MS-A0402 Diskreetin matematiikan perusteet
Yhteenveto, osa II

G. Gripenberg

Aalto-yliopisto

3. huhtikuuta 2014

Jaollisuus

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

Modulofunktio mod

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

Kongruenssi modulo

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

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

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

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

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

Huom!

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

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

Voidaan osoittaa, että jos

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

niin

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

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

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

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

Suurin yhteinen tekijä

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

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

(syt=suurin yhteinen tekijä, gcd= greatest common divisor, ja tavallisesti määritellään $\text{syt}\,(0, 0) = 0$*)*
Jos $\text{syt}\,(m, n) = 1$ *niin luvut m ja n ovat keskenään jaottomia.*
Huomaa, että määritelmästä seuraa, että
$\text{syt}\,(m, n) = \text{syt}\,(n, m) = \text{syt}\,(|m|, |n|)$.

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

Jos $[m]_n \in \mathbb{Z}/n\mathbb{Z}$ *ja on olemassa jäännösluokka* $[j]_n \in \mathbb{Z}/n\mathbb{Z}$ *siten, että* $[m]_n \cdot [j]_n = [1]_n$, *eli* $m \cdot j \equiv_n 1$ *niin sanotaan, että* $[m]_n$*:llä on käänteisalkio tai että* $[m]_n$ *on kääntyvä* $\mathbb{Z}/n\mathbb{Z}$*:ssa och käänteisalkio on* $[j]_n = [m]_n^{-1}$. *Tässä tapauksessa voidaan jakaa* $[m]_n$*:llä koska se on yhtäpitävää sen kanssa, että kerrotaan* $[j]_n$*:llä.*
Koska $m \cdot j \equiv_n 1$ *niin on olemassa kokonaisluku* k *siten, että* $m \cdot j = 1 + k \cdot n$. *Jos nyt* $d|m$ *ja* $d|n$ *niin pätee* $d|(m \cdot j - k \cdot n)$ *eli* $d|1$ *joten* $d = 1$. *Näin ollen* $\text{syt}\,(m, n) = 1$. *Voidaan osoitaa, että myös käänteinen tulos pätee joten*

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

Huom

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

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

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

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

  kun $j \geq 2$ *ja* $r_{j-1} > 0$.
- $\text{syt}\,(m, n) = r_{k-1}$ *jos* $r_k = 0$.

Miksi Eukleideen algoritmi toimii?

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

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

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

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

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

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

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

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

Eulerin φ-funktio

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

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

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

Huomaa että $[0]_1$*:llä on käänteisalkio joukossa* $\mathbb{Z}/1\mathbb{Z}$ *joten* $\varphi(1) = 1$ *mutta* $[0]_n$*:llä ei tietenkään (?) ole käänteisalkiota joukossa* $\mathbb{Z}/n\mathbb{Z}$ *kun* $n > 1$.
Matlab/octave:ssä tämän funktion laskemiseksi voidaan käyttää funktiota `@(n)sum(gcd(0:n-1,n)==1)`.

Eulerin lause

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

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

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

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

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

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

Miten RSA-algoritmin avaimet on valittava?

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

Miksi RSA-algoritmi toimii?

- *Oleta yksinkertaisuuden vuoksi, että* $\operatorname{syt}(a, n) = 1$.
- *Voidaan osoittaa, että $\varphi(n) = \varphi(p \cdot q) = (p - 1) \cdot (q - 1) = m$.*
- *Eulerin lauseen mukaan $[a^m]_n = [1]_n$.*
- *Koska $[d]_m = [k]_m^{-1}$ niin $k \cdot d = 1 + r \cdot m$ ja*

$$\left[b^d\right]_n = \left[a^{k \cdot d}\right]_n = \left[a^{1 + r \cdot m}\right]_n = [a]_n \cdot [a^m]_n^r = [a]_n \cdot [1]_n^r = [a]_n,$$

josta seuraa, että $\operatorname{mod}(b^d, n) = \operatorname{mod}(a, n) = a$.

