

Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
`mikhirve@utu.fi`

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2023

Määritelmä

Boolean algebra on joukko B jossa on määritelty kaksi binääristä operaatiota $\wedge$ (konjunktio) ja $\vee$ (disjunktio), yksi unaarinen operaatio $\neg$ (negaatio) ja kaksi nollapaikkaista operaatiota (eli vakiota) $\top$ (verum) ja $\perp$ (falsum) jotka toteuttavat seuraavat aksioomat:

- $a \vee (b \vee c) = (a \vee b) \vee c$ ja $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (assosiatiivisuus).
- $a \vee b = b \vee a$ ja $a \wedge b = b \wedge a$ (kommutatiivisuus)
- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ ja $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ (distributiivisuus)
- $a \vee \perp = a$, $a \wedge \top = a$ (neutraalialkiot)
- $a \vee \neg a = \top$ ja $a \wedge \neg a = \perp$ (vasta-alkiot)

Huomautus

On myös tapana merkitä 1 verumin $\top$ ja 0 falsumin $\perp$ sijasta.

Huomautus

Boolean algebrassa ovat kummankin operaation $\wedge$ ja $\vee$ suhteen analogiset distributiivisäännöt voimassa, siis

- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ ja
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Näin ei ole esimerkiksi kokonaislukujen renkaassa, jossa kertolasku on distributiivinen yhteenlaskun yli: $a \cdot (b + c) = a \cdot b + a \cdot c$, mutta päinvastoin $a + (b \cdot c) = (a + b) \cdot (a + c)$ ei yleensä pidä paikkansa.

Boolean algebra

Lause

Boolean algebrassa pätee $a \vee a = a$ ja $a \wedge a = a$.

Lause

Boolean algebrassa pätee $a \vee \top = \top$ ja $a \wedge \perp = \perp$.

Lause

Boolean algebrassa pätee $a \wedge (a \vee b) = a$ ja $a \vee (a \wedge b) = a$
(absorptio)

Lause

Boolean algebrassa pätee $\neg(a \wedge b) = \neg a \vee \neg b$ ja
 $\neg(a \vee b) = \neg a \wedge \neg b$ (De Morganin säännöt)

Esimerkki

Joukkojen Boolean algebra

Rekursio

Rekursio tarkoittaa järjestettyjen matemaattisten objektien määrittelemistä pienempien objektien avulla. Kaikkein pienimmät, ns. rekursion pohja, pitää määritellä muutoin, esim. luettelemalla.

Esimerkki

Kertomafunktio $n!$ voidaan määritellä $0! = 1$ ja $(n + 1)! = (n + 1) \cdot n!$.

Seuraus

$$n! = n(n - 1)(n - 2) \cdot \dots \cdot 1 = \prod_{i=1}^n i.$$

(Ei rekursiivinen määritelmä)

Fibonaccin luvut



Fibonaccin luvut

$$F_0 = 0, F_1 = 1,$$

$$F_{n+2} = F_{n+1} + F_n$$

aina, kun $n \geq 0$. Täten

$$F_2 = F_1 + F_0 = 1 + 0 = 1$$

$$F_3 = F_2 + F_1 = 1 + 1 = 2$$

$$F_4 = F_3 + F_2 = 2 + 1 = 3$$

$$F_5 = F_4 + F_3 = 3 + 2 = 5$$

$$F_6 = F_5 + F_4 = 5 + 3 = 8$$

$$F_7 = F_6 + F_5 = 5 + 8 = 13$$

$$F_8 = F_7 + F_6 = 13 + 8 = 21$$

$$F_9 = F_8 + F_7 = 21 + 13 = 34$$

$$F_{10} = F_9 + F_8 = 34 + 21 = 55$$

$$F_{11} = F_{10} + F_9 = 55 + 34 = 89$$

....

Joukko $\mathbb{N}$

- Rekursion pohja 1
- Seuraajafunktio s
- $1 \rightarrow s(1) \rightarrow s(s(1)) \rightarrow s(s(s(1))) \rightarrow s(s(s(s(1)))) , \dots$
- $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow \dots$
- $s(n) = n + 1$ (seuraajafunktio)

Määritelmä

Joukossa X määritelty osittainen järjestys $\preceq$ on *hyvinjärjestys* jos

- Kaikille $a, b \in X$ pätee joko $a \preceq b$ tai $b \preceq a$ (kaikki alkiot ovat vertailukelpoisia, ns. lineaarinen järjestys).
- Jokaisessa epätyhjässä osajoukossa $Y \subseteq X$ on pienin alkio järjestyksen $\preceq$ suhteen.

Esimerkki

Joukko $\mathbb{N}$ on hyvinjärjestetty tavallisen järjestysrelaation $\leq$ suhteen.

