MS-A0402 Diskreetin matematiikan perusteet
Esimerkkejä ym., osa II

G. Gripenberg

Aalto-yliopisto

1. huhtikuuta 2015

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*

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

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* $\operatorname{mod}(11031x246, 31) = 18$ *ja tämän tiedon avulla voimme laskea luvun* x *esimerkiksi näin:*
Kirjoitamme $11031x246 = 110310246 + x \cdot 1000$ *jolloin saamme yhtälön*

$$[18]_{31} = [11031x246]_{31} = [110310246]_{31} + [x]_{31} \cdot [1000]_{31}.$$

Koska $\operatorname{mod}(110310246, 31) = 1$ *ja* $\operatorname{mod}(1000, 31) = 8$ *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* $0 \le x \le 9$ *niin* $x = 6$.

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

Jäännösluokan käänteisalkio

Jos haluamme laskea $[23]_{67}^{-1}$*:n niin ensin laskemme* $\operatorname{syt}(67, 23)$*: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 $\operatorname{syt}(67, 23)$*:n lukujen* 67 *ja* 23 *avulla laskemme takaperin :*

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

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?

Oleta, että m ei ole p:llä jaollinen. Silloin pätee $\operatorname{syt}(p, m) = 1$ *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 $\operatorname{syt}(m, n)$ 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 $r_M = 0$ ja silloin $r_{M-1} = \operatorname{syt}(m, n)$. 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

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

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 $j = 1, \ldots, M$.

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

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

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 lause, todistus

Oletamme, että $[x_1]_n, \ldots, [x_{\phi(n)}]$ *ovat* $\mathbb{Z}/n\mathbb{Z}$*:n alkiot joilla on käänteisalkio eli ovat kääntyviä. Koska* 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* $[x_1]_n, \ldots, [x_{\phi(n)}]$ *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* 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*

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

Potenssit joukossa $\mathbb{Z}/p\mathbb{Z}$ kun p on alkuluku

Jos on laskettava $\operatorname{mod}(a^m, p)$ *kun p on alkuluku niin tulos on 0 jos* $\operatorname{syt}(a, p) \neq 1$ *(koska silloin* $\operatorname{syt}(a, p) = p$ *ja $p|a$ koska p on alkuluku) ja muissa tapauksissa voidaan käyttää hyväksi tietoa, että* $a^{p-1} \equiv_p 1$ *koska siitä seuraa, että* $a^m \equiv_p a^{\operatorname{mod}(m, p-1)}$ *mikä voi olla helpommin laskettavissa.*

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

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

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

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

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

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.*
- $G = \{ A : A$ *on* $n \times n$*-matriisi ja* $\det(A) \neq 0 \}$ *ja* $\bullet$ *on matriisien kertolasku. Neutraalialkio on yksikkömatriisi ja käänteeisalkio 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* $|X| \geq 3$.

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 $[\mathbb{Z}/7\mathbb{Z} \setminus \{[0]_7\}, \cdot]$ *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.*

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 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 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.

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*

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

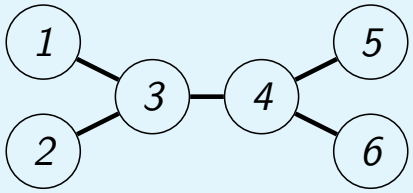
Tässä tapauksessa tulos $|G| = |Gx| \cdot |G_x|$ *ei sano muuta kuin, että* $4 = 2 \cdot 2$.

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.*

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

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

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*

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

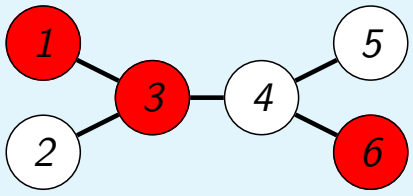
joten $\sum_{a\in G}|X_a| = \sum_{x\in X}|G_x|$.
Merkitsemme ratojen joukkoa X/G*:llä ja ne ovat ekvivalenssiluokkia kun ekvivalenssirelaatio* $\sim$ *on* $x \sim y$ *jos ja vain jos* $x = ay$ *jollain* $a \in G$. *Eri radoilla ei ole yhteisiä alkioita ja ratojen unioni on* X *eli* $X = \cup_{A\in X/G}A$.
Koska $|G_x| = \frac{|G|}{|Gx|}$ *ja* Gx *on rata, johon alkio* x *kuuluu niin saamme väitteemme seuraavan laskun avulla:*

