Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2025

Propositiologiikan semantiikkaa

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	$*$

Propositiologiikan semantiikkaa

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 $f_1, \ldots, f_m$: $\{0,1\}^m \to \{0,1\}$.

Propositiologiikkaa

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.

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 $\neg\phi_1 \equiv \neg\phi_1$ 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

Boolen algebra on joukko B jossa on määritelty kaksi binääristä operaatiota $\wedge$ ja $\vee$, yksi unaarinen operaatio $\neg$ ja kaksi nollapaikkaista operaatiota (eli vakiota) $\bot$ 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)
- $a \vee \bot = a$, $a \wedge \top = a$ (neutraalialkiot)
- $a \vee \neg a = \top$ ja $a \wedge \neg a = \bot$ (vasta-alkiot)

Boolen algebra

Lause

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

Lause

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

Lause

Boolen algebrassa pätee $a \vee \top = \top$ ja $a \wedge \bot = \bot$.

Lause

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

Lause

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

Boolen algebra

Lause

Propositiologiikan ekvivalenssiluokat toteutuvuusekvivalenssin suhteen muodostavat Boolen algebran, kun negaatioksi, disjunktioksi, ja konjunktioksi 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 $x \to y$ siten, että $\alpha(x \to y) = 0$ ainoastaan jos $\alpha(x) = 1$ ja $\alpha(y) = 0$.

Esimerkki

Hornin propositiot

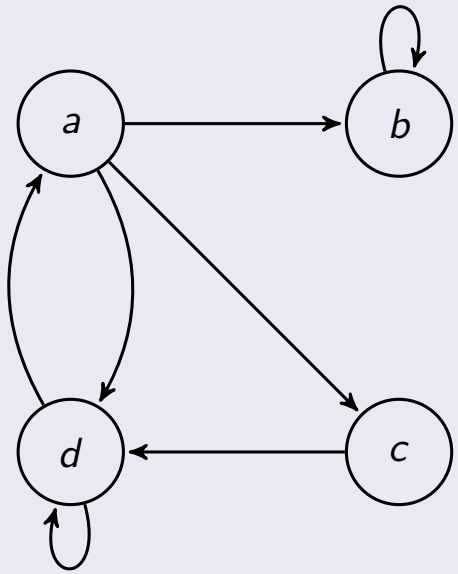
Graafit

Määritelmä

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

Esimerkki

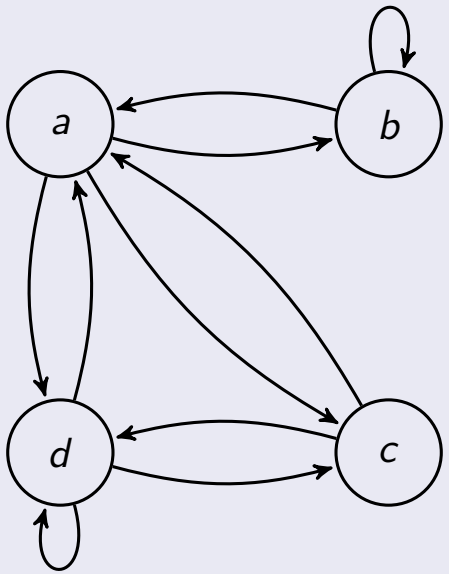
$V = \{a, b, c, d\}$ ja
$E = \{(a, b), (a, c), (a, d), (b, b), (c, d), (d, a), (d, d)\}$



