

JOHDATUS

DISKREETTIIN

MATEMATIIKKAAN

SISÄLLYSLUETTELO

LUKU I JOUKOT

1. Joukon määritelmä. Osajoukko, tyhjä joukko, potenssijoukko	1
2. Yhdistys, leikkaus ja erotus.	6
3. Perusjoukko ja komplementti.	11
4. Tulojoukko.	14

LUKU II KUVAUKSET.

1. Relaatiot.	17
2. Kuvaukset.	22
3. Kuvausten ominaisuuksia. Käänteiskuvaus.	25
4. Äärelliset joukot. Joukon koko.	28

LUKU III INDUKTIO.

1. Induktiotodistus.	35
2. Rekursiiviset määritelmät.	42

LUKU IV KERTOMA JA BINOMIKERTOIMET

1. Kertoma.	50
2. Binomikertoimet.	53
3. Stirlingin kaava.	62

LUKU V VERKOT.

1. Verkon määritelmä.	69
2. Pisteiden asteet.	76
3. Kulku verkossa. Yhtenäisyys.	79
4. Puut. Järjestely.	87

Annamme aluksi lukuohjeita loogisille merkeille \wedge , \vee , \Rightarrow , \Leftrightarrow , \forall ja \exists :

$P \wedge Q$ “ P ja Q ”.

$P \vee Q$ “ P tai Q ”.

$P \Rightarrow Q$ “ P :sta seuraa Q ” tai “jos P , niin Q ”.

$P \Leftrightarrow Q$ “ P jos ja vain jos Q ”.

$\forall x$ “jokaisella x ” tai “kaikilla x ”.

$\forall x \in A$ “jokaisella joukon A alkiolla x ”.

$\forall x P(x)$ “jokaisella x on ominaisuus $P(x)$ ” tai “jokainen x toteuttaa ehdon $P(x)$ ”

$\exists x$ “on olemassa x ” tai “jollain x ”.

I. JOUKOT.

I 1. Joukon määritelmä. Osajoukko, tyhjä joukko, potenssijoukko

Joukolla tarkoitamme joidenkin objektien muodostamaa kokonaisuutta A ; kyseiset objektit ovat joukon A *alkioita* ja sanomme, että kukin niistä *kuuluu* joukkoon A . Sanomme myös, että joukko *koostuu* alkioistaan.

Toisinaan puhumme “joukon” asemasta “kokoelmasta”, “luokasta” tai “perheestä” ja “alkion” asemasta “jäsenestä” tai (tilanteen mukaan) esimerkiksi “pisteestä” tai “luvusta”.

Merkinnällä $a \in A$ tarkoitamme, että a on joukon A alkio eli a kuuluu joukkoon A . Jos a ei kuulu joukkoon A , niin merkitsemme $a \notin A$.

Joukon “alkioiden” oletamme olevan (ainakin periaatteessa) “toisistaan erottuvia”. Näin on laita ainakin kaikkien aineellisten olioiden tapauksessa. Esimerkiksi kaikki tämän huoneen ilmassa olevat kaasumolekyylit ovat periaatteessa (muttei käytännössä) erotettavissa toisistaan ja voimme myös “muodostaa” (ajatuksissamme) joukon, jonka alkioina ovat täsmälleen kyseiset molekyylit.

Joukon “muodostaminen” vastaa pelkistetyssä muodossa erästä keskeistä ajattelun elementtiä, abstrahoimista. Kun “alkiot” “kootaan” “joukoksi”, tehdään abstraktio, nousee ylemmälle käsitetasolle.

“Naivissa” joukko-opissa, jota käsittelemme tällä kurssilla, otamme “joukon”, “alkion”, “muodostamisen”, “kuulumisen”, jne., käsitteet tunnettuina ja yritämme kehittää teoriaa, joka on sopusoinnussa intuitiivisen näkemyksemme kanssa.

“Abstraktissa” joukko-opissa ei kanneta huolta käsitteiden intuitiivisesta merkityksestä vaan luotetaan siihen, että annetut aksiomat johtavat joukkoihin, jotka vastaavat intuitiotamme riittävän hyvin. Aksiomat ovat (nk. “valinta-aksiomaa” lukuunottamatta) jokseenkin luonnollisen ja itsestäänselvän tuntuksia perusväitteitä, kuten

Ekstensioaksioma: $A = B \iff \forall x (x \in A \iff x \in B)$

Yhdistysaksioma: $\forall A \forall B \exists C \forall x (x \in C \iff x \in A \vee x \in B)$

Erotteluaksioma: Olkoon $P(x)$ “joukko-opin kaava”, jossa x on ainoa “vapaa” muuttuja. Tällöin $\forall A \exists B \forall x (x \in B \iff x \in A \wedge P(x))$.

Erotteluaksioman tulkinta on, että jokaisen joukon A tapauksessa voimme muodostaa uuden joukon, jonka alkioina ovat täsmälleen ne joukon A alkiot, joilla on “ominaisuus P ”.

Huomautus: *Erotteluaksioman muotoilu osoittaa, miten tarkkana aksiomaattisessa lähestymistavassa on oltava, ettei jouduta ristiriitaan. Alunperin aksioma esitettiin seuraavassa muodossa:*

$$\exists B \forall x (x \in B \iff P(x)).$$

B. Russell huomasi vuonna 1901, että tässä muodossa aksioma johtaa ristiriitaan (“Russellin paradoksi”): olkoon P kaava $x \notin x$ ja olkoon R se joukko, jolle on voimassa $\forall x (x \in R \iff P(x))$. Jos nyt $R \in R$, niin on voimassa $P(R)$ eli $R \notin R$. Jos taas $R \notin R$, niin $P(R)$ ei päde eli on voimassa $R \in R$. Edellisen nojalla saamme ristiriidan: $R \in R$ ja $R \notin R$.

(Tutumpi muotoilu tästä paradoksista on kompakysymys Sevillan parturista.)

Jatkossa unohdamme aksiomat ja käsittelemme pelkästään “naivia” joukko-oppia. Joukon määritelmäksi otamme seuraavan kuvailun:

Joukko on alkoidensa muodostama kokonaisuus.

Huomaa, että naivi määritelmämme antaa ekstensioaksioman: kaksi joukkoa A ja B ovat samat, $A = B$, jos ja vain jos A :lla ja B :llä on samat alkiot.

Merkitsemme joukon “muodostamista” aaltosulkujen avulla, mainitsemalla alkiot sulkujen sisällä. Yksinkertaisissa tapauksissa voimme tässä suoraan luetella joukon alkiot: esimerkiksi $\{a\}$, $\{a, b, c\}$ tai $\{x_1, \dots, x_n\}$. Viimeiselle joukolle otamme käyttöön vaihtoehdoisen merkitsemistävän $\{x_i : i = 1, \dots, n\}$.

Käytämme myös aaltosulkuja muodostaaksemme “vanhoista joukoista uusia”: merkintä

$$\{x \in A : P(x)\}$$

tarkoittaa sitä (erotteluaksioman takaamaa) joukkoa, joka koostuu niistä A :n alkioista, joilla on ominaisuus P .

Edellisen kaltaisen merkinnän avulla voimme kirjoittaa joukon määrittelevän ominaisuuden muotoon $A = \{a : a \in A\}$.

Huomautus: Kukin alkio kuuluu joukkoon “vain yhden kerran” vaikka se alkioiden luettelossa esiintyisikin usemman kerran. Esimerkiksi

$$\{1, 2, 1, 3, 1\} = \{1, 1, 3, 3, 1, 2, 1, 3, 3, 2\} = \{1, 2, 3\}.$$

Otamme seuraavaksi käyttöön omia merkintöjä eräille matematiikassa usein esiintyvillä joukoilla, joiden alkiot ovat lukuja.

Diskreetissä matematiikassa on keskeisellä sijalla

$$\text{luonnollisten lukujen joukko } \mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

Koko matematiikan ehkä tärkein joukko on

$$\text{reaalilukujen joukko } \mathbb{R}.$$

Kaksi muuta tärkeitä lukujoukkoa ovat

$$\text{kokonaislukujen joukko } \mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \text{ ja}$$

$$\text{rationaalilukujen joukko } \mathbb{Q} = \left\{\frac{n}{k} : n, k \in \mathbb{Z} \text{ ja } k \neq 0\right\}.$$

Edellä mainittujen avulla voimme nyt muodostaa uusia joukkoja. Määrittelemme esimerkiksi seuraavasti \mathbb{R} :n *suljetun välin*, jonka *päätepisteinä* ovat reaaliluvut a ja b :

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}.$$

Vastaavasti määrittelemme \mathbb{N} :n *n-segmentin*:

$$[n] = \{1, 2, \dots, n\}.$$

Panemme merkille, että on voimassa $[0] = \emptyset$, $[1] = \{1\}$, $[2] = \{1, 2\}$, jne.

Esimerkki Esitä joukko $\left\{x \in \mathbb{Z} : x \geq \left(\frac{x}{3}\right)^2\right\}$ luettelemalla sen alkioit.

Ratkaisu. Joukossa on vain epänegatiivisia lukuja, koska $\left(\frac{x}{3}\right)^2 \geq 0$ jokaisella $x \in \mathbb{Z}$. Näemme helposti, että 0 on joukon alkio. Joukossa $\{x \in \mathbb{Z} : x > 0\}$ epäyhtälö $x \geq \left(\frac{x}{3}\right)^2$ on yhtäpitävä epäyhtälön $1 \geq \frac{x}{9}$, ja edelleen epäyhtälön $x \leq 9$ kanssa. Täten epäyhtälön toteuttavat 0:n lisäksi vain kokonaisluvut 1, 2, ..., 9. Näin ollen on voimassa

$$\left\{x \in \mathbb{Z} : x \geq \left(\frac{x}{3}\right)^2\right\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}. \quad \square$$

Jos A ja B ovat sellaisia joukkoja, että jokainen joukon B alkio on joukon A alkio, niin sanomme, että B on A :n *osajoukko* ja merkitsemme

$$B \subset A \quad \text{tai vaihtoehtoisesti} \quad A \supset B.$$

Esimerkki (a) $\{1, 3, 12\} \subset \mathbb{N}$

(b) $\{2n : n \in \mathbb{N}\} \subset \mathbb{N}$

(c) $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. (Tämä "sisältymisjono" on lyhennetty merkintä sille, että on voimassa $\mathbb{N} \subset \mathbb{Z}$ ja $\mathbb{Z} \subset \mathbb{Q}$ ja $\mathbb{Q} \subset \mathbb{R}$.)

(d) On voimassa $\{x\} \subset A$ jos ja vain jos on voimassa $x \in A$.

Jos on voimassa $B \subset A$ ja $B \neq A$, niin sanomme, että B on A :n *aito osajoukko* ja käytämme merkintää $B \subsetneq A$.

Esimerkki (a) Edellisen esimerkin (a)-, (b)- ja (c)-kohtien sisältymiset ovat aitoja.

(b) Jokaiselle joukolle A pätee, että $A \subset A$ mutta ei päde, että $A \subsetneq A$.

Lause Kaikille joukoille A, B, C on voimassa

(i) $A \subset A$ ("refleksiivisyys").

(ii) Jos $A \subset B$ ja $B \subset A$, niin $A = B$ ("antisymmetrisyys")

(iii) Jos $A \subset B$ ja $B \subset C$, niin $A \subset C$ ("transitiivisuus")

Todistus. *Refleksiivisyys* pätee triviaalisti.

Antisymmetrisyys. Oletamme, että on voimassa $A \subset B$ ja $B \subset A$. Koska $A \subset B$, jokaiselle x pätee, että jos $x \in A$, niin $x \in B$. Koska $B \subset A$, jokaiselle x pätee, että jos $x \in B$, niin $x \in A$. Näin ollen jokaisella x on voimassa: $x \in A$ jos ja vain jos $x \in B$. Toisin sanoen

$$\forall x (x \in A \iff x \in B).$$

Edellinen merkitsee, että $A = B$.

Transitiivisuus. Oletamme, että on voimassa $A \subset B \subset C$. Nyt jokaiselle x pätee, että jos $x \in A$, niin $x \in B$ (koska $A \subset B$) ja jos $x \in B$, niin $x \in C$ (koska $B \subset C$); tästä seuraa, että jokaiselle x pätee, että jos $x \in A$, niin $x \in C$. Edellisen nojalla on voimassa $A \subset C$. \square

Refleksiivisyydestä ja antisymmetrisyydestä seuraa, että kaikille joukoille A ja B on voimassa

$$A = B \text{ joss } A \subset B \text{ ja } B \subset A.$$

Käytännössä on usein edullista todistaa kahden joukon identtisyys todistamalla sisältyminen “molempiin suuntiin”.

Esimerkki Näytä, että on voimassa $\{2n + 1 : n \in \mathbb{N}\} = \{n \in \mathbb{N} : \frac{n}{2} \notin \mathbb{N}\}$.

Todistus. Merkitsemme $A = \{2n + 1 : n \in \mathbb{N}\}$ ja $B = \{n \in \mathbb{N} : \frac{n}{2} \notin \mathbb{N}\}$. Osoitamme, että on voimassa $A \subset B$ ja $B \subset A$.

$A \subset B$ Olkoon x joukon A alkio. Tällöin on olemassa sellainen $n \in \mathbb{N}$, että $x = 2n + 1$. Nyt $x \in \mathbb{N}$ ja $\frac{x}{2} = n + \frac{1}{2} \notin \mathbb{N}$. Edellisen nojalla $x \in B$.

$B \subset A$ Olkoon x joukon B alkio. Tällöin on voimassa $x \in \mathbb{N}$ ja $\frac{x}{2} \notin \mathbb{N}$. Merkitsemme n :llä osamäärää, jonka saamme kun jaamme lukua x luvulla 2 (esimerkiksi jakokulmassa) ja merkitsemme k :lla jakojäännöstä; tällöin on voimassa $n \in \mathbb{N}, k \in \mathbb{N}, k < 2$ ja $x = n \cdot 2 + k$. Jako ei mene tasan, koska $\frac{x}{2} \notin \mathbb{N}$. Täten on voimassa $k \neq 0$; tästä seuraa, koska $k \in \mathbb{N}$ ja $k < 2$, että $k = 1$. Edellisen nojalla pätee, että $x = 2n + 1$; näin ollen $x \in A$. \square

Tyhjä joukko on se joukko, jolla ei ole yhtään alkioita; tyhjistä joukosta käytämme merkintää \emptyset . *Yksiö* on sellainen joukko, jolla on täsmälleen yksi alkio, eli muotoa $\{a\}$ oleva joukko. *Kaksiö* on muotoa $\{a, b\}$ oleva joukko, missä $a \neq b$, jne.

Tyhjä joukko on jokaisen joukon osajoukko: kun A on joukko, niin

$$\emptyset = \{x \in A : x \neq x\} \subset A.$$

Joukon A kaikki osajoukot muodostavat joukon, jota kutsutaan joukon A *potenssijoukoksi* ja jota merkitään symbolilla $\mathcal{P}(A)$. Siis

$$\mathcal{P}(A) = \{B : B \subset A\}.$$

Potenssijoukossa on (sisällymisen suhteen) “suurin” joukko, nimittäin joukko A ja lisäksi “pienin” joukko, nimittäin tyhjä joukko \emptyset .

Esimerkki (a) Olkoon $A = \{a\}$. Tällöin

$$\mathcal{P}(A) = \{\emptyset, \{a\}\}.$$

(b) Olkoon $B = \{a, b\}$, missä $a \neq b$. Tällöin

$$\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

(b) Olkoon $C = \{1, 2, 3\}$. Tällöin

$$\mathcal{P}(C) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Panemme merkille, että edellisessä esimerkissä esiintyvien joukkojen alkioden lukumäärät ovat seuraavat:

A	$\mathcal{P}(A)$	B	$\mathcal{P}(B)$	C	$\mathcal{P}(C)$
1	2	2	4	3	8

Edellisen valossa näyttää siltä, että kun joukossa E on n alkioita, niin joukon $\mathcal{P}(E)$ alkioden lukumäärä on 2^n . Myöhemmin osoitamme, että tämä tosiaan pätee.

I 2. Yhdistys, leikkaus ja erotus.

Kahden joukon A ja B *yhdistysjoukko* (lyhyesti: A :n ja B :n *yhdiste*) on joukko

$$A \cup B = \{x : x \in A \text{ tai } x \in B\},$$

siis niiden alkioden joukko, jotka kuuluvat joko joukkoon A tai joukkoon B (tai molempiin).

Joukkojen A ja B *leikkausjoukko* (lyhyesti: A :n ja B :n *leikkaus*) on joukko

$$A \cap B = \{x : x \in A \text{ ja } x \in B\},$$

siis niiden alkioden joukko, jotka kuuluvat sekä joukkoon A että joukkoon B .

Joukkojen A ja B *erotusjoukko* (lyhyesti: A :n ja B :n *erotus*) on joukko

$$A \setminus B = \{x : x \in A \text{ ja } x \notin B\} (= \{x \in A : x \notin B\}),$$

siis niiden joukon A alkioden joukko, jotka eivät kuulu joukkoon B (toisinaan puhumme myös *joukon B komplementista joukossa A*).

Esimerkkejä (a) Olkoon $A = \{2, 3, 4, 5\}$ ja $B = \{1, 3, 5, 7\}$. Tällöin

$$A \cup B = \{1, 2, 3, 4, 5, 7\}, A \cap B = \{3, 5\}, A \setminus B = \{2, 4\} \text{ ja } B \setminus A = \{1, 7\}.$$

(b) $\mathbb{Z} \cup \mathbb{Q} = \mathbb{Q}$, $\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}$, $\mathbb{Z} \setminus \mathbb{Q} = \emptyset$ ja $\mathbb{Q} \setminus \mathbb{Z} = \{x \in \mathbb{Q} : x \text{ ei ole kokonaisluku}\}$.

Näemme helposti seuraavien yhtälöiden olevan voimassa:

$$A \cup B = B \cup A, A \cap B = B \cap A,$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Alarivin yhtälöt antavat mahdollisuuden yksinkertaistaa sellaisia lausekkeita, joissa esiintyy vain jompikumpi joukko-operaatioista \cup tai \cap : voimme jättää sulkuumerkit pois ja kirjoittaa alarivin lausekkeiden tilalle $A \cup B \cup C$ ja $A \cap B \cap C$. Vastaavasti voimme lyhentää esimerkiksi lausekkeet $(A \cup (B \cup C)) \cup D$ ja $A \cap (B \cap (C \cap (D \cap E)))$ muotoon $A \cup B \cup C \cup D$ ja $A \cap B \cap C \cap D \cap E$. On huomattava, että sulkuja *ei voi* jättää pois “sekalausekkeista”, sillä esimerkiksi lausekkeet $(A \cap B) \cup C$ ja $A \cap (B \cup C)$ eivät yleensä määritä samaa joukkoa.

Seuraavat “sekalausekkeita” koskevat yhtälöt vaativat hieman perusteluja.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Todistamme vain ensimmäisen yhtälön ja jätämme toisen yhtälön todistuksen harjoitustehtäväksi.

Lause Kaikille joukoille A, B, C on voimassa $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Todistus. $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$ Olkoon x joukon $A \cup (B \cap C)$ alkio. Tällöin on voimassa $x \in A$ tai $x \in B \cap C$; tarkastelemme erikseen näitä kahta tapausta.

Jos $x \in A$, niin on voimassa $x \in A \cup B$ ja $x \in A \cup C$ ja täten $x \in (A \cup B) \cap (A \cup C)$.

Jos taas $x \in B \cap C$, niin on voimassa $x \in B$ ja $x \in C$ ja täten $x \in A \cup B$ ja $x \in A \cup C$, mistä seuraa, että $x \in (A \cup B) \cap (A \cup C)$.

Edellisen nojalla on voimassa $x \in (A \cup B) \cap (A \cup C)$.

$\boxed{(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)}$ Olkoon x joukon $(A \cup B) \cap (A \cup C)$ alkio. Tällöin $x \in A \cup B$ ja $x \in A \cup C$.

Tapauksessa $x \in A$ on voimassa $x \in A \cup (B \cap C)$, joten voimme olettaa, että $x \notin A$. Koska $x \in A \cup B$ ja $x \notin A$, on voimassa $x \in B$ ja vastaavasti, koska $x \in A \cup C$ ja $x \notin A$, on voimassa $x \in C$. Edellisen nojalla on voimassa $x \in B \cap C$ ja täten $x \in A \cup (B \cap C)$. \square

Seuraavat kaksi joukkoyhtälöä tunnetaan *de Morganin lakeina*.

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \quad , \quad A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C).$$

Todistamme vain ensimmäisen de Morganin lain ja jätämme toisen lain todistamisen harjoitustehtäväksi.

Lause Kaikille joukoille A, B, C on voimassa

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C).$$

Todistus. $\boxed{A \setminus (B \cup C) \subset (A \setminus B) \cap (A \setminus C)}$ Olkoon x joukon $A \setminus (B \cup C)$ alkio. Tällöin on voimassa $x \in A$ ja $x \notin B \cup C$. Koska $x \notin B \cup C$, on voimassa $x \notin B$ ja $x \notin C$. Edellisen nojalla pätee, että $x \in A$ ja $x \notin B$ eli että $x \in A \setminus B$ ja myös, että $x \in A$ ja $x \notin C$ eli että $x \in A \setminus C$; näin ollen on voimassa $x \in (A \setminus B) \cap (A \setminus C)$.

$\boxed{(A \setminus B) \cap (A \setminus C) \subset A \setminus (B \cup C)}$ Olkoon $x \in (A \setminus B) \cap (A \setminus C)$. Tällöin on voimassa $x \in (A \setminus B)$ eli $x \in A$ ja $x \notin B$ ja on myös voimassa $x \in (A \setminus C)$ eli $x \in A$ ja $x \notin C$. Koska $x \notin B$ ja $x \notin C$, on voimassa $x \notin (B \cup C)$. Edellä esitetyn nojalla pätee, että $x \in A$ ja $x \notin (B \cup C)$ eli että $x \in A \setminus (B \cup C)$. \square

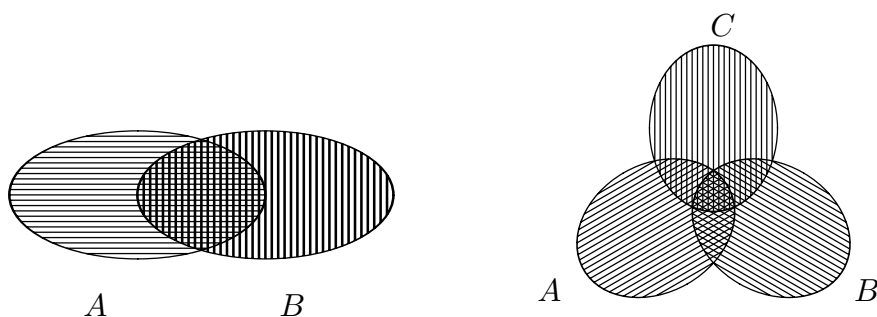
Seuraava tulos luonnehtii sisältymisrelaatiota joukko-operaatioiden avulla.

Lause Seuraavat ehdot ovat keskenään yhtäpitävät joukoille A ja B :

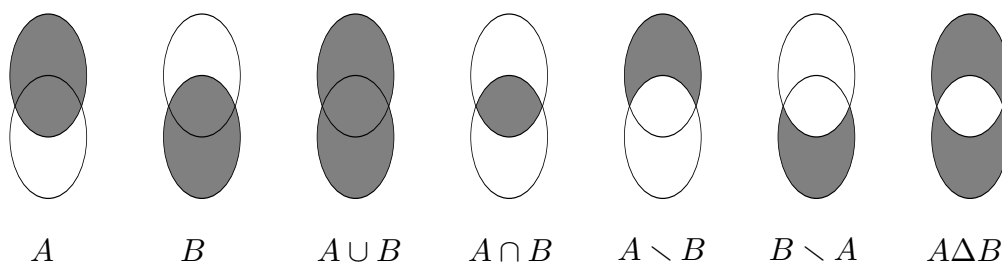
- (i) $A \subset B$.
- (ii) $A \cap B = A$.
- (iii) $A \cup B = B$.
- (iv) $A \setminus B = \emptyset$.

Todistus. Jätämme todistuksen yksityiskohdat lukijalle, mutta huomautamme, että todistus kannattaa tehdä “implikaatioketjun” muodossa. Meidän pitäisi näyttää, että on voimassa $(i) \Leftrightarrow (ii)$, $(i) \Leftrightarrow (iii)$, $(i) \Leftrightarrow (iv)$, $(ii) \Leftrightarrow (iii)$, $(ii) \Leftrightarrow (iv)$ ja $(iii) \Leftrightarrow (iv)$, mutta pääsemme paljon helpommalla, jos todistamme vaikkapa ketjun $(i) \Rightarrow (iii) \Rightarrow (ii) \Rightarrow (iv) \Rightarrow (i)$. Käyttämällä (toistuvasti) lauselogiikan transitiivisuussääntöä $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ (eli nk. “syllogismia”), saamme edellisen ketjun neljästä implikaatiosta $((i) \Rightarrow (iii)$, $(iii) \Rightarrow (ii)$, $(ii) \Rightarrow (iv)$ ja $(iv) \Rightarrow (i)$) johdettua ensin implikaation $(i) \Rightarrow (ii)$ ja sitten implikaation $(i) \Rightarrow (iv)$; vastaavasti “kiertämällä ketjua” jostain muusta kohdasta alkaen, saamme johdettua kaikki mahdolliset implikaatiot $P \Rightarrow Q$, missä P ja Q ovat kaksi lausetta joukosta $\{(i), (ii), (iii), (iv)\}$. Täten saamme neljän implikaation avulla johdettua halutut kuusi ekvivalenssia. \square

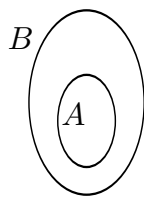
Voimme kätevästi havainnollistaa edellisiä joukkoyhtälöitä ja muitakin kahden tai useamman joukon välisiä suhteita nk. *Vennin kaavioiden* avulla. Voimme esimerkiksi piirtää kahden joukon ja kolmen joukon tapauksiin liittyvät Vennin kaaviot seuraavan näköisiksi.



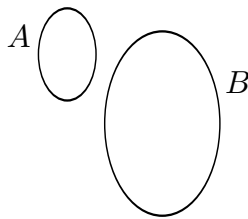
Seuraavassa kuvassa esitämme joukko-operaatiot \cup , \cap , \setminus ja Δ kaavioiden avulla. ($A \Delta B$ on joukkojen A ja B *symmetrinen erotus*; katso harjoitustehtävää 6/1).



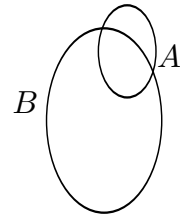
Seuraava kuva esittää eri tapoja, joilla kaksi joukkoa voi “sijaita toisiinsa nähden”.



$$A \subset B$$



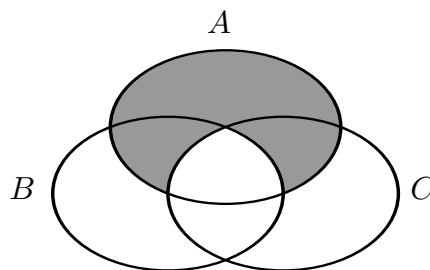
$$A \cap B = \emptyset$$



$$A \not\subset B, B \not\subset A \text{ ja } A \cap B \neq \emptyset$$

Yllä keskimmäisen kuvion tilanteessa, eli ehdon $A \cap B = \emptyset$ vallitessa sanomme, että joukot A ja B ovat *erilliset*; jos $A \cap B \neq \emptyset$, niin sanomme, että A ja B *leikkaavat toisiaan*.

Kaaviot ovat kätevimmillään kolmen joukon tapauksessa. Näemme esimerkiksi helposti, että seuraavassa kuvassa varjostettu alue voidaan määrittää sekä lausekkeella $A \setminus (B \cap C)$ että lausekkeella $(A \setminus B) \cup (A \setminus C)$; täten saamme kuvallisen perustelun toiselle de Morganin laille. Joukkoyhtälöiden “todistukset Vennin kaavioiden avulla” eivät kuitenkaan ole varsinaisia matemaattisia todistuksia, koska ne ovat hyvin huonosti formalisoitavissa. Kuvien varsinainen käyttötarkoitus on joukkoihin liittyvien seikkojen havainnollistaminen, ei niiden täsmällinen matemaattinen perustelu.



Mainitsemme vielä seuraavat yhdistysten ja leikkausten yleistyksset.

Jos \mathcal{A} on *joukkoperhe*, eli sellainen joukko, jonka jokainen alkio on joukko, niin määrittelemme *perheen* \mathcal{A} *yhdistyksen* ja *leikkauksen* kaavoilla

$\bigcup \mathcal{A} = \{x : x \in A \text{ jollain } A \in \mathcal{A}\} \quad \bigcap \mathcal{A} = \{x : x \in A \text{ jokaisella } A \in \mathcal{A}\}.$

Jos I on jokin joukko (“indeksijoukko”) ja A_i on jokin joukko jokaisella $i \in I$, niin määrittelemme *joukkojen* A_i , $i \in I$, *yhdistyksen* ja *leikkauksen* joukkoperheen $\{A_i : i \in I\}$

yhdistyksenä ja leikkauksena:

$$\bigcup_{i \in I} A_i = \bigcup \{A_i : i \in I\} \quad \bigcap_{i \in I} A_i = \bigcap \{A_i : i \in I\}.$$

Esimerkki Jokainen joukko A voidaan esittää sisältämiensä yksiiöiden yhdisteenä:

$$A = \bigcup_{a \in A} \{a\},$$

eli joukkoperheen $\{\{a\} : a \in A\}$ yhdisteenä.

I 3. Perusjoukko ja komplementti.

Toisinaan on luonnollista suorittaa joukko-opillisia tarkasteluja jonkun, tarkastelun yhteydessä kiinteänä pysyvän, “perusjoukon” eli “avaruuden” puitteissa”: jos perusjoukko on X , niin käytämme tarkastelussa vain X :n alkioita, X :n osajoukkoja, X :n osajoukkojen muodostamia “joukkoperheitä”, jne.

Jos tarkastelun perusjoukosta ei ole epäselvyyttä, voimme myös joukkoja muodostaessamme jättää perusjoukon merkitsemättä näkyviin.

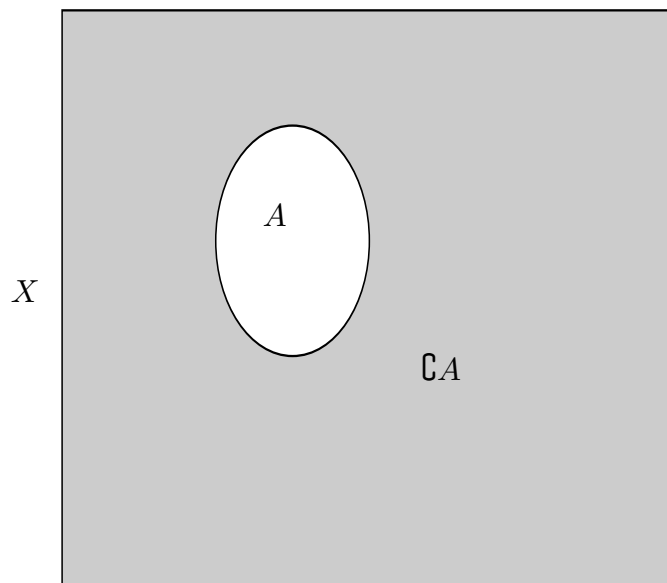
Esimerkkejä (a) Jos esimerkiksi tarkastelemme reaalilukuihin liittyviä asioita, niin merkintä $\{x : x > 0\}$ tarkoittaa positiivisten reaalilukujen joukkoa $\{x \in \mathbb{R} : x > 0\}$.

(b) Jos tarkastelemme kokonaislukuaritmetiikkaa, niin merkintä $\{x : 3 \text{ jakaa } x:n\}$ tarkoittaa kolmella jaollisten kokonaislukujen joukkoa $\{x \in \mathbb{Z} : 3 \text{ jakaa } x:n\}$ eli joukkoa $\{3n : n \in \mathbb{Z}\}$.

Perusjoukon X osajoukon A *komplementti* (perusjoukossa X) on joukko

$$\complement A = \{x \in X : x \notin A\},$$

eli niiden X :n alkioiden joukko, jotka eivät kuulu joukkoon A .



Huomautus Voimme esittää joukon A komplementin perusjoukossa X muodossa

$$\complement A = X \setminus A.$$

Toisaalta voimme esittää perusjoukon osajoukkojen A ja B erotuksen komplementin ja leikkauksen avulla:

$$A \setminus B = A \cap \complement B.$$

Esimerkki Jos $X = \mathbb{Z}$, niin $\complement \mathbb{N} = \{n \in \mathbb{Z} : n < 0\}$.

Komplementti riippuu perusjoukosta:

Esimerkki Olkoon $A = \{2, 3, 4\}$.

Jos perusjoukkona on \mathbb{N} , niin

$$\complement A = \{0, 1, 5, 6, 7, 8, \dots\}.$$

Jos taas perusjoukkona sattuu olemaan \mathbb{R} , niin

$$\complement A = \{x \in \mathbb{R} : x < 2 \text{ tai } 2 < x < 3 \text{ tai } 3 < x < 4 \text{ tai } x > 4\}.$$

Perusjoukko X ja tyhjä joukko \emptyset ovat toistensa komplementteja:

$$\complement X = \{x \in X : x \notin X\} = \emptyset \quad \text{ja} \quad \complement \emptyset = \{x \in X : x \notin \emptyset\} = X.$$

Merkitsemme $\complement \complement A$:llä X :n osajoukon A komplementin $\complement A$ komplementtia. Edellisen nojalla pätee, että

$$\complement \complement X = \complement \emptyset = X \quad \text{ja} \quad \complement \complement \emptyset = \complement X = \emptyset.$$

Tämä pätee yleisesti:

Lause Jokaisella $A \subset X$ on voimassa

$$\boxed{\complement \complement A = A.}$$

Todistus. Jokaisella $x \in X$ on voimassa

$$x \in A \iff x \notin \complement A \iff x \in \complement \complement A. \quad \square$$

Komplementointi liittyy yhdisteet ja leikkaukset toisiinsa seuraavien sääntöjen nojalla.

Lause Perusjoukon X osajoukoille A ja B on voimassa

$$\boxed{\complement(A \cup B) = \complement A \cap \complement B \quad \text{ja} \quad \complement(A \cap B) = \complement A \cup \complement B.}$$

Todistus. Harjoitustehtävä. \square

Panemme lopuksi merkille, että komplementointi “kääntää” sisältymisen:

Lause Perusjoukon X osajoukoille A ja B on voimassa

$$\boxed{A \subset B \iff \complement B \subset \complement A.}$$

Todistus. \implies Oletamme, että on voimassa $A \subset B$. Osoitamme, että $\complement B \subset \complement A$. Olkoon x joukon $\complement B$ alkio. Tällöin $x \notin B$ ja tästä seuraa, että $x \notin A$, koska muussa tapauksessa sisältymisestä $A \subset B$ seuraisi, että $x \in B$, mikä ei pidä paikkaansa. Täten on voimassa $x \notin B \implies x \notin A$ ja näin ollen $\complement B \subset \complement A$.

\impliedby Edellisen nojalla kaikilla $D, E \subset X$ on voimassa $D \subset E \implies \complement E \subset \complement D$. Tästä seuraa, että on voimassa $\complement B \subset \complement A \implies \complement \complement A \subset \complement \complement B$. Koska $\complement \complement A = A$ ja $\complement \complement B = B$, on voimassa $\complement B \subset \complement A \implies A \subset B$. \square

I 4. Tulojoukko.

