MS-A0409 Grundkurs i diskret matematik II

G. Gripenberg

Aalto-universitetet

23 september 2015

Delbarhet

Ett tal a delar ett tal b eller b är delbart med a om det finns ett **heltal** *k så att $b = ak$, dvs. $b \in a\mathbb{Z}$. Detta skrivs också ofta som $a \mid b$. Då säger man också att b är en (heltals)multipel av a.*

Modulofunktionen mod

Om $n > 0$ så är $\operatorname{mod}(m, n) = j$ ifall $0 \leq j < n$ och $m = j + kn$ där $k \in \mathbb{Z}$. (men $\operatorname{mod}(m, 0) = m$ och $\operatorname{mod}(m, n) = \operatorname{mod}(m, -n) + n$ om $n < 0$). Om m och n är positiva tal så är $\operatorname{mod}(m, n)$ den rest som erhålls då man dividerar m med n men om $m < 0$ är denna rest inte positiv.

Kongruens modulo

Två tal a och b är kongruenta modulo n vilket skrivs $a \equiv_n b$ eller $a \equiv b \pmod{n}$ om n delar $a - b$, dvs. $b - a$ är en multipel av n:

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

$\mathbb{Z}/n\mathbb{Z}$, kongruensklasser

Relationen $a \equiv_n b$ är en ekvivalensrelation i $\mathbb{Z}$ ($x \sim x$, $x \sim y \to y \sim x$, $x \sim y$ AND $y \sim z \to x \sim z$) och delar upp $\mathbb{Z}$ i ekvivalensklasser, som kallas **kongruensklasser** *(eller restklasser), dvs. delmängder $\{\ldots, -2n, -n, 0, n, 2n \ldots\}$, $\{\ldots, -2n + 1, -n + 1, 1, n + 1, 2n + 1 \ldots\}$, $\ldots$, $\{\ldots, -n - 1, -1, n - 1, 2n - 1, \ldots\}$ där alla element i samma ekvivalensklass är kongruenta modulo n med varandra. Vi använder följande beteckningar:*

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

Obs!

Eftersom $\operatorname{mod}(m_1, n) = \operatorname{mod}(m_2, n) \Leftrightarrow [m_1]_n = [m_2]_n$ så väljer man ofta elementet $\operatorname{mod}(m, n)$ för att representera kongruensklassen $[m]_n$ så att man tex. kan tala om talen $0, 1, 2, \ldots, 5$ som elementen i $\mathbb{Z}/6\mathbb{Z}$ istället för mängderna $[0]_6, [1]_6, \ldots, [5]_6$. Ofta används $\overline{k}_n$ istället för $[k]_n$ och $\mathbb{Z}_n$ istället för $\mathbb{Z}/n\mathbb{Z}$.

Addition, subtraktion och multiplikation i $\mathbb{Z}/n\mathbb{Z}$

Man kan visa att om

$$a_1 \equiv_n a_2 \quad \text{och} \quad b_1 \equiv_n b_2$$

så är

$$\begin{aligned}(a_1 + b_1) &\equiv_n (a_2 + b_2)\\ (a_1 - b_1) &\equiv_n (a_2 - b_2)\\ (a_1 b_1) &\equiv_n (a_2 b_2)\end{aligned}$$

Därför kan man definiera räkneoperationer i $\mathbb{Z}/n\mathbb{Z}$ *med*

$$\begin{aligned}[a]_n + [b]_n &= [a+b]_n,\\ [a]_n - [b]_n &= [a-b]_n,\\ [a]_n \cdot [b]_n &= [a \cdot b]_n,\end{aligned}$$

och alla "normala" räkneregler gäller (bortsett från de som gäller olikheter).

