

MS-A0401 Diskreetin matematiikan perusteet

Esimerkkejä ym., osa II

G. Gripenberg

Aalto-yliopisto

14. lokakuuta 2015

- 1 Modulaariaritmetiikka
 - Eukleideen algoritmi
 - RSA-algoritmi
- 2 Ryhmät ja permutaatiot
 - Permutaatiot
 - Sykli-indeksi
 - Pólyan "väritys"-lause
- 3 Verkot
 - Algoritmeja

😊 Esimerkki

Päteekö 3 | 5742385242417 eli jakaako 3 luvun 5742385242417?

Vastaus on kyllä koska luvun numeroiden summa

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

Mutta miksi tämä sääntö pätee?

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

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

💡 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 $530576 + x \cdot 1000$ ja silloin saamme annettujen tietojen avulla

$$\begin{aligned} [9]_{23} &= [530576 + x \cdot 1000]_{23} = [530576]_{23} + [x]_{23} \cdot [1000]_{23} \\ &= [12]_{23} + [x]_{23} \cdot [11]_{23}, \end{aligned}$$

koska $\text{mod}(530576, 23) = 12$ ja $\text{mod}(1000, 23) = 11$. Tästä seuraa, että $[x]_{23} \cdot [11]_{23} = [-3]_{23}$ ja koska $[11]_{23}^{-1} = [21]_{23}$ koska $\text{mod}(21 \cdot 11, 23) = \text{mod}(231, 23) = 1$ 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

Kun laskemme $\text{sy}(634, 36):n$ Eukleideen algoritmin avulla saamme seuraavat tulokset:

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

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

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

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

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

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

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

💡 Jäännösluokan käänteisalkio

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

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

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

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

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

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

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

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

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

😊 Jaollisuustulos

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

Miksi?

Oletamme, että m ei ole p :llä jaollinen. Silloin pätee $\text{sy}(p, m) = 1$ 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.

😊 Eulerin lause, todistus

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

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

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

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

Miksi? Koska p ja q ovat alkulukuja niin joukko

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

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

😊 Fermat'n pieni lause

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

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

💡 RSA-algoritmi

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

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

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

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

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

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

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

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

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

💡 RSA-algoritmi, jatk.

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

Purkamista varten toteamme, että $7 = 4 + 2 + 1 = 2^2 + 2^1 + 2^0$ joten $14^7 = 14^4 \cdot 14^2 \cdot 14$ ja saamme

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

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

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

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

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

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

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

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

- Koska oletamme, että $0 < a < n$ niin $\text{syt}(a, n) \neq 1$ ainoastaan jos $p \mid a$ tai $q \mid a$. Oletamme seuraavaksi, että $p \mid a$ joten $a = p^j \cdot c$ missä $\text{syt}(c, n) = 1$
- Nyt $[b^d]_n = [((p^j \cdot c)^k)^d]_n = [(p^k)^d]_n^j \cdot [(c^k)^d]_n$ ja koska $\text{syt}(c, n) = 1$ 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 $\text{syt}(p, q) = 1$ 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 $-n$.
- $G = (0, \infty)$ (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.
- $G = \{A : A \text{ on } n \times n\text{-matriisi ja } \det(A) \neq 0\}$ ja \bullet on matriisien kertolasku. Neutraalialkio on yksikkömatriisi ja käänteisalkio on käänteismatriisi. Tämä ryhmä ei ole kommutatiivinen kun $n \geq 2$.
- $G = \{f : f \text{ on bijektio: } X \rightarrow X\}$ ja $\bullet = \circ$ eli funktioiden yhdistäminen. Tämä ei ole kommutatiivinen ryhmä jos $|X| \geq 3$.

😊 Esimerkki: Isomorfismi

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

😊 Esimerkki: Syklinen ryhmä

Ryhmä $[\mathbb{Z}/17\mathbb{Z} \setminus \{[0]_{17}\}, \cdot]$ on syklinen ryhmä koska jos esimerkiksi $a = [3]_{17}$ niin $\{a^j : j = 1, 2, \dots, 16\} = \mathbb{Z}/17\mathbb{Z} \setminus \{[0]_{17}\}$. 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.

