MS-A0401 Diskreetin matematiikan perusteet
Esimerkkejä ym., osa I

G. Gripenberg

Aalto-yliopisto

30. syyskuuta 2015

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

Edellä on esitetty ns. naiivi joukko-oppi missä esimerkiksi pidetään selvänä, että luonnolliset luvut muodostavat joukon ja niin kauan kun tarkasteltavissa joukoissa on vain äärellisen monta alkiota tai käsitellään luonnollisten lukujen joukkoa, ongelmia ei juuri esiinny. Mutta klassinen esimerkki, joka osoittaa että myös ns. aksiomaattinen joukko-oppi on tarpeen, on ns. Russellin paradoksi: Määritellään

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

Jos $A \in A$ 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 lause on epätosi" tai jos puhumme "parturista, joka leikkaa hiukset kaikilta niiltä, jotka eivät itse leikkaa hiuksiaan".

Joukot ja implikaatiot: Esimerkkejä

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) $x \in A \cap C \to x \in B$ *kaikilla* x*?*

(b) $A \subseteq B \to C \subseteq A$*?*

(c) *On olemassa* $y \in C$ *siten, ettei päde* $y \in B \to y \in A$*?*

Vastaus:

(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* $A \cap C \subseteq B$*).*

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

(c) *Väite* $y \in B \to y \in A$ *ei päde jos ja vain jos* $y \in B$ *ja* $y \notin A$ *eli* $y \in B \setminus A = \{0\}$ *ja* $0 \notin C$ *joten väite on epätosi.*

Päättelysäännöt ja todistukset logiikassa

Todistus on lista lauseista joissa jokainen lause on joko aksiomi (eli oletetaan olevan tosi) tai johdettu aikaisemmistä lauseista päättelysääntöjen avulla. Esimerkiksi ns. modus ponens eli

$$\frac{x \qquad x \to y}{y}$$

on tärkeä päättelysääntö ja perustuu siihen, että $(x \text{ AND } (x \to y)) \to y$ *on tautologia, eli aina tosi riippumatta* x*:n ja* y*:n totuusarvoista. Tämä (kuten muutkin päättelysäännöt) käytetään siten, että jos todistuslistassa on jo lauseet* a *ja* $a \to b$ *niin listaan lisätään lause* b*.*

Päättelysäännöt ja todistukset logiikassa

Olkoot p *ja* q *kaksi lausetta. Nyt todistamme, että* q *on tosi jos* p AND (NOT p) *on tosi, eli jos oletetaan ristiriitainen väite voidaan todistaa mitä vaan. Päättelysääntöinä käytämme tässä*

(a) $\dfrac{x \text{ OR } y \qquad \text{NOT } x}{y}$

(b) $\dfrac{x \text{ AND } y}{x}$

(c) $\dfrac{x}{x \text{ OR } y}$

(d) $\dfrac{x \text{ AND } y}{y \text{ AND } x}$

Päättelysäännöt ja todistukset logiikassa, jatk.

Todistus näyttää nyt seuraavanlaiselta:

(1) p AND (NOT p)*:* *Oletus*

(2) p*:* *(1) ja (b) missä* $x = p$ *ja* $y =$ NOT p

(3) p OR q*:* *(2) ja (c) missä* $x = p$ *ja* $y = q$

(4) (NOT p) AND p*:* *(1) ja (d) missä* $x = p$ *ja* $y =$ NOT p

(5) NOT p*:* *(4) ja (b) missä* $x =$ NOT p *ja* $y = p$

(6) q*:* *(3), (5) ja (a) missä* $x = p$ *ja* $y = q$*.*

Näin lause q *on tullut todistetuksi.*

Esimerkki suorasta ja epäsuorasta todistuksesta

(a) *Väite: Jos* $0 < a < 1$ *niin* $a^2 < a$*.*
Suora todistus:
- $1 - a > 0$ *koska* $a < 1$*.*
- $a \cdot (1 - a) > 0$ *koska* $a > 0$ *ja* $(1 - a) > 0$*.*
- $a^2 < a$ *koska* $a \cdot (1 - a) = a - a^2 > 0$ *jolloin* $a = a - a^2 + a^2 > a^2$*.*

(b) *Väite: Jos* $0 < a < 1$ *niin* $\sqrt{a} > a$*.*
Epäsuora todistus:
- *Vastaoletus:* $\sqrt{a} \le a$*.*
- $a = \sqrt{a}^2 \le a^2$ *koska* $\sqrt{a}$ *ja* $a > 0$ *ja funktio* $x \mapsto x^2$ *on kasvava välillä* $[0, \infty)$*.*
- $a \cdot (1 - a) = a - a^2 \le 0$ *koska* $a \le a^2$*.*
- $a \le 0$ *koska* $1 - a > 0$ *kun* $a < 1$ *ja kun jaamme positiivisellä luvulla epäyhtälö pysyy muuttumattomana.*
- $a \le 0$ *on ristiriidassa oletuksen* $a > 0$ *kanssa joten vastaoletus ei pidä paikkansa.*

Huomaa, ettei tällaisissa todistuksissa ole olemassa yksi ainoa oikea lukumäärä välivaiheita tai välivaiheiden perusteluita! Tavoite on, että todistuksesta tulee vakuuttava ja ymmärrettävä ja se taas riippuu lukijastakin.

