MS-A0401 Diskreetin matematiikan perusteet
Yhteenveto ja esimerkkejä ym., osa II

G. Gripenberg

Aalto-yliopisto

20. lokakuuta 2016

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 $\operatorname{mod}(m, n) = j$ jos $0 \leq j < n$ ja $m = j + kn$ missä $k \in \mathbb{Z}$, (mutta $\operatorname{mod}(m, 0) = m$ ja $\operatorname{mod}(m, n) = \operatorname{mod}(m, -n) + n$ jos $n < 0$). Jos m ja n ovat positiivisia lukuja niin $\operatorname{mod}(m, n)$ on jakojäännös joka saadaan kun m jaetaan n:llä mutta jos $m < 0$ niin tämä jakojäännos 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 $a \equiv b \pmod{n}$:

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

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

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

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

Huom!

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

$$a_1 \equiv_n a_2 \quad ja \quad b_1 \equiv_n b_2$$

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 $3 \mid 5742385242417$ *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*

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

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* $[j]_n = [m]_n^{-1}$.
- *Jos* $[m]_n$*:llä on käänteisalkio voidaan jakaa* $[m]_n$*:llä koska se on yhtäpitävää sen kanssa, että kerrotaan* $[j]_n$*:llä.*
- *Jos* $[j]_n = [m]_n^{-1}$ *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* $\text{syt}\,(m,n) = 1$. *Voidaan osoittaa, että myös käänteinen tulos pätee joten*

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

Huom

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

Opiskelijanumero

Eräässä yliopistossa opiskelijanumerot sisältävät kuusi numeroa ja tarkistuskirjaimen. Opiskelija kirjoitti numeronsa muodossa $53x576J$ *missä numero* x *jäi niin suttuisaksi, ettei siitä saanut selvää. Mikä* x *on? Tarkistuskirjain* J *tarkoittaa, että kun* J*:tä edeltävien numeroiden muodostama luku jaetaan* 23*:lla niin jakojäännös on* 9*. Voimme kirjoittaa luvun* $53x576$ *muodossa* $530\,576 + x \cdot 1\,000$ *ja silloin saamme annettujen tietojen avulla*

$$[9]_{23} = [530\,576 + x \cdot 1\,000]_{23} = [530\,576]_{23} + [x]_{23} \cdot [1\,000]_{23} = [12]_{23} + [x]_{23} \cdot [11]_{23},$$

koska $\operatorname{mod}(530\,576, 23) = 12$ *ja* $\operatorname{mod}(1\,000, 23) = 11$*. Tästä seuraa, että* $[x]_{23} \cdot [11]_{23} = [-3]_{23}$ *ja koska* $[11]_{23}^{-1} = [21]_{23}$ *koska* $\operatorname{mod}(21 \cdot 11, 23) = \operatorname{mod}(231, 23) = 1$ *joten*

$$[x]_{23} = [-3]_{23} \cdot [11]_{23}^{-1} = [-3]_{23} \cdot [21]_{23} = [-63]_{23} = [-63 + 3 \cdot 23]_{23} = [6]_{23},$$

ja voimme päätellä, että $x = 6$ *koska* $0 \leq x \leq 9$*.*

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

- *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* $r_{j-1} > 0$*.*
- $\operatorname{syt}(m, n) = r_{k-1}$ *jos* $r_k = 0$*.*

Miksi Eukleideen algoritmi toimii?

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

Eukleideen algoritmi

Kun laskemme $\operatorname{syt}(634, 36)$*:n Eukleideen algoritmin avulla saamme seuraavat tulokset:*

$$\begin{aligned} 634 &= 17 \cdot 36 + 22 \\ 36 &= 1 \cdot 22 + 14 \\ 22 &= 1 \cdot 14 + 8 \\ 14 &= 1 \cdot 8 + 6 \\ 8 &= 1 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

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

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* $j = 2, \ldots, k$ *kaavalla* $r_{j-2} = q_j r_{j-1} + r_j$ *kunnes* $r_k = 0$, *jolloin* $r_{k-1} = \operatorname{syt}(m, n)$ *niin voidaan laskea takaperin lähtien yhtälöstä* $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ *joka voidaan kirjoittaa muotoon*

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

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* $\operatorname{syt}(m, n) = a_j r_j + b_j r_{j+1}$ *kaikilla* $j = k - 2, k - 1, \ldots, 0$, *eli lopuksi*

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

missä $a = a_0$ *ja* b_0.
Jos nyt $\operatorname{syt}(m, n) = 1$ *niin*

$$\begin{aligned} [a]_n \cdot [m]_n = [1]_n \quad \textit{eli} \quad [a]_n = [m]_n^{-1}, \\ [b]_m \cdot [n]_m = [1]_m \quad \textit{eli} \quad [b]_m = [n]_m^{-1}. \end{aligned}$$

Jäännösluokan käänteisalkio

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

$$\begin{aligned} 67 &= 2 \cdot 23 + 21 \\ 23 &= 1 \cdot 21 + 2 \\ 21 &= 10 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

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

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

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?

Oletamme, että m *ei ole* p*:llä jaollinen. Silloin pätee* $\text{syt}\,(p, m) = 1$ *koska* p *on alkuluku. 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 syt (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 $r_K = 0$ ja silloin $r_{K-1} = \text{syt}(m, n)$. Tähän tarvitaan $K - 1$ jakolaskua. Meidän pitää siis arvioida miten iso K voi olla ja tätä varten valitsemme $x_1 = 1$, $x_2 = 2$ ja

$$x_{j+2} = x_{j+1} + x_j, \quad j \geq 1. \tag{$\star$}$$

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

$$r_{K-(j+1)} = q_{K-j+1} r_{K-j} + r_{K-j+1} \geq r_{K-j} + r_{K-j+1} \geq x_j + x_{j-1} = x_{j+1}.$$

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

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

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

josta seuraa, että

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

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

Eulerin φ-funktio

$\varphi(n) =$ *alkioiden lukumäärä joukossa*

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

$=$ *niiden joukon* $\mathbb{Z}/n\mathbb{Z}$ *alkioiden 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 `@(n)sum(gcd(0:n-1,n)==1)`*.*

Eulerin lause

Jos $\operatorname{syt}(a,n) = 1$ *ja* $n > 1$ *niin*

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

Eulerin lause, todistus

Oletamme, että $[x_1]_n, \ldots, [x_{\varphi(n)}]$ *ovat* $\mathbb{Z}/n\mathbb{Z}$*:n alkiot joilla on käänteisalkio eli ovat kääntyviä. Koska* $\operatorname{syt}(a,n) = 1$ *niin myös* $[a]_n$ *on kääntyvä ja koska* $[\alpha]_n \cdot [\beta]_n$ *on kääntyvä jos* $[\alpha]_n$ *ja* $[\beta]_n$ *ovat kääntyviä, niin* $[a]_n \cdot [x_j]$ *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 alkiot* $[a]_n \cdot [x_1]_n, \ldots [a]_n \cdot [x_{\varphi(n)}]_n$ *ovat samat kuin alkiot* $[x_1]_n, \ldots, [x_{\varphi(n)}]$ *mutta mahdollisesti eri järjestyksessä. Mutta tulot ovat samat, eli*

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

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

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 $\{ k \in \mathbb{Z} : 0 \leq k < p \cdot q, \operatorname{syt}(k, p \cdot q) \neq 1 \}$ on $\{0\} \cup \{q, 2 \cdot q, \ldots (p-1) \cdot q\} \cup \{p, 2 \cdot p, \ldots (q-1) \cdot p\}$ ja tässä joukossa on $1 + (p-1) + (q-1)$ alkiota. Koska joukossa $\{0, 1, 2, \ldots, p \cdot q - 1\}$ on $p \cdot q$ alkiota niin $\varphi(p \cdot q) = p \cdot q - \big(1 + (p-1) + (q-1)\big) = (p-1) \cdot (q-1)$.

