuudesta ”ja päinvastoin”
- toisen perustelemiseksi tarkastelemme mitä tahansa mahdollista tilannetta
- jos siinä yksikin $kaava_i$ on tosi, niin
  - [1]:n mukaan $kaava_{i+1}, kaava_{i+2}, \ldots, kaava_n$ ovat tosi
    ja $kaava_{i-1}, kaava_{i-2}, \ldots, kaava_1$ ovat tosi

  $\Rightarrow$ sekä $kaava_1$ että $kaava_n$ on tosi
- muussa tapauksessa mikään kaavoista $kaava_i$ ei ole tosi,
  joten kumpikaan kaavoista $kaava_1$ ja $kaava_n$ ei ole tosi
- kolmas on pätevä, koska $kaava$ on tosi silloin ja vain silloin kun se on tosi

Jokaisessa mahdollisessa tilanteessa tosi kaava $\Leftrightarrow$:n avulla ilmaistuna

$$\mathit{kaava} \Leftrightarrow \mathsf{T} \text{ jos ja vain jos jokaisessa mahdollisessa tilanteessa } \mathit{kaava} \text{ tuottaa } \mathsf{T}. \qquad [3]$$

Jos tarkoitus on väittää, että $\mathit{kaava}_1, \ldots, \mathit{kaava}_n$ ovat jokaisessa mahdollisessa tilanteessa tosi, niin yhtäpitävyysketjun voi aloittaa "$\mathsf{T} \Leftrightarrow \mathit{kaava}_1$"

- esim. jokaisella a ja b pätee $ab \le \frac{a^2+b^2}{2}$, koska aina $(a-b)^2 \ge 0$, joten ...:

$$\mathsf{T} \;\Leftrightarrow\; (a-b)^2 \ge 0 \;\Leftrightarrow\; a^2 - 2ab + b^2 \ge 0 \;\Leftrightarrow\; a^2 + b^2 \ge 2ab \;\Leftrightarrow\; ab \le \tfrac{a^2+b^2}{2}$$

  - jokainen yhtäpitävyysketjun kaava on tosi kaikilla reaaliluvuilla a ja b
- vertaa yhtälön $x^2 + 2x - 15 = 0$ juuret ovat $x = -5 \vee x = 3$, koska ...:

$$x^2 + 2x - 15 = 0 \;\Leftrightarrow\; x = \tfrac{-2 \pm \sqrt{2^2 - 4 \cdot 1 \cdot (-15)}}{2} \;\Leftrightarrow\; x = -5 \vee x = 3$$

  - kukin yhtäpitävyysketjun kaava on tosi silloin ja vain silloin kun $x = -5$ tai $x = 3$

Vastaesimerkki (*counter-example*)

- vastaesimerkki tarkoittaa yksittäistapausta, jossa jokin väite, sääntö tms. rikkoutuu
- esim. $x = \frac{1}{2}$ on vastaesimerkki väitteelle, että reaaliluvuilla aina $x^2 \geq x$
  - $\left(\frac{1}{2}\right)^2 = \frac{1}{4} < \frac{1}{2}$
- vastaesimerkki yhtäpitävyydelle $\mathit{vasen} \Leftrightarrow \mathit{oikea}$ on tilanne, jossa
  - voimassa olevat oletukset toteutuvat
  - toinen kaavoista vasen ja oikea on tosi, ja
  - toinen kaavoista vasen ja oikea ei ole tosi
- vastaesimerkki osoittaa, että väite, sääntö tms. ei ole yleispätevä
- matematiikassa ”pätevä” tarkoittaa yleispätevää
  - yksikin vastaesimerkki riittää kumoamaan väitteen, säännön tms.
  - toisinaan väite, sääntö tms. saadaan päteväksi lisäämällä ehto, joka estää poikkeustapaukset
  - esim. $x \cdot \frac{1}{x} = 1$ ei ole pätevä, mutta jos $x \neq 0$ niin $x \cdot \frac{1}{x} = 1$ on
  - esim. $\sqrt{a}\sqrt{b} = \sqrt{ab}$ ei ole pätevä, mutta jos $a \geq 0 \wedge b \geq 0$ niin $\sqrt{a}\sqrt{b} = \sqrt{ab}$ on
- väite, päättelysääntö tms. on pätevä jos ja vain jos sillä ei ole yhtään vastaesimerkkiä
- esim. jos $0x = 3$, niin $x + 1 = 7$ on pätevä
  - ei ole olemassa lukua, jolle $0x = 3$, joten ei ole olemassa lukua, jolle $0x = 3$ mutta ei $x + 1 = 7$
- jopa jos $0x = 3$, niin $0x = 4$, joten $3 = 4$ on pätevä

Kaksoiskiellon poisto

- jos ei ole niin, että ei sada, niin sataa
- jos sataa, niin ei ole niin, että ei sada
- siis "ei ole niin, että ei sada" tarkoittaa samaa kuin "sataa"

$$\neg(\neg(S)) \;\Leftrightarrow\; (S)$$

- tämä ei päde pelkästään satamiselle, vaan pätee kun S:n tilalla on mikä tahansa kaava
- kaavoja on tapana merkitä kreikkalaisilla kirjaimilla φ (fii), ψ (psii) ja χ (khii)

$$\neg(\neg(\varphi)) \;\Leftrightarrow\; (\varphi)$$

- sallimme jättää sulkeet pois silloin, kun niiden rajaama alue on selvä ilmankin

$$\neg\neg\varphi \;\Leftrightarrow\; \varphi \qquad [4]$$

Vaihdannaisuus

- $oikea \wedge vasen$ on tosi täsmälleen silloin kun $vasen \wedge oikea$ on tosi

$$\varphi \wedge \psi \;\Leftrightarrow\; \psi \wedge \varphi \qquad [5]$$

- esim. Oslo on Norjassa $\wedge$ Jyväskylä on Ruotsissa on epätosi
- $oikea \vee vasen$ on tosi täsmälleen silloin kun $vasen \vee oikea$ on tosi

$$\varphi \vee \psi \;\Leftrightarrow\; \psi \vee \varphi \qquad [6]$$

De Morganin lait

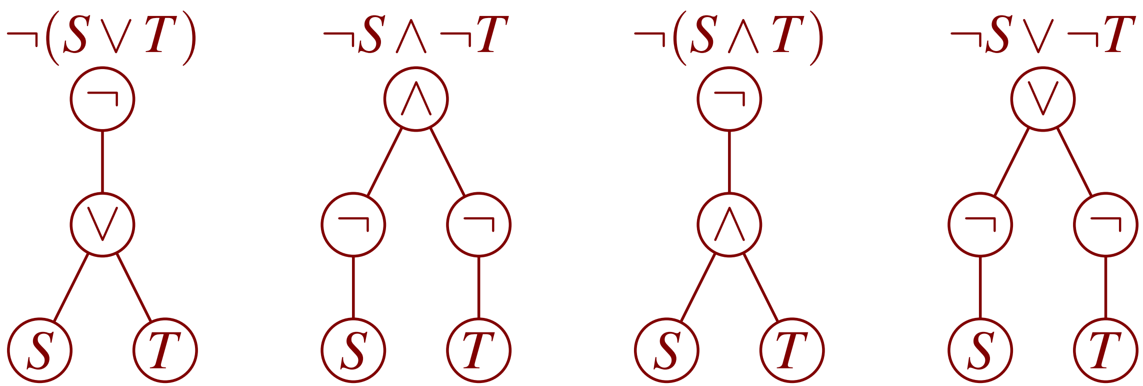
Suomen kielen ”eikä” on logiikan ”ja ei”

- jos ei ole niin, että sataa tai tuulee, niin ei sada eikä tuule
- jos ei sada eikä tuule, niin ei ole niin, että sataa tai tuulee
- siis ”ei ole niin, että sataa tai tuulee” tarkoittaa samaa kuin ”ei sada ja ei tuule”

$$\neg(S \vee T) \;\Leftrightarrow\; (\neg S) \wedge (\neg T)$$

- sulkeiden määrän vähentämiseksi on omaksuttu seuraava käytäntö:
  - $\neg$ lasketaan ensin
  - sitten $\wedge$
  - sitten $\vee$

$$\neg(S \vee T) \;\Leftrightarrow\; \neg S \wedge \neg T$$



- ”ei ole niin, että sataa ja tuulee” tarkoittaa samaa kuin ”ei sada tai ei tuule”

$$\neg(S \wedge T) \;\Leftrightarrow\; \neg S \vee \neg T$$

- nämä kaksi yhtäpitävyyttä pätevät, kun S:n ja T:n tilalla on mitkä tahansa kaavat

$$\neg(\varphi \vee \psi) \;\Leftrightarrow\; \neg\varphi \wedge \neg\psi \qquad \neg(\varphi \wedge \psi) \;\Leftrightarrow\; \neg\varphi \vee \neg\psi \qquad [7]$$

- edellä olevan kuvan tapa esittää lauseke tai kaava piirroksena on *lausekepuu*

Absorptiolait

- kaksi hassunoloista lakia, joista kuitenkin on päättelemisessä hyötyä
- jos sataa ja (sataa tai tuulee), niin sataa
- jos sataa, niin sataa tai tuulee
  $\Rightarrow$ sataa ja (sataa tai tuulee)
- niinpä "sataa ja (sataa tai tuulee)" tarkoittaa samaa kuin "sataa"
- tämäkin pätee myös kun "sataa" ja "tuulee" korvataan millä tahansa kaavoilla
  $$\varphi \wedge (\varphi \vee \psi) \;\Leftrightarrow\; \varphi$$
- se pätee myös kun φ:n tilalla on $\neg\varphi$ ja ψ:n tilalla on $\neg\psi$
  $$\neg\varphi \wedge (\neg\varphi \vee \neg\psi) \;\Leftrightarrow\; \neg\varphi$$
- (kaksiarvologiikassa pätee) jos *vasen* $\Leftrightarrow$ *oikea*, niin $\neg$ *vasen* $\Leftrightarrow \neg$ *oikea*
  $$\neg(\neg\varphi \wedge (\neg\varphi \vee \neg\psi)) \;\Leftrightarrow\; \neg\neg\varphi$$
- kaksoiskiellon poistolla [4], De Morganin laeilla [7] ja sillä, että "$\Leftrightarrow$" toimii molempiin suuntiin samalla tavalla [2], saadaan
  $$\varphi \;\Leftrightarrow\; \neg\neg\varphi \;\Leftrightarrow\; \neg(\neg\varphi \wedge (\neg\varphi \vee \neg\psi)) \;\Leftrightarrow\; \neg\neg\varphi \vee \neg(\neg\varphi \vee \neg\psi)$$
  $$\Leftrightarrow\; \varphi \vee (\neg\neg\varphi \wedge \neg\neg\psi) \;\Leftrightarrow\; \varphi \vee (\varphi \wedge \psi)$$
- niinpä [2] $\varphi \vee (\varphi \wedge \psi) \;\Leftrightarrow\; \varphi$
- kaikkiaan saatiin kaksi absorptiolakia:
  $$\varphi \wedge (\varphi \vee \psi) \;\Leftrightarrow\; \varphi \qquad\qquad \varphi \vee (\varphi \wedge \psi) \;\Leftrightarrow\; \varphi$$

[8]

Ohjelmoinnissa, matematiikassa ja arjessa esiintyy myös määrittelemättömiä väitteitä

- esim. `olio = null; if( olio.kenttä == 0 ){ ... }`
- esim. seuraavan palauttama arvo on 1: `i=0; while(true){i=1;} return i;`
- esim. $-\frac{1}{0} < \frac{1}{0}$
- esim. Suomen kuningatar antoi tulipalon sammuttajalle urhoollisuusmitalin

Sellaiset väitteet eivät ole tosia, mutta myöskään "ei" edessä ei tee niistä tosia

- esim. `olio = null; if( olio.kenttä != 0 ){ ... }`
- esim. seuraavan palauttama arvo ei ole 1: `i=0; while(true){i=1;} return i;`
- esim. $-\frac{1}{0} \geq \frac{1}{0}$
- esim. Suomen kuningatar ei antanut tulipalon sammuttajalle urhoollisuusmitalia

Siksi toisinaan tarvitaan kolmas totuusarvo "määrittelemätön" U

- $\mathit{vasen} \wedge \mathit{oikea}$ on määrittelemätön jos ja vain jos jompikumpi puoli on määrittelemätön ja toinen puoli ei ole epätosi
- $\mathit{vasen} \vee \mathit{oikea}$ on määrittelemätön jos ja vain jos jompikumpi puoli on määrittelemätön ja toinen puoli ei ole tosi
- $\neg\,\mathit{oikea}$ on määrittelemätön jos ja vain jos oikea on määrittelemätön
- *kaksiarvoisessa* (*two-valued*) logiikassa U ei ole ja *kolmiarvoisessa* (*three-valued*) on käytössä

Huomaa!

- ”ei ole tosi” ei ole sama kuin ”epätosi”
- se on sama kuin ”epätosi tai määrittelemätön”

Jos ajatellaan, että F on pienin, U on keskimmäinen ja T on suurin, niin

- $vasen \wedge oikea$ tuottaa minimin siitä mitä $vasen$ ja $oikea$ tuottavat
- $vasen \vee oikea$ tuottaa maksimin siitä mitä $vasen$ ja $oikea$ tuottavat

Yhteenveto taulukoina

- T tarkoittaa ”tosi”
- F tarkoittaa ”epätosi”
- U tarkoittaa ”määrittelemätön”

¬	
F	T
U	U
T	F

∧	F	U	T
F	F	F	F
U	F	U	U
T	F	U	T

∨	F	U	T
F	F	U	T
U	U	U	T
T	T	T	T

[9]

Huomaa ero

- T, U ja F ovat muuttujia, jotka voivat saada minkä tahansa totuusarvon
- T, U ja F ovat totuusarvoja

Propositiomuuttuja voi mahdollisessa tilanteessa saada arvokseen vain F tai T. [10]

- tämä rajoitus varmistaa, että määrittelemättömän käsittely menee aina järkevästi
  - tarkemmat yksityiskohdat kuuluvat kurssin ulkopuolelle
- sovellusten kannalta se tarkoittaa mm. että aina joko sataa tai ei sada; koskaan ei ole määrittelemätöntä, sataako
- propositiomuuttujan tilalle laitettava kaava voi tuottaa U
- tämä on samankaltaista sen kanssa, että tavallisen muuttujan arvo ei koskaan ole määrittelemätön, mutta muuttujan tilalle laitettava lauseke voi olla

Laki ja päättelysääntö

- tällä kurssilla *laki* tarkoittaa kaavaa, yhtäpitävyyttä, päättelyimplikaatiota tai yhtätotuutta, joka on voimassa *jokaisella* muuttujien arvojen yhdistelmällä
  - esim. $a+b=b+a$
  - ei tarkasteta pelkästään mahdollisissa tilanteissa, vaan kaikissa tilanteissa
  - ”päättelyimplikaatio” esitellään luvussa 6 ja ”yhtätotuus” luvussa 5
- tärkeä periaate:

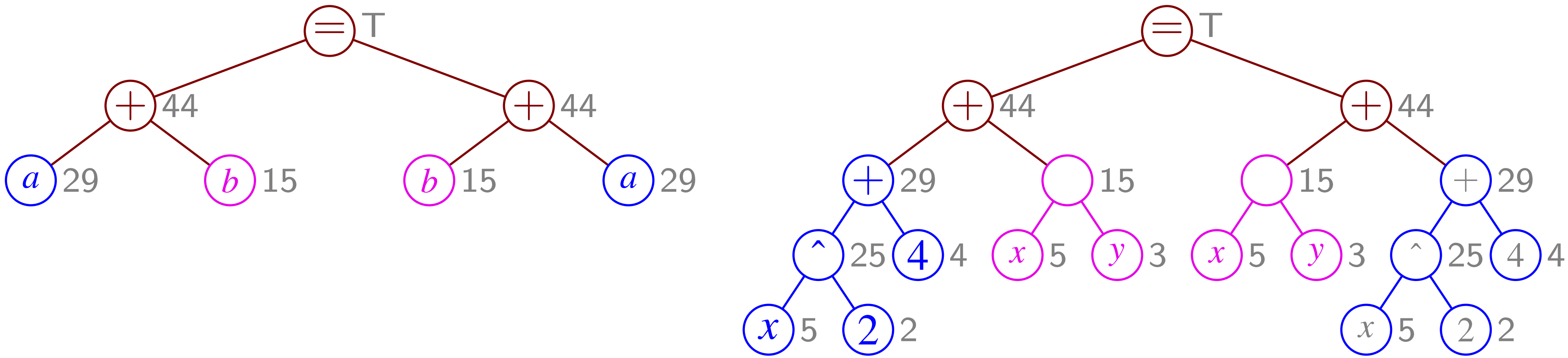
  Ilman muita oletuksia kuin T johdettu kaava, yhtäpitävyys, päättelyimplikaatio tai yhtätotuus on laki. [11]

  - puheenaiheen lakeja, kuten $a+b=b+a$, ei katsota oletuksiksi
- oletusten alaisena johdetusta kaavasta tms. saadaan laki ilmaisemalla oletukset osana kaavaa tms.
  - esim. jos $b \neq 0$, niin $\frac{a}{b} \cdot b = a$
  - esim. $b = 0 \vee \frac{a}{b} \cdot b = a$
  - asiaan palataan kun on otettu käyttöön symboli ilmaisemaan ”jos ... niin ...”
- tällä kurssilla *päättelysääntö* tarkoittaa sääntöä, jonka mukaan saa johtaa kaavan, yhtäpitävyyden tai päättelyimplikaation
  - esim. jos on johdettu kaavat φ ja ψ, niin saa johtaa $\varphi \wedge \psi$
  - esim. jos on johdettu $\varphi_1 \Leftrightarrow \varphi_2$ ja $\varphi_2 \Leftrightarrow \varphi_3$, niin saa johtaa $\varphi_1 \Leftrightarrow \varphi_3$ [2]
- päättelysäännön käyttö päättelyssä on *päättelyaskel*

Eräs hyvin yleisesti käytetty päättelysääntö:

> Jos laissa ei esiinny symboleita $\forall$ eikä $\exists$, niin lain muuttujien tilalle saa sijoittaa mitkä tahansa määritellyt lausekkeet. [12]

- saattaa olla tarpeen lisätä sulkeita laskujärjestyksen säilyttämiseksi
  - esim. laista $0a = 0$ saa johtaa $0(x+1) = 0$ sijoittamalla a:ksi $x+1$, mutta ei saa johtaa $0x+1=0$
- saman muuttujan jokaisen esiintymän tilalle on sijoitettava sama lauseke
  - esim. laista $a+b=b+a$ saa johtaa $(x^2+4)+xy = xy+(x^2+4)$ sijoittamalla a:ksi x^2+4 ja b:ksi xy
- [12] on pätevä, koska laskun jatkamisen kannalta vain välituloksen arvolla on merkitystä, ei sillä saatiinko se suoraan muuttujasta vai laskun tuloksena
  - esim. tilanne $x = 5 \land y = 3$



- välituloksen pitää kuitenkin olla määritelty, jotta se kelpaisi muuttujan tilalle
  - esim. laista $a = a$ ei saa johtaa $\frac{1}{0} = \frac{1}{0}$

Miksi $(x^2+4)+xy = xy+(x^2+4)$ eikä $x^2+4+xy = xy+x^2+4$?

- siksi, että katsomme nyt asiaa hyvin yksityiskohtaisella tasolla
  - $x^2+4+xy = xy+x^2+4$ on oikein
  - käytännössä siihen saa hypätä suoraan
  - oikeasti siihen pääseminen vaatii kuitenkin useamman kuin yhden päättelyaskeleen
- vakiintuneen käytännön mukaan x^2+4+xy tarkoittaa samaa kuin $(x^2+4)+xy$ ja $(xy+x^2)+4$ tarkoittaa samaa kuin $xy+x^2+4$
- ns. liitäntälaista voidaan johtaa $xy+(x^2+4) = (xy+x^2)+4$ [12]

$\Rightarrow$ $x^2+4+xy = (x^2+4)+xy = xy+(x^2+4) = (xy+x^2)+4 = xy+x^2+4$

- $=$:n lakeja ja [12] käyttämällä siitä saadaan $x^2+4+xy = xy+x^2+4$
- jos et ole varma, tarvitaanko sulkeita, niin lisää ne varmuuden vuoksi

Miksi $\forall$ ja $\exists$ on kielletty?

- ne otetaan käyttöön luvussa 11
- niiden vaikutuksesta se, mitä muuttujaa esim. x tarkoittaa, voi vaihtua

$\Rightarrow$ varomaton sijoitus niiden alaisuudessa voi tuottaa samankaltaisen virheen kuin "kuusi plus yksi on seitsemän, joten joulukuusi plus yksi on jouluseitsemän"

- tähän ongelmaan on ratkaisu, mutta tässä vaiheessa se on vaikea selittää
- yksinkertaisinta on kieltää ne kunnes niiden oikea käyttötapa voidaan kertoa

Tässä luvussa kohtaamiamme logiikan käsitteitä:

- *totuusarvot tosi* T, *epätosi* F ja *määrittelemätön* U
- *propositio* on vakio tai muuttuja, jonka arvo on totuusarvo
  - käytettävissä olevat propositiot riippuvat puheenaiheesta
  - esim. ”Jyväskylä on Suomessa”
- *tilanne* on muuttujien arvojen yhdistelmä
  - propositiomuuttujat, kuten ”sataa”
  - tavalliset muuttujat kuten x, jotka sisältävät esim. lukuja ja esiintyvät mm. vertailussa kuten $x^2+4 \leq 3x$
- *kaavoja* merkitään kreikkalaisilla kirjaimilla φ (fii), ψ (psii) ja χ (khii)
  - kaava tuottaa totuusarvon T, F tai U
  - hyvin monen kaavan tuottama totuusarvo riippuu tilanteesta, mutta ei kaikkien
- *oletus* rajoittaa tilanteita, jotka otetaan huomioon
- *mahdollinen tilanne* on tilanne, joka toteuttaa kaikki voimassa olevat oletukset
- *ei* $\neg\varphi$, *ja* $\varphi \wedge \psi$ ja *tai* $\varphi \vee \psi$
  - $\neg$ lasketaan ensin, sitten $\wedge$ ja vasta sitten $\vee$
  - $\neg$T $\Leftrightarrow$ F, $\neg$F $\Leftrightarrow$ T ja $\neg$U $\Leftrightarrow$ U
  - F $\wedge\, \varphi \Leftrightarrow \varphi\, \wedge$ F $\Leftrightarrow$ F, T $\wedge\, \varphi \Leftrightarrow \varphi\, \wedge$ T $\Leftrightarrow \varphi$ ja U $\wedge$ U $\Leftrightarrow$ U
  - F $\vee\, \varphi \Leftrightarrow \varphi\, \vee$ F $\Leftrightarrow \varphi$, T $\vee\, \varphi \Leftrightarrow \varphi\, \vee$ T $\Leftrightarrow$ T ja U $\vee$ U $\Leftrightarrow$ U

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

- *yhtäpitävyys* $\varphi \Leftrightarrow \psi$
  - on *pätevä*, jos ja vain jos jokaisessa mahdollisessa tilanteessa, jossa toinen φ:stä ja ψ:stä on tosi, toinenkin on tosi
  - muutoin se on *epäpätevä*
  - yhtäpitävyyttä tarkastettaessa otetaan huomioon vain ne muuttujien arvojen yhdistelmät, jotka toteuttavat tehdyt oletukset
- *päättelysääntö* on sääntö, jolla saa johtaa kaavan, yhtäpitävyyden tms.
  - moni päättelysääntö tarvitsee lähtökohdakseen kaavoja ja/tai yhtäpitävyyksiä tms.
- *laki* on kaava, yhtäpitävyys tms., joka on voimassa jokaisessa tilanteessa
  - on voimassa, vaikka ei olisi tehty mitään oletuksia
  - myöhemmin esiteltävä päättelysääntö [39] kertoo, kuinka kaavasta tms. saadaan laki
- *vastaesimerkki* on tilanne, jossa kaava ei ole tosi tai yhtäpitävyys tms. ei päde
  - kaava tms. on laki jos ja vain jos sillä ei ole yhtään vastaesimerkkiä
- muutama kaavoja koskeva laki

$\neg\neg\varphi \Leftrightarrow \varphi$		kaksoiskiellon poisto
$\varphi \wedge \psi \Leftrightarrow \psi \wedge \varphi$	$\varphi \vee \psi \Leftrightarrow \psi \vee \varphi$	vaihdannaisuus
$\neg(\varphi \vee \psi) \Leftrightarrow \neg\varphi \wedge \neg\psi$	$\neg(\varphi \wedge \psi) \Leftrightarrow \neg\varphi \vee \neg\psi$	De Morganin lait
$\varphi \wedge (\varphi \vee \psi) \Leftrightarrow \varphi$	$\varphi \vee (\varphi \wedge \psi) \Leftrightarrow \varphi$	absorptiolait

3 Esimerkki: ihmisten sukulaissuhteet

esimerkit yms. ovat ruskealla

yleispätevät asiat ovat tummansinisellä

Joukko ihmisiä

- heihin voidaan viitata
  - nimillä, esim. Diana, Harry
  - muuttujilla, esim. x, y

Laskutoimitukset eli *funktiosymbolit* $vanhA(x)$, $vanhB(x)$ ja $puoliso(x)$

- ottavat ihmisen ja tuottavat ihmisen tai ei mitään
  $\Rightarrow$ edustavat *osittaisia* tai *täysiä funktioita*
- esim. $vanhA(\text{Lilibet}) = \text{Meghan}$
  - vanhemmista ensin syntynyt on vanhempi-A
- esim. $puoliso(\text{Meghan}) = \text{Harry}$
- esim. $puoliso(\text{Lilibet})$ ei tuota mitään (ei ole määritelty), Lilibetillä ei ole puolisoa
- esim. $vanhB(puoliso(vanhA(\text{Lilibet}))) = \text{Diana}$

Relaatiosymbolit eli *predikaatit* $lapsi(x,y)$, $sisarus(x,y)$, $parisuhteessa(x)$, ...

- ottavat yhden tai kaksi ihmistä ja tuottavat totuusarvon
- esim. $sisarus(\text{Harry},\text{William}) \Leftrightarrow \text{T}$
- esim. $sisarus(\text{Diana},\text{Harry}) \Leftrightarrow \text{F}$

Kumpi on tosi, $\mathit{lapsi}(\text{Harry}, \text{Diana})$ vai $\mathit{lapsi}(\text{Diana}, \text{Harry})$?

- ainakin toinen on tosi: $\mathit{lapsi}(\text{Harry}, \text{Diana}) \vee \mathit{lapsi}(\text{Diana}, \text{Harry})$
- korkeintaan toinen on tosi: $\neg(\mathit{lapsi}(\text{Harry}, \text{Diana}) \wedge \mathit{lapsi}(\text{Diana}, \text{Harry}))$

$\Rightarrow$ otamme käyttöön helpommin muistettavan merkinnän $\mathit{lapsi} \hookleftarrow \mathit{vanhempi}$
  - esim. $\text{Harry} \hookleftarrow \text{Diana}$

- $x \hookleftarrow y \;\Leftrightarrow\; y = \mathit{vanhA}(x) \vee y = \mathit{vanhB}(x)$

Huomaa ero

väreillä helpotetaan symbolien esiintymien löytämistä

- ihmisiä verrataan *yhtäsuuruuden* symbolilla $=$
- totuusarvoja verrataan *yhtäpitävyyden* symbolilla $\Leftrightarrow$
- esim. $x \hookleftarrow y \;\Leftrightarrow\; y = \mathit{vanhA}(x) \vee y = \mathit{vanhB}(x)$

Huomaa ero: puolison ja vanhemmat voi ilmaista laskutoimituksina, lasta ei voi

- laskutoimitus voi tuottaa enintään yhden lopputuloksen
- puolisoita on enintään yksi ja vanhempia enintään kaksi

$\Rightarrow$ kolme laskutoimitusta riittää: $\mathit{puoliso}(x)$, $\mathit{vanhA}(x)$ ja $\mathit{vanhB}(x)$

- lapsien määrää ei ole rajattu

$\Rightarrow$ tarvittaisiin loputtomasti laskutoimituksien symboleita

Miksi on valittu, että ensin syntynyt vanhempi on vanhempi-A?

- pitäisikö olla $\mathit{vanhA}(\text{Lilibet}) = \text{Meghan}$ ja $\mathit{vanhB}(\text{Lilibet}) = \text{Harry}$ vai toisinpäin?
- sallitaanko $\begin{array}{l} \mathit{vanhA}(\text{Lilibet}) = \mathit{vanhB}(\text{Archie}) \land \\ \mathit{vanhB}(\text{Lilibet}) = \mathit{vanhA}(\text{Archie}) \end{array}$?
- sisarus, jos jokaisen vanhemmat voivat olla kummin päin vaan:

eri vaihtoehdot eri väreillä

$$\begin{array}{l} \mathit{sisarus}(x,y) \;\Leftrightarrow \\ \quad (\; (\mathit{vanhA}(x) = \mathit{vanhA}(y) \land \mathit{vanhB}(x) = \mathit{vanhB}(y)) \lor \\ \quad\quad (\mathit{vanhA}(x) = \mathit{vanhB}(y) \land \mathit{vanhB}(x) = \mathit{vanhA}(y)) \\ \quad) \land x \neq y \end{array}$$

- sisarus, jos sisarusten vanhemmilla on sama järjestys:

$$\mathit{sisarus}(x,y) \;\Leftrightarrow\; \mathit{vanhA}(x) = \mathit{vanhA}(y) \land \mathit{vanhB}(x) = \mathit{vanhB}(y) \land x \neq y$$

$\Rightarrow$ vanhempien asettaminen järjestykseen yksinkertaistaa kaavoja

- valitsemme mielivaltaisesti, että aikaisemmin syntynyt on vanhempi-A

Jotta esimerkkimme ei muuttuisi liian monimutkaiseksi,
oletamme että jokaisella on täsmälleen kaksi vanhempaa:

$$\mathit{vanhA}(x) \neq \mathit{vanhB}(x) \;\Leftrightarrow\; \mathsf{T}$$

$\Rightarrow$ $\mathit{vanhA}(x)$ ja $\mathit{vanhB}(x)$ ovat aina määritellyt (harjoitustehtävä)

Voidaan ilmaista mm. seuraavasti, että kukaan ei ole oma lapsensa:

- $x \hookleftarrow x \;\Leftrightarrow\;$ F
- $\neg(x \hookleftarrow x) \;\Leftrightarrow\;$ T
  - pelkkä $\neg(x \hookleftarrow x)$ jättää avoimeksi, tarkoitetaanko, että pätee kaikille x
- $x \not\hookleftarrow x \;\Leftrightarrow\;$ T
- $x \neq vanhA(x) \wedge x \neq vanhB(x) \;\Leftrightarrow\;$ T

Esimerkki päättelystä yhtäsuuruusketjulla

- jos $vanhB(puoliso(vanhA(\text{Lilibet})))$ on määritelty, niin

$$
\begin{array}{lll}
 & vanhB(puoliso(vanhA(\text{Lilibet}))) & \\
= & vanhB(puoliso(\text{Meghan})) & vanhA(\text{Lilibet}) = \text{Meghan [sivu 29]} \\
= & vanhB(\text{Harry}) & puoliso(\text{Meghan}) = \text{Harry [sivu 29]} \\
= & \text{Diana} & vanhB(\text{Harry}) = \text{Diana Wikipedia}
\end{array}
$$

- $vanhB(\text{Harry})$ jne. on määritelty, joten $vanhB(puoliso(vanhA(\text{Lilibet}))) = \text{Diana}$

Esimerkki päättelystä yhtäpitävyysketjulla: $sisarus(x,y) \;\Leftrightarrow\; sisarus(y,x)$

$$
\begin{array}{lll}
 & sisarus(x,y) & \\
\Leftrightarrow & vanhA(x) = vanhA(y) \wedge vanhB(x) = vanhB(y) \wedge x \neq y & sisarus\text{:n määritelmä} \\
\Leftrightarrow & vanhA(y) = vanhA(x) \wedge vanhB(y) = vanhB(x) \wedge y \neq x & =\text{:n symmetrisyys} \\
\Leftrightarrow & sisarus(y,x) & sisarus\text{:n määritelmä}
\end{array}
$$

Puoliso-suhde on symmetrinen: $x = puoliso(y) \;\Leftrightarrow\; y = puoliso(x)$

- niinpä jos $y = puoliso(x)$, niin $x = puoliso(y)$, joten $x = puoliso(puoliso(x))$

Onko jokainen puolisonsa puoliso?

- Lilibetillä ei ole puolisoa, joten hän ei ole puolisonsa puoliso

Voimmeko merkitä $puoliso(\text{Lilibet}) =$ ”olematon”?

- Archiellakaan ei ole puolisoa, joten päteekö

  $puoliso(\text{Lilibet}) = \text{"olematon"} = puoliso(\text{Archie})$

  ja edelleen

  $puoliso(\text{Lilibet}) = puoliso(\text{Archie})$?
- on luontevaa ajatella, että kumpikaan seuraavista ei ole totta:

  $puoliso(\text{Lilibet}) = puoliso(\text{Archie})$
  $puoliso(\text{Lilibet}) \neq puoliso(\text{Archie})$
- jos kumpi tahansa olisi epätosi, niin toinen olisi tosi
  - haluamme pitää kiinni siitä, että $a \neq b$ tarkoittaa samaa kuin $\neg(a = b)$
- logiikka saadaan tältä osin toimivaksi seuraavalla käytännöllä:

  Vertailu (yleisemmin relaatio) tuottaa U jos ja vain jos ainakin yksi sen osapuoli on määrittelemätön. [13]

Jokainen, jolla on puoliso, on puolisonsa puoliso

- $parisuhteessa(x)$ tarkoittakoon, että x:llä on puoliso
- silloin

$$parisuhteessa(x) \;\Leftrightarrow\; x = puoliso(puoliso(x))$$

- jos x:llä on puoliso, niin molemmat puolet ovat tosi
- jos x:llä ei ole puolisoa, niin vasen puoli on epätosi ja oikea puoli määrittelemätön
- kumpikaan tapaus ei riko määritelmää [1]:

  ”$vasen \Leftrightarrow oikea$ tarkoittaa, että jokaisessa mahdollisessa tilanteessa, jossa $vasen$ on tosi, myös $oikea$ on tosi, ja päinvastoin”

Sama hieman eri tavalla

$$\neg parisuhteessa(x) \vee x = puoliso(puoliso(x)) \;\Leftrightarrow\; \mathsf{T}$$

- jos x:llä on puoliso, niin $x = puoliso(puoliso(x))$ on tosi, kuten edellä nähtiin
- jos x:llä ei ole puolisoa, niin $\neg parisuhteessa(x)$ on tosi määritelmien mukaan

$\Rightarrow$ aina $\vee$:n jompikumpi puoli on tosi

Kukaan ei ole oma puolisonsa

- tämä ei toimi: $x \neq \mathit{puoliso}(x) \;\Leftrightarrow\;$ T
  - Lilibet $\neq \mathit{puoliso}($Lilibet$)$ ei ole tosi vaan määrittelemätön
  - $x =$ Lilibet on vastaesimerkki yhtäpitävyydelle $x \neq \mathit{puoliso}(x) \;\Leftrightarrow\;$ T
- kertaus [sivu 17]: vastaesimerkki on tapaus, jossa väite, yhtäpitävyys tms. ei päde
  - kumoaa sen, että väite tms. on yleispätevä eli pätee **jokaisessa** tapauksessa
- silti tämä toimii: $x = \mathit{puoliso}(x) \;\Leftrightarrow\;$ F
  - jos x:llä on puoliso, niin molemmat puolet ovat epätosi
  - jos x:llä ei ole puolisoa, niin vasen puoli on määrittelemätön ja oikea puoli epätosi
- tämäkin toimii: $\neg \mathit{parisuhteessa}(x) \vee x \neq \mathit{puoliso}(x) \;\Leftrightarrow\;$ T

Älä käytä symbolia $\not\Leftrightarrow$

- on epäselvää, tarkoittaisiko $\mathit{vasen} \not\Leftrightarrow \mathit{oikea}$ ”jossain tilanteessa” vai ”kaikissa tilanteissa” ”toinen puoli on ja toinen puoli ei ole T”

Tässä luvussa kohtaamiamme logiikan käsitteitä:

- *laskutoimitukset* eli *funktiosymbolit*
  - tuottavat puheenaiheen alkion (tässä luvussa ihminen) tai ei mitään
  - tuloksia voi verrata $=$:lla ja $\neq$:lla
- *relaatiosymbolit* eli *predikaatit*
  - tuottavat totuusarvon
  - tuloksia voi verrata $\Leftrightarrow$:lla
  - (älä käytä $\not\Leftrightarrow$)
- lain ilmaiseminen muodossa $\varphi \Leftrightarrow \psi$, $\varphi \Leftrightarrow \mathsf{T}$ tai $\varphi \Leftrightarrow \mathsf{F}$
  - "$\Leftrightarrow$ T" ja "$\Leftrightarrow$ F" korvataan tyylikkäämmällä keinolla luvussa 11
- ensimmäiset esimerkit *päättelemisestä* tiedettyjä kaavoja ja lakeja käyttäen
- *yhtäpitävyyden tarkastaminen* tarkastamalla eri tapausten tuottamat totuusarvot

Lisäksi kohtasimme puheenaiheesta riippuvia käsitteitä:

- vakiosymbolit Diana, William, Harry, Meghan, Lilibet ja Archie
- laskutoimitukset $vanhA(x)$, $vanhB(x)$ ja $puoliso(x)$
- relaatiosymbolit $parisuhteessa(x)$, $lapsi(x,y)$, $sisarus(x,y)$, $serkku(x,y)$, $x \hookleftarrow y$
- lakeja, kuten $x = puoliso(y) \;\Leftrightarrow\; y = puoliso(x)$ $\quad x \hookleftarrow x \;\Leftrightarrow\; \mathsf{F}$

$$x \hookleftarrow y \;\Leftrightarrow\; y = vanhA(x) \vee y = vanhB(x) \qquad vanhA(x) \neq vanhB(x) \;\Leftrightarrow\; \mathsf{T}$$

4 Lausekkeet ja sijoittaminen

Predikaattilogiikan *kieli* (*language*) jakaa symbolijonot kahtia

- niihin, joilla ei ole merkitystä
  - esim. $1 + = \leq) x$
- niihin, joilla on merkitys
  - esim. $x < 2$
  - esim. $x \geq y \land 3 = 4$
- kieleen kuuluvat ne ja vain ne, joilla on merkitys
- kieleen kuuluvien symbolijonojen ei tarvitse olla tosia
  - kun tilanne on valittu, tuottaa kieleen kuuluva jonkin totuusarvon F, T tai U
  - kieleen kuulumaton ei tuota

Predikaattilogiikan kielessä on kaksi tasoa: lausekkeet ja kaavat

- *lausekkeet* (*expression, term*) tuottavat puheenaiheen alkioita
- *kaavat* (*formula*) tuottavat totuusarvoja
- kaavat sisältävät usein lausekkeita, mutta ei toisinpäin

Lausekkeiden rakenne riippuu puheenaiheesta

$\Rightarrow$ se, mitä sanotaan predikaattilogiikan kieleksi, on itse asiassa monta eri kieltä

- kaavojen rakenne ei muilta osin riipu puheenaiheesta (mutta voi riippua puhujasta)

Lausekkeen rakenne

- *lauseke* muodostuu *vakiosymboleista*, muuttujista, *funktiosymboleista* ja/tai sulkeista
  - vakiosymboli on vakion nimi, esim. Diana
  - funktiosymboli on (osittaisen) funktion nimi, esim. $puoliso(x)$
- esim. $vanhB(puoliso(vanhA(\text{Lilibet})))$ sisältää 4 lauseketta
- esim. reaaliluvuilla $-2x+3y$ sisältää 8 lauseketta
- käytettävissä olevat vakiosymbolit ja funktiosymbolit riippuvat puheenaiheesta
  - esim. edellisessä luvussa Diana, Harry, $vanhA(x)$, $puoliso(x)$, ...
  - esim. reaaliluvuilla 0, 3810, $+$, $\cdot$, ...
- lausekkeen muuttujat saavat ja lausekkeet tuottavat puheenaiheen alkioita
  - luvussa 3 muuttujat saivat ja lausekkeet tuottivat arvoikseen ihmisiä
  - luvussa 7 muuttujat saavat ja lausekkeet tuottavat reaalilukuja
- kullakin funktiosymbolilla on *paikkaluku* (*arity*)
  - funktiosymbolin argumenttien määrä
  - positiivinen kokonaisluku
    (0-paikkaisten funktiosymboleiden tilalla on vakiosymbolit)
  - esim. $puoliso$:n paikkaluku on 1 ja $+$:n paikkaluku on 2
- eri puheenaiheilla on omia merkintätapoja funktiosymboleiden käytölle
  - esim. reaaliluvuilla ei merkitä $/(-(x,1),+(x,1))$ vaan $\frac{x-1}{x+1}$
  - esim. Java-ohjelmointikielessä ei merkitä `size(A)` vaan `A.size()`

Lauseke esittää osittaisen funktion puheenaiheen alkiomonikoilta puheenaiheen alkioille

- 1-paikkainen osittainen funktio $f(x)$ tuottaa yhdestä alkiosta enintään yhden alkion
- 2-paikkainen osittainen funktio $f(x,y)$ tuottaa kahdesta alkiosta enintään yhden
- 3-paikkainen osittainen funktio $f(x,y,z)$ tuottaa kolmesta alkiosta enintään yhden
- ...
- esim. $vanhA(\,vanhB(\,x\,)\,)$ tuottaa kullekin henkilölle yhden hänen isovanhemmistaan
- esim. $vanhA(\,puoliso(\,x\,)\,)$ tuottaa parisuhteessa olevalle henkilölle hänen puolisonsa vanhemmista yhden, ja muille se ei ole määritelty
- $h(1-\frac{a}{100})$ tuottaa alennetun hinnan, kun alkuperäinen hinta on h ja alennus on $a\,\%$
- matematiikassa tätä merkitään usein $f(x_1,\ldots,x_n) = lauseke$
  - esim. $kanta\text{-}asiakashinta(h,a) = h(1-\frac{a}{100})$

Puheenaiheessa on aina oltava vähintään yksi alkio

- tämä on ainoa predikaattilogiikan teorian asettama rajoitus puheenaiheille
- ilman sitä moni laki ja sääntö monimutkaistuisi melkein turhan takia
  - puheenaiheista, joissa ei ole yhtään alkiota, pystyy hyvin harvoin tekemään hyödyllisiä kaavoja tai päättelyitä
- yksisarvisia ei ole, joten kummallekaan seuraavista ei ole vastaesimerkkejä:
  - jokainen yksisarvinen on vaaleanpunainen
  - mikään yksisarvinen ei ole vaaleanpunainen

Määrittelemättömistä lausekkeista

- seuraava periaate on osoittautunut hyväksi:

  Lauseke on määrittelemätön jos ja vain jos se sisältää määrittelemättömän laskutoimituksen. [14]

- esim. vaikka $0a = 0$ jokaisella reaaliluvulla a, ei $0\sqrt{-1}$ ole 0 vaan määrittelemätön, koska $\sqrt{-1}$ ei ole määritelty
- muuttujat ovat aina määritellyt
- emme ota käyttöön symbolia edustamaan määrittelemättömän lausekkeen tulosta
  $\Rightarrow$ vakiosymbolit ovat aina määritellyt
  - esim. $\sqrt{-1}$ ei ole vakiosymboli vaan kolmesta osasta koostuva lauseke
- matematiikassa määrittelemätöntä edustamaan käytetään toisinaan symbolia $\perp$
  - jos $\perp$ olisi kuten luvut, niin voitaisiin päätellä $\sqrt{-1} = \perp = \frac{1}{0}$ ja edelleen $\sqrt{-1} = \frac{1}{0}$

  $\Rightarrow$ $\perp$:n haitat olisivat suuremmat kuin hyödyt
- ohjelmoinnin `null` on samankaltainen kuin $\perp$
- ohjelmoinnin `NaN` (not a number) poikkeaa molemmista
  - `0./0. == 0./0.` tuottaa `false`
  - `0./0. != 0./0.` tuottaa `true`
- määrittelemätön lauseke vastaa ikuiseen silmukkaan jääneen aliohjelman tulosta
  - sieltä ei saada ”poikkeus”, ”erikoistilanne” tms. vaan sieltä ei saada yhtään mitään

Jokaiselle funktiosymbolille on kaava, joka kertoo milloin funktio on määritelty

- esim.
  - $\frac{x}{y}$ on määritelty, jos ja vain jos $y \neq 0$
  - $\sqrt{x}$ on määritelty, jos ja vain jos $x \geq 0$
  - $\mathit{puoliso}(x)$ on määritelty, jos ja vain jos $x = \text{Harry} \vee x = \text{Meghan} \vee \ldots$
- ”on määritelty” -kaavalle ei ole vakiintunutta merkintää
- merkitsemme tällä kurssilla sitä $\lceil f \rfloor$
- esim.
  - $\lceil \frac{x}{y} \rfloor$ on $y \neq 0$
  - $\lceil \sqrt{x} \rfloor$ on $x \geq 0$
  - $\lceil \mathit{puoliso}(x) \rfloor$ on $x = \text{Harry} \vee x = \text{Meghan} \vee \ldots$
- jos ”on määritelty” -kaavassa esiintyy funktiosymboleita, niin niiden ”on määritelty” -kaavojen pitää olla T
  - tavallisesti niissä ei esiinny funktiosymboleita

$\Rightarrow$ ”on määritelty” -kaava ei koskaan tuota U

Monimutkaisemman lausekkeen ”on määritelty” -kaava saadaan rekursiivisesti [14]

- jos *lauseke* on vakio- tai muuttujasymboli, niin $\lceil lauseke \rfloor$ on T
- $\lceil \frac{lauseke_1}{lauseke_2} \rfloor$ on $lauseke_2 \neq 0 \wedge \lceil lauseke_1 \rfloor \wedge \lceil lauseke_2 \rfloor$
- $\lceil lauseke_1 + lauseke_2 \rfloor$ on $\lceil lauseke_1 \rfloor \wedge \lceil lauseke_2 \rfloor$
- ...
- esim.
  - $\lceil x \rfloor$ ja $\lceil 2 \rfloor$ ovat T
  - $\lceil x+2 \rfloor$ on $\mathsf{T} \wedge \mathsf{T}$
  - $\lceil \sqrt{x+2} \rfloor$ on $x+2 \geq 0 \wedge (\mathsf{T} \wedge \mathsf{T})$
  - $\lceil xy \rfloor$ on $\mathsf{T} \wedge \mathsf{T}$

  $\Rightarrow$ $\lceil \frac{\sqrt{x+2}}{xy} \rfloor$ on $xy \neq 0 \wedge (x+2 \geq 0 \wedge (\mathsf{T} \wedge \mathsf{T})) \wedge (\mathsf{T} \wedge \mathsf{T})$
- osuudet $\wedge\, \mathsf{T}$ ja $\mathsf{T} \wedge$ saa jättää pois
  - $\lceil x+2 \rfloor$ on T
  - $\lceil \sqrt{x+2} \rfloor$ on $x+2 \geq 0$
  - $\lceil xy \rfloor$ on T

  $\Rightarrow$ $\lceil \frac{\sqrt{x+2}}{xy} \rfloor$ on $xy \neq 0 \wedge x+2 \geq 0$

Lausekkeiden edustajat $\mathfrak{f}$, $\mathfrak{g}$, $\mathfrak{f}_i$ jne.