Esimerkki: Potenssijoukko

Olkoon $\mathcal{P}(X)$ joukon X osajoukkojen joukko, eli $A \in \mathcal{P}(X)$ jos ja vain jos $A \subseteq X$. Jos nyt X ja Y ovat kaksi joukkoa niin onko toinen joukoista $\mathcal{P}(X) \setminus \mathcal{P}(Y)$ ja $\mathcal{P}(X \setminus Y)$ toisen osajoukko?

- *Koska tyhjä joukko on jokaisen joukon osajoukko niin $\emptyset \in \mathcal{P}(X \setminus Y)$. Samoin $\emptyset \in \mathcal{P}(Y)$ joten $\emptyset \notin \mathcal{P}(X) \setminus \mathcal{P}(Y)$. Tästä seuraa, ettei koskaan päde $\mathcal{P}(X \setminus Y) \subseteq \mathcal{P}(X) \setminus \mathcal{P}(Y)$ (eli aina pätee $\mathcal{P}(X \setminus Y) \not\subseteq \mathcal{P}(X) \setminus \mathcal{P}(Y)$).*
- *Jos $X = Y$ niin $\mathcal{P}(X) = \mathcal{P}(Y)$ joten $\mathcal{P}(X) \setminus \mathcal{P}(Y) = \emptyset \subseteq \mathcal{P}(X \setminus Y) = \{\emptyset\}$ koska tyhjä joukko on jokaisen joukon osajoukko.*
- *Mutta jos esimerkiksi $X = \{0,1\}$ ja $Y = \{0\}$ niin $\mathcal{P}(X) \setminus \mathcal{P}(Y) = \{\{0,1\},\{1\}\}$ mutta $X \notin \mathcal{P}(X \setminus Y) = \{\{1\},\emptyset\}$ joten tässä tapauksessa $\mathcal{P}(X) \setminus \mathcal{P}(Y) \not\subseteq \mathcal{P}(X \setminus Y)$*
- *Lopputulos on siis ettei koskaan päde $\mathcal{P}(X \setminus Y) \subseteq \mathcal{P}(X) \setminus \mathcal{P}(Y)$ mutta riippuu joukoista X ja Y pätekö $\mathcal{P}(X) \setminus \mathcal{P}(Y) \subseteq \mathcal{P}(X \setminus Y)$ vai ei.*

Esimerkki: Järjestetyn parin koordinaatit

Parin $[x,y]$ (tai (x,y) erityisesti jos kyseessä on xy-tason piste) ensimmäinen koordinaatti on (tietenkin) x ja toinen on y. Jos parin määritelmäksi otetaan $[a,b] = \{\{a\},\{a,b\}\}$ niin voimme 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:

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

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

$$T(p,y) = \exists z((z \in p) \text{ AND } (y \in z)) \text{ AND}$$
$$\forall u \forall v\,((u \in p) \text{ AND } (v \in p) \text{ AND NOT } (u == v) \to \text{NOT } (y \in u) \text{ OR NOT } (y \in v)),$$

missä $u == v$ on predikaatti, joka sanoo, että u on sama joukko kuin v. Lyhyemmin tämän voimme esittää muodossa

$$T(p,y) = \exists z \in p\,(y \in z)$$
$$\text{AND } \forall u \in p \forall v \in p\,(\text{NOT } (u == v) \to (y \notin u) \text{ OR } (y \notin v)).$$

Induktio: Esimerkki

Osoitamme induktion avulla, että

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

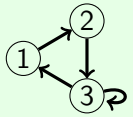
Väite $P(n)$ on siis $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ ja $n_0 = 1$. Näin ollen väite $P(n_0)$ on sama kuin $1 = \frac{1(1+1)}{2}$ mikä pitää paikkansa. Oletamme seuraavaksi, että $P(k)$ on tosi ja $k \geq 1$. Koska $P(k)$ pätee, niin $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ mistä seuraa, että

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

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

Relaatioiden esitystapoja

- *Jos $X = \{1,2,3\}$ niin $W = \{[1,2],[2,3],[3,1],[3,3]\}$ on relaatio X:ssä ja tätä relaatiota voi esittää verkkona*