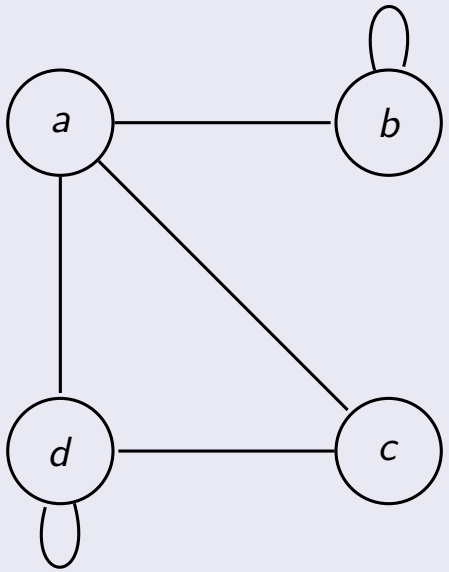
Määritelmä

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

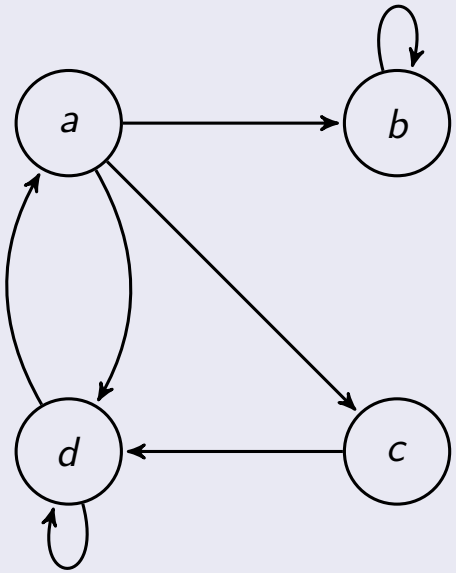
Esimerkki



Esimerkki



Vierusmatriisi

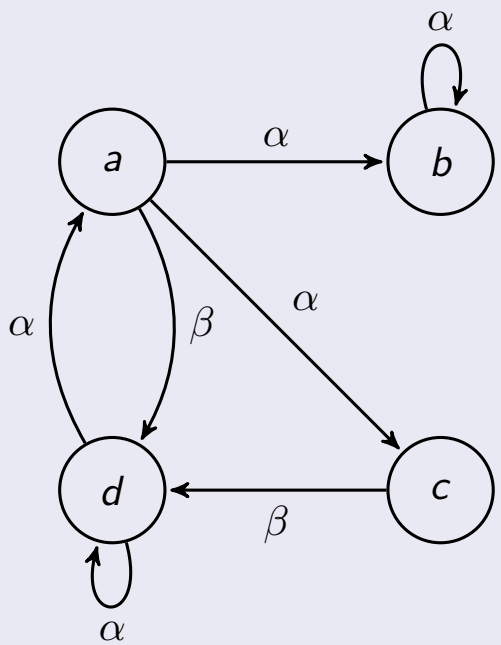


$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

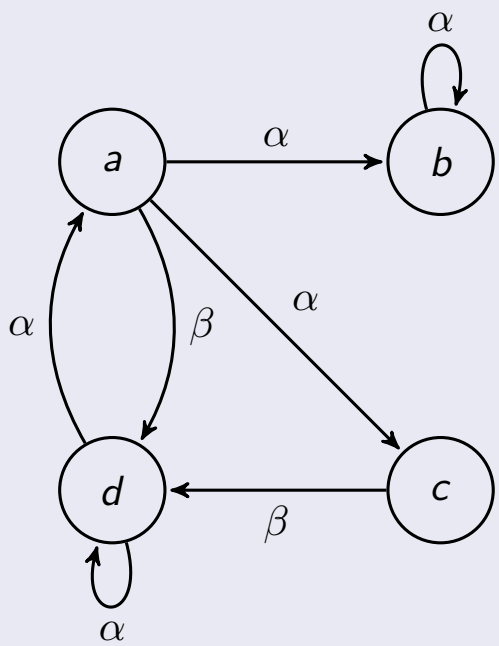
Määritelmä

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

Esimerkki

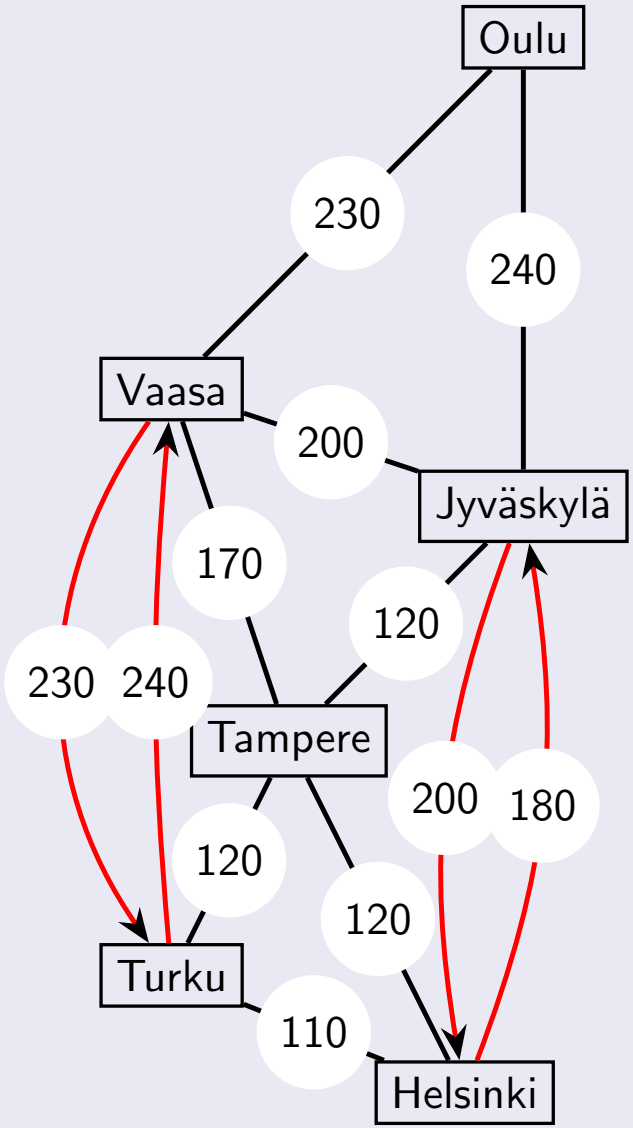


Leimatun graafin vierusmatriisi



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

