Kombinatoriikka

Vesa Halava

Luentomoniste

Turun yliopisto
Matematiikan laitos
20014 Turku

2004

Sisältö

Johdanto

Kombinatoriikan kysymykset voidaan jakaa karkeasti kahteen: 1) onko olemassa tietyt ominaisuuden omaavia kombinaatioita, 2) kuinka monta tällaista kombinaatiota on olemassa.

Käsite "kombinatorinen todistus" on tuttu monilta eri matematiikan aloilta. Tällöin annettu väite osoitetaan oikeaksi käymällä läpi kaikki kombinaatiot, osoittamalla, että joitakin kombinaatioita on/ei ole olemassa tai laskemalla niiden lukumäärä.

Tällä kurssilla on tarkoitus käydä läpi kombinatoriikan perusteita. Erityisesti tarkastellaan kombinatorisia laskenta- ja todistusmenetelmiä sekä jonoja ja niiden jäsenten ratkaisemista. Esimerkkejä ja sovelluksia esiintyy monilta matematiikan aloilta.

Luentomoniste perustuu seuraaviin lähteisiin:

AIGNER, M. AND ZIEGLER, G. M., Proofs from the Book , Springer, 1998.

JACKSON, B. W. AND THORO, D., Applied Combinatorics with Problem Solving, Addison-Wesley, 1990.

VAN LINT, J. H. AND WILSON, R. M., A course in combinatorics, Cambridge University Press, 1996.

WILF, HERBERT S., generatingfunctionology, Academic Press, 1994. (http://www.cis.upenn.edu/∼wilf/index.html)

1 BINOMIKERROIN

1.1 Joukoista

Olkoon A joukko, sen *alkioiden lukumäärää* merkitään $|A|$:lla. Jos $A = \{a_1, a_2, \ldots, a_n\}$, niin se on ns. *äärellinen* joukko. Jos A on *ääretön* joukko, niin joskus merkitään $|A| = \infty$.

Määritelmä 1.1. Olkoot A ja B kaksi joukkoa, määritellään joukkojen

(i) *unioni* $A \cup B = \{a \mid a \in A \vee a \in B\}$,

(ii) *leikkaus* $A \cap B = \{a \mid a \in A \wedge a \in B\}$,

(iii) *erotus* $A \setminus B = \{a \mid a \in A \wedge a \notin B\}$ ja

(iv) *(karteesinen) tulo* $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

Joukon $A(\subseteq E)$ *komplementti* $A^C = E \setminus A$, missä E on niin sanottu *perusjoukko*.

Sanotaan, että joukot A ja B ovat *erillisiä*, jos $A \cap B = \emptyset$.

Lemma 1.1. *Olkoot $A_1, A_2, \ldots, A_n$ äärellisiä joukkoja.*

(i) (Summasääntö) Jos joukot $A_1, A_2, \ldots, A_n$ ovat (parittain) erillisiä, niin

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|.$$

(ii) (Tulosääntö)

$$|A_1 \times A_2 \times \cdots \times A_n| = \prod_{i=1}^{n} |A_i|.$$

Todistus. Induktiolla, osoitetaan ensin, että $|A_1 \cup A_2| = |A_1| + |A_2|$ ja $|A_1 \times A_2| = |A_1||A_2|$. □

Huomaa, että kohdassa (i) joukkojen pitää siis olla erillisiä eli $\forall i \neq j$, $A_i \cap A_j = \emptyset$. Seuraavassa luvussa tarkastellaan tapausta, jossa tämä ehto ei välttämättä ole voimassa.

Joukon A tuloa $A \times A$ itsensä kanssa merkitään myös A^2:lla. Kun sovitaan, että $A^0 = \emptyset$ ja $A^1 = A$, niin tämä yleistyy $k \geq 0$ kertaiselle tulolle A^k, jota kutsutaan joukon A k:neksi *potenssiksi*.

Esimerkki 1.1. Äärellistä symbolijoukkoa $X = \{a_1, a_2, \ldots, a_n\}$ kutsutaan *aakkostoksi*. Aakkoston X *sana* on jono X:n symboleja, esimerkiksi $a_2a_6a_1a_2$. Sanan *pituus* on siinä esiintyvien symbolien lukumäärä. Tulosäännön nojalla k-pituisia aakkoston X sanoja on $|X|^k$.

Esimerkki 1.2. Kirjastossa on 5 espanjan, 6 tanskan ja 7 englannin kielistä kirjaa. Kuinka monella tavalla voidaan valita kaksi eri kielistä kirjaa?

1.2 Permutaatiot ja kombinaatiot

Määritelmä 1.2. Kuvaus $\alpha\colon X \to X$ on joukon $X = \{a_1, a_2, \ldots, a_n\}$ *permutaatio*, jos se on bijektio. Kaikki n alkioisen joukon permutaatiot muodostavat ryhmän, ns. *symmetrisen ryhmän* $\mathcal{S}_n$.

Permutaatioita merkitään monella eri tapaa. Esimerkiksi voidaan merkitä

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix},$$

missä $\alpha(a_j) = a_{i_j}$ kaikilla $1 \leq j \leq n$. Seuraavassa esimerkissä esitellään myös ns. *syklimerkintä*

Esimerkki 1.3. Olkoon $X = \{1, 2, \cdots, 4\}$ ja tarkastellaan permutaatiota $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$. Permutaation α voidaan kirjoittaa myös muotoon $\alpha = (12)(3)(4)(= (12))$.

Permutaatiot voidaan ajatella n:n alkion järjestyksinä. Helposti huomataan, että n-alkioisella joukolla on $n(n-1)\cdots 1 = n!$ permutaatiota, ts. $|\mathcal{S}_n| = n!$

Seuraavaksi tarkastellaan tapauksia, missä n-alkioisesta joukosta valitaan k alkiota.

Määritelmä 1.3. Olkoon A n-alkioinen joukko. A:n k alkioista osajoukkoa kutsutaan A:n *k-kombinaatioksi*. Merkitään n-alkioisen joukon k-kombinaatioiden lukumäärää $C(n,k)$:lla.

A:n k **eri** alkioista jonoa kutsutaan A:n *k-permutaatioksi*. Merkitään n-alkioisen joukon k-permutaatioden lukumäärää $P(n,k)$:lla.

Huomautus 1. k-kombinaatiossa alkioden keskinäisellä järjestyksellä ei ole väliä, kun taas k-permutaatiossa on. Huomaa myös, että toistoja ei sallita, jokainen alkio esiintyy siis korkeintaan kerran.

Lause 1.1. $P(n,k) = \dfrac{n!}{(n-k)!}$ *ja* $C(n,k) = \dfrac{n!}{(n-k)!k!} \left(= \binom{n}{k}\right)$.

Todistus. Olkoon $A = \{a_1, a_2, \ldots, a_n\}$. Tarkastellaan ensin k-permutaatioiden määrää. Kun valitaan k-permutaatiota, niin voidaan ajatella, että 1. paikalle on n vaihtoehtoa, 2:lle $(n-1)$ jne. k:nelle $(n-k+1)$. Toisin sanoen

$$P(n,k) = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}.$$

Jokaisen k-permutaation alkiot voidaan järjestää $k!$ tavalla, joten

$$C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{(n-k)!k!}.$$

□

Merkitään siis lukua $\frac{n!}{(n-k)!k!} = \binom{n}{k}$, missä $n \in \mathbb{N}$ ja $0 \leq k \leq n$ (lue n yli k:n). Näitä lukuja kutsutaan yleisesti *binomikertoimiksi*.

Jos $k < 0$ tai $k > n$, niin määritellään $\binom{n}{k} = 0$.

Koska k:n alkion valinta vastaa $n-k$ valitsematta jättämistä, saadaan

Seuraus 1.1. $C(n,k) = \binom{n}{k} = \binom{n}{n-k} = C(n,n-k)$.

Esimerkki 1.4. $|\mathcal{S}_n| = P(n,n) = n!$.

Esimerkki 1.5. Kymmenen joukkueen yksinkertaisessa sarjassa (kaikki pelaavat kaikkia vastaan kerran) on $C(10,2) = \frac{10!}{8!2!} = 45$ ottelua.

Esimerkki 1.6. 10 kirjaimen aakkostosta muodostetaan 8 kirjaimisia sanoja, joissa kukin kirjain saa esiintyä vain kerran. Tällaisia sanoja on $P(10,8)$.

Esimerkki 1.7. Yhdistyksessä on n tyttöä ja m poikaa. Kuinka monta sellaista johtokuntaa, jossa on k tyttöä ja ℓ poikaa, voidaan muodostaa?

1.3 Toistokombinaatiot ja -permutaatiot

Edellisen pykälän kombinaatioissa ja permutaatioissa ei sallittu toistoa. Tarkastellaan seuraavaksi tapauksia, joissa toistot sallittaan.

Joukko on ns. *toistojoukko*, jos samat alkiot voivat esiintyä moneen kertaan. Esimerkiksi $\{1,1,2,4,3,2\}$ on toistojoukko.

Määritelmä 1.4. Olkoon A n-alkioinen joukko. Toistojoukkoa B sanotaan A:n *k-toistokombinaatioksi*, jos $|B| = k$ ja jokainen B:n alkio on A:n alkio. Merkitään n-alkioisen joukon k-toistokombinaatioiden määrää $C_T(n,k)$:lla.

Jonoa, jossa on k kappaletta A:n alkioita kutsutaan A:n *k-toistopermutaatioksi*. Käytetään n-alkioisen joukon k-toistopermutaatioden lukumäärälle merkintää $P_T(n,k)$.

Lause 1.2. *$P_T(n,k) = n^k$ ja $C_T(n,k) = \binom{n+k-1}{k}$.*

Todistus. Joukon A k-toistopermutaatiot voidaan ajatella joukon A^k alkioina (tai k-pituisina sanoina), joten tulosäännön mukaan $P_T(n,k) = |A^k| = n^k$.

Olkoon $A = \{a_1, a_2, \ldots, a_n\}$ ja B A:n k-toistokombinaatio. Joukossa B on x_1 kappaletta alkiota a_1, x_2 alkiota a_2, jne, x_n alkiota a_n, ja

$$x_1 + x_2 + \cdots + x_n = k. \tag{1}$$

$C_T(n,k)$ on siis yhtälön (1) kokonaislukuratkaisujen lukumäärä, kun oletetaan, että $x_i \geq 0$ kaikilla $1 \leq i \leq n$. Tämä lukumäärä taas on ekvivalentti sen kanssa, kuinka monella tavalla k 1:stä voidaan jakaa n lokeroon. Tarkastellaan jonoa $\underbrace{11\cdots1}_{k\text{kpl}}$, ja lisätään siihen $n-1$ erotinta $|$, esim. $1||1|1|$, kun $n = 5$ ja $k = 3$. Näin k 1:stä on jaettu n lokeroon. Jonossa on nyt $n+k-1$ paikkaa (k ykköstä, $n-1$ pystyviivaa). Siis k-toistokombinaatioiden määrä saadaan kun lasketaan kuinka monella tavalla k ykköstä voidaan sijoittaa $n+k-1$ paikkaan (loput paikat täyttyvät pystyviivoilla). k-toistokombinaatioiden määrä on siis yhtä suuri kuin $n+k-1$-alkioisen joukon k-kombinaatioiden lukumäärä $\binom{n+k-1}{k}$. □

Esimerkki 1.8. Ed. lauseen todistuksesta saadaan, että yhtälön

$$x_1 + x_2 + \cdots + x_n = k$$

sellaisten kokonaislukuratkaisujen, missä $x_i \geq 0$, lukumäärä on $\binom{n+k-1}{k}$. Esimerkiksi yhtälöllä

$$x_1 + x_2 + x_3 + x_4 + x_5 = 3$$

on $\binom{5+3-1}{3} = \binom{7}{3} = 35$ ei-negatiivista kokonaislukuratkaisua.

Esimerkki 1.9. Mikä on yhtälön $x_1 + x_2 + x_3 + x_4 = 10$ kokonaislukuratkaisujen lukumäärä, kun **a)** $\forall i$, $x_i > 0$, **b)** $x_1 \geq 2$, $x_2 \geq 1$, $x_3 \geq 4$ ja $x_4 \geq 0$?

1.4 Multinomiluku

Määritelmä 1.5. Joukon A *partitio* on sen jako erillisiin epätyhjiin osajoukkoihin. Siis $A_1, A_2, \ldots, A_k$ on joukon A partitio, jos

$$\forall i \neq j\colon A_i \cap A_j = \emptyset \quad \text{ja} \quad \bigcup_{i=1}^{k} A_i = A.$$

Määritelmä 1.6. *Multinomiluku* eli *multinomikerroin* $\binom{n}{r_1, r_2, \ldots, r_m}$ ilmoittaa, kuinka monella eri tavalla n-alkioinen joukko voidaan jakaa m joukon partitioon, jossa joukot ovat r_1-,r_2-,...,r_m-alkioiset. Huomaa, että $r_1 + r_2 + \cdots + r_m = n$.

Huomautus 2. Partitiossa joukkojen järjestyksellä on väliä. Esimerkki joukolla $\{1, 2\}$ on kaksi partiota yksi alkioisiksi joukoiksi, nimittäin $A_1 = \{1\}$, $A_2 = \{2\}$ ja $A_1 = \{2\}$, $A_2 = \{1\}$.

Huomautus 3. Edellisessä määritelmässä myös tapaus $r_i = 0$ sallitaan.

Lause 1.3. $\binom{n}{r_1, r_2, \ldots, r_m} = \dfrac{n!}{r_1! r_2! \cdots r_m!}$.

Todistus. n alkiosta r_1 voidaan valita $\binom{n}{r_1}$ tavalla, $n - r_1$ alkiosta r_2 voidaan valita $\binom{n - r_1}{r_2}$ tavalla jne. Tulosäännön mukaan saadaan, että

$$\begin{aligned}\binom{n}{r_1, r_2, \ldots, r_m} &= \binom{n}{r_1}\binom{n - r_1}{r_2} \cdots \binom{n - r_1 - \cdots - r_{m-1}}{r_m} \\ &= \frac{n!}{r_1! r_2! \cdots r_m!}.\end{aligned}$$

□

Esimerkki 1.10. Tarkastellaan aakkostoa $\{a, b, c\}$. Kuinka monta sellaista sanaa on olemassa, joissa on 3 a:ta, 2 b:tä ja 4 c:tä?

Sanojen pituus on siis 9. Sanan 9 "paikkaa" partitioidaan siis 2, 3 ja 4 alkiosiksi osajoukoiksi, joten sanoja on

$$\binom{9}{2, 3, 4} = 1260.$$

Esimerkki 1.11. Kuinka monella tavalla sanan VAKAVA kirjaimet voidaan järjestää?

Esimerkki 1.12. Osoita, että

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{r_1 + r_2 + \cdots + r_m = n} \binom{n}{r_1, r_2, \ldots, r_m} x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m}.$$

1.5 Binomikerroin kaavoja

Tässä pykälässä tarkastellaan binomikertoimeen liittyviä kaavoja ja yhtälöitä. Näille kaavoille ja yhtälöille on olemassa monia erilaisia todistuksia.

Edellä todettiin jo, että

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

ks. Seuraus 1.1.

Lause 1.4. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Todistus. DEMO. □

Lauseen 1.4 mukaan binomikertoimet voidaan järjestää ns. *Pascalin kolmioksi.*

$n=0$						1							
$n=1$					1		1						
$n=2$				1		2		1					
$n=3$			1		3		3		1				
$n=4$		1		4		6		4		1			
$n=5$	1		5		10		10		5		1		
$n=6$	1		6		15		20		15		6		1
$n=7$	1	7		21		35		35		21		7	1

Lause 1.5. $\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}$.

Todistus. Tarkastellaan lukua $\binom{n+k+1}{k}$ eli $(n+k+1)$-alkioisen joukon $\{1, 2, \ldots, n+k+1\}$ k-kombinaatioita. On olemassa $\binom{n+k}{k}$ kombinaatioita, joihin 1 ei kuulu, $\binom{n+k-1}{k-1}$ kombinaatiota, joihin 1 kuuluu, mutta 2 ei kuulu, $\binom{n+k-2}{k-2}$ kombinaatiota, joihin 1 ja 2 kuuluu, mutta 3 ei kuulu, jne. □

Huomautus 4. Edellinen lause voidaan todistaa myös Lauseen 1.4 avulla tai vaikka tarkastelemalla Pascalin kolmiota.

Lause 1.6. $\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$

Todistus. DEMO. □

Lause 1.7. $\binom{n+m}{k} = \binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \cdots + \binom{n}{k}\binom{m}{0}$.

Todistus. Vasen puoli ilmoittaa, kuinka monella tavalla n naisesta ja m miehestä voidaan valita k-jäseninen joukko. Oikealla puolella $\binom{n}{i}\binom{m}{k-i}$ kertoo kuinka monella tavalla voidaan valita i naista ja $k-i$ miestä. □

Lause 1.8. $\binom{m}{0}\binom{n}{0} + \binom{m}{1}\binom{n}{1} + \cdots + \binom{m}{n}\binom{n}{n} = \binom{m+n}{n}$.

Todistus. Luku $\binom{m+n}{n}$ kertoo kuinka monella tavalla n naisesta ja m miehestä voidaan valita n-alkioinen joukko. Oletetaan, että on valittu k miestä, valitaan siis $n-k$ naista. Koska naisia on n kappaletta, $n-k$ voidaan valita yhtä monella tavalla kuin jättää k valitsematta. Siis k miestä ja $n-k$ naista sisältäviä joukkoja on $\binom{m}{k}\binom{n}{k}$ kappaletta. □

Lause 1.9. $\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}$.