Fermat'n pieni lause

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

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

RSA-algoritmi

RSA-algoritmissa käytetään julkista avainta (n, k) viestin kryptaamiseen eli salaamiseen ja yksityistä avainta (n, d) kryptatun viestin purkamiseen:

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

Menetelmä perustuu siihen, että julkisen avaimen avulla on (pitää olla) ylivoimaisen vaikeata määrittää yksityistä avainta 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* $\operatorname{syt}(k, m) = 1$ *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* $\operatorname{syt}(a, n) = 1$.
- $\varphi(n) = \varphi(p \cdot q) = (p-1) \cdot (q-1) = m$.
- *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 $\operatorname{mod}(b^d, n) = \operatorname{mod}(a, n) = a$.

RSA-algoritmi

Jos RSA-algoritmilla ja julkisella avaimella $(55, 23)$ *haluamme salata viestin* 9 *niin meidän pitää laskea* $\operatorname{mod}(9^{23}, 55)$. *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*

$$\operatorname{mod}(9^2, 55) = \operatorname{mod}(81, 55) = 26,$$
$$\operatorname{mod}(9^3, 55) = \operatorname{mod}(26 \cdot 9, 55) = \operatorname{mod}(234, 55) = 14$$
$$\operatorname{mod}(9^4, 55) = \operatorname{mod}(26^2, 55) = \operatorname{mod}(676, 55) = 16,$$
$$\operatorname{mod}(9^7, 55) = \operatorname{mod}(16 \cdot 14, 55) = \operatorname{mod}(224, 55) = 4,$$
$$\operatorname{mod}(9^8, 55) = \operatorname{mod}(16^2, 55) = \operatorname{mod}(256, 55) = 36,$$
$$\operatorname{mod}(9^{16}, 55) = \operatorname{mod}(36^2, 55) = \operatorname{mod}((-19)^2, 55) = \operatorname{mod}(361, 55) = 31,$$
$$\operatorname{mod}(9^{23}, 55) = \operatorname{mod}(31 \cdot 4, 55) = \operatorname{mod}(124, 55) = 14,$$

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

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* $\operatorname{mod}(23 \cdot 7, 40) = \operatorname{mod}(161, 40) = 1$. *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*

$$\begin{aligned}
&\operatorname{mod}(14^2, 55) = \operatorname{mod}(196, 55) = 31,\\
&\operatorname{mod}(14^3, 55) = \operatorname{mod}(14^2 \cdot 14, 55)\\
&\qquad = \operatorname{mod}(31 \cdot 14, 55) = \operatorname{mod}(434, 55) = 49,\\
&\operatorname{mod}(14^4, 55) = \operatorname{mod}(31^2, 55) = \operatorname{mod}(961, 55) = 26,\\
&\operatorname{mod}(14^7, 55) = \operatorname{mod}(14^4 \cdot 14^2 \cdot 14, 55) = \operatorname{mod}(26 \cdot 49, 55)\\
&\qquad = \operatorname{mod}(26 \cdot (-6), 55) = \operatorname{mod}(-156, 55) = 9,
\end{aligned}$$

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

Miksi RSA-algortimi toimii jos $\operatorname{syt}(a, n) \neq 1$?

- *Koska oletamme, että* $0 < a < n$ *niin* $\operatorname{syt}(a, n) \neq 1$ *ainoastaan jos* $p \mid a$ *tai* $q \mid a$. *Oletamme seuraavaksi, että* $p \mid a$ *joten* $a = p^j \cdot c$ *missä* $\operatorname{syt}(c, n) = 1$.
- *Nyt* $[b^d]_n = [((p^j \cdot c)^k)^d]_n = [(p^k)^d]_n^j \cdot [(c^k)^d]_n$ *ja koska* $\operatorname{syt}(c, n) = 1$ *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* $\operatorname{syt}(p, q) = 1$ *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:

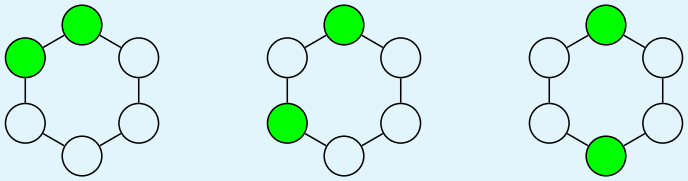
- *A laskee tiivisteen eli hajautusarvon $h(a)$ viestistä a.*
- *A salaa viestin a B:n julkisella avaimella (n_B, k_B) salatuksi viestiksi $b = \mathrm{mod}\,(a^{k_B}, n_B)$.*
- *A salaa tiivisteen $h(a)$ omalla yksityisellä avaimellaan (n_A, d_A) allekirjotukseksi $s = \mathrm{mod}\,(h(a)^{d_A}, n_A)$.*
- *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 vihreiksi ja muut valkoisiksi?

- *Jos pallot ovat identtiset on vain yksi tapa, 2 väritetään vihreiksi ja 4 valkoisiksi.*
- *Jos pallot on numeroitu niin on $\binom{6}{2} = 15$ tapaa valita ne, jotka väritetään vihreiksi ja loput valkoisiksi.*
- *Jos pallot ovat säännöllisen 6-kulmion kulmissa ja tätä 6-kulmiota voi kiertää ja 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 bentseenimolekyylin vetyatomia on korvattu metyyliryhmillä.

Ryhmät

Ryhmä on pari $[G, \bullet]$ missä G on joukko ja $\bullet$ on binäärinen operaatio G:ssä eli funktio $G \times G \to G$, jolla on seuraavat ominaisuudet:

- *Sulkeutuneisuus: $a \bullet b \in G$ jos a ja $b \in G$.* *(Seuraus oletuksesta, että $\bullet : G \times G \to G$ on funktio.)*
- *Assosiatiivisuus: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ 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.*
- *Merkinnän $a \bullet b$ (tai $\bullet(a, b)$) sijasta kirjoitetaan usein ab. Neutraalialkiota merkitään myös 1:llä tai I:llä. Lisäksi $a^0 = e$, $a^m = \underbrace{a \bullet a \bullet \ldots \bullet a}_{m}$ ja $a^{-m} = (a^{-1})^m$ kun $m > 0$.*

Esimerkkejä ryhmistä $[G, \bullet]$

- *$G = \mathbb{Z}$ ja $\bullet = +$ jolloin neutraalialkio on 0 ja n:n käänteisalkio on $-n$.*
- *$G = (0, \infty)$ (eli $]0, \infty[$) 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.*
- *$G = \{ A : A$ on $n \times n$-matriisi ja $\det(A) \neq 0 \}$ ja $\bullet$ on matriisien kertolasku. Neutraalialkio on yksikkömatriisi ja käänteisalkio on käänteismatriisi. Tämä ryhmä ei ole kommutatiivinen kun $n \geq 2$.*
- *$G = \{ f : f$ on bijektio: $X \to X \}$ 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 : $G_1 \to G_2$.

