

MS-A0402 Diskreetin matematiikan perusteet

Yhteenveto ja esimerkkejä ym., osa II

G. Gripenberg

Aalto-yliopisto

2. huhtikuuta 2015

💡 Jaollisuus

Luku b on jaollinen luvulla a eli b on a :n monikerta eli a jakaa luvun b jos on olemassa **kokonaisluku** k siten, että $b = ak$, eli $b \in a\mathbb{Z}$. Tämä merkitään usein $a \mid b$.

💡💡 Modulofunktio mod

Jos $n > 0$ niin $\text{mod}(m, n) = j$ jos $0 \leq j < n$ ja $m = j + kn$ missä $k \in \mathbb{Z}$. (mutta $\text{mod}(m, 0) = m$ ja $\text{mod}(m, n) = -\text{mod}(m, -n)$ jos $n < 0$). Jos m ja n ovat positiivisia lukuja niin $\text{mod}(m, n)$ on jakojäännös joka saadaan kun m jaetaan n :llä mutta jos $m < 0$ niin tämä jakojäännös ei ole positiivinen.

💡💡 Kongruenssi modulo

Luku a on kongruentti luvun b kanssa modulo n jos $a - b$ on jaollinen n :llä ja tämä merkitään $a \equiv_n b$ tai $a \equiv b \pmod{n}$:

$$\begin{aligned} a \equiv_n b &\leftrightarrow a \equiv b \pmod{n} \leftrightarrow n \mid (a - b) \\ &\leftrightarrow a = b + kn, \quad k \in \mathbb{Z} \leftrightarrow \text{mod}(a, n) = \text{mod}(b, n) \end{aligned}$$

💡 $\mathbb{Z}/n\mathbb{Z}$, kongruenssi- eli jäännösluokat

Relaatio \equiv_n on ekvivalenssirelaatio joukossa \mathbb{Z} ($x \equiv_n x$, $x \equiv_n y \rightarrow y \equiv_n x$, $x \equiv_n y$ AND $y \equiv_n z \rightarrow x \equiv_n z$) ja jakaa \mathbb{Z} ekvivalenssiluokkiin joita kutsutaan kongruenssi- tai jäännösluokiksi, ja nämä ovat joukot $\{\dots, -2n, -n, 0, n, 2n, \dots\}$, $\{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$, \dots , $\{\dots, -n-1, -1, n-1, 2n-1, \dots\}$ joissa kaikki alkiot ovat kongruentteja toistensa kanssa modulo n . Seuraavia merkintöjä käytetään:

$$[k]_n \stackrel{\text{def}}{=} \{ m \in \mathbb{Z} : m \equiv_n k \} = \{ m \in \mathbb{Z} : \text{mod}(m, n) = \text{mod}(k, n) \},$$
$$\mathbb{Z}/n\mathbb{Z} \stackrel{\text{def}}{=} \{ [k]_n : k = 0, 1, 2, \dots, n-1 \}, \quad \text{jos } n > 0.$$

💡 Huom!

Koska $\text{mod}(m_1, n) = \text{mod}(m_2, n) \Leftrightarrow [m_1]_n = [m_2]_n$ niin usein valitaan alkio $\text{mod}(m, n)$ edustamaan jäännösluokkaa $[m]_n$ niin että voidaan esim. puhua luvuista $0, 1, 2, \dots, 5$ joukon $\mathbb{Z}/6\mathbb{Z}$ alkioina joukkojen $[0]_6, [1]_6, \dots, [5]_6$ sijasta. Joskus kirjoitetaan $[k]_n$:n sijasta \bar{k}_n ja $\mathbb{Z}/n\mathbb{Z}$:n sijasta \mathbb{Z}_n .

💡 Yhteen-, vähennys- ja kertolasku $\mathbb{Z}/n\mathbb{Z}$:ssa

Voidaan osoittaa, että jos

$$a_1 \equiv_n a_2 \quad \text{ja} \quad b_1 \equiv_n b_2$$

niin

$$(a_1 + b_1) \equiv_n (a_2 + b_2)$$

$$(a_1 - b_1) \equiv_n (a_2 - b_2)$$

$$(a_1 \cdot b_1) \equiv_n (a_2 \cdot b_2)$$

Näin ollen voidaan määritellä laskuoperaatioita joukossa $\mathbb{Z}/n\mathbb{Z}$ seuraavasti:

$$[a]_n + [b]_n = [a + b]_n,$$

$$[a]_n - [b]_n = [a - b]_n,$$

$$[a]_n \cdot [b]_n = [a \cdot b]_n,$$

ja kaikki "normaalit" laskusäännöt (paitsi epäyhtälöihin liittyvät) pätevät edelleen.

😊 Esimerkki

Päteekö 3 | 5742385242417 eli jakaako 3 luvun 5742385242417?

Vastaus on kyllä koska luvun numeroiden summa

$5 + 7 + 4 + 2 + 3 + 8 + 5 + 2 + 4 + 2 + 4 + 1 + 7$ on kolmella jaollinen.

Mutta miksi tämä sääntö pätee?

- Kymmenjärjestelmässä luvulla $x_n x_{n-1} \dots x_1 x_0$ tarkoitetaan lukua $m = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \dots + x_1 \cdot 10 + x_0 \cdot 10^0$.
- $[10^j]_3 = [10]_3^j = [1]_3^j = [1^j]_3 = [1]_3$.
- Tästä seuraa, että

$$\begin{aligned} [m]_3 &= [x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \dots + x_1 \cdot 10 + x_0 \cdot 10^0]_3 \\ &= [x_n]_3 \cdot [10^n]_3 + [x_{n-1}]_3 \cdot [10^{n-1}]_3 + \dots + [x_1]_3 \cdot [10]_3 + [x_0]_3 \cdot [1]_3 \\ &= [x_n]_3 + [x_{n-1}]_3 + \dots + [x_1]_3 + [x_0]_3 \\ &= [x_n + x_{n-1} + \dots + x_1 + x_0]_3. \end{aligned}$$

💡 Suurin yhteinen tekijä

Jos m ja n ovat kokonaislukuja jotka eivät molemmat ole 0 niin niiden suurin yhteinen tekijä on

$$\text{syt}(m, n) = \max\{d \in \mathbb{Z} : d|m \text{ ja } d|n\}.$$

(syt= suurin yhteinen tekijä, gcd= greatest common divisor, ja tavallisesti määritellään $\text{syt}(0, 0) = 0$)

Jos $\text{syt}(m, n) = 1$ niin luvut m ja n ovat keskenään jaottomia.

Huomaa, että määritelmästä seuraa, että

$$\text{syt}(m, n) = \text{syt}(n, m) = \text{syt}(|m|, |n|).$$

💡 Käänteisalkiot $\mathbb{Z}/n\mathbb{Z}$:ssa

Jos $[m]_n \in \mathbb{Z}/n\mathbb{Z}$ ja on olemassa jäännösluokka $[j]_n \in \mathbb{Z}/n\mathbb{Z}$ siten, että $[m]_n \cdot [j]_n = [1]_n$, eli $m \cdot j \equiv_n 1$ niin sanotaan, että $[m]_n$:llä on käänteisalkio tai että $[m]_n$ on kääntyvä $\mathbb{Z}/n\mathbb{Z}$:ssa ja käänteisalkio on $[j]_n = [m]_n^{-1}$.

Tässä tapauksessa voidaan jakaa $[m]_n$:llä koska se on yhtäpitävää sen kanssa, että kerrotaan $[j]_n$:llä.

Koska $m \cdot j \equiv_n 1$ niin on olemassa kokonaisluku k siten, että $m \cdot j = 1 + k \cdot n$. Jos nyt $d|m$ ja $d|n$ niin pätee $d|(m \cdot j - k \cdot n)$ eli $d|1$ joten $d = 1$. Näin ollen $\text{sy}(m, n) = 1$. Voidaan osoittaa, että myös käänteinen tulos pätee joten

$$[m]_n \text{:llä on käänteisalkio } \mathbb{Z}/n\mathbb{Z} \text{:ssa} \quad \leftrightarrow \quad \text{sy}(m, n) = 1.$$

💡 Huom

Jos p on alkuluku niin kaikilla $\mathbb{Z}/p\mathbb{Z}$:n alkiolla paitsi $[0]_p$:llä on käänteisalkio.

Esimerkki: Henkilötunnus

Jos $11031xA246K$ on henkilötunnus, niin mikä on x ?

Tässä A tarkoittaa, että kyseinen henkilö on syntynyt 2000-luvulla ja tarkistusmerkki K tarkoittaa, että $\text{mod}(11031 \times 246, 31) = 18$ ja tämän tiedon avulla voimme laskea luvun x esimerkiksi näin:

Kirjoitamme $11031 \times 246 = 110310246 + x \cdot 1000$ jolloin saamme yhtälön

$$[18]_{31} = [11031 \times 246]_{31} = [110310246]_{31} + [x]_{31} \cdot [1000]_{31}.$$

Koska $\text{mod}(110310246, 31) = 1$ ja $\text{mod}(1000, 31) = 8$ niin yhtälö onkin

$$[18]_{31} = [1]_{31} + [x]_{31} \cdot [8]_{31}$$

josta saamme ratkaisuksi

$$[x]_{31} = ([18]_{31} - [1]_{31}) \cdot [8]_{31}^{-1} = [17]_{31} \cdot [4]_{31} = [68]_{31} = [6]_{31},$$

missä käytimme tulosta $[8]_{31}^{-1} = [4]_{31}$, joka seuraa siitä että

$8 \cdot 4 = 32 = 1 + 31$. Koska $0 \leq x \leq 9$ niin $x = 6$.

💡 Eukleideen algoritmi ja $\text{syt}(m, n)$

- Oleta, että $m \geq n > 0$.
- Valitse $r_0 = m$ ja $r_1 = n$.
- Laske q_j ja r_j siten, että $0 \leq r_j < r_{j-1}$ ja

$$r_{j-2} = q_j r_{j-1} + r_j$$

kun $j \geq 2$ ja $r_{j-1} > 0$.

- $\text{syt}(m, n) = r_{k-1}$ jos $r_k = 0$.

😊 Miksi Eukleideen algoritmi toimii?

Koska $r_{j-2} = q_j r_{j-1} + r_j$ niin $\text{syt}(r_{j-2}, r_{j-1}) = \text{syt}(r_{j-1}, r_j)$ kun oletetaan, että $r_{j-1} > 0$. Koska $d \mid 0$ kaikilla d niin $\text{syt}(r_{k-1}, 0) = r_{k-1}$ joten $\text{syt}(m, n) = \text{syt}(r_0, r_1) = \dots = \text{syt}(r_{k-1}, r_k) = \text{syt}(r_{k-1}, 0) = r_{k-1}$ jos $r_k = 0$.

💡💡 Eukleideen algoritmi

Kun laskemme syt (634, 36):n Eukleideen algoritmin avulla saamme seuraavat tulokset:

$$634 = 17 \cdot 36 + 22$$

$$36 = 1 \cdot 22 + 14$$

$$22 = 1 \cdot 14 + 8$$

$$14 = 1 \cdot 8 + 6$$

$$8 = 1 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0$$

joten $\text{syt}(634, 36) = 2$.

💡 Eukleideen algoritmi ja $\mathbb{Z}/n\mathbb{Z}$:n käänteisalkiot

Jos Eukleideen algoritmissa on valittu $r_0 = m$, $r_1 = n$ ja sitten laskettu q_j ja r_j kun $j = 2, \dots, k$ kaavalla $r_{j-2} = q_j r_{j-1} + r_j$ kunnes $r_k = 0$, jolloin $r_{k-1} = \text{syt}(m, n)$ niin voidaan laskea takaperin lähtien yhtälöstä $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ joka voidaan kirjoittaa muotoon

$$\text{syt}(m, n) = r_{k-1} = r_{k-3} - q_{k-1} r_{k-2} = a_j r_j + b_j r_{j+1},$$

missä $j = k - 3$. Tähän sijoitetaan $r_{j+1} = r_{j-1} - q_{j+1} r_j$ yhtälöstä $r_{j-1} = q_{j+1} r_j + r_{j+1}$ jolloin nähdään, että $\text{syt}(m, n) = a_j r_j + b_j r_{j+1}$ kaikilla $j = k - 2, k - 1, \dots, 0$, eli lopuksi

$$\text{syt}(m, n) = am + bn.$$

missä $a = a_0$ ja b_0 .

Jos nyt $\text{syt}(m, n) = 1$ niin

$$[a]_n \cdot [m]_n = [1]_n \quad \text{eli} \quad [a]_n = [m]_n^{-1},$$

$$[b]_m \cdot [n]_m = [1]_m \quad \text{eli} \quad [b]_m = [n]_m^{-1}.$$

💡 Jäännösluokan käänteisalkio

Jos haluamme laskea $[23]_{67}^{-1}$:n niin ensin laskemme $\text{sy}(67, 23)$:n eli

$$67 = 2 \cdot 23 + 21$$

$$23 = 1 \cdot 21 + 2$$

$$21 = 10 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Jotta voisimme esittää $\text{sy}(67, 23)$:n lukujen 67 ja 23 avulla laskemme takaperin :

$$\begin{aligned}\text{sy}(67, 23) &= 1 = 21 - 10 \cdot 2 = 1 \cdot 21 - 10 \cdot (23 - 1 \cdot 21) \\ &= -10 \cdot 23 + 11 \cdot 21 = -10 \cdot 23 + 11 \cdot (67 - 2 \cdot 23) \\ &= 11 \cdot 67 - 32 \cdot 23\end{aligned}$$

Tästä seuraa, että $(-32) \cdot 23 = 1 - 11 \cdot 67$ joten $(-32) \cdot 23 \equiv 1 \pmod{67}$ mikä on yhtäpitävää sen kanssa, että

$$[23]_{67}^{-1} = [-32]_{67} = [-32 + 67]_{67} = [35]_{67}.$$

😊 Jaollisuustulos

Jos m ja n ovat kokonaislukuja ja p on alkuluku siten, että $m \cdot n$ on p :llä jaollinen niin joko m tai n on p :llä jaollinen.