Todistus. Sijoitetaan edelliseen lauseeseen $m = n$. □

Esimerkki 1.12 sisältää tapauksen

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}. \tag{2}$$

Tätä yhtälöä kutsutaan *binomikaavaksi*. Binomikaavan avulla voidaan helposti todistaa monia binomikertoimien summakaavoja.

Lause 1.10. $\sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.

Todistus. Sijoitetaan binomikaavaan (2) $x = y = 1$. □

Lause 1.11. $\sum_{i=0}^{n} (-1)^i \binom{n}{i} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - + \cdots + (-1)^n \binom{n}{n} = 0$.

Todistus. Sijoitetaan binomikaavaan $y = 1$ ja $x = -1$. □

Lause 1.12. $\sum_{i=1}^{n} i\binom{n}{i} = \binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n} = n2^{n-1}$.

Todistus. Sijoitetaan binomikaavaan $y = 1$ ja derivoidaan puolittain x:n suhteen, saadaan

$$n(x+1)^{n-1} = \sum_{i=1}^{n} i\binom{n}{i} x^{i-1}. \tag{3}$$

Kun tähän sijoitetaan $x = 1$, niin saadaan väite. □

Lause 1.13. $\sum_{i=1}^{n}(-1)^{i-1}i\binom{n}{i} = \binom{n}{1} - 2\binom{n}{2} + - \cdots + (-1)^{n-1}n\binom{n}{n} = 0.$

Todistus. Sijoitetaan yhtälöön (3) $x = -1$. □

Binomikaavasta saadaan monia summakaavoja derivoimalla usempaan kertaa tai integroimalla ja lopuksi sijoittamalla sopiva x.

1.6 Sovellus: TN-laskenta

Esimerkki 1.13. Millä todennäköisyydellä lotossa yhden rivin täyttämällä saa tarkalleen

a) 7 oikein,
b) 6 oikein,
c) 6 oikein ja lisänumero,
d) 5 oikein ja lisänumero,
e) 5 oikein ja ainakin 1 lisänumero?

a) Lotossa arvotaan 7 numeroa 39:stä. Lottorivejä on siis $\binom{39}{7}$. Täten todennäköisyys sille, että rivissä on 7 oikein on

$$\frac{1}{\binom{39}{7}} \approx 6,5 \cdot 10^{-8}.$$

b) Kuusi oikein rivissä taas pitää olla 6 seitsemästä arvotusta ja yksi muu numero. Tulosäännön mukaan näitä on siis $\binom{7}{6}\binom{32}{1} = 224$ kappaletta. Todennäköisyys on siis

$$\frac{224}{\binom{39}{7}} \approx 1,5 \cdot 10^{-5}.$$

c) Lotossa arvotaan 7 numeron lisäksi 3 lisänumeroa. 6 ja lisänumero rivejä on siis tulosäännön mukaan $\binom{7}{6}\binom{3}{1} = 21$. Todennäköisyys on siis

$$\frac{21}{\binom{39}{7}} \approx 1,4 \cdot 10^{-6}.$$

d) Näitä rivejä on $\binom{7}{5}\binom{3}{1}\binom{29}{1} = 1827$. Todennäköisyys on siis

$$\frac{1827}{\binom{39}{7}} \approx 1,19 \cdot 10^{-4}.$$

e) Nyt lasketaan siis ne rivit, joissa on 5 oikein ja yksi tai kaksi lisänumeroa. Näitä rivejä on summasäännön mukaan $\binom{7}{5}\binom{3}{1}\binom{29}{1} + \binom{7}{5}\binom{3}{2}\binom{29}{0} =$

1890. Todennäköisyys on siis

$$\frac{1890}{\binom{39}{7}} \approx 1,22 \cdot 10^{-4}.$$

Opetus: kannattaa keskittyä taitopeleihin!

Esimerkki 1.14. Vakioveikkauksessa on 13 kohdetta (yleensä jalkapalloottelua), joihin veikataan 1,x tai 2. Vakioveikkauksen oikea rivi ei muodostu satunnaisesti kuten lotossa, mutta oletetaan nyt, että englannissa on lumimyrsky ja oikea rivi muodostetaan arpomalla (ilman painotuksia).

Millä todennäköisyydellä satunnaisesti valitussa rivissä on

a) 13 oikein,

b) ainakin 10 oikein?

c) Kuinka monta sellaista riviä on, joissa on 9 ykköstä, 2 ristiä ja 2 kakkosta?

a) Vakioveikkausrivejä on $P_T(3,13) = 3^{13}$ kappaletta. Todennäköisyys 13 oikein tulokselle on siis

$$\frac{1}{3^{13}} \approx 6,3 \cdot 10^{-7}.$$

(Siis n. 10 kertaa todennäköisempää kuin lotossa 7 oikein.)

b) 13 oikein rivejä on 1. Rivejä, joissa on tarkalleen 12 oikein eli yksi väärin (vääriä merkkejä on kaksi vaihtoehtoa) on $C(13,1) \cdot P_T(2,1) = 13 \cdot 2 = 26$. Tarkalleen 11 oikein rivejä on $C(13,2) \cdot P_T(2,2) = \binom{13}{2} \cdot 2^2 = 312$ ja tarkalleen 10 oikein rivejä on $C(13,3) \cdot P_T(3,3) = \binom{13}{3} \cdot 2^3 = 2288$.

Yhteensä rivejä, joissa on 10 oikein $1 + 26 + 312 + 2288 = 2627$, joten 10 oikein todennäköisyys on

$$\frac{2627}{3^{13}} \approx 0,0016.$$

c) 13 alkion joukko pitää siis partitioida kolmeen joukkoon, joiden alkioden lukumäärät ovat 9, 2 ja 2. Tämän mukaan rivejä on

$$\binom{13}{9,2,2} = \frac{13!}{9!2!2!} = 4290.$$

1.7 Sovellus: Virheitä korjaavat koodit

Rajoitutaan tässä esityksessä ns. *binäärisiin koodeihin*. Tarkastellaan joukkoa $\{0,1\}^n$ eli n-pituisten binääristen sanojen joukkoa. Sen sajoukkoa $C \subseteq \{0,1\}^n$ kutsutaan *koodiksi*. Sanoja, jotka kuuluvat koodiin C, kutsutaan (n-pituisiksi) *koodisanoiksi*.

Yleensä myös kirjoitetaan $\mathbb{F}_2^n$ joukon $\{0,1\}^n$ sijaan. $\mathbb{F}_2$ on (äärellinen) kahden alkion kunta $\{0,1\}$, missä operaatioina on yhteen- ja kertolasku modulo 2. Nyt $\mathbb{F}_2^n$ voidaan ajatella n-ulotteisena vektoriavaruutena yli kunnan

$\mathbb{F}_2$. Tällä algebrallisella esityksellä pystytään tiettyjä koodien ja koodisanojen ominaisuuksia esittämään helposti. Tämä esitys voidaan yleistää myös muille äärellisille kunnille, esim. $\mathbb{F}_3^n$ osajoukot ovat ns. *ternäärisiä* koodeja.

Käytetään koodisanoista merkintää $\mathbf{v} = (a_1, a_2, \ldots, a_n) = a_1 a_2 \ldots a_n$, missä $a_i \in \{0, 1\}$, eli kirjoitetaan koodisanat vektoreina tai sanoina.

Määritelmä 1.7. Koodisanan $\mathbf{u} = u_1 u_2 \ldots u_n$ *paino*

$$w(\mathbf{u}) = |\{i \mid u_i = 1\}|,$$

ts. paino on koodisanan ykkösten lukumäärä.

Koodisanojen $\mathbf{u} = u_1 u_2 \ldots u_n$ ja $\mathbf{v} = v_1 v_2 \ldots v_n$ ns. *Hamming etäisyys*

$$d(\mathbf{u}, \mathbf{v}) = |\{i \mid u_i \neq v_i\}|.$$

Koodisanoille voidaan määritellä yhteen- ja vähennyslasku,

$$\mathbf{u} + \mathbf{v} = a_1 a_2 \ldots a_n, \text{ missä } a_i = u_i + v_i,$$
$$(\mathbf{u} - \mathbf{v} = a_1 a_2 \ldots a_n, \text{ missä } a_i = u_i - v_i).$$

Huomaa, että binääritapauksessa yhteen- ja vähennyslasku antavat aina saman tuloksen. Nyt painolle ja etäisyydelle saadaan yhteys

$$d(\mathbf{u}, \mathbf{v}) = w(\mathbf{u} - \mathbf{v}). \tag{4}$$

Esimerkki 1.15. Olkoon $\mathbf{u} = 010011$ ja $\mathbf{v} = 010110$. Nyt $w(\mathbf{u}) = 3$, $\mathbf{u} - \mathbf{v} = 000101$, joten $d(\mathbf{u}, \mathbf{v}) = 2$.

Esimerkki 1.16. Kuinka paljon on

a) r-painoisia n-pituisia koodisanoja?

b) enintään r-painoisia n-pituisia koodisanoja?

a) $|\{\mathbf{c} \in \mathbb{F}_2^n \mid w(\mathbf{c}) = r\}| = C(n, r) = \binom{n}{r}$.

b) $|\{\mathbf{c} \in \mathbb{F}_2^n \mid w(\mathbf{c}) \leq r\}| = \sum_{i=0}^{r} \binom{n}{i}$.

Määritelmä 1.8. Olkoon $\mathbf{a}$ jokin n-pituinen koodisana ja $e \in \mathbb{N}$. Määritellään $\mathbf{a}$-keskinen e-säteinen *pallo*

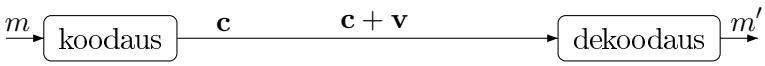
$$B(\mathbf{a}, e) = \{\mathbf{x} \in \mathbb{F}_2^n \mid d(\mathbf{a}, \mathbf{x}) \leq e\}.$$

Lemma 1.2. *e-säteisen pallon alkioiden lukumäärä*

$$B_e = |B(\mathbf{a}, e)| = \sum_{i=0}^{e} \binom{n}{i}.$$

Todistus. DEMO. □

Tarkastellaan lyhyesti tiedonsiirtoa tietoliikennekanavassa. Kanavassa lähetetään viesti m. Aluksi suoritetaan ns. *koodaus*, jossa m muunnetaan koodisanojen jonoksi $\mathbf{c}_1\mathbf{c}_2\ldots$. Koodisanat voidaan ajatella lähetettäväksi yksi kerrallaan. Kun lähetetään koodisana $\mathbf{c}$, häiriöisessä kanavassa voi tapahtua virhe $\mathbf{v}(\in \mathbb{F}_2^n)$, jolloin vastaanottaja saa sanan $\mathbf{c}+\mathbf{v}$. *Dekoodauksessa* koodisanat muunnetaan takaisin viestiksi m'.



Kuva 1: Tiedonsiirtokanava.

Toivottavaa tietysti on, että m ja m' ovat samat. Koodi $C \subseteq \mathbb{F}_2^n$ on e virhettä korjaava, jos dekoodaus onnistuu aina oikein, kun $w(\mathbf{v}) \leq e$. Tämä tarkoittaa, että koodisana keskeiset e-säteiset pallot eivät leikkaa, siis C on e virhettä korjaava, jos

$$\forall \mathbf{a}, \mathbf{b} \in C\colon \mathbf{a} \neq \mathbf{b} \implies B(\mathbf{a}, e) \cap B(\mathbf{b}, e) = \emptyset.$$

Määritelmä 1.9. Koodin $C \subseteq \mathbb{F}_2^n$ *minimietäisyys*

$$d(C) = \min\{d(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in C,\ \mathbf{u} \neq \mathbf{v}\}.$$

Jos nyt C on e virhettä korjaava, niin $d(C) \geq 2e+1$. Koodausteoriassa pyritään löytämään mahdollisimman hyviä koodeja joidenkin annettujen kriteerien mukaan. Esimerkiksi voidaan etsiä koodia, jonka pituus on n, minimietäisyys d, ja jossa on mahdollisimman monta koodisanaa.

Seuraava lause antaa koodisanojen lukumäärälle ns. *Hamming-rajan* (*pallopakkausraja*).

Lause 1.14. *Olkoon $C \subseteq \mathbb{F}_2^n$ koodi, jonka minimietäisyys on $d = 2e+1$. Tällöin*

$$|C| \leq \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}}. \tag{5}$$

Todistus. Minietäisyyden nojalla

$$|C| \cdot B_e \leq |\mathbb{F}_2^n| = 2^n,$$

ja nyt lemman 1.2 nojalla saadaan väite. □

Jos koodille C yhtälössä (5) on voimassa yhtäsuuruus, niin se on ns. *täydellinen koodi*.

Esimerkki 1.17. 7-pituisessa 3 virhettä korjaavassa koodissa on koodisanoja enintään

$$\frac{2^7}{1+7+21+35} = 2.$$

Esimerkiksi $\{0000000, 1111111\}$ on tälläinen koodi.

Koodi $C \subseteq \mathbb{F}_2^n$ on *lineaarinen*, jos se on $\mathbb{F}_2^n$:n aliavaruus. Lineaarisille koodeille saadaan lineaarialgebran avulla mukavia ominaisuuksia.

Olkoon $C \subseteq \mathbb{F}_2^n$ lineaarinen koodi. Aliavaruuskriteerien mukaisesti: jos $\mathbf{u}, \mathbf{v} \in C$, niin $\mathbf{u}+\mathbf{v} \in C$. Lisäksi $\mathbf{0} \in C$. Koodin minimietäisyys voidaan nyt määritellä

$$d(C) = \min\{w(\mathbf{c}) \mid \mathbf{c} \in C \setminus \{\mathbf{0}\}\}.$$

Koodilla C on myös kanta, sanotaan $B = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k\}$, missä $k = \dim C$. Koska kaikilla koodin C vektoreilla on yksikäsitteinen kantaesitys, niin

$$|C| = 2^k.$$

Koodin C *generoiva matriisi* on

$$G = \begin{pmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_k \end{pmatrix} \in \mathbb{F}_2^{k\times n}.$$

Nyt

$$\mathbf{c} \in C \iff \exists \mathbf{u} \in \mathbb{F}_2^k \colon \mathbf{u}G = \mathbf{c}.$$

Voidaan olettaa, että G on redusoitu porrasmatriisi, ts. $G = \begin{pmatrix} I_k & P \end{pmatrix}$, missä P on $k \times (n-k)$-matriisi.

Lineaarisella koodilla C on ns. *tarkistusmatriisi* $H \in \mathbb{F}_2^{(n-k)\times n}$, joka toteuttaa ehdon

$$\mathbf{c} \in C \iff \mathbf{c}H^T = \mathbf{0},$$

missä H^T on matriisin H transpoosi. Voidaan osoittaa, että matriisi

$$H = \begin{pmatrix} P^T & I_{n-k} \end{pmatrix},$$

on koodin C tarkistusmatriisi. Nyt matriisin H aste $r(H) = n-k$. Tästä saadaan koodisanojen lukumäärälle uusi lauseke, nimittäin, jos H on C:n tarkistusmatriisi, niin

$$|C| = 2^{n-r(H)} = (2^{n-(n-k)} = 2^k).$$

Esimerkki 1.18. Tarkastellaan koodia

$$\mathcal{H}_7 = \left\{\mathbf{c} \in \mathbb{F}_2^7 \mid \mathbf{c}H^T = \mathbf{0}\right\},$$

missä

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

2 PERUSMENETELMIÄ

2.1 Lokeroperiaate

Lokeroperiaate on kaikille tuttu. Kaikessa yksinkertaisuudessaan se voidaan esittää seuraavasti:

Jos n lokerossa on enemmän kuin n palloa, niin ainakin yhdessä lokerossa on enemmän kuin yksi pallo.

Ts. jos meillä on n lokeroa, $n+1$ palloa, niin ainakin yhdessä lokerossa on kaksi palloa.

Lokeroperiaatetta kutsutaan joskus nimellä *Dirichlet'n* lokeroperiaate tai *kyyhkyslakkaperiaate* (engl. pigeon hole principle).

Vaikka lokeroperiaate hienoudessaan omaksutaan jo koulussa sukkien ja pallojen avulla, sitä ei pidä väheksyä. Lokeroperiaatetta käytetään monien vaikeiden teorioiden kombinatorisissa todistuksissa. Lokeroperiaatteesta esiintyy myös seuraava yleistetty muoto:

Jos n lokerossa on enemmän kuin nm palloa, niin ainakin yhdessä lokerossa on enemmän kuin m palloa.

Esimerkki 2.1. Osoita, että jos joukosta $\{1, 2, \ldots, 2n\}$ valitaan $n+1$ alkioinen osajoukko, niin siinä on kaksi lukua, joiden osamäärä on 2:n potenssi.

Olkoon $A = \{a_1, a_2, \ldots, a_{n+1}\}$ jokin edellä mainittu $n+1$ alkioinen joukko. Kirjoitetaan luvut a_i muodossa

$$a_i = k_i \cdot 2^{\ell_i},$$

missä k_i on luvun a_i suurin pariton tekijä. Luvuilla a_i suurimpina parittomina tekijöinä voivat esiintyä luvut $1, 3, 5, \cdots, 2n-1$. Näitä parittomia lukuja on siis n kappaletta. Jaetaan luvut a_i lukujen k_i mukaisesti näihin n lokeroon. Lukuja a_i on $n+1$ kappaletta, joten lokeroperiaatteen mukaan jossakin lokerossa on ainakin kaksi lukua, sanotaan a_{i_1} ja a_{i_2} ja näiden osamäärä on $2^{\ell_{i_1} - \ell_{i_2}}$.