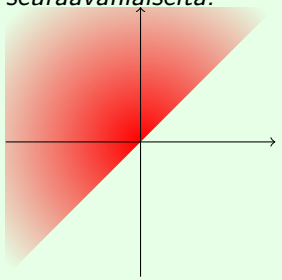


taulukkona

	1	2	3
1		•	
2			•
3	•		•

tai matriisina $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

- *Jos $X = \mathbb{R}$ ja W on relaatio "aidosti pienempi kuin" niin $W = \{\,[x,y] : x, y \in \mathbb{R},\ x < y\,\}$ ja xy-tason osajoukkona se näyttää seuraavanlaiselta:*



Esimerkki: Osittaisjärjestys

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 $\subseteq$: $A \subseteq B$ jos ja vain jos A on B:n osajoukko. Tämä relaatio on osittaisjärjestys koska se on

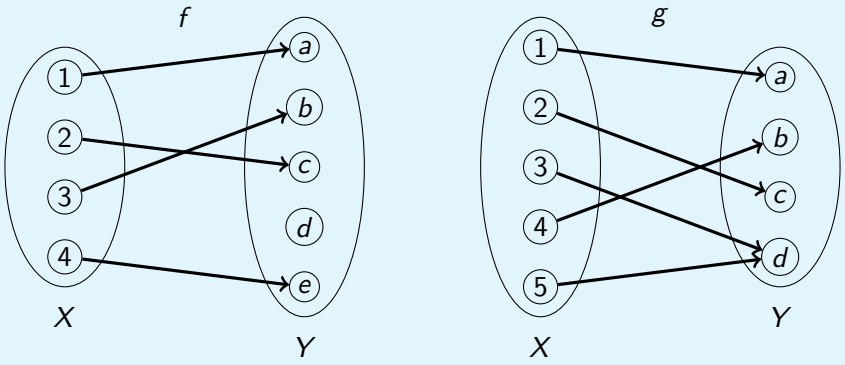
- *refleksiivinen: $A \subseteq A$,*
- *antisymmetrinen: Jos $A \subseteq B$ ja $A \neq B$ niin on olemassa $x \in B$ siten että $x \notin A$ jolloin $B \not\subseteq A$,*
- *transitiivinen: Jos $A \subseteq B$ ja $B \subseteq C$ niin jokainen A:n alkio on B:n alkio ja koska jokainen B:n alkio on C:n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

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 $A \subseteq C$, $B \subseteq C$ (eli C on yläraja) ja jos $A \subseteq D$ ja $B \subseteq D$ niin $C \subseteq D$ (eli C on pienin yläraja). Selvästikin $C = A \cup B$. Vastaavasti löytyy myös suurin ala-raja, joka (tietenkin) on $A \cap B$.

Esimerkki: Ekvivalenssiluokat

Joukossa $X = \{ [m, n] : m, n \in \mathbb{Z}, n \neq 0 \}$ voimme määritellä ekvivalenssirelaation $\sim$ siten, että $[m_1, n_1] \sim [m_2, n_2]$ jos ja vain jos $m_1 \cdot n_2 = m_2 \cdot n_1$. Nämä ekvivalenssiluokat "ovat" rationaaliluvut koska $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ täsmälleen silloin kun $m_1 \cdot n_2 = m_2 \cdot n_1$.

Injektiot ja surjektiot



Funktio $f : X \to Y$ on injektio ("jokaiseen Y:n alkioon tulee **korkeintaan** *yksi suunnattu kaari") mutta se ei ole surjektio koska X:stä ei löydy yhtään alkiota x, siten, että $f(x) = d$.*
Funktio $g : X \to Y$ on surjektio ("jokaiseen Y:n alkioon tulee **vähintään** *yksi suunnattu kaari") mutta se ei ole injektio koska $g(3) = g(5)$ ja $3 \neq 5$.*

Listat, lukujonot ja karteesiset tulot funktioina

- *Lista $[a, b, c, d]$ on funktio f, jonka määrittelyjoukko on $\{1, 2, 3, 4\}$ (tai $\{0, 1, 2, 3\}$) siten, että $f(1) = a$, $f(2) = b$, $f(3) = c$ ja $f(4) = d$.*
- *Lukujono $(a_n)_{n=0}^{\infty} = (a_0, a_1, a_2, \ldots)$ on funktio a, jonka määrittelyjoukko on $\mathbb{N}_0$ siten, että $a(n) = a_n$ kaikilla $n \in \mathbb{N}_0$.*
- *Jos X_j on joukko jokaisella $j \in J$ missä J on (toinen) joukko niin karteesinen tulo $\prod_{j \in J} X_j$ on joukko, johon kuuluu täsmälleen kaikki funktiot $f : J \to \bigcup_{j \in J} X_j$ siten, että $f(j) \in X_j$ kaikilla $j \in J$.*

Esimerkki: Funktio, alkukuva, ym.