Määritelmä

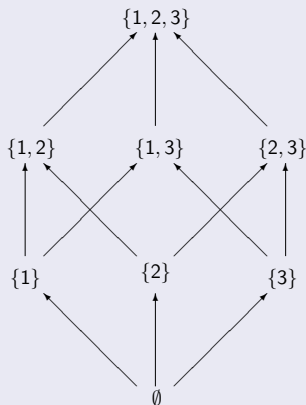
Puu (tree) on pari $(X, \preceq)$ missä X on joukko (verteksit eli solmut eli pisteet) ja $\preceq$ on joukossa X määritelty osittainen järjestys, joka toteuttaa seuraavat ehdot:

- Kaikille $x \in X$ joukko $\{y \in X \mid y \preceq x\}$ on hyvinjärjestetty (alkoista x alaspäin kulkeva polku ei haaraudu).
- Kaikilla hyvinjärjestetyillä joukoilla $\{y \in X \mid y \preceq x\}$ on sama minimaalinen alkio (kaikki alaspäin johtavat polut päättyvät samaan alkioon).

Määritelmä

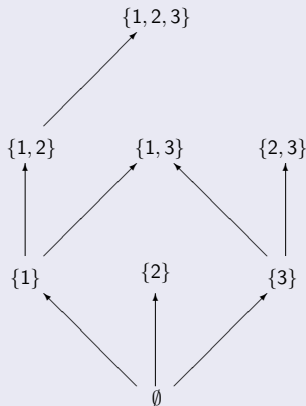
Puuhun kuuluvia relaationuolia $x \rightarrow y \Leftrightarrow x \preceq y$ kutsutaan myös *kaariksi* tai *viivoiksi*.

Esimerkki



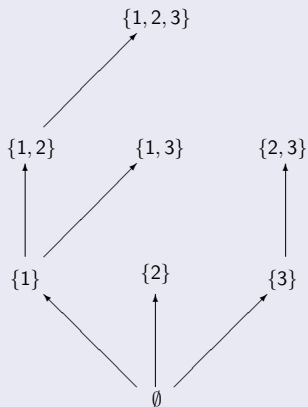
Ei ole puu, koska esim. alkiota $\{1, 2, 3\}$ pienemmät alkiot $\{1, 2\}$ ja $\{1, 3\}$ ovat vertailukelvottomia.

Esimerkki



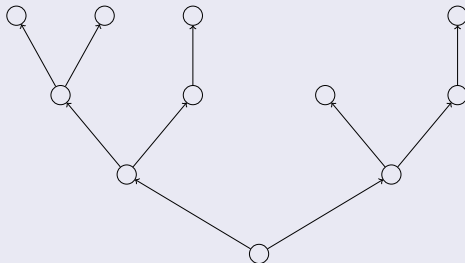
Ei ole puu, koska alkioita $\{1, 3\}$ pienemmät alkioita $\{1\}$ ja $\{3\}$ ovat vertailukelvottomia.

Esimerkki



On puu. Maksimaalisia alkioita $\{1, 2, 3\}$, $\{1, 3\}$, $\{2, 3\}$ ja $\{2\}$ kutsutaan *lehdiksi* ja minimaalista alkioita $\emptyset$ *juureksi*.

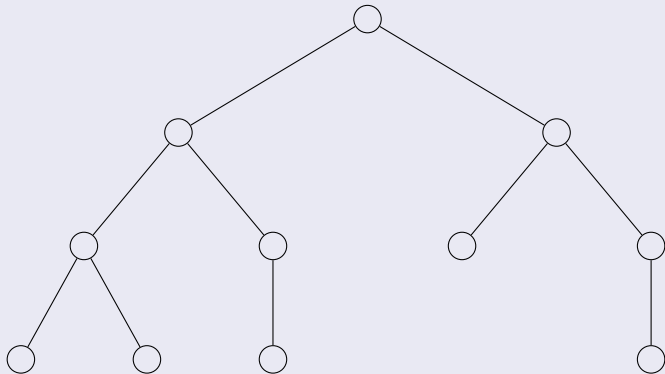
Esimerkki



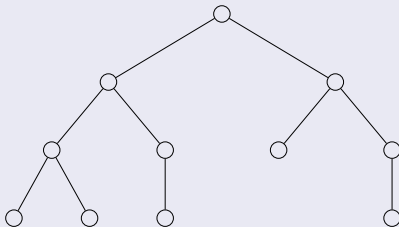
Rekursiivinen määritelmä (äärelliset puut)

- Lehdet ℓ ovat yhden alkion puita joiden juuri on ℓ .
- Jos $T_1, \dots, T_n$ ovat puita, joiden juurille $r_1, \dots, r_n$ pätee $r \rightarrow r_i$, on $T_1 \cup \dots \cup T_n \cup \{r\}$ puu, jossa r on juuri.

Yleinen esitystapa: Juuri ylhäällä, lehdet alhaalla



Puurakenteen käyttötarkoituksia



- Muistin hakemistohierarkiat
- Kirjaston luokitukset
- Evoluution kuvaaminen
- Sukupuu

Määritelmä

Propositiologiikan aakkosto koostuu

- Numeroituvasti äärettömästä joukosta *propositiomuuttujia* (atomaariset propositiot) $x_1, x_2, x_3, \dots$
- *Loogisista konnektiiveista* $\wedge, \vee, \neg$
- Sulkumerkeistä (ja).