Kun esitämme joukon alkioidensa luettelon avulla, ei alkioiden luettelujärjestyksellä tai joidenkin alkioiden mahdollisella toistumisella luettelossa ole mitään merkitystä: esimerkiksi

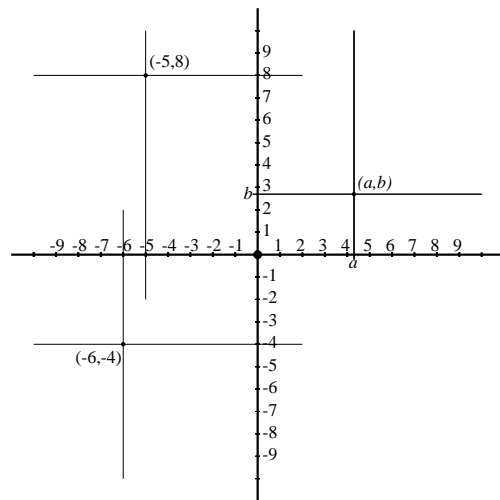
$$\{1, 2, 3\} = \{3, 1, 2\} = \{2, 2, 1, 3, 3, 3, 3\}.$$

Käytännössä joudumme kuitenkin yleensä tarkastelemaan luetteloita, joissa sekä esiintymisjärjestyksellä että toistoilla on olennainen merkitys; tällaisia luetteloita voimme matematiikassa tarkastella *jonojen* avulla.

Kahden alkion muodostamaa jonoa kutsumme *järjestetyksi pariiksi*. Jos alkiot ovat x ja y (tässä järjestyksessä!), niin merkitsemme paria (x, y) :llä. Järjestettyjen parien määrittelevä ominaisuus on seuraava identtisyyskriteerio:

$$(x, y) = (a, b) \iff x = a \text{ ja } y = b.$$

Tyypillinen esimerkki järjestetystä parista on tason piste ilmaistuna suorakulmaisessa koordinaatistossa:



Järjestetyn parin voi helposti määritellä joukkona niin, että yllä esitetty identtisyyssehto toteutuu: yleisesti käytetty määritelmä on $(x, y) = \{\{x\}, \{x, y\}\}$. Tämä määritelmä on kuitenkin varsin keinotekoinen ja tulemme hyvin toimeen ilman täsmällistä määritelmää, joten seuraavassa vain oletamme, että järjestetyt parit on määritelty niin, että identtisyyssehto toteutuu.

Analogisesti analyyttisen geometrian tarkastelujen kanssa voimme nyt määritellä kahden joukon “karteesisen tulon”: olkoot A ja B joukkoja. Joukkojen A ja B *tulojoukko* eli (*karteesinen*) *tulo* on joukko

$$A \times B = \{(x, y) : x \in A \text{ ja } y \in B\}.$$

Tulojoukko $A \times B$ koostuu siis täsmälleen kaikista niistä järjestetyistä pareista (x, y) , joilla on voimassa $x \in A$ ja $y \in B$.

Esimerkki Olkoon $A = \{a, b, c\}$ ja $B = \{1, 2\}$. Tällöin

$$A \times A = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\};$$

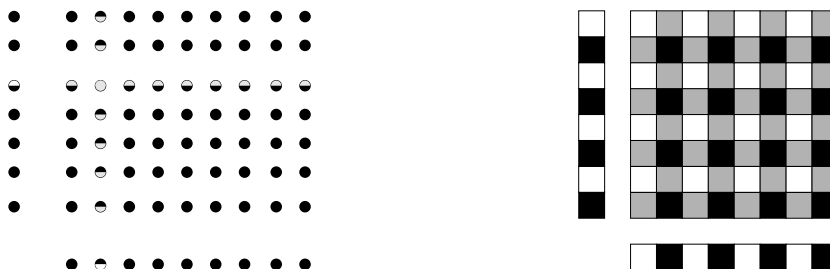
$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\};$$

$$B \times A = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\};$$

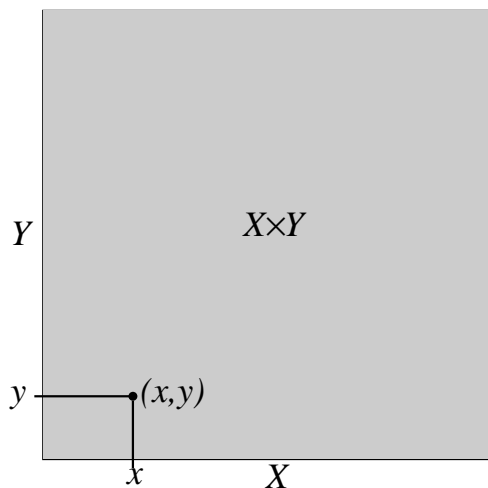
$$B \times B = \{(1, 1), (1, 2), (2, 1), (2, 2)\}.$$

Muotoa $E \times E$ olevalle karteesiselle tulolle käytämme toisinaan potenssimerkintää E^2 .

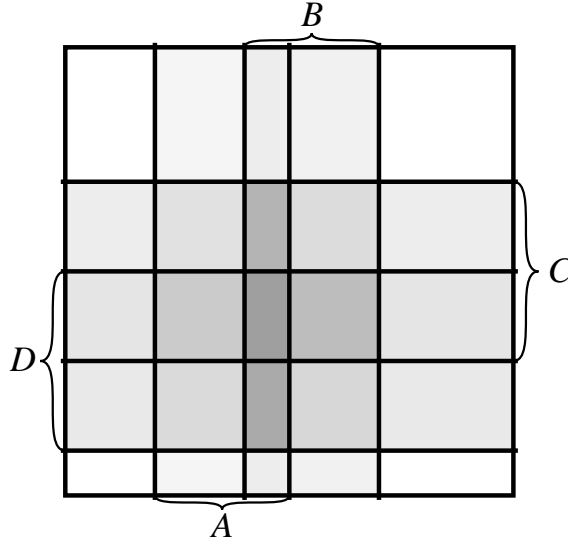
Voimme havainnollistaa karteesisia tuloja vaikkapa seuraavan kaltaisilla kuvioilla:



Yleensä tyydyimme yksinkertaisempiin (ja selkeämpiin) kuviin:



Seuraavan kaavion avulla näemme eräiden joukkoyhtälöiden paikkansapitävyyden.



Edellisestä kaaviosta voimme päätellä esimerkiksi seuraavaa.

$$(A \cup B) \times (C \cup D) = (A \times C) \cup (A \times D) \cup (B \times C) \cup (B \times D).$$

$$(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D).$$

$$(A \setminus B) \times (C \setminus D) = ((A \setminus B) \times C) \cap (A \times (C \setminus D)).$$

$$(A \times C) \setminus (B \times D) = ((A \setminus B) \times C) \cup (A \times (C \setminus D)).$$

Huomaa, että kolmas yhtälö seuraa helposti toisesta. Todistamme esimerkin vuoksi neljännen yhtälön.

Lause Kaikille joukoille A, B, C ja D on voimassa

$$(A \times C) \setminus (B \times D) = ((A \setminus B) \times C) \cup (A \times (C \setminus D)).$$

Todistus.

$$\begin{aligned} (x, y) \in (A \times C) \setminus (B \times D) &\iff (x, y) \in A \times C \wedge (x, y) \notin B \times D \\ &\iff (x \in A \wedge y \in C) \wedge (x \notin B \vee y \notin D) \\ &\iff (x \in A \wedge y \in C \wedge x \notin B) \vee (x \in A \wedge y \in C \wedge y \notin D) \\ &\iff (x \in A \setminus B \wedge y \in C) \vee (x \in A \wedge y \in C \setminus D) \\ &\iff ((x, y) \in (A \setminus B) \times C) \vee ((x, y) \in A \times (C \setminus D)) \\ &\iff (x, y) \in ((A \setminus B) \times C) \cup (A \times (C \setminus D)). \quad \square \end{aligned}$$

II. KUVAUKSET.

II 1. Relaatiot.

Alustava määritelmä: *Relaatio* on kahden (tai useamman, saman tai eri) joukon alkoiden välinen ominaisuus tai suhde.

Esimerkkejä Kokonaisluvut x ja y voivat olla keskenään mm. seuraavissa relaatioissa:
 (a) $y \leq x$ (b) $y|x$ (“ y jakaa $x:n$ ”) (c) $\text{syt}(y, x) = 1$ “ y :llä ja x :llä ei ole yhteisiä tekijöitä”
 (d) $y = 2 + x$

Matematiikassa voimme määritellä relaatiot (kuten monet muutkin asiat) joukkoina.

Määritelmä *Relaatio* on joukko, jonka jokainen alkio on järjestetty pari.

Jos X ja Y ovat joukkoja ja $R \subset X \times Y$, niin R on *joukkojen X ja Y välinen relaatio*.

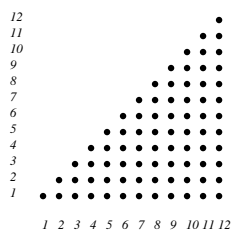
Jos $R \subset X \times X$, niin sanomme myös, että R on *joukon X relaatio*.

Jokainen relaatio R voidaan tulkita kahden joukon väliseksi relaatioksi, sillä on voimassa $R \subset A \times B$, missä $A = \{a : (a, b) \in R \text{ jollain } b\}$ ja $B = \{b : (a, b) \in R \text{ jollain } a\}$.

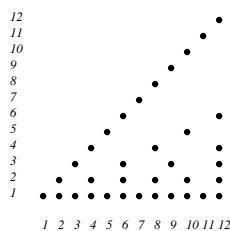
Edellä määritellyt relaatiot ovat nk. *kaksipaikkaisia relaatioita* eli *binäärirelaatioita*. Matematiikassa tarkastellaan toisinaan myös useampipaikkaisia relaatioita, mutta koska emme sellaisia seuraavassa tarvitse, määrittelemme relaatiot vain kaksipaikkaisina.

Esimerkkejä (a) Joukon $X \times X$ *lävistäjä* on relaatio $\Delta_X \subset X \times X$, missä $\Delta_X = \{(x, x) : x \in X\}$. Tämä on sama kuin identtisyysrelaatio X :ssä: $(x, z) \in \Delta_X \iff x = z$.

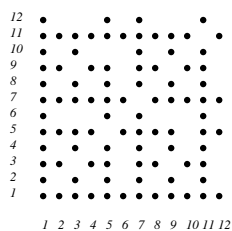
(b) Merkitään X :lla kokonaislukujen $1, 2, \dots, 12$ muodostamaa joukkoa. Edellä mainitut kokonaislukujen väliset relaatiot (a) – (d) vastaavat seuraavia joukon $X \times X$ osajoukkoja:



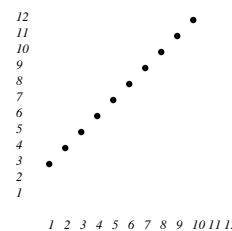
$$y \leq x$$



$$y|x$$



$$\text{syt}(y, x) = 1$$



$$y = 2 + x$$

Relaation määrittely karteesisen tulon osajoukkona ei ole kaikissa tilanteissa luontevaa ja relaatioita esitetään myös monin muin tavoin. Yksi kätevä, vaikkakin epähavainnollinen, esitystapa on *seuraajaluettelo*. Kun R on relaatio, niin kuvaamme toisinaan sitä tilannetta, että $(x, y) \in R$ sanomalla, että y on x :n *seuraaja* relaatiossa R . Voimme esittää relaation $R \subset X \times Y$ luettelemalla jokaisella $x \in X$ ne alkio $y \in Y$, jotka ovat x :n seuraajia R :ssä.

Esimerkki Edellinen relaatio $y|x$ esitettynä seuraajaluetteloiden avulla:

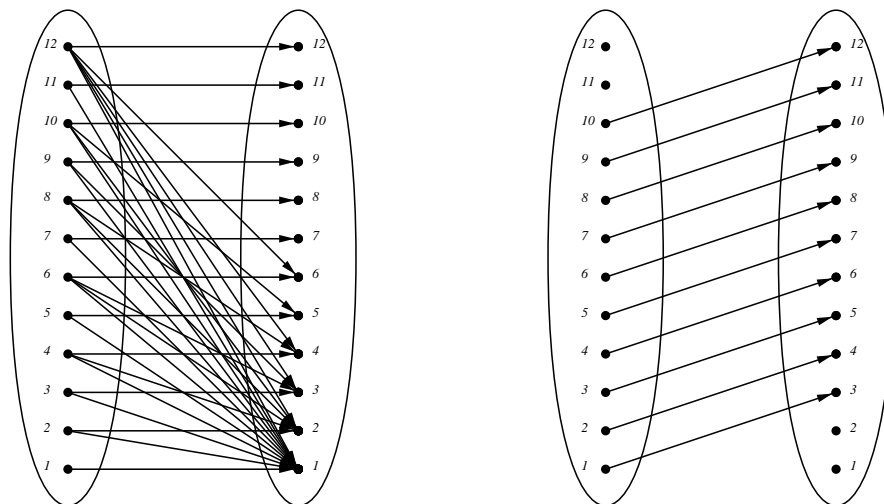
1	1
2	1,2
3	1,3
4	1,2,4

5	1,5
6	1,2,3,6
7	1,7
8	1,2,4,8

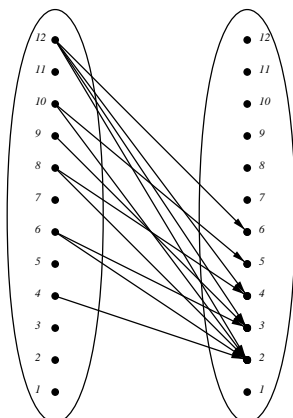
9	1,3,9
10	1,2,5,10
11	1,11
12	1,2,3,4,6,12

Erittäin havainnollinen tapa esittää “pieniä” relaatioita (eli sellaisia, joissa on mukana “vain muutamia” pareja) on *nuolikaavio*: esitämme joukot X ja Y tason pistejoukkoina ja esitämme relaation $R \subset X \times Y$ piirtämällä nuolen pisteestä $x \in X$ pisteeseen $y \in Y$ aina kun $(x, y) \in R$.

Esimerkki Edelliset relaatiot $y|x$ ja $y = x + 2$ nuolikaaviona:

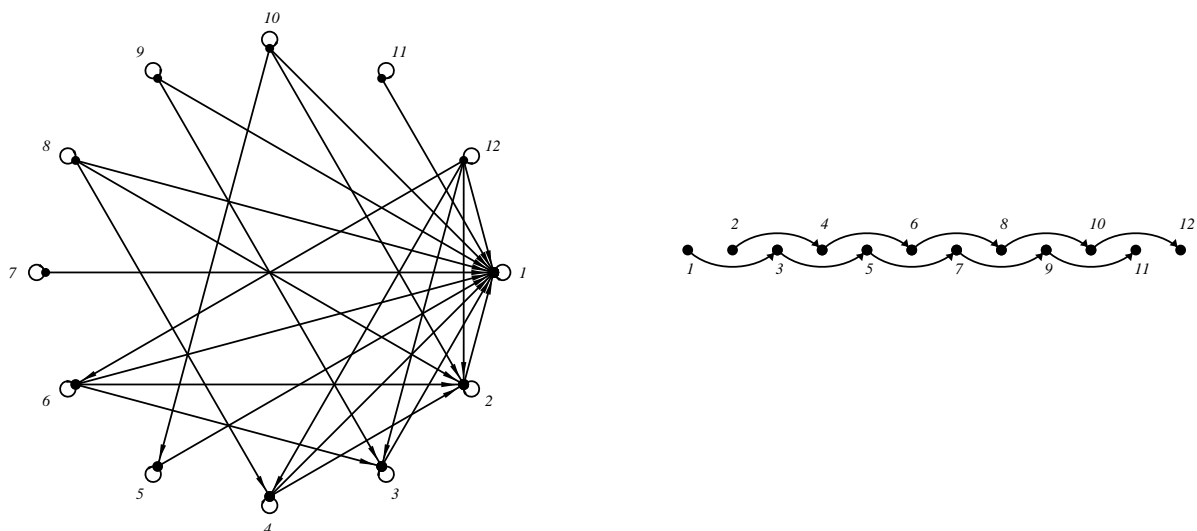


Vasemmanpuolisessa kuviossa on liikaa nuolia, eikä se ole kovin käyttökelpoinen. Jos pitää mielessä, että relaatiossa $y|x$ jokainen luku on itsensä seuraaja ja 1 on jokaisen luvun seuraaja, niin näihin liittyvät nuolet voi jättää merkitsemättä, jolloin kuvioista tulee huomattavasti selkeämpi.



Relaatiolle $R \subset X \times X$ (eli joukon X relaatiolle) voimme antaa vaihtoehdoisen esityksen nuolikaaviona kun panemme merkille, että edellisissä kuvioissa on sama joukko X ($= [12]$) esitetty kahteen kertaan. Voimme yhtä hyvin piirtää kuvaan joukon X vain yhteen kertaan ja voimme silti merkitä kaikki relaatioon liittyvät nuolet näkyviin. Toisinaan tämä johtaa sekavaan kuvioon, josta ei pysty näkemään mitään relaation ominaisuuksia, mutta jos nuolia ei ole liikaa ja jos kuviossa valitaan huolellisesti joukon X alkioita esittävien pisteiden paikat, niin usein saadaan relaatiolle esitys, josta näkee yhdellä silmäyksellä monia relaation ominaispiirteitä.

Esimerkki Vaihtoehdoiset nuolikaaviot joukon $[12]$ relaatioille $y|x$ ja $y = x + 2$.



Kun R on joukkojen X ja Y välinen relaatio ja $x \in X$, $y \in Y$, niin sanomme, että x ja y ovat relaatiossa R jos (ja vain jos) $(x, y) \in R$. Usein merkintä $(x, y) \in R$ korvataan merkinnällä $y R x$.

Jokaisella $A \subset X$ merkitsemme $R(A) = \{y \in Y : \exists a \in A \text{ siten, että } y R a\}$ ja sanomme, että $R(A)$ on *joukon A kuva relaatiossa R* (tai A :n *kuvajoukko R :n suhteen*). Joukon X alkion x käytämme joukosta $R(\{x\})$ lyhennettyä merkintää $R\{x\}$; toteamme, että $R\{x\} = \{y \in Y : y R x\}$.

Yllä annettuja merkintöjä käyttäen on kaikilla $x \in X$ ja $y \in Y$ voimassa

$$(x, y) \in R \iff y R x \iff y \in R\{x\}$$

Edelliset yhtäpitävyydet osoittavat, että relaation $R \subset X \times Y$ määrittämiseksi riittää tuntea kuvajoukot $R\{x\}$, $x \in X$: itse asiassa voimme kirjoittaa $R = \bigcup_{x \in X} \{x\} \times R\{x\}$. Relaatio määritelläänkin usein antamalla siihen kuuluvien järjestettyjen parien asemasta siihen liittyvät yksiöiden kuvajoukot.

Tarkastelemme vielä hieman kuvajoukkojen ominaisuuksia.

Lause *Olkoon R joukkojen X ja Y välinen relaatio ja olkoot A ja B X :n osajoukkoja.*

Tällöin on voimassa

(i) $R(A \cup B) = R(A) \cup R(B)$.

(ii) $R(A \cap B) \subset R(A) \cap R(B)$.

(iii) $R(A \setminus B) \supset R(A) \setminus R(B)$.

Todistus. Todistamme esimerkin vuoksi kohdan (iii) ja jätämme kohtien (i) ja (ii) todistukset harjoitustehtäviksi.

Olkoon $y \in R(A) \setminus R(B)$. Tällöin $y \in R(A)$, joten on olemassa sellainen $a \in A$, että $(a, y) \in R$. Toisaalta $y \notin R(B)$, joten on oltava $a \notin B$. Edellisen nojalla $a \in A \setminus B$; näin ollen $y \in R(A \setminus B)$. \square

Näytämme, että kohtien (ii) ja (iii) sisältymiset voivat olla aitoja.

Esimerkki *Olkoon X kaikkien tällä hetkellä elävien ihmisten joukko ja olkoon L joukon X relaatio: $hLk \iff h$ on k :n lapsi.*

Olkoon *Matti* ja *Maija* Virtasella poika *Kalle*. Tällöin $Kalle \in L\{Matti\} \cap L\{Maija\}$, joten $L\{Matti\} \cap L\{Maija\} \neq \emptyset$. Toisaalta $L(\{Maija\} \cap \{Matti\}) = L(\emptyset) = \emptyset$.

Oletamme, että *Kalle* on *Matti* ja *Maija* Virtasen ainoa lapsi. Tällöin $L\{Matti\} \setminus L\{Maija\} = \{Kalle\} \setminus \{Kalle\} = \emptyset$. Toisaalta $L(\{Matti\} \setminus \{Maija\}) = L(\{Matti\}) = \{Kalle\}$. \square

Joukkojen X ja Y välisistä relaatioista R ja S voimme muodostaa uusia joukkojen X ja Y välisiä relaatioita joukko-operaatioiden avulla: $R \cup S$, $R \cap S$ ja $R \setminus S$ ovat joukkojen X ja Y välisiä relaatioita ja samoin on $\complement R$ kun komplementti on muodostettu perusjoukon $X \times Y$ suhteen.

Jokaiseen relaatioon liittyy myös luonnollisella tavalla “käännetty” relaatio, joka saadaan “kääntämällä” kaikki relaatioon kuuluvat järjestetyt parit.

Olkoon $R \subset X \times Y$ joukkojen X ja Y välinen relaatio. Relaation R *käänteisrelaatio* on joukkojen Y ja X välinen relaatio

$$R^{-1} = \{(y, x) : (x, y) \in R\}.$$

Vaihtoehtoisella merkinnällä ilmaistuna käänteisrelaation määrittelevä ehto on seuraava.

$$xR^{-1}y \iff yRx$$

Esimerkki Olkoot X ja Y ihmisjoukkoja. Merkitsemme L :llä joukkojen X ja Y välistä relaatiota: $yLx \iff y$ on x :n lapsi. Tällöin L^{-1} on joukkojen Y ja X välinen relaatio: $xL^{-1}y \iff x$ on y :n äiti tai isä. \square

Jos relaatio on esitetty nuolikaavion avulla, niin saamme kaaviosta käänteisrelaation nuolikaavion “kääntämällä kaikkien nuolien suunnat”. Mikäli relaatio R on esitetty tason $\mathbb{R} \times \mathbb{R}$ pistejoukkona, niin saamme käänteisrelaation relaation “peilikuvana” suoran $y = x$ suhteen.

Mainitsemme lopuksi eräitä käänteisrelaation ominaisuuksia.

Lause *Kaikille $R, S \subset X \times Y$ on voimassa*

- (a) $(R^{-1})^{-1} = R$.
- (b) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$.
- (c) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$.
- (d) $(R \setminus S)^{-1} = R^{-1} \setminus S^{-1}$.

Todistus. Harjoitustehtävä. \square

II 2. Kuvaukset.

Havainnollisesti “kuvaus” joukolta X joukkoon Y tarkoittaa “vastaavuutta”, “sääntöä”, “lakia” tai vain “luettelo”, joka liittää jokaiseen joukon X alkioon jonkun joukon Y alkion. Jos karsimme tästä intuitiivisesta mielikuvasta pois kaiken epäoleellisen, niin jäljelle jää seuraava idea: kuvaus “liittää” jokaiseen alkioon $x \in X$ täsmälleen yhden alkion $y \in Y$. Jos merkitsemme kuvausta symbolilla f , niin käytämme merkintää $f(x)$ sille yksikäsitteiselle alkion y , jonka f liittää alkioon x .

“Funktio” on vaihtoehtoinen nimitys kuvaukselle. Termiä “funktio” käytetään yleensä “numeerisille kuvauksille” eli kuvauksille joltain joukolta joukolle \mathbb{R} . “Reaalimuuttujan reaalifunktio” on kuvaus f joukolta A joukolle \mathbb{R} , missä $A \subset \mathbb{R}$. Tällaista funktiota f tutkitaan usein sen “kuvaajan” eli “graafin” avulla: f :n *kuvaaja* on tason \mathbb{R}^2 osajoukko $\{(x, f(x)) : x \in A\}$.

Matkimalla kuvaajan ideaa, saamme kätevän koodauksen mielivaltaiselle kuvaukselle: seuraava määritelmä yksinkertaisesti samaistaa kuvauksen sen “kuvaajaan”.

Määritelmä *Kuvaus joukolta X joukkoon Y on sellainen joukon $X \times Y$ osajoukko f , että jokaisella $x \in X$ on olemassa yksi ja vain yksi sellainen $y \in Y$, että $(x, y) \in f$.*

Kuvaus joukolta X joukkoon Y on siis joukkojen X ja Y välinen relaatio.

Kun f on kuvaus joukolta X joukolle Y , niin merkitsemme $f : X \rightarrow Y$; lisäksi määrittelemme jokaisella $x \in X$ joukon Y alkion $f(x)$ kaavalla

$$\boxed{\{f(x)\} = f\{x\} .}$$

Sanomme, että $f(x)$ on x :n *kuva* (tai *kuva-alkio*) kuvauksessa f (voimme myös puhua “funktion f arvosta” alkiolla tai “pisteellä” tai “luvulla” x).

Panemme merkille, että kuvaus $f : X \rightarrow Y$ voidaan esittää muodossa

$$\boxed{f = \{(x, f(x)) : x \in X\} .}$$

Jos f on kuvaus $X \rightarrow Y$, niin kutsumme joukkoa X kuvauksen f *määrittäjäjoukoksi* tai *lähtöjoukoksi* ja joukkoa Y kuvauksen f *maalijoukoksi*.

Koska kuvaus $f : X \rightarrow Y$ on joukkojen X ja Y välinen relaatio, niin jokaiselle $A \subset X$ on määritelty kuvajoukko $f(A) = \{y \in Y : \exists \text{ sellainen } x \in A, \text{ että } (x, y) \in f\}$. Käyttämällä hyväksi kuvauksen ominaisuuksia, saamme kuvajoukolle yksinkertaisemman lausekkeen.

$$f(A) = \{f(a) : a \in A\}.$$

Kuvauksen $f : X \rightarrow Y$ käänteisrelaatio f^{-1} ei yleensä ole kuvaus, mutta se on joukkojen Y ja X välinen relaatio, joten jokaiselle $C \subset Y$ on määritelty kuvajoukko $f^{-1}(C)$; sanomme, että joukko $f^{-1}(C)$ on joukon C *alkukuva* kuvauksessa f . Myös alkukuville saadaan yleisen määritelmän antamaa yksinkertaisempi lauseke.

$$f^{-1}(C) = \{x \in X : f(x) \in C\}.$$

Kuvauksen f *arvojoukko* on joukko

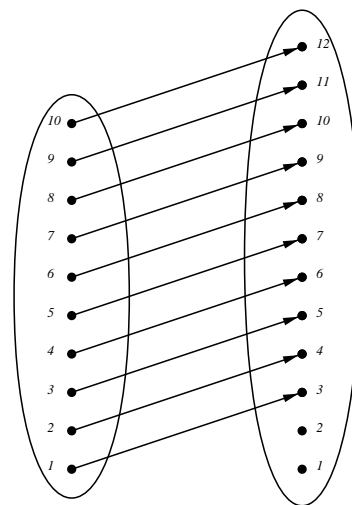
$$f(X) = \{f(x) : x \in X\}.$$

Kuvauksen arvojoukko voi olla kuvauksen maalijoukon aito osajoukko. Sen sijaan kuvauksen määritelmästä seuraa, että kuvauksen “alkuarvojoukko” on aina sama kuin kuvauksen määrittäjäjoukko: kuvaukselle $f : X \rightarrow Y$ on voimassa $f^{-1}(Y) = X$.

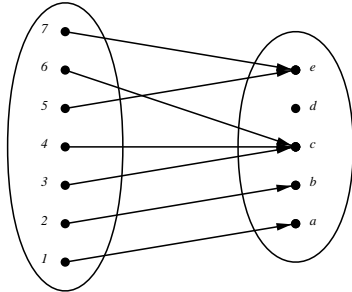
Esimerkki Voimme havainnoida kuvauksia nuolikaavioiden avulla.

(a) Edellä tarkastelimme joukon $[12]$ relaatiota $y = x + 2$. Tämä *ei ole* kuvaus, sillä jos $x = 11$ tai $x = 12$, niin joukossa $[12]$ ei ole sellaista alkioita y , että $y = x + 2$ (sama asia yksinkertaisemmin: $13 \notin [12]$ ja $14 \notin [12]$).

Voimme kuitenkin tarkastella samaa relaatiota $R = \{(x, y) \in [12] \times [12] : y = x + 2\}$ joukkojen $[10]$ ja $[12]$ välisenä relaationa ja tällöin kyseessä on kuvaus $[10] \rightarrow [12]$. Saamme kuvaukselle nuolikaavion muuntamalla hieman aikaisempaa kaaviota:



(b) Jos määrittelemme kuvauksen $f : [7] \rightarrow \{a, b, c, d, e\}$ alla olevalla nuolikaaviolla, niin voimme lukea kuviosta esimerkiksi seuraavat tiedot:



$$f(7) = f(5) = e$$

$$f(\{5, 7\}) = \{e\}$$

$$f(\{1, 2\}) = \{a, b\}$$

$$f^{-1}(\{c\}) = \{3, 4, 6\}$$

$$f^{-1}(\{a, b, e\}) = \{1, 2, 5, 7\}$$

Totesimme edellä, että kuvajoukon muodostaminen relaation suhteen ei aina “säilytä joukko-operaatioita”: saattaa olla voimassa $R(A \cap B) \subsetneq R(A) \cap R(B)$ tai $R(A \setminus B) \supsetneq R(A) \setminus R(B)$. Näin voi käydä myös kuvauksen tapauksessa. Sen sijaan alkukuvan muodostaminen “säilyttää joukko-operaatiot”.

Lause Olkoon $f : X \rightarrow Y$. Tällöin kaikilla $C, D \subset Y$ on voimassa

(i) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

(ii) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

(iii) $f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$.

Todistus. Todistamme esimerkin vuoksi kohdan (iii) ja jätämme kohtien (i) ja (ii) todistukset harjoitustehtäviksi.

$$\begin{aligned} x \in f^{-1}(C \setminus D) &\iff f(x) \in C \setminus D \\ &\iff f(x) \in C \wedge f(x) \notin D \\ &\iff x \in f^{-1}(C) \wedge x \notin f^{-1}(D) \\ &\iff x \in f^{-1}(C) \setminus f^{-1}(D). \quad \square \end{aligned}$$

Panemme merkille, että kuvauksille $f : X \rightarrow Y$ ja $g : Z \rightarrow V$ on voimassa $f \subset g$ jos ja vain jos $X \subset Z$ ja $f(x) = g(x)$ jokaisella $x \in X$. Jos on voimassa $f \subset g$, niin sanomme, että g on kuvauksen f jatke ja f on kuvauksen g rajoittuma.

Olkoon f kuvaus $X \rightarrow Y$ ja $A \subset X$. Kuvauksen f rajoittuma joukkoon A on relaatio $f \cap (A \times Y)$; merkitsemme tätä relaatiota symbolilla $f|A$. Rajoittuma $f|A$ on se kuvaus

$g : A \rightarrow Y$, joka määräytyy ehdosta: $g(a) = f(a)$ jokaisella $a \in A$. Kuvaus f on kuvauksen $f|A$ jatke.

Kuvaukset määräytyvät usein jonkun säännön nojalla, joka määrää kuva-alkion kuvattavan alkion avulla. Esityksen yksinkertaistamiseksi jätämme seuraavassa usein kuvauksen nimeämättä ja viittaamme siihen esittämällä sen säännön, josta kuvaus määräytyy. Voimme esimerkiksi puhua luonnollisten lukujen joukossa \mathbb{N} määritellystä kuvauksesta

$$n \mapsto n + 1$$

kun tarkoitamme sitä kuvausta $f : \mathbb{N} \rightarrow \mathbb{N}$, jolle $f(n) = n + 1$ jokaisella $n \in \mathbb{N}$.

II 3. Kuvausten ominaisuuksia. Käänteiskuvaus.

Määrittelemme nyt eräitä tärkeitä kuvausten ominaisuuksia kuvauksen “säikeiden” avulla. Kun f on kuvaus $X \rightarrow Y$ ja $y \in Y$, niin kutsumme yksiön $\{y\}$ alkukuvajoukkoa $f^{-1}\{y\}$ alkion y säikeeksi kuvauksen f suhteen.

Määritelmä Olkoot X ja Y joukkoja. Kuvaus $f : X \rightarrow Y$ on

- (i) *injektio*, mikäli joukossa $f^{-1}\{y\}$ on korkeintaan yksi alkio jokaisella $y \in Y$.
- (ii) *surjektio*, mikäli joukossa $f^{-1}\{y\}$ on ainakin yksi alkio jokaisella $y \in Y$.
- (iii) *bijektio*, mikäli joukossa $f^{-1}\{y\}$ on täsmälleen yksi alkio jokaisella $y \in Y$.

Voimme luonnehtia näitä ominaisuuksia seuraavilla tavoilla.

Kuvaus f on injektio jos ja vain jos kaikilla $x, z \in X$ pätee, että jos $x \neq z$, niin $f(x) \neq f(z)$ (“mitkään kaksi X :n alkioita eivät kuvaudu samalle Y :n alkiolle”).

Kuvaus f surjektio jos ja vain jos jokainen Y :n alkio on jonkun X :n alkion kuva (eli jos ja vain jos $f(X) = Y$).

Kuvaus f on bijektio jos ja vain jos f on sekä injektio että surjektio.

Esimerkkejä (a) Joukon X identtinen kuvaus id_X on bijektio $X \rightarrow X$.

(b) Kuvaus $x \mapsto x + 1$ on bijektio parillisten luonnollisten lukujen joukosta $\{0, 2, 4, \dots\}$ parittomien luonnollisten lukujen joukkoon $\{1, 3, 5, \dots\}$.

(c) Kuvaus $x \mapsto x + 1$ on injektio $\mathbb{N} \rightarrow \mathbb{N}$, mutta se ei ole surjektio, koska 0 ei ole minkään alkion kuva.

(d) Kuvaus $a \mapsto \{a\}$ on injektio $A \rightarrow \mathcal{P}(A)$ jokaisella joukolla A .

Esimerkki Näytämme, että millään joukolla X ei ole olemassa surjektiota $X \rightarrow \mathcal{P}(X)$.

Todistus. Olkoon X joukko ja olkoon ϕ kuvaus $X \rightarrow \mathcal{P}(X)$. Osoitamme, että ϕ ei ole surjektio.

Merkitsemme $A = \{x \in X : x \notin \phi(x)\}$. Näytämme, että $A \notin \phi(X)$. Teemme vasta- väitteen: on olemassa sellainen $z \in X$, että $\phi(z) = A$. Tarkastelemme kahta mahdollista tapausta ja toteamme, että kumpikin johtaa ristiriitaan.

Tapaus 1° $z \in A$. Tällöin $z \in \phi(z)$ ja A :n määritelmä osoittaa, että $z \notin A$ – ristiriita.

Tapaus 2° $z \notin A$. Tällöin $z \notin \phi(z)$ ja A :n määritelmä osoittaa, että $z \in A$ – ristiriita.

