MS-A0401 Diskreetin matematiikan perusteet
Yhteenveto ja esimerkkejä ym., osa I

G. Gripenberg

Aalto-yliopisto

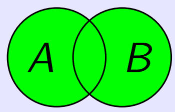
30. syyskuuta 2015

Joukot

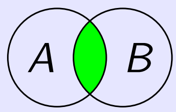
- *Joukko-opissa peruskäsite on $\in$ eli $x \in A$ kun "alkio x kuuluu joukkoon A" ja $x \notin A$ kun "alkio x ei kuulu joukkoon A".*
- *Merkintätapoja:* $\{2, 4, 5, 8\}$ *on joukko jonka alkiot ovat* 2, 4, 5 *ja* 8 *ja* $\{4, 5, \ldots 2014\}$ *on joukko, jonka alkiot ovat kaikki kokonaisluvut j joille pätee* $4 \leq j \leq 2014$.
  $\{\, x \in A : P(x) \,\}$ *tai* $\{\, x : x \in A,\ P(x) \,\}$ *on joukko johon kuluvat ne joukon A alkiot joille väite $P(x)$ on tosi ja yleisemmin* $\{\, \texttt{lauseke} : \texttt{ehto} \,\}$ *on joukko johon kuuluu* `lausekkeen` *antamat alkiot kun* `ehto` *on voimassa, esim.*
  $\{\, x^2 : 2 < x < 10,\ x \text{ on kokonaisluku} \,\} = \{9, 16, 25, \ldots, 81\}$.
- *Tyhjä joukko:* $\emptyset = \{\}$ *on tyhjä joukko johon ei kuulu yhtään alkiota, eli* $x \in \emptyset$ *on aina epätosi.*
- $A = B$ *jos on totta, että* $x \in A$ *jos ja vain jos* $x \in B$*, eli esimerkiksi* $\{1, 2, 2, 3\} = \{3, 2, 1\}$.
- *Ei-negatiiviset kokonaisluvut joukkoina: Jos* $\emptyset$ *"on" luku* 0 *niin* $\{\emptyset\}$ *"on" luku* 1, $\{\emptyset, \{\emptyset\}\}$ *"on" luku* 2, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ *"on" luku* 3 *jne.*

Joukko-opin perusmerkintöjä

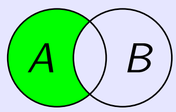
- *Yhdiste tai unioni:* $x \in A \cup B$ *jos ja vain jos* $x \in A$ **tai** $x \in B$.



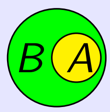
- *Leikkaus:* $x \in A \cap B$ *jos ja vain jos* $x \in A$ **ja** $x \in B$.



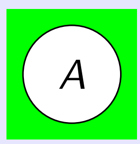
- *Joukkoerotus:* $x \in A \setminus B$ *jos ja vain jos* $x \in A$ **mutta** $x \notin B$.



- *Osajoukko:* $A \subseteq B$ *jos jokainen A:n alkio on myös B:n alkio.*



- *Potenssijoukko:* $\mathcal{P}(A)$ *on joukon kaikkien osajoukkojen muodostama joukko.*
- *Yhtäläisyys:* $A = B$ *jos* $A \subseteq B$ *ja* $B \subseteq A$.
- *Komplementti:* $A^c = \Omega \setminus A$ *jos* $A \subseteq \Omega$ *ja on selvää mikä* Ω *on.*



- *Yhdiste tai unioni:* $x \in \cup_{j \in J} A_j$ *jos ja vain jos* $x \in A_j$ *jollakin* $j \in J$.
- *Leikkaus:* $x \in \cap_{j \in J} A_j$ *jos ja vain jos* $x \in A_j$ *kaikilla* $j \in J$.

Huom!

Usein kirjoitetaan $A \subseteq B$:n sijasta $A \subset B$ ja silloin kirjoitetaan $A \subsetneq B$ kun A on B:n aito osajoukko, eli $A \subseteq B$ mutta $A \neq B$.

Standardimerkintöjä

- $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ *on luonnollisten lukujen (missä* 0 *on mukana) joukko.*
- *Merkinnällä* $\mathbb{N}$ *tarkoitetaan joskus* $\mathbb{N}_0$ *ja joskus* $\{1, 2, 3, \ldots\} = \mathbb{N}_0 \setminus \{0\}$.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ *on kokonaislukujen joukko.*
- $\mathbb{Q} = \{ \frac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0 \}$ *on rationaalilukujen joukko.*
- $\mathbb{R}$ *on reaalilukujen joukko.*

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".

Propositiologiikka eli lausekalkyyli

Jos a ovat b lauseita tai väitteitä, jotka voivat olla tosia tai epätosia mutta ei mitään siltä väliltä niin

- *Lause a* AND *b on tosi kun a on tosi ja b on tosi*
- *Lause a* OR *b on tosi kun a on tosi tai b on tosi (ja myös kun molemmat ovat tosia).*
- *Lause* NOT *a on tosi kun a ei ole tosi eli a on epätosi.*
- *Lause $a \to b$ on tosi kun (*NOT *a)* OR *b on tosi, eli kun b on tosi tai a on epätosi.*
- *Lause $a \leftrightarrow b$ kun $(a \to b)$* AND *$(b \to a)$ on tosi.*

Matemaattisessa logiikassa käytetään yleisesti AND*:n sijasta $\wedge$,* OR*:n sijasta $\vee$ ja* NOT*:n sijasta $\neg$.*

Implikaatio $\to$

Logiikan lause $a \to b$ ei täysin vastaa jokapäiväisen kielenkäytön "jos a niin b" koska se on tosi kun a on epätosi eikä sillä välttämättä ole mitään tekemistä syy-seuraus suhteen kanssa.

