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

G. Gripenberg

Aalto-yliopisto

3. huhtikuuta 2014

## Eukleideen algoritmi

*Kun laskemme* syt $(634, 36)$*:n Eukleideen algortmin 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* $\text{syt}\,(634, 36) = 2$.



## Jäännösluokan käänteisalkio

*Jos haluamme laskea* $[23]_{67}^{-1}$*:n niin ensin laskemme* 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* 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?

*Oleta, että $m$ ei ole $p$:llä jaollinen. Silloin pätee* $\operatorname{syt}(p, m) = 1$ *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.*



## Suomalaisen henkilötunnuksen tarkistusmerkki

*Suomalaisen henkilötunnuksen tarkistusmerkki määritetään jakojäännöksen perusteella, kun tarkistusmerkkiä edeltävien numeroiden muodostama luku jateaan 31:lla. Nyt on selvitettävä voiko tarkistusmerkki pysyä muttumattomana jos kaksi (eri) lukua vaihtavat paikkaa?*
*Oletamme, että numero $a$ jonka alkuperäinen paikka oli sijalla $j$ oikealta laskettuna vaihtaa paikkaansa numeron $b$ kanssa, jonka alkuperäinen paikka oli sijalla $k$ myös oikealta laskettuna. Oleta myös, että $j > k$. Numeroista muodostettujen lukujen välinen erotus on silloin*

$$m = (a-b) \cdot 10^{j-1} - (a-b) \cdot 10^{k-1} = \big((a-b) \cdot (10^{j-k} - 1)\big) \cdot 10^{k-1}.$$

*Tarkistusmerkki pysyy muuttumattomana jos ja vain jos* $\operatorname{mod}(m, 31) = 0$ *eli $m$ on 31:llä jaollinen. Koska 31 on alkuluku niin joko $a - b$, $10^{j-k} - 1$ tai $10^{k-1}$ on 31:llä jaolloinen. Koska $a \neq b$ niin $0 < |a - b| \leq 9$ eikä $a - b$ voi olla 31:llä jaollinen. Samoin luvun $10^{k-1}$ ainoat alkulukutekijät ovat 2 ja 5 joten myös* $\operatorname{mod}(10^{k-1}, 31) \neq 0$. *Käymällä läpi kaikki mahdollisuudet todetään että myös* $\operatorname{mod}(10^{j-k} - 1, 31) \neq 0$ *kun $j - k = 1, \ldots, 8$, (mutta* $\operatorname{mod}(10^{15} - 1, 31) = 0$*). Tästä päättelemme, että $m$ ei ole 31:llä jaollinen ja siitä syystä tarkistusmerkki muuttuu.*

## RSA-algoritmi

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

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

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



## 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 vastaukeksi* $[7]_{40}$ *koska* $\mod(23 \cdot 7, 40) = \mod(161, 40) = 1$. *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*

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

*joten* $\mod(14^7, 55) = 9$.

## 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* $\text{syt}\,(a, n) = 1$ *niin myös* $[a]_n$ *on kääntyvä ja koska* $[\alpha]_n \cdot [\beta]_n$ *on kääntyvä jos* $[\alpha]_n$ *ja* $[\beta]_n$ *ovat kääntyviä, niin* $[a]_n \cdot [x_j]$ *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* $\text{mod}\,(a^{\varphi(n)}, n) = 1$.



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

- *Koska oletamme, että* $0 < a < n$ *niin* $\text{syt}\,(a, n) \neq 1$ *ainoastaan jos* $p|a$ *tai* $q|a$*. Oletamme seuraavaksi, että* $p|a$ *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* $p^{q-1} \equiv 1 \pmod{q}$.
- *Silloin myös* $p^{(q-1)(p-1)r} \equiv 1 \pmod{q}$ *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* $kd = 1 + mr = 1 + (p-1)(q-1)r$ *ja näin ollen* $[(p^k)^d]_n = [p^{1+(q-1)(p-1)r}]_n = [p]_n$ *ja algoritmi toimii siis myös tässä tapauksessa!*

## Permutaatiot ja syklinotaatio

*Oleta, että* $\alpha$ *on joukon* $A = \{1, 2, 3, 4, 5, 6, 7\}$ *permutaatio*

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

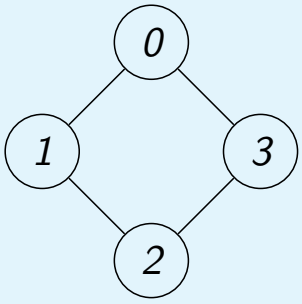
*missä siis tämä merkintätapa tarkoitaa, että esim.* $\alpha(1) = 2$ *ja* $\alpha(4) = 3$. *Nyt näemme, että* $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$ *(eli* $\alpha(1) = 2$, $\alpha(2) = 4$ *jne.) ja tästä saamme syklin* $\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ *joka siis on permutaatio* $\beta_1$ *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* $\beta_2$ *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.*



