Tommi Tanskanen

SEULAPERIAATE

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Huhtikuu 2023

TIIVISTELMÄ

Tommi Tanskanen: Seulaperiaate
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastollisen data-analyysin kandidaattiohjelma
Huhtikuu 2023

Tässä työssä perehdytään lähdekirjallisuuden pohjalta seulaperiaatteeseen eli inkluusio-ekskluusioperiaatteeseen, joka on kombinatoriikan menetelmä. Seulaperiaatteessa keskeistä on se, että kun tarkastellaan tunnettua äärellistä perusjoukkoa, sen tiettyjen osajoukkojen komplementtien leikkauksen koko voidaan määrittää, jos tiedetään kyseisten osajoukkojen ja niiden välisten leikkausten koot. Edellisessä tapauksessa myös osajoukkojen yhdisteen koko on määritettävissä. Seulaperiaatteen hyödyllisyys ilmenee varsinkin silloin, kun lasketaan äärellisen joukon alkioita, joilla ei ole joitain tiettyjä ominaisuuksia.

Seulaperiaatteella on erilaisia sovelluksia, joista tässä työssä esitetään muutama. Seulaperiaatetta hyödyntämällä voidaan esimerkiksi laskea äärellisten joukkojen välisten surjektioiden lukumääriä, kunhan vain joukkojen koot tunnetaan. Käyttämällä seulaperiaatetta on lisäksi mahdollista muodostaa kaava, jonka avulla voidaan laskea minkä tahansa äärellisen epätyhjän joukon sekoituspermutaatioiden lukumäärä, jos joukon koko on tiedossa. Joukon sekoituspermutaatioilla tarkoitetaan kyseisen joukon bijektioita, joissa minkään alkion kuva ei ole alkio itse. Viimeinen esitettävä sovellus on Eulerin ϕ-funktion arvojen laskemiseen käytettävän kaavan todistus. Eulerin ϕ-funktio on funktio, jonka arvo kullakin positiivisella kokonaisluvulla m on niiden positiivisten kokonaislukujen määrä, jotka ovat pienempiä tai yhtä suuria kuin m ja joista kukin on keskenään jaoton luvun m kanssa.

Seulaperiaatteelle on olemassa myös yleistys, jota voidaan käyttää, kun tarkasteltavia äärellisen perusjoukon osajoukkoja on m kappaletta ja kyseisten osajoukkojen ja niiden välisten leikkausten koot tiedetään. Jos tällöin n on positiivinen kokonaisluku, joka on pienempi tai yhtä suuri kuin m, voidaan määrittää niiden alkioiden lukumäärä, joista kukin kuuluu täsmälleen n osajoukkoon. Yleistetty seulaperiaate on hyödyllinen, kun tutkitaan äärellisen joukon alkioiden tiettyjä ominaisuuksia ja halutaan määrittää niiden alkioiden lukumäärä, joista kullakin on tietty määrä tutkittavia ominaisuuksia.

Avainsanat: seulaperiaate, inkluusio-ekskluusioperiaate, kombinatoriikka

Sisällys

1 Johdanto

Tässä tutkielmassa tarkastellaan seulaperiaatetta eli inkluusio-ekskluusioperiaatetta, joka on kombinatoriikan käsite. Luvussa 3 esitetään ja todistetaan seulaperiaatetta koskevia kaavoja. Erityisesti osoitetaan, että kun tarkastellaan tunnettua äärellistä perusjoukkoa, sen tiettyjen osajoukkojen komplementtien leikkauksen koko voidaan määrittää, jos tiedetään kyseisten osajoukkojen ja niiden välisten leikkausten koot.

Luku 4 käsittelee seulaperiaatteen sovelluksia. Aliluvussa 4.1 lasketaan seulaperiaatetta hyödyntämällä äärellisten joukkojen välisten surjektioiden lukumääriä. Aliluvussa 4.2 puolestaan muodostetaan seulaperiaatteen avulla kaava, jolla voidaan laskea sekoituspermutaatioiden lukumääriä. Lopuksi aliluvussa 4.3 todistetaan seulaperiaatetta käyttämällä kaava, jolla voidaan laskea Eulerin ϕ-funktion arvoja.

Luvussa 5 todistetaan yleistetty seulaperiaatteen kaava, jota voidaan käyttää, kun tarkastellaan äärellisen perusjoukon m osajoukkoa ja tiedetään kyseisten osajoukkojen ja niiden välisten leikkausten koot. Jos tällöin n on positiivinen kokonaisluku, joka on pienempi tai yhtä suuri kuin m, kyseisellä kaavalla voidaan määrittää niiden alkioiden lukumäärä, joista kukin kuuluu täsmälleen n osajoukkoon.

Esitietoina luvussa 2 todistetaan muutama lause, joita käytetään myöhempien lukujen todistuksissa.