Joukot ja implikaatiot: Esimerkkejä

Olkoon $A = \{1, 2, 3, 4\}$, $B = \{0, 3, 4\}$ ja $C = \{x : x$ 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

$$\frac{\begin{array}{l} x \\ x \rightarrow y \end{array}}{y}$$

on tärkeä päättelysääntö ja perustuu siihen, että $(x \text{ AND } (x \rightarrow y)) \rightarrow y$ *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* $a \rightarrow b$ *niin listaan lisätään lause* b*.*

Päättelysäännöt ja todistukset logiikassa

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

(a) $$\frac{\begin{array}{l} x \text{ OR } y \\ \text{NOT } x \end{array}}{y}$$

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

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

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

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.*

Predikaattilogiikka

- *Lause* $\forall x\, P(x)$ *on tosi kun* $P(x)$ *on tosi kaikilla* x.
- *Lause* $\exists x\, P(x)$ *on tosi kun on olemassa* x *siten, että* $P(x)$ *on tosi.*

*Predikaattilogiikka on lausekalkyylin laajennus, jossa operaatioden eli konnektiivien (*NOT , AND, OR, $\rightarrow$ *ja* $\leftrightarrow$*) lisäksi käytetään universaali- ja eksistenssi kvanttorit* $\forall$ *("kaikilla") ja* $\exists$ *("on olemassa"), ja lauseiden lisäksi käytetään muuttujia* $x, y, \ldots$ *ja predikaatteja* $P, Q, \ldots$.
Predikaateilla on äärellinen määrä argumentteja, esim. $P(x)$, $Q(x, y)$, *jne., ja predikaatti joiden argumenttien lukumäärä on* 0 *on lause.*
Predikaattien lisäksi voidaan käyttää funktioita joiden arvot kuuluvat samaan käsiteltävään aihepiiriin ("domain of discourse") kuin muuttujat.
Funktio, jolla ei ole muuttujaa on vakio. Funkiot ja vakiot voidaan esittää predikaattien avulla, mutta se on usein kömpelö vaihtoehto.

Prioriteettijärjestys

Jos ei käytetä sulkuja, joilla tietenkin on korkein prioriteetti, niin loogiset konnektiivit evaluoidaan tavallisesti seuraavassa järjestyksessä: Ensin NOT *, sitten* $\forall$ *ja* $\exists$*, sitten* AND *ja* OR *ja lopuksi* $\rightarrow$ *ja* $\leftrightarrow$*.*

$\forall x \in A$ ja $\exists x \in A$

Lauseet $\forall x \in A\,(P(x))$ *ja* $\exists x \in A\,(P(x))$ *ovat lyhenteitä lauseista*

$$\forall x\,(x \in A \rightarrow P(x)),$$
$$\exists x\,(x \in A \text{ AND } P(x)),$$

ja tarkoittavat (tietenkin) että "kaikilla A:n alkiolla x *pätee* $P(x)$*" ja "on olemassa A:n alkio* x*, jolla* $P(x)$ *pätee".*

Negaatio NOT , konnektiivit AND ja OR sekä kvanttorit $\forall$ ja $\exists$

Kaikilla lauseilla a ja b pätee

$$\text{NOT}\,(a \text{ AND } b) \leftrightarrow (\text{NOT } a) \text{ OR } (\text{NOT } b),$$
$$\text{NOT}\,(a \text{ OR } b) \leftrightarrow (\text{NOT } a) \text{ AND } (\text{NOT } b),$$

eli esimerkiksi NOT $(a$ AND $b)$ *on tosi täsmälleen silloin kun* NOT a OR NOT b *on tosi ja lause* NOT $(a$ AND $b) \leftrightarrow$ NOT a OR NOT b *on tautologia koska se on tosi riippumatta a:n ja b:n totuusarvoista.*
Samoin kaikilla predikaateilla P pätee

$$\text{NOT}\,(\forall x(P(x))) \leftrightarrow \exists x(\text{NOT } P(x)),$$
$$\text{NOT}\,(\exists x(P(x))) \leftrightarrow \forall x(\text{NOT } P(x)).$$

Suora, käänteinen suora ja epäsuora päättely

- *Suorassa päättelyssä johdetaan väite "suoraan" oletuksista.*
- *Jos pitää osoittaa, että oletuksesta a seuraa väite b, niin käänteisessä suorassa, eli kontrapositiivisessa, päättelyssä osoitetaan, että jos väite b ei ole tosi niin silloin oletus a ei myöskään ole tosi. Tämä perustuu siihen että lause $a \to b$ on ekvivalentti lauseen $(\textsc{not}\ b) \to (\textsc{not}\ a)$ kanssa.*
- *Epäsuorassa päättelyssä oletetaan, että väite b ei päde ja johdetaan siitä ristiriita. Tässä siis osoitetaan (annetuilla oletuksilla) että lause $(\textsc{not}\ b) \to (c\ \textsc{and}\ (\textsc{not}\ c))$ on tosi. Mutta tämä lause on $(\textsc{not}\ (\textsc{not}\ b))\ \textsc{or}\ (c\ \textsc{and}\ (\textsc{not}\ c))$ ja koska $(c\ \textsc{and}\ (\textsc{not}\ c))$ on epätosi niin $(\textsc{not}\ (\textsc{not}\ b))$ eli b on tosi.*

Käänteinen suora päättely on erikoistapaus epäsuorasta päättelystä koska ristiriidaksi tulee $a\ \textsc{and}\ (\textsc{not}\ a)$ jos oletetaan, että $a \to b$ ei ole tosi eli $a\ \textsc{and}\ (\textsc{not}\ b)$ on tosi ja osoitetaan, että $(\textsc{not}\ b) \to (\textsc{not}\ a)$ on tosi.