## 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* $\alpha$*, että jos* $x$ *ja* $y$ *ovat naapureita, eli niiden välillä on kaari, niin myös* $\alpha(x)$ *ja* $\alpha(y)$ *ovat naapureita (eli vaadimme, että* $\alpha$ *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.*

## 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 $\zeta_{D_4,X}(s+v+r, s^2+v^2+r^2, s^3+v^3+t^3, s^4+v^4+r^4)$ 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 $3 \times 3$-ruudukko ja olemme kirjoittaneet 2:een ruutuun **x**:n, 2:een **o**:n ja 5 ruutua ovat tyhjinä. Tämä on tehtävissä $\binom{9}{2,2,5} = 756$ eri tavalla jos paperi pidetään paikallaan. Mutta jos voimme kiertää paperia kulman $0$, $\frac{\pi}{2}$, $\pi$ tai $\frac{3\pi}{2}$ verran keskipisteen ympäri niin näiden vaihtoehtojen lukumäärä pienenee ja jotta voisimme systemaattisella tavalla selvittää montak 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 määritää 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 $\pi$ niin saamme 4 rataa, joilla molemmilla on 2 ruutua (vastakkaiset kulmat ja vastaikkaiset ruudut niiden välillä) 1 rata johon kuuluu 1 ruutu.*

## Pólyan lause ja ristinolla, jatk.

*Sykli-indeksiksi saamme näin ollen*

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

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

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

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



## Suora sivuluokkana

*$[\mathbb{R}^2, +]$ on ryhmä, jossa origo on neutraalialkio ja* **v***:n käänteisalkio on* $-\mathbf{v}$. *Jos nyt* $\mathbf{u} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}$ *niin* $H = \{\, t\mathbf{u} : t \in \mathbb{R} \,\}$ *on $[\mathbb{R}^n, +]$ aliryhmä ja sivuluokka* $\mathbf{w} + H$ *on kaikkien pisteen* **w***:n kautta kulkevan* **u***-suuntaisen suoran pisteet (tai niiden paikkavektorit).*

## Jäännösluokat tekijäryhminä

*Oleta, että $n > 1$. Silloin $[\mathbb{Z}, +]$ on ryhmä ja $n\mathbb{Z} = \{\, n \cdot j : j \in \mathbb{Z} \,\}$ on sen aliryhmä ja koska yhteenlasku on additiivinen operaatio $(a + b = b + a)$ niin se on normaali aliryhmä. Aliryhmän $n\mathbb{Z}$ sivuluokat ovat jäännösluokat modulo $n$ ja ne muodostavat tekijäryhmän $Z/n\mathbb{Z}$ missä operaatio on yhteenlasku. Niille voi tietenkin määritellä kertolasku mutta sen suhteen ei saada ryhmää. Sen sijaan, jos $p$ on alkuluku niin $[\mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}, \cdot]$ on ryhmä.*

## Normaalit aliryhmät ja tekijäryhmät

*Olkoon $G$ ryhmä ja $H$ sen aliryhmä.*

- $aH = Ha$ *kaikilla* $a \in G$ *jos ja vain jos* $axa^{-1} \in H$ *kaikilla* $a \in G$ *ja* $x \in H$.
  *Miksi? Olkoot* $a \in G$ *ja* $x \in H$. *Nyt pätee* $ax \in aH$ *joten jos* $aH = Ha$ *niin on olemassa* $y \in H$ *siten, että* $ax = ya$ *ja silloin* $axa^{-1} = y \in H$. *Jos toisaalta* $axa^{-1} = y \in H$ *niin* $ax = ya$ *joten* $aH \subset Ha$. *Mutta jos* $a$ *korvataan* $a^{-1}$*:llä niin saamme* $a^{-1}H \subset Ha^{-1}$ *josta seuraa, että myös* $Ha = aa^{-1}Ha \subset aHa^{-1}a = aH$ *pätee.*
- *Jos* $aH = Ha$ *kaikilla* $a \in G$ *niin ehdoista* $a_1H = a_2H$ *ja* $b_1H = b_2H$ *seuraa* $a_1b_1H = a_2b_2H$ *jolloin sivuluokkkien* $aH$ *ja* $bH$ *"tuloksi" voidaan määritellä* $(aH)(bH) = abH$.
  *Miksi? Käyttämällä oletusta* $aH = Ha$ *monta kertaa saamme*

