

MS-A0402 Diskreetin matematiikan perusteet

Esimerkkejä ym., osa I

G. Gripenberg

Aalto-yliopisto

12. maaliskuuta 2015

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

Niin kauan kun tarkasteltavissa joukoissa on vain äärellisen monta alkioita, kuten joukossa $\{1, 3, 4, 7\}$, ongelmia ei juuri esiinny mutta klassinen vastaesimerkki on ns. Russellin paradoksi: Määritellään

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

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

💡 Joukot ja implikaatiot

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

$C = \{x : x \text{ on kokonaisluku } \geq 2\}$. Mitkä seuraavista väitteistä ovat tosia?

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

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

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

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

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

😊 Päättelysäännöt ja todistukset logiikassa

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

x

$x \rightarrow y$

y

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

😊 Päätelysäännöt ja todistukset logiikassa

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

(a) $X \text{ OR } y$

NOT X

y

(b) $X \text{ AND } y$

X

(c) X

$X \text{ OR } y$

(d) $X \text{ AND } y$

$y \text{ AND } X$

😊 Päätelysäännöt ja todistukset logiikassa, jatk.

Todistus näyttää nyt seuraavalaiselta:

(1) $p \text{ AND } (\text{NOT } p)$: *Oletus*

(2) p : (1) ja (b) missä $x = p$ ja $y = \text{NOT } p$

(3) $p \text{ OR } q$: (2) ja (c) missä $x = p$ ja $y = q$

(4) $(\text{NOT } p) \text{ AND } p$: (1) ja (d) missä $x = p$ ja $y = \text{NOT } p$

(5) $\text{NOT } p$: (1) ja (b) missä $x = \text{NOT } p$ ja $y = p$

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

Näin lause q on tullut todistetuksi.

😊 Esimerkki: Potenssijoukko

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

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

😊 Järjestetyn parin koordinaatit

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

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

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

$$T(p, y) = \exists z((z \in p) \text{ AND } (y \in z)) \text{ AND}$$

$$\forall u \forall v ((u \in p) \text{ AND } (v \in p) \text{ AND NOT } (u == v) \rightarrow \text{NOT } (y \in u) \text{ OR NOT } (y \in v)),$$

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

$$T(p, y) = \exists z \in p(y \in z)$$

$$\text{AND } \forall u \in p \forall v \in p (\text{NOT } (u == v) \rightarrow (y \notin u) \text{ OR } (y \notin v)).$$

💡 Induktio

Osoitamme induktion avulla, että

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

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

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

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

😊 Esimerkki: Osittaisjärjestys

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

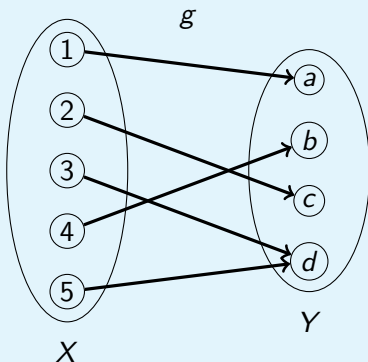
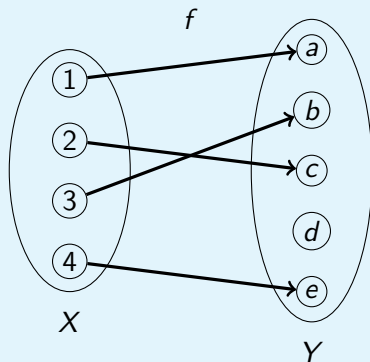
- refleksiivinen: $A \subseteq A$,
- antisymmetrinen: Jos $A \subseteq B$ ja $A \neq B$ niin on olemassa $x \in B$ siten että $x \notin A$ jolloin $B \not\subseteq A$,
- transitiivinen: Jos $A \subseteq B$ ja $B \subseteq C$ niin jokainen A :n alkio on B :n alkio ja koska jokainen B :n alkio on C :n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

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

😊 Esimerkki: Ekvivalenssiluokat

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

Injektiot ja surjektiot



Funktio $f: X \rightarrow Y$ on injektio ("jokaiseen Y :n alkioon tulee korkeintaan yksi suunnattu kaari") mutta se ei ole surjektio koska X :stä ei löydy yhtään alkioita x , siten, että $f(x) = d$.

Funktio $g: X \rightarrow Y$ on surjektio ("jokaiseen Y :n alkioon tulee vähintään yksi suunnattu kaari") mutta se ei ole injektio koska $g(3) = g(5)$ ja $3 \neq 5$.