Esimerkki 2.2. Juhlissa ihmiset kättelevät toisiaan. Osoita, että juhlien aikana kaksi ihmistä kättelee yhtä monta ihmistä.

Esimerkki 2.3. Olkoot A ja B äärellisiä joukkoja, joille $|A| = n > r = |B|$, ja f kuvaus, $f\colon A \to B$.

Osoita, että jollekin $b \in B$, $|f^{-1}(b)| \geq \left\lceil \frac{n}{r} \right\rceil$.

2.2 Sovellus: Kasvavat ja vähenevät osajonot

Tarkastellaan n-pituista reaalilukujonoa $u = u_1, u_2, \ldots, u_n$, missä siis $u_i \in \mathbb{R}$. Jonon u k-pituinen *osajono* $u_{i_1}, u_{i_2}, \ldots u_{i_k}$, missä $i_1 < i_2 < \cdots < i_k$, on *kasvava*, jos

$$u_{i_1} < u_{i_2} < \cdots < u_{i_k}$$

ja *vähenevä*, jos

$$u_{i_1} > u_{i_2} > \cdots > u_{i_k}.$$

Lause 2.1. *Olkoot $m, n > 0$. Jokainen erisuurien reaalilukujen jono $u_1, u_2, \ldots, u_{mn+1}$ sisältää $(m+1)$-pituisen kasvavan osajonon tai $(n+1)$ pituisen vähenevän osajonon, tai molemmat.*

Todistus. Merkitään t_i:llä u_i:stä alkavan pisimmän kasvavan osajonon pituutta. Jos jokin luvuista $t_i \geq m+1$, väite on tosi. Oletetaan siis, että $t_i < m+1$ kaikilla $1 \leq i \leq mn+1$. Nyt siis t_i:t kuuluvat joukkoon $\{1, 2, \ldots, m\}$ ja koska näitä lukuja on $mn+1$, yleistetyn lokeroperiaatteen mukaan on olemassa vähintään $n+1$ lukua i välillä $1, \ldots, mn+1$, joilla on sama t_i:n arvo. Merkitään näitä lukuja

$$u_{i_1}, u_{i_2}, \ldots, u_{i_{n+1}}, \text{ missä } i_1 < i_2 < \cdots < i_{n+1}. \tag{6}$$

Tarkastellaan nyt kahta peräkkäistä lukua u_{i_j} ja $u_{i_{j+1}}$. Huomataan, että $u_{i_j} > u_{i_{j+1}}$, koska muuten u_{i_j}:stä alkava pisin kasvava lukujono on pitempi kuin $u_{i_{j+1}}$:stä alkava, mikä on vastoin oletusta. Siis jono (6) on vähenevä $(n+1)$-pituinen osajono. □

Tämä tulos on paras mahdollinen, sillä on olemassa mn pituisia lukujonoja, joilla ei ole $(m+1)$-pituista kasvavaa tai $(n+1)$-pituista vähenevää. Esimerkiksi, jos $m = n = 4$, niin jono,

$$4, 3, 2, 1, 8, 7, 6, 5, 12, 11, 10, 9, 16, 15, 14, 13$$

ei sisällä viiden pituista kasvavaa tai vähenevää osajonoa.

2.3 Kaksoislaskenta

Kaksoislaskenta on lokeroperiaatteen tavoin hyvin yksinkertainen periaate.

Olkoot A ja B kaksi äärellistä joukkoa ja (*relaatio*) $R \subseteq A \times B$. Jos $(a, b) \in R$, niin sanotaan, että a ja b ovat *relaatiossa* R. Merkitään α_a:lla a:n kanssa ($a \in A$) relaatiossa olevien B:n alkioiden lukumäärää ja β_b:llä vastaavasti b:n kanssa ($b \in B$) relaatiossa olevien A:n alkioiden lukumäärää. Nyt

$$\sum_{a \in A} \alpha_a = |R| = \sum_{b \in B} \beta_b \ (\textit{kaksoislaskenta}).$$

Kaksoislaskennan yhtälö on itsestään selvä. Se osoittautuu kuitenkin hyväksi menetelmäksi joissain tapauksissa.

Esimerkki 2.4. Osoitetaan, että

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

tarkastelemalla relaatiota $R = \{(x, y) \mid x < y\} \subseteq \{1, 2, \ldots, n+1\}^2$.

Kaksoislaskenta voidaan tulkita myös toisella tavalla. Olkoon $A = \{a_1, a_2, \cdots, a_m\}$ ja $B = \{b_1, b_2, \ldots, b_n\}$. Relaation $R \subseteq A \times B$ *relaatiomatriisi* on $m \times n$-matriisi M_R, jossa alkio

$$(i, j) = \begin{cases} 1, & \text{jos } (a_i, b_j) \in R, \\ 0, & \text{muulloin.} \end{cases}$$

Kaksoislaskentayhtälön mukaan matriisin M_R ykkösten määrä on sama laskettuna vaakariveittäin tai pystyriveittäin.

2.4 Sovellus: Jakajien lukumäärän keskiarvo

Tarkastellaan kaksoislaskennan sovelluksena luonnollisten lukujen jakajien keskiarvoa. Olkoon $A_n = \{1, 2, \ldots, n\}$ ja relaatio $R = \{(i, j) \mid i|j\} \subseteq A_n \times A_n$, missä merkintä $i|j$ tarkoittaa, että "i jakaa j:n". Tarkastellaan matriisia M_R. Alla esimerkki tapaus $n = 8$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Tarkastellaan funktiota $t(i)$, joka antaa luvun i jakajien lukumäärän. Jos i on alkuluku, $t(i) = 2$, ja jos $i = 2^k$, niin $t(i) = k + 1$. Funktion t arvot siis vaihtelevat paljon. Entäpä jakajien lukumäärän keskiarvo? Merkitään funktion t keskiarvoa joukossa A_n $\bar{t}(n)$:llä, siis

$$\bar{t}(n) = \frac{1}{n} \sum_{i=1}^{n} t(i). \tag{7}$$

Keskiarvo $\bar{t}(n)$ saadaan matriisista M_R laskemalla ykkösten lukumäärä ja jakamalla n:llä. Määritelmässä (7) tämä on tehty pystyriveittäin. Lasketaan samat ykköset vaakariveittäin: luku i jakaa luvut $1i, 2i, 3i, \ldots, \left\lfloor \frac{n}{i} \right\rfloor i$.

Jokaisella vaakarivillä on siis $\left\lfloor \frac{n}{i} \right\rfloor$ ykköstä, ja

$$\bar{t}(n) = \frac{1}{n} \sum_{i=1}^{n} \left\lfloor \frac{n}{i} \right\rfloor = \frac{1}{n} \sum_{i=1}^{n} \left(\frac{n}{i} - c_i \right),$$

missä $0 \leq c_i < 1$ kaikille $i \in \{1, 2, \ldots, n\}$. Näin ollen yhteen laskettu virhe summassa on alle n, joten keskiarvossa virhe on alle 1. Saatiin siis, että

$$\bar{t}(n) = \frac{1}{n} \sum_{i=1}^{n} \frac{n}{i} - c = \sum_{i=1}^{n} \frac{1}{i} - c = H_n - c,$$

missä $0 \leq c < 1$. Analyysin kursseilta tiedetään, että harmoonisen sarjan osasummalle H_n on voimassa, että

$$\ln n + \frac{1}{n} < H_n < \ln n + 1,$$

joten saadaan, että

$$\ln n + \frac{1}{n} - c < \bar{t}(n) < \ln n + 1 - c,$$

ja siis

$$\ln n - 1 < \bar{t}(n) < \ln n + 1,$$

Saadaan siis, että $\bar{t}(n)$ poikkeaa $\ln n$:stä siis alle 1 verran. Nyt siis

$$\lim_{n \to \infty} \frac{\bar{t}(n)}{\ln n} = 1.$$

Yleensä merkitään $\bar{t}(n) \sim \ln n$.

2.5 Seulaperiaate

Edellisessä luvussa esitetyn summasäännön nojalla

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|,$$

jos joukot A_i ovat erillisiä. Tarkastellaan nyt tapausta, jossa erillisyys-ehto ei välttämättä ole voimassa. On helppo osoittaa, että

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

Yleistetään tämä useammalle joukolle seuraavassa lauseessa. Sen laskenta menetelmää kutsutaan *seulaperiaatteeksi* (engl. principle of inclusion and exclusion).

Esitellään aluksi merkinnät. Olkoot A_i, $1 \leq i \leq n$, äärellisiä joukkoja. Merkitään

$$\begin{aligned} S_1 &= |A_1| + |A_2| + \cdots |A_n|, \\ S_2 &= |A_1 \cap A_2| + |A_1 \cap A_3| + \cdots = \sum_{i<j} |A_i \cap A_j|, \\ S_3 &= |A_1 \cap A_2 \cap A_3| + \cdots = \sum_{i_1<i_2<i_3} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|, \\ &\vdots \\ S_n &= |A_1 \cap A_2 \cap \cdots \cap A_n|. \end{aligned} \tag{8}$$

Lause 2.2. $|A_1 \cup A_2 \cup \cdots \cup A_n| = S_1 - S_2 + S_3 - + \cdots (-1)^{n-1} S_n$.

Todistus. Osoitetaan, että jokainen joukon $A_1 \cup A_2 \cup \cdots \cup A_n$ alkio tulee laskettua kerran oikean puolen summaan. Oletetaan, että x kuuluu tarkalleen m joukkoon joukoista A_i. S_1:ssä x lisätään $C(m,1) = \binom{m}{1}$ kertaa, vähennetään S_2:ssa $C(m,2) = \binom{m}{2}$ kertaa, jne. S_i:ssä x aiheutta termin $(-1)^{i-1}C(m,i) = (-1)^{i-1}\binom{m}{i}$. Saadaan, että x:n aiheuttama kokonaissumma oikealla puolella on

$$\begin{aligned} \sum_{i=1}^{n}(-1)^{i-1}\binom{m}{i} &= \sum_{i=1}^{m}(-1)^{i-1}\binom{m}{i} = 1 - \binom{m}{0} + \sum_{i=1}^{m}(-1)^{i-1}\binom{m}{i} \\ &= 1 - \sum_{i=0}^{m}(-1)^{i}\binom{m}{i} = 1, \end{aligned}$$

lauseen 1.11 mukaan. □

Seuraus 2.1. *Olkoon* $|X| = N$ *ja* $A_i \subseteq X$, *aina kun* $1 \leq i \leq n$. *Nyt*

$$|X \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = N - S_1 + S_2 - + \cdots + (-1)^n S_n.$$

Esimerkki 2.5. Olkoon $\{a,b,c\}$ aakkosto. Kuinka monta sellaista 8 pituista sanaa on olemassa, joissa kaikki kirjaimet esiintyvät ainakin kerran?

Kahdeksan pituisia sanoja on $3^8 = 6561$ kappaletta. Merkitään aakkoston X k-pituisten sanojen joukkoa X^k:lla. Valitaan joukot $A_1 = \{a,b\}^8$, $A_2 = \{a,c\}^8$ ja $A_3 = \{b,c\}^8$. Lasketaan kuinka monessa kahdeksan mittaisessa sanassa on korkeintaan kaksi kirjainta käytössä. Nyt $S_1 = |A_1|+|A_2|+|A_3| = 3 \cdot 2^8 = 768$ (korkeintaan kahta kirjainta), ja $S_2 = |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| = 3$ (korkeintaan yhtä kirjainta). Seulaperiaatteen mukaan sanoja, joissa kaikki kolme kirjainta esiintyy on

$$3^8 - 3 \cdot 2^8 + 3 = 5796.$$

Esimerkki 2.6. Kuinka monessa nelinumeroisessa luonnollisessa luvussa ei ole nollaa tai ykköstä? Entä kuinka monessa on nolla tai yksi?

Esimerkki 2.7. Korttipakassa on 52 korttia, jotka jakaantuvat neljään maahan, kuhunkin 13 korttia. Kuinka monta sellaista viiden kortin "kättä" on olemassa, joissa on kaikkia maita?

2.6 Sovellus: Derangement-ongelma

Tarkastellaan nyt sovellusta, josta yleisesti käytetään nimeä *derangements*-ongelma.

Ongelma 2.1. Sihteerillä on n osoitteellista kirjekuorta ja niihin n kirjettä, jotka myös on osoitettu nimenomaisille vastaanottajille. Hän laittaa yhden kirjeen jokaiseen kuoreen. Kuinka monella tavalla hän voi laittaa kirjeet kuoriin siten, että kaikki kirjeet menevät vääriin kuoriin?

Merkitään lukumäärää D_n:llä. Tarkastellaan n alkion joukon permutaatioita eli joukkoa

$$\mathcal{S}_n = \{\pi \mid \pi\colon\ \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}\,,\ \pi \text{ on bijektio }\}\,.$$

D_n on siis niiden permutaatioiden π lukumäärä, joissa kaikilla $i \in \{1,2,\ldots,n\}$ $\pi(i) \neq i$. Näitä permutaatioita kutsutaan muuten usein *derangement*-permutaatioiksi. Määritellään joukko

$$A_i = \{\pi \in \mathcal{S}_n \mid \pi(i) = i\}\,,$$

kaikille $i \in \{1,2,\ldots,n\}$. Lasketaan niiden permutaatioden lukumäärä, joissa ainakin yksi kirje menee oikeaan kuoreen, seulaperiaatteella. Summa S_r on siis niiden permutaatioiden lukumäärä, joissa vähintäin r alkiota kuvautuu itsekseen eli vähintään r kuorta menee oikeaan kuoreen. Toisaalta nämä r kuorta voidaan valita $\binom{n}{r}$ tavalla ja loput alkiot järjestää $(n-r)!$ tavalla, joten

$$S_r = \binom{n}{r}(n-r)! = \frac{n!}{r!}.$$

Nyt seulaperiaattella saadaan, että vähintään yksi kirje menee oikeaan kuoreen

$$\frac{n!}{1!} - \frac{n!}{2!} + - \cdots + (-1)^{n-1}\frac{n!}{n!} = n!\Big(\sum_{i=1}^{n}(-1)^{i-1}\frac{1}{i!}\Big)$$

tavalla, mistä seuraa, että

$$D_n = |\mathcal{S}_n| - n!\Big(\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i!}\Big) = n!\Big(\sum_{i=0}^{n}\frac{(-1)^{i}}{i!}\Big).$$

2.7 Sovellus: Eulerin funktio ja Möbiuksen funktio

Tämä pykälän sovellukset tulevat lukuteoriasta ja liittyvät luvun tekijöihin.

Eulerin funktio $\varphi\colon \mathbb{N} \to \mathbb{N}$ määritellään luvulle $n \in \mathbb{N}$, $n \geq 2$,

$$\varphi(n) = |\,\{x \in \mathbb{N} \mid 1 \leq x \leq n,\ \mathrm{syt}(x,n) = 1\}\,|.$$

Eulerin funktio kertoo siis lukua n pienempien sen kanssa suhteellisten alkulukujen lukumäärän, tai vielä yksinkertaisemmin, niiden lukua n pienempien lukujen lukumäärän, jotka eivät ole luvun n jakajan monikertoja.

Oletetaan, että luvun n alkutekijäesitys on

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

missä luvut p_i ovat eri alkulukuja. Nyt

$$d = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

jakaa n:n tarkalleen silloin kun $f_i \leq e_i$ kaikille $1 \leq i \leq k$. Luvulle $\varphi(n)$ saadaan kaava seulaperiaatteen avulla.

Lause 2.3. $\varphi(n) = n\Big(1 - \dfrac{1}{p_1}\Big)\Big(1 - \dfrac{1}{p_2}\Big) \cdots \Big(1 - \dfrac{1}{p_k}\Big)$.

Todistus. Olkoon $A_j = \left\{ ip_j \mid 1 \leq i \leq \dfrac{n}{p_j} \right\}$ $(1 \leq j \leq k)$. Seulaperiaatteen mukaan

$$\varphi(n) = n - |A_1 \cup A_2 \cup \cdots \cup A_k| = n - S_1 + S_2 - + \cdots + (-1)^k S_k,$$

missä S_j:t ovat kuten yhtälöissä (8). Leikkaus

$$A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_\ell}$$

muodostuu luvun $P = p_{j_1} p_{j_2} \cdots p_{j_\ell}$ monikerroista joukossa $\{1, 2, \ldots, n\}$. Siis

$$|A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_\ell}| = \frac{n}{P} = n \cdot \frac{1}{p_{j_1}} \frac{1}{p_{j_2}} \cdots \frac{1}{p_{j_\ell}} \tag{9}$$

ja

$$\begin{aligned} \varphi(n) =& n - n\Big(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k}\Big) + n\Big(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots\Big) - + \\ & \cdots + (-1)^k n \cdot \frac{1}{p_1 p_2 \cdots p_k} \\ =& n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big). \end{aligned} \tag{10}$$

□

Esimerkki 2.8. Luku $60 = 2^2 \cdot 3 \cdot 5$, joten

$$\varphi(60) = 60\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{3}\Big)\Big(1 - \frac{1}{5}\Big) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16.$$

Määritellään seuraavaksi ns. *Möbiuksen funktio*

$$\mu(d) = \begin{cases} 1, & \text{jos } d = 1, \\ (-1)^k, & \text{jos } d \text{ on } k \text{ eri alkuluvun tulo,} \\ 0, & \text{muulloin (jos } \ell^2 | d,\ \ell > 1). \end{cases}$$

Esimerkki 2.9. Lasketaan $\mu(15) = (-1)^2 = 1$, $\mu(30) = (-1)^3 = -1$ ja $\mu(60) = 0$.

Lause 2.4. $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.

