Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2026

Tekijärakenne

Polynomirenkaan ihanteet

- $\mathbb{R}[x]/\langle x^2+1\rangle$
- $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$

Matemaattinen induktio

Induktioperiaate joukossa $\mathbb{N}$

Tässä $P(n)$ tarkoittaa, että luonnollisella luvulla n on ominaisuus P. Mikäli

- $P(1)$
- $(\forall n)(P(n) \rightarrow P(n+1))$

Niin tällöin ominaisuus P on jokaisella luonnollisella luvulla $\mathbb{N}$.

Dominoperiaate

- Palikka nro 1 kaatuu.
- Jos palikka nro n kaatuu, niin myös palikka nro $n+1$ kaatuu.
- Johtopäätös: Kaikki palikat kaatuvat.

Induktioperiaate joukossa $\mathbb{N}$

Määritelmä

- Ominaisuuden $P(1)$ oikeaksi todistaminen on nimeltään *induktion lähtökohta*
- $(\forall n)(P(n) \to P(n+1))$ oikeaksi todistaminen on nimeltään *induktioaskel*
- Induktioaskel todistetaan oikeaksi seuraavasti:
- 1) Näytetään toteen väittämä $P(n) \to P(n+1)$ olettamatta mitään luvusta n.
- 2a) Edellämainittu tapahtuu olettamalla $P(n)$ (Induktio-oletus) ja
- 2b) johtamalla tästä $P(n+1)$ (Induktioväite)

Esimerkki

Väite

$$\sum_{i=1}^{n} i = \frac{1}{2} n(n+1)$$

Induktion lähtökohta $n = 1$

$$\sum_{i=1}^{1} i = \frac{1}{2} \cdot 1 \cdot (1+1) \Leftrightarrow 1 = 1, \text{ tosi.}$$

Esimerkki

Induktioaskel

Induktio-oletus: Väite pitää paikkansa luvulle n.
Induktioväite: Väite pitää paikkansa luvulle $n+1$
Todistus:

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + n + 1 = \frac{1}{2}n(n+1) + n + 1 = \frac{1}{2}(n+1)(n+2).$$

Esimerkki

Newtonin binomikaava

Väite:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

Induktion lähtökohta $n = 1$

$$(x+y)^1 = \sum_{i=0}^{1} \binom{1}{i} x^{1-i} y^i \quad \Leftrightarrow \quad x+y = \binom{1}{0} x^1 y^0 + \binom{1}{1} x^0 y^1$$

$$\Leftrightarrow \quad x+y = x+y, \quad \text{tosi}$$

Muistettava

$$\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$$

Induktioaskel

Induktio-oletus: Väite on tosi jollekin luvulle n.
Induktioväite: Väite on tosi luvulle $n+1$.
Todistus:

$$
\begin{aligned}
& (x+y)^{n+1} \\
= \; & (x+y)(x+y)^n = (x+y)\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i \\
= \; & x\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i + y\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i \\
= \; & \sum_{i=0}^{n}\binom{n}{i}x^{n+1-i}y^i + \sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^{i+1} \\
= \; & x^{n+1} + \sum_{i=1}^{n}\binom{n}{i}x^{n+1-i}y^i + \sum_{i=0}^{n-1}\binom{n}{i}x^{n-i}y^{i+1} + y^{n+1}
\end{aligned}
$$

Induktioaskel (jatkoa)

$$
\begin{aligned}
& (x+y)^{n+1} \\
= \; & x^{n+1} + \sum_{i=1}^{n} \binom{n}{i} x^{n+1-i} y^i + \sum_{i=0}^{n-1} \binom{n}{i} x^{n-i} y^{i+1} + y^{n+1} \\
= \; & x^{n+1} + \sum_{i=1}^{n} \binom{n}{i} x^{n+1-i} y^i + \sum_{i=1}^{n} \binom{n}{i-1} x^{n-(i-1)} y^{i-1+1} + y^{n+1} \\
= \; & x^{n+1} + \sum_{i=1}^{n} \binom{n}{i} x^{n+1-i} y^i + \sum_{i=1}^{n} \binom{n}{i-1} x^{n+1-i} y^i + y^{n+1} \\
= \; & x^{n+1} + \sum_{i=1}^{n} \left(\binom{n}{i} + \binom{n}{i-1} \right) x^{n+1-i} y^i + y^{n+1}
\end{aligned}
$$

Induktioaskel (jatkoa)

$$
\begin{aligned}
& (x+y)^{n+1} \\
= \; & x^{n+1} + \sum_{i=1}^{n} \left(\binom{n}{i} + \binom{n}{i-1} \right) x^{n+1-i} y^i + y^{n+1} \\
= \; & x^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} x^{n+1-i} y^i + y^{n+1} \\
= \; & \sum_{i=0}^{n+1} \binom{n+1}{i} x^{n+1-i} y^i .
\end{aligned}
$$

Esimerkki

Väite

Fibonaccin luvut F_n toteuttavat epäyhtälön $F_n \leq 2^n$.

Induktion lähtökohta $n \in \{0, 1\}$

$F_0 = 0 \leq 2^0 = 1$, $F_1 = 1 \leq 2^1 = 2$, tosi.

Induktioaskel

Induktio-oletus: Väite on tosi jollekin luvulle $n \geq 1$ *ja myös* luvulle $n - 1$.

Induktioväite: Väite on tosi luvulle $n + 1$.

Todistus:

$$F_{n+1} = F_n + F_{n-1} \leq 2^n + 2^{n-1} \leq 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

Predikaattilogiikkaa

Esimerkki

$$\frac{\text{Jokainen ihminen on kuolevainen (pääpremissi)} \qquad \text{Sokrates on ihminen (alipremissi)}}{\text{Sokrates on kuolevainen (johtopäätös)}}$$

Huomautus

Johtopäätös seuraa premisseistä.

Abstrahointi

$I(x) =$ "x on ihminen", $K(x) =$ "x on kuolevainen" ja $s=$"Sokrates".

Syllogismi uudelleen

$$\frac{(\forall x)(I(x) \rightarrow K(x)) \qquad I(s)}{K(s)}$$

Toinen esitysmuoto:

$$\{(\forall x)(I(x) \rightarrow K(x)), I(s)\} \models K(s)$$

Syntaksi

Predikaattilogiikan aakkosto

- Loogiset konnektiivit $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.
- Yhtäsuuruusmerkki $=$, sulkumerkit (ja) ja pilkku ,.
- Universaalikvanttori $\forall$ ja eksistentiaalikvanttori $\exists$.
- Muuttujasymbolit x_1, x_2, x_3, ...
- Nolla, yksi- tai useampipaikkaiset *predikaatti-* eli *relaatiosymbolit* R_1, R_2, R_3, ...
- Funktiosymbolit f_1, f_2, f_3, ... ja *vakiosymbolit* c_1, c_2, c_3, ...

$\vee R_1 \neg x \forall \rightarrow) c_1 f_1 \wedge f_2$?

Syntaksi

Predikaattilogiikan termit:

- Muuttujasymbolit x_1, x_2, x_3, ... ja vakiosymbolit c_1, c_2, c_3 ... ovat termejä
- Jos t_1, t_2, ..., ovat termejä ja f funktiosymboli, niin $f(t_1, t_2, \ldots)$ on termi.

Predikaattilogiikan kaavat:

- Jos R on relaatiosymboli ja t_1, t_2, ... termejä, niin $R(t_1, t_2, \ldots)$ on kaava.
- Jos t_1 ja t_2 ovat termejä, niin $(t_1 = t_2)$ on kaava. Tätä muotoa olevaa kaavaa sanotaan myös *yhtälöksi*.
- Jos ϕ ja ψ ovat kaavoja, niin $(\neg\phi)$, $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$ ja $(\phi \leftrightarrow \psi)$ ovat kaavoja.
- Jos ϕ on kaava ja x muuttuja, niin $((\forall x)\phi)$ ja $((\exists x)\phi)$ ovat kaavoja.