- edellä *lauseke*$_1$ ja *lauseke*$_2$ oli kömpelö merkintä!
- kun jatkossa haluamme puhua lausekkeesta kertomatta mikä lauseke, käytämme fraktuurakirjaimia $\mathfrak{f}$, $\mathfrak{g}$ jne.
- ne erottuvat kaavoista, koska kaavoille käytetään kreikkalaisia kirjaimia φ, ψ jne.
- ne erottuvat myös niistä käsitteistä, joille käytetään kursiivia, kuten x ja *puoliso*
- esim. reaaliluvuilla $x = x$ on aina tosi mutta $\mathfrak{f} = \mathfrak{f}$ ei ole aina tosi
  - x saa lukuarvoja, ja jokainen luku on yhtäsuuri itsensä kanssa
  - $\mathfrak{f}$:n tilalla saa olla lauseke $\frac{1}{0}$, eikä $\frac{1}{0} = \frac{1}{0}$ ole tosi vaan määrittelemätön
- lausekkeen rakenne voidaan nyt ilmaista seuraavasti: vakiosymboli, muuttuja tai muotoa $f(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$, missä
  - f on funktiosymboli
  - n on f:n paikkaluku
  - $\mathfrak{f}_1$, ..., $\mathfrak{f}_n$ ovat lausekkeita
  - merkintätavan $f(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ tilalla voi olla puheenaiheen oma merkintätapa

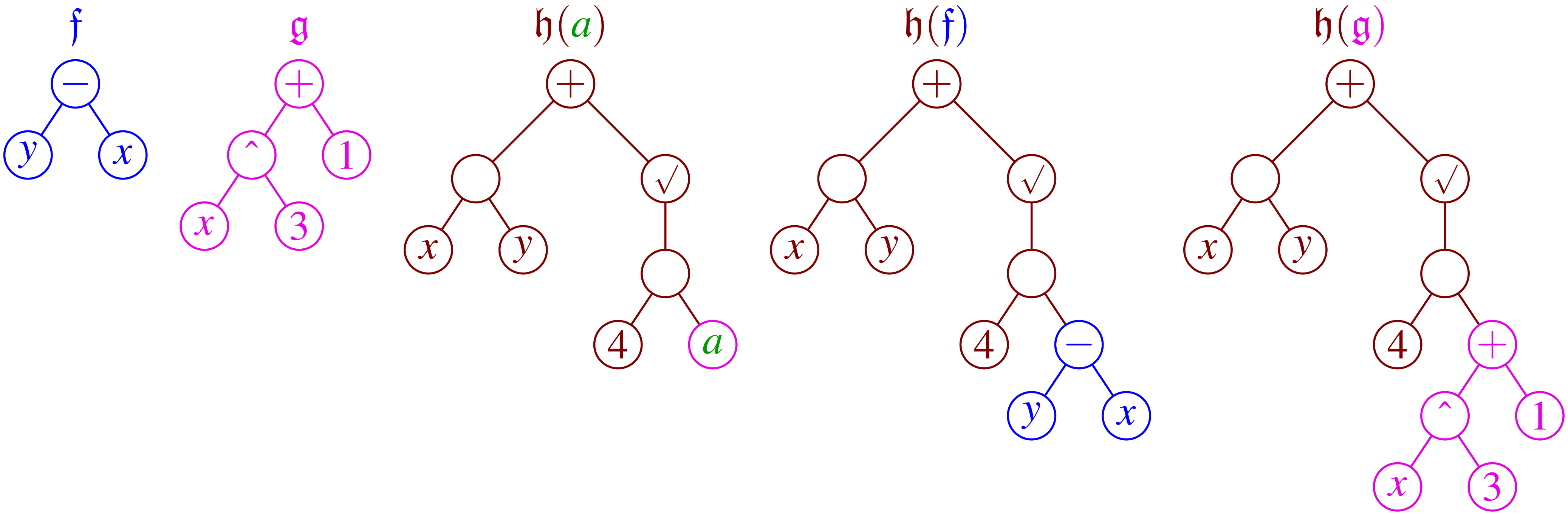
Merkinnöillä $\mathfrak{f}(x_1,\ldots,x_n)$ ja $\mathfrak{f}(\mathfrak{g}_1,\ldots,\mathfrak{g}_n)$ esitetään lausekkeiden $\mathfrak{g}_1,\ldots,\mathfrak{g}_n$ sijoittaminen muuttujien $x_1,\ldots,x_n$ tilalle lausekkeessa $\mathfrak{f}$

- esim. jos $\mathfrak{f}(x)$ on $\mathit{vanhB}(\mathit{puoliso}(x))$ ja $\mathfrak{g}$ on $\mathit{vanhA}(\text{Lilibet})$,
  niin $\mathfrak{f}(\mathfrak{g})$ on $\mathit{vanhB}(\mathit{puoliso}(\mathit{vanhA}(\text{Lilibet})))$
- kun lauseke sijoitetaan muuttujan tilalle, saattaa olla tarpeen lisätä sulkeet tai $\cdot$
  - jos $\mathfrak{f}(x,y)$ on x^2-3y ja $\mathfrak{g}$ on $5b$ ja $\mathfrak{h}$ on 6 ,
    niin $\mathfrak{f}(\mathfrak{g},\mathfrak{h})$ on $(5b)^2-3\cdot 6$
  - jos on epävarma tarvitaanko sulkeita, ne voi lisätä varmuuden vuoksi
  - esim. jos $\mathfrak{f}(x)$ on $1+x$ ja $\mathfrak{g}$ on 3, niin saa kirjoittaa $1+(3)$
- sijoitus tehdään muuttujan jokaiseen esiintymään lausekkeessa
  - jos $\mathfrak{f}(x,y)$ on x^2-2xy ja $\mathfrak{g}$ on $x+1$ ja $\mathfrak{h}$ on 6 ,
    niin $\mathfrak{f}(\mathfrak{g},\mathfrak{h})$ on $(x+1)^2-2(x+1)\cdot 6$
- merkintä $\mathfrak{f}(x)$ ei takaa, että x esiintyy $\mathfrak{f}$:ssä
  - esim. $\mathfrak{g}(a)$ on 0 sivulla 52
- merkinnässä $\mathfrak{f}(x_1,\ldots,x_n)$ ei välttämättä näytetä sulkeissa kaikkia muuttujia
  - asian kannalta tarpeettomat muuttujat vievät tilaa ja häiritsevät lukemista

Esimerkki lausekepuiden avulla

- $\mathfrak{f}$ on $y-x$, $\mathfrak{g}$ on x^3+1 ja $\mathfrak{h}(a) = xy + \sqrt{4a}$

$\Rightarrow$ $\mathfrak{h}(\mathfrak{f})$ on $xy+\sqrt{4(y-x)}$ ja $\mathfrak{h}(\mathfrak{g})$ on $xy+\sqrt{4(x^3+1)}$



Yhtäsuuruuden symmetrisyys lausekkeilla ilmaistuna

Jos $\mathfrak{f}$ ja $\mathfrak{g}$ ovat mitkä tahansa lausekkeet, niin $\mathfrak{f} = \mathfrak{g} \;\Leftrightarrow\; \mathfrak{g} = \mathfrak{f}$. [15]

- päättelysäännöllä [15] voidaan johtaa esim.

  $$\mathit{puoliso}(\textsf{Harry}) = \mathit{vanhA}(x) \;\Leftrightarrow\; \mathit{vanhA}(x) = \mathit{puoliso}(\textsf{Harry})$$

  valitsemalla $\mathfrak{f}$:ksi $\mathit{puoliso}(\textsf{Harry})$ ja $\mathfrak{g}$:ksi $\mathit{vanhA}(x)$
- tässä esimerkissä
  - joillakin x kuten Lilibet "$\Leftrightarrow$":n molemmat puolet tuottavat T
  - joillakin x kuten Harry "$\Leftrightarrow$":n kumpikaan puoli ei tuota T
  - millään x ei käy niin, että toinen puoli tuottaa ja toinen ei tuota T
- olennaista on, että kun valitaan muuttujille mitkä tahansa arvot, niin joko sekä $\mathfrak{f} = \mathfrak{g}$ että $\mathfrak{g} = \mathfrak{f}$ tai ei kumpikaan tuottaa T
  - voi olla, että molemmat tuottavat aina T, esim. $x + x = 2x \;\Leftrightarrow\; 2x = x + x$
  - voi olla, että kumpikaan ei tuota koskaan T, esim. $x + 1 = x \;\Leftrightarrow\; x = x + 1$
  - voi olla, että toisinaan molemmat tuottavat ja toisinaan kumpikaan ei tuota T
  - ei voi koskaan olla, että toinen tuottaa ja toinen ei tuota T
- päättelysäännöllä [15] todellakin voidaan johtaa $0 = 1 \Leftrightarrow 1 = 0$ ja se on pätevä
  - sillä ei todellakaan ole yhtään vastaesimerkkiä
  - intuitio, että $0 = 1 \Leftrightarrow 1 = 0$ on virheellinen koska $0 = 1$ on epätosi, johtaa harhaan

Yhtäsuuren sijoittaminen lausekkeeseen

Jos $\lceil \mathfrak{h}(\mathfrak{f}) \rfloor \vee \lceil \mathfrak{h}(\mathfrak{g}) \rfloor$ ja $\mathfrak{f} = \mathfrak{g}$, niin $\mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{g})$. [16]

- esim. tiedosta $\mathit{puoliso}(\text{Meghan}) = \text{Harry}$ [sivu 29] voidaan johtaa $\mathit{vanhB}(\mathit{puoliso}(\text{Meghan})) = \mathit{vanhB}(\text{Harry})$ valitsemalla seuraavasti:

$\mathfrak{h}(x)$	on	$\mathit{vanhB}(x)$	$\mathit{vanhB}(x)$ on aina määritelty [sivu 31]
$\mathfrak{f}$	on	$\mathit{puoliso}(\text{Meghan})$	
$\mathfrak{g}$	on	Harry	Harry on määritelty
$\mathfrak{h}(\mathfrak{f})$	on	$\mathit{vanhB}(\mathit{puoliso}(\text{Meghan}))$	
$\mathfrak{h}(\mathfrak{g})$	on	$\mathit{vanhB}(\text{Harry})$	$\mathit{vanhB}(\text{Harry})$ on määritelty

- esim. jos on oletettu $x+5<y$ ja tiedetään $y-x=x^3+1$, niin voidaan johtaa $xy+\sqrt{4(y-x)} = xy+\sqrt{4(x^3+1)}$ valitsemalla seuraaavasti:

$\mathfrak{h}(a)$	on	$xy+\sqrt{4a}$	
$\mathfrak{f}$	on	$y-x$	
$\mathfrak{g}$	on	x^3+1	
$\mathfrak{h}(\mathfrak{f})$	on	$xy+\sqrt{4(y-x)}$	on määritelty, koska oletettiin $x+5<y$
$\mathfrak{h}(\mathfrak{g})$	on	$xy+\sqrt{4(x^3+1)}$	

- jollei vaadittaisi, että $\mathfrak{h}(\mathfrak{f})$ on määritelty, voitaisiin tiedosta $0=0$ valitsemalla $\mathfrak{h}(x)$:ksi $\frac{1}{x}$ johtaa $\frac{1}{0}=\frac{1}{0}$

Miksi [16] on pätevä?

- tarkastelemme mitä tahansa tilannetta, jossa $\mathfrak{h}(\mathfrak{f})$ tai $\mathfrak{h}(\mathfrak{g})$ on määritelty ja $\mathfrak{f} = \mathfrak{g}$
  - "tilanne" tarkoittaa muuttujien arvojen yhdistelmää
- $\mathfrak{f} = \mathfrak{g}$ tarkoittaa, että $\mathfrak{f}$ ja $\mathfrak{g}$ ovat määritellyt [13] ja tuottavat saman alkion

$\Rightarrow$ $\mathfrak{h}(x)$ saa $\mathfrak{h}(\mathfrak{f})$:ssä saman alkion x:ksi kuin $\mathfrak{h}(\mathfrak{g})$:ssä

$\Rightarrow$ $\mathfrak{h}(\mathfrak{f})$ tuottaa saman lopputuloksen kuin $\mathfrak{h}(\mathfrak{g})$

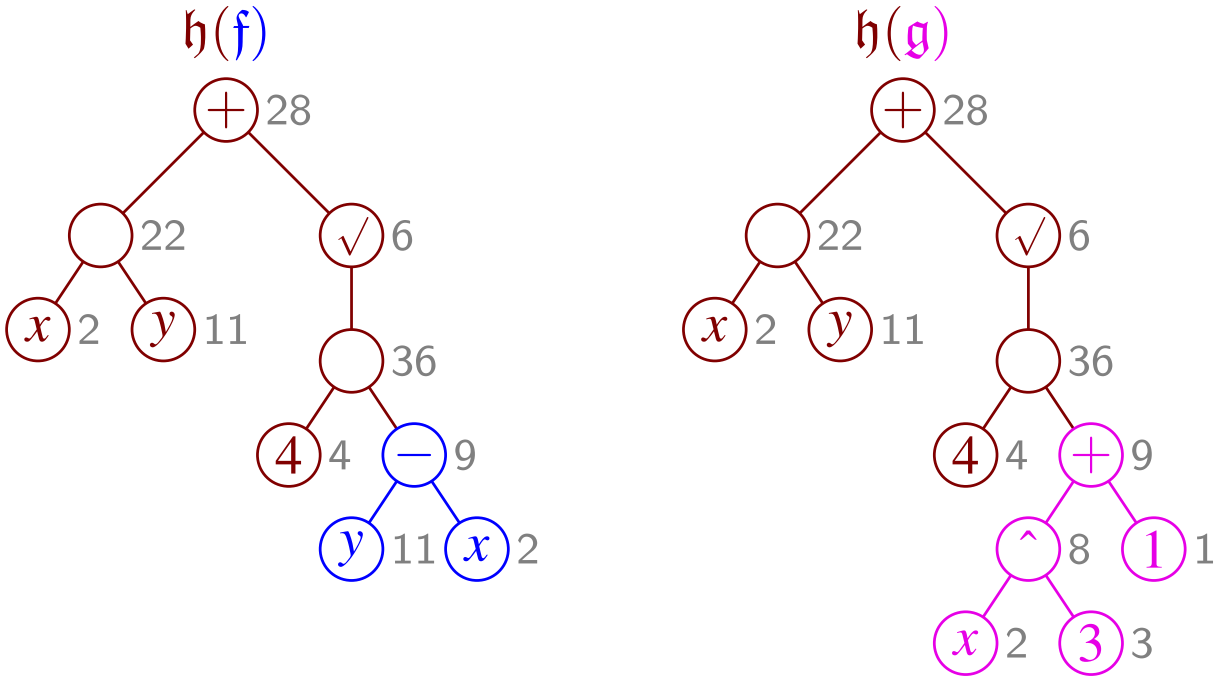
$\Rightarrow$ koska $\mathfrak{h}(\mathfrak{f})$:n tai $\mathfrak{h}(\mathfrak{g})$:n lopputulos on määritelty, pätee $\mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{g})$

Esimerkki

- $\mathfrak{f}$ on $y - x$, $\mathfrak{g}$ on $x^3 + 1$ ja $\mathfrak{h}(a) = xy + \sqrt{4a}$
- kun $x = 2$ ja $y = 11$, niin
  - $\mathfrak{f}$, $\mathfrak{g}$ ja $\mathfrak{h}(\mathfrak{f})$ tuottavat $11 - 2 = 9$, $2^3 + 1 = 9$ ja $2 \cdot 11 + \sqrt{4 \cdot 9} = 22 + \sqrt{36}$, joten $\mathfrak{h}(\mathfrak{f})$ on määritelty ja $\mathfrak{f} = \mathfrak{g}$

  $\Rightarrow$ sekä $\mathfrak{h}(\mathfrak{f})$ että $\mathfrak{h}(\mathfrak{g})$ laskevat $\mathfrak{h}(9)$ eli $2 \cdot 11 + \sqrt{4 \cdot 9}$
  - se on määritelty, koska $\mathfrak{h}(\mathfrak{f})$ on määritelty
  - se on yhtäsuuri itsensä kanssa
- samoin tapahtuu jokaisella x ja y, joilla $xy + \sqrt{4(y-x)}$ on määritelty ja $y - x = x^3 + 1$
- ei ole väliä mitä tapahtuu kun $x = -2$ ja $y = -9$, koska $xy + \sqrt{4(y-x)}$ ei silloin ole määritelty
- ei ole väliä mitä tapahtuu kun $x = 1$ ja $y = 1$, koska $y - x = x^3 + 1$ ei silloin toteudu

- tilanne $x = 2$ ja $y = 11$ kuvana



Sen muuttujan nimen, johon päättelysäännössä [16] sijoitetaan, saa valita vapaasti kunhan se ei sekaannu muihin muuttujiin

- siitä, että $x = 5$, voi johtaa $x^2 + 2x + 1 = x^2 + 2 \cdot 5 + 1$ sijoittamalla a:n tilalle x ja 5 lausekkeessa $x^2 + 2a + 1$ [16]
- jos kohdemuuttujan nimi ei olisi a vaan x, tulisi $x^2 + 2x + 1$ ja $5^2 + 2 \cdot 5 + 1$

Usein sen, että $\mathfrak{h}(\mathfrak{f})$ on määritelty, voi varmistaa jakamalla käsittely tapauksiin

- esim. yhtälöä $x^2 = x$ ratkaistaessa saa päätellä seuraavasti:
- jos $x \neq 0$, niin
  - $\frac{x^2}{x}$ on määritelty [14]

  $\Rightarrow$ jos $x^2 = x$, niin $\frac{x^2}{x} = \frac{x}{x}$ [16]
  - syistä, joihin ei mennä nyt, pätee jos $x \neq 0$ niin $x = \frac{x^2}{x}$ ja $\frac{x}{x} = 1$

  $\Rightarrow$ jos $x \neq 0$ ja $x^2 = x$, niin $x = \frac{x^2}{x} = \frac{x}{x} = 1$, joten $x = 1$
  - sijoittamalla on helppo tarkastaa, että jos $x = 1$, niin $x^2 = x$
- muussa tapauksessa $x = 0$, joten $x^2 = 0$ ja $x = 0$, joten $x^2 = x$
- niinpä $x^2 = x \;\Leftrightarrow\; x = 0 \vee x = 1$

Yhtäsuuruutena esitetyn lain soveltaminen

Jos $\mathfrak{h}_1, \ldots, \mathfrak{h}_n$ ovat määritellyt, niin laista $\mathfrak{f}(a_1, \ldots, a_n) = \mathfrak{g}(a_1, \ldots, a_n)$ saa johtaa kaavan $\mathfrak{f}(\mathfrak{h}_1, \ldots, \mathfrak{h}_n) = \mathfrak{g}(\mathfrak{h}_1, \ldots, \mathfrak{h}_n)$. [17]

- tarkastelemme mitä tahansa muuttujien arvojen yhdistelmää, jolla $\mathfrak{h}_1, \ldots, \mathfrak{h}_n$ ovat määritellyt
- koska $\mathfrak{h}_1, \ldots, \mathfrak{h}_n$ ovat määritellyt, kukin niistä tuottaa jonkin alkion
- se, että $\mathfrak{f}(a_1, \ldots, a_n) = \mathfrak{g}(a_1, \ldots, a_n)$ on laki, tarkoittaa, että aina kun $\mathfrak{f}$ saa argumenteikseen samat alkiot kuin $\mathfrak{g}$ saa, tuottaa $\mathfrak{f}$ tulokseekseen saman alkion kuin $\mathfrak{g}$ tuottaa
  - koska tuotos on alkio, ovat $\mathfrak{f}(a_1, \ldots, a_n)$ ja $\mathfrak{g}(a_1, \ldots, a_n)$ määritellyt
- koska $\mathfrak{f}$ tuottaa saman alkion kuin $\mathfrak{g}$ kun $a_1, \ldots, a_n$ ovat mitkä tahansa alkiot, se pätee myös kun $a_1, \ldots, a_n$ ovat ne alkiot, jotka $\mathfrak{h}_1, \ldots, \mathfrak{h}_n$ tuottavat

Esimerkiksi reaalilukujen laista $a + b = b + a$ voidaan päättelysäännöllä [17] johtaa $2x + 3 = 3 + 2x$ valitsemalla seuraavasti:

$\mathfrak{f}(a, b)$	on	$a + b$	
$\mathfrak{g}(a, b)$	on	$b + a$	
$\mathfrak{h}_a$	on	$2x$	on aina määritelty, koska kertolasku on aina määrit. [14]
$\mathfrak{h}_b$	on	3	on aina määritelty, koska siinä ei ole laskutoimituksia [14]
$\mathfrak{f}(\mathfrak{h}_a, \mathfrak{h}_b)$	on	$2x + 3$	
$\mathfrak{g}(\mathfrak{h}_a, \mathfrak{h}_b)$	on	$3 + 2x$	

Esimerkiksi reaalilukujen laista $0a = 0$ voidaan päättelysäännöllä [17] johtaa $0(x^2+1) = 0$ valitsemalla seuraavasti:

$\mathfrak{f}(a)$	on	$0a$	
$\mathfrak{g}(a)$	on	0	
$\mathfrak{h}$	on	x^2+1	on aina määritelty, koska a^2 ja $a+b$ ovat aina määr. [14]
$\mathfrak{f}(\mathfrak{h})$	on	$0(x^2+1)$	
$\mathfrak{g}(\mathfrak{h})$	on	0	

Päättelysäännölle [17] riittää, että $\mathfrak{h}_i$:t ovat määritellyt *mahdollisissa* tilanteissa

- esim. jos on oletettu, että $x \neq 0$, niin laista $0a = 0$ voidaan johtaa $0 \cdot \frac{1}{x} = 0$:
  - kuten edellä, $\mathfrak{f}(a)$ ja $\mathfrak{g}(a)$ ovat $0a$ ja 0
  - valitaan $\mathfrak{h}$:ksi $\frac{1}{x}$

  $\Rightarrow$ $\mathfrak{f}(\mathfrak{h})$ on $0 \cdot \frac{1}{x}$ ja $\mathfrak{g}(\mathfrak{h})$ on 0
- jollei vaadittaisi, että $\mathfrak{h}_i$:t ovat määritellyt, niin voitaisiin johtaa $0 \cdot \frac{1}{0} = 0$
  - nytkin käytetään lakia $0a = 0$, joten $\mathfrak{f}(a)$ ja $\mathfrak{g}(a)$ ovat kuten edellä
  - valitaan $\mathfrak{h}$:ksi $\frac{1}{0}$

  $\Rightarrow$ $\mathfrak{f}(\mathfrak{h})$ on $0 \cdot \frac{1}{0}$ ja $\mathfrak{g}(\mathfrak{h})$ on 0

Sen sijaan ei riitä, että $\mathfrak{f}(a_1,\ldots,a_n) = \mathfrak{g}(a_1,\ldots,a_n)$ on voimassa mahdollisissa tilanteissa

- vaikka $a \neq 0$ takaa $\frac{1}{a} = \frac{1}{a}$ ja $a-1$ on määritelty, ei $a \neq 0$ takaa $\frac{1}{a-1} = \frac{1}{a-1}$

Päättelysääntö [17] on suora seuraus päättelysäännöstä [12]

5 Kaavat

Atomikaava (*atomic formula*) voi olla viittä eri muotoa

- F, T tai U
- muotoa $\mathfrak{f} = \mathfrak{g}$ tai $\mathfrak{f} \neq \mathfrak{g}$
  - $\mathfrak{f}$ ja $\mathfrak{g}$ ovat lausekkeita
  - esim. $x^2 + 3x + 2 = 0$
- muotoa $P(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$
  - P on *relaatiosymboli* eli *predikaatti* ja n on sen paikkaluku ($n \in \mathbb{Z}^+$)
  - $\mathfrak{f}_1$, …, $\mathfrak{f}_n$ ovat lausekkeita
  - esim. $x^2 + 3x + 2 < 0$
  - esim. $\mathit{parisuhteessa}(\text{Archie})$
- muotoa X
  - X on propositiomuuttuja
  - sen tilalle voi sijoittaa kaavan
- muotoa $(\mathit{atomikaava})$
  - tehtävä on toisarvoinen: sallia turhat sulkeet

$=$ ja $\neq$ käsitellään erikseen muista relaatiosymboleista, koska

- ne ovat mielekkäitä kaikille puheenaiheille
- niillä on omia päättelysääntöjä

Käytettävissä olevat relaatiosymbolit (muut kuin $=$ ja $\neq$) riippuvat puheenaiheesta

- esim. luvussa 3 $\mathit{parisuhteessa}(x)$, $\mathit{sisarus}(x, y)$, ...
- esim. reaaliluvuilla $x \leq y$, $x < y$, ...

Eri puheenaiheilla on omia merkintätapoja relaatiosymbolien käytölle

- esim. luvussa 3 ei $\hookleftarrow(\mathfrak{f}, \mathfrak{g})$ vaan $\mathfrak{f} \hookleftarrow \mathfrak{g}$
- esim. reaaliluvuilla ei $\leq(\mathfrak{f}, \mathfrak{g})$ vaan $\mathfrak{f} \leq \mathfrak{g}$

Kaava on atomikaava tai mikä tahansa seuraavista muodoista:

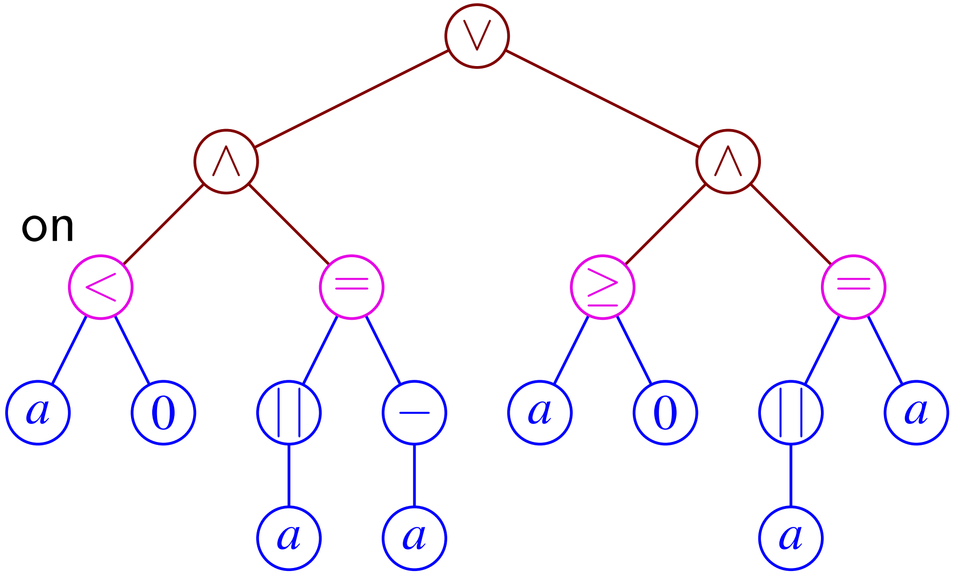
$$(\varphi) \qquad \neg\varphi \qquad \varphi \wedge \psi \qquad \varphi \vee \psi \qquad \varphi \rightarrow \psi \qquad \varphi \leftrightarrow \psi \qquad \forall x : \varphi \qquad \exists x : \varphi$$

- $\varphi \rightarrow \psi$ ja $\varphi \leftrightarrow \psi$ esitellään sivulla 87
- $\forall x : \varphi$ ja $\exists x : \varphi$ esitellään luvussa 11
- kaavan muuttujat saavat puheenaiheen alkioita ja kaavat tuottavat totuusarvoja
  - (kaavan tavalliset muuttujat, nyt ei puhuta propositiomuuttujista)
  - esim. luvussa 3 muuttujat saivat arvoikseen ihmisiä
  - esim. monessa muussa esimerkissä muuttujat saavat arvoikseen reaalilukuja
- (tavalliset) muuttujat eivät koskaan saa arvokseen ”määrittelemätön”
  - lausekkeet voivat olla määrittelemättömiä, muuttujat eivät voi
- kaavan propositiomuuttujat saavat arvoikseen totuusarvoja
  - mahdollisissa tilanteissa ei kuitenkaan totuusarvoa U
- jos jokainen funktiosymboli on aina määritelty ja jos kaavaa U ei käytetä, niin mikään kaava ei tuota U
  - logiikka on silloin kaksiarvoinen
  - esim. reaaliluvut niin että laskutoimituksina on vain $+$ ja $\cdot$
  - esim. pelkällä propositiologiikalla mallinnetut asetelmat

Esimerkki: itseisarvon määritelmä

Jokaisella reaaliluvulla a pätee $a < 0 \wedge |a| = -a \vee a \geq 0 \wedge |a| = a$. [18]

- tarkoittaa samaa kuin että
  - jos $a \geq 0$ niin $|a| = a$, ja
  - jos $a < 0$ niin $|a| = -a$



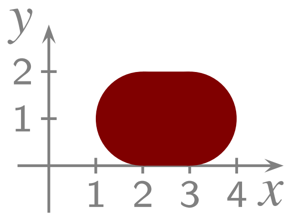
- kaavassa $a < 0 \wedge |a| = -a \vee a \geq 0 \wedge |a| = a$ on
  - 1 vakiosymboli: 0, yhteensä 2 esiintymää
  - 1 muuttujasymboli: a, yhteensä 6 esiintymää
  - 2 eri yksipaikkaista funktiosymbolia: $|\ |$ ja $-$, yhteensä 3 esiintymää
  - 4 eri lauseketta: a, 0, $|a|$, ja $-a$, yhteensä 11 esiintymää
  - 3 eri relaatiosymbolia: $<$, $=$ ja $\geq$, yhteensä 4 esiintymää
  - 4 eri atomikaavaa: $a < 0$, $|a| = -a$, $a \geq 0$ ja $|a| = a$
  - 3 eri muuta kaavaa: $a < 0 \wedge |a| = -a$, $a \geq 0 \wedge |a| = a$ ja koko alkuperäinen kaava

Kaava esittää (täyden) funktion puheenaiheen alkiomonikoilta totuusarvoille

- koska $\mathit{vanhA}(\text{Harry}) = \text{Charles}$, $\mathit{puoliso}(\text{Charles}) = \text{Camilla}$ ja $\mathit{puoliso}(\text{Diana})$ ei ole määritelty, saamme

x	Archie	Lilibet	Harry	...
$\mathit{puoliso}(\mathit{vanhA}(x)) = \mathit{vanhB}(x)$	T	T	F	...
$\mathit{vanhA}(x) = \mathit{puoliso}(\mathit{vanhB}(x))$	T	T	U	...

- jos piste (x, y) on kuvan ruskealla alueella, niin seuraava kaava tuottaa T, ja muutoin se tuottaa F:
  $(x-2)^2 + (y-1)^2 \leq 1 \vee (x-3)^2 + (y-1)^2 \leq 1 \vee 2 < x < 3 \wedge 0 \leq y \leq 2$



Lausekkeen sijoittaminen muuttujan tilalle kaavassa

- merkinnöillä $\varphi(x)$ ja $\varphi(\mathfrak{f})$ esitetään $\mathfrak{f}$:n sijoittaminen x:n tilalle kaavassa φ
- esim. jos $\varphi(x, y)$ on $\mathit{sisarus}(\mathit{puoliso}(x), y)$ ja $\mathfrak{f}$ on $\mathit{vanhA}(\text{Lilibet})$ ja $\mathfrak{g}$ on William, niin $\varphi(\mathfrak{f}, \mathfrak{g})$ on $\mathit{sisarus}(\mathit{puoliso}(\mathit{vanhA}(\text{Lilibet})), \text{William})$
- esim. jos $\varphi(a)$ on

  $$a < 0 \wedge |a| = -a \vee a \geq 0 \wedge |a| = a$$

  ja $\mathfrak{f}$ on $x^2 - 2$, niin $\varphi(\mathfrak{f})$ on

  $$x^2 - 2 < 0 \wedge |x^2 - 2| = -(x^2 - 2) \vee x^2 - 2 \geq 0 \wedge |x^2 - 2| = x^2 - 2$$

Yhtäsuuren sijoittaminen kaavaan

Jos $\mathfrak{f} = \mathfrak{g}$ tai sekä $\mathfrak{f}$ että $\mathfrak{g}$ on määrittelemätön, ja jos φ ei sisällä symboleita $\forall$ ja $\exists$, niin $\varphi(\mathfrak{f}) \Leftrightarrow \varphi(\mathfrak{g})$. [19]

- kun $\mathfrak{f} = \mathfrak{g}$, saa φ argumentikseen $\varphi(\mathfrak{f})$:ssä saman alkion kuin $\varphi(\mathfrak{g})$:ssä, joten se tuottaa saman totuusarvon
- kun sekä $\mathfrak{f}$ että $\mathfrak{g}$ on määrittelemätön, saa sekä $\varphi(\mathfrak{f})$ että $\varphi(\mathfrak{g})$ argumentikseen määrittelemättömän lausekkeen, joten ne tuottavat saman totuusarvon
- nytkin riittää, että jokaisessa *mahdollisessa* tilanteessa $\mathfrak{f} = \mathfrak{g}$ tai sekä $\mathfrak{f}$ että $\mathfrak{g}$ on määrittelemätön
- ehto, että φ ei saa sisältää $\forall$ ja $\exists$, korvataan lievemmällä luvussa 11

Esimerkiksi siitä, että $3x-2(2x-3) = 3x-4x+6$, voidaan päättelysäännöllä [19] johtaa

$$y = 2x-3 \land 3x-2(2x-3) = 2 \;\Leftrightarrow\; y = 2x-3 \land 3x-4x+6 = 2$$

valitsemalla seuraavasti:

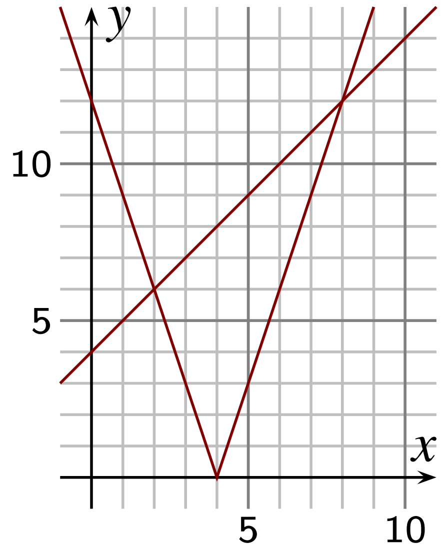
$\varphi(a)$	on	$y = 2x-3 \land a = 2$	
$\mathfrak{f}$	on	$3x-2(2x-3)$	on aina määritelty [14]
$\mathfrak{g}$	on	$3x-4x+6$	on aina määritelty [14]
$\varphi(\mathfrak{f})$	on	$y = 2x-3 \land 3x-2(2x-3) = 2$	
$\varphi(\mathfrak{g})$	on	$y = 2x-3 \land 3x-4x+6 = 2$	

Esimerkiksi siitä, että kun $x \geq 0$ pätee $\sqrt{4x} = 2\sqrt{x}$, voidaan johtaa $\sqrt{4x} = 6 \Leftrightarrow 2\sqrt{x} = 6$

- kun $x < 0$, ovat sen molemmat puolet määrittelemättömät

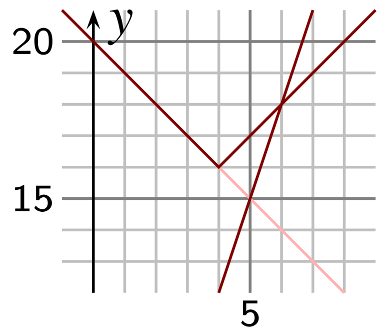
Esimerkiksi $3|x-4| = x+4$ voidaan ratkaista seuraavasti:

- joko $x < 4 \wedge |x-4| = -(x-4)$ tai $x \geq 4 \wedge |x-4| = x-4$ [18]
- jos $x < 4$, niin $|x-4| = -(x-4)$, joten [19]
  $3|x-4| = x+4 \Leftrightarrow 3(-(x-4)) = x+4 \Leftrightarrow -3x+12 = x+4 \Leftrightarrow x = 2$
- jos $x \geq 4$, niin $|x-4| = x-4$, joten [19]
  $3|x-4| = x+4 \Leftrightarrow 3(x-4) = x+4 \Leftrightarrow 3x-12 = x+4 \Leftrightarrow x = 8$
- tapauksista yhteensä saadaan $x < 4 \wedge x = 2 \vee x \geq 4 \wedge x = 8 \Leftrightarrow x = 2 \vee x = 8$
- kaiken kaikkiaan $3|x-4| = x+4 \Leftrightarrow x = 2 \vee x = 8$



Esimerkiksi $|x-4|+16=3x$ voidaan ratkaista seuraavasti:

- joko $x<4 \land |x-4| = -(x-4)$ tai $x \geq 4 \land |x-4| = x-4$ [18]
- jos $x<4$, niin $|x-4| = -(x-4)$, joten [19]
  $|x-4|+16=3x \;\Leftrightarrow\; -(x-4)+16=3x \;\Leftrightarrow\; 20=4x \;\Leftrightarrow\; x=5$
- jos $x \geq 4$, niin $|x-4| = x-4$, joten [19]
  $|x-4|+16=3x \;\Leftrightarrow\; x-4+16=3x \;\Leftrightarrow\; 12=2x \;\Leftrightarrow\; x=6$
- tapauksista yhteensä saadaan $x<4 \land x=5 \lor x \geq 4 \land x=6 \;\Leftrightarrow\; \mathsf{F} \lor x=6 \;\Leftrightarrow\; x=6$
- kaiken kaikkiaan $|x-4|+16=3x \;\Leftrightarrow\; x=6$



Melko vaatimattomalta vaikuttava päättelysääntö

Jos $\mathfrak{f}$ on määritelty, niin $\mathfrak{f} = \mathfrak{f}$. [20]

Päättelysäännöillä [2], [19] ja [20] voidaan johtaa [16]:n ensimmäinen osa seuraavasti

- jos $\mathfrak{h}(\mathfrak{f})$ on määritelty, niin $\mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{f})$ [20]
- valitaan $\varphi(x)$:ksi $\mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(x)$
- jos lisäksi $\mathfrak{f} = \mathfrak{g}$, niin $\varphi(\mathfrak{f}) \Leftrightarrow \varphi(\mathfrak{g})$ eli $\mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{f}) \Leftrightarrow \mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{g})$ [19]

$\Rightarrow$ jos $\mathfrak{h}(\mathfrak{f})$ on määritelty ja $\mathfrak{f} = \mathfrak{g}$, niin $\mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{g})$ [2]

Toinen osa voidaan johtaa $=$:n symmetrisyydellä [15] ensimmäisestä seuraavasti

- jos $\mathfrak{f} = \mathfrak{g}$ niin $\mathfrak{g} = \mathfrak{f}$ [15]
- jos lisäksi $\mathfrak{h}(\mathfrak{g})$ on määritelty, niin [16]:n ensimmäisen osan nojalla $\mathfrak{h}(\mathfrak{g}) = \mathfrak{h}(\mathfrak{f})$

$\Rightarrow$ $\mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{g})$ [15]

Toinen osa voidaan johtaa ilman $=$:n symmetrisyyttä seuraavasti

- jos $\mathfrak{h}(\mathfrak{g})$ on määritelty, niin $\mathfrak{h}(\mathfrak{g}) = \mathfrak{h}(\mathfrak{g})$ [20]
- valitaan $\varphi(x)$:ksi $\mathfrak{h}(x) = \mathfrak{h}(\mathfrak{g})$
- jos lisäksi $\mathfrak{f} = \mathfrak{g}$, niin $\varphi(\mathfrak{f}) \Leftrightarrow \varphi(\mathfrak{g})$ eli $\varphi(\mathfrak{g}) \Leftrightarrow \varphi(\mathfrak{f})$ [2]
  eli $\mathfrak{h}(\mathfrak{g}) = \mathfrak{h}(\mathfrak{g}) \Leftrightarrow \mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{g})$ [19]

$\Rightarrow$ jos $\mathfrak{h}(\mathfrak{g})$ on määritelty ja $\mathfrak{f} = \mathfrak{g}$, niin $\mathfrak{h}(\mathfrak{f}) = \mathfrak{h}(\mathfrak{g})$ [2]

Kaavan sisältämän yhtäsuuruuden soveltaminen

Jos φ ei sisällä symboleita $\forall$ ja $\exists$, niin $\mathfrak{f} = \mathfrak{g} \land \varphi(\mathfrak{f}) \;\Leftrightarrow\; \mathfrak{f} = \mathfrak{g} \land \varphi(\mathfrak{g})$. [21]

- kun $\mathfrak{f} = \mathfrak{g}$ tuottaa F, tuottaa [21]:n $\Leftrightarrow$:n kumpikin puoli F
- kun $\mathfrak{f} = \mathfrak{g}$ tuottaa U, tuottaa [21]:n $\Leftrightarrow$:n kumpikin puoli enintään U [9]
- kun $\mathfrak{f} = \mathfrak{g}$ tuottaa T, saa φ saman alkion argumentikseen sekä $\varphi(\mathfrak{f})$:ssä että $\varphi(\mathfrak{g})$:ssä, joten se tuottaa saman tuloksen, joka on samalla $\Leftrightarrow$:n kummankin puolen totuusarvo
- nytkin $\forall$:n ja $\exists$:n kielto korvataan lievemmällä ehdolla luvussa 11
- [21] on melkein sama kuin [19], mutta "$\mathfrak{f} = \mathfrak{g}$" on kaavassa eikä taustalla oletuksena
  - toisinaan [21] on kätevämpi esim. yhtälöryhmien ratkaisemisessa

Päättelysäännöllä [21] voidaan esimerkiksi johtaa

$$\begin{aligned} & y = 2x - 3 \land 3x - 2y = 2 \\ \Leftrightarrow \quad & y = 2x - 3 \land 3x - 2(2x - 3) = 2 \end{aligned}$$

valitsemalla seuraavasti:

$\mathfrak{f}$	on	y
$\mathfrak{g}$	on	$2x - 3$
$\varphi(a)$	on	$3x - 2a = 2$
$\varphi(\mathfrak{f})$	on	$3x - 2y = 2$
$\varphi(\mathfrak{g})$	on	$3x - 2(2x - 3) = 2$

Propositiologiikan kaavan käyttäminen

- koska φ, ψ jne. edustavat mielivaltaisia kaavoja, saa niiden tilalle laittaa mielivaltaiset kaavat
- esimerkiksi propositiologiikan laista [5] eli $\varphi \wedge \psi \Leftrightarrow \psi \wedge \varphi$ voidaan johtaa

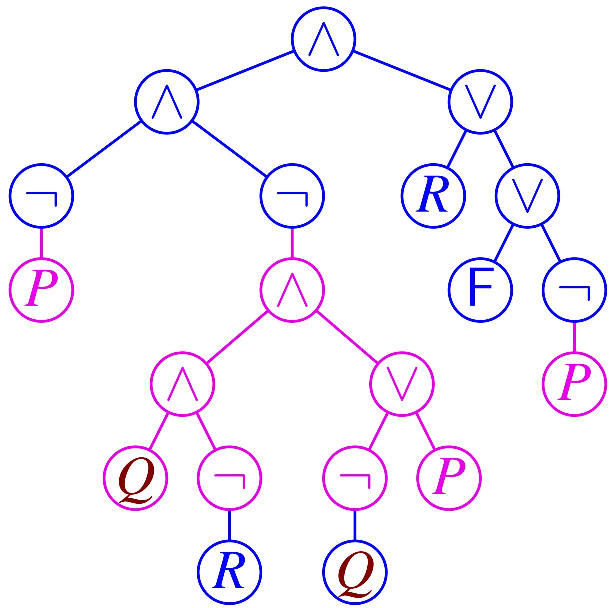
$$x^2 - 2 < 0 \wedge |x^2 - 2| = -(x^2 - 2) \Leftrightarrow |x^2 - 2| = -(x^2 - 2) \wedge x^2 - 2 < 0$$

valitsemalla seuraavasti:

φ	on	$x^2 - 2 < 0$
ψ	on	$\lvert x^2 - 2\rvert = -(x^2 - 2)$
$\varphi \wedge \psi$	on	$x^2 - 2 < 0 \wedge \lvert x^2 - 2\rvert = -(x^2 - 2)$
$\psi \wedge \varphi$	on	$\lvert x^2 - 2\rvert = -(x^2 - 2) \wedge x^2 - 2 < 0$

Parillisen ja parittoman määrän ¬:a alaisuudessa oleminen

- $(\neg P \wedge \neg((Q \wedge \neg R) \wedge (\neg Q \vee P))) \wedge (R \vee (\mathsf{F} \vee \neg P))$
- R on vain parillisen määrän alaisuudessa
- P on vain parittoman määrän alaisuudessa
- Q on sekä parillisen että parittoman määrän alaisuudessa



Kaavan sijoittaminen propositiomuuttujan tilalle kaavassa, sääntö 1

- merkinnöillä $\varphi(X)$ ja $\varphi(\psi)$ esitetään ψ:n sijoittaminen X:n tilalle kaavassa φ

  Jos $\psi \Leftrightarrow \chi$ ja jos X ei ole $\varphi(X)$:ssä muiden symbolien alaisuudessa kuin $\land$, $\lor$ ja parillinen määrä symbolia $\neg$, niin $\varphi(\psi) \Leftrightarrow \varphi(\chi)$. [22]

- saamme tämän todistamiseen riittävän keinon vasta sivulla 128
  - vaikeutena on sulkea pois mahdollisuus, että $\varphi(\mathrm{U})$ tuottaa T mutta $\varphi(\mathrm{F})$ ei tuota

Esimerkiksi sivulla 46 johdetusta

$$vanhA(x) = vanhA(y) \;\Leftrightarrow\; vanhA(y) = vanhA(x)$$

voidaan päättelysäännöllä [22] johtaa

$$\begin{aligned} & vanhA(x) = vanhA(y) \land vanhB(x) = vanhB(y) \land x \neq y \\ \Leftrightarrow\; & vanhA(y) = vanhA(x) \land vanhB(x) = vanhB(y) \land x \neq y \end{aligned}$$

valitsemalla seuraavasti:

$$\begin{array}{lll} \varphi(X) & \text{on} & X \land vanhB(x) = vanhB(y) \land x \neq y \\ \psi & \text{on} & vanhA(x) = vanhA(y) \\ \chi & \text{on} & vanhA(y) = vanhA(x) \\ \varphi(\psi) & \text{on} & vanhA(x) = vanhA(y) \land vanhB(x) = vanhB(y) \land x \neq y \\ \varphi(\chi) & \text{on} & vanhA(y) = vanhA(x) \land vanhB(x) = vanhB(y) \land x \neq y \end{array}$$

- toistamalla sama keski- ja loppuosalle saadaan sivulla 32 käytetty yhtäpitävyys

Symmetria	F	U	T	¬	∧	∨	∀	∃
	T	U	F	¬	∨	∧	∃	∀

- jos kaavassa ei ole muuta kuin atomikaavoja ja taulukon symboleita, niin jos kaavan symbolit ja atomikaavojen totuusarvot vaihdetaan taulukon mukaisesti, niin myös kaavan tuottama totuusarvo vaihtuu taulukon mukaisesti [7,95]
- kolmiarvologiikassa $\Leftrightarrow$ ei säilytä tätä symmetriaa, koska U $\Leftrightarrow$ F mutta ei ¬U $\Leftrightarrow$ ¬F
- melko pian esiteltävä $\equiv$ säilyttää symmetrian

Kaavan sijoittaminen propositiomuuttujan tilalle kaavassa, sääntö 2

Jos $\psi \Leftrightarrow \chi$, jos ψ ja χ tuottavat U vain yhtäaikaa, ja jos φ ei sisällä symboleita $\forall$ ja $\exists$, niin $\varphi(\psi) \Leftrightarrow \varphi(\chi)$, ja $\varphi(\psi)$ ja $\varphi(\chi)$ tuottavat U vain yhtäaikaa.