- *Olkoon f funktio:* $\{1,2,3,4,5\} \to \{1,2,3,4,5\}$ *siten, että* $f(1)=2$, $f(2)=4$, $f(3)=2$, $f(4)=4$ *ja* $f(5)=4$. *Matlab/Octavessa voimme esittää tämän funktion vektorina* `f=[2,4,2,4,4]`.
- *Jos* $A=\{1,2,5\}$ *niin* $f(A)=f^{\to}(A)=\{\,f(x) : x \in A\,\}=\{2,4\}$ *ja voimme laskea tämän komennolla* `f([1,2,5])` *joka antaa tulokseksi* `[2,4,4]` *joka on tulkittava joukkona* $\{2,4\}$.
- *Jos* $B=\{1,2,3\}$ *niin* B*:n alkukuva* $f^{\leftarrow}(B)=\{\,x : f(x) \in B\,\}=\{1,3\}$ *ja voimme laskea tämän komennolla* `find(f==1 | f==2 | f==3)` *tai komennolla* `find(sum(f==[1,2,3]',1))`.
- *Huomaa, että riippumatta siitä miten valitsemme joukon* B *niin aina pätee esimerkiksi* $f^{\leftarrow}(B) \neq \{1\}$ *(eli tässä tapauksessa* $f^{\leftarrow}$ *ei ole surjektio:* $\mathcal{P}(\{1,2,3,4,5\}) \to \mathcal{P}(\{1,2,3,4,5\})$*) koska jos* $2 \notin B$ *niin* $1 \notin f^{\leftarrow}(B)$ *ja jos* $2 \in B$ *niin* $\{1,3\} \subseteq f^{\leftarrow}(B)$.

Esimerkki: Alkukuva ja injektiivisyys

Jos $f : X \to Y$ *on surjektio niin* $f^{\leftarrow} : \mathcal{P}(Y) \to \mathcal{P}(X)$ *on injektio missä* $f^{\leftarrow}(B)=\{\,x \in X : f(x) \in B\,\}$.
Miksi?

- *Jos* $B_1 \neq B_2$ *niin on olemassa* $y \in B_1$ *siten, että* $y \notin B_2$ *tai on olemassa* $y \in B_2$ *siten, että* $y \notin B_1$. *Oletamme nyt, että* $y \in B_1$ *mutta* $y \notin B_2$.
- *Koska* f *on surjektio niin on olemassa* $x \in X$ *siten, että* $f(x)=y$.
- *Tästä seuraa, että* $x \in f^{\leftarrow}(B_1)$ *mutta* $x \notin f^{\leftarrow}(B_2)$ *joten olemme osoittaneet, että jos* $B_1 \neq B_2$ *niin* $f^{\leftarrow}(B_1) \neq f^{\leftarrow}(B_2)$ *eli* $f^{\leftarrow}$ *on injektio.*

Rekursiivinen funktio: Esimerkkinä Fibibonaccin luvut

Määrittelemme funktion F *seuraavasti:*

$$F(n)=\begin{cases}1, & \text{jos } n=1 \text{ tai } n=2,\\ F(n-1)+F(n-2), & \text{jos } n>2.\end{cases}$$

Voidaan osoittaa, että

$$F(n)=\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right),$$

eli `F=@(n)(((1+sqrt(5))/2)^n-((1-sqrt(5))/2)^n)/sqrt(5)`.
Toinen vaihtoehto on laskea funktion arvot suoraan määritelmästä esim. seuraavalla rekursiivisella funktiolla

```
function f=F(n)
  if n==1 || n==2, f=1;
  else f=F(n-1)+F(n-2); end
endfunction
```


Rekursiivinen funktio: Esimerkkinä Fibonaccin luvut. jatk.

Jos haluamme laskea esim luvut $F(1), F(2), F(3), \ldots, F(15)$ *voimme ensin laskea* `F=[1,1];` *ja sitten laskea*
`for j=3:15, F(j)= F(j-1)+F(j-2); end`
Mutta silloin esim. `F(20)` *ei ole lainkaan määritelty.*
Vaihtoehtoisesti voimme muodostaa vektorit $X_n=[X_n(1), X_n(2)]$ *missä* $X_n(1)=F(n-1)$ *ja* $X_n(2)=F(n)$ *jolloin* $X_2=[1,1]$ *ja* $X_n=[F(n-1),F(n)]=[F(n-1),F(n-1)+F(n-2)]=[X_{n-1}(2),X_{n-1}(2)+X_{n-1}(1)]$. *Näin ollen voimme myös kirjoittaa* $X_n=G(X_{n-1})$ *missä* $G(Y)=[Y(2),Y(2)+Y(1)]$. *Nyt voimme laskea vektorit* X_n *seuraavalla tavalla:*
`X(1,:)=[0,1]; X(2,:)=[1,1]; G=@(Y)[Y(2),Y(2)+Y(1)];`
`for n=3:15, X(n,:)=G(X(n-1,:)); end`
jolloin `X(15,:)` *on* $[F(14),F(15)]$.
Jos haluamme vain laskea luvut $F(14)$ *ja* $F(15)$ *voimme menetellä seuraavasti jolloin tuloksena* `X` *on* $[F(14),F(15)]$*:*
`X=[1,1]; G=@(Y)[Y(2),Y(2)+Y(1)];`
`for n=3:15, X=G(X);end`

Monen muuttujan funktiot?

