

Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
`mikhirve@utu.fi`

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2023

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.

Määritelmä

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

Väite

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

Induktion lähtökohta $n = 1$

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

Induktioaskel

Induktio-oletus: Väite pitää paikkansa luvulle n .

Induktioväite: Väite pitää paikkansa luvulle $n + 1$

Todistus:

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

Newtonin binomikaava

Väite:

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

Induktion lähtökohta $n = 1$

$$\begin{aligned}(x + y)^1 &= \sum_{i=0}^1 \binom{1}{i} x^{1-i} y^i \Leftrightarrow x + y = \binom{1}{0} x^1 y^0 + \binom{1}{1} x^0 y^1 \\ &\Leftrightarrow x + y = x + y, \quad \text{tosi}\end{aligned}$$

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)

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

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:

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

Määritelmä

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

- Propositiomuuttujille $x_1, x_2, x_3, \dots$ arvot $\alpha(x_i) \in \{0, 1\}$ kiinnitetään mielivaltaisella tavalla.
- Jos ϕ ja ψ ovat propositiesiioita, 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 propositiesiio 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 .

Väite

Totuusarvotus $\alpha : \text{HMK} \rightarrow \{0, 1\}$ 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

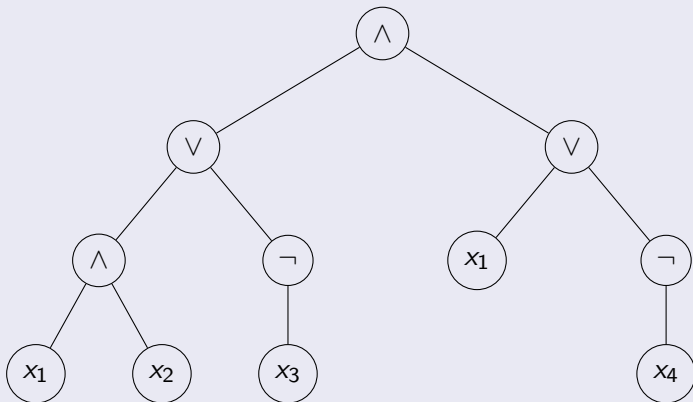
Induktio-oletus: Väittämä pitää paikkansa joillekin propositiolle ϕ ja ψ . Induktioväite: Väittämä pitää paikkansa myös propositiolle $(\neg\phi)$, $(\phi \wedge \psi)$, ja $(\phi \vee \psi)$.

Todistus: Suoraan arvotuksen α määritelmästä:

$$\alpha((\neg\phi)) = 1 - \alpha(\phi), \quad \alpha((\phi \wedge \psi)) = \min\{\alpha(\phi), \alpha(\psi)\}, \quad \text{ja} \\ \alpha((\phi \vee \psi)) = \max\{\alpha(\phi), \alpha(\psi)\}$$