- *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).*

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 $\langle a \rangle = \{ a^j : j \in Z \}$ on a:n generoima G:n syklinen aliryhmä.*
- *Kaikki sykliset ryhmät, joissa on m alkiota ovat isomorfiset ja 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 $\psi :]0, \infty[\to \mathbb{R}$ 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 $[\mathbb{Z}/17\mathbb{Z} \setminus \{[0]_{17}\}, \cdot]$ on syklinen ryhmä koska jos esimerkiksi $a = [3]_{17}$ niin $\{ a^j : j = 1, 2, \ldots, 16 \} = \mathbb{Z}/17\mathbb{Z} \setminus \{[0]_{17}\}$. Jäännösluokka $[13]_{17}$ taas generoi syklisen aliryhmän $[\{[1]_{17}, [13]_{17}, [16]_{17}, [4]_{17}\}, \cdot]$.

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 $\psi : G \to G'$ 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 $G \to G'$ 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 $\psi : G \to G/H$ 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 $A \to A$.*

- *Kaikki joukon A permutaatiot muodostavat ryhmän kun ryhmäoperaatio on funktioiden yhdistäminen. Kaikki m-alkioisten joukkojen kaikkien permutaatioiden muodostamat ryhmät ovat isomorfiset ja 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 joukot $\{\alpha^j(a) : j \in \mathbb{Z}\}$ eli ekvivalenssiluokat kun ekvivalenssirelaationa on $x \sim y$ jos ja vain jos $y = \alpha^j(x)$ jollain $j \in \mathbb{Z}$.*
- **Sykli** *on A:n permutaatio α jolle pätee $\alpha(x_j) = x_{j+1}$, $j = 1, 2, \ldots, k-1$ ja $\alpha(x_k) = x_1$ missä $x_1, x_2, \ldots, x_k \in A$ ja $\alpha(x) = x$ kaikilla $x \in A \setminus \{x_1, \ldots, x_k\}$.* **Syklimerkinnöillä** *kirjoitetaan $\alpha = \begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}$. Tällaisen syklin α* **pituus** *on k ja sanotaan, että α on k-sykli. Syklin α radat ovat $\{x_1, x_2, \ldots, x_k\}$ ja joukot $\{x\}$ kaikilla $x \in A \setminus \{x_1, \ldots, x_k\}$.*
- *Jos α on permutaatio niin jokaista sen rataa vastaa sykli ja α voidaan esittää näiden syklien tulona (eli yhdistettynä funktiona).*

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 $\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ 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 $\beta_3 = \begin{pmatrix} 6 & 7 \end{pmatrix}$. Syklinotaatiolla voimme nyt kirjoittaa

$$\alpha = \beta_1\beta_3 = \begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}\begin{pmatrix} 6 & 7 \end{pmatrix},$$

koska β_2 on identiteettifunktio. Mutta on myös muita esitystapoja syklien tuloina, esim. $\alpha = \begin{pmatrix} 7 & 6 \end{pmatrix}\begin{pmatrix} 4 & 3 & 1 & 2 \end{pmatrix}$.
Joukot $A_1 = \{1, 2, 4, 3\}$, $A_2 = \{5\}$ ja $A_3 = \{6, 7\}$ ovat permutaation α radat.

Parilliset ja parittomat permutaatiot

- *Jokainen sykli, jonka pituus on $k \geq 2$ voidaan kirjoittaa $k-1$:n 2-syklin tulona koska*
  $(x_1 \quad x_2 \quad \ldots \quad x_k) = (x_1 \quad x_k)\,(x_1 \quad x_{k-1}) \ldots (x_1 \quad x_3)\,(x_1 \quad x_2)$.
- *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* $\operatorname{sign}(\alpha) = (-1)^r$.
- *Jos α on sykli, jonka pituus on k niin* $\operatorname{sign}(\alpha) = (-1)^{k+1}$.
- *Jos α on n-alkioisen joukon permutaatio ja α:lla on m rataa niin* $\operatorname{sign}(\alpha) = (-1)^{n-m}$.
- *Permutaation α on* **parillinen** *jos* $\operatorname{sign}(\alpha) = 1$ *ja muuten* **pariton**.
- *Jos α ja β ovat saman joukon permutaatioita niin* $\operatorname{sign}(\alpha\beta) = \operatorname{sign}(\alpha)\operatorname{sign}(\beta)$.

Sykli-indeksi

- *Jos a on joukon X permutaatio niin a:n* **sykli-indeksi** *on monomi*

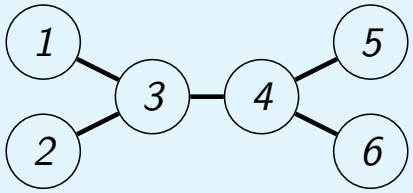
$$\zeta_{a,X}(t_1, \ldots, t_n) = t_1^{j_1} \cdot t_2^{j_2} \cdot \ldots \cdot t_n^{j_n}$$

  missä j_k on a:n k-pituisten ratojen lukumäärä.
- *Jos G on ryhmä joukon X permutaatiota niin G:n* **sykli-indeksi** *on*

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

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

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

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 $x(f \diamond g) = (xf)g$ 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 homomorfismiominaisuudeksi 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).

Ryhmän toiminta ja "väritykset"

Oletetaan, että ryhmä G toimii joukossa X. Joukon X väritys on funktio $\omega : X \to K$ 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 $\Omega \subseteq K^X$ 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 $\omega \sim \eta$ jos ja vain jos $\omega = a\eta$ jollakin $a \in G$ ja silloin näitä värityksiä pidetään samoina. Näin ollen G:n toiminnan suhteen "erilaisten" väritysten lukumäärä on sama kuin ekvivalenssiluokkien lukumäärä.

Pólyan "väritys"-lause

Olkoon G ryhmä joukon X permutaatioita ja olkoon $K = \{v_1, v_2, \ldots, v_r\}$ joukko "värejä", joilla X:n alkioita väritetään. Silloin termin

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

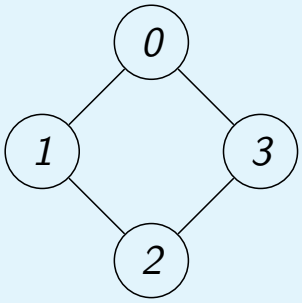
kerroin polynomissa

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

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 $\zeta_{G,X}(r, r, \ldots, r)$ 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 alkiota 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
$\alpha(1) = \mod(\alpha(0) + 1, 4)$ *tai* $\mod(\alpha(0) - 1, 4)$. *Koska $\alpha(2)$ ei saa olla $\alpha(0)$:n naapuri niin $\alpha(2) = \mod(\alpha(0) + 2, 4)$ ja samoin*
$\alpha(3) = \mod(\alpha(1) + 2, 4)$.
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 (tai D_8:lla).