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 *päteekö* $\mathcal{P}(X) \setminus \mathcal{P}(Y) \subseteq \mathcal{P}(X \setminus Y)$ *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*

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

Induktioperiaate

Jos $P(n)$ on väite (joka kaikilla $n \geq n_0$ on joko tosi tai epätosi) ja

(a) *$P(n_0)$ on tosi*

(b) *$P(k+1)$ on tosi jos $P(k)$ on tosi (eli $P(k) \to P(k+1)$ on tosi) kun $k \geq n_0$*

niin $P(n)$ on tosi kaikilla $n \geq n_0$.

Joskus on tarpeen ottaa induktio-oletukseksi väite, että $P(j)$ on tosi kun $n_0 \leq j \leq k$ sen sijaan että pelkästään oletetaan, että $P(k)$ on tosi.

Miksi induktioperiaate toimii?

Olkoon $E = \{\, n \in \mathbb{Z} : n \geq n_0,\ P(n) \text{ ei ole tosi} \,\}$. Oletamme, että E ei ole tyhjä, eli että $P(n)$ ei ole tosi kaikilla $n \geq n_0$. Silloin joukossa E on pienin alkio. Olkoon tämä luku n_1. (a)-kohdan nojalla $n_1 \neq n_0$ joten $n_1 > n_0$ jolloin $k = n_1 - 1 \geq n_0$. Koska n_1 oli pienin alkio joukossa E väite $P(k)$ on tosi jolloin (b)-kohdasta seuraa, että $P(k+1) = P(n_1)$ on tosi. Mutta koska $n_1 \in E$ niin tämä on ristiriita joten oletus, että E ei ole tyhjä ei pidä paikkansa vaan $P(n)$ on tosi kaikilla $n \geq n_0$.

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

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

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

Karteesinen tulo

Kahden joukon X ja Y karteesinen tulo $X \times Y$ on joukko johon kuuluvat kaikki järjestetyt parit $[a, b]$ (tai (a, b)) missä $a \in X$ ja $b \in Y$, eli

$$X \times Y = \{ [a, b] : a \in X \text{ ja } b \in Y \}.$$

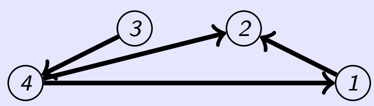
Järjestyn pari $[a, b]$ määritelmäksi otetaan tässä joukko $\{\{a\}, \{a, b\}\}$. (Muitakin mahdollisuuksia on olemassa ja harvoin tätä määritelmää todella joudutaan käyttämään.)

Relaatiot

Relaatio joukosta X joukkoon Y (tai relaatio joukossa X jos $Y = X$) on karteesisen tulon $X \times Y$ osajoukko.

Verkko?

Verkko, eli graafi muodostuu joukosta solmuja ja joukosta niiden väilisiä kaaria (tai linkkejä), esim näin:



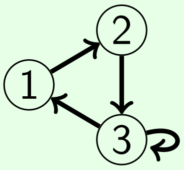
Suunnatussa verkossa jokaisella kaarella on lähtösolmu ja kohdesolmu kun suuntaamattomassa verkossa ei tehdä eroa lähtö- ja kohdesolmun välillä.

- *Suunnattu verkko on järjestetty pari $[V, E]$ ($V =$"vertex", $E =$"edge") missä V on joukko (tavallisesti äärellinen ja ei-tyhjä) ja $E \subset V \times V$, eli E on relaatio joukossa V.*
- *Suuntaamaton verkko on järjestetty pari $[V, E]$ missä V on joukko (tavallisesti äärellinen ja ei-tyhjä) ja $E \subset \{ \{a, b\} : a \in V, b \in V \}$.*

Suuntaamaton verkko voidaan myös ajatella olevan suunnattu verkko missä relaatio E on symmetrinen, eli $[a, b] \in E \to [b, a] \in E$.

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*

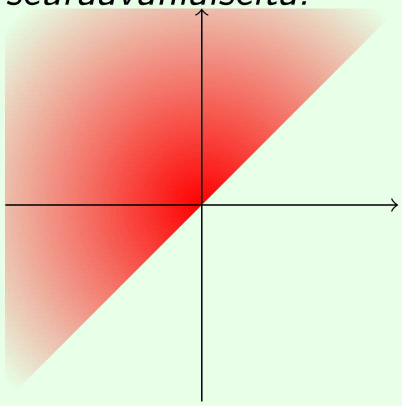


taulukkona

	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:*



Erilaisia relaatioita joukossa X

Relaatio W *joukossa* X *on*

- *refleksiivinen jos* $[x,x] \in W$ *kaikilla* $x \in X$.
- *symmetrinen jos* $[x,y] \in W \to [y,x] \in W$ *kaikilla* x *ja* $y \in X$.
- *transitiivinen jos* $[x,y] \in W$ AND $[y,z] \in W \to [x,z] \in W$ *kaikilla* x, y *ja* $z \in X$.
- *antisymmetrinen jos* $[x,y] \in W$ AND $x \neq y \to [y,x] \notin W$ *eli* $[x,y] \in W$ AND $[y,x] \in W \to x = y$ *kaikilla* x *ja* $y \in X$.
- *asymmetrinen jos* $[x,y] \in W \to [y,x] \notin W$ *kaikilla* x *ja* $y \in X$.
- *totaalinen tai täydellinen jos* $[x,y] \in W$ OR $[y,x] \in W$ *kaikilla* x *ja* $y \in X$.
- **ekvivalenssirelaatio** *jos* W *on refleksiivinen, symmetrinen ja transitiivinen.*
- **osittaisjäjestys** *jos* W *refleksiivinen, antisymmetrinen ja transitiivinen.*

Usein kirjoitetaan $[x,y] \in W$*:n sijasta* xWy *esim.* $x \prec y$ *eikä* $[x,y] \in \prec$.

