

MS-A0402 Diskreetin matematiikan perusteet

Esimerkkejä, todistuksia ym., osa I

G. Gripenberg

Aalto-yliopisto

3. huhtikuuta 2014

- 1 Joukko-oppi ja logiikka
 - Induktio
 - Todistukset logiikassa

- 2 Relaatiot ja funktiot

- 3 Kombinatoriikka

Joukot ja implikaatiot

Olkoon $A = \{1, 2, 3, 4\}$, $B = \{0, 3, 4\}$ ja $C = \{x : x \text{ on kokonaisluku } \geq 2\}$. Mitkä seuraavista väitteistä ovat tosia?

- (a) $x \in A \cap C \rightarrow x \in B$ kaikilla x ?
- (b) $A \subset B \rightarrow C \subset A$?
- (c) On olemassa $y \in C$ siten, että $y \in B \rightarrow y \notin A \cup B$?
- (d) $y \notin B \rightarrow y \notin A$ kaikilla $y \in C$?

Ratkaisu: (a) Koska $A \cap C = \{2, 3, 4\}$ niin pätee $2 \in A \cap C$ mutta koska $2 \notin B$ niin tämä väite ei päde (ja väite sanoo, että $A \cap C \subset B$).

(b) Koska $2 \in A$ mutta $2 \notin B$ niin ei päde $A \subset B$ ja näin ollen implikaatio $A \subset B \rightarrow C \subset A$ on tosi.

(c) Tämäkin väite on tosi koska esim. $2 \in C$, mutta $2 \notin B$ mistä seuraa, että $2 \in B$ on epätosi joten $2 \in B \rightarrow 2 \notin A \cup B$ on tosi.

(d) Tämä väite on epätosi koska esim. $2 \in C$ ja $2 \notin B$ mutta $2 \in A$ joten $2 \notin A$ on epätosi.

😊 Miksi joukko-oppi ei ole niin yksinkertaista kuin miltä näyttää?

Niin kauan kun tarkastelvissa joukoissa on vain ärellisen monta alkiota, kuten joukossa $\{1, 3, 4, 7\}$, ongelmia ei juuri esiinny mutta klassinen esimerkki ongelmista on jos yritämme määritellä joukkoa A kaavalla

$$A = \{x : x \notin x\}.$$

Jos nyt $A \in A$ niin $x \notin x$ ei päde kun x on A ja A :n määritelmän mukaan $A \notin A$ ja olemme saaneet aikaan ristiriidan. Jos sen sijaan $A \notin A$ niin ehto $x \notin x$ on voimassa kun x on A joten $A \in A$ ja taas tuloksena on ristiriita. Vastaavanlaisia ongelmia syntyy jos sanomme "Tämä on valhe" tai jos puhumme "parturista, joka leikkaa hiukset kaikilla niillä henkilöillä, jotka eivät itse leikkaa hiuksiaan".

💡 Induktio

Osoitamme induktion avulla, että

$$\sum_{i=1}^n i = 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}, \quad n \geq 1.$$

Väite $P(n)$ on siis $\sum_{i=1}^n i = \frac{n(n+1)}{2}$ ja $n_0 = 1$. Näin ollen väite $P(n_0)$ on sama kuin $1 = \frac{1(1+1)}{2}$ mikä pitää paikkansa. Oleta seuraavaksi, että $P(k)$ on tosi ja $k \geq 1$. Koska $P(k)$ pätee, niin $\sum_{i=1}^k i = \frac{k(k+1)}{2}$ mistä seuraa, että

$$\begin{aligned} \sum_{i=1}^{k+1} i &= \sum_{i=1}^k i + (k+1) = \frac{k(k+1)}{2} + (k+1) \\ &= (k+1) \left(\frac{k}{2} + 1 \right) = \frac{(k+1)(k+2)}{2} = \frac{(k+1)((k+1)+1)}{2}, \end{aligned}$$

joka taas merkitsee sitä, että $P(k+1)$ on tosi. Induktioperiaatteen nojalla toteamme, että $P(n)$ pätee kaikilla $n \geq 1$.

😊 Päätelysäännöt ja todistukset logiikassa

Todistus on lista lauseista joissa jokainen lause on joko aksiomi (eli oletetaan olevan tosi) tai johdettu aikaisemmista lauseista.

Päätelysäännöt ovat seuraavanlaisia:

$$\begin{array}{l} L_1 \\ L_2 \\ \vdots \\ L_n \\ \hline \therefore Q \end{array}$$

eli jos L_1, \dots, L_n ovat lauseita todistuksessa, voidaan todistukseen lisätä lause Q .