Koska kumpikin kahdesta mahdollisesta eri tapauksesta johti ristiriitaan, vastaväite on väärä ja on voimassa $A \notin \phi(X)$. \square

Määritelmän nojalla kuvaus $f : X \rightarrow Y$ on injektio jos ja vain jos f on bijektio $X \rightarrow f(X)$. Voimme myös luonnehtia injektioita seuraavasti.

Lause *Kuvaus $f : X \rightarrow Y$ on injektio jos ja vain jos f :n käänteisrelaatio f^{-1} on kuvaus $f(X) \rightarrow X$.*

Todistus. Koska $f = \{(x, f(x)) : x \in X\}$, on voimassa $f \subset X \times f(X)$ ja täten edelleen $f^{-1} \subset f(X) \times X$. Näin ollen f^{-1} on kuvaus $f(X) \rightarrow X$, jos ja vain jos jokaisella $y \in f(X)$ joukossa $f^{-1}\{y\}$ on täsmälleen yksi alkio. Täten on voimassa:

$$\begin{aligned} f \text{ on injektio} &\iff (x \neq z \implies f(x) \neq f(z)) \\ &\iff \forall y \in f(X) \exists \text{ täsmälleen yksi sellainen } x \in X, \text{ että } f(x) = y \\ &\iff \forall y \in f(X) \text{ joukossa } f^{-1}\{y\} \text{ on täsmälleen yksi alkio} \\ &\iff f^{-1} \text{ on kuvaus } f(X) \rightarrow X. \quad \square \end{aligned}$$

Seuraus *Kuvaus $f : X \rightarrow Y$ on bijektio jos ja vain jos f :n käänteisrelaatio f^{-1} on kuvaus $Y \rightarrow X$.*

Todistus. *Välttämättömyys.* Jos f on bijektio, niin $f(X) = Y$ ja relaatio f^{-1} on edellisen lauseen nojalla kuvaus $Y \rightarrow X$.

Riittävyys. Oletamme, että relaatio f^{-1} on kuvaus $Y \rightarrow X$. Tällöin kuvaus f on edellisen lauseen nojalla injektio. Lisäksi kuvaus f on surjektio, sillä jos y on Y :n alkio, niin voimme merkitä $x = f^{-1}(y)$, jolloin on voimassa $x \in X$ ja $x f^{-1} y$ eli $y f x$ eli $y = f(x)$. \square

Jos kuvauksen $f : X \rightarrow Y$ käänteisrelaatio f^{-1} on kuvaus $Y \rightarrow X$, niin kutsumme kuvausta f^{-1} kuvauksen f *käänteiskuvaukseksi*. Yllä olevan tuloksen nojalla kuvauksella on käänteiskuvaus jos ja vain jos kuvaus on bijektio. Annamme nyt vaihtoehtoisen luonnehdinnan käänteiskuvaukselle.

Lause Kuvaus $g : Y \rightarrow X$ on kuvauksen $f : X \rightarrow Y$ käänteiskuvaus jos ja vain jos jokaisella $x \in X$ on voimassa $g(f(x)) = x$ ja jokaisella $y \in Y$ on voimassa $f(g(y)) = y$.

Todistus. *Välttämättömyys.* Oletamme, että on voimassa $g = f^{-1}$. Tällöin f on edellisen seurauslauseen nojalla bijektio. Jokaisella $x \in X$ on voimassa $g(f(x)) = x$, koska $x \in f^{-1}\{f(x)\} = g\{f(x)\}$. Toisaalta jokaisella $y \in Y$ on voimassa $f(g(y)) = y$, koska f :n surjektiivisuuden nojalla pätee, että $y \in f(f^{-1}\{y\})$ eli $y \in f(g\{y\})$.

Riittävyys. Oletamme, että jokaisella $x \in X$ on voimassa $g(f(x)) = x$ ja jokaisella $y \in Y$ on voimassa $f(g(y)) = y$. Tällöin kaikille $x \in X$ ja $y \in Y$ on voimassa, että jos $f(x) = y$, niin $g(y) = g(f(x)) = x$ ja myös, että jos $g(y) = x$, niin $f(x) = f(g(y)) = y$. Näin ollen kaikilla $x \in X$ ja $y \in Y$ on voimassa

$$f(x) = y \iff g(y) = x \quad \text{eli} \quad (x, y) \in f \iff (y, x) \in g .$$

Tämä merkitsee sitä, että on voimassa $g = f^{-1}$. \square

Jos kutsumme kuvausta f funktioksi ja jos f :llä on käänteiskuvaus, niin kutsumme sitä yleensä f :n *käänteisfunktiksi*.

Esimerkki Määrittelemme funktiot $f, g : \mathbb{R} \rightarrow \mathbb{R}$ kaavoilla

$$f(x) = x^3 \quad \text{ja} \quad g(x) = \sqrt[3]{x} .$$

Tällöin jokaisella $r \in \mathbb{R}$ on voimassa

$$f(g(r)) = (\sqrt[3]{r})^3 = r \quad \text{ja} \quad g(f(r)) = \sqrt[3]{r^3} = r .$$

Edellisen lauseen nojalla f ja g ovat toistensa käänteisfunktioita. Tästä seuraa aikaisemman lauseen nojalla, että f ja g ovat bijektioita $\mathbb{R} \rightarrow \mathbb{R}$. \square

Edellisen käänteiskuvauksen luonnehdinnan avulla voimme helposti todistaa seuraavan hyödyllisen “bijektioiden yhdistämislauseen”.

Seuraus Olkoot $f : X \rightarrow Y$ ja $g : Y \rightarrow Z$ bijektioita. Tällöin kaavan $h(x) = g(f(x))$ määrittelemä kuvaus on bijektio $X \rightarrow Z$.

Todistus. Määrittelemme kuvauksen $\ell : Z \rightarrow X$ kaavalla $\ell(z) = f^{-1}(g^{-1}(z))$. Osoitamme edellisen lauseen avulla, että ℓ on h :n käänteiskuvaus.

Olkoon $x \in X$. Edellisen lauseen nojalla pätee, että $g^{-1}(g(f(x))) = f(x)$ ja $f^{-1}(f(x)) = x$. Täten on voimassa

$$\ell(h(x)) = f^{-1}(g^{-1}(g(f(x)))) = f^{-1}(f(x)) = x.$$

Olkoon $z \in Z$. Edellisen lauseen nojalla pätee, että $f(f^{-1}(g^{-1}(z))) = g^{-1}(z)$ ja $g(g^{-1}(z)) = z$. Täten on voimassa

$$h(\ell(z)) = g(f(f^{-1}(g^{-1}(z)))) = g(g^{-1}(z)) = z.$$

Edellisen lauseen nojalla ℓ on h :n käänteiskuvaus. Tästä seuraa, että h on bijektio. \square

II 4. Äärelliset joukot. Joukon koko.

Määrittelimme edellä joukon \mathbb{N} osajoukot $[n] = \{1, \dots, n\}$. Panemme merkille, että joukossa $[0] = \emptyset$ ei ole yhtään alkioita, joukossa $[1] = \{1\}$ on yksi alkio, joukossa $[2] = \{1, 2\}$ kaksi, joukossa $[3] = \{1, 2, 3\}$ kolme, ja yleisesti, joukossa $[n] = \{1, 2, \dots, n\}$ on n alkioita. Tämän ominaisuuden vuoksi voimme käyttää joukkoja $[n]$ "mittatikkuina", joiden avulla määritämme eräiden muiden joukkojen "koko" eli alkioden lukumäärää.

Koon mittaamisessa voimme käyttää hyväksi bijektioita. Näemme esimerkiksi, että joukoissa $\{a, b, c, d, e\}$ ja $\{h, i, j, k, l\}$ on sama määrä alkioita, koska on olemassa yksi-yhteen vastaavuus näiden joukkojen alkioden välillä, kuten vaikkapa $a \leftrightarrow l$, $b \leftrightarrow k$, $c \leftrightarrow j$, $d \leftrightarrow i$ ja $e \leftrightarrow h$; toisin sanoen, koska on olemassa bijektio $\{a, b, c, d, e\} \rightarrow \{h, i, j, k, l\}$.

Yhdistämällä edelliset kaksi ideaa päädyimme yrittämään seuraavaa: pyrimme määrittämään joukon A koon löytämällä sopivan luonnollisen luvun n ja bijektio $[n] \rightarrow A$. Kohtaamme tässä kaksi ongelmaa: tuollaista lukua n ei välttämättä löydy ja vaikka löytyisi, ei ole itsestäänselvää, että kyseinen luku on yksikäsitteinen. Jälkimmäinen ei ole todellinen ongelma, mutta edellinen on; tästä syystä joudumme rajoittamaan "mitattavien" joukkojen luokkaa.

Määritelmä Joukko X on *äärellinen*, mikäli jollain $n \in \mathbb{N}$ on olemassa bijektio $[n] \rightarrow X$. Jos X ei ole äärellinen, niin sanomme, että X on *ääretön*.

Koska bijektioon käänteiskuvaus on bijektio, joukko X on äärellinen jos ja vain jos jollain $n \in \mathbb{N}$ on olemassa bijektio $X \rightarrow [n]$.

Koska identtinen kuvaus on bijektio joukolta itselleen, näemme että joukot $[n]$ ovat äärellisiä. Erityisesti, tyhjä joukko $[0]$ on äärellinen. Myös jokainen yksiö $\{a\}$ on äärellinen, sillä ehto $1 \mapsto a$ määrittelee bijektio $[1] \rightarrow \{a\}$.

Todistamme nyt että bijektioita $[n] \rightarrow A$ voi olla olemassa vain yhdellä $n \in \mathbb{N}$. Tarvitsemme tähän aputulosta, jonka todistus perustuu seuraavaan luonnollisten lukujen ominaisuuteen (kyseessä on *induktioperiaatteen* yleinen muoto):

- *Jokaisessa \mathbb{N} :n epätyhjässä osajoukossa on pienin luku.*

Lemma Olkoot $n, k \in \mathbb{N}$ ja $k < n$. Tällöin ei ole olemassa injektiota $[n] \rightarrow [k]$.

Todistus. Meidän on osoitettava, että joukko

$$A = \{n \in \mathbb{N} : \exists \text{ injektio } [n] \rightarrow [k] \text{ jollain } k < n\}$$

on tyhjä. Teemme vastaväitteen: on voimassa $A \neq \emptyset$.

Yllä mainitun induktioperiaatteen nojalla on olemassa sellainen luku $m \in A$, että $m \leq n$ jokaisella $n \in A$. Koska $m \in A$, on olemassa $k < m$ ja injektio $\phi : [m] \rightarrow [k]$. Panemme merkille, että on voimassa $k > 0$ (koska $m > k \geq 0$ ja on olemassa kuvaus $[m] \rightarrow [k]$). Määrittelemme nyt kuvauksen $\psi : [m-1] \rightarrow [k]$ seuraavasti. Jos on voimassa $k \notin \phi([m-1])$, niin valitsemme ψ :ksi rajoittumakuvauksen $\phi|_{[m-1]}$. Mikäli on olemassa sellainen $i \in [m-1]$, että $\phi(i) = k$, niin määrittelemme kuvauksen ψ asettamalla $\psi(i) = \phi(m)$ ja $\psi(j) = \phi(j)$ jokaisella $j \neq i$. Näemme helposti, että molemmissa tapauksissa kuvaus ψ on injektio $[m-1] \rightarrow [k-1]$. Tästä seuraa, että on voimassa $m-1 \in A$, mutta tämä on ristiriidassa luvun m minimaalisuusominaisuuden kanssa. Täten vastaväite on väärä ja on voimassa $A = \emptyset$. \square

Lause Kun A on äärellinen joukko, niin vain yhdellä $n \in \mathbb{N}$ on olemassa bijektio $[n] \rightarrow A$.

Todistus. Teemme vastaväitteen: on olemassa sellaiset luonnolliset luvut n ja k , että $k < n$ ja on olemassa bijektiot $f : [n] \rightarrow A$ ja $g : [k] \rightarrow A$. Kuvaus g^{-1} on bijektio $A \rightarrow [k]$ ja voimme määritellä kuvauksen $h : [n] \rightarrow [k]$ kaavalla $h(i) = g^{-1}(f(i))$. Bijektioiden

yhdistämislauseen nojalla h on bijektio $[n] \rightarrow [k]$. Tämä on kuitenkin ristiriidassa edellisen lemmän kanssa. \square

Olkoon A äärellinen joukko. Käytämme edellisen lauseen yksikäsitteiseksi todistamasta luvusta n merkintää $|A|$ (“ A :n alkioiden lukumäärä” tai “ A :n koko”). Kun $|A| = n > 0$, niin voimme esittää joukon A muodossa $A = \{a_1, \dots, a_n\}$: asetamme $a_i = \varphi(i)$ jokaisella $i \in [n]$, kun φ on bijektio $[n] \rightarrow A$.

Kun A on äärellinen joukko ja $|A| = n$, niin sanomme, että A on n -joukko tai n -alkioinen joukko. Käytämme seuraavassa sekä merkintää “ $|B| = n$ ” että sanontoja “ B on n -joukko” ja “ B on n -alkioinen joukko” lyhennyksenä ilmaisulle “ B on äärellinen joukko ja n on luonnollinen luku, jolle on voimassa $|B| = n$ ”.

Tyhjä joukko on ainoa 0-joukko. Yksiö on sama asia kuin 1-joukko. Jokaisella $n \in \mathbb{N}$ on voimassa $|[n]| = n$, koska joukon identtinen kuvaus on aina bijektio joukolta itselleen.

Osoitamme nyt, että joukkojen välinen bijektio “säilyttää” joukkojen äärellisyyden ja niiden koon.

Lause *Olkoot A ja B sellaisia joukkoja, että on olemassa bijektio $A \rightarrow B$. Jos joko A tai B on äärellinen, niin tällöin sekä A että B ovat äärellisiä ja on voimassa $|A| = |B|$.*

Todistus. Olkoon f bijektio $A \rightarrow B$.

Oletamme, että joukko A on äärellinen. Tällöin on olemassa $n \in \mathbb{N}$ ja bijektio $\varphi : [n] \rightarrow A$. Näemme helposti, että kaavan $h(k) = f(\varphi(k))$ määrittämä kuvaus h on bijektio $[n] \rightarrow B$. Täten B on äärellinen ja on voimassa $|B| = n = |A|$.

Koska kuvaus f^{-1} on bijektio $B \rightarrow A$, edellä esitetystä seuraa, että jos B on äärellinen, niin tällöin A on äärellinen ja $|A| = |B|$. \square

Seuraavaksi osoitamme, että äärellisten joukkojen osajoukot ovat äärellisiä. Todistamme tämän ensin joukkojen $[n]$, $n \in \mathbb{N}$, osajoukoille.

Lemma *Olkoon n luonnollinen luku ja olkoon A joukon $[n]$ aito osajoukko. Tällöin jollain $k < n$ on olemassa bijektio $[k] \rightarrow A$.*

Todistus. Merkitsemme E :llä niiden lukujen $n \in \mathbb{N}$ muodostamaa joukkoa, joilla on olemassa sellainen $A \subsetneq [n]$, että millään $k < n$ ei ole olemassa bijektiota $[k] \rightarrow A$. Haluamme osoittaa, että on voimassa $E = \emptyset$.

Käytämme jälleen epäsuoraa todistusta ja induktioperiaatetta. Oletamme, että $E \neq \emptyset$. Induktioperiaatteen nojalla joukossa E on pienin luku m . Koska $m \in E$, on olemassa sellainen joukko $A \subsetneq [m]$, että millään $k < m$ ei ole olemassa bijektiota $[k] \rightarrow A$. Koska tyhjällä joukolla $[0]$ ei ole aitoja osajoukkoja, on voimassa $m > 0$ ja koska m on joukon E pienin luku, on voimassa $m - 1 \notin E$.

Merkitsemme $B = A \cap [m - 1]$ eli $B = A \setminus \{m\}$. Jos olisi voimassa $B = [m - 1]$, niin tällöin olisi voimassa $A = [m - 1]$ ja identtinen kuvaus olisi bijektio $[m - 1] \rightarrow A$, ristiriidassa joukon A ominaisuuden kanssa. Näin ollen on voimassa $B \subsetneq [m - 1]$. Koska $m - 1 \notin E$, on olemassa $\ell < m - 1$ ja bijektio $[\ell] \rightarrow B$. Edellisestä seuraa, että on voimassa $B \neq A$ eli $m \in A$. Jatkamme nyt kuvauksen φ kuvaukseksi $\bar{\varphi} : [\ell + 1] \rightarrow A$ asettamalla $\bar{\varphi}(\ell + 1) = m$. Näemme helposti, että $\bar{\varphi}$ on bijektio $[\ell + 1] \rightarrow A$, mutta tämä on ristiriidassa joukon A ominaisuuden kanssa, koska $\ell + 1 < m$.

Vastaväite johti ristiriitaan, joten se on väärä ja on voimassa $E = \emptyset$. \square

Lause *Olkoon A äärellinen joukko ja olkoon B A :n aito osajoukko. Tällöin B on äärellinen ja $|B| < |A|$.*

Todistus. Koska A on äärellinen, on olemassa $n = |A|$ ja bijektio $f : A \rightarrow [n]$. Merkitään $C = f(B) = \{f(b) : b \in B\}$. Koska f on bijektio ja $B \subsetneq A$, on voimassa $C \subsetneq [n]$. Edellisen lemmän nojalla on olemassa $k < n$ ja bijektio $g : C \rightarrow [k]$. Kuvaus $\varphi : B \rightarrow [k]$, missä $\varphi(b) = g(f(b))$ jokaisella $b \in B$, on bijektio. Täten B on äärellinen ja $|B| = k < n = |A|$. \square

Todistamme seuraavaksi tärkeän “summalauseen”.

Lause *Olkoot A ja B keskenään erillisiä äärellisiä joukkoja. Tällöin joukko $A \cup B$ on äärellinen ja*

$$\boxed{|A \cup B| = |A| + |B| .}$$

Todistus. Olkoon $|A| = n$ ja $|B| = k$ ja olkoot $\phi : [n] \rightarrow A$ ja $\psi : [k] \rightarrow B$ bijektioita. Määrittelemme nyt kuvauksen $\theta : [n + k] \rightarrow A \cup B$ seuraavasti: $\theta(i) = \phi(i)$ jos $i \leq n$ ja $\theta(i) = \psi(i - n)$ jos $i > n$. Näemme helposti, että θ on bijektio $[n + k] \rightarrow A \cup B$. \square

Seuraus *Olkoon A äärellinen joukko ja $B \subset A$. Tällöin*

$$\boxed{|A \setminus B| = |A| - |B| .}$$

Todistus. Äärellisen joukon A osajoukot B ja $A \setminus B$ ovat äärellisiä; lisäksi ne ovat erillisiä, joten edellisen lauseen nojalla on voimassa $|B| + |A \setminus B| = |B \cup (A \setminus B)| = |A|$; tästä seuraa yhtälö $|A \setminus B| = |A| - |B|$. \square

Seuraus Olkoot A ja B äärellisiä joukkoja. Tällöin joukko $A \cup B$ on äärellinen ja

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

Todistus. On voimassa $A \cup B = A \cup (B \setminus A)$ ja tästä seuraa edellisten tulosten nojalla, koska joukot A ja $B \setminus A$ ovat äärellisiä ja $A \cap (B \setminus A) = \emptyset$, että joukko $A \cup B$ on äärellinen ja $|A \cup B| = |A| + |B \setminus A|$. Koska $B \setminus A = B \setminus (A \cap B)$ ja $A \cap B \subset B$, niin edellisen seurauslauseen nojalla on voimassa $|B \setminus A| = |B| - |A \cap B|$. Näinollen on voimassa

$$|A \cup B| = |A| + |B \setminus A| = |A| + |B| - |A \cap B| . \quad \square$$

Edellisiä kahden joukon yhdisteen kokoa koskevia tuloksia on helppo yleistää kolmelle, neljälle, viidelle,... joukolle. Jos esimerkiksi A, B ja C ovat keskenään erillisiä äärellisiä joukkoja, niin tällöin $A \cup B$ on aikaisemman nojalla $|A| + |B|$ -joukko; soveltamalla tulosta toistamiseen, näemme että joukko $(A \cup B) \cup C$, eli joukko $A \cup B \cup C$ on $|A| + |B| + |C|$ -joukko. Käyttämällä hyväksi tätä kolmea joukkoa koskevaa tulosta näemme vastaavalla tavalla, että jos jos joukot A, B, C ja D ovat keskenään erillisiä äärellisiä joukkoja, niin $A \cup B \cup C \cup D$ on $|A| + |B| + |C| + |D|$ -joukko.

Koska voimme jatkaa edellistä päättelyä loputtomiin, tuntuu itsestään selvältä, että seuraava tulos on voimassa: jos $n \in \mathbb{N}$ ja jos joukot A_1, A_2, \dots, A_n ovat keskenään erillisiä äärellisiä joukkoja, niin joukko $A_1 \cup A_2 \cup \dots \cup A_n$ on äärellinen ja $|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$. Jos kuitenkin haluamme todistaa tuon tuloksen täsmällisesti, niin emme voi vedota siihen, että “voimme jatkaa edellistä päättelyä loputtomiin”. Täsmälliseen todistukseen tarvitsemme jo aikaisemmin pari kertaa kohtaamaamme “induktioperiaatetta”.

Ilmaisemme erillisten joukkojen yhdisteeseen liittyvän tuloksen yleisessä muodossa käyttämällä yleistettyjä yhdistys- ja summamerkintöjä. Teemme seuraavat sopimukset koskien “tyhjää summaa” ja “tyhjää yhdistettä”: $\sum_{i \in \emptyset} r_i = 0$ ja $\bigcup_{i \in \emptyset} A_i = \emptyset$.

Lause Olkoon I äärellinen joukko ja olkoot $A_i, i \in I$, keskenään erillisiä äärellisiä joukkoja. Tällöin joukko $\bigcup_{i \in I} A_i$ on äärellinen ja

$$\boxed{\left| \bigcup_{i \in I} A_i \right| = \sum_{i \in I} |A_i| .}$$

Todistus. Käytämme epäsuoraa päättelyä ja induktioperiaatetta samaan tapaan kuin kahdessa aikaisemmassa todistuksessa: teemme vastaväitteen ja merkitsemme m :llä pienintä luonnollista lukua $|I|$, missä I on äärellinen indeksijoukko, jota vastaa sellainen kokoelma keskenään erillisiä äärellisiä joukkoja $A_i, i \in I$, että lauseen johtopäätös *ei* toteudu.

Panemme merkille, että on voimassa $I \neq \emptyset$ (yllä tekemiemme sopimusten nojalla). Olkoon ι joukon I alkio. Merkitsemme $J = I \setminus \{\iota\}$. Tällöin on voimassa $|J| = |I| - |\{\iota\}| = m - 1$, joten lauseen johtopäätös toteutuu joukoille $A_j, j \in J$. Täten joukko $\bigcup_{j \in J} A_j$ on äärellinen ja $\left| \bigcup_{j \in J} A_j \right| = \sum_{j \in J} |A_j|$. Mutta nyt A_ι ja $\bigcup_{j \in J} A_j$ ovat keskenään erillisiä äärellisiä joukkoja, joten joukko $A_\iota \cup \bigcup_{j \in J} A_j$, eli joukko $\bigcup_{i \in I} A_i$, on äärellinen ja on voimassa

$$\left| \bigcup_{i \in I} A_i \right| = |A_\iota| + \left| \bigcup_{j \in J} A_j \right| = |A_\iota| + \sum_{j \in J} |A_j| = \sum_{i \in I} |A_i| .$$

Tämä on kuitenkin ristiriidassa joukkojen $A_i, i \in I$, oletetun ominaisuuden kanssa. \square

Seuraus Äärellisen monen äärellisen joukon yhdiste on äärellinen.

Todistus. Olkoot A_1, \dots, A_n äärellisiä joukkoja. Merkitsemme $B_k = A_k \setminus \bigcup_{i=1}^{k-1} A_i$ jokaisella $k = 1, \dots, n$ (huomaa, että $B_1 = A_1$, koska $\bigcup_{i=1}^{k-1} A_i = \bigcup_{i \in \emptyset} A_i = \emptyset$). Jokaisella $k \leq n$ joukko B_k on äärellisen joukon A_k osajoukkona äärellinen. Kaikilla $1 \leq j < k \leq n$ on voimassa $B_j \subset A_j$ ja $B_k \cap A_j = \emptyset$, joten joukot B_j ja B_k ovat erilliset. Edellisen lauseen nojalla joukko $\bigcup_{i=1}^n B_i$ on äärellinen.

Panemme lopuksi merkille, että on voimassa $\bigcup_{i=1}^n B_i = \bigcup_{i=1}^n A_i$. Koska $B_k \subset A_k$ jokaisella $k = 1, \dots, n$, on voimassa $\bigcup_{i=1}^n B_i \subset \bigcup_{i=1}^n A_i$. Toisaalta on voimassa $\bigcup_{i=1}^n A_i \subset \bigcup_{i=1}^n B_i$, sillä jos $x \in \bigcup_{i=1}^n A_i$, niin epätyhjässä joukossa $\{i \leq n : x \in A_i\}$ on pienin luku m ja tälle pätee, että $x \in A_m \setminus \bigcup_{i < m} A_i = B_m$. \square

Edellisen lauseen avulla voimme myös laskea kahden äärellisen joukon karteesisen tulon koon.

Lause Olkoot A ja B äärellisiä joukkoja. Tällöin joukko $A \times B$ on äärellinen ja

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

Todistus. Voimme esittää tulojoukon $A \times B$ yhdisteenä $\bigcup_{a \in A} (\{a\} \times B)$. Joukot $\{a\} \times B = \{(a, b) : b \in B\}$, $a \in A$, ovat keskenään erillisiä. Jokaisella $a \in A$, joukko $\{a\} \times B$ on $|B|$ -joukko, koska kuvaus $b \mapsto (a, b)$ on bijektio $B \rightarrow \{a\} \times B$. Edellisen lauseen nojalla joukko $\bigcup_{a \in A} (\{a\} \times B)$, eli joukko $A \times B$, on äärellinen ja on voimassa

$$|A \times B| = \sum_{a \in A} |\{a\} \times B| = \sum_{a \in A} |B| = |A| \cdot |B|. \quad \square$$

Määritämme myöhemmin erilaisten äärellisten joukkojen kokoja, kunhan saamme käyttöömmme tarvittavia apuvälineitä. Esimerkiksi seuraavassa luvussa määritämme äärellisen joukon potenssijoukon koon käyttämällä hyväksi sopivaa induktioperiaatetta.

III. INDUKTIO.

III 1. Induktiodistust.

“Induktio” tarkoittaa johtopäätösten tekemistä “yksityisestä yleiseen”.

Tämä menetelmä *ei* sinänsä toimi matematiikassa: yksittäisten esimerkkien nojalla *ei voida todistaa* yleisiä tuloksia.

Esimerkki Vanhan kiinalaisen “teoreeman” mukaan pätee, että – jos luonnollinen luku n jakaa luvun $2^n - 2$, niin n on alkuluku.

Kiinalaiset matemaatikot varmistivat tuloksen 2500 vuotta sitten monille n :n arvoille ja päättelivät, että tulos pätee yleisesti. Myöhemmin on varmistettu, että väite pätee jokaiselle $n = 1, 2, \dots, 300$.

Kuitenkin luku $341 = 11 \cdot 31$ jakaa luvun $2^{341} - 2$: käyttämällä hyväksi sitä tulosta, että luku $k - 1$ jakaa luvun $k^n - 1$ jokaisella $n = 1, 2, \dots$ (“geometrisen summan” kaavan nojalla on voimassa $\frac{k^n - 1}{k - 1} = 1 + k + \dots + k^{n-1}$), näemme että on voimassa $(2^{10})^{34} - 1 = N \cdot (2^{10} - 1)$, missä N on kokonaisluku. Näin ollen on voimassa:

$$\begin{aligned} 2^{341} - 2 &= 2(2^{340} - 1) \\ &= 2((2^{10})^{34} - 1) \\ &= 2(N \cdot (2^{10} - 1)) \\ &= 2 \cdot N \cdot 1023 = 2 \cdot N \cdot 3 \cdot 341. \end{aligned}$$

“Teoreema” ei siis päde yleisesti. \square

Edellisen kaltaisista esimerkeistä huolimatta matematiikassa on pätevä todistustapa, jota kutsutaan “matemaattiseksi induktioksi” tai “induktioperiaatteenksi”.

Edellä nimitimme “induktioperiaatteenksi” seuraavaa tulosta, joka tunnetaan myös “luonnollisten lukujen hyvinjärjestyslauseena”. Otamme tuloksen käyttöön ilman todistusta, yhtenä luonnollisten lukujen teorian perusolettamuksista eli aksiomeista.

Induktioaksioma: *Jokaisessa joukon \mathbb{N} epättyhjässä osajoukossa on pienin luku.*

Johdamme seuraavassa induktioaksiomasta eräitä muunnelmia, jotka varsinaisemmin liittyvät “induktiopäätelyyn”. Ensimmäinen muunnelmamme on vielä sangen yleistä muotoa.

Lause (*Yleinen induktioperiaate*) Olkoon A joukon \mathbb{N} osajoukko ja olkoon P sellainen luonnollisten lukujen ominaisuus, että jokaiselle luvulle $a \in A$ pätee, että luvulla a on ominaisuus P , mikäli jokaisella lukua a pienemmällä joukon A luvulla on ominaisuus P . Tällöin jokaisella A :n alkiolla on ominaisuus P .

Todistus. Merkitsemme $B = \{n \in A : n\text{llä ei ole ominaisuutta } P\}$. On osoitettava, että $B = \emptyset$. Teemme vastaväitteen: $B \neq \emptyset$. Induktioaksioman nojalla joukossa B on pienin luku a . Koska B :ssä ei ole a :ta pienempiä lukuja, B :n määritelmästä seuraa, että jokaisella a :ta pienemmällä A :n alkiolla on ominaisuus P . Tästä seuraa ominaisuutta P koskevan oletuksen nojalla, että a :lla on ominaisuus P ; tämä on kuitenkin ristiriidassa sen kanssa, että $a \in B$. Vastaväite johti ristiriitaan, joten se on väärä. Täten on voimassa $B = \emptyset$. \square

Olkoon P luonnollisten lukujen ominaisuus ja n luonnollinen luku. Otamme käyttöön merkinnän $P(n)$ osoittamaan, että luvulla n on ominaisuus P . Tällöin voimme kirjoittaa edellisen lauseen ominaisuutta P koskevan oletuksen muotoon

$$(\forall a \in A) \left[((\forall b \in A) (b < a \Rightarrow P(b))) \Rightarrow P(a) \right].$$

Toteamme, että jos a on joukon A pienin luku, niin $\{b \in A : b < a\} = \emptyset$, joten yllä hakasuluissa oleva lauseke pätee luvulle a jos ja vain jos $P(a)$.

Edellinen lause sisältää *induktioperiaatteen* hyvin yleisessä muodossa ja siitä voidaan helposti johtaa periaatteelle eri muunnelmia. Ennen kuin esitämme “varsinaisia” induktioperiaatteita, tarkastelemme eräitä valaisevia esimerkkejä.

Esimerkki Kun kuuluisa matemaatikko C.F. Gauss oli (1700-luvun lopussa) alakoulussa, opettaja yritti kerran vaientaa luokan vähäksi aikaa antamalla oppilaille työhönsä tehtävän: laskea yhteen sata ensimmäistä positiivista kokonaislukua. Gauss pilasi opettajan yrityksen viittaamalla melkein samantien ja kertomalla, että summa on 5050. Opettajan ihmeteltyä Gaussin nopeutta tämä kertoi käyttäneensä seuraavaa yksinkertaista päättelyä: hän oli mielessään muodostanut summan kahteen kertaan ja hän oli ryhmitellyt kaksinkertaisen summan termit seuraavasti:

$$(1+2+\cdots+99+100)+(100+99+\cdots+2+1) = (1+100)+(2+99)+\cdots+(99+2)+(100+1).$$

Oikealla jokainen suluissa oleva kahden luvun summa on 101 ja sulkutermejä on 100 kappaletta. Täten kaksinkertainen summa on $100 \cdot 101 = 10100$ ja kysytty summa on $\frac{1}{2} \cdot 10100 = 5050$.

Tuntuu ilmeiseltä, että voimme soveltaa samaa päättelyä n :n ensimmäisen positiivisen kokonaisluvun summaan ja saamme tulokseksi

$$1 + 2 + \dots + n = \frac{n(n+1)}{2}.$$

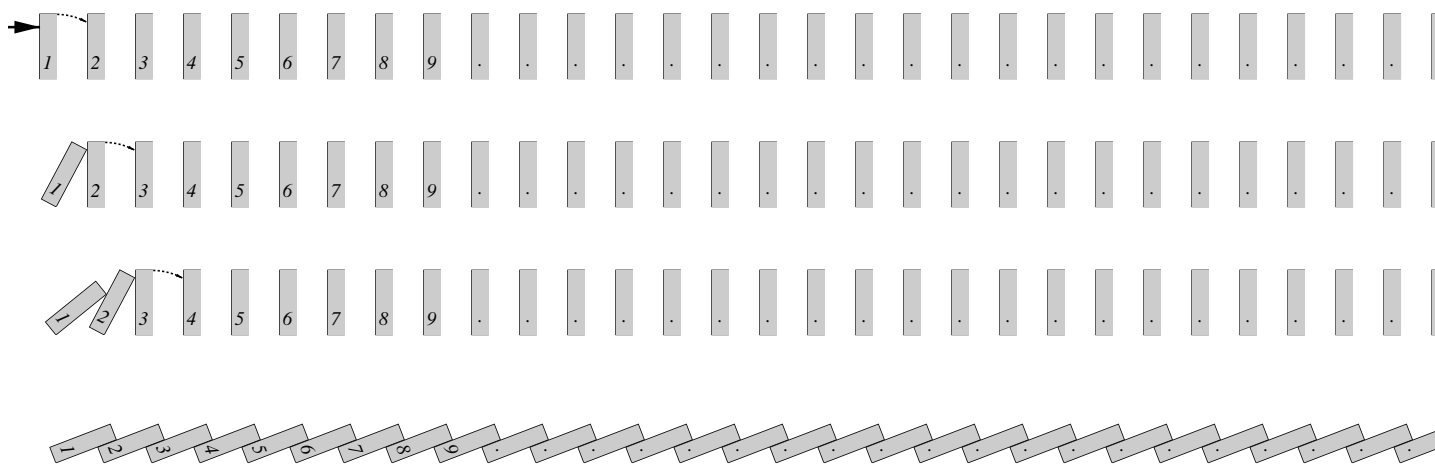
Valitettavasti tämä päättely ei ole suoraan formalisoitavissa kelvolliseksi matemaattiseksi todistukseksi, joka antaisi mainitun *kaikkia* positiivisia kokonaislukuja koskevan tuloksen.

Voimme kuitenkin vedota induktioperiaatteeseen ja todistaa tuloksen seuraavaan tapaan:

- (i) Toteamme, että tulos pätee arvolla $n = 0$ (koska $1 + 2 + \dots + 0 = \sum_{k \in \emptyset} k = 0 = \frac{0 \cdot 1}{2}$).
- (ii) Osoitamme, että jos tulos pätee luvulle n , niin se pätee myös luvulle $n + 1$ (tämä on nyt voimassa, sillä jos pätee, että $1 + 2 + \dots + n = \frac{n(n+1)}{2}$, niin tällöin pätee, että $1 + 2 + \dots + (n+1) = (1 + 2 + \dots + n) + (n+1) = \frac{n(n+1)}{2} + (n+1) = (\frac{n}{2} + 1)(n+1) = \frac{(n+1)(n+2)}{2}$).
- (iii) Päättellemme *induktioperiaatteen nojalla*, että tulos pätee jokaisella $n \in \mathbb{N}$.