Syntaksi

- t_1, t_2, t_3, ..., termejä
- $R(t_1, t_2, \ldots)$ ja $(t_1 = t_2)$ ovat *atomikaavoja*
- Atomikaavoista saadaan konnektiiveilla ja kvanttoreilla muita kaavoja: $(\neg\phi)$, $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$, $(\phi \leftrightarrow \psi)$, $((\forall x)\phi)$ ja $((\exists x)\phi)$.

Lyhennysmerkinnät 1

- $\neg$ sitoo vahvemmin kuin $\wedge$ ja $\vee$, siis $\neg\phi \wedge \psi$ merkitsee kaavaa $(\neg\phi) \wedge \psi$, ei kaavaa $\neg(\phi \wedge \psi)$.
- $\wedge$ ja $\vee$ sitovat vahvemmin kuin $\rightarrow$ ja $\leftrightarrow$, siis $\neg\phi \wedge \psi \rightarrow \eta$ on lyhennysmerkintä kaavasta $(((\neg\phi) \wedge \psi) \rightarrow \eta)$.
- Kvanttorit sitovat vahvemmin kuin $\neg$ tai $\vee$, siis $(\forall x)\phi \vee \psi$ tarkoittaa kaavaa $(((\forall x)\phi) \vee \psi)$.

Lyhennysmerkinnät 2

- $\sqrt{x}$ tulkitaan yksipaikkaiseksi funktiosymboliksi
- $x > y$ tulkitaan kaksipaikkaiseksi relaatiosymboliksi
- jne.

Vapaat / sidotut muuttujat, kaavat / lauseet

Jos ϕ on predikaattilogiikan kaava ja x siinä esiintyvä muuttuja, sanotaan, että kaavassa $(\forall x)\phi$ ja $(\exists x)\phi$ x on *sidottu* muuttuja. Jos muuttuja ei ole sidottu, se on *vapaa*. Kaavaa, jossa ei ole vapaita muuttujia, kutsutaan *lauseeksi*.

Esimerkki

- $(x + y)^2 = x^2 + 2xy + y^2$ on kaava.
- $(\forall x)(\forall y)((x + y)^2 = x^2 + 2xy + y^2)$ on myös lause.

Peanon aksioomat

- Jos $n \neq m$, niin $s(n) \neq s(m)$ (kahdella eri luonnollisella luvulla on eri seuraaja).
- Kaikille joukon $\mathbb{N}$ alkioille n pätee $s(n) \neq 1$ (ykkönen ei ole minkään luonnollisen luvun seuraaja).
- Jos joukko A sisältää luvun 1 ja jokaisen sisältämänsä luvun seuraajan, niin silloin A sisältää kaikki luonnolliset luvut (*induktioaksiooma*).

Predikaattilogiikan merkinnöin:

- $(\forall x)(\forall y)(\neg(x = y) \rightarrow \neg(s(x) = s(y)))$
- $(\forall x)\neg(s(x) = 1)$
- $(\forall A)((1 \in A \wedge (\forall x)(x \in A \rightarrow s(x) \in A)) \rightarrow (\forall x)(x \in A))$

Määritelmä

Predikaattilogiikan tulkinta I koostuu

- Tulkintajoukosta A,
- Vakiosymbolien tulkinnasta joukon A alkioiksi,
- Funktiosymbolien tulkinnasta joukossa A määritellyiksi funktioiksi,
- Predikaattisymbolien tulkinnasta joukon A relaatioiksi,
- Vapaiden muuttujien tulkinnasta joukon A alkioiksi.

Kvanttorit ja konnektiivit tulkittava myös.

Atomikaavojen tulkinta

- Atomikaava $R(t_1, t_2, \ldots)$ on *tosi* annetussa tulkinnassa, mikäli termien t_1, t_2, ... tulkinnat ovat siinä tulkintajoukon relaatiossa, joksi R tulkitaan.
- Atomikaava $t_1 = t_2$ on *tosi* annetussa tulkinnassa, mikäli termit t_1 ja t_2 tulkitaan samaksi joukon A alkioksi.

Tulkinnan antama *totuusarvo* kaavalle ϕ on 0 mikäli ϕ tulkitaan epätodeksi ja 1 mikäli ϕ tulkitaan todeksi. Jos tulkintaa merkitään symbolilla I, merkitään kaavan ϕ totuusarvoa tulkinnassa I $\alpha_I(\phi)$:llä.

Kvanttorit

Olkoon $\phi(x)$ predikaattilogiikan kaava, jossa x on vapaa muuttuja.

- $(\forall x)\phi(x)$ tulkitaan todeksi, jos kaava $\phi(x)$ tulkitaan todeksi *kaikilla* x:n valinnoilla (tulkintajoukosta)
- $(\exists x)\phi(x)$ tulkitaan todeksi, jos *on olemassa* sellainen x:n valinta tulkintajoukosta, että kaava $\phi(x)$ voidaan tulkita todeksi.

Konnektiivit

Olkoot ϕ ja ψ kaavoja. Niiden totuusarvojen perusteella saadaan konnektiiveilla rakennettujen kaavojen totuusarvot seuraavan taulukon mukaan.

ϕ	ψ	$\neg\phi$	$\phi \wedge \psi$	$\phi \vee \psi$	$\phi \rightarrow \psi$	$\phi \leftrightarrow \psi$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Esimerkki

Kaavan

$$(I(s) \wedge (\forall x)(I(x) \rightarrow K(x))) \rightarrow K(s)$$

tulkinta, kun tulkintajoukko on $\mathbb{N}$, $I(x)$ tulkitaan "x on parillinen", $K(x)$ "x on suurempi kuin kymmenen", ja s tulkitaan luvuksi 2:

- $I(s)$="2 on parillinen", siis tosi
- $I(x) \rightarrow K(x)$: epätosi vain jos $I(x)$ tosi ja $K(x)$ epätosi
- Jos esim x tulkitaan luvuksi 4, on $I(x)$ tosi ja $K(x)$ epätosi
- Tällöin $(\forall x)(I(x) \rightarrow K(x))$ epätosi
- Konnektiivin $\wedge$ tulkinnan mukaan $I(s) \wedge (\forall x)(I(x) \rightarrow K(x))$ tulkitaan epätodeksi
- Konnektiivin $\rightarrow$ tulkinnan mukaan koko kaava tulkitaan todeksi.

Kaava

$$(I(s) \wedge (\forall x)(I(x) \rightarrow K(x))) \rightarrow K(s)$$

on tosi *kaikissa tulkinnoissa*:

- *Voisi* olla epätosi vain jos $I(s) \wedge (\forall x)(I(x) \rightarrow K(x))$ tosi ja $K(s)$ epätosi
- Olkoon J tulkinta jossa näin käy
- $\Rightarrow$ J:ssä sekä $I(s)$ että $(\forall x)(I(x) \rightarrow K(x))$ tosia
- $\Rightarrow$ $I(x) \rightarrow K(x)$ tulkittava todeksi kaikilla tulkintajoukon alkiolla
- $\Rightarrow$ $I(s) \rightarrow K(s)$ tulkittava todeksi
- Ristiriita! (kts. aikaisempi vaatimus $I(s)$:n ja $K(s)$:n tulkinnasta)

Määritelmä

Kaava on

- *Toteutuva* jos se on tosi ainakin yhdessä tulkinnassa (eli sillä on ainakin yksi malli).
- *Kumoutuva* jos se on epätosi ainakin yhdessä tulkinnassa.
- *Tautologia* eli loogisesti tosi, jos se on tosi kaikissa tulkinnoissa.
- *Kontradiktio* eli loogisesti epätosi, jos se on epätosi kaikissa tulkinnoissa.
- *Kontingentti*, jos se ei ole tautologia eikä kontradiktio.

Otetaan käyttöön merkinnät $\top$ (verum) ja $\bot$ (falsum). Nämä ovat nollapaikkaisia predikaattisymboleja, jotka tulkitaan kaikissa tulkinnoissa samoin: $\top$ tulkitaan todeksi ja $\bot$ epätodeksi.