Päätelysäännöt perustuvat siihen, että $L_1 \& L_2 \& \dots \& L_n \rightarrow Q$ on tautologia eli on aina tosi ja tärkein päätelysääntö on ns. modus ponens eli

$$\begin{array}{l} x \\ x \rightarrow y \\ \hline \therefore y. \end{array}$$

😊 Päätelysäännöt ja todistukset logiikassa

Olkoot p ja q kaksi lausetta. Nyt todistamme, että q on tosi jos p & $!p$ on tosi, eli jos oletetaan ristiriitainen väite voidaan todistaa mitä vaan.

Päätelysäännöteinä käytetään tässä

$$(a) \frac{x \mid y}{!x} \\ \therefore y$$

$$(b) \frac{x \& y}{\therefore x}$$

$$(c) \frac{x}{\therefore x \mid y}$$

$$(d) \frac{x \& y}{\therefore y \& x}$$

😊 Päätelysäännöt ja todistukset logiikassa, jatk.

Todistus näyttää nyt seuraavanlaiselta:

(1) $p \& !p$: Oletus

(2) p : (1) ja (b) missä $x = p$ ja $y = !p$

(3) $p \mid q$: (2) ja (c) missä $x = p$ ja $y = q$

(4) $!p \& p$: (1) ja (d) missä $x = p$ ja $y = !p$

(5) $!p$: (1) ja (b) missä $x = !p$ ja $y = p$

(6) q : (3), (4) ja (a) missä $x = p$ ja $y = q$.

Näin lause q on tullut todistetuksi.

😊 Järjestetyn parin koordinaatit

Parin $[x, y]$ (tai (x, y)) ensimmäinen koordinaatti on (tietenkin) x ja toinen on y . Jos parin määritelmäksi otetaan $\{\{a\}, \{a, b\}\}$ niin voidaan määritellä predikaatit $E(p, x)$ ja $T(p, y)$ jotka sanovat, että x on p :n ensimmäinen koordinaatti ja y on p :n toinen koordinaatti seuraavalla tavalla:

$$E(p, x) = \forall z((z \in p) \rightarrow (x \in z))$$

(tai lyhyemmin $\forall z \in p(x \in z)$) ja

$$T(p, y) = (\exists z((z \in p) \& (y \in p))) \& (\forall u(\forall v(((u \in p) \& (v \in p)) \& !(u = v)) \rightarrow ((!(y \in u)) \mid !(y \in v))))).$$

Tässä lausekkeessa on häiritsevän monta sulkua ja voimme myös kirjoittaa $\exists z((z \in p) \& (y \in p)) \& \forall u \forall v((u \in p) \& (v \in p) \& !(u = v) \rightarrow !(y \in u) \mid !(y \in v))$. Vielä lyhyempi muoto olisi

$$\exists z \in p(y \in p) \& \forall u \in p \forall v \in p(!(u = v) \rightarrow (y \notin u) \mid (y \notin v)).$$

😊 Esimerkki osittaisjärjestyksestä

Olkoon X jokin (ei-tyhjä) joukko ja $\mathcal{P}(X)$ sen kaikkien osajoukkojen muodostama joukko (eli ns. potenssijoukko). Joukossa $\mathcal{P}(X)$ meillä on relaatio $\subset: A \subset B$ jos ja vain jos A on B :n osajoukko (ja muista että $A \subset B$ myös kun $A = B$). Tämä relaatio on osittaisjärjestys koska se on

- refleksiivinen: $A \subset A$,
- antisymmetrinen: Jos $A \subset B$ ja $A \neq B$ niin on olemassa $x \in B$ siten että $x \notin A$ jolloin $B \not\subset A$,
- transitiivinen: Jos $A \subset B$ ja $B \subset C$ niin jokainen A :n alkio on B :n alkio ja koska jokainen B :n alkio on C :n alkio niin jokainen A :n alkio on C :n alkio, eli $A \subset C$.

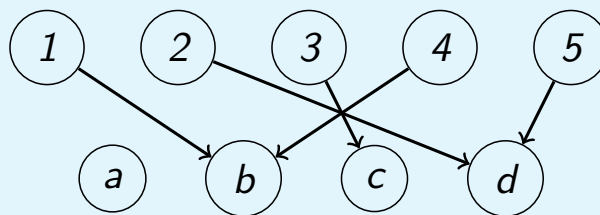
Lisäksi tällä relaatiolla on muitakin ominaisuuksia kuten, että jos $A, B \in \mathcal{P}(X)$ niin joukoille A ja B löytyy pienin yläraja, eli joukko C siten, että $A \subset C, B \subset C$ (eli C on yläraja) ja jos $A \subset D$ ja $B \subset D$ niin $C \subset D$ (eli C on pienin yläraja). Selvästikin $C = A \cup B$. Vastaavasti löytyy myös suurin ala-raja joka (tietenkin) on $A \cap B$.