Esimerkki

Aakkoston merkkijono:

$$x_1) \neg x_3) \wedge x_2 x_5 \wedge \wedge (x_3 \neg$$

Määritelmä

Propositiologiikan (hyvinmuodostetut) kaavat eli propositiot määritellään seuraavasti

- Propositionmuuttujat $x_1, x_2, x_3, \dots$ ovat kaavoja.
- Jos φ ja ψ ovat kaavoja, niin myös $(\neg\varphi)$, $(\varphi \wedge \psi)$ ja $(\varphi \vee \psi)$ ovat kaavoja.
- Ylläolevat ehdot määrittelevät kaikki propositiologiikan kaavat.

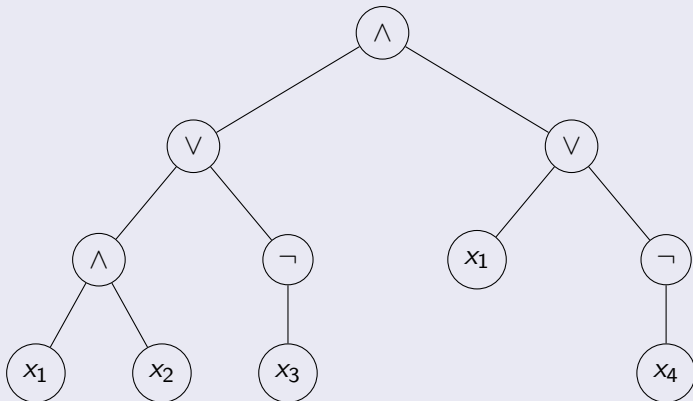
Lyhennysmerkitöjä

- $x_1, x_2, x_3 \rightarrow x, y, z$
- $((\neg x) \wedge y) \rightarrow \neg x \wedge y$
- $(x \vee (\neg y)) \rightarrow x \vee \neg y$
- Sanotaan, että $\neg$ *sitoo vahvemmin* kuin $\wedge$ tai $\vee$
- Merkintä $\neg x \wedge y$ tarkoittaa kaavaa $((\neg x) \wedge y)$, ei kaavaa $(\neg(x \wedge y))$
- Vrt. $a \cdot b + c$ tarkoittaa kaavaa $(a \cdot b) + c$, ei kaavaa $a \cdot (b + c)$.

$$\begin{aligned} & (((x_1 \wedge x_2) \vee (\neg x_3)) \wedge (x_1 \vee (\neg x_4))) \\ \rightarrow & ((x_1 \wedge x_2) \vee (\neg x_3)) \wedge (x_1 \vee (\neg x_4)) \\ \rightarrow & ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4) \end{aligned}$$

Rekursiivinen rakenne

Esim. $((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$





Määritelmä

Matemaattinen induktio on menetelmä, jolla rekursiivista rakennetta koskeva väittämä voidaan todistaa oikeaksi äärettömälle määrälle erikoistapauksia.

- Perustuu kahteen askeleeseen:
- 1) Väittämän todistaminen rekursion pohjimmaisille alkioille (induktion lähtökohta).
- 2) Väittämän totuusarvon siirtäminen rekursiossa ylöspäin (induktioaskel).
- Nimestään huolimatta matemaattinen induktio ei ole induktiivista vaan deduktiivista päättelyä.
- Sekoitetaan usein *täydelliseen induktioon*, joka kuitenkin on tieteenfilosofian kannalta eri asia.

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)

Bernoullin epäyhtälö

Olkoon $x \geq -1$. Tällöin $(1 + x)^n \geq 1 + nx$ aina, kun $n \in \mathbb{N}$.

Todistus induktiolla

Olkoon $P(n)$ väite, jonka mukaan $(1 + x)^n \geq 1 + nx$.

1) Induktion lähtökohta $P(1)$:

$$(1 + x)^1 \geq 1 + 1 \cdot x \Leftrightarrow 1 + x \geq 1 + x, \text{ tosi.}$$

2) Induktioaskel $(\forall n)(P(n) \rightarrow P(n + 1))$

Osoitetaan oikeaksi todistamalla implikaatio $P(n) \rightarrow P(n + 1)$ olettamatta luvusta n mitään.

Implikaatio $P(n) \rightarrow P(n + 1)$ osoitetaan oikeaksi olettamalla $P(n)$ todeksi ja johtamalla tästä $P(n + 1)$.

Induktioaskel

Oletetaan, että jollekin luvulle n $P(n)$ on tosi, siis
 $(1+x)^n \geq 1+nx$ (Induktio-oletus).

Tällöin

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x) \geq (1+nx)(1+x) \\ &= 1+x+nx+nx^2 \geq 1+(n+1)x,\end{aligned}$$

siis $(1+x)^{n+1} \geq 1+(n+1)x$. Näin ollen $P(n+1)$ on tosi.
Tämä osoittaa implikaation $P(n) \rightarrow P(n+1)$ todeksi, ja koska luvusta n ei oletettu muuta kuin $n \in \mathbb{N}$, on myös
 $(\forall n)(P(n) \rightarrow P(n+1))$ tosi.