- missä tahansa mahdollisessa tilanteessa ψ ja χ tuottavat saman totuusarvon
  $\Rightarrow$ φ saa siinä saman argumentin $\varphi(\psi)$:ssä kuin $\varphi(\chi)$:ssä
  $\Rightarrow$ $\varphi(\psi)$ ja $\varphi(\chi)$ tuottavat saman totuusarvon

Yllä olevassa säännössä todellakin täytyy vaatia että U tuotetaan vain yhtäaikaa

- muutoin valitsemalla $\varphi(X)$:ksi $\neg X$ voitaisiin siitä, että U $\Leftrightarrow$ F, johtaa U $\Leftrightarrow$ T seuraavasti: U $\Leftrightarrow$ ¬U $\Leftrightarrow$ ¬F $\Leftrightarrow$ T

$\lceil\ \rfloor$:n yleistäminen kaavoihin

- sivulla 41 asetettiin vaatimus, että jokaisella funktiosymbolilla f on oltava kaava $\lceil f \rfloor$, joka tuottaa T kun f on määritelty ja F muulloin
  $\Rightarrow$ ei koskaan tuota U
- sivulla 42 se yleistettiin lausekkeisiin periaatteen [14] mukaisesti
  - lauseke on määrittelemätön jos ja vain jos se sisältää määrittelemättömän laskutoimituksen
- nyt se yleistetään kaavoihin siten, että $\lceil \varphi \rfloor$ tuottaa F kun φ tuottaa U, ja muulloin $\lceil \varphi \rfloor$ tuottaa T (eli kun φ tuottaa T tai F)
  $\Rightarrow$ ei koskaan tuota U
- tietenkin $\lceil \mathrm{F} \rfloor \Leftrightarrow \lceil \mathrm{T} \rfloor \Leftrightarrow \mathrm{T}$ ja $\lceil \mathrm{U} \rfloor \Leftrightarrow \mathrm{F}$
- $\lceil \mathfrak{f} = \mathfrak{g} \rfloor \;\Leftrightarrow\; \lceil \mathfrak{f} \neq \mathfrak{g} \rfloor \;\Leftrightarrow\; \lceil \mathfrak{f} < \mathfrak{g} \rfloor \;\Leftrightarrow\; \ldots \;\Leftrightarrow\; \lceil \mathfrak{f} \rfloor \wedge \lceil \mathfrak{g} \rfloor$ [13]
- $\lceil P(\mathfrak{f}_1, \ldots, \mathfrak{f}_n) \rfloor \;\Leftrightarrow\; \lceil \mathfrak{f}_1 \rfloor \wedge \cdots \wedge \lceil \mathfrak{f}_n \rfloor$ [13]
- jos X on propositiomuuttuja, niin mahdollisissa tilanteissa $\lceil X \rfloor \Leftrightarrow \mathrm{T}$ [10]
- $\lceil \neg\varphi \rfloor \;\Leftrightarrow\; \lceil \varphi \rfloor$ [9]
- $\lceil \varphi \wedge \psi \rfloor \;\Leftrightarrow\; \lceil \varphi \rfloor \wedge \lceil \psi \rfloor \vee \lceil \varphi \rfloor \wedge \neg\varphi \vee \lceil \psi \rfloor \wedge \neg\psi$ [9]
  - $\lceil \varphi \rfloor \wedge \neg\varphi$ eikä $\neg\varphi$, jotta kaava ei koskaan tuottaisi U
- $\lceil \varphi \vee \psi \rfloor$ harjoitustehtäväksi
- $\lceil\ \rfloor$ ei ole logiikan vaan metakielen symboli
  - ei ota ja tuota totuusarvoa, vaan ottaa ja tuottaa kaavan

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

Yhtätotuus $\equiv$

- sivun 65 sääntö sisältää kahdesti samankaltaisen melko pitkän ilmauksen

  Jos $\psi \Leftrightarrow \chi$, jos ψ ja χ tuottavat U vain yhtäaikaa, ja jos φ ei sisällä symboleita $\forall$ ja $\exists$, niin $\varphi(\psi) \Leftrightarrow \varphi(\chi)$, ja $\varphi(\psi)$ ja $\varphi(\chi)$ tuottavat U vain yhtäaikaa.

$\Rightarrow$ jotta jatkossa ei tarvitsisi kirjoittaa yhtä kömpelösti,
otamme käyttöön uuden merkinnän

  Vasen $\equiv$ *oikea* tarkoittaa, että jokaisessa mahdollisessa tilanteessa *vasen* ja *oikea* saavat saman totuusarvon. [23]

- $\equiv$:n ja $\Leftrightarrow$:n ero on, että $\Leftrightarrow$ sallii mutta $\equiv$ ei salli toisen puolen tuottaa F ja toisen U
  - kaksiarvologiikassa $\equiv$ ja $\Leftrightarrow$ tarkoittavat samaa
- molemmat tarvitaan
  - $\equiv$ on informatiivisempi, joillekin säännöille välttämätön ja ehkä luontevampikin
  - $\Leftrightarrow$ tarvitaan mm. ilmaisemaan yhtälöiden ratkaisuja, kuten

    $$3\sqrt{x-1} = x+1 \;\Leftrightarrow\; x = 2 \vee x = 5$$

  - kun $x = 0$, $3\sqrt{x-1} = x+1$ tuottaa U mutta $x = 2 \vee x = 5$ tuottaa F, joten $\equiv$ ei toimi
- $\equiv$ ei ole melkein missään muualla kuin tässä kurssissa käytössä tässä merkityksessä
  - kolmiarvologiikkaa käytetään vähän, päättelyoperaattoreiden kanssa hyvin vähän
  - $\equiv$ on toisinaan käytössä kaksiarvologiikassa kuten $\Leftrightarrow$ tai $\leftrightarrow$ [sivu 87]

Yhtätotuuden päättelysääntöjä

jos on päätelty	ja	niin saa päätellä	ja	ja	
$\varphi \equiv \psi$		$\psi \equiv \varphi$			
$\varphi_1 \equiv \varphi_2 \equiv \ldots \equiv \varphi_n$		$\varphi_1 \equiv \varphi_n$			
		$\varphi \equiv \varphi$			[24]
$\varphi \equiv \psi$		$\varphi \Leftrightarrow \psi$	$\neg\varphi \Leftrightarrow \neg\psi$	$\lceil\varphi\rfloor \Leftrightarrow \lceil\psi\rfloor$	
$\varphi \Leftrightarrow \psi$	$\neg\varphi \Leftrightarrow \neg\psi$	$\varphi \equiv \psi$			
$\varphi \Leftrightarrow \psi$	$\lceil\varphi\rfloor \Leftrightarrow \lceil\psi\rfloor$	$\varphi \equiv \psi$			

- $\Leftrightarrow$-säännöt [3,15,19] pätevät myös $\equiv$:lle

  $\varphi \equiv$ T jos ja vain jos jokaisessa mahdollisessa tilanteessa φ tuottaa T.

  Jos $\mathfrak{f}$ ja $\mathfrak{g}$ ovat mitkä tahansa lausekkeet, niin $\mathfrak{f} = \mathfrak{g} \ \equiv \ \mathfrak{g} = \mathfrak{f}$. [25]

  Jos $\mathfrak{f} = \mathfrak{g}$ tai sekä $\mathfrak{f}$ että $\mathfrak{g}$ on määrittelemätön, ja jos φ ei sisällä symboleita $\forall$ ja $\exists$, niin $\varphi(\mathfrak{f}) \equiv \varphi(\mathfrak{g})$.

- [21] ei: Jos φ ei sisällä symboleita $\forall$ ja $\exists$, niin $\mathfrak{f} = \mathfrak{g} \wedge \varphi(\mathfrak{f}) \ \Leftrightarrow \ \mathfrak{f} = \mathfrak{g} \wedge \varphi(\mathfrak{g})$.
  - vastaesimerkki: jos $\varphi(a)$ on $a < 0$, $\mathfrak{f}$ on $\frac{0}{0}$ ja $\mathfrak{g}$ on 1, niin saadaan

    U $\equiv$ $\frac{0}{0} = 1 \wedge \frac{0}{0} < 0 \ \Leftrightarrow \ \frac{0}{0} = 1 \wedge 1 < 0$ $\equiv$ F

Nyt sivun 65 sääntö voidaan kirjoittaa näppärämmin

Jos $\psi \equiv \chi$ ja φ ei sisällä symboleita $\forall$ ja $\exists$, niin $\varphi(\psi) \equiv \varphi(\chi)$. [26]

Nämä propositiologiikan $\Leftrightarrow$-lait pätevät myös $\equiv$:lle

$$
\begin{array}{rclrclrcl}
\varphi \wedge \mathsf{F} & \equiv & \mathsf{F} & \neg\neg\varphi & \equiv & \varphi & \varphi \wedge (\varphi \vee \psi) & \equiv & \varphi \\
\varphi \vee \mathsf{T} & \equiv & \mathsf{T} & & & & \varphi \vee (\varphi \wedge \psi) & \equiv & \varphi \\
\varphi \wedge \mathsf{T} & \equiv & \varphi & \varphi \wedge \psi & \equiv & \psi \wedge \varphi & \varphi \wedge (\psi \wedge \chi) & \equiv & (\varphi \wedge \psi) \wedge \chi \\
\varphi \vee \mathsf{F} & \equiv & \varphi & \varphi \vee \psi & \equiv & \psi \vee \varphi & \varphi \vee (\psi \vee \chi) & \equiv & (\varphi \vee \psi) \vee \chi \\
\varphi \wedge \varphi & \equiv & \varphi & \neg(\varphi \wedge \psi) & \equiv & \neg\varphi \vee \neg\psi & \varphi \wedge (\psi \vee \chi) & \equiv & (\varphi \wedge \psi) \vee (\varphi \wedge \chi) \\
\varphi \vee \varphi & \equiv & \varphi & \neg(\varphi \vee \psi) & \equiv & \neg\varphi \wedge \neg\psi & \varphi \vee (\psi \wedge \chi) & \equiv & (\varphi \vee \psi) \wedge (\varphi \vee \chi)
\end{array}
\quad [27]
$$

- sivulla 129 esitettävä [58] kertoo, miten ne voi todistaa helposti siitä, että ne $\Leftrightarrow$-pätevät

On (vain) neljä tärkeää 2-arvoisen propositiologiikan lakia, jotka eivät $\equiv$-päde 3-arvoisessa propositiologiikassa

- $\varphi \vee \neg\varphi \Leftrightarrow \mathsf{T}$
  - kolmannen poissuljetun laki sanoo että kolmatta totuusarvoa ei ole

  $\Rightarrow$ ei tietenkään edes $\Leftrightarrow$-päde, $\mathsf{U} \vee \neg\mathsf{U} \equiv \mathsf{U}$
- $\varphi \wedge \neg\varphi \Leftrightarrow \mathsf{F}$
  - ristiriidattomuuden laki $\Leftrightarrow$-pätee, $\mathsf{U} \wedge \neg\mathsf{U} \equiv \mathsf{U}$
- $\varphi \wedge (\neg\varphi \vee \psi) \ \Leftrightarrow\ \varphi \wedge \psi$
  - jos $\varphi \equiv \mathsf{U}$ ja $\psi \equiv \mathsf{F}$, niin $\varphi \wedge (\neg\varphi \vee \psi) \equiv \mathsf{U}$ ja $\varphi \wedge \psi \equiv \mathsf{F}$
- $\varphi \vee (\neg\varphi \wedge \psi) \ \Leftrightarrow\ \varphi \vee \psi$

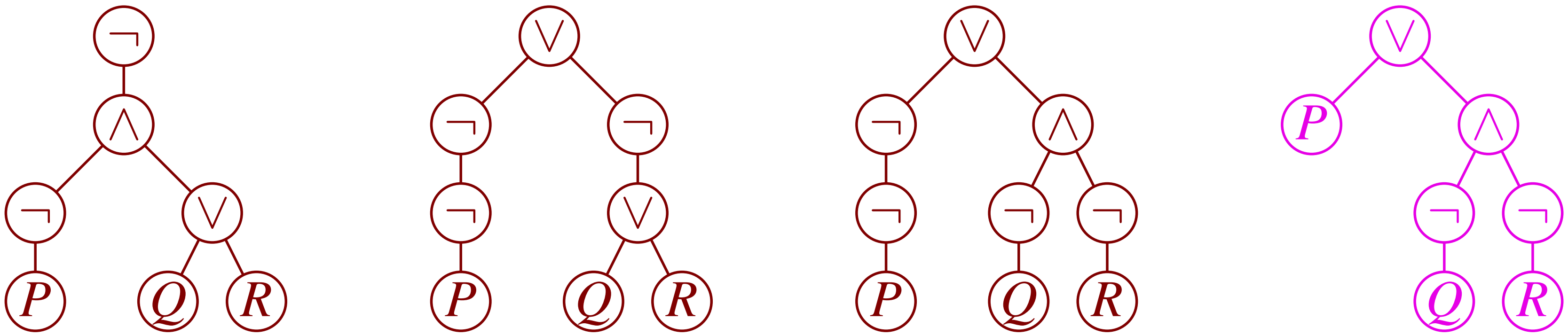
$\varphi \wedge (\neg\varphi \vee \psi)$ toimii kuten monien ohjelmointikielten `eka && toka`

- jos $\varphi \equiv \mathsf{F}$, niin $\varphi \wedge (\neg\varphi \vee \psi) \equiv \mathsf{F}$
  - jos `eka` tuottaa `false`, niin `toka` ei lasketa vaan palautetaan `false`
- jos $\varphi \equiv \mathsf{T}$, niin $\varphi \wedge (\neg\varphi \vee \psi) \equiv \psi$
  - jos `eka` tuottaa `true`, niin lasketaan `toka` ja palautetaan se minkä `toka` tuottaa
  - jos tällöin `toka` kaatuu, niin `eka && toka` kaatuu
- jos $\varphi \equiv \mathsf{U}$, niin $\varphi \wedge (\neg\varphi \vee \psi) \equiv \mathsf{U}$
  - jos `eka` kaatuu, niin `eka && toka` kaatuu

$\varphi \vee (\neg\varphi \wedge \psi)$ toimii kuten monien ohjelmointikielten `eka || toka`

Negaatioiden painaminen alas

- tarkastellaan mitä tahansa kaavaa muotoa $\neg\varphi$, jossa ei esiinny muuta kuin atomikaavoja ja symboleita $\neg$, $\wedge$ ja $\vee$ (ja sulkeita)
- De Morganin laeilla voidaan osoittaa, että se säilyy yhtätotena seuraavassa muunnoksessa (sulkeita voidaan joutua lisäämään):
  - ylin $\neg$ poistetaan
  - jokainen $\wedge$ korvataan $\vee$:lla ja päinvastoin
  - jokaisen atomikaavan eteen lisätään $\neg$



- siis $\neg\, kaava^{\wedge}(\varphi_1, \ldots, \varphi_n) \equiv kaava_{\vee}(\neg\varphi_1, \ldots, \neg\varphi_n)$, missä
  - φ_1, . . . , φ_n ovat atomikaavoja
  - $kaava_{\vee}$ saadaan kaavasta $kaava^{\wedge}$ vaihtamalla $\wedge$ ja $\vee$ toisikseen

Mikä tahansa kaava, jossa esiintyy vain edellä mainittuja symboleita, voidaan muuttaa yhtätodeksi kaavaksi, jossa kunkin $\neg$:n alaisuudessa on vain atomikaava

- tehdään edellä mainittu muunnos jokaiselle osakaavalle
  $\neg\varphi$, jossa on muutakin kuin atomikaavoja ja $\neg$:ta
  $\Rightarrow$ kunkin $\neg$:n alaisuudessa on vain nolla tai useampi $\neg$ sekä atomikaava
- poistetaan jokainen $\neg\neg$
- lisäksi atomikaavoja voi tietenkin muokata seuraavasti:
  $\neg\mathsf{F} \equiv \mathsf{T}$ $\neg\mathsf{U} \equiv \mathsf{U}$ $\neg\mathsf{T} \equiv \mathsf{F}$ $\neg(\mathfrak{f} = \mathfrak{g}) \equiv \mathfrak{f} \neq \mathfrak{g}$ $\neg(\mathfrak{f} \neq \mathfrak{g}) \equiv \mathfrak{f} = \mathfrak{g}$ $\neg(\mathfrak{f} \leq \mathfrak{g}) \equiv \mathfrak{f} > \mathfrak{g}$ ...

Yhtätotena säilymisen perustelu käy läpi eri kaavamuodot (rakenteellinen induktio)

- $$\begin{aligned} & \neg(vasen^{\wedge}(\varphi_1,\ldots,\varphi_n) \wedge oikea^{\wedge}(\varphi_1,\ldots,\varphi_n)) & \\ \equiv\ & \neg vasen^{\wedge}(\varphi_1,\ldots,\varphi_n) \vee \neg oikea^{\wedge}(\varphi_1,\ldots,\varphi_n) & \text{De Morgan 1} \\ \equiv\ & vasen_{\vee}(\neg\varphi_1,\ldots,\neg\varphi_n) \vee oikea_{\vee}(\neg\varphi_1,\ldots,\neg\varphi_n) & \text{induktio-oletus, [26]} \end{aligned}$$
- $$\begin{aligned} & \neg(vasen^{\wedge}(\varphi_1,\ldots,\varphi_n) \vee oikea^{\wedge}(\varphi_1,\ldots,\varphi_n)) & \\ \equiv\ & \neg vasen^{\wedge}(\varphi_1,\ldots,\varphi_n) \wedge \neg oikea^{\wedge}(\varphi_1,\ldots,\varphi_n) & \text{De Morgan 2} \\ \equiv\ & vasen_{\vee}(\neg\varphi_1,\ldots,\neg\varphi_n) \wedge oikea_{\vee}(\neg\varphi_1,\ldots,\neg\varphi_n) & \text{induktio-oletus, [26]} \end{aligned}$$
- $\neg(\neg kaava^{\wedge}(\varphi_1,\ldots,\varphi_n)) \equiv \neg\neg kaava^{\wedge}(\varphi_1,\ldots,\varphi_n) \equiv \neg kaava_{\vee}(\neg\varphi,\ldots,\neg\varphi_n)$

Propositiologiikan lakien, joissa esiintyvät vain $\neg$, $\wedge$, $\vee$ ja $\equiv$, symmetria

- kuten [27] havainnollistaa, ei muuta kuin niitä sisältävät lait esiintyvät pareina, joissa toinen osapuoli saadaan toisesta vaihtamalla jokaisen $\wedge$ tilalle $\vee$ ja toisinpäin
  - $\neg\neg\varphi \equiv \varphi$ on oma parinsa
- tämän todistamiseksi riittää De Morganin laki 1, kaksoiskiellon poisto, [24] ja [26]
- De Morganin laki 2 voidaan johtaa De Morganin laista 1

$$\begin{array}{lll} & \neg(\varphi \vee \psi) & \\ \equiv & \neg(\neg\neg\varphi \vee \neg\neg\psi) & \text{kaksoiskiellon poisto takaperin [24,26]} \\ \equiv & \neg\neg(\neg\varphi \wedge \neg\psi) & \text{De Morgan 1 takaperin [24,26]} \\ \equiv & \neg\varphi \wedge \neg\psi & \text{kaksoiskiellon poisto} \end{array}$$

- jos $\mathit{vasen}^{\wedge}(\varphi,\psi) \equiv \mathit{oikea}^{\wedge}(\varphi,\psi)$, niin $\mathit{vasen}_{\vee}(\varphi,\psi) \equiv \mathit{oikea}_{\vee}(\varphi,\psi)$
  - jos $\mathit{kaava}_{\vee}$ saadaan kaavasta $\mathit{kaava}^{\wedge}$ vaihtamalla $\wedge$ ja $\vee$, niin $\mathit{kaava}^{\wedge}$ saadaan kaavasta $\mathit{kaava}_{\vee}$ vaihtamalla $\wedge$ ja $\vee$
  - negaation alas painamisen todistus ei käyttänyt muuta kuin edellä mainittuja

$$\begin{array}{lll} & \mathit{vasen}_{\vee}(\varphi,\psi) & \\ \equiv & \neg\neg\,\mathit{vasen}_{\vee}(\varphi,\psi) & \text{kaksoiskiellon poisto takaperin [24]} \\ \equiv & \neg\,\mathit{vasen}^{\wedge}(\neg\varphi,\neg\psi) & \text{negaation painaminen alas [26]} \\ \equiv & \neg\,\mathit{oikea}^{\wedge}(\neg\varphi,\neg\psi) & \text{oletus } \mathit{vasen}^{\wedge}(\varphi,\psi) \equiv \mathit{oikea}^{\wedge}(\varphi,\psi) \text{ [26]} \\ \equiv & \mathit{oikea}_{\vee}(\neg\neg\varphi,\neg\neg\psi) & \text{negaation painaminen alas} \\ \equiv & \mathit{oikea}_{\vee}(\varphi,\psi) & \text{kaksoiskiellon poisto [26]} \end{array}$$

6 Kaksi eri implikaatiota (ja muutakin)

Päättelyimplikaatio $\Rightarrow$ ja $\Leftarrow$

Vasen $\Rightarrow$ *oikea* tarkoittaa, että jokaisessa mahdollisessa tilanteessa, jossa *vasen* on tosi, myös *oikea* on tosi. [28]

- toisinpäin ei välttämättä päde
- esim. $x = \text{Lilibet} \Rightarrow x \hookleftarrow \text{Harry}$ mutta ei toisinpäin, koska myös $\text{Archie} \hookleftarrow \text{Harry}$
- esim. $x \geq 3 \Rightarrow x^2 \geq 9$ mutta ei toisinpäin, koska myös $(-4)^2 \geq 9$
- tässäkin yhteydessä "mahdollinen tilanne" tarkoittaa "muuttujien arvojen yhdistelmä, joka toteuttaa tehdyt oletukset"

Vasen $\Leftarrow$ *oikea* tarkoittaa samaa kuin *oikea* $\Rightarrow$ *vasen*. [29]

Päättelyimplikaation päättelysääntöjä

jos on päätelty	ja	niin saa päätellä	ja	ja
$\varphi \Leftrightarrow \psi$		$\varphi \Rightarrow \psi$	$\psi \Rightarrow \varphi$	
$\varphi \Rightarrow \psi$	$\psi \Rightarrow \varphi$	$\varphi \Leftrightarrow \psi$		
$\varphi_1 \Rightarrow \varphi_2 \Rightarrow \ldots \Rightarrow \varphi_n$		$\varphi_1 \Rightarrow \varphi_n$		
		$\mathsf{F} \Rightarrow \varphi$	$\varphi \Rightarrow \mathsf{T}$	$\varphi \Rightarrow \varphi$

[30]

- kolmas säilyy pätevänä, vaikka osuudessa $\varphi_1 \Rightarrow \varphi_2 \Rightarrow \ldots \Rightarrow \varphi_n$ yhden tai useamman "$\Rightarrow$" tilalle laitettaisiin "$\Leftrightarrow$" tai "$\equiv$"

Mahdottomasta todellakin saa päätellä mitä tahansa!

- ehkä yllättäen, $x^2 < 0 \;\Rightarrow\; x = 0$ on pätevä päättelyaskel!
- ”jokaisessa mahdollisessa tilanteessa, jossa *vasen* on tosi, myös *oikea* on tosi”
- $x^2 < 0$ ei ole tosi missään tilanteessa, joten osuuden $x = 0$ ei tarvitse olla tosi missään tilanteessa
- tarkastelkaamme melkein kaikkien päteväksi hyväksymää päättelyä $x > 1 \Rightarrow x > 0$
  - jos $x \leq 0$, se tuottaa F $\Rightarrow$ F
  - jos $0 < x \leq 1$, se tuottaa F $\Rightarrow$ T
  - jos $1 < x$, se tuottaa T $\Rightarrow$ T
  - se ei voi tuottaa T $\Rightarrow$ F
- tarkastelkaamme melkein kaikkien vääränä pitämää päättelyä $x > 0 \Rightarrow x > 1$
  - jos $x \leq 0$, se tuottaa F $\Rightarrow$ F
  - jos $0 < x \leq 1$, se tuottaa T $\Rightarrow$ F
  - jos $1 < x$, se tuottaa T $\Rightarrow$ T
  - (se ei voi tuottaa F $\Rightarrow$ T)

$\Rightarrow$ on järkevää hyväksyä päättelyaskel jos ja vain jos se ei missään mahdollisessa tilanteessa tuota T $\Rightarrow$ F

- sitäpaitsi tätä ilmiötä olisi vaikea estää vaikka yritettäisiin, koska useimpien hyväksymillä säännöillä todella voi johtaa väärästä lähtökohdasta monenlaista
  - oletetaan $1 = 2$
  - kertomalla molemmat puolet mielivaltaisella luvulla a saadaan $a = 2a$
  - vähentämällä molemmilta puolilta a saadaan $0 = a$
  - sama onnistuu toisellekin mielivaltaiselle luvulle b, joten $0 = b$
  - $a = 0 = b$, joten $a = b$

  $\Rightarrow$ kaikki luvut ovat yhtäsuuria!
- se, että päättelyn lopputulos on selvästi väärä, ei välttämättä tarkoita, että päättely on virheellinen
  - voi olla, että päättely on itsessään oikein, mutta sen lähtökohdissa on virhe
- vertaa jos Jaana pitää jäätelöstä, niin Jaana ei pidä jäätelöstä

Ristiriitatodistus

- oletetaan, että se, mikä halutaan todistaa, ei ole tosi (on epätosi tai määrittelemätön)
- johdetaan mahdoton lopputulos

$\Rightarrow$ tehdyn oletuksen täytyy olla väärä, joten se, mikä haluttiin todistaa, on tosi

Esimerkki

- tarkoittakoon *merkkijonotin* aliohjelmaa, joka ottaa argumentikseen yhden merkkijonon, ja joka pysähtyy tai ei pysähdy

```
void on_palindromi( string S ){
  for( int i=0, j=S.size()-1; i<j; ++i, --j ){
    if( S[i] != S[j] ){ i=0; j=S.size()-1; }
  }
}
```

- oletetaan, että on olemassa `bool pysähtyy( string koodi, string syöte )` , joka
  - palauttaa `true`, jos `koodi`:n sisältö on merkkijonotin, joka pysähtyy syötteellä `syöte`
  - muutoin palauttaa `false`
- `void rr( string S ){ while( pysähtyy( S, S ) ){} }` on merkkijonotin
- `rr( rr );` ajaa `while( pysähtyy( rr, rr ) ){}` , joten jos `rr( rr );`
  - pysähtyy, niin `while`-silmukka pyörii ikuisesti, joten `rr( rr );` ei pysähdykään
  - ei pysähdy, niin `while`-silmukka lopettaa heti, joten `rr( rr );` pysähtyykin
- ristiriita, joten `pysähtyy` ei voi olla olemassa
- se, että `pysähtyy` ei ole olemassa, on yksi logiikan ja teoreettisen tietojenkäsittelytieteen tärkeimpiä tuloksia!

Kaksiarvologiikassa $\varphi \Rightarrow \psi$ jos ja vain jos $\neg\psi \Rightarrow \neg\varphi$. [31]

- vasemman puolen vastaesimerkissä $\varphi \equiv \mathsf{T}$ mutta $\psi \equiv \mathsf{F}$
  - silloin $\neg\psi \equiv \mathsf{T}$ mutta $\neg\varphi \equiv \mathsf{F}$
  - $\Rightarrow$ se on myös oikean puolen vastaesimerkki
- oikean puolen vastaesimerkissä $\neg\psi \equiv \mathsf{T}$ mutta $\neg\varphi \equiv \mathsf{F}$
  - silloin $\varphi \equiv \mathsf{T}$ mutta $\psi \equiv \mathsf{F}$
  - $\Rightarrow$ se on myös vasemman puolen vastaesimerkki

$\Rightarrow$ joko molemmat puolet ovat epäpätevät, tai kumpikaan ei ole epäpätevä

- *kontrapositiotodistus* käyttää tätä
- esim.
  - vahtimestari ei kuullut räjähdystä
  - jos kassakaappi olisi räjäytetty viimeistään kun vahtimestari lähti töistä, niin vahtimestari olisi kuullut räjähdyksen
  - $\Rightarrow$ kassakaappi räjäytettiin sen jälkeen kun vahtimestari lähti töistä
- kontrapositiotodistus on melkein sama asia kuin ristiriitatodistus
  - jos oletuksesta $\neg\psi$ saadaan johdettua $\neg\varphi$, niin ollaan ristiriidassa oletuksen φ kanssa, joten oletuksella φ pätee ψ
- niitä yhdessä kutsutaan nimellä *epäsuora todistaminen*

Kolmiarvologiikassa asia on monimutkaisempi

- vaikka $\mathsf{U} \Rightarrow \mathsf{F}$, silti ei $\neg\mathsf{F} \Rightarrow \neg\mathsf{U}$, koska muutoin $\mathsf{T} \equiv \neg\mathsf{F} \Rightarrow \neg\mathsf{U} \equiv \mathsf{U} \Leftrightarrow \mathsf{F}$ joten $\mathsf{T} \Rightarrow \mathsf{F}$
- kolmiarvologiikassa mm. $\varphi \Rightarrow \psi$ jos ja vain jos $\neg\psi \vee \neg\lceil\psi\rfloor \Rightarrow \neg\varphi \vee \neg\lceil\varphi\rfloor$
- tämän näkee vaikka miettimällä eri tapaukset
  - jos $\varphi \equiv \mathsf{F}$ tai $\varphi \equiv \mathsf{U}$, niin $\neg\varphi \vee \neg\lceil\varphi\rfloor \equiv \mathsf{T}$, joten kumpikaan $\Rightarrow$ ei rikkoonnu
  - jos $\psi \equiv \mathsf{T}$, niin $\neg\psi \vee \neg\lceil\psi\rfloor \equiv \mathsf{F}$, joten kumpikaan $\Rightarrow$ ei rikkoonnu
  - muutoin $\varphi \equiv \mathsf{T}$ mutta $\psi \equiv \mathsf{F}$ tai $\psi \equiv \mathsf{U}$, joten kumpikin $\Rightarrow$ rikkoontuu
- yleisemmin olettaen että, ”jotkin” ja ”muut” kattavat kaiken eivätkä mene limittäin

  φ:n jotkin vaihtoehdot $\Rightarrow$ ψ:n jotkin vaihtoehdot jos ja vain jos
  ψ:n muut vaihtoehdot $\Rightarrow$ φ:n muut vaihtoehdot

- oletus: ylärivi pätee
  - jos alarivi ei päde, niin ψ:n muu mutta φ:n jokin vaihtoehto toteutuu

  $\Rightarrow$ oletuksen vuoksi ψ:n jokin vaihtoehto toteutuu
  - ristiriita, joten alarivi pätee
- oletus: alarivi pätee
  - jos ylärivi ei päde, niin φ:n jokin mutta ψ:n muu vaihtoehto toteutuu

  $\Rightarrow$ oletuksen vuoksi φ:n muu vaihtoehto toteutuu
  - ristiriita, joten ylärivi pätee
- esim. $\varphi \Rightarrow \neg\psi \vee \neg\lceil\psi\rfloor$ jos ja vain jos $\psi \Rightarrow \neg\varphi \vee \neg\lceil\varphi\rfloor$

Ehdollisena yhtäsuuruutena esitetyn lain soveltaminen

- päättelysääntöä [17] voi käyttää vain aina päteviin yhtäsuuruuksiin
- esim. $\frac{x}{x} = 1$ ei päde aina, vaan vain kun $x \neq 0$

$\Rightarrow$ seuraava [17]:n yleistys on hyödyllinen

> Jos $\mathfrak{h}_1, \ldots, \mathfrak{h}_n$ ovat määritellyt, φ ei sisällä symboleita $\forall$ ja $\exists$ ja $\varphi(\mathfrak{h}_1, \ldots, \mathfrak{h}_n)$ on tosi, niin laista $\varphi(a_1, \ldots, a_n) \Rightarrow \mathfrak{f}(a_1, \ldots, a_n) = \mathfrak{g}(a_1, \ldots, a_n)$ saa johtaa $\mathfrak{f}(\mathfrak{h}_1, \ldots, \mathfrak{h}_n) = \mathfrak{g}(\mathfrak{h}_1, \ldots, \mathfrak{h}_n)$. [32]

- tarkastelemme mitä tahansa mahdollista tilannetta
- jos $\mathfrak{h}_1, \ldots, \mathfrak{h}_n$ ovat siinä määritellyt, niin kukin niistä tuottaa jonkin alkion $a_1, \ldots, a_n$
- jos φ on niille tosi, niin lain mukaan myös $\mathfrak{f} = \mathfrak{g}$ on niille tosi

$\wedge$:n poistolait ja lisäyssääntö

$$\varphi \wedge \psi \Rightarrow \varphi \quad [33]$$

$$\varphi \wedge \psi \Rightarrow \psi \quad [34]$$

Jos $\varphi \Rightarrow \psi$ ja $\varphi \Rightarrow \chi$, niin $\varphi \Rightarrow \psi \wedge \chi$. [35]

- välittömiä seurauksia siitä, että $\wedge$ esittää samaa kuin luonnollisen kielen ”ja”

$\vee$:n lisäyslait ja poistosääntö

$$\varphi \Rightarrow \varphi \vee \psi \quad [36]$$

$$\psi \Rightarrow \varphi \vee \psi \quad [37]$$

Jos $\varphi \Rightarrow \chi$ ja $\psi \Rightarrow \chi$, niin $\varphi \vee \psi \Rightarrow \chi$. [38]

- päättely jakamalla tapauksiin perustuu näihin

Esimerkki: $\Leftrightarrow$-absorptiolakien johtaminen

$$\begin{array}{lcll}
\varphi \wedge (\varphi \vee \psi) & \Rightarrow & \varphi & [33] \\
\varphi & \Rightarrow & \varphi & [30] \\
\varphi & \Rightarrow & \varphi \vee \psi & [36] \\
\varphi & \Rightarrow & \varphi \wedge (\varphi \vee \psi) & [35] \\
\varphi \wedge (\varphi \vee \psi) & \Leftrightarrow & \varphi & [30]
\end{array}$$

$$\begin{array}{lcll}
\varphi & \Rightarrow & \varphi & [30] \\
\varphi \wedge \psi & \Rightarrow & \varphi & [33] \\
\varphi \vee (\varphi \wedge \psi) & \Rightarrow & \varphi & [38] \\
\varphi & \Rightarrow & \varphi \vee (\varphi \wedge \psi) & [36] \\
\varphi \vee (\varphi \wedge \psi) & \Leftrightarrow & \varphi & [30]
\end{array}$$

Voimassa olevat oletukset ja "$\Rightarrow$"

- $x^2 = 9 \;\Rightarrow\; x = -3$ ei sellaisenaan ole pätevä, koska $x = 3$ on vastaesimerkki
- jos on oletettu, että $x \leq 2$, niin se on pätevä
  - mikään sen vastaesimerkki ei toteuta $x \leq 2$
- toisaalta $x \leq 2 \wedge x^2 = 9 \;\Rightarrow\; x = -3$ on pätevä
- tämä on esimerkki siitä, että oletuksen vaikutus ei riipu siitä, tapahtuuko päättely oletuksen alaisuudessa vai ilmaistaanko oletus "$\Rightarrow$":n vasemmalla puolella
- jos oletus esitetään "$\Rightarrow$":n vasemmalla puolella, niin sitä voi joutua toistamaan
  - esim. $x \leq 2 \wedge x^2 - 4 = 5 \;\Rightarrow\; x \leq 2 \wedge x^2 = 9 \;\Rightarrow\; x = -3$
- moni päättelysääntö muuttuisi kömpelöksi, jos se pitäisi muotoilla niin että kaikki oletukset ovat "$\Rightarrow$":n vasemmalla ja "$\Leftrightarrow$":n tai "$\equiv$":n molemmilla puolilla
  - esim. jos $\lceil \mathfrak{h} \rfloor$, niin $\mathfrak{f} = \mathfrak{g} \;\Leftrightarrow\; \mathfrak{f} + \mathfrak{h} = \mathfrak{g} + \mathfrak{h}$ [49] olisikin esim.
    $(\text{muut oletukset}) \wedge \lceil \mathfrak{h} \rfloor \wedge \mathfrak{f} = \mathfrak{g} \;\Leftrightarrow\; (\text{muut oletukset}) \wedge \mathfrak{f} + \mathfrak{h} = \mathfrak{g} + \mathfrak{h}$

$\Rightarrow$ usein on kätevämpää tehdä päättely oletuksen alaisuudessa

- toisaalta osa päättelysäännöistä, kuten [17] ja [32], tarvitsee lähtökohdakseen lain
  - tällä kurssilla *laki* tarkoittaa kaavaa, yhtäpitävyyttä, päättelyimplikaatiota tai yhtätotuutta, joka on voimassa jokaisella muuttujien arvojen yhdistelmällä [sivu 24]
- jotta sellaisessa päättelysäännössä voitaisiin käyttää oletuksen alaisena johdettua tulosta, täytyy oletus esittää "$\Rightarrow$":n vasemmalla puolella

$\Rightarrow$ seuraavaksi esitettävä joukko päättelysääntöjä on hyödyllinen

Oletuksen siirto implikaatioon tai yhtäpitävyyteen ja toisinpäin

- alla Γ tarkoittaa mitä tahansa äärellistä joukkoa oletuksia

  φ on tosi jokaisessa mahdollisessa tilanteessa oletuksilla Γ ja γ, jos ja vain jos $\gamma \Rightarrow \varphi$ on pätevä oletuksilla Γ.

  $\varphi \Rightarrow \psi$ on pätevä oletuksilla Γ ja γ, jos ja vain jos $\gamma \land \varphi \Rightarrow \psi$ on pätevä oletuksilla Γ.