Semantiikka: Looginen seuraus

Malli

Kaava- tai lausejoukon Γ *malli* on tulkinta I, jossa kaikki Γ:n kaavat ovat tosia

Määritelmä

Päättely *premisseistä* Γ *johtopäätösjoukkoon* Δ on *pätevä* eli *loogisesti sitova*, jos kaikki joukon Γ mallit ovat myös Δ:n malleja. Tällöin merkitään $\Gamma \models \Delta$ ja sanotaan, että Δ on *looginen seuraus* joukon Γ kaavoista.
Jos $\Delta = \{\phi\}$, merkitään $\Gamma \models \phi$ ja sanotaan, että kaava ϕ on kaavajoukon Γ looginen seuraus.
Jos $\Gamma \models \Delta$ ja $\Delta \models \Gamma$, sanotaan, että Γ ja Δ ovat loogisesti *ekvivalentit* ja merkitään $\Gamma \equiv \Delta$.
$\emptyset \models \Delta$ merkitsee, että Δ:n kaavat ovat tosia kaikissa tulkinnoissa. Tämä merkitään myös $\models \Delta$.

Esimerkki

Päättely

$$\{I(s), (\forall x)(I(x) \rightarrow K(x))\} \models K(s)$$

on loogisesti sitovaa:

- Olkoon J tulkinta jossa premissit ovat tosia
- $\Rightarrow$ $I(s)$ tosi ja $(\forall x)(I(x) \rightarrow K(x))$ tosi
- $\Rightarrow$ $(I(s) \rightarrow K(s))$ tosi
- $\Rightarrow$ $K(s)$ tosi

Loogisen seurauksen toteennäyttäminen

- Suora todistus:

$$\Gamma_1 \models \Gamma_2 \models \ldots \models \Gamma_n \models \phi,$$

- Epäsuora todistus:

$$\Gamma \cup \{\neg\phi\} \models \bot$$

Semantiikka: Looginen seuraus

Lause (Epäsuora todistus)

Jos $\Gamma \cup \{\neg\phi\} \models \bot$, niin $\Gamma \models \phi$.

Aputulos (Lemma)

Jos $\Delta \models \bot$, niin Δ:lla ei ole mallia.
Todistus: Jokainen Δ:n malli olisi myös sen loogisten seurausten malli.

Lauseen todistus

Oletetaan, että I on Γ:n malli. On näytettävä, että se on myös ϕ:n malli. Vastaoletus: I ei ole ϕ:n malli. $\Rightarrow$ I on $\neg\phi$:n malli.$\Rightarrow$ I on $\Gamma \cup \{\neg\phi\}$:n malli. Ristiriita!

Vastaesimerkki

$$\Gamma \not\models \phi,$$

jos on olemassa Γ:n malli, jossa ϕ ei ole tosi.

Gentzenin järjestelmä

- Automatisoitavissa oleva systeemi, jonka sääntöjen mukaan aiemmista kaavoista kirjoitetaan uusia (käsittely syntaktisesti)
- Tavoitteena mahdollisimman hyvä kytkentä sääntöjen (syntaksi) ja loogisen seurauksen (semantiikka) välille

Konnektiivien introduktiosäännöt

$$(I\wedge): \quad \frac{\phi \quad \psi}{\phi \wedge \psi} \qquad (I\vee): \quad \frac{\phi}{\phi \vee \psi} \quad \text{ja} \quad \frac{\psi}{\phi \vee \psi}$$

$$(I\to): \quad \frac{\begin{array}{c}[\phi^{\checkmark}]\\ \vdots \\ \psi\end{array}}{\phi \to \psi} \qquad (I\neg): \quad \frac{\begin{array}{c}[\phi^{\checkmark}]\\ \vdots \\ \bot\end{array}}{\neg\phi} \qquad (I\leftrightarrow): \quad \frac{\begin{array}{cc}[\phi^{\checkmark}] & [\psi^{\checkmark}]\\ \vdots & \vdots \\ \psi & \phi\end{array}}{\phi \leftrightarrow \psi}$$

$\phi^{\checkmark}$ tarkoittaa sitä, että säännön soveltamisen jälkeen ϕ merkitään "poistetuksi"

Konnektiivien eliminointisäännöt

$$(E\wedge):\quad \frac{\phi\wedge\psi}{\phi}\qquad \frac{\phi\wedge\psi}{\psi}$$

$$(E\vee):\quad \frac{\phi\vee\psi \qquad \begin{array}{c}\phi^{\checkmark}\\ \vdots\\ \eta\end{array} \qquad \begin{array}{c}\psi^{\checkmark}\\ \vdots\\ \eta\end{array}}{\eta}$$

$$(E\to):\quad \frac{\phi \quad \phi\to\psi}{\psi}$$

$$(E\neg):\quad \frac{\phi \quad \neg\phi}{\bot}$$

$$(E\leftrightarrow):\quad \frac{\phi \quad \phi\leftrightarrow\psi}{\psi}\qquad \frac{\psi \quad \phi\leftrightarrow\psi}{\phi}$$

$$(E\bot):\quad \frac{\bot}{\phi}$$

Reductio Ad Absurdum

$$(RAA): \dfrac{\begin{array}{c}\neg\phi^{\checkmark}\\ \vdots\\ \bot\end{array}}{\phi}$$

Kvanttorisäännöt

$$(I\forall): \quad \frac{\phi(x)}{(\forall x)\phi(x)} \qquad (I\exists): \quad \frac{\phi(t)}{(\exists x)\phi(x)}$$

$$(E\forall): \quad \frac{(\forall x)\phi(x)}{\phi(t)} \qquad (E\exists): \quad \frac{(\exists x)\phi(x) \qquad \begin{array}{c}\phi^{\checkmark}\\ \vdots \\ \psi\end{array}}{\psi}$$

Kvanttorisääntöjen rajoitukset: $(I\forall)$: x ei saa esiintyä vapaana missään (poistamattomassa) oletuksessa, josta $\phi(x)$ on johdettu. $(E\exists)$: x ei saa olla vapaa ψ:ssä tai johdon $\phi \ldots \psi$ muissa oletuksissa kuin ϕ:ssä. $(E\forall)$ ja $(I\exists)$: mikään vapaa muuttuja termissä t ei saa tulla sidotuksi, kun kaavaan $\phi(x)$ sijoitetaan x:n paikalle t (Tällöin sanotaan, että t on x-vapaa ϕ:n suhteen).

Kvanttorisääntöjen rajoitukset, esimerkkejä

- $(I\forall)$: $(x = c) \vdash (\forall x)(x = c)$. Väärin, koska x esiintyy vapaana poistamattomassa oletuksessa $x = c$.
- $(I\exists)$: $(\forall y)(-y + y = 0) \vdash (\exists x)(\forall y)(x + y = 0)$. Väärin, koska termissä $t = -y$ tulee y sidotuksi, jos kaavaan $(\forall y)(x + y = 0)$ sijoitetaan x:n paikalle $-y$.

Yhtäsuuruussäännöt

$$(YS1): \quad \frac{}{x = x} \qquad (YS2): \quad \frac{x = y}{y = x} \qquad (YS3): \quad \frac{x = y \quad y = z}{x = z}$$

$$(YS4): \quad \frac{x_1 = y_1 \quad x_2 = y_2 \quad \ldots \quad x_n = y_n}{f(x_1, x_2, \ldots, x_n) = f(y_1, y_2, \ldots, y_n)}$$

$$(YS5): \quad \frac{x_1 = y_1 \quad x_2 = y_2 \quad \ldots \quad x_n = y_n \quad R(x_1, x_2, \ldots, x_n)}{R(y_1, y_2, \ldots, y_n)}$$

Gentzenin järjestelmä

Huomattava:

Säännöillä voidaan johtaa vain premissien loogisia seurauksia

Esimerkki

$$(I\wedge): \quad \frac{\phi \quad \psi}{\phi \wedge \psi}$$

Jokainen joukon $\{\phi, \psi\}$ malli on myös $\phi \wedge \psi$:n malli, siis $\{\phi, \psi\} \models \phi \wedge \psi$

Esimerkki

$$(E\rightarrow): \quad \frac{\phi \quad \phi \rightarrow \psi}{\psi}$$

Jos ϕ ja $\phi \rightarrow \psi$ ovat molemmat tosia, on välttämättä myös ψ tosi, siis $\{\phi, \phi \rightarrow \psi\} \models \psi$

Gentzenin järjestelmä

Johtaminen

Jos Γ on joukko kaavoja, sanotaan, että kaava ϕ voidaan *johtaa* joukosta Γ luonnollisen deduktion järjestelmällä, mikäli ϕ voidaan saavuttaa Γ:n kaavoista tai vapaasti lisätyistä oletuksista deduktiosääntöjä käyttämällä siten että lopuksi kaikki Γ:n ulkopuoliset oletukset ovat poistettu. Tällöin merkitään $\Gamma \vdash \phi$.