Esimerkki Voimme havainnollistaa edellä kuvailtua induktioperiaatetta seuraavan “dominovertauksen” avulla:

Ajattelemme, että dominopalikoita on asetettu jonoon tasavälein kuten alla ylärivillä. Jos ensimmäinen palikka kaadetaan, niin se kaataa toisen, joka puolestaan kaataa kolmannen, joka kaataa neljännen, jne. Induktioperiaate sanoo, että kaikki dominot kaatuvat, vaikka niitä olisi äärettömän monta (tällöin tosin kaikkien kaatumiseen kuluisi “ääretön aika”). “Lopulta” oltaisiin siis alarivin tilanteessa.



Muotoilemme nyt edellisissä esimerkeissä kuvaillun induktioperiaatteen täsmällisesti.

Lause (*Ensimmäinen induktioperiaate*) Olkoon P sellainen luonnollisten lukujen ominaisuus, että on voimassa:

1° $P(0)$.

2° $(\forall n \in \mathbb{N}) (P(n) \Rightarrow P(n + 1))$.

Tällöin on voimassa $(\forall n \in \mathbb{N}) P(n)$.

Todistus. Kun valitsemme edellisessä lauseessa joukoksi A joukon \mathbb{N} , niin ominaisuus P toteuttaa lauseessa tehdyn oletuksen, koska ehdon 1° nojalla on voimassa $P(0)$ ja koska ehdosta 2° seuraa, että jokaisella $a > 0$ on voimassa $P(a - 1) \Rightarrow P(a)$. Lauseen nojalla on voimassa $(\forall n \in \mathbb{N}) P(n)$. \square

Huomaamme, että voimme ilmaista ehdon 2° yllä myös seuraavasti:

$$(\forall n > 0) [P(n - 1) \Rightarrow P(n)] .$$

“*Todistus induktiolla $n:n$ suhteen*” suoritetaan seuraavasti:

1° Todistamme (tai toteamme), että luvulla 0 on ominaisuus P (“*Induktion alku*”).

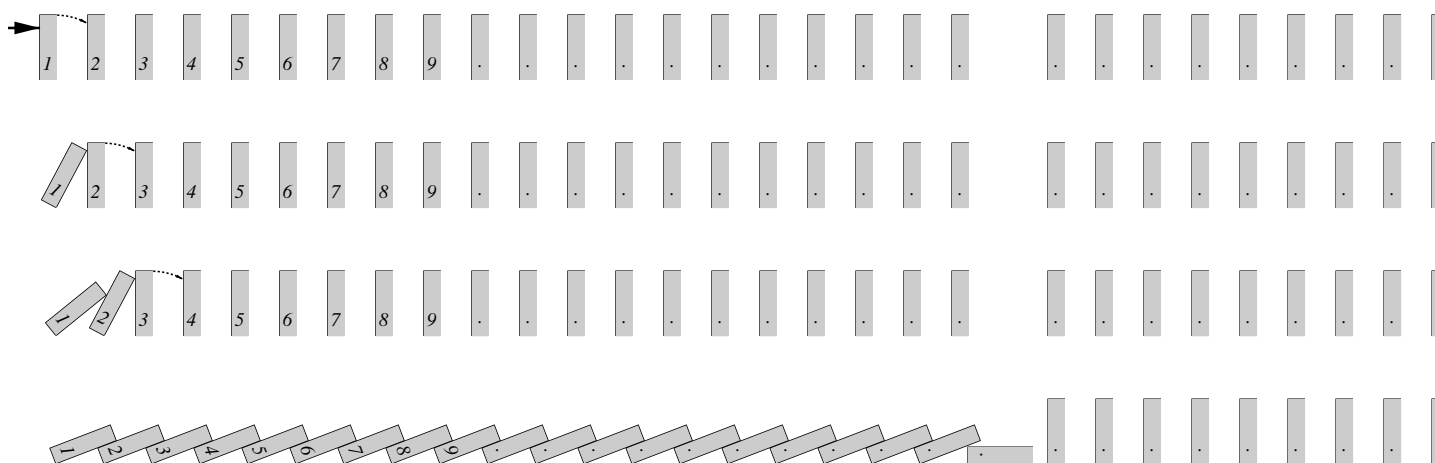
2° Mielivaltaiselle $n \in \mathbb{N}$ oletamme, että luvulla n on ominaisuus P (“*Induktio-oletus*”) ja todistamme tämän oletuksen avulla, että luvulla $n + 1$ on ominaisuus P (“*Induktioaskel*”).

3° *Johtopäätöksenä* (induktioperiaatteen nojalla) on, että jokaisella luonnollisella luvulla on ominaisuus P .

Esimerkki Aikaisemmassa esimerkissä totesimme, että jos $P(n)$ tarkoittaa yhtälön $1 + \dots + n = \frac{n(n+1)}{2}$ voimassaoloa, niin yllä olevat ehdot 1° ja 2° toteutuvat. Täten ehto $P(n)$ toteutuu jokaisella $n \in \mathbb{N}$ ensimmäisen induktioperiaatteen nojalla. Nyt olemme siis *todistaneet* sen edellä havaitsemamme tuloksen, että

$$1 + 2 + \dots + n = \frac{n(n + 1)}{2} \quad \text{jokaisella } n \in \mathbb{N} . \quad \square$$

Dominovertauksen avulla näemme hyvin selvästi, miten tärkeää induktiotodistuksessa on osoittaa, että induktioaskel $P(n) \implies P(n+1)$ pätee *jokaisella* $n \in \mathbb{N}$:



Voimme helposti todistaa induktioperiaatteelle eri tilanteisiin soveltuvia muunnelmia. Voimme esimerkiksi aloittaa induktion luvun 0 asemasta jostakin luvusta $m > 0$: jos korvaamme ehdot 1° ja 2° ehdoilla 1# $P(m)$ ja 2# $(\forall n \geq m) [P(n) \implies P(n+1)]$, niin saamme johtopäätökseksi $(\forall n \geq m) P(n)$.

Mainitsemme erikseen vain seuraavan induktioperiaatteen muunnelman; tämä periaate on muodollisesti vahvempi kuin 1. induktioperiaate, koska siinä on induktio-oletuksen $P(n)$ vastineena vahvempi ehto $(\forall k \leq n) P(k)$.

Lause (Toinen induktioperiaate) *Olkoon P sellainen luonnollisten lukujen ominaisuus, että on voimassa:*

1* $P(0)$.

2* $(\forall n \in \mathbb{N}) \left(((\forall k \leq n) P(k)) \implies P(n+1) \right)$.

Tällöin on voimassa $(\forall n \in \mathbb{N}) P(n)$.

Todistus. Merkitsemme Q :llä luonnollisten lukujen ominaisuutta $Q(n) \iff (\forall k \leq n) P(k)$.

Tällöin $Q(0) \iff P(0)$, joten Q toteuttaa 1. induktioperiaatteen ehdon 1°; lisäksi Q toteuttaa ehdon 2°, koska voimme esittää yllä olevan ehdon 2* yhtäpitävässä muodossa

$$(\forall n \in \mathbb{N}) [((\forall k \leq n) P(k)) \implies ((\forall k \leq n+1) P(k))]$$

eli muodossa $(\forall n \in \mathbb{N}) (Q(n) \implies Q(n+1))$. Päättelemme 1. induktioperiaatteen nojalla,

että $Q(n)$ pätee jokaisella $n \in \mathbb{N}$. Koska jokaisella $n \in \mathbb{N}$ on voimassa $Q(n) \implies P(n)$, myös $P(n)$ pätee jokaisella $n \in \mathbb{N}$. \square

Annamme nyt muutamia esimerkkejä edellisten induktioperiaatteiden käytöstä.

Esimerkkejä (a) Todista kaava

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

Todistus. Käytämme ensimmäistä induktioperiaatetta. Merkitsemme $s(n) = 1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1)$ jokaisella $n \in \mathbb{N}$.

Alkuaskel: Kaava pätee muodossa $0 = 0$ kun $n = 0$.

Induktioaskel: Oletamme, että $k \geq 0$ ja että kaava pätee kun $n = k$, eli että on voimassa yhtälö $s(k) = \frac{k(k+1)(k+2)}{3}$. Tämän induktio-oletuksen nojalla saamme seuraavan yhtälöketjun

$$\begin{aligned} s(k+1) &= 1 \cdot 2 + \cdots + (k+1) \cdot (k+2) \\ &= (1 \cdot 2 + \cdots + k \cdot (k+1)) + (k+1) \cdot (k+2) \\ &= s(k) + (k+1) \cdot (k+2) \\ &= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \\ &= \left(\frac{k}{3} + 1\right)(k+1)(k+2) \\ &= \frac{(k+1)(k+2)(k+3)}{3}. \end{aligned}$$

(Huomaa, että induktio-oletusta tarvittiin yllä neljännen yhtäsuuruusmerkin perusteena.)

Olemme osoittaneet, että yhtälö pätee kun $n = k + 1$.

Johtopäätös: Ensimmäisen induktioperiaatteen nojalla kaava pätee jokaisella $n \in \mathbb{N}$. \square

(b) Todista kaava

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

Todistus. Käytämme ensimmäistä induktioperiaatetta. Merkitsemme $s(n) = 1^3 + 2^3 + \cdots + n^3$ jokaisella $n \in \mathbb{N}$. Koska aikaisemman nojalla on voimassa $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, todistettava kaava voidaan kirjoittaa muotoon $s(n) = \frac{n^2(n+1)^2}{4}$.

Alkuaskel: Jälleen kaava pätee muodossa $0 = 0$ kun $n = 0$.

Induktioaskel: Oletamme, että $k \geq 0$ ja että kaava pätee kun $n = k$, eli että on voimassa yhtälö $s(k) = \frac{k^2(k+1)^2}{4}$. Tämän induktio-oletuksen nojalla saamme seuraavan yhtälöketjun

$$\begin{aligned} s(k+1) &= 1^3 + 2^3 \cdots + k^3 + (k+1)^3 \\ &= (1^3 + 2^3 + \cdots + k^3) + (k+1)^3 \\ &= s(k) + (k+1)^3 \\ &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= \left(\frac{k^2}{4} + k + 1\right)(k+1)^2 \\ &= \frac{(k+1)^2(k^2 + 4k + 4)}{4} \\ &= \frac{(k+1)^2(k+2)^2}{4}. \end{aligned}$$

(Huomaa, että induktio-oletusta tarvittiin yllä neljännen yhtäsuuruusmerkin perusteena.)

Olemme osoittaneet, että yhtälö pätee kun $n = k + 1$.

Johtopäätös: Ensimmäisen induktioperiaatteen nojalla kaava pätee jokaisella $n \in \mathbb{N}$. \square

(c) Osoita, että jokainen kokonaisluku $n \geq 2$ voidaan esittää alkulukujen tulona (jos n on alkuluku, niin kyseessä on “yksitekijäinen tulo”).

Todistus. Todistamme toisen induktioperiaatteen avulla, että jokainen $n \in \mathbb{N}$, $n \geq 2$, voidaan esittää alkulukujen tulona.

Aloitus. Tulos pätee luvulle $n = 2$, koska 2 on alkuluku.

Induktioaskel: Oletamme, että $n \geq 2$ ja jokainen luvuista $2, \dots, n$ voidaan esittää alkulukujen tulona. Osoitamme tämän *induktio-oletuksen* avulla, että luku $n + 1$ voidaan esittää alkulukujen tulona. Tämä pätee, mikäli $n + 1$ on alkuluku (“yhden luvun tulo”). Oletamme, että $n + 1$ ei ole alkuluku. Tällöin on olemassa sellaiset luonnolliset luvut k ja ℓ , että $k \neq 1$, $\ell \neq 1$ ja $n + 1 = k \cdot \ell$. Nyt on voimassa $2 \leq k \leq n$ ja $2 \leq \ell \leq n$, joten induktio-oletuksen nojalla voimme kirjoittaa $k = p_1 \cdots p_i$ ja $\ell = q_1 \cdots q_j$, missä luvut p_1, \dots, p_i ja q_1, \dots, q_j ovat alkulukuja. Mutta nyt on voimassa

$$n + 1 = k \cdot \ell = p_1 \cdots p_i \cdot q_1 \cdots q_j,$$

joten väite pätee luvulle $n + 1$.

Johtopäätös: Toisen induktioperiaatteen nojalla väite pätee jokaisella $n = 1, 2, 3, \dots$. \square

III 2. Rekursiiviset määritelmät.

Induktioperiaatteen avulla voimme osoittaa ns. *rekursiivisten määritelmien* oikeellisuuden. Esimerkkinä määrittelemme järjestettyjen parien yleistykseenä (äärelliset) *jonot*. Määrittelemme yhden alkion jonot asettamalla $(x) = x$ jokaisella x . Kahden alkion jono on järjestetty pari. Jos n :n alkion jonot on jo määritelty, niin $n + 1$:n alkion jono (x_1, \dots, x_{n+1}) määräytyy rekursiivisesti *palautuskaavasta* eli *rekursioyhtälöstä*

$$(x_1, \dots, x_{n+1}) = ((x_1, \dots, x_n), x_{n+1}).$$

Induktiolla voimme osoittaa, että k :n alkion jonot tulevat edellä esitetyllä tavalla määritellyiksi jokaiselle $k \in \mathbb{N}$. Voimme myös osoittaa, että kahdelle k :n alkion jonolle (x_1, \dots, x_k) ja (y_1, \dots, y_k) on voimassa

$$(x_1, \dots, x_k) = (y_1, \dots, y_k) \text{ jos ja vain jos } x_i = y_i \text{ jokaisella } i = 1, \dots, k. \quad (*)$$

Todistamme edelliset kaksi väitettä samanaikaisesti soveltamalla induktioperiaatetta seuraavaan luonnollisten lukujen ominaisuuteen P :

$$P(n) \iff \text{kaikilla } x_1, \dots, x_n \text{ ja } y_1, \dots, y_n \text{ jonot } (x_1, \dots, x_n) \text{ ja } (y_1, \dots, y_n)$$

on määritelty ja ehto $(*)$ on voimassa.

Todistus. Näemme helposti, että luvuilla 0, 1 ja 2 on ominaisuus P ; täten voimme aloittaa induktion luvusta 2. Jos nyt luvulla $n \geq 2$ on ominaisuus P , niin edellä annettu palautuskaava määrittelee kaikki $n + 1$:n alkion jonot. Lisäksi ehto $(*)$ toteutuu (k :n arvolla $n + 1$), sillä jos $(x_1, \dots, x_{n+1}) = (y_1, \dots, y_{n+1})$, niin tällöin $((x_1, \dots, x_n), x_{n+1}) = ((y_1, \dots, y_n), y_{n+1})$ ja tästä seuraa järjestettyjen parien perusominaisuuden nojalla, että on voimassa $(x_1, \dots, x_n) = (y_1, \dots, y_n)$ ja $x_{n+1} = y_{n+1}$. Koska ehto $(*)$ on voimassa k :n arvolla n , toiseksi viimeisestä yhtälöstä seuraa, että on voimassa $x_i = y_i$ jokaisella $i = 1, \dots, n$. Edellisen nojalla $x_i = y_i$ jokaisella $i = 1, \dots, n + 1$. Täten olemme suorittaneet induktiioaskelen ja päättelemme 1. induktioperiaatteen nojalla, että jokaisella luvulla $n \geq 2$ on ominaisuus P . Näin ollen jokaisella luonnollisella luvulla on ominaisuus P . \square

Annamme toisenkin esimerkin siitä, miten edellinen rekursiivinen määritelmä sopii yhteen induktiotodistusten kanssa.

Äärellisten jonojen määritelmän avulla voimme nyt määritellä useamman joukon karteesiset tulot seuraavasti.

Määritelmä Joukkojen A_1, \dots, A_n *karteesinen tulo* (eli *tulojoukko*) on

$$A_1 \times \cdots \times A_n = \{(a_1, \dots, a_n) : a_i \in A_i \text{ jokaisella } i = 1, \dots, n\}.$$

Tämä määritelmä antaa kahden joukon tapauksessa saman tulojoukon kuin aikaisempi määritelmä. Yleistämme nyt aikaisempaa kahden äärellisen joukon tulojoukon kokoa koskevaa tulosta.

Lause Olkoon $n > 0$ ja olkoot A_1, \dots, A_n äärellisiä joukkoja. Tällöin

$$|A_1 \times \cdots \times A_n| = |A_1| \cdots |A_n|.$$

Todistus. Todistamme väitteen induktiolla luvun n suhteen.

Tapauksessa $n = 1$ väite pätee muodossa $|A_1| = |A_1|$.

Oletamme, että väite pätee n :n äärellisen joukon karteesisille tuloille. Olkoot nyt A_1, \dots, A_{n+1} äärellisiä joukkoja. Tällöin

$$\begin{aligned} A_1 \times \cdots \times A_{n+1} &= \{(a_1, \dots, a_n, a_{n+1}) : a_i \in A_i \text{ jokaisella } i = 1, \dots, n+1\} \\ &= \{((a_1, \dots, a_n), a_{n+1}) : a_i \in A_i \text{ jokaisella } i = 1, \dots, n \text{ ja } a_{n+1} \in A_{n+1}\} \\ &= \{((a_1, \dots, a_n), a_{n+1}) : (a_1, \dots, a_n) \in A_1 \times \cdots \times A_n \text{ ja } a_{n+1} \in A_{n+1}\} \\ &= (A_1 \times \cdots \times A_n) \times A_{n+1}. \end{aligned}$$

Koska induktiooletuksen nojalla on voimassa $|A_1 \times \cdots \times A_n| = |A_1| \cdots |A_n|$, edellisestä seuraa yhdessä aikaisemman, kahden äärellisen joukon karteesista tuloa koskevan lauseen nojalla, että on voimassa

$$\begin{aligned} |A_1 \times \cdots \times A_n \times A_{n+1}| &= |(A_1 \times \cdots \times A_n) \times A_{n+1}| \\ &= |A_1 \times \cdots \times A_n| \cdot |A_{n+1}| \\ &= (|A_1| \cdots |A_n|) \cdot |A_{n+1}| \\ &= |A_1| \cdots |A_{n+1}|. \end{aligned}$$

Olemme suorittaneet induktioaskeleen ja voimme päätellä 1. induktioperiaatteen nojalla, että lauseen väite pätee jokaisella $n > 0$. \square

Jos $A_i = A$ jokaisella $i = 1, \dots, n$, niin merkitsemme tulojoukkoa $A_1 \times \cdots \times A_n$ symbolilla A^n .

Seuraus Olkoon $n > 0$ ja olkoon A äärellinen joukko. Tällöin

$$|A^n| = |A|^n.$$

Edellisen tuloksen avulla voimme määrittää äärellisen joukon potenssijoukon koon.

Seuraus Olkoon A k -joukko. Tällöin $\mathcal{P}(A)$ on 2^k -joukko.

Todistus. Näemme helposti, että samankokoisten joukkojen potenssijoukot ovat samankokoisia: jos f on bijektio joukolta D joukolle E , niin kaavan $\varphi(G) = f(G)$ määrittämä kuvaus φ on bijektio $\mathcal{P}(D) \rightarrow \mathcal{P}(E)$ (tarkista tämä!).

Edellisen huomion nojalla voimme olettaa, että $A = [k]$. Määrittelemme kuvauksen $\psi : \mathcal{P}[k] \rightarrow \{0, 1\}^k$ asettamalla $\psi(B) = (\chi_B(1), \dots, \chi_B(k))$, missä χ_B on joukon B karakteristinen funktio: $\chi_B(i) = 1$ jos $i \in B$ ja $\chi_B(i) = 0$ jos $i \notin B$. Kuvauksella ψ on käänteiskuvaus $\theta : \{0, 1\}^k \rightarrow \mathcal{P}[k]$, joka määräytyy kaavasta $\theta((b_1, \dots, b_k)) = \{i \in [k] : b_i = 1\}$ (tarkista!). Täten ψ on bijektio ja on voimassa

$$|\mathcal{P}[k]| = |\{0, 1\}^k| = |\{0, 1\}|^k = 2^k. \quad \square$$

Palaamme nyt tarkastelemaan rekursiota. Voimme määritellä myös yksittäisiä joukkoja rekursiivisesti, esimerkiksi parillisten luonnollisten lukujen joukon E seuraavasti:

$$0 \in E \quad \text{ja} \quad (\forall n \in \mathbb{N} \setminus \{0\})(n \in E \iff n - 1 \notin E).$$

Tämän ja myöhemmin annettavien rekursiivisten määritelmien oikeellisuuden voimme osoittaa vastaavasti kuten edellä äärellisten jonojen tapauksessa.

Panemme merkille, että olisimme voineet määritellä äärelliset jonot toisellakin tavalla, ilman rekursiota: olisimme voineet sanoa, että n -jono on kuvaus, jonka määrittäjäjoukko on $[n]$; tällaisilla kuvauksilla on suoraviivainen yhteys yllä määriteltyihin jonoihin: jos (a_1, \dots, a_n) on jono, niin voimme tarkastella kuvausta $k \mapsto a_k$; toisaalta, jos f on kuvaus joukolta $[n]$, niin voimme tarkastella n -jonoa $(f(1), \dots, f(n))$.

Edellä käytetty “perinteinen” määritelmä on äärellisen jonon tapauksessa luonnollisempi kuin määritelmä kuvauksena, mutta “äärettömän” eli “päättymättömän” jonon käsite on jo sinänsä “epäluonnollinen” ja voimme sellaiselle yhtä hyvin käyttää mahdollisimman yksinkertaista määritelmää. Sanomme, että kuvaus $f : \mathbb{N} \rightarrow A$ määrittelee jonon a_0, a_1, a_2, \dots , missä $a_n = f(n)$ jokaisella $n \in \mathbb{N}$.

Äärettömiä *lukuonoja*, eli funktioita $\mathbb{N} \rightarrow \mathbb{R}$ (tai vaikkapa $\mathbb{N} \rightarrow \mathbb{N}$) määritellään usein rekursiivisesti. Esimerkiksi *kertomafunktio* $n \mapsto n!$ määritellään rekursiivisesti asettamalla $0! = 1$ ja $(n + 1)! = (n + 1) \cdot n!$ jokaisella n . Sanomme, että $n!$ on luonnollisen luvun n *kertoma*. On voimassa $1! = 1 \cdot 1$, $2! = 1 \cdot 2$, $3! = 2 \cdot 3$ ja, yleisesti, jokaisella $n > 0$ on voimassa $n! = 1 \cdot \dots \cdot n$.

Annamme toisenkin esimerkin rekursiivisesti määritellystä äärettömästä lukujonosta.

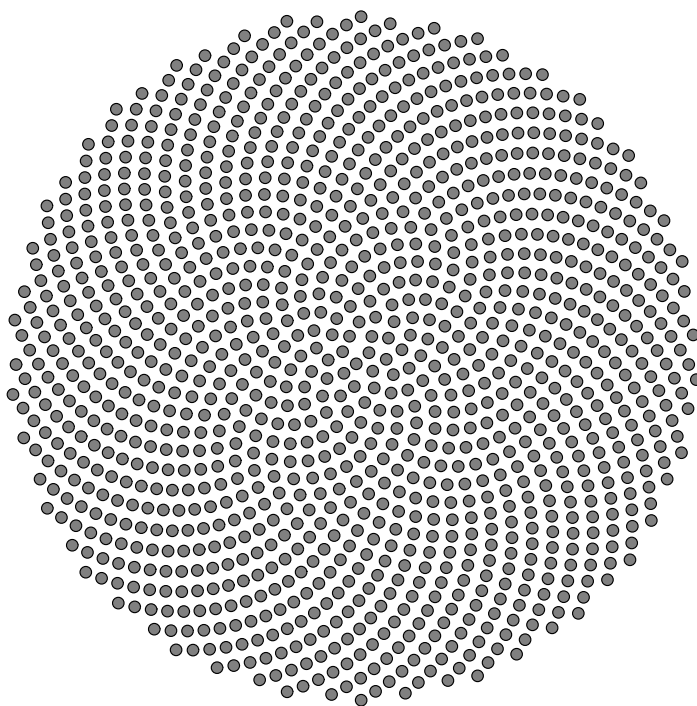
Esimerkki Fibonaccin luvut F_0, F_1, F_2, \dots määritellään käyttämällä *alkuarvoja* $F_0 = 0$ ja $F_1 = 1$ sekä rekursioyhtälöä

$$F_{n+1} = F_n + F_{n-1}.$$

Fibonaccin lukujonon alku näyttää seuraavalta:

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946,

Fibonaccin luvut esiintyvät luonnossa monessa eri yhteydessä, mm. käpyjen ja anaksen ulkorakenteessa, auringonkukkien siementen sijoittelussa jne. Seuraavassa on yksi malli auringonkukan siemenkodalle. Kuvassa näkyy 55 myötäpäivään kiertävää spiraalaa ja 89 vastapäivään kiertävää; myös muita peräkkäisiä Fibonaccin lukuja esiintyy tällä tavalla auringonkukan siemenkodissa.



Fibonacciin luvuille ei aivan helposti löydy mitään ei-rekursiivista, analyttistä lauseketta. Sellainen on kuitenkin löydetty nk. *generoivien funktioiden* avulla. Induktion avulla voimme helposti varmistaa seuraavan lausekkeen pätevyyden.

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right].$$

Todistus. Näemme helposti, että lauseke saa arvon 0 kun $n = 0$ ja arvon 1 kun $n = 1$.

Oletamme nyt, että $k > 0$ ja että lauseke pätee F_n :lle kun $n = 0, \dots, k$. Osoitamme, että se pätee myös kun $n = k + 1$.

On voimassa $F_{k+1} = F_k + F_{k-1}$ ja tästä seuraa induktio-oletuksen nojalla seuraavaa:

$$\begin{aligned} F_{k+1} &= \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^k - \left(\frac{1 - \sqrt{5}}{2} \right)^k \right] + \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^{k-1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{k-1} \right] \\ &= \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^k \left(1 + \frac{2}{1 + \sqrt{5}} \right) - \left(\frac{1 - \sqrt{5}}{2} \right)^k \left(1 + \frac{2}{1 - \sqrt{5}} \right) \right] \\ &= \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^k \left(\frac{3 + \sqrt{5}}{1 + \sqrt{5}} \right) - \left(\frac{1 - \sqrt{5}}{2} \right)^k \left(\frac{3 - \sqrt{5}}{1 - \sqrt{5}} \right) \right] \\ &= \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^k \left(\frac{-2 - 2\sqrt{5}}{-4} \right) - \left(\frac{1 - \sqrt{5}}{2} \right)^k \left(\frac{-2 + 2\sqrt{5}}{-4} \right) \right] \\ &= \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^{k+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{k+1} \right]. \end{aligned}$$

Täten vaadittu esitys pätee F_{k+1} :lle. Toisen induktioperiaatteen nojalla päättelemme, että annettu lauseke pätee jokaisella $n \in \mathbb{N}$. \square

Mainitsemme vielä muutamia esimerkkejä rekursiivista määritelmistä.

Esimerkkejä (a) Luonnollisten lukujen kertolasku voidaan määritellä rekursiivisesti yhteenlaskun avulla:

$$m \cdot 0 = 0 ; \quad m \cdot (n + 1) = m \cdot n + m .$$

(b) Potenssi voidaan määritellä kertolaskun avulla:

$$m^0 = 1 ; \quad m^{n+1} = m^n \cdot m .$$

Seuraavaksi annamme yksinkertaisen esimerkin rekursiivisen määritelmän käytöstä todistuksessa.

Lemma *Olkoon $A \subset \mathbb{N}$ epätyhjä äärellinen joukko, $|A| = m$. Tällöin joukolla A on sellainen esitys $A = \{a_i : i \in [m]\}$, että jokaisella $i \in [m - 1]$ on voimassa $a_i < a_{i+1}$.*

Todistus. Määrittelemme alkiot a_1, \dots, a_m rekursiivisesti valitsemalla aina a_i :ksi joukon $A \setminus \{a_j : j \in [i - 1]\}$ pienimmän alkion; tämä määritelmä on pätevä, koska $j \mapsto a_j$ on bijektio $[i - 1] \rightarrow \{a_j : 1 \leq j < i\}$, joten $|\{a_j : 1 \leq j < i\}| = i - 1 < |A|$ ja näin ollen $A \setminus \{a_j : 1 \leq j < i\} \neq \emptyset$. Toisaalta $|\{a_1, \dots, a_m\}| = m = |A|$, joten $\{a_1, \dots, a_m\} = A$. Määritelmästä seuraa suoraan, että jokaisella $i \in [m - 1]$ on voimassa $a_i < a_{i+1}$. \square

Jos A :lla on esitys $\{a_i : i \in [m]\}$ kuten yllä, niin jokaisella $a \in A$ on voimassa $a \leq a_m$; täten seuraava tulos on voimassa.

Seuraus *Jokaisessa joukon \mathbb{N} epätyhjässä äärellisessä osajoukossa on suurin luku.*

Panemme merkille, että suurimman luvun olemassaolo luonnehtii \mathbb{N} :n epätyhjän osajoukon äärellisyyttä: jos m on joukon $A \subset \mathbb{N}$ suurin luku, niin tällöin on voimassa $A \subset [m] \cup \{0\}$ ja tästä seuraa aikaisemman nojalle, että A on äärellinen.

Mainitsemme lopuksi, että induktiota ja rekursiota voidaan suorittaa muidenkin “struktuurien” kuin luonnollisten lukujen \mathbb{N} suhteen. Esimerkkinä tarkastelemme induktiota äärellisten joukkojen osajoukkojen suhteen. Huomautamme ensin, että induktioperiaatteesta seuraa suoraan, että äärellisiä joukkoja koskevia väitteitä voidaan todistaa *induktiolla joukkojen koon suhteen*. Tällaiset induktiotodistukset ovat seuraavaa muotoa. Olkoon \mathcal{A} jokin kokoelma äärellisiä joukkoja ja olkoon P jokin joukkojen ominaisuus. Nyt voimme tarkastella seuraavaa luonnollisten lukujen ominaisuutta Q :

$$Q(n) \iff (\forall A \in \mathcal{A}) (|A| = n \implies P(A)).$$

Jos saamme todistettua induktiolla, että jokaisella luonnollisella luvulla on ominaisuus Q , niin voimme päätellä, että jokaisella kokoelman \mathcal{A} joukolla on ominaisuus P .

Koska äärellisen joukon koko on luonnollinen luku, induktio äärellisten joukkojen koon suhteen on vain tavallista induktiota. Sen sijaan seuraavassa induktioperiaatteessa ei esiinny luonnollisia lukuja.

Olkoon jälleen \mathcal{A} kokoelma äärellisiä joukkoja ja P jokin joukkojen ominaisuus.

$$\left[(\forall A \in \mathcal{A}) ((\forall \{B \in \mathcal{A} : B \subsetneq A\}) P(B)) \implies P(A) \right] \implies (\forall A \in \mathcal{A}) P(A). \quad (*)$$

Toisinsanoen, jokaisella kokoelman \mathcal{A} joukolla on ominaisuus P , mikäli tämä ominaisuus on jokaisella sellaisella \mathcal{A} :n joukolla, jonka jokaisella \mathcal{A} :han kuuluvalla aidolla osajoukolla on kyseinen ominaisuus (tämä on kyseistä joukkoa koskeva *induktio-oletus*). Induktioperiaate (*) (*induktio osajoukkojen suhteen*) todistetaan osoittamalla seuraavan lemmän avulla, että joukko $\mathcal{B} = \{A \in \mathcal{A} : A \text{lla ei ole ominaisuutta } P\}$ on tyhjä.

Lemma *Olkoon \mathcal{B} epätyhjä kokoelma äärellisiä joukkoja. Tällöin on olemassa sellainen $B \in \mathcal{B}$, että mikään joukon B aito osajoukko ei kuulu kokoelmaan \mathcal{B} .*

Todistus. Koska $\mathcal{B} \neq \emptyset$, joukko $\{|B| : B \in \mathcal{B}\}$ on epätyhjä ja induktioaksioman nojalla on olemassa sellainen $B \in \mathcal{B}$, että jokaisella $C \in \mathcal{B}$ on voimassa $|B| \leq |C|$. Koska jokaiselle $C \subsetneq B$ on voimassa $|B| > |C|$, nähdään ettei mikään B :n aito osajoukko kuulu joukkoon \mathcal{B} . \square

Todistamme nyt tämän periaatteen avulla seuraavan tuloksen.

Lemma *Olkoon f surjektio äärelliseltä joukolta X joukolle Y . Tällöin on olemassa sellainen X :n osajoukko Z , että rajoittumakuvaus $f|_Z$ on bijektio $Z \rightarrow Y$.*

Todistus. Käytämme induktiota osajoukkojen suhteen kokoelmalle $\mathcal{P}(X)$.

Väite pätee tyhjälle joukolle: “tyhjien joukkojen välinen tyhjä kuvaus” on bijektio.

Olkoon nyt $A \subset X$ sellainen epätyhjä joukko, että väite pätee surjektioille $B \rightarrow U$, missä $B \subsetneq A$. Osoitamme, että se pätee myös surjektioille $g : A \rightarrow V$. Jos g on injektio, niin g on bijektio. Oletamme, että g ei ole injektio. Tällöin on olemassa sellaiset A :n alkiot p ja q , että $p \neq q$ ja $g(p) = g(q)$. Merkitsemme $B = A \setminus \{p\}$ ja panemme merkille, että rajoittumakuvaus $g|_B$ on surjektio $B \rightarrow V$. Induktio-oletuksesta seuraa, että on olemassa sellainen $C \subset B$, että kuvaus $(g|_B)|_C$ on bijektio $C \rightarrow V$. Mutta nyt $C \subset A$ ja kuvaus $g|_C = (g|_B)|_C$ on bijektio $C \rightarrow V$. Olemme suorittaneet induktioaskeleen. Induktioperiaatteen (*) nojalla väite pätee kaikille X :n osajoukoille ja täten myös X :lle. \square

Seuraus *Jos äärelliseltä joukolta A on surjektio joukolle B , niin joukko B on äärellinen ja $|A| \geq |B|$.*

Induktio osajoukkojen suhteen vastaa pikemminkin toista kuin ensimmäistä induktioperiaatetta, koska siihen liittyvässä induktio-oletuksessa vaadimme joukon *kaikkien* (\mathcal{A} :han kuuluvien) aitojen osajoukkojen toteuttavan ehdon P . Mainitsemme vielä lopuksi heikommän version tästä induktiosta, joka vastaa ensimmäistä induktioperiaatetta.

Edellisessä todistuksessa suoritimme induktiota osajoukkojen suhteen äärellisen joukon X potenssijoukossa $\mathcal{P}(X)$ ja saimme haluttua johtopäätöstä $P(X)$ vahvemman johtopäätöksen $(\forall A \subset X)P(A)$. Mikäli meille tällaisessa tilanteessa riittää johtopäätös $P(X)$, niin voimme käyttää seuraavaa käyttökelpoista heikompa versiota edellisestä induktioperiaatteesta:

$$P(\emptyset) \& [(\forall A \subset X)((\forall x \in X \setminus A)(P(A) \implies P(A \cup \{x\})) \implies P(X)]. \quad (**)$$

Tämän tuloksen avulla voimme todistaa äärellisiä joukkoja koskevia väitteitä “yksi alkio kerrallaan”.