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 $A \cap B$.

Ekvivalenssiluokat

Jos X on ei-tyhjä joukko ja $\sim$ on ekvivalenssirelaatio joukossa X, eli $\sim$ on refleksiivinen, symmetrinen ja transitiivinen, niin se jakaa joukon X osajoukkoihin $Y_j \neq \emptyset$, $j \in J$ joita kutsutaan ekvivalenssiluokiksi siten, että

- *$\cup_{j\in J} Y_j = X$,*
- *$Y_j \cap Y_k = \emptyset$ jos $j \neq k$,*
- *$a \sim b \leftrightarrow a$ ja b kuuluvat samaan joukkoon Y_j.*

Usein ajatellaan, että kaksi alkiota jotka ovat ekvivalenttia, eli niiden muodostama pari kuuluu relaatioon $\sim$, ovatkin "samat" jolloin joukon X sijasta tarkastellaan joukkoa $\{ Y_j : j \in J \}$, jonka alkiot ovat ekvivalenssiluokat.

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 $m_1 \cdot n_2 = m_2 \cdot n_1$.

Funktiot

Jos X ja Y ovat joukkoja niin funktio $f : X \to Y$ on relaatio joukosta X joukkoon Y eli $X \times Y$:n osajoukko siten, että

- *jokaisella $x \in X$ on olemassa $y \in Y$ siten, että $[x, y] \in f$.*
- *jos $[x, y_1] \in f$ ja $[x, y_2] \in f$ niin $y_1 = y_2$.*

Tavallisesti funktio esitetään siten, että $[x, y] \in f$ jos ja vain jos $y = f(x)$

(vaikka xf tms. voisi olla parempi merkintätapa jos luetaan vasemmalta oikealle).

Toisin sanoen, funktio f joukosta X joukkoon Y on "sääntö", joka jokaisella $x \in X$ antaa vastaukseksi yksikäsitteisen alkion $y = f(x)$ joukosta Y.

- *Jos $f : X \to Y$ on funktio niin X on sen määrittely- eli lähtöjoukko ja Y on sen maalijoukko.*
- *$Y^X = \{ f : f$ on funktio joukosta X joukkoon $Y \}$.*
- *Jos $f : X \to Y$ on funktio ja $A \subset X$ niin $f_{|A} : A \to Y$ on funktio f rajoitettuna joukkoon A eli relaationa $f_{|A} = \{ [x, y] : [x, y] \in f,\ x \in A \}$.*

Anonyymit funktiot

Voidaan puhua esim. luvusta 2 ilman sekaantumisen vaaraa, mutta jos puhutaan lausekkeesta $x + 3$ ei ole välttämättä selvää tarkoitetaanko funktiota, joka antaa tulokseksi argumenttinsa johon on lisätty 3 vai tämän funktion arvo kun argumentti on x. Jos tarkoitetaan funktiota eikä sen arvoa niin voidaan kirjoittaa $x \mapsto x + 3$ tai `@(x)x+2` *tai* `function(x){return x+3;}` *tai jotain muuta vastaavaa.*

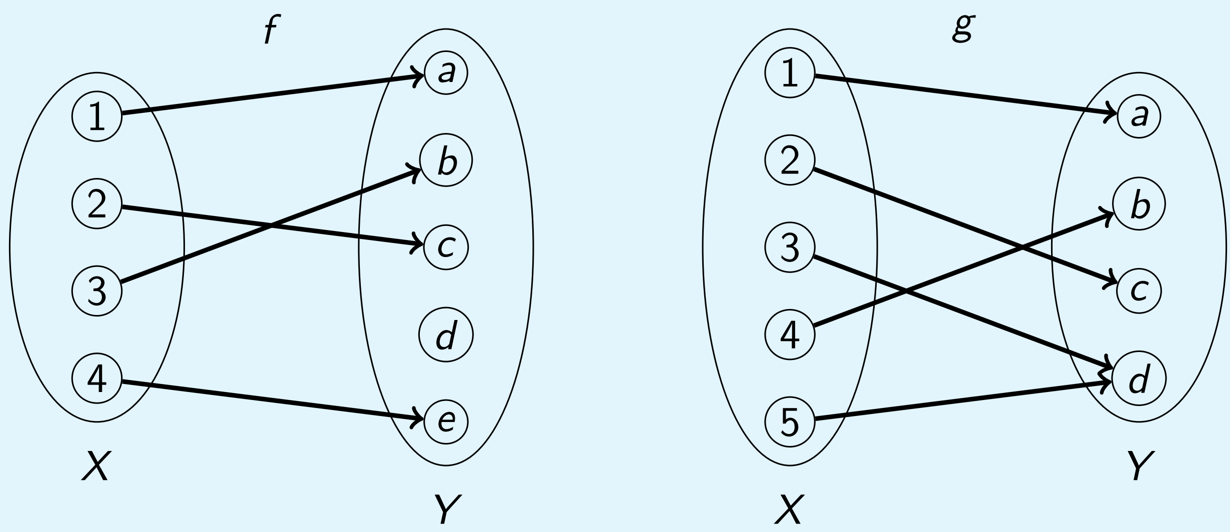
Injektiot, surjektiot ja bijektiot

Funktio $f : X \to Y$ on

- *injektio jos $f(x_1) = f(x_2) \to x_1 = x_2$ kaikilla x_1, $x_2 \in X$.*
- *surjektio jos kaikilla $y \in Y$ on olemassa $x \in X$ siten, että $f(x) = y$.*
- *bijektio jos se on sekä injektio että surjektio.*