$$a_1b_1H = a_1Hb_1 = a_2Hb_1 = a_2b_1H = a_2b_2H.$$



## $X_a$ ja $G_x$?

*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*

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

*ja*

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

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

*Oleta, 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 riittää konstruoida bijektio $\psi$ aliryhmän $G_x$ sivuluokkien joukosta rataan $Gx$.*
*Määrittele $\psi(aG_x) = ax$. 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 $\psi$ 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 $\psi$ 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 $\psi$ 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 $X$. Koska $|G_x| = \frac{|G|}{|Gx|}$ ja $Gx$ on rata, johon alkio $x$ kuuluu niin saamme väitteemme seuraavan laskun avulla:*

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

## Pólyan värityslauseen todistus

*Oletamme, että $\Omega$ on joukko $X$:n värityksiä siten, että $G\Omega \subset \Omega$ missä $G$ on ryhmä joka toimii joukossa $X$ ja siten myös väritysten joukossa $\Omega$. Aikaisempien tulosten perusteella ratojen lukumäärä (eli ei-ekvivalenttien väritysten, eli ekvivalenssiluokkien lukumäärä) $G$:n toiminnassa $\Omega$:ssa on*

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

*missä $\Omega_a = \{\,\omega \in \Omega : a\omega = \omega\,\}$ on väritysten joukko joka pysyy muuttumattomina $a$:n toiminnassa. Nämä väritykset taas ovat ne, jotka ovat vakioita jokaisella $a$:n radalla sen toiminnassa joukossa $X$.*
*Jos nyt $\Omega$ on joukko värityksiä joissa käytetään väriä $v_j$ täsmälleen $i_j$ kertaa, niin meidän pitää osoittaa, että*

$$|\Omega_a| = \text{kerroin}\Big(\zeta_{a,X}(v_1 + \ldots + v_r, \ldots, v_1^n + \ldots + v_r^n), v_1^{i_1} \cdot \ldots \cdot v_r^{i_r}\Big).$$



## Pólyan värityslauseen todistus, jatk.

*Oletamme, että $R_{a,1}, R_{a,2}, \ldots R_{a,m_a}$ ovat radat $a$:n toiminnassa ja määrittelemme $s_j = |R_{a,j}|$. Nyt on tietenkin olemassa yksi tapa käyttää väriä $v_j$ täsmälleen $s_1$ kertaa kun väritämme joukon $R_{a,1}$ alkioita värillä $v_j$. Voimme esittää tämän väitteen (ns. generoivalla) funktiolla $v_1^{s_1} + \ldots + v_r^{s_1}$ niin että termin $v_j^{s_1}$ kerroin on vaihtoehtojen lukumäärä (joka siis tässä on 1).*
*Seuraavaksi oletamme, että $p_k(v_1, \ldots, v_r) = \prod_{j=1}^{k}(v_1^{s_j} + \ldots + v_r^{s_j})$ on (genereroiva) funktio siten, että termin $v_1^{i_1} \cdot v_2^{i_2} \cdot \ldots \cdot v_r^{i_r}$ kerroin on vaihtoehtojen lukumäärä kun väritämme radat $R_{a,1}, \ldots R_{a,k}$ niin että käytämme väriä $v_j$ täsmälleen $i_j$ kertaa. Radan $R_{a,k+1}$ alkioita voimme värittää siten, että käytämme tiettyä väriä $s_{k+1}$ kertaa ja eri valinnat johtavat eri väritysvaihtoehtoihin.*
*Jos väritämme rataa $R_{a,k+1}$ värillä $v_q$ och haluamme käyttää väriä $v_p$ täsmälleen $i_p$ kertaa ratojen $R_{a,1}, \ldots R_{a,k}, R_{a,k+1}$ värittämiseen niin ratojen $R_{a,1}, \ldots R_{a,k}$ värittämiseen meidän täytyy käyttää väriä $v_p$ täsmälleen $i_p$ kertaa kun $p \neq q$ ja väriä $v_q$ täsmälleen $i_q - s_{k+1}$ kertaa.*