Lukijan oletetaan tuntevan yliopistomatematiikan perusteet etenkin joukko-opista, kombinatoriikasta ja lukuteoriasta. Muun muassa de Morganin lait, permutaatiot, kombinaatiot, binomilause ja aritmetiikan peruslause oletetaan tunnetuiksi. Lähteinä käytetään erinäisiä kombinatoriikkaa käsitteleviä teoksia.

2 Esitietoja

Tässä luvussa todistetaan myöhemmissä todistuksissa käytettäviä lauseita, joista osa on esitetty lähteissä ilman todistusta.

Lause 2.1. *Olkoon $n \in \mathbb{Z}_+$. Tällöin*

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0. \tag{2.1}$$

Todistus (vrt. [1, s. 132]). Soveltamalla binomilausetta binomin potenssiin $(1+(-1))^n$ saadaan

$$\begin{aligned}(1+(-1))^n &= \sum_{k=0}^{n} \binom{n}{k} 1^{n-k}(-1)^k \\ &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \\ &= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n}.\end{aligned}$$

Siis

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = (1+(-1))^n = 0^n = 0.$$

□

Lause 2.2 (vrt. [2, s. 69])**.** *Olkoot n, m ja k sellaisia kokonaislukuja, että $0 \leq k \leq m \leq n$. Tällöin*

$$\binom{m}{k}\binom{n}{m} = \binom{n}{k}\binom{n-k}{m-k}. \tag{2.2}$$

Todistus. Koska

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

ja

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

niin

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

□

Lause 2.3 (vrt. [2, s. 167]). *Olkoon $n \in \mathbb{Z}_+$. Jos $r_1, r_2, \ldots, r_n \in \mathbb{R}$, niin*

$$
\begin{aligned}
(2.3) \qquad (1-r_1)(1-r_2)\cdots(1-r_n) = 1 - \sum_{i=1}^{n} r_i &+ \sum_{1\le i_1<i_2\le n} r_{i_1}r_{i_2} \\
&- \sum_{1\le i_1<i_2<i_3\le n} r_{i_1}r_{i_2}r_{i_3} \\
&+ \cdots + (-1)^n r_1 r_2 \cdots r_n.
\end{aligned}
$$

Todistus. Käytetään induktiota luvun n suhteen. Jos $n = 1$ ja $r_1 \in \mathbb{R}$, niin $1 - r_1 = 1 - \sum_{i=1}^{n} r_i$, joten väite pätee tapauksessa $n = 1$. Oletetaan sitten, että väite pätee luvulla n. Olkoot $r_1, r_2, \ldots, r_n, r_{n+1} \in \mathbb{R}$. Oletuksen nojalla

$$
\begin{aligned}
&(1-r_1)(1-r_2)\cdots(1-r_n)(1-r_{n+1}) \\
&= (1-r_{n+1})\left(1 - \sum_{i=1}^{n} r_i + \sum_{1\le i_1<i_2\le n} r_{i_1}r_{i_2} - \cdots + (-1)^n r_1 r_2\cdots r_n\right) \\
&= 1 - \sum_{i=1}^{n} r_i + \sum_{1\le i_1<i_2\le n} r_{i_1}r_{i_2} - \cdots + (-1)^n \sum_{1\le i_1<i_2<\cdots<i_n\le n} r_{i_1}r_{i_2}\cdots r_{i_n} \\
&\quad + \Bigg(-r_{n+1} + \sum_{i=1}^{n} r_i r_{n+1} - \cdots + (-1)^n \sum_{1\le i_1<i_2<\cdots<i_{n-1}\le n} r_{i_1}r_{i_2}\cdots r_{i_{n-1}}r_{n+1} \\
&\quad + (-1)^{n+1} r_1 r_2 \cdots r_n r_{n+1}\Bigg) \\
&= 1 - \left(\sum_{i=1}^{n} r_i + r_{n+1}\right) + \left(\sum_{1\le i_1<i_2\le n} r_{i_1}r_{i_2} + \sum_{1\le i_1<i_2=n+1} r_{i_1}r_{i_2}\right) \\
&\quad - \cdots + (-1)^n \left(\sum_{1\le i_1<i_2<\cdots<i_n\le n} r_{i_1}r_{i_2}\cdots r_{i_n} + \sum_{1\le i_1<i_2<\cdots<i_n=n+1} r_{i_1}r_{i_2}\cdots r_{i_n}\right) \\
&\quad + (-1)^{n+1} r_1 r_2 \cdots r_{n+1} \\
&= 1 - \sum_{i=1}^{n+1} r_i + \sum_{1\le i_1<i_2\le n+1} r_{i_1}r_{i_2} - \cdots + (-1)^n \sum_{1\le i_1<i_2<\cdots<i_n\le n+1} r_{i_1}r_{i_2}\cdots r_{i_n} \\
&\quad + (-1)^{n+1} r_1 r_2 \cdots r_{n+1}.
\end{aligned}
$$

Siis väite pätee luvulla $n + 1$. Induktioperiaatteen nojalla väite pätee kaikilla $n \in \mathbb{Z}_+$. □

3 Seulaperiaatteen kaavat

Seuraava lause 3.1 ja sen seuraus 3.1 muodostavat seulaperiaatteen. Joissain kirjoissa seuraus 3.1 todistetaan ensin, minkä jälkeen sen avulla todistetaan lause 3.1.