Esimerkki


Oulu
230
240
Vaasa
200
Jyväskylä
170
120
230
240
Tampere
200
180
120
120
Turku
110
Helsinki

Määritelmä

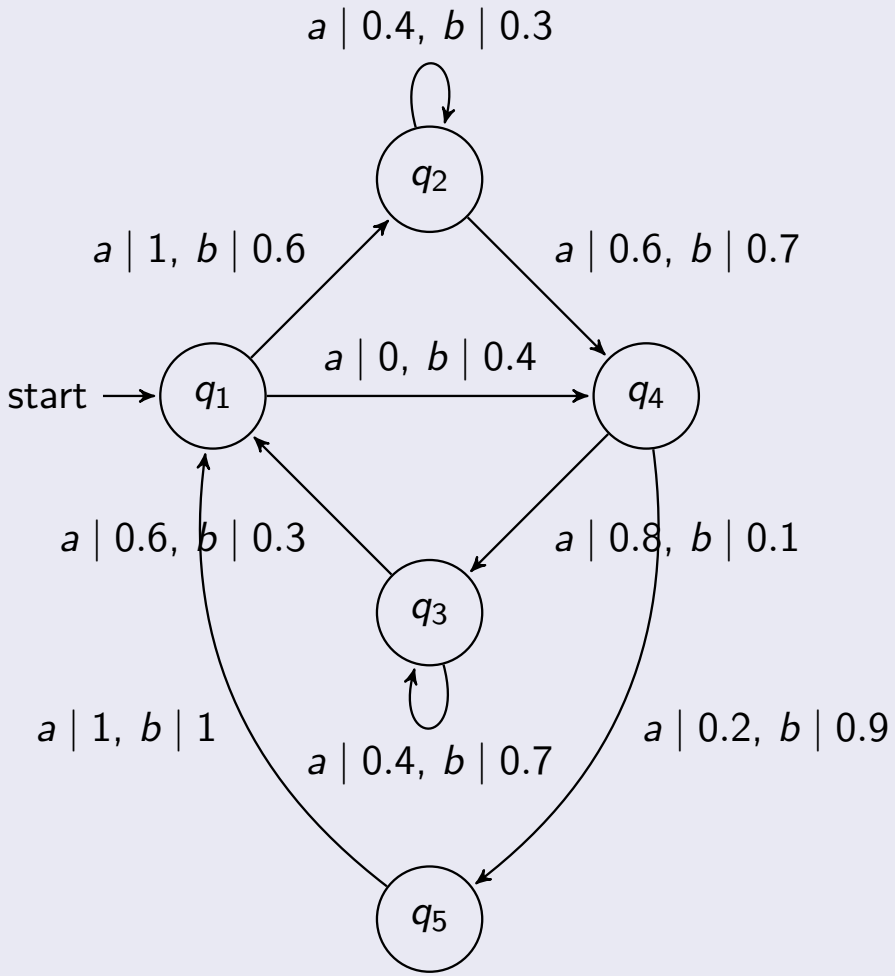
Äärellinen (probabilistinen) automaatti koostuu äärellistä tilajoukosta S, äärellisestä syöttäaakkostosta Σ, ja *transitiofunktiosta* δ, joka liittää jokaiseen tilapariin (q_1, q_2) ja syöttöaakkoston kirjaimeen todennäköisyyden $\delta(q_1, a, q_2) \in [0, 1]$, jolla automaatti siirtyy tilasta q_1 tilaan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