  $\varphi \Leftrightarrow \psi$ on pätevä oletuksilla Γ ja γ, jos ja vain jos $\gamma \land \varphi \Leftrightarrow \gamma \land \psi$ on pätevä oletuksilla Γ. [39]

  $\varphi \equiv \psi$ on pätevä oletuksilla Γ ja γ, jos ja vain jos $\lceil \gamma \rfloor \land \gamma \land \varphi \equiv \lceil \gamma \rfloor \land \gamma \land \psi$ on pätevä oletuksilla Γ.

- toiseksi ylimmän perustelu
  - tilanne, jossa γ ei tuota T, ei ole kummankaan rivin vastaesimerkki koska ylärivillä se ei ole mahdollinen ja alarivillä $\gamma \land \varphi$ ei tuota T
  - tilanne, jossa φ ei tuota T tai ψ tuottaa T, ei ole kummankaan rivin vastaesimerkki, koska se ei riko $\varphi \Rightarrow \psi$ eikä $\gamma \land \varphi \Rightarrow \psi$
  - muissa tilanteissa γ ja φ tuottavat T mutta ψ ei tuota
  - jos Γ sallii tilanteen, niin se on molempien rivien vastaesimerkki
  - muussa tapauksessa se kuuluu tarkastelun ulkopuolelle
- ylin palautuu toiseksi ylimpään valitsemalla ψ:ksi φ ja φ:ksi T [3,30,9]

Alimman perustelu

> $\varphi \equiv \psi$ on pätevä oletuksilla Γ ja γ, jos ja vain jos
> $\lceil\gamma\rfloor \wedge \gamma \wedge \varphi \equiv \lceil\gamma\rfloor \wedge \gamma \wedge \psi$ on pätevä oletuksilla Γ

- jos Γ ei salli tilannetta, niin se ei ole kummankaan rivin vastaesimerkki
- jos Γ sallii mutta γ ei, niin
  - ylärivillä tilanne on mahdoton
  - $\lceil\gamma\rfloor \wedge \gamma$, $\lceil\gamma\rfloor \wedge \gamma \wedge \varphi$ ja $\lceil\gamma\rfloor \wedge \gamma \wedge \psi$ tuottavat F

  $\Rightarrow$ tilanne ei ole alarivin vastaesimerkki

  $\Rightarrow$ tilanne ei ole kummankaan rivin vastaesimerkki
- muussa tapauksessa sekä Γ että γ sallivat tilanteen
  - $\gamma \equiv \mathsf{T}$

  $\Rightarrow$ $\lceil\gamma\rfloor \wedge \gamma \wedge \varphi \equiv \varphi$ ja $\lceil\gamma\rfloor \wedge \gamma \wedge \psi \equiv \psi$

  $\Rightarrow$ tilanne on joko molempien tai ei kummankaan rivin vastaesimerkki

$\Rightarrow$ ylärivillе on vastaesimerkki jos ja vain jos alarivillekin on

Kolmanneksi ylimmän perustelu harjoitustehtäväksi

Päättelysäännöllä [39] voidaan kaavasta, implikaatiosta tai yhtäpitävyydestä tehdä laki

- esim. sivulla 105 käytetty $b \neq 0 \;\Rightarrow\; \frac{a}{b} \cdot b = a$ ei ole reaalilukujen peruslaki, vaan on esim. johdettu oletuksen $b \neq 0$ alaisuudessa seuraavasti

$$
\begin{array}{cll}
 & \frac{a}{b} \cdot b & \\
= & (a \cdot \frac{1}{b}) \cdot b & \text{jakolaskun määritelmä } b \neq 0 \Rightarrow \frac{a}{b} = a \cdot \frac{1}{b}, \text{ [32,39,16]} \\
= & a \cdot (\frac{1}{b} \cdot b) & \text{kertolaskun liitännäisyys } (ab)c = a(bc), \text{ [17]} \\
= & a \cdot (b \cdot \frac{1}{b}) & \text{kertolaskun vaihdannaisuus } ab = ba, \text{ [17,16]} \\
= & a \cdot 1 & \text{käänteisarvon määritelmä } a \neq 0 \Rightarrow a \cdot \frac{1}{a} = 1, \text{ [32,39,16]} \\
= & a & \text{ykkösen määritelmä } a \cdot 1 = a
\end{array}
$$

  ja oletus $b \neq 0$ on lisätty tulokseen $\frac{a}{b} \cdot b = a$ päättelysäännöllä [39]

Nyt voidaan johtaa $\mathfrak{f} = \mathfrak{g} \wedge \mathfrak{g} = \mathfrak{h} \;\Rightarrow\; \mathfrak{f} = \mathfrak{h}$

- valitaan [19]:n $\varphi(x)$:ksi $x = \mathfrak{h}$
- oletuksella $\mathfrak{f} = \mathfrak{g}$ saadaan $\mathfrak{f} = \mathfrak{h} \Leftrightarrow \mathfrak{g} = \mathfrak{h}$
- siitä [2] tuottaa $\mathfrak{g} = \mathfrak{h} \;\Rightarrow\; \mathfrak{f} = \mathfrak{h}$
- siis oletuksella $\mathfrak{f} = \mathfrak{g}$ saatiin $\mathfrak{g} = \mathfrak{h} \;\Rightarrow\; \mathfrak{f} = \mathfrak{h}$, joten [39] tuottaa

$$\mathfrak{f} = \mathfrak{g} \wedge \mathfrak{g} = \mathfrak{h} \;\Rightarrow\; \mathfrak{f} = \mathfrak{h} \qquad [40]$$

[15] voidaan johtaa seuraavasti

- valitaan [19]:n $\varphi(x)$:ksi $x = \mathfrak{f}$
- oletuksella $\mathfrak{f} = \mathfrak{g}$ saadaan $\top \Leftrightarrow \lceil \mathfrak{f} \rfloor \Rightarrow \mathfrak{f} = \mathfrak{f} \Leftrightarrow \mathfrak{g} = \mathfrak{f}$ [3,2,13,20,19]
- siis oletuksella $\mathfrak{f} = \mathfrak{g}$ saatiin $\mathfrak{g} = \mathfrak{f}$ [2], joten $\mathfrak{f} = \mathfrak{g} \Rightarrow \mathfrak{g} = \mathfrak{f}$ [39]
- samoin oletuksella $\mathfrak{g} = \mathfrak{f}$ saadaan $\mathfrak{f} = \mathfrak{g}$, joten $\mathfrak{g} = \mathfrak{f} \Rightarrow \mathfrak{f} = \mathfrak{g}$
- niinpä $\mathfrak{f} = \mathfrak{g} \Leftrightarrow \mathfrak{g} = \mathfrak{f}$ [30]

Materiaalinen implikaatio $\rightarrow$ ja materiaalinen ekvivalenssi $\leftrightarrow$

- $\Rightarrow$ ja $\Leftrightarrow$ ottavat kaksi kaavaa ja tuottavat ”pätevä” tai ”epäpätevä”
  - sijaitsevat kaavojen välissä
  - lopputulos riippuu *jokaisesta mahdollisesta* tilanteesta
  - (silti voidaan sanoa ”pätevä tilanteessa”, koska voidaan valita että vain se tilanne on mahdollinen)
- $\rightarrow$ ja $\leftrightarrow$ ottavat kaksi totuusarvoa ja tuottavat totuusarvon
  - sijaitsevat kaavojen sisällä
  - lopputulos lasketaan *kullekin tilanteelle erikseen*

$$\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$$

$$\varphi \leftrightarrow \psi \equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$$

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

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

[41]

- esim.
  - $x \geq 3 \Rightarrow x \geq 1$ on pätevä
  - $x \geq 3 \rightarrow x \geq 1$ tuottaa T, kun $x = 2$
  - $x \geq 3 \rightarrow x \geq 1$ tuottaa T, kun x on mikä tahansa luku
  - $x \geq 1 \Rightarrow x \geq 3$ ei ole pätevä (ellei tehdyistä oletuksista seuraa $x < 1 \vee x \geq 3$)
  - $x \geq 1 \rightarrow x \geq 3$ tuottaa T, kun $x = 4$
  - $x \geq 1 \rightarrow x \geq 3$ tuottaa T, kun $x = 0$
  - $x \geq 1 \rightarrow x \geq 3$ tuottaa F, kun $x = 2$

$\Rightarrow$:n ja $\Leftrightarrow$:n pätevyys $\rightarrow$:n ja $\leftrightarrow$:n avulla ilmaistuina

Kaksiarvoisessa logiikassa $\varphi \Rightarrow \psi$ jos ja vain jos $\varphi \rightarrow \psi \Leftrightarrow$ T,
ja $\varphi \Leftrightarrow \psi$ jos ja vain jos $\varphi \leftrightarrow \psi \Leftrightarrow$ T. [42]

- kaksiarvoisessa logiikassa
  - $\varphi \Rightarrow \psi$ on pätevä, jos ja vain jos jokaisesssa mahdollisessa tilanteessa $\varphi \rightarrow \psi$
  - $\varphi \Leftrightarrow \psi$ on pätevä, jos ja vain jos jokaisesssa mahdollisessa tilanteessa $\varphi \leftrightarrow \psi$
- kolmiarvoisessa logiikassa asia on monimutkaisempi

$\varphi \Rightarrow \psi$ jos ja vain jos $\varphi \wedge \lceil \varphi \rfloor \rightarrow \psi \wedge \lceil \psi \rfloor \Leftrightarrow$ T, ja
$\varphi \Leftrightarrow \psi$ jos ja vain jos $\varphi \wedge \lceil \varphi \rfloor \leftrightarrow \psi \wedge \lceil \psi \rfloor \Leftrightarrow$ T. [43]

- vastaesimerkki kaavavertailulle $\varphi \Rightarrow \psi$ on mahdollinen tilanne, jossa φ tuottaa T mutta ψ tuottaa F tai U
- täsmälleen samat tilanteet ovat vastaesimerkkejä kaavavertailulle $\varphi \wedge \lceil \varphi \rfloor \rightarrow \psi \wedge \lceil \psi \rfloor \Leftrightarrow$ T
- vastaesimerkki kaavavertailulle $\varphi \Leftrightarrow \psi$ on mahdollinen tilanne, jossa joko φ tuottaa T mutta ψ ei tuota, tai toisinpäin
- täsmälleen samat tilanteet ovat vastaesimerkkejä kaavavertailulle $\varphi \wedge \lceil \varphi \rfloor \leftrightarrow \psi \wedge \lceil \psi \rfloor \Leftrightarrow$ T

Laskujärjestys

- ensin $\neg$, sitten $\wedge$, sitten $\vee$, sitten $\rightarrow$ ja lopuksi $\leftrightarrow$
- $\varphi \rightarrow \psi \rightarrow \chi$ lasketaan kuten $\varphi \rightarrow (\psi \rightarrow \chi)$
  - poikkeavaa, sillä esim. $a - b - c$ lasketaan kuten $(a - b) - c$
  - syy lienee siinä, että $\varphi \rightarrow (\psi \rightarrow \chi)$ on paljon useammin tarpeellinen ja käyttäytyy johdonmukaisemmin kuin $(\varphi \rightarrow \psi) \rightarrow \chi$

Päättelyoperaattorit käyttäytyvät syntaktisesti kuten vertailut

- esim. $\varphi \Leftrightarrow \psi \Rightarrow \chi$ tarkoittaa, että $\varphi \Leftrightarrow \psi$ on pätevä askel ja $\psi \Rightarrow \chi$ on pätevä askel
  - vrt. $0 \leq x < 1$ tarkoittaa että $0 \leq x$ ja $x < 1$
- esim. $(x^2 > 0 \rightarrow x^2 < 0) \rightarrow x = 0$ tuottaa aina T
  - jos $x = 0$, se tuottaa (F $\rightarrow$ F) $\rightarrow$ T joka tuottaa T $\rightarrow$ T joka tuottaa T
  - jos $x \neq 0$, se tuottaa (T $\rightarrow$ F) $\rightarrow$ F joka tuottaa F $\rightarrow$ F joka tuottaa T
- mutta $(x^2 > 0 \;\Rightarrow\; x^2 < 0) \;\Rightarrow\; x = 0$ on syntaksivirhe
  - päättelyn ympärillä ei saa olla sulkeita
  - vrt. $(0 \leq x) < 1$
- lisäksi $x^2 > 0 \;\Rightarrow\; x^2 < 0 \;\Rightarrow\; x = 0$ on virheellinen päättely
  - $x^2 > 0 \;\Rightarrow\; x^2 < 0$ ei ole pätevä: kun $x = 1$ niin $x^2 > 0$ mutta ei $x^2 < 0$
- esim. C++ sallii sekä `1<1<1` että `(1<1)<1`, ja sen mielestä molemmat ovat `true`!
  - `1<1` tuottaa `false` eli `0`, joten `1<1<1` tuottaa saman kuin `0<1` eli `1` eli `true`

  $\Rightarrow$ matematiikan $<$ ja ohjelmoinnin `<` ketjuttuvat olennaisesti eri tavalla

Toisinaan $\Rightarrow$ on parempi formalisointi ilmaukselle ”jos ... niin ...” kuin $\rightarrow$

- esim. Jos Kaino on Lontoossa niin hän on Pariisissa, tai jos hän on Pariisissa niin hän on Jyväskylässä
- monien, kenties enemmistön, mielestä se kuulostaa selvästi väärältä
- tarkoittakoon x Kainon sijaintia ja L, P ja J Lontoota, Pariisia ja Jyväskylää
  - tiedetään $L \neq P \neq J \neq L$
  - $x = L$, $x = P$ ja $x = J$ eivät voi tuottaa U [14,13]
- formalisoimalla ”jos ... niin ...” materiaaliseksi implikaatioksi saadaan
  $$(x = L \rightarrow x = P) \vee (x = P \rightarrow x = J)$$
- jos $x = P$ niin $x = L \rightarrow x = P$ tuottaa T
- muussa tapauksessa $x \neq P$, joten $x = P \rightarrow x = J$ tuottaa T

$\Rightarrow$ $(x = L \rightarrow x = P) \vee (x = P \rightarrow x = J)$ on aina tosi

- formalisoimalla ”jos ... niin ...” $\Rightarrow$:n avulla saadaan väite, että $x = L \Rightarrow x = P$ on pätevä tai $x = P \Rightarrow x = J$ on pätevä
- kumpikaan ei ole pätevä
  - $x = L$ on vastaesimerkki ensimmäiselle
  - $x = P$ on vastaesimerkki jälkimmäiselle

$\Rightarrow$ formalisointi $\Rightarrow$:n avulla tuottaa arkijärkeä vastaavan lopputuloksen, $\rightarrow$:n avulla ei tuota

Vertailu $\rightarrow$ ja $\leftrightarrow$ vastaan $\Rightarrow$ ja $\Leftrightarrow$

- tuloksen tyyppi on eri
  - $\rightarrow$ ja $\leftrightarrow$: totuusarvo F, U tai T
  - $\Rightarrow$ ja $\Leftrightarrow$: päättelyaskel on tai ei ole pätevä (ei ole kolmatta vaihtoehtoa)
- syntaktiset säännöt ovat erit
  - $\varphi \rightarrow (\psi \rightarrow \chi)$ tuottaa saman lausekepuun kuin $\varphi \rightarrow \psi \rightarrow \chi$
  - $\varphi \Rightarrow (\psi \Rightarrow \chi)$ on syntaksivirhe
- suhtautuminen asiayhteyteen on erilainen
  - $x^2 = 4 \rightarrow x = -2$ ei ole aina tosi, koska se tuottaa F kun $x = 2$
  - $x^2 = 4 \Rightarrow x = -2$ on pätevä päättelyaskel kun käsitellään tapausta $x < 0$
- käyttäytyminen määrittelemättömissä tilanteissa on erilainen

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

$\Rightarrow$	F	U	T
F	$\times$	$\times$	$\times$
U	$\times$	$\times$	$\times$
T	$-$	$-$	$\times$

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

$\Leftrightarrow$	F	U	T
F	$\times$	$\times$	$-$
U	$\times$	$\times$	$-$
T	$-$	$-$	$\times$

- monessa kirjassa esitellään vain $\Rightarrow$ ja $\Leftrightarrow$ tai vain $\rightarrow$ ja $\leftrightarrow$, ja saatetaan antaa esitellyille edellisten ja jälkimmäisten ominaisuuksia ristiin

Yhtäsuuruuden perusominaisuudet

- *ekvivalenssi* jonkin joukon alkioille tarkoittaa mitä tahansa $\approx$, joka ottaa kaksi alkiota ja tuottaa totuusarvon siten, että jokaisella alkiolla a, b ja c pätee

1.	$a \approx a$	refleksiivisyys
2.	$a \approx b \wedge b \approx c \;\Rightarrow\; a \approx c$	transitiivisuus
3.	$a \approx b \;\Rightarrow\; b \approx a$	symmetrisyys

- "$=$" ja "yhtäsuuruus" tarkoittavat tavallisesti "sama alkio"

$\Rightarrow$ jos "$\approx$" on "$=$", niin jokaisella kaavalla φ ja alkiolla a ja b pätee

4.	jos $a \approx b$ ja φ ei sisällä $\forall$ eikä $\exists$, niin $\varphi(a) \equiv \varphi(b)$	Leibnizin sääntö

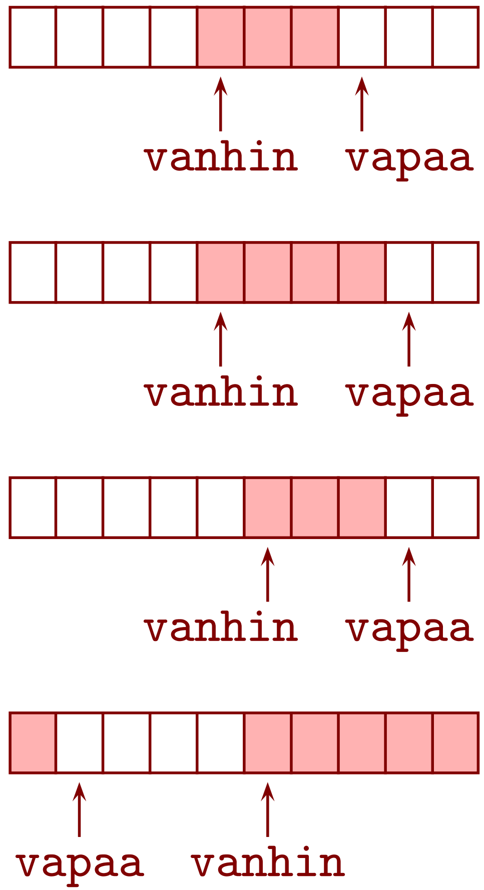
- tällä kurssilla ominaisuuksia (1), ..., (4) vastaavat [20], [40], [15] ja [19]
  - ne on muotoiltu lausekkeille eikä alkioille

  $\Rightarrow$ [20] tarvitsee lisäehdon, että $\mathfrak{f}$ on määritelty
- vain [20] ja [19] tarvittaisiin perussäännöiksi, koska [40] ja [15] voitiin johtaa niistä
- on olemassa ekvivalensseja, joille (4) ei päde
  - esim. "$\approx$" on ihmisten ekvivalenssi "sama syntymävuosi" ja φ on "elossa 1.1.2023"
  - päteminen voi riippua siitä, mitä laskutoimituksia ja relaatiosymb. φ:ssä saa olla
- usein halutaan, että vaikka "$\approx$" ei ole "$=$", niin silti (4) pätee
  - joudutaan olemaan huolellisia, mitä laskutoimituksia ja relaatiosymb. saa käyttää

Tämä aihepiiri tulee vastaan mm. tietorakenteissa

- samalla tietosisällöllä voi olla erilaisia esityksiä
  ⇒ ”sama tietosisältö” ei välttämättä ole sama kuin ”tavu tavulta sama”
  ⇒ ohjelmointikielen valmis == ei välttämättä tee mitä halutaan
- rajapinta, joka sallii vain jotkin toiminnot, tukee (4):n voimassaoloa
- esim. rengaspuskuri

```
const int koko = ...;   oltava > 0

alkio taulu[ koko ];
int vanhin = 0, vapaa = 0;

bool tyhja(){ return vanhin == vapaa; }

bool täysi(){ return (vapaa + 1) % koko == vanhin; }

void lisää( alkio & uusi ){
  taulu[ vapaa ] = uusi; vapaa = (vapaa + 1) % koko;
}

alkio poista(){
  int apu = vanhin; vanhin = (vanhin + 1) % koko;
  return taulu[ apu ];
}
```



Lausekkeita tarvitsee sijoittaa muuttujiin muutenkin kuin yhtäsuuruuksien tuottamiseksi

- [32] sallii johtaa $\mathfrak{f}(\mathfrak{h}_1,\ldots,\mathfrak{h}_n) = \mathfrak{g}(\mathfrak{h}_1,\ldots,\mathfrak{h}_n)$ ehdollisesta yhtäsuuruudesta $\varphi(a_1,\ldots,a_n) \;\Rightarrow\; \mathfrak{f}(a_1,\ldots,a_n) = \mathfrak{g}(a_1,\ldots,a_n)$, jos
  - $\varphi \;\Rightarrow\; \mathfrak{f} = \mathfrak{g}$ on laki, eli voimassa jokaisella a_1:n, ..., a_n:n arvojen yhdistelmällä
  - tehtyjen oletusten ollessa voimassa $\mathfrak{h}_1,\ldots,\mathfrak{h}_n$ ovat määritellyt
  - tehtyjen oletusten ollessa voimassa $\varphi(\mathfrak{h}_1,\ldots,\mathfrak{h}_n)$ tuottaa T
- esim. jos on oletettu $x > 4$, saa laista $a \geq 0 \;\Rightarrow\; \left(\sqrt{a}\right)^2 = a$ johtaa $\left(\sqrt{\frac{x}{x-2}}\right)^2 = \frac{x}{x-2}$
  - kun $x > 4$, on $x \neq 2$, joten $\frac{x}{x-2}$ on määritelty
  - kun $x > 4$, on $x \geq 0$ ja $x-2 > 0$, joten $\frac{x}{x-2} \geq 0$

  $\Rightarrow$ myös $\left(\sqrt{\frac{x}{x-2}}\right)^2$ on määritelty
- tämä ei kuitenkaan riitä mm. seuraavissa tilanteissa:
  - halutaan johtaa $\mathfrak{f} < 0 \wedge |\mathfrak{f}| = -\mathfrak{f} \vee \mathfrak{f} \geq 0 \wedge |\mathfrak{f}| = \mathfrak{f}$ siitä, että $\mathfrak{f}$ on määritelty ja aina $a < 0 \wedge |a| = -a \vee a \geq 0 \wedge |a| = a$
  - halutaan johtaa $\mathfrak{f} < \mathfrak{g} \;\Rightarrow\; \mathfrak{f} \neq \mathfrak{g}$ siitä, että $a < b \;\Rightarrow\; a \neq b$

Päättelysäännön [32] yleistys muuhun kuin yhtäsuuruuksiin

Jos $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ ovat määritellyt ja φ ja ψ eivät sisällä symboleita $\forall$ ja $\exists$, niin

- laista $\varphi(a_1, \ldots, a_n)$ saa johtaa kaavan $\varphi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$, [44]
- oletuksesta $\psi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ ja laista $\psi(a_1, \ldots, a_n) \Rightarrow \varphi(a_1, \ldots, a_n)$ saa johtaa kaavan $\varphi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$, [45]
- laista $\psi(a_1, \ldots, a_n) \Rightarrow \varphi(a_1, \ldots, a_n)$ saa johtaa $\psi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n) \Rightarrow \varphi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$, [46]
- laista $\psi(a_1, \ldots, a_n) \Leftrightarrow \varphi(a_1, \ldots, a_n)$ saa johtaa $\psi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n) \Leftrightarrow \varphi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ ja [47]
- laista $\psi(a_1, \ldots, a_n) \equiv \varphi(a_1, \ldots, a_n)$ saa johtaa $\psi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n) \equiv \varphi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$. [48]

- ehto, että φ ei saa sisältää $\forall$ ja $\exists$, korvataan lievemmällä luvussa 11

Esimerkki: jos $\mathfrak{f}$ on määritelty, niin $\mathfrak{f} < 0 \land |\mathfrak{f}| = -\mathfrak{f} \lor \mathfrak{f} \geq 0 \land |\mathfrak{f}| = \mathfrak{f}$

- $a < 0 \land |a| = -a \lor a \geq 0 \land |a| = a$ pätee reaaliluvuilla, eikä sisällä symboleita $\forall$ ja $\exists$
- niinpä [44] tuottaa väitteen

Laajentaminen määrittelemättömiin lausekkeisiin

- oletus, että $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ ovat määritellyt, on toisinaan osittain tai kokonaan tarpeeton
- usein on helppo miettiä, päteekö lopputulos, jos lausekkeissa on määrittelemättömiä
  - jos lausekkeen osa on määrittelemätön, niin myös koko lauseke on [14]

  ⇒ vertailu, johon se kuuluu, tuottaa U [13]

  ⇒ ∧-ketju, johon se kuuluu, tuottaa U tai F [9]
- esim. $\mathfrak{f} < \mathfrak{g} \;\Rightarrow\; \mathfrak{f} \neq \mathfrak{g}$
  - $a < b \;\Rightarrow\; a \neq b$ pätee reaaliluvuilla, eikä sisällä symboleita ∀ ja ∃

  ⇒ jos $\mathfrak{f}$ ja $\mathfrak{g}$ ovat määritellyt, niin [46] tuottaa $\mathfrak{f} < \mathfrak{g} \;\Rightarrow\; \mathfrak{f} \neq \mathfrak{g}$
  - muussa tapauksessa $\mathfrak{f}$ tai $\mathfrak{g}$ ei ole määritelty, joten $\mathfrak{f} < \mathfrak{g}$ ei tuota T [13]

  ⇒ $\mathfrak{f} < \mathfrak{g} \;\Rightarrow\; \mathfrak{f} \neq \mathfrak{g}$ pätee vaikka ei oletettaisi, että $\mathfrak{f}$ ja $\mathfrak{g}$ ovat määritellyt [28]

Päättelysääntöjen [44], ..., [47] perustelu

- [45]
  - tarkastelemme mitä tahansa oletusten sallimaa muuttujien arvojen yhdistelmää, jolla $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ ovat määritellyt
  - koska kukin $\mathfrak{f}_i$ on määritelty, se tuottaa puheenaiheen jonkin alkion a_i
  - koska oletettiin $\psi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$, se tuottaa T, joten $\psi(a_1, \ldots, a_n)$ tuottaa T
  - koska $\psi(a_1, \ldots, a_n) \Rightarrow \varphi(a_1, \ldots, a_n)$ on laki, myös $\varphi(a_1, \ldots, a_n)$ tuottaa T
  - niinpä $\varphi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ tuottaa T
- [44] saadaan päättelysäännöllä [45] valitsemalla ψ:ksi T
  - T voidaan aina olettaa todeksi, koska se on aina tosi
  - jos φ on laki, niin φ on tosi jokaisessa tilanteessa, joten φ on tosi jokaisessa tilanteessa jossa T on tosi, joten T $\Rightarrow \varphi$ on laki
- [46] saadaan päättelysäännöstä [45] päättelysäännöllä [39]
- [47] saadaan päättelysäännöstä [46] päättelysäännöllä [30]

Päättelysääntö [32] voidaan johtaa päättelysäännöstä [45]

- [32] olettaa, että $\mathfrak{h}_1, \ldots, \mathfrak{h}_n$ ovat määritellyt, φ ei sisällä symboleita $\forall$ ja $\exists$, $\varphi(\mathfrak{h}_1, \ldots, \mathfrak{h}_n)$ on tosi ja $\varphi(a_1, \ldots, a_n) \Rightarrow \mathfrak{f}(a_1, \ldots, a_n) = \mathfrak{g}(a_1, \ldots, a_n)$ on laki
- valitsemme [45]:n $\mathfrak{f}_i$:ksi [32]:n $\mathfrak{h}_i$:t, φ:ksi $(\mathfrak{f} = \mathfrak{g})$:n ja ψ:ksi φ:n

$\Rightarrow$ [45]:n oletukset pätevät: $\mathfrak{f}_i$:t ovat määritellyt, φ ja ψ eivät sisällä $\forall$ eikä $\exists$, $\psi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ on tosi ja $\psi(a_1, \ldots, a_n) \Rightarrow \varphi(a_1, \ldots, a_n)$ on laki

$\Rightarrow$ [45] tuottaa $\varphi(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ eli [32]:n $\mathfrak{f}(\mathfrak{h}_1, \ldots, \mathfrak{h}_n) = \mathfrak{g}(\mathfrak{h}_1, \ldots, \mathfrak{h}_n)$

7 Reaaliluvut ja niiden yhtälöt

Reaaliluvut ovat lukusuoran luvut

- kokonaisluvut, kuten 0, 3810 ja -567
- muut rationaaliluvut, kuten $\frac{25}{3}$ ja $-\frac{3}{7}$
- irrationaaliluvut, kuten $\sqrt{2}$ ja π

Reaalilukujen laskutoimituksia eli funktiosymboleita

- yhteenlasku $x+y$
- vastaluku $-x$
- vähennyslasku $x-y$
  - tarkoittaa samaa kuin $x+(-y)$
- kertolasku $x \cdot y$ tai xy
- jakolasku $\frac{x}{y}$ tai x/y
  - ei määritelty, kun $y=0$
  - muulloin tarkoittaa samaa kuin $x \cdot \frac{1}{y}$, missä $\frac{1}{y}$ on sellainen luku, että $y \cdot \frac{1}{y} = 1$
- itseisarvo $|x|$

- neliöjuuri $\sqrt{x}$
  - ei määritelty, kun $x < 0$
- potenssi x^y
  - ei määritelty, kun $x = 0 \wedge y < 0$ eikä kun $x < 0$ ja (monimutkainen ehto y:lle)
- log, sin, ...
- reaalilukujen yhteen-, vähennys-, kerto- ja jakolaskun lait oletetaan tutuiksi
  - $a + b = b + a$, $a - a = 0$, $1a = a$, $a(b + c) = ab + ac$, ...

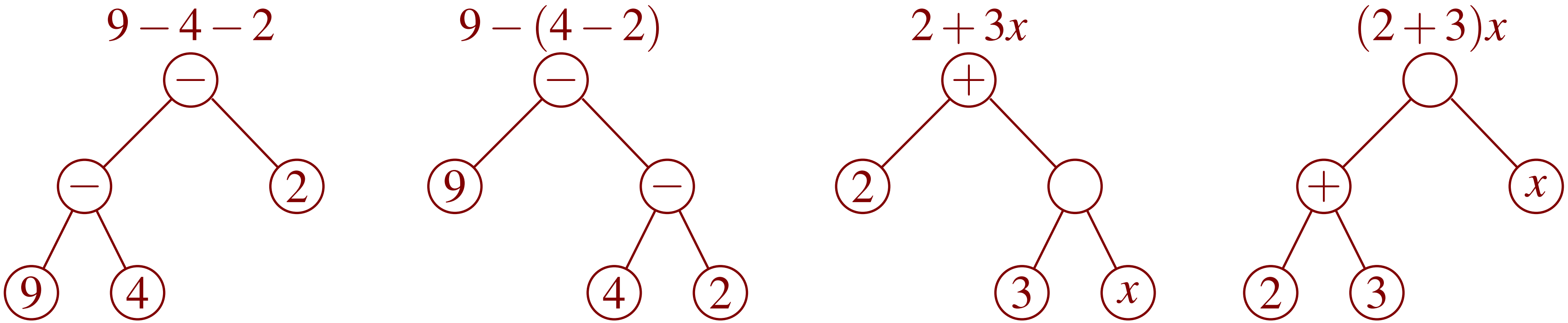
  $\Rightarrow$ ellei toisin sanota, niitä saa käyttää vapaasti esimerkeissä, harjoitustehtävissä jne., eikä tarvitse kertoa, mitä käytettiin

Vertailut

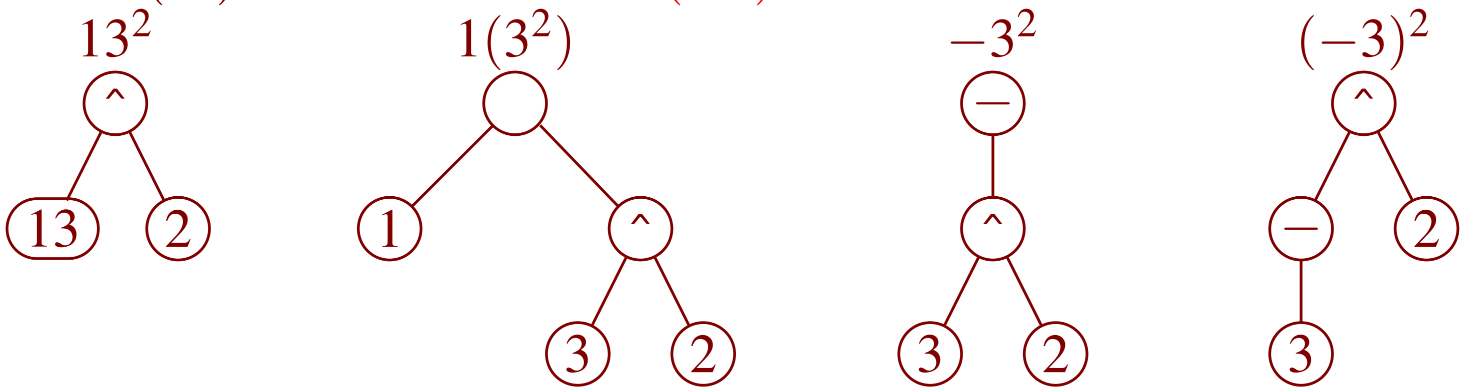
- $<$, $\leq$, $\geq$ ja $>$
  - ottavat kaksi reaalilukua ja tuottavat totuusarvon
  - riittää määritellä yksi, sillä muut saa sen ja logiikan yleisten käsitteiden avulla
  - esim. $x \leq y \;\Leftrightarrow\; x < y \vee x = y$
- $=$ ja $\neq$ katsotaan kuuluviksi logiikan yleisiin eikä reaalilukujen käsitteisiin
  - ovat mielekkäitä missä tahansa puheenaiheessa
  - esim. $\mathit{vanhA}(\text{Archie}) = \text{Meghan}$
  - tietenkin $x \neq y \;\Leftrightarrow\; \neg(x = y)$

Laskujärjestys osoitetaan sulkeilla tai määräytyy yleisesti tunnetuilla säännöillä

- esim. $9-4-2 = (9-4)-2 = 5-2 = 3$
  eikä $9-4-2 = 9-(4-2) = 9-2 = 7$
- esim. $2+3x$ tarkoittaa $2+(3x)$ eikä $(2+3)x$,
  joten $2+3x = 2+(3x)$ aina,
  mutta $2+3x = (2+3)x$ vain kun $x=1$



- esim. $13^2 = (13)^2 = 169$ eikä $13^2 = 1(3^2) = 9$
- silti $-3^2 = -(3^2) = -9$ eikä $-3^2 = (-3)^2 = 9$



Huomaa ero

- lukuja verrataan symbolilla $=$
  - yhtäsuuruus
- totuusarvoja verrataan symbolilla $\Leftrightarrow$
  - yhtäpitävyys

Esimerkki päättelystä yhtäsuuruusketjulla: summan ja erotuksen tulon kaava

- tässä esimerkissä
  - tehdään useita asioita samassa askeleessa
  - moni logiikan päättelysääntöjen käyttö on piilossa pitkän askeleen sisällä
  - vähennyslaskua käsitellään itsenäisenä eikä vastaluvun vähentämisenä
- muuttujat, yhteenlasku, vähennyslasku, kertolasku ja neliö ovat aina määriteltyjä

$\Rightarrow$ päättelysäännön [16] ehto, että $\mathfrak{h}(\mathfrak{f})$ on määritelty, toteutuu alla aina [14]

$$\begin{array}{rll} & (a+b)(a-b) & \\ = & aa-ab+ba-bb & \text{sulut kerrottu auki} \\ = & a^2-ab+ab-b^2 & xx=x^2,\ xy=yx,\ [16] \\ = & a^2-b^2 & -ab \text{ ja } +ab \text{ kumoavat toisensa, } [16] \end{array}$$

- niinpä $(a+b)(a-b)=a^2-b^2$

Sama yksityiskohtaisemmin

- tässä esimerkissä
  - logiikan päättelysääntöjen käytöt on näytetty, paitsi ne [17]:n käytöt, joissa vain muuttuja vaihtuu
  - vähennyslaskua käsitellään vastaluvun vähentämisenä
  - vaihetta ”yhteenlaskun järjestyksellä ei ole väliä” ei ole purettu osiin
  - päätelmää ”$x(-y) = -xy$” ei ole purettu osiin
- muuttujat, yhteenlasku, kertolasku, vastaluku, neliö ja 0 ovat aina määriteltyjä

⇒ päättelysäännön [16] ehto, että $\mathfrak{h}(\mathfrak{f})$ on määritelty, toteutuu alla aina

- samoin päättelysäännön [17] ehto, että $\mathfrak{h}_i$:t ovat määritellyt

$$
\begin{array}{rll}
 & (a+b)(a-b) & \\
= & (a+b)(a+-b) & x-y=x+-y,\ [16] \\
= & a(a+-b)+b(a+-b) & (x+y)z=xz+yz,\ [17] \\
= & (aa+a(-b))+(ba+b(-b)) & x(y+z)=xy+xz,\ [17{,}16] \\
= & (aa+-ab)+(ba+-bb) & x(-y)=-xy,\ [16] \\
= & aa+(ba+-ab)+-bb & \text{yhteenlaskun järjestyksellä ei ole väliä} \\
= & a^2+(ab+-ab)+-b^2 & xx=x^2,\ xy=yx,\ [16] \\
= & a^2+0+-b^2 & x+-x=0,\ [17{,}16] \\
= & a^2+-b^2 & x+0=x,\ [17{,}16] \\
= & a^2-b^2 & x-y=x+-y,\ [17{,}15]
\end{array}
$$

Neljä yhtälöiden ratkaisemisessa tärkeää yhtäpitävyyttä

Jos $\lceil \mathfrak{h} \rfloor$, niin $\mathfrak{f} = \mathfrak{g} \;\equiv\; \mathfrak{f} + \mathfrak{h} = \mathfrak{g} + \mathfrak{h}$.
Jos $\lceil \mathfrak{h} \rfloor$, niin $\mathfrak{f} = \mathfrak{g} \;\equiv\; \mathfrak{f} - \mathfrak{h} = \mathfrak{g} - \mathfrak{h}$. [49]

Jos $\mathfrak{h} \neq 0$, niin $\mathfrak{f} = \mathfrak{g} \;\equiv\; \mathfrak{f}\mathfrak{h} = \mathfrak{g}\mathfrak{h}$.
Jos $\mathfrak{h} \neq 0$, niin $\mathfrak{f} = \mathfrak{g} \;\equiv\; \frac{\mathfrak{f}}{\mathfrak{h}} = \frac{\mathfrak{g}}{\mathfrak{h}}$. [50]

Perustelu sille, että $\lceil \mathfrak{f} \rfloor \Leftrightarrow \lceil \mathfrak{g} \rfloor$

- jos $\mathfrak{f}$ ei ole määritelty, niin $\mathfrak{f}$ sisältää määrittelemättömän laskutoimituksen [14]
  $\Rightarrow$ $\mathfrak{f} + \mathfrak{h}$, $\mathfrak{f} - \mathfrak{h}$, $\mathfrak{f}\mathfrak{h}$ ja $\frac{\mathfrak{f}}{\mathfrak{h}}$ sisältävät määrittelemättömän laskutoimituksen
  $\Rightarrow$ $\mathfrak{f} = \mathfrak{g}$, $\mathfrak{f} + \mathfrak{h} = \mathfrak{g} + \mathfrak{h}$, $\mathfrak{f} - \mathfrak{h} = \mathfrak{g} - \mathfrak{h}$, $\mathfrak{f}\mathfrak{h} = \mathfrak{g}\mathfrak{h}$ ja $\frac{\mathfrak{f}}{\mathfrak{h}} = \frac{\mathfrak{g}}{\mathfrak{h}}$ tuottavat U [13]
- samalla tavalla jos $\mathfrak{g}$ ei ole määritelty, niin kaikki vertailut tuottavat U

$\Rightarrow$ jokaisen $\equiv$:n molemmat puolet tuottavat U

- muissa tilanteissa sekä $\mathfrak{f}$ että $\mathfrak{g}$ on määritelty
  - lisäksi $\mathfrak{h}$ on määritelty joko oletuksen vuoksi tai seurauksena oletuksesta $\mathfrak{h} \neq 0$ [13]

  $\Rightarrow$ kaikki lausekkeet ovat määritellyt
  $\Rightarrow$ minkään $\equiv$:n kumpikaan puoli ei tuota U

Enää tarvitsee perustella $\mathfrak{f} \Leftrightarrow \mathfrak{g}$ [24]

- riittää osoittaa erikseen "$\Rightarrow$" ja "$\Leftarrow$" [30]
- jokaisen "$\Rightarrow$" seuraa suoraan laista [16]

- ylemmän päättelysäännön [49] "$\Leftarrow$" saadaan seuraavasti:

$$\begin{array}{lll} & \mathfrak{f}+\mathfrak{h}=\mathfrak{g}+\mathfrak{h} & \\ \Rightarrow & (\mathfrak{f}+\mathfrak{h})-\mathfrak{h}=(\mathfrak{g}+\mathfrak{h})-\mathfrak{h} & [16] \\ \Leftrightarrow & \mathfrak{f}=\mathfrak{g} & (x+y)-y=x,\ [17,19] \end{array}$$

- alemman päättelysäännön [49] "$\Leftarrow$" saadaan samalla tavalla, koska $(x-y)+y=x$:

$$\mathfrak{f}-\mathfrak{h}=\mathfrak{g}-\mathfrak{h} \;\Rightarrow\; (\mathfrak{f}-\mathfrak{h})+\mathfrak{h}=(\mathfrak{g}-\mathfrak{h})+\mathfrak{h} \;\Leftrightarrow\; \mathfrak{f}=\mathfrak{g}$$

- ylemmän päättelysäännön [50] "$\Leftarrow$" saadaan seuraavasti:
  - reaaliluvuilla pätee $b \neq 0 \Rightarrow \frac{ab}{b}=a$

  $\Rightarrow$ koska $\mathfrak{f}$, $\mathfrak{g}$ ja $\mathfrak{h}$ ovat määritellyt ja $\mathfrak{h} \neq 0$, pätee $\frac{\mathfrak{f}\mathfrak{h}}{\mathfrak{h}}=\mathfrak{f}$ ja $\frac{\mathfrak{g}\mathfrak{h}}{\mathfrak{h}}=\mathfrak{g}$ [32]

$$\begin{array}{lll} & \mathfrak{f}\mathfrak{h}=\mathfrak{g}\mathfrak{h} & \\ \Rightarrow & \frac{\mathfrak{f}\mathfrak{h}}{\mathfrak{h}}=\frac{\mathfrak{g}\mathfrak{h}}{\mathfrak{h}} & [13,16] \\ \Leftrightarrow & \mathfrak{f}=\mathfrak{g} & [19,2] \end{array}$$

- alemman päättelysäännön [50] "$\Leftarrow$" saadaan seuraavasti:
  - reaaliluvuilla pätee $b \neq 0 \Rightarrow \frac{a}{b}\cdot b=a$

  $\Rightarrow$ koska $\mathfrak{f}$, $\mathfrak{g}$ ja $\mathfrak{h}$ ovat määritellyt ja $\mathfrak{h} \neq 0$, pätee $\frac{\mathfrak{f}}{\mathfrak{h}}\cdot\mathfrak{h}=\mathfrak{f}$ ja $\frac{\mathfrak{g}}{\mathfrak{h}}\cdot\mathfrak{h}=\mathfrak{g}$ [32]

$$\begin{array}{lll} & \frac{\mathfrak{f}}{\mathfrak{h}}=\frac{\mathfrak{g}}{\mathfrak{h}} & \\ \Rightarrow & \frac{\mathfrak{f}}{\mathfrak{h}}\cdot\mathfrak{h}=\frac{\mathfrak{g}}{\mathfrak{h}}\cdot\mathfrak{h} & [13,16] \\ \Leftrightarrow & \mathfrak{f}=\mathfrak{g} & [19,2] \end{array}$$

Esimerkki yhtälön ratkaisemisesta y:n suhteen yhtäpitävyysketjulla

$$
\begin{array}{lll}
 & 2x-y=3 & \\
\Leftrightarrow & 2x-y+(y-3)=3+(y-3) & \text{lisätty } y-3, \text{ [49]} \\
\Leftrightarrow & 2x-3=y & 2x-y+(y-3)=2x-3, \\
 & & 3+(y-3)=y, \text{ [19]} \\
\Leftrightarrow & y=2x-3 & \text{[15]}
\end{array}
$$