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 $t_1^{j_1} t_2^{j_1} \dots t_n^{j_n}$ jos permutaatiolla on j_k rataa, joiden pituus on k, $k = 1, 2, \dots, n$. Tässä tapauksessa sykli-indeksiksi tulee

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

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

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

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) sekä 1 rata johon kuuluu 1 ruutu.

Pólyan lause ja ristinolla, jatk.

Sykli-indeksiksi saamme näin ollen

$$\zeta_{G,X}(t_1, t_2, \ldots, t_9) = \frac{1}{4}\left(t_1^9 + 2t_1 t_4^2 + t_1 t_2^4\right).$$

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**. *Termin $x^2o^2t^5$ kerroin lausekkeessa $(x+o+t)^9$ on $\binom{9}{2,2,5}$, lausekkeesta $2(x+o+t)(x^4+o^4+t^4)^2$ ei tule yhtään $x^2o^2t^5$-termiä ja termin $x^2o^2t^5$ kerroin lausekkeessa $(x+o+t)(x^2+o^2+t^2)^2$ on termin $x^2o^2t^4$ kerroin lausekkeessa $(x^2+o^2+t^2)^2$ eli $\binom{4}{1,1,2}$. Vaihtoehtojen lukumääräksi tulee siis*

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

Radat ja kiinnittäjäaliryhmät

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

- *Jos $x \in X$ niin sen* **rata** *G:n toiminnassa on joukko $Gx = \{ ax : a \in G \} \subseteq X$.*
- *Jos $x \in X$ niin sen* **rata** *alkion $a \in G$ toiminnassa on joukko $\langle a \rangle x = \{ a^j x : j \in \mathbb{Z} \} \subseteq X$.* *($\langle a \rangle$ 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, Gx 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 Gx *on*

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

ja kiintopistejoukko X_a *on*

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

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

Permutaation generoima syklinen ryhmä

Olkoon $\alpha = \beta_1 \beta_2 \dots \beta_k$ *joukon* X *permutaatio, missä sykleillä* β_j, $j = 1, \dots k$ *ei ole yhteisiä alkoita ja missä syklin* β_j *pituus on* b_j *ja olkoon* G *permutaation* α *generoima syklinen ryhmä. Silloin*

- β_j^r *on identiteetti funktio jos ja vain jos* $b_j \mid r$.
- α*:n generoiman syklisen ryhmän alkioiden lukumäärä* $|G|$ *on lukujen* $b_1, b_2, \dots, b_k$ *pienin yhteinen jaettava koska* $|G|$ *on pienin positiivinen luku* q *siten, että* α^q *on identiteettifunktio (eli sama kuin* α^0*).*
- *Jos* $\beta_j = (x_1\ x_2\ \dots\ x_{b_j})$ *ja* $1 \le i \le b_j$ *niin* $\beta_j^m x_i = \alpha^m x_i = x_i$ *kun* $0 \le m < |G|$ *jos ja vain jos* $b_j \mid m$, *josta seuraa, että kiinnittäjäaliryhmä* G_{x_i} *on*

$$G_{x_i} = \{\, \alpha^m : m = 0, b_j, 2 \cdot b_j, \dots, (\tfrac{|G|}{b_j} - 1) \cdot b_j \,\}.$$

Miksi $|G_x| \cdot |Gx| = |G|$?

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 alkiota kuin H:ssa ja niiden unioni on G). Koska G_x on G:n aliryhmä niin valitsemme $H = G_x$ ja konstruoimme bijektion ψ aliryhmän G_x sivuluokkien joukosta rataan Gx jolloin osoitamme, että $m = |Gx|$ josta seuraa, että $|G| = |G_x| \cdot |Gx|$.
Määrittelemme $\psi(aG_x) = ax$. Jos $a_1 G_x = a_2 G_x$ niin pätee $a_2^{-1} a_1 \in G_x$ joten $a_2^{-1} a_1 x = x$ eli $a_1 x = a_2 x$ joten ψ on hyvin määritelty.
Jos $a_1 x = a_2 x$ niin pätee $a_2^{-1} a_1 x = x$ joten $a_2^{-1} a_1 \in G_x$, josta seuraa, että $a_1 G_x = a_2 G_x$ 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.

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

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

Ratojen lukumäärä ryhmän toiminnassa värityksillä

Erityisesti, jos ryhmä G toimii joukon X värityksillä, niin G:n toiminnan suhteen erilaisten väritysten lukumäärä eli ratojen lukumäärä 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.

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*

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

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* $X = \cup_{R\in X/G} R$.
Koska $|G_x| = \frac{|G|}{|Gx|}$ *ja* Gx *on rata, johon alkio* x *kuuluu niin saamme väitteemme seuraavan laskun avulla:*

$$\sum_{a\in G}|X_a| = \sum_{x\in X}|G_x| = \sum_{R\in X/G}\sum_{x\in R}|G_x| = \sum_{R\in X/G}\sum_{x\in R}\frac{|G|}{|Gx|}$$

$$= |G|\sum_{R\in X/G}\sum_{x\in R}\frac{1}{|R|} = |G|\sum_{R\in X/G}\frac{1}{|R|}\sum_{x\in R}1 = |G|\sum_{R\in X/G}1 = |G|\cdot|X/G|.$$

Mitkä väritykset ovat invariantteja ryhmäalkion a toiminnassa?

Oletetaan, että G *on ryhmä joukon* X *permutaatioita,* $a \in G$ *ja* X*:n radat* a*:n toiminnassa ovat* $R_{a,1}, R_{a,2}, \ldots, R_{a,m_a}$.
Jos ω *on* X*:n väritys (eli funktio:* $X \to K$ *missä* K *on joukko värejä) niin* $a\omega = \omega$ *jos ja vain jos* ω *on vakio jokaisella radalla* $R_{a,j}$, $j = 1, \ldots, m_a$.

Miksi?

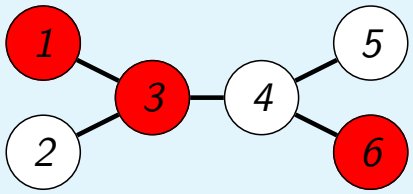
Koska $a\omega = \omega$ *niin pätee* $a^j\omega = \omega$ *kaikilla* $j \in \mathbb{Z}$. *Jos nyt* x *ja* y *kuuluvat samaan rataan* a*:n toiminnassa niin on olemassa luku* j *siten, että* $a^j x = y$ *eli* $a^{-j}y = x$. *Alkion* $a \in G$ *toiminnan määritelmän* $((a\omega)(x) = \omega(a^{-1}x))$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