a | 0.4, b | 0.3
q2
a | 1, b | 0.6
a | 0.6, b | 0.7
a | 0, b | 0.4
start
q1
q4
a | 0.6, b | 0.3
a | 0.8, b | 0.1
q3
a | 1, b | 1
a | 0.4, b | 0.7
a | 0.2, b | 0.9
q5

Vierusmatriisit

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

Aloitusdistribuutio

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

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 $\boldsymbol{v}_0$ aloitusdistribuutio ja $\boldsymbol{p}$ $\{0,1\}$-arvoinen vektori joka määrittää lopputilat, saadaan syötesanan $w = a_1 a_2 \dots a_n$ hyväksymistodennäköisyys muodossa

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

Rekursio

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

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

(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

$F_2 = F_1 + F_0 = 1 + 0 = 1$
$F_3 = F_2 + F_1 = 1 + 1 = 2$
$F_4 = F_3 + F_2 = 2 + 1 = 3$
$F_5 = F_4 + F_3 = 3 + 2 = 5$
$F_6 = F_5 + F_4 = 5 + 3 = 8$
$F_7 = F_6 + F_5 = 5 + 8 = 13$
$F_8 = F_7 + F_6 = 13 + 8 = 21$
$F_9 = F_8 + F_7 = 21 + 13 = 34$
$F_{10} = F_9 + F_8 = 34 + 21 = 55$
$F_{11} = F_{10} + F_9 = 55 + 34 = 89$
....

Rekursio

Joukko $\mathbb{N}$

- Rekursion pohja 1
- Seuraajafunktio s
- $1 \to s(1) \to s(s(1)) \to s(s(s(1))) \to s(s(s(s(1)))), \ldots$
- $1 \to 2 \to 3 \to 4 \to \ldots$
- $s(n) = n + 1$ (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