## Pólyan värityslauseen todistus, jatk.

*Kun väritämme rataa $R_{a,k+1}$ ainoat vaihtoehdot liittyvät värin $v_q$ valitsemiseen ja silloin induktio-oletuksen nojalla väritysvaihtoehtojen lukumääräksi tulee*

$$\sum_{q=1}^{r} \text{kerroin}(p(v_1,\ldots,v_r), v_1^{j_1}\cdot\ldots\cdot v_{q-1}^{j_{q-1}}\cdot v_q^{j_q-s_{k+1}}\cdot v_{q+1}^{j_{q+1}}\cdot\ldots\cdot v_r^{j_r}).$$

*Mutta tämä luku on sama kuin*

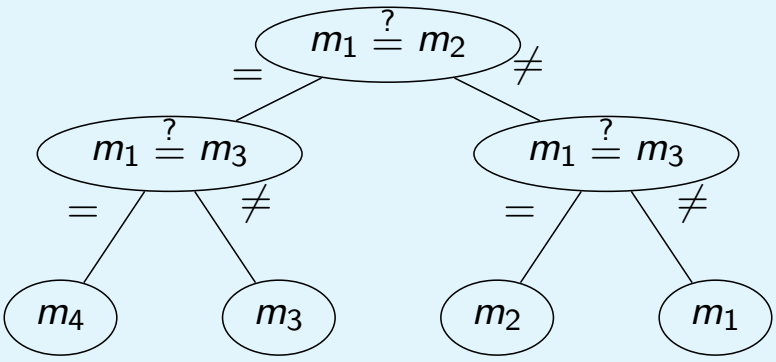
$$\text{kerroin}(p(v_1,\ldots,v_r)\cdot(v_1^{s_{k+1}}+\ldots+v_r^{s_{k+1}}), v_1^{j_1}\cdot\ldots\cdot v_r^{j_r}),$$

*josta seuraa, että induktio-askel toimii ja saamme lauseen todistetuksi. Jos käytämme r väriä, jolloin siis muita rajoituksia kuin että värien lukumäärä on r ei ole, niin voimme todeta, että jos ryhmän G alkiolla a on k rataa niin $|\Omega_a| = r^k$ koska kyseessä on k-kertainen järjestetty valinta palauttaen joukosta jossa on r alkiota. Koska myös $\zeta_{a,X}(r,\ldots r) = r^k$ niin saamme väiteen tässäkin tapauksessa.*



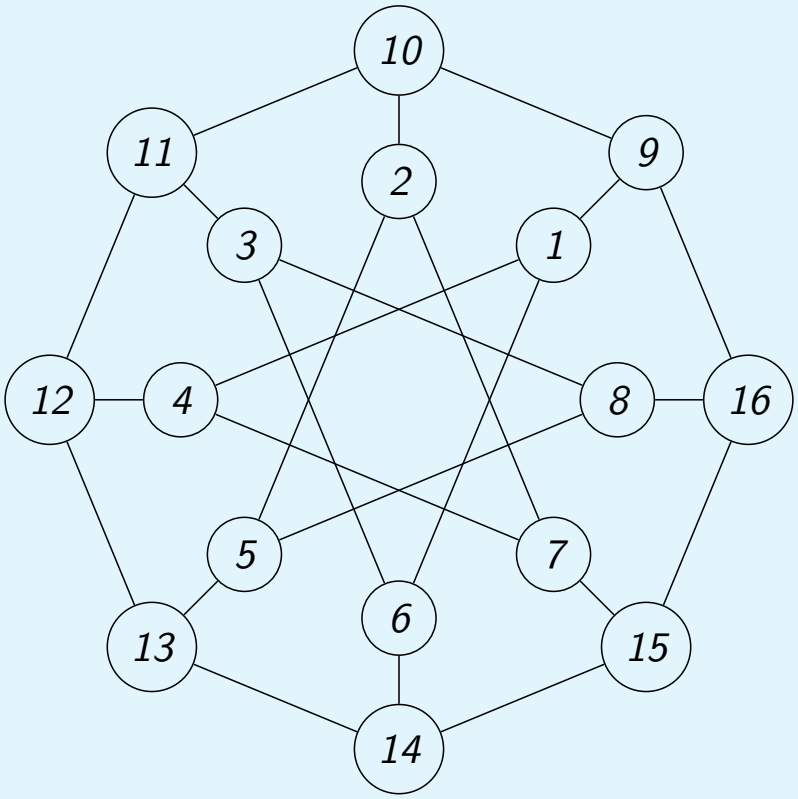
## Verkko päätösprosessin kuvaajana

*Oleta, että meillä on neljä kolikkoa, joista tiedämme että yksi on väärennetty, niin että sen paino poikkeaa muiden painosta mutta emme tiedæ onko se painavampi vai kevyempi. 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 $m_j$, $j = 1,2,3,4$, on väärennetty:*