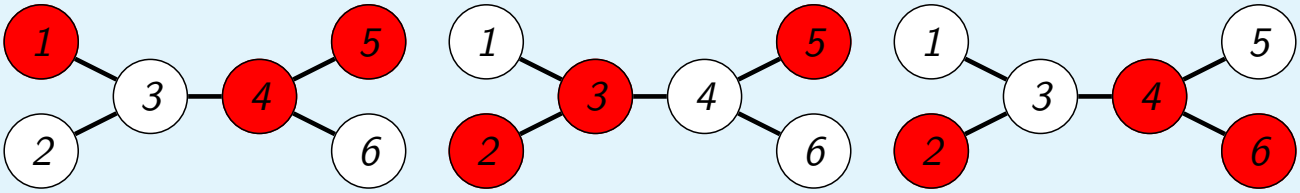
Alla olevan verkon solmut on väritetty värityksellä ω_0 *missä* $\omega_0(1) = p$, $\omega_0(2) = v$, $\omega_0(3) = p$, $\omega_0(4) = v$, $\omega_0(5) = v$ *ja* $\omega_0(6) = p$*:*



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:*

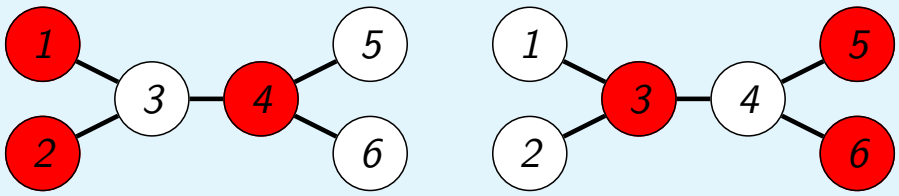


Esimerkki: Permutaation toiminta värityksillä, jatk.

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 lemman 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_2t_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^3v^3*-termiä eli* p^3v^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* $\{4\}$ *alkiot 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* $(p+v)^2(p^2+v^2)^2 = v^6 + 2\,p\,v^5 + 3\,p^2\,v^4 + 4\,p^3\,v^3 + 3\,p^4\,v^2 + 2\,p^5\,v + p^6$. *Ryhmän* G *sykli-indeksi on* $\zeta_{G,V}(t_1,t_2,t_4) = \frac{1}{8}\left(t_1^6 + t_1^2 t_2^2 + 2t_1^4 t_2 + 2t_2^3 + 2t_2 t_4\right)$ *ja termin* $p^3 v^3$ *kerroin polynomissa* $\zeta_{G,V}(p+v, p^2+v^2, p^4+v^4)$ *on*

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

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* $E \subseteq \{\,\{a,b\} : a, b \in V\,\}$ *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.*

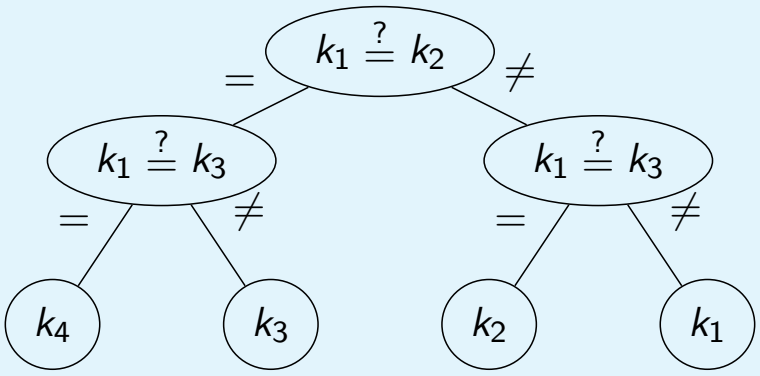
Useimmiten V*:n alkioiden lukumäärä on positiivinen mutta äärellinen.*

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:



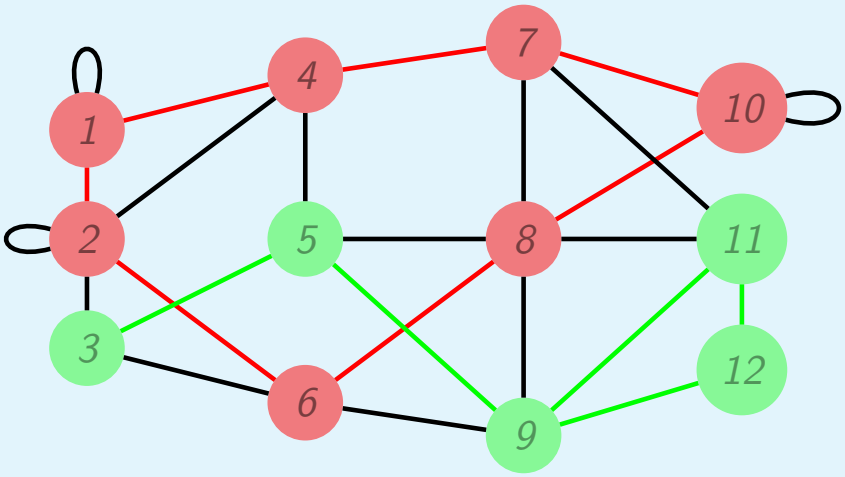
Tässä verkon kaareilla on määritelty funktio, jonka maalijoukko on $\{=, \neq\}$.

Määritelmiä

- *Verkon* $[V, E]$ **polku** *(solmusta* v_0 *solmuun* v_n*) on jono* $[v_0, v_1, \ldots, v_n]$ *missä* $v_j \in V$, $j = 0, 1, \ldots, n$ *ja jokaisella* $j = 1, \ldots, n$ *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* $[v_0, v_1, \ldots, v_n]$ **pituus** *on* n.
- *Verkon* $[V, E]$ **sykli** *(tai kierros) on sen polku* $[v_0, v_1, \ldots, v_n]$ *missä* $v_n = v_0$.
- *Polku* $[v_0, v_1, \ldots, v_n]$ *on* **yksinkertainen** *jos* $v_j \neq v_k$, $0 \leq j < k \leq n$.
- *Sykli* $[v_0, v_1, \ldots, v_n]$ *on* **yksinkertainen** *jos* $[v_0, v_1, \ldots, v_{n-1}]$ *on yksinkertainen ja suuntaamattomassa verkossa* $n \neq 2$.
- *Verkon* $[V, E]$ **Eulerin** *polku (tai sykli) on sen polku (tai sykli)* $[v_0, v_1, \ldots, v_n]$, *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)* $[v_0, v_1, \ldots, v_n]$, *jossa* $\{v_0, \ldots, v_n\} = V$ *eli se käy läpi kaikki verkon solmut (syklitapauksessa paitsi* $v_0 = v_n$*) täsmälleen kerran.*

Esimerkki

Alla oleva verkko ei ole yksinkertainen (mutta yhtenäinen, eli jokaisesta solmusta on polku jokaiseen toiseen solmuun).



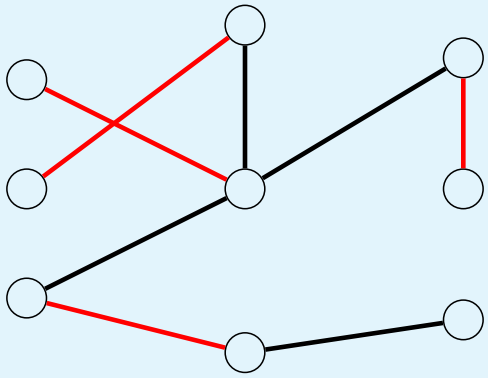
Punaisella on piirretty yksinkertainen sykli $[1, 2, 6, 8, 10, 7, 4, 1]$ *ja vihreällä polku* $[3, 5, 9, 11, 12, 9]$*, joka ei ole yksinkertainen. Solmujono* $[1, 2, 3, 4, 5, 6]$ *ei sen sijaan ole polku koska esimerkiksi* $\{3, 4\}$ *ei ole kaari.*

Määritelmiä, jatk.