Miksi?

Oleta, että m ei ole p :llä jaollinen. Silloin pätee $\text{syt}(p, m) = 1$ koska p on alkuluku ja Eukleideen laajennetun algoritmin nojalla on olemassa kokonaislukuja a ja b siten, että $a \cdot p + b \cdot m = 1$. Kerromme tämän yhtälön molemmat puolet n :llä ja saamme

$$n = n \cdot 1 = n \cdot a \cdot p + b \cdot m \cdot n.$$

Koska $m \cdot n$ on p :llä jaollinen niin on olemassa kokonaisluku k siten, että $m \cdot n = k \cdot p$. Tästä seuraa, että

$$n = n \cdot a \cdot p + b \cdot k \cdot p = (n \cdot a + b \cdot k) \cdot p,$$

josta seuraa, että n on p :llä jaollinen.

😊 Montako laskutoimitusta tarvitaan kun $\text{sy}(m, n)$ lasketaan Eukleideen algoritmilla?

Oletamme, että $m > n$. Eukleideen algoritmissa valitsemme $r_0 = m$, $r_1 = n$ ja sitten laskemme r_i ja q_i siten, että $r_{i-2} = q_i r_{i-1} + r_i$ kun $i \geq 2$ kunnes $r_M = 0$ ja silloin $r_{M-1} = \text{sy}(m, n)$. Tähän tarvitaan $M - 1$ jakolaskua. Meidän pitää siis arvioida miten iso M voi olla ja tätä varten valitsemme $x_1 = 1$, $x_2 = 2$ ja

$$x_{j+2} = x_{j+1} + x_j, \quad j \geq 1. \quad (*)$$

Tiedämme, että $r_{M-1} \geq x_1$ ja $r_{M-2} \geq x_2$ koska $r_{M-2} > r_{M-1}$. Jos nyt oletamme, että $r_{M-j} \geq x_j$ kun $1 \leq j \leq k$ niin saamme, koska $q_{M-k+1} \geq 1$ että

$$r_{M-(k+1)} = q_{M-k+1} r_{M-k} + r_{M-k+1} \geq r_{M-k} + r_{M-k+1} \geq x_k + x_{k-1} = x_{k+1}.$$

Induktioperiaatteesta seuraa nyt, että $r_{M-j} \geq x_j$ kaikilla $j = 1, \dots, M$.

😊 Montako laskutoimitusta tarvitaan kun syt (m, n) lasketaan Eukleideen algoritmilla? jatk.

Voisimme ratkaista yhtälön (\star) mutta on ehkä yksinkertaisempaa osoittaa, induktion avulla, että $x_j \geq \left(\frac{1+\sqrt{5}}{2}\right)^{j-1}$ kun $j \geq 1$ (toteamalla, että

$$x_1 = 1 = \left(\frac{1+\sqrt{5}}{2}\right)^{1-1}, \quad x_2 = 2 \geq \left(\frac{1+\sqrt{5}}{2}\right)^{2-1} \text{ ja että}$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{j+1-1} + \left(\frac{1+\sqrt{5}}{2}\right)^{j-1} = \left(\frac{1+\sqrt{5}}{2}\right)^{j+2-1} \text{) ja tästä seuraa, että}$$

$$m = r_0 \geq x_M \geq \left(\frac{1+\sqrt{5}}{2}\right)^{M-1},$$

josta seuraa, että

$$M - 1 \leq \frac{\log(m)}{\log\left(\frac{1+\sqrt{5}}{2}\right)},$$

eli tarvitaan $O(\log(\max(m, n)))$ laskutoimitusta syt (m, n) :n laskemiseksi Eukleideen algoritmin avulla. Tästä seuraa myös, että $[n]_m^{-1}$:n laskemiseksi tarvitaan $O(\log(m))$ laskutoimitusta.

💡 Eulerin φ -funktio

$\varphi(n) =$ alkoiden lukumäärä joukossa

$$\{ m \in \mathbb{Z} : 0 \leq m \leq n - 1, \text{syt}(m, n) = 1 \},$$

$=$ niiden joukon $\mathbb{Z}/n\mathbb{Z}$ alkoiden lukumäärä, joilla on käänteisalkio.

Huomaa että $[0]_1$:llä on käänteisalkio joukossa $\mathbb{Z}/1\mathbb{Z}$ joten $\varphi(1) = 1$ mutta

$[0]_n$:llä ei tietenkään (?) ole käänteisalkiota joukossa $\mathbb{Z}/n\mathbb{Z}$ kun $n > 1$.

Matlab/octave:ssä tämän funktion laskemiseksi voidaan käyttää funktiota

$\text{@}(n) \text{sum}(\text{gcd}(0:n-1, n) == 1)$.

💡 Eulerin lause

Jos $\text{sy}(a, n) = 1$ ja $n > 1$ niin

$$a^{\varphi(n)} \equiv_n 1 \quad \text{eli} \quad \text{mod}(a^{\varphi(n)}, n) = 1 \quad \text{eli} \quad [a^{\varphi(n)}]_n = [1]_n.$$

😊 Eulerin lause, todistus

Oletamme, että $[x_1]_n, \dots, [x_{\phi(n)}]_n$ ovat $\mathbb{Z}/n\mathbb{Z}$:n alkioita joilla on käänteisalkio eli ovat kääntyviä. Koska $\text{syt}(a, n) = 1$ niin myös $[a]_n$ on kääntyvä ja koska $[\alpha]_n \cdot [\beta]_n$ on kääntyvä jos $[\alpha]_n$ ja $[\beta]_n$ ovat kääntyviä, niin $[a]_n \cdot [x_j]_n$ on kääntyvä kaikilla j . Jos nyt $[a]_n \cdot [x_j]_n = [a]_n \cdot [x_k]_n$ niin $[x_j]_n = [a]_n^{-1} \cdot [a]_n \cdot [x_j]_n = [a]_n^{-1} \cdot [a]_n \cdot [x_k]_n = [x_k]_n$ josta seuraa, että alkioita $[a]_n \cdot [x_1]_n, \dots, [a]_n \cdot [x_{\phi(n)}]_n$ ovat samat kuin alkioita $[x_1]_n, \dots, [x_{\phi(n)}]_n$ mutta mahdollisesti eri järjestyksessä. Mutta tulot ovat samat, eli

$$[a]_n^{\varphi(n)} \prod_{i=1}^{\varphi(n)} [x_i]_n = \prod_{i=1}^{\varphi(n)} ([a]_n \cdot [x_i]_n) = \prod_{i=1}^{\varphi(n)} [x_i]_n.$$

Koska kaikki alkioita $[x_i]_n$ ovat kääntyviä niin voimme supistaa pois kaikki $[x_i]_n$:t ja lopputulos on, että $[a]_n^{\varphi(n)} = [1]_n$ eli $\text{mod}(a^{\varphi(n)}, n) = 1$.

💡 Jos p ja q ovat alkulukuja ja $p \neq q$ niin $\varphi(p \cdot q) = (p - 1) \cdot (q - 1)$

Miksi? Koska p ja q ovat alkulukuja niin joukko

$\{k \in \mathbb{Z} : 0 \leq k < p \cdot q, \text{syt}(k, p \cdot q) \neq 1\}$ on

$\{0\} \cup \{q, 2 \cdot q, \dots, (p - 1) \cdot q\} \cup \{p, 2 \cdot p, \dots, (q - 1) \cdot p\}$ ja tässä joukossa on $1 + (p - 1) + (q - 1)$ alkioita. Koska joukossa $\{0, 1, 2, \dots, p \cdot q - 1\}$ on $p \cdot q$ alkioita niin $\varphi(p \cdot q) = p \cdot q - (1 + (p - 1) + (q - 1)) = (p - 1) \cdot (q - 1)$.

😊 Fermat'n pieni lause

Jos p on alkuluku ja $\text{syt}(a, p) = 1$ niin

$$a^{p-1} \equiv_p 1 \quad \text{eli} \quad \text{mod}(a^{p-1}, p) = 1 \quad \text{eli} \quad [a^{p-1}]_p = [1]_p.$$

💡💡 RSA-algoritmi

RSA-algoritmissa käytetään julkista avainta (n, k) viestin saalaamiseen ja yksityistä avainta (n, d) salatun viestin purkamiseen:

- *Salaaminen: Viesti a , joka on luku $0:n$ ja $n - 1:n$ väliltä salataan lähetettäväksi viestiksi $b = \text{mod}(a^k, n)$.*
- *Vastaanotettu viesti b puretaan alkuperäiseksi viestiksi $a = \text{mod}(b^d, n)$.*

Menetelmä perustuu siihen, että julkisen avaimen avulla on (pitää olla) ylivoimaisen vaikeata määrittää yksityistä avainta julkisesta avaimesta jolloin kuka tahansa voi lähettää viestin, joka on salattu vastaanottajan julkisella avaimella mutta ainoastaan vastaanottaja, joka tuntee oman yksityisen avaimensa pystyy purkamaan salatun viestin.

💡💡 Miten RSA-algoritmin avaimet on valittava?

- Valitaan $n = pq$ missä p ja q ovat kaksi "erittäin isoa" alkulukua siten, että luvun n jakaminen alkulukutekijöiksi on ylivoimaisen vaikeata (eli esim. myös $|p - q|:n$ on oltava "iso").
- k on "riittävän iso" luku siten että $\text{syt}(k, m) = 1$ missä $m = (p - 1) \cdot (q - 1)$
- Eukleideen algoritmin avulla voidaan laskea d siten, että $[d]_m = [k]_m^{-1}$ ja tähän tarvitaan tieto siitä mitä p ja q ovat.

😊 Miksi RSA-algoritmi toimii?

- Oleta yksinkertaisuuden vuoksi, että $\text{sy}(a, n) = 1$.
- $\varphi(n) = \varphi(p \cdot q) = (p - 1) \cdot (q - 1) = m$.
- Eulerin lauseen mukaan $[a^m]_n = [1]_n$.
- Koska $[d]_m = [k]_m^{-1}$ niin $k \cdot d = 1 + r \cdot m$ ja
$$\left[b^d \right]_n = \left[a^{k \cdot d} \right]_n = \left[a^{1+r \cdot m} \right]_n = [a]_n \cdot [a^m]_n^r = [a]_n \cdot [1]_n^r = [a]_n,$$
josta seuraa, että $\text{mod}(b^d, n) = \text{mod}(a, n) = a$.

💡 RSA-algoritmi

Jos RSA-algoritmillä ja julkisella avaimella (55, 23) haluamme salata viestin 9 niin meidän pitää laskea $\text{mod}(9^{23}, 55)$. Laskujen nopeuttamiseksi toteamme ensin, että $23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0$ joten $9^{23} = 9^{16} \cdot 9^4 \cdot 9^2 \cdot 9 = (((9^2)^2)^2)^2 \cdot (9^2)^2 \cdot 9^2 \cdot 9$ ja saamme

$$\text{mod}(9^2, 55) = \text{mod}(81, 55) = 26,$$

$$\text{mod}(9^3, 55) = \text{mod}(26 \cdot 9, 55) = \text{mod}(234, 55) = 14$$

$$\text{mod}(9^4, 55) = \text{mod}(26^2, 55) = \text{mod}(676, 55) = 16,$$

$$\text{mod}(9^7, 55) = \text{mod}(16 \cdot 14, 55) = \text{mod}(224, 55) = 4,$$

$$\text{mod}(9^8, 55) = \text{mod}(16^2, 55) = \text{mod}(256, 55) = 36,$$

$$\text{mod}(9^{16}, 55) = \text{mod}(36^2, 55) = \text{mod}((-19)^2, 55) = \text{mod}(361, 55) = 31,$$

$$\text{mod}(9^{23}, 55) = \text{mod}(31 \cdot 4, 55) = \text{mod}(124, 55) = 14,$$

joten $\text{mod}(9^{23}, 55) = 14$.

💡 RSA-algoritmi, jatk.

Jotta voisimme purkaa lähetettyä viestiä 14 meidän täytyy tietää mikä yksityinen avain on ja koska $55 = 5 \cdot 11$ ja $(5 - 1) \cdot (11 - 1) = 40$ niin meidän täytyy laskea $[23]_{40}^{-1}$ ja saamme vastaukseksi $[7]_{40}$ koska $\text{mod}(23 \cdot 7, 40) = \text{mod}(161, 40) = 1$. Yksityinen avain on siis $(55, 7)$. Purkamista varten toteamme, että $7 = 4 + 2 + 1 = 2^2 + 2^1 + 2^0$ joten $14^7 = 14^4 \cdot 14^2 \cdot 14$ ja saamme

$$\text{mod}(14^2, 55) = \text{mod}(196, 55) = 31,$$

$$\text{mod}(14^3, 55) = \text{mod}(14^2 \cdot 14, 55)$$

$$= \text{mod}(31 \cdot 14, 55) = \text{mod}(434, 55) = 49,$$

$$\text{mod}(14^4, 55) = \text{mod}(31^2, 55) = \text{mod}(961, 55) = 26,$$

$$\text{mod}(14^7, 55) = \text{mod}(14^4 \cdot 14^2 \cdot 14, 55) = \text{mod}(26 \cdot 49, 55)$$

$$= \text{mod}(26 \cdot (-6), 55) = \text{mod}(-156, 55) = 9,$$

joten $\text{mod}(14^7, 55) = 9$.