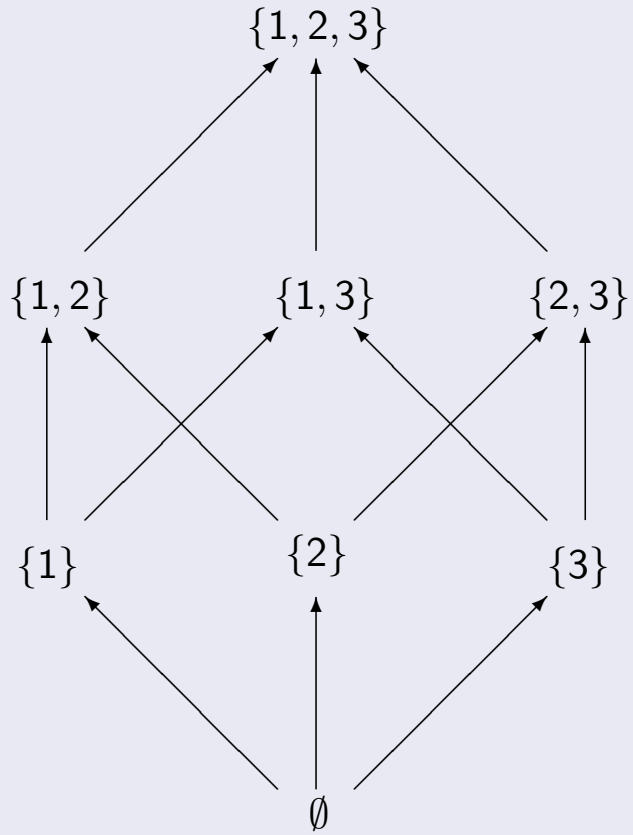
Puu (tree) on pari $(X, \preceq)$ missä X on joukko (verteksit eli solmut eli pisteet) ja $\preceq$ on joukossa X määritelty osittainen järjestys, joka toteuttaa seuraavat ehdot:

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

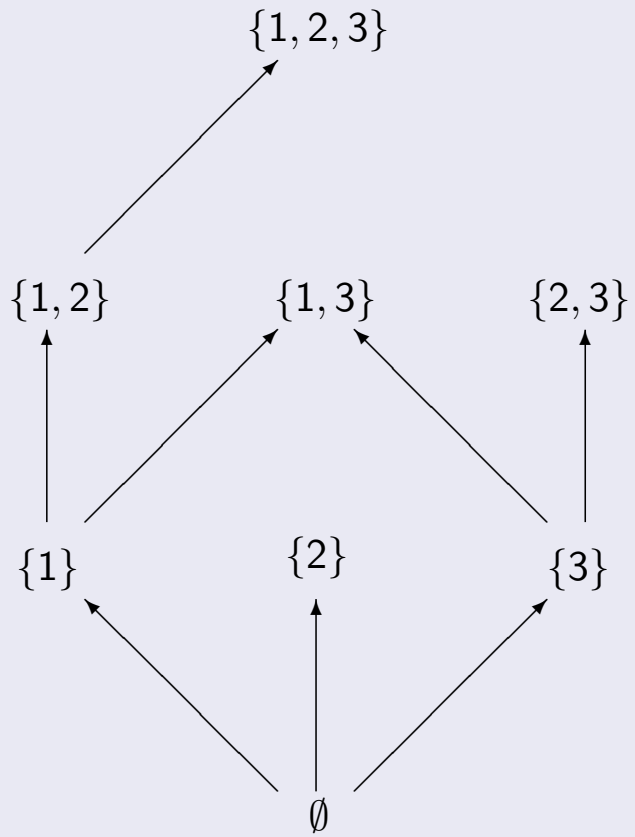
Puuhun kuuluvia relaationuolia $x \to y \Leftrightarrow x \preceq y$ kutsutaan myös *kaariksi* tai *viivoiksi*.

Esimerkki



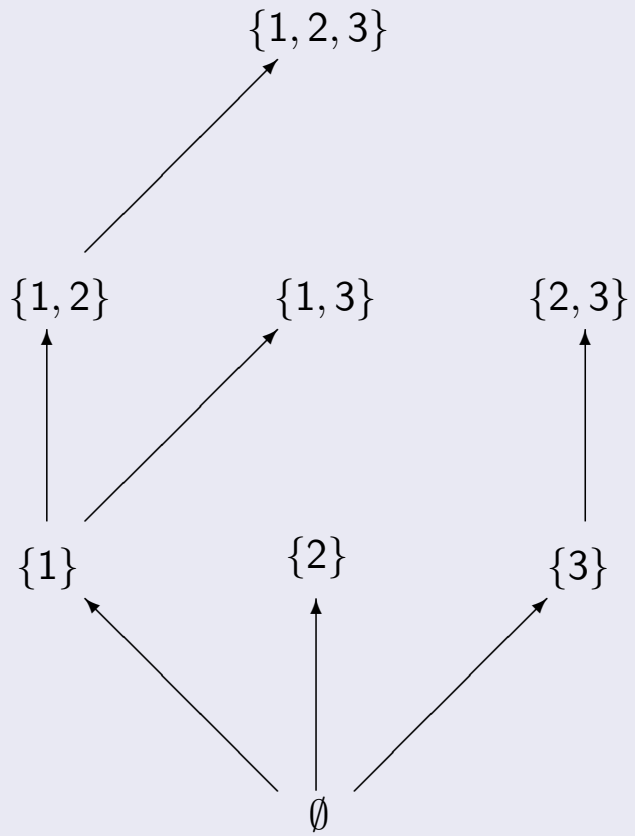
Ei ole puu, koska esim. alkiota $\{1, 2, 3\}$ pienemmät alkiot $\{1, 2\}$ ja $\{1, 3\}$ ovat vertailukelvottomia.