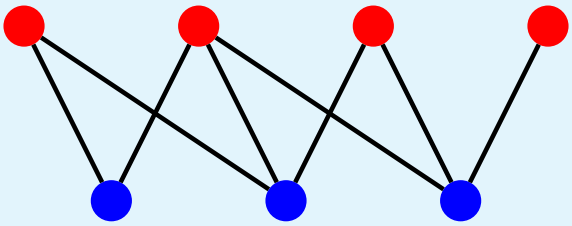
- *Verkko on* **yhtenäinen** *jos jokaisesta solmusta on polku jokaiseen toiseen solmuun.*
- *Verkko on* **puu** *jos se on yksinkertainen ja jokaisesta solmusta on täsmälleen yksi yksinkertainen polku jokaiseen toiseen solmuun.*
- *Verkko on* **metsä** *jos se on yksinkertainen ja jokaisesta solmusta 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* $E \subseteq \{\{x, y\} : x \in X, y \in Y\}$ *(tai* $E \subseteq X \times Y$*).*
- *Verkon* $[V, E]$ **pariutus** *on kaarien osajoukko* $M \subseteq E$ *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* $\omega : V \to K$ *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.*

Esimerkkejä

Alla oleva verkko on puu ja punaiset kaaret muodostavat pariutuksen eikä tähän pariutukseen voida lisätä yhtään kaarta niin, että se pysyy pariutuksena.



Alla oleva verkko on kaksijakoinen jolloin sen kromaattinen luku on 2:



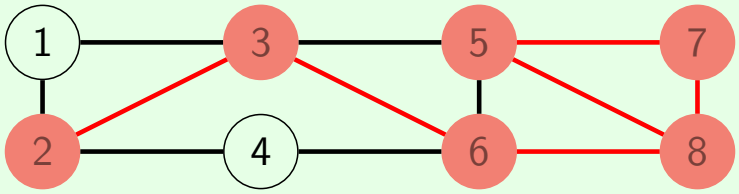
Suuntaamaton verkko on kaksijakoinen jos ja vain jos sen kromaattinen luku on korkeintaan 2

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* $\omega : V \to \{a, b\}$ *on solmujen väritys kahdella värillä niin voimme valita* $X = \{ v \in V : \omega(v) = a \}$ *ja* $Y = \{ v \in V : \omega(v) = b \}$*. Ehdosta* $\{x, y\} \in E \to \omega(x) \neq \omega(y)$ *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* $\{x, y\} = \{y, x\}$*).*

Milloin yhtenäisessä, yksinkertaisessa ja suuntaamattomassa verkossa on Eulerin polku?

Yhtenäisessä, yksinkertaisessa ja suuntaamattomassa verkossa on Eulerin polku jos (ja vain jos) verkossa on 0 tai 2 solmua, joilla on pariton määrä naapureita.
Miksi?

- *Jos verkossa on kaksi solmua, joilla on pariton määrä naapureita valitaan toinen niistä polun ensimmäiseksi solmuksi v_0, muuten valitsemme polun ensimmäisen solmun mielivaltaisesti. Sitten konstruoimme polun siten, että jos polku $[v_0, \ldots, v_k]$ missä $k \geq 0$ on jo konstruoitu niin mikäli on olemassa solmu v_{k+1} siten, että $\{v_k, v_{k+1}\} \in E$ mutta $\{v_k, v_{k+1}\} \notin \{\{v_{j-1}, v_j\} : 1 \leq j \leq k\}$ niin uusi polku on $[v_0, \ldots, v_k, v_{k+1}]$ ja muuten konstruktio on valmis.*
- *Tällä tavalla saamme alla olevassa verkossa polun $[2, 3, 6, 8, 7, 5, 8]$:*

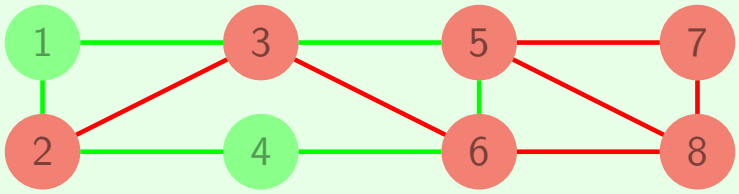


Milloin yhtenäisessä, yksinkertaisessa ja suuntamattomassa verkossa on Eulerin polku? Jatk.

- *Koska polussa esiintyvät kaaret ovat erilaiset niin polun solmujen naapureita voimme laskea seuraavasti: Jos solmu on polussa ensimmäisenä tai viimeisenä niin lisäämme naapureiden lukumäärään 1 ja joka kerta kun solmu esiintyy muuten polussa lisäämme naapureiden lukumäärään 2. Tästä seuraa, että jos ensimmäisellä solmulla on pariton määrä naapureita niin näin on myös viimeisellä solmulla ja muuten polku on sykli. (Tästä seuraa myös "ja vain jos" osa väitteestä.)*
- *Jos kaarien joukosta poistamme ne kaaret, joiden läpi olemme jo käyneet polussa, niin jäljellä on verkko, joiden kaikilla solmuilla on parillinen määrä naapureita. Ja jos jäljellä on kaareja voimme näistä, samalla tavalla kuin edellä, muodostaa syklin, jossa käymme saman kaaren läpi korkeintaan kerran.*

Milloin yhtenäisessä, yksinkertaisessa ja suuntamattomassa verkossa on Eulerin polku? Jatk.

- *Edellisessä esimerkissä saamme tällä tavalla syklin* $[2, 1, 3, 5, 6, 4, 2]$*:*



- *Tällaisen syklin voimme yhdistää jo aikaisemmin muodostettuun polkuun niin, että saamme polun, joka edelleen täyttää ehdon, että käymme jokaisen kaaren läpi korkeintaan kerran. Esimerkissä saamme polun* $[2, 1, 3, 5, 6, 4, 2, 3, 6, 8, 7, 5, 8]$.
- *Näin voimme jatkaa kunnes kaareja ei enää ole jäljellä ja silloin meillä on Eulerin polku.*

Naapurimatriisi

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

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

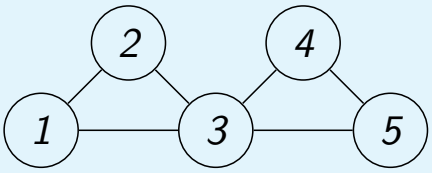
Jos $n \geq 1$ *niin* $(A^n)(j,k)$ *on* n*-pituisten polkujen lukumäärä solmusta* v_j *solmuun* v_k*.*

Huom

Jos verkon kaareille annetaan numeroarvoja eli määritellään funktio $w : E \to \mathbb{R}$*, 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

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

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* $\psi : V \to V'$ *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*