💡 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

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

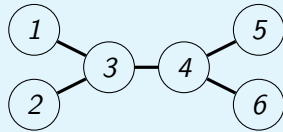
missä siis tämä merkintätapa tarkoittaa, että esim. $\alpha(1) = 2$ ja $\alpha(4) = 3$. Nyt näemme, että $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$ (eli $\alpha(1) = 2, \alpha(2) = 4$ jne.) ja tästä saamme syklin $(1 \ 2 \ 4 \ 3)$ joka siis on permutaatio β_1 jolle pätee $\beta_1(1) = 2, \beta_1(2)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

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

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

💡 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:

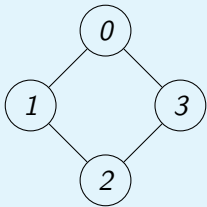
- (1) : 6 rataa, joissa on 1 alkio.
- $(1\ 2), (5\ 6)$: 4 rataa, joissa on 1 alkio, 1 rata, jossa on 2 alkioita.
- $(1\ 2)(5\ 6)$: 2 rataa, joissa on 1 alkio, 2 rataa, joissa on 2 alkioita.
- $(3\ 4)(1\ 5)(2\ 6), (3\ 4)(1\ 6)(2\ 5)$: 3 rataa, joissa on 2 alkioita.
- $(3\ 4)(1\ 5\ 2\ 6), (3\ 4)(1\ 6\ 2\ 5)$: 1 rata, jossa on 2 alkioita, 1 rata, jossa on 4 alkioita.

Näin ollen sykli-indeksi tulee olemaan

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

💡 4-kulmion symmetriat

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



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

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

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

Näiden permutaatioiden muodostama ryhmä on ns. diedriryhmä ja sitä merkitään D_4 :llä (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 $t_1^1 t_2^1 \dots t_n^1$ jos permutaatiolla on j_k rataa, joiden pituus on k , $k = 1, 2, \dots, n$. Tässä tapauksessa sykli-indeksiksi tulee

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

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

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

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

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

😊 Esimerkki: G_x , G_x ja X_a

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

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

rata G_x on

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

ja kiintopistejoukko X_a on

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

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

😊 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 alkoiden 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 $1 \leq i \leq b_j$ niin $\beta_j^m x_i = \alpha^m x_i = x_i$ kun $0 \leq m < |G|$ jos ja vain jos $b_j \mid m$, josta seuraa, että kiinnittäjäaliryhmä G_{x_i} on

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

😊 Miksi $|G_x| \cdot |G_x| = |G|$?

Oletamme, että G on äärellinen ryhmä. Jos H on G :n aliryhmä niin $|H| \cdot m = |G|$ missä m on H :n (esim. vasempien) sivuluokkien lukumäärä (koska kaikissa sivuluokissa on yhtä monta alkioita kuin H :ssa ja niiden unioni on G). Koska G_x on G :n aliryhmä niin valitsemme $H = G_x$ ja konstruoinme bijektio ψ aliryhmän G_x sivuluokkien joukosta rataan G_x jolloin osoitamme, että $m = |G_x|$ josta seuraa, että $|G| = |G_x| \cdot |G_x|$. Määrittelimme $\psi(aG_x) = ax$. Jos $a_1G_x = a_2G_x$ niin pätee $a_2^{-1}a_1 \in G_x$ joten $a_2^{-1}a_1x = x$ eli $a_1x = a_2x$ joten ψ on hyvin määritelty. Jos $a_1x = a_2x$ niin pätee $a_2^{-1}a_1x = x$ joten $a_2^{-1}a_1 \in G_x$, josta seuraa, että $a_1G_x = a_2G_x$ eli ψ on injektio. Jos $y \in G_x$ niin on olemassa $a \in G$ siten, että $y = ax$ ja silloin $y = \psi(aG_x)$ josta seuraa, että ψ on surjektio.