😊 Miksi RSA-algoritmi toimii jos $\text{sy}(a, n) \neq 1$?

- Koska oletamme, että $0 < a < n$ niin $\text{sy}(a, n) \neq 1$ ainoastaan jos $p \mid a$ tai $q \mid a$. Oletamme seuraavaksi, että $p \mid a$ joten $a = p^j \cdot c$ missä $\text{sy}(c, n) = 1$
- Nyt $[b^d]_n = [((p^j \cdot c)^k)^d]_n = [(p^k)^d]_n^j \cdot [(c^k)^d]_n$ ja koska $\text{sy}(c, n) = 1$ niin $[(c^k)^d]_n = [c]_n$ ja meidän täytyy vielä osoittaa, että $[(p^k)^d]_n = [p]_n$ koska silloin $[b^d]_n = [p]_n^j \cdot [c]_n = [p^j \cdot c]_n = [a]_n$.
- Koska q on alkuluku ja $p \neq q$ niin $\text{sy}(p, q) = 1$ ja näin ollen Fermat'n lauseesta seuraa, että $[p^{q-1}]_q = [1]_q$.
- Silloin myös $[p^{(q-1)(p-1)r}]_q = [1]_q$ eli $p^{(q-1)(p-1)r} = 1 + sq$ ja kun kerromme molemmat puolet p :llä saamme $p^{1+(q-1)(p-1)r} = p + spq = p + sn$. Koska $[d]_m = [k]_m^{-1}$ niin $k \cdot d = 1 + mr = 1 + (p-1)(q-1)r$ ja näin ollen $[(p^k)^d]_n = [p^{1+(q-1)(p-1)r}]_n = [p]_n$ ja algoritmi toimii siis myös tässä tapauksessa!

😊 RSA-algoritmi ja allekirjoitukset

Jos A haluaa lähettää viestin a B:lle ja B haluaa tulla vakuuttuneeksi siitä, että viesti todella on peräisin A:lta niin he voivat toimia seuraavalla tavalla:

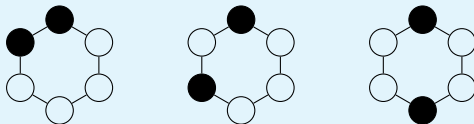
- *A laskee tiivisteen eli hajautusarvon $h(a)$ viestistä a .*
- *A salaa viestin a B:n julkisella avaimella (n_B, k_B) salatuksi viestiksi $b = \text{mod}(a^{k_B}, n_B)$.*
- *A salaa tiivisteen $h(a)$ omalla yksityisellä avaimellaan (n_A, d_A) allekirjotukseksi $s = \text{mod}(h(a)^{d_A}, n_A)$.*
- *A lähettää b :n ja s :n B:lle.*
- *B purkaa b :n yksityisellä avaimellaan (n_B, d_B) ja saa tulokseksi a :n.*
- *B laskee tiivisteen $h(a)$:n ja purkaa s :n A:n julkisella avaimella (n_A, k_A) ja jos tulos on sama kuin $h(a)$ niin hän tulee vakuuttuneeksi siitä, että viesti a todella on peräisin A:lta koska kukaan muu ei pysty salaamaan $h(a)$:ta A:n yksityisellä avaimella (n_A, d_A) .*

Koska $[k]_m = [d]_m^{-1}$ niin viesti joka on salattu yksityisellä avaimella voidaan purkaa julkisella avaimella.

💡 Väritysongelma

Jos meillä on 6 palloa, monellako tavalla voimme värittää 2 niistä mustiksi ja muut valkoisiksi?

- *Jos pallot ovat identtiset on vain yksi tapa, 2 väritetään mustiksi ja 4 valkoisiksi.*
- *Jos pallot on numeroitu niin on $\binom{6}{2} = 15$ tapaa valita ne, jotka väritetään mustiksi ja loput valkoisiksi.*
- *Jos pallot ovat säännöllisen 6-kulmion kulmissa ja tätä 6-kulmiota voi kääntää niin on 3 vaihtoehtoa:*



Mutta miten ratkaistaan monimutkaisemmat tämäntyyppiset ongelmat?

Huomaa, ettei "väritystä" pidä ymmärtää kirjaimellisesti. Yllä olevat kuvat voivat myös esittää ksyleenin (C_8H_{10}) isomeerejä missä kaksi vetyatomia on korvattu metyyliiryhmillä.

💡 Ryhmät

Ryhmä on pari $[G, \bullet]$ missä G on joukko ja \bullet on binäärinen operaatio G :ssä eli funktio $G \times G \rightarrow G$ siten, että

- Sulkeutuneisuus: $a \bullet b \in G$ jos a ja $b \in G$. (Seuraus oletuksesta, että $\bullet : G \times G \rightarrow G$ on funktio.)
- Assosiativisuus: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ jos a, b ja $c \in G$.
- Neutraalialkio: On olemassa alkio $e \in G$ siten, että $e \bullet a = a \bullet e = a$ jos $a \in G$.
- Käänteisalkio: Jos $a \in G$, niin on olemassa alkio $a^{-1} \in G$ (joka osoittautuu yksikäsitteiseksi) siten, että $a \bullet a^{-1} = a^{-1} \bullet a = e$.

💡 Huom!

- Usein sanotaan " G on ryhmä" jos on selvää, mikä ryhmäoperaatio on tai jos sillä ei ole merkitystä.
- Merkinnän $a \bullet b$ (tai $\bullet(a, b)$) sijasta kirjoitetaan usein ab , $a^0 = e$ ja $a^m = \underbrace{a \bullet a \bullet \dots \bullet a}_m$. Neutraalialkiota merkitään myös 1:llä tai I :llä.

💡 Esimerkkejä ryhmistä $[G, \bullet]$

- $G = \mathbb{Z}$ ja $\bullet = +$ jolloin neutraalialkio on 0 ja n :n käänteisalkio on $-n$.
- $G = \mathbb{R} \setminus \{0\}$ ja $\bullet = \cdot$ eli tavallinen kertolasku jolloin neutraalialkio on 1 ja x :n käänteisalkio on x^{-1} eli $\frac{1}{x}$
- $G = \mathbb{Z}/7\mathbb{Z} \setminus \{[0]_7\}$ ja \bullet on jäännösluokkien kertolasku.
- $G = \{A : A \text{ on } n \times n\text{-matriisi ja } \det(A) \neq 0\}$ ja \bullet on matriisien kertolasku. Neutraalialkio on yksikkömatriisi ja käänteisalkio on käänteismatriisi. Tämä ryhmä ei ole kommutatiivinen kun $n \geq 2$.
- $G = \{f : f \text{ on bijektio: } X \rightarrow X\}$ ja $\bullet = \circ$ eli funktioiden yhdistäminen. Tämä ei ole kommutatiivinen ryhmä jos $|X| \geq 3$.

💡 Kommutatiiviset eli Abelin ryhmät

Jos $[G, \bullet]$ on ryhmä siten, että $a \bullet b = b \bullet a$ kaikilla a ja $b \in G$ niin ryhmä on **kommutatiivinen** eli Abelin ryhmä. Tässä tapauksessa ryhmäoperaatiota merkitään usein $+$:lla, neutraalikalkiota 0 :lla ja a :n käänteisalkiota $-a$:llä.

💡💡 Aliryhmä

Jos G (eli $[G, \bullet]$) on ryhmä niin joukon G ei-tyhjä osajoukko H on G :n aliryhmä jos seuraavat ehdot pätevät ja silloin H (eli $[H, \bullet|_{H \times H}]$) on myös ryhmä:

- Jos a ja $b \in H$ niin $a \bullet b \in H$.
- Jos $a \in H$ niin $a^{-1} \in H$.

Jos H on äärellinen joukko niin jälkimmäinen ehto seuraa edellisestä koska $a^m \in H$ kaikilla $m \geq 1$ ja $|H| < \infty$ niin on olemassa luvut $m > k \geq 1$ siten, että

$a^m = a^k$ jolloin $a^{m-k} = e$ ja silloin $a = e = a^{-1} \in H$ jos $m = k + 1$ ja $a^{-1} = a^{m+k-1} \in H$ jos $m > k + 1$.

💡 Homomorfismit ja isomorfismit

Oletetaan, että $[G_1, \bullet_1]$ ja $[G_2, \bullet_2]$ ovat kaksi ryhmää ja ψ on funktio :
 $G_1 \rightarrow G_2$.

- ψ on **homomorfismi** jos $\psi(a \bullet_1 b) = \psi(a) \bullet_2 \psi(b)$ kaikilla a ja $b \in G_1$.
- ψ on **isomorfismi** jos se on homomorfismi ja bijektio (jolloin myös ψ^{-1} on homomorfismi).

Ryhmät ovat tässä epäolennaisia, oleellista on, että homomorfismi "säilyttää struktuurin"!

💡 Sykliset ryhmät

Ryhmä G on syklinen jos on olemassa $a \in G$ siten, että $G = \{ a^j : j \in \mathbb{Z} \}$.
Silloin sanotaan, että G on a :n generoima syklinen ryhmä ja merkitään $G = \langle a \rangle$.

Jos G on ryhmä ja $a \in G$ niin $\langle a \rangle = \{ a^j : j \in \mathbb{Z} \}$ on a :n generoima G :n syklinen aliryhmä.

Koska kaikki sykliset ryhmät, joissa on m alkioita ovat isomorfiset niin tällaista ryhmää merkitään C_m :llä.

😊 Sivuluokat

Olkoon G ryhmä, H sen aliryhmä ja $a \in G$.

- Joukko $aH = \{ ab : b \in H \}$ on H :n **vasen sivuluokka** joka sisältää a :n.
- Joukko $Ha = \{ ba : b \in H \}$ on H :n **oikea sivuluokka** joka sisältää a :n.

Sivuluokilla on seuraavia ominaisuuksia (tässä ainoastaan vasemmat sivuluokat):

- $|aH| = |H|$ kaikilla $a \in G$.
- Jos a ja $b \in G$ niin joko $aH = bH$ tai $aH \cap bH = \emptyset$.
- $\cup_{a \in G} aH = G$.
- Jos a ja $b \in G$ ja $aH = bH$ niin pätee $b^{-1}a \in H$.
- $|G| = |H| \cdot |\{ aH : a \in G \}|$ ja näin ollen luku $|H|$ jakaa luvun $|G|$.

😊 Esimerkki: Isomorfismi

Jos $\psi(x) = \log(x)$ niin $\psi : (0, \infty) \rightarrow \mathbb{R}$ on isomorfismi kun laskutoimitus joukossa $G_1 = (0, \infty)$ on kertolasku ja laskutoimitus joukossa $G_2 = \mathbb{R}$ on yhteenlasku, eli $[G_1, \bullet_1] = [(0, \infty), \cdot]$ ja $[G_2, \bullet_2] = [\mathbb{R}, +]$.

😊 Esimerkki: Syklinen ryhmä

Ryhmä $[\mathbb{Z}/7\mathbb{Z} \setminus \{[0]_7\}, \cdot]$ on syklinen ryhmä koska jos $a = [3]_7$ niin $a^2 = [2]_7$, $a^3 = [6]_7$, $a^4 = [4]_7$, $a^5 = [5]_7$ ja $a^6 = a^0 = [1]_7$. Jäännösluokka $[2]_7$ generoi syklisen aliryhmän $\{[2]_7, [4]_7, [1]_7\}, \cdot]$.

😊 Esimerkki: Sivuluokka

Jos $G = \mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ ja laskutoimitus on yhteenlasku $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ niin $\{(t, 2 \cdot t) : t \in \mathbb{R}\}$ on ryhmän $[G, +]$ aliryhmä ja sen sivuluokat ovat joukot $\{(u + t, v + 2 \cdot t) : t \in \mathbb{R}\}$ missä $(u, v) \in G$ eli suoran $y = 2x$ suuntaisten suorien pistejoukot.

😊 Homomorfismit, normaalit aliryhmät ja tekijäryhmät

Olkoon G ryhmä.

- Jos G' on ryhmä, jonka neutraalialkio on e' ja $\psi : G \rightarrow G'$ on homomorfismi niin $H = \{ a \in G : \psi(a) = e' \}$ (ψ :n ydin) on G :n aliryhmä.
- G :n aliryhmä H on muotoa $\{ a \in G : \psi(a) = e' \}$ jollakin homomorfismilla $G \rightarrow G'$ jos ja vain jos $aH = Ha$ kaikilla $a \in G$ (tai yhtäpitävästi, $aba^{-1} \in H$ kaikilla $a \in G$ ja $b \in H$). Tässä tapauksessa sanotaan, että H on G :n **normaali** aliryhmä.
- Jos H on G :n normaali aliryhmä niin sivuluokat (vasen sama kuin oikea) muodostavat **tekijäryhmän**, jota merkitään G/H :lla ja jonka ryhmäoperaatio on $(aH)(bH) = (ab)H$, neutraalialkio H ja käänteisalkio $(aH)^{-1} = a^{-1}H$. Funktio $\psi : G \rightarrow G/H$ jonka määritelmä on $\psi(a) = aH$ on homomorfismi, jonka ydin on H .