Edellä on käsitelty ainoastaan yhden muuttujan funktioita. Samalla tavalla voidaan määritellä monen muuttujan funktioita, mutta se ei ole aivn välttämätöntä koska näiden funktioiden kohdalla on olemassa erilaisia lähestymistapoja ja seuraavassa esitetään miten tietty kahden muuttujan funktio voidaan määritellä ja sen arvoja laskea eri tavoilla:

- *Kahden muuttujan funktiona:* $f(x,y) = sin(x+3\cdot y)$
  ja Matlab/Octavessa esim. `f=@(x,y)sin(x+3*y)`
  jolloin funktion arvo pisteessä $(1,2)$ *on* `f(1,2)`.
- *Yhden* **vektori***muuttujan funktiona:* $f([x,y]) = \sin(x+3\cdot y)$
  tai esim. `f=@(X)sin(X(1)+3*X(2))`
  jolloin funktion arvo pisteessä $(1,2)$ *on* `f([1,2])`.
- *Yhden (eli ensimmäisen) muuttujan* **funktio***arvoisena funktiona:*
  $x \mapsto (y \mapsto \sin(x+3\cdot y))$
  tai esim. `f=@(x)@(y)sin(x+3*y)`
  jolloin funktion arvo pisteessä $(1,2)$ *on* `f(1)(2)` *(Ei toimi Matlabissa!).*

Esimerkki: Iso-O

- *Jos* $f \in O(n^2)$ *ja* $g \in O(n^3)$ *niin* $f\cdot g \in O(n^5)$ *koska* $|f(n)| \le C_f n^2$ *kun* $n \ge N_f$ *ja* $|g(n)| \le C_g n^3$ *kun* $n \ge N_g$ *joten* $|f(n)g(n)| \le C_f C_g n^{2+3}$ *kun* $n \ge \max(N_f, N_g)$. *Vastaava tulos ei päde jakolaskun kohdalla koska* $O(g)$ *antaa vain ylärajan, ei alarajaa.*
- *Jos* $f(n) = n^2$ *ja* $g(n) = n^3$ *niin* $f \in O(n^2)$, $g \in O(n^3)$ *ja* 5 *on (tietenkin?) pienin luku* p *siten, että* $f\cdot g \in O(n^p)$.
- *Mutta jos* 2 *on pienin luku* p_f *siten, että* $f \in O(n^{p_f})$ *ja* 3 *on pienin luku* p_g *siten, että* $g \in O(n^{p_g})$ *niin siitä ei välttämättä seuraa, että* 5 *olisi pienin luku* p *siten, että* $f\cdot g \in O(n^p)$ *koska voimme esimerkiksi valita*

$$f(n) = \begin{cases} n^2, & n \text{ on pariton} \\ 0, & n \text{ on parillinen,} \end{cases} \quad \text{ja} \quad g(n) = \begin{cases} 0, & n \text{ on pariton} \\ n^3, & n \text{ on parillinen} \end{cases}$$

jolloin $f(n)g(n) = 0$ *kaikilla* n *ja* $f\cdot g \in O(n^p)$ *kaikilla* $p \in \mathbb{Z}$.

Montako vertailua tarvitaan, jotta löytäisimme luvun, jonka suuruusjärjestysnumero on p jos joukossa on n lukua?

Jos $p = 1$ *(pienin luku) tai* $p = n$ *(suurin luku) niin* $n-1$ *vertailua riittää mutta mikä on tilanne yleisessä tapauksessa?*
Seuraavaksi osoitamme, että jos $1 \le p \le n$ *niin tarvittavien vertailujen lukumäärä kuuluu joukkoon* $O(n)$, *eli on olemassa vakio* C *siten, että vertailujen lukumäärä on korkeintaan* Cn *emmekä välitä kovinkaan paljon siitä mikä tämä vakio on:*

- *Oletamme että tarvitaan korkeintaan* Ck *vertailua kun joukossa on* $k < n$ *lukua.*
- *Jaamme luvut osajoukkoihin joissa on* 5 *lukua: Ei vertailuja.*
- *Määritämme näiden osajoukkojen mediaanit:* $O(n)$ *vertailua.*
- *Määritämme mediaanien mediaani:* $C(\frac{1}{5}n+1)$ *vertailua.*
- *Jaamme luvut kahteen joukkoon, riippuen siitä ovatko ne suurempia tai pienempiä kuin mediaanien mediaani:* $O(n)$ *vertailua.*
- *Kumpikin näistä joukoista sisältää korkeintaan* $(1-\frac{1}{5}\cdot\frac{1}{2}\cdot 3)n + O(1) = \frac{7}{10}n + O(1)$ *lukua!*

Montako vertailua tarvitaan, jotta löytäisimme luvun, jonka suuruusjärjestysnumero on p jos joukossa on n lukua?, jatk.