Jos $\Gamma = \emptyset$, merkitään myös $\vdash \phi$.

Huomautus:

$\Gamma \models \phi$ määritellään semanttisesti, $\Gamma \vdash \phi$ syntaktisesti.

Esimerkkejä

- $\vdash \phi \to (\psi \to \phi)$
- $\vdash \phi \wedge \psi \to \psi \wedge \phi$
- $\{(\forall x)(I(x) \to K(x)), I(s)\} \vdash K(s)$
- $\vdash (\forall x)(\forall y)(\forall z)(x = y \to x + z = y + z)$
- Jos y ei esiinny kaavassa $\phi(x)$, $\vdash (\forall x)\phi(x) \leftrightarrow (\forall y)\phi(y)$
- Jos y ei esiinny kaavassa $\phi(x)$, $(\exists x)\phi(x) \vdash (\exists y)\phi(y)$

Predikaattilogiikan aakkosto

- Loogiset konnektiivit $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.
- Yhtäsuuruusmerkki $=$, sulkumerkit (ja) ja pilkku ,.
- Universaalikvanttori $\forall$ ja eksistentiaalikvanttori $\exists$.
- Muuttujasymbolit x_1, x_2, x_3, ...
- Nolla, yksi- tai useampipaikkaiset *predikaatti-* eli *relaatiosymbolit* R_1, R_2, R_3, ...
- Funktiosymbolit f_1, f_2, f_3, ... ja *vakiosymbolit* c_1, c_2, c_3, ...

Propositiologiikan aakkosto

- Loogiset konnektiivit $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.
- Yhtäsuuruusmerkki $=$, sulkumerkit (ja) ja pilkku ,.
- Universaalikvanttori $\forall$ ja eksistentiaalikvanttori $\exists$.
- Muuttujasymbolit x_1, x_2, x_3, ...
- Nolla, yksi- tai useampipaikkaiset *predikaatti-* eli *relaatiosymbolit* R_1, R_2, R_3, ...
- Funktiosymbolit f_1, f_2, f_3, ... ja *vakiosymbolit* c_1, c_2, c_3, ...

Propositiot

- 0-paikkaisia predikaattisymboleja kutsutaan *propositiomuuttujiksi* tai *atomaarisiksi propositioiksi*
- Syntaksi periytyy predikaattilogiikasta: Atomaarisista propositioista voidaan konnektiiveilla muodostaa molekulaarisia propositioita.
- Semantiikka periytyy predikaattilogiikasta: Kukin propositio on "tosi" tai "epätosi" riippuen tulkinnasta.
- Atomaaristen propositioiden tulkinta määrää muiden propositioiden tulkinnan
- Äärellinen määrä tulkintoja riittää!

Propositiologiikan semantiikkaa

Määritelmä

Olkoon HMK propositiologiikan hyvinmuodostettujen kaavojen joukko. Propositiologiikan *totuusarvotus* eli *arvotus* on funktio $\alpha : \text{HMK} \to \{0, 1\}$, joka voidaan määritellä rekursiivisesti seuraavalla tavalla:

- Propositiomuuttujille x_1, x_2, x_3, ... arvot $\alpha(x_i) \in \{0, 1\}$ kiinnitetään mielivaltaisella tavalla.
- Jos ϕ ja ψ ovat propositioita, niin $\alpha((\neg\phi)) = 1 - \alpha(\phi)$, $\alpha((\phi \wedge \psi)) = \min\{\alpha(\phi), \alpha(\psi)\}$, ja $\alpha((\phi \vee \psi))) = \max\{\alpha(\phi), \alpha(\psi)\}$.

Määritelmä

Olkoon ϕ jokin propositio ja α jokin arvotus. Jos $\alpha(\phi) = 0$, sanotaan, että ϕ on *epätosi* arvotuksessa α. Jos $\alpha(\phi) = 1$, sanotaan, että ϕ on *tosi* arvotuksessa α.

Propositiologiikan semantiikkaa

Väite

Totuusarvotus $\alpha : \text{HMK} \to \{0, 1\}$ tulee edellämainitulla tavalla yksikäsitteisesti määritellyksi joukossa HMK

Todistus induktiolla

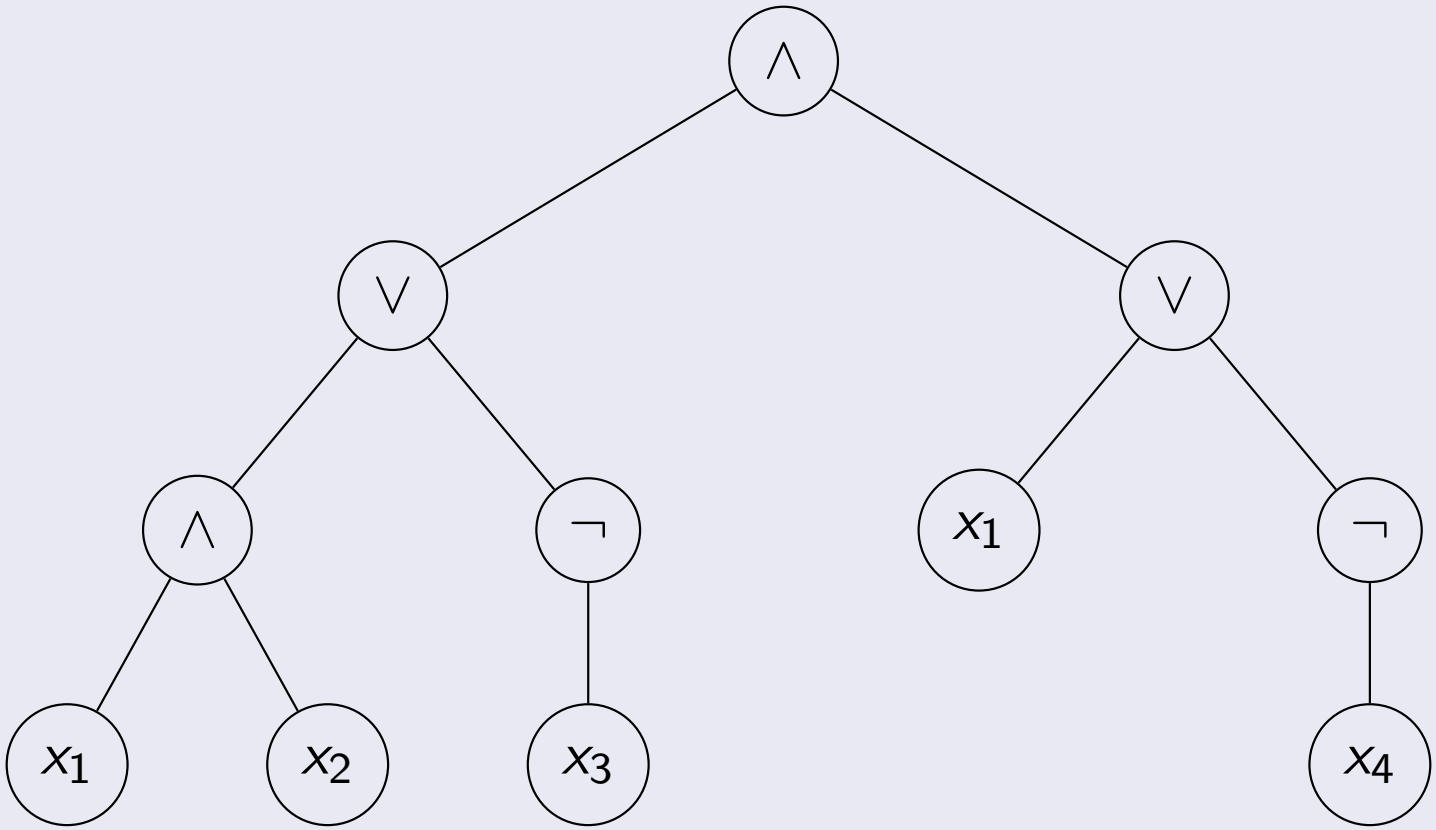
Induktion lähtökohta: Määritelmän mukaan α kiinnittää arvon jokaiselle propositiomuuttujalle x_i, joten induktion lähtökohta on tosi.