- niinpä $2x-y=3 \;\Leftrightarrow\; y=2x-3$

Toinen esimerkki yhtälön ratkaisemisesta yhtäpitävyysketjulla

$$
\begin{array}{lll}
 & 3x-4x+6=2 & \\
\Leftrightarrow & -x+6=2 & 3x-4x=-x, \text{ [19]} \\
\Leftrightarrow & -x+6-6=2-6 & \text{lisätty } -6, \text{ [49]} \\
\Leftrightarrow & -x=-4 & -x+6-6=-x,\ 2-6=-4, \text{ [19]} \\
\Leftrightarrow & x=4 & \text{kerrottu } -1\text{:llä, } a(-1)=-a, \text{ [50] takaperin}
\end{array}
$$

- niinpä $3x-4x+6=2 \;\Leftrightarrow\; x=4$

Esimerkki yhtälöparin ratkaisemisesta yhtäpitävyysketjulla

- yhtälöpari on kaava, jossa kaksi yhtälöä on yhdistetty $\wedge$:lla

$$\begin{array}{lll}
 & 2x-y=3 \wedge 3x-2y=2 & \\
\Leftrightarrow & y=2x-3 \wedge 3x-2y=2 & y \text{ ratkaistu ensimmäisestä, [sivu 106], [22]} \\
\Leftrightarrow & y=2x-3 \wedge 3x-2(2x-3)=2 & y\text{:n lauseke sijoitettu toiseen, [sivu 62]} \\
\Leftrightarrow & y=2x-3 \wedge 3x-4x+6=2 & \text{toista sievennetty, [sivu 58]} \\
\Leftrightarrow & y=2x-3 \wedge x=4 & \text{toinen ratkaistu, [sivu 106], [22]} \\
\Leftrightarrow & x=4 \quad \wedge y=2x-3 & \text{[5]} \\
\Leftrightarrow & x=4 \quad \wedge y=2\cdot4-3 & x\text{:n lauseke sijoitettu toiseen, [21]} \\
\Leftrightarrow & x=4 \quad \wedge y=5 & 2\cdot4-3=5\text{, [19]}
\end{array}$$

- niinpä $2x-y=3 \wedge 3x-2y=2 \;\Leftrightarrow\; x=4 \wedge y=5$
- käytännössä sama esitettäisiin tiiviimmin, esim.

$$\begin{array}{lll}
 & 2x-y=3 \wedge 3x-2y=2 & \\
\Leftrightarrow & y=2x-3 \wedge 3x-2(2x-3)=2 & \\
\Leftrightarrow & x=4 \quad \wedge y=5 & (*)
\end{array}$$

(*) $3x-2(2x-3)=2 \;\Leftrightarrow\; -x+6=2 \;\Leftrightarrow\; x=4$

Esimerkin tuloksen tarkastus

- tarkastus $\Rightarrow$-suuntaan
  - käytetään [16] ja reaalilukujen lakeja
    $x = 4 \wedge y = 5 \;\Rightarrow\; 2x - y = 2 \cdot 4 - 5 = 8 - 5 = 3 \;\Rightarrow\; 2x - y = 3$
    $x = 4 \wedge y = 5 \;\Rightarrow\; 3x - 2y = 3 \cdot 4 - 2 \cdot 5 = 12 - 10 = 2 \;\Rightarrow\; 3x - 2y = 2$
  - siksi $x = 4 \wedge y = 5 \;\Rightarrow\; 2x - y = 3 \wedge 3x - 2y = 2$
- yhtälöparilla voi olla useampi kuin yksi juuri
  - sekä $x = 4 \wedge y = 0$ että $x = 0 \wedge y = -2$ on parin $3x - 6y = 12 \wedge 4x - 8y = 16$ juuri

  $\Rightarrow$ tarvitsee tarkastaa myös $\Leftarrow$-suuntaan
- tarkastus $\Leftarrow$-suuntaan
  - käytetään analyyttisen geometrian tietoja
  - 1. asteen x-y-yhtälön juuret muodostavat ei mitään, suoran tai koko x-y-tason

  $\Rightarrow$ jos 1. asteen yhtälöparilla on monta juurta, niin joko toisen yhtälön kaikki juuret ovat myös toisen juuria tai toisinpäin
  - $x = 2 \wedge y = 1$ on ensimmäisen mutta ei toisen juuri
  - $x = 0 \wedge y = -1$ on toisen mutta ei ensimmäisen juuri

  $\Rightarrow$ yhtälöparillamme on enintään 1 juuri
  - siksi $x = 4 \wedge y = 5 \;\Leftarrow\; 2x - y = 3 \wedge 3x - 2y = 2$
- onnistui molempiin suuntiin, joten $2x - y = 3 \wedge 3x - 2y = 2 \;\Leftrightarrow\; x = 4 \wedge y = 5$

Esimerkkitehtävän voi ratkaista muillakin tavoilla

- olisi voitu aloittaa ratkaisemalla x ensimmäisestä, tai x tai y toisesta
- voidaan aloittaa muutenkin kuin ratkaisemalla jokin muuttuja jommastakummasta

	$2x-y=3$	$\land\ 3x-2y=2$	
$\Leftrightarrow$	$4x-2y=6$	$\land\ 3x-2y=2$	ensimm. kerrottu 2:lla, $2\neq 0$, [50,22]
$\Leftrightarrow$	$\begin{array}{rcr} & 4x-2y & = \quad 6 \\ - & (3x-2y) & \quad -2 \end{array}$	$\land\ 3x-2y=2$	ensimmäisestä vähennetty toinen (*)
$\Leftrightarrow$	$x=4$	$\land\ 3x-2y=2$	vähennyslaskut laskettu, [19]
$\Leftrightarrow$	$x=4$	$\land\ 3\cdot 4-2y=2$	$x=4$ sijoitettu toiseen, [21]
$\Leftrightarrow$	$x=4$	$\land\ -2y=-10$	lisätty -12, laskut laskettu, [49,19,22]
$\Leftrightarrow$	$x=4$	$\land\ y=5$	takaperin kerrottu -2:lla, [50,19,22]

(*) aputulos yksityiskohtaisesti johdettuna

	$4x-2y=6\ \land\ 3x-2y=2$	
$\Leftrightarrow$	$3x-2y=2\ \land\ 4x-2y=6$	[5]
$\Leftrightarrow$	$3x-2y=2\ \land\ 4x-2y-2=6-2$	lisätty -2, [49,22]
$\Leftrightarrow$	$3x-2y=2\ \land\ 4x-2y-(3x-2y)=6-2$	[21] takaperin
$\Leftrightarrow$	$4x-2y-(3x-2y)=6-2\ \land\ 3x-2y=2$	[5]

Vielä yksi yhtälöiden ratkaisemisessa hyödyllinen yhtäpitävyys

$$\frac{\mathfrak{f}}{\mathfrak{g}} = \mathfrak{h} \;\Leftrightarrow\; \mathfrak{g} \neq 0 \wedge \mathfrak{f} = \mathfrak{g}\mathfrak{h} \qquad [51]$$

- jos $\mathfrak{f}$, $\mathfrak{g}$ tai $\mathfrak{h}$ on määrittelemätön, niin $\Leftrightarrow$:n vasen puoli tuottaa U ja oikea U tai F [9]
- jos $\mathfrak{g} = 0$, niin vasen puoli tuottaa U ja oikea F
- muissa tilanteissa $\mathfrak{g} \cdot \frac{\mathfrak{f}}{\mathfrak{g}} = \mathfrak{f}$ [sivu 105] ja $\frac{\mathfrak{f}}{\mathfrak{g}} = \mathfrak{h} \;\Leftrightarrow\; \mathfrak{g} \cdot \frac{\mathfrak{f}}{\mathfrak{g}} = \mathfrak{g}\mathfrak{h} \;\Leftrightarrow\; \mathfrak{f} = \mathfrak{g}\mathfrak{h}$ [50,19]

Esimerkki

$$\frac{x^2+x-6}{x-2} = 2x-5 \;\Leftrightarrow\; x-2 \neq 0 \wedge x^2+x-6 = (x-2)(2x-5) = 2x^2-9x+10$$

- ratkaistaan $x^2+x-6 = 2x^2-9x+10$

$$\Leftrightarrow\; x^2-10x+16=0 \;\Leftrightarrow\; x = \frac{10 \pm \sqrt{10^2-4\cdot 1\cdot 16}}{2} = \frac{10 \pm \sqrt{36}}{2} \;\Leftrightarrow\; x=2 \vee x=8$$

- siis $x \neq 2 \wedge (x=2 \vee x=8)$, joten $x=8$

Seuraavat määrittelevät reaalilukujen neliöjuuren tyhjentävästi:

$$a \geq 0 \;\Rightarrow\; \sqrt{a} \geq 0 \wedge \left(\sqrt{a}\right)^2 = a \qquad [52]$$

Jos $a < 0$, niin $\sqrt{a}$ ei ole määritelty. [53]

- jos $\sqrt{a} = \sqrt{b}$, niin $a \geq 0 \wedge b \geq 0$, joten $a = \left(\sqrt{a}\right)^2 = \left(\sqrt{b}\right)^2 = b$

Harjoitustehtävä: keksi yhtäpitävyys yhtälöiden $\sqrt{\mathfrak{f}} = \mathfrak{g}$ ratkaisemiseksi

Yhtälöt logiikan näkökulmasta

- *yhtälö* (*equation*) on kaava muotoa $vasen = oikea$
- yhtälön *juuret* (*roots*) ovat ne luvut, lukuparit tms., jotka toteuttavat kaavan
  - juuria kutsutaan myös ”ratkaisuiksi”
  - toisaalta ”ratkaisu” tarkoittaa myös ratkaisuprosessin esitystä

  $\Rightarrow$ suosimme sanaa ”juuri”, kun tarkoitamme lukuarvoja eikä ratkaisuprosessia
- *tuntematon* (*unknown*) on muuttuja, jonka arvo halutaan selvittää
- esimerkki
  - $2+3x = (2+3)x$ on yhtälö
  - x on tuntematon
  - 1 on juuri
  - $2+3x = (2+3)x \;\Leftrightarrow\; 2+3x = 5x \;\Leftrightarrow\; 2 = 2x \;\Leftrightarrow\; x = 1$ on ratkaisu
- yhden muuttujan yhtälön ratkaiseminen tarkoittaa mahdollisimman helppotajuisen kaavan etsimistä, joka
  - on tosi täsmälleen silloin kun alkuperäinen kaava on tosi, eli $yhtälö \Leftrightarrow vastaus$
  - ei koskaan tuota U
- ratkaisuprosessin voi usein, mutta ei aina, esittää kätevästi muodossa

$$vasen = oikea \;\Leftrightarrow\; \ldots \;\Leftrightarrow\; lopullinen\ vastaus$$

- toisinaan ei ole selvää, mikä muoto on helppotajuisin

$\Rightarrow$ sallitaan vaihtelevia esitystapoja, mutta ei ihan mitä tahansa

Yhden muuttujan yhtälön juurten esittäminen mahdollisimman helppotajuisesti

- yhden muuttujan x yhtälön juuret voidaan usein ilmoittaa muodossa

  $x = \mathfrak{c}_1 \vee x = \mathfrak{c}_2 \vee \cdots \vee x = \mathfrak{c}_n$ (c tulee sanasta "constant")

  missä $\mathfrak{c}_1, \ldots, \mathfrak{c}_n$ ovat vakiolausekkeita
  - vakiolauseke tarkoittaa lauseketta, jossa ei esiinny muuttujia
  - tuntematon on aina =-merkin vasemmalla puolella
  - $\mathfrak{c}_i$:t ovat aidosti kasvavassa järjestyksessä
  - esim. $x - 1 = \frac{1}{x} \;\Leftrightarrow\; x \neq 0 \wedge x^2 - x - 1 = 0 \;\Leftrightarrow\; x = \frac{1-\sqrt{5}}{2} \vee x = \frac{1+\sqrt{5}}{2}$
- vakiolausekkeet sievennetään mahdollisimman helppotajuiseen muotoon
  - esim. ei $\frac{6+\sqrt{20}}{2}$ vaan $3 + \sqrt{5}$
  - toisinaan ei ole selvää, mikä muoto on helppotajuisin, esim. $2\sqrt{5}$ vai $\sqrt{20}$
- jos juuria ei ole lainkaan, niin lopullinen kaava on F
  - esim. $8x + 2 - 3x = 5x + 3 \;\Leftrightarrow\; 5x + 2 = 5x + 3 \;\Leftrightarrow\; 2 = 3 \;\Leftrightarrow\;$ F
- jos jokainen luku on juuri, niin lopullinen kaava on T
  - esim. $8x + 2 - 3x = 5x + 2 \;\Leftrightarrow\; 5x + 2 = 5x + 2 \;\Leftrightarrow\; 2 = 2 \;\Leftrightarrow\;$ T
- juurista voi muodostua myös lukuvälejä
  - esim. $(x+1)\sqrt{x^2} = (x+1)x \;\Leftrightarrow\; x = -1 \vee \sqrt{x^2} = x \;\Leftrightarrow\; x = -1 \vee x \geq 0$

Monen muuttujan yhtälöstä ratkaistaan jokin tuntematon muiden lausekkeena

- esim. $3x - 2y = 2 \;\Leftrightarrow\; 2y = 3x - 2 \;\Leftrightarrow\; y = \frac{3}{2}x - 1$

Yhden muuttujan *epäyhtälön* (*inequation*) juurista tulee tyypillisesti lukuvälejä

- epäyhtälö on muuten kuten yhtälö, mutta $=$-merkin tilalla on $<$, $\leq$, $\geq$, $>$ tai $\neq$
- esim. $x^2+15>8x \;\Leftrightarrow\; x<3 \vee x>5$

Yhden muuttujan lukuvälien esittäminen mahdollisimman helppotajuisesti

- esitetään aidosti kasvavassa järjestyksessä
  - esim. ei $5 \geq x > 3 \vee x = 2$ vaan $x = 2 \vee 3 < x \leq 5$
- poikkeus: välit, joilla ei ole ylärajaa, saa esittää muuttuja vasemmalla
  - esim. $x < -2 \vee x = 3 \vee x \geq 5$
- poikkeus: esim. $1 < x \leq 8 \wedge x \neq 2 \wedge x \neq 5$ voi olla helppotajuisempi kuin $1 < x < 2 \vee 2 < x < 5 \vee 5 < x \leq 8$
- välit yhdistetään jos mahdollista
  - esim. ei $x = 3 \vee 2 < x \leq 5 \vee 4 \leq x \leq 7$ vaan $2 < x \leq 7$
  - esim. ei $x < 7 \vee x = 7 \vee x > 7$ vaan T
  - esim. ei $1 \leq x < 17 \vee 12\sqrt{2} < x \leq 18$ vaan $1 \leq x \leq 18$

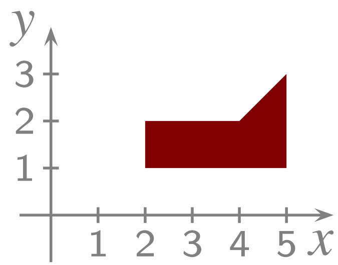
Mistä tiedetään, että $12\sqrt{2} < 17$?

- näin yksinkertaisen voi katsoa laskimella
  - yleisemmin on vaara, että pyöristysvirheet voivat johtaa väärään lopputulokseen
- jos olisi $12\sqrt{2} \geq 17$, niin olisi

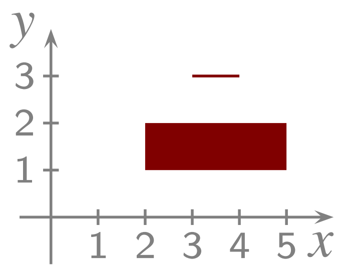
$$288 = 144 \cdot 2 = 12^2(\sqrt{2})^2 = (12\sqrt{2})(12\sqrt{2}) \geq 17 \cdot 12\sqrt{2} \geq 17 \cdot 17 = 289$$

Jos muuttujia on monta, niin esitystapa kannattaa valita tapauskohtaisesti

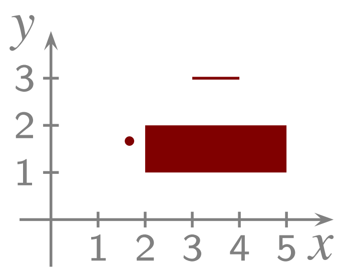
- mikään osien esitysjärjestys ei välttämättä ole muita helppotajuisempi
- toisinaan hyvä tapa
  - muuttujat esitetään johdonmukaisesti samassa järjestyksessä
  - muuttujaa verrataan vain lukuihin ja järjestyksessä aikaisempiin muuttujiin
  - osat eivät mene päällekkäin
  - esim. $2 \leq x < 4 \wedge 1 \leq y \leq 2 \vee 4 \leq x \leq 5 \wedge 1 \leq y \leq x - 2$



- voi olla suuri merkitys sillä, mikä muuttuja on ensimmäisenä
  - esim. $1 \leq y \leq 2 \wedge 2 \leq x \leq 5 \vee y = 3 \wedge 3 \leq x \leq 4$
  - vertaa $2 \leq x < 3 \wedge 1 \leq y \leq 2 \vee 3 \leq x \leq 4 \wedge (1 \leq y \leq 2 \vee y = 3) \vee$ $4 < x \leq 5 \wedge 1 \leq y \leq 2$

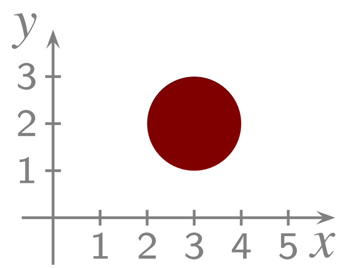


- tämän tavan tarkka noudattaminen ei ole aina järkevää
  - esim. $x = y = \frac{5}{3} \vee 2 \leq x \leq 5 \wedge 1 \leq y \leq 2 \vee 3 \leq x \leq 4 \wedge y = 3$



- nämä suositukset koskevat *(epä)yhtälö(ryhmä)n juurten esittämistä*, eivät kaavoja yleisesti!
- esim. $(x-3)^2 + (y-2)^2 \leq 1$ ei esitä x:ää eikä y:tä ratkaistuna, mutta voi silti olla helppotajuisempi kuin

$$2 \leq x \leq 4 \wedge 2 - \sqrt{1 - (x-3)^2} \leq y \leq 2 + \sqrt{1 - (x-3)^2}$$



Tulon nollasääntö

$$\mathfrak{f}\mathfrak{g} = 0 \;\Leftrightarrow\; \mathfrak{f} = 0 \wedge \lceil \mathfrak{g} \rfloor \vee \mathfrak{g} = 0 \wedge \lceil \mathfrak{f} \rfloor \qquad [54]$$

Ratkaisemme yhtälön $x = \sqrt{a^2}$

- koska $a^2 \geq 0$, on $\sqrt{a^2}$ määritelty [52,45], joten jollakin x on $x = \sqrt{a^2}$ tosi
- x^2 on määritelty, joten $x^2 = \left(\sqrt{a^2}\right)^2 = a^2$ [16,52,32]
- $x^2 = a^2 \;\Leftrightarrow\; (x+a)(x-a) = x^2 - a^2 = 0 \;\Leftrightarrow\; x+a = 0 \vee x-a = 0 \;\Leftrightarrow\; x = -a \vee x = a$ [49,54]
- koska $x = \sqrt{a^2} \geq 0$ [52,45], pätee [18]
  - jos $a < 0$, niin $x = a$ on mahdoton, joten $x = -a = |a|$
  - jos $a = 0$, niin $x = -a = -0 = 0 \vee x = a = 0$, joten $x = 0 = |a|$
  - jos $a > 0$, niin $x = -a$ on mahdoton, joten $x = a = |a|$
- muita tapauksia ei ole [61], joten $x = |a| \;\Rightarrow\; \sqrt{a^2} = |a|$ [38]

$$\sqrt{a^2} = |a| \qquad [55]$$

8 Lisää päättelemistä propositiologiikan keinoin

Motivaatio

- päättelyissä on usein osia, jotka eivät edellytä atomikaavojen sisään katsomista
  - koskevat vain symbolien $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\Leftrightarrow$, $\Rightarrow$, $\Leftarrow$ ja $\equiv$ käyttäytymistä
  - toisin sanoen, koskevat vain propositiologiikkaa
- tässä luvussa tarkastellaan niihin sopivia päättelykeinoja

Usein riittää käyttää kaksiarvologiikkaa

- kaavassa ei ole määrittelemättömiä laskutoimituksia, esim. $x^2 > x+3 \vee x - x^2 = -3$
- voimassa olevat oletukset tekevät kaikesta määriteltyä
  - esim. $3\sqrt{-x-1} \geq x+1$ oletuksen $x < -1$ alaisuudessa
- propositiomuuttuja ei voi mahdollisessa tilanteessa saada arvoa U [10]

Propositiologiikassa voidaan usein tarkastella jokainen tilanne erikseen

- usein pohdittavana on vain äärellinen määrä kaavoja
- niissä on yhteensä vain äärellinen määrä eri propositiomuuttujia
  - kaavat ovat äärellisiä

$\Rightarrow$ on vain äärellinen määrä eri tilanteita

- tällöin jokaisen tilanteen tarkasteleminen erikseen on yleispätevä yksinkertainen keino
  - sitä saa ja kannattaa käyttää, jos eri propositiomuuttujia on vähän

Esimerkki

- tämä tehtävä on naamioitu säännön [60] [sivu 132] todistamisessa tarvittavasta
- Greta ja Filip eivät asu Jyväskylässä, mutta saattavat käydä siellä
  - joka kerta kun Filip käy Jyväskylässä, hän käy Harjulla yhdessä Gretan kanssa
  - jos Filip ja Greta käyvät Harjulla, kumpikin on käymässä Jyväskylässä
  - Greta saa käydä Jyväskylässä ilman että samalla Filip käy siellä
  - onko totta, että muulloin kuin edellisen rivin tilanteissa, joko kumpikaan ei ole käymässä Jyväskylässä tai he käyvät yhdessä Harjulla?
- tarkoittakoot
  - F että Filip on käymässä Jyväskylässä
  - G että Greta on käymässä Jyväskylässä
  - H että he käyvät yhdessä Harjulla
- F, G ja H eivät koskaan tuota U [10]
  - ei tarvitse (eikä edes saa) tutkia totuusarvoa U
  - $\varphi \Rightarrow \psi$ pätee jos ja vain jos jokaisessa mahdollisessa tilanteessa $\varphi \rightarrow \psi$ tuottaa T [42]
- ensimmäinen tieto sanoo, että $F \Rightarrow H$
- toinen tieto sanoo, että $H \Rightarrow F \wedge G$
- kolmas ei vaikuta mahdollisiin tilanteisiin, mutta määrää, mitä ”muulloin” tarkoittaa
- päteekö $\neg(G \wedge \neg F) \Rightarrow \neg F \wedge \neg G \vee H$?

Tehtävä ratkaistuna perinteisellä totuustaululla

- $\Rightarrow$ ja mahdollisen tilan käsite eivät ole käytettävissä

$\Rightarrow$ käytämme kaavoja muotoa oletukset $\rightarrow$ väite ja tilanne on mahdollinen $\rightarrow$ väite

- lupaus ja tieto voidaan esittää $F \rightarrow H$ ja $H \rightarrow F \wedge G$
- se, josta kysyttiin onko totta, voidaan esittää $\neg(G \wedge \neg F) \rightarrow \neg F \wedge \neg G \vee H$
- koko tehtävä voidaan esittää
  $(F \rightarrow H) \wedge (H \rightarrow F \wedge G) \;\rightarrow\; (\neg(G \wedge \neg F) \rightarrow \neg F \wedge \neg G \vee H)$

F	G	H	$F \rightarrow H$	$H \rightarrow F \wedge G$	$G \wedge \neg F$	$\neg F \wedge \neg G$	$\neg(G \wedge \neg F) \rightarrow \neg F \wedge \neg G \vee H$	lopputulos
F	F	F	T	T	F	T	T	T
F	F	T	T	F	F	T	T	T
F	T	F	T	T	T	F	T	T
F	T	T	T	F	T	F	T	T
T	F	F	F	T	F	F	F	T
T	F	T	T	F	F	F	T	T
T	T	F	F	T	F	F	F	T
T	T	T	T	T	F	F	T	T

- työlästä ja virhealtista

Totuustaulu tulkiten $F \Rightarrow H$ ja $H \Rightarrow F \wedge G$ mahdollisten tilanteiden määritelmäksi

- ei tarvitse muuntaa $\Rightarrow$ $\rightarrow$:ksi

F	G	H	$F \Rightarrow H$	$H \Rightarrow F \wedge G$	$G \wedge \neg F$	$\neg F \wedge \neg G$	lopputulos
F	F	F	ok	ok	F	T	T
F	F	T	ok	-	F	T	T
F	T	F	ok	ok	T	F	T
F	T	T	ok	-	T	F	T
T	F	F	-	ok	F	F	F
T	F	T	ok	-	F	F	T
T	T	F	-	ok	F	F	F
T	T	T	ok	ok	F	F	T

$\Rightarrow$ luontevampaa ja vähemmän työlästä kuin edellinen

- mahdottomia tilanteita ei tarvitse tutkia

$\Rightarrow$ taulukon himmeät kohdat voidaan jättää tutkimatta

Edellinen niin että kutakin tilannetta tutkitaan vain kunnes tulos on selvä

- hyödynnetään ensin sellainen tieto, jolla saadaan käsiteltyä mahdollisimman paljon tilanteita mahdollisimman helposti
- Filip ja Greta käyvät yhdessä Harjulla eli H
- kumpikaan ei ole Jyväskylässä eli $\neg F \wedge \neg G$
- Filip on Jyväskylässä, mutta ei käykään Gretan kanssa Harjulla eli $F \wedge \neg H$
- jäljellä on enää tilanne $\neg F \wedge G \wedge \neg H$
  - siinä Greta on Jyväskylässä, mutta Filip ei ole

F	G	H	$F \Rightarrow H$	$H \Rightarrow F \wedge G$	$G \wedge \neg F$	$\neg F \wedge \neg G$	lopputulos
F	F	F					T
F	F	T					T
F	T	F			T		T
F	T	T					T
T	F	F	-				-
T	F	T					T
T	T	F	-				-
T	T	T					T

- työmäärä riviä kohden on vähentynyt huomattavasti
- joudutaan yhä luomaan paljon rivejä

Edellinen rivejä niputtamalla

- tehdään vain yksi rivi tilanteista, joissa H on tosi
- tehdään vain yksi rivi tilanteista, joissa $\neg F \wedge \neg G$ on tosi
- tehdään vain yksi rivi tilanteista, joissa $F \wedge \neg H$ on tosi
- jäljellä olevissa tilanteissa
  - H on F, koska kaikki joissa H on T on käsitelty
  - F on F, koska niistä, joissa H on F, on käsitelty kaikki joissa F on T
  - G on T, koska niistä, joissa H ja F ovat F, on käsitelty se jossa G on F

F	G	H	$F \Rightarrow H$	$H \Rightarrow F \wedge G$	$G \wedge \neg F$	$\neg F \wedge \neg G$	lopputulos
		T					T
F	F						T
T		F	-				-
F	T	F			T		T

- työmäärä vähentyi entisestään, eikä enää ole verrannollinen rivien määrään
- tietoa $H \Rightarrow F \wedge G$ ei käytetty tässä eikä edellisessä lainkaan
- siitä huolehtiminen, että jokainen rivi käsitellään, on vaikeutunut

Jäljellä olevien tilanteiden muodostaminen De Morganin laeilla [7]

- sivun 117 ”muulloin kuin edellisen rivin tilanteissa” kattaa ne ja vain ne tilanteet, joissa Greta ei ole Jyväskylässä tai Filip on
  - $\neg(G \wedge \neg F) \Leftrightarrow \neg G \vee \neg\neg F \Leftrightarrow \neg G \vee F$
- kysymyksestä näkee suoraan, että väite pätee jos kumpikaan ei ole Jyväskylässä
  - ”onko totta, että . . . , joko kumpikaan ei ole käymässä Jyväskylässä tai . . . ?”

⇒ jäljellä on enää tilanteet, joissa Greta ei ole Jyväskylässä tai Filip on ja ainakin toinen on Jyväskylässä
  - $\neg(\neg F \wedge \neg G) \Leftrightarrow \neg\neg F \vee \neg\neg G \Leftrightarrow F \vee G$

- jos Filip ei ole Jyväskylässä, niin
  - jos Greta ei ole Jyväskylässä, niin ainakin toinen on Jyväskylässä ei toteudu
  - muutoin Greta ei ole Jyväskylässä tai Filip on ei toteudu

⇒ jäljellä olevissa tilanteissa Filip on Jyväskylässä
  ⇒ ensimmäisen tiedon mukaan he käyvät yhdessä Harjulla
  ⇒ väite pätee

Totuusarvojen tarkasteleminen sijoittaen ja sieventäen yksi propositiomuuttuja kerrallaan

- mikä tahansa $\neg$-, $\wedge$-, $\vee$-, $\rightarrow$- tai $\leftrightarrow$-kaava, jonka jokin osapuoli on F tai T, sievenee pienemmäksi, monet paljon pienemmäksi [9]

kaava	kaava	tuottavat
$\mathsf{F} \wedge \varphi$	$\varphi \wedge \mathsf{F}$	F
$\mathsf{T} \wedge \varphi$	$\varphi \wedge \mathsf{T}$	φ
$\mathsf{F} \vee \varphi$	$\varphi \vee \mathsf{F}$	φ
$\mathsf{T} \vee \varphi$	$\varphi \vee \mathsf{T}$	T
$\mathsf{F} \leftrightarrow \varphi$	$\varphi \leftrightarrow \mathsf{F}$	$\neg\varphi$
$\mathsf{T} \leftrightarrow \varphi$	$\varphi \leftrightarrow \mathsf{T}$	φ

kaava	tuottaa
$\neg\mathsf{F}$	T
$\neg\mathsf{T}$	F
$\mathsf{F} \rightarrow \varphi$	T
$\mathsf{T} \rightarrow \varphi$	φ
$\varphi \rightarrow \mathsf{F}$	$\neg\varphi$
$\varphi \rightarrow \mathsf{T}$	T

$\Rightarrow$ moni kaksiarvologiikan kaava tai kaavavertailu voidaan tutkia kätevästi seuraavasti:
- valitaan jokin sen propositiomuuttuja
- sijoitetaan siihen F ja sievennetään
- sijoitetaan siihen T ja sievennetään
- poistetaan $\neg\neg$ [4]
- verrataan lopputuloksia
- tarvittaessa jatketaan uudella propositiomuuttujalla

- usein kannattaa valita propositiomuuttuja, joka esiintyy monessa kohdassa
  $\Rightarrow$ kaava sievenee kerralla paljon

Esimerkki: päteekö $\neg P \wedge \neg(Q \wedge \neg R \wedge (\neg Q \vee P)) \wedge (Q \rightarrow R) \;\Leftrightarrow\; \neg(P \vee \neg(Q \leftrightarrow R))$?

- yritetään ensin $Q \Leftrightarrow \mathsf{T}$

$$
\begin{array}{llll}
 & \neg P \wedge \neg(Q \wedge \neg R \wedge (\neg Q \vee P)) \wedge (Q \rightarrow R) & & \neg(P \vee \neg(Q \leftrightarrow R)) \\
\Leftrightarrow & \neg P \wedge \neg(\mathsf{T} \wedge \neg R \wedge (\neg \mathsf{T} \vee P)) \wedge (\mathsf{T} \rightarrow R) & \Leftrightarrow & \neg(P \vee \neg(\mathsf{T} \leftrightarrow R)) \\
\Leftrightarrow & \neg P \wedge \neg(\neg R \wedge (\mathsf{F} \vee P)) \wedge R & \Leftrightarrow & \neg(P \vee \neg R) \\
\Leftrightarrow & \neg P \wedge \neg(\neg R \wedge P) \wedge R & &
\end{array}
$$

- vielä ei näy ovatko yhtäpitävät, yritetään $P \Leftrightarrow \mathsf{T}$

$$
\begin{array}{llll}
 & \neg P \wedge \neg(\neg R \wedge P) \wedge R & & \neg(P \vee \neg R) \\
\Leftrightarrow & \neg \mathsf{T} \wedge \neg(\neg R \wedge \mathsf{T}) \wedge R & \Leftrightarrow & \neg(\mathsf{T} \vee \neg R) \\
\Leftrightarrow & \mathsf{F} \wedge \neg\neg R \wedge R & \Leftrightarrow & \neg \mathsf{T} \\
\Leftrightarrow & \mathsf{F} & \Leftrightarrow & \mathsf{F}
\end{array}
$$

- täsmää, yritetään $P \Leftrightarrow \mathsf{F}$

$$
\begin{array}{llll}
 & \neg P \wedge \neg(\neg R \wedge P) \wedge R & & \neg(P \vee \neg R) \\
\Leftrightarrow & \neg \mathsf{F} \wedge \neg(\neg R \wedge \mathsf{F}) \wedge R & \Leftrightarrow & \neg(\mathsf{F} \vee \neg R) \\
\Leftrightarrow & \mathsf{T} \wedge \neg \mathsf{F} \wedge R & \Leftrightarrow & \neg\neg R \\
\Leftrightarrow & \mathsf{T} \wedge R & \Leftrightarrow & R \\
\Leftrightarrow & R & &
\end{array}
$$

- täsmää, jäljellä on $Q \Leftrightarrow \mathsf{F}$

$$\begin{array}{cl} & \neg P \wedge \neg(Q \wedge \neg R \wedge (\neg Q \vee P)) \wedge (Q \rightarrow R) \\ \Leftrightarrow & \neg P \wedge \neg(\mathsf{F} \wedge \neg R \wedge (\neg \mathsf{F} \vee P)) \wedge (\mathsf{F} \rightarrow R) \\ \Leftrightarrow & \neg P \wedge \neg \mathsf{F} \wedge \mathsf{T} \\ \Leftrightarrow & \neg P \end{array} \qquad \begin{array}{cl} & \neg(P \vee \neg(Q \leftrightarrow R)) \\ \Leftrightarrow & \neg(P \vee \neg(\mathsf{F} \leftrightarrow R)) \\ \Leftrightarrow & \neg(P \vee \neg\neg R) \\ \Leftrightarrow & \neg(P \vee R) \end{array}$$

- nyt näkyy, että eroa tulee täsmälleen silloin kun P tuottaa eri totuusarvon kuin $P \vee R$
  $\Rightarrow$ silloin kun $P \Leftrightarrow \mathsf{F}$ ja $R \Leftrightarrow \mathsf{T}$
- oltiin oletuksen $Q \Leftrightarrow \mathsf{F}$ alaisuudessa

$\Rightarrow$ kaikkiaan eroa tulee jos ja vain jos $P \Leftrightarrow Q \Leftrightarrow \mathsf{F}$ ja $R \Leftrightarrow \mathsf{T}$

Kommentteja

- kun rutiini kehittyy, ei tarvita yhtä paljoa välivaiheita kuin edellä
- jos oltaisiin yritetty ensin $Q \Leftrightarrow \mathsf{F}$, niin vastaesimerkki olisi löytynyt paljon nopeammin
- toisaalta tutkimalla kaikki mahdollisuudet saatiin kattava luettelo vastaesimerkeistä
- analyysiä voi nopeuttaa mm. De Morganin laeilla [7] ja absorptiolaeilla [8]
- esim.
  - $\neg P \wedge \neg(\neg R \wedge P) \wedge R \;\Leftrightarrow\; \neg P \wedge (\neg\neg R \vee \neg P) \wedge R \;\Leftrightarrow\; \neg P \wedge (R \vee \neg P) \wedge R \;\Leftrightarrow\; \neg P \wedge R$
  - $\neg(P \vee \neg R) \;\Leftrightarrow\; \neg P \wedge \neg\neg R \;\Leftrightarrow\; \neg P \wedge R$

  $\Rightarrow$ tapaus $Q \Leftrightarrow \mathsf{T}$ ratkeaa ilman että kokeillaan P:n totuusarvot

Symboleista $\leftrightarrow$ ja $\rightarrow$ pääsee aina eroon sillä, että [41]

$$\varphi \leftrightarrow \psi \equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$$
$$\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$$

- esim. kaksiarvologiikassa
  - $P \rightarrow P \vee Q \Leftrightarrow \neg P \vee P \vee Q \Leftrightarrow \mathsf{T} \vee Q \Leftrightarrow \mathsf{T}$
  - $P \vee Q \rightarrow P \Leftrightarrow \neg P \wedge \neg Q \vee P \Leftrightarrow (\neg P \vee P) \wedge (\neg Q \vee P) \Leftrightarrow \mathsf{T} \wedge (Q \rightarrow P) \Leftrightarrow Q \rightarrow P$
  - $P \leftrightarrow P \vee Q \Leftrightarrow (P \rightarrow P \vee Q) \wedge (P \vee Q \rightarrow P) \Leftrightarrow \mathsf{T} \wedge (Q \rightarrow P) \Leftrightarrow Q \rightarrow P$
- esim. tarkoittakoon J, että Jaana pitää jäätelöstä
  - oletamme sen olevan tosi tai epätosi (ei määrittelemätön) [10]

  $\Rightarrow$ jos Jaana pitää jäätelöstä, niin Jaana ei pidä jäätelöstä sievenee
  $J \rightarrow \neg J \Leftrightarrow \neg J \vee \neg J \Leftrightarrow \neg J$

  $\Rightarrow$ se tarkoittaa samaa kuin Jaana ei pidä jäätelöstä

Toisinaan $\Rightarrow$-todistuksissa [33], . . . , [38] ovat tehokkaita

- ääriesimerkki $\varphi \wedge \psi \Rightarrow \varphi \Rightarrow \varphi \vee \psi$

Kasvavuus ja vähenevyys

> Jos $\psi \Rightarrow \chi$ ja X ei ole $\varphi(X)$:ssä muiden symbolien alaisuudessa kuin $\wedge$, $\vee$ ja parillinen määrä $\neg$, niin $\varphi(\psi) \Rightarrow \varphi(\chi)$.
>
> Kaksiarvologiikassa jos $\psi \Rightarrow \chi$ ja X ei ole $\varphi(X)$:ssä muiden symbolien alaisuudessa kuin $\wedge$, $\vee$ ja pariton määrä $\neg$, niin $\varphi(\chi) \Rightarrow \varphi(\psi)$. [56]

- jos ajatellaan, että F on pienin, U on keskimmäinen ja T on suurin, niin [sivu 22]
  - $\mathit{vasen} \wedge \mathit{oikea}$ tuottaa minimin siitä mitä *vasen* ja *oikea* tuottavat
  - $\mathit{vasen} \vee \mathit{oikea}$ tuottaa maksimin siitä mitä *vasen* ja *oikea* tuottavat
- $\neg$F $\equiv$ T, $\neg$U $\equiv$ U ja $\neg$T $\equiv$ F

$\Rightarrow$ jos P muuttuu F:stä U:ksi tai U:sta T:ksi ja Q ei muutu, niin
  - $P \wedge Q$ ja $Q \wedge P$ joko eivät muutu tai muuttuvat samaan suuntaan kuin P
  - $P \vee Q$ ja $Q \vee P$ joko eivät muutu tai muuttuvat samaan suuntaan kuin P
  - $\neg P$ muuttuu vastakkaiseen suuntaan kuin P
- kaksiarvologiikassa ylemmän vastaesimerkki vaatisi $\varphi(\psi) \equiv$ T mutta $\varphi(\chi) \equiv$ F
  - muuttumissuunnan vuoksi pitäisi olla $\psi \equiv$ T ja $\chi \equiv$ F, vastoin oletusta $\psi \Rightarrow \chi$
- todistamme ylemmän 3-arvologiikassa myöhemmin, koska se tarvitsee uuden käsitteen
- alempi saadaan ylemmästä säännöllä [31]
  - alemman oletuksilla $\neg\varphi(X)$ täyttää ylemmän oletukset, joten $\neg\varphi(\psi) \Rightarrow \neg\varphi(\chi)$

  $\Rightarrow$ [31] tuottaa $\varphi(\chi) \equiv \neg\neg\varphi(\chi) \Rightarrow \neg\neg\varphi(\psi) \equiv \varphi(\psi)$

Säännöllisyys propositiomuuttujan suhteen

- olkoon $\varphi(X)$ kaava, jossa X on propositiomuuttuja

  Missä tahansa tilanteessa joko $\varphi(\mathsf{U})$ tuottaa U,
  tai $\varphi(\mathsf{F})$ ja $\varphi(\mathsf{T})$ tuottavat saman kuin $\varphi(\mathsf{U})$. [57]

- esim. jos $\varphi(X)$ on $X \to P \vee X$, niin
  - jos P on F tai P on U, niin $\varphi(\mathsf{U})$ tuottaa U
  - jos P on T, niin $\varphi(\mathsf{F})$, $\varphi(\mathsf{U})$ ja $\varphi(\mathsf{T})$ tuottavat T
- tätä voidaan käyttää helpottamaan määrittelemättömän tapauksen miettimistä
  - esim. $\varphi(X)$ olkoon $X \wedge (\neg X \vee Q)$
  - $\varphi(\mathsf{F})$ tuottaa F ja $\varphi(\mathsf{T})$ tuottaa saman kuin Q

  $\Rightarrow$ jos Q ei ole F, niin [57]:n alarivi ei voi toteutua, joten $\varphi(\mathsf{U})$ tuottaa U
  - laskemalla saadaan, että jos Q on F, niin $\varphi(\mathsf{U})$ tuottaa U
- [57]:n todistus ei ole vaikea, mutta on pitkä
  $\Rightarrow$ jätämme väliin
- [57]:n pätevyys riippuu siitä, että kaavat muodostetaan
  vain kuten sivulla 55 kerrotaan

Todistamisvaivaa säästävä propositiologiikan lause

Jos $\varphi \Leftrightarrow \psi$ pätee kaksiarvologiikassa, jos φ ja ψ eivät sisällä muuta kuin F, T, ¬, ∧, ∨, (,) ja propositiomuuttujia, ja jos mikään propositiomuuttuja ei esiinny φ:ssä sekä parillisen että parittoman määrän ¬ alaisuudessa ja samoin ψ:lle, niin $\varphi \equiv \psi$ pätee kolmiarvologiikassa. [58]

- jokainen [27]:n kaavavertailu todistuu tällä siitä, että se pätee kaksiarvologiikassa $\Leftrightarrow$-muodossa
- $\varphi \wedge \neg\varphi \Leftrightarrow \mathsf{F}$ ja $\varphi \wedge (\neg\varphi \vee \psi) \Leftrightarrow \varphi \wedge \psi$
  - eivät päde kolmiarvologiikassa $\equiv$-muodossa
  - φ esiintyy sekä parillisen että parittoman määrän ¬ alaisuudessa
- $\varphi \vee \neg\varphi \Leftrightarrow \mathsf{T}$ ja $\varphi \vee (\neg\varphi \wedge \psi) \Leftrightarrow \varphi \vee \psi$
  - eivät päde kolmiarvologiikassa edes $\Leftrightarrow$-muodossa
  - φ esiintyy sekä parillisen että parittoman määrän ¬ alaisuudessa
- lauseessa voidaan sallia myös $\rightarrow$, koska $\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$

Lauseen [58] todistus

- ristiriidan johtamiseksi tarkastelemme tilannetta, jossa φ ja ψ tuottavat eri totuusarvon
- jonkin propositiomuuttujan arvon on oltava U, koska
  - muutoin φ tuottaa F tai T ja ψ tuottaa F tai T

  $\Rightarrow$ oletuksen $\varphi \Leftrightarrow \psi$ vuoksi φ tuottaa saman kuin ψ
- siis $\varphi(\mathsf{U})$ tuottaa eri totuusarvon kuin $\psi(\mathsf{U})$

  $\Rightarrow$ joko $\varphi(\mathsf{U})$ tai $\psi(\mathsf{U})$ ei tuota U
  - riittää tutkia $\psi(\mathsf{U})$, koska tapaus $\varphi(\mathsf{U})$ on samanlainen
- säännöllisyyden vuoksi $\psi(\mathsf{T}) \equiv \psi(\mathsf{U}) \equiv \psi(\mathsf{F})$
- jos $\varphi(\mathsf{T}) \equiv \psi(\mathsf{T})$ tai $\varphi(\mathsf{F}) \equiv \psi(\mathsf{F})$ ei päde, niin kiinnitämme ko. propositiomuuttujan arvoksi T tai F ja palaamme todistuksen alkuun
  - paluu ei voi uusiutua loputtomiin, koska kaavassa on vain äärellinen määrä propositiomuuttujia
- muussa tapauksessa $\varphi(\mathsf{T}) \equiv \psi(\mathsf{T}) \equiv \psi(\mathsf{U}) \equiv \psi(\mathsf{F}) \equiv \varphi(\mathsf{F})$ mutta ei $\varphi(\mathsf{U}) \equiv \psi(\mathsf{U})$

$\Rightarrow$ $\varphi(\mathsf{T}) \equiv \varphi(\mathsf{F})$ mutta ei $\varphi(\mathsf{T}) \equiv \varphi(\mathsf{U})$
  - ristiriita sen kanssa, että ollaan joko vain parillisen tai vain parittoman määrän $\neg$ alaisuudessa

Säännöllisyys tavallisen muuttujan suhteen

- olkoon $\varphi(x)$ kaava, jossa x on tavallinen muuttuja

  Olkoon $\mathfrak{f}_\perp$ määrittelemätön lauseke. Missä tahansa tilanteessa
  joko $\varphi(\mathfrak{f}_\perp)$ tuottaa U, tai $\varphi(a)$ tuottaa saman kuin $\varphi(\mathfrak{f}_\perp)$ [59]
  kun a on mikä tahansa puheenaiheen alkio.