Seuraavassa lauseessa ja yleisestikin tässä tutkielmassa minkä tahansa joukon S komplementtia merkitään $\overline{S}$ ja mahtavuutta $|S|$.

Lause 3.1. *Olkoon S äärellinen perusjoukko, olkoon $m \in \mathbb{Z}_+$, ja olkoot $A_1, A_2, \dots, A_m$ joukon S osajoukkoja. Tällöin*

$$
\begin{aligned}
(3.1) \quad |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m| = |S| - \sum_{i=1}^{m} |A_i| &+ \sum_{1 \le i_1 < i_2 \le m} |A_{i_1} \cap A_{i_2}| \\
&- \sum_{1 \le i_1 < i_2 < i_3 \le m} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\
&+ \cdots + (-1)^m |A_1 \cap A_2 \cap \cdots \cap A_m|.
\end{aligned}
$$

Todistus (vrt. [1, s. 163–164]). Yhtälön (3.1) vasemman puolen tulos on joukon S niiden alkioiden lukumäärä, jotka eivät kuulu mihinkään osajoukoista $A_1, A_2, \dots, A_m$. Yhtälön oikean puolen jokainen termi muodostuu joukon S joidenkin alkioiden lukumäärien summasta ja kertoimesta 1 tai -1. Yhtälö voidaan osoittaa voimassa olevaksi osoittamalla, että jos x on joukon S alkio, joka ei kuulu mihinkään osajoukkoon, niin alkion x kokonaisvaikutus yhtälön oikean puolen tulokseen on 1, ja jos y on joukon S alkio, joka kuuluu vähintään yhteen osajoukkoon, niin alkion y kokonaisvaikutus yhtälön oikean puolen tulokseen on 0.

Oletetaan ensin, että x on joukon S alkio, joka ei kuulu mihinkään osajoukoista $A_1, A_2, \dots, A_m$. Siis x ei kuulu mihinkään osajoukkojen väliseen leikkaukseen, ja alkion x kokonaisvaikutus yhtälön (3.1) oikean puolen tulokseen on

$$1 - 0 + 0 - 0 + \cdots + (-1)^m \cdot 0 = 1.$$

Oletetaan sitten, että y on joukon S alkio, joka kuuluu vähintään yhteen osajoukoista $A_1, A_2, \dots, A_m$. Siis on olemassa sellainen $n \in \{1, 2, \dots, m\}$, että y kuuluu täsmälleen n osajoukkoon.

Alkion y vaikutus lausekkeen $|S|$ tulokseen on $1 = \binom{n}{0}$. Alkion y vaikutus lausekkeen $\sum_{i=1}^{m} |A_i|$ tulokseen on $n = \binom{n}{1}$, sillä y kuuluu täsmälleen n joukkoon A_i $(1 \le i \le m)$. Edelleen alkion y vaikutus lausekkeen $\sum_{1 \le i_1 < i_2 \le m} |A_{i_1} \cap A_{i_2}|$ tulokseen on $\binom{n}{2}$, sillä niistä n osajoukosta, joihin y kuuluu, voidaan valita kaksi joukkoa

$\binom{n}{2}$ tavalla, joten y kuuluu täsmälleen $\binom{n}{2}$ joukkoon $A_{i_1} \cap A_{i_2}$ $(1 \leq i_1 < i_2 \leq m)$. Vastaavasti alkion y vaikutus lausekkeen $\sum_{1 \leq i_1 < i_2 < i_3 \leq m} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|$ tulokseen on $\binom{n}{3}$, jne.

Siispä alkion y kokonaisvaikutus yhtälön (3.1) oikean puolen tulokseen on

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^m \binom{n}{m}.$$

Koska $n \leq m$, niin edellinen lauseke saadaan muotoon

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n} + \cdots + (-1)^m \binom{n}{m},$$

ja tämä lauseke on yhtä suuri kuin

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n},$$

sillä $\binom{n}{k} = 0$, jos $k > n$. Saatu viimeinen lauseke on lauseen 2.1 nojalla yhtä suuri kuin 0, joten alkion y kokonaisvaikutus yhtälön (3.1) oikean puolen tulokseen on 0.