Induktioaskel

Induktio-oletus: Väittämä pitää paikkansa joillekin propositiolle ϕ ja ψ. Induktioväite: Väittämä pitää paikkansa myös propositiolle $(\neg\phi)$, $(\phi \wedge \psi)$, ja $(\phi \vee \psi)$.
Todistus: Suoraan arvotuksen α määritelmästä:
$\alpha((\neg\phi)) = 1 - \alpha(\phi)$, $\alpha((\phi \wedge \psi)) = \min\{\alpha(\phi), \alpha(\psi)\}$, ja
$\alpha((\phi \vee \psi)) = \max\{\alpha(\phi), \alpha(\psi)\}$

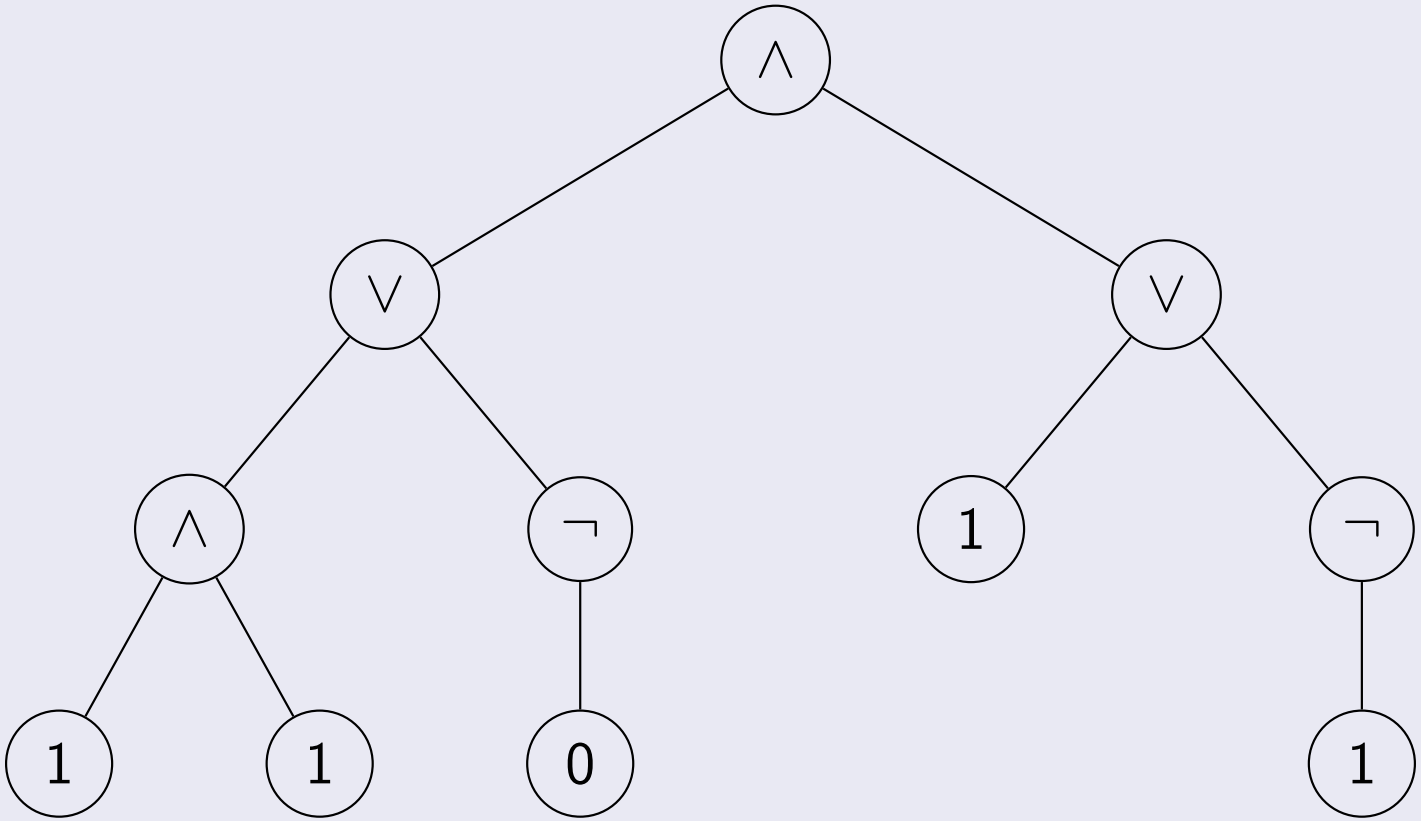
Esimerkki

$\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.



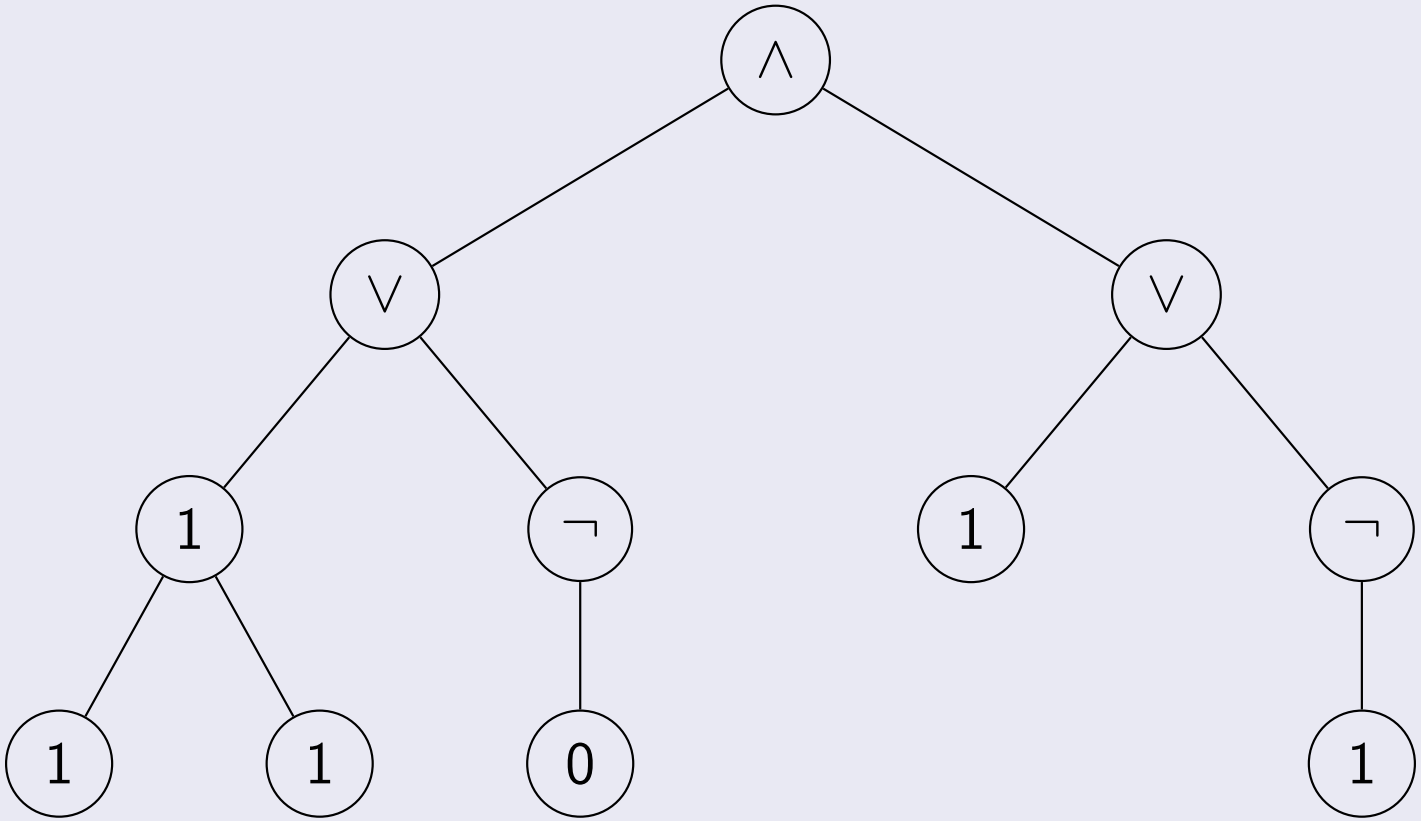
Esimerkki

$\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.