## Ahne väritys

*Tehtävänä on määrittää jokin alla olevan verkon solmujen väritys:*






## Ahne värity, jatk.

*Ahneen väritysalgoritmen 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* |

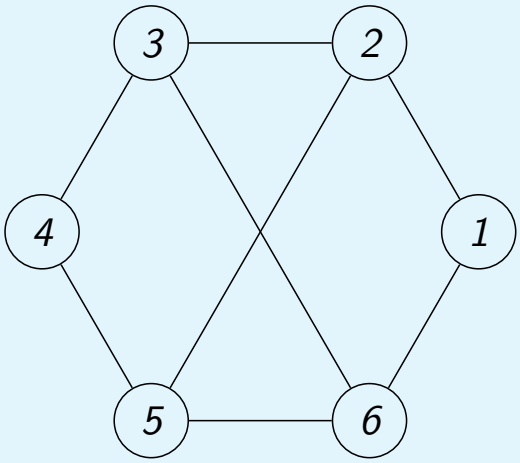
*Jos sen sijaan otamme solmut järjestyksessä* $9, 10, \ldots, 15, 16, 1, 2, 7, 8$ *niin väritykseksi tulee*

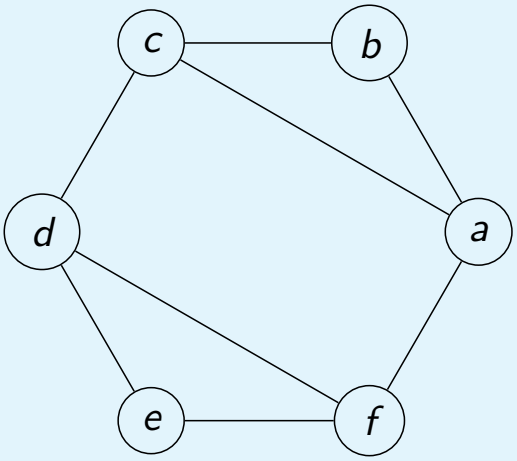
| *Solmu* | *9* | *10* | *11* | *12* | *13* | *14* | *15* | *16* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Väri* | *a* | *b* | *a* | *b* | *a* | *b* | *a* | *b* | *b* | *a* | *b* | *a* | *b* | *a* | *b* | *a* |

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

## Isomorfiset verkot

*Ovatko alla olevat verkot isomorfiset?*



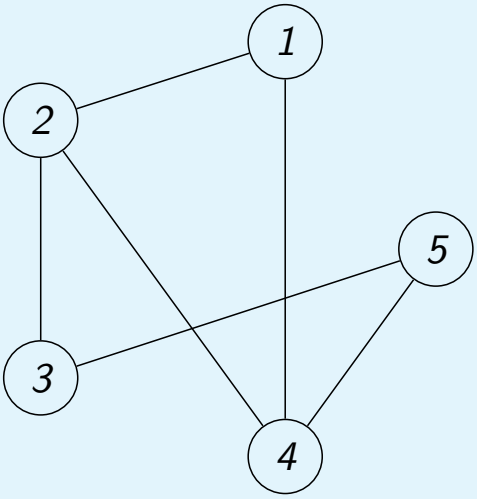



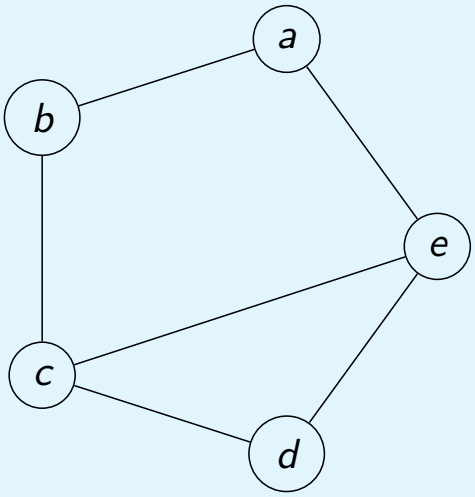

*Molemmissa verkoissa on 4 solmua joiden aste on 3, eli joilla on 3 naapuria ja 2 joiden on aste on 2, joten tästä emme voi päätellä etteivät verkot olisivat isomorfiset. Sensijaan vasemmanpuoleisessa verkossa ei ole yhtään sykliä, jonka pituus olisi 3 mutta sellaisia on oikeanpuoleisessa verkossa. Tästä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