Ekvivalentti määritelmä on, että $f : X \to Y$ on injektio jos $x_1 \neq x_2 \to f(x_1) \neq f(x_2)$ kaikilla x_1, $x_2 \in X$ ja f on surjektio jos arvojoukko $f(X) = \{ f(x) : x \in X \}$ on sama kuin maalijoukko Y eli $f(X) = Y$.

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.*

Yhdistetyt funktiot ja käänteisfunktiot

- *Jos* $f : X \to Y$ *ja* $g : Y \to Z$ *ovat kaksi funktiota niin* $h = g \circ f : X \to Z$ *on funktio* $h(x) = g(f(x))$.
- *Jos* $f : X \to Y$, $g : Y \to Z$ *ja* $h : Z \to W$ *ovat funktioita niin* $(h \circ g) \circ f = h \circ (g \circ f)$ *joten tämä funktio voidaan myös kirjoittaa muodossa* $h \circ g \circ f$.
- *Jos* $f : X \to Y$ *sellainen funktio, että on olemassa funktio* $g : Y \to X$ *siten että* $(g \circ f)(x) = x$ *ja* $(f \circ g)(y) = y$ *kaikilla* $x \in X$ *ja* $y \in Y$ *niin* f *on kääntyvä,* g *on* f*:n käänteisfunktio ja tavallisesti kirjoitetaan* $g = f^{-1}$.
- *Funktio* $f : X \to Y$ *on kääntyvä jos ja vain jos se on bijektio.*
- *Jos* $f : X \to Y$ *on kääntyvä niin* $(f^{-1})^{-1} = f$ *eli käänteisfunktio on myös kääntyvä ja sen käänteisfunktio on* f.

Huomaa ,ettei f^{-1} *ole sama funktio kuin* $h(x) = f(x)^{-1}$ *joka edyllyttää että* Y*:n (tai ainakin arvojoukon) elementeillä on kääntееisalkioita mikä on esim. tilanne joukossa* $\mathbb{R} \setminus \{0\}$ *mutta ei joukossa* $\mathbb{Z}$.

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 muttujan 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!)*.

Ordo eli Iso-O: $f \in O(g)$

- *Jos g on funktio, joka on määritelty kaikilla "riittävän isoilla" kokonaisluvuilla niin $f \in O(g)$ kertoo että myös f on määritelty kaikilla "riittävän isoilla" kokonaisluvuilla ja on olemassa vakioita C_f ja N_f siten, että*

$$|f(n)| \leq C_f |g(n)|, \quad n \geq N_f.$$

- *Tämän merkinnän käyttö tarkoittaa myös sitä, ettei ole erityisen oleellista mitä vakiot C_f ja N_f oikeasti ovat tai miten pieniksi niitä voi valita.*
- *Usein kirjoitetaan $f \in O(g)$:n sijasta $f(n) = O(g(n))$ ja silloin merkinnällä $O(g)$ tarkoitetaan jokin funktio f , jolla on se ominaisuus, että $|f(n)| \leq C|g(n)|$ kun $n \geq N$.*
- *Jos $O(n) + O(n^2) \subseteq O(n^2)$ sijasta kirjoitetaan $O(n) + O(n^2) = O(n^2)$ niin pitää muistaa, ettei tästä seuraa $O(n) = 0$!*
- *Tässä käsitellään yksinkertaisuuden vuoksi vain (tietyillä) kokonaisluvuilla märiteltyjä funktioita ja ainoastaan mitä tapahtuu kun $n \to \infty$ mutta se ei ole mitenkään oleellista. Esimerkiksi pätee myös $\frac{x^4 - x^3}{x^3 + x^2} \in O(x)$ kun $x \to 0$.*

Esimerkki: Iso-O

- *Jos $f \in O(n^2)$ ja $g \in O(n^3)$ niin $f \cdot g \in O(n^5)$ koska $|f(n)| \leq C_f n^2$ kun $n \geq N_f$ ja $|g(n)| \leq C_g n^3$ kun $n \geq N_g$ joten $|f(n)g(n)| \leq C_f C_g n^{2+3}$ kun $n \geq \max(N_f, N_g)$. 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*
$$\begin{aligned} O(n) + \frac{1}{5}Cn + C + O(n) + \frac{7}{10}Cn + CO(1) &= \frac{9}{10}Cn + CO(1) + O(n) \\ &= \frac{9}{10}Cn + (C+n)c_0, \end{aligned}$$
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.

Joukon mahtavuus eli alkioiden lukumäärä

- *Kahdella joukolla A ja B on sama lukumäärä alkioita $|A|$ ja $|B|$ eli ne ovat yhtä mahtavia, jos on olemassa bijektio $A \to B$.*
- *Joukolla A on vähemmän tai yhtä monta alkiota kuin joukolla B, eli $|A| \leq |B|$, jos on olemassa injektio $A \to B$. Erityisesti, $|A| \leq |B|$ jos $A \subseteq B$.*
- *Joukolla A on vähemmän alkioita kuin joukolla B, eli $|A| < |B|$, jos on olemassa injektio $A \to B$ mutta ei bijektiota $A \to B$.*
- *Jos $A = \{0, 1, 2, \ldots, n-1\}$ niin $|A| = n$.*
- *Joukko A on äärellinen jos on olemassa $n \in \mathbb{N}_0$ siten, että $|A| = n$.*
- *Joukko A on numeroituva jos $|A| = |\mathbb{N}|$ ja ylinumeroituva jos $|A| > |\mathbb{N}|$.*

Huom!