😊 Listat, jonot ja karteesiset tulot funktioina

- Listaa $[a, b, c, d]$ voidaan tulkita olevan funktio f joukosta $\{1, 2, 3, 4\}$ (tai joukosta $\{0, 1, 2, 3\}$) joukkoon joka sisältää esim kaikki aakkoset siten, että $f(1) = a$, $f(2) = b$, $f(3) = c$ och $f(4) = d$.
- Reaalinen lukujono $(a_n)_{n=0}^{\infty} = (a_0, a_1, a_2, \dots)$ voidaan tulkita olevan funktio f joukosta \mathbb{N}_0 joukkoon \mathbb{R} siten, että $f(n) = a_n$ kaikilla $n \in \mathbb{N}_0$.
- Jos Y_j on joukko jokaisella $j \in J$ missä J on (toinen) joukko niin voidaan määritellä karteesinen tulo $\prod_{j \in J} Y_j$ joukkona, jonka alkiot ovat kaikki funktiot $f : J \rightarrow \bigcup_{j \in J} Y_j$ siten, että $f(j) \in Y_j$. Jos $Y_j = Y$ kaikilla $j \in J$ niin joukko $\prod_{j \in J} Y_j$ on täsmälleen kaikki funktiot $J \rightarrow Y$ ja tälle joukolle käytetään merkintää Y^J eli esim. $Y^{\{1,2,3\}} = Y \times Y \times Y = Y^3$.

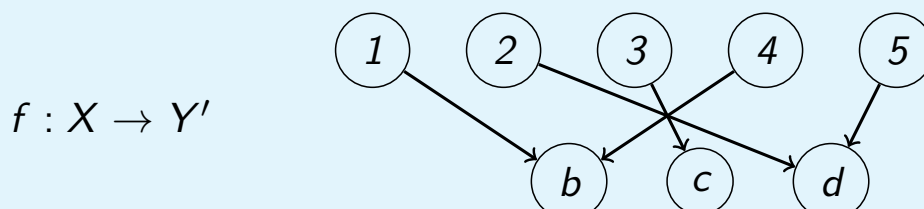
😊 Injektio, surjektio, bijektio

Alla oleva verkko esittää funktiota $f : X \rightarrow Y$:



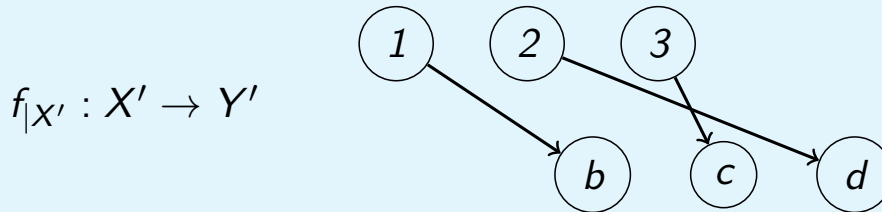
Tässä tapauksessa määrittely- eli lähtöjoukko on $X = \{1, 2, 3, 4, 5\}$ ja maalijoukko on $Y = \{a, b, c, d\}$ ja kyseessä on funktio koska jokainen X :n alkio on täsmälleen yhden kaaren lähtösolmu.

Kyseinen funktio ei ole surjektio koska $a \notin f(X)$ mutta siitä tulee surjektio jos Y korvataan joukolla $Y' = Y \setminus \{a\}$. Funktion arvot eivät tästä muutu, ainostaan maalijoukko korvataan toisella ja käytännön kannalta (vaikka ei ehkä periaatteessa) meillä on edelleen täsmälleen sama funktio.

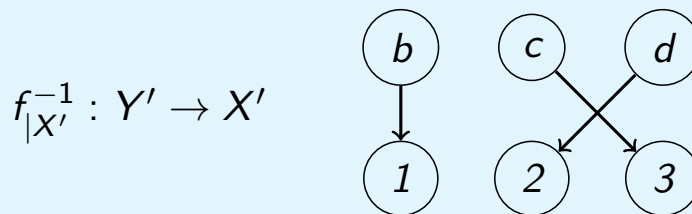


😊 Injektio, surjektio, bijektio, jatk.

Funktio f ei ole myöskään injektio koska esim. $f(1) = f(4)$, mutta siitä voidaan konstruoida injektio poistamalla esim. alkioita 4 ja 5 joukosta X ja rajoittamalla f joukkoon $X' = X \setminus \{4, 5\}$. Näin saatu funktio $f|_{X'} : X' \rightarrow Y'$ on bijektio.