- *Joukkojen alkioiden lukumäärien perusteella tiedämme missä joukossa hakemamme luku on ellei se ole mediaanien mediaani ja mikä sen järjestysnumero siinä on joten haemme sen osajoukosta:* $C\frac{7}{10}n + CO(1)$ *vertailua.*
- *Olemme käyttäneet*

$$O(n) + \frac{1}{5}Cn + C + O(n) + \frac{7}{10}Cn + CO(1) = \frac{9}{10}Cn + CO(1) + O(n) = \frac{9}{10}Cn + (C+n)c_0,$$

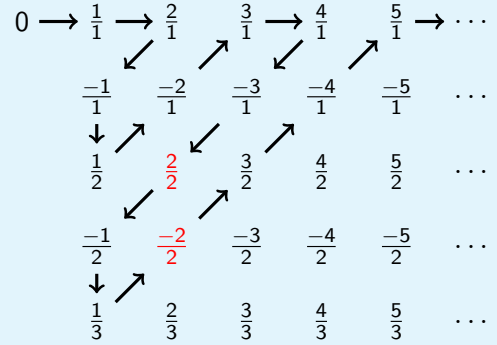
  vertailua missä c_0 *on vakio.*
- *Jos* $n \le 20c_0$ *voimme järjestää luvut käyttäen* $n^2 \le (20c_0)n$ *vertailua (tosiasiassa* $n\log_2(n)$ *vertailua riittää) ja siten löytää hakemamme luku joten jos valitsemme* $C \ge 20c_0$ *jolloin* $c_0 \le \frac{1}{20}C$ *niin kun* $n > 20c_0$ *eli* $c_0 < \frac{1}{20}n$ *toteamme että*

$$\frac{9}{10}Cn + (C+n)c_0 \le \frac{9}{10}Cn + \frac{1}{20}Cn + \frac{1}{20}Cn = Cn$$

  ja induktiopäättely toimii.

$|\mathbb{Z}|$ ja $|\mathbb{Q}|$

- $|\mathbb{N}_0| = |\mathbb{Z}|$ *koska* $f : \mathbb{N}_0 \to \mathbb{Z}$ *missä* $f(0) = 0$, $f(2k-1) = k$ *ja* $f(2k) = -k$ *kun* $k \geq 1$ *on bijektio.*
- $|\mathbb{N}_0| = |\mathbb{Q}|$ *koska voimme konstruoida bijektion seuraavalla tavalla:*



Jos hyppäämme niiden lukujen yli, jotka jo ovat listalla, niin saamme seuraavan bijektion: $f(0) = 0$, $f(1) = 1$, $f(2) = 2$, $f(3) = -1$, $f(4) = \frac{1}{2}$, $f(5) = -2$, $f(6) = 3$, $f(7) = 4$, $f(8) = -3$, $f(9) = -\frac{1}{2}$ *(eikä* $\frac{2}{2} = 1$*)*, $f(10) = \frac{1}{3}$, $f(11) = \frac{3}{2}$ *(eikä* $\frac{-2}{2} = -1$*)*, $f(12) = -4$, *jne.*

Esimerkki: Lokeroperiaate

Olkoon S *joukon* $\{1, 2, \ldots, 2 \cdot n - 1, 2 \cdot n\}$ *osajoukko siten, että* $|S| = n + 1$. *Silloin joukkoon* S *kuuluu kaksi eri lukua* a *ja* b *siten, että joko* a *jakaa* b*:n tai* b *jakaa* a*:n (eli* $a \,|\, b$ *tai* $b \,|\, a$*).*
Miksi?

- *Voimme esittää* S*:n luvut muodossa* $2^{k_j} \cdot q_j$ *missä* $k_j \geq 0$, $1 \leq q_j < 2 \cdot n$, q_j *on pariton,* $j = 1, 2, \ldots, n+1$ *ja lisäksi* $[k_i, q_i] \neq [k_j, q_j]$ *kun* $i \neq j$.
- *Parittomat luvut* q_j, $j = 1, \ldots, n+1$ *kuuluvat joukkoon* $\{1, 2, \ldots, 2 \cdot n - 1, 2 \cdot n\}$.
- *Joukossa* $\{1, 2, \ldots, 2 \cdot n - 1, 2 \cdot n\}$ *on* n *paritonta lukua* $1, 3, 5, \ldots, 2 \cdot n - 1$.
- *Lokeroperiaatteen nojalla on olemassa luvut* $i \neq j$ *siten, että* $q_i = q_j$ *jolloin* $k_i \neq k_j$ *koska* $[k_i, q_i] \neq [k_j, q_j]$.
- *Voimme valita* $a = 2^{k_i} \cdot q_i$ *ja* $b = 2^{k_j} \cdot q_j$ *jolloin väite pätee koska joko* $k_i < k_j$ *jolloin* $a \,|\, b$ *tai* $k_j < k_i$ *jolloin* $b \,|\, a$.

