

Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2026

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 –suurena (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.

Esimerkki

Propositiot $x \wedge \neg y$ ja $\neg(\neg x \vee y)$ eivät ole yhtäsuuret, mutta saavat samat totuusarvot kaikissa mahdollisissa totuusarvotuksissa

x	y	$x \wedge \neg y$	$\neg(\neg x \vee y)$
0	0	0	0
0	1	0	0
1	0	1	1
1	1	0	0

Määritelmä

Propositiot ϕ ja ψ ovat *ekvivalentit*, mikäli $\alpha(\phi) = \alpha(\psi)$ kaikille totuusarvotuksille α . Tällöin merkitään $\phi \equiv \psi$. On suoraviivaista nähdä, että \equiv on ekvivalenssirelaatio.

Lause

Edellämainittu \equiv on paitsi ekvivalenssi(relaatio), myös kongruenssi operaatioiden \neg , \wedge ja \vee suhteen.

Huomautus

Ylläolevan lauseen kongruenssiominaisuus merkitsee sitä, että jos $\phi_1 \equiv \phi_2$ ja $\psi_1 \equiv \psi_2$, niin $\neg\phi_1 \equiv \neg\phi_2$ ja $\phi_1 \wedge \psi_1 \equiv \phi_2 \wedge \psi_2$ ja $\phi_1 \vee \psi_1 \equiv \phi_2 \vee \psi_2$

Määritelmä

Boolean algebra on joukko B jossa on määritelty kaksi binääristä operaatiota \wedge ja \vee , yksi unaarinen operaatio \neg ja kaksi nollapaikkaista operaatiota (eli vakiota) \perp ja \top 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)

Lause

Boolean algebrassa pätee $\neg\neg a = a$.

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)

Lause

Propositiologiikan ekvivalenssiluokat toteutuvuusekvivalenssin suhteen muodostavat Boolean algebran, kun negaatioksi, disjunktiksi, ja konjunktiksi valitaan ekvivalenssiluokille määriteltävät operaatiot \neg , \vee ja \wedge .

Esimerkki

$$\begin{aligned} & (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) \\ \equiv & (x_1 \vee (\neg x_1 \wedge x_2)) \wedge (\neg x_2 \vee (\neg x_1 \wedge x_2)) \\ \equiv & ((x_1 \vee \neg x_1) \wedge (x_1 \vee x_2)) \wedge ((\neg x_2 \vee \neg x_1) \wedge (\neg x_2 \vee x_2)) \\ \equiv & (\top \wedge (x_1 \vee x_2)) \wedge (\neg x_1 \vee \neg x_2) \wedge \top \\ \equiv & (x_1 \vee x_2) \wedge \neg(x_1 \wedge x_2) \end{aligned}$$

Esimerkki

Määritellään kaksipaikkainen konnektiivi $x \rightarrow y$ siten, että $\alpha(x \rightarrow y) = 0$ ainoastaan jos $\alpha(x) = 1$ ja $\alpha(y) = 0$.

Esimerkki

Hornin propositiot

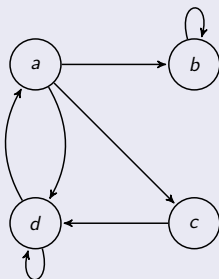
Määritelmä

Graafi on pari (V, E) , jossa V on *pisteiden* (*vertices, nodes*) ja $E \subseteq V \times V$ *nuolien* eli *viivojen* (*edges*) joukko.

Esimerkki

$V = \{a, b, c, d\}$ ja

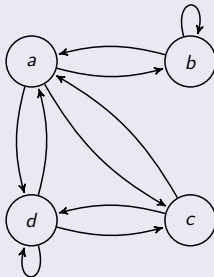
$E = \{(a, b), (a, c), (a, d), (b, b), (c, d), (d, a), (d, d)\}$



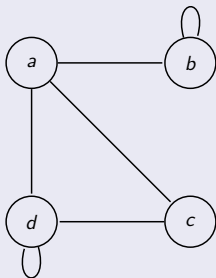
Määritelmä

Graafi on symmetrinen eli suuntaamaton, jos $(u, v) \in E \implies (v, u) \in E$

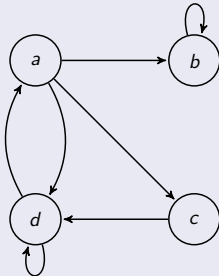
Esimerkki



Esimerkki



Vierusmatriisi

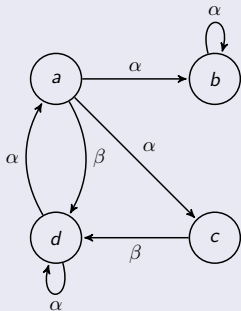


$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

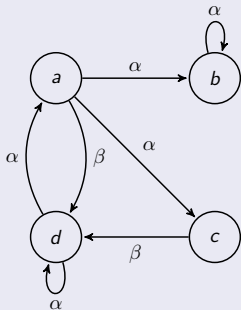
Määritelmä

Funktio $l : E \rightarrow L$ leimaa graafin. Tällöin graafia sanotaan *leimatuksi*