Siispä yhtälö (3.1) on voimassa. □

Seuraus 3.1. *Olkoon $m \in \mathbb{Z}_+$, ja olkoot $A_1, A_2, \ldots, A_m$ äärellisiä joukkoja. Tällöin*

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_m| = \sum_{i=1}^{m} |A_i| &- \sum_{1 \leq i_1 < i_2 \leq m} |A_{i_1} \cap A_{i_2}| \\ &+ \sum_{1 \leq i_1 < i_2 < i_3 \leq m} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ &- \cdots + (-1)^{m+1} |A_1 \cap A_2 \cap \cdots \cap A_m|. \end{aligned} \tag{3.2}$$

Todistus (vrt. [1, s. 164]). Olkoon $S = A_1 \cup A_2 \cup \cdots \cup A_m$ perusjoukko. Siis S on äärellinen ja $A_1, A_2, \ldots, A_m$ ovat joukon S osajoukkoja. Käyttämällä lausetta 3.1 saadaan

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_m| &= |S| - 0 \\ &= |S| - |\overline{S}| \\ &= |S| - |\overline{A_1 \cup A_2 \cup \cdots \cup A_m}| \\ &= |S| - |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m| \qquad \text{(de Morganin lait)} \\ &= |S| - \Bigg(|S| - \sum_{i=1}^{m} |A_i| + \sum_{1 \leq i_1 < i_2 \leq m} |A_{i_1} \cap A_{i_2}| \\ &\quad - \sum_{1 \leq i_1 < i_2 < i_3 \leq m} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \end{aligned}$$

$$
\begin{aligned}
&+\cdots+(-1)^m|A_1\cap A_2\cap\cdots\cap A_m|\Bigg)\\
&=\sum_{i=1}^{m}|A_i|-\sum_{1\le i_1<i_2\le m}|A_{i_1}\cap A_{i_2}|\\
&+\sum_{1\le i_1<i_2<i_3\le m}|A_{i_1}\cap A_{i_2}\cap A_{i_3}|\\
&-\cdots+(-1)^{m+1}|A_1\cap A_2\cap\cdots\cap A_m|.
\end{aligned}
$$

□

Lause 3.1 on käyttökelpoinen, kun halutaan määrittää äärellisen joukon niiden alkioiden lukumäärä, joilla ei ole joitain tiettyjä ominaisuuksia. Kun lasketaan alkioita, joilla on vähintään yksi ominaisuuksista, seuraus 3.1 on kätevä. Seuraavassa seulaperiaatetta havainnollistavassa esimerkissä ominaisuudet koskevat jaollisuutta.

Esimerkki 3.1. Olkoon $S = \{1, 2, \ldots, 500\}$ perusjoukko. Määritetään joukon S niiden kokonaislukujen määrä, jotka eivät ole jaollisia millään luvuista 3, 4 ja 7.

Olkoon $B_n = \{\, x \in S \mid x \text{ on jaollinen luvulla } n \,\}$ kaikilla $n \in \mathbb{Z}_+$. Tavoitteena on määrittää joukon $\overline{B}_3 \cap \overline{B}_4 \cap \overline{B}_7$ alkioiden lukumäärä.

Huomioidaan, että kaikilla $n \in \mathbb{Z}_+$ pätee $|B_n| = \lfloor \frac{500}{n} \rfloor$, missä $\lfloor \frac{500}{n} \rfloor$ on suurin kokonaisluku, joka on pienempi tai yhtäsuuri kuin $\frac{500}{n}$. Siispä

$$
|B_3| = \left\lfloor \frac{500}{3} \right\rfloor = 166, \qquad |B_4| = \left\lfloor \frac{500}{4} \right\rfloor = 125, \qquad |B_7| = \left\lfloor \frac{500}{7} \right\rfloor = 71.
$$

Lisäksi luku $x \in S$ on jaollinen positiivisilla kokonaisluvuilla a ja b, jos ja vain jos x on jaollinen luvulla $\mathrm{pyj}(a, b)$, missä $\mathrm{pyj}(a, b)$ on lukujen a ja b pienin yhteinen jaettava. Koska $\mathrm{pyj}(3, 4) = 12$, $\mathrm{pyj}(3, 7) = 21$ ja $\mathrm{pyj}(4, 7) = 28$, niin

$$
\begin{aligned}
|B_3 \cap B_4| = |B_{12}| &= \left\lfloor \frac{500}{12} \right\rfloor = 41,\\
|B_3 \cap B_7| = |B_{21}| &= \left\lfloor \frac{500}{21} \right\rfloor = 23,\\
|B_4 \cap B_7| = |B_{28}| &= \left\lfloor \frac{500}{28} \right\rfloor = 17.
\end{aligned}
$$

Vastaavasti luku $x \in S$ on jaollinen luvuilla 3, 4 ja 7, jos ja vain jos x on jaollinen luvulla $\mathrm{pyj}(3, 4, 7) = 84$. Siispä

$$
|B_3 \cap B_4 \cap B_7| = |B_{84}| = \left\lfloor \frac{500}{84} \right\rfloor = 5.
$$

Käyttämällä lausetta 3.1 saadaan

$$
\begin{aligned}
|\overline{B}_3 \cap \overline{B}_4 \cap \overline{B}_7| &= |S| - (|B_3| + |B_4| + |B_7|) + (|B_3 \cap B_4| + |B_3 \cap B_7| + |B_4 \cap B_7|) \\
&\quad - |B_3 \cap B_4 \cap B_7| \\
&= 500 - (166 + 125 + 71) + (41 + 23 + 17) - 5 \\
&= 500 - 362 + 81 - 5 \\
&= 214.
\end{aligned}
$$

Lauseen 3.1 kaavasta esitetään vielä erityistapauksessa hyödyllinen yksinkertaistettu muoto.