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

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

Esimerkki: Permutaation toiminta värityksillä

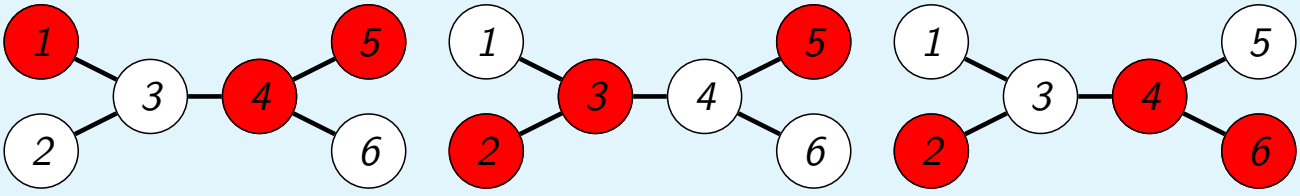
Alla olevan verkon solmut on väritetty värityksellä ω_0 *missä* $\omega(1) = p$, $\omega_0(2) = v$, $\omega_0(3) = p$, $\omega_0(4) = v$, $\omega_0(5) = v$ *ja* $\omega_0(6) = p$*:*



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:*

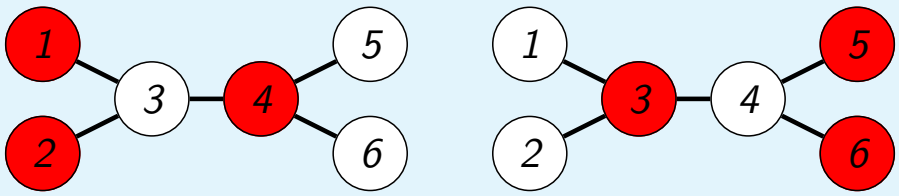


Esimerkki: Permutaation toiminta värityksillä, jatk.

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.

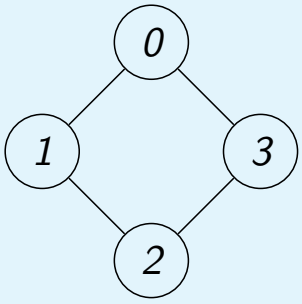
Jos sen sijaan tarkastelemme permutaatiota $a^2 = (1\ 2)(6\ 5)$ niin silloin esimerkiksi seuraavat väritykset kuuluvat joukkoon X_{a^2} koska vaatimus on nyt, että ratojen $\{1,2\}$, $\{5,6\}$, $\{3\}$ ja $\{4\}$ alkiot saavat saman värin:



Näiden väritysten lisäksi kiintopistejoukkoon X_a^2 kuuluu 2 muuta väritystä jolloin $|X_{a^2}| = 4$. Permutaation a^2 sykli-indeksi on $t_1^2t_2^2$ joten tässäkin tapauksessa $|X_{a^2}|$ tulee olemaan termin p^3v^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
$\zeta_{G,V}(t_1,t_2,t_4) = \frac{1}{8}\left(t_1^6+t_1^2t_2^2+2t_1^4t_2+2t_2^3+2t_2t_4\right)$ *ja termin p^3v^3 kerroin polynomissa $\zeta_{G,V}(p+v,p^2+v^2,p^4+v^4)$ on*