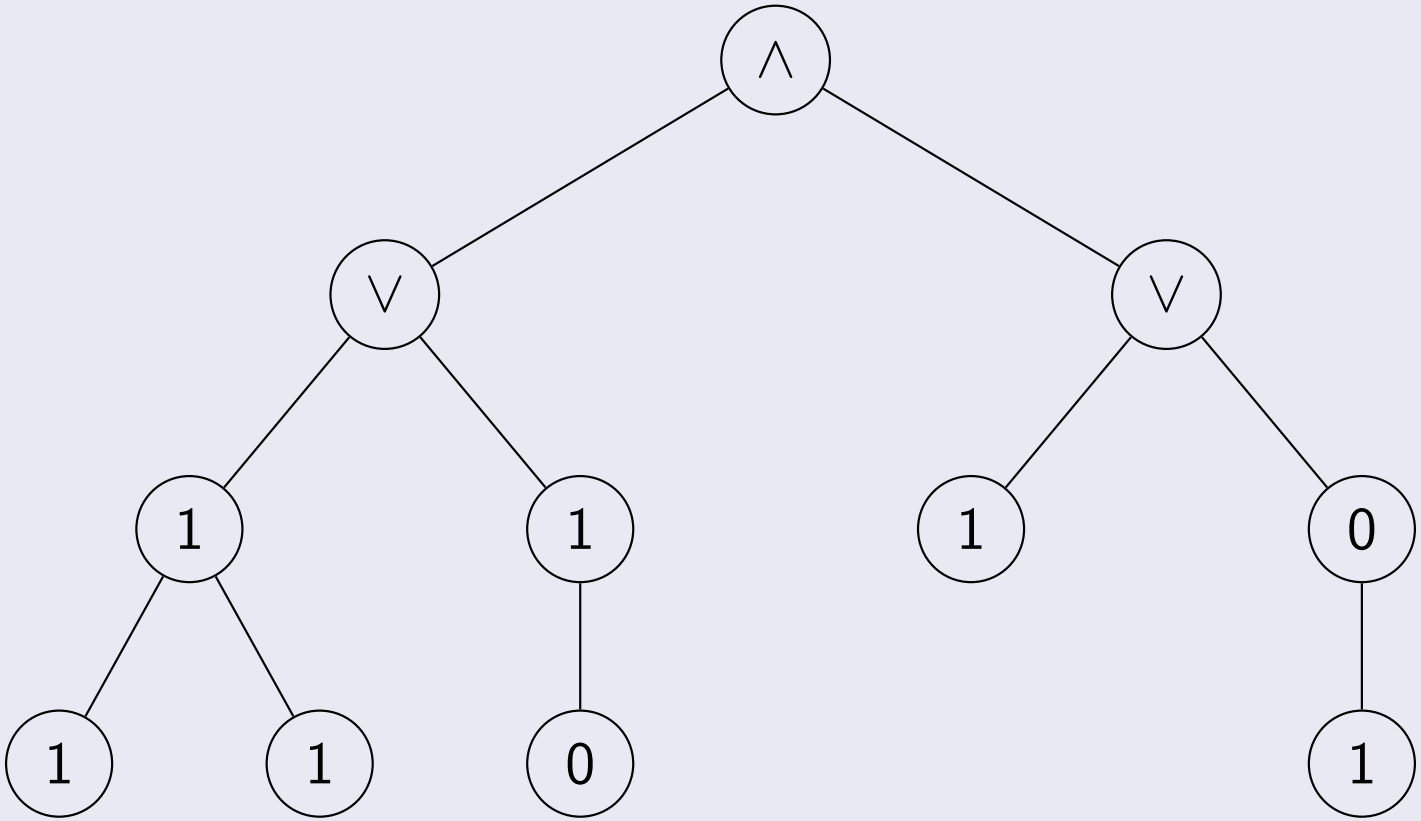
Esimerkki

$\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.



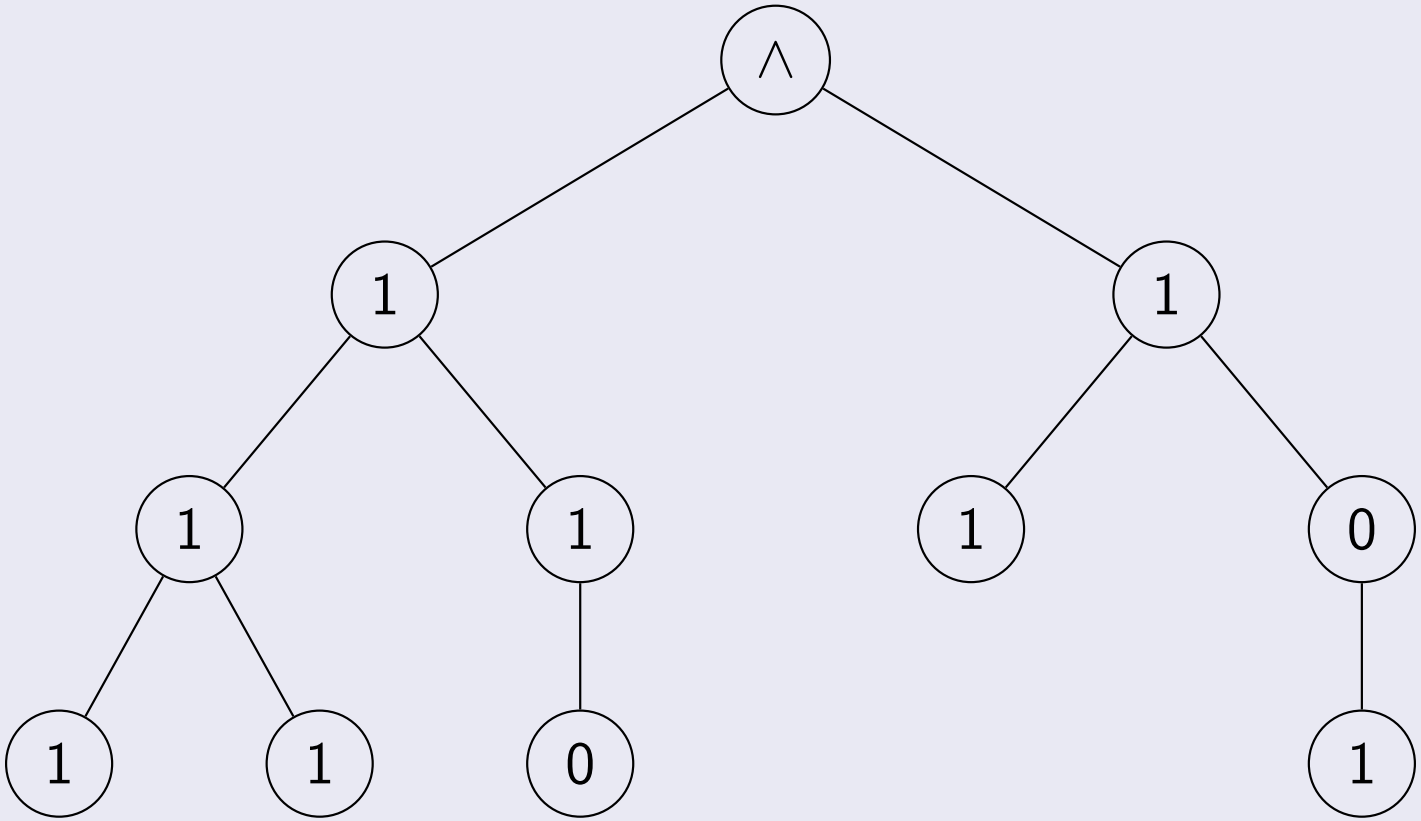
Esimerkki

$\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.