Paitsi osajoukkojen suhteen, voimme suorittaa induktiota ja rekursiota vaikkapa (äärellisen) luettelon osaluetteloiden tai lauseen osalauseiden suhteen. Mainitsemme tässä esimerkkinä nk L-systeemit, jotka perustuvat “uudelleenkirjoitukseen”: lähdemme liikkeelle merkkijonosta, vaikkapa $+F - -F + +F$, kirjoitamme sen uudelleen sijoittamalla jokaisen F :n tilalle saman merkkijonon, jolloin saamme jonon $+ + F - -F + +F - - + F - -F + +F + + + F - -F + +F$; toistamme tätä “uudelleenkirjoitusta” halutun määrän kertoja jolloin päädyimme merkkijonoon, jonka “suoritamme” korvaamalla siinä esiintyvät F :t jollain “toimenpiteellä”: esimerkiksi toimenpiteellä “piirrä 1cm pituinen viiva eteenpäin”, jolloin “eteenpäin määräytyy aikaisemmasta jonon osasta kun merkki $+$ on tulkittu komentona “käännä kulman α verran myötäpäivään” ja merkki $-$ komentona “käännä kulman α verran vastapäivään”. Suhteellisen yksinkertaisten L-systeemien avulla voimme kuvata esimerkiksi kasvien muotoa ja monia muita asioita.

IV. KERTOMA JA BINOMIKERTOIMET

IV 1. Kertoma.

Määrittelimme edellä luonnollisen luvun n kertoman $n!$ rekursiivisesti ja totesimme, että $n!$ on tulo $1 \cdot 2 \cdot \dots \cdot n$. Näillä luvuilla on suuri merkitys laskettaessa erilaisia lukumääriä ja äärellisten joukkojen kokoja. Seuraavassa tarkastelemme eräitä lukumääräongelmia. Luvun lopussa esitämme arvion lukujen $n!$ suuruusluokasta lukuihin n^n nähden suurilla $n:n$ arvoilla.

Tiedämme aikaisemmasta, että erikokoisten äärellisten joukkojen välillä ei ole bijektiivistä kuvausta. Kertomien avulla voimme määrittää samankokoisten joukkojen välisten bijektioiden lukumäärän.

Lause Jos X ja Y ovat n -joukkoja, niin

$$|\{f : f \text{ on bijektio } X \rightarrow Y\}| = n!$$

Todistus. Merkitsemme $B(X, Y) = \{f : f \text{ on bijektio } X \rightarrow Y\}$ ja todistamme induktiolla luvun $n = |X| = |Y|$ suhteen, että $|B(X, Y)| = n!$

Jos $n = 0$, niin tällöin $X = Y = \emptyset$; tässä tapauksessa on voimassa $B(X, Y) = \{\emptyset\}$ ja näinollen $|B(X, Y)| = 1 = 0!$

Olkoon nyt $n > 0$ sellainen luku, että väite pätee luvulle $n - 1$. Olkoon a joukon X alkio. Merkitsemme jokaisella $y \in Y$,

$$B_y = \{f \in B(X, Y) : f(a) = y\}.$$

Panemme merkille, että $B(X, Y) = \bigcup_{y \in Y} B_y$. Koska joukon $B(X, Y)$ alkioit ovat kuvauksia, joukot B_y , $y \in Y$, ovat keskenään erillisiä. Täten on voimassa $|B(X, Y)| = \sum_{y \in Y} |B_y|$.

Osoitamme, että jokaisella $y \in Y$ on voimassa $|B_y| = (n - 1)!$ Olkoon y joukon Y alkio. Merkitsemme $Z = X \setminus \{a\}$ ja $V = Y \setminus \{y\}$. Koska $|Z| = |V| = n - 1$, induktio-oletuksen nojalla pätee, että $|B(Z, V)| = (n - 1)!$ Määrittelemme kuvauksen $\varphi : B(Z, V) \rightarrow B_y$ merkitsemällä $\varphi(g) = g \cup \{(a, y)\}$ jokaisella $g \in B(Z, V)$; panemme merkille, että $\varphi(g)$ määräytyy ehdoista $\varphi(g)|_Z = g$ ja $\varphi(g)(a) = y$. Kuvaus φ on bijektio, koska sillä on

käänteiskuvaus $\psi : B_y \rightarrow B(Z, V)$, missä $\psi(f) = f|Z$ (tarkista!). Edellisen nojalla pätee, että $|B_y| = |B(Z, V)| = (n - 1)!$

Edellä esitetyn nojalla on voimassa

$$|B(X, Y)| = \sum_{y \in Y} |B_y| = \sum_{y \in Y} (n - 1)! = n \cdot (n - 1)! = n! \quad \square$$

Edellisessä todistuksessa annoimme täsmällisemmän formuloinnin seuraavalle havainnolliselle “todistukselle”. Esitämme joukon X muodossa $X = \{x_1, \dots, x_n\}$. Määrittäessämme bijektiota $f : X \rightarrow Y$ voimme valita $f(x_1)$:ksi minkä tahansa joukon Y n :stä alkioista, $f(x_2)$:ksi minkä tahansa joukon $Y \setminus \{f(x_1)\}$ $n-1$:stä alkioista, ..., ja viimein $f(x_n)$:ksi voimme valita minkä tahansa joukon $Y \setminus \{f(x_1), \dots, f(x_{n-1})\}$ 1:stä alkioista. Täten voimme muodostaa bijektion $n \cdot (n - 1) \cdots 1 = n!$ eri tavalla.

Joukon X kaikki bijektiot itselleen muodostavat joukon X *symmetrisen ryhmän*, jota merkitsemme seuraavasti:

$$Sym(X) = \{f : f \text{ on bijektio } X \rightarrow X\}.$$

Termi “ryhmä” viittaa tässä tiettyyn algebralliseen struktuuriin: joukossa $Sym(X)$ voidaan määritellä “laskutoimitus” \circ merkitsemällä kaikilla $f, g \in Sym(X)$ $g \circ f$:llä kuvausten f ja g yhdistettyä kuvausta (katso harj. 2, teht. 1). Tällä laskutoimituksella “varustettuna” $Sym(X)$ on “ryhmä”; emme kuitenkaan tässä tarkastele tätä algebrallista struktuuria vaan käsittelemme $Sym(X)$:ää ainoastaan joukkona. Edellisen tuloksen nojalla joukolle $Sym(X)$ on voimassa seuraavaa:

Seuraus *Kun X on äärellinen joukko, niin*

$$\boxed{|Sym(X)| = |X|!}$$

Esimerkki Laske kuinka monella eri tavalla voimme sijoittaa kahdeksan tornia shakkilaudan eri ruuduille kun vaadimme, etteivät mitkään kaksi tornia uhkaa toisiaan (kaksi laudalle asetettua tornia uhkaavat toisiaan, mikäli ne ovat joko samalla ruutujen muodostamalla “vaakarivillä” tai samalla “pystyrivillä”).

Ratkaisu: Voimme kuvata kahdeksan tornin sijoittelua kahdeksanalkioisella joukolla $S \subset [8] \times [8]$ kun sovimme, että alkion (i, j) mukanaolo joukossa S merkitsee sitä, että i :nnen

“vaakarivin” ja j :n “pystyrivin” leikkausruutuun on sijoitettu yksi torni. Selvästikin kahteen eri sijoitteluun liittyvät joukot eroavat toisistaan. Täten voimme määrittää “sallittujen” sijoittelujen lukumäärän laskemalla niihin liittyvien joukkojen lukumäärä.

Kahdeksan tornin sijoittelu toteuttaa vaaditun ehdon, että mitkään kaksi tornia eivät uhkaa toisiaan, jos ja vain jos millään ruutujen muodostamalla vaakarivillä ei ole kahta tornia eikä millään pystyrivillä ole kahta tornia; sijoitteluun liittyvän joukon S avulla ilmaistuna kyseinen ehto saa seuraavan muodon: jos (i, j) ja (k, l) ovat joukon S kaksi eri alkioita, niin on oltava voimassa $i \neq k$ ja $j \neq l$. Jos tarkastelemme joukkoa S joukon $[8]$ relaationa, niin ehto $(i, j) \neq (k, l) \Rightarrow i \neq k$ merkitsee sitä, että S :n on oltava kuvaus ja ehto $(i, j) \neq (k, l) \Rightarrow j \neq l$ merkitsee sitä, että kuvauksen S on oltava injektio. Vaatimus, että kuvaus S on joukon $[8] \times [8]$ kahdeksanalkioinen osajoukko merkitsee sitä, että S :n on oltava kuvaus $[8] \rightarrow [8]$; injektio $S : [8] \rightarrow [8]$ on välttämättä bijektio.

Olemme osoittaneet, että jos sijoittelu täyttää vaaditun ehdon, niin siihen liittyvä joukko on bijektio $[8] \rightarrow [8]$; toisaalta näemme helposti, että jokaiseen bijektioon $[8] \rightarrow [8]$ liittyvä sijoittelu toteuttaa vaaditun ehdon. Näin ollen sallittuja sijoitteluja on yhtä monta kuin bijektioita $[8] \rightarrow [8]$ eli $8! = 40320$. □

Palautamme mieliin, että joukon X bijektioita itselleen kutsutaan X :n permutaatioiksi. Toisinaan puhumme myös joukon X järjestyistä. Tässä on taustalla ajatus, että jos “järjestämme” joukon X , eli asetamme sen alkiot johonkin jonoon x_1, x_2, \dots, x_n , missä $n = |X|$, niin permutaatio $f : X \rightarrow X$ “uudelleenjärjestää” X :n jonoon $f(x_1), f(x_2), \dots, f(x_n)$. Kääntäen, permutaation f käänteiskuvaus f^{-1} uudelleenjärjestää jonon $f(x_1), f(x_2), \dots, f(x_n)$ jonoksi x_1, x_2, \dots, x_n .

Jos X on kirjainjoukko, esimerkiksi $\{A, I, N, O, S, T\}$, niin voimme tulkita X :n alkoiden järjestykset “sanoiksi” (joista useimmat ovat “hölynpölyä”), esimerkiksi NOSAIT, ANSIOT, NTIASO, jne. Tällaisessa yhteydessä puhumme myös *anagrammeista* ja sanomme esimerkiksi, että sanat ANSIOT ja SANOIT ovat toistensa anagrammeja.

Edellisen tuloksen nojalla tiedämme, että sanasta ANSIOT voidaan muodostaa $6! = 720$ eri “sanaa” järjestelemällä sen kirjaimet uudelleen. Myöhemmin esitämme kaavan, jonka avulla voimme laskea sanasta tällä tavalla muodostettavien uusien sanojen lukumäärän siinäkin tapauksessa, että sanassa esiintyy samoja kirjaimia useampaan kertaan (kuten vaikkapa sanassa ANSIOTTA).

Olkoon X n -joukko ja Y k -joukko. Edellisen lauseen ja aikaisempien tulosten nojalla kaikkien bijektioiden $X \rightarrow Y$ lukumäärä on 0, mikäli $n \neq k$ ja se on $n!$, mikäli $n = k$. Myöhemmin laskemme kaikkien injektioiden $X \rightarrow Y$ lukumäärän. Seuraava tulos antaa lausekkeen kaikkien kuvausten $X \rightarrow Y$ lukumäärälle.

Lause *Olkoon X n -joukko ja Y k -joukko. Tällöin*

$$|\{f : f \text{ on kuvaus } X \rightarrow Y\}| = k^n$$

Todistus. Merkitsemme $K = \{f : f \text{ on kuvaus } X \rightarrow Y\}$. Esitämme joukon X muodossa $X = \{x_1, \dots, x_n\}$. Määrittelemme kuvauksen $\varphi : K \rightarrow Y^n$ asettamalla $\varphi(f) = (f(x_1), \dots, f(x_n)) \in Y^n$ jokaisella $f \in K(X, Y)$. Kuvaus φ on injektio, koska jokaisella $f \in K$ alkio $f(x_1), \dots, f(x_n)$ määräävät kuvauksen f . Kuvaus φ on surjektio, sillä jokaisella $(y_1, \dots, y_n) \in Y^n$, jos f on kuvaus $x_i \mapsto y_i$, niin tällöin on voimassa $\varphi(f) = (y_1, \dots, y_n)$. Täten φ on bijektio ja aikaisempien tulosten nojalla pätee, että $|K| = |Y|^n$. \square

Olkoon X n -joukko. Kuvauksia $X \rightarrow X$ on edellisen nojalla n^n kappaletta. Koska bijektioita $X \rightarrow X$ on $n!$ kappaletta, niin myöhemmin johdettava arvio lukujen $n!$ ja n^n suhteen suuruusluokasta voidaan tulkita arvioksi siitä, mikä osuus kaikista kuvauksista $X \rightarrow X$ on bijektioita.

IV 2. Binomikertoimet.

Palautamme mieliin, että annetun joukon X potenssijoukko on joukko $\mathcal{P}(X) = \{A : A \subset X\}$. Jos $k \in \mathbb{N}$, niin käytämme joukosta $\mathcal{P}([k])$ lyhennettyä merkintää $\mathcal{P}[k]$.

Koska äärellisen joukon kaikkien osajoukkojen joukko on äärellinen, niin myös sen k -osajoukkojen joukko (missä $k \in \mathbb{N}$) on äärellinen. Joukon $[n]$ k -osajoukkojen lukumäärää merkitsemme symbolilla $\binom{n}{k}$. Annetun joukon X k -alkioisten osajoukkojen muodostamaa joukkoa merkitsemme symbolilla $\mathcal{P}_k(X)$ (jos $X = [m]$, niin merkitsemme lyhyemmin $\mathcal{P}_k[m]$). Siis

$$\binom{n}{k} = |\{A \in \mathcal{P}[n] : |A| = k\}| = |\mathcal{P}_k[n]|$$

Binomikerroin $\binom{n}{k}$ on määritelty kaikilla $n, k \in \mathbb{N}$, mutta $\binom{n}{k} = 0$, mikäli $k > n$; tästä syystä lukuja $\binom{n}{k}$ tarkastellaan lähinnä tilanteessa $k \leq n$.

Selvästi $\binom{n}{0} = \binom{n}{n} = 1$, sillä joukolla on vain yksi tyhjä ja yksi täysi osajoukko. Samoin selvästi $\binom{n}{1} = n$. Toisaalta huomaamme helposti, että luvut $\binom{n}{k}$ ovat parametrin k suhteen *symmetrisiä*: $\binom{n}{k} = \binom{n}{n-k}$ kaikille $k \in [n]$. Tämä seuraa yksinkertaisesti siitä, että jokaista joukon $[n]$ k -osajoukkoa A vastaa yksikäsitteisesti sen komplementti $[n] \setminus A$, joka on $(n - k)$ -osajoukko. Koska luvut $\binom{n}{0}, \dots, \binom{n}{n}$ luettelevat joukon $[n]$ kaikkien osajoukkojen lukumäärät, saamme Luvussa III.2 johdetun, potenssijoukon kokoa koskevan tuloksen nojalla seuraavan identiteetin:

$$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

Pascalin identiteetin nimellä tunnettu palautuskaava ilmaisee luvut $\binom{n}{k}$ lukujen $\binom{n-1}{i}$ avulla seuraavasti.

Lause (Pascalin identiteetti) *Olkoot $n, k \in \mathbb{N}$ ja $0 < k < n$. Tällöin*

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

Todistus. Määritellään $\phi : \mathcal{P}_k[n] \rightarrow \mathcal{P}_{k-1}[n-1] \cup \mathcal{P}_k[n-1]$ kaavalla $\phi(A) = A \setminus \{n\}$. Lukija voi helposti tarkistaa, että kuvaus ϕ on bijektio. \square

Pascalin palautuskaava antaa ns. *Pascalin kolmion*, jossa luvut $\binom{n}{k}$ on lueteltu palautuskaavan mukaisessa järjestyksessä. Seuraavassa kaaviossa luetellaan kyseisen kolmion seitsemän ensimmäistä riviä.

$$\begin{array}{ccccccc} & & & & & & 1 \\ & & & & & & 1 & 1 \\ & & & & & 1 & 2 & 1 \\ & & & 1 & 3 & 3 & 1 \\ & & 1 & 4 & 6 & 4 & 1 \\ & 1 & 5 & 10 & 10 & 5 & 1 \\ 1 & 6 & 15 & 20 & 15 & 6 & 1 \end{array}$$

(Mainittakoon, että Pascalin (1623 – 1662) kolmio julkaistiin Kiinassa v. 1303, ja se oli tunnettu jo aikaisemmin.)

Pienillä $n:n$ arvoilla voimme määrittää luvut $\binom{n}{k}$ täydentämällä Pascalin kolmiota, mutta suuremmille $n:n$ arvoille tämä on liian työlästä. Teoreettisia tarkasteluja varten tarvitsemme joka tapauksessa selkeän lausekkeen luvuille $\binom{n}{k}$. Tällaisen lausekkeen voim-
mekin antaa kertomafunktion avulla.

Lause Kaikille $n, k \in \mathbb{N}$, missä $k \leq n$, on voimassa

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

Todistus. Todistamme lauseen induktiolla luvun n suhteen. Koska $\binom{0}{0} = |\mathcal{P}_0(\emptyset)| = 1 = \frac{0!}{0!0!}$, väite pätee arvolla 0. Oletamme nyt, että $n > 0$ on sellainen luonnollinen luku, että väite pätee arvolla $n - 1$. Olkoon luvulle $k \in \mathbb{N}$ voimassa $k \leq n$. Osoitamme, että $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Jos $k = 0$ tai $k = n$, niin kaava pätee, koska $\binom{n}{0} = \binom{n}{n} = 1 = \frac{n!}{0!n!}$. Oletamme että $0 < k < n$. Pascalin identiteetin nojalla on voimassa $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ ja induktio-
oletuksen nojalla pätee, että $\binom{n-1}{k-1} = \frac{(n-1)!}{(k-1)!(n-k)!}$ ja $\binom{n-1}{k} = \frac{(n-1)!}{k!(n-1-k)!}$; yhdistämällä nämä yhtälöt saamme luvulle $\binom{n}{k}$ lausekkeen

$$\begin{aligned} \binom{n}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1)!}{(k-1)!(n-1-k)!} \left(\frac{1}{n-k} + \frac{1}{k} \right) \\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!} \cdot \frac{n}{k(n-k)} = \frac{n!}{k!(n-k)!}. \quad \square \end{aligned}$$

Yksinkertaisia todennäköisyysongelmia voidaan usein ratkaista laskemalla erilaisten joukkojen tai kuvausten lukumääriä.

Esimerkki Olet täyttänyt lottokaavakkeesta yhden ruudukon eli valinnut seitsemän lukua joukosta [39]. Lottoarvonnassa arvotaan joukon [39] seitsemän alkioita valitsemalla umpimähkään seitsemän palloa, jotka on numeroitu 1,2,3,...,39. Mikä on todennäköisyys, että valitsemasi numerot ovat samat kuin arvonnassa antamat?

Ratkaisu: Arvonta määrää yhden alkion joukosta $\mathcal{P}_7[39]$; koska joukon $\mathcal{P}_7[39]$ kaikkien alkioiden lukumäärä on $\binom{39}{7}$, niin arvonnassa "umpimähkäisyyden" nojalla todennäköisyys

sille, että valintasi antoi “seitsemän oikein” on

$$\frac{1}{\binom{39}{7}} = \frac{7!32!}{39!} = \frac{1 \cdot 2 \cdots 7}{33 \cdot 34 \cdots 39} = \frac{1}{15380937}. \quad \square$$

Olemme jo maininneet muutamia lukuihin $\binom{n}{k}$ liittyviä yhtälöitä. Monia tällaisia yhtälöitä voidaan helposti todistaa edellä johdettua lukujen $\binom{n}{k}$ eksplisiittistä lauseketta käyttämällä, mutta usein voimme perustella yhtälön luontevammin jollain kombinatorisella päättelyllä.

Esimerkki Johdamme kahdella eri tavalla yhtälön

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

(a) *Laskemalla:*

$$\begin{aligned} \binom{n}{r} \binom{r}{k} &= \frac{n!}{r!(n-r)!} \cdot \frac{r!}{k!(r-k)!} = \frac{n!}{(n-r)!k!(r-k)!} \\ &= \frac{n!(n-k)!}{(n-r)!k!(r-k)!(n-k)!} = \frac{n!}{k!(n-k)!} \cdot \frac{(n-k)!}{(n-r)!(r-k)!} = \binom{n}{k} \binom{n-k}{r-k}. \end{aligned}$$

(b) *Kombinatorisella päättelyllä:*

Valitsemme joukon $[n]$ r -osajoukon, ja siitä k -osajoukon. Tämä vastaa valintoja, joissa valitsemme ensin joukon $[n]$ k -osajoukon, ja sitten jäljelle jääneen osan $r-k$ -osajoukon. \square

Lukuja $\binom{n}{k}$ kutsutaan myös *binomikertoimiksi*, sillä ne esiintyvät aukikehitetyn polynomin $(x+y)^n$ termien $x^k y^{n-k}$ kertoimina.

Binomilause: Kaikilla $n \in \mathbb{N}$ ja $x, y \in \mathbb{R}$ on voimassa

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

Todistus. Harjoitustehtävä. \square

Esimerkki: Laske termin x^6 kerroin polynomissa $(1+x)^8$.

Ratkaisu: Binomikaavan nojalla

$$(1+x)^8 = \sum_{i=0}^8 \binom{8}{i} 1^i x^{8-i},$$

joten termin x^6 kerroin on

$$\binom{8}{2} = \frac{8!}{2!6!} = \frac{8 \cdot 7}{2} = 28. \quad \square$$

Edellä määritimme kahden äärellisen joukon välisten bijektioiden sekä kaikkien kuvausten lukumäärät; binomikertoimien avulla voimme nyt määrittää injektioiden lukumäärät. Palautamme ensin mieliin sen tuloksen (harjoitustehtävä 2/2), että mikään kuvaus äärelliseltä joukolta pienempikokoiseen joukkoon ei ole injektio.

Lause *Olkoon X n -joukko ja Y k -joukko. Oletamme, että $n \leq k$. Tällöin*

$$|\{f : f \text{ on injektio } X \rightarrow Y\}| = \frac{k!}{(k-n)!}$$

Todistus. Merkitsemme $I = \{f : f \text{ on injektio } X \rightarrow Y\}$. Kun $f \in I$, niin f on bijektio $X \rightarrow f(X)$, joten on voimassa $f(X) \in \mathcal{P}_n(Y)$. Merkitsemme jokaisella $A \in \mathcal{P}_n(Y)$, $I_A = \{f \in I : f(X) = A\}$; panemme merkille, että on voimassa $I_A = \{f : f \text{ on bijektio } X \rightarrow A\}$, joten aikaisemman lauseen tuloksesta seuraa, että $|I_A| = n!$. Joukot I_A , $A \in \mathcal{P}_n(Y)$, ovat erillisiä ja on voimassa $I = \bigcup_{A \in \mathcal{P}_n(Y)} I_A$; tästä seuraa, että on voimassa

$$|I| = \sum_{A \in \mathcal{P}_n(Y)} |I_A| = \sum_{A \in \mathcal{P}_n(Y)} n! = |\mathcal{P}_n(Y)| \cdot n!$$

Koska on voimassa $|\mathcal{P}_n(Y)| = \binom{k}{n} = \frac{k!}{n!(k-n)!}$, saamme luvulle $|I|$ halutun lausekkeen

$$|I| = |\mathcal{P}_n(Y)| \cdot n! = \frac{k!}{n!(k-n)!} \cdot n! = \frac{k!}{(k-n)!}. \quad \square$$

Ratkaisemme nyt edellisen lauseen avulla seuraavan ongelman:

Ongelma *Mikä on todennäköisyys, että satunnaisesti valitussa $n:n$ ihmisen joukossa kahdella henkilöllä on sama syntymäpäivä?*

Ratkaisu. Ratkaisemme ongelman vain eräiden yksinkertaistavien oletusten vallitessa. Ensinnäkin oletamme, että joukosta on karsittu pois karkauspäivinä syntyneet henkilöt. Toiseksi oletamme, että “satunnaisuudella” on tässä yhteydessä se seuraus, että kaikki vuoden 365 päivää ovat “yhtä todennäköisiä” tarkastelujoukon henkilöiden syntymäpäivinä.

Merkitsemme S :llä mahdollisten syntymäpäivien joukkoa ja J :llä “satunnaista” ihmisjoukkoamme. Tällöin S on 365-joukko ja J on n -joukko. Merkitsemme $s(h)$:llä henkilön $h \in J$ syntymäpäivää. Tällöin s on kuvaus $J \rightarrow S$ ja se ehto, että *kahdella joukon J henkilöllä on sama syntymäpäivä*, voidaan ilmaista ehtona, että *kuvaus s ei ole injektio*.

Koska kaikki syntymäpäivät ovat “yhtä todennäköisiä”, myös kaikki eri “syntymäpäiväjakaumat” eli kuvaukset $J \rightarrow S$ ovat “yhtä todennäköisiä”. Täten voimme laskea etsityn todennäköisyyden osamääränä $\frac{\ell}{k}$, missä ℓ on “suotuisien alkeistapausten”, eli kaikkien epäinjektiivisten kuvausten $J \rightarrow S$ lukumäärä ja k on “kaikkien alkeistapausten”, eli kaikkien kuvausten $J \rightarrow S$ lukumäärä. Kun merkitsemme i :llä kaikkien injektioiden $J \rightarrow S$ lukumäärää, voimme esittää etsityn todennäköisyyden muodossa $\frac{k-i}{k}$ ja siis muodossa $1 - \frac{i}{k}$.

Mikäli on voimassa $n > 365$ eli $|J| > |S|$, niin yksikään kuvaus $J \rightarrow S$ ei ole injektio; tässä tapauksessa on voimassa $i = 0$ ja etsitty todennäköisyys on yksi. Oletamme nyt, että on voimassa $n \leq 365$. Edellisen lauseen nojalla on voimassa $i = \frac{365!}{(365-n)!}$. Aikaisemman tuloksen nojalla on voimassa $k = 365^n$ ja tästä seuraa, että etsitty todennäköisyys on

$$1 - \frac{365!}{365^n \cdot (365 - n)!} = 1 - \frac{(365 - n + 1) \cdot (365 - n + 2) \cdots 364 \cdot 365}{365^n}.$$

Nämä todennäköisyydet lähenevät n :n kasvaessa yllättävän nopeasti lukua 1: todennäköisyys on jo yli $\frac{1}{2}$, jos joukossa on 23 ihmistä ja se on yli 0,97, jos joukossa on 50 ihmistä. \square

Monissa tilanteissa on tarpeen tietää sellaisten kuvausten $f : [n] \rightarrow [k]$ lukumäärä, joilla alkukuvien $f^{-1}\{i\}$, $i \in [k]$, koot on ennalta annettu. Voimme ilmaista tällaiset lukumäärät nk. *multinomikertoimien* avulla. Määrittellemme nämä kertoimet seuraavasti: kun n ja j_1, \dots, j_k ovat sellaisia luonnollisia lukuja, että $j_1 + \dots + j_k = n$, niin asetamme

$$\binom{n}{j_1 \cdots j_k} = \frac{n!}{j_1! \cdot j_2! \cdots j_k!}.$$

Multinomikertoimet yleistävät binomikertoimia, sillä voimme esittää binomikertoimen $\binom{n}{j}$ multinomikertoimena muodossa $\binom{n}{j \ n-j}$. Toisaalta voimme palauttaa multinomikertoimet binomikertoimiin seuraavan palautuskaavan avulla.

Lemma Kun luonnollisille luvuille n ja j_1, \dots, j_k , missä $k > 1$, on voimassa $j_1 + \dots + j_k = n$, niin

$$\binom{n}{j_1 \dots j_k} = \binom{n}{j_1} \binom{n-j_1}{j_2 \dots j_k} = \binom{n-j_k}{j_1 \dots j_{k-1}} \binom{n}{j_k}.$$

Todistus. Todistamme yhtälön $\binom{n}{j_1 \dots j_k} = \binom{n}{j_1} \binom{n-j_1}{j_2 \dots j_k}$. Yhtälö $\binom{n}{j_1 \dots j_k} = \binom{n-j_k}{j_1 \dots j_{k-1}} \binom{n}{j_k}$ todistetaan aivan vastaavasti.

$$\binom{n}{j_1} \binom{n-j_1}{j_2 \dots j_k} = \frac{n!}{j_1! \cdot (n-j_1)!} \cdot \frac{(n-j_1)!}{j_2! \dots j_k!} = \frac{n!}{j_1! \cdot j_2! \dots j_k!} = \binom{n}{j_1 \dots j_k}. \quad \square$$

Palautuskaavan avulla voimme helposti todistaa seuraavan tuloksen, jolla on paljon käyttöä kombinatoriikassa.

Lause Olkoon X n -joukko ja $\{y_1, \dots, y_k\}$ k -joukko, missä $k > 0$, ja olkoon luonnollisille luvuille j_1, \dots, j_k voimassa $j_1 + \dots + j_k = n$. Tällöin joukon

$$\left\{ f : f \text{ on kuvaus } X \rightarrow Y \text{ ja } |f^{-1}\{y_i\}| = j_i \text{ jokaisella } i \in [k] \right\}$$

koko on $\binom{n}{j_1 \dots j_k}$.

Todistus. Todistamme lauseen induktiolla luvun k suhteen. Jos $k = 1$, niin $j_1 = n$ ja väite pätee koska $|\{f : f \text{ on kuvaus } X \rightarrow \{y_1\}\}| = 1 = \binom{n}{n}$.

Oletamme, että $k > 1$ ja väite on jo todistettu kaikille joukoille Z , $k-1$ -joukoille $\{u_1, \dots, u_{k-1}\}$ ja luvuille $h_i \in \mathbb{N}$, missä $h_1 + \dots + h_{k-1} = |Z|$. Olkoon nyt X n -joukko, $\{y_1, \dots, y_k\}$ k -joukko ja olkoon luonnollisille luvuille j_1, \dots, j_k voimassa $j_1 + \dots + j_k = n$. Merkitsemme

$$F = \{f : f \text{ on kuvaus } X \rightarrow \{y_1, \dots, y_k\} \text{ ja } |f^{-1}\{y_i\}| = j_i \text{ jokaisella } i \in [k]\}.$$

Jokaisella $A \in \mathcal{P}_{n-j_k}(X)$ merkitsemme

$$G_A = \{g : g \text{ on kuvaus } A \rightarrow \{y_1, \dots, y_{k-1}\} \text{ ja } |g^{-1}\{y_i\}| = j_i \text{ jokaisella } i \in [k-1]\}$$

ja panemme merkille, että induktio-oletuksen nojalla on voimassa $|G_A| = \binom{n-j_k}{j_1 \dots j_{k-1}}$.

Merkitsemme $G = \bigcup\{G_A : A \in \mathcal{P}_{n-j_k}(X)\}$ ja panemme merkille, että voimme määrittellä kuvauksen $\Theta : F \rightarrow G$ kaavalla $\Theta(f) = f|(X \setminus f^{-1}\{y_k\})$. Tämä kuvaus on bijektio, koska sillä on käänteiskuvaus $\Psi : G \rightarrow F$, missä $\Psi(g)$ on se kuvauksen $g \in G_A$ jatke $X \rightarrow \{y_1, \dots, y_k\}$, jolla on vakioarvo y_k joukossa $X \setminus A$. Näin ollen on voimassa $|F| = |G|$.

Määritämme vielä joukon G koon. Joukot G_A , $A \in \mathcal{P}_{n-j_k}(X)$, ovat keskenään erillisiä, joten on voimassa $|G| = \sum\{|G_A| : A \in \mathcal{P}_{n-j_k}(X)\}$; tästä seuraa aikaisemman nojalla, että on voimassa

$$|G| = \sum\left\{\binom{n-j_k}{j_1 \cdots j_{k-1}} : A \in \mathcal{P}_{n-j_k}(X)\right\} = |\mathcal{P}_{n-j_k}(X)| \binom{n-j_k}{j_1 \cdots j_{k-1}} = \binom{n}{j_k} \binom{n-j_k}{j_1 \cdots j_{k-1}}.$$

Edellisen lemmän sisältämä palautuskaava antaa nyt halutun lausekkeen $\binom{n}{j_1 \cdots j_k}$ luvulle $|G| = |F|$. Induktioaskel on täten suoritettu. \square

Annamme muutamia esimerkkejä edellisen lauseen käytöstä.

Ongelma *Montako eri sanaa voimme muodostaa sanan RAIVORAITTIIT kirjaimista järjestelemällä ne uudelleen?*

Ratkaisu. Voimme esittää sanat 13-jonoina eli (oleellisesti) kuvauksina $[13] \rightarrow \{A, I, O, R, T, V\}$. Sanan on sisällettävä neljä I:tä, kolme T:tä, kaksi A:ta ja R:ää sekä yksi O ja V. Halutunlainen kuvaus $f : [13] \rightarrow \{A, I, O, R, T, V\}$ toteuttaa siis ehdot $|f^{-1}\{I\}| = 4$, $|f^{-1}\{T\}| = 3$, $|f^{-1}\{A\}| = |f^{-1}\{R\}| = 2$ ja $|f^{-1}\{O\}| = |f^{-1}\{V\}| = 1$; tällaisten kuvausten lukumäärä on

$$\binom{13}{4 \ 3 \ 2 \ 2 \ 1 \ 1} = \frac{13!}{4!3!2!2!1!1!} = 2 \cdot 5 \cdot 7 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 = 10810800. \quad \square$$

Ongelma *Muodostamme sanoja järjestelemällä sanan MAANALAINEN kirjaimet uudelleen.*

(a) *Montako eri sanaa näin saadaan?*

(b) *Monessako sanassa on sama ensimmäinen ja viimeinen kirjain?*

Ratkaisu. Sanassa MAANALAINEN on 4 A:ta, 3 N:ää ja yksi M, L, I ja E.

(a) Eri sanoja on $\binom{11}{4 \ 3 \ 1 \ 1 \ 1 \ 1} = 277200$ kappaletta.

(b) Sellaisia sanoja, joilla on A ensimmäisenä ja viimeisenä kirjaimena on yhtä monta kuin sanan MNALAINEN kirjainten erilaisia uudelleenjärjestelyjä eli $\binom{9}{2 \ 3 \ 1 \ 1 \ 1 \ 1} = 30240$ kappaletta. Sellaisia sanoja, joilla on N ensimmäisenä ja viimeisenä kirjaimena on yhtä

monta kuin sanan MAAALAIEN kirjainten erilaisia uudelleenjärjestelyjä eli $\binom{9}{411111} = 15120$ kappaletta. Yhteensä näitä on 45360 kappaletta. \square

Panemme merkille, että edellisen lauseen kuvausjoukko koostuu surjektioista jos ja vain jos on voimassa $j_i > 0$ jokaisella $i \in [k]$. Emme laske tässä n -joukon ja k -joukon välisten surjektioiden lukumäärää yleisesti, mutta selvitämme yhden yksinkertaisen erikoistapauksen edellisen lauseen avulla.

Lemma *Olkoon X n -joukko ja Y $(n-1)$ -joukko. Tällöin surjektioiden $X \rightarrow Y$ lukumäärä on $\frac{n-1}{2} \cdot n!$*

Todistus. Esitämme joukon Y muodossa $\{y_1, \dots, y_{n-1}\}$. Jos j_1, \dots, j_{n-1} ovat sellaisia positiivisia luonnollisia lukuja, että $j_1 + \dots + j_{n-1} = n$, niin luvuista yksi on 2 ja muut ykkösiä. Tästä seuraa edellisen lauseen nojalla, että surjektioiden $X \rightarrow Y$ lukumäärä on

$$\binom{n}{211\dots 1} + \binom{n}{121\dots 1} + \binom{n}{112\dots 1} + \dots + \binom{n}{111\dots 2}.$$

Tässä summassa on $n-1$ yhteenlaskettavaa, joista jokainen on arvoltaan $\frac{n!}{2}$. Täten saamme surjektioiden $X \rightarrow Y$ lukumääräksi $\frac{(n-1)}{2} \cdot n!$ \square

Annamme vielä yhden esimerkin edellisten tulosten käytöstä lukumääräongelmien yhteydessä.