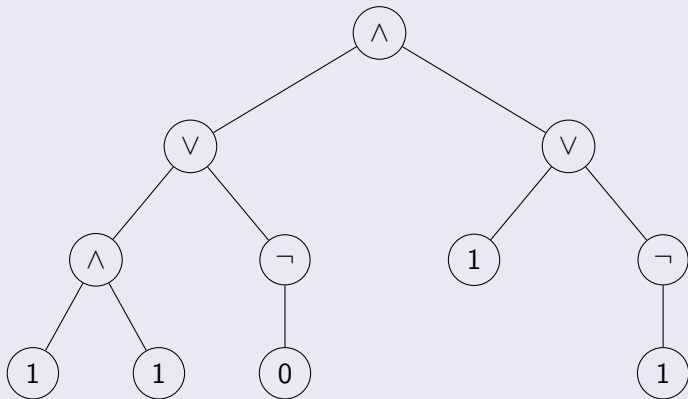
Esimerkki

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



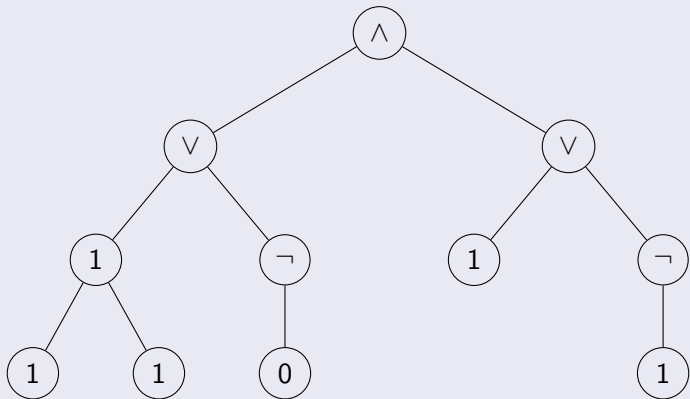
Esimerkki

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



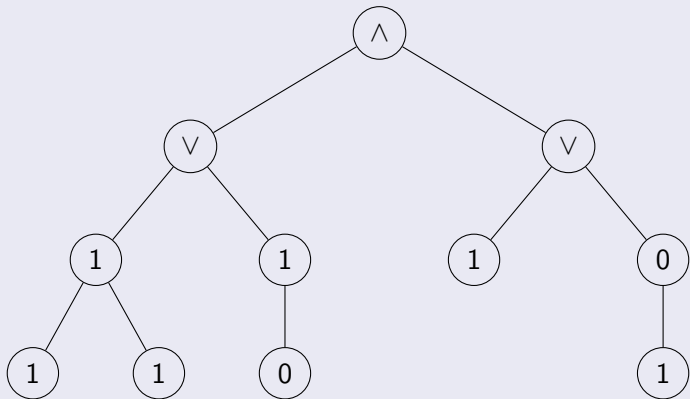
Esimerkki

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



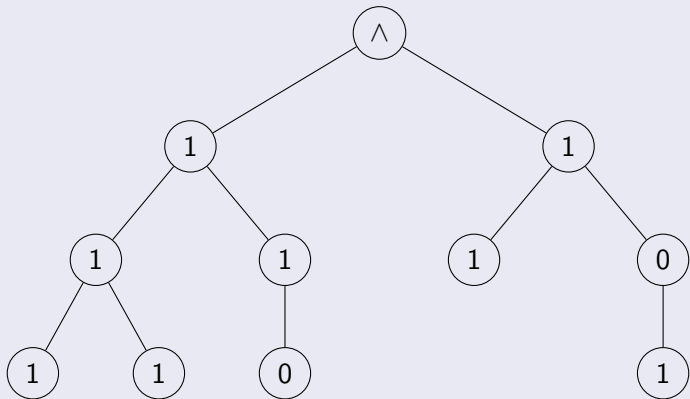
Esimerkki

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



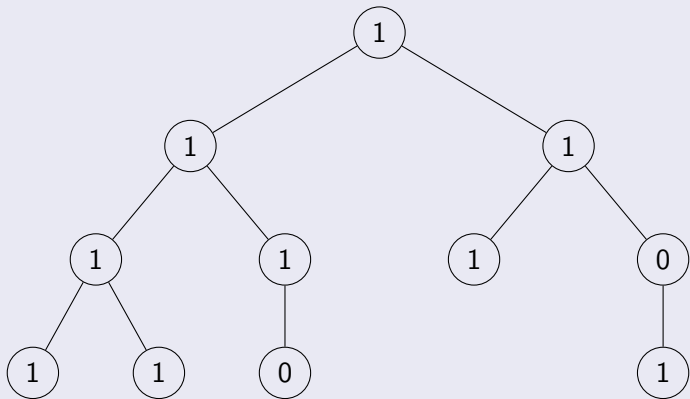
Esimerkki

$\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ 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 $\alpha(x_4) = 1$.



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

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

Totuustaulukko

x_1	x_2	$\dots$	x_{n-1}	x_n	$\phi(x_1, \dots, x_n)$
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	*

Propositiologiikan semantiikkaa

Totuustaulukon rakentaminen

									0	0	0	0	
									0	0	0	1	
									0	0	1	0	
									0	0	1	1	
				0	0	0			0	1	0	0	
				0	0	1			0	1	0	1	
				0	1	0			0	1	1	0	
				0	1	1			0	1	1	1	
0	→	0	0	→	0	1	0	→	0	1	1	1	→ jne.
1		1	0		1	0	0		1	0	0	0	
		1	1		1	0	1		1	0	0	1	
					1	1	0		1	0	1	0	
					1	1	1		1	0	1	1	
									1	1	0	0	
									1	1	0	1	
									1	1	1	0	
									1	1	1	1	

Toteutuvuus

- Onko arvotusta, jossa $\phi(x_1, \dots, x_n)$ tosi?
- Voidaan selvittää käymällä läpi kaikki 2^n arvotusta
- Vaikeus: 2^n suuri jo pienillä n :n arvoilla.
- Onko olemassa oleellisesti tehokkaampaa (polynomiaikaista) menetelmää?
- Jos on, **P = NP**, muutoin **P $\neq$ NP**
- **P $\neq$ 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 proposition $(x \wedge y) \wedge z$ tai proposition $x \wedge (y \wedge z)$. Lyhennysmerkintä $x \vee y \vee z$ niinikään tarkoittaa proposition $(x \vee y) \vee z$ tai proposition $x \vee (y \vee z)$.

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: $x_1 + x_2 + \dots + x_n$.

Määritelmä

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

Seuraus

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

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 $f : \{0, 1\}^n \rightarrow \{0, 1\}$.

Lause

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

Todistuksen idea

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

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

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

Esimerkki

Olkoon $f : \{0, 1\}^2 \rightarrow \{0, 1\}$ 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 $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ voidaan koostaa m :stä totuusfunktioista $f_1, \dots, f_m : \{0, 1\}^n \rightarrow \{0, 1\}$.

Sovelluksia

- Jännite mahdollista mieltää 0 / 1 –suureena (0 V vs. 5 V).
- Virtapiireissä mahdollista rakentaa $\neg$, $\wedge$, ja $\vee$ -rakenteita.
- Puolijohdetekniikka mahdollistaa rakenteiden toteuttamiseen pienessä tilassa.
- Nykyaikaisten klassisen informaation tietokoneiden toiminta on kuvattavissa totuusfunktioiden avulla.

Esimerkki

Summa $x_1 + x_2$ modulo 2.