RSA-algoritmi ja allekirjoitukset

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

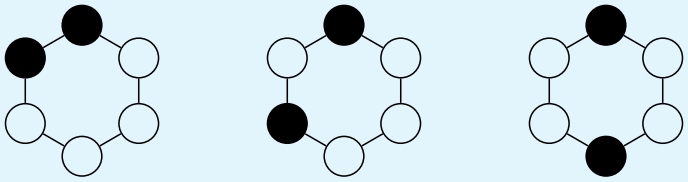
- *A laskee tiivisteen $h(a)$ viestistä a* (ja tiivisteestä $h(a)$ viestiä ei voida palauttaa).
- *A salaa viestin a B:n julkisella avaimella (n_B, k_B) salatuksi viestiksi $b = \operatorname{mod}(a^{k_B}, n_B)$.*
- *A salaa tiivisteen $h(a)$ omalla yksityisella avaimellaan (n_A, d_A) allekirjotukseksi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

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

Väritysongelma

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

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



Mutta miten ratkaistaan monimutkaisemmat tämäntyyppiset ongelmat?

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

Ryhmät

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

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

Huom!

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

Kommutatiiviset eli Abelin ryhmät

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

Aliryhmä

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

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

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

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

Homomorfismit ja isomorfismit

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

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

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

Sykliset ryhmät

Ryhmä G on syklinen jos on olemassa $a \in G$ siten, että $G = \{ a^j : j \in \mathbb{Z} \}$. Silloin sanotaan, että G on a:n generoima syklinen ryhmä ja merkitään $G = \langle a \rangle$.
Jos G on ryhmä ja $a \in G$ niin $\langle a \rangle = \{ a^j : j \in Z \}$ on a:n generoima G:n syklinen aliryhmä.
Koska kaikki sykliset ryhmät, joissa on m alkiota ovat isomorfiset niin tällaista ryhmää merkitään C_m:llä.

Sivuluokat

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

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

Sivuluokilla on seuraavia ominaisuuksia (tässä ainoastaan vasemmat sivuluokat):

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

Homomorfismit, normaalit aliryhmät ja tekijäryhmät

Olkoon G ryhmä.

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

Permutaatiot

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

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

Permutaatiot, radat, syklimerkinnät

Olkoon A äärellinen ei-tyhjä joukko.

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

Huom!

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

Parilliset ja parittomat permutaatiot

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

Ryhmän toiminta

Jos G eli $[G, \bullet]$ on ryhmä ja X on joukko niin G:n **toiminta** *joukossa X on homomorfismi G:ltä X:n permutaatioiden ryhmälle.*
Jos yhdistetty funktio määritellään (normaalilla) tavalla $(f \circ g)(x) = f(g(x))$ *niin saadaan* **vasen toiminta** *ja jos määritellään $x(f \diamond g) = (xf)g$ niin saadaan* **oikea toiminta**. *Sen sijaan että kirjoitettaisiin $\psi(a)(x)$ missä ψ on homomorfismi $a \in G$ ja $x \in X$ kirjoitetaan useimmiten ax ja sanotaan että G* **toimii** *joukossa X. Vasemmalle toiminnalle homomorfismiominaisuudeksi tulee $(ab)x = a(bx)$, $a, b \in G$, $x \in X$.*

Huom

Jos G on ryhmä X:n permutaatioita niin identiteettifunktio on homomorfismi eikä toiminta-käsitettä tarvita.
Jos G on ryhmä niin se toimii itsessään esim. siten, että $\psi(a)(x) = ax$ (vasen toiminta), $\psi(a)(x) = axa^{-1}$ (vasentoiminta), $\psi(a)(x) = xa$ (oikea toiminta) tai $\psi(a)(x) = a^{-1}xa$ (oikea toiminta).