Ongelma *n palloa sijoitetaan umpimähkäisesti n :ään laatikkoon. Mikä on todennäköisyys, että täsmälleen yksi laatikko jää tyhjäksi?*

Ratkaisu. Laskemme todennäköisyyden “suotuisien alkeistapausten” lukumäärän suhteen kaikkien alkeistapausten lukumäärään. Voimme ratkaista tehtävän monella eri tavalla: voimme ajatella pallojen ja/tai laatikoiden olevan keskenään joko identtisiä tai toisistaan erottuvia. Alkeistapausten lukumäärät ovat näissä eri tapauksissa erilaiset, mutta ne antavat saman todennäköisyyden tapahtumalle “täsmälleen yksi laatikko jäi tyhjäksi”.

Koska haluamme käyttää hyväksi edellä johdettuja lausekkeita kuvausten lukumäärille, oletamme että kaikki pallot ja kaikki laatikot ovat toisistaan erottuvia. Tällöin voimme tulkita alkeistapaukset kuvauksina n -joukolta P n -joukolle L . Merkitsemme $K = \{f : f \text{ on kuvaus } P \rightarrow L\}$. Aikaisemman lauseen nojalla on voimassa $|K| = n^n$; tämä on siis kaikkien alkeistapausten lukumäärä.

Laskemme suotuisien alkeistapausten lukumäärän. Merkitsemme $S_\ell = \{f \in K : f(P) = L \setminus \{\ell\}\}$ jokaisella $\ell \in L$. Suotuisien alkeistapausten joukko on $S = \bigcup_{\ell \in L} S_\ell$. Koska joukot S_ℓ , $\ell \in L$, ovat keskenään erillisiä, suotuisien alkeistapausten lukumäärä on $\sum_{\ell \in L} |S_\ell|$.

Jokaisella $\ell \in L$ joukko S_ℓ koostuu kaikista surjektioista $P \rightarrow L \setminus \{\ell\}$. Koska $|P| = n$ ja $|L \setminus \{\ell\}| = n - 1$, edellinen lemma antaa yhtälön $|S_\ell| = \frac{n-1}{2} \cdot n!$. Näin ollen on voimassa

$$|S| = \sum_{\ell \in L} |S_\ell| = n \cdot \frac{n-1}{2} \cdot n! = \binom{n}{2} \cdot n!$$

Etsitty todennäköisyys on edellisen nojalla

$$\frac{|S|}{|K|} = \binom{n}{2} \frac{n!}{n^n}. \quad \square$$

IV 3. Stirlingin kaava.

Todistamme nyt “asymptoottisen” lausekkeen $c \cdot \sqrt{n} e^{-n} n^n$ luonnollisen luvun n kertomalle $n!$ *Asymptoottisuus* tarkoittaa tässä sitä, että lukujen $n!$ ja $c \cdot \sqrt{n} e^{-n} n^n$ osamäärä lähestyy ykköstä luvun n kasvaessa. On syytä panna merkkille, että asymptoottisuudesta *ei seuraa*, että luvut $c \cdot \sqrt{n} e^{-n} n^n$ arvioisivat (eli “approksimoisivat”) lukuja $n!$ “absoluutisesti” eli siten, että erotukset $n! - c \cdot \sqrt{n} e^{-n} n^n$ lähestyisivät nollaa luvun n kasvaessa. Kyseiset erotukset kasvavat rajatta $n:n$ kasvaessa, joten luvut $c \cdot \sqrt{n} e^{-n} n^n$ eivät anna hyvää arviota kertomille $n!$ Sen sijaan kertomien $n!$ ja lukujen $c \cdot \sqrt{n} e^{-n} n^n$ osamäärät lähenevät $n:n$ kasvaessa “hyvin nopeasti” ykköstä, joten saamme hyvän arvion lukujen $n!$ “suuruusluokalle” suurilla $n:n$ arvoilla. Tämän suuruusluokka-arvion käyttökelpoisuus perustuu siihen, että on (laskennallisesti) paljon helpompi arvioida lukujen $c \cdot \sqrt{n} e^{-n} n^n$ kuin kertomien $n!$ suuruutta.

Merkitsemme edellä määritellyä asymptoottisuutta seuraavasti:

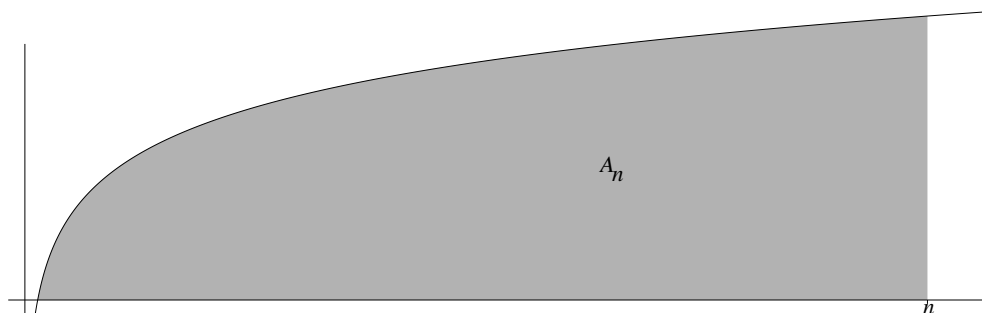
$$n! \sim c \cdot \sqrt{n} e^{-n} n^n.$$

Koska olemme tässä vain kiinnostuneita kertomien suuruusluokasta, meidän ei tarvitse määrittää vakion $c \in \mathbb{R}$ tarkkaa arvoa. Kuuluisa *Stirlingin kaava* sisältää myös tiedon $c:n$ arvosta:

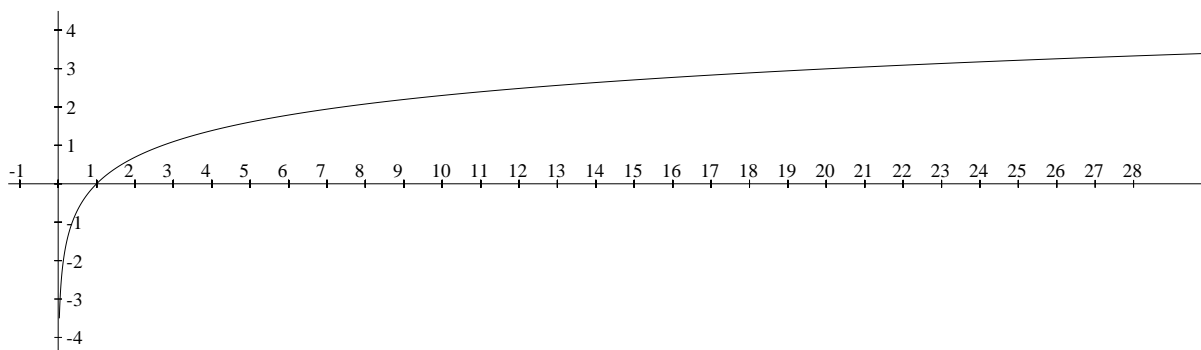
$$n! \sim \sqrt{2\pi n} e^{-n} n^n.$$

(Mainittakoon, että heikomman tuloksen $n! \sim c \cdot \sqrt{n} e^{-n} n^n$ todisti de Moivre jo ennen Stirlingia; Stirlingin ansiona on vakion c tarkan arvon $\sqrt{2\pi}$ määrittäminen.)

Ryhdyimme nyt todistamaan (de Moivren) kaavaa $n! \sim c \cdot \sqrt{n} e^{-n} n^n$. Todistus perustuu siihen, että arvioimme luonnollisen logaritmfunktion kuvaajakäyrän $y = \ln x$ ja x -akselin osan $[1, n]$ väliin jäävän alueen $A_n = \{(x, y) \in \mathbb{R}^2 : 1 \leq x \leq n \text{ ja } 0 \leq y \leq \ln x\}$ pinta-alaa.



Oikeasti logaritmikäyrä $y = \ln x$ on seuraavan näköinen, mutta olemme muuttaneet mittakaavoja pysty- ja vaakasuunnissa, jotta voisimme paremmin havainnollistaa todistuksen kulkua.



Logaritmfunktio $y = \ln x$ on tässä yhteydessä käyttökelpoinen siitä syystä, että logaritmien laskusäännön $\ln(ab) = \ln a + \ln b$ nojalla voimme esittää luonnollisen luvun n kertoman logaritmin lukujen $1, 2, \dots, n$ logaritmien summana:

$$\ln n! = \ln 1 + \ln 2 + \dots + \ln n.$$

Palautamme nyt mieleen muutamia logaritmfunktion ominaisuuksia, joita tarvitsemme seuraavassa todistuksessa. Funktio $y = \ln x$ on määritelty positiivisille x :n arvoille ja $\ln 1 = 0$. Funktio $y = \ln x$ on koko määritysjoukossaan derivoituva ja sen derivaattafunktio on $y = \frac{1}{x}$. Koska derivaatan arvo on jokaisella $x > 0$ positiivinen, funktio $y = \ln x$ on aidosti kasvava. Toisaalta derivaatan arvo, eli kuvaajakäyrälle pisteeseen $(x, \ln x)$ piirretyn tangentin kulmakerroin, pienenee x :n kasvaessa ja tästä seuraa, että kuvaajakäyrä

on *ylöspäin kupera*, mikä tarkoittaa sitä, että käyrän kahden pisteen $(x, \ln x)$ ja $(z, \ln z)$ yhdysjana on aina käyrän alapuolella.

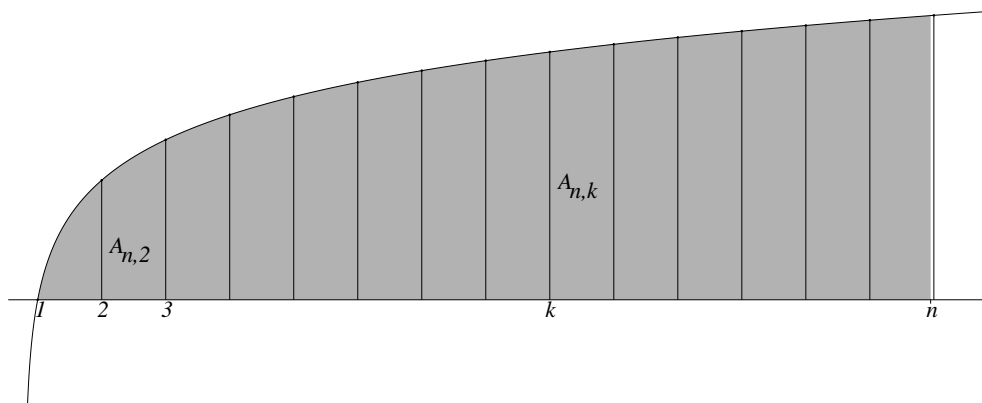
Funktion $y = \ln x$ integraalifunktio on $y = x \ln x - x$, kuten näemme derivoimalla:

$$D(x \ln x - x) = \ln x + x \frac{1}{x} - 1 = \ln x.$$

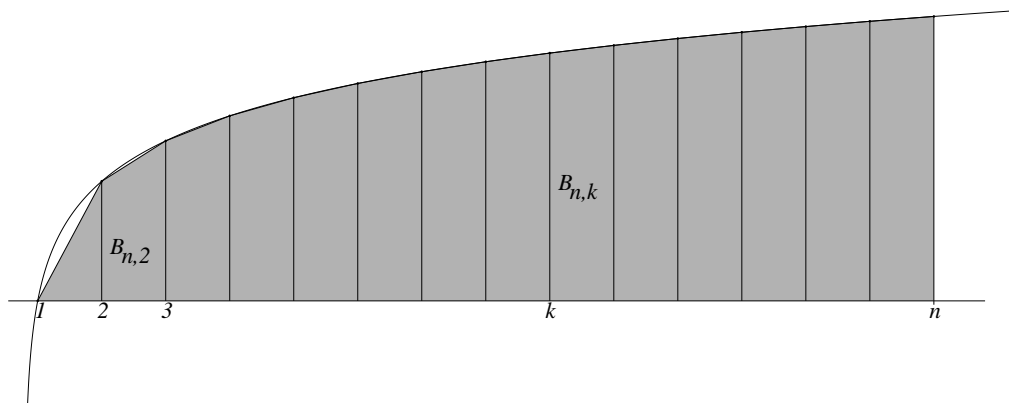
Edellä mainitun tasoalueen A_n pinta-alalle a_n saamme integroimalla tarkan arvon:

$$a_n = \int_1^n \ln x dx = \int_1^n x \ln x - x = n \ln n - n + 1.$$

Aikomuksenamme on nyt arvioida pinta-alaa a_n sekä alas- että ylöspäin. Jaamme x -akselin välin $[1, n]$ osaväleihin $[1, 2], [2, 3], \dots, [n-1, n]$ ja tarkastelemme vastaavien alueen A_n osien $A_{n,k} = \{(x, y) \in A_n : k \leq x \leq k+1\}$ pinta-aloja. On voimassa $A_n = \bigcup_{i=1}^{n-1} A_{n,i}$ ja tästä seuraa, koska alueet $A_{n,k}$ ovat “reunaviivojaan lukuunottamatta” keskenään erillisiä, että alueen A_n pinta-ala voidaan esittää summana osa-alueiden A_1, A_2, \dots, A_{n-1} pinta-aloista. Näin ollen voimme erikseen arvioida osa-alueiden pinta-aloja alas- ja ylöspäin.



Arvioidessamme pinta-aloja alaspäin tarkastelemme alueen A_n asemasta siihen sisältyvää aluetta B_n , joka jää x -akselin ja käyrän pisteitä $(1, \ln 1), (2, \ln 2), \dots, (n, \ln n)$ yhdistävän murtoviivan väliin.



Kyseinen alue sisältyy alueeseen A_n koska käyrän $y = \ln x$ pisteiden yhdysjanoat ovat (päätepisteitään lukuunottamatta) kokonaisuudessaan käyrän alapuolella (käyrän ylöspäin kuperuuden nojalla).

Alueen A_n osa-alueen $A_{n,k}$ ja alueen B_n leikkausaluetta $B_{n,k}$ rajoittaa puolisuunnikas, jonka kärkinä ovat pisteet $(k, 0)$, $(k + 1, 0)$, $(k + 1, \ln(k + 1))$ ja $(k, \ln k)$ (alue $B_{n,1}$ on itse asiassa kolmio, joka tässä tulkitaan “surkastuneeksi puolisuunnikkaaksi”).

Puolisuunnikkaan pinta-ala saadaan kertomalla keskenään yhdensuuntaisten sivujen pituuksien keskiarvo ja yhdensuuntaisten sivujen välinen etäisyys. Aluetta $B_{n,k}$ rajoittavalla puolisuunnikkaalla on kaksi pystysuoraa sivua, joiden keskinäinen etäisyys on yksi ja joiden pituudet ovat $\ln k$ ja $\ln(k + 1)$; täten $B_{n,k}$:n pinta-ala on $\frac{1}{2}(\ln k + \ln(k + 1))$.

Edellisen nojalla alueen B_n pinta-alalla b_n on lauseke

$$\begin{aligned} b_n &= \frac{1}{2}[(\ln 1 + \ln 2) + (\ln 2 + \ln 3) + \cdots + (\ln(n - 1) + \ln n)] \\ &= (\ln 2 + \ln 3 + \cdots + \ln(n - 1) + \ln n) - \frac{1}{2} \ln n \\ &= \ln n! - \frac{1}{2} \ln n. \end{aligned}$$

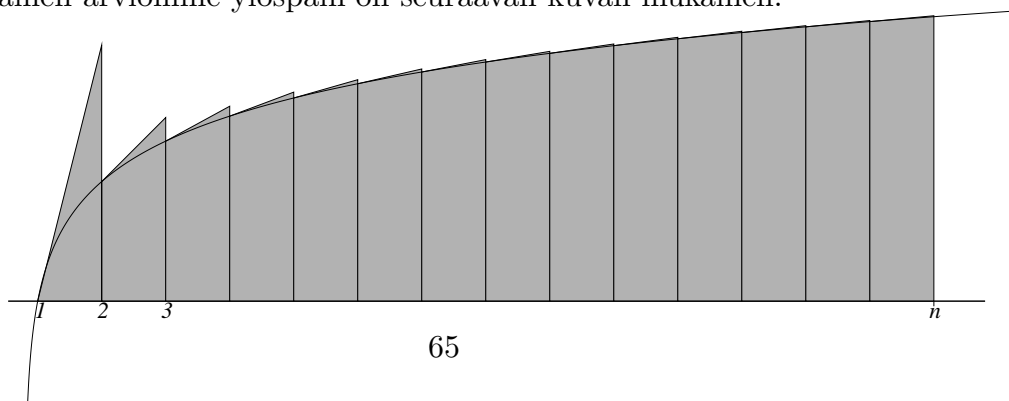
Tarkastelemme seuraavassa alueiden A_n ja B_n pinta-alojen erotusta

$$\varepsilon_n = a_n - b_n = (n \ln n - n + 1) - (\ln n! - \frac{1}{2} \ln n) = (n + \frac{1}{2}) \ln n - n + 1 - \ln n!$$

Tiedämme edellisestä, että luku ε_n on positiivinen jokaisella $n = 1, 2, \dots$. Lisäksi lukujen määritelmästä seuraa, että luvut ε_n kasvavat n :n kasvaessa. Pyrimme seuraavassa löytämään luvuille ε_n yhteisen ylärajan. Tässä tarkoituksessa arvioimme pinta-aloja a_n kahdella eri tavalla ylöspäin.

Käyrän $y = \ln x$ ylöspäin kuperuudesta seuraa, että käyrä on jokaisen tangenttinsa alapuolella. Käytämme hyväksi käyrälle pisteisiin $(k, \ln k)$ piirrettyjä tangentteja ja konstruimme alueita $A_{n,k}$ laajempia puolisuunnikkaiden rajoittamia alueita.

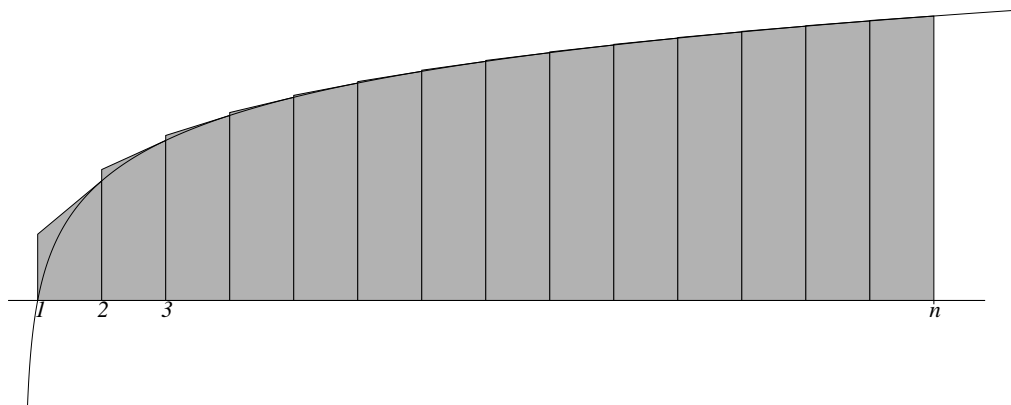
Ensimmäinen arviomme ylöspäin on seuraavan kuvan mukainen:



Pisteeseen $(k, \ln k)$ logaritmikäyrälle piirretyn tangentin kulmakerroin on $\frac{1}{k}$ ja tangentin yhtälö on siten $y - \ln k = \frac{1}{k}(x - k)$; sijoittamalla tähän yhtälöön x :n arvoksi luvun $k + 1$ näemme, että tangentti leikkaa (pysty)suoran $x = k + 1$ pisteessä $(k + 1, \ln k + \frac{1}{k})$; tämän pisteen sekä pisteiden $(k, \ln k)$, $(k, 0)$ ja $(k + 1, 0)$ määrittämä puolisuunnikas sisältää alueen $A_{n,k}$. Täten puolisuunnikkaan pinta-ala $\frac{1}{2}(\ln k + \ln k + \frac{1}{k}) = \ln k + \frac{1}{2k}$ on suurempi tai yhtäsuuri kuin alueen $A_{n,k}$ pinta-ala. Laskemalla yhteen syntyvien $n - 1$:n puolisuunnikkaan pinta-alat saamme seuraavan ylärajan luvulle a_n :

$$\begin{aligned} a_n &\leq \ln 1 + \frac{1}{2} + \ln 2 + \frac{1}{4} + \cdots + \ln(n-1) + \frac{1}{2(n-1)} \\ &= \ln 1 + \ln 2 + \cdots + \ln(n-1) + \ln n - \ln n + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2(n-1)} \\ &= \ln n! - \ln n + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2(n-1)}. \end{aligned}$$

Toinen arviomme ylöspäin on seuraavan kuvan mukainen:



Pisteeseen $(k + 1, \ln(k + 1))$ logaritmikäyrälle piirretyn tangentin kulmakerroin on $\frac{1}{k+1}$ ja tangentin yhtälö on siten $y - \ln(k + 1) = \frac{1}{k+1}(x - k - 1)$; sijoittamalla tähän yhtälöön x :n arvoksi luvun k näemme, että tangentti leikkaa (pysty)suoran $x = k$ pisteessä $(k, \ln(k + 1) - \frac{1}{k+1})$; tämän pisteen sekä pisteiden $(k + 1, \ln(k + 1))$, $(k + 1, 0)$ ja $(k, 0)$ määrittämä puolisuunnikas sisältää alueen $A_{n,k}$. Täten puolisuunnikkaan pinta-ala $\frac{1}{2}(\ln(k + 1) + \ln(k + 1) - \frac{1}{k+1}) = \ln(k + 1) - \frac{1}{2(k+1)}$ on suurempi tai yhtäsuuri kuin alueen $A_{n,k}$ pinta-ala. Laskemalla yhteen syntyvien $n - 1$:n puolisuunnikkaan pinta-alat, saamme seuraavan ylärajan luvulle a_n :

$$a_n \leq \ln 2 - \frac{1}{4} + \ln 3 - \frac{1}{6} + \cdots + \ln n - \frac{1}{2n} = \ln n! - \frac{1}{4} - \frac{1}{6} - \cdots - \frac{1}{2n}.$$

Meillä on nyt kaksi ylärajaa luvulle a_n ja myös näiden ylärajojen keskiarvo on luvun a_n yläraja. Täten on voimassa

$$\begin{aligned} a_n &\leq \frac{1}{2} \left[\left(\ln n! - \ln n + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2(n-1)} \right) + \left(\ln n! - \frac{1}{4} - \frac{1}{6} - \cdots - \frac{1}{2n} \right) \right] \\ &= \ln n! - \frac{\ln n}{2} + \frac{1}{4} - \frac{1}{4n} \\ &\leq \ln n! - \frac{1}{2} \ln n + \frac{1}{4}. \end{aligned}$$

Epäyhtälön $a_n \leq \ln n! - \frac{1}{2} \ln n + \frac{1}{4}$ ja aikaisemmin johdetun yhtälön $b_n = \ln n! - \frac{1}{2} \ln n$ avulla saamme nyt n :stä riippumattoman ylärajan luvulle $\varepsilon_n = a_n - b_n$:

$$\varepsilon_n = a_n - b_n \leq \ln n! - \frac{1}{2} \ln n + \frac{1}{4} - (\ln n! - \frac{1}{2} \ln n) = \frac{1}{4}.$$

Koska lukujono $\varepsilon_1, \varepsilon_2, \dots$ on aidosti kasvava ja koska on voimassa $\varepsilon_n \leq \frac{1}{4}$ jokaisella n , jonolla on (reaalilukujen täydellisyysaksioman nojalla) raja-arvo $r \in \mathbb{R}$. On siis voimassa $\varepsilon_n \rightarrow r$, kun $n \rightarrow \infty$. Palautamme nyt mieliin aikaisemmasta, että $\varepsilon_n = (n + \frac{1}{2}) \ln n - n + 1 - \ln n!$ jokaisella n . Näin ollen on voimassa

$$\left(n + \frac{1}{2}\right) \ln n - n + 1 - \ln n! \rightarrow r \quad \text{kun } n \rightarrow \infty$$

Vetoamme nyt eksponenttifunktion $y = e^x$ jatkuvuuteen ja päätelemme edellisen nojalla, että on voimassa

$$e^{(n+\frac{1}{2}) \ln n - n + 1 - \ln n!} \rightarrow e^r \quad \text{kun } n \rightarrow \infty$$

Eksponenttien laskusääntöjen ja logaritmin määritelmän nojalla on voimassa

$$\begin{aligned} e^{(n+\frac{1}{2}) \ln n - n + 1 - \ln n!} &= e^{\ln n \cdot (n+\frac{1}{2})} \cdot e^{-n} \cdot e^1 \cdot e^{-\ln n!} \\ &= n^{n+\frac{1}{2}} \cdot e^{-n} \cdot e \cdot (n!)^{-1} \\ &= \frac{e \cdot \sqrt{n} \cdot n^n \cdot e^{-n}}{n!} \end{aligned}$$

Kun merkitsemme $c = e^{1-r}$, niin edellisen nojalla on voimassa

$$\frac{c \cdot \sqrt{n} \cdot n^n \cdot e^{-n}}{n!} \rightarrow 1 \quad \text{kun } n \rightarrow \infty.$$

Edellisestä seuraa, että on voimassa $n! \sim c \cdot \sqrt{n} n^n e^{-n}$. \square

Annamme esimerkin siitä, miten voimme käyttää edellä johtamaamme kertoman asymp-
toottista lauseketta myös binomikertoimien tarkasteluun.

Pascalin kolmion tarkastelu antaa vaikutelman, että kiinteällä n :n arvolla binomi-
kertoimet $\frac{n}{k}$ ovat suurimmillaan kun k on lähellä lukua $\frac{n}{2}$. Tämä tosiaan pitää yleisesti
paikkansa, kuten näemme tarkastelemalla kahden (luvun k suhteen) peräkkäisen binomi-
kertoimen suhdetta:

$$\frac{\binom{n}{k}}{\binom{n}{k+1}} = \frac{\frac{n!}{k!(n-k)!}}{\frac{n!}{(k+1)!(n-k-1)!}} = \frac{k+1}{n-k}.$$

On voimassa $\frac{k+1}{n-k} \leq 1$ kun $k \leq \frac{n}{2} - \frac{1}{2}$ ja $\frac{k+1}{n-k} \geq 1$ kun $k \geq \frac{n}{2} - \frac{1}{2}$. Koska k ja n ovat
kokonaislukuja, ehto $k \leq \frac{n}{2} - \frac{1}{2}$ toteutuu, mikäli on voimassa $k < \frac{n}{2}$. Täten on voimassa

$$\binom{n}{k} \leq \binom{n}{k+1} \text{ kun } k < \frac{n}{2} \text{ ja } \binom{n}{k} \geq \binom{n}{k+1} \text{ kun } k \geq \frac{n}{2}.$$

Edellisestä seuraa, että jos n on parillinen, niin $\binom{n}{k}$ saa suurimman arvon kun $k = \frac{n}{2}$ ja
jos n on pariton, niin $\binom{n}{k}$ saa suurimman arvon kun $k = \frac{n \pm 1}{2}$.

Arvioimme nyt Stirlingin kaavan avulla parilliseen lukuun $2n$ liittyvää suurinta bino-
mikertointia $\binom{2n}{n}$. Saamme asymp-
toottisen arvion

$$\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!} \sim \frac{c\sqrt{2ne^{-2n}}(2n)^{2n}}{(c\sqrt{ne^{-n}}n^n)^2} = \frac{\sqrt{2}}{c\sqrt{n}} 2^{2n}.$$

Sijoittamalla c :n tilalle sen arvon $\sqrt{2\pi}$, saamme tulokseksi

$$\binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{\pi n}}.$$

Koska 2^{2n} ilmoittaa $2n$ -joukon kaikkien osajoukkojen lukumäärän, saamme edellisen no-
jalla asymp-
toottisen arvion n -osajoukkojen suhteelliselle osuudelle $2n$ -joukon kaikkien osa-
joukkojen perheessä:

$$\boxed{\frac{\binom{2n}{n}}{2^{2n}} \sim \frac{1}{\sqrt{\pi n}}.}$$

V. VERKOT.

V 1. Verkon määritelmä.

Mainitsimme aikaisemmin, että äärellisen joukon relaatioita voidaan usein tarkastella kuvallisten esitysten, nk. nuolikaavioiden avulla. Puhumme *suhteikosta* (X, R) kun tarkastelemme äärellisen joukon X relaatiota R sellaisen nuolikaavion avulla, jossa X :n alkiot on esitetty vain yhteen kertaan. Palautamme mieliin, että saamme suhteikolle (X, R) graafisen esityksen tällaisena nuolikaaviona kun esitämme joukon X alkiot tason pisteinä (esimerkiksi paperilla) ja sitten piirrämme alkioita x ja y esittävien pisteiden välille nuolen aina kun xRy . Jos xRx , niin nuolen suunnalla ei ole merkitystä ja piirrämme nuolen asemasta “silmutkan” alkioita x esittävän pisteen kohdalle.

Tarkastelemme seuraavassa vain sellaisia suhteikkoja (X, R) , joissa ei ole silmukoita ja joissa “kaikki nuolet ovat käännettävissä”. Silmukattomuus tarkoittaa relaation R irrefleksiivisyyttä eli ehdon $R \cap \Delta_X = \emptyset$ voimassaoloa. Nuolten käännettävyys puolestaan tarkoittaa relaation R symmetrisyyttä eli ehdon $R^{-1} = R$ voimassaoloa.

Jos tiedämme relaation R symmetriseksi, niin järjestetyn parin (x, y) “järjestyksellä ei ole väliä” relaatiossa R mukana olon kannalta. Tästä syystä voimme esittää symmetrisen relaation R “järjestämättömien parien”, eli joukkojen $\{x, y\}$, missä $(x, y) \in R$, avulla. Jos lisäksi tiedämme R :n olevien irrefleksiivinen, niin edellisessä esityksessä ei ole mukana yhtään yksiötä $\{x, x\}$. Tällä tavoin päädyimme seuraavaan määritelmään.

Määritelmä *Verkko* on sellainen pari $G = (X, V)$, missä X on äärellinen joukko ja $V \subset \mathcal{P}_2(X)$.

Kutsumme joukon X alkioita verkon G *pisteiksi* ja joukon V alkioita G :n *viivoiksi*.

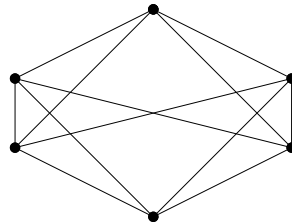
Otamme käyttöön eräitä verkkojen geometriseen esitykseen liittyviä havainnollisia merkintöjä ja nimityksiä. Kutsumme seuraavassa kaikkia kaksioita $\{x, y\}$ *viivoiksi* ja käytämme viivalle $\{x, y\} \in V$ kuvaavaa lyhennysmerkintää \overline{xy} . Sanomme, että alkiot x ja y ovat viivan \overline{xy} *päätepisteitä*. Panemme merkille, että $\overline{xy} = \overline{yx}$.

Olkoon $G = (X, V)$ verkko. Jos $\overline{xz} \in V$, niin sanomme, että “ G :ssä on x :n ja z :n välinen viiva” tai “ x ja z ovat vierekkäin G :ssä”.

Kun $G = (X, V)$ on verkko, niin merkitsemme G :n pisteiden joukkoa X symbolilla P_G ja merkitsemme G :n viivojen joukkoa V symbolilla V_G . Näillä merkinnöillä on voimassa $G = (P_G, V_G)$.

Esitämme verkon $G = (X, V)$ graafisesti esittämällä joukon X alkioit tason pisteinä ja piirtämällä pisteiden x ja y välille viivan tai kaaren aina kun $\overline{xy} \in V$.

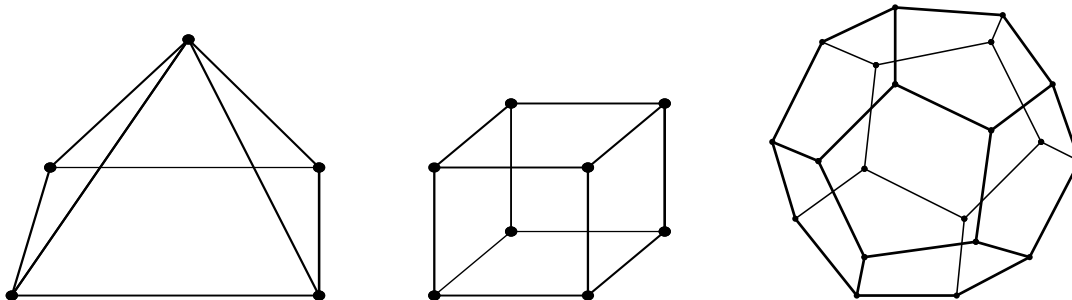
Esimerkki Seuraava kuvio esittää erästä kuusipisteistä ja 12-viivaista verkkoa:



Verkon G piste x on G :n *eristetty piste*, mikäli x ei ole yhdenkään verkon G viivan päätepisteenä. Toisin sanoen, piste x on eristetty G :ssä, mikäli x ei ole vierekkäin minkään G :n pisteen kanssa.

Jos verkon pisteiden joukko on tyhjä, niin tällöin myös verkon viivojen joukko on tyhjä; kutsumme verkkoa (\emptyset, \emptyset) “tyhjäksi verkoksi” ja muiden verkkojen sanomme olevan “epätyhjiä verkkoja”. Huomaamme, että epätyhjässäkin verkossa voi viivojen joukko olla tyhjä; tällaisessa verkossa kaikki pisteet ovat eristettyjä.

Verkkoja esiintyy mitä moninaisimmissa yhteyksissä, kuten ilmenee sellaisista nimityksistä kuten “puhelinverkko”, “tietoverkko”, “hermoverkko” ja “katuverkosto”; myös erilaisia kulkukaavioita, tietokantoja, etsintäpuita, molekyyylimalleja, jne. voidaan esittää verkkoina. Usein käytämme eri yhteyksiin havainnollisesti liittyvää sanastoa yllä esitetyn sanaston asemesta. Esimerkiksi jokaiseen avaruuden \mathbb{R}^3 monitahokkaaseen liittyvä verkko, jonka pisteinä ovat tahokkaan *kärjet* ja viivoina tahokkaan *särmät*. Pyramidiin, kuutioon ja säännölliseen 12-tahokkaaseen (eli dodekaedriin) liittyvät verkot ovat seuraavan kaltaisia:

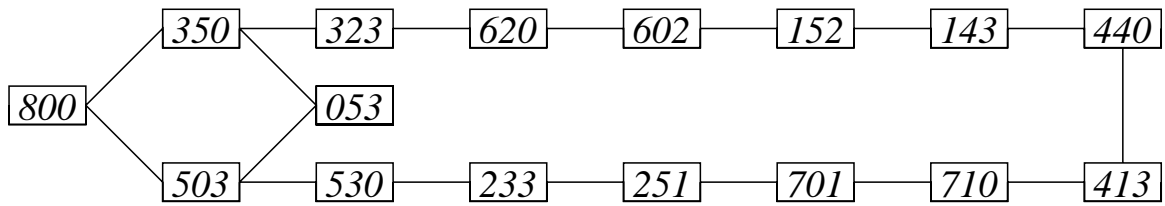


Muissa yhteyksissä voimme puhua esimerkiksi verkon pisteiden ja viivojen asemasta *tiloista* ja *siirtymistä*, verkossa vierekkäin olevien pisteiden voidaan sanoa olevan toistensa *naapureita* jne.