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

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

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

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

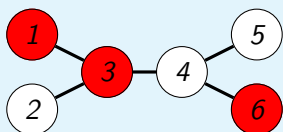
Merkitsemme ratojen joukkoa X/G :llä ja ne ovat ekvivalenssiluokkia kun ekvivalenssirelaatio \sim on $x \sim y$ jos ja vain jos $x = ay$ jollain $a \in G$. Eri radoilla ei ole yhteisiä alkioita ja ratojen unioni on X eli $X = \cup_{R \in X/G} R$.

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

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

💡 Esimerkki: Permutaation toiminta värityksillä

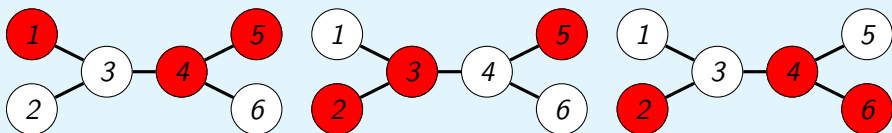
Alla olevan verkon solmut on väritetty värityksellä ω_0 missä $\omega_0(1) = p$, $\omega_0(2) = v$, $\omega_0(3) = p$, $\omega_0(4) = v$, $\omega_0(5) = v$ ja $\omega_0(6) = p$:



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

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

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



💡 Esimerkki: Permutaation toiminta värityksillä, jatk.

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

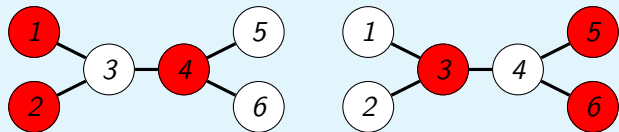
Tässä tapauksessa ei ole kovin hankalaa löytää kaikki ne 5 väritystä, jotka eivät ole ekvivalentteja ja joissa on 3 punaista ja 3 valkoista solmua mutta seuraavaksi määritämme tämän lukumäärän toisella tavalla:

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

Jos nyt a on permutaatio $(3\ 4)(1\ 5\ 2\ 6)$ niin $X_a = \emptyset$ koska ehdosta $a\omega = \omega$ seuraa, että ω saa saman arvon radan $\{3, 4\}$ solmuilla ja saman arvon radan $\{1, 5, 2, 6\}$ solmuilla ja tämä on mahdotonta jos vaaditaan, että solmuista kolme ovat punaisia ja kolme valkoisia. Tämän permutaation sykli-indeksi on t_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 $(p+v)^2(p^2+v^2)^2 = v^6 + 2pv^5 + 3p^2v^4 + 4p^3v^3 + 3p^4v^2 + 2p^5v + p^6$. Ryhmän G sykli-indeksi on

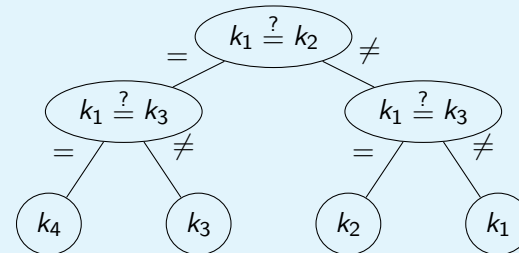
$$\zeta_{G,V}(t_1, t_2, t_4) = \frac{1}{8} (t_1^6 + t_1^2 t_2^2 + 2t_1^4 t_2 + 2t_2^3 + 2t_2 t_4)$$

ja termin $p^3 v^3$ kerroin polynomissa $\zeta_{G,V}(p+v, p^2+v^2, p^4+v^4)$ on

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

😊 Verkko päätösprosessin kuvaajana

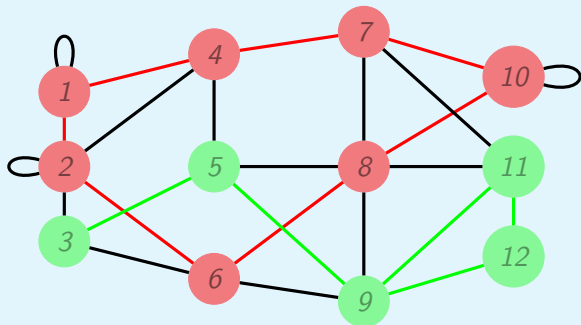
Meillä on neljä kolikkoa, joista tiedämme että yksi on väärennetty, niin että sen paino poikkeaa muiden painosta mutta emme tiedä onko se painavampi vai kevyempi kuin muut. Meillä on varsivaaka, jonka avulla voimme määrittää onko kahdella kolikolla (tai kolikkoparilla, jne.) sama paino vai ei. Seuraava 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 $\{=, \neq\}$.