- esim. jos $\varphi(x)$ on $x < 3 \rightarrow y \geq 0$, niin
  - jos $y < 0$, niin $\varphi(\sqrt{-1})$ tuottaa U
  - jos $y \geq 0$, niin $\varphi(\sqrt{-1})$ ja $\varphi(a)$ tuottavat T riippumatta a:n arvosta
- [59]:n pätevyys riippuu säännöistä [13] ja [14] sekä siitä,
  että kaavat muodostetaan vain kuten sivulla 55 kerrotaan

Seuraus

Jos $\lceil \mathfrak{f} \rfloor \Rightarrow \mathfrak{f} = \mathfrak{g}$, niin $\varphi(\mathfrak{f}) \Rightarrow \varphi(\mathfrak{g})$. [60]

- voi olla, että joissakin tilanteissa $\mathfrak{g}$ on määritelty mutta $\mathfrak{f}$ ei ole
  - esim. $\mathfrak{f}$ on $\frac{x-2}{x-2}$ ja $\mathfrak{g}$ on 1
  - sellaisessa tilanteessa $\varphi(\mathfrak{f})$ tuottaa U tai saman kuin $\varphi(\mathfrak{g})$ tuottaa
  - kumpikaan ei ole vastaesimerkki päättelyimplikaatiolle $\varphi(\mathfrak{f}) \Rightarrow \varphi(\mathfrak{g})$
- edellä selvitettiin, että muissa tilanteissa joko kumpikaan ei ole määritelty tai $\mathfrak{f} = \mathfrak{g}$
  - F (eli Filip on Jyväskylässä) tarkoittaa, että $\mathfrak{f}$ on määritelty eli $\lceil \mathfrak{f} \rfloor$
  - G (eli Greta on Jyväskylässä) tarkoittaa, että $\mathfrak{g}$ on määritelty eli $\lceil \mathfrak{g} \rfloor$
  - kumpikaan niistä ei voi tuottaa U, koska mikään $\lceil \ldots \rfloor$ ei tuota U [sivu 41]
  - H (eli he käyvät yhdessä Harjulla) tarkoittaa, että $\mathfrak{f} = \mathfrak{g}$ on tosi
  - $F \Rightarrow H$ [60]:n jos-osa
  - $H \Rightarrow F \wedge G$ [13]
  - H ei esiinny negaation alaisena, joten tapausta $H \equiv$ U ei tarvita (ei erotu tapauksesta $H \equiv$ F)
  - edellä osoitettiin, että näistä seuraa $\neg(G \wedge \neg F) \Rightarrow \neg F \wedge \neg G \vee H$
- niissä tilanteissa $\varphi(\mathfrak{f})$ ja $\varphi(\mathfrak{g})$ tuottavat saman totuusarvon

Päättelysäännöstä [60] seuraa, että (epä)yhtälö(ryhmiä) saa ratkaista seuraavasti

- määrittelemättömiä sievennetään määritellyiksi
  - esim. sievennetään $\frac{x-2}{x-2} \rightsquigarrow 1$ vaikka x voi olla 2
- lopuksi tarkastetaan määrittelemättömyyttä aiheuttavat juuret
  - hylätään ne, joilla koko kaava tuottaa U
- esim.

$$\begin{array}{lll}
& \frac{(x-1)(x-2)(x-3)}{x-2} = 2x-5 \lor x^2 - x = \frac{2x+2}{x+1} & \\
\Rightarrow & (x-1)(x-3) = 2x-5 \lor x^2 - x = 2 & [60] \\
\Leftrightarrow & x^2 - 4x + 3 = 2x - 5 \quad \lor x^2 - x - 2 = 0 & \\
\Leftrightarrow & x = 2 \lor x = 4 \quad \lor x = -1 \lor x = 2 & \\
\Leftrightarrow & x = -1 \lor x = 2 \lor x = 4 &
\end{array}$$

  - juurta $x = 4$ ei tarvitse tarkastaa, koska se ei aiheuta määrittelemättömyyttä
  - kun $x = -1$, tuottaa koko kaava U, joten $x = -1$ hylätään
  - kun $x = 2$, tuottaa koko kaava T, joten $x = 2$ hyväksytään
  - niinpä $\frac{(x-1)(x-2)(x-3)}{x-2} = 2x-5 \lor x^2 - x = \frac{2x+2}{x+1} \Leftrightarrow x = 2 \lor x = 4$

9 Reaalilukujen suuruusjärjestys

Käymme seuraavaksi läpi reaalilukujen suuruusjärjestyksen neljä perusominaisuutta

- kaikki reaalilukujen suuruusjärjestyksen ”tutut” ominaisuudet ovat pääteltävissä niistä
  - tarkemmin sanoen: reaaliluvut symboleilla 0, 1, $+$, $\cdot$ ja $<$ voidaan määritellä tavalla, jossa ei mainita $<$ muualla kuin niissä
  - muut maininnat voidaan hävittää sen avulla, että $a < b$ jos ja vain jos on olemassa sellainen c, että $\neg(c = 0) \wedge a + c^2 = b$

Jokaisella reaaliluvulla a ja b pätee täsmälleen yksi seuraavista: $a < b$, $a = b$ tai $b < a$.

- ilmaistaan yleensä sanallisesti, koska kaavana se on vaikeatajuinen:

$$(a < b \vee a = b \vee b < a) \wedge \neg(a < b \wedge a = b) \wedge \neg(a < b \wedge b < a) \wedge \neg(a = b \wedge b < a)$$

- jos a:n ja b:n tilalle laitetaan lausekkeet, niin väite muuttuu seuraavaan muotoon [44]:

  Jokaisessa mahdollisessa tilanteessa pätee täsmälleen yksi seuraavista: $\mathfrak{f}$ tai $\mathfrak{g}$ tai molemmat ovat määrittelemättömiä, $\mathfrak{f} < \mathfrak{g}$, $\mathfrak{f} = \mathfrak{g}$ tai $\mathfrak{g} < \mathfrak{f}$. [61]

- esim.
  - kun $x < 0$, pätee $\frac{1}{x} < 1$
  - kun $x = 0$, on $\frac{1}{x}$ määrittelemätön
  - kun $0 < x < 1$, pätee $1 < \frac{1}{x}$
  - kun $x = 1$, pätee $\frac{1}{x} = 1$
  - kun $1 < x$, pätee $\frac{1}{x} < 1$

Seuraava kaava on reaalilukujen laki, eli pätee jokaisella a ja b:

$$(a < b \vee a = b \vee b < a) \wedge \neg(a < b \wedge a = b) \wedge \neg(a < b \wedge b < a)$$

Jokaisella reaaliluvulla a, b ja c pätee: jos $a < b < c$, niin $a < c$.

- sama $\Rightarrow$:n avulla ilmaistuna: $a < b < c \;\Rightarrow\; a < c$
- sama $\wedge$:n avulla ilmaistuna: $a < b \wedge b < c \;\Rightarrow\; a < c$
- pätee myös kun a:n, b:n ja c:n tilalla on mielivaltaiset lausekkeet (harjoitustehtävä)

$$\mathfrak{f} < \mathfrak{g} < \mathfrak{h} \;\Rightarrow\; \mathfrak{f} < \mathfrak{h}$$ [62]

Jokaisella reaaliluvulla a, b ja c pätee: $a < b \Leftrightarrow a + c < b + c$.

- sama sanoilla ilmaistuna: $a < b$ jos ja vain jos $a + c < b + c$
- tietenkin myös $a < b \Leftrightarrow a - c < b - c$

$$
\begin{array}{lll}
 & a < b & \\
\Leftrightarrow & a + -c < b + -c & \text{edellinen, [47]} \\
\Leftrightarrow & a - c < b - c & a + -c = a - c,\ b + -c = b - c,\ \text{[19]}
\end{array}
$$

- sama tiiviimmin: $a < b \Leftrightarrow a - c = a + -c < b + -c = b - c \Leftrightarrow a - c < b - c$
- pätee myös kun a:n ja b:n tilalla on mielivaltaiset lausekkeet $\mathfrak{f}$ ja $\mathfrak{g}$, ja c:n tilalla on mielivaltainen määritelty lauseke $\mathfrak{h}$

Jos $\lceil \mathfrak{h} \rfloor$, niin $\mathfrak{f} < \mathfrak{g} \equiv \mathfrak{f} + \mathfrak{h} < \mathfrak{g} + \mathfrak{h}$.
Jos $\lceil \mathfrak{h} \rfloor$, niin $\mathfrak{f} < \mathfrak{g} \equiv \mathfrak{f} - \mathfrak{h} < \mathfrak{g} - \mathfrak{h}$. [63]

  - jos $\mathfrak{f}$ tai $\mathfrak{g}$ on määrittelemätön, tuottavat molemmat puolet U [14,13]
  - jos $\mathfrak{h}$:n ei tarvitsisi olla määritelty, voitaisiin johtaa mm. $0 < 1 \Leftrightarrow 0 + \frac{1}{0} < 1 + \frac{1}{0}$
- [63] muistuttaa päättelysääntöä [49]
- esimerkki: $a < 0 \Leftrightarrow 0 < -a$

$$
\begin{array}{lll}
 & a < 0 & \\
\Leftrightarrow & a - a < 0 - a & a \text{ on määritelty, [63]} \\
\Leftrightarrow & 0 < -a & a - a = 0,\ 0 - a = -a,\ \text{[19]}
\end{array}
$$

Jokaisella reaaliluvulla a ja b pätee: jos $0 < a$ ja $0 < b$, niin $0 < ab$.

- sama $\Rightarrow$:n ja $\wedge$:n avulla ilmaistuna: $0 < a \wedge 0 < b \;\Rightarrow\; 0 < ab$
- pätee myös kun a:n ja b:n tilalla on mielivaltaiset lausekkeet

$$0 < \mathfrak{f} \wedge 0 < \mathfrak{g} \;\Rightarrow\; 0 < \mathfrak{f}\mathfrak{g} \qquad [64]$$

- myös pätee $a < 0 \wedge 0 < b \;\Rightarrow\; ab < 0$

$$\begin{array}{lll}
 & a < 0 \wedge 0 < b & \\
\Leftrightarrow & 0 < -a \wedge 0 < b & a < 0 \Leftrightarrow 0 < -a,\ [22] \\
\Rightarrow & 0 < (-a)b & [64] \\
\Leftrightarrow & 0 < -ab & (-a)b = -ab,\ [19] \\
\Leftrightarrow & 0 + ab < -ab + ab & ab \text{ on määritelty, } [63] \\
\Leftrightarrow & ab < 0 & 0 + ab = ab,\ -ab + ab = 0,\ [19]
\end{array}$$

- sama esitettynä tiiviimmin, myös $a < 0 \Leftrightarrow 0 < -a$ johdettu, käytetyt lait näyttämättä

$$a < 0 \wedge 0 < b \;\Leftrightarrow\; 0 = a - a < 0 - a = -a \wedge 0 < b \;\Rightarrow\; 0 < (-a)b = -ab \;\Leftrightarrow\; ab = 0 + ab < -ab + ab = 0 \;\Leftrightarrow\; ab < 0$$

- tietenkin myös $0 < a \wedge 0 < b \;\Rightarrow\; 0 < \frac{a}{b}$
  - jos olisi $0 < a \wedge 0 < b \wedge \frac{a}{b} = 0$, niin olisi $a = \frac{a}{b} \cdot b = 0b = 0$ [16] $\;\Rightarrow\; a = 0$
  - jos olisi $0 < a \wedge 0 < b \wedge \frac{a}{b} < 0$, niin olisi $a = \frac{a}{b} \cdot b < 0$ [sivu 137] $\;\Rightarrow\; a < 0$
  - muita tapauksia ei ole [61]

Esimerkkejä

- $a < b \land 0 < c \;\Rightarrow\; ac < bc$ voidaan osoittaa seuraavasti:

	$a < b$	yksi lähtöoletuksista
$\Leftrightarrow$	$0 < b - a$	lisätty $-a$ [63], $a - a = 0$, [19]
$\Rightarrow$	$0 < (b-a)c$	edellinen, oletus $0 < c$, [64]
$\Leftrightarrow$	$0 < bc - ac$	$(b-a)c = bc - ac$, [19]
$\Leftrightarrow$	$ac < bc$	lisätty ac [63], $0 + ac = ac$, $(bc - ac) + ac = bc$, [19]

- $a < b \land c < 0 \;\Rightarrow\; bc < ac$ voidaan osoittaa seuraavasti:

	$c < 0$	yksi lähtöoletuksista
$\Leftrightarrow$	$0 < -c$	lisätty $-c$ [63], $c - c = 0$, $0 - c = -c$, [19]
$\Rightarrow$	$a(-c) < b(-c)$	oletus $a < b$, edellinen ja $a < b \land 0 < c \Rightarrow ac < bc$ [45]
$\Leftrightarrow$	$-ac < -bc$	$a(-c) = -ac$, $b(-c) = -bc$, [19]
$\Leftrightarrow$	$bc < ac$	lisätty $ac + bc$ [63], puolet sievennetty, [19]

Kolme tuttua merkintää

$\mathfrak{f} > \mathfrak{g}$ tarkoittaa samaa kuin $\mathfrak{g} < \mathfrak{f}$.

$\mathfrak{f} \leq \mathfrak{g}$ tarkoittaa samaa kuin $\mathfrak{f} < \mathfrak{g} \vee \mathfrak{f} = \mathfrak{g}$. [65]

$\mathfrak{f} \geq \mathfrak{g}$ tarkoittaa samaa kuin $\mathfrak{g} < \mathfrak{f} \vee \mathfrak{f} = \mathfrak{g}$ tarkoittaa samaa kuin $\mathfrak{f} > \mathfrak{g} \vee \mathfrak{f} = \mathfrak{g}$.

Esimerkki: seuraavasti voidaan osoittaa, että jokaisella a pätee $a^2 \geq 0$

jos $a = 0$, niin		$a^2 = 0$	$0^2 = 0$, [19] takaperin
	$\Rightarrow$	$0 < a^2 \vee a^2 = 0$	[37]
	$\Leftrightarrow$	$a^2 \geq 0$	[65]
jos $a > 0$, niin		$aa > 0$	[65], $0 < a$ ja $0 < a$ [64]
	$\Leftrightarrow$	$a^2 > 0$	$aa = a^2$, [19]
	$\Rightarrow$	$0 < a^2 \vee a^2 = 0$	[65,36]
	$\Leftrightarrow$	$a^2 \geq 0$	[65]
jos $a < 0$, niin		$0a < aa$	$a < b \wedge c < 0 \Rightarrow bc < ac$ [sivu 138] (*)
	$\Leftrightarrow$	$a^2 > 0$	$0a = 0$, $aa = a^2$, [19,65]
	$\Rightarrow$	$a^2 \geq 0$	kuten edellä
T	$\Leftrightarrow$	$a < 0 \vee a = 0 \vee a > 0$	[61]
	$\Rightarrow$	$a^2 \geq 0$	[38]

(*) sijoittamalla a:ksi a, b:ksi 0 ja c:ksi a laki $a < b \wedge c < 0 \;\Rightarrow\; bc < ac$
tuottaa $a < 0 \wedge a < 0 \;\Rightarrow\; 0a < aa$

Kertolaskun tuloksen etumerkki

	$b<0$	$b>0$
$a<0$	$ab>0$	$ab<0$
$a>0$	$ab<0$	$ab>0$

	$b\leq 0$	$b=0$	$b\geq 0$
$a\leq 0$	$ab\geq 0$	$ab=0$	$ab\leq 0$
$a=0$	$ab=0$	$ab=0$	$ab=0$
$a\geq 0$	$ab\leq 0$	$ab=0$	$ab\geq 0$

- oikea alanurkka seuraa suoraan laista [64]
- oikea ylänurkka osoitettiin sivulla 137
- jos $a>0$ ja $b<0$, niin
  - $b<0$ ja $a>0$ [5]

  $\Rightarrow$ oikean ylänurkan mukaan $ba<0$

  $\Rightarrow$ vasen alanurkka, koska $ba=ab$
- vasen ylänurkka harjoitustehtäväksi
- tapaukset $ab=0$ ovat ilmeiset
- $\leq$- ja $\geq$-tapaukset seuraavat $<$- ja $>$-tapauksista ja siitä, että $a=0\vee b=0\Rightarrow ab=0$

Jakolaskulle $\frac{a}{b}$ pätevät muuten samat taulukot, mutta jakaja b ei saa olla 0

- jos $b\neq 0$, niin $\frac{a}{b}=a\cdot\frac{1}{b}$ ja $\frac{1}{b}$:llä on sama etumerkki kuin b:llä
  - aina $\frac{1}{b}\neq 0$
  - jos olisi $b>0$ ja $\frac{1}{b}<0$ tai $b<0$ ja $\frac{1}{b}>0$, niin olisi $1=b\cdot\frac{1}{b}<0$

$$b>0 \;\Leftrightarrow\; \frac{1}{b}>0 \;\text{ ja }\; b<0 \;\Leftrightarrow\; \frac{1}{b}<0\,. \qquad [66]$$

Päättelysäännön [50] vastine <:lle

$$\mathfrak{h} \neq 0 \wedge \mathfrak{f} < \mathfrak{g} \;\Leftrightarrow\; \mathfrak{h} < 0 \wedge \mathfrak{f}\mathfrak{h} > \mathfrak{g}\mathfrak{h} \vee \mathfrak{h} > 0 \wedge \mathfrak{f}\mathfrak{h} < \mathfrak{g}\mathfrak{h}$$
$$\mathfrak{h} \neq 0 \wedge \mathfrak{f} < \mathfrak{g} \;\Leftrightarrow\; \mathfrak{h} < 0 \wedge \frac{\mathfrak{f}}{\mathfrak{h}} > \frac{\mathfrak{g}}{\mathfrak{h}} \vee \mathfrak{h} > 0 \wedge \frac{\mathfrak{f}}{\mathfrak{h}} < \frac{\mathfrak{g}}{\mathfrak{h}} \qquad [67]$$

- tarkastelemme mitä tahansa mahdollista tilannetta
- jos $\mathfrak{h}$ ei ole määritelty, niin $\mathfrak{h} \neq 0$, $\mathfrak{h} < 0$ ja $\mathfrak{h} > 0$ tuottavat U
  $\Rightarrow$ kumpikin puoli tuottaa U tai F
- jos $\mathfrak{f}$ tai $\mathfrak{g}$ ei ole määritelty, niin $\mathfrak{f} < \mathfrak{g}$, $\mathfrak{f}\mathfrak{h} > \mathfrak{g}\mathfrak{h}$, $\mathfrak{f}\mathfrak{h} < \mathfrak{g}\mathfrak{h}$, $\frac{\mathfrak{f}}{\mathfrak{h}} > \frac{\mathfrak{g}}{\mathfrak{h}}$ ja $\frac{\mathfrak{f}}{\mathfrak{h}} < \frac{\mathfrak{g}}{\mathfrak{h}}$ tuottavat U
  $\Rightarrow$ kumpikin puoli tuottaa U tai F
- muussa tapauksessa olkoot a, b ja c ne luvut, jotka $\mathfrak{f}$, $\mathfrak{g}$ ja $\mathfrak{h}$ tuottavat
- jos $c = 0$, niin $\mathfrak{h} \neq 0$, $\mathfrak{h} < 0$ ja $\mathfrak{h} > 0$ tuottavat F
  $\Rightarrow$ kumpikin puoli tuottaa F
- jos $c > 0$, niin $\mathfrak{h} \neq 0$ ja $\mathfrak{h} > 0$ tuottavat T, $\mathfrak{h} < 0$ tuottaa F, ja $\mathfrak{f} < \mathfrak{g}$, $ac < bc$, $\mathfrak{f}\mathfrak{h} < \mathfrak{g}\mathfrak{h}$, $\frac{a}{c} < \frac{b}{c}$ ja $\frac{\mathfrak{f}}{\mathfrak{h}} < \frac{\mathfrak{g}}{\mathfrak{h}}$ tuottavat saman kuin $a < b$ [sivu 138], [66]
  $\Rightarrow$ kumpikin puoli tuottaa saman kuin $a < b$
- loput perustelusta harjoitustehtäväksi

Päättelysäännön [50] vastine ≤:lle

$$\mathfrak{h} \neq 0 \wedge \mathfrak{f} \leq \mathfrak{g} \;\Leftrightarrow\; \mathfrak{h} < 0 \wedge \mathfrak{f}\mathfrak{h} \geq \mathfrak{g}\mathfrak{h} \vee \mathfrak{h} > 0 \wedge \mathfrak{f}\mathfrak{h} \leq \mathfrak{g}\mathfrak{h}$$
$$\mathfrak{h} \neq 0 \wedge \mathfrak{f} \leq \mathfrak{g} \;\Leftrightarrow\; \mathfrak{h} < 0 \wedge \frac{\mathfrak{f}}{\mathfrak{h}} \geq \frac{\mathfrak{g}}{\mathfrak{h}} \vee \mathfrak{h} > 0 \wedge \frac{\mathfrak{f}}{\mathfrak{h}} \leq \frac{\mathfrak{g}}{\mathfrak{h}}$$

Päättelysäännön [51] vastine $<$:lle

$$\frac{\mathfrak{f}}{\mathfrak{g}} < \mathfrak{h} \;\Leftrightarrow\; \mathfrak{g} < 0 \land \mathfrak{f} > \mathfrak{g}\mathfrak{h} \lor \mathfrak{g} > 0 \land \mathfrak{f} < \mathfrak{g}\mathfrak{h} \qquad [68]$$

- tarkastelemme mitä tahansa mahdollista tilannetta
- jos $\mathfrak{f}$, $\mathfrak{g}$ tai $\mathfrak{h}$ ei ole määritelty, niin $\frac{\mathfrak{f}}{\mathfrak{g}} < \mathfrak{h}$, $\mathfrak{f} > \mathfrak{g}\mathfrak{h}$ ja $\mathfrak{f} < \mathfrak{g}\mathfrak{h}$ tuottavat U
  $\Rightarrow$ kumpikin puoli tuottaa U tai F
- muussa tapauksessa olkoot a, b ja c ne luvut, jotka $\mathfrak{f}$, $\mathfrak{g}$ ja $\mathfrak{h}$ tuottavat
- jos $b = 0$, niin vasen puoli tuottaa U ja oikea puoli tuottaa F
- jos $b > 0$, niin $\mathfrak{g} < 0$ tuottaa F, $\mathfrak{g} > 0$ tuottaa T,
  ja $\frac{\mathfrak{f}}{\mathfrak{g}} < \mathfrak{h}$ ja $\mathfrak{f} < \mathfrak{g}\mathfrak{h}$ tuottavat saman kuin $a < bc$
  - kumpikin puoli tuottaa saman kuin $a < bc$
- muussa tapauksessa $b < 0$, joten kumpikin puoli tuottaa saman kuin $a > bc$

$a \geq b \geq c \;\Rightarrow\; a \geq c$ voidaan osoittaa seuraavasti:

- $a \geq b \geq c$ tarkoittaa samaa kuin $a \geq b \wedge b \geq c$
- $\mathfrak{f} \geq \mathfrak{g}$ tarkoittaa samaa kuin $\mathfrak{f} > \mathfrak{g} \vee \mathfrak{f} = \mathfrak{g}$ [65]
- $a \geq b \wedge b = c \;\Leftrightarrow\; a \geq c \wedge b = c \;\Rightarrow\; a \geq c$ [5,21,33]
- $a = b \wedge b \geq c \;\Leftrightarrow\; a = b \wedge a \geq c \;\Rightarrow\; a \geq c$ [21,2,34]
- $a > b \wedge b > c \;\Rightarrow\; a > c \;\Rightarrow\; a > c \vee a = c \;\Leftrightarrow\; a \geq c$ [62,36,65]
- nämä kattavat kaikki tapaukset, koska jos $a \geq b \wedge b \geq c$ mutta ei $a = b$ eikä $b = c$, niin $a > b \wedge b > c$
- osatulokset voidaan yhdistää päättelysäännöllä [38]:
  - $a \geq b \wedge b = c \;\Rightarrow\; a \geq c$
  - $a = b \wedge b \geq c \;\Rightarrow\; a \geq c$
  - $a > b \wedge b > c \;\Rightarrow\; a \geq c$

Pätellessä muodostetaan usein ketjuja muotoa $\mathfrak{f}_0 \sim_1 \mathfrak{f}_1 \sim_2 \ldots \sim_n \mathfrak{f}_n$, missä kukin $\sim_i$ on $<$, $\leq$, $=$, $\neq$, $\geq$ tai $>$

jokin $\sim_i$	muut $\sim_i$	saa päätellä		
$=$	$=$	$\mathfrak{f}_0 = \mathfrak{f}_n$	$\mathfrak{f}_0 \leq \mathfrak{f}_n$	$\mathfrak{f}_0 \geq \mathfrak{f}_n$
$\leq$	$\leq\ =$	$\mathfrak{f}_0 \leq \mathfrak{f}_n$		
$<$	$<\ \leq\ =$	$\mathfrak{f}_0 < \mathfrak{f}_n$	$\mathfrak{f}_0 \leq \mathfrak{f}_n$	$\mathfrak{f}_0 \neq \mathfrak{f}_n$
$\geq$	$\geq\ =$	$\mathfrak{f}_0 \geq \mathfrak{f}_n$		
$>$	$>\ \geq\ =$	$\mathfrak{f}_0 > \mathfrak{f}_n$	$\mathfrak{f}_0 \geq \mathfrak{f}_n$	$\mathfrak{f}_0 \neq \mathfrak{f}_n$
$\neq$	$=$	$\mathfrak{f}_0 \neq \mathfrak{f}_n$		

- jos $\mathfrak{f}$ on määritelty, niin saa päätellä $\mathfrak{f} = \mathfrak{f}$, $\mathfrak{f} \leq \mathfrak{f}$ ja $\mathfrak{f} \geq \mathfrak{f}$ [20,65]

Vielä yksi päättelysääntö

$$\mathfrak{f} \leq \mathfrak{g} \land \mathfrak{f} \geq \mathfrak{g} \;\Leftrightarrow\; \mathfrak{f} = \mathfrak{g} \qquad [69]$$

- perustelu
  - jos $\mathfrak{f} = \mathfrak{g}$, niin kumpikin puoli tuottaa T
  - jos $\mathfrak{f} < \mathfrak{g}$, niin $\mathfrak{f} \geq \mathfrak{g}$ ja $\mathfrak{f} = \mathfrak{g}$ tuottavat F [61], joten kumpikin puoli tuottaa F
  - jos $\mathfrak{g} < \mathfrak{f}$, niin ..., joten kumpikin puoli tuottaa F
  - muussa tapauksessa $\mathfrak{f}$ tai $\mathfrak{g}$ ei ole määritelty [61], joten kumpikin puoli tuottaa U
- seuraus: jos $\mathfrak{f}_1 \leq \mathfrak{f}_2 \leq \ldots \leq \mathfrak{f}_n \leq \mathfrak{f}_1$, niin $\mathfrak{f}_1 = \mathfrak{f}_2 = \ldots = \mathfrak{f}_n$

Jatkoa varten osoitamme $\sqrt{b} \leq a \leq -\sqrt{b} \;\Leftrightarrow\; a = b = 0$

- oletamme seuraavat tunnetuiksi:
  - $\sqrt{0} = 0$
  - jos $b > 0$, niin $\sqrt{b} > 0$
- jos $b < 0$, niin $\sqrt{b}$ ei ole määritelty [53]
  $\Rightarrow$ $\sqrt{b} \leq a \leq -\sqrt{b}$ ei ole tosi [13]
  - toisaalta $\Leftrightarrow$:n oikea puoli ei ole tosi, koska $b = 0$ ei ole tosi [61]

  $\Rightarrow$ $\Leftrightarrow$:n kumpikaan puoli ei ole tosi
- jos $b = 0$, niin
  - $\sqrt{b} \leq a \leq -\sqrt{b} \;\Leftrightarrow\; 0 \leq a \leq 0 \;\Leftrightarrow\; a = 0$ [19,69]
  - $a = b = 0 \;\Leftrightarrow\; a = 0 = 0 \;\Leftrightarrow\; a = 0$

  $\Rightarrow$ niinpä $\sqrt{b} \leq a \leq -\sqrt{b} \;\Leftrightarrow\; \ldots \;\Leftrightarrow\; a = 0 \;\Leftrightarrow\; \ldots \;\Leftrightarrow\; a = b = 0$
- muussa tapauksessa $b > 0$ [61]
  $\Rightarrow$ $\sqrt{b} > 0$
  $\Rightarrow$ jos $\Leftrightarrow$:n vasen puoli olisi tosi, niin $0 < \sqrt{b} \leq a \leq -\sqrt{b} < 0$ [63]
  $\Rightarrow$ $0 < 0$ [62]
  - niinpä $\Leftrightarrow$:n vasen puoli ei ole tosi [61]

  $\Rightarrow$ $\Leftrightarrow$:n kumpikaan puoli ei ole tosi

Esimerkki: ratkaisemme y:n epäyhtälöstä $(x-3)^2+(y-2)^2 \le 1$

- vähentämällä $(x-3)^2$ molemmilta puolilta [63,19] saadaan
  $$(x-3)^2+(y-2)^2 \le 1 \;\Leftrightarrow\; (y-2)^2 \le 1-(x-3)^2$$
- nyt tarvittaisiin molemmilta puolilta neliöjuuri, mutta miten merkit käyttäytyvät?
- aputulos: ratkaisemme a:n epäyhtälöstä $a^2 \le b^2$ summan ja erotuksen tulon kaavalla

$$\begin{array}{lll} & a^2 \le b^2 & \\ \Leftrightarrow & a^2-b^2 \le 0 & \text{lisätty } -b^2 \text{ [63,19]} \\ \Leftrightarrow & (a+b)(a-b) \le 0 & \text{[sivu 102] takaperin, [19]} \\ \Leftrightarrow & a+b \le 0 \land a-b \ge 0 \;\lor\; a+b \ge 0 \land a-b \le 0 & \text{tulon etumerkki} \\ \Leftrightarrow & b \le a \le -b \;\lor\; -b \le a \le b & \text{lisätty } b \text{ tai } -b \end{array}$$

- aputulos: ratkaisemme a:n epäyhtälöstä $a^2 \le b$
  - $a^2 \le b \;\Leftrightarrow\; b \ge 0 \land a^2 \le b$, koska $a^2 \le b \;\Rightarrow\; b \ge 0$, koska $a^2 \ge 0$ (harjoitusteht.)
  - oletuksella $b \ge 0$

$$\begin{array}{lll} & a^2 \le b & \\ \Leftrightarrow & a^2 \le \left(\sqrt{b}\right)^2 & b = \left(\sqrt{b}\right)^2 \text{ [52], [19]} \\ \Leftrightarrow & (\sqrt{b} \le a \le -\sqrt{b} \;\lor\; -\sqrt{b} \le a \le \sqrt{b}) & a^2 \le b^2 \text{ juuret, [47]} \\ \Leftrightarrow & (a = b = 0 \;\lor\; -\sqrt{b} \le a \le \sqrt{b}) & \text{[sivu 145], [22]} \\ \Leftrightarrow & -\sqrt{b} \le a \le \sqrt{b} & a = b = 0 \Rightarrow -\sqrt{b} \le \ldots, \text{ [38,37]} \end{array}$$

  - siis $a^2 \le b \;\Leftrightarrow\; b \ge 0 \land a^2 \le b \;\Leftrightarrow\; b \ge 0 \land -\sqrt{b} \le a \le \sqrt{b}$ [39]

- aputuloksen mukaan

$$\begin{array}{ll} & (y-2)^2 \leq 1-(x-3)^2 \\ \Leftrightarrow & 1-(x-3)^2 \geq 0 \wedge -\sqrt{1-(x-3)^2} \leq y-2 \leq \sqrt{1-(x-3)^2} \end{array}$$

- ratkaisemme alkuosan

$$\begin{array}{lll} & 1-(x-3)^2 \geq 0 & \\ \Leftrightarrow & (x-3)^2 \leq 1 & (x-3)^2 \text{ lisätty, puolet vaihdettu} \\ \Leftrightarrow & 1 \geq 0 \wedge -\sqrt{1} \leq x-3 \leq \sqrt{1} & \text{aputulos} \\ \Leftrightarrow & -1 \leq x-3 \leq 1 & 1 \geq 0 \Leftrightarrow \mathsf{T},\ \sqrt{1}=1 \\ \Leftrightarrow & 2 \leq x \leq 4 & 3 \text{ lisätty} \end{array}$$

- yhdistämme osatulokset ja lisäämme 2:n

$$\begin{array}{ll} & (x-3)^2+(y-2)^2 \leq 1 \\ \Leftrightarrow & 1-(x-3)^2 \geq 0 \wedge -\sqrt{1-(x-3)^2} \leq y-2 \leq \sqrt{1-(x-3)^2} \\ \Leftrightarrow & 2 \leq x \leq 4 \wedge 2-\sqrt{1-(x-3)^2} \leq y \leq 2+\sqrt{1-(x-3)^2} \end{array}$$

10 Predikaattilogiikkaa luonnollisille luvuille

Luonnollisten lukujen joukko $\mathbb{N} = \{0, 1, 2, \ldots\}$

- jotkut kirjoittajat aloittavat luonnolliset luvut ykkösestä
- logiikassa ja tietojenkäsittelytieteessä ne aloitetaan melkein aina **nollasta**
- vähennyslasku $n - m$ on määritelty jos ja vain jos $n \geq m$; silloin $(n - m) + m = n$

⇒ päättelyssä on usein tarpeen tarkastaa, että vähennyslasku on määritelty

Ohjelmoinnissa lähin vastine on erikokoiset `unsigned`-tyypit

- perus-`unsigned`-luvut ovat tyypillisesti $0, 1, \ldots, 2^{32} - 1$ eli $0, 1, \ldots, 4\,294\,967\,295$
- ohjelmoinnissa kaikilla lukujen perustyypeillä on myös ylivuodon vaara

⇒ ohjelmista päätellessä on tarpeen tarkastaa sekä ali- että ylivuodot

- b-bittisillä `unsigned`-luvuilla tyypillinen tietokone laskee modulo 2^b
  - tulos pakotetaan välille $0, \ldots, 2^b - 1$ lisäämällä tarvittaessa 2^b:n monikerta
- esim. 32-bittisillä `unsigned`-luvuilla

```
n = 1000; m = 968295; std::cout << n-m << ' ';
n = 3000000000; std::cout << 2*n << '\n';
```

  tulostaa `4294000001 1705032704`
- luonnollisia lukuja esittämään voi käyttää myös `int`- yms. tyyppejä, kunhan varoo tuottamasta negatiivisia lukuja

Luonnollisten lukujen suuruusjärjestyksen omia lakeja

- [61], . . . , [64], [65] ja [69] pätevät myös luonnollisille luvuille ja kokonaisluvuille
  - esim. [66] ei voi käyttää kokonaisluvuille, koska $\frac{1}{b}$ ei yleensä ole kokonaisluku
- luonnollisille luvuille ja kokonaisluvuille pätee lisäksi

$$n > m \;\Leftrightarrow\; n \geq m+1 \qquad [70]$$

- luonnollisille luvuille pätee lisäksi

$n \geq m$ jos ja vain jos on olemassa sellainen k, että $n = m+k$. [71]

$$n+m \geq n \qquad [72]$$

Jos $n-m$ on määritelty, niin $n-m \leq n$. [73]

$$n = 0 \vee n > 0 \qquad [74]$$

$$n > 0 \Rightarrow nm \geq m \qquad [75]$$

- [72] seuraa laista [71] valitsemalla n:ksi $n+m$, m:ksi n ja k:ksi m
- jos $n-m$ on määritelty, niin $(n-m)+m = n$
  - [73] seuraa laista [72] valitsemalla n:ksi $n-m$ ja m:ksi m
- [74] harjoitustehtäväksi
- [75] seuraa siitä, että jos $n > 0$, niin $n \geq 1$ [70]
  $\Rightarrow$ $n-1$ on määritelty ja $(n-1)+1 = n$
  $\Rightarrow$ $nm = ((n-1)+1)m = (n-1)m+m \geq m$ [16,72]

Luonnollisilla luvuilla ei voi laskea jakolaskuja samoin kuin reaaliluvuilla

- esim. reaalilukujen $\frac{1}{3}$ ei ole kokonaisluku

⇒ lasketaan *osamäärä* $n \operatorname{div} d$ ja *jakojäännös* $n \bmod d$
  - ohjelmoinnissa esim. `n / d` ja `n % d`

- esim. jaetaan 25 ilmapalloa 7 lapselle mahdollisimman tasan
  - jokainen lapsi saa 3 ilmapalloa
  - jakamatta jää 4 ilmapalloa
  - $25 = 7 \cdot 3 + 4$

$$\begin{aligned}\text{(ilmapallojen kokonaismäärä)} &= \quad \text{(lasten määrä)} \cdot \text{(kunkin lapsen saama määrä)} \\ &\quad + \text{(yli jääneiden määrä)}\end{aligned}$$

- yleisemmin $n = d(n \operatorname{div} d) + (n \bmod d)$
- ilmapalloja jaetaan lapsille niin paljon kuin mahdollista

⇒ yli jääneiden määrä on pienempi kuin lasten määrä
  - muutenhan jokaiselle lapselle voitaisiin antaa ainakin yksi ilmapallo lisää

- yleisemmin $n \bmod d < d$

Saatiin luonnollisten lukujen *jakoyhtälö*

$$\text{Jos } d > 0, \text{ niin } \; n = d(n \operatorname{div} d) + (n \bmod d) \; \text{ ja } \; n \bmod d < d \; . \qquad [76]$$

- kun $d > 0$, niin vaikka jakoyhtälö ei kerro, miten $n \operatorname{div} d$ ja $n \bmod d$ lasketaan, se silti määrää ne yksikäsitteisesti

Tarvitsemme jatkossa seuraavia ominaisuuksia

$n \operatorname{div} 0$ ja $n \bmod 0$ eivät ole määritellyt. [77]

- muistisääntö: nollalla ei voi jakaa
- matemaattisempi syy: niitä ei voi määritellä siten, että jakoyhtälö ei mene rikki
  - osuus $n \bmod d < d$ ei voi luonnollisilla luvuilla toteutua, jos $d = 0$
  - osuus $n = d(n \operatorname{div} d) + (n \bmod d)$ ei ota kantaa siihen paljonko $n \operatorname{div} d$ on, jos $d = 0$

Jos $d > 0$, niin $n \bmod d = n - d(n \operatorname{div} d)$. [78]

- [76]:n välitön seuraus

Jos $d > 0$, niin $n \bmod d \leq n$. [79]

- edellisen välitön seuraus [73]

Jos $n < d$, niin $n \operatorname{div} d = 0$ ja $n \bmod d = n$. [80]

- koska $n < d$, on $d > 0$ [74], joten $n \operatorname{div} d$ ja $n \bmod d$ ovat määritellyt
- jos olisi $n \operatorname{div} d > 0$, niin olisi $n = d(n \operatorname{div} d) + (n \bmod d) \geq d(n \operatorname{div} d) \geq d$ [76,72,75]
- muutoin $n \operatorname{div} d = 0$ [74], joten $n = d(n \operatorname{div} d) + (n \bmod d) = n \bmod d$

Tekijä

d on n:n *tekijä*, jos ja vain jos on olemassa sellainen k, että $n = dk$. [81]

- merkitään $d \mid n$
- tämä on sanan ”tekijä” ja merkinnän ”$d \mid n$” määritelmä, joten sitä ei tarvitse osoittaa
  - ei kerro matemaattista tosiasiaa
  - kertoo nimen ja symbolin, jotka on annettu eräälle käsitteelle
- tällöin myös $k \mid n$, koska $dk = kd$
- $d \nmid n$ tarkoittaa samaa kuin $\neg(d \mid n)$

Onko 0 0:n tekijä?