Annamme nyt esimerkin verkkojen käytöstä “käytännön tilanteessa”.

Esimerkki Kahdella henkilöllä on kahdeksan litran vetoinen ruukku täynnä viiniä. Lisäksi heillä on kaksi tyhjää ruukkua, viiden ja kolmen litran vetoiset. Onko heidän mahdollista jakaa viini keskenään tasan kun käytettävissä ei ole muita mittausvälineitä kuin kyseiset kolme ruukkua (ainoa “sallittu” mittaustoimenpide on siis kaataa viiniä ruukusta A ruukkuun B yli läikyttämättä siten, että joko ruukku A tyhjenee tai ruukku B tulee täyteen)?

Ratkaisu: Merkitsemme lukukolmikolla xyz tilannetta, jossa kahdeksan litran ruukussa on x litraa viiniä, viiden litran ruukussa on y litraa ja kolmen litran ruukussa z litraa. Alkutilanne on siis 800. Alkutilanteesta pääsee sallituilla mittaustoimenpiteillä tilanteisiin 350 ja 503. Tilanteesta 350 pääsee takaisin alkutilanteeseen 800 ja lisäksi tilanteisiin 323 ja 053; tilanteesta 503 pääsee tilanteisiin 800, 530 ja 053. Voisimme kirjata muistiin mahdolliset siirtymät tilanteesta toiseen “seuraajaluetteloiden” avulla, mutta saamme paljon havainnollisemman kuvan siirtymien kokonaisuudesta piirtämällä kaavion, jossa kahden eri tilanteen välillä on nuoli, mikäli ensimmäisestä pääsee toiseen sallitulla mittaustoimenpiteellä; kaavio yksinkertaistuu huomattavasti kun piirrämme sen vaiheittain alkamalla alkutilanteesta ja jättämällä pois sellaiset nuolet, jotka vievät “takaisinpäin” (eli viimeisessä vaiheessa saavutetusta tilanteesta sellaiseen tilanteeseen, johon oli jo päästy jossain aikaisemmassa vaiheessa). Jos aloitamme kaavion piirtämisen sivun vasemmasta laidasta ja sijoitamme uudet tilanteet vanhojen oikealle puolen, niin voimme jättää nuolten suunnat merkitsemättä ja päädyimme seuraavan näköiseen kaavioon.



Voimme siis kuvata ongelmaa verkolla, josta näkyy suoraan, että annettu tehtävä on ratkaistavissa ja että viini voidaan jakaa tasan seitsemällä mittauksella.

Määrittelemme seuraavaksi tilanteen, jossa kaksi verkkoa ovat “samanrakenteisia” ja siten verkkojen teorian kannalta oleellisesti samoja.

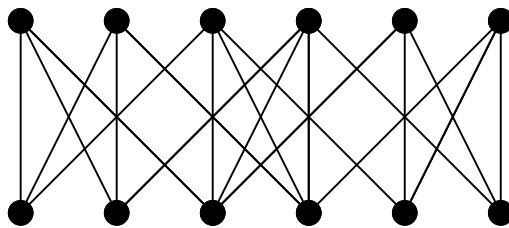
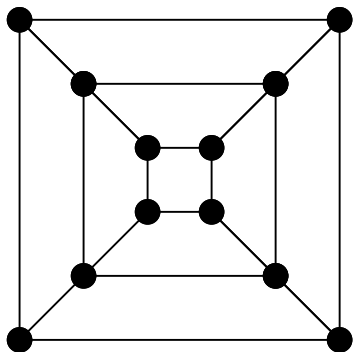
Määritelmä Verkot G ja H ovat *isomorfiset* jos on olemassa sellainen bijektio $\varphi : P_G \rightarrow P_H$, että kaikilla $x, z \in P_G$ on voimassa $\overline{xz} \in V_G$ jos ja vain jos $\overline{\varphi(x)\varphi(z)} \in V_H$; tällaista bijektiota φ kutsutaan verkkojen G ja H väliseksi *isomorfismiksi*.

Voimme liittää jokaiseen injektioon $g : X \rightarrow Y$ vastaavan “viivakuvauksen” $\bar{g} : \mathcal{P}_2(X) \rightarrow \mathcal{P}_2(Y)$, jonka määrittelemme kaavalla $\bar{g}(\overline{xz}) = \overline{g(x)g(z)}$. Tällä merkinnällä voimme luonnehtia verkkojen G ja H pistejoukkojen välisen kuvauksen φ isomorfisuutta seuraavasti:

φ on verkkojen G ja H välinen isomorfismi jos ja vain jos
 φ on bijektio $P_G \rightarrow P_H$ ja $\bar{\varphi}$ on bijektio $V_G \rightarrow V_H$.

Määritelmästä seuraa suoraan, että jos verkot G ja H ovat keskenään isomorfiset, niin tällöin joukoissa P_G ja P_H on yhtä monta alkioita ja joukoissa V_G ja V_H on yhtä monta alkioita. Täten pisteiden, nuolien tai viivojen lukumäärien laskeminen saattaa toisinaan riittää osoittamaan sen, että annetut kaksi verkkoa eivät ole keskenään isomorfiset. Tämä päättely *ei toimi* toiseen suuntaan: verkkojen G ja H isomorfisuuteen ei riitä, että on olemassa bijektiot $\varphi : P_G \rightarrow P_H$ ja $\theta : V_G \rightarrow V_H$, vaan vaaditaan lisäksi, että on oltava $\theta = \bar{\varphi}$.

Usein kahden verkon keskinäisen isomorfisuuden tai ei-isomorfisuuden osoittaminen on käytännössä vaikeaa, varsinkin jos verkkojen pisteiden ja viivojen lukumäärät ovat suuria. Seuraavassa kuvassa esiintyy kaksi erinäköistä verkkoa, jotka voimme kuitenkin suhteellisen helposti nähdä keskenään isomorfisiksi.



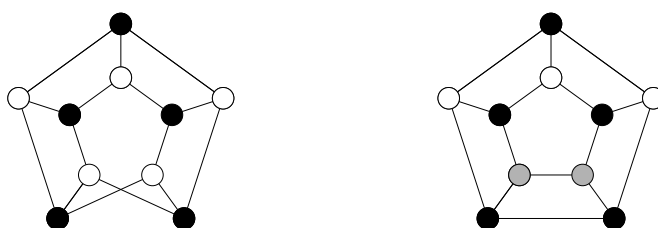
Harjoitustehtävä: Osoita, että edelliset kaksi verkkoa ovat isomorfiset.

Testatessamme annettujen verkkojen mahdollista epäisomorfsuutta meidän kannattaa laskea verkkojen kaikkien pisteiden lukumäärien ohella myös eristettyjen pisteiden lukumäärät: isomorfisilla verkoilla nämä lukumäärät ovat selvästikin samat. Erityisesti, kaksi verkkoa ovat epäisomorfiset, jos toisessa on eristetty piste, mutta toisessa ei ole. Mainitsemme nyt yhden epäisomorfsuustestin, joka ei ole yhtä ilmeinen kuin pelkkä lukumäärien laskeminen.

Sanomme, että verkko G on *kaksijakoinen*, mikäli sen pisteet voidaan värittää kahdella värillä niin, etteivät mitkään kaksi samanväristä pistettä ole verkossa vierekkäin. Tällainen verkko voidaan aina esittää samalla lailla kuin yllä oikeanpuolimmainen verkko: verkon pisteiden joukko jakautuu kahteen erilliseen osaan ja kaikki verkon viivat “kulkevat noiden kahden osan välillä”.

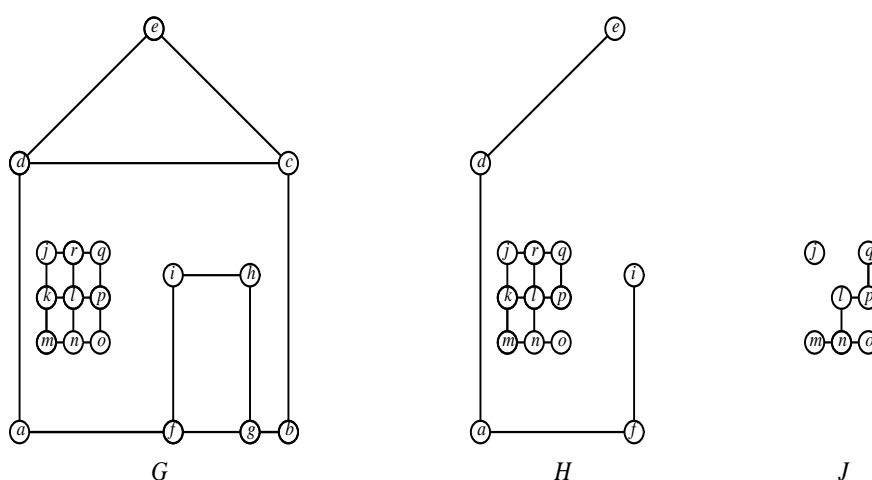
Vaikka verkko olisikin kaksijakoinen, ei tätä ominaisuutta välttämättä huomaa, jos verkolle annettu esitys ei muistuta yllä kuvattua. Kaksijakoisuutta voi kuitenkin helposti testata väritlemällä verkon pisteitä seuraavalla tavalla: aloitamme mielivaltaisesta pisteestä ja väritämme sen mustaksi. Sitten väritämme pisteen kaikki naapurit valkoisiksi, kaikki näiden naapurit mustiksi ja niin edelleen. Jos saamme täten väritettyä kaikki verkon pisteet, eikä missään vaiheessa tule samanvärisiä vierekkäisiä pisteitä, niin verkko on kaksijakoinen. Jos sen sijaan tämä värittäminen päättyy “ristiriitatilanteeseen”, jossa kahdelle vierekkäiselle pisteelle tulee sama väri, niin voimme päätellä, että verkko *ei ole* kaksijakoinen. Koska kaksijakoisuus selvästi “säilyy isomorfismeissa”, voimme päätellä kahden verkon epäisomorfsisuuden siitä, että yksi niistä on kaksijakoinen ja toinen ei ole.



Esimerkki Alla kuvattujen verkkojen ylimmät pisteet on värjätty mustiksi, ylimmän pisteen naapurit valkoisiksi ja näiden naapurit taas mustiksi; tässä vaiheessa oikeanpuolisen verkon alimmat pisteet ovat molemmat mustia ja saimme “ristiriidan”, koska nämä pisteet ovat verkossa vierekkäin. Oikeanpuolinen verkko ei siis ole kaksijakoinen. Kuten alla näkyy, voimme saattaa vasemmanpuolisen verkon värityksen loppuun ilman, että syntyy “ristiriitaa”; tämä verkko on siis kaksijakoinen. Näin näemme, että nämä kaksi verkkoa eivät ole keskenään isomorfiset.



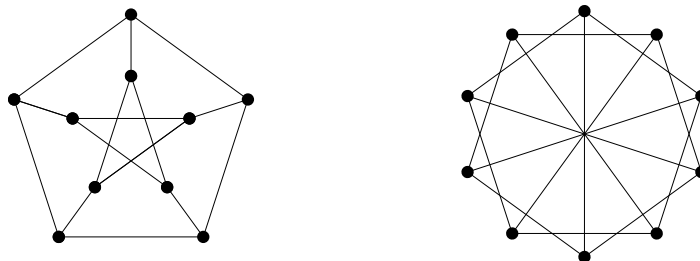
Määritelmä Olkoot G ja H verkkoja. Verkko H on verkon G *aliverkko*, jos $P_H \subset P_G$ ja $V_H \subset V_G$. Verkon G pisteiden joukon P_G osajoukon A *virittämä* G :n *aliverkko* on se G :n aliverkko H , joka määräytyy ehtojen $P_H = A$ ja $V_H = \{\overline{xz} \in V_G : \{x, z\} \subset A\}$ nojalla.

Esimerkki Seuraavista verkoista H on G :n aliverkko ja J on joukon P_H osajoukon $\{j, l, m, n, o, p, q\}$ virittämä H :n aliverkko.

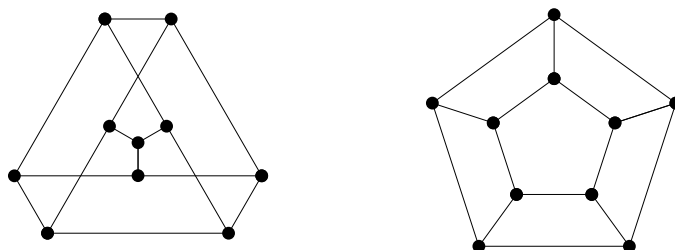


Aliverkkojen tarkastelu auttaa toisinaan isomorfisuustarkasteluissa. Voimme esimerkiksi etsiä annetuista verkoista yksinkertaisia ja suhteellisen helposti havaittavia aliverkkoja, kuten vaikkapa “kolmioita”  tai “nelikulmioita” .

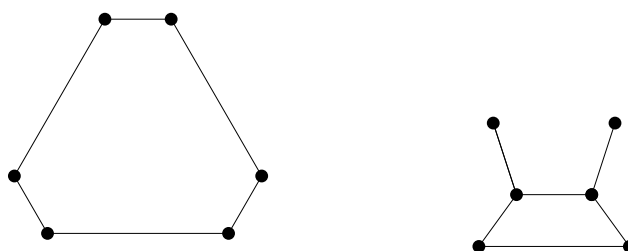
Esimerkki (a) Alla oikeanpuolisessa verkossa on nelikulmio, mutta vasemmanpuolisessa ei ole; verkot ovat siis epäisomorfiset.



(b) Samalla perustelulla kuin (a)-kohdassa voimme osoittaa, että myöskään seuraavat kaksi verkkoa eivät ole keskenään isomorfiset.

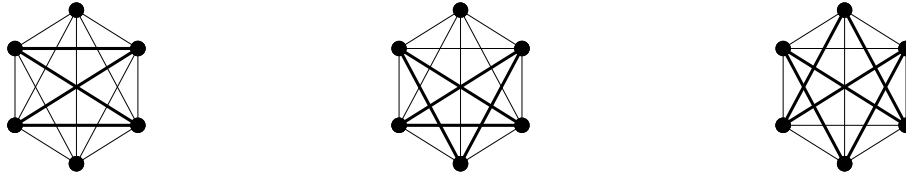


Annamme näiden verkkojen epäisomorfisuudelle toisenkin perustelun. Nämä verkot eivät ole keskenään isomorfiset, sillä jos “poistamme” vasemmanpuolisesta verkosta “keskipisteen” ja sen kolme naapuria, niin jäljellejäävät pisteet virittävät kuusikulmioaliverkon, mutta jos poistamme oikeanpuolisesta verkosta minkä tahansa pisteen (vaikkapa ylimmän pisteen) ja kaikki sen naapurit, niin jäljelle jäävien pisteiden virittämä aliverkko ei ole kuusikulmioverkko, kuten alla oleva kuva osoittaa:



Mainitsemme vielä, että (a)- ja (b)-kohtien vasemmanpuoliset verkot *ovat* keskenään isomorfiset: ne molemmat esittävät nk. *Petersenin verkkoa*.

Kuten jo edellisen esimerkin (a)-kohta osoittaa, suhteellisen yksinkertaistakaan kuviota, kuten 4-, 5- tai 6-kulmiota, ei välttämättä aivan helposti huomaa verkosta, koska tällainen kuvio voi esiintyä “epätavallisessa muodossa”:



Kuviot ovat kaikkein havainnollisin tapa esittää “pieniä” verkkoja mutta jos pisteitä ja nuolia on paljon, tulee kuvioista usein sekavia, eikä niistä ole enää hyötyä. Tästä syystä verkkoja esitetään myös muilla tavoin, esimerkiksi nk. *seuraajaluetteloilla*, joissa luetellaan, jokaiselle verkon $G = (X, V)$ pisteelle x , kaikki pisteen x naapurit G :ssä.

Esimerkki Aikaisemman esimerkin verkko J esitettynä seuraajaluetteloiden avulla:

j	
l	p, n
m	n

n	m, l, o
o	n

p	l, q
q	p

Voimme myös antaa verkon viivajoukon jonkin säännön tai kaavan avulla. Esimerkiksi voimme määrittellä verkon G , jonka pistejoukkona on joukon $[5]$ 2-osajoukkojen perhe, eli $P_G = \mathcal{P}_2[5]$ ja jonka viivajoukko määritellään säännöllä $\overline{AB} \in V_G \iff A \cap B = \emptyset$.

V 2. Pisteiden asteet.

Johdamme seuraavassa hyödyllisen lausekkeen verkon viivojen lukumäärälle. Tähän tarvitsemme verkon pisteen “asteen” käsitettä.

Määritelmä Verkon $G = (X, V)$ pisteen x *aste* on luku

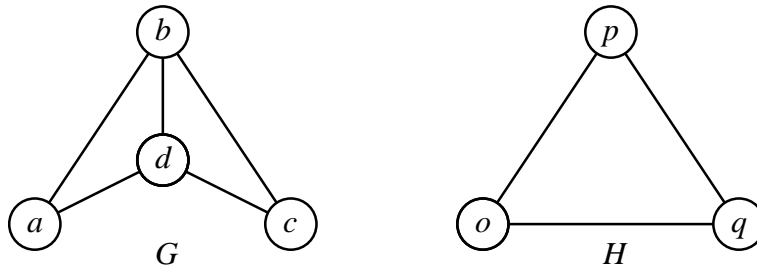
$$d_G(x) = |\{z \in X : \overline{xz} \in V\}|.$$

Luku $d_G(x)$ ilmoittaa siis niiden G :n viivojen lukumäärän, joilla on piste x yhtenä päätepisteenä, eli “pisteestä x lähtevien” viivojen lukumäärän.

Esimerkkejä (a) Olkoon f erillisten äärellisten joukkojen X ja Y välinen kuvaus. Määrittellemme verkon F ehdoilla $P_F = X \cup Y$ ja $V_F = \{\{x, f(x)\} : x \in X\}$. Panemme merkille, että verkko F on kaksijakoinen. Koska f on kuvaus, jokaisella $x \in X$ on voimassa

$d_F(x) = 1$. Kuvaus f on injektio jos ja vain jos jokaisella $y \in Y$ on voimassa $d_F(y) \leq 1$ ja f on surjektio jos ja vain jos jokaisella $y \in Y$ on voimassa $d_F(y) \geq 1$.

(b) Seuraavassa verkossa G on voimassa $d_G(a) = d_G(c) = 2$ ja $d_G(b) = d_G(d) = 3$; verkossa H on jokaisen pisteen aste 2.



Todistamme nyt seuraavan verkon viivojen lukumäärää koskevan tuloksen.

Lause *Verkolle G on voimassa*

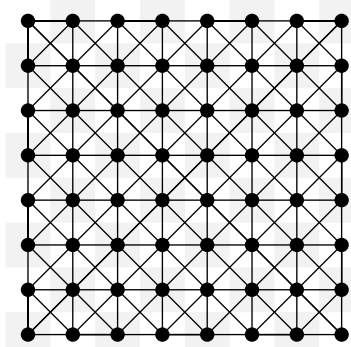
$$\sum_{x \in P_G} d_G(x) = 2 \cdot |V_G|$$

Todistus. On voimassa

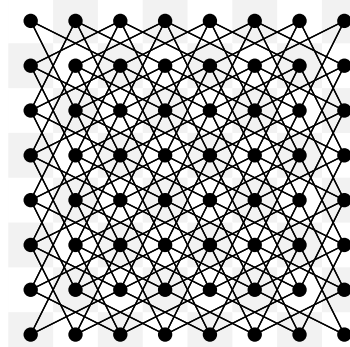
$$\sum_{x \in P_G} d_G(x) = \sum_{x \in P_G} |\{z \in P_G : \overline{xz} \in V_G\}|$$

ja oikeanpuolisessa lausekkeessa kuhunkin viivaan $\overline{ab} \in V_G$ liittyy kaksi alkioita, eli sen päätepisteet a ja b , jotka kumpikin lisäävät yhden summattaviin lukumääriin; näin ollen oikeanpuolisen lausekkeen arvo on $2|V_G|$. \square

Esimerkki Kuhunkin shakkipelin nappulaan, sotamiestä lukuunottamatta, liittyy verkko, jonka pisteinä ovat shakkilaudan *ruudut* ja jossa viiva “yhdistää” kahta ruutua, mikäli yhdestä voi siirtyä toiseen kyseisellä nappulalla. Kuninkaaseen ja hevoseen liittyvät verkot ovat seuraavan näköisiä:



K



H

Käyttämällä edellisen lauseen tulosta voimme helposti laskea edellä kuvattujen verkkojen K ja H viivojen lukumäärät.

Verkossa K laudan “sisäruudun” aste on 8 kun taas “kulmaruutujen” aste on 3 ja muiden “reunaruutujen” aste on 5. Täten verkon K viivojen lukumäärä on puolet luvusta $36 \cdot 8 + 4 \cdot 3 + 24 \cdot 5$ eli $v_K = 210$.

Verkon H pisteen aste on joko 2,3,4,6 tai 8. Neljän kulmaruudun aste on 2. Kulmaruutujen viereisten kahdeksan reunaruudun aste on 3. Lopuilla kuudellatoista reunaruudulla on kullakin asteena 4. Jos poistamme laudan reunaruudut ja tarkastelemme jäljellejäävän 6×6 ruudukon reunaruutuja, niin näemme että neljällä kulmaruudulla on asteena 4 ja muilla kuudellatoista reunaruudulla on kullakin asteena 6. Pienemmän ruudukon kuudellatoista sisäruudulla on kullakin asteena 8. Täten verkon H viivojen lukumäärä on puolet luvusta $4 \cdot 2 + 8 \cdot 3 + 16 \cdot 4 + 4 \cdot 4 + 16 \cdot 6 + 16 \cdot 8$ eli $v_H = 168$. \square

Sanomme verkon G pisteen x olevan *parillisasteinen*, jos luku $d_G(x)$ on parillinen ja *paritonasteinen*, jos luku $d_G(x)$ on pariton. Koska verkon pisteiden asteiden summa on edellisen lauseen nojalla parillinen, saamme lauseelle seuraavan korollaan.

Seuraus *Verkon paritonasteisten pisteiden lukumäärä on parillinen.*

Esimerkki Osoita, että jos talossa on vain yksi ulko-ovi, niin siinä on ainakin yksi huone, jossa on pariton määrä ovia.

Ratkaisu: Merkitsemme talon huoneiden joukkoa H :lla ja merkitsemme u :lla talon ulkopuolta; seuraavassa kutsumme myös u :ta “huoneeksi”. Merkitsemme O :lla huoneiden välisten ovien joukkoa.

Merkitsemme G :llä ehtojen $P_G = H \cup \{u\} \cup O$ ja $V_G = \{\overline{ho} : o \text{ on huoneen } h \text{ ovi}\}$ määrittämää verkkoa. Panemme merkille, että $d_G(u) = 1$. Edellisen korollaarin nojalla on olemassa sellainen G :n paritonasteinen piste a , että $a \neq u$. Jokainen ovi o on kahden huoneen välinen ovi, joten on voimassa $d_G(o) = 2$ ja siten $a \neq o$. Edellisen nojalla pätee, että $a \in H$. Huoneen a ovien lukumäärä on $d_G(a)$, joten tämä lukumäärä on pariton. \square

Sanomme verkon olevan *parillisasteinen*, mikäli sen jokainen piste on parillisasteinen ja *paritonasteinen*, mikäli sen jokainen piste on paritonasteinen. Edellisen korollaarin tuloksesta seuraa, että paritonasteisessa verkossa on parillinen määrä pisteitä.

Mainitsemme lopuksi, että asteiden tarkastelu auttaa toisinaan osoittamaan kahden verkon G ja H epäisomorfisuuden: jos esimerkiksi joukot $\{x \in P_G : d_G(x) = k\}$ ja $\{x \in P_H : d_H(x) = k\}$ ovat erikokoiset (jollain luvulla $k \in \mathbb{N}$), niin G ja H eivät ole isomorfiset tai jos vaikkapa G :ssä on vierekkäin k -asteinen piste ja ℓ -asteinen piste, mutta H :ssa ei ole tällaisia vierekkäisiä pisteitä, niin tällöinkään G ja H eivät ole isomorfiset.

Esimerkki Seuraavat kaksi verkkoa eivät ole isomorfiset: molemmissa on täsmälleen kaksi neliaasteista pistettä, mutta vasemmanpuolisessa verkossa näillä on kaksi yhteistä naapuria ja oikeanpuolisessa vain yksi.



V 3. Kulku verkossa. Yhtenäisyys.

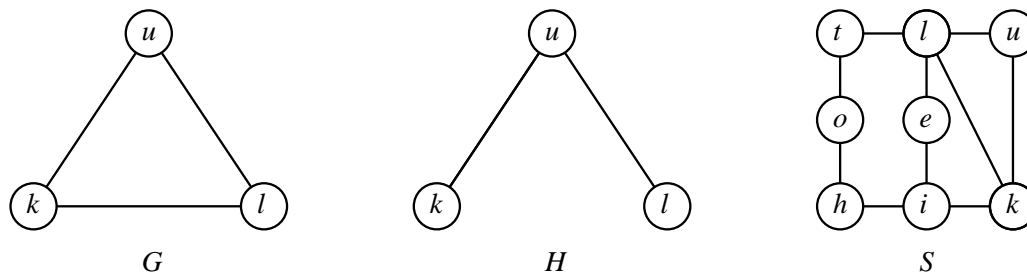
Määrittelemme nyt käsitteen, joka liittyy siihen, miten verkossa “pääsee” pisteestä toiseen.

Määritelmä Olkoon G verkko. *Kulku* G :ssä on sellainen jono $\bar{x} = (x_0, \dots, x_n)$ G :n pisteitä, että $n \in \mathbb{N}$ ja jokaisella $i \in [n]$, viiva $\overline{x_{i-1}x_i}$ on verkon G viiva.

Otamme käyttöön kulkuihin liittyvää sanastoa ja merkintöjä. Olkoon $\bar{x} = (x_0, \dots, x_n)$ kulku verkossa G . Sanomme, että kulku \bar{x} käy pisteissä x_0, \dots, x_n . Sanomme myös, että

\bar{x} on kulku pisteestä x_0 pisteeseen x_n ja merkitsemme $\bar{x} : x_0 \rightarrow x_n$. Jos $x_0 = x_n$, niin sanomme, että \bar{x} on pisteestä x_0 lähtevä kierros G :ssä.

Esimerkkejä (a) Jono (k, u, l, k, u) on kulku allaolevassa verkossa G mutta ei G :n aliverkossa H ; jono $(o, h, i, k, u, l, k, u, k, i, e, l, t, o)$ on kierros verkossa S .



(b) Verkkoja tutkitaan usein kulkujen avulla ja yritetään esimerkiksi selvittää, onko annetussa verkossa G Eulerin kulkua, eli sellaista kulkua, joka kulkee “pitkin jokaista G :n viivaa” täsmälleen yhden kerran tai Hamiltonin kulkua, eli sellaista kulkua, joka käy jokaisessa G :n pisteessä täsmälleen yhden kerran. Hamiltonin kulun olemassaolo on vaikea kysymys, mutta Eulerin kulun olemassaoloa voidaan luonnehtia yksinkertaisilla ja helposti todennettavilla ehdoilla: esimerkiksi, jos G :ssä ei ole eristettyjä pisteitä, niin G :ssä on Eulerin kierros jos ja vain jos G on parillisasteinen ja “yhtenäinen” (määrittelemme tämän käsitteen myöhemmin tässä luvussa).

Olkoon $\bar{x} = (x_0, \dots, x_n)$ kulku verkossa G . Sanomme, että \bar{x} on n -askeleinen kulku ja sanomme myös, että n on kulun \bar{x} pituus. Panemme merkille, että 0-askeleinen kulku verkossa G on jono (x) , missä $x \in P_G$, ja 1-askeleinen kulku on jono (x, y) , missä $\overline{xy} \in V_G$.

Olkoot $\bar{x} = (x_0, \dots, x_n)$ ja $\bar{y} = (y_0, \dots, y_m)$ kulkuja verkossa G . Jos $x_n = y_0$, niin sanomme, että \bar{x} ja \bar{y} ovat peräkkäisiä kulkuja; tässä tilanteessa määrittelemme kulun $\bar{x} \star \bar{y} = (z_0, \dots, z_{n+m})$ asettamalla $z_i = x_i$ jokaisella $0 \leq i \leq n$ ja $z_i = y_{i-n}$ jokaisella $n < i \leq n + m$. Panemme merkille, että kulun $\bar{x} \star \bar{y}$ askelten lukumäärä on kulkujen \bar{x} ja \bar{y} askelten lukumäärien summa.

Olkoot \bar{x} , \bar{y} ja \bar{z} kulkuja verkossa G . Näemme helposti, että jos kulut \bar{x} ja \bar{y} ovat peräkkäisiä ja kulut \bar{y} ja \bar{z} ovat peräkkäisiä, niin tällöin kulut $\bar{x} \star \bar{y}$ ja \bar{z} ovat peräkkäisiä, kulut \bar{x} ja $\bar{y} \star \bar{z}$ ovat peräkkäisiä ja on voimassa

$$(\bar{x} \star \bar{y}) \star \bar{z} = \bar{x} \star (\bar{y} \star \bar{z}).$$

Näin ollen voimme jättää yllä sulut pois ja merkitä yhtälössä esiintyvää kulkua yksinkertaisesti $\bar{x} \star \bar{y} \star \bar{z}$:llä. Vastaavasti voimme esimerkiksi kirjoittaa $\bar{x} \star \bar{y} \star \bar{z} \star \bar{u} \star \bar{v}$, kun kulut \bar{x} ja \bar{y} , kulut \bar{y} ja \bar{z} , kulut \bar{z} ja \bar{u} ja kulut \bar{u} ja \bar{v} ovat peräkkäisiä.

Esimerkki Useissa lautapeleissä, kuten esimerkiksi “Afrikan tähdessä”, pelaaja suorittaa peräkkäisiä kulkuja pelilaudan määräämässä verkossa; pelaaja heittää kunkin pelivuoronsa alussa yhtä tai useampaa noppaa ja tämän jälkeen hän saa tehdä pelinappulallaan peliverkossa jonkun sellaisen kulun, jonka alkupiste on edellisellä vuorolla suoritettun kulun loppupiste ja jonka askelten lukumäärä on heitettyjen noppien silmälukujen summa. \square

Määritelmä Pisteiden x ja y etäisyys $\rho_G(x, y)$ verkossa G on pienin sellainen luku $n \in \mathbb{N}$, että G :ssä on n -askeleinen kulku $x \rightarrow y$; jos G :ssä ei ole yhtään kulkua $x \rightarrow y$, niin asetamme $\rho_G(x, y) = \infty$.

Esimerkki Viereisessä verkossa G

on voimassa

$$\rho_G(a, b) = 4$$

$$\rho_G(a, c) = 8$$

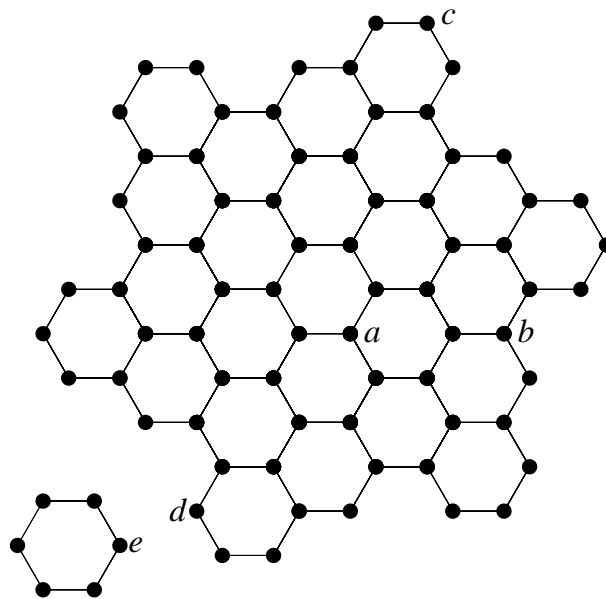
$$\rho_G(a, d) = 6$$

$$\rho_G(b, c) = 8$$

$$\rho_G(b, d) = 8$$

$$\rho_G(c, d) = 14$$

$$\rho_G(d, e) = \infty$$



Laaennamme reaalilukujen yhteenlaskun ja järjestyksen joukkoon $\mathbb{R} \cup \{\infty\}$ sopimalla, että jokaisella $r \in \mathbb{R} \cup \{\infty\}$ on voimassa $r + \infty = \infty + r = \infty$ ja lisäksi $r < \infty$ jos $r \in \mathbb{R}$.

Lemma Verkon G etäisyysfunktio ρ_G toteuttaa seuraavat ehdot kaikilla $a, b, c \in P_G$:

$$1^\circ \rho_G(a, b) = 0 \iff a = b$$

$$2^\circ \rho_G(a, b) = \rho_G(b, a) \quad \text{Symmetrisyysehto}$$

$$3^\circ \rho_G(a, c) \leq \rho_G(a, b) + \rho_G(b, c) \quad \text{Kolmioepäyhtälö}$$

Todistus. Ehdon 1^o voimassaolo seuraa suoraan siitä, että 0-askeleiset kulut ovat muotoa (x) , missä $x \in P_G$.

Ehdon 2^o voimassaolo seuraa siitä, että jos (x_0, \dots, x_n) on kulku G :ssä $a \rightarrow b$, niin (x_n, \dots, x_0) on kulku G :ssä $b \rightarrow a$.

Kohdan 3^o epäyhtälö on selvästi voimassa jos $\rho_G(a, b) = \infty$ tai $\rho_G(b, c) = \infty$. Oletamme, että $\rho_G(a, b) < \infty$ ja $\rho_G(b, c) < \infty$. Tällöin G :ssä on sellaiset kulut $\bar{x} = (x_0, \dots, x_n)$ ja $\bar{y} = (y_0, \dots, y_k)$, että $n = \rho_G(a, b)$, $k = \rho_G(b, c)$, $x_0 = a$, $x_n = b = y_0$ ja $y_k = c$. Kulut \bar{x} ja \bar{y} ovat peräkkäisiä ja $\bar{x} \star \bar{y}$ on kulku G :ssä $a \rightarrow c$. Kulun $\bar{x} \star \bar{y}$ askelten lukumäärä on $n + k = \rho_G(a, b) + \rho_G(b, c)$. Edellisen nojalla on voimassa $\rho_G(a, c) \leq \rho_G(a, b) + \rho_G(b, c)$. \square

Etäisyysfunktion avulla voimme nyt helposti määrittellä ne verkot, joissa mistä tahansa pisteestä "pääsee" mihin tahansa muuhun pisteeseen.

Määritelmä Verkko G on *yhtenäinen*, jos kaikilla $x, y \in P_G$ on voimassa $\rho_G(x, y) < \infty$.

Edellisestä määritelmästä ja etäisyysfunktion määritelmästä seuraa suoraan, että verkko G on yhtenäinen jos ja vain jos G :ssä on kulku $x \rightarrow y$ kaikilla $x, y \in P_G$. Annamme nyt eräitä muita luonnehdintoja verkon yhtenäisyydelle.