💡 Jäännösluokat tekijäryhminä

Jos $n > 1$ niin $n\mathbb{Z} = \{n \cdot j : j \in \mathbb{Z}\}$ on ryhmän $[\mathbb{Z}, +]$ aliryhmä ja koska yhteenlasku on kommutatiivinen laskutoimitus ($a + b = b + a$) niin $n\mathbb{Z}$ on normaali aliryhmä. Aliryhmän $n\mathbb{Z}$ sivuluokat ovat jäännösluokat modulo n ja ne muodostavat tekijäryhmän $\mathbb{Z}/n\mathbb{Z}$ missä laskutoimitus on yhteenlasku.

💡💡 Permutaatiot

Joukon A **permutaatio** on bijektio $A \rightarrow A$.

- Kaikki joukon A permutaatiot muodostavat ryhmän kun ryhmäoperaatio on funktioiden yhdistäminen. Koska kaikki m -alkioisten joukkojen kaikkien permutaatioiden muodostamat ryhmät ovat isomorfiset niin tällaista ryhmää merkitään S_m :llä.
- Jokainen ryhmä $[G, \bullet]$ on isomorfinen jonkin joukon permutaatioiden aliryhmän kanssa koska joukoksi voidaan valita G ja isomorfismiksi voidaan valita $\psi(a)(b) = a \bullet b$ mutta tästä ei seuraa että aina olisi hyödyllistä käsitellä ryhmää tällaisena permutaatioryhmänä.

💡💡 Permutaatiot, radat, syklimerkinnät

Olkoon A äärellinen ei-tyhjä joukko.

- Jos α on A :n permutaatio niin α :n **radat** ovat pienimmät mahdolliset osajoukot $A_j \subset A$, $j = 1, 2, \dots, m$ siten, että $A_j \cap A_k = \emptyset$ kun $j \neq k$, $\bigcup_{j=1}^m A_j = A$ ja $\alpha(A_j) = \{\alpha(a) : a \in A_j\} = A_j$.
- **Sykli** on A :n permutaatio α jolle pätee $\alpha(x_j) = x_{j+1}$, $j = 1, 2, \dots, k-1$ ja $\alpha(x_k) = x_1$ missä $x_1, x_2, \dots, x_k \in A$ ja $\alpha(x) = x$ kaikilla $x \in A \setminus \{x_1, \dots, x_k\}$. **Syklimerkinnöillä** kirjoitetaan $\alpha = (x_1 \ x_2 \ \dots \ x_k)$. Tällaisen syklin α **pituus** on k ja sanotaan, että α on k -sykli. Syklin α radat ovat $\{x_1, x_2, \dots, x_k\}$ ja joukot $\{x\}$ kaikilla $x \in A \setminus \{x_1, \dots, x_k\}$.
- Jos α on permutaatio niin jokaista sen rataa vastaa sykli ja α voidaan esittää näiden syklien tulona (eli yhdistettynä funktiona).

😊 Huom!

Permutaation α radat ovat ekvivalenssiluokat kun ekvivalenssirelaatioksi määritellään $x \sim y$ kun $\alpha^j(x) = y$ jollain $j \in \mathbb{Z}$.

💡 Permutaatiot ja syklinotaatio

Funktio α on joukon $A = \{1, 2, 3, 4, 5, 6, 7\}$ permutaatio

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 3 & 5 & 7 & 6 \end{pmatrix},$$

missä siis tämä merkintätapa tarkoittaa, että esim. $\alpha(1) = 2$ ja $\alpha(4) = 3$. Nyt näemme, että $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$ (eli $\alpha(1) = 2$, $\alpha(2) = 4$ jne.) ja tästä saamme syklin $(1 \ 2 \ 4 \ 3)$ joka siis on permutaatio β_1 jolle pätee $\beta_1(1) = 2$, $\beta_1(2) = 4$, $\beta_1(4) = 3$, $\beta_1(3) = 1$ ja $\beta(x) = x$ kaikilla $x \in \{5, 6, 7\}$. Koska $\alpha(5) = 5$ saamme syklin $\beta_2 = (5)$ jolle siis $\beta_2(x) = x$ kaikilla $x \in A$. Lopuksi näemme, että $6 \mapsto 7 \mapsto 6$ joten saamme syklin $\beta_3 = (6 \ 7)$. Syklinotaatiolla voimme nyt kirjoittaa

$$\alpha = \beta_1\beta_3 = (1 \ 2 \ 4 \ 3) (6 \ 7),$$

koska β_2 on identiteettifunktio. Mutta on myös muita esitystapoja syklien tuloina, esim. $\alpha = (7 \ 6) (4 \ 3 \ 1 \ 2)$.

Joukot $A_1 = \{1, 2, 4, 3\}$, $A_2 = \{5\}$ ja $A_3 = \{6, 7\}$ ovat permutaation radat koska $\cup_{j=1}^3 A_j = A$, $A_j \cap A_k = \emptyset$ kun $j \neq k$, $\alpha(A_j) = A_j$, $j = 1, 2, 3$ eikä löydy pienempiä joukkoja, joilla olisi nämä ominaisuudet.

😊 Parilliset ja parittomat permutaatiot

- Jokainen sykli, jonka pituus on $k \geq 2$ voidaan kirjoittaa $k - 1:n$ 2-syklin tulona koska
$$(x_1 \ x_2 \ \dots \ x_k) = (x_1 \ x_k) (x_1 \ x_{k-1}) \dots (x_1 \ x_3) (x_1 \ x_2).$$
- Jokainen sykli voidaan kirjoittaa tulona sykleistä joiden pituudet ovat 2 (tai 1).
- Jos permutaatio α on kirjoitettu sekä $r:n$ että $r':n$ 2-syklin tulona niin $(-1)^r = (-1)^{r'}$ ja permutaation **merkki** on $\text{sign}(\alpha) = (-1)^r$.
- Jos α on sykli, jonka pituus on k niin $\text{sign}(\alpha) = (-1)^{k+1}$.
- Jos α on n -alkioisen joukon permutaatio ja α :lla on m rataa niin $\text{sign}(\alpha) = (-1)^{n-m}$.
- Permutaation α on **parillinen** jos $\text{sign}(\alpha) = 1$ ja muuten **pariton**.
- Jos α ja β ovat saman joukon permutaatioita niin $\text{sign}(\alpha\beta) = \text{sign}(\alpha)\text{sign}(\beta)$.

💡 Ryhmän toiminta

Jos G eli $[G, \bullet]$ on ryhmä ja X on joukko niin G :n **toiminta** joukossa X on homomorfismi G :ltä X :n permutaatioiden ryhmälle.

Jos yhdistetty funktio määritellään (normaalilla) tavalla

$(f \circ g)(x) = f(g(x))$ niin saadaan **vasen toiminta** ja jos määritellään $x(f \circ g) = (xf)g$

niin saadaan oikea toiminta. Sen sijaan että kirjoitettaisiin $\psi(a)(x)$ missä ψ on homomorfismi, $a \in G$ ja $x \in X$ kirjoitetaan useimmiten ax ja sanotaan että G **toimii** joukossa X . Vasemmalle toiminnalle homomorfisminominaisuudeksi tulee $(ab)x = a(bx)$, $a, b \in G$, $x \in X$.

😊 Huom

Jos G on ryhmä X :n permutaatioita niin identiteettifunktio on homomorfismi eikä toiminta-käsitettä tarvita.

Jos G on ryhmä niin se toimii itsessään esim. siten, että $\psi(a)(x) = ax$ (vasen toiminta), $\psi(a)(x) = axa^{-1}$ (vasen toiminta), $\psi(a)(x) = xa$ (oikea toiminta) tai $\psi(a)(x) = a^{-1}xa$ (oikea toiminta).

💡 Radat ja kiinnittäjäaliryhmät

Oletetaan, että ryhmä G toimii joukossa X (vasemmalta).

- Jos $x \in X$ niin sen **rata** G :n toiminnassa on joukko $Gx = \{ ax : a \in G \} \subset X$.
- Jos $x \in X$ niin sen **rata** alkion $a \in G$ toiminnassa on joukko $\langle a \rangle x = \{ a^j x : j \in \mathbb{Z} \} \subset X$. ($\langle a \rangle$ on a :n generoima syklinen ryhmä.)
- Jos $x \in X$ niin sen **kiinnittäjäaliryhmä** G :n toiminnassa on joukko $G_x = \{ a \in G : ax = x \}$, joka on G :n aliryhmä.
- Jokaisella $x \in X$ pätee $|Gx| \cdot |G_x| = |G|$.

💡 Huom!

Jos G toimii joukossa X niin voidaan määritellä ekvivalenssirelaatio \sim joukossa X siten, että $x \sim y$ jos ja vain jos $x = ay$ jollakin $a \in G$. Radat ovat silloin ekvivalenssiluokat ja usein voi olla hyödyllistä pitää saman ekvivalenssiluokan alkioita samoina.

😊 Esimerkki: G_x , G_x ja X_a

Olkoon $X = \{1, 2, 3, 4\}$ ja G seuraava joukon X permutaatioryhmä:
 $G = \{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$. Jos nyt a on permutaatio $(1\ 2)$ ja x on alkio 3 niin kiinnittäjäaliryhmä G_x on

$$G_x = \{a \in G : ax = x\} = \{(1), (1\ 2)\},$$

rata G_x on

$$G_x = \{3, 3, 4, 4\} = \{3, 4\},$$

ja kiintopistejoukko X_a on

$$X_a = \{x \in X : ax = x\} = \{3, 4\}.$$

Tässä tapauksessa tulos $|G| = |G_x| \cdot |G_x|$ ei sano muuta kuin, että $4 = 2 \cdot 2$.

😊 Miksi $|G_x| \cdot |G_x| = |G|$?

Oletamme, että G on äärellinen ryhmä. Jos H on G :n aliryhmä niin $|H| \cdot m = |G|$ missä m on H :n (esim. vasempien) sivuluokkien lukumäärä (koska kaikissa sivuluokissa on yhtä monta alkioita kuin H :ssa ja niiden unioni on G). Koska G_x on G :n aliryhmä niin valitsemme $H = G_x$ ja konstruoimme bijektio ψ aliryhmän G_x sivuluokkien joukosta rataan Gx jolloin osoitamme, että $m = |G_x|$ josta seuraa, että $|G| = |G_x| \cdot |G_x|$.

Määrittelemme $\psi(aG_x) = ax$. Jos $a_1G_x = a_2G_x$ niin pätee $a_2^{-1}a_1 \in G_x$ joten $a_2^{-1}a_1x = x$ eli $a_1x = a_2x$ joten ψ on hyvin määritelty.

Jos $a_1x = a_2x$ niin pätee $a_2^{-1}a_1x = x$ joten $a_2^{-1}a_1 \in G_x$, josta seuraa, että $a_1G_x = a_2G_x$ eli ψ on injektio.

Jos $y \in Gx$ niin on olemassa $a \in G$ siten, että $y = ax$ ja silloin $y = \psi(aG_x)$ josta seuraa, että ψ on surjektio.

💡💡 Sykli-indeksi

- Joukon X permutaation a tai joukossa X toimivan ryhmän G alkion a **sykli-indeksi** on monomi

$$\zeta_{a,X}(t_1, \dots, t_n) = t_1^{j_1} \cdot t_2^{j_2} \cdot \dots \cdot t_n^{j_n}$$

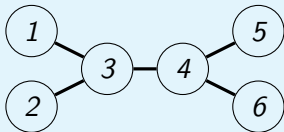
missä j_k on k -pituisten ratojen lukumäärä a :n toiminnassa.

- Joukon X permutaatioryhmän G tai joukossa X toimivan ryhmän G **sykli-indeksi** on

$$\zeta_{G,X}(t_1, \dots, t_n) = \frac{1}{|G|} \sum_{a \in G} \zeta_{a,X}(t_1, \dots, t_n).$$

💡 Esimerkki: Sykli-indeksi

Olkoon G ryhmä, joka muodostuu kaikista alla olevan verkon solmujen permutaatiosta f siten, että jos solmujen a ja b välillä on kaari, niin myös solmujen $f(a)$ ja $f(b)$ välillä on kaari.



Koska solmuilla 3 ja 4 on 3 naapuria niin joko $f(3) = 3$ ja $f(4) = 4$ tai $f(3) = 4$ ja $f(4) = 3$. Solmut 1 ja 2 kuvautuvat solmun $f(3)$ naapureille ja samoin solmut 5 ja 6 kuvautuvat solmun $f(4)$ naapureille.

Näin ollen kyseiset permutaatiot ovat: (1) , $(1\ 2)$, $(5\ 6)$, $(1\ 2)(5\ 6)$, $(3\ 4)(1\ 5)(2\ 6)$, $(3\ 4)(1\ 6)(2\ 5)$, $(3\ 4)(1\ 5\ 2\ 6)$ ja $(3\ 4)(1\ 6\ 2\ 5)$.

💡 Esimerkki: Sykli-indeksi

Seuraavaksi on laskettava näiden permutaatioiden ratojen pituudet:

(1) : 6 rataa, joissa on 1 alkio.