Pari epäyhtälöä

Olkoot A, B *ja* C *kolme joukkoa.*

- *Koska* $A \cap B \cap C \subseteq A \cap B$ *niin* $|A \cap B \cap C| \leq |A \cap B|$. *Samoin pätee* $|A \cap B \cap C| \leq |B \cap C|$ *ja* $|A \cap B \cap C| \leq |A \cap C|$.
- *Koska* $(A \cap B) \cup (A \cap C) = A \cap (B \cup C) \subseteq A$ *niin*

$$|A| \geq |(A \cap B) \cup (A \cap C)| = |A \cap B| + |A \cap C| - |A \cap B \cap A \cap C|,$$

josta seuraa, että

$$|A \cap B \cap C| \geq |A \cap B| + |A \cap C| - |A|.$$

Vaihtamalla A, B *ja* C *keskenään saadaan myös epäyhtälöt* $|A \cap B \cap C| \geq |A \cap B| + |B \cap C| - |B|$ *ja* $|A \cap B \cap C| \geq |A \cap C| + |B \cap C| - |C|$.

Esimerkki: Otokset

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 sille montako paperia sama henkilö voi saada. Silloin valvojat valitsevat 150 *kertaa tenttijän, jolle paperi annetaan, joukosta, jossa on* 160 *alkiota, "palauttaen" eikä valintajärjestyksellä ole merkitystä. Vaihtoehtojen lukumääräksi tulee silloin* $\binom{150 + 160 - 1}{160 - 1} = \frac{309!}{159! \cdot 150!}$.

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

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

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

Huomaa, että kun $m < n$ ei ole surjektioita $A \to B$ joten silloin $\sum_{k=0}^n \binom{n}{k}(-1)^{n-k}k^m = 0$, mikä ehkä ei ole aivan ilmeistä.

Miksi $\sum_{k=0}^n \binom{n}{k}(-1)^{n-k}k^m = 0$ kun $m < n$?

Binomikaavan nojalla pätee $\left(e^t - 1\right)^n = \sum_{k=0}^{n}\binom{n}{k}e^{kt}(-1)^{n-k}$, joten jos $f(t) = \left(e^t - 1\right)^n$ niin

$$f^{(m)}(t) = \sum_{k=0}^{n}\binom{n}{k}e^{kt}(-1)^{n-k}k^m \quad ja \quad f^{(m)}(0) = \sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}k^m.$$

Seuraavaksi osoitamme, että $f^{(k)}(t) = (e^t - 1)^{n-k}p_k(e^t)$ kun $0 \leq k \leq n$ missä p_k on polynomi. Tämä pätee selvästikin kun $k = 0$ jolloin $p_0(x) = 1$ ja jos $f^{(k)}(t) = (e^t - 1)^{n-k}p_k(e^t)$ ja $k < n$ niin

$$f^{(k+1)}(t) = (n-k)(e^t - 1)^{n-k-1}e^t p_k(e^t) + (e^t - 1)^{n-k}p_k'(e^t)e^t = (e^t - 1)^{n-k-1}p_{k+1}(e^t),$$

missä $p_{k+1}(x) = (n-k)xp_k(x) + (x-1)xp_k'(x)$ on myös polynomi. Nyt voimme todeta, että jos $m < n$ niin $f^{(m)}(0) = (e^0 - 1)^{n-m}p_m(0) = 0$ ja väite seuraa.

Esimerkki

Montako erilaista sellaista viiden pelikortin riviä (normaalista 52 kortin pakasta) on olemassa, jossa esiintyy täsmälleen kaksi kuningatarta?

- *Valitsemme ensin ne kaksi paikkaa, joihin kuningattaret tulevat. Vaihtoehtoja on $\binom{5}{2} = 10$.*
- *Sitten valitsemme kuningattaret näihin paikkoihin ja nyt vaihtoehtojen lukumäärä on $4 \cdot 3 = 12$ koska on otettava huomioon missä järjestyksessä ne tulevat.*
- *Lopuksi valitsemme muut kolme korttia 48:n kortin joukosta jolloin vaihtoehtojen lukumääräksi tulee $48 \cdot 47 \cdot 46 = 103776$*
- *Tuloperiaatteen nojalla erilaisten rivien lukumääräksi tulee*

$$10 \cdot 12 \cdot 103\,776 = 12\,453\,120.$$

Montako vertailua tarvitaan järjestämisalgoritmissa?