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

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

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

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

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

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

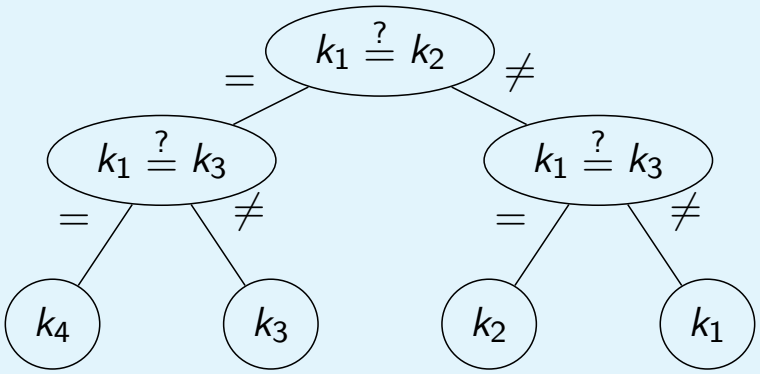
Jotta voisimme laskea ei-ekvivalenttien "väritysten" lukumäärää korvaamme muuttujan t_j *lausekkeella* $x^j + o^j + t^j$ *ja silloin termin* $x^2 o^2 t^5$ *kerroin on ei-ekvivalenttien "väritysten" lukumäärä kun meillä* 2 *kappaletta* **x**, 2 *kappaletta* **o**, *ja* 5 *kappaletta* **t**. *Täksi kertoimeksi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

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:

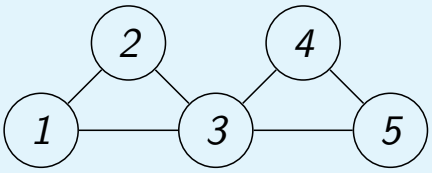


Verkko on kaksijakoinen jos ja vain jos sen kromaattinen luku on korkeintaan 2

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 $\{x, y\} = \{y, x\}$).

Naapurimatriisi

Verkon



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

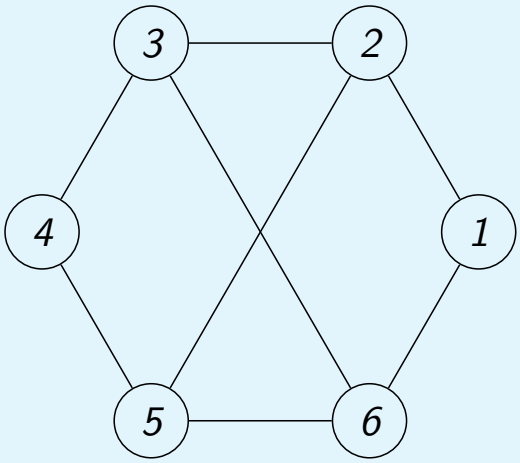
Nyt

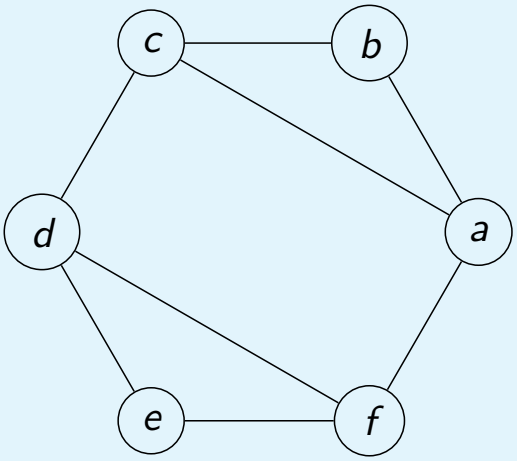
$$A^2 = \begin{bmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 4 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{bmatrix} \quad \textit{ja} \quad A^3 = \begin{bmatrix} 2 & 3 & 5 & 2 & 2 \\ 3 & 2 & 5 & 2 & 2 \\ 5 & 5 & 4 & 5 & 5 \\ 2 & 2 & 5 & 2 & 3 \\ 2 & 2 & 5 & 3 & 2 \end{bmatrix},$$

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

Ovatko alla olevat verkot isomorfiset?