(1 2), (5 6) : 4 rataa, joissa on 1 alkio,
1 rata, jossa on 2 alkiota.

(1 2)(5 6) : 2 rataa, joissa on 1 alkio,
2 rataa, joissa on 2 alkiota.

(3 4)(1 5)(2 6), (3 4)(1 6)(2 5) : 3 rataa, joissa on 2 alkiota.

(3 4)(1 5 2 6), (3 4)(1 6 2 5) : 1 rata, jossa on 2 alkiota,
1 rata, jossa on 4 alkiota.

Näin ollen sykli-indeksi tulee olemaan

$$\zeta_{G,X}(t_1, t_2, t_3, t_4) = \frac{1}{8} \left(t_1^6 + t_1^2 t_2^2 + 2t_1^4 t_2 + 2t_2^3 + 2t_2 t_4 \right)$$

😊 Ratojen lukumäärä ryhmän toiminnassa (Burnsiden lemma)

Oletetaan, että (äärellinen) ryhmä G toimii joukossa X . Jokaiselle $a \in G$ määritellään **kiintopistejoukko** X_a siten, että

$$X_a = \{ x \in X : ax = x \}.$$

(Tätä joukkoa merkitään joskus myös X^a :lla tai $F(a)$:lla.) Silloin ratojen lukumäärä ryhmän G toiminnassa joukossa X on

$$\frac{1}{|G|} \sum_{a \in G} |X_a|.$$

😊 Miksi ratojen lukumäärä ryhmän toiminnassa on $\frac{1}{|G|} \sum_{a \in G} |X_a|$?

Olkoon $E = \{ [a, x] \in G \times X : ax = x \}$. Summeerausjärjestystä vaihtamalla saamme

$$|E| = \sum_{a \in G} |\{x \in X : ax = x\}| = \sum_{x \in X} |\{a \in G : ax = x\}|,$$

joten $\sum_{a \in G} |X_a| = \sum_{x \in X} |G_x|$.

Merkitsemme ratojen joukkoa X/G :llä ja ne ovat ekvivalenssiluokkia kun ekvivalenssirelaatio \sim on $x \sim y$ jos ja vain jos $x = ay$ jollain $a \in G$. Eri radoilla ei ole yhteisiä alkioita ja ratojen unioni on X eli $X = \cup_{A \in X/G} A$.

Koska $|G_x| = \frac{|G|}{|A|}$ ja G_x on rata, johon alkio x kuuluu niin saamme väitteemme seuraavan laskun avulla:

$$\begin{aligned} \sum_{a \in G} |X_a| &= \sum_{x \in X} |G_x| = \sum_{A \in X/G} \sum_{x \in A} |G_x| = \sum_{A \in X/G} \sum_{x \in A} \frac{|G|}{|A|} \\ &= |G| \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|A|} = |G| \sum_{A \in X/G} \frac{1}{|A|} \sum_{x \in A} 1 = |G| \sum_{A \in X/G} 1 = |G| \cdot |X/G|. \end{aligned}$$

💡 Ryhmän toiminta ja "väriykset"

Oletetaan, että ryhmä G toimii joukossa X . Joukon X väritys on funktio $\omega : X \rightarrow K$ missä K on joukko "värejä". Ryhmä G toimii kaikkien väritysten joukossa K^X siten, että $(a\omega)(x) = \omega(a^{-1}x)$, $a \in G$, $x \in X$. Tämä on vasen toiminta koska

$$(a(b\omega))(y) = (b\omega)(a^{-1}y) = \omega(b^{-1}a^{-1}y) = \omega((ab)^{-1}y) = ((ab)\omega)(y).$$

Jos $\Omega \subset K^X$ on X :n väritysten osajoukko niin G toimii joukossa Ω mikäli $G\Omega = \Omega$.

Ryhmän G toiminta väritysjoukolla Ω määrittelee ekvivalenssirelaation Ω :lla siten, että samaan rataan kuluvat väriykset ovat ekvivalentteja, eli $\omega \sim \eta$ jos ja vain jos $\omega = a\eta$ jollakin $a \in G$ ja silloin näitä väriyksiä pidetään samoina. Näin ollen G :n toiminnan suhteen "erilaisten" väritysten lukumäärä on sama kuin ratojen lukumäärä, joka on

$$\frac{1}{|G|} \sum_{a \in G} |\Omega_a|$$

missä $\Omega_a = \{\omega \in \Omega : a\omega = \omega\}$ on niiden väritysten joukko, jotka ovat invariantteja, eli kiintopisteitä, a :n toiminnassa.

💡 Mitkä väritykset ovat invariantteja ryhmäalkion a toiminnassa?

Oletetaan, että ryhmä G toimii joukossa X ja että $a \in G$ ja X :n radat a :n toiminnassa ovat $R_{a,1}, R_{a,2}, \dots, R_{a,m_a}$.

Jos ω on X :n väritys (eli funktio: $X \rightarrow K$ missä K on joukko värejä) niin $a\omega = \omega$ jos ja vain jos ω on vakio jokaisella radalla $R_{a,j}$, $j = 1, \dots, m_a$.

😊 Miksi?

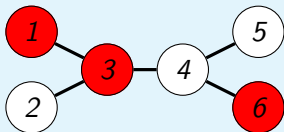
Koska $a\omega = \omega$ niin pätee $a^j\omega = \omega$ kaikilla $j \in \mathbb{Z}$. Jos nyt x ja y kuuluvat samaan rataan a :n toiminnassa niin on olemassa luku j siten, että $a^jx = y$ eli $a^{-j}y = x$. Alkion $a \in G$ toiminnan määritelmän ($(a\omega)(x) = \omega(a^{-1}x)$) nojalla ja koska $a^j\omega = \omega$ saamme

$$\omega(y) = (a^j\omega)(y) = \omega(a^{-j}y) = \omega(x).$$

Jos taas ω on vakio jokaisella radalla niin $\omega(x) = \omega(a^{-1}x)$ kaikilla $x \in X$. Tästä seuraa, että $\omega(x) = (a\omega)(x)$ kaikilla x , eli $\omega = a\omega$.

💡 Esimerkki: Permutaation toiminta värityksillä

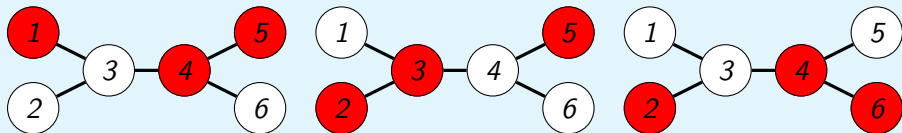
Alla olevan verkon solmut on väritetty värityksellä ω_0 missä $\omega_0(1) = p$, $\omega_0(2) = v$, $\omega_0(3) = p$, $\omega_0(4) = v$, $\omega_0(5) = v$ ja $\omega_0(6) = p$:



Jos a on solmujen permutaatio, niin a :n toiminta värityksellä ω_0 on määritelmän mukaan $a\omega_0(y) = \omega_0(a^{-1}(y))$. Jos esimerkiksi $a = (3\ 4)(1\ 5\ 2\ 6)$ niin $a^{-1} = (3\ 4)(1\ 6\ 2\ 5)$ jolloin

$$a^{-1}(1) = 6, a^{-1}(2) = 5, a^{-1}(3) = 4, a^{-1}(4) = 3, a^{-1}(5) = 1, a^{-1}(6) = 2,$$

ja näin ollen väritykset $a\omega_0$, $a^2\omega_0$ ja $a^3\omega_0$ näyttävät seuraavanlaisilta:



💡 Esimerkki: Permutaation toiminta värityksillä, jatk.

Jos otamme huomioon muutkin ryhmään G kuuluvat permutaatiot, jotka säilyttävät naapurit naapureina saamme 4 väritystä lisää, jotka ovat ekvivalentteja alkuperäisen ω_0 :n kanssa.

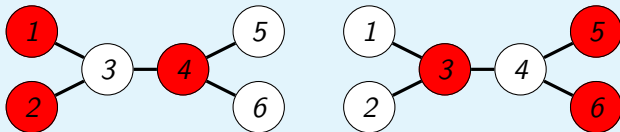
Tässä tapauksessa ei ole kovin hankalaa löytää kaikki ne 5 väritystä, jotka eivät ole ekvivalentteja ja joissa on 3 punaista ja 3 valkoista solmua mutta seuraavaksi määritämme tämän lukumäärän toisella tavalla:

Burnsiden lemmän nojalla ratojen lukumäärä ryhmän G toiminnassa joukossa X on $\frac{1}{|G|} \sum_{a \in G} |X_a|$ missä $X_a = \{\omega \in X : a\omega = \omega\}$. Tässä tapauksessa X on verkon solmujen väritykset ω , jotka värittävät kolme solmua punaiseksi ja kolme valkoiseksi.

Jos nyt a on permutaatio $(3\ 4)(1\ 5\ 2\ 6)$ niin $X_a = \emptyset$ koska ehdosta $a\omega = \omega$ seuraa, että ω saa saman arvon radan $\{3, 4\}$ solmuilla ja saman arvon radan $\{1, 5, 2, 6\}$ solmuilla ja tämä on mahdotonta jos vaaditaan, että solmuista kolme ovat punaisia ja kolme valkoisia. Tämän permutaation sykli-indeksi on $t_2 t_4$ ja jos t_2 :n paikalle sijoitetaan $p^2 + v^2$ ja t_4 :n paikalle $p^4 + t^4$ saadaan polynomi $(p^2 + v^2)(p^4 + t^4)$ ja tässä polynomissa ei ole yhtään $p^3 v^3$ -termiä eli $p^3 v^3$:n kerroin on 0.

💡 Esimerkki: Permutaation toiminta värityksillä, jatk.

Jos sen sijaan tarkastelemme permutaatiota $a^2 = (1\ 2)(6\ 5)$ niin silloin esimerkiksi seuraavat väritykset kuuluvat joukkoon X_{a^2} koska vaatimus on nyt, että ratojen $\{1, 2\}$, $\{5, 6\}$, $\{3\}$ ja $\{4\}$ alkioit saavat saman värin:



Näiden väritysten lisäksi kiintopistejoukkoon X_a^2 kuuluu 2 muuta väritystä jolloin $|X_{a^2}| = 4$. Permutaation a^2 sykli-indeksi on $t_1^2 t_2^2$ joten tässäkin tapauksessa $|X_{a^2}|$ tulee olemaan termin $p^3 v^3$ kerroin polynomissa $(p+v)^2(p^2+v^2)^2 = v^6 + 2pv^5 + 3p^2v^4 + 4p^3v^3 + 3p^4v^2 + 2p^5v + p^6$. Ryhmän G sykli-indeksi on

$\zeta_{G,v}(t_1, t_2, t_4) = \frac{1}{8} (t_1^6 + t_1^2 t_2^2 + 2t_1^4 t_2 + 2t_2^3 + 2t_2 t_4)$ ja termin $p^3 v^3$ kerroin polynomissa $\zeta_{G,v}(p+v, p^2+v^2, p^4+v^4)$ on

$$\frac{1}{8} \left(\frac{6!}{3! \cdot 3!} + 2 \cdot 2 + 2 \cdot \left(\frac{4!}{3! \cdot 1!} \cdot 1 + \frac{4!}{3! \cdot 1!} \cdot 1 \right) + 2 \cdot 0 + 2 \cdot 0 \right) = \frac{40}{8} = 5.$$

💡 Pólyan "väritys"-lause

Oletetaan, että G toimii joukossa X ja että K^X on kaikkien X :n "väritysten" joukko missä "värien" joukko on $K = \{v_1, v_2, \dots, v_r\}$. Silloin monomin

$$v_1^{i_1} \cdot v_2^{i_2} \cdot \dots \cdot v_r^{i_r},$$

kerroin polynomissa

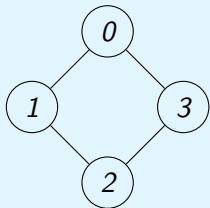
$$\zeta_{G,X}(v_1^1 + \dots + v_r^1, v_1^2 + \dots + v_r^2, \dots, v_1^n + \dots + v_r^n)$$

on niiden X :n väritysten lukumäärä, joissa väriä v_j käytetään täsmälleen i_j kertaa (eli $|\{x : \omega(x) = v_j\}| = i_j$) ja jotka eivät ole ekvivalentteja G :n toiminnassa.

Jos käytetään r väriä mutta muita rajoituksia ei ole niin $\zeta_{G,X}(r, r, \dots, r)$ on niiden X :n väritysten lukumäärä, jotka eivät ole ekvivalentteja G :n toiminnassa.

💡 4-kulmion symmetriat

Olkoon $X = \{0, 1, 2, 3\}$. Koska joukossa X on 4 alkioita niin on olemassa $4! = 24$ joukon X permutaatiota. Mutta jos X :n alkiot ovat vasemmalla olevan verkon solmut ja jos vaadimme permutaatiolta α , että jos x ja y ovat naapureita, eli niiden välillä on kaari, niin myös $\alpha(x)$ ja $\alpha(y)$ ovat naapureita (eli vaadimme, että α on verkko-isomorfismi) niin tilanne muuttuu.



Tässä tapauksessa 0 voi kuvautua mille tahansa solmulle 0, 1, 2 tai 3.