Lause 3.2. *Olkoon S äärellinen perusjoukko, olkoon $m \in \mathbb{Z}_+$, ja olkoot $A_1, A_2, \ldots, A_m$ joukon S osajoukkoja. Oletetaan, että on olemassa sellaiset luvut $N_1, N_2, \ldots, N_m$, että $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = N_k$ aina, kun $k \in \{1, 2, \ldots, m\}$ ja $1 \leq i_1 < i_2 < \cdots < i_k \leq m$. Tällöin*

$$
|\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m| = |S| + \sum_{k=1}^{m} (-1)^k \binom{m}{k} N_k. \tag{3.3}
$$

Todistus (vrt. [3, s. 158]). Tarkastellaan mitä tahansa summaa

$$
\sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq m} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|,
$$

missä $1 \leq k \leq m$. Summan termien lukumäärä on joukon $\{1, 2, \ldots, m\}$ $k-$kombinaatioiden lukumäärä $\binom{m}{k}$, ja oletuksen nojalla jokainen termi on yhtä suuri kuin N_k. Siispä summa on yhtä suuri kuin $\binom{m}{k} N_k$.

Käyttämällä lausetta 3.1 ja edellistä tulosta saadaan

$$
\begin{aligned}
|\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_m| &= |S| - \sum_{i=1}^{m} |A_i| + \sum_{1 \leq i_1 < i_2 \leq m} |A_{i_1} \cap A_{i_2}| \\
&\quad - \sum_{1 \leq i_1 < i_2 < i_3 \leq m} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\
&\quad + \cdots + (-1)^m |A_1 \cap A_2 \cap \cdots \cap A_m| \\
&= |S| - \binom{m}{1} N_1 + \binom{m}{2} N_2 - \binom{m}{3} N_3 + \cdots + (-1)^m \binom{m}{m} N_m \\
&= |S| + \sum_{k=1}^{m} (-1)^k \binom{m}{k} N_k.
\end{aligned}
$$

□

4 Sovelluksia

4.1 Surjektioiden lukumäärä

Lause 4.1. *Olkoot* $m, n \in \mathbb{Z}_+$, *ja olkoon* $\mathrm{Surj}(m, n)$ *surjektioiden lukumäärä* m-*alkioiselta joukolta* n-*alkioiseen joukkoon. Tällöin*

$$\mathrm{Surj}(m, n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m. \tag{4.1}$$

Todistus (vrt. [3, s. 161]). Olkoon $X = \{x_1, x_2, \ldots, x_m\}$ m-alkioinen joukko ja $Y = \{y_1, y_2, \ldots, y_n\}$ n-alkioinen joukko. Lisäksi olkoon S kaikkien kuvausten $f : X \to Y$ joukko. Kun muodostetaan kuvausta $f \in S$, niin jokainen arvoista $f(x_1)$, $f(x_2), \ldots$, $f(x_m)$ voidaan valita n eri tavalla. Siispä $|S| = n^m$.

Tarkastellaan joukkoa S perusjoukkona. Olkoon kaikilla $i \in \{1, 2, \ldots, n\}$

$$A_i = \{\, f \in S \mid y_i \text{ ei kuulu kuvauksen } f \text{ kuvajoukkoon} \,\}.$$

Kuvaus $f \in S$ on surjektio, jos ja vain jos f ei kuulu mihinkään joukoista A_1, $A_2, \ldots, A_n$. Siispä $\mathrm{Surj}(m, n) = |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n|$. Käytetään luvun $\mathrm{Surj}(m, n)$ määrittämiseen seulaperiaatetta.

Tarkastellaan mitä tahansa joukkoa $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}$, missä $k \in \{1, 2, \ldots, n\}$ ja $1 \le i_1 < i_2 < \cdots < i_k \le n$. Kuvaus $f \in S$ kuuluu joukkoon $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}$, jos ja vain jos $f = g$, missä g on kuvaus m-alkioiselta joukolta X $(n-k)$-alkioiseen joukkoon $Y \setminus \{y_{i_1}, y_{i_2}, \ldots, y_{i_k}\}$. Kaikkien kuvausten $g : X \to Y \setminus \{y_{i_1}, y_{i_2}, \ldots, y_{i_k}\}$ lukumäärä on $(n-k)^m$, joten $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = (n-k)^m$.

Edellisen tuloksen ja lauseen 3.2 perusteella

$$\begin{aligned}
\mathrm{Surj}(m, n) &= |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n| \\
&= n^m + \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)^m \\
&= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.
\end{aligned}$$

□

4.2 Sekoituspermutaatiot

Tässä aliluvussa määritellään sekoituspermutaatio ja muodostetaan seulaperiaatteen avulla kaava, jolla voidaan laskea sekoituspermutaatioiden lukumääriä (vrt. [3, s. 163]).