Esimerkki



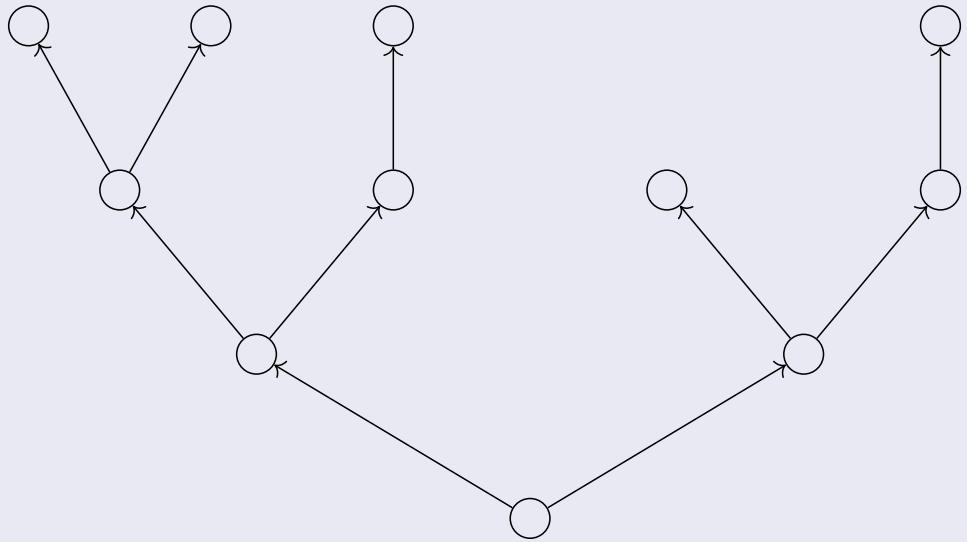
Ei ole puu, koska alkiota $\{1, 3\}$ pienemmät alkiot $\{1\}$ ja $\{3\}$ ovat vertailukelvottomia.