## Isomorfiset verkot

*Ovatko alla olevat verkot isomorfiset?*




*Tässä tapauksessa verkot ovat isomorfiset koska bijektioksi voidaan valita funktio $\psi$ siten, että $\psi(1) = d$, $\psi(2) = c$, $\psi(3) = b$, $\psi(4) = e$ ja $\psi(5) = a$ ja tälla funktiolla on vaadittavat ominaisuudet.*

## Miksi dynaaminen optimointi toimii kun haetaan "minimietäisyyksiä"?

*Määrittelemme funktion $s$ kaavalla* $s(v) = \min\{\sum_{j=1}^{k} w(\{\tilde{v}_{j-1}, \tilde{v}_j\} : [\tilde{v}_0, \tilde{v}_1, \ldots, \tilde{v}_k]$ *on polku solmusta* $\tilde{v}_0 = v_0$ *solmuun* $\tilde{v}_k = v\}$ *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 ainostaan 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* $t_{j+1}(v_{j+1}) = \min_{v \in V \setminus V_j} t_{j+1}(v)$. *Funktion* $t_{j+1}$ *määritelmästä seuraa, että* $s(v_{j+1}) \leq t_{j+1}(v_{j+1})$ *joten joko* $s(v_{j+1}) = t_{j+1}(v_{j+1})$ *tai* $s(v_{j+1}) < t_{j+1}(v_{j+1})$. *Jälkimmäisessä tapauksessa meillä olisi 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* $\sum_{i=1}^{k} w(\{\tilde{v}_{i-1}, \tilde{v}_i\}) < t_{j+1}(v_{j+1})$.



## Miksi dynaaminen optimointi toimii kun haetaan "minimietäisyyksiä"? jatk.

*Nyt on olemassa suurin indeksi* $i_0$ *siten, että* $\tilde{v}_{i_0} \in V_j$ *jolloin siis* $\tilde{v}_{i_0+1} \in V \setminus V_j$ *ja oletuksesta* $w(e) \geq 0$ *ja funktion* $t_{j+1}$ *määritelmästä seuraa, että*

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

*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 löytää kahden solmun välisen "etäisyyden" minimi?

*Oletamme, että $[V, E]$ on yhtenäinen (suuntaamaton) verkko ja jokaiselle kaarelle $\{v_j, v_k\} \in E$ 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.*
*Eräs mahdollisuus on laskea summa kaikkien polkujen yli ja valita pienin. Jos $|V| = n$ ja jos kaikkien solmujen välillä on kaari niin on olemassa $\sum_{j=0}^{n-2} \frac{(n-2)!}{j!} \geq (n-2)!$ yksinkertaista polkua.*
*Jos käytämme dynaamista optimointia ja olemme laskeneet optimiarvon $j$:lle solmulle niin meidän pitää laskea uudet testiarvot korkeintaan $n-j$:lle solmulle käyttäen korkeintaan $n-j$ yhteenlaskua ja yhtä monta vertailua ja sitten valita niistä pienin johon tarvitaan $n-j-1$ vertailua. Tästä seuraa, että 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. Tästä seuraa, että yhteenlaskujen ja vertailujen lukumäärä kuuluu joukkoon $O(n^2)$ kun verkossa on $n$ solmua.*



## Aputulos: Kaarien vaihto

*Jos $[V, E]$ on (suuntaamaton) puu, $x$ ja $y \in V$, $x \neq y$ ja $[v_0, v_1, \ldots, v_k]$ on polku solmusta $x$ solmuun $y$ niin $[V, (E \cup \{\{x, y\}\}) \setminus \{\{v_{j-1}, v_j\}\}]$, missä $j \in \{1, \ldots, k\}$, on myös puu.*