Määritelmä 4.1 (**Sekoituspermutaatio**)**.** Olkoon S joukko. Joukon S *sekoituspermutaatio* on bijektio $f\colon S \to S$, jolle pätee $f(x) \neq x$ kaikilla $x \in S$.

Olkoon tästedes D_n joukon $\{1, 2, \dots, n\}$ sekoituspermutaatioiden joukko ja $d_n = |D_n|$, kun $n \in \mathbb{Z}_+$. Määritellään lisäksi, että D_0 on tyhjän joukon sekoituspermutaatioiden joukko, jonka ainoa alkio on kuvaus tyhjältä joukolta tyhjään joukkoon, ja $d_0 = |D_0| = 1$. Jos S on äärellinen joukko ja $|S| = n$, niin selvästi joukon S sekoituspermutaatioiden lukumäärä on d_n.

Lause 4.2. *Olkoon $n \in \mathbb{Z}_+$. Tällöin*

$$d_n = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}. \tag{4.2}$$

Todistus. Todistus etenee samankaltaisesti kuin lauseen 4.1 todistus. Olkoon S joukon $\{1, 2, \dots, n\}$ permutaatioiden joukko, kun joukon $\{1, 2, \dots, n\}$ permutaatio tulkitaan bijektioksi joukolta $\{1, 2, \dots, n\}$ itselleen. Kyseisten permutaatioiden lukumäärä on $|S| = n!$.

Tarkastellaan joukkoa S perusjoukkona. Olkoon $A_i = \{ f \in S \mid f(i) = i \}$ kaikilla $i \in \{1, 2, \dots, n\}$. Joukko D_n koostuu täsmälleen niistä joukkoon S kuuluvista permutaatioista, jotka eivät kuulu mihinkään joukoista $A_1, A_2, \dots, A_n$. Siispä $D_n = \overline{A}_1 \cap \overline{A}_2 \cap \dots \cap \overline{A}_n$ ja $d_n = |\overline{A}_1 \cap \overline{A}_2 \cap \dots \cap \overline{A}_n|$.

Tarkastellaan mitä tahansa joukkoa $A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}$, missä $k \in \{1, 2, \dots, n\}$ ja $1 \leq i_1 < i_2 < \dots < i_k \leq n$. Permutaatio $f \in S$ kuuluu joukkoon $A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}$, jos ja vain jos sillä on k kiinnitettyä arvoa $f(i_1) = i_1, f(i_2) = i_2, \dots, f(i_k) = i_k$ ja sen muut $n - k$ arvoa vastaavat joukon $\{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_k\}$ jonkin permutaation arvoja. Viimeksi mainitun joukon permutaatioiden lukumäärä on $(n - k)!$, joten $|A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| = (n - k)!$.

Edellisen tuloksen ja lauseen 3.2 perusteella

$$\begin{aligned} d_n &= |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n| \\ &= n! + \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)! \\ &= n! + \sum_{k=1}^{n} (-1)^k \frac{n!}{k!(n-k)!} (n-k)! \\ &= n! \left(1 + \sum_{k=1}^{n} (-1)^k \frac{1}{k!} \right) \\ &= n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}. \end{aligned}$$

□

4.3 Eulerin ϕ-funktio

Määritelmä 4.2 (**Eulerin ϕ-funktio**, vrt. [3, s. 161]). Olkoon $m \in \mathbb{Z}_+$. *Eulerin ϕ-funktio* $\phi(m)$ on niiden kokonaislukujen $x \in \{1, 2, \dots, m\}$ määrä, joille pätee $\mathrm{syt}(x, m) = 1$, missä $\mathrm{syt}(x, m)$ on lukujen x ja m suurin yhteinen tekijä.

Lause 4.3 (vrt. [3, s. 161]). *Olkoon $m \in \mathbb{Z}_+$. Oletetaan, että $m \geq 2$ ja $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ on luvun m aritmetiikan peruslauseen mukainen alkutekijäesitys. Tällöin*

$$\phi(m) = m \prod_{k=1}^{n} \left(1 - \frac{1}{p_k} \right). \tag{4.3}$$

Todistus (vrt. [2, s. 167–168]). Olkoon $S = \{1, 2, \dots, m\}$ perusjoukko. Olkoon kaikilla $i \in \{1, 2, \dots, n\}$

$$A_i = \{\, x \in S \mid x \text{ on jaollinen luvulla } p_i \,\}.$$

Luvulle $x \in S$ on voimassa

$$\begin{aligned} \mathrm{syt}(x, m) = 1 &\Leftrightarrow \text{luvuilla } x \text{ ja } m \text{ ei ole yhteistä tekijää, joka on alkuluku} \\ &\Leftrightarrow \text{luku } x \text{ ei ole jaollinen millään luvuista } p_1, p_2, \dots, p_n \\ &\Leftrightarrow x \in \overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n. \end{aligned}$$

Siispä $\phi(m) = |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n|$, ja voidaan käyttää seulaperiaatetta.