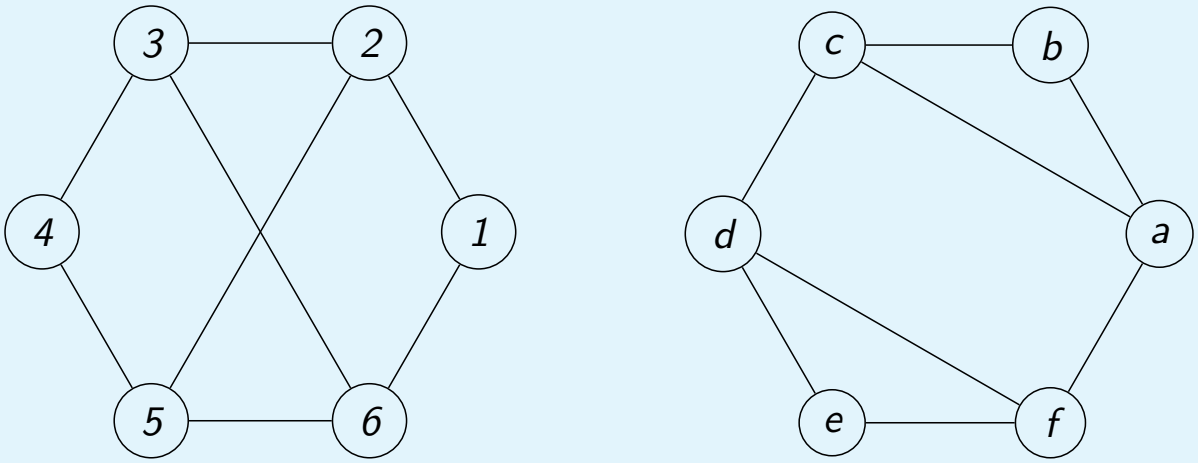
- *on olemassa pariutus* M *siten, että jokainen* $x \in X$ *on jonkin* M*:n kaaren päätepiste eli* M *on ns. kaksijakoisen verkon täydellinen pariutus*

jos ja vain jos

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

Isomorfiset verkot

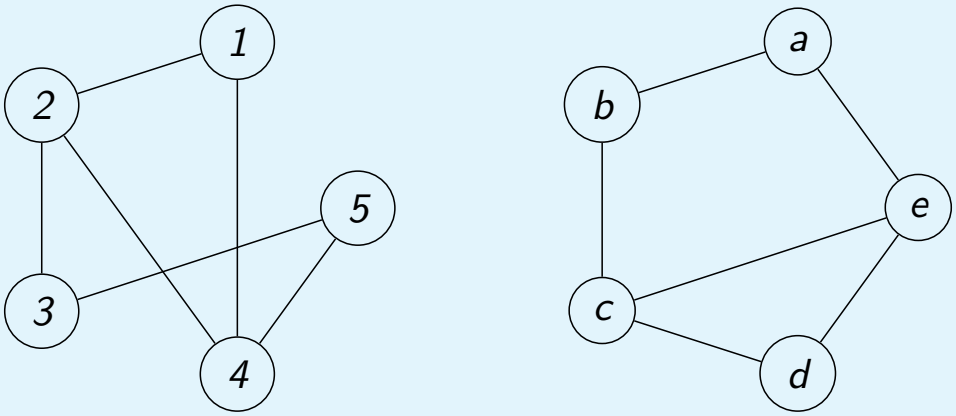
Ovatko alla olevat verkot isomorfiset?



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.

Esimerkki

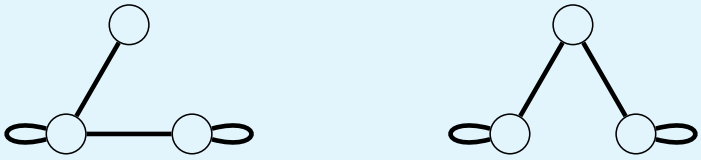
Montako suuntaamatonta verkkoa löytyy, joissa on 3 solmua ja 4 kaarta?

- *Jos vaadimme, että verkko on yksinkertainen niin ei löydy yhtään koska yksinkertaisessa verkossa, jossa on 3 solmua on korkeintaan 3 kaarta.*
- *Naapurimatriisissa on 3 riviä ja saraketta ja koska verkko on suuntaamaton niin tämä matriisi on symmetrinen, eli tiedämme mikä se on jos tunnemme alkiot rivillä i ja sarakkeella j kun $1 \leq i \leq j \leq 3$. Koska verkossa on 4 kaarta niin 4 näistä 6:sta alkiosta ovat 1 ja muut 0. Näin ollen vaihtoehtojen lukumäärä on $\binom{6}{4} = 15$.*
  Mutta osa näistä verkoista ovat tietenkin isomorfisia keskenään.
- *Jos kysymys on ei-isomorfisten verkkojen lukumäärästä, niin voimme tehdä kaikista vaihtoehdoista luettelon. Ensiksi toteamme kuten edellä että ainakin yksi solmu on oma naapurinsa joten meillä on on vaihtoehdot että 1, 2 tai 3 solmua ovat oma naapurinsa. Ensimmäisessä vaihtoehdossa eri solmujen välillä on oltava 3 kaarta, toisessa 2 kaarta ja viimeisessä 1 kaari.*

Esimerkki, jatk.

- *Jos 1 tai 3 solmua ovat oma naapurinsa niin molemmissa tapauksissa meillä on vain yksi vaihtoehto ja ne ovat*

- *Jos 2 solmua ovat oma naapurinsa niin meillä on kaksi ei-isomorfista verkkoa ja ne ovat*



- *Näin ollen on olemassa 4 ei-isomorfista verkkoa, joissa on 3 solmua ja 4 kaarta.*

Esimerkki, jatk.

Entä miten tämä kysymys ratkaistaan Pólyan lauseen avulla?

- *Jos solmujen joukko on* $\{1,2,3\}$ *niin tämän joukon permutaatiot ovat* (1), $(1\ 2)$, $(1\ 3)$, $(2\ 3)$, $(1\ 2\ 3)$ *ja* $(1\ 3\ 2)$.
- *Jotta voimme nähdä miten solmujen permutaatiot toimivat verkoilla esitämme verkot naapurimatriiseinä missä emme välitä lävistäjän alapuolella olevista alkioista:* $\begin{bmatrix} a & b & c \\ & d & e \\ & & f \end{bmatrix}$. *Lisäksi näemme, että verkko jossa on* 4 *kaarta on tällaisen matriisin "väritys" ykkösillä ja nollilla siten, että neljästä alkiosta tehdään* 1 *ja kahdesta* 0.
- *Vaatimus, että naapurit pysyvät naapureina antaa homomorfismin* ψ *solmujen permutaatioista joukon* $\{a,b,c,d,e,f\}$ *permutaatioden ryhmään ja tämä homomorfismi on seuraava:*

Esimerkki, jatk.