Todistus. Kun tarkastellaan Lauseen 2.3 todistuksen yhtälöitä (9) ja (10), niin nähdään, että summattavat ovat muotoa

$$(-1)^\ell n \cdot \frac{1}{p_{j_1}} \frac{1}{p_{j_2}} \cdots \frac{1}{p_{j_\ell}} = (-1)^\ell \frac{n}{d},$$

missä $d = p_{j_1} \cdots p_{j_\ell}$ eli ℓ eri alkuluvun tulo. Nyt $(-1)^\ell$ voidaan korvata $\mu(d)$:llä ja laskea summa yli kaikkien n:n jakajien, koska Möbius funktion arvo on 0 niille jakajille, jotka eivät sisälly summaan. □

Lause 2.5. $\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{jos } n = 1, \\ 0, & \textit{jos } n \geq 2. \end{cases}$

Todistus. Jos $n = 1$, niin väite seuraa Möbiuksen funktion määritelmästä. Tarkastellaan siis tapausta $n \geq 2$. Olkoon $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, missä p_i:t ovat alkulukuja. Jos $d|n$, niin $d = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, missä $f_i \leq e_i$ kaikille $1 \leq i \leq k$. Jos $\mu(d) \neq 0$, niin jokainen f_i on 0 tai 1. Jokaista tällaista jakajaa d vastaa siis joukon $\{p_1, p_2, \ldots, p_k\}$ osajoukko. ℓ alkioisia osajoukkoja on $C(k, \ell) = \binom{k}{\ell}$ ja kaikille ℓ alkuluvun tuloille d $\mu(d) = (-1)^\ell$. Siis

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} = 0.$$

□

Seuraavaksi todistetaan ns. *Möbiuksen inversiokaava.*

Lause 2.6. *Jos kuvaus* $g\colon \mathbb{N} \to \mathbb{C}$ *ja* f *on määritelty yhtälöllä*

$$f(n) = \sum_{d|n} g(d), \tag{11}$$

niin

$$g(n) = \sum_{d|n} \mu(d) f\Big(\frac{n}{d}\Big). \tag{12}$$

Todistus. Sijoittamalla yhtälö (11) saadaan

$$\begin{aligned}\sum_{d|n} \mu(d) f\Big(\frac{n}{d}\Big) &= \sum_{d|n} \mu\Big(\frac{n}{d}\Big) f(d) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \sum_{d'|d} g(d') \\ &= \sum_{d|n} \sum_{d'|d} \mu\Big(\frac{n}{d}\Big) g(d') = \sum_{d'|n} g(d') \sum_{m|\frac{n}{d'}} \mu(m) = g(n),\end{aligned}$$

koska sisäsumma on 0 aina kun $d' \neq n$.

□

Möbiuksen inversiokaava voidaan todistaa myös muilla tavoin. Esimerkiksi voidaan tarkastella ns. lukuteoreettisia funktioita, jotka muodostavat renkaan (*konvoluution* ja *summan* suhteen). Möbiuksen inversiokaavan käytöstä tarkastellaan seuraavaa sovellusta, joka liittyy sanoihin.

2.8 Sovellus: Primitiiviset sanat

Tarkastellaan aakkostoa X. Merkitään X^*:llä kaikkien aakkoston X äärellisten sanojen joukkoa. X^*:ssä voidaan määritellä (assosiatiivinen) operaatio *katenaation*, missä sanat kirjoitetaan peräkkäin. Esimerkiksi, jos $X = \{a, b\}$, niin $aba \cdot bba = ababba$. Huomaa, että ns. *tyhjä sana* ε kuuluu joukkoon X^*.

Sanan $w \in X^*$ pituudelle käytetään merkintää $|w|$. Erityisesti $|\varepsilon| = 0$.

Määritelmä 2.1. Sanan $u \in X^*$ k:s *potenssi* u^k määritellään induktiivisesti, $u^0 = \varepsilon$, $u^1 = u$ ja $u^{i+1} = u^i u$ kaikilla $i \geq 2$.

Sana $w \in X^*$ on *primitiivinen*, jos

$$w = u^k \implies u = w \text{ ja } k = 1,$$

ts. primitiivinen sana ei ole minkään muun sanan potenssi.

Esimerkki 2.10. Sana $abbaabbaabba = (abba)^3$ ja sana $abaababa$ on primitiivinen.

Määritelmä 2.2. Sana u on sanan x *primitiivinen juuri*, jos $x = u^k$ ja u on primitiivinen. Luonnollista lukua k kutsutaan x:n *eksponentiksi*. Huomaa, että $k|(|x|)$.

Lemma 2.1. *Jos sanoille u ja v on voimassa $uv = vu$, niin silloin on olemassa sana w ja luvut ℓ ja k, joille*

$$u = w^\ell \quad ja \quad v = w^k.$$

Ts. sanoilla u ja v on yhteinen primitiivinen juuri.

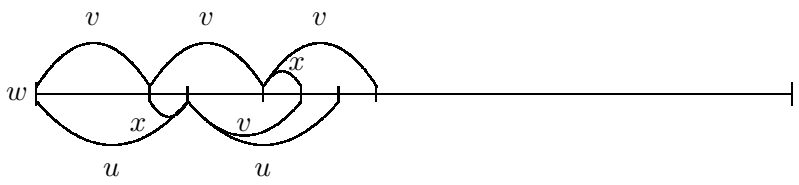
Todistus. Sivuutetaan. □

Lemma 2.2. *Sanan primitiivinen juuri on yksikäsitteinen.*

Todistus. Tehdään vastaoletus, nimittäin oletetaan, että jollekin sanalle w, $w = u^\ell$ ja $w = v^k$, missä $u \neq v$ ja molemmat sanat u ja v ovat primitiivisiä. Oletetaan (symmetrian nojalla), että $|u| \geq |v|$. Nyt $w = u^\ell = v^k$, joten on olemassa luku i ja sana x, joille $u = v^i x$, ja x on sanan v alkuosa. Edelleen saadaan, että

$$uv = v^i xv = v^i vx,$$

ks. Kuva 2. Näin ollen $vx = xv$, joten Lemman 2.1 mukaan niillä on yhteinen primitiivinen juuri, ja siis sanoilla u ja v on yhteinen primitiivinen juuri. Tämä taas on ristiriidassa oletuksen kanssa. □



Kuva 2: Sanan w jako u:n ja v:n avulla. Huomaa, että $i = 1$ koska $|u| < 2|v|$.

Määritelmä 2.3. Sanat x ja y ovat *konjugaatteja*, jos on olemassa sellaiset sanat u ja v, että $x = uv$ ja $y = vu$.

Esimerkki 2.11. Sanat *abbbabbbc* ja *abbbcabbb* ovat konjugaatteja.

Huomautus 5. Sanat ovat konjugaateja, jos ne saadaan toisistaan ns. syklisin siirroin eli siirtämällä kirjaimia lopusta yksi kerrallaan alkuun. Esimerkiksi *abcd*, *dabc*, *cdab*, *bcda* ovat konjugaatteja.

Seuraava lause antaa summamuodon k-kirjaimisen aakkoston n-pituisten primitiivisten sanojen lukumäärälle $p_n(k)$.

Tarkastellaan aluksi n-pituisten sanojen *konjugaattiluokkia*. Sanotaan, että x ja y kuuluvat samaan konjugaattiluokkaan, jos ne ovat konjugaatteja.

Lemma 2.3. *Olkoon u sanan x primitiivinen juuri ja $x = u^\ell$. Tällöin x:n konjugaattiluokkaan kuuluu $\frac{|x|}{\ell}$ eri sanaa.*

Todistus. Sivuutetaan. □

Edellisellä lemmalla on seuraava seuraus, joka tosin voitaisiin todistaa suoraankin.

Seuraus 2.2. *Jos x on primitiivinen, niin kaikki sen konjugaattiluokkaan kuuluvat sanat ovat primitiivisiä ja erisuuria.*

Merkitään $\ell_n(k)$:lla k-kirjaimisen aakkoston n-pituisten primitiivisten sanojen **konjugaattiluokkien** lukumäärää. Huomaa, että edellisen seurauksen mukaan $n\ell_n(k) = p_n(k)$.

Lemma 2.4. $k^n = \sum_{d|n} d l_d(k)$.

Todistus. Tarkastellaan n-pituisia aakkoston X sanoja, kun $|X| = k$,

$$\begin{aligned} k^n = |X^n| &= |\{u^m \mid u \text{ on primitiivinen, } |u| = d,\ md = n\}| \\ &= \sum_{d|n} |\{u \mid u \text{ on prim. ja } |u| = d\}| \\ &= \sum_{d|n} d \cdot l_d(k). \end{aligned}$$

□

Nyt olemme valmiit todistamaan primitiivisten sanojen lukumäärälle summakaavan.

Lause 2.7. $p_n(k) = \sum_{d|n} \mu\left(\frac{n}{d}\right) k^d$.

Todistus. Koska $p_n(k) = n\ell_n(k)$, ja tiedetään, että $\ell_n(k)$ toteuttaa yhtälön

$$k^n = \sum_{d|n} d l_d(k).$$

Nyt Möbiuksen inversiokaavan mukaan

$$(p_n(k) =) n\ell_n(k) = \sum_{d|n} \mu(d) k^{\frac{n}{d}} = \sum_{d|n} \mu\left(\frac{n}{d}\right) k^d.$$

□

Saatu kaava ei ole kovin käyttökelpoinen suurille luvuille n, mutta siitä nähdään, että asymptoottisesti "melkein kaikki" sanat ovat primitiivisiä.

3 REKURSIOT

3.1 Palautuskaava

Tässä luvussa tarkastellaan lukujonoja ja niiden jäsenten esityksiä.

Olkoon $(u_n)_{n=0}^{\infty}$ jokin lukujono. Yhtälöä

$$u_{n+k} = h(u_{n+k-1}, u_{n+k-2}, \ldots, u_n),$$

jonka jonon $(u_n)_{n=0}^{\infty}$ jäsenet toteuttavat, kutsutaan jonon *palautuskaavaksi* tai *rekursioksi*. h on kuvaus joukkoon $\mathbb{C}$, se saa argumenteikseen jononjäseniä ja luvun n. Jononjäsenet lausutaan siis k edellisen jäsenen funktiona. Jäseniä $u_0, u_1, \ldots, u_{k-1}$ kutsutaan *alkuehdoiksi*. Käytetään jonosta $(u_n)_{n=0}^{\infty}$ yksinkertaisesti merkintää (u_n), jos sekaannuksen vaaraa ei ole.

Palautuskaava on *lineaarinen*, jos h on lineaarinen (ensimmäistä astetta) jäsenten u_i suhteen ja *vakiokertoiminen*, jos funktiossa h jäsenten u_i kertoimet ovat vakioita. Usein lineaarinen vakiokertoiminen palautuskaava annetaan muodossa

$$\begin{cases} u_0 = b_0, u_1 = b_1, \ldots, u_{k-1} = b_{k-1}, \\ u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n + f(n) \end{cases} \quad (n \geq 0), \qquad (13)$$

missä $a_i \in \mathbb{C}$ kaikilla $1 \leq i \leq k$, $a_k \neq 0$ ja $f\colon \mathbb{N} \to \mathbb{C}$ on funktio. Tällöin sanotaan, että palautuskaava on *kertalukua* k. Palautuskaava on *homogeeninen*, jos $f(n) = 0$ (kaikilla n). Sanotaan, että funktio $g\colon \mathbb{N} \to \mathbb{C}$ on palautuskaavan *ratkaisu*, jos $u_n = g(n)$ kaikille $n \in \mathbb{N}$.

Joskus palautuskaava (13) esitetään muodossa

$$\begin{cases} u_0 = b_0, u_1 = b_1, \ldots, u_{k-1} = b_{k-1}, \\ u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + f_2(n) \end{cases} \quad (n \geq k). \qquad (14)$$

Huomaa, että $f_2(n) = f(n-k)$, ts. epähomogeeninen osa on muuttunut.

Esimerkki 3.1. Olkoon a_n sellaisten n-pituisten binäärilukujen lukumäärä, joissa ei ole kahta peräkkäistä nollaa. Etsi jonolle (a_n) palautuskaava.

3.2 Homogeenisen lineaarisen palautuskaavan ratkaisu

Tarkastellaan homogeenista palautuskaavaa

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n, \qquad (15)$$

missä $a_k \neq 0$.

Määritelmä 3.1. Palautuskaavan (15) *karakteristinen yhtälö* on

$$x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_{k-1} x - a_k = 0 \tag{16}$$

Karakteristisen yhtälön ratkaisuja $r_1, r_2, \ldots, r_k (\in \mathbb{C})$ kutsutaan *karakteristisiksi juuriksi*. Huomaa, että $a_k \neq 0$, joten 0 ei voi olla karakteristinen juuri. Karakteristisen yhtälön (16) polynomia kutsutaan joskus jono *karakteristiseksi polynomiksi*.

Jokaisella rekursiolla on useita ratkaisuja, jos alkuehtoja ei oteta huomioon. Rekursion *yleisellä ratkaisulla* tarkoitetaan ratkaisua, jossa alkuehtoja ei oteta huomioon vaan vakiokertoimet ovat muuttujia ja rekursion jokainen ratkaisu voidaan esittää ratkaisemalla nämä kertoimet alkuehdoista.

Lemma 3.1. *Jono $u_n = r^n$, $r \neq 0$ on rekursion ratkaisu silloin ja vain silloin kun r on rekursion karakteristinen juuri.*

Todistus. Jono r^n toteuttaa rekursion (15) silloin ja vain silloin kun

$$r^{n+k} = a_1 r^{n+k-1} + a_2 r^{n+k-2} + \cdots + a_k r^n,$$

kaikille $n \geq 0$. Kertomalla tämä yhtälö puolittain r^{-n}:llä saadaan

$$r^k - a_1 r^{k-1} - a_2 r^{k-2} - \cdots - a_k = 0,$$

joten r on yhtälön (16) juuri. □

Karakteristisen juuren antamaa ratkaisua $(u_n)_{n=0}^{\infty} = (r^n)_{n=0}^{\infty}$ kutsutaan rekursion *perusratkaisuksi*.

Määritelmä 3.2. Lukujonojen $(u_n)_{n=0}^{\infty}$ ja $(v_n)_{n=0}^{\infty}$ *summa*

$$(u_n)_{n=0}^{\infty} + (v_n)_{n=0}^{\infty} = (u_n + v_n)_{n=0}^{\infty}$$

ja *erotus*

$$(u_n)_{n=0}^{\infty} - (v_n)_{n=0}^{\infty} = (u_n - v_n)_{n=0}^{\infty}.$$

Vakiolle $c \in \mathbb{C}$ ja jonolle $(u_n)_{n=0}^{\infty}$ määritellään *tulo*

$$c(u_n)_{n=0}^{\infty} = (cu_n)_{n=0}^{\infty}.$$

Lemma 3.2. *Jos jonot (v_n) ja (y_n) ovat rekursion (15) kaksi ratkaisua, niin myös jonot $(v_n) + (y_n)$ ja (cv_n) ovat ratkaisuja kaikilla $c \in \mathbb{C}$.*

Todistus. DEMO. □

Edellisen lemman mukaan siis, jos $r_1, r_2, \ldots, r_m$ rekursion karakteristisia juuria, niin

$$u_n = c_1 r_1^n + c_2 r_2^n + \cdots + c_m r_m^n$$

on myös ratkaisu. Huomaa, että tässä karakteristiset juuret voivat olla samoja. Tarkastellaan nyt rekursiota, jolla on moninkertaisia karakteristisia juuria. Olkoon $x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k = 0$ jonon u_n karakteristinen yhtälö. Tiedetään, että polynomi

$$x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k = (x - r_1)(x - r_2) \cdots (x - r_k)$$

missä luvut $r_k \in \mathbb{C}$ ovat yhtälön karakteristiset juuret. Jos karakteristisella yhtälöllä on moninkertaisia juuria, niin

$$x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k = (x - r_1)^{j_1}(x - r_2)^{j_2} \cdots (x - r_m)^{j_m},$$

missä $r_i \neq r_j$ aina kun $i \neq j$, $j_i \geq 1$ kaikilla i ja $j_1 + j_2 + \cdots + j_m = k$. Sanotaan, että r_i on *j_i-kertainen* juuri.

Lemma 3.3. *Jos r on rekursion karakteristisen yhtälön j-kertainen juuri ($j \geq 2$), niin jonot r^n, nr^n, $n^2 r^n, \ldots, n^{j-1} r^n$ ovat rekursion perusratkaisuja.*

Todistus. Tarkastellaan rekursiota

$$u_n - a_1 u_{n-1} - a_2 u_{n-2} - \cdots - a_k u_{n-k} = 0.$$

Jonon karakteristinen yhtälö on siis

$$x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k = 0.$$

Kun kerrotaan se puolittain x^{n-k}:lla, derivoidaan puolittain ja vielä kerrotaan x:llä , saadaan

$$nx^n - a_1(n-1)x^{n-1} - a_2(n-2)x^{n-2} - \cdots - a_k(n-k)x^{n-k} = 0. \quad (17)$$

r on myös tämän yhtälön juuri (itse asiassa $(j-1)$-kertainen juuri), ja huomataan, että jono $v_n = nr^n$ toteuttaa alkuperäisen rekursion. Derivoimalla uudelleen ja kertomalla x:llä saadaan, että jono $v_n = n^2 r^n$ toteuttaa alkuperäisen rekursion, jne. jonot $n^3 r^n, \ldots, n^{j-1} r^n$.