## Miksi?

*Jos $\{x, y\} \in E$ kaareja ei vaihdeta ja verkko pysyy muuttumattomana joten oletamme, että $\{x, y\} \notin E$.*
*Merkitsemme $\hat{E} = (E \cup \{\{x, y\}\}) \setminus \{\{v_{j-1}, v_j\}\}$ ja valitsemme mielivaltaisesti $a$ ja $b \in V$. Koska $[V, E]$ on puu niin on olemassa polku $[\tilde{v}_0, \tilde{v}_1, \ldots, \tilde{v}_m]$ solmusta $a$ solmuun $b$. Jos nyt on olemassa $p$ siten, että $\tilde{v}_{p-1} = v_{j-1}$ ja $\tilde{v}_p = v_j$ niin saamme verkossa $[V, \hat{E}]$ polun $a$:sta $b$:hen käymällä ensin $a$:sta $v_{p-1}$:een polkua $[\tilde{v}_0, \ldots, \tilde{v}_{p-1}]$ pitkin , sieltä $x$:ään polkua $[v_{j-1}, \ldots, v_0]$ pitkin, sitten $y$:hyn, sieltä $\tilde{v}_p$:hen polkua $[v_k, \ldots, v_j]$ pitkin ja sieltä solmuun $b$ polkua $[\tilde{v}_p, \ldots, \tilde{v}_m]$ pitkin. (Jos $\tilde{v}_{p-1} = v_j$ ja $\tilde{v}_p = v_{j-1}$ menetellään vastaavalla tavalla.) Tästä polusta saadaan yksinkertainen polku poistamalla ylimääräiset solmut.*

## Miksi? jatk.

*Jos meillä olisi toinenkin yksinkertainen polku solmusta a solmuun b niin $\{x, y\}$ on kaari tällä polulla koska muuten alkuperäinen verkko $[V, E]$ ei olisi puu. Tästä syystä myös solmu x tulee ensimmäisenä vastaan tällä polulla ja koska $[V, E]$ on puu niin on olemassa vain yksi yksinkertainen polku solmusta a solmuun x ja solmusta y solmuun b ja siten vain yksi yksinkerteinen polku solmusta a solmuun b uudessa verkossa.*
*Jos kaari $\{v_{j-1}, v_j\}$ ei ole mukana polussa $[\tilde{v}_0, \tilde{v}_1, \ldots, \tilde{v}_m]$ niin on olemassa täsmällen yksi yksinkertainen polku a:sta b:hen verkossa $[V, E \setminus \{\{v_{j-1}, v_j\}\}$ ja siten myös verkossa $[V, \hat{E}]$.*



## Minimaalinen virittävä puu ja ahne algoritmi I (Prim)

*Oletamme, että $[V, E]$ yhtenäinen verkko, jossa jokaiselle kaarelle $\{v_j, v_k\}$ on annettu paino $w(\{v_j, v_k\})$ ja oletamme myös, että $T_* = [V, E_*]$ 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 $|V| = n$ ja $E_1 = \emptyset$). Jos $E_* = E_n$ niin tämä algoritmi on optimaalinen ja jos $E_* \neq E_n$ niin on 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 solmuu 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 aputuloksen nojalla uusi verkko $T_{**}$ on myös puu 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 induktiolla seuraa, että $E_n$ on optimaalen virittävä puu.*

## Minimaalinen virittävä puu ja ahne algoritmi II (Kruskal)

*Oletamme, että* $[V, E]$ *yhtenäinen verkko, jossa jokaiselle kaarelle* $\{v_j, v_k\}$ *on annettu paino* $w(\{v_j, v_k\})$. *Kruskalin ahneella algoritmilla konstruoimme metsät* $M_j = [V, E_j]$, $j = 0, \ldots, q$. *Konstruktion mukaisesti* $M_q$ *on metsä. Jos* $M_q$ *ei ole puu niin on olemassa solmut* $a$ *ja* $b$ *niin ettei niiden välillä ole polku verkossa* $M_q$. *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* $M_q$. *(Jos sellainen pari ei löydy niin solmujen* $a$ *ja* $b$ *välillä on polku.) Ny voimme verkossa* $[V, E_q]$ *lisätä kaaren* $\{v_{j-1}, v_j\}$ *joukkoon* $E_q$ *siten, että* $[V, E_q \cup \{\{v_{j-1}, v_j\}\}$ *edelleen on metsä. Näin ollen algoritmi antaa tuloksena puun.*
*Seuraavaksi oletamme että* $T_* = [V, E_*]$ *on puu siten, että* $w(T_*) = \sum_{e \in E_*} w(e)$ *on mahdollisimman pieni. Jos* $E_* = E_{n-1}$ *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* $\{x, y\} \notin E_*$.