Tarkastellaan mitä tahansa joukkoa $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}$, missä $k \in \{1, 2, \ldots, n\}$ ja $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. Luvulle $x \in S$ on voimassa

$$\begin{aligned} x \in A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k} &\Leftrightarrow x \text{ on jaollinen erisuurilla alkuluvuilla } p_{i_1}, p_{i_2}, \ldots, p_{i_k} \\ &\Leftrightarrow x \text{ on jaollinen luvulla } p_{i_1} p_{i_2} \cdots p_{i_k}. \end{aligned}$$

Siispä $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|$ on yhtä suuri kuin positiivisella kokonaisluvulla $p_{i_1} p_{i_2} \cdots p_{i_k}$ jaollisten lukujen määrä joukossa S. Näin ollen $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = \left\lfloor \frac{m}{p_{i_1} p_{i_2} \cdots p_{i_k}} \right\rfloor = \frac{m}{p_{i_1} p_{i_2} \cdots p_{i_k}}$, sillä m on jaollinen luvulla $p_{i_1} p_{i_2} \cdots p_{i_k}$.

Edellisen tuloksen ja lauseen 3.1 perusteella

$$\begin{aligned} \phi(m) &= |\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n| \\ &= m - \sum_{i=1}^{n} \frac{m}{p_i} + \sum_{1 \leq i_1 < i_2 \leq n} \frac{m}{p_{i_1} p_{i_2}} - \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \frac{m}{p_{i_1} p_{i_2} p_{i_3}} \\ &\quad + \cdots + (-1)^n \frac{m}{p_1 p_2 \cdots p_n} \\ &= m \Bigg(1 - \sum_{i=1}^{n} \frac{1}{p_i} + \sum_{1 \leq i_1 < i_2 \leq n} \frac{1}{p_{i_1}} \cdot \frac{1}{p_{i_2}} - \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \frac{1}{p_{i_1}} \cdot \frac{1}{p_{i_2}} \cdot \frac{1}{p_{i_3}} \\ &\quad + \cdots + (-1)^n \frac{1}{p_1} \cdot \frac{1}{p_2} \cdots \frac{1}{p_n} \Bigg) \\ &= m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right) \qquad \text{(lause 2.3)} \\ &= m \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

□

5 Yleistetty seulaperiaate

Lause 5.1 (vrt. [4, s. 335]). *Olkoon S äärellinen perusjoukko, olkoon $m \in \mathbb{Z}_+$, ja olkoot $A_1, A_2, \ldots, A_m$ joukon S osajoukkoja. Merkitään*

$$\alpha_k = \sum_{1 \leq i_1 < i_2 \cdots < i_k \leq m} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|, \quad \text{kun } k \in \{1, 2, \ldots, m\}.$$

Olkoon $n \in \{1, 2, \ldots, m\}$ ja E_n joukon S niiden alkioiden lukumäärä, joista kukin kuuluu täsmälleen n joukkoon osajoukoista $A_1, A_2, \ldots, A_m$. Tällöin

$$E_n = \alpha_n - \binom{n+1}{n}\alpha_{n+1} + \binom{n+2}{n}\alpha_{n+2} - \cdots + (-1)^{m-n}\binom{m}{n}\alpha_m. \tag{5.1}$$

Todistus (vrt. [2, s. 151–152] ja [4, s. 335–336]). Todistuksen idea on sama kuin lauseen 3.1 todistuksessa. Olkoon $x \in S$ ja oletetaan, että x kuuluu täsmälleen t joukkoon osajoukoista $A_1, A_2, \ldots, A_m$. Yhtälö (5.1) osoitetaan voimassa olevaksi osoittamalla, että jos $t = n$, niin alkion x kokonaisvaikutus yhtälön oikean puolen tulokseen on 1, ja jos $t \neq n$, niin alkion x kokonaisvaikutus yhtälön oikean puolen tulokseen on 0.

Olkoon $k \in \{n, n+1, n+2, \ldots, m\}$. Niistä t osajoukosta, joihin x kuuluu, voidaan valita k joukkoa $\binom{t}{k}$ tavalla, joten x kuuluu täsmälleen $\binom{t}{k}$ joukkoon $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}$ $(1 \leq i_1 < i_2 \cdots < i_k \leq m)$. Siispä alkion x vaikutus lausekkeen α_k tulokseen on $\binom{t}{k}$.