Esimerkki

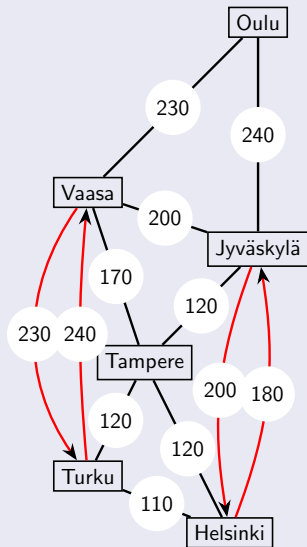


Leimatun graafin vierusmatriisi



$$M = \begin{pmatrix} 0 & \alpha & \alpha & \beta \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & \beta \\ \alpha & 0 & 0 & \alpha \end{pmatrix}$$

Esimerkki



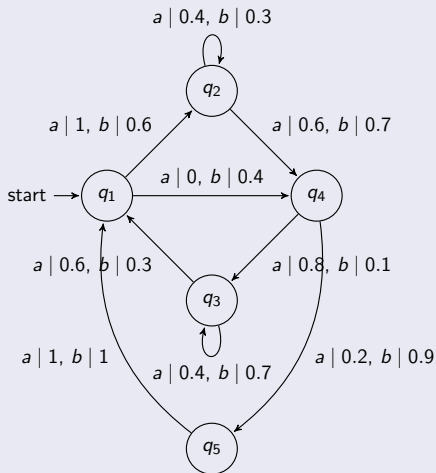
Määritelmä

Äärellinen (probabilistinen) automaatti koostuu äärellistä tilajoukosta S , äärellisestä syöttöaakkostosta Σ , ja *transitiofunktiosta* δ , joka liittää jokaiseen tilapariin (q_1, q_2) ja syöttöaakkoston kirjaimen todennäköisyyden $\delta(q_1, a, q_2) \in [0, 1]$, jolla automaatti siirtyy tilasta q_1 tilaan q_2 kun syötteenä luetaan kirjain a .

Äärellinen automaatti edustaa yksinkertaista laskentalaitetta, joka joko hyväksyy tai hylkää syötejonon.

Automaatille kiinnitetään *alkujakauma* sekä *hyväksyvät lopputilat*.
Automaatti esitetään yleensä leimattuna graafina.

Esimerkki



Vierusmatriisit

$$M_a = \begin{pmatrix} 0 & 0 & 0.6 & 0 & 1 \\ 1 & 0.4 & 0 & 0 & 0 \\ 0 & 0 & 0.4 & 0.8 & 0 \\ 0 & 0.6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.2 & 0 \end{pmatrix}, M_b = \begin{pmatrix} 0 & 0 & 0.3 & 0 & 1 \\ 0.6 & 0.3 & 0 & 0 & 0 \\ 0 & 0 & 0.7 & 0.1 & 0 \\ 0.4 & 0.7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.9 & 0 \end{pmatrix},$$

Aloitusedistributio

$\mathbf{v}_0 = (1, 0, 0, 0, 0)^T$. Kun luetaan symboli a , päädytään jakaumaan $M_a \mathbf{v}_0 = (0, 1, 0, 0, 0)^T$. Jos alussa luettaisiin symboli b , päädytään jakaumaan $M_b \mathbf{v}_0 = (0, 0.6, 0, 0.4, 0)^T$. Kun taas luetaan jono ba , päädytään jakaumaan $M_a M_b \mathbf{v}_0 = (0, 0.24, 0.32, 0.36, 0.08)^T$. Jonon aba lukeminen tuottaa jakauman $M_a M_b M_a \mathbf{v}_0 = (0, 0.12, 0.56, 0.18, 0.14)$

Matriisiesitys

n -tilainen (stokastinen automaatti) on joukko $\{M_a \mid a \in \Sigma\}$ stokastisia matriiseja (=jokainen sarake on todennäköisyysjakauma), varustettuna aloitusdistribuutiolla sekä lopputilojen määrittelyllä. Jos \mathbf{v}_0 aloitusdistribuutio ja \mathbf{p} $\{0, 1\}$ -arvoinen vektori joka määrittää lopputilat, saadaan syötesanan $w = a_1 a_2 \dots a_n$ hyväksymistodennäköisyys muodossa

$$\mathbb{P}(w) = \mathbf{p}^T M_{a_n} \dots M_{a_2} M_{a_1} \mathbf{v}_0.$$

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
- $1 \rightarrow s(1) \rightarrow s(s(1)) \rightarrow s(s(s(1))) \rightarrow s(s(s(s(1))))$, ...
- $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow \dots$
- $s(n) = n + 1$ (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 alkioit ovat vertailukelpoisia, ns. lineaarinen järjestys).
- Jokaisessa epätyhjässä osajoukossa $Y \subseteq X$ on pienin alkio järjestyksen \preceq suhteen.