Jotta nämä määritelmät olisivat järkeviä pitää osoittaa, että on olemassa bijektio $\{0, 1, 2, \ldots, n-1\} \to \{0, 1, 2, \ldots, m-1\}$ jos ja vain jos $m = n$ ja jos on olemassa injektioita $A \to B$ ja $B \to A$ niin löytyy myös bijektio $A \to B$.

$|\mathbb{Z}|$ 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:*

$$
\begin{array}{ccccccccccccc}
0 & \longrightarrow & \frac{1}{1} & \longrightarrow & \frac{2}{1} & & \frac{3}{1} & \longrightarrow & \frac{4}{1} & & \frac{5}{1} & \longrightarrow & \cdots \\
 & & & \swarrow & & \nearrow & & \swarrow & & \nearrow & & & \\
 & & \frac{-1}{1} & & \frac{-2}{1} & & \frac{-3}{1} & & \frac{-4}{1} & & \frac{-5}{1} & & \cdots \\
 & & \downarrow & \nearrow & & \swarrow & & \nearrow & & & & & \\
 & & \frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \frac{5}{2} & & \cdots \\
 & & & \swarrow & & \nearrow & & & & & & & \\
 & & \frac{-1}{2} & & \frac{-2}{2} & & \frac{-3}{2} & & \frac{-4}{2} & & \frac{-5}{2} & & \cdots \\
 & & \downarrow & \nearrow & & & & & & & & & \\
 & & \frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \frac{4}{3} & & \frac{5}{3} & & \cdots
\end{array}
$$

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.

Summaperiaate, yksinkertaisin muoto

Jos A ja B ovat kaksi (äärellistä) joukkoa siten, että $A \cap B = \emptyset$ niin

$$|A \cup B| = |A| + |B|.$$

Tästä seuraa, että jos $B \subseteq A$ niin $|A \setminus B| = |A| - |B|$.

Tuloperiaate, yksinkertaisin muoto

Jos A ja B ovat kaksi (äärellistä) joukkoa niin

$$|A \times B| = |A| \cdot |B|.$$

Lokero- eli kyyhkyslakkaperiaate

Jos $m \geq 1$ esinettä laitetaan $n \geq 1$ lokeroon niin ainakin yhdessä lokerossa on vähintään $\left\lceil \frac{m}{n} \right\rceil$ esinettä!
Miksi? Jos yhdessä lokerossa olevien esineiden lukumäärien maksimi on k niin $k \cdot n \geq m$ joten $k \geq \frac{m}{n}$ ja koska määritelmän mukaan $\lceil \frac{m}{n} \rceil$ on pienin kokonaisluku joka on $\geq \frac{m}{n}$ niin $k \geq \lceil \frac{m}{n} \rceil$.

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 $a \mid b$ tai $b \mid a$).
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 $a \mid b$ tai $k_j < k_i$ jolloin $b \mid a$.*

Seulaperiaate eli yleistetty summaperiaate

Jos A_j, $j = 1, 2, \ldots$ ovat äärellisiä joukkoja niin

$$
\begin{aligned}
|A_1 \cup A_2| &= |A_1| + |A_2| - |A_1 \cap A_2|, \\
|A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| \\
&\quad - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|, \\
\Big|\bigcup_{j=1}^{k} A_j\Big| &= \sum_{r=1}^{k} (-1)^{r+1} \sum_{1 \le j_1 < j_2 < \ldots < j_r \le k} \Big|\bigcap_{i=1}^{r} A_{j_i}\Big|.
\end{aligned}
$$

Pari epäyhtälöä

Olkoot A, B ja C kolme joukkoa.

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

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

  josta seuraa, että

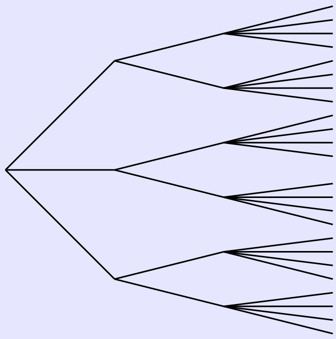
  $$|A \cap B \cap C| \ge |A \cap B| + |A \cap C| - |A|.$$

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

Tuloperiaate

Jos valinta- tai päätösprosessissa on k vaihetta ja vaiheessa j on n_j vaihtoehtoa, riippumatta siitä mitä valintoja tai päätöksiä on aikaisemmissa vaiheissa tehty, ja jos kaikki valinnat johtavat erilaisiin lopputuloksiin, niin kaikkien vaihtoehtojen lukumääräksi tulee

$$n_1 \cdot n_2 \cdot \ldots \cdot n_k$$



$$3 \cdot 2 \cdot 4 = 24$$

Toisin sanoen, jos

$$C = \{\, (x_1, x_2, \ldots, x_k) : x_1 \in A_1,\ x_2 \in A_{2,x_1},\ \ldots, x_k \in A_{k,x_1,\ldots,x_{k-1}} \,\},$$

missä $|A_1| = n_1$, *jokaisella* $x_1 \in A_1$ *pätee* $|A_{2,x_1}| = n_2$ *ja yleisesti jos* $x_1 \in A_1$, $x_2 \in A_{2,x_1}$, $x_3 \in A_{3,x_1,x_2}$ *jne., niin pätee* $|A_{j,x_1,x_2,\ldots,x_{j-1}}| = n_j$, $1 \le j \le k$, *niin silloin* $|C| = n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

Kertoma

Jos n on positiivinen kokonaisluku niin

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n.$$

Lisäksi $0! = 1$.