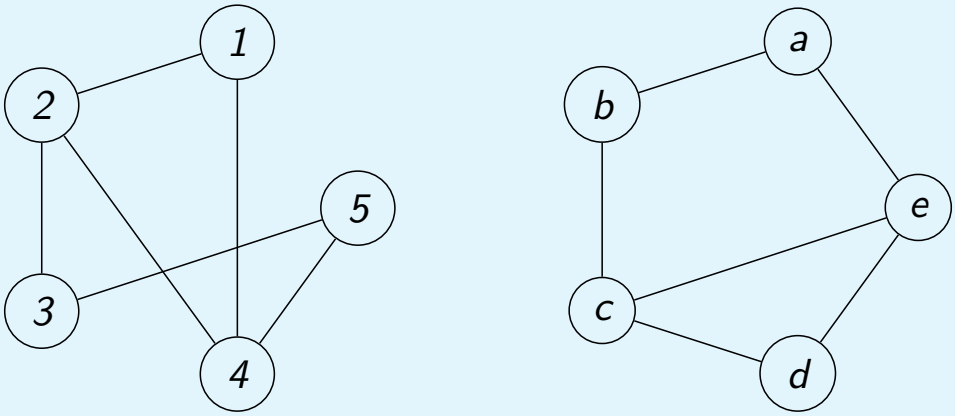




Molemmissa verkoissa on 4 *solmua, joilla on* 3 *naapuria ja* 2 *joilla on* 2 *naapuria, joten tästä emme voi päätellä etteivät verkot olisivat isomorfiset. Sensijaan vasemmanpuoleisessa verkossa ei ole yhtään sykliä, jonka pituus olisi* 3 *mutta sellaisia on oikeanpuoleisessa verkossa. Tästä seuraa,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

Isomorfiset verkot, jatk.

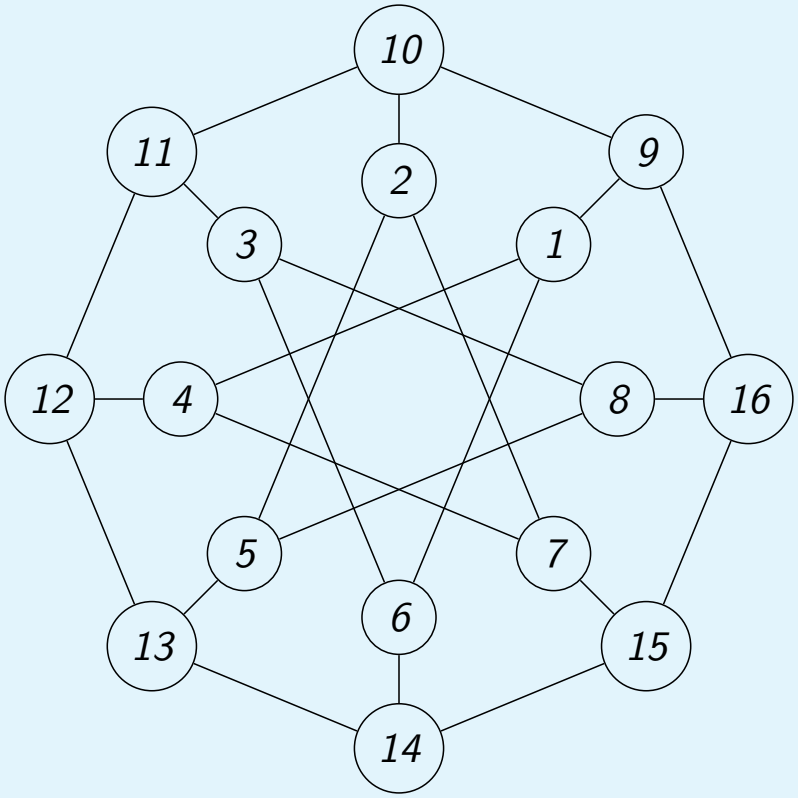
Ovatko alla olevat verkot isomorfiset?



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 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*

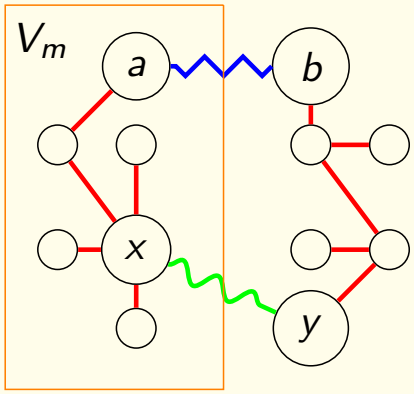
Solmu	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
Väri	*a*	*b*	*a*	*b*	*a*	*b*	*a*	*b*	*b*	*a*	*b*	*a*	*b*	*a*	*b*	*a*

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

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* $E_m \subset E_*$*. 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 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 $F_j = [V, E_j]$, $j = 1, \ldots, n$.*
- *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 $[v_0, v_1, \ldots, v_k]$ 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, 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.*

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* $O(n^2)$.

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*.*