Esimerkki

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

Määritelmä

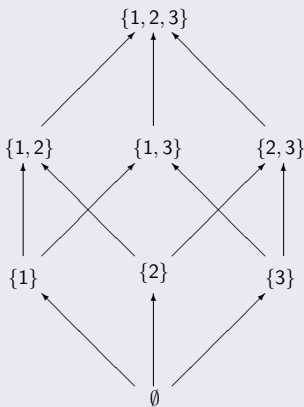
Puu (tree) on pari (X, \preceq) missä X on joukko (verteksit eli solmut eli pisteet) ja \preceq on joukossa X määritelty osittainen järjestys, joka toteuttaa seuraavat ehdot:

- Kaikille $x \in X$ joukko $\{y \in X \mid y \preceq x\}$ on hyvinjärjestetty (alkiosta 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

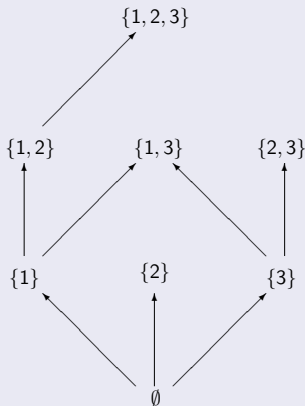
Puuhun kuuluvia relationuolia $x \rightarrow y \Leftrightarrow x \preceq y$ kutsutaan myös *kaariksi* tai *viivoiksi*.

Esimerkki



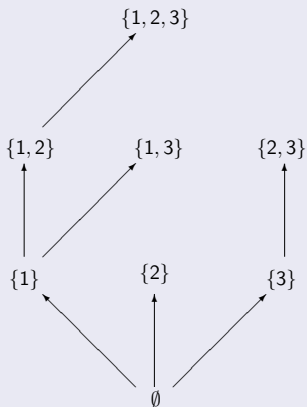
Ei ole puu, koska esim. alkioita $\{1, 2, 3\}$ pienemmät alkioita $\{1, 2\}$ ja $\{1, 3\}$ ovat vertailukelvottomia.

Esimerkki



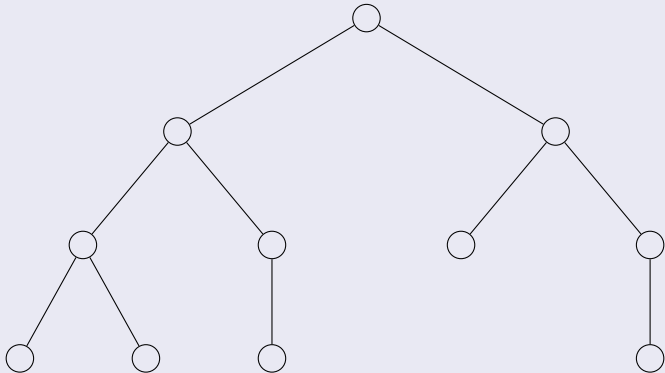
Ei ole puu, koska alkioita $\{1, 3\}$ pienemmät alkioita $\{1\}$ ja $\{3\}$ ovat vertailukelvottomia.

Esimerkki

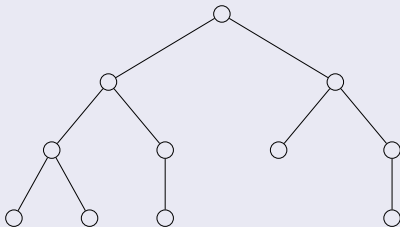


On puu. Maksimaalisia alkioita $\{1, 2, 3\}$, $\{1, 3\}$, $\{2, 3\}$ ja $\{2\}$ kutsutaan *lehdiksi* ja minimaalista alkioita \emptyset *juureksi*.

Yleinen esitystapa: Juuri ylhäällä, lehdet alhaalla



Puurakenteen käyttötarkoituksia



- Kovalevyn hakemistohierarkiat
- Kirjaston luokitukset
- Evoluution kuvaaminen
- Sukupuu