Esimerkki



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

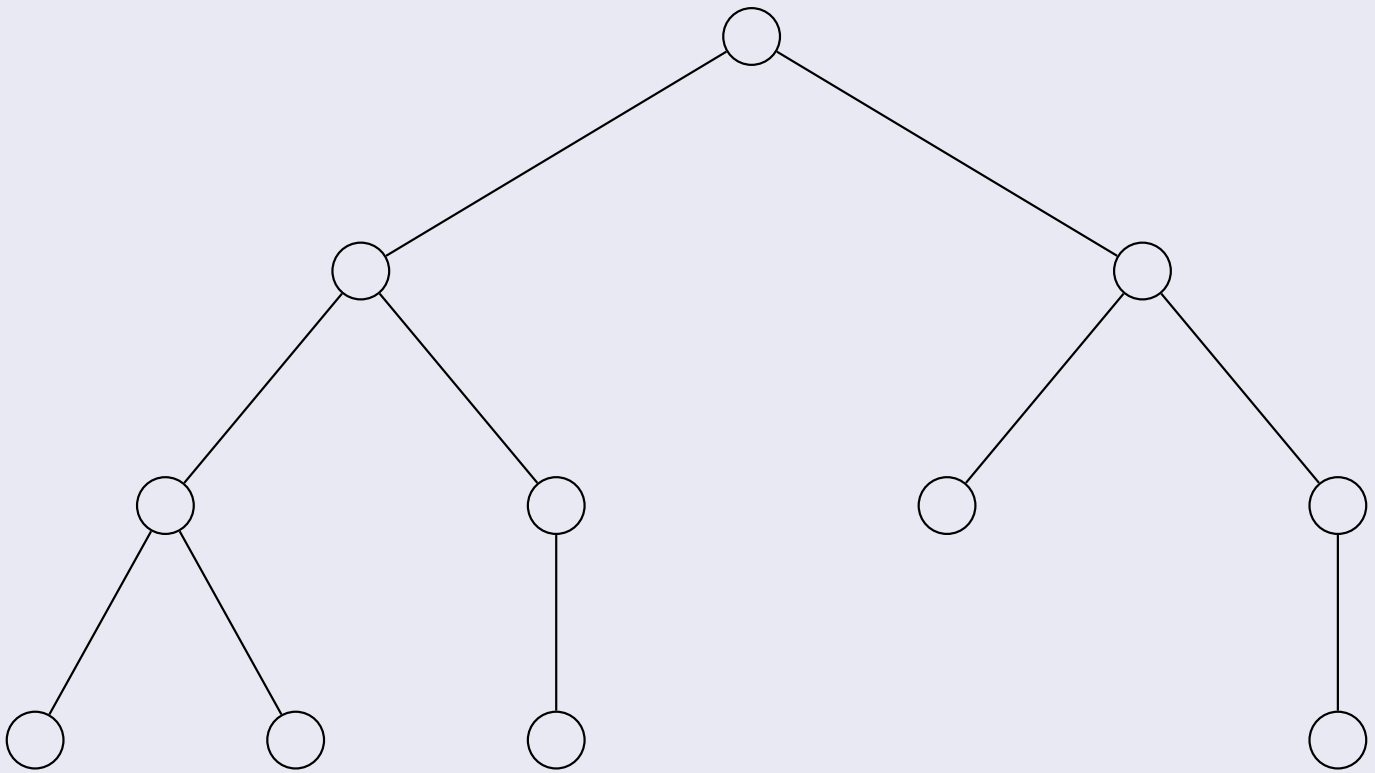
Esimerkki



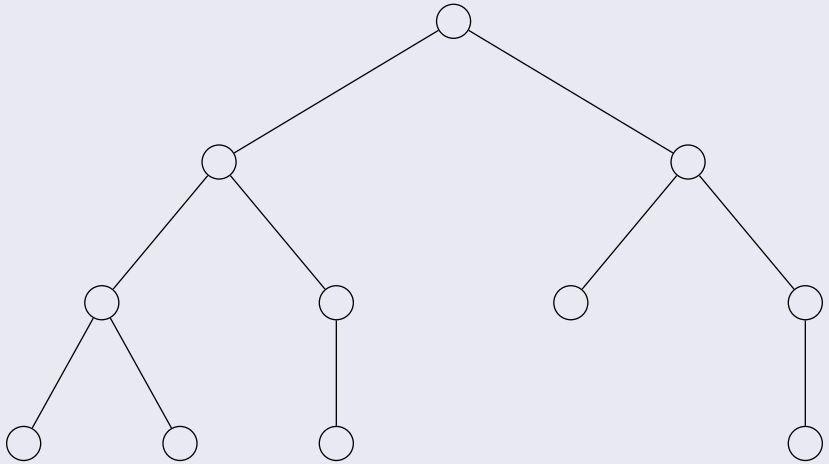
Rekursiivinen määritelmä (äärelliset puut)

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

Yleinen esitystapa: Juuri ylhäällä, lehdet alhaalla



Puurakenteen käyttötarkoituksia



- Kovalevyn hakemistohierarkiat
- Kirjaston luokitukset
- Evoluution kuvaaminen
- Sukupuu