- $$\psi((1)) = (a), \qquad \psi((1\ 2)) = (a\ d)(c\ e),$$
$$\psi((1\ 3)) = (a\ f)(b\ e)), \qquad \psi((2\ 3) = (d\ f)(b\ c),$$
$$\psi((1\ 2\ 3)) = (a\ d\ f)(b\ e\ c), \qquad \psi((1\ 3\ 2)) = (a\ f\ d)(b\ c\ e).$$
- *Tästä saamme sykli-indeksiksi*
$$\frac{1}{6}(t_1^6 + 3 \cdot t_1^2 \cdot t_2^2 + 2 \cdot t_3^2).$$
- *Pólyan lauseen mukaan termin* $y^4 n^2$ *kerroin lauseekkeessa* $\frac{1}{6}((y+n)^6 + 3(y+n)^2(y^2+n^2)^2 + 2(y^3+n^3)^2)$ *on ei-isomorfisten verkkojen, joissa on* 3 *solmua ja* 4 *kaarta, lukumäärä ja tämä kerroin on*
$$\frac{1}{6}\left(\binom{6}{4} + 3 \cdot \left(\binom{2}{0} \cdot \binom{2}{1} + \binom{2}{2} \cdot \binom{2}{0}\right) + 0\right)$$
$$= \frac{1}{6}(15 + 3(2+1)) = 4.$$

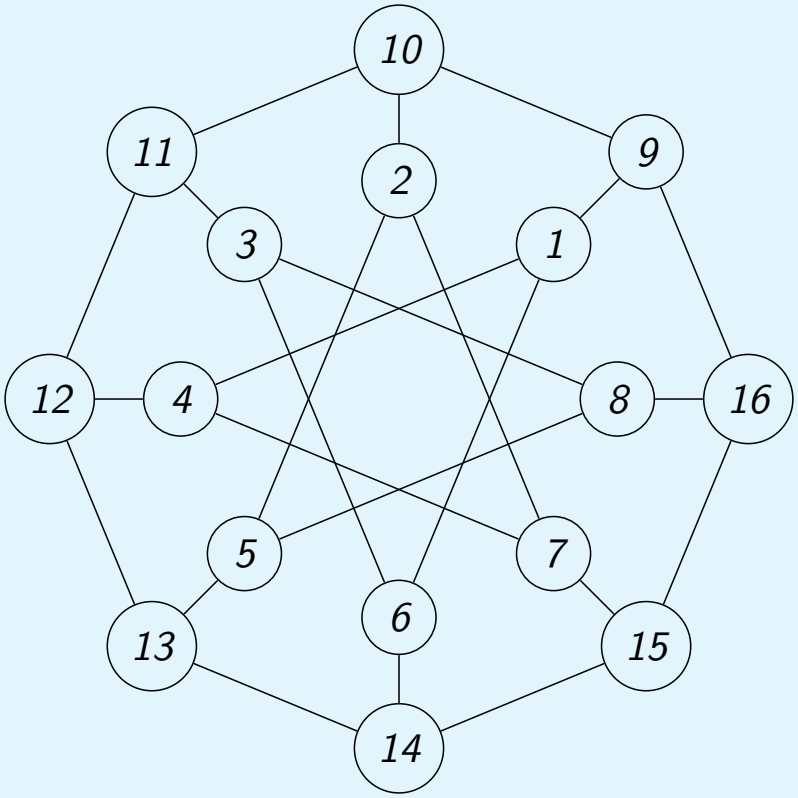
Ahne väritysalgoritmi

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

- *Aseta solmut johonkin järjestykseen:* $[v_1, v_2, \ldots, v_n]$.
- *Aseta värit johonkin järjestykseen:* $[c_1, c_2, \ldots, c_r]$.
- *Väritä ensimmäinen solmu ensimmäisellä värillä, eli* $\omega(v_1) = c_1$.
- *Jos solmut* $v_1, \ldots, v_k$ *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, ... ja otamme solmut järjestyksessä $1, 2, 3, 4, \ldots, 16$ *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 $9, 10, \ldots, 15, 16, 1, 2, 7, 8$ *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.*

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* $[v_0, v_1, \ldots, v_n]$ *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* $s(v) = \min\{\sum_{j=1}^{k} w(\{v_{j-1}, v_j\}) : [v_0, v_1, \ldots, v_k]$ *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 optimaliset 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 $s(v) = \min\{\sum_{j=1}^{k} w(\{v_{j-1}, v_j\} : [v_0, v_1, \ldots, v_k]$ on polku solmusta v_0 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 $[\tilde{v}_0, \tilde{v}_1, \ldots, \tilde{v}_k]$ 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 $[v_0, v_1, \ldots, v_k]$ 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 $O(n^2)$.*

Minimaalinen virittävä puu, ahne algoritmi I (Prim)

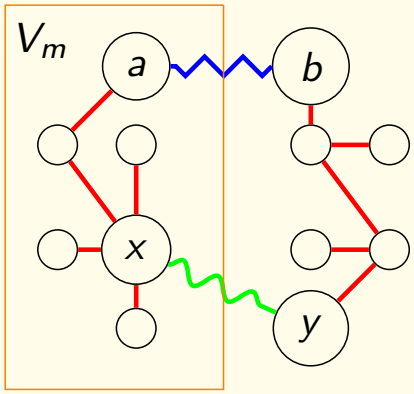
Jos $[V, E]$ on yhtenäinen (suuntaamaton) verkko ja jokaiselle kaarelle $\{v_j, v_k\}$ on annettu paino $w(\{v_j, v_k\})$ (ja $w(\{v_j, v_k\}) = \infty$ jos $\{v_j, v_k\} \notin E$) niin minimaalinen virittävä puu on verkko $[V, E_T]$ missä $E_T \subseteq E$ (eli aliverkko) joka on puu ja sellainen, 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* $T_j = [V_j, E_j]$, $j = 1, \ldots, n$ *(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* $E_m \subseteq E_*$*. 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* T_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

- *Olkoon $[V, E]$ 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 $F_j = [V, E_j]$, $j = 1, \ldots, n$. 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 $[v_0, v_1, \ldots, v_k]$ 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 siten, 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 $E_m \subseteq E_*$ 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 $E_m \cup \{\{a, b\}\} \subseteq E_*$ josta seuraa, että myös $[V, E_m \cup \{\{a, b\}\}]$ on metsä, niin täytyy olla $w(\{x, y\}) = w(\{a, b\})$ eli T_{**} ja $E_{m+1} \subseteq E_{**}$ on myös optimaalinen puu. Toistamalla tarvittaessa tätä päättelyä voimme todeta, että F_n on optimaalinen puu.*

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 $A \subseteq X$ (jolloin siis $H(A)$ on A:n solmujen naapureiden joukko).

- *Jos M on verkon täydellinen pariutus verkossa niin $|A| \leq |H(A)|$ kaikilla $A \subseteq X$ 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 $\hat{X} \subseteq X \setminus \{a\}$ joilla $\hat{X} \neq \emptyset$.*
- *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* $\hat{E} = \{\, \{x, y\} \in E : x \in \hat{X} \,\}$. *Mutta oletus "*$|A| \leq |H(A)|$ *kaikilla* $A \subseteq X$*" 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 joukolla* $A \subseteq X \setminus \hat{X}$ *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.
- *Oletamme seuraavaksi, että* $|H(\hat{X})| \geq |\hat{X}| + 1$ *kaikilla* $\hat{X} \subseteq X \setminus \{a\}$ *joilla* $\hat{X} \neq \emptyset$. *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* $A \subseteq X$*" 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.