Edellisen tuloksen perusteella alkion x kokonaisvaikutus yhtälön (5.1) oikean puolen tulokseen on

$$\lambda = \binom{t}{n} - \binom{n+1}{n}\binom{t}{n+1} + \binom{n+2}{n}\binom{t}{n+2} - \cdots + (-1)^{m-n}\binom{m}{n}\binom{t}{m}.$$

Jos $t < n$, niin

$$\lambda = 0 - \binom{n+1}{n} \cdot 0 + \binom{n+2}{n} \cdot 0 - \cdots + (-1)^{m-n}\binom{m}{n} \cdot 0 = 0.$$

Oletetaan sitten, että $t \geq n$. Tällöin $n \leq t \leq m$. Koska lisäksi $\binom{t}{r} = 0$, jos $r > t$, niin saadaan

$$\begin{aligned}
\lambda = \binom{t}{n} &- \binom{n+1}{n}\binom{t}{n+1} + \binom{n+2}{n}\binom{t}{n+2} - \cdots + (-1)^{t-n}\binom{t}{n}\binom{t}{t} \\
&+ \cdots + (-1)^{m-n}\binom{m}{n}\binom{t}{m} \\
= \binom{t}{n} &- \binom{n+1}{n}\binom{t}{n+1} + \binom{n+2}{n}\binom{t}{n+2} - \cdots + (-1)^{t-n}\binom{t}{n}\binom{t}{t}
\end{aligned}$$

$$= \binom{t}{n} - \binom{t}{n}\binom{t-n}{n+1-n} + \binom{t}{n}\binom{t-n}{n+2-n} - \cdots + (-1)^{t-n}\binom{t}{n}\binom{t-n}{t-n} \quad \text{(lause 2.2)}$$
$$= \binom{t}{n}\left(1 - \binom{t-n}{1} + \binom{t-n}{2} - \cdots + (-1)^{t-n}\binom{t-n}{t-n}\right)$$
$$= \binom{t}{n}\left(\binom{t-n}{0} - \binom{t-n}{1} + \binom{t-n}{2} - \cdots + (-1)^{t-n}\binom{t-n}{t-n}\right).$$

Jos $t = n$, niin $t - n = 0$ ja

$$\lambda = \binom{t}{n}\left(\binom{t-n}{0} - \binom{t-n}{1} + \binom{t-n}{2} - \cdots + (-1)^{t-n}\binom{t-n}{t-n}\right) = \binom{n}{n}\binom{0}{0} = 1.$$

Jos $t > n$, niin $t - n > 0$ ja lauseen 2.1 nojalla

$$\lambda = \binom{t}{n}\left(\binom{t-n}{0} - \binom{t-n}{1} + \binom{t-n}{2} - \cdots + (-1)^{t-n}\binom{t-n}{t-n}\right) = \binom{t}{n} \cdot 0 = 0.$$

Siis jos $t = n$, niin $\lambda = 1$, ja jos $t \neq n$, niin $\lambda = 0$. Siispä yhtälö (5.1) on voimassa. □

Esimerkki 5.1. Kuten esimerkissä 3.1, olkoon $S = \{1, 2, \ldots, 500\}$ perusjoukko ja $B_n = \{\, x \in S \mid x \text{ on jaollinen luvulla } n \,\}$ kaikilla $n \in \mathbb{Z}_+$.

Olkoon E_1 joukon S niiden kokonaislukujen määrä, joista kukin on jaollinen täsmälleen yhdellä luvuista 3, 4 ja 7. Siis E_1 on joukon S niiden alkioiden lukumäärä, joista kukin kuuluu täsmälleen yhteen joukoista B_3, B_4 ja B_7. Lauseen 5.1 ja esimerkin 3.1 perusteella

$$\begin{aligned} E_1 &= (|B_3| + |B_4| + |B_7|) - \binom{2}{1}(|B_3 \cap B_4| + |B_3 \cap B_7| + |B_4 \cap B_7|) \\ &\quad + \binom{3}{1}|B_3 \cap B_4 \cap B_7| \\ &= (166 + 125 + 71) - 2 \cdot (41 + 23 + 17) + 3 \cdot 5 \\ &= 362 - 162 + 15 \\ &= 215. \end{aligned}$$

Jos E_2 on joukon S niiden kokonaislukujen määrä, joista kukin on jaollinen täsmälleen kahdella luvuista 3, 4 ja 7, niin vastaavasti

$$\begin{aligned} E_2 &= (|B_3 \cap B_4| + |B_3 \cap B_7| + |B_4 \cap B_7|) - \binom{3}{2}|B_3 \cap B_4 \cap B_7| \\ &= (41 + 23 + 17) - 3 \cdot 5 \\ &= 66. \end{aligned}$$

Lähteet

[1] Brualdi, Richard A. *Introductory Combinatorics*. 4th ed. Upper Saddle River, New Jersey: Pearson Prentice Hall, 2004.

[2] Chen, Chuan-Chong & Koh, Khee-Meng. *Principles and Techniques in Combinatorics*. Singapore: World Scientific Publishing Co. Pte. Ltd., 1992.

[3] Loehr, Nicholas A. *Bijective Combinatorics*. Boca Raton: Chapman & Hall/CRC, 2011.

[4] Tucker, Alan. *Applied Combinatorics*. 6th ed. United States of America: John Wiley & Sons, Inc., 2012.