Mutta $\alpha(1)$:n on oltava $\alpha(0)$:n naapuri josta seuraa, että

$\alpha(1) = \text{mod}(\alpha(0) + 1, 4)$ tai $\text{mod}(\alpha(0) - 1, 4)$. Koska $\alpha(2)$ ei saa olla $\alpha(0)$:n naapuri niin $\alpha(2) = \text{mod}(\alpha(0) + 2, 4)$ ja samoin $\alpha(3) = \text{mod}(\alpha(1) + 2, 4)$.

Meillä on siis seuraavat permutaatiot syklinotaatiolla: $(0)(1)(2)(3)$, $(0)(1\ 3)(2)$, $(0\ 1\ 2\ 3)$, $(0\ 1)(2\ 3)$, $(0\ 2)(1\ 3)$, $(0\ 2)(1)(3)$, $(0\ 3\ 2\ 1)$ ja $(0\ 3)(1\ 2)$ joista 4 ovat rotaatioita ja 4 peilauksia.

Näiden permutaatioiden muodostama ryhmä on ns. diedriryhmä ja sitä merkitään D_4 :llä.

💡 4-kulmion symmetriat, jatk.

Seuraavaksi käytämme Pólyan lausetta laskemaan monellako tavalla voimme värittää solmut niin, että yksi on musta, yksi valkoinen ja kaksi punaista. Lisäksi pidämme kaksi väritystä samanlaisina jos rotaatiolla ja/tai peilauksella saadaan toinen toisesta. Tätä varten meidän pitää ensin laskea ryhmän D_4 sykli-indeksi joka saadaan permutaatioiden sykli-indeksien keskiarvona ja permutaation sykli-indeksi on $t_1^{j_1} t_2^{j_2} \dots t_n^{j_n}$ jos permutaatiolla on j_k rataa, joiden pituus on k , $k = 1, 2, \dots, n$. Tässä tapauksessa sykli-indeksiksi tulee

$$\zeta_{D_4, X}(t_1, t_2, t_3, t_4) = \frac{1}{8} \left(t_1^4 + t_1^2 t_2 + t_4 + t_2^2 + t_2^2 + t_1^2 t_2 + t_4 + t_2^2 \right).$$

Erilaisten väritysten lukumäärä on nyt termin mvp^2 kerroin polynomissa $\zeta_{D_4, X}(s + v + r, s^2 + v^2 + r^2, s^3 + v^3 + t^3, s^4 + v^4 + r^4)$ eli polynomissa

$$\frac{1}{8}(s+v+r)^4 + \frac{1}{4}(m+v+p)^2(m^2+v^2+p^2) + \frac{3}{8}(m^2+v^2+p^2)^2 + \frac{1}{4}(m^4+v^4+p^4)$$

ja se on

$$\frac{1}{8} \cdot \frac{4!}{1! \cdot 1! \cdot 2!} + \frac{1}{4} \cdot 2 + 0 + 0 = 2.$$

💡 Pólyan lause ja ristinolla

Meillä on 3×3 -ruudukko ja olemme kirjoittaneet 2:een ruutuun $x:n$, 2:een $o:n$ ja 5 ruutua ovat tyhjinä. Tämä on tehtävissä $\binom{9}{2,2,5} = 756$:lla eri tavalla jos paperi pidetään paikallaan. Mutta jos voimme kiertää paperia kulman 0 , $\frac{\pi}{2}$, π tai $\frac{3\pi}{2}$ verran keskipisteen ympäri niin näiden vaihtoehtojen lukumäärä pienenee ja jotta voisimme systemaattisella tavalla selvittää montako vaihtoehtoa meillä silloin on niin meidän pitää ensin selvittää miten $\frac{\pi}{2}$ kulman rotaation generoima ryhmä toimii ruudukolla ja erityisesti mikä on tämän toiminnan sykli-indeksi. Eli meidän pitää määrittää erilaisten ratojen pituudet. Tulokset ovat seuraavanlaiset:

Identiteettifunktiolla (rotaatio 0) on 9 rataa, joihin kaikkiin kuuluu 1 ruutu. Kierrolla kulman $\frac{\pi}{2}$ verran on 2 rataa, joilla molemmilla on 4 ruutua (toinen sisältää kulmaruudut, toinen niiden välillä olevat ruudut) ja 1 rata johon kuuluu 1 ruutu (ruutu keskellä). Sama pätee jos kierretään kulman $\frac{3\pi}{2}$ verran.

Jos kiertokulma on π niin saamme 4 rataa, joilla molemmilla on 2 ruutua (vastakkaiset kulmat ja vastakkaiset ruudut niiden välillä) 1 rata johon kuuluu 1 ruutu.

💡 Pólyan lause ja ristinolla, jatk.

Sykli-indeksiksi saamme näin ollen

$$\zeta_{G,X}(t_1, t_2, \dots, t_9) = \frac{1}{4} (t_1^9 + 2t_1t_4^2 + t_1t_2^4).$$

Jotta voisimme laskea ei-ekvivalenttien "väritysten" lukumäärää korvaamme muuttujan t_j lausekkeella $x^j + o^j + t^j$ ja silloin termin $x^2o^2t^5$ kerroin on ei-ekvivalenttien "väritysten" lukumäärä kun meillä 2 kappaletta x , 2 kappaletta o , ja 5 kappaletta t . Täksi kertoimeksi tulee

$$\frac{1}{4} \left(\binom{9}{2, 2, 5} + \binom{4}{1, 1, 2} + 0 \right) = \frac{1}{4} (756 + 12) = 192.$$

(Huomaa, ettei lausekkeesta $(x + o + t)(x^4 + o^4 + t^4)^2$ tule yhtään $x^2o^2t^5$ -termiä.)

💡💡 Verkot

- *Suunnattu verkko on pari $[V, E]$ missä V on joukko, jonka alkiot ovat verkon solmut ja E on joukon $V \times V$ osajoukko, jonka alkiot ovat solmujen väliset (suunnatut) kaaret eli linkit.*
- *Suuntaamaton verkko (tai vain verkko) on pari $[V, E]$ missä V on joukko, jonka alkiot ovat verkon solmut ja $E \subset \{ \{a, b\} : a, b \in V \}$ on verkon solmujen välisten kaarien joukko.*
- *Suuntamaton verkko $[V, E]$ on yksinkertainen jos $\{v, v\} = \{v\} \notin E$ kaikilla $v \in V$ ja suunnatun verkon tapauksessa jos $[v, v] \notin E$ kaikilla $v \in V$.*
- *Jos verkon kahden solmun välillä on kaari niin ne ovat toistensa naapureita ja kyseisen kaaren päätesolmut.*

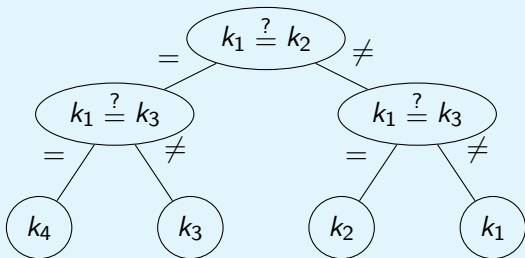
Useimmiten V :n alkioiden lukumäärä on positiivinen mutta äärellinen.

💡 Huom!

Näissä verkoissa on siis kahden solmun välillä korkeintaan yksi kaari ja verkko on yksinkertainen jos mikään solmu ei ole oma naapurinsa.

😊 Verkko päätösprosessin kuvaajana

Meillä on neljä kolikkoa, joista tiedämme että yksi on väärennetty, niin että sen paino poikkeaa muiden painosta mutta emme tiedä onko se painavampi vai kevyempi kuin muut. Meillä on varsivaaka, jonka avulla voimme määrittää onko kahdella kolikolla (tai kolikkoparilla, jne.) sama paino vai ei. Seuraava verkko, joka on puu, kuvaa menetelmän jolla voi päätellä mikä kolikoista k_j , $j = 1, 2, 3, 4$, on väärennetty:



💡 Määritelmiä

- Verkon $[V, E]$ **polku** (solmusta v_0 solmuun v_n) on jono $[v_0, v_1, \dots, v_n]$ missä $v_j \in V$, $j = 0, 1, \dots, n$ ja jokaisella $j = 1, \dots, n$ on olemassa kaari solmujen v_{j-1} ja v_j välillä, (eli $\{v_{j-1}, v_j\} \in E$ tai $[v_{j-1}, v_j] \in E$).
- Polun $[v_0, v_1, \dots, v_n]$ **pituus** on n .
- Verkon $[V, E]$ **sykli** on sen polku $[v_0, v_1, \dots, v_n]$ missä $v_n = v_0$.
- Polku $[v_0, v_1, \dots, v_n]$ on **yksinkertainen** jos $v_j \neq v_k$ $0 \leq j < k \leq n$.
- Sykli $[v_0, v_1, \dots, v_n]$ on **yksinkertainen** jos $n \geq 3$ ja $[v_0, v_1, \dots, v_{n-1}]$ on yksinkertainen.
- Verkon $[V, E]$ **Eulerin polku** (tai sykli) on sen polku (tai sykli) $[v_0, v_1, \dots, v_n]$, jossa $\cup_{j=1}^n \{v_{j-1}, v_j\} = E$ ja $\{v_{j-1}, v_j\} \neq \{v_{k-1}, v_k\}$ kun $1 \leq j < k \leq n$ ($\cup_{j=1}^n [v_{j-1}, v_j] = E$ ja $[v_{j-1}, v_j] \neq [v_{k-1}, v_k]$ kun $1 \leq j < k \leq n$) eli se käy läpi verkon kaikki kaaret täsmälleen kerran.
- Verkon $[V, E]$ **Hamiltonin polku** (tai sykli) on sen yksinkertainen polku (tai sykli) $[v_0, v_1, \dots, v_n]$, jossa $\{v_0, \dots, v_n\} = V$ eli se käy läpi kaikki verkon solmut (syklitapauksessa paitsi $v_0 = v_n$) täsmälleen kerran.

💡💡 Määritelmiä, jatk.

- Verkko on **yhtenäinen** jos jokaisesta solmusta on polku jokaiseen toiseen solmuun.
- Verkko on **puu** jos se on yksinkertainen ja jokaisesta solmusta on täsmälleen yksi yksinkertainen polku jokaiseen toiseen solmuun.
- Verkko on **metsä** jos se on yksinkertainen ja jokaisesta solmusta on korkeintaan yksi yksinkertainen polku jokaiseen toiseen solmuun.
- Verkko $[V, E]$ on **kaksijakoinen** osilla X ja Y jos $V = X \cup Y$, $X \cap Y = \emptyset$ ja $E \subset \{ \{x, y\} : x \in X, y \in Y \}$ (tai $E \subset X \times Y$).
- Verkon $[V, E]$ **pariutus** on kaarien osajoukko $M \subset E$ siten, että kahdella eri M :n kaarilla ei ole yhteisiä päätesolmuja, eli jos $e_1 = \{v_1, v'_1\}$ ja $e_2 = \{v_2, v'_2\}$ niin $e_1 \cap e_2 \neq \emptyset \leftrightarrow e_1 = e_2$ (jos $[v_1, v'_1] \in M$ ja $[v_2, v'_2] \in M$ niin $\{v_1, v'_1\} \cap \{v_2, v'_2\} \neq \emptyset \leftrightarrow [v_1, v'_1] = [v_2, v'_2]$)
- Yksinkertaisen verkon $[V, E]$ **solmujen väritys** on funktio $\omega : V \rightarrow K$ siten, että $\omega(v_j) \neq \omega(v_k)$ jos $\{v_j, v_k\} \in E$ ($[v_j, v_k] \in E$). Verkon **kromaattinen luku** on pienin solmujen väritykseen tarvittava värien lukumäärä.

😊 Verkko on kaksijakoinen jos ja vain jos sen kromaattinen luku on korkeintaan 2

Jos kromaattinen luku on 0 niin verkossa ei ole yhtään solmua ja jos se on 1 niin verkossa ei ole yhtään kaarta joten näistä tapauksista ei tarvitse välittää.

Jos verkko $[X \cup Y, E]$ on kaksijakoinen niin voimme värittää joukon X solmut värillä a ja joukon Y solmut värillä b , josta seuraa, että kromaattinen luku on korkeintaan 2.

Jos kromaattinen luku on 2, ja $\omega : V \rightarrow \{a, b\}$ on solmujen väritys kahdella värillä niin voimme valita $X = \{v \in V : \omega(v) = a\}$ ja $Y = \{v \in V : \omega(v) = b\}$. Ehdosta $\{x, y\} \in E \rightarrow \omega(x) \neq \omega(y)$ seuraa, nyt, että jos $\{x, y\} \in E$ eli jos solmujen x ja y välillä on kaari, niin joko $x \in X$ ja $y \in Y$ tai $x \in Y$ ja $y \in X$ josta seuraa, että verkko on kaksijakoinen (koska $\{x, y\} = \{y, x\}$).

💡 Naapurimatriisi

Jos $[V, E]$ on verkko, jossa on m solmua $V = \{v_1, \dots, v_m\}$ niin sen **naapurimatriisi** on $m \times m$ -matriisi

$$A(j, k) = \begin{cases} 1, & \{v_j, v_k\} \in E, & ([v_j, v_k] \in E), \\ 0, & \{v_j, v_k\} \notin E, & ([v_j, v_k] \notin E). \end{cases}$$

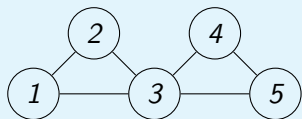
Jos $n \geq 1$ niin $(A^n)(j, k)$ on n -pituisten polkujen lukumäärä solmusta v_j solmuun v_k .