- määritelmän [81] mukaan on: $0 = 0 \cdot 3810$
- kirjallisuudessa esiintyy myös vaihtoehtoinen määritelmä, jossa erikseen sanotaan, että tekijän pitää olla muu kuin 0
  - sillä määritelmällä d on n:n tekijä jos ja vain jos jakolasku $\frac{n}{d}$ menee tasan
- tällaiset yksityiskohdat valitaan usein sen mukaan, mikä on jatkossa kätevintä
  - ⇒ tällaiset erot käsitteiden sisällössä ovat matematiikassa tavallisia
  - ⇒ jos lukee monia lähteitä, pitää ottaa huomioon, että sama sana tai merkintä voi tarkoittaa niissä hieman eri asiaa

Seuraavat pätevät jokaisella n ja d

$$1 \mid n \text{ ja } n \mid n \qquad [82]$$

- koska $n = 1n$ [81]

$$d \mid 0 \qquad [83]$$

- koska $0 = d \cdot 0$ [81]

Jos $n > 0$ ja $d \mid n$, niin $0 < d \leq n$. [84]

- jos $n > 0$ ja $d \mid n$, niin
  - on olemassa sellainen k, että $n = dk$ [81]
  - $d > 0$ ja $k > 0$, koska muutoin olisi $d = 0 \vee k = 0$ [74] ja $n = dk = 0$

  $\Rightarrow$ $n = kd \geq d$ [75]

Jos $d \mid n$ ja $d \mid m$, niin $d \mid (n+m)$. [85]

- jos $n = dk$ ja $m = dh$, niin $n + m = dk + dh = d(k+h)$ [81]

Jos $n \geq m$ ja $d \mid n$ ja $d \mid m$, niin $d \mid (n-m)$. [86]

- olkoot $n = dk$ ja $m = dh$
- jos $k \leq h$, niin $n = dk \leq dh = m$

$\Rightarrow$ jos $n > m$, niin $k > h$, joten $n - m = dk - dh = d(k-h)$ [81]

- jos $n = m$, niin $n - m = 0$, joten $d \mid (n-m)$ [83]

Osoitamme, että

$$d > 0 \wedge (d \mid n) \;\Leftrightarrow\; n \bmod d = 0 \qquad [87]$$

- jos $n \bmod d = 0$, niin
  - $n \bmod d$ on määritelty [13], joten $d > 0$ [77]
  - $n = d(n \operatorname{div} d)$ [76], joten $d \mid n$ [81]
- jos $d > 0$ ja $d \mid n$, niin
  - on olemassa sellainen k, että $n = dk$ [81]
  - $n \bmod d = n - d(n \operatorname{div} d) = dk - d(n \operatorname{div} d) = d(k - (n \operatorname{div} d))$ [78]
  - koska $n \bmod d < d$ [76], pätee $d(k - (n \operatorname{div} d)) < d$, joten $k - (n \operatorname{div} d) < 1$

  $\Rightarrow$ $k - (n \operatorname{div} d) = 0$ [74]

  $\Rightarrow$ $n \bmod d = d(k - (n \operatorname{div} d)) = d \cdot 0 = 0$

Suurin yhteinen tekijä

- greatest common divisor

  $\mathrm{gcd}(n,m)$ on suurin luku, joka on sekä n:n että m:n tekijä. [88]

  Jos $n > 0$, niin $0 < \mathrm{gcd}(n,m) = \mathrm{gcd}(m,n) \leq n$.
  Jos $m > 0$, niin $0 < \mathrm{gcd}(n,m) = \mathrm{gcd}(m,n) \leq m$. [89]

- 1 on n:n ja m:n yhteinen tekijä [82]
- jos $n > 0$, niin mikään luku, joka on suurempi kuin n, ei ole n:n tekijä [84]
- jos $m > 0$, niin mikään luku, joka on suurempi kuin m, ei ole m:n tekijä

$\Rightarrow$ $\mathrm{gcd}(n,m)$ ja $\mathrm{gcd}(m,n)$ ovat olemassa ja ovat luvatulla välillä

- ”sekä n:n että m:n tekijä” tarkoittaa samaa kuin ”sekä m:n että n:n tekijä”

$\Rightarrow$ $\mathrm{gcd}(n,m) = \mathrm{gcd}(m,n)$

  $\mathrm{gcd}(0,0)$ ei ole määritelty. [90]

- jokainen luonnollinen luku on 0:n tekijä [83]

$\Rightarrow$ suurinta 0:n ja 0:n tekijää ei ole

- vaihtoehtoinen tulkinta
  - jotkut tulkitsevat ”suurin” tarkoittamaan ”jaollinen mahdollisimman isoilla luvuilla”
  - heille $\mathrm{gcd}(0,0) = 0$

Sovelluksia

- murtolukujen sieventäminen:
  - jos $g = \gcd(n,m)$, niin $\dfrac{n}{m} = \dfrac{\frac{n}{g}}{\frac{m}{g}}$
  - $\frac{n}{m}$ ei sievene enempää
- vastaava toiminto polynomeille on tärkeä tietokonealgebrassa
- käytössä myös mm. salausmenetelmissä

Suurimman yhteisen tekijän laskeminen sopii algoritmien todistamiseen tutustumiseen

- yksinkertainen, mutta silti tehokas ja hyödyllinen algoritmi
- tarvitsee vain osan algoritmien todistamisen perustekniikoista

Suurin yhteinen tekijä voidaan laskea nopeasti modernilla Eukleideen algoritmilla

```
unsigned gcd( unsigned n, unsigned m ){
  while( true ){
    if( m == 0 ){ return n; }
    n %= m;
    if( n == 0 ){ return m; }
    m %= n;
  }
}
```

- palauttaa $\gcd(n,m)$ jos se on olemassa, ja 0 muutoin
  - 0 sopii merkiksi siitä, että $\gcd(n,m)$ ei ole olemassa, koska aina $\gcd(n,m) \neq 0$ [89]
  - jos olisimme määritelleet $\gcd(0,0) = 0$, olisi tulos 0 silti oikein
- `unsigned` on ylivuotovaaraa lukuun ottamatta sama kuin luonnollinen luku
  - suurin `unsigned`-luku on tyypillisesti $2^{32} - 1 = 4\,294\,967\,295$
- `n %= m` tarkoittaa $n := n \bmod m$

Ei määrittelemättömiä toimintoja

- algoritmin ainoa toiminto, joka ei ole aina määritelty, on $\bmod$
- $\bmod$ on määritelty, jos ja vain jos jakaja ei ole 0
- molemmissa algoritmin $\bmod$:ssa edeltävä **if**-lause varmistaa, että jakaja ei ole 0

```
1 unsigned gcd( unsigned n, unsigned m ){
2   while( true ){
3     if( m == 0 ){ return n; }
4     n %= m;
5     if( n == 0 ){ return m; }
6     m %= n;
7   }
8 }
```

Jatkossa

- g tarkoittaa algoritmin lopputulosta eli algoritmin palauttamaa arvoa
- n_i ja m_i, missä $1 \leq i \leq 7$, tarkoittavat muuttujien `n` ja `m` arvoja rivin i alussa

Pätee

- kun riville 2 tullaan ensimmäisen kerran, niin $n_2 = n_1 \wedge m_2 = m_1$
- $n_3 = n_2 \wedge m_3 = m_2$
- jos suoritus etenee riville 4, niin $n_4 = n_3 \wedge n_5 = n_4 \bmod m_4 \wedge m_5 = m_4 = m_3 > 0$
- jos suoritus etenee riville 6, niin $n_7 = n_6 = n_5 > 0 \wedge m_6 = m_5 \wedge m_7 = m_6 \bmod n_6$
- kun riville 2 tullaan muulloin kuin ensimmäisen kerran, niin $n_2 = n_7 \wedge m_2 = m_7$
- jos lopetetaan, niin $g = n_3 \wedge m_3 = 0 \vee n_5 = 0 \wedge g = m_5$

```
1 unsigned gcd( unsigned n, unsigned m ){
2   while( true ){
3     if( m == 0 ){ return n; }
4     n %= m;
5     if( n == 0 ){ return m; }
6     m %= n;
7   }
8 }
```

Osoitamme, että algoritmi lopettaa

- n ja m eivät koskaan kasva, koska aina $n \bmod m \leq n$ ja $m \bmod n \leq m$ [79]
- jokaisella kierroksella, jolla ei lopeteta, joko n tai m tai molemmat pienenevät
  - jos $n_4 \geq m_4$, niin $n_5 = n_4 \bmod m_4 < m_4 \leq n_4$ [76]
  - kuten edellä todettiin, $n_4 = n_3 = n_2$, koska ei lopetettu rivillä 3

  $\Rightarrow n_5 < n_2$
  - muussa tapauksessa $n_4 < m_4$, joten $n_6 = n_5 = n_4 \bmod m_4 = n_4$ [80]
  - siksi $m_7 = m_6 \bmod n_6 = m_4 \bmod n_4 < n_4 < m_4 = m_2$

  $\Rightarrow m_7 < m_2$

$\Rightarrow n + m$ pienenee jokaisella kierroksella, jolla ei lopeteta

$\Rightarrow n + m \in \mathbb{N}$, joten lopetetaan viimeistään $n_1 + m_1$ kierroksen jälkeen

```
1  unsigned gcd( unsigned n, unsigned m ){
2    while( true ){
3      if( m == 0 ){ return n; }
4      n %= m;
5      if( n == 0 ){ return m; }
6      m %= n;
7    }
8  }
```

Osoitamme, että jokainen parametrien yhteinen tekijä on myös lopputuloksen tekijä

- osoitamme ensin, että jos $d \mid n$ ja $d \mid m$, niin $d \mid (n \bmod m)$
  - koska $d \mid n$ ja $d \mid m$, on olemassa sellaiset k ja h, että $n = dk$ ja $m = dh$ [81]
  - $n \bmod d \;=\; n - m(n \operatorname{div} d) \;=\; dk - dh(n \operatorname{div} d) \;=\; d(k - h(n \operatorname{div} d))$ [78]

  $\Rightarrow$ $n \bmod d = d(k - h(n \operatorname{div} d))$

  $\Rightarrow$ $d \mid (n \bmod d)$ [81]

$\Rightarrow$ jos $d \mid n_4$ ja $d \mid m_4$, niin $d \mid n_5$ ja $d \mid m_5$, koska $n_5 = n_4 \bmod m_4$ ja $m_5 = m_4$

- samalla tavalla voidaan osoittaa, että jos $d \mid n_6$ ja $d \mid m_6$, niin $d \mid n_7$ ja $d \mid m_7$
- muilla riveillä n ja m eivät muutu

$\Rightarrow$ jos $d \mid n_1$ ja $d \mid m_1$, niin koko suorituksen ajan $d \mid n_i$ ja $d \mid m_i$

$\Rightarrow$ jos $d \mid n_1$ ja $d \mid m_1$, niin $d \mid g$

```
unsigned gcd( unsigned n, unsigned m ){
  while( true ){
    if( m == 0 ){ return n; }
    n %= m;
    if( n == 0 ){ return m; }
    m %= n;
  }
}
```

Osoitamme, että lopputulos on parametrien yhteinen tekijä

- osoitamme ensin, että jos $d \mid m$ ja $d \mid (n \bmod m)$, niin $d \mid n$
  - on olemassa sellaiset k ja h, että $m = dk$ ja $n \bmod m = dh$ [81]
  - $n = m(n \operatorname{div} m) + (n \bmod m) = dk(n \operatorname{div} m) + dh = d(k(n \operatorname{div} m) + h)$ [76] [81]

$\Rightarrow$ jos $d \mid n_5$ ja $d \mid m_5$, niin
  - $d \mid m_4$, koska $m_5 = m_4$
  - $d \mid (n_4 \bmod m_4)$, koska $n_5 = n_4 \bmod m_4$

  $\Rightarrow$ $d \mid n_4$

- samalla tavalla voidaan osoittaa, että jos $d \mid n_7$ ja $d \mid m_7$, niin $d \mid n_6$ ja $d \mid m_6$
- muilla riveillä n ja m eivät muutu
- lopussa $g \mid n$ ja $g \mid m$, koska lopussa joko $g = n \wedge m = 0$ tai $g = m \wedge n = 0$ [82] [83]

$\Rightarrow$ koko suorituksen ajan $g \mid n$ ja $g \mid m$, joten myös alussa $g \mid n$ ja $g \mid m$

Gcd-algoritmin todistuksen viimeistely

- nyt n ja m tarkoittavat parametrien arvoja
- on helppo nähdä, että jos $n = m = 0$, niin algoritmi palauttaa 0 kuten pitääkin
- muussa tapauksessa $n > 0$ tai $m > 0$

$\Rightarrow$ $\gcd(n,m)$ on olemassa [89]

- osoitamme, että $g > 0$
  - jos $n > 0$ niin, koska lopputulos on parametrien yhteinen tekijä [sivu 161], pätee $n > 0 \wedge (g \mid n)$, joten $g > 0$ [84]
  - muussa tapauksessa $m > 0$, joten sama päättely m:lle tuottaa $g > 0$
- osoitamme, että $\gcd(n,m) \leq g$
  - $\gcd(n,m)$ on parametrien yhteinen tekijä
  - jokainen parametrien yhteinen tekijä on myös lopputuloksen tekijä [sivu 160]

  $\Rightarrow$ $\gcd(n,m) \mid g$

  $\Rightarrow$ $\gcd(n,m) \leq g$, koska $g > 0$ [84]
- koska lopputulos on parametrien yhteinen tekijä [sivu 161], se on enintään niiden suurin yhteinen tekijä, eli $g \leq \gcd(n,m)$

$\Rightarrow$ $g = \gcd(n,m)$

11 Kvanttorit ja niiden lait

Kaikkikvanttori (*universal quantifier*)

$\forall x : \varphi(x)$ tuottaa T jos ja vain jos $\varphi(x)$ tuottaa T jokaisella x:n arvolla.
$\forall x : \varphi(x)$ tuottaa F jos ja vain jos $\varphi(x)$ tuottaa F ainakin yhdellä x:n arvolla. [91]
Muussa tapauksessa $\forall x : \varphi(x)$ tuottaa U.

- esim. $\forall x : x^2 \geq 0$ tuottaa reaaliluvuilla T
- esim. $\forall x : x^2 > 0$ tuottaa reaaliluvuilla F
- esim. $\forall x : x^2 = -1$ tuottaa reaaliluvuilla F
- esim. $\forall a : \forall b : a + b = b + a$ tuottaa reaaliluvuilla T
- esim. $\forall x : x > 1 \rightarrow x \geq 2$ tuottaa reaaliluvuilla F ja kokonaisluvuilla T
- esim. $\forall x : \frac{x}{x} = 1$ tuottaa reaaliluvuilla U
- esim. $\forall x : \frac{x}{x} = 2$ tuottaa reaaliluvuilla F
- esim. $\forall x : \frac{x}{x} = x$ tuottaa reaaliluvuilla F
- $\forall x : \varphi(x)$ tuottaa U jos ja vain jos ainakin yhdellä x:n arvolla $\varphi(x)$ tuottaa U, ja muilla x:n arvoilla $\varphi(x)$ tuottaa T tai U
- jos puheenaiheessa on vain äärellinen määrä eri arvoja ja ne ovat $a_1, \ldots, a_n$, niin $\forall x : \varphi(x)$ tuottaa saman kuin $\varphi(a_1) \wedge \varphi(a_2) \wedge \cdots \wedge \varphi(a_n)$

Olemassaolokvanttori (*existential quantifier*)

$\exists x : \varphi(x)$ tuottaa T jos ja vain jos $\varphi(x)$ tuottaa T ainakin yhdellä x:n arvolla.
$\exists x : \varphi(x)$ tuottaa F jos ja vain jos $\varphi(x)$ tuottaa F jokaisella x:n arvolla. [92]
Muussa tapauksessa $\exists x : \varphi(x)$ tuottaa U.

- esim. $\exists x : x^2 \geq 0$ tuottaa reaaliluvuilla T
- esim. $\exists x : x^2 > 0$ tuottaa reaaliluvuilla T
- esim. $\exists x : x^2 = -1$ tuottaa reaaliluvuilla F
- esim. $\exists a : \exists b : a + b = b + a$ tuottaa reaaliluvuilla T
- esim. $\exists x : x > 1 \rightarrow x \geq 2$ tuottaa reaaliluvuilla T ja kokonaisluvuilla T
- esim. $\exists x : \frac{x}{x} = 1$ tuottaa reaaliluvuilla T
- esim. $\exists x : \frac{x}{x} = 2$ tuottaa reaaliluvuilla U
- esim. $\exists x : \frac{x}{x} = x$ tuottaa reaaliluvuilla T
- $\exists x : \varphi(x)$ tuottaa U jos ja vain jos ainakin yhdellä x:n arvolla $\varphi(x)$ tuottaa U, ja muilla x:n arvoilla $\varphi(x)$ tuottaa F tai U
- jos puheenaiheessa on vain äärellinen määrä eri arvoja ja ne ovat $a_1, \ldots, a_n$, niin $\exists x : \varphi(x)$ tuottaa saman kuin $\varphi(a_1) \vee \varphi(a_2) \vee \cdots \vee \varphi(a_n)$

Kvanttorien yhteydessä käytettävä välimerkki vaihtelee kirjallisuudessa

- : on tietojenkäsittelytieteessä melko yleinen
- matematiikassa on tavallista että välimerkkiä ei ole lainkaan

Esimerkkejä eri puheenaiheista

- reaaliluvut: $\forall x : x \geq 0 \rightarrow \exists y : y^2 = x$
- kokonaisluvut: $\forall n : \forall m : m \neq 0 \rightarrow \exists q : \exists r : n = qm + r \wedge 0 \leq r < |m|$
- merkkijonot: $\forall \alpha : \forall \beta : \mathrm{takaperin}(\alpha\beta) = \mathrm{takaperin}(\beta)\mathrm{takaperin}(\alpha)$
  - $\mathrm{takaperin}(\texttt{yli}) = \texttt{ily}$
  - $\mathrm{takaperin}(\texttt{opisto}) = \texttt{otsipo}$
  - $\mathrm{takaperin}(\texttt{yliopisto}) = \texttt{otsipoily} = \mathrm{takaperin}(\texttt{opisto})\mathrm{takaperin}(\texttt{yli})$
- merkkijonot: $\exists \alpha : \mathrm{takaperin}(\alpha) = \alpha$
  - `saippuakauppias`
- taulukot: $\forall i : 1 \leq i < n \rightarrow A[i] \leq A[i+1]$

Muuttujasymbolin vapaa ja sidottu esiintymä

- jokainen seuraavista väittää eri asiaa:
  - $\forall x : x > 5$ tuottaa F, koska $x > 5$ tuottaa F esim. kun $x = 2$
  - $x > 5$ tuottaa F tai T, riippuen x:n arvosta
  - $\exists x : x > 5$ tuottaa T, koska $x > 5$ tuottaa T esim. kun $x = 8$
- muuttujasymbolin x esiintymä on *sidottu* (*bound*), jos ja vain jos se on jonkin $\forall x :$ tai $\exists x :$ vaikutuspiirissä
  - myös $\forall x$ ja $\exists x$ itse otetaan huomioon
- muut muuttujasymbolin x esiintymät ovat *vapaita* (*free*)
- esim. $x = 0 \land (\exists x : x^2 = 2x) \lor x = 1$ sisältää kaksi vapaata ja kolme sidottua x:n esiintymää
- ohjelmoijalle on luontevaa ajatella, että vapaana esiintyvä muuttujasymboli tarkoittaa eri muuttujaa kuin sidottuna esiintyvä, vaikka sillä on sama nimi
  - myös eri kvantifioinneilla luodut muuttujat kannattaa ajatella eri muuttujiksi
  - esim.

    $$(\exists x : (\forall x : x^2 \neq 2) \lor x^2 = 2) \lor x \neq 1 \land (\forall x : x^2 > 0 \lor x = 0) \lor x = 1$$

    sisältää neljä eri muuttujaa, joiden nimi on x
  - mitä ”Kauppakatu” tarkoittaa riippuu siitä, ollaanko Jyväskylässä vai Kuopiossa

Tärkeä ero

- x käy ilmauksissa $\forall x : \varphi(x)$ ja $\exists x : \varphi(x)$ läpi puheenaiheen *kaikki* arvot, mutta ilmauksissa $\varphi(x) \Rightarrow \psi(x)$ ja $\varphi(x) \Leftrightarrow \psi(x)$ vain arvot *mahdollisissa tilanteissa*
- esim. jos on oletettu $x > 5$, niin $2x \geq 7 \Leftrightarrow$ T on pätevä mutta $\forall x : 2x \geq 7$ tuottaa F
  - $x > 5 \;\Leftrightarrow\; 2x > 10 \;\Rightarrow\; 2x \geq 7$
  - kun $x = 3$, $2x \geq 7$ tuottaa F
- jos kaavassa on sekä vapaita että sidottuja muuttujia, niin
  - sidotut muuttujat saavat kaikki arvot
  - vapaat muuttujat saavat vain voimassa olevien oletusten sallimat arvot
- esim. $\forall x : x^2 + y > 2$
  - tuottaa F tai T riippuen y:n arvosta
  - tuottaa aina T, jos on oletettu $y \geq 7$
  - tuottaa F, jos oletukset sallivat $y = 0$, koska $x = y = 0$ on vastaesimerkki
- jos samanniminen muuttuja esiintyy sekä vapaana että sidottuna, niin
  - sen vapaat esiintymät ovat eri muuttuja kuin sen sidotut esiintymät

  $\Rightarrow$ oletukset vaikuttavat sen vapaisiin mutta ei sidottuihin esiintymiin
- esim. vaikka $xy > 1$ aina kun $1 \leq x < y$
  - oletuksen $1 \leq x < y$ alaisuudessa on $\exists x : xy = 1$ reaaliluvuilla tosi
  - $1 \leq x < y \rightarrow \exists x : xy = 1$ on reaaliluvuilla tosi

Isompi esimerkki

- olkoon oletettu $y \geq x+4$
- $x^2+y^2>3 \Leftrightarrow \mathsf{T}$ on pätevä
  - jos $x \geq -2$, niin $y \geq -2+4=2 \geq 0$, joten $x^2+y^2 \geq y^2 \geq 2y \geq 2 \cdot 2 = 4 > 3$
  - muutoin $x < -2 < 0$, joten $x^2+y^2 \geq x^2 > -2x > (-2)(-2) = 4 > 3$
- mutta $\forall y: x^2+y^2>3$ tuottaa F, kun $-\sqrt{3} \leq x \leq \sqrt{3}$
  - kun $x=1$ ja $y=0$, $x^2+y^2>3$ tuottaa F

  $\Rightarrow$ kun $x=1$, $\forall y: x^2+y^2>3$ tuottaa F
- oletuksella $y \geq x+4$ ilmaus $x^2+y^2>3 \Leftrightarrow \mathsf{T}$ käy läpi kaikki x:n ja kaikki y:n arvot, mutta ei kaikkia niiden yhdistelmiä
  - käy läpi $x=a$ esim. kun $y=a+4$
  - käy läpi $y=a$ esim. kun $x=a-4$
  - ei käy läpi mm. $x=1 \wedge y=0$, koska sille ei päde $y \geq x+4$
- ilmaus $\forall y: x^2+y^2>3$ käy läpi kaikki mahdollisissa tilanteissa esiintyvät x:n arvot ja jokaiselle niistä kaikki y:n arvot

  $\Rightarrow$ käy läpi kaikki yhdistelmät

Avoin (*open*) kaava sisältää ja *suljettu* (*closed*) kaava
ei sisällä ainakin yhden vapaan esiintymän

- esim.
  - $\forall x : x > 0$ on suljettu
  - $x > 0$ on avoin
  - $\exists x : x > 0$ on suljettu
  - $(\exists x : (\forall x : x^2 \neq 2) \vee x^2 = 2) \vee x \neq 1 \wedge (\forall x : x^2 > 0 \vee x = 0) \vee x = 1$ on avoin
- suljetulla kaavalla on yksikäsitteinen totuusarvo F, U tai T
- avoimen kaavan totuusarvo voi riippua vapaiden muuttujien arvoista
  - esim. $\sqrt{x} > 0$ tuottaa U kun $x < 0$, F kun $x = 0$ ja T kun $x > 0$
  - ei kuitenkaan välttämättä riipu, esim. $x^2 > -1$

Termin sijoittaminen muuttujasymbolin vapaiden esiintymien tilalle

- jos x on muuttujasymboli, $\mathfrak{f}$ on lauseke ja $\varphi(x)$ on kaava, niin $\varphi(\mathfrak{f})$ tarkoittaa kaavaa, joka saadaan korvaamalla x:n jokainen *vapaa* esiintymä $\varphi(x)$:ssä $\mathfrak{f}$:llä
- kuten ennenkin, korvauksen tulee tapahtua lausekepuun, ei tekstin tasolla
  $\Rightarrow$ voi olla tarpeen lisätä sulkeita
  - esim. $n+1 \rightsquigarrow x$ kaavassa $x^2 \geq 0$: ei $n+1^2 \geq 0$ vaan $(n+1)^2 \geq 0$
- mikään lausekkeen muuttujasymboleista ei saa olla sidottu missään korvauskohdassa
  - esim. jokaisella $x \in \mathbb{R}$ pätee $\exists y : y > x$
  - x:n korvaaminen siinä $y+1$:llä tuottaisi $\exists y : y > y+1$, joka ei päde
  - tämä ongelma ratkeaa kohta ”sidotun muuttujasymbolin vaihdolla”
- esimerkkejä

$\varphi(x)$	$\mathfrak{f}$	$\varphi(\mathfrak{f})$
$x(y+z) = xy + xz$	$a-3$	$(a-3)(y+z) = (a-3)y + (a-3)z$
$x \geq 0 \rightarrow \exists y : y^2 = x$	z^2+1	$z^2+1 \geq 0 \rightarrow \exists y : y^2 = z^2+1$
$x \geq 0 \rightarrow \exists y : y^2 = x$	y^2+1	$y^2+1 \geq 0 \rightarrow \exists y : y^2 = y^2+1$

Sidotun muuttujasymbolin vaihto

Jos y ei esiinny $\varphi(x)$:ssä, niin
$\forall x : \varphi(x) \equiv \forall y : \varphi(y)$ ja $\exists x : \varphi(x) \equiv \exists y : \varphi(y)$. [93]

- esim. $\exists x : x > y$ ja $\exists z : z > y$ mutta ei $\exists y : y > y$
- esim. $\forall x : \exists y : x = y + 1$ ja $\forall z : \exists y : z = y + 1$ mutta ei $\forall y : \exists y : y = y + 1$
- esim. $y^2 + 1$ voidaan sijoittaa x:n tilalle kaavaan $x \geq 0 \rightarrow \exists y : y^2 = x$ vaihtamalla ensin sidotun y:n tilalle z [93]:
$$x \geq 0 \rightarrow \exists y : y^2 = x \equiv x \geq 0 \rightarrow \exists z : z^2 = x \rightsquigarrow y^2 + 1 \geq 0 \rightarrow \exists z : z^2 = y^2 + 1$$
- yleistys: y saa esiintyä $\varphi(x)$:ssä sillä ehdolla, että
  - y esiintyy $\varphi(x)$:ssä vain sidottuna
  - x ei esiinny vapaana siellä missä y on sidottu
- riittää, että x:n vapaat esiintymät $\varphi(x)$:ssä ovat täsmälleen samoissa kohdissa kuin y:n vapaat esiintymät $\varphi(y)$:ssä

Ehdon, että φ ei saa sisältää $\forall$ ja $\exists$, korvaaminen lievemmällä

> Jokaisessa edellä olleessa laissa tai säännössä, jossa kiellettiin $\forall$ ja $\exists$, ne sallitaan sillä ehdolla, että mikään sijoitettavan lausekkeen tai kaavan (vapaa) muuttujasymboli ei joudu sidotuksi missään korvauskohdassa. [94]

- lausekkeen tapauksessa muuttujasymboli, kaavan tapauksessa vapaa muuttujasymboli
- esim. [19,25]

  > Jos $\mathfrak{f} = \mathfrak{g}$ tai sekä $\mathfrak{f}$ että $\mathfrak{g}$ on määrittelemätön, ja jos φ ei sisällä symboleita $\forall$ ja $\exists$, niin $\varphi(\mathfrak{f}) \equiv \varphi(\mathfrak{g})$.

  muuttuu muotoon

  > Jos $\mathfrak{f} = \mathfrak{g}$ tai sekä $\mathfrak{f}$ että $\mathfrak{g}$ on määrittelemätön, ja jos mikään $\mathfrak{f}$:n tai $\mathfrak{g}$:n muuttujasymboli ei ole sidottu minkään vapaan x kohdalla $\varphi(x)$:ssä, niin $\varphi(\mathfrak{f}) \equiv \varphi(\mathfrak{g})$.

  – ilman vaatimusta "ei joudu sidotuksi" voitaisiin esim. oletuksesta $x = 0$ valitsemalla $\varphi(a)$:ksi $\forall x : x^2 \geq a$ johtaa F $\Leftrightarrow$ $\forall x : x^2 \geq x$ $\Leftrightarrow$ $\forall x : x^2 \geq 0$ $\Leftrightarrow$ T

Lisää predikaattilogiikan lakeja

- De Morganin lait

$$\neg\forall x : \varphi(x) \;\equiv\; \exists x : \neg\varphi(x) \qquad\qquad \neg\exists x : \varphi(x) \;\equiv\; \forall x : \neg\varphi(x) \tag{95}$$

- samanlaisten kvanttorien vaihto

$$\forall x : \forall y : \varphi(x,y) \;\equiv\; \forall y : \forall x : \varphi(x,y) \qquad\qquad \exists x : \exists y : \varphi(x,y) \;\equiv\; \exists y : \exists x : \varphi(x,y) \tag{96}$$

- erilaisten kvanttorien vaihto toimii vain toiseen suuntaan

$$\exists x : \forall y : \varphi(x,y) \;\Rightarrow\; \forall y : \exists x : \varphi(x,y) \tag{97}$$

  - toisinpäin ei päde, esim. $\forall y : \exists x : x \neq y$ mutta ei $\exists x : \forall y : x \neq y$

- kvanttorien kasvavuus

  Jos x:stä ei ole oletettu mitään ja $\varphi(x) \Rightarrow \psi(x)$, niin
  $\forall x : \varphi(x) \Rightarrow \forall x : \psi(x)$ ja $\exists x : \varphi(x) \Rightarrow \exists x : \psi(x)$. [98]

- kvantifioinnin jakaminen kahdeksi
  - huomaa jälkimmäisten suunnat!

$$\begin{aligned}
\forall x : \varphi(x) \wedge \psi(x) \;&\equiv\; (\forall x : \varphi(x)) \wedge (\forall x : \psi(x)) \\
\exists x : \varphi(x) \vee \psi(x) \;&\equiv\; (\exists x : \varphi(x)) \vee (\exists x : \psi(x)) \\
\forall x : \varphi(x) \vee \psi(x) \;&\Leftarrow\; (\forall x : \varphi(x)) \vee (\forall x : \psi(x)) \\
\exists x : \varphi(x) \wedge \psi(x) \;&\Rightarrow\; (\exists x : \varphi(x)) \wedge (\exists x : \psi(x))
\end{aligned} \tag{99}$$

Joihinkin lakeihin liittyy ehtoja, jotka estävät eri muuttujia sekoittumasta toisiinsa

- esim.
  - mikään $\mathfrak{f}$:n tai $\mathfrak{g}$:n muuttujasymboli ei ole sidottu minkään vapaan x kohdalla $\varphi(x)$:ssä
  - x:stä ei ole oletettu mitään
- kirjallisuudessa ehdot vaikuttavat sekavilta
- valitettavasti ne vaikuttavat sekavilta myös näissä luennoissa ☹
- niiden kanssa pärjää, kun ajattelee, että eri muuttujilla voi olla sama nimi, ja pitää huolta, että nimen esiintymä viittaa aina oikeaan muuttujaan
- sidotun muuttujasymbolin vaihto auttaa usein, mutta sekin on toki tehtävä oikein!

Osakaavan siirto kvanttorin vaikutusalueeseen

Jos x ei esiinny vapaana φ:ssä, niin

$$\begin{array}{lll} \varphi \land \forall x : \psi(x) \equiv \forall x : \varphi \land \psi(x) & \varphi \land \exists x : \psi(x) \equiv \exists x : \varphi \land \psi(x) & \\ \varphi \lor \forall x : \psi(x) \equiv \forall x : \varphi \lor \psi(x) & \varphi \lor \exists x : \psi(x) \equiv \exists x : \varphi \lor \psi(x) \,. & [100] \end{array}$$

- ilman ehtoa voitaisiin erehtyä esim. $x < 1 \land \forall x : x^2 \geq 0 \stackrel{?}{\equiv} \forall x : x < 1 \land x^2 \geq 0$
- $(x < 1)$:n x tarkoittaa eri muuttujia virheellisen $\equiv$:n eri puolilla

Kvanttorien luonti- ja eliminointilait

- kaikkikvanttorin poisto

  Jos $\mathfrak{f}$ on määritelty ja mikään sen muuttujasymboli ei ole sidottu minkään vapaan x kohdalla $\varphi(x)$:ssä, niin $\forall x : \varphi(x) \;\Rightarrow\; \varphi(\mathfrak{f})$. [101]

- kaikkikvanttorin luonti

  Jos muuttujasymbolista x ei ole oletettu mitään, niin $\varphi(x) \;\Rightarrow\; \forall x : \varphi(x)$. [102]

- olemassaolokvanttorin luonti

  Jos mikään $\mathfrak{f}$:n muuttujasymboli ei ole sidottu minkään vapaan x kohdalla $\varphi(x)$:ssä, niin $\varphi(\mathfrak{f}) \;\Rightarrow\; \exists x : \varphi(x)$. [103]

  – ei tarvita oletusta, että $\mathfrak{f}$ on määritelty (jollei ole mutta $\varphi(\mathfrak{f})$ tuottaa T, niin $\varphi(a)$ tuottaa T jokaisella puheenaiheen alkiolla [59], ja niitä on olemassa [sivu 39])

- olemassaolokvanttorin poisto

  Jos muuttujasymboli c ei esiinny aiemmin, $\varphi(x)$:ssä eikä ψ:ssä, ja jos $\varphi(c) \Rightarrow \psi$, niin $\exists x : \varphi(x) \;\Rightarrow\; \psi$. [104]

  – usein ensin päätellään $\exists x : \varphi(x)$ ja sitten johdetaan $\varphi(c)$:stä ψ
  – c edustaa arvoa, jonka $\exists x : \varphi(x)$ lupaa olevan olemassa
  – jos $\varphi(x)$:n muut vapaat muuttujat kuin x ovat $x_1, \ldots, x_n$, niin c voi riippua niistä; tätä voi korostaa merkinnällä $c(x_1, \ldots, x_n)$ tai $c_{x_1,\ldots,x_n}$

Kuinka nämä lait voi muistaa?

- en tiedä, minä en muista niitä kaikkia!
- aika moni on (varsinkin 2-arvologiikassa) ilmeinen, kun miettii symboleiden merkitystä
- esim. $\neg\forall x : \varphi(x) \;\Rightarrow\; \exists x : \neg\varphi(x)$
  - jos $\varphi(x)$ ei jokaisella x tuota T, niin on olemassa jokin x jolla $\varphi(x)$ ei tuota T
  - jonkin niistä täytyy tuottaa F, jotta $\neg\forall x : \varphi(x)$ tuottaisi T eikä U
- esim. $\exists x : \forall y : \varphi(x,y) \;\Rightarrow\; \forall y : \exists x : \varphi(x,y)$
  - se x:n arvo, joka kelpaa vasemmalla, kelpaa oikeallakin
  - laki ei päde toisinpäin, koska vaikka jokaisella y olisi sopiva x, *sama* x ei välttämättä kelpaa jokaiselle y
  - jokaisella on tai on ollut äiti, mutta kukaan ei ole ollut jokaisen äiti
  - esim. $\forall y : \exists x : x = y$ tuottaa T mutta $\exists x : \forall y : x = y$ tuottaa F

$\forall$:n ja $\exists$:n symmetria ???

- jokainen $\forall$ korvataan $\exists$:lla ja päinvastoin
- $\neg(\forall x : kaava^{\wedge}(\varphi_1, \ldots, \varphi_n)) \;\equiv\; \exists x : \neg\, kaava^{\wedge}(\varphi_1, \ldots, \varphi_n) \;\equiv\; \exists x : kaava_{\vee}(\neg\varphi_1, \ldots, \neg\varphi_n)$
- $\neg(\exists x : kaava^{\wedge}(\varphi_1, \ldots, \varphi_n)) \;\equiv\; \forall x : \neg\, kaava^{\wedge}(\varphi_1, \ldots, \varphi_n) \;\equiv\; \forall x : kaava_{\vee}(\neg\varphi_1, \ldots, \neg\varphi_n)$

Rajoitettu kvanttori, tapaus 1

- $\forall x \in A : \varphi(x)$ tarkoittaa ”jokaiselle joukkoon A kuuluvalle x:lle pätee $\varphi(x)$”
  - tarkoittaa samaa kuin $\forall x : x \in A \rightarrow \varphi(x)$

- $\exists x \in A : \varphi(x)$ tarkoittaa ”jollekin joukkoon A kuuluvalle x:lle pätee $\varphi(x)$”
  - tarkoittaa samaa kuin $\exists x : x \in A \wedge \varphi(x)$
- näissä A on yleensä jokin yksinkertaisesti ilmaistavissa oleva joukko, esim. $\mathbb{R}$
  - siis A:ta käytetään usein kuten tyyppimääreitä ohjelmoinnissa, vrt. `int n`

Rajoitettu kvanttori, tapaus 2

- $\forall x\,;\chi(x) : \varphi(x)$ tarkoittaa samaa kuin $\forall x : \chi(x) \rightarrow \varphi(x)$
- $\exists x\,;\chi(x) : \varphi(x)$ tarkoittaa samaa kuin $\exists x : \chi(x) \wedge \varphi(x)$
- käytetään erityisesti taulukoita käsittelevien ohjelmien todistamiseen
- keskiosa on tarkoitettu rajoittamaan taulukon indeksit sallitulle alueelle
  - esim. $\forall i\,;1 \leq i < n : A[i] \leq A[i+1]$
- keskiosan määrittelemä alue voi olla tarkoituksellisesti tyhjä
  - jokainen sellainen väite tuottaa T
  - esim. $\forall i\,;1 \leq i < 0 : A[i] \leq A[i+1]$ tuottaa T
  - harvoin kirjoitetaan tahallaan $\forall i\,;1 \leq i < 0 : \varphi$, mutta usein kirjoitetaan tahallaan $\forall i\,;1 \leq i < n : \varphi$ kun n voi olla 0 tai 1

Rajoitettu kvanttori voi aiheuttaa yllätyksen, kun keskiosa määrittelee tyhjän alueen

- esim. $\forall x : \varphi(x) \;\Rightarrow\; \exists x : \varphi(x)$ on pätevä [sivu 39] tai [101,103], mutta $\forall x ; \chi(x) : \varphi(x) \;\Rightarrow\; \exists x ; \chi(x) : \varphi(x)$ ei ole
  - virhe syntyy täsmälleen sellaisilla χ ja φ, että $\chi(x)$ ei millään x:n arvolla tuota T, ja $\varphi(x)$ tuottaa T niillä x:n arvoilla joilla $\chi(x)$ tuottaa U
  - nyt vastaesimerkit eivät ole x:n arvoja vaan kaavoja, esim. $\frac{1}{x} = 0$ ja $x = 0$
- perusmuotoisilla kvanttoreilla ei tätä yllätystä voi tulla, koska puheenaiheessa on aina oltava ainakin yksi alkio

Esimerkki: $A[i]$ on pienempi kuin mikään muu taulukon $A[1\ldots n]$ alkio, missä i on laillinen indeksi

- $1 \leq i \leq n \wedge \forall j ; 1 \leq j \leq n \wedge i \neq j : A[i] < A[j]$ sanoo sen oikein
  - $1 \leq i \leq n \wedge$ huolehtii, että i on laillinen indeksi
  - kun $n = 0$, osuus $1 \leq i \leq n$ ja samalla koko kaava tuottaa F, kuten pitääkin
- j ei esiinny vapaana osakaavassa $1 \leq i \leq n$
- jos x ei esiinny vapaana φ:ssä, niin $\varphi \wedge \forall x : \psi(x) \;\Leftrightarrow\; \forall x : \varphi \wedge \psi(x)$ [100]
- silti $\forall j ; 1 \leq j \leq n \wedge i \neq j : 1 \leq i \leq n \wedge A[i] < A[j] \;\Leftrightarrow\;$ T , kun $n = 0$

Vastaavasti $\exists x ; \chi(x) : \varphi(x)$ voi aiheuttaa yllätyksen, kun $\chi(x)$ tuottaa F jokaisella x

- esim. jos x ei esiinny vapaana φ:ssä, niin $\varphi \vee \exists x : \psi(x) \;\Leftrightarrow\; \exists x : \varphi \vee \psi(x)$ [100], mutta ei välttämättä $\varphi \vee \exists x ; \chi(x) : \psi(x) \;\Leftrightarrow\; \exists x ; \chi(x) : \varphi \vee \psi(x)$

Tapauksissa $\forall x\,; \chi(x) : \varphi(x)$ ja $\exists x\,; \chi(x) : \varphi(x)$ päteviä lakeja voi johtaa em. määritelmien avulla

- esim. $\exists$-kvantifioinnin jakaminen kahdeksi

$$
\begin{array}{lll}
 & \exists x\,; \chi(x) : \varphi(x) \lor \psi(x) & \\
\Leftrightarrow & \exists x : \chi(x) \land (\varphi(x) \lor \psi(x)) & \exists x\,; \chi(x) : \varphi(x) \text{ määritelmä} \\
\Leftrightarrow & \exists x : \chi(x) \land \varphi(x) \lor \chi(x) \land \psi(x) & [9] \text{ ??? ei } [22] \\
\Leftrightarrow & (\exists x : \chi(x) \land \varphi(x)) \lor \exists x : \chi(x) \land \psi(x) & [99] \\
\Leftrightarrow & (\exists x\,; \chi(x) : \varphi(x)) \lor \exists x\,; \chi(x) : \psi(x) & \exists x\,; \chi(x) : \varphi(x) \text{ määritelmä}
\end{array}
$$

siis $\exists x\,; \chi(x) : \varphi(x) \lor \psi(x) \;\Leftrightarrow\; (\exists x\,; \chi(x) : \varphi(x)) \lor \exists x\,; \chi(x) : \psi(x)$

- esim. De Morganin laki

$$
\begin{array}{lll}
 & \neg\forall x\,; \chi(x) : \varphi(x) & \\
\Leftrightarrow & \neg\forall x : \chi(x) \rightarrow \varphi(x) & \forall x\,; \chi(x) : \varphi(x) \text{ määritelmä} \\
\Leftrightarrow & \neg\forall x : \neg\chi(x) \lor \varphi(x) & [41] \\
\Leftrightarrow & \exists x : \neg(\neg\chi(x) \lor \varphi(x)) & [95] \\
\Leftrightarrow & \exists x : \chi(x) \land \neg\varphi(x) & [7] \\
\Leftrightarrow & \exists x\,; \chi(x) : \neg\varphi(x) & \exists x\,; \chi(x) : \varphi(x) \text{ määritelmä}
\end{array}
$$

???

12 Modernin logiikan suuria tuloksia

Tässä luvussa käydään pikaisesti läpi predikaattilogiikan suuria tuloksia

- kaikki tulokset ovat kaksiarvologiikalle (siis U ei ole käytössä)
- nimet ja vuosiluvut ovat varhaisin suunnilleen sama tulos
  - tulosten nykyversioissa on laajennoksia ja selkeytyksiä

Tähän asti käsitelty predikaattilogiikka on *ensimmäistä kertalukua* (*first-order*)

- kvanttorien kohteina on vain muuttujia
- esim. jos ei-loogisissa symboleissa on yksipaikkainen funktio f, niin voi sanoa, että jokin alkio ei ole f:n tulos ja f tuottaa eri alkioista eri tulokset

$$(\exists a : \neg \exists x : a = f(x)) \wedge (\forall x : \forall y : f(x) = f(y) \rightarrow x = y)$$

$\Rightarrow$ $a, f(a), f(f(a)), \ldots$ ovat kaikki eri alkioita
$\Rightarrow$ puheenaiheessa on ääretön määrä eri alkioita

- jollei f:stä sanota muuta, niin se ei aiheuta muuta kuin että alkioita on äärettömästi

Toisessa kertaluvussa kvanttorien kohteina saa olla myös relaatioita ja funktioita

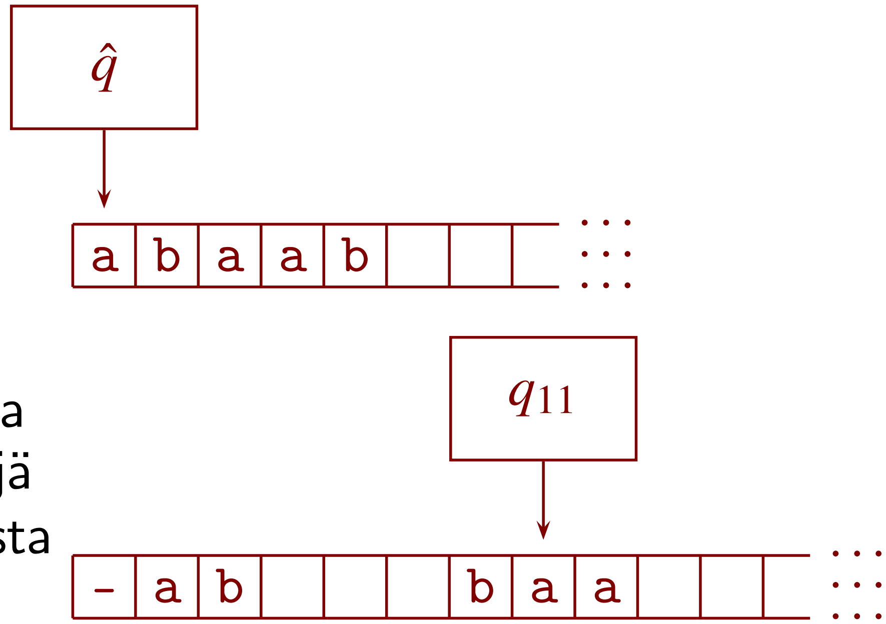
- voi sanoa esim. että puheenaiheessa on vain äärellinen määrä eri alkioita:

$$\neg \exists f : (\exists a : \neg \exists x : a = f(x)) \wedge (\forall x : \forall y : f(x) = f(y) \rightarrow x = y)$$

- (kolmannen jne. kertaluvun predikaattilogiikka ovat vielä yleisempiä)

Turingin kone (Alan Turing 1937)

- (monenlaisia muunnelmia esiintyy)
- ohjausyksikkö, jolla on äärellinen määrä sisäisiä tiloja
  - yksi niistä on alkutila
  - yksi niistä on hyväksymistila, johon saavuttuaan kone pysähtyy
- yhteen suuntaan ääretön ruutuihin jaettu nauha
  - *aakkosto* on jokin äärellinen joukko merkkejä
  - kussakin ruudussa on yksi merkki aakkostosta
  - yksi aakkostoon kuuluva merkki on ”tyhjä”



- kussakin askeleessa sisäisen tilan ja ohjausyksikön kohdalla olevan merkin perusteella
  - vaihtaa ohjausyksikön kohdalla olevan merkin toiseen tai jättää sen ennalleen
  - siirtyy yhden ruudun verran vasemmalle tai oikealle, tai pysyy paikallaan
  - menee uuteen (tai samaan) sisäiseen tilaan
- aluksi syöte on nauhan alussa ja muu osa nauhaa on tyhjä
- koneen pysähdyttyä (jos pysähtyy) tulos on se mikä on nauhan alussa
- voi laskea kaiken, minkä oikea tietokonekin, eikä muisti lopu kesken
  - ohjelmoijan ja pysähtymisen odottajan kärsivällisyys voivat loppua kesken!
- yleisin logiikassa käytetty kriteeri sille, mitä voi ja ei voi automatisoida

Hyvin paljon voi ilmaista merkkijonojen kaavoina konkatenoinnilla

- ei-loogiset symbolit ovat merkkijonovakiot ja merkkijonojen liittäminen peräkkäin
  - esim. jos $x =$ "vä" , niin "Jy"x"s""kylä" $=$ "Jyväskylä"
  - rajoittimina sallitaan myös ..." jne., alussa ja lopussa sama määrä pisteitä

  $\Rightarrow$ myös ", .", .." jne. saadaan merkkijonovakion sisältöön ilman \-koodeja tms.
- esimerkkejä
  - x ei sisällä lainausmerkkiä: $\forall y : \forall z : x \neq y.\text{''''}.\text{''}z$
  - x alkaa ja loppuu samaan merkkiin:
    $\exists c : c \neq \text{''''} \wedge (\forall y : \forall z : c = yz \rightarrow y = \text{''''} \vee z = \text{''''}) \wedge \exists y : x = cyc$
- on olemassa algoritmi, joka mille tahansa Turingin koneelle tekee kaavan TK(s,l,t), joka on tosi jos ja vain jos l on syötteellä s alkava ja tuloksella t pysähtyvä laskenta
  - Turingin koneen *konfiguraatio* kertoo sisäisen tilan, sijainnin nauhalla ja nauhan epätyhjän alkuosan sisällön
  - esitetään TK:n peräkkäiset konfiguraatiot merkkijonona
  - jollakin kikalla ilmaistaan konfiguraatioiden väliset rajat

$\Rightarrow$ minkä tahansa merkkijonojen ominaisuuden, jonka voi tarkastaa Turingin koneella, voi ilmaista kaavana $\exists l :$ TK$(s,l,$"oikein!"$)$

$\Rightarrow$ minkä tahansa merkkijonojen ominaisuuden, jonka voi tarkastaa algoritmilla, voi ilmaista kaavana
  - kaavasta tulee usein erittäin pitkä!