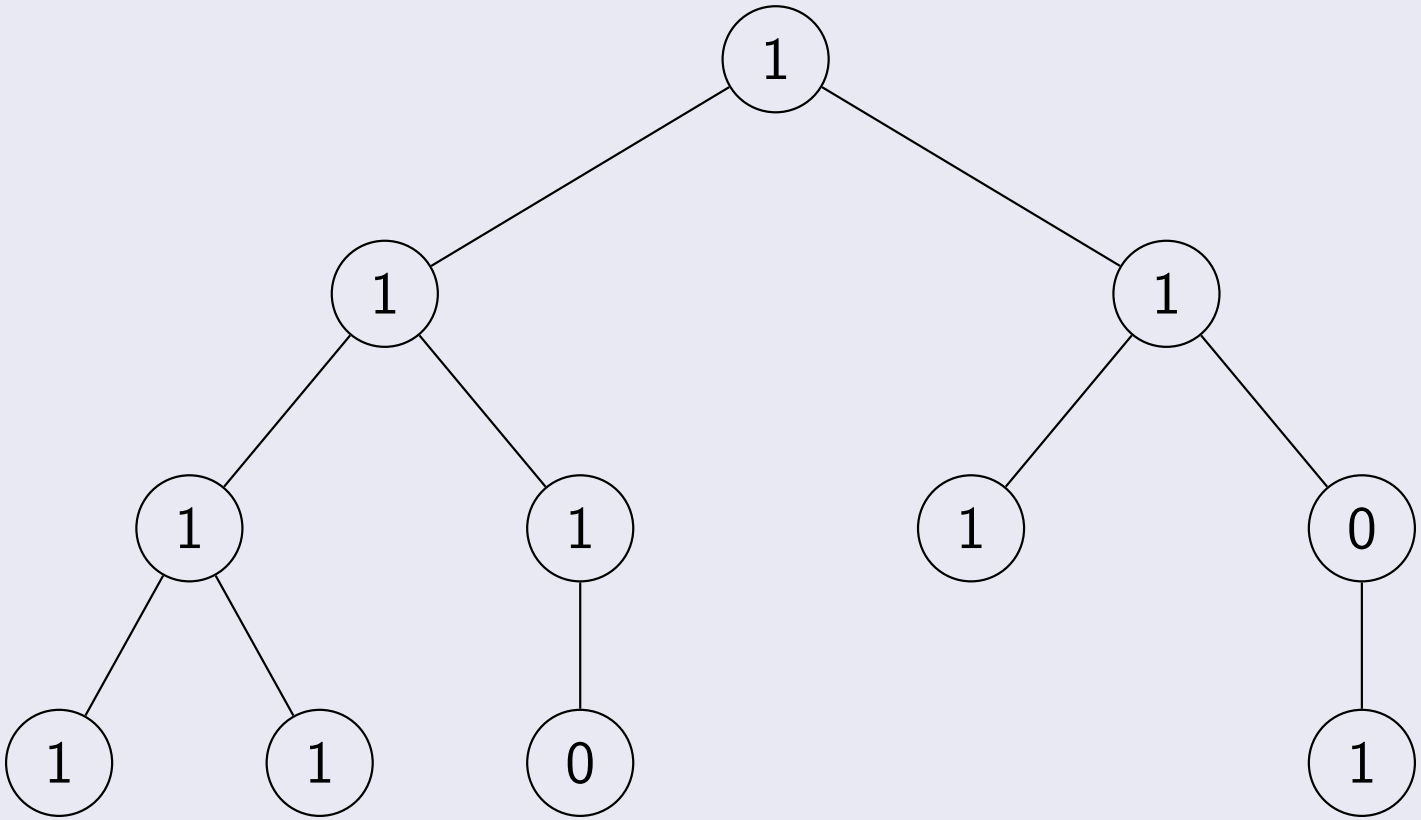
Esimerkki

$\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.



Esimerkki

$\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.



Propositiologiikan semantiikkaa

Määritelmä

Arvotus α on *pienempi tai yhtäsuuri kuin* arvotus β (merkitään $\alpha \preceq \beta$), jos $\alpha(x_i) \leq \beta(x_i)$ jokaiselle propositiomuuttujalle x_i.
Huomautus: $\alpha \preceq \beta$ on osittainen järjestys arvotusten joukossa.

Määritelmä

Propositio ϕ on *monotoninen*, jos ehdosta $\alpha \preceq \beta$ seuraa $\alpha(\phi) \leq \beta(\phi)$.

Lause

Jos propositio ϕ muodostetaan rekursiivisesti käyttämällä vain konnektiiveja $\wedge$ ja $\vee$, eikä lainkaan konnektiivia $\neg$, on ϕ monotoninen.

Todistus

Olkoot α ja β arvotuksia ja $\alpha \preceq \beta$.
Induktion lähtökohta: Jos $\phi = x_i$ (propositiomuuttuja), on määritelmän mukaan $\alpha(x_i) \leq \beta(x_i)$, joten $\phi = x_i$ on monotoninen.

Induktioaskel

Oletetaan, että väittämä pitää paikkansa propositiolle ϕ ja ψ ja näytetään toteen, että se pitää paikkansa myös propositiolle $(\phi \wedge \psi)$ ja $(\phi \vee \psi)$.
Todistus:

$$\alpha(\phi \wedge \psi) = \min\{\alpha(\phi), \alpha(\psi)\} \leq \min\{\beta(\phi), \beta(\psi)\} = \beta(\phi \wedge \psi).$$

Samoin

$$\alpha(\phi \vee \psi) = \max\{\alpha(\phi), \alpha(\psi)\} \leq \max\{\beta(\phi), \beta(\psi)\} = \beta(\phi \vee \psi).$$

Määritelmä

Taulukkoa, jossa esitetään kaikki mahdolliset tulkinnat äärelliselle määrälle propositiomuuttujia, kutsutaan *totuustaulukoksi*.

Esimerkki

Propositioiden $p \to q$ ja $\neg p \to \neg q$ kaikki mahdolliset tulkinnat:

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg p \to \neg q$
0	0	1	1	1	1
0	1	1	0	1	0
1	0	0	1	0	1
1	1	0	0	1	1

Loogisen seurauksen selvittäminen:

Rivit 1,2 ja 4 ovat $p \to q$:n malleja, mutta rivi 2 ei ole $\neg p \to \neg q$:n malli. Täten $\neg p \to \neg q$ ei ole looginen seuraus $p \to q$:sta.

Loogisen seurauksen selvittäminen

- Olkoot ϕ_1, ϕ_2, ..., ϕ_n propositiomuuttujat, jotka esiintyvät propositiojoukkojen Γ ja Δ propositioissa.
- Loogisen seurauksen $\Gamma \models \Delta$ selvittämiseksi on tarkistettava, onko jokainen Γ:n malli myös Δ:n malli.
- Tarkistettavien tulkintojen määrä on 2^n: ϕ_1:n tulkinta voidaan valita joko 0:ksi tai 1:ksi, samoin ϕ_2:n, jne.