💡 Huom

Jos verkon kaareille annetaan numeroarvoja eli määritellään funktio $w : E \rightarrow \mathbb{R}$, esimerkiksi kuvaamaan solmujen välisiä "etäisyyksiä" niin kannattaa vaihtaa A :n määritelmäksi $A(j, k) = w(\{v_j, v_k\})$ jos $\{v_j, v_k\} \in E$ ja esimerkiksi $+\infty$ muuten.

💡 Naapurimatriisi

Verkon



naapurimatriisi on $A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$

Nyt

$$A^2 = \begin{bmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 4 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{bmatrix} \quad \text{ja} \quad A^3 = \begin{bmatrix} 2 & 3 & 5 & 2 & 2 \\ 3 & 2 & 5 & 2 & 2 \\ 5 & 5 & 4 & 5 & 5 \\ 2 & 2 & 5 & 2 & 3 \\ 2 & 2 & 5 & 3 & 2 \end{bmatrix},$$

ja matriisin A^3 alkio $(A^3)(1,2) = 3$ kertoo, että solmusta 1 on kolme polkua solmuun 2, joiden pituus on 3 eli $[1, 3, 1, 2]$, $[1, 2, 1, 2]$ ja $[1, 2, 3, 2]$.

💡 Isomorfiset verkot

Verkot $[V, E]$ ja $[V', E']$ ovat isomorfiset jos on olemassa bijektio

$\psi : E \rightarrow E'$ siten, että $\{\psi(a), \psi(b)\} \in E' \leftrightarrow \{a, b\} \in E$ (ja suunnatussa tapauksessa

$\{\psi(a), \psi(b)\} \in E' \leftrightarrow [a, b] \in E$) eli "naapurit kuvautuvat naapureille".

💡 Kaksijakoiset verkot ja pariutukset

Olkoon $[X \cup Y, E]$ kaksijakoinen verkko (jonka osat ovat X ja Y). Silloin

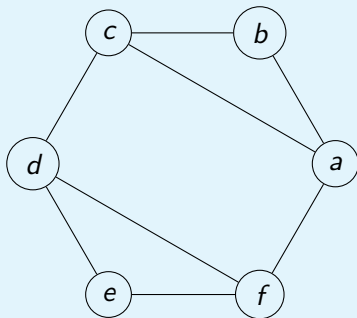
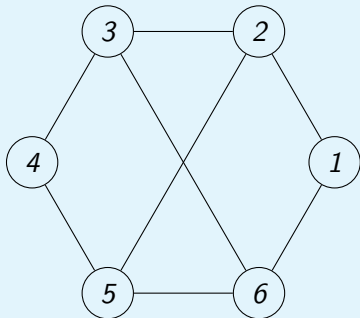
- on olemassa pariutus M siten, että jokainen $x \in X$ on jonkin M :n kaaren päätepiste eli M on ns. täydellinen pariutus

jos ja vain jos

- jokaisella $A \subset X$ pätee, että A :n alkioden lukumäärä $|A|$ on pienempi tai yhtäsuuri kuin A :n alkioden naapureiden lukumäärä eli $|A| \leq |\{y \in Y : \{x, y\} \in E_{([x, y] \in E)}, x \in A\}|$.

💡 Isomorfiset verkot

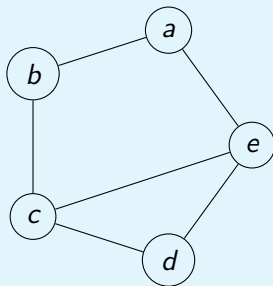
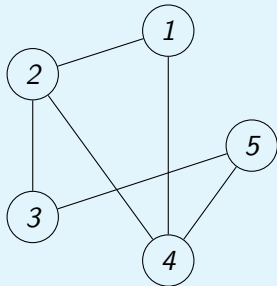
Ovatko alla olevat verkot isomorfiset?



Molemmissa verkoissa on 4 solmua, joilla on 3 naapuria ja 2 joilla on 2 naapuria, joten tästä emme voi päätellä etteivät verkot olisivat isomorfiset. Sensijaan vasemmanpuoleisessa verkossa ei ole yhtään sykliä, jonka pituus olisi 3 mutta sellaisia on oikeanpuoleisessa verkossa. Tästä seuraa, etteivät verkot voi olla isomorfiset.

💡 Isomorfiset verkot, jatk.

Ovatko alla olevat verkot isomorfiset?



Molemmissa verkoissa on kaksi solmua, joilla on kolme naapuria, eli solmut 2 ja 4 ja solmut c ja e. Jos verkot ovat isomorfiset niin isomorfismi voisi olla sellainen, että $\psi(2) = c$ ja $\psi(4) = e$ (tai päinvastoin). Koska solmu 1 on sekä solmun 2 ja solmun 4 naapuri ja samoin solmu d on sekä solmun c että solmun e naapuri täytyy olla $\psi(1) = d$. Jäljellä olevista solmuista solmu 3 on solmun 2 muttei solmun 4 naapuri ja solmu b on solmun c muttei solmun e naapuri, joten $\psi(3) = b$ jolloin täytyy olla $\psi(5) = a$. Näin määritelty funktio ψ on isomorfismi ja verkot ovat isomorfiset.

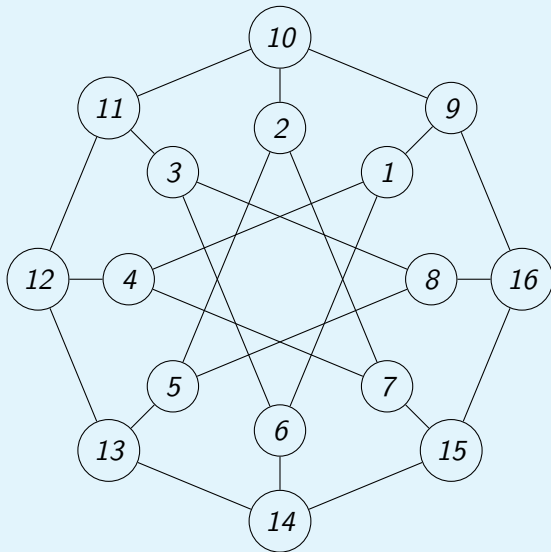
💡💡 Ahne väritysalgoritmi

*Helppo, mutta ei välttämättä optimaalinen tapa solmujen värityksen löytämiseksi on seuraava **ahne** algoritmi:*

- *Aseta solmut johonkin järjestykseen: $[v_1, v_2, \dots, v_n]$.*
- *Aseta värit johonkin järjestykseen: $[c_1, c_2, \dots, c_r]$.*
- *Väritä ensimmäinen solmu ensimmäisellä värillä, eli $\omega(v_1) = c_1$.*
- *Jos solmut v_1, \dots, v_k on väritetty niin väritä solmu v_{k+1} ensimmäisellä käytettävissä olevalla värillä siten, että ehto ettei naapureita väritetä samalla värillä toteutuu, eli $\omega(v_{k+1}) = c_j$ missä $j = \min\{i \geq 1 : \{v_p, v_{k+1}\} \in E \text{ AND } p \leq k \rightarrow \omega(v_p) \neq c_i\}$.*

💡 Ahne väritys

Tehtävänä on määrittää jokin alla olevan verkon solmujen väritys:



💡 Ahne väritys, jatk.

Ahneen väritysalgoritmin mukaisesti toimimme seuraavalla tavalla: Järjestämme solmut ja värit jollain tavalla ja käymme läpi solmut järjestyksessä ja annamme jokaiselle solmulle ensimmäisen mahdollisen värin joka siis ei ole sama kuin sen jollekin naapurille jo annettu väri. Jos värit ovat a, b, c, \dots ja otamme solmut järjestyksessä $1, 2, 3, 4, \dots, 16$ niin väritykseksi tulee:

Solmu	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Väri	a	a	a	b	b	b	c	c	b	c	b	a	c	a	b	a

Jos sen sijaan otamme solmut järjestyksessä $9, 10, \dots, 15, 16, 1, 2, 7, 8$ niin väritykseksi tulee

Solmu	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
Väri	a	b	a	b	a	b	a	b	b	a	b	a	b	a	b	a

Näin ollen pienin mahdollinen värien lukumäärä eli verkon kromaattinen luku on 2 koska se ei voi olla 1 jos verkossa on ainakin yksi kaari.

💡 Minimaalinen virittävä puu, ahne algoritmi I (Prim)

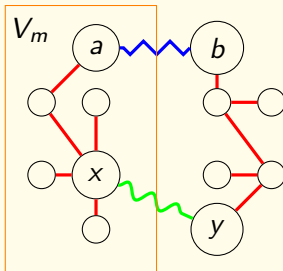
Jos $[V, E]$ on yhtenäinen (suuntaamaton) verkko ja jokaiselle kaarelle $\{v_j, v_k\}$ on annettu paino $w(\{v_j, v_k\})$ (ja $w(\{v_j, v_k\}) = \infty$ jos $\{v_j, v_k\} \notin E$) niin minimaalinen virittävä puu on verkko $[V, E_T]$ missä $E_T \subset E$ (eli aliverkko) joka on puu ja sellainen, että $\sum_{\{v_j, v_k\} \in E_T} w(\{v_j, v_k\})$ on mahdollisimman pieni. Minimaalinen virittävä puu voidaan konstruoida esimerkiksi seuraavalla ahneella algoritmilla:

- Valitse $T_1 = [\{v_1\}, \emptyset]$ missä v_1 on V :n mielivaltainen alkio.
- Jos $T_m = [V_m, E_m]$ on valittu ja $V_m \neq V$ niin valitse $v_j \in V_m$ ja $v_k \in V \setminus V_m$ siten, että $w(\{v_j, v_k\})$ on mahdollisimman pieni jolloin $T_{m+1} = [V_m \cup \{v_k\}, E_m \cup \{\{v_j, v_k\}\}]$, eli verkon T_m solmuihin lisätään solmu v_k ja kaareihin solmujen v_j ja v_k välinen kaari.

😊 Minimaalinen virittävä puu ja Primin ahne algoritmi

- $[V, E]$ yhtenäinen verkko, jossa jokaiselle kaarelle $\{v_j, v_k\}$ on annettu paino $w(\{v_j, v_k\})$ ja $T_* = [V, E_*]$ on puu siten, että $w(T_*) = \sum_{e \in E_*} w(e)$ on mahdollisimman pieni.
- Primin ahneella algoritmilla konstruoimme puut $T_j = [V_j, E_j]$, $j = 1, \dots, n$ (missä $|V_1| = 1$, $|V| = n$ ja $E_1 = \emptyset$).
- Jos $E_* = E_n$ niin tämä algoritmi on optimaalinen ja jos $E_* \neq E_n$ niin on olemassa suurin luku m , $1 \leq m < n$ siten, että $E_m \subset E_*$. Olkoon $\{x, y\} \in E_{m+1} \setminus E_m$ missä $x \in V_m$ ja $y \in V_{m+1} \setminus V_m$ jolloin siis $\{x, y\} \notin E_*$.
- On olemassa polku verkossa T_* solmusta x solmuun y (koska T_* on puu). Tähän polkuun sisältyy kaari $\{a, b\}$ siten, että $a \in V_m$ ja $b \in V \setminus V_m$. Jos nyt vaihdamme T_* :n kaaren $\{a, b\}$ kaareksi $\{x, y\}$ niin uusi verkko T_{**} on myös puu.

😊 Minimaalinen virittävä puu ja Primin ahne algoritmi, jatk.



- *Lisäksi algoritmin mukainen $\{x, y\}$:n valinta takaa että $w(T_{**}) \leq w(T_*)$. Tästä seuraa, että meillä on optimaalinen puu $[V, E_{**}]$ siten, että $E_{m+1} \subset E_{**}$ josta, tarvittaessa toistamalla tätä päättelyä, seuraa, että E_n on optimaalinen virittävä puu.*

😊 Minimaalinen virittävä puu, ahne algoritmi II (Kruskal)

Jos $[V, E]$ on yhtenäinen (suuntaamaton) verkko ja jokaiselle kaarelle $\{v_j, v_k\}$ on annettu paino $w(\{v_j, v_k\})$ (ja $w(\{v_j, v_k\}) = \infty$ jos $\{v_j, v_k\} \notin E$) niin minimaalinen virittävä puu voidaan konstruoida myös seuraavalla ahneella algoritmilla:

- Valitse $E_1 = \emptyset$.
- Niin kauan kun verkko $[V, E_m]$ ei ole puu niin valitse $e \in E \setminus E_m$ siten, että $w(e)$ on mahdollisimman pieni ja verkko $[V, E_{m+1}]$, missä $E_{m+1} = E_m \cup \{e\}$, on metsä.