Jos meillä on n erisuurta luka ja haluamme järjestää ne suuruusjärjestykseen niin on olemassa algoritmi, joka pahimmassakin tapauksessa tekee korkeintaan $n\log_2(n)$ vertailua (esimerkiksi niin, että ensin jaetaan luvut kahteen joukkoon, nämä laitetaan järjestykseen tällä algoritmilla ja sitten joukot yhdistetään niin että järjestys säilyy).
Mutta onko olemassa algoritmi, joka käyttää oleellisesti vähemmän, (esim. $O(n\log(\log(n)))$) vertailuja, pahimmassakin tapauksessa?
Koska voimme järjestää n lukua $n!$ eri tavalla järjestämisalgoritmin pitää pystyä tuottamaan $n!$ eri vastausta. Koska jokaisen vertailun tuloksena on korkeintaan kaksi vaihtoehtoa niin tuloperiaatteen takia algoritmi, joka tekee korkeintaan m vertailua tuottaa korkeintaan 2^m eri vastausta eli jos se toimii, niin pitää olla $2^m \geq n!$ eli $m \geq \log_2(n!)$. Koska

$$\log_2(n!) = \log_2(1 \cdot 2 \cdot \ldots \cdot n) = \sum_{j=1}^{n}\log_2(j) \geq \sum_{j=\lfloor \frac{n}{2} \rfloor}^{n}\log_2(j) \geq \frac{n}{2}\log_2\left(\frac{n}{3}\right) = \frac{n}{2}\log_2(n) - \frac{n}{2}\log_2(3) \geq \frac{n}{3}\log_2(n),$$

kun $n \geq 3^3$ joten oleellisesti parempi tulos kuin $n\log_2(n)$ ei ole mahdollinen.

Monellako tavalla voidaan jakaa joukko, johon kuuluu n alkiota, k:hon ei-tyhjään osajoukkoon?

Toisella tavalla: Monellako tavalla voimme laittaa n numeroitua palloa k:hon identtiseen laatikkoon, siten, että jokaiseen laatikkoon tulee ainakin yksi pallo?
Olkoon tämä lukumäärä $S(n,k)$, ns. Stirlingin (2. lajin) luku. Mitä voimme sanoa näistä luvuista?

- *Selvästikin (?)* $S(n,1) = S(n,n) = 1$ *ja* $S(n,k) = 0$ *jos* $k > n$.
- $S(n,k) = S(n-1,k-1) + kS(n-1,k)$ *kun* $2 \leq k \leq n-1$.
  Miksi? Olkoon x kyseisen joukon tietty alkio. Silloin meillä on kaksi toisiaan poissulkevaa tapausta:
  - $\{x\}$ *on yksi osajoukoista (johon siis ei kuulu muita alkioita):Muut* $n-1$ *alkiota on jaettava* $k-1$*:een ei-tyhjään osajoukkoon ja vaihtoehtojen lukumäärä on* $S(n-1,k-1)$.
  - $\{x\}$ *ei ole yksi osajoukoista: Jaetaan ensin muut* $n-1$ *alkiota k:hon osajoukkoon (*$S(n-1,k)$ *vaihtoehtoa) jonka jälkeen x sijoitetaan johonkin näistä osajoukoista (k vaihtoehtoa) jolloin kaikkien vaihtoehtojen lukumäärä on* $kS(n-1,k)$.

Monellako tavalla voidaan jakaa joukko, johon kuuluu n alkiota, k:hon ei-tyhjään osajoukkoon? Jatk.

- $S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}j^n$.
  Miksi? Voimme numeroida k osajoukkoa $k!$ eri tavalla ja jako ei-tyhjiin numeroituihin osajoukkoihin määrittelee surjektion (koska osajoukot ovat ei-tyhjiä) alkuperäisestä joukosta numeroitujen osajoukkojen muodostamaan joukkoon eli $\mathrm{Sur}(n,k) = k!S(n,k)$ *missä* $\mathrm{Sur}(n,k)$ *on surjektioiden lukumäärä joukosta, jossa on n alkiota joukkoon, jossa on k alkiota.* Sur*-funktiolle johdetun kaavan avulla saamme väiteen.*
- $S(n,n-1) = \frac{1}{(n-1)!}\sum_{j=0}^{n-1}\binom{n-1}{j}(-1)^{k-j}j^n = \binom{n}{2}$.
  Miksi? Kun osajoukkoja on $n-1$ *kappaletta niin yhteen joukkoon tulee kaksi alkiota ja vaihtoehdot eroavat toisistaan ainoastaan siinä, mitkä kaksi alkiota laitetaan samaan osajoukkoon ja joukosta, jossa on n alkiota voidaan valita osajoukko, johon kuuluu kaksi alkiota* $\binom{n}{2}$*:lla eri tavalla.*