Binomikerroin

Jos n ja k ovat kokonaislukuja siten, että $0 \le k \le n$ niin

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

jolloin $\binom{n}{k} = \binom{n}{n-k}$.

Multinomikerroin

Jos $n_j \ge 0$ kun $j = 1, 2, \ldots, m$ ja $n = n_1 + n_2 + \ldots n_m$ niin

$$\binom{n}{n_1, n_2, \ldots, n_m} = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_m!}.$$

Järjestetty otos

A on joukko jossa on n alkiota (eli $|A| = n$).

- *Jos valitaan k alkiota joukosta A ja muodostetaan niistä jono $[x_1, x_2, \ldots, x_k]$ ja tehdään tämä* **palauttamatta**, *eli samaa alkiota ei valita monta kertaa jolloin $x_i \neq x_j$ kun $i \neq j$ niin saadaan ns. k-permutaatio. Näiden jonojen eli k-permutaatioiden lukumäärä on tuloperiaatteen nojalla*
$$n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$
- *Jos valitaan k alkiota joukosta A ja muodostetaan niistä jono $[x_1, x_2, \ldots, x_k]$ ja tehdään tämä* **palauttaen**, *eli voidaan valita sama alkio monta kertaa jolloin ainoa vaatimus on, että $x_j \in A$ kun $1 \leq j \leq k$ niin tuloperiaatteen nojalla näiden jonojen lukumäärä on*
$$|A|^k = n^k.$$

Huomaa, että molemmissa tapauksissa on oleellista että kyseessä on järjestetty otos eli sillä, missä järjestyksessä alkiot valitaan A:sta, on merkitystä.

Otos palauttamatta kun järjestystä ei oteta huomioon

Jos joukosta A, jossa on n alkiota, valitaan valitaan osajoukko johon kuuluu k alkiota, eli valitaan k alkiota palauttamatta, (jokaista alkiota voidaan valita korkeintaan kerran), eikä valintajärjestyksellä ole merkitystä niin vaihtoehtojen lukumäärä on

$$\binom{n}{k} = \binom{n}{n-k}.$$

Miksi? Jos kyseinen lukumäärä on $b(n,k)$ niin palauttamatta otettujen järjestettyjen otosten lukumäärä on $b(n,k) \cdot k!$ koska k alkiota voidaan järjestää jonoksi $k!$ eri tavalla. Näin ollen $b(n,k) \cdot k! = \frac{n!}{(n-k)!}$ joten $b(n,k) = \binom{n}{k}$.

Otos palauttaen kun järjestystä ei oteta huomioon

Jos joukosta A, jossa on n alkiota, valitaan k alkiota palauttaen, eli voidaan valita sama alkio monta kertaa, eikä valintajärjestyksellä ole merkitystä niin vaihtoehtojen lukumäärä on

$$\binom{k+n-1}{n-1} = \binom{k+n-1}{k}.$$

Miksi? Olkoon $A = \{x_1, x_2, \ldots, x_n\}$. *Kun valitsemme k alkiota, palauttaen, joukosta A eikä järjestyksellä ole merkitystä niin voimme esittää tuloksen esim. näin:*

$$\underline{*}\ \underline{*}\ \underline{|}\ \underline{*}\ \underline{|}\ \underline{|}\ \underline{*}\ \underline{*}\ \underline{*}\ \underline{|}\ \underline{*}\ \underline{*}\ \underline{|}\ \underline{*}\ \underline{*}\ \underline{|}\ \underline{*}$$

Tämä on tulkittava siten, että olemme kaksi kertaa valinnet x_1*:n, kerran* x_2*:n, ei kertaakaan* x_3*:ta, kolme kertaa* x_4*:n, kaksi kerta* x_5*:n ja kolme kertaa* x_6*:n joten tässä* $n = 6$ *ja* $k = 2+1+0+3+2+3 = 11$.
Jokainen valinta vastaa listaa missä on k alkiota $*$ *ja* $n-1$ *erotusmerkkiä* $|$*, eli pituus on* $k+n-1$*, ja valitsemme jonosta ne* $n-1$ *paikkaa, joihin sijoitamme erotusmerkit* $|$ *jolloin alkiot* $*$ *sijoitetaan jäljelle jääviin paikkoihin (tai päinvastoin). Tämä on otos palauttamatta missä valintajärjestyksellä ei ole merkitystä*

Otos palauttamatta, palauttaen, valintajärjestyksellä merkitystä, ei merkitystä: Yhteenveto

Valitaan k alkiota joukosta, jossa on n alkiota:

	palauttamatta	*palauttaen*
Valintajärjestyksellä on merkitystä	$\frac{n!}{(n-k)!}$	n^k
Valintajärjestyksellä ei ole merkitystä	$\binom{n}{k}$	$\binom{k+n-1}{n-1}$

Allokointimallit eli vaihtoehtoinen ajattelutapa

On sijoitettava k palloa n:ään numeroituun laatikkoon.