Totuustaulukko

ϕ_1	ϕ_2	$\dots$	ϕ_{n-1}	ϕ_n	$\psi(\phi_1, \dots, \phi_n)$
0	0	$\dots$	0	0	$*$
0	0	$\dots$	0	1	$*$
0	0	$\dots$	1	0	$*$
0	0	$\dots$	1	1	$*$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
1	1	$\dots$	1	1	$*$

Totuustaulukon rakentaminen

0			0	0			0	0	0		0	0	0	0	
1	$\rightarrow$		0	1	$\rightarrow$		0	0	1	$\rightarrow$	0	0	0	1	
			1	0			0	1	0		0	0	1	0	
			1	1			0	1	1		0	0	1	1	
							1	0	0		0	1	0	0	
							1	0	1		0	1	0	1	
							1	1	0		0	1	1	0	
							1	1	1		0	1	1	1	
											1	0	0	0	
											1	0	0	1	
											1	0	1	0	
											1	0	1	1	
											1	1	0	0	
											1	1	0	1	
											1	1	1	0	
											1	1	1	1	

$\rightarrow$ jne.

Määritelmä

Taulukkoa, jossa esitetään kaikki mahdolliset tulkinnat äärelliselle määrälle propositiomuuttujia, kutsutaan *totuustaulukoksi*.

Esimerkki

Propositioiden $p \to q$ ja $\neg p \to \neg q$ kaikki mahdolliset tulkinnat:

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg p \to \neg q$
0	0	1	1	1	1
0	1	1	0	1	0
1	0	0	1	0	1
1	1	0	0	1	1

Loogisen seurauksen selvittäminen:

Rivit 1,2 ja 4 ovat $p \to q$:n malleja, mutta rivi 2 ei ole $\neg p \to \neg q$:n malli. Täten $\neg p \to \neg q$ ei ole looginen seuraus $p \to q$:sta.

Loogisen seurauksen selvittäminen

- Olkoot ϕ_1, ϕ_2, ..., ϕ_n propositiomuuttujat, jotka esiintyvät propositiojoukkojen Γ ja Δ propositioissa.
- Loogisen seurauksen $\Gamma \models \Delta$ selvittämiseksi on tarkistettava, onko jokainen Γ:n malli myös Δ:n malli.
- Tarkistettavien tulkintojen määrä on 2^n: ϕ_1:n tulkinta voidaan valita joko 0:ksi tai 1:ksi, samoin ϕ_2:n, jne.

Totuustaulukko

ϕ_1	ϕ_2	$\dots$	ϕ_{n-1}	ϕ_n	$\psi(\phi_1, \dots, \phi_n)$
0	0	$\dots$	0	0	$*$
0	0	$\dots$	0	1	$*$
0	0	$\dots$	1	0	$*$
0	0	$\dots$	1	1	$*$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
1	1	$\dots$	1	1	$*$

Totuustaulukon rakentaminen

$$
\begin{array}{c} 0 \\ 1 \end{array}
\rightarrow
\begin{array}{cc} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{array}
\rightarrow
\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{array}
\rightarrow
\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{array}
\rightarrow \text{jne.}
$$

Toteutuvuus

- Onko tulkintaa, jossa $\psi(\phi_1, \ldots, \phi_n)$ tosi?
- Voidaan selvittää käymällä läpi kaikki 2^n tulkintaa.
- Vaikeus: 2^n suuri jo pienillä n:n arvoilla.
- Onko olemassa oleellisesti tehokkaampaa (polynomiaikaista) menetelmää?
- Jos on, $\mathbf{P} = \mathbf{NP}$, muutoin $\mathbf{P} \neq \mathbf{NP}$
- $\mathbf{P} \neq \mathbf{NP}$ toistaiseksi selvittämätön ongelma.
- \$1000000 palkinto ongelman selvittämisestä! (Clay Mathematics Institute).

Huomautus

Propositiologiikan kaavat $x \wedge (y \wedge z)$ ja $(x \wedge y) \wedge z$ eivät ole yhtäsuuret. Kuitenkin $x \wedge (y \wedge z)$ saa totuusarvon 1 tarkalleen silloin kun jokainen propositiomuuttuja x, y ja z saa arvon 1, ja samoin on proposition $(x \wedge y) \wedge z$ laita.

Määritelmä

Lyhennysmerkintä $x \wedge y \wedge z$ tarkoittaa propositiota $(x \wedge y) \wedge z$ tai propositiota $x \wedge (y \wedge z)$. Lyhennysmerkintä $x \vee y \vee z$ niinikään tarkoittaa propositiota $(x \vee y) \vee z$ tai propositiota $x \vee (y \vee z)$.

Vertaa:

Summamerkinnät $(x + y) + z$ ja $x + (y + z)$ eivät merkkijonoina ole yhtäsuuret, mutta esim. reaalilukujen teoriassa näillä summilla on täsmälleen sama lukuarvo, olipa reaaliluvuilla x, y ja z mitkä reaaliarvot hyvänsä. Tällöin voidaan molemmista summista käyttää merkintää $x + y + z$ ilman sulkeita. Yleistys: $x_1 + x_2 + \ldots + x_n$.

Määritelmä

$x_1 \wedge x_2 \wedge \ldots \wedge x_n$ on propositiologiikan kaava, joka voidaan rekursiivisesti määritellä kaavana $x_1 \wedge (x_2 \wedge \ldots \wedge x_n)$ tai kaavana $(x_1 \wedge \ldots \wedge x_{n-1}) \wedge x_n$. Kaava $x_1 \vee x_2 \vee \ldots \vee x_n$ määritellään samoin.

Seuraus

Jos $\alpha : \{x_1, x_2, x_3, \ldots\} \to \{0, 1\}$ on jokin totuusarvotus, on $\alpha(x_1 \wedge x_2 \wedge \ldots \wedge x_n) = \min\{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_n)\}$ ja $\alpha(x_1 \vee x_2 \vee \ldots \vee x_n) = \max\{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_n)\}$

Esimerkki

Kaava $x \wedge \neg y \wedge z$ saa arvon 1 tarkalleen silloin, kun $(x, y, z) = (1, 0, 1)$ ja kaava $x \wedge y \wedge \neg z$ saa arvon 1 tarkalleen silloin $(x, y, z) = (1, 1, 0)$. Näin ollen kaava $(x \wedge \neg y \wedge z) \vee (x \wedge y \wedge \neg z)$ saa arvon 1 tarkalleen kun $(x, y, z) = (1, 0, 1)$ tai $(x, y, z) = (1, 1, 0)$.

Määritelmä

n-paikkainen *totuusfunktio* f on funktio $f : \{0,1\}^n \to \{0,1\}$.

Lause

Jokainen n-paikkainen totuusfunktio f voidaan esittää propositiologiikan kaavana, jossa esiintyvät propositiomuuttujat x_1, $\ldots$, x_n.

Todistuksen idea

Totuusfunktio $f : \{0,1\}^n \to \{0,1\}$ joka saa arvon 1 tarkalleen alkukuvissa $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N$ voidaan määritellä *disjunktiivisella* muodolla

$$f = \eta_1 \vee \eta_2 \vee \ldots \vee \eta_N,$$

missä η_i on *konjunktiivista* muotoa $\eta_i = y_1 \wedge y_2 \wedge \ldots \wedge y_n$, missä edelleen jokainen y_i on joko x_i tai $\neg x_i$.

Esimerkki

Olkoon $f : \{0,1\}^2 \to \{0,1\}$ totuusfunktio, jolle pätee $f(x_1, x_2) = 0$, jos $x_1 = x_2$ ja $f(x_1, x_2) = 1$, jos $x_1 \neq x_2$, siis $f(0,0) = f(1,1) = 0$ ja $f(1,0) = f(0,1) = 1$. Tämä funktio voidaan muodostaa osakaavoista $x_1 \wedge \neg x_2$ ja $\neg x_1 \wedge x_2$, joista ensimmäinen saa arvon 1, kun $(x_1, x_2) = (1,0)$ ja toinen arvon 1, kun $(x_1, x_2) = (0,1)$. Näin ollen haluttu funktio saadaan osakaavojen disjunktiona $(x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$.

Huomautus

Jokainen funktio $f : \{0,1\}^n \to \{0,1\}^m$ voidaan koostaa m:stä totuusfunktiosta $f_1, \ldots, f_m$: $\{0,1\}^m \to \{0,1\}$.