Kontrolltecknet i finländska personnummer

Kontrolltecknet i finska personnummer räknas som resten vid division av det tal som de nio första siffrorna bildar med 31. *Kan kontrolltecknet bli oförändrat om två siffror som är olika byter plats?*
Anta att siffran a som ursprungligen finns i position j bakifrån byter plats med siffran b som som ursprungligen finns i position k bakifrån. Antag också att $j > k$. *Skillnaden mellan de två talen är då*

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

För att kontrolltecknet skall förbli oförändrat borde $\operatorname{mod}(m, 31) = 0$ *dvs.* $31|m$ *och eftersom* 31 *är ett primtal måste* 31 *då dela åtminstone ett av talen* $a-b$, $10^{j-k}-1$ *och* 10^{k-1}. *Eftersom* $a \neq b$ *är* $0 < |a-b| \leq 9$ *och därför delar inte* 31 *talet* $a-b$. *De enda primtal som delar* 10^{k-1} *är* 2 *och* 5 *så* 31 *kan inte dela* 10^{k-1} *och genom att gå genom alla möjligheter ser man också att* $\operatorname{mod}(10^{j-k}-1, 31) \neq 0$ *då* $j-k = 1, \ldots, 8$, *(men* $\operatorname{mod}(10^{15}-1, 31) = 0$*). Detta innebär att* 31 *inte delar m och därför ändras kontrolltecknet.*

Största gemensamma delare

Om m och n är heltal som inte båda är noll så är deras största gemensamma delare

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

(sgd=största gemensamma delare, gcd= greatest common divisor, och vanligen definierar man $\text{sgd}\,(0,0) = 0$*)*
Om $\text{sgd}\,(m,n) = 1$ *sägs talen m och n vara relativt prima.*
Observera att av defintionen följer att $\text{sgd}\,(m,n) = \text{sgd}\,(n,m)$.

Inverser i $\mathbb{Z}/n\mathbb{Z}$

Om $[m]_n \in \mathbb{Z}/n\mathbb{Z}$ *och det finns en kongruensklass* $[j]_n \in \mathbb{Z}/n\mathbb{Z}$ *så att* $[m]_n \cdot [j]_n = [1]_n$, *dvs* $m \cdot j \equiv_n 1$ *så säger man att* $[m]_n$ *(eller bara m) är inverterbar i* $\mathbb{Z}/n\mathbb{Z}$ *och inversen är* $[j]_n = [m]_n^{-1}$. *Detta innebär att man kan dividera med* $[m]_n$ *för det är det samma som att multiplicera med* $[j]_n$. *Om nu* $m \cdot j \equiv_n 1$ *så finns det ett heltal k så att* $m \cdot j = 1 + k \cdot n$. *Om nu* $d > 0$, $d|m$ *och* $d|n$ *så gäller* $d|(m \cdot j - k \cdot n)$ *dvs.* $d|1$ *och då är* $d = 1$. *Därför måste* $\text{sgd}\,(m,n) = 1$. *Man kan också visa att det omvända gäller så att*

$$[m]_n \text{ är inverterbar i } \mathbb{Z}/n\mathbb{Z} \quad \Leftrightarrow \quad \text{sgd}\,(m,n) = 1.$$

Obs

Om p är ett primtal så är alla element i $\mathbb{Z}/p\mathbb{Z}$ *som inte är* $[0]_p$ *inverterbara.*

Exempel

Kongruensklasserna $[1]_6$ *och* $[5]_6$ *är de enda som är inverterbara i* $\mathbb{Z}_6$.

Euklides algoritm för att räkna sgd (m, n)

- *Antag att* $m > n$ *(*$\text{sgd}(m, m) = m$*).*
- *Låt* $r_0 = m$ *och* $r_1 = n$*.*
- *Räkna ut* q_i *och* r_i *så att* $0 \leq r_i < r_{i-1}$ *och*

$$r_{i-2} = q_i r_{i-1} + r_i$$

  då $i \geq 2$ *så länge* $r_{i-1} \neq 0$*.*
- $\text{sgd}(m, n) = r_{k-1}$ *om* $r_k = 0$*.*

Varför fungerar Euklides algoritm?