💡 Esimerkki

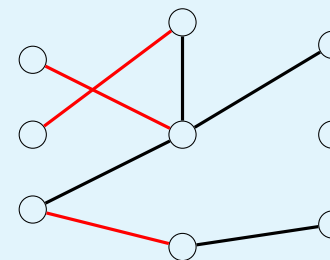
Alla oleva verkko ei ole yksinkertainen (mutta yhtenäinen, eli jokaisesta solmusta on polku jokaiseen toiseen solmuun).



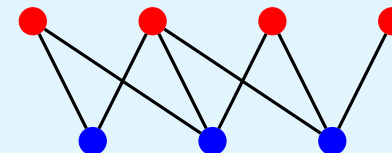
Punaisella on piirretty yksinkertainen sykli $[1, 2, 6, 8, 10, 7, 4, 1]$ ja vihreällä polku $[3, 5, 9, 11, 12, 9]$, joka ei ole yksinkertainen. Solmujono $[1, 2, 3, 4, 5, 6]$ ei sen sijaan ole polku koska esimerkiksi $\{3, 4\}$ ei ole kaari.

💡 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:



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

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

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

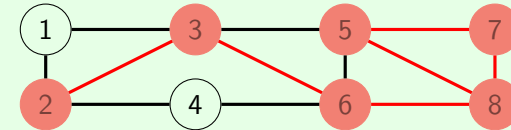
Jos kromaattinen luku on 2, ja $\omega : V \rightarrow \{a, b\}$ on solmujen väritys kahdella värillä niin voimme valita $X = \{v \in V : \omega(v) = a\}$ ja $Y = \{v \in V : \omega(v) = b\}$. Ehdosta $\{x, y\} \in E \rightarrow \omega(x) \neq \omega(y)$ seuraa, nyt, että jos $\{x, y\} \in E$ eli jos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

😊 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 konstruoiimme polun siten, että jos polku $[v_0, \dots, v_k]$ 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 $[v_0, \dots, v_k, v_{k+1}]$ ja muuten konstruktio on valmis.
- Tällä tavalla saamme alla olevassa verkossa polun $[2, 3, 6, 8, 7, 5, 8]$:

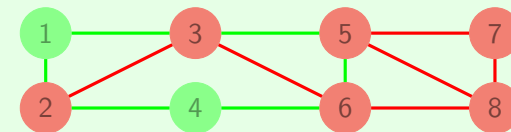


😊 Milloin yhtenäisessä, yksinkertaisessa ja suuntaamattomassa verkossa on Eulerin polku? Jatk.

- 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 suuntaamattomassa verkossa on Eulerin polku? Jatk.

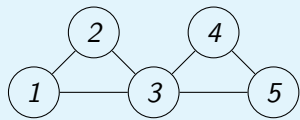
- Edellisessä esimerkissä saamme tällä tavalla syklin $[2, 1, 3, 5, 6, 4, 2]$:



- 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

Verkon



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

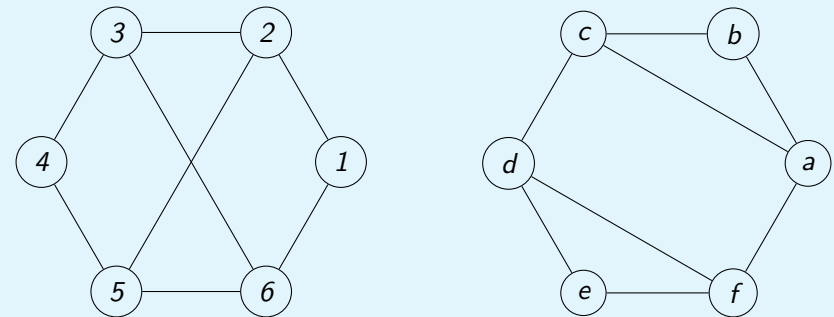
Nyt

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

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

💡 Isomorfiset verkot

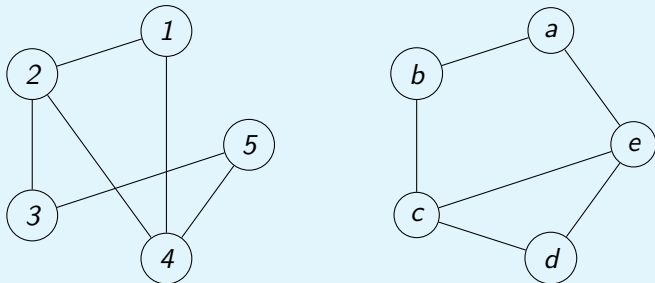
Ovatko alla olevat verkot isomorfiset?



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?

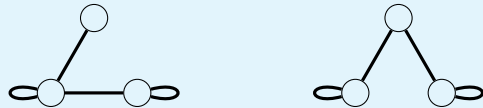
- Jos vaadimme, että verkko on yksinkertainen niin ei löydy yhtään koska yksinkertaisessa verkossa, jossa on 3 solmua on korkeintaan 3 kaarta.
- Naapurimatriisissa on 3 riviä ja saraketta ja koska verkko on suuntaamaton niin tämä matriisi on symmetrinen, eli tiedämme mikä se on jos tunnemme alkioita rivillä i ja sarakkeella j kun $1 \leq i \leq j \leq 3$. Koska verkossa on 4 kaarta niin 4 näistä 6:sta alkioista 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 nolilla siten, että neljästä alkioista tehdään 1 ja kahdesta 0.

- Vaatimus, että naapurit pysyvät naapureina antaa homomorfismin ψ solmujen permutaatioista joukon $\{a, b, c, d, e, f\}$ permutaatioiden ryhmään ja tämä homomorfismi on seuraava:

😊 Esimerkki, jatk.

- $\psi((1)) = (a), \quad \psi((1\ 2)) = (a\ d)(c\ e),$
 $\psi((1\ 3)) = (a\ f)(b\ e), \quad \psi((2\ 3)) = (d\ f)(b\ c),$
 $\psi((1\ 2\ 3)) = (a\ d\ f)(b\ e\ c), \quad \psi((1\ 3\ 2)) = (a\ f\ d)(b\ c\ e).$

- Tästä saamme sykli-indeksiksi

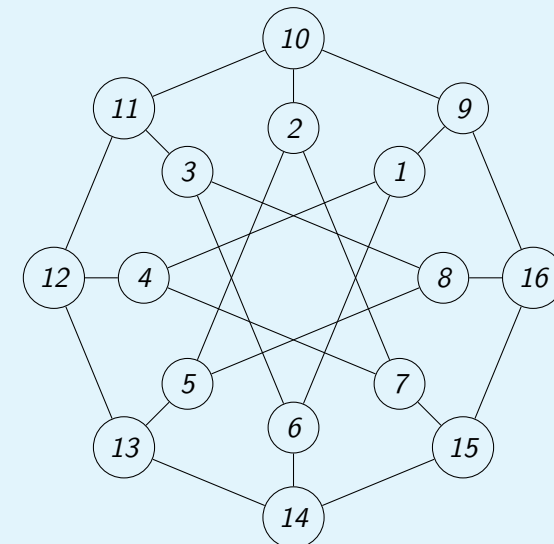
$$\frac{1}{6}(t_1^6 + 3 \cdot t_1^2 \cdot t_2^2 + 2 \cdot t_3^2).$$

- Pólyan lauseen mukaan termin $y^4 n^2$ kerroin lausekkeessa $\frac{1}{6}((y+n)^6 + 3(y+n)^2(y^2+n^2)^2 + 2(y^3+n^3)^2)$ 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 väritys

Tehtävänä on määrittää jokin alla olevan verkon solmujen väritys:



💡 Ahne väritys, jatk.