Osoitetaan vielä, että r on yhtälön (17) $(j-1)$-kertainen juuri. Tarkastellaan karakteristinen yhtälö vasenta puolta ja kirjoitetaan se muotoon

$$(x - r)^j p(x),$$

missä $p(x)$ on astetta $(k - j)$ oleva polynomi. Kerrotaan tämä polynomi x^{n-k}:lla, derivoidaan käyttäen tulon derivoimissääntöä ja kerrotaan x:llä, saadaan muoto

$$\begin{aligned} &x(x^{n-k-1}(x-r)^j p(x) + jx^{n-k}(x-r)^{j-1}p(x) + x^{n-k}(x-r)^j p'(x)) \\ &= x^{n-k}(x-r)^{j-1}((x-r)p(x) + jxp(x) + x(x-r)p'(x)). \end{aligned}$$

Selvästi r on tämän polynomin $(j-1)$-kertainen juuri. □

Jono yleiselle ratkaisulle saadaan seuraava lause.

Lause 3.1. *Olkoot $r_1, r_2, \ldots, r_m$ rekursion karakteristisen yhtälön erisuuret juuret, r_i kertalukua j_i, kaikilla $1 \leq i \leq m$, ja $j_1 + j_2 + \cdots + j_m = k$. Tällöin rekursion yleinen ratkaisu on*

$$\begin{aligned} u_n &= c_{11}r_1^n + c_{12}nr_1^n + \cdots + c_{1j_1}n^{j_1-1}r_1^n + \cdots + c_{m1}r_m^n + \cdots + c_{mj_m}n^{j_m-1}r_m^n \\ &= \sum_{i=1}^{m}\sum_{\ell=1}^{j_i} c_{i\ell}n^{\ell-1}r_i^n. \end{aligned}$$

Todistus. Todistetaan tässä tapaus, jossa karakteristiset juuret ovat erisuuret. Lauseen todistus yleisessä muodossa esitetään seuraavassa luvussa generoivien funktioiden avulla.

Oletetaan siis, että $m = k$ ja $j_i = 1$ kaikilla $1 \leq i \leq k$, ja osoitetaan, että

$$u_n = c_1r_1^n + c_2r_2^n + \cdots + c_kr_k^n. \tag{18}$$

on rekursion (15) yleinen ratkaisu. Lemmojen 3.1 ja 3.2 mukaan tämä on rekursion ratkaisu ja koska kertoimet c_i voidaan valita kaikille alkuehdoille $u_0 = b_0, \ldots, u_{k-1} = b_{k-1}$, niin kyseessä on yleinen ratkaisu. Kertoimet c_i voidaan valita sopivasti, koska yhtälöryhmällä

$$\begin{cases} c_1 & +c_2 & +\cdots+c_k & = b_0 \\ c_1r_1 & +c_2r_2 & +\cdots+c_kr_k & = b_1 \\ c_1r_1^2 & +c_2r_2^2 & +\cdots+c_kr_k^2 & = b_2 \\ \vdots & \vdots & \vdots & \vdots \\ c_1r_1^{k-1} & +c_2r_2^{k-1} & +\cdots+c_kr_k^{k-1} & = b_{k-1} \end{cases}$$

on aina yksi käsitteinen ratkaisu, sillä kertoimien muodostama determinantti on ns. Vandermonden determinantti, joka on erisuuri kuin 0. □

Edellinen lause antaa myös menetelmän rekursion yksittäisen ratkaisun etsimiseen, kun alkuehdot tunnetaan. Silloin kertoimet c_i löydetään ratkaisemalla yhtälöryhmä, joka muodostetaan alkuehdoista.

Esimerkki 3.2. *Fibonaccin luvut* F_i voidaan määritellään palautuskaavalla

$$\begin{cases} F_0 = 1, F_1 = 1, \\ F_{n+2} = F_{n+1} + F_n \end{cases} \qquad (n \geq 0).$$

Lukujono alkaa siis 1, 1, 2, 3, 5, 8, 13, 21, ... Ratkaistaan Fibonaccin lukujen palautuskaava.

Karakteristinen yhtälö on $x^2 - x - 1 = 0$, jonka juuret ovat

$$r_{1,2} = \frac{1 \pm \sqrt{5}}{2}.$$

Yleinen ratkaisu on siis

$$F_n = a \cdot \Big(\frac{1+\sqrt{5}}{2}\Big)^n + b \cdot \Big(\frac{1-\sqrt{5}}{2}\Big)^n.$$

Kertoimet a ja b ratkaistaan yhtälöryhmästä

$$\begin{cases} a & +b & = 1 \\ a \cdot \dfrac{1+\sqrt{5}}{2} & +b \cdot \dfrac{1-\sqrt{5}}{2} & = 1 \end{cases}$$

ja saadaan, että $a = \dfrac{1+\sqrt{5}}{2\sqrt{5}}$ ja $b = -\dfrac{1-\sqrt{5}}{2\sqrt{5}}$. Nyt

$$F_n = \frac{1}{\sqrt{5}}\Big(\Big(\frac{1+\sqrt{5}}{2}\Big)^{n+1} - \Big(\frac{1-\sqrt{5}}{2}\Big)^{n+1}\Big).$$

Esimerkki 3.3. Ratkaise rekursio $u_0 = 1$, $u_1 = 0$, $u_2 = 1$, ja $u_{n+3} = -2u_{n+2} + u_{n+1} + 2u_n$, kun $n \geq 0$.

Esimerkki 3.4. Ratkaise Esimerkin 3.1 palautuskaava.

Esimerkki 3.5. Etsi yleinen ratkaisu rekursiolle $u_n = 5u_{n-1} - 6u_{n-2} - 4u_{n-3} + 8u_{n-4}$.

Rekursion karakteristinen yhtälö on $x^4 - 5x^3 + 6x^2 + 4x - 8 = 0$, jonka juuret ovat -1 ja 2, nimittäin $x^4 - 5x^3 + 6x^2 + 4x - 8 = (x-2)^3(x+1)$. Yleinen ratkaisu on siis

$$u_n = c_1 2^n + c_2 n 2^n + c_3 n^2 2^n + c_4(-1)^n.$$

Esimerkki 3.6. Ratkaise rekursio $u_n = 2u_{n-1} - u_{n-2}$, $u_0 = 1$ ja $u_1 = 2$.

Esimerkki 3.7. Ratkaise rekursio $u_n = 2u_{n-1} - u_{n-2} + 2u_{n-3}$, $u_0 = 3$, $u_1 = 2$ ja $u_2 = 2$.

Olemme nähneet, että homogeenisen lineaarisen vakiokertoimisen palautuskaavan ratkaisu löydetään karakteristen juurten avulla. Käytännössä siis ongelmaksi muodostuu näiden juurien löytäminen.

Kirjoitetaan Lause 3.1 vielä uudellen toisen kertaluvun palutuskaavoille. Olkoon (u_n) jono, jonka alkuehdot ovat $u_0 = c_0$, $u_1 = c_1$ ja palautuskaava

$$u_{n+2} = a_1 u_{n+1} + a_2 u_n. \tag{19}$$

Olkoot α ja β karakteristisen yhtälön

$$x^2 - a_1 x - a_2 = 0. \tag{20}$$

juuret.

Lause 3.2. *Olkoon* (u_n) *kuten edellä. Silloin*

(i) *jos* $\alpha \neq \beta$, *niin*

$$u_n = a\alpha^n + b\beta^n$$

kaikille $n \geq 0$, *missä* $a = \dfrac{c_1 - c_0\beta}{\alpha - \beta}$ *ja* $b = \dfrac{c_1 - c_0\alpha}{\beta - \alpha}$

(ii) *jos* $\alpha = \beta$, *niin*

$$u_n = (cn + d)\alpha^n$$

kaikille $n \geq 0$, *missä* $d = c_0$ *ja* $c = \dfrac{c_1 - c_0\alpha}{\alpha}$.

3.3 Epähomogeenisen lineaarisen palautuskaavan ratkaisu

Tarkastellaan nyt epähomogeenisen lineaarisen vakiokertoimisen palautuskaavan

$$\begin{cases} u_0 = b_0, u_1 = b_1, \ldots, u_{k-1} = b_{k-1}, \\ u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n + f(n) \end{cases} \quad (n \geq 0), \qquad (21)$$

määrittelemää lukujonoa $(u_n)_{n=0}^{\infty}$. Palautuskaavan (21) *homogeeninen osa* on

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n. \qquad (22)$$

Lemma 3.4. *Jos jonot* (x_n) *ja* (y_n) *toteuttavat palautuskaavan* (21), *niin jono* $(x_n - y_n)$ *toteuttaa homogeenisen lineaarisen palautuskaavan* (22).

Todistus. DEMO. □

Edellinen lemma siis tarkoittaa, että kun on löydetty yksi epähomogeenisen rekursion ratkaisu, muut ratkaisut poikkeavat siitä vain homogeenisen osan ratkaisulla. Toisin sanoen, epähomogeeninen lineaarinen palautuskaava voidaan ratkaista seuraavalla tavalla:

(i) Etsi jokin *yksittäisratkaisu*.

(ii) Etsi homogeenisen osan yleinen ratkaisu.

(iii) Yhdistä kaksi edellistä ja ratkaise kertoimet alkuehdoista.

Kohdat (ii) ja (iii) ovat jo tuttuja juttuja, tarkastellaan nyt yksittäisratkaisun etsimistä tapauksissa, joissa $f(n)$ on polynomi tai eksponenttifunktio. Yksittäisratkaisu etsitään (kuten differentiaaliyhtälöissä) ratkaisemalla ns. *yrite*.

$f(n)$ on polynomi

Jos $f(n)$ on astetta m oleva polynomi, yrite on myös m-asteinen polynomi, jonka kertoimet ratkaistaan ns. määräämättömien kertoimien menetelmällä sijoittamalla se palautuskaavaan.

Esimerkki 3.8. Etsi rekursion $a_n = a_{n-1} + a_{n-2} + 2n$ yksittäisratkaisu.

Koska $f(n) = 2n$ on astetta yksi oleva polynomi, yrite on siis $p(n) = bn + c$. Nyt sijoitetaan $p(n)$ rekursioon, saadaan

$$bn + c = (b(n-1) + c) + (b(n-2) + c) + 2n \iff -bn + (3b - c) = 2n$$

mistä saadaan, että $b = -2$ ja $c = -6$, joten yksittäisratkaisu on $p(n) = -2n - 6$.

Esimerkki 3.9. Ratkaise rekursio $a_n = a_{n-1} + 2a_{n-2} - 4$, $a_0 = 6$ ja $a_1 = 7$.

Yrite on $p(n) = d$, koska $f(n)$ on vakio. Sijoittamalla saadaan

$$d = d + 2d - 4 \iff d = 2,$$

joten $p(n) = 2$. Homogeenisen osan $a_n = a_{n-1} + 2a_{n-2}$ yleinen ratkaisu on $a'_n = b(-1)^n + c2^n$. Rekursion ratkaisu on siis $a_n = b(-1)^n + c2^n + 2$. Kertoimet b ja c ratkaistaan nyt alkuehdoista ja saadaan

$$a_n = (-1)^n + 3 \cdot 2^n + 2.$$

$f(n)$ on eksponenttifunktio

Jos $f(n) = b \cdot r^n$, niin yrite on $p(n) = c \cdot r^n$. Jos r on homogeenisen osan karakteristisen yhtälön juuri, niin tämä yrite ei toimi. Voidaan osoittaa, että jos r on m-kertainen karakteristinen juuri, niin jono $v_n = cn^m r^n$ on yksittäisratkaisu jollakin $c \in \mathbb{C}$, ts. yrite on $p(n) = cn^m r^n$.

Esimerkki 3.10. Ratkaise rekursio $u_n = u_{n-1} + 6u_{n-2} + 2^n$, $u_0 = 0$ ja $u_1 = 1$.

Yrite on $p(n) = c \cdot 2^n$ ja homogeenisen osan karakteristinen yhtälö on $x^2 - x - 6 = 0$, joten karakteristiset juuret ovat -2 ja 3. Saadaan, että ratkaisu on muotoa

$$u_n = a \cdot (-2)^n + b \cdot 3^n + c \cdot 2^n.$$

Kertoimet voidaan ratkaista alkuehdoista, kun vielä huomataan, että $u_2 = 5$. Saadaan, että

$$u_n = 3^n - 2^n.$$

Huomaa, että tässä yrite ja itse rekursio ratkaistiin samalla kertaa. Jos yrite on väärä, vastauskin on väärä, siksi yrite kannattaa ratkaista ensin.

Esimerkki 3.11. Ratkaise rekursio $u_n = 4u_{n-1} - 4u_{n-2} + 2^n$, $u_0 = 1$, $u_1 = -1$.

Esimerkki 3.12. Ratkaise rekursio $u_n = 3u_{n-1} - 4n + 3 \cdot 2^n$, $u_0 = 4$.

Esimerkki 3.13. Tasossa on n suoraa, jotka kaikki leikkaavat toisensa, mutta mitkään kolme eivät leikkaa samassa pisteessä. Kuinka moneen osaan taso on jaettu?

3.4 Matriisit ja rekursiot

Tässä pykälässä esitetään homogeenisen lineaarisen vakiokertoimisen rekursion ja matriisien välinen yhteys.

Tarkastellaan $n \times n$-(neliö)matriiseja, joiden alkiot ovat kompleksilukuja ja merkitään näiden matriisien joukkoa $\mathbb{C}^{n\times n}$. Palautetaan aluksi mieleen muutamia matriisien peruskäsitteitä.

Matriisi

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}_{n\times n}$$

on ns. *identiteetti matriisi.*

Tarkastellaan n-alkioisen joukon permutaatioita. Merkitään permutaatiota

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$$

yksinkertaisesti $(j_1, j_2, \dots, j_n)$. Permutaation $\alpha = (j_1, j_2, \dots, j_n)$ *merkki*

$$\operatorname{sign}(j_1, j_2, \dots, j_n) = (-1)^{t(\alpha)},$$

missä $t(\alpha)$ on permutaation α *inversioiden* lukumäärä, ts. tapausten $j_l > j_k$ ja $l < k$ lukumäärä permutaatiossa α.

Neliömatriisin $A = (a_{ij}) \in \mathbb{C}^{n\times n}$ determinantti

$$\begin{aligned} \det(A) &= \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \\ &= \sum_{(j_1,j_2,\dots,j_n)\in\mathcal{S}_n} \operatorname{sign}(j_1, j_2, \dots, j_n) a_{1j_1} a_{2j_2} \cdots a_{nj_n}, \end{aligned} \tag{23}$$

Olkoon $A \in \mathbb{C}^{n\times n}$. Matriisin A *ominaisarvo* $\lambda \in \mathbb{C}$ ja *ominaisvektori* $\mathbf{x} \in \mathbb{C}^n$, $\mathbf{x} \neq (0, \dots, 0)$, toteuttavat yhtälön

$$A\mathbf{x}^T = \lambda \mathbf{x}^T, \tag{24}$$

missä $\mathbf{x}^T$ on vektorin $\mathbf{x}$ transpoosi (ts. $\mathbf{x}$ pystyvektorina).

Yhtälö (24) voidaan kirjoittaa muotoon

$$(A - \lambda I)\mathbf{x}^T = \mathbf{0}^T.$$

Tämä taas voidaan tutkita yhtälö(ryhmä)nä, jolla on epätriviaali ratkaisu $\mathbf{x}^T$ silloin ja vain silloin, kun

$$\det(A - \lambda I) = 0.$$

Tätä yhtälöä kutsutaan matriisin A *karakteristiseksi yhtälöksi*. Yhtälön vasenta puolta kutsutaan *karakteristiseksi polynomiksi*, merkitään matriisin A karakteristista polynomia $c_A(\lambda)$:lla (tässä λ on muuttuja),

$$c_A(\lambda) = (-1)^n(\lambda^n + c_1\lambda^{n-1} + \cdots + c_n).$$

Karakteristinen polynomi on astetta n, jos $A \in \mathbb{C}^{n\times n}$, ja kertoimet $c_i \in \mathbb{C}$. Jos $z \in \mathbb{C}$ on A:n ominaisarvo, niin siis $c_A(z) = 0$.

Olkoon $p(x)$ polynomi, jonka kertoimet ovat kompleksilukuja, sanotaan $p(x) = c_1x^k + c_2x^{k-1} + \cdots + c_{k+1}$. Nyt matriisille $A \in \mathbb{C}^{n\times n}$ määritellään

$$p(A) = c_1A^k + c_2A^{k-1} + \cdots + c_{k+1}I.$$

Seuraava lause on ns. *Cayleyn–Hamiltonin* lause.

Lause 3.3. *Jos A on neliömatriisi ja c_A on sen karakteristinen polynomi, niin*

$$c_A(A) = 0,$$

missä $0 = (0)_{n\times n}$ on ns. nollamatriisi.

Olkoon $A \in \mathbb{C}^{k\times k}$ ja $\mathbf{u}, \mathbf{v} \in \mathbb{C}^k$. Määritellään jono $(a_n)_{n=0}^{\infty}$ yhtälöllä

$$a_n = \mathbf{u}A^n\mathbf{v}^T, \quad (n \geq 0). \tag{25}$$

Osoitetaan seuraavaksi, että tämä lukujono toteuttaa homogeenisen lineaarisen vakiokertoimisen rekursion.

Lause 3.4. *Jono* (25) *toteuttaa homogeenisen lineaarisen vakiokertoimisen rekursion.*

Todistus. Olkoon

$$c_A(\lambda) = (-1)^k(\lambda^k + c_1\lambda^{k-1} + \cdots + c_k),$$

A:n karakteristinen polynomi. Cayleyn–Hamiltonin lauseen mukaan

$$(c_A(A) =)A^k + c_1A^{k-1} + \cdots + c_kI = 0.$$

Kerrotaan tämä yhtälö vasemmalta $\mathbf{u}A^n$:llä ja oikealta pystyvektorilla $\mathbf{v}^T$, saadaan

$$a_{n+k} + c_1a_{n+k-1} + \cdots + c_ka_n = 0, \tag{26}$$

joten jono $(a_n)_{n=0}^{\infty}$ toteuttaa siis tämän rekursion. Rekursion alkuehdot saadaan laskemalla k ensimmäistä arvoa määritelmästä (25). □

Osoitetaan seuraavaksi, että jokaisella homogeenisella lineaarisella vakiokertoimisella rekursiolla on matriisiesitys (25).