Jokaisella bijektioilla on käänteisfunktio ja tässä tapauksessa sen verkkoesitys on seuraavanlainen:



Surjektioiden $A \rightarrow B$ lukumäärä kun $|A| = m$ ja $|B| = n$

Oleta $B = \{b_1, b_2, \dots, b_n\}$. Olkoon $F = B^A$ kaikkien funktioiden $A \rightarrow B$ joukko ja $F_j = (B \setminus \{b_j\})^A \subset F$ kaikkien funktioiden $A \rightarrow B \setminus \{b_j\}$ joukko eli niiden F :n alkoiden f joukko joille pätee, että $f(x) \neq b_j$ kaikilla $x \in A$. Surjektioiden joukko on siten $F \setminus \bigcup_{j=1}^n F_j$. Nyt $F_{j_1} \cap F_{j_2} \cap \dots \cap F_{j_r}$ on joukko $(B \setminus \{b_{j_1}, b_{j_2}, \dots, b_{j_r}\})^A$ johon kuuluvat kaikki funktiot $A \rightarrow B$ jotka eivät saa arvoja b_{j_1}, \dots, b_{j_r} . Jos $1 \leq j_1 < \dots < j_r \leq n$ niin $|F_{j_1} \cap F_{j_2} \cap \dots \cap F_{j_r}| = (n - r)^m$. Koska on $\binom{n}{r}$ eri tapaa valita indeksit $1 \leq j_1 < \dots < j_r \leq n$ niin seulaperiaatteesta seuraa, että surjektioiden $A \rightarrow B$ lukumäärä on

$$n^m - \left(\sum_{k=1}^n (-1)^{k+1} \binom{n}{k} (n - k)^m \right) = \sum_{r=0}^n (-1)^r \binom{n}{r} (n - r)^m = \sum_{r=0}^n (-1)^{n-r} \binom{n}{r} r^m.$$

Huomaa, että kun $m < n$ ei ole surjektioita $A \rightarrow B$ joten

$\sum_{r=0}^n (-1)^{n-r} \binom{n}{r} r^m = 0$ kun $m < n$, mikä ehkä ei ole aivan ilmeistä.

Monellako tavalla voidaan sijoittaa k identtistä palloa n :ään identtiseen laatikkoon?

Olkoon $A(k, n)$ tämä lukumäärä. Koska voimme sijoittaa $k \geq 0$ palloa 1:een laatikkoon vain yhdellä tavalla niin $A(k, 1) = 1$ kun $k \geq 0$. Jos $k = 0$ niin kaikki laatikot ovat tyhjiä ja meillä on vain yksi vaihtoehto eli $A(0, n) = 1$ kaikilla $n \geq 1$.

Oleta nyt, että $k \geq 1$ ja $n \geq 2$. Olkoon j ($j \geq 0$) pallojen lukumäärä siinä laatikossa missä on vähiten palloja. Eri j :n arvoilla saadaan varmasti erilaisia vaihtoehtoja. Nyt sijoitamme ensin j palloa jokaiseen laatikkoon ja sen jälkeen jäljellä olevat $k - n \cdot j$ palloa niihin $n - 1$:een laatikkoon joissa voi olla enemmän kun j palloa ja tämä on mahdollista $A(k - n \cdot j, n - 1)$:llä eri tavalla. Jos $j > \frac{k}{n}$ niin $k - n \cdot j < 0$, joten rekursioyhtälöksi tulee

$$A(k, n) = \sum_{j=0}^{\lfloor \frac{k}{n} \rfloor} A(k - n \cdot j, n - 1).$$

Esimerkki

Tentissä valvojat jakavat 150 tehtäväpaperia 160:lle tenttijälle. Monellako tavalla tämä on mahdollista?

Tässä oletetaan, että tehtäväpaperit ovat identtiset mutta tenttijät eivät ole.

Ensimmäinen, järkevä, vaihtoehto on että jokaiselle tenttijälle annetaan korkeintaan yksi paperi. Silloin on kysymys siitä monellako tavalla voimme 160 henkilön joukosta valita ne 150, jotka saavat paperin. Tässä on kyse valinnasta palauttamatta kun järjestyksellä ei ole merkitystä, joten

vaihtoehtoja on $\binom{160}{150} = \binom{160}{10}$

Toinen, vähemmän järkevä, vaihtoehto on, ettei aseteta mitään rajoituksia montako paperia sama henkilö voi saada. Silloin valvojat valitsevat 150 kertaa tenttijän, jolle paperi annetaan, joukosta, jossa on 160 alkia, "palauttaen" eikä valintajärjestyksellä ole merkitystä. Vaihtoehtojen lukumääräksi tulee silloin

$$\binom{150 + 160 - 1}{160 - 1} = \frac{309!}{159! \cdot 150!}.$$