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

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

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

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

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

😊 Miksi dynaaminen optimointi toimii kun haemme "minimietäisyyksiä"?

- Määrittelemme funktion s kaavalla $s(v) = \min\{\sum_{j=1}^k w(\{v_{j-1}, v_j\}) : [v_0, v_1, \dots, v_k]$ 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 $[\tilde{v}_0, \tilde{v}_1, \dots, \tilde{v}_k]$ siten että $\tilde{v}_0 = v_0$, $\tilde{v}_k = v_{j+1}$ ja $\sum_{i=1}^k w(\{\tilde{v}_{i-1}, \tilde{v}_i\}) < t_{j+1}(v_{j+1})$.
- Silloin on olemassa suurin indeksi $i_0 < k$ siten, että $\tilde{v}_{i_0} \in V_j$ jolloin siis $\tilde{v}_{i_0+1} \in V \setminus V_j$ ja funktion t_{j+1} määritelmästä ja oletuksesta $w(e) \geq 0$ seuraa, että

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

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

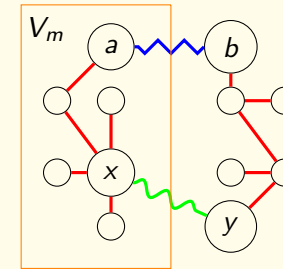
😊 Miten hankalaa on "minimietäisyyksien" löytäminen verkossa?

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

😊 Minimaalinen virittävä puu ja Primin ahne algoritmi

- $[V, E]$ yhtenäinen verkko, jossa jokaiselle kaarelle $\{v_j, v_k\}$ on annettu paino $w(\{v_j, v_k\})$ ja $T_* = [V, E_*]$ on puu siten, että $w(T_*) = \sum_{e \in E_*} w(e)$ on mahdollisimman pieni.
- Primin ahneella algoritmilla konstruoimme puut $T_j = [V_j, E_j]$, $j = 1, \dots, n$ (missä $|V_1| = 1$, $|V| = n$ ja $E_1 = \emptyset$).
- Jos $E_* = E_n$ niin tämä algoritmi on optimaalinen ja jos $E_* \neq E_n$ niin on olemassa suurin luku m , $1 \leq m < n$ siten, että $E_m \subseteq E_*$. 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 $E_{m+1} \subseteq E_{**}$ 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 $F_j = [V, E_j]$, $j = 1, \dots, n$.
- Konstruktion mukaisesti F_n on metsä. Jos F_n ei ole puu niin on olemassa solmut a ja b niin ettei niiden välillä ole polku verkossa F_n . Mutta verkossa $[V, E]$ on olemassa polku $[v_0, v_1, \dots, v_k]$ missä $v_0 = a$ ja $v_k = b$. Olkoon j pienin luku, siten, että solmujen v_{j-1} ja v_j välillä ei ole polku verkossa F_n eikä erityisesti $\{v_{j-1}, v_j\} \in E_n$. (Jos sellainen pari ei löydy niin solmujen a ja b välillä on polku.) Nyt voimme lisätä kaaren $\{v_{j-1}, v_j\}$ joukkoon E_n , että $[V, E_n \cup \{\{v_{j-1}, v_j\}\}]$ edelleen on metsä koska muuten solmujen v_{j-1} ja v_j välillä olisi jo kaari verkossa F_n . Näin ollen algoritmi antaa varmasti tulokseksi puun.

😊 Minimaalinen virittävä puu ja Kruskalin ahne algoritmi, jatk.

- Jos $E_* = E_n$ niin tämä algoritmi on optimaalinen ja jos $E_* \neq E_n$ niin on olemassa suurin luku m , $1 \leq m < n$ siten, että $E_m \subseteq E_*$ 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 $A \subseteq X$ 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 $\hat{X} \subseteq X \setminus \{a\}$ 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 $\hat{X} \subseteq X \setminus \{a\}$ 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 joukolle $A \subseteq X \setminus \hat{X}$ 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 .