😊 Minimaalinen virittävä puu ja Kruskalin ahne algoritmi

- $[V, E]$ on yhtenäinen verkko, jossa jokaiselle kaarelle $\{v_j, v_k\}$ on annettu paino $w(\{v_j, v_k\})$ ja $T_* = [V, E_*]$ on puu siten, että $w(T_*) = \sum_{e \in E_*} w(e)$ on mahdollisimman pieni.
- Kruskalin ahneella algoritmilla konstruoimme metsät $F_j = [V, E_j]$, $j = 1, \dots, n$.
- Konstruktion mukaisesti F_n on metsä. Jos F_n ei ole puu niin on olemassa solmut a ja b niin ettei niiden välillä ole polku verkossa F_n . Mutta verkossa $[V, E]$ on olemassa polku $[v_0, v_1, \dots, v_k]$ missä $v_0 = a$ ja $v_k = b$. Olkoon j pienin luku, siten, että solmujen v_{j-1} ja v_j välillä ei ole polku verkossa F_n eikä erityisesti $\{v_{j-1}, v_j\} \in E_n$. (Jos sellainen pari ei löydy niin solmujen a ja b välillä on polku.) Nyt voimme lisätä kaaren $\{v_{j-1}, v_j\}$ joukkoon E_n , että $[V, E_n \cup \{\{v_{j-1}, v_j\}\}]$ edelleen on metsä koska muuten solmujen v_{j-1} ja v_j välillä olisi jo kaari verkossa F_n . Näin ollen algoritmi antaa varmasti tulokseksi puun.

😊 Minimaalinen virittävä puu ja Kruskalin ahne algoritmi, jatk.

- Jos $E_* = E_n$ niin tämä algoritmi on optimaalinen ja jos $E_* \neq E_n$ niin on olemassa suurin luku m , $1 \leq m < n$ siten, että $E_m \subset E_*$ ja jos $\{x, y\} \in E_{m+1} \setminus E_m$ niin $\{x, y\} \notin E_*$.
- Puussa T_* on olemassa polku solmusta x solmuun y . Koska F_n on puu ja $\{x, y\} \notin E_*$ niin tähän polkuun sisältyy kaari $\{a, b\}$ siten, että $\{a, b\} \notin E_n$. Jos $E_{**} = E \cup \{x, y\} \setminus \{a, b\}$ niin $[V, E_{**}]$ on myös puu ja koska T_* oli optimaalinen niin pätee $w(\{x, y\}) \geq w(\{a, b\})$. Koska otimme kaaren $\{x, y\}$ mukaan joukkoon E_{m+1} , vaikka $\{a, b\}$ olisi ollut mahdollinen valinta koska $E_m \cup \{\{a, b\}\} \subset E_*$ josta seuraa, että myös $[V, E_m \cup \{\{a, b\}\}]$ on metsä, niin täytyy olla $w(\{x, y\}) = w(\{a, b\})$ eli T_{**} ja $E_{m+1} \subset E_{**}$ on myös optimaalinen puu. Toistamalla tarvittaessa tätä päättelyä voimme todeta, että F_n on optimaalinen puu.

💡 Dynaaminen optimointi ja verkot

Olkoon $[V, E]$ yksinkertainen ja yhtenäinen (suuntaamaton) verkko jossa jokaiselle kaarelle $\{v_j, v_k\}$ on annettu paino $w(\{v_j, v_k\}) \geq 0$ (ja $w(\{v_j, v_k\}) = \infty$ jos $\{v_j, v_k\} \notin E$). Jos tehtävänä on löytää polku $[v_0, v_1, \dots, v_n]$ tietystä solmusta v_0 johonkin toiseen solmuun v_n siten, että $\sum_{j=1}^n w(\{v_{j-1}, v_j\})$ on mahdollisimman pieni voidaan menetellä seuraavalla tavalla:

- Määrittele $s(v) = \min\{\sum_{j=1}^k w(\{v_{j-1}, v_j\}) : [v_0, v_1, \dots, v_k]$ on polku solmusta v_0 solmuun $v_k = v\}$.
- Huomaa, että funktio s toteuttaa **dynaamisen optimoinnin** periaatetta:

$$s(v) = \min_{v' \in V} (s(v') + w(\{v', v\})).$$

- Määritä **optimaaliset arvot** $s(v)$ seuraavalla tavalla:
 - ◇ Valitse $V_0 = \{v_0\}$ ja $s(v_0) = 0$.
 - ◇ Jos optimaaliset arvot $s(v)$ on määritetty kun $v \in V_j$ niin laske V_j :n naapureille testiarvot $t(v) = \min_{v' \in V_j} (s(v') + w(\{v', v\}))$, $v \in V \setminus V_j$.
 - ◇ Valitse $V_{j+1} = V_j \cup \{v\}$ ja $s(v) = t(v)$ jos $v \in V \setminus V_j$ ja $t(v) = \min_{v' \in V \setminus V_j} t(v')$.

😊 Miksi dynaaminen optimointi toimii kun haemme "minimietäisyyksiä"?

- Määrittelemme funktion s kaavalla

$s(v) = \min\{\sum_{j=1}^k w(\{v_{j-1}, v_j\}) : [v_0, v_1, \dots, v_k] \text{ on polku solmusta } v_0 \text{ solmuun } v_k = v\}$ kun $v \neq v_0$ ja $s(v_0) = 0$.

- Valitsemme $V_0 = \{v_0\}$, $V_{-1} = \emptyset$ ja määrittelemme testiarvot $t_0(v) = \infty$ kaikilla $v \in V \setminus \{v_0\}$. Jos $j \geq 0$ ja tunnemme funktion s arvot joukon V_j solmuissa ja testifunktion

$t_j(v) = \min_{v' \in V_{j-1}} (s(v') + w(\{v', v\}))$ arvot kaikissa muissa solmuissa niin meidän pitää laskea uusi testifunktio ja lisätä joukkoon V_j seuraava piste.

- Koska määrittelemme $t_{j+1}(v) = \min_{v' \in V_j} (s(v') + w(\{v', v\}))$, $v \in V \setminus V_j$, niin $t_{j+1}(v) = t_j(v)$ jos v ei ole viimeksi lisätyn solmun v_j naapuri joten meidän täytyy ainoastaan laskea

$t_{j+1}(v) = \min\{t_j(v), s(v_j) + w(\{v_j, v\})\}$ kun $v \in V \setminus V_j$ on v_j :n naapuri. Sitten valitsemme solmun v_{j+1} joukosta $V \setminus V_j$ siten että $t_{j+1}(v_{j+1}) = \min_{v \in V \setminus V_j} t_{j+1}(v)$.

Miksi dynaaminen optimointi toimii kun haemme "minimietäisyyksiä"? jatk.

- Nyt joko $s(v_{j+1}) = t_{j+1}(v_{j+1})$ ja induktioaskel toimii tai $s(v_{j+1}) < t_{j+1}(v_{j+1})$ ja meidän pitää osoittaa, että jälkimmäinen vaihtoehto johtaa ristiriitaan.
- Jos $s(v_{j+1}) < t_{j+1}(v_{j+1})$ niin on olemassa polku $[\tilde{v}_0, \tilde{v}_1, \dots, \tilde{v}_k]$ siten että $\tilde{v}_0 = v_0$, $\tilde{v}_k = v_{j+1}$ ja $\sum_{i=1}^k w(\{\tilde{v}_{i-1}, \tilde{v}_i\}) < t_{j+1}(v_{j+1})$.
- Silloin on olemassa suurin indeksi $i_0 < k$ siten, että $\tilde{v}_{i_0} \in V_j$ jolloin siis $\tilde{v}_{i_0+1} \in V \setminus V_j$ ja funktion t_{j+1} määritelmästä ja oletuksesta $w(e) \geq 0$ seuraa, että

$$\begin{aligned} s(\tilde{v}_{i_0}) + w(\{\tilde{v}_{i_0}, \tilde{v}_{i_0+1}\}) &\geq t_{j+1}(\tilde{v}_{i_0+1}) \geq t_{j+1}(v_{j+1}) \\ &> \sum_{i=1}^k w(\{\tilde{v}_{i-1}, \tilde{v}_i\}) \geq \sum_{i=1}^{i_0+1} w(\{\tilde{v}_{i-1}, \tilde{v}_i\}) \geq s(\tilde{v}_{i_0}) + w(\{\tilde{v}_{i_0}, \tilde{v}_{i_0+1}\}) \end{aligned}$$

joka on ristiriita. Näin ollen $s(v_{j+1}) = t_{j+1}(v_{j+1})$, voimme valita $V_{j+1} = V_j \cup \{v_{j+1}\}$ ja induktio toimii.



Miten hankalaa on "minimietäisyyksien" löytäminen verkossa?

- Oletamme, että $G = [V, E]$ on yhtenäinen verkko, jossa jokaiselle kaarelle $e \in E$ on annettu paino $w(e) \geq 0$ (ja $w(\{v_j, v_k\}) = \infty$ jos $\{v_j, v_k\} \notin E$) ja tehtävänä on löytää polku $[v_0, v_1, \dots, v_k]$ kahden annetun solmun v_* ja v_{**} välillä siten, että $\sum_{j=1}^k w(\{v_{j-1}, v_j\})$ on mahdollisimman pieni.
- Jos $|V| = n$ ja kaikkien solmujen välillä on kaari niin on olemassa $\sum_{j=2}^n \frac{(n-2)!}{(n-j)!} \geq (n-2)!$ eri vaihtoehtoa mutta yleensä vaihtoehtojen lukumäärä on kuitenkin paljon pienempi.
- Jos käytämme dynaamista optimointia ja olemme laskeneet optimiarvon j :ssä pisteessä niin meidän pitää laskea korkeintaan $n-j$ uutta testiarvoa käyttäen korkeintaan $n-j$ yhteenlaskua ja yhtä monta vertailua ja sitten valita pienin mikä vaatii korkeintaan $n-j-1$ vertailua.
- Näin ollen meidän pitää laskea korkeintaan $\sum_{j=1}^{n-1} (n-j) = \frac{1}{2}n(n-1)$ yhteenlaskua ja tehdä $\sum_{j=1}^{n-1} (n-j + n-j-1) = (n-1)^2$ vertailua. Yhteenlaskujen ja vertailujen lukumäärät ovat siis joukossa $O(n^2)$.

😊 Milloin kaksijakoisessa verkossa on täydellinen pariutus?

Oletamme, että $G = [X \cup Y, E]$ on kaksijakoinen verkko ja $H(A) = \{y \in Y : \exists x(x \in A \text{ AND } \{x, y\} \in E)\}$ kun $A \subset X$ (jolloin siis $H(A)$ on A :n solmujen naapureiden joukko).

- Jos M on verkon täydellinen pariutus verkossa niin $|A| \leq |H(A)|$ kaikilla $A \subset X$ koska $x \in A \mapsto y \in H(A)$ missä $\{x, y\} \in M$ on injektio pariutuksen määritelmän nojalla.
- Seuraavaksi osoitamme, että jos $|A| \leq |H(A)|$ kaikilla $A \subset X$ niin on olemassa verkon täydellinen pariutus. Näin on varmasti jos $|X| = 1$ ja oletamme nyt, että väite pätee myös kun $1 \leq |X| \leq k$ ja $k \geq 1$.
- Jos $|X| = k + 1$ niin valitsemme solmun $a \in X$ ja mikäli mahdollista valitsemme osajoukon $\hat{X} \subset X \setminus \{a\}$ siten, että $|H(\hat{X})| = |\hat{X}| > 0$. Näin ollen meillä on kaksi tapausta riippuen siitä löytyykö tällainen joukko vai onko niin, että $|H(\hat{X})| \geq |\hat{X}| + 1$ kaikilla $\hat{X} \subset X \setminus \{a\}$ kun $\hat{X} \neq \emptyset$.
- Jos pystymme osoittamaan, että molemmissa tapauksissa löytyy täydellinen pariutus, niin väite seuraa induktioperiaatteen nojalla.

😊 Milloin kaksijakoisessa verkossa on täydellinen pariutus? jatk.

- Jos $|H(\hat{X})| = |\hat{X}| > 0$ ja $\hat{X} \subset X \setminus \{a\}$ niin induktio-oletuksen nojalla on olemassa täydellinen pariutus M_1 verkossa $G_1 = [\hat{X} \cup H(\hat{X}), \hat{E}]$ missä $\hat{E} = \{\{x, y\} \in E : x \in \hat{X}, y \in H(\hat{X})\}$. Mutta oletus " $|A| \leq |H(A)|$ kaikilla $A \subset X$ " pätee myös verkossa $G_2 = [(X \setminus \hat{X}) \cup (Y \setminus H(\hat{X})), \{\{x, y\} \in E : x \in X \setminus \hat{X}, y \in Y \setminus H(\hat{X})\}]$ koska jos tämä ehto ei ole voimassa jollakin joukolle $A \subset X \setminus \hat{X}$ niin se ei voi olla voimassa verkossa G joukolla $A \cup \hat{X}$ koska $|H(\hat{X})| = |\hat{X}|$. Induktio-oletuksesta seuraa taas, että verkossa G_2 on täydellinen pariutus M_2 ja $M_1 \cup M_2$ on täydellinen pariutus verkossa G .
- Jos $|H(\hat{X})| \geq |\hat{X}| + 1$ kaikilla $\hat{X} \subset X \setminus \{a\}$ siten, että $\hat{X} \neq \emptyset$. Koska $1 = |\{a\}| \leq |H(\{a\})|$ niin löytyy $b \in Y$ siten, että $\{a, b\} \in E$ ja voimme valita $M_1 = \{\{a, b\}\}$. Ehto " $|A| \leq |H(A)|$ kaikilla $A \subset X$ " on voimassa verkossa $G_2 = [(X \setminus \{a\}) \cup (Y \setminus \{b\}), E \setminus (\{\{a, y\} : y \in Y\} \cup \{\{x, b\} : x \in X\})]$ koska korkeintaan yksi naapuri on poistettu. Induktio-oletuksen nojalla verkossa G_2 on täydellinen pariutus M_2 ja $M_1 \cup M_2$ on taas täydellinen pariutus verkossa G .