😊 Listat, lukujonot ja karteesiset tulot funktioina

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

😊 Esimerkki: Funktio, alkukuva, ym.

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

😊 Esimerkki: Alkukuva ja injektiivisyys

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

Miksi?

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

Esimerkki: Iso-O

- Jos $f \in O(n^2)$ ja $g \in O(n^3)$ niin $f \cdot g \in O(n^5)$ koska $|f(n)| \leq C_f n^2$ kun $n \geq N_f$ ja $|g(n)| \leq C_g n^3$ kun $n \geq N_g$ joten $|f(n)g(n)| \leq C_f C_g n^{2+3}$ kun $n \geq \max(N_f, N_g)$.
- Jos $f(n) = n^2$ ja $g(n) = n^3$ niin $f \in O(n^2)$, $g \in O(n^3)$ ja 5 on (tietenkin?) pienin luku p siten, että $f \cdot g \in O(n^p)$.
- Mutta jos 2 on pienin luku p_f siten, että $f \in O(n^{p_f})$ ja 3 on pienin luku p_g siten, että $g \in O(n^{p_g})$ niin siitä ei välttämättä seuraa, että 5 olisi pienin luku p siten, että $f \cdot g \in O(n^p)$ koska voimme esimerkiksi valita

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

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

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

Jos $p = 1$ (pienin luku) tai $p = n$ (suurin luku) niin $n - 1$ vertailua riittää mutta mikä on tilanne yleisessä tapauksessa?

Seuraavaksi osoitamme, että jos $1 \leq p \leq n$ niin tarvittavien vertailujen lukumäärä kuuluu joukkoon $O(n)$, eli on olemassa vakio C siten, että vertailujen lukumäärä on korkeintaan Cn emmekä välitä kovinkaan paljon siitä mikä tämä vakio on:

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

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

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

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

vertailua missä c_0 on vakio.

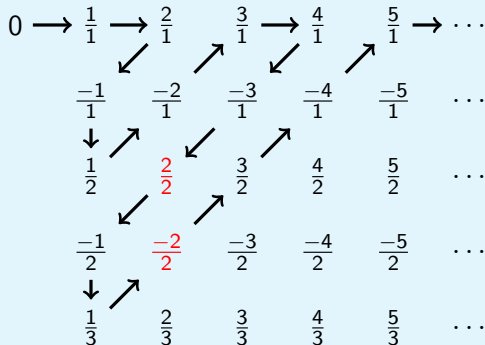
- *Jos $n \leq 20c_0$ voimme järjestää luvut käyttäen $n \log_2(n) \leq n \log_2(20c_0) \leq (20c_0)n$ vertailua ja siten löytää hakemamme luku joten jos valitsemme $C \geq 20c_0$ jolloin $c_0 \leq \frac{1}{20} C$ niin kun $n > 20c_0$ eli $c_0 < \frac{1}{20} n$ toteamme että*

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

ja induktiopäätely toimii.

😊 $|\mathbb{Z}|$ ja $|\mathbb{Q}|$

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



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

😊 Esimerkki: Laatikkoperiaate

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

Miksi?

- *Voimme esittää S :n luvut muodossa $2^{k_j} \cdot q_j$ missä $k_j \geq 0$.
 $1 \leq q_j < 2 \cdot n$ ja q_j on pariton, $j = 1, 2, \dots, n + 1$ ja lisäksi $[k_i, q_i] \neq [k_j, q_j]$ kun $i \neq j$.*
- *Joukossa $\{1, 2, \dots, 2 \cdot n - 1, 2 \cdot n\}$ on ainoastaan n paritonta lukua.*
- *Laatikkoperiaatteen mukaan on olemassa luvut $i \neq j$ siten, että $q_i = q_j$ jolloin $k_i \neq k_j$.*
- *Jos nyt $k_i < k_j$ niin luku $2^{k_i} \cdot q_i$ jakaa luvun $2^{k_j} \cdot q_j$.*

💡 Pari epäyhtälöä

Olkoot A , B ja C kolme joukkoa.

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

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

josta seuraa, että

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

Vaihtamalla A , B ja C keskenään saadaan myös epäyhtälöt

$$|A \cap B \cap C| \geq |A \cap B| + |B \cap C| - |B| \text{ ja}$$

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

💡 Esimerkki: Otokset

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

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

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

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

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

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

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

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

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

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

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

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

$f(t) = (e^t - 1)^n$ niin

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

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

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

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

💡 Esimerkki

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

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

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

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

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

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

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