Det följer av ett allmänt resultat att om $r_{i-2} = q_i r_{i-1} + r_i$ *så är* $\text{sgd}(r_{i-2}, r_{i-1}) = \text{sgd}(r_{i-1}, r_i)$ *för alla* $i \geq 2$ *för vilka* $r_{i-1} \neq 0$*. Eftersom* $d|0$ *för alla* d *gäller* $\text{sgd}(r_{k-1}, 0) = r_{k-1}$ *vilket innebär att* $\text{sgd}(m, n) = \text{sgd}(r_0, r_1) = \ldots = \text{sgd}(r_{k-1}, r_k) = \text{sgd}(r_{k-1}, 0) = r_{k-1}$ *om* $r_k = 0$*.*

Euklides algoritm

Om vi vill räkna ut $\text{sgd}(634, 36)$ *så får vi följande resultat:*

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

så att $\text{sgd}(634, 36) = 2$*.*

Euklides algoritm och inversa element i $\mathbb{Z}/n\mathbb{Z}$

Om man i Euklides algoritm valt $r_0 = m$, $r_1 = n$ *och sedan räknat* q_i *och* r_i *för* $i = 2, \ldots, k$ *med formeln* $r_{i-2} = q_i r_{i-1} + r_i$ *tills* $r_k = 0$, *så att* $r_{k-1} = \operatorname{sgd}(m, n)$ *så kan man räkna baklänges så att man startar med ekvationen* $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ *så får man*

$$\operatorname{sgd}(m, n) = r_{k-1} = r_{k-3} - q_{k-1} r_{k-2}.$$

Sedan sätter man in r_{k-2} *ur ekvationen* $r_{k-2} = r_{k-4} - q_{k-2} r_{k-3}$ *och uttrycker* $\operatorname{sgd}(m, n)$ *med hjälp av* r_{k-4} *och* r_{k-3} *och fortsätter tills man får*

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

Om nu $\operatorname{sgd}(m, n) = 1$ *betyder dethär att*

$$[a]_n \cdot [m]_n = [1]_n \quad \textit{dvs.} \quad [a]_n = [m]_n^{-1},$$

och

$$[b]_m \cdot [n]_m = [1]_m \quad \textit{dvs.} \quad [b]_m = [n]_m^{-1}.$$

Inversen av en kongurensklass

Om man vill räkna $[23]_{67}^{-1}$ *räknar man först ut* $\operatorname{sgd}(67, 23)$ *och får*

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

För att uttrycka $\operatorname{sgd}(67, 23)$ *med hjälp av* 67 *och* 23 *räknar vi baklänges:*

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

Dethär innebär att $(-32) \cdot 23 = 1 - 11 \cdot 67$ *så att* $(-32) \cdot 23 \equiv_{67} 1$ *eller* $[-32]_{67} \cdot [23]_{67} = [1]_{67}$ *vilket är detsamma som att*

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

Hur många räkenoperationer behövs i Euklides algoritm för att räkna ut $\gcd(m,n)$

Antag att $m > n$. I Euklides algoritm väljer vi $r_0 = m$, $r_1 = n$ och räknar sedan ut r_i och q_i så att $r_{i-2} = q_i r_{i-1} + r_i$ för $i \geq 2$ tills vi fått $r_M = 0$ och då är $r_{M-1} = \gcd(m,n)$. För detta behövs alltså $M-1$ "divisioner med rest". Nu skall vi alltså uppskatta hur stort M kan vara och för det låter vi $x_1 = 1$, $x_2 = 2$ och

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

Nu vet vi att $r_{M-1} \geq x_1$ och $r_{M-2} \geq x_2$ eftersom $r_{M-2} > r_{M-1}$. Om vi nu antar att $r_{M-j} \geq x_j$ för $1 \leq j \leq k$ så får vi, eftersom $q_{M-k+1} \geq 1$ att

$$r_{M-(k+1)} = q_{M-k+1} r_{M-k} + r_{M-k+1} \geq r_{M-k} + r_{M-k+1} \geq x_k + x_{k-1} = x_{k+1}.$$

Av induktionsprincipen följer nu att $r_{M-j} \geq x_j$ för alla $j = 1, \ldots, M$.

Hur många räkenoperationer behövs i Euklides algoritm för att räkna ut $\gcd(m,n)$, forts.