Lause Seuraavat ehdot ovat yhtäpitävät epätyhjälle verkolle G :

A. G on yhtenäinen.

B. G :ssä on piste, josta on kulku jokaiseen G :n pisteeseen.

C. G :ssä on kierros, joka käy jokaisessa G :n pisteessä.

Todistus. $A \Rightarrow B$: Tämä seuraa suoraan yhtenäisyyden määritelmästä.

$B \Rightarrow C$: Oletamme, että e on sellainen G :n piste, josta on kulku jokaiseen G :n pisteeseen.

Olkoon $P_G = \{a_1, a_2, \dots, a_n\}$. Jokaisella $i \in [n]$, verkossa G on kulku $\bar{x}_i : e \rightarrow a_i$ ja voimme määrittellä e :stä lähtevän kierroksen \bar{y}_i seuraavasti: jos $\bar{x}_i = (z_0, \dots, z_k)$, niin asetamme

$$\bar{y}_i = (z_0, \dots, z_{k-1}, z_k, z_{k-1}, z_{k-2}, \dots, z_0).$$

Nyt $\bar{y} = \bar{y}_1 \star \bar{y}_2 \star \dots \star \bar{y}_n$ on e :stä lähtevä kierros verkossa G ja \bar{x} käy jokaisessa G :n pisteessä.

$C \Rightarrow A$: Olkoon $\bar{x} = (x_0, \dots, x_n)$ sellainen kulku verkossa G , joka käy jokaisessa G :n pisteessä. Osoitamme, että G on yhtenäinen. Olkoot a ja b G :n pisteitä. Tällöin on olemassa

sellaiset $0 \leq i, j \leq n$, että $x_i = a$ ja $x_j = b$. Olkoon nyt vaikkapa $i \leq j$. Tällöin (x_i, \dots, x_j) on kulku G :ssä $a \rightarrow b$. Täten $\rho_G(a, b) < \infty$. \square

Seuraavassa yhtenäisyyden luonnehdinnassa ei esiinny kulkuja lainkaan.

Lause Verkko G on yhtenäinen jos ja vain jos jokaisella joukon P_G epätyhjällä aidolla osajoukolla A on olemassa sellainen G :n viiva, jonka toinen päätepiste on joukossa A ja toinen joukossa $P_G \setminus A$.

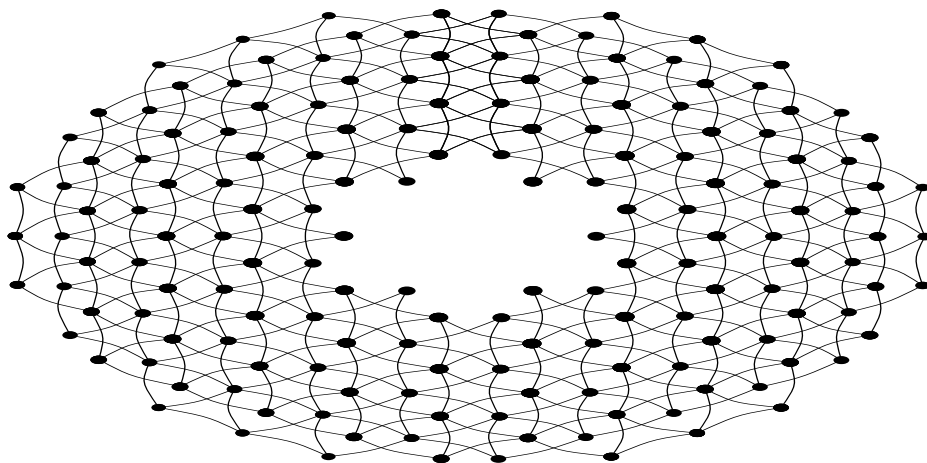
Todistus. *Välttämättömyys.* Olkoon G yhtenäinen verkko ja $A \subsetneq P_G$, $A \neq \emptyset$. Valitsemme pisteen a epätyhjältä joukosta A ja pisteen b epätyhjältä joukosta $P_G \setminus A$. Koska G on yhtenäinen, G :ssä on kulku $(x_0, \dots, x_n) : a \rightarrow b$. Merkitsemme k :lla joukon $\{i \leq n : x_i \in A\}$ suurinta lukua. Tällöin on voimassa $k < n$, koska $x_n = b \in P_G \setminus A$. Nyt $\overline{x_k x_{k+1}}$ on verkon G viiva ja luvun k määritelmän nojalla on voimassa $x_k \in A$ ja $x_{k+1} \notin A$.

Riittävyys. Oletamme, että lauseen ehto toteutuu ja osoitamme, että G on yhtenäinen. Olkoon a G :n piste. Merkitsemme $A = \{z \in P_G : G\text{:ssä on kulku } a \rightarrow z\}$ ja näytämme, että on voimassa $A = P_G$. Teemme vastaväitteen: $A \subsetneq P_G$. On voimassa $A \neq \emptyset$, koska $a \in A$ ja oletuksemme nojalla G :ssä on sellainen viiva \overline{zy} , että $z \in A$ ja $y \notin A$. Koska $z \in A$, verkossa G on kulku $\bar{x} : a \rightarrow z$. Mutta nyt $\bar{x} \star (z, y)$ on kulku G :ssä $a \rightarrow y$ ja tämä on ristiriidassa sen kanssa, että $y \notin A$. Vastaväite johti ristiriitaan ja on siis väärä. Näin ollen pätee, että $A = P_G$. Olemme osoittaneet, että G on yhtenäinen. \square

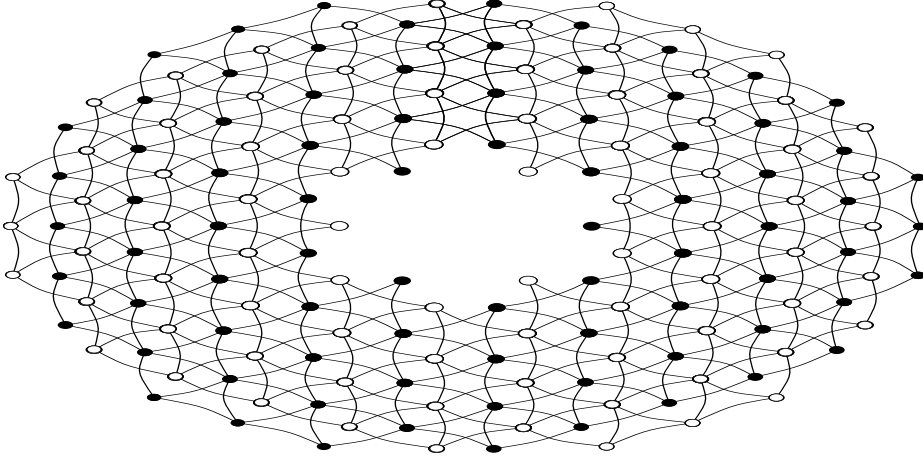
Verkon yhtenäisyyden tai epäyhtenäisyyden osoittaminen saattaa olla hyvin hankalaa, jos verkossa on paljon pisteitä ja viivoja.

Esimerkki

Viereisestä verkosta ei aivan ensimmäisellä silmäyksellä näe yhtenäisyyttä tai epäyhtenäisyyttä:



Yksityiskohtaisempi tarkastelu paljastaa kuitenkin verkosta kaksi “erillään olevaa osaa”:



Verkko on siis edellisen lauseen nojalla epäyhtenäinen. \square

Määrittelemme seuraavaksi eräitä kulkuihin liittyviä verkon osajoukkoja ja tunnuslukuja.

Olkoon G verkko ja a verkon G piste. Määrittelemme rekursiivisesti joukon P_G osajoukot $V_n^G(a)$, $n \in \mathbb{N}$. Asetamme $V_0^G(a) = \{a\}$. Jos joukko $V_n^G(a)$ on jo määritelty, niin joukko $V_{n+1}^G(a)$ koostuu joukon $V_n^G(a)$ pisteistä ja kaikista näiden pisteiden naapureista.

Kutsumme joukkoa $V_n^G(a)$ pisteen a n -ympäristöksi verkossa G . Voimme luonnehtia näitä ympäristöjä seuraavasti:

Lemma Jokaisella $n \in \mathbb{N}$ on voimassa

$$V_n^G(a) = \{x \in P_G : \rho_G(a, x) \leq n\}.$$

Todistus. Todistamme väitteen induktiolla luvun n suhteen.

Väite pätee n :n arvolla 0, koska on voimassa $\rho_G(a, b) = 0 \iff a = b$.

Oletamme, että väite pätee luvulle n . Tällöin se pätee myös luvulle $n + 1$, sillä jokaisella $x \in P_G$ on voimassa

$$\rho_G(a, x) \leq n + 1 \iff \rho_G(a, x) \leq n \text{ tai } \rho_G(a, x) = n + 1$$

$$\iff x \in V_n^G(a) \text{ tai } \exists G\text{:n polku } (z_0, \dots, z_{n+1}) : a \rightarrow x$$

$$\iff x \in V_n^G(a) \text{ tai } \exists \text{ sellainen } z_n \in P_G, \text{ että } \rho_G(a, z_n) \leq n \text{ ja } \overline{z_n x} \in V_G$$

$$\iff x \in V_n^G(a) \text{ tai } \exists \text{ sellainen } z \in V_n^G(a), \text{ että } \overline{z x} \in V_G$$

$$\iff x \in V_{n+1}^G(a). \quad \square$$

Seuraus Jokaisella $n > 0$ on voimassa $V_n^G(a) \setminus V_{n-1}^G(a) = \{x \in P_G : \rho_G(a, x) = n\}$.

Koska $V_0^G(a) = \{a\}$ ja koska joukko $V_1^G(a)$ koostuu pisteestä a ja kaikista a :n naapureista, on voimassa $|V_0^G(a)| = 1$ ja $|V_1^G(a)| = 1 + d_G(a)$. Esitämme nyt arvion yleisen n -ympäristön koolle.

Lause Olkoon G verkko ja $M = \max(\{d_G(x) : x \in P_G\} \cup \{1\})$. Tällöin kaikilla $a \in P_G$ ja $n \geq 1$ on voimassa

$$|V_n^G(a)| \leq M^{n-1}(1 + d_G(a)).$$

Todistus. Panemme aluksi merkille, että jokaisella $n \geq 1$ on voimassa $|V_{n+1}^G(a) \setminus V_n^G(a)| \leq (M - 1)|V_n^G(a) \setminus V_{n-1}^G(a)|$. Tämä seuraa siitä, että jokainen joukon $V_{n+1}^G(a) \setminus V_n^G(a)$ piste on joukon $V_n^G(a) \setminus V_{n-1}^G(a)$ jonkin pisteen naapuri, mutta jokaisella joukon $V_n^G(a) \setminus V_{n-1}^G(a)$ pisteellä on ainakin yksi naapuri joukossa $V_{n-1}^G(a)$, joten pisteellä on joukkoon $V_{n+1}^G(a) \setminus V_n^G(a)$ kuuluvia naapureita korkeintaan $M - 1$ kappaletta.

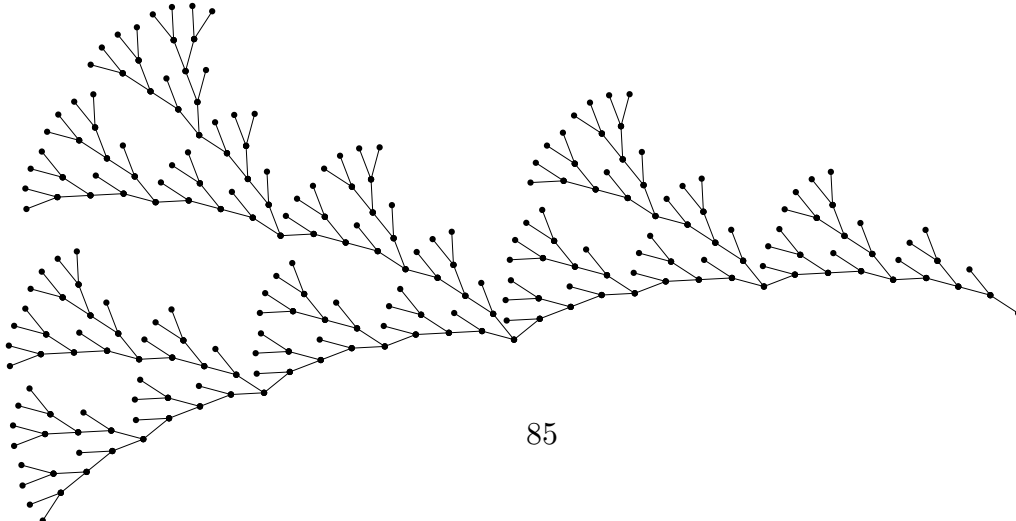
Edellisen nojalla jokaisella $n \geq 1$ on voimassa

$$|V_{n+1}^G(a)| = |V_n^G(a)| + |V_{n+1}^G(a) \setminus V_n^G(a)| \leq |V_n^G(a)| + (M - 1)|V_n^G(a) \setminus V_{n-1}^G(a)| \leq M|V_n^G(a)|.$$

Koska $|V_1^G(a)| = 1 + d_G(a)$, niin edellisen nojalla pätee, että $|V_2^G(a)| \leq M(1 + d_G(a))$, $|V_3^G(a)| \leq M^2(1 + d_G(a))$ jne. Induktiolla n :n suhteen voimme todistaa lauseen epäyhtälön jokaiselle $n \geq 1$. Jätämme induktiotodistuksen yksityiskohdat lukijan suoritettaviksi. \square

Erityisesti, jos yllä on voimassa $d_G(a) < M$, niin saamme arvion $|V_n^G(a)| \leq M^n$ jokaisella $n \in \mathbb{N}$.

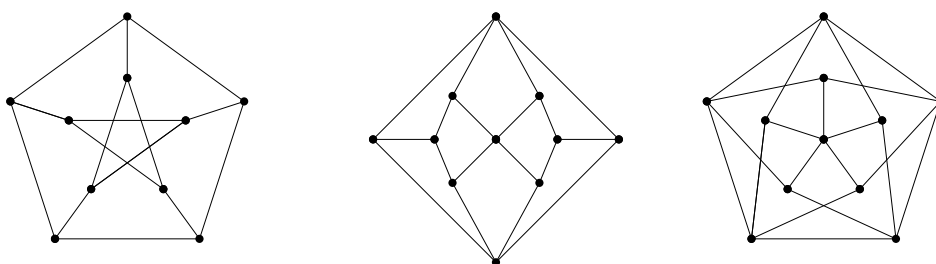
Esimerkki Seuraavan verkon (“L-systeemipuun”) T jokaiselle pisteelle x on voimassa joko $d_T(x) = 3$ tai $d_T(x) = 1$. Edellisen lauseen luku M on siis tässä 3 ja saamme arvion $|V_n^T(a)| \leq 4 \cdot 3^{n-1}$ verkon pisteen a n -ympäristön koolle.



Olkoon G yhtenäinen verkko. Tällöin etäisyys $\rho_G(x, y)$ on luonnollinen luku kaikilla $x, y \in P_G$ ja näin ollen $\{\rho_G(x, y) : x, y \in P_G\}$ on äärellinen lukujoukko. Merkitsemme δ_G :llä kyseisen lukujoukon suurinta lukua ja sanomme, että δ_G on verkon G läpimitta.

Esimerkkejä (a) Edellisen esimerkin verkon T läpimitta on 32 ja verkosta löytyy useampia eri pistepareja a, b , joilla $\rho_T(a, b) = 32$.

(b) Alla vasemmalla kuvatun *Petersenin verkon* ja oikealla kuvatun *Grötzschin verkon* läpimitta on 2. Keskellä kuvatun *Herschelin verkon* läpimitta on 4.



Annamme lopuksi erään arvion verkon läpimitalle verkon pisteiden lukumäärän ja pisteiden asteiden avulla. Arvio perustuu siihen huomioon, että verkon G jokaiselle pisteelle a on voimassa $V_k^G(a) = P_G$ kun $k \geq \delta_G$.

Sanomme, että verkko G on *tasa-asteinen*, mikäli $d_G(x) = d_G(y)$ kaikilla $x, y \in P_G$. Edellisessä esimerkissä kuvattu Petersenin verkko on tasa-asteinen, sillä sen jokaisen pisteen aste on 3.

Olkoon G n -pisteinen verkko, joka *ei ole* tasa-asteinen. Merkitsemme $M = \max\{d_G(x) : x \in P_G\}$. Edellisen lauseen jälkeisen huomautuksen nojalla G :ssä on sellainen piste a , että $|V_\ell^G(a)| \leq M^\ell$ jokaisella $\ell \in \mathbb{N}$. Erityisesti luvulle $k = \delta_G$ on voimassa $n = |P_G| = |V_k^G(a)| \leq M^k$. Ottamalla puolittain logaritmit epäyhtälöstä $n \leq M^k$ saamme epäyhtälön $k \geq \frac{\log n}{\log M}$ eli epäyhtälön

$$\delta_G \geq \frac{\log |P_G|}{\log M}.$$

Panemme vielä merkille, että tasa-asteisen verkon tapauksessa edellinen epäyhtälö ei välttämättä päde: Petersenin verkolle G on voimassa $|P_G| = 10$ ja $M = 3$ ja näin ollen $\frac{\log |P_G|}{\log M} = \frac{1}{\log 3} > 2 = \delta_G$.

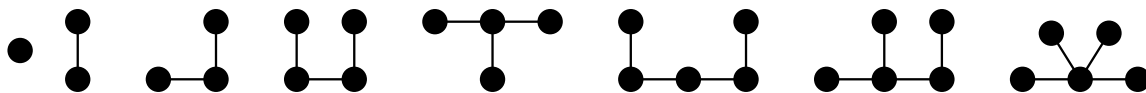
V 4. Puut. Järjestely.



Tarkastelemme vielä lyhyesti “minimaalisesti yhtenäisiä verkkoja”.

Määritelmä Verkko G on *puu*, mikäli G on yhtenäinen, mutta G :llä ei ole sellaista yhtenäistä aliverkkoa H , että $P_H = P_G$ ja $V_H \subsetneq V_G$.

Toisin sanoen, yhtenäinen verkko on puu, mikäli yhdenkin viivan “poistaminen” tekee verkosta epäyhtenäisen.

Esimerkki Seuraavassa on kuvattu kahdeksan “pientä” puuta:



“Monikulmioverkot”, kuten esimerkiksi verkot  ja , ovat yhtenäisiä, mutta ne *eivät ole* puita, sillä niistä kustakin voi poistaa minkä tahansa viivan “tuhoamatta yhtenäisyyttä”. Itse asiassa tällaiset monikulmioverkot ovat tyypillisiä ei-puumaisia yhtenäisiä verkkoja, sillä voidaan osoittaa, että mikä tahansa yhtenäinen verkko, joka ei ole puu, sisältää n -kulmion jollain $n \geq 3$.

Käytämme puiden yhteydessä yleisiin verkkoihin liittyvän sanaston ohella myös oikeisiin puihin liittyvää terminologiaa. Sanomme esimerkiksi, että puun T piste x on T :n *lehti*, mikäli $d_T(x) = 1$. Ne puun pisteet x , joilla $d_G(x) \geq 3$, ovat puun *haarapisteitä*.

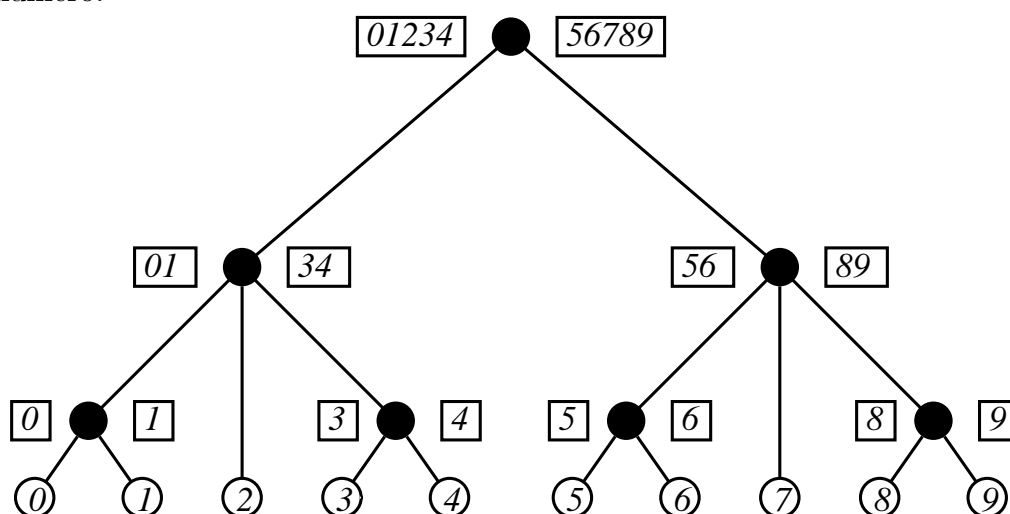
Usein “juurutamme” puun T valitsemalla yhden sen pisteistä “juureksi”. Jos T :n piste a on valittu juureksi, niin merkitsemme T_a :lla näin saatua *juurrettua puuta*. Sanomme, että piste $x \in P_T$ on *korkeudella* $\rho_T(x, a)$ juurretussa puussa T_a . Juurretun puun T_a *korkeus* on luku $\max\{\rho_T(x, a) : x \in P_T\}$. Toinen juurretun puun tunnusluku on “haaraisuus”: T_a :n *haaraisuus* on lukujoukon $\{d_T(a)\} \cup \{d_T(x) - 1 : x \in P_T \setminus \{a\}\}$ suurin luku. Juurretun puun T_a lehdet ovat puun T lehtiä, sillä poikkeuksella, että juuri a ei ole T_a :n lehti, vaikka se olisikin T :n lehti.

Puun juurtaminen on luontevaa siitä syystä, että puita esiintyy mitä erilaisimmissa yhteyksissä (sukupuut, etsintäpuut,...) ja usein puun kaikki pisteet eivät ole tarkastelun

kannalta samanarvoisia, vaan joku niistä on valittu “alkupisteeksi” (yhteinen esi-isä tai -äiti, etsinnän alkutilanne, jne). Termi “juuri” on verraten vakiintunut, mutta huolimatta tähän terminologiaan liittyvistä mielikuvista, suunnatut puut kuvataan usein siten, että “juuri” tulee piirrettävän kuvion ylimmäiseksi pisteeksi.

Esimerkki Seuraava kuva esittää etsintäpuuta, jolla voimme ratkaista yhden (yksinkertaisen) tapauksen niin kutsutusta *väärän kolikon ongelmasta*: tehtävänä on etsiä annetusta kolikkojoukosta mahdollinen väärä raha kun tiedämme, että väärä kolikko on eripainoinen kuin oikeat, keskenään samanpainoiset, kolikot. Apuvälineenä on tasavarsivaaka, joka näyttää joko punnittavien samanpainoisuuden tai eripainoisten punnittavien painojärjestyksen.

Ongelmasta on monta versiota, mutta tarkastelemme sitä tässä yksinkertaisimmillaan: tiedämme, että joukossa on yksi väärä raha, joka on painavampi kuin muut. Jos rahoja on kymmenen kappaletta, niin voimme selvittää kolmella punnituksella, mikä rahoista on väärä: seuraavassa kuvattu puu osoittaa, miten voimme menetellä. Tutkittavat kolikot on numeroitu $0 \dots 9$. Puun mustalla merkityt pisteet vastaavat punnituksia ja niiden viereen on merkitty vaakakuppien sisältö; punnituksen jälkeen haaraudutaan alaoikealle, jos oikeanpuoleisen vaakakupin sisältö osoittautuu painavammaksi kuin vasemmanpuoleisen; alavasemmalle, jos vasemmanpuoleisen kupin sisältö osoittautuu painavammaksi kuin oikeanpuoleisen; suoraan alaspäin, jos kuppien sisällöt osoittautuvat samanpainoisiksi. Puun lehdet vastaavat “etsinnän” lopputulosta: niihin on merkitty vääräksi osoittautuneen kolikon numero.



Kaksi punnitusta ei aina riitä väärän kolikon löytämiseen kymmenen kolikon joukosta. Kuhunkin etsintämenetelmään liittyvän juurretun puun haaraisuus on korkeintaan kolme ja jos jossakin menetelmässä selvittäisiin kahdella punnituksella, niin vastaavan juurretun puun korkeus olisi kaksi. Ei ole vaikea osoittaa, että juurretun puun tunnuslukujen h (haaraisuus), k (korkeus) ja ℓ (lehtien lukumäärä) välillä pätee epäyhtälö $\ell \leq h^k$; erityisesti, jos lehtien lukumäärä on kymmenen ja haaraisuus on kolme, niin korkeuden on oltava suurempi kuin kaksi. Emme kuitenkaan todista mainittua epäyhtälöä, vaan arvioimme seuraavassa (karkeasti) nk. “järjestelypuiden” lehtien lukumäärää.

“Lajittelussa” eli “järjestelyssä” on tehtävänä luetella annetun luku- tai sanalistan (eli -jonon) termit tietyssä järjestyksessä (esimerkiksi suuruus- tai aakkosjärjestyksessä). Olemme kiinnostuneita järjestelymenetelmien “tehokkuudesta” eli siitä, montako eri vaihetta menetelmä vaatii, jotta sen avulla saadaan järjestelyä n :n alkion lista.

Tarkastelemme tässä vain seuraavanlaista järjestelytehtävää: annetun reaalityön (x_1, \dots, x_n) termit on järjesteltävä sellaiseksi jonoksi (y_1, \dots, y_n) , että $y_i \leq y_{i+1}$ jokaisella $i < n$. Voimme ajatella, että “uudelleenjärjestely” jono (y_1, \dots, y_n) on saatu alkuperäisestä jonosta indeksijoukon $[n]$ permutaation φ avulla: $y_i = x_{\varphi(i)}$ jokaisella $i \in [n]$. Näin ollen etsimme sellaista $[n]$:n permutaatiota, eli joukkoon $Sym[n]$ kuuluvaa kuvausta φ , että jonon $(x_{\varphi(1)}, \dots, x_{\varphi(n)})$ luvut ovat nousevassa järjestyksessä.

Rajoitamme vieläkin hieman tehtävänasettelua: yksinkertaisuuden vuoksi oletamme, että jonon (x_1, \dots, x_n) termit ovat kaikki eri lukuja: $x_i \neq x_j$ kun $i \neq j$. Tällöin edellä kuvattuja “kelvollisia” permutaatioita φ on vain yksi.

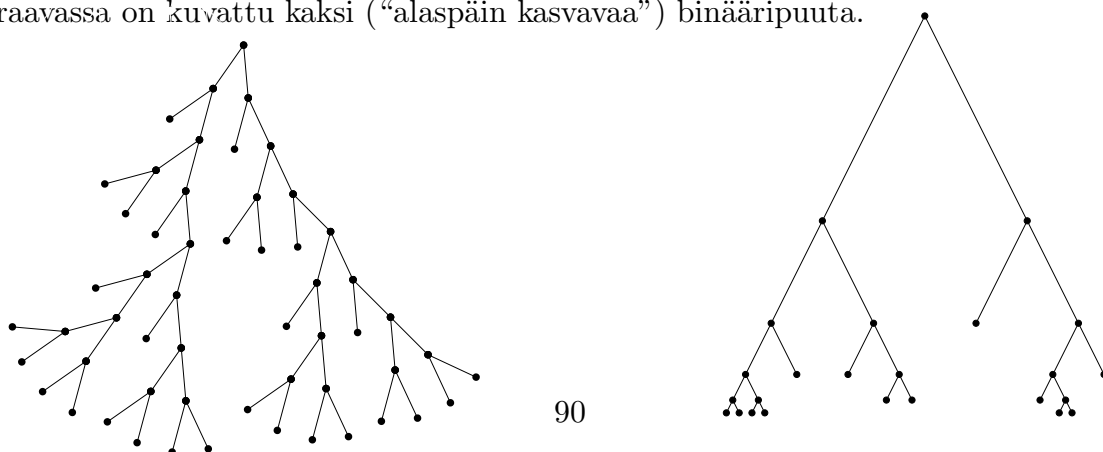
Jos tiedämme etukäteen jotakin jonon (x_1, \dots, x_n) termeistä, vaikkapa että ne kaikki kuuluvat joukkoon $[1000000]$, niin voimme suunnitella järjestelymenetelmän tämän tiedon pohjalta. Tässä tarkastelemme kuitenkin “yleispätevämpiä” menetelmiä, jotka eivät aseta rajoituksia jonon (x_1, \dots, x_n) pituuden tai lukujen x_1, \dots, x_n suuruuden suhteen. Tällaiset yleiset menetelmät perustuvat yleensä “vertailuun”: teemme järjestelyä askeleittain ja k :nnellä askeleella vertaamme joitain kahta luvusta x_1, \dots, x_n ja vertailun tuloksen pohjalta rajoitamme “mahdollisten” järjestelyjen (eli vastaavien permutaatioiden) joukkoa: jos esimerkiksi saimme selville, että $x_i < x_j$, niin järjestelyn aikaisemmissa vaiheissa mahdollisiksi kelpuutetuista permutaatioista hyväksymme enää ne permutaatiot θ , joilla $\theta(i) < \theta(j)$. Tällä tavalla määritämme vaiheittain etsimäämme permutaatiota φ rajoitta-

malla “mahdollisten” permutatioiden joukkoa: pyrimme siihen, että lopulta meillä on vain yksi “mahdollinen”, joka on siten etsimämme “kelvollinen” permutaatio φ .

Yksinkertaisin vertailumenetelmä (eli -algoritmi) on sellainen, jossa vuoronperään vertaillaan kaikkia mahdollisia lukuja x_i ja x_j , missä $i \neq j$. Tällaisia vertailuja on $\binom{n}{2} = \frac{n(n-1)}{2}$ kappaletta. Koska $\frac{n^2}{3} \leq \frac{n(n-1)}{2} \leq n^2$ jokaisella $n \geq 3$, voimme sanoa, että tällaisen järjestelymenetelmän “tehokkuus” (oikeasti “tehottomuus”, esimerkiksi “aikavaativuuden” mielessä) on “suuruusluokkaa” n^2 . Kyseessä on sängen “tehoton” algoritmi: tietojenkäsittelyn kursseilla esitellään järjestelyalgoritmeja, joiden tehokkuus on suuruusluokkaa $n \ln n$. Näiden kahden suuruusluokan ero on huomattava: jos vaikkapa $n = 1\,000\,000$, niin $n^2 = 1\,000\,000\,000\,000$, mutta $n \ln n < 14\,000\,000$. Osoitamme seuraavassa, että tehokkuudeltaan suuruusluokkaa $n \ln n$ oleva järjestelyalgoritmi on tietyssä mielessä “mahdollisimman tehokas”.

Emme rajoitu nimenomaan vertailuun perustuviin järjestelyalgoritmeihin, mutta teemme kuitenkin seuraavat rajoitukset. Oletamme, että jonon (x_1, \dots, x_n) järjestelyssä käyttämämme algoritmi jakautuu vaiheisiin, joissa kussakin esitetään yksi jonoa koskeva kysymys; oletamme lisäksi, että kysymyksellä on kunkin jonon tapauksessa jompikumpi kahdesta mahdollisesta vastauksesta (esimerkiksi kyllä/ei, $1/0$ tai $>/<$). “Yleispätevyyden” vuoksi oletamme, että tehtävät kysymykset ja niihin saatavat vastaukset eivät riipu jonon (x_1, \dots, x_n) luvuista, vaan ainoastaan niiden keskinäisistä suuruussuhteista.

Jos tulkitsemme järjestelyalgoritmin etenemisen edellä kuvailtuun tapaan mahdollisten permutaatioiden joukon rajoittamisena, niin voimme kuvata suoritettavaa järjestelyä “binäärisen” etsintäpuun avulla. Binäärisellä puulla tarkoitamme sellaista puuta, jossa on yksi kaksiasteinen piste ja jokainen muu piste on joko lehti tai kolmiasteinen. Tarkastellemme binääristä puuta juurrettuna puuna, jonka juurena on puun kaksiasteinen piste. Seuraavassa on kuvattu kaksi (“alaspäin kasvavaa”) binääripuuta.



Olkoon binäärinen “ n -jonojen järjestelypuumme” T_n ja olkoon a puun T_n kaksiasteinen piste. Puun T_n lehtinä ovat etsintämme mahdolliset lopputulokset, eli jonon (x_1, \dots, x_n) uudelleenjärjestelyjä määrittäviä permutaatioita vastaavat yksiöt $\{\varphi\}$. Täten puun lehtien lukumäärä on joukon $Sym[n]$ koko, eli $n!$ Lisäksi tiedämme, että puun haaraisuus on kaksi. Yritämme nyt arvioida puun T_n korkeutta k_n alaspäin näiden tietojen avulla.

Palautamme mieleen, että T_n :n korkeus on luku $k_n = \max\{\rho_{T_n}(x, a) : x \in P_{T_n}\}$. Näin ollen on voimassa

$$\{x \in P_{T_n} : \rho_{T_n}(x, a) \leq k_n\} = P_{T_n}.$$

Aikaisemmasta tiedämme, että edellisessä yhtälössä vasemmalla puolella oleva joukko voidaan esittää pisteen a k_n -ympäristönä:

$$\{x \in P_{T_n} : \rho_{T_n}(x, a) \leq k_n\} = V_{k_n}^{T_n}(a).$$

Täten saamme yhtälön $V_{k_n}^{T_n}(a) = P_{T_n}$. Puulle T_n on tapauksessa $n \geq 3$ voimassa $M = \max\{d_{T_n}(x) : x \in P_{T_n}\} = 3$ ja tästä seuraa aikaisemman lauseen nojalla, koska $d_{T_n}(a) = 2 < M$, että on voimassa epäyhtälö $|V_{k_n}^{T_n}(a)| \leq M^{k_n}$ eli $|P_{T_n}| \leq 3^{k_n}$. Koska T_n :ssä on $n!$ lehteä, saamme edellisen nojalla epäyhtälön $3^{k_n} \geq n!$ (joka pätee myös n :n arvoilla 1 ja 2).

Ottamalla epäyhtälöstä $3^{k_n} \geq n!$ puolittain logaritmin kantaluvun e suhteen, saamme epäyhtälön $k_n \ln 3 \geq \ln n!$ eli $k_n \geq \frac{\ln n!}{\ln 3}$. Stirlingin kaavasta $n! \sim c\sqrt{n}n^n e^{-n}$ saamme luvuille $\ln n!$ asympotoottisen arvion $\ln n! \sim \ln c + \frac{1}{2} \ln n + n \ln n - n$ ja tämän arvion sekä edellisen epäyhtälön $k_n \geq \frac{\ln n!}{\ln 3}$ nojalla saamme “asymptoottisen alarajan”

$$\frac{\ln c + \frac{1}{2} \ln n + n \ln n - n}{\ln 3}$$

luville k_n . Tästä seuraa, että on olemassa sellainen positiivinen vakio γ , että on voimassa $k_n \geq \gamma \cdot n \ln n$ jokaisella n ja tämä merkitsee sitä, että järjestelyalgoritmin “tehottomuutta” kuvaava luku k_n on vähintäänkin “suuruusluokkaa $n \ln n$ ”.

[Mainitsemme vielä, että yllä löydetty “asymptoottinen alaraja” ei ole paras mahdollinen: suhteellisen pienellä vaivalla saisimme korvattua alarajan lausekkeen nimittäjän luvulla $\ln 2$; tällä paremmalla arviolla ei kuitenkaan ole merkitystä, jos olemme kiinnostuneita vain “suuruusluokista”.]