## Minimaalinen virittävä puu ja ahne algoritmi II (Kruskal), jatk.

*Puussa* $T_*$ *on olemassa polku* $[v_0, v_1, \ldots, v_k]$ *solmusta* $x$ *solmuun* $y$. *Koska* $M_q$ *on puu niin on olemassa indeksi* $j$ *siten, että* $\{v_{j-1}, v_j\} \notin E_q$. *Jos* $E_{**} = E \cup \{x, y\} \setminus \{v_{j-1}, v_j\}$ *niin* $[V, E_{**}]$ *on myös puu ja koska* $T_*$ *oli optimaalinen niin pätee* $w(\{x, y\}) \geq w(\{v_{j-1}, v_j\})$. *Koska otimme kaaren* $\{x, y\}$ *mukaan joukkoon* $E_{m+1}$ *niin täytyy olla* $w(\{x, y\}) = w(\{v_{j-1}, v_j\})$ *eli* $T_{**}$ *on myös optimaalinen puu. Induktiolla voimme sitten päätellä, että tämäkin algoritmi antaa optimaalisen tuloksen.*

## Milloin löytyy täydellinen pariutus kaksijakoisessa verkossa?

*Oletamme, että* $[X \cup Y, E]$ *on kaksijakoinen verkko, jonka osat ovat* $X$ *ja* $Y$*. Jos* $A \subset X$ *niin merkitään*
$N(A) = \{\, y \in Y : \exists x(x \in A \,\&\, \{x, y\} \in E)\,\}$*. Jos* $M$ *on verkon täydellinen pariutus niin* $|A| \leq |N(A)|$ *kaikilla* $A \subset X$ *koska funktio* $x \in A \mapsto y$ *missä* $\{x, y\} \in M$ *on injektio pariutuksen määritelmän nojalla.*
*Seuraavaksi osoitamme, että jos* $|A| \leq |N(A)|$ *kaikilla* $A \subset X$ *niin verkossa* $[X \cup Y, E]$ *on olemassa täydellinen pariutus. Tämä pätee varmasti jos* $|X| = 1$ *ja oletamme, että se pätee myös kun* $|X| = k$*. Jos nyt* $|X| = k + 1$ *niin valitsemme solmun* $a \in X$*. Mikäli mahdollista valitsemme myös osajoukon* $\widehat{X} \subset X \setminus \{a\}$ *siten, että* $|N(\widehat{X})| = |\widehat{X}| > 0$*.*
*Jos tämä ei ole mahdollista niin tiedämme, että* $|N(\widehat{X})| \geq |\widehat{X}| + 1$ *kaikilla* $\widehat{X} \subset X \setminus \{a\}$ *joille pätee* $\widehat{X} \neq \emptyset$*. Nyt on olemassa* $b \in Y$ *siten, että* $\{a, b\} \in E$ *ja ehto "*$|A| \leq |N(A)|$ *kaikilla* $A \subset X$*" pätee kaksijakoisessa verkossa*

$$[(X \setminus \{a\}) \cup (Y \setminus \{b\}), E \setminus (\{\, \{a, y\} : y \in Y \,\} \cup \{\, \{x, b\} : x \in X \,\})],$$

*koska korkeintaan yksi naapuri poistetaan.*



## Milloin löytyy täydellinen pariutus kaksijakoisessa verkossa? jatk.

*Kun sovellamme induktio-oletusta tähän verkkoon ja sitten lisäämme kaaren* $\{a, b\}$ *saamme pariutuksen alkuperäiselle verkolle eli väite pätee myös kun* $card(X) = k + 1$*.*
*Toisaalta, jos löydämme joukon* $\widehat{X} \subset X \setminus \{a\}$ *siten, että* $|N(\widehat{X})| = |\widehat{X}| > 0$ *niin voimme soveltaa induktio-oletusta verkkoon* $G_1 = [\widehat{X} \cup N(\widehat{X}), \widehat{E}]$ *missä* $\widehat{E} = \{\, \{x, y\} \in E : x \in \widehat{X}, y \in N(\widehat{X})\,\}$*. Mutta oletus "*$|A| \leq |N(A)|$ *kaikilla* $A \subset X$*" pätee myös verkossa*
$G_2 = [(X \setminus \widehat{X}) \cup (Y \setminus N(\widehat{X})), \{\, \{x, y\} \in E : x \in X \setminus \widehat{X}, y \in Y \setminus N(\widehat{X})\,\}]$ *koska jos näin ei ole jonkin joukon* $A \subset X \setminus \widehat{X}$ *osalta, niin oletus ei ole voimassa alkuperäisessä verkossakaan joukon* $A \cup \widehat{X}$ *kohdalla.*
*Induktio-oletuksen nojalla ja ottamalla verkkojen* $G_1$ *ja* $G_2$ *pariutusten unioni saamme alkuperäisen verkon pariutuksen, eli väite pätee tässäkin tapauksessa kun* $|X| = k + 1$*. Induktioperiaatteen nojalla toteamme, että väite pätee aina.*