Man kan lösa ekvation ($\star$) men det är enklare att visa med induktion att $x_j \geq \left(\frac{1+\sqrt{5}}{2}\right)^{j-1}$ då $j \geq 1$ (genom att konstatera att $x_1 = 1 = \left(\frac{1+\sqrt{5}}{2}\right)^{1-1}$, $x_2 = 2 \geq \left(\frac{1+\sqrt{5}}{2}\right)^{2-1}$ och att $\left(\frac{1+\sqrt{5}}{2}\right)^{j+1-1} + \left(\frac{1+\sqrt{5}}{2}\right)^{j-1} = \left(\frac{1+\sqrt{5}}{2}\right)^{j+2-1}$) och dethär innebär att

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

av vilket följer att

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

eller, antalet räkningar för att bestämma $\gcd(m,n)$ är av storleksordningen $O(\log(\max(m,n)))$.

Eulers φ-funktion

$$\varphi(n) = \textit{antalet tal i mängden } \{\, m \in \mathbb{Z} : 0 \leq m \leq n-1, \operatorname{sgd}(m,n) = 1 \,\},$$
$$= \textit{antalet element i } \mathbb{Z}/n\mathbb{Z} \textit{ som har en en invers.}$$

Notera att $[0]_1$ *är inverterbar i* $\mathbb{Z}/1\mathbb{Z}$ *så att* $\varphi(1) = 1$ *men* $[0]_n$ *är förstås (?) inte inverterbar i* $\mathbb{Z}/n\mathbb{Z}$ *då* $n > 1$.

Eulers teorem

Om $\operatorname{sgd}(a,n) = 1$ *och* $n > 1$ *så är*

$$a^{\varphi(n)} \equiv_n 1.$$

Eulers teorem, bevis

Antag att $[x_1]_n, \ldots, [x_{\varphi(n)}]$ *är de invertibla elementen i* $\mathbb{Z}/n\mathbb{Z}$.
Eftersom $\operatorname{sgd}(a,n) = 1$ *har också* $[a]_n$ *en invers och eftersom* $[\alpha]_n \cdot [\beta]_n$ *är invertibelt om* $[\alpha]_n$ *och* $[\beta]_n$ *är det, är också* $[a]_n \cdot [x_j]$ *invertibelt för alla* j.
Om nu $[a]_n \cdot [x_j]_n = [a]_n \cdot [x_k]_n$ *så är*
$[x_j]_n = [a]_n^{-1} \cdot [a]_n \cdot [x_j]_n = [a]_n^{-1} \cdot [a]_n \cdot [x_k]_n = [x_k]_n$ *vilket innebär att elementen* $[a]_n \cdot [x_1]_n, \ldots [a]_n \cdot [x_{\varphi(n)}]_n$ *är elementen* $[x_1]_n, \ldots, [x_{\varphi(n)}]$ *eventuellt i en annan ordning.*
Men produkterna är desamma, dvs.

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

Eftersom varje element $[x_i]_n$ *är inverterbart, kan vi dividera bort alla* $[x_i]_n$ *och slutresultatet är att* $[a]_n^{\varphi(n)} = [1]_n$ *dvs.* $\operatorname{mod}(a^{\varphi(n)}, n) = 1$.

Fermats lilla teorem

Om p är ett primtal och $\text{sgd}\,(a,p)=1$ *så är*

$$a^{p-1}\equiv_p 1.$$

Potenser i $\mathbb{Z}/p\mathbb{Z}$ då p är ett primtal

Om man skall räkna ut $\text{mod}\,(a^m,p)$ *då p är ett primtal får man naturligtvis* 0 *om* $\text{sgd}\,(a,p)\neq 1$ *(för då är* $\text{sgd}\,(a,p)=p$ *och $p|a$ eftersom p är ett primtal) och annars kan man utnyttja det faktum att* $a^{p-1}\equiv_p 1$ *för det innebär att* $a^m\equiv_p a^{\text{mod}\,(m,p-1)}$ *vilket kan vara mycket enklare att räkna ut.*

RSA-algoritmen

I RSA-algoritmen används en publik nyckel (n,k) *för kryptering och en privat nyckel* (n,d) *för dekryptering:*

- *Kryptering: "Meddelandet" a, som är ett tal mellan* 0 *och* $n-1$ *krypteras till* $b=\text{mod}\,(a^k,n)$.
- *Det mottagna meddelandet b dekrypteras till* $a=\text{mod}\,(b^d,n)$.