Radat ja kiinnittäjäaliryhmät

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

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

Jokaisella $x \in X$ pätee $|Gx| \cdot |G_x| = |G|$.

Huom!

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

Sykli-indeksi

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

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

missä j_k on k-pituisten ratojen lukumäärä a:n toiminnassa.
Joukon X permutaatioryhmän G tai joukossa X toimivan ryhmän G **sykli-indeksi** *on*

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

Ratojen lukumäärä ryhmän toiminnassa (Burnsiden lemma)

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

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

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

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

Ryhmän toiminta ja "väritykset"

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

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

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

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

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

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

Mitkä väritykset ovat invariantteja ryhmäalkion a toiminnassa?

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

Miksi?

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

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

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

Pólyan "väritys"-lause

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

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

kerroin polynomissa

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

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

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

Verkot

- *Sunnattu verkko on pari* $[V, E]$ *missä* V *on joukko, jonka alkiot ovat verkon solmut ja* E *on joukon* $V \times V$ *osajoukko, jonka alkiot ovat solmujen väliset (suunnatut) kaaret eli linkit.*
- *Suuntaamaton verkko (tai vain verkko) on pari* $[V, E]$ *missä* V *on joukko, jonka alkiot ovat verkon solmut ja* $E \subset \{\{a, b\} : a, b \in V\}$*on verkon solmujen välisten kaarien joukko.*
- *Verkko* $[V, E]$ *on yksinkertainen jos* $|k| = 2$ *kaikilla* $k \in E$ *ja suunnatun verkon tapauksessa jos* $[v, v] \notin E$ *kaikilla* $v \in V$*.*
- *Jos verkon kahden solmun väillä on kaari niin ne ovat toistensa naapureita ja kyseisen kaaren päätesolmut.*

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

Huom!

Näissä verkoissa on siis kahden solmun välilä korkeintaan yksi kaari ja verkko on yksinkertainen jos mistään solmusta ei ole kaarta samaan solmuun.

Määritelmiä

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

Määritelmiä, jatk.

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

Isomorfiset verkot

Verkot $[V, E]$ *ja* $[V', E']$ *ovat isomorfiset jos on olemassa bijektio* $\psi : E \to E'$ *siten, että* $\{\psi(a), \psi(b)\} \in E' \leftrightarrow \{a, b\} \in E$ *(ja suunnatussa tapauksessa* $[\psi(a), \psi(b)] \in E' \leftrightarrow [a, b] \in E$*) eli "naapurit kuvautuvat naapureille".*

Ahne väritysalgoritmi

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

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

Naapurimatriisi

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

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

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

Kaksijakoiset verkot ja pariutukset

Jos $[X \cup Y, E]$ *on kaksijakoinen verkko (jonka osat ovat* X *ja* Y*) niin on olemassa pariutus* M *siten, että jokainen* $x \in X$ *on jonkin* M*:n kaaren päätepiste eli* M *on ns. täydellinen pariutus*
jos ja vain jos
jokaiselle $A \subset X$ *pätee, että* A*:n alkioiden lukumäärä* $|A|$ *on pienempi tai yhtäsuuri kuin* A*:n alkioiden naapureiden lukumäärä eli*
$|A| \leq |\{\, y \in Y : \{x, y\} \in E \ ([x,y] \in E), x \in A \,\}|$

Minimaalinen virittävä puu, ahne algoritmi I (Prim)

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

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

Minimaalinen virittävä puu, ahne algoritmi II (Kruskal)

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

- *Valitaan $E_0 = \emptyset$.*
- *Niin kauan kun verkko $[V, E_m]$ ei ole puu niin $E_{m+1} = E_m \cup \{e\}$ missä $e \in E \setminus E_m$ valitaan siten, että $w(e)$ on mahdollisimman pieni ja verkko $[V, E_m \cup \{e\}]$ on metsä.*

Dynaaminen optimointi ja verkot

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

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

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

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