- *Numeroidut pallot* $\leftrightarrow$ *Valintajärjestyksellä on merkitystä.*
- *Identtiset pallot* $\leftrightarrow$ *Valintajärjestyksellä ei ole merkitystä.*
- *Jokaiseen laatikkoon korkeintaan yksi pallo* $\leftrightarrow$ *Valinta palauttamatta.*
- *Jokaiseen laatikkoon mielivaltainen määrä palloja* $\leftrightarrow$ *Valinta palauttaen.*

	Pallojen lukumäärä laatikoissa ≤ 1	*ei rajoituksia*
Numeroidut pallot	$\frac{n!}{(n-k)!}$	n^k
Identtiset pallot	$\binom{n}{k}$	$\binom{k+n-1}{n-1}$

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

Multinomikertoimet

$$\binom{n}{n_1, n_2, \ldots, n_m} = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_m!} \qquad n = n_1 + n_2 + \ldots + n_m.$$

- $\binom{n}{n_1, n_2, \ldots, n_m}$ *on vaihtoehtojen lukumäärä kun joukko* A *jaetaan osajoukoiksi* A_j, $j = 1, \ldots, m$ *siten, että* $\cup_{j=1}^{m} A_j = A$, $A_i \cap A_j = \emptyset$ *kun* $i \neq j$, *ja* $|A_j| = n_j$.
- $\binom{n}{n_1, n_2, \ldots, n_m}$ *on vaihtoehtojen lukumäärärä kun järjestetään* n_1 *oliota tyyppiä* y_1, n_2 *tyyppiä* y_2 *jne. missä* $n = n_1 + n_2 + \ldots + n_m$ *ja samaa tyyppiä olevat oliot ovat identtiset.*
- *Jos* A *on joukko, jossa on* n *alkiota ja* $B = \{y_1, \ldots, y_m\}$ *on joukko, jossa on* m *alkiota ja* $n_1, n_2, \ldots, n_m$ *ovat ei-negatiivisia lukuja siten, että* $n_1 + n_2 + \ldots n_m = n$ *niin* $\binom{n}{n_1, n_2, \ldots, n_m}$ *on niiden funktioiden* $f : A \to B$ *lukumäärä joille pätee* $|\{\, x \in A : f(x) = y_j \,\}| = n_j$.

Binomi- ja multinomikaavat

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j},$$

$$(x_1 + \ldots + x_m)^n = \sum_{\substack{n_1 + \ldots + n_m = n \\ n_j \geq 0}} \binom{n}{n_1, n_2, \ldots, n_m} x_1^{n_1} \cdot \ldots \cdot x_m^{n_m}.$$

Miksi? Binomikaava on erikoistapaus multinomikaavasta koska $\binom{n}{j} = \binom{n}{j, n-j}$ *ja multinomikaava pätee koska* $(x_1 + \ldots + x_m)^n$ *voidaan kirjoittaa summana jossa on* m^n *termiä jotka ovat tyyppiä* $y_1 \cdot y_2 \cdot \ldots \cdot y_n$ *missä jokainen* $y_i \in \{x_1, x_2, \ldots, x_m\}$. *Jokainen muotoa* $x_1^{n_1} \cdot \ldots \cdot x_m^{n_m}$ *termi syntyy siitä, että joukko* $\{1, \ldots, n\}$ *jaetaan osajoukkoihin* A_j, $j = 1, \ldots, m$ *siten että* $i \in A_j$ *jos ja vain jos* $y_i = x_j$ *jolloin siis* $|A_j| = n_j$. *Tällaisia osituksia on täsmälleen* $\binom{n}{n_1, n_2, \ldots, n_m}$ *kappaletta.*

Funktioiden lukumäärät

Oletetaan, että $|A| = m$ *ja* $|B| = n$.

- *Funktiodien* $A \to B$ *lukumäärä on* $|B^A| = n^m$.
  Miksi? Funktio $f : A \to B$ *on järjestetty* m*-kokoinen otos palauttaen joukosta jossa on* n *alkiota.*
- *Injektioiden* $A \to B$ *lukumäärä on*
  $n \cdot (n-1) \cdot \ldots \cdot (n-m+1) = \dfrac{n!}{(n-m)!}$, $m \leq n$.
  Miksi? Injektio $A \to B$ *on järjestetty* m*-kokoinen otos palauttamatta joukosta jossa on* n *alkiota.*
- *Surjektioiden* $A \to B$ *lukumäärä on* $\displaystyle\sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} k^m$.

Osajoukkojen lukumäärä: $|\mathcal{P}(A)| = 2^{|A|}$

Jos joukossa A *on* m *alkiota niin joukossa* $\mathcal{P}(A)$ *on* 2^m *alkiota, eli* A*:n osajoukkojen lukumäärä on* $2^{|A|}$ *koska jokaista osajoukkoa* B *vastaa funktio* $f_B : A \to \{0,1\}$ *siten, että* $f_B(x) = 1$ *jos* $x \in B$ *ja muuten* 0.

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

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

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

$$\begin{aligned} f^{(k+1)}(t) = (n-k)(\mathrm{e}^t - 1)^{n-k-1}\mathrm{e}^t p_k(\mathrm{e}^t) + (\mathrm{e}^t - 1)^{n-k}p_k'(\mathrm{e}^t)\mathrm{e}^t \\ = (\mathrm{e}^t - 1)^{n-k-1}p_{k+1}(\mathrm{e}^t), \end{aligned}$$

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* $f^{(m)}(0) = (\mathrm{e}^0 - 1)^{n-m}p_m(0) = 0$ *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.

- $S(n,k) = \dfrac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}j^n.$

  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.*

- $S(n,n-1) = \dfrac{1}{(n-1)!}\sum_{j=0}^{n-1}\binom{n-1}{j}(-1)^{k-j}j^n = \binom{n}{2}.$

  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.