Idéen är den att vem som helst kan skicka meddelanden krypterade med den publika nyckeln men bara den som känner till den privata nyckeln, som är "svår" at räkna ut bara med hjälp av n och k, kan dekryptera meddelandet.

Hur skall nycklarna i RSA-algoritmen väljas?

- *$n = pq$ där p och q är två olika "mycket stora" primtal.*
- *k är ett "inte alltför litet" tal så att $sgd(k, m) = 1$ där $m = (p-1)\cdot(q-1)$ (och det "svåra" med att räkna ut d är att bestämma p och q och därmed m om man bara känner till n).*
- *Med hjälp av Euklides algoritm kan d bestämmas så att $[d]_m = [k]_m^{-1}$.*

Varför fungerar RSA-algoritmen?

- *Antag för enkelhets skull att* $\text{sgd}\,(a, n) = 1$.
- *Man kan visa att $\varphi(n) = m$.*
- *Enligt Eulers teorem gäller $a^m \equiv_n 1$ eller $[a^m]_n = [1]_n$.*
- *Eftersom $k \cdot d = 1 + r \cdot m$ är*

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

vilket betyder att $\text{mod}\,(b^d, n) = \text{mod}\,(a, n) = a$.

Vad händer i RSA-algoritmen om $\text{sgd}\,(a, n) \neq 1$?

- *Eftersom man antar att $0 < a < n$ så är* $\text{sgd}\,(a, n) \neq 1$ *endast då $p|a$ eller $q|a$. Anta att $p|a$ så att $a = p^j \cdot c$ där* $\text{sgd}\,(c, n) = 1$
- *Nu är $[b^d]_n = [((p^j \cdot c)^k)^d]_n = [(p^k)^d]_n^j \cdot [(c^k)^d]_n$ och eftersom* $\text{sgd}\,(c, n) = 1$ *så är $[(c^k)^d]_n = [c]_n$ och det återstår att visa att $[(p^k)^d]_n = [p]_n$ för då är $[b^d]_n = [p]_n^j \cdot [c]_n = [p^j \cdot c]_n = [a]_n$.*
- *Eftersom q är ett primtal och $p \neq q$ så är* $\text{sgd}\,(p, q) = 1$ *och därför följer det av enligt Fermats teorem att $p^{q-1} \equiv_q 1$.*
- *Då är också $p^{(q-1)(p-1)r} \equiv_q 1$ dvs. $p^{(q-1)(p-1)r} = 1 + sq$ och därför också $p^{1+(q-1)(p-1)r} = p + spq$ dvs. $[p^{1+m\cdot r}]_n = [p]_n$ vilket visar att $[(p^k)^d]_n = [p]_n$ eftersom $k \cdot d = 1 + m \cdot r$.*

Algoritmen fungerar alltså också i detta fall!

RSA-algoritmen

Om man med RSA-algoritmen skall kryptera meddelandet 9 *och använda den publika nyckeln* $(55, 23)$ *så skall man räkna ut* $\bmod(9^{23}, 55)$. *För att göra räkningen enklare observerar vi först att*
$23 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0$ *så att*
$9^{23} = 9^{16} \cdot 9^4 \cdot 9^2 \cdot 9 = (((9^2)^2)^2)^2 \cdot (9^2)^2 \cdot 9^2 \cdot 9$ *och man får*

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

så att $\bmod(9^{23}, 55) = 14$.

RSA-algoritmen, forts.

Om man vill dekryptera meddelandet 14 *måste man känna till den privata nyckeln och den är* $(55, 7)$ *därför att* $55 = 5 \cdot 11$, $(5-1) \cdot (11-1) = 40$ *och* $\bmod(23 \cdot 7, 40) = \bmod(161, 40) = 1$. *För dekryptering observerar man att* $7 = 4 + 2 + 1 