Lause 3.5. *Olkoon $(a_n)_{n=0}^{\infty}$ jono, joka toteuttaa homogeenisen lineaarisen vakiokertoimisen rekursion*

$$\begin{cases} a_0 = b_0, a_1 = b_1, \ldots, a_{k-1} = b_{k-1}, \\ a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_k a_n \end{cases} \qquad (n \geq 0),$$

missä $c_k \neq 0$. Tällöin on olemassa sellainen $k \times k$ matriisi A ja sellaiset vektorit $\mathbf{u}, \mathbf{v} \in \mathbb{C}^k$, että

$$a_n = \mathbf{u} A^n \mathbf{v}^T$$

kaikilla $n \geq 0$.

Todistus. Määritellään

$$\mathbf{u} = (1, 0, \ldots, 0), \quad A = \begin{pmatrix} 0 & 1 & 0 & . & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & \ldots & 1 \\ c_k & \ldots & \ldots & \ldots & c_1 \end{pmatrix}, \quad \mathbf{v} = (b_0, b_1, \ldots, b_{k-1}).$$

Matriiseja A kutsutaan joskus *seuralaismatriiseiksi.*

Osoitetaan, että $\mathbf{u} A^n \mathbf{v}^T = a_n$ kaikilla $n \geq 0$, tarkastelemalla matriisin A karakteristista polynomia kuten edellisen lauseen todistuksessa.

$$\begin{aligned} \det(A - \lambda I) &= \begin{vmatrix} -\lambda & 1 & 0 & \cdots & 0 \\ 0 & -\lambda & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 0 & -\lambda & 1 \\ c_k & \ldots & \ldots & \ldots & c_1 - \lambda \end{vmatrix} \\ &= \sum_{i=1}^{k} (-1)^{k-i} c_{k-i+1} (-\lambda)^{i-1} + (-\lambda)^k, \end{aligned}$$

missä viimeinen muoto seuraa determinantin määritelmästä ja siitä, että sellaiset matriisin alkioiden tulot kyseisessä määritelmässä, jotka ovat erisuuria kuin 0, vastaavat permutaatiot $(1, \ldots, i-1, i+1, \ldots, k, i)$. Alkio $A_{ki} = c_{k-i+1}$ ja näissä permutaatioissa on $(k-i)$ inversiota, joten niiden merkki on $(-1)^{k-i}$. Termi $(-\lambda)^k$ vastaa permutaatioita $(1, 2, \ldots, k)$ ja alkion $(c_1 - \lambda)$ termiä $-\lambda$. Nyt

$$\begin{aligned} \det(A - \lambda I) &= \sum_{i=1}^{k} (-1)^{k-i+i-1} c_{k-i+1} \lambda^{i-1} + (-1)^k \lambda^k \\ &= (-1)^k \Big(\sum_{i=1}^{k} (-1) c_{k-i+1} \lambda^{i-1} + \lambda^k \Big) \\ &= (-1)^k (\lambda^k - c_1 \lambda^{k-1} - \cdots - c_k). \end{aligned}$$

Nyt Lauseen 3.4 tapaan saadaan, että jono $\mathbf{u}A^n\mathbf{v}^T$ toteuttaa oletetun rekursion. Kun vielä huomataan, että $\mathbf{u}A^n\mathbf{v}^T = b_n$ kun $0 \leq n \leq k-1$, niin on osoitettu, että jono $a_n = \mathbf{u}A^n\mathbf{v}^T$ kaikilla $n \geq 0$. □

3.5 Sovellus: Solubiologiasta

Tarkastelussa esiintyy kolmen tyyppisiä soluja: a-soluja, b-soluja ja c-soluja. Vuorokaudessa a-solu jakaantuu kahdeksi a soluksi, b-solu solujonoksi $aaaaab$ ja c-solu solujonoksi $bbbc$. Aloitetaan tilanteesta, jossa kaikkia soluja on yksi kappale, siis solujonosta abc. Kuinka monta solua on yhteensä n päivän kuluttua?

Tehtävän voi ratkaista monella tavalla, esitetään nyt kuitenkin matriiseihin perustuva tapa. Merkitään x_n:llä a-solujen määrää n vuorokauden kuluttua, samoin y_n:llä b-solujen määrää ja z_n:llä c-solujen määrää. Nämä toteuttavat ehdon

$$(x_{n+1}, y_{n+1}, z_{n+1}) = \begin{pmatrix} 2 & 5 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} (x_n, y_n, z_n)^T.$$

Solujen kokonaismäärä $u_n = x_n + y_n + z_n$ saadaan siis jonosta

$$u_n = (1,1,1) \begin{pmatrix} 2 & 5 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}^n (1,1,1)^T.$$

Matriisin $\begin{pmatrix} 2 & 5 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ karakteristinen polynomi on $(-1)(\lambda^3 - 4\lambda^2 + 5\lambda - 2)$, joten u_n toteuttaa rekursion

$$\begin{cases} u_0 = 3, u_1 = 12, u_2 = 42, \\ u_{n+3} - 4u_{n+2} + 5u_{n+1} - 2u_n = 0 \end{cases} \qquad (n \geq 0).$$

Ratkaisemalla tämä saadaan

$$u_n = 21 \cdot 2^n - 12n - 18.$$

3.6 Sovellus: Skolemin ongelma

Määritellään ns. *Skolemin ongelma*:

Ongelma 3.1. Annettuna matriisi $A \in \mathbb{Z}^{n \times n}$. Onko olemassa sellaista lukua $k \geq 1$, että $(A^k)_{1n} = 0$?

Skolemin ongelmassa kysytään siis, onko matriisin A jossakin potenssissa oikeassa yläkulmassa nolla.

Laskettavuuden teoriassa ongelmaa sanotaan *ratkeavaksi*, jos on olemassa *algoritmi*, joka ratkaisee kyseisen ongelman. Algoritmin voidaan ajatella olevan (hyvin määritelty, äärellinen) laskentaprosessi, joka **päättyy** kaikille syötteille ja vastaa oikein. Itseasiassa algoritmin teoreettinen malli on ns. *Turingin kone*, mutta tällä kurssilla riittää intuitiivinen algoritmin käsite.

Esimerkki 3.14. Ongelma, jossa kysytään, onko annettu luonnollinen luku alkuluku, on ratkeava. Ongelman ratkaisee esim. seuraava algoritmi:

Syöte $n \in \mathbb{N}$,

(1) Muodosta joukko $S := \{2, 3, 4, \ldots \lfloor\sqrt{n}\rfloor\}$.

(2) Valitse pienin luku $m \in S$.

(3) Jos $m|n$, tulosta "n ei ole alkuluku", muutoin $S := S \setminus \{m, 2m, \ldots, \}$.

(4) Jos $S = \emptyset$, tulosta "n on alkuluku", muutoin palaa kohtaan (2).

Jos ongelma ei ole ratkeava, niin se on *ratkeamaton*. Ongelman ratkeamattomaksi todistaminen ei ole helppoa. Yleensä jokin jo ratkeamattomaksi tunnettu ongelma redusoidaan käsiteltävään ongelmaan niin, että ratkeamattomuus seuraa.

Esimerkki 3.15. Seuraava ongelma on ratkeamaton: annettuna m kappaletta 3×3 kokonaislukumatriiseja, sanotaan $M_1, M_2, \ldots, M_m$. Onko olemassa sellaista jonoa i_j, missä $1 \leq i_j \leq m$ kaikilla j, että

$$M_{i_1} M_{i_2} \cdots M_{i_k} = 0?$$

Myös ongelma, jossa kysytään, onko olemassa jonoa i_j, jolle

$$(M_{i_1} M_{i_2} \cdots M_{i_k})_{13} = 0,$$

on ratkeamaton.

Skolemin ongelman ratkeavuutta tai ratkeamattomuutta ei ole pystytty osoittamaan. Tiedetään kuitenkin, että se on ratkeava, kun $n \leq 5$. Skolemin ongelmalla on yhteyksiä moniin muihin matriisiongelmiin.

Skolemin ongelma voidaan esittää seuraavasti: annettuna matriisi $A \in \mathbb{Z}^{n\times n}$, onko olemassa sellaista lukua $k \geq 1$, että

$$(1, 0, 0)A^k(0, 0, 1)^T = 0.$$

Edellisen pykälän mukaan siis, jos pystytään ratkaisemaan esiintyykö kokonaislukukertoimisen lineaarisen homogeenisen rekursion toteuttavassa jonossa 0, niin Skolemin ongelma voidaan myös ratkaista.

Toisaalta tiedetään, että ongelma, jossa kysytään, esiintyykö nolla äärettömän monta kertaa oikeassa yläkulmassa, on ratkeava kaikille kokonaislukumatriiseille. Tietysti sama ratkeavuus tulos seuraa homogeenisille kokonaislukukertoimisille rekursioille.

4 GENEROIVAT FUNKTIOT

4.1 Jono ja generoiva funktio

Tässä luvussa tarkastellaan (kompleksi)lukujonoja ja niiden jäsenten esittämistä ns. generoivien funktioiden avulla.

Määritelmä 4.1. Kompleksilukujonon $(u_i)_{i=0}^{\infty}$ *generoiva funktio* on

$$U(x) = \sum_{i=0}^{\infty} u_i x^i.$$

Jonon generoiva funktio on siis *formaalinen potenssisarja*. Sarjan *termissä* $u_i x^i$ *kerroin* u_i on tärkeä. Pelkistetysti ajateltuna muuttujan x potensseja käytetään vain jonon jäsenten erotteluun.

Klassisessa sarjateoriassa tarkastellaan yleensä sarjojen suppenemista ja suppenemisympyröiden sisällä olevien sarjojen operaatioita. Tällä kurssilla näihin asioihin ei kiinnitetä huomiota, vaan tarkastellaan sarjoja pelkästään jonojen jäseniä esittävinä generoivina funktioina. Sarjoja käsitellään siis algebrallisessa mielessä eikä analyyttisessä mielessä.

Esimerkki 4.1. Jonon $u = 1, -1, 1, -1, 1, \ldots$ generoiva funktio on

$$1 - x + x^2 - x^3 + x^4 - \cdots$$

Esimerkki 4.2. Jonon $\left(\binom{n}{i}\right)_{i=0}^{\infty}$ generoiva funktio on

$$\sum_{i=0}^{\infty} \binom{n}{i} x^i = \sum_{i=0}^{n} \binom{n}{i} x^i = (1+x)^n.$$

Tässä muoto $(1+x)^n$ on generoivan funktion *suljettu muoto*.

Esimerkki 4.3. Binomikertoimen $\binom{n}{k}$ määritelmä voidaan laajentaa koskemaan muitakin kuin positiivisia kokonaislukuja n. Määritellään yleistetyt binomikertoimet seuraavasti:

$$\forall z \in \mathbb{C},\ \forall k \in \mathbb{N} \setminus \{0\} : \binom{z}{k} = \frac{z(z-1)(z-2)\cdots(z-k+1)}{k!}.$$

Lisäksi sovitaan, että $\binom{z}{0} = 1$ kaikilla $z \in \mathbb{C}$. Nyt erityisesti

$$\binom{-z}{k} = (-1)^k \binom{z+k-1}{k}. \tag{27}$$

Binomikaava voidaan nyt yleistää muotoon

$$(1+x)^z = \sum_{i=0}^{\infty} \binom{z}{i} x^i \quad (\text{kun } |x| < 1). \tag{28}$$

Tarkastellaan nyt jonoa $\left(\binom{n+i-1}{i}\right)_{i=0}^{\infty}$, kun $n \in \mathbb{N}$. Sen generoiva funktio on yhtälöiden (27) ja (28) mukaan

$$U(x) = \sum_{i=0}^{\infty} \binom{n+i-1}{i} x^i = (1-x)^{-n} = \frac{1}{(1-x)^n}.$$

Esimerkki 4.4. Edellisellä esimerkillä on kaksi tärkeää seurausta, nimittäin

$$\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i = 1 + x + x^2 + x^3 + x^4 + \cdots \quad \text{ja}$$

$$\frac{1}{1+x} = \sum_{i=0}^{\infty} (-1)^i x^i = 1 - x + x^2 - x^3 + x^4 - + \cdots,$$

ks. Esimerkki 4.1.

Esimerkki 4.5. Osoita, että $\dfrac{1-x^{n+1}}{1-x} = 1 + x + x^2 + \cdots + x^n$.

Esimerkki 4.6. Tarkastellaan sarjaa $\dfrac{1}{(1-cx)^n}$, missä $c \in \mathbb{C}$.

Huomautus 6. Yhtälössä (28) esiintyi ehto $|x| < 1$. Itse asiassa, jos sarjoja tarkastellaan klassisen sarjateorian puitteissa, niin sama ehto pitäisi olla voimassa myös aina kun kyseessä on binomikaava johdannainen sarja. Esimerkissä 4.5 riittää ehto $x \neq 1$.

4.2 Tulo- ja summaperiaate

Generoivia funktioita voidaan käyttää esimerkiksi jonon jäsenten etsimiseen tai palautuskaavojen ratkaisuun. Yleensä tämä johtaa siihen, että jokin generoivan funktion toteuttama yhtälö pitää ratkaista. Määritellään seuraavaksi formaalisten potenssisarjojen laskutoimitukset ja niihin liittyvät perusperiaatteet.

Määritelmä 4.2. Olkoot $U(x) = \sum_{i=0}^{\infty} u_i x^i$ ja $V(x) = \sum_{i=0}^{\infty} v_i x^i$ kaksi formaalista potenssisarjaa. Määritellään sarjojen yhteen- ja kertolasku seuraavasti,

$$U(x) + V(x) = \sum_{i=0}^{\infty} (u_i + v_i) x^i \quad \text{ja}$$

$$U(x) \cdot V(x) = \left(\sum_{i=0}^{\infty} u_i x^i\right)\left(\sum_{i=0}^{\infty} v_i x^i\right) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} u_i v_{k-i}\right) x^k.$$

Esimerkki 4.7. Tarkastellaan yhtälöä $(1+x)^n(1+x)^m = (1+x)^{n+m}$ puolittain,

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

Toisaalta

$$(1+x)^n(1+x)^m = (1+x)^{n+m} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k.$$

Koska termin x^k kertoimet ovat samat molemmissa yhtälöissä, löysimme todistuksen Lauselle 1.7.

Esimerkki 4.8. Laske $\left(\sum_{n=0}^{\infty} x^n \right) \left(\sum_{n=0}^{\infty} 2^n x^n \right)$

Seuraavaksi esitettävät generoivien funktioiden periaatteet on hankala esittää sanallisesti, mutta yritetään. Ensin ns. *tuloperiaate*:

Tarkastellaan jonoa, jossa jäsen muodostuu m *laskenta-askeleella*, ja askeleen i generoiva funktio on $A_i(x)$. Jos askeleet ovat itsenäisiä, ts. askeleiden järjestyksellä ei ole väliä, niin jonon generoiva funktio on $A_1(x)A_2(x)\cdots A_m(x)$.

Esimerkki 4.9. Tarkastellaan n alkiosen joukon k-alkioisten osajoukkojen määrää. Generoivassa funktiossa siis termin x^k kerroin on n alkioisen joukon k-alkioisten osajoukkojen lukumäärä.

Jokainen alkio joko kuuluu tai ei kuulu osajoukkoon, ja alkioiden lukumäärä (siis potenssi) kasvaa yhdellä, jos alkio valitaan. Yksittäisen alkion valinnan generoiva funktio on siis $(1+x)$, missä $x^0 = 1$ vastaa tapausta, että alkiota ei valita (potenssi 0 ei kasvata alkioiden lukumäärää) ja $x^1 = x$, tapausta, että alkio valittiin (jolloin alkioiden lukumäärä kasvaa yhdellä). Nyt askeleita on n, valitaan tai ei valita alkio alkiolta. Siis k-alkioisten osajoukkojen lukumäärän generoiva funktio on

$$\underbrace{(1+x)(1+x)\cdots(1+x)}_{n\text{kpl}} = (1+x)^n,$$

mikä tosin oli jo tiedossa esimerkin 4.2 nojalla.

Esimerkki 4.10. Kuinka monella tavalla 25 samanlaista vaunua voidaan jakaa 7 eri junaan siten, että jokaiseen junaan tulee vähintään 2 ja korkeintaan 6 vaunua?