Ei ole olemassa algoritmia, joka tarkastaisi jokaisen suljetun kaavan totuuden

- sen pitäisi mille tahansa suljetulle kaavalle vastata oikein ”tosi” tai ”epätosi”
- $\exists l : \exists t :$ TK(s, l, t) sanoo ”Turingin kone TK pysähtyy syötteellä s”
- seuraavalla tavalla toimiva algoritmi olisi pysähtymistesteri:
  - käännä testattava aliohjelma Turingin koneeksi TK
  - muodosta TK:sta ja s:stä kaava $\exists l : \exists t :$ TK(s, l, t)
  - aja suljettujen kaavojen totuustesteri muodostamallesi kaavalle

Siis kaavoina voi ilmaista enemmän kuin mitä voi tarkastaa algoritmeilla

- lisätietoa
  - Wikipedia: Arithmetical Hierarchy
  - Stanford Encyclopedia of Philosophy: Recursive Functions
    $\rightsquigarrow$ 3.6.1 The arithmetical hierarchy

Hyvin paljon voi ilmaista luonnollisten lukujen kaavoina symboleilla 0, 1, $+$ ja $\cdot$

- olkoon p alkuluku, joka on vähintään yhtä suuri kuin aakkoston koko
- numeroidaan aakkoston merkit ykkösestä alkaen
- merkkijonon $c_1c_2\cdots c_n$ voi esittää lukuna $c_1p^{n-1}+c_2p^{n-2}+\ldots+c_{n-2}p^2+c_{n-1}p+c_n$
  - $\frac{p^n-1}{p-1} \leq$ tulos $< \frac{p^{n+1}-1}{p-1}$
- sen, että x:n merkkijono ja y:n merkkijono peräkkäin tuottavat z:n merkkijonon, voi esittää kaavana
  - kukin $(1+\ldots+1)$ sisältää p ykköstä
  - rivi 1 sanoo, että on olemassa k, joka on p:n potenssi
  - rivit 3 ja 2 sanovat, että $k \leq (p-1)y+1 < pk$

  $\Rightarrow$ k on juuri se p:n potenssi, joka vastaa y:n merkkijonon pituutta

  $\Rightarrow$ $kx+y$ vastaa sitä, että x:n merkkijono lisätään y:n merkkijonon eteen

1	$\exists k:$		$(\forall i:\forall j:k=ij\rightarrow i=1\vee\exists h:i=(1+\ldots+1)h)$
2		$\wedge$	$(\exists h:(1+\ldots+1)y+1+1+h=(1+\ldots+1)k+y)$
3		$\wedge$	$(\exists h:(1+\ldots+1)y+1=k+y+h)$
4		$\wedge$	$z=kx+y$

$\Rightarrow$ kaiken minkä voi ilmaista merkkijonojen kaavoina konkatenoinnilla, voi ilmaista helposti tulkittavalla tavalla koodattuna luonnollisten lukujen kaavoina

- alkuperäinen kaava on suljettu jos ja vain jos muunnoksen tuloskin on

Kaavana voi ilmaista "φ:n sisältö on suljettu kaava", mutta ei "φ:n sisältö on tosi suljettu kaava" (Tarski 1933)

- oletetaan, että tsk(φ) sanoo "φ:n sisältö on tosi suljettu kaava"
- jos tsk(φ) olisi olemassa, voitaisiin kirjoittaa seuraavanlainen suljettu kaava:
  - tarvittava pisteiden määrä riippuu tsk(φ):stä, tässä on havainnollisuuden vuoksi 6

$$\exists q : \neg\mathsf{tsk}(q...".....".....\textcolor{green}{...."}....."q..."....."....."\textcolor{green}{...."}.....") \land q =$$
$$......"\textcolor{green}{\exists q : \neg\mathsf{tsk}(q...".....".....".....".....".....q..."....."....."....."....."....")\land q =}......"$$

- lukemisen helpottamiseksi merkkijonovakioiden sisällöt ovat vihreällä
  - vihreässä ..." on aina vähemmän pisteitä peräkkäin kuin ympäröivissä mustissa ..."
  - ⇒ mikään vihreä ..." ei lopeta merkkijonovakiota ennenaikaisesti
- alarivin vihreä osa on täsmälleen sama kuin ylärivi, ja sama kuin q:n sisältö
- ylärivissä ...".....".....".....".....” muodostaa ......"

⇒ tsk:n parametri on seuraavat peräkkäin: q:n sisältö, ...", q:n sisältö ja ......"

⇒ tsk:n parametri on koko kaava

⇒ kaava matkii Willard Van Orman Quinen lausetta (1962), joka ei ole tosi eikä epätosi:

"laitettuna lainausmerkeissä itsensä eteen tuottaa epätoden väittämän."
laitettuna lainausmerkeissä itsensä eteen tuottaa epätoden väittämän.

⇒ kaavaa tsk(φ) ei ole olemassa

Huomatuksia

- todistusperiaate toimii myös luonnollisille luvuille
  - lausekkeet ja kaavat koodataan luonnollisiksi luvuiksi kuten Gödel teki 1931
  - kaavan laittaminen puhumaan itsestään monimutkaistuu paljon, *diagonal lemma*

  $\Rightarrow$ todistus on paljon edellä esitettyä vaikeatajuisempi
- tavallisesti tämä tulos esitetään luonnollisille luvuille eikä merkkijonoille
- Tarski esitti todistusperiaatteen yleisenä ja todistuksen luonnollisille luvuille
- myös Gödel oli keksinyt tuloksen, ehkä ennen Tarskia, mutta ei julkaissut sitä

Gödelin ensimmäisen epätäydellisyyslauseen kevytversio merkkijonoille

- mitä tahansa ei voida hyväksyä päteviin päättelyperiaatteisiin
  - ”syötyäni kaksi kärpässientä näin seuraavana yönä unessa, että asia on niin”
  - ”suuri kunnioitettu johtajamme on valtameren laajuisessa viisaudessaan kansamme kaikinpuoliseksi hyväksi ja eduksi sanonut, että asia on niin”

⇒ täytyy (ainakin periaatteessa) olla olemassa todistukset tarkastava algoritmi
  - nykyisin sitä pystytään tekemään paljon käytännössäkin tietokoneilla, mutta ...
  - ... sellaiset todistukset ovat usein hyvin pitkiä ja ihmisille epäselviä

- olkoon $\mathsf{Tod}(\varphi, p)$ kaava, joka on tosi jos ja vain jos φ on suljettu kaava ja todistukset tarkastavan algoritmin mielestä p on sille pätevä todistus
- $\exists p : \mathsf{Tod}(\varphi, p)$ ilmaisee ”φ:n sisältö on suljettu kaava, jonka voi todistaa”
- tämä kaava on suljettu ja sanoo, että sitä itseään ei voi todistaa:

$$\exists q : \neg\exists p : \mathsf{Tod}(q\ldots\text{''}\ldots\ldots\text{''}\ldots\ldots\text{''}\ldots\text{''}\ldots\ldots\text{''}q\ldots\text{''}\ldots\ldots\text{''}\ldots\ldots\text{''}\ldots\text{''}\ldots\ldots\text{''}, p) \wedge q =$$
$$\ldots\ldots\text{''}\exists q : \neg\exists p : \mathsf{Tod}(q\ldots\text{''}\ldots\ldots\text{''}\ldots\ldots\text{''}\ldots\text{''}\ldots\ldots\text{''}q\ldots\text{''}\ldots\ldots\text{''}\ldots\ldots\text{''}\ldots\text{''}\ldots\ldots\text{''}, p) \wedge q = \ldots\ldots\text{''}$$

- jos sen voi todistaa, se on epätosi suljettu kaava jonka voi todistaa
  ⇒ todistusjärjestelmä on rikki

⇒ jos todistusjärjestelmä on ehjä, niin ym. on tosi suljettu kaava, jota ei voi todistaa

⇒ jokaisella ehjällä merkkijonojen konkatenoinnin todistusjärjestelmällä on tosi suljettu kaava, jota järjestelmä ei todista

Jokaisella ehjällä merkkijonojen konkatenoinnin todistusjärjestelmällä on äärettömän monta totta suljettua kaavaa, joita järjestelmä ei todista

- jos niitä olisi vain äärellinen määrä, niin niistä voisi olla luettelo
- todistusjärjestelmä aloittaisi katsomalla onko annettu kaava siinä

Edellisen sivun alareunan tuloksen voi todistaa myös siitä, että pysähtymistesteriä ei ole

- jos jokainen tosi suljettu kaava ja vain ne voitaisiin todistaa, niin seuraava ohjelma olisi pysähtymistesteri

  pysähtymistesteri(merkkijono o, merkkijono s)

  if o ei ole aliohjelma **then return** ”ei ole aliohjelma”
  käännä o Turingin koneeksi TK ja muodosta kaava $\varphi := \exists l : \exists t : \mathsf{TK}(s,l,t)$
  merkkijono $p :=$ ””
  while T **do**
      if Tod(φ, p) **then** return ”pysähtyy”
      if Tod($\neg\varphi, p$) **then** return ”ei pysähdy”
      $p :=$ seuraava_merkkijono(p)

- jos todistusjärjestelmä todistaa myös epätosia suljettuja kaavoja, niin ohjelma voi vastata väärin
- jos todistusjärjestelmä ei todista kaikkia tosia suljettuja kaavoja, niin ohjelma voi laskea ikuisesti

Emme olettaneet todistusjärjestelmältä muuta kuin että
on olemassa algoritmi, jolla todistukset voi tarkastaa!

- todistusjärjestelmä on *ehjä* jos ja vain jos jokainen sen todistama kaava on tosi
- todistusjärjestelmä on *täydellinen* jos ja vain jos se todistaa jokaisen toden kaavan
- merkkijono p todistaa tai ei todista kaavan φ
- jos p ei todista φ:tä, niin ei saatu tietoa siitä, onko φ tosi
  - ”kahvi on epäterveellistä, koska Wikipedian sivulla Kurt Gödel lukee niin”
  - se, että siellä ei todellisuudessa lue niin, ei todista kahvia epäterveelliseksi
- emme olettaneet, että todistukset yhtään muistuttavat tuttua loogista päättelyä

$\Rightarrow$ Gödelin ensimmäisen epätäydellisyyslauseen kevytversio on erittäin yleinen

Jos todistusjärjestelmä todistaa jokaisen toden suljetun kaavan ja vain ne, niin
edellisen ohjelman loppuosa on algoritmi suljettujen kaavojen totuuden testaamiseksi

- puheenaihe valituilla ei-loogisilla symboleilla on *ratkeava* jos ja vain jos
  sille on algoritmi suljettujen kaavojen totuuden testaamiseksi
- sellainen algoritmi itsessään kelpaa todistusjärjestelmäksi em. mielessä
  - todistusjärjestelmän ei ole pakko käyttää p:tä apuna φ:n totuuden selvittämisessä

$\Rightarrow$ merkkijonot konkatenoinnilla ei ole ratkeava
  - siitä tulee ratkeava, jos konkatenoinnin sijaan on merkin lisääminen alkuun

Myöskään luonnolliset luvut symboleilla 0, 1, $+$ ja $\cdot$ ei ole ratkeava

- edellä esitetyn muunnoksen merkkijonoista luonnollisiin lukuihin voi suorittaa algoritmilla

$\Rightarrow$ jos luonnollisille luvuille olisi suljettujen kaavojen totuuden ratkaisualgoritmi, niin myös merkkijonoille olisi
  - käännetään merkkijonojen suljettu kaava luonnollisten lukujen suljetuksi kaavaksi
  - käytetään luonnollisten lukujen ratkaisualgoritmia

$\Rightarrow$ jokaisella ehjällä luonnollisten lukujen kaavojen todistusjärjestelmällä on tosi suljettu kaava, jota järjestelmä ei todista
  - tulos olettaa, että käytettävissä ovat 0, 1, $+$ ja $\cdot$

- myöskään mikään sellainen puheenaihe ei ole ratkeava, jolle merkkijonojen kaavat konkatenoinnilla tai luonnollisten lukujen 0, 1, $+$, $\cdot$ kaavat voi kääntää algoritmilla

$\Rightarrow$ epätäydellisyystulos on todellakin erittäin yleinen

Jättämällä $+$ tai $\cdot$ (tai molemmat) pois, luonnolliset luvut muuttuvat ratkeavaksi

- $+$ on mutta $\cdot$ puuttuu: Presburger-aritmetiikka
  - ratkaisualgoritmin voi perustaa niin sanottuihin äärellisiin automaatteihin
  - huonoimman tapauksen aikavaativuus on suuri
  - silti riittävän nopea moniin tarkoituksiin, mm. MathCheck
- $\cdot$ on mutta $+$ puuttuu: Skolem-aritmetiikka

Yllätys!

- reaaliluvut symboleilla 0, 1, $+$, $\cdot$ ja $<$ on ratkeava!
  - Tarski (ja Seidenberg), ehkä 1949, tolkuttoman hidas
  - käytännöllinen algoritmi: cylindrical algebraic decomposition (Collins 1975) $O(2^{2^n})$
  - *reaalisuljettu kunta* (*real closed field*)
- tämä on yllätys, koska
  - luonnolliset luvut ovat reaalilukujen osajoukko
  - reaalilukujen tuttu määritelmä sisältää monimutkaisen täydellisyysaksiooman
  - reaalilukuja on ylinumeroituva mutta luonnollisia lukuja vain numeroituva määrä
- miksei reaalilukujen ratkaisualgoritmia voi käyttää luonnollisten lukujen ratkaisualgoritmina?
  - siksi, että joidenkin kaavojen totuus riippuu siitä, kummassa ne tulkitaan
  - esim. $\exists x : 0 < x < 1$
- eikö tämä ratkea lisäämällä osa, joka sanoo, että x on luonnollinen luku?
  - esim. $\exists x : 0 < x < 1 \wedge \text{on\_luonnollinen}(x)$
  - kaavaa on_luonnollinen(x) ei voi kirjoittaa vain symboleilla 0, 1, $+$, $\cdot$ ja $<$
- jos lisätään sinifunktio, niin $\text{on\_luonnollinen}(x) \;\Leftrightarrow$

$$\exists p : \sin px = 0 \wedge p > 0 \wedge \sin p = 0 \wedge (\forall x : 0 < x < p \rightarrow \sin x \neq 0)$$

$\Rightarrow$ jos lisätään sinifunktio, niin reaaliluvut muuttuvat ratkeamattomaksi

- on avoin ongelma, muuttuvatko ne ratkeamattomaksi jos lisätään e^x (eikä $\sin$)

Gödelin ensimmäinen epätäydellisyyslause (Kurt Gödel 1931)

- vuoden 1930 tienoilla eli voimakkaana ajatus, että tieteelliset väitteet pitää perustella havainnoilla ja/tai loogisella todistuksella
- aikakausi ei olisi hyväksynyt käsitettä ”tosi suljettu kaava, jota ei voi todistaa”
  - jos sitä ei voi todistaa, niin millä perusteella / missä mielessä se on tosi?

$\Rightarrow$ Gödel kiersi tämän käyttämällä käsitettä
”sellainen suljettu kaava φ, että todistusjärjestelmä ei todista φ eikä $\neg\varphi$”

- todistusjärjestelmä on *täydellinen* jos ja vain jos sellaista kaavaa ei ole olemassa
  - uusi merkitys sanalle ”täydellinen”, vrt. sivu 190
- hän näytti, että kaavat ja todistukset voi esittää luonnollisilla luvuilla symboleilla 0, 1, $+$, $\cdot$
- hän oletti, että todistusjärjestelmä pystyy ainakin niihin asioihin, joita alla käytetään
  - oletukset ovat varsin vaatimattomat, mutta silti enemmän kuin kevytversio vaatii
- yksi oletuksista on nykykielellä: on olemassa algoritmi, joka tarkastaa, onko luku p kaavan numero k jonkin todistuksen numero
  - koska Turingin konetta ei vielä ollut keksitty, Gödel joutui ilmaisemaan sen toisin
- Gödelin esitystavasta seuraa: jos p on / ei ole kaavan, jonka numero on k, jonkin todistuksen numero, niin järjestelmä todistaa $\mathrm{Tod}(k,p)$ / $\neg\mathrm{Tod}(k,p)$

Gödelin todistuksen pääpiirteet

- hän osoitti, että on olemassa luku g, jolle kaavan $\neg\exists p : \mathsf{Tod}(g,p)$ numero on g
  - kaava sanoo ”mikään luku ei ole kaavan numero g minkään todistuksen numero”
  - luvun g olemassaolon todistus on vaikeatajuinen!
- jos jokin luku, vaikka 3810, on kaavan $\neg\exists p : \mathsf{Tod}(g,p)$ todistuksen numero, niin
  - järjestelmä todistaa $\neg\exists p : \mathsf{Tod}(g,p)$
  - järjestelmä todistaa $\mathsf{Tod}(g,3810)$ ja edelleen $\exists p : \mathsf{Tod}(g,p)$

  $\Rightarrow$ ristiriita
- muussa tapauksessa
  - järjestelmä ei todista $\neg\exists p : \mathsf{Tod}(g,p)$
  - järjestelmä todistaa $\neg\mathsf{Tod}(g,0)$, $\neg\mathsf{Tod}(g,1)$, ...
- jos järjestelmä ei todista $\exists p : \mathsf{Tod}(g,p)$, niin se on epätäydellinen
- muussa tapauksessa järjestelmä todistaa, että p on olemassa, mutta todistaa jokaisesta luvusta erikseen, että se ei kelpaa p:ksi
  - tämä ei ole ristiriita, mutta on silti mahdoton hyväksyä
  - sen nimi on ω-ristiriita

Gödelin toinen epätäydellisyyslause

- kaava numero g eli $\neg\exists p : \mathsf{Tod}(g,p)$ sanoo "mikään luku ei todista kaavaa numero g"
- näimme edellä, että jos jokin luku todistaa kaavan numero g, niin seuraa ristiriita

$\Rightarrow$ jos todistusjärjestelmä on ristiriidaton, niin
  - ei ole olemassa lukua, joka todistaa kaavan numero g
  - mutta juuri sen kaava numero g sanoo, joten kaava numero g on tosi

- sama ajatuskulku voidaan esittää luonnollisilla luvuilla kaavojen numeroilla
  - ristiriidattomuus voidaan ilmaista esim. $\neg\exists p : \mathsf{Tod}(f,p)$, missä f on kaavan $0 = 1$ numero

$\Rightarrow$ jos luonnollisten lukujen todistusjärjestelmä "tietää", että se itse on ristiriidaton, eli jos se todistaa $\neg\exists p : \mathsf{Tod}(f,p)$, niin se todistaa kaavan g

- silloin jokin luku on kaavan g todistuksen numero, jolloin tulee em. ristiriita

$\Rightarrow$ mikään luonnolliset luvut symboleilla 0, 1, $+$ ja $\cdot$ ja peruslogiikan sisältävä ristiriidaton todistusjärjestelmä ei voi todistaa omaa ristiriidattomuuttaan

On tavallista tulkita tämän tarkoittavan, että matematiikka ei voi todistaa omaa ristiriidattomuuttaan, paitsi jos se on ristiriitainen

- tavallinen ristiriitainen todistusjärjestelmä kyllä todistaa oman ristiriidattomuutensa!
  - ristiriidasta voidaan tavallisissa todistusjärjestelmissä todistaa ihan mitä tahansa

J. Barkley Rosser näytti 1936, miten voidaan välttää tarve puhua ω-ristiriidoista

- Rosserin kaava R on $\forall p : (\mathrm{Tod}(r,p) \to \exists x : x \leq p \wedge \mathrm{Tod}(\bar{r},x))$
  - ym. kaavan numero on r
  - sen negaation numero on $\bar{r}$
  - ”jokaiselle luvulle, joka todistaa minut, on olemassa enintään yhtä suuri luku, joka todistaa negaationi”
- jos vaikka 3810 todistaa R:n, niin todistusjärjestelmä todistaa kaavat R, $\mathrm{Tod}(r,3810)$ ja $\exists x : x \leq 3810 \wedge \mathrm{Tod}(\bar{r},x))$
  - jos sellainen x on olemassa, niin järjestelmä todistaa $\neg R$, jolloin saatiin ristiriita
  - muussa tapauksessa se todistaa $\neg\mathrm{Tod}(\bar{r},0)$, $\neg\mathrm{Tod}(\bar{r},1)$, ..., $\neg\mathrm{Tod}(\bar{r},3810)$ ja niistä $\neg\exists x : x \leq 3810 \wedge \mathrm{Tod}(\bar{r},x)$, taas ristiriita
- jos vaikka 3810 todistaa $\neg R$:n, niin todistusjärjestelmä todistaa kaavat $\mathrm{Tod}(\bar{r},3810)$ ja $\exists p : \mathrm{Tod}(r,p) \wedge \neg\exists x : x \leq p \wedge \mathrm{Tod}(\bar{r},x)$
  - se todistaa $\exists p : \mathrm{Tod}(r,p) \wedge p < 3810$
  - jos sellainen p on olemassa, niin se todistaa R:n, joten saatiin ristiriita
  - muussa tapauksessa järjestelmä todistaa $\neg\mathrm{Tod}(r,0)$, $\neg\mathrm{Tod}(r,1)$, ..., $\neg\mathrm{Tod}(r,3809)$, taas ristiriita
- Rosserin tuloksen vuoksi ω-ristiriitaisuus ei ole tärkeää epätäydellisyydelle (toisin kuin joidenkin tiedettä havainnollistavien tekstien perusteella voisi luulla)

Aksioomat ja päättelyjärjestelmät

- edellä tässä luvussa olemme olettaneet hyvin vähän siitä, miten kaavoja todistetaan
  - todistusten on oltava tarkastettavissa algoritmilla
  - epätäydellisyyslauseet olettavat jonkin verran predikaattilogiikan päättelykykyä
- matematiikassa ja logiikassa hyvin tavallinen rakenne:
  ei-loogiset symbolit, aksioomat ja päättelyjärjestelmä $\rightsquigarrow$ teoria
- ei-loogiset symbolit ovat puheenaiheen vakiot, funktiot ja relaatiot
- *todistusjärjestelmä* voi olla *päättelyjärjestelmä ja aksioomat*, tai olla muunlainen

Aksioomat

- puheenaiheen mukaan valittu (mahdollisesti ääretön) joukko suljettuja kaavoja
- usein vaaditaan, että ”on aksiooma” on oltava tarkastettavissa algoritmilla
- *aksioomaskeema* esittää (tyypillisesti äärettömän) joukon aksioomia siten, että voidaan tarkastaa algoritmilla, kuuluuko annettu merkkijono siihen

Päättelyjärjestelmä

- sen avulla johdetaan joukosta kaavoja lisää kaavoja
  - aksioomista teoreemoja
  - jo johdetuista kaavoista ja tilapäisistä oletuksista kaavoja
- samaa päättelyjärjestelmää voidaan käyttää monelle eri puheenaiheelle
- pian tulee esimerkki, ns. luonnollinen päättely

Esimerkki: Peanon aritmetiikka (1. kertaluku)

$$\forall x : x+1 \neq 0 \qquad \forall x : \forall y : x+1 = y+1 \to x = y$$
$$\forall x : x+0 = x \qquad \forall x : \forall y : x+(y+1) = (x+y)+1$$
$$\forall x : x \cdot 0 = 0 \qquad \forall x : \forall y : x(y+1) = xy+x$$

Jokaiselle kaavalle φ, missä φ:n vapaat muuttujat ovat $x, y_1, \ldots, y_n$:

$$\forall y_1 : \ldots \forall y_n : (\varphi(0) \land \forall x : \varphi(x) \to \varphi(x+1)) \to \forall x : \varphi(x)$$

- (usein "$\ldots + 1$":n tilalla on "$S(\ldots)$", mutta ne tarkoittavat samaa)
- ylimmät kaksi takaavat, että 0, $0+1$, $0+1+1$, ... ovat erisuuret
- seuraavat neljä määrittelevät yhteen- ja kertolaskun
- vielä tarvitaan "muita luonnollisia lukuja ei ole"
- 2. kl. pred.logiikassa sen voi sanoa $\forall X : (X(0) \land \forall x : X(x) \to X(x+1)) \to \forall x : X(x)$
  - jos $\mathbb{N}$:n osajoukko sisältää 0 ja jokaisen sisältämänsä luvun seuraajan, niin se on $\mathbb{N}$
  - mutta 2. kl. pred.logiikassa on ongelmansa, joiden vuoksi usein halutaan 1. kl.
- alin aksiooma on nimeltään *induktioaksiooma*
  - sama idea kuin edellä, mutta vain kaavoina määriteltävissä oleville $\mathbb{N}$:n osajoukoille
  - ei ole yksi aksiooma, vaan aksioomaskeemana ilmaistu ääretön joukko aksioomia
  - usein $y_1, \ldots, y_n$ jätetään näyttämättä $\Rightarrow$ epäolennainen virhe (ei ole suljettu kaava)
- 1. epätäydellisyyslauseen vuoksi kummallakaan tavalla ei saada täydellisyyttä
  - esim.: Paris-Harringtonin lause

Esimerkki: reaalisuljetut kunnat

- kunta-aksioomat

$$\forall x : \forall y : x + y = y + x \qquad \forall x : \forall y : xy = yx$$
$$\forall x : \forall y : \forall z : (x + y) + z = x + (y + z) \qquad \forall x : \forall y : (xy)z = x(yz)$$
$$\forall x : x + 0 = x \qquad \forall x : x \cdot 1 = x$$
$$\forall x : \exists y : x + y = 0 \qquad \forall x : x \neq 0 \rightarrow \exists y : xy = 1$$
$$0 \neq 1 \qquad \forall x : \forall y : \forall z : x(y + z) = xy + xz$$

- järjestysaksioomat

$$\forall x : \forall y : x \leq y \vee y \leq x \qquad \forall x : \forall y : x \leq y \wedge y \leq x \leftrightarrow x = y$$
$$\forall x : \forall y : \forall z : x \leq y \wedge y \leq z \rightarrow x \leq z$$
$$\forall x : \forall y : \forall z : x \leq y \rightarrow x + z \leq y + z \qquad \forall x : \forall y : 0 \leq x \wedge 0 \leq y \rightarrow 0 \leq xy$$

- täydellisyysaksiooman korvikkeet

$$\forall x : 0 \leq x \rightarrow \exists y : yy = x$$

Jokaiselle parittomalle n:

$$\forall a_n : \ldots \forall a_2 : \forall a_1 : \forall a_0 : a_n = 0 \vee \exists x : a_n x \cdots x + \ldots + a_2 xx + a_1 x + a_0 = 0$$

- matematiikan ”täydellisyysaksiooma” ei ole 1. kl (on 2. kl)
  $\Rightarrow$ ei käytetä reaalisuljettujen kuntien määritelmässä
  - jokaisella epätyhjällä ylhäältä rajoitetulla joukolla on pienin yläraja

Yksinkertainen ”luonnollisen päättelyn” järjestelmä

- alla Γ ja Δ ovat kaavojen joukkoja
- symboleita T ja $\neq$ ei käytetä
- lähtökohdat ja päätellyt kaavat muodostavat kasvavan joukon, jonka kaikkia kaavoja saa käyttää jatkopäättelyssä

P1 $\{\varphi\} \vdash \varphi$

P2 Jos $\Gamma \vdash \varphi$ niin $\Gamma \cup \Delta \vdash \varphi$.

P3 Jos $\Gamma \vdash \varphi$ ja $\Gamma \cup \{\varphi\} \vdash \psi$, niin $\Gamma \vdash \psi$.

- ”$\neg$” vaihtaa totuusarvon, ja kolmatta totuusarvoa ei ole

C1	$\emptyset \vdash \varphi \vee \neg\varphi$	jokaisessa tilanteessa kukin kaava on tosi tai epätosi
C2	$\{\mathsf{F}\} \vdash \varphi$	epätodesta seuraa mitä tahansa
C3	$\{\varphi, \neg\varphi\} \vdash \mathsf{F}$	ristiriita on epätosi

- ”$\wedge$” ja ”$\vee$” käyttäytyvät kuten luonnollisen kielen ”ja” ja ”tai”

$\wedge$-**I**	$\{\varphi, \psi\} \vdash \varphi \wedge \psi$	$\vee$-**I1**	$\{\varphi\} \vdash \varphi \vee \psi$
$\wedge$-**E1**	$\{\varphi \wedge \psi\} \vdash \varphi$	$\vee$-**I2**	$\{\psi\} \vdash \varphi \vee \psi$
$\wedge$-**E2**	$\{\varphi \wedge \psi\} \vdash \psi$	$\vee$-**E**	Jos $\Gamma \cup \{\varphi\} \vdash \chi$ ja $\Gamma \cup \{\psi\} \vdash \chi$, niin $\Gamma \cup \{\varphi \vee \psi\} \vdash \chi$.

- yhtäsuuruuden perusominaisuudet

=-1 $\emptyset \vdash \mathfrak{f} = \mathfrak{f}$

=-2 Jos $\mathfrak{f}$ ja $\mathfrak{g}$ voidaan sijoittaa x:n tilalle $\varphi(x)$:ssä, niin $\{(\mathfrak{f} = \mathfrak{g}), \varphi(\mathfrak{f})\} \vdash \varphi(\mathfrak{g})$.

- kvanttorien perusominaisuudet

∀-E Jos $\mathfrak{f}$ voidaan sijoittaa x:n tilalle $\varphi(x)$:ssä, niin $\{\forall x : \varphi(x)\} \vdash \varphi(\mathfrak{f})$.

∀-I Jos $\Gamma \vdash \varphi(x)$ ja x ei esiinny vapaana Γ:ssa, niin $\Gamma \vdash \forall x : \varphi(x)$.

∃-I Jos $\mathfrak{f}$ voidaan sijoittaa x:n tilalle $\varphi(x)$:ssä, niin $\{\varphi(\mathfrak{f})\} \vdash \exists x : \varphi(x)$.

∃-E Jos $\Gamma \cup \{\varphi(y)\} \vdash \psi$ ja y ei esiinny Γ:ssa, $(\exists x : \varphi(x))$:ssä eikä ψ:ssä, niin $\Gamma \cup \{\exists x : \varphi(x)\} \vdash \psi$.

- esim. mistä tahansa voidaan todistaa $\neg$F

1	$\emptyset$	$\vdash$	F $\vee \neg$F	C1
2	{F}	$\vdash$	$\neg$F	C2
3	{$\neg$F}	$\vdash$	$\neg$F	P1
4	{F $\vee \neg$F}	$\vdash$	$\neg$F	$\vee$-E, 2, 3, $\Gamma = \emptyset$
5	$\emptyset$	$\vdash$	$\neg$F	P3, 1, 4, $\Gamma = \emptyset$
6	Γ	$\vdash$	$\neg$F	P2, 5

- esim. jos $\Gamma \cup \{\neg\varphi\} \vdash \mathsf{F}$, niin $\Gamma \vdash \varphi$

1	$\emptyset$	$\vdash$	$\varphi \vee \neg\varphi$	C1
2	Γ	$\vdash$	$\varphi \vee \neg\varphi$	P2, 1
3	$\{\varphi\}$	$\vdash$	φ	P1
4	$\Gamma \cup \{\varphi\}$	$\vdash$	φ	P2, 3
5	$\Gamma \cup \{\neg\varphi\}$	$\vdash$	F	lähtöoletus
6	$\{\mathsf{F}\}$	$\vdash$	φ	C2
7	$\Gamma \cup \{\neg\varphi\} \cup \{\mathsf{F}\}$	$\vdash$	φ	P2, 6
8	$\Gamma \cup \{\neg\varphi\}$	$\vdash$	φ	P3, 5, 7
9	$\Gamma \cup \{\varphi \vee \neg\varphi\}$	$\vdash$	φ	$\vee$-E, 4, 8
10	Γ	$\vdash$	φ	P3, 2, 9

- melkein samoin saadaan, että jos $\Gamma \cup \{\varphi\} \vdash \mathsf{F}$, niin $\Gamma \vdash \neg\varphi$

Mallin olemassaololause (olettaen korkeintaan numeroituva määrä ei-loogisia symboleita)

- Γ on *ristiriitainen* (*inconsistent*), jos ja vain jos $\Gamma \vdash \mathsf{F}$
- jos $\Gamma \nvdash \mathsf{F}$, niin on olemassa puheenaihe, jossa on äärellinen tai numeroituvasti ääretön määrä alkioita ja joka toteuttaa jokaisen $\varphi \in \Gamma$
- todistus mukailee päättelyä, jonka julkaisi Leon Henkin 1949 väitöskirjansa pohjalta

Otetaan käyttöön numeroituvasti ääretön määrä uusia muuttujia $v_0, v_1, v_2, \ldots$

”Käydään läpi” jokainen kaava φ jonka valituilla symboleilla voi kirjoittaa, ja lisätään Γ:an kaavoja ristiriidat välttäen seuraavasti

- ”käydään läpi” on tässä vain puhetapa, sitä ei voi kirjaimellisesti toteuttaa
  - mutta ”läpikäynnin” lopputulos on joukko-opin mukaan todistettavasti olemassa
- jos $\Gamma \cup \{\varphi\} \nvdash \mathsf{F}$, niin lisätään φ, muussa tapauksessa lisätään $\neg\varphi$
  - sivun 202 ja P3 vuoksi ja koska $\Gamma \nvdash \mathsf{F}$, jos $\Gamma \cup \{\varphi\} \vdash \mathsf{F}$ niin $\Gamma \cup \{\neg\varphi\} \nvdash \mathsf{F}$
- jos lisättävä kaava on muotoa $\neg\forall x : \psi(x)$, niin lisätään myös $\neg\psi(v_i)$, missä v_i on jokin muuttujista $v_0, v_1, v_2, \ldots$, jota ei ole vielä käytetty
  - tämä varmistaa, että $\neg\forall x : \psi(x)$ on totta siinä puheenaiheessa, jota rakennamme
  - jos $\Gamma \cup \{\neg\psi(v_i)\} \vdash \mathsf{F}$, niin $\Gamma \vdash \psi(v_i)$
  - koska v_i on aiemmin käyttämätön, $\forall$-I tuottaa $\Gamma \vdash \forall v_i : \psi(v_i)$ ja $\Gamma \vdash \forall x : \psi(x)$
  - niin ei voi olla, koska lisäyksen ehto oli $\neg\forall x : \psi(x) \nvdash \mathsf{F}$

  $\Rightarrow \Gamma \cup \{(\neg\forall x : \psi(x)), (\neg\psi(v_i))\} \nvdash \mathsf{F}$

- jos lisättävä kaava on muotoa $\exists x : \psi(x)$, niin lisätään myös $\psi(v_i)$, missä v_i on ...
  - jos $\Gamma \cup \{\psi(v_i)\} \vdash$ F, niin $\exists$-E:n mukaan $\Gamma \cup \{\exists x : \psi(x)\} \vdash$ F, vastoin lisäysehtoa
- jos lisättävä kaava on muotoa $c = c$ tai $f(v_{i_1}, \ldots, v_{i_n}) = f(v_{i_1}, \ldots, v_{i_n})$, niin lisätään myös $c = v_i$ tai $f(v_{i_1}, \ldots, v_{i_n}) = v_i$, missä v_i on ... eikä v_i ole mikään v_{i_j}
  - tämä lisäys on tarpeeton, mutta helpottaa todistuksen jatkon ymmärtämistä
  - jos $\Gamma \cup \{\mathfrak{f} = v_i\} \vdash$ F, niin $\Gamma \vdash \neg(\mathfrak{f} = v_i)$
  - $\forall$-I:n mukaan $\Gamma \vdash \forall v_i : \neg(\mathfrak{f} = v_i)$, joten $\forall$-E:n mukaan $\neg(\mathfrak{f} = \mathfrak{f})$, josta $=$-1 tuottaa F

Lopullinen Γ on ristiriidaton

- jos se olisi ristiriitainen, olisi ristiriidalle olemassa todistus
- kukin todistus käyttää vain äärellistä määrää kaavoja

$\Rightarrow$ ristiriitaisuuden todistus menisi läpi heti kun jokainen tarvittava kaava on Γ:ssa, siis ennen kuin Γ on valmis

- mahdotonta, koska jokainen Γ:n laajennos säilyttää ristiriidattomuuden

Lopullisessa Γ:ssa mukana olevat kaavat vastaavat symboleiden merkityksiä

- puheenaiheen arvoiksi valitaan ne v_i, joille ei ole Γ:ssa mikään $v_j = v_i$, missä $j < i$
  - vakioiden arvot määräytyvät mukana olevista kaavoista muotoa $c = v_i$
  - funktioiden arvot määräytyvät mukana olevista kaavoista $f(v_{i_1}, \ldots, v_{i_n}) = v_i$
  - relaatioiden totuusarvot määräytyvät mukana olevista kaavoista $\neg P(v_{i_1}, \ldots, v_{i_n})$
  - $=$-1:n ja $=$-2:n ansiosta lausekkeiden ja kaavojen lopputulos ei riipu siitä, mitkä keskenään yhtäsuurista lausekkeista ovat argumentteina
- jos mukana on $\varphi \wedge \psi$, niin mukana on φ eikä $\neg\varphi$, koska muutoin $\wedge$-E1:llä voitaisiin johtaa ristiriita
- jos mukana on $\forall x : \varphi(x)$, niin $\forall$-E:n vuoksi mukana ei ole mikään $\neg\varphi(c)$
- jos mukana on $\neg\forall x : \varphi(x)$, niin mukana on samalla lisätty $\neg\varphi(c)$
- ...

Gödelin täydellisyyslause

- jos $\Gamma \nvdash \varphi$, niin sivun 202 mukaan $\Gamma \cup \{\neg\varphi\} \nvdash$ F

$\Rightarrow$ mallin olemassaololauseen mukaan on olemassa puheenaihe, joka toteuttaa sekä jokaisen Γ:an kuuluvan kaavan että $\neg\varphi$:n

- siksi olisi väärin, jos Γ:sta voitaisiin todistaa φ

$\Rightarrow$ edellä esitetty päättelyjärjestelmä todistaa kaiken mitä pitääkin, eikä yhtään enempää

- Gödelin oma todistus (1929) oli erilainen, väitöskirjasta sekin

Ei ole olemassa täydellistä 2. kl. päättelyjärjestelmää

- luonnolliset luvut 0, 1, $+$, $\cdot$ voidaan määritellä tyhjentävästi 2. kl. predikaattilogiikalla
- epätäydellisyyslauseen vuoksi luonnollisilla luvuilla joko määrittelemisen tai päättelemisen tai molempien täytyy olla jotenkin puutteellisia
- luonnollisten lukujen ja monen muun puheenaiheen kohdalla tilanne on seuraava:
  - 2. kl.: voidaan määritellä tyhjentävästi, ei voida päätellä kaikkia seurauksia
  - 1. kl.: ei voida määritellä tyhjentävästi, mutta kaikki seuraukset voidaan päätellä
- yleisin valinta matematiikassa on käyttää taustateoriana 1. kl. joukko-oppia

Mallin olemassaololauseen todistuksella on omituinen seuraus

- todistuksessa muodostetussa puheenaiheessa on enintään numeroituvasti ääretön määrä alkioita

$\Rightarrow$ 1. kl. määritelmät reaaliluvuille ja joukko-opille toteutuvat numeroituvalla määrällä alkioita (paitsi jos ei-loogisia symboleita on ylinumeroituva määrä)

- ”oikeita” reaalilukuja ja ”oikeita” joukkoja on ylinumeroituva määrä
- tämä ristiriidalta vaikuttava tosiasia on nimeltään Skolemin paradoksi
  - sen huomasivat jo Leopold Löwenheim 1915 ja Thoralf Skolem 1920
- reaaliluvut voidaan määritellä tyhjentävästi 2. kl. predikaattilogiikalla, mutta siitä ei saada kaikkea irti, koska ei ole olemassa täydellistä 2. kl. päättelyjärjestelmää!
- myös Peanon aksioomilla on epästandardeja numeroituvia toteutumia

Saavutettavuutta ei voi määritellä 1. kl. kaavoilla

- alkioiden määrän voi pakottaa äärettömäksi seuraavalla aksioomaskeemalla

  $\exists x_1 : \exists x_2 : x_1 \neq x_2$
  $\exists x_1 : \exists x_2 : \exists x_3 : x_1 \neq x_2 \neq x_3 \neq x_1$
  $\exists x_1 : \exists x_2 : \exists x_3 : \exists x_4 : x_1 \neq x_2 \neq x_3 \neq x_4 \neq x_1 \neq x_3 \wedge x_2 \neq x_4$
  $\ldots$
- 1. kl. tapauksessa sitä ei voi pakottaa äärelliseksi muuten kuin kiinnittämällä ylärajan
  - voi sanoa, että alkioita on enintään 1000
  - ei voi sallia miten suurta äärellistä määrää tahansa sallimatta samalla äärettömän
- oletetaan mikä tahansa ristiriidaton 1. kl. määritelmä, joka ei salli ääretöntä määrää
  - kun siihen lisätään ym. aksioomaskeema, sitä ei enää toteuta mikään puheenaihe
  - mallin olemassaololauseen mukaan voidaan todistaa F
  - todistus voi käyttää vain äärellistä määrää skeeman aksioomia, koska todistukset ovat äärellisiä
  - olkoon suurin jota se käyttää vaikka ”alkioita on ainakin 1000”

  $\Rightarrow$ puheenaiheessa ei voi olla tuhat tai enemmän alkioita
- tarkoittakoon $E^*(x,y)$, että on olemassa polku x:stä y:hyn, eli sellaiset $x_0,\ldots,x_n$, että $x = x_0 \wedge E(x_0,x_1) \wedge E(x_1,x_2) \wedge \cdots \wedge E(x_{n-1},x_n) \wedge x_n = y$
- silmukan voi määritellä näin: $\forall x : (\forall y : E^*(x,y)) \wedge \exists y : E(x,y) \wedge \forall z : E(x,z) \rightarrow z = y$
- on olemassa mielivaltaisen suuria äärellisiä, mutta ei äärettömiä silmukoita

$\Rightarrow$ $E^*(x,y)$ ei voi määritellä 1. kl. keinoin

13 Lopuksi

Loppu