Muodostetaan generoiva funktio jonolle, missä x^i:n kerroin kertoo kuinka monella tavalla i vaunua voidaan jakaa seitsemään junaan. Merkitään j_k:llä

junaan k valittujen vaunujen lukumäärää. Nyt siis $2 \leq j_k \leq 6$ kaikille $1 \leq k \leq 7$. Jos vaunuja on i kpl, ne voidaan siis jakaa juniin yhtämonella tavalla, kuin saadaan esitettyä i muodossa

$$j_1 + \cdots + j_7 = i.$$

Jokaisessa junassa tulee 2-6 vaunua, joten jokaisen junaan valittujen vaunujen lukumäärän generoiva funktio on

$$x^2 + x^3 + x^4 + x^5 + x^6,$$

sillä vaunut voidaan valita vain yhdellä tavalla lukumäärästä riippumatta, koska vaunut ovat samanlaisia. Tuloperiaatteen mukaan polynomin

$$(x^2 + x^3 + x^4 + x^5 + x^6)^7$$

termin $x^i = x^{j_1}x^{j_2}\cdots x^{j_7}$ kerroin on yhtäsuuri kuin i vaunun jako annetulla tavalla. Näin ollen 25 vaunua voidaan jakaa x^{25} kertoimen ilmoittamalla tavalla. Nyt

$$\begin{aligned}\left(\sum_{i=2}^{6} x^i\right)^7 &= x^{14}\cdot(1+x+x^2+x^3+x^4)^7 = x^{14}\left(\frac{1-x^5}{1-x}\right)^7 \\ &= x^{14}(1-x^5)^7(1-x)^{-7} = x^{14}\sum_{i=0}^{7}\binom{7}{i}(-x^5)^i\sum_{j=0}^{\infty}\binom{7+j-1}{j}x^j \\ &= x^{14}\sum_{i=0}^{7}\binom{7}{i}(-1)^i(x^5)^i\sum_{j=0}^{\infty}\binom{6+j}{j}x^j\end{aligned}$$

Tarkastellaan termin x^{25} kerrointa. Nyt siis i voi olla 0, 1 tai 2, jolloin j on 11, 6 tai 1, vastaavasti. Näin ollen kerroin on

$$(-1)^0\binom{7}{0}\binom{6+11}{11} + (-1)^1\binom{7}{1}\binom{6+6}{6} + (-1)^2\binom{7}{2}\binom{6+1}{1} = 6055.$$

Esimerkki 4.11. Laske yhtälön $x_1 + x_2 + x_3 + x_4 = 15$ kokonaislukuratkaisujen lukumäärä, kun $1 \leq x_i \leq 5$ kaikilla $1 \leq i \leq 4$.

Lopuksi esitetään ns. *summaperiaate*, jota on itseasiassa käytetty jo monta kertaa, kun on määrätty yksittäisen askeleen generoivaa funktiota.

Tarkastellaan jonoa, jossa jäsen muodostuu m eri tapauksen summana. Jos tapauksen i generoiva funktio on $A_i(x)$, niin jonon generoiva funktio on $A_1(x) + A_2(x) + \cdots + A_m(x)$.

4.3 Teoriaa

Tarkastellaan joukkoa

$$\mathbb{C}[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i \mid \forall i\colon a_i \in \mathbb{C} \right\}.$$

Tätä joukkoa kutsutaan *formaalisten potenssisarjojen joukoksi*. Voidaan osoittaa, että joukko $\mathbb{C}[[x]]$ muodostaa kommutatiivisen renkaan, jossa operaatioina ovat Määritelmässä 4.2 määritellyt yhteen- ja kertolasku. Tämän renkaan *ykkösalkio* on sarja $1 + 0x + 0x^2 + \cdots = 1$.

Seuraava lause kertoo potenssisarjan ja sen käänteissarjan esiintymisestä.

Lause 4.1. $\left(\sum_{i=0}^{\infty} a_i x^i \right)^{-1} \in \mathbb{C}[[x]]$ *jos ja vain jos* $a_0 \neq 0$.

Todistus. Olkoon $A(x) = \sum_{i=0}^{\infty} a_i x^i$ ja $U(x) = \sum_{i=0}^{\infty} u_i x^i$. Nyt $U(x) = A(x)^{-1}$, ts.

$$U(x)A(x) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i u_{k-i} \right) x^k = 1$$

silloin ja vain silloin kun

$$\begin{cases} a_0 u_0 = 1 \\ a_0 u_1 + a_1 u_0 = 0 \\ a_0 u_2 + a_1 u_1 + a_2 u_0 = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \end{cases}$$

Tällä yhtälöryhmällä taas on ratkaisu silloin ja vain silloin kun $a_0 \neq 0$. □

Yleensä sarjan $A(x)$ käänteisalkiota merkitään $A(x)^{-1} = \dfrac{1}{A(x)}$.

Esimerkki 4.12. Sarjan $(1 - x)$ käänteissarja on Esimerkin 4.4 mukaan

$$\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i = 1 + x + x^2 + x^3 + x^4 + \cdots$$

Tarkastellaan nyt jonoja ja niiden generoivia funktioita, erityisesti generoivan funktion suljetun muodon muuttamista sarjamuotoon. Sarjamuoto tarvitaan esimerkiksi jono jäsenten selvittämiseen. Tämä onnistuu analyysistä tutulla *Taylorin kaavalla*: jos $f(x)$ on jonon $(a_n)_{n=0}^{\infty}$ generoiva funktio, niin

$$a_n = \frac{f^{(n)}(0)}{n!}.$$

Myös niin sanotut Taylorin sarjat ovat siis generoivia funktioita.

Esimerkki 4.13. Jonon $\left(\frac{1}{n!}\right)_{n=0}^{\infty}$ generoiva funktio on

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

Käytännössä Taylorin kaavan mukaisesta derivoinnista voi tulla liian työlästä. Tarkastellaan nyt polynomien käänteisalkioiden etsimistä tai tarkemmin sanottuna rationaalipolynomin sarjamuodon etsimistä. Tähän tarkoitukseen analyysin kursseilla opittu osamurtoihin jako on erinomainen keino. Osamurtoihin jaolla voidaan rationaalipolynomin $\frac{p(x)}{g(x)}$ sarjamuoto selvittää.

Lause 4.2. *Olkoon $p(x)$ ja $g(x)$ kaksi polynomia, $\deg g(x) > \deg p(x)$, ja oletetaan, että $g(x)^{-1} \in C[[x]]$. Jos $\alpha_1, \ldots, \alpha_k$ ovat polynomin $g(x)$ erisuuret nollakohdat ja α_i on kertalukua m_i, niin on olemassa sellaiset luvut $c_{ij} \in \mathbb{C}$, että*

$$\begin{aligned}\frac{p(x)}{g(x)} =& \frac{c_{11}}{(\alpha_1 - x)} + \frac{c_{12}}{(\alpha_1 - x)^2} + \cdots + \frac{c_{1m_1}}{(\alpha_1 - x)^{m_1}} \\ &+ \frac{c_{21}}{(\alpha_2 - x)} + \frac{c_{22}}{(\alpha_2 - x)^2} + \cdots + \frac{c_{2m_2}}{(\alpha_2 - x)^{m_2}} + \cdots \\ &+ \frac{c_{k1}}{(\alpha_k - x)} + \frac{c_{k2}}{(\alpha_k - x)^2} + \cdots + \frac{c_{km_k}}{(\alpha_k - x)^{m_k}}\end{aligned} \tag{29}$$

Todistus. Sivuutetaan. □

Yhtälön (29) oikeaa puolta kutsutaan rationaalipolynomin $\frac{p(x)}{g(x)}$ osamurtokehitelmäksi. Osamurtokehitelmän luvut c_{ij} etsitään ns. määräämättömien kerrointen menetelmällä. Huomaa myös, että koska $g(x)^{-1}$ on olemassa, niin $g(x)$:n vakiotermi ei ole 0, joten $\alpha_i \neq 0$ kaikilla $1 \leq i \leq k$.

Esimerkki 4.14. Etsi rationaalipolynomin $\frac{1}{1-x^2}$ osamurtokehitelmä.

Koska $1 - x^2 = (1 - x)(1 + x)$, niin edellisen lauseen mukaan

$$\frac{1}{1-x^2} = \frac{a}{1-x} + \frac{b}{1+x}.$$

Kun nyt kerrotaan puolittain $(1 - x^2)$:lla, saadaan yhtälö $1 = a(1 + x) + b(1-x) = a+b+(a-b)x$, josta voidaan ratkaista a ja b. Nimittäin, $a+b = 1$ ja $a - b = 0$, joten $a = b = \frac{1}{2}$. Siis

$$\frac{1}{1-x^2} = \frac{1}{2}\frac{1}{1-x} + \frac{1}{2}\frac{1}{1+x}$$

Rationaalipolynomin määrittelemän funktion potenssisarjamuoto saadaan ratkaistua, kun etsitään rationaalipolynomin osamurtokehitelmä ja käytetään apuna sarjojen $\frac{1}{(1-cx)^n}$ sarjamuotoa. Voidaan nimittäin osoittaa, että yhtälö (29) voidaan kirjoittaa muotoon

$$\begin{aligned}\frac{p(x)}{g(x)} =& \frac{b_{11}}{(1-\alpha_1^{-1}x)} + \frac{b_{12}}{(1-\alpha_1^{-1}x)^2} + \cdots + \frac{b_{1m_1}}{(1-\alpha_1^{-1}x)^{m_1}} \\ &+ \frac{b_{21}}{(1-\alpha_2^{-1}x)} + \frac{b_{22}}{(1-\alpha_2^{-1}x)^2} + \cdots + \frac{b_{2m_2}}{(1-\alpha_2^{-1}x)^{m_2}} + \cdots \\ &+ \frac{b_{k1}}{(1-\alpha_k^{-1}x)} + \frac{b_{k2}}{(1-\alpha_k^{-1}x)^2} + \cdots + \frac{b_{km_k}}{(1-\alpha_k^{-1}x)^{m_k}},\end{aligned}$$

missä $b_{ij} \in \mathbb{C}$.

Esimerkki 4.15. Etsitään rationaalipolynomin $\frac{x}{1-5x+6x^2}$ määrittelemän potenssisarjan sarjamuoto.

$1-5x+6x^2 = 6(x-\frac{1}{2})(x-\frac{1}{3})(=(1-2x)(1-3x))$, joten

$$\frac{x}{1-5x+6x^2} = \frac{a}{1-2x} + \frac{b}{1-3x}.$$

Kun kerrotaan yhtälö puolittain $1-5x+6x^2$:lla, saadaan, että $x = a(1-3x) + b(1-2x)$. Yhtälön kertoimista seuraa kaksi yhtälöä, $a+b=0$ ja $-3a-2b=1$, joista saadaan, että $a=-1$, $b=1$. Olemme siis saaneet, että

$$\begin{aligned}\frac{x}{1-5x+6x^2} &= -\frac{1}{1-2x} + \frac{1}{1-3x} \\ &= -\sum_{i=0}^{\infty}(2x)^i + \sum_{i=0}^{\infty}(3x)^i = \sum_{i=0}^{\infty}(3^i-2^i)x^i\end{aligned}$$

Huomaa, että $\frac{x}{1-5x+6x^2}$ on siis jonon $(3^n-2^n)_{n=0}^{\infty}$ generoiva funktio.

4.4 Laskusäännöt

Käydään seuraavaksi läpi generoivien funktioiden laskusääntöjä.

Olkoon $(a_n)_{n=0}^{\infty}$ lukujono ja $f(x)$ sen generoiva funktio. Jonon $(a_{n+1})_{n=0}^{\infty}$ generoiva funktio on

$$\sum_{n=0}^{\infty} a_{n+1}x^n = \frac{1}{x}\sum_{n=1}^{\infty} a_n x^n = \frac{f(x)-a_0}{x}.$$

Jatkamalla samaa päättelyä, saadaa, että jonon $(a_{n+2})_{n=0}^{\infty}$ generoiva funktio on

$$\frac{\frac{f(x)-a_0}{x} - a_1}{x} = \frac{f(x)-a_0-a_1x}{x^2}.$$

Sääntö 1. Jos $f(x)$ on jonon $(a_n)_{n=0}^{\infty}$ generoiva funktio, niin jonon $(a_{n+k})_{n=0}^{\infty}$ generoiva funktio on

$$\frac{f(x) - a_0 - a_1 x - \cdots - a_{k-1}x^{k-1}}{x^k}.$$

Esimerkki 4.16. Olkoon $f(x)$ Fibonaccin lukujen F_n generoiva funktio. Säännön 1, palautuskaavan $F_{n+2} = F_{n+1} + F_n$ ja alkuehtojen $F_0 = 1$, $F_1 = 1$ avulla saadaan generoivalle funktiolle f yhtälö

$$\frac{f(x) - x - 1}{x^2} = \frac{f(x) - 1}{x} + f(x).$$

Oikea puoli saadaan summaperiaatteella. Kun tästä ratkaistaan $f(x)$, saadaan, että

$$f(x) = \frac{1}{1 - x - x^2}.$$

Olkoon taas $(a_n)_{n=0}^{\infty}$ lukujono ja $f(x)$ sen generoiva funktio. Jonon $(na_n)_{n=0}^{\infty}$ generoiva funktio on

$$\sum_{n=0}^{\infty} na_n x^n = x\sum_{n=1}^{\infty} na_n x^{n-1} = xD\left(\sum_{n=0}^{\infty} a_n x^n\right) = x(Df(x)) = xDf(x).$$

Merkitään (xD):llä operaatiota, jossa ensin derivoidaan ja sitten kerrotaan x:llä. Tämä operaatio voidaan tietysti yleistää muotoon: jonon $(n^k a_n)_{n=0}^{\infty}$ generoiva funktio on

$$\underbrace{(xD)(xD)\cdots(xD)}_{k\text{kpl}} f(x) = (xD)^k f(x).$$

Summaperiaatteen mukaan saadaan seuraava sääntö:

Sääntö 2. Jos $f(x)$ on jonon $(a_n)_{n=0}^{\infty}$ generoiva funktio ja p on jokin polynomi, niin jonon $(p(n)a_n)_{n=0}^{\infty}$ generoiva funktio on

$$p(xD)f(x).$$

Esimerkki 4.17. Mikä on jonon $(3 - n^2)_{n=0}^{\infty}$ generoiva funktio?

Jonon $(1)_{n=0}^{\infty}$ generoiva funktio on $f(x) = \dfrac{1}{1-x}$. Säännön 2 mukaan jonon $(3 - n^2)_{n=0}^{\infty}$ generoiva funktio on

$$\begin{aligned}(3 - (xD)^2)f(x) &= (3 - (xD)^2)\frac{1}{1-x} = \frac{3}{1-x} - (xD)\frac{x}{(1-x)^2} \\ &= \frac{3}{1-x} - x\left(\frac{1}{(1-x)^2} + \frac{2x}{(1-x)^3}\right) = \frac{3 - 7x + 2x^2}{(1-x)^3}.\end{aligned}$$

Esimerkki 4.18. Lasketaan summa $\displaystyle\sum_{n=0}^{\infty} \frac{n^2+4n+5}{n!}$.

Esimerkin 4.13 mukaan jonon $\left(\frac{1}{n!}\right)_{n=0}^{\infty}$ generoiva funktio on e^x. Säännön 2 mukaan siis jonon $\left((n^2+4n+5)/n!\right)_{n=0}^{\infty}$ generoiva funktio on siis

$$((xD)^2+4(xD)+5)e^x = (x^2+4x+5)e^x.$$

Kun tähän sijoitetaan $x=1$, saadaan tulos

$$\sum_{n=0}^{\infty} \frac{n^2+4n+5}{n!} = 10e.$$

Huomaa, että sarjan (tässä tapauksessa e^x) tulee olla suppeneva sijoitetulla x:n arvolla.

Seuraavat säännöt koskevat generoivien funktioiden tuloa.

Sääntö 3. Jos $f(x)$ on jonon $(a_n)_{n=0}^{\infty}$ generoiva funktio ja $g(x)$ on jonon $(b_n)_{n=0}^{\infty}$ generoiva funktio, niin $f(x)g(x)$ on jonon

$$\left(\sum_{r=0}^{n} a_r b_{n-r}\right)_{n=0}^{\infty}$$

generoiva funktio.

Sääntö 4. Jos $f(x)$ on jonon $(a_n)_{n=0}^{\infty}$ generoiva funktio, niin $(f(x))^k$ on jonon

$$\left(\sum_{n_1+n_2+\cdots n_k=n} a_{n_1}a_{n_2}\cdots a_{n_k}\right)_{n=0}^{\infty}$$

generoiva funktio.

Esimerkki 4.19. Olkoon $r(n,k)$ yhtälön

$$x_1+x_2+\cdots+x_n = k$$

ei-negatiivisten kokonaislukuratkaisujen lukumäärä. Koska jonon $(1)_{n=0}^{\infty}$ generoiva funktio on $\dfrac{1}{1-x}$, niin Säännön 4 mukaan jonon $(r(n,k))_{n=0}^{\infty}$ generoiva funktio on

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k.$$

Tämä tulos oli tosin tiedossa jo Lauseen 1.2 mukaan.

Jos $f(x)$ on jonon $(a_n)_{n=0}^{\infty}$ generoiva funktio, niin

$$\begin{aligned}\frac{f(x)}{1-x} &= (a_0 + a_1x + a_2x^2 + \cdots)(1 + x + x^2 + \cdots) \\ &= a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + (a_0 + a_1 + a_2 + a_3)x^3 + \cdots\end{aligned}$$

joten saadaan

Sääntö 5. Jos $f(x)$ on jonon $(a_n)_{n=0}^{\infty}$ generoiva funktio, niin

$$\frac{f(x)}{1-x}$$

on jonon

$$\left(\sum_{i=0}^{n} a_i\right)_{n=0}^{\infty}$$

generoiva funktio.

Esimerkki 4.20. Etsi harmonisten lukujen $H_n = \sum_{i=1}^{n} \frac{1}{i}$ muodostaman jonon $(H_n)_{n=1}^{\infty}$ generoiva funktio.

Säännön 5 mukaan jonon generoiva funktio saadaan kertomalla jonon $\left(\frac{1}{n}\right)_{n=1}^{\infty}$ generoiva funktio funktiolla $\frac{1}{1-x}$. Jonon $\left(\frac{1}{n}\right)_{n=1}^{\infty}$ generoiva funktio on

$$\sum_{n=1}^{\infty} \frac{1}{n}x^n = g(x).$$

Selvästi $D(g(x)) = \frac{1}{1-x}$, joten $g(x) = -\ln(1-x)$ (tämä näkyy myös funktion $\ln(1+x)$ Taylorin sarjasta). Säännön 5 mukaan

$$\sum_{n=1}^{\infty} H_n x^n = \frac{1}{1-x} \ln\left(\frac{1}{1-x}\right).$$

4.5 Rekursiot ja generoivat funktiot

Tarkastellaan seuraavaksi palautuskaavojen ratkaisemista generoivien funktioiden avulla. Olkoon $(u_n)_{n=0}^{\infty}$ lukujono, joka toteuttaa jonkin palautuskaavan. Ratkaisu löydetään seuraavan algoritmin avulla:

(i) Etsitään jonon $(u_n)_{n=0}^{\infty}$ palautuskaavan avulla jonon generoivaa funktiota $U(x)$ koskeva yhtälö. Yleensä yhtälö saadan sijoitamalla generoivan yhtälön sarjamuotoon alkuehdot ja palautuskaava, tai se muodostetaan palautuskaavasta edellä olleiden viiden laskusäännön avulla.

(ii) Ratkaistaan saadusta yhtälöstä $U(x)$.

(iii) Etsitään funktion $U(x)$ sarjamuoto, yleensä osamurtokehitelmän avulla. Kertoimista nähdään rekursion ratkaisu.

Esimerkki 4.21. Ratkaistaan rekursio $u_n = u_{n-1} + n$, $u_0 = 1$.

$$\begin{aligned}
\text{(i): } U(x) &= \sum_{n=0}^{\infty} u_n x^n = 1 + \sum_{n=1}^{\infty} (u_{n-1} + n) x^n = 1 + \sum_{n=0}^{\infty} u_n x^{n+1} + \sum_{n=0}^{\infty} n x^n \\
&= 1 + x \sum_{n=0}^{\infty} u_n x^n + \sum_{n=0}^{\infty} (n+1) x^{n+1} = 1 + xU(x) + x \sum_{n=0}^{\infty} (n+1) x^n \\
&= 1 + xU(x) + (xD) \frac{1}{1-x} = 1 + xU(x) + \frac{x}{(1-x)^2} \\
\text{(ii): } U(x) &= 1 + xU(x) + \frac{x}{(1-x)^2} \iff \\
U(x) &= \frac{1 + x(1-x)^{-2}}{1-x} = \frac{1}{1-x} + \frac{x}{(1-x)^3}.
\end{aligned}$$

$$\begin{aligned}
\text{(iii): } U(x) &= \sum_{n=0}^{\infty} x^n + x \sum_{n=0}^{\infty} \binom{n+2}{n} x^n = \sum_{n=0}^{\infty} \left(1 + \binom{n+1}{n-1}\right) x^n \\
&= \sum_{n=0}^{\infty} \left(1 + \frac{n(n+1)}{2}\right) x^n
\end{aligned}$$

Siis saatiin, että $u_n = 1 + \dfrac{n(n+1)}{2} = \dfrac{1}{2}(n^2 + n + 2)$.

Esimerkki 4.22. Ratkaistaan Fibonaccin lukujen rekursio.

Todistetaan seuraavaksi Lause 3.1. Olkoon $(u_n)_{n=0}^{\infty}$ lukujono, joka toteuttaa palautuskaavan

$$\begin{cases} u_0 = b_0, u_1 = b_1, \ldots, u_{k-1} = b_{k-1}, \\ u_{n+k} + a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n = 0 \end{cases} \qquad (n \geq 0), \qquad (30)$$

missä $a_k \neq 0$. Aloitetaan jonon generoivaa funktiota koskevalla lauseella

Lause 4.3. *Palautuskaavan* (30) *määrittelemän jonon* $(u_n)_{n=0}^{\infty}$ *generoiva funktio*

$$U(x) = \frac{r(x)}{1 + a_1 x + a_2 x^2 + \cdots + a_k x^k},$$

missä $r(x)$ *on polynomi, jonka* $\deg r(x) < k$. *Alkuehdot* (30) *määräävät* $r(x)$*:n kertoimet yksikäsitteisesti.*

Todistus. Olkoon $U(x)$ jonon $(u_n)_{n=0}^{\infty}$ generoiva funktio. Nyt

$$(1 + a_1x + a_2x^2 + \cdots + a_kx^k)U(x) = (1 + a_1x + a_2x^2 + \cdots + a_kx^k)\sum_{n=0}^{\infty} u_nx^n$$
$$= u_0 + (u_1 + a_1u_0)x + \cdots + (u_{k-1} + a_1u_{k-2} + \cdots + a_{k-1}u_0)x^{k-1}$$
$$+ \sum_{n=0}^{\infty}(u_{n+k} + a_1u_{n+k-1} + a_2u_{n+k-2} + \cdots + a_ku_n)x^{n+k}$$
$$= u_0 + (u_1 + a_1u_0)x + \cdots + (u_{k-1} + a_1u_{k-2} + \cdots + a_{k-1}u_0)x^{k-1} = r(x).$$

Huomaa, että $r(x)$:n kertoimet seuraavat alkuehdoista. □

Tarkastellaan jonon (30) karakteristista yhtälöä,

$$x^k + a_1x^{k-1} + \cdots + a_k = 0.$$

Jos $r_1, r_2, \ldots, r_m$ ovat jonon erisuuret karakteristiset juuret, niin saadaan yhtälö

$$x^k + a_1x^{k-1} + \cdots + a_k = (x - r_1)^{j_1}(x - r_2)^{j_2} \cdots (x - r_m)^{j_m}.$$

Kerrotaan tämä yhtälö puolittain x^{-k}:lla, saadaan

$$1 + a_1x^{-1} + \cdots + x^{-k}a_k = (1 - \frac{r_1}{x})^{j_1}(1 - \frac{r_2}{x})^{j_2} \cdots (1 - \frac{r_m}{x})^{j_m}.$$

Tehdään nyt muuttujanvaihdos, kirjoitetaan $x := \frac{1}{x}$, saadaan yhtälö

$$1 + a_1x^1 + \cdots + x^ka_k = (1 - r_1x)^{j_1}(1 - r_2x)^{j_2} \cdots (1 - r_mx)^{j_m}.$$

Edellisen lauseen tulos voidaan nyt siis kirjoittaa muotoon

$$U(x) = \frac{r(x)}{(1 - r_1x)^{j_1}(1 - r_2x)^{j_2} \cdots (1 - r_mx)^{j_m}}. \tag{31}$$

Nyt olemme valmiit todistamaan Lauseen 3.1. Kirjoitetaan se seuraavaan muotoon.

Lause 3.1. *Olkoot $r_1, r_2, \ldots, r_m$ rekursion karakteristisen yhtälön erisuuret juuret, r_i kertalukua j_i, kaikilla $1 \leq i \leq m$. Tällöin rekursion yleinen ratkaisu on*

$$u_n = p_1(n)r_1^n + p_2(n)r_2^n + \cdots + p_m(n)r_m^n,$$

missä kukin $p_i(n)$ on enintään astetta $j_i - 1$ oleva polynomi.

Todistus. Osoitetaan, että kaikkillla alkuehdoilla jono u_n on lauseen väitteen muotoa. Yhtälön (31) ja Lauseen 4.2 mukaan on olemassa sellaiset luvut γ_{it}, että

$$\begin{aligned} U(x) &= \sum_{i=1}^{m} \sum_{t=1}^{j_i} \frac{\gamma_{it}}{(1-r_i x)^t} \\ &= \sum_{n=0}^{\infty} \left(\sum_{i=1}^{m} \sum_{t=1}^{j_i} \gamma_{it} \binom{n+t-1}{n} r_i^n \right) x^n. \end{aligned}$$

Siis

$$u_n = p_1(n) r_1^n + p_2(n) r_2^n + \cdots + p_m(n) r_m^n,$$

missä

$$p_i(n) = \sum_{t=1}^{j_i} \gamma_{it} \binom{n+t-1}{n}$$

on n:n suhteen enintään astetta $j_i - 1$ oleva polynomi. □

4.6 Sovellus: Catalanin luvut

Tarkastellaan esimerkkinä generoivien funktioiden käytöstä ns. *Catalanin lukuja* $f(n)$. Näille luvuille on olemassa useita erilaisia määritelmiä tai oikeastaan on olemassa lukuisia eri laskentaongelmia, joiden ratkaisuna Catalanin luvut ovat.

Käytetään seuraavaa määritelmää luvuille $f(n)$: annettuna n sulkuparia, luku $f(n)$ ilmoittaa kuinka monella tavalla ne voidaan järjestää *laillisesti*. Sulkujen muodostama sana on laillinen, jos siinä vasemmalta oikealle luettaessa ei missään kohtaa ole luettuna enempää oikeaa kuin vasenta sulkua. Esimerkiksi, jos $n = 3$, niin lailliset sulkusanat ovat

$$((())),\ (()()),\ (())(),\ ()()(),\ ()(()). \tag{32}$$

Siis $f(3) = 5$. Lisäksi sovitaan, että $f(0) = 1$.

Seuraavaksi muodostetaan luvuille $f(n)$ palautuskaava. Olkoon w jokin laillinen n sulkuparin muodostama sana, ts. $|w| = 2n$. Liitetään nyt jokaiseen lailliseen n sulkuparin sanaan kokonaisluku k seuraavasti: k *pienin* sellainen kokonaisluku, että sanan w $2k$-pituisessa alkuosassa on k sulkuparia. Ts. tämä alkuosa on laillinen k sulkuparin muodostama sana. Esimerkiksi sanoille (32) luvut k ovat 3, 3, 2, 1 ja 1, vastaavasti. Sana w on *primitiivinen sulkusana*, jos $k = n$. Merkitään $g(n)$:llä laillisten primitiivisten n sulkuparin sanojen lukumäärää.

Lemma 4.1. *Jos $k \geq 1$, niin*

$$g(k) = f(k-1).$$

Todistus. Jokaisesta laillisesta $(k-1)$ sulkuparin sanasta saadaan k sulkuparin primitiivinen sana lisäämällä alkuun vasen ja loppuun oikea sulku.

Toisaalta jokaisesta primitiivisestä k sulkuparin primitiivisestä saadaan laillinen $(k-1)$ sulkuparin sana poistamalla ensimmäinen ja viimeinen sulku. □

Tarkastellaan nyt laillisia n-sulkuparin sanoja lukuja k kohti. Nämä ovat siis sanoja, joissa on alussa jokin k sulkuparin primitiivinen sulkusana ja sen jälkeen mikä tahansa $(n-k)$ sulkuparin sana. Siis näitä sanoja on

$$g(k)f(n-k) = f(k-1)f(n-k).$$

Nyt saamme muodostettua luvuille $f(n)$ palautuskaavan, kun summataan yli kaikkien mahdollisten lukujen k, ts.

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

Olkoon $F(x)$ jonon $(f(n))_{n=0}^{\infty}$ generoiva funktio. Nyt siis

$$\begin{aligned} F(x) &= 1 + \sum_{n=1}^{\infty}\sum_{k=1}^{n} f(k-1)f(n-k)x^n = 1 + \sum_{n=1}^{\infty}\sum_{k=0}^{n-1} f(k)f((n-1)-k)x^n \\ &= 1 + x\sum_{n=1}^{\infty}\sum_{k=0}^{n-1} f(k)f((n-1)-k)x^{n-1} = 1 + xF(x)^2. \end{aligned}$$

Tästä saadaan yhtälö

$$xF(x)^2 - F(x) + 1 = 0, \tag{33}$$

josta voidaan ratkaista $F(x)$,

$$F(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Tässä nimittäjässä olevalla potenssisarjalla $2x$ ei ole käänteisalkiota. Lemman 4.1 nojalla jonon $(g(n))_{n=0}^{\infty}$ generoivalle funktiolla $G(x)$ on tiedossa, että $G(x) = xF(x)$, kun $g(0) = 0$. Kerrotaan yhtälö (33) puolittain x:llä ja sijoitetaan $xF(x) = G(x)$. Saadaan siis, että

$$G(x)^2 - G(x) + x = 0.$$

Ratkaistaan tästä jonon $(g(n))$ generoiva funktio

$$G(x) = \frac{1 \pm \sqrt{1-4x}}{2}.$$

Kirjoitetaan oikeapuoli auki, ja koitetaan päätellä onko merkki + vai −.

$$G(x) = \frac{1}{2}(1 \pm (1-4x)^{\frac{1}{2}}) = \frac{1}{2}\left(1 \pm \sum_{n=0}^{\infty}(-1)^n\binom{\frac{1}{2}}{n}(4x)^n\right)$$
$$= \frac{1}{2}\left(1 \pm 1 \pm \sum_{n=1}^{\infty} -\frac{1}{n2^{2n-1}}\binom{2n-2}{n-1}2^{2n}x^n\right),$$

ja koska $g(0) = 0$, merkki on − ja

$$G(x) = -\frac{1}{2}\sum_{n=1}^{\infty} -\frac{1}{n2^{2n-1}}\binom{2n-2}{n-1}2^{2n}x^n\Bigg),$$
$$= \sum_{n=1}^{\infty}\frac{1}{n}\binom{2n-2}{n-1}x^n.$$

Nyt siis

$$F(x) = \sum_{n=0}^{\infty}\frac{1}{n+1}\binom{2n}{n}x^n,$$

ja

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

Huomautus 7. Catalanin luvut määritellään joissain lähteissä sellaisten laillisten sulkusanojen lukumääräksi, joissa uloimmat sulkeet ovat yli koko sanan, ts. lasketaan vain primitiiviset sulkusanat. Tällöin Catalanin luvut ovat siis edellisen nojalla

$$g(n) = f(n-1) = \frac{1}{n}\binom{2n-2}{n-1}.$$

Esimerkki 4.23. Määritellään xy-tasossa seuraavat siirrot kokonaislukupisteistä toiseen, $Y\colon (x,y) \to (x+1, y+1)$ ja $A\colon (x,y) \to (x+1, y-1)$. Kuinka monta sellaista polkua on origosta $(0,0)$ pisteeseen $(2n,0)$ käyttäen näitä siirtoja, että missään kohtaa polulla ei mennä x-akselin alapuolelle? Entä jos x-akselin sivuaminenkin kielletään?

4.7 Eksponentiaalinen generoiva funktio

Määritelmä 4.3. Jonon $(u_n)_{n=0}^{\infty}$ *eksponentiaalinen generoiva funktio*

$$E(x) = \sum_{n=0}^{\infty} u_n\frac{x^n}{n!}.$$

Esimerkki 4.24. Jonon $(1)_{n=0}^{\infty}$ ekponentiaalinen generoiva funktio on

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots .$$

Funktio $\dfrac{1}{1-x}$ on jonon $(n!)_{n=0}^{\infty}$ eksponentiaalinen generoiva funktio, sillä

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} \frac{n!}{n!} x^n.$$

Yhteen- ja kertolasku tapahtuvat samalla tavalla kuin tavallisille generoiville funktioille. Eksponentiaalisille generoiville funktioille voidaan todistaa laskusääntöjä aivan kuten tavallisille generoiville funktioille. Rajoitutaan tässä kuitenkin seuraavaan esimerkkiin.

4.8 Sovellus: Derangement-ongelma

Tarkastellaan uudelleen ns. derangement-ongelmaa, joka ratkaistiin jo pykälässä 2.6.

Tarkastellaan joukon $\mathcal{S}_n$ permutaatiota α. Olkoon

$$|\{i \mid \alpha(i) = i,\ 1 \leq i \leq n\}| = k,$$

ts. k alkiota kuvautuu itsekseen (näitä kutsutaan α:n *kiintopisteiksi*). Nyt loput $n-k$ alkiota eivät siis kuvaudu itsekseen, joten ne muodostavat siis $(n-k)$ alkion derangement permutaation. k kiintopistettä taas voidaan valita $\binom{n}{k}$ tavalla, joten saadaan, että

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k} \quad (n \geq 0).$$

Ajatellaan tämän yhtälön vasen- ja oikeapuoli jonoina. Vasemman puolen eksponentiaalinen generoiva funktio on $\dfrac{1}{1-x}$. Tarkastellaan seuraavaksi oikean puolen jonon generoivaa funktiota. Olkoon $D(x)$ jonon $(D_n)_{n=0}^{\infty}$ eksponentiaalinen generoiva funktio. Nyt

$$\sum_{n=0}^{\infty} \left(\left(\sum_{k=0}^{n} \binom{n}{k} D_{n-k} \right) /n! \right) x^n = \sum_{n=0}^{\infty} \left(\left(\sum_{k=0}^{n} \frac{n!}{k!(n-k)!} D_{n-k} \right) /n! \right) x^n$$
$$= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{1}{k!} \frac{D_{n-k}}{(n-k)!} \right) x^n = \sum_{n=0}^{\infty} \frac{1}{n!} x^n \sum_{i=0}^{\infty} \frac{D_i}{i!} x^i = e^x D(x).$$

Saadaan siis yhtälö

$$\frac{1}{1-x} = e^x D(x),$$

ja kun ratkaistaan $D(x)$, saadaan

$$D(x) = \frac{e^{-x}}{1-x} = \sum_{n=0}^{\infty}(-1)^n \frac{1}{n!}x^n \sum_{i=0}^{\infty} x^i = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(-1)^k \frac{1}{k!}\right)x^n.$$

Nyt kun tarkastellaan molempien puolien x^n-termin kertoimia, saadaan,

$$\frac{D_n}{n!} = \sum_{k=0}^{n}(-1)^k \frac{1}{k!},$$

josta jo pykälässä 2.6 saatu tulos derangement-permutaatioiden lukumääräksi seuraa, nimittäin

$$D_n = n!\left(\sum_{k=0}^{n}\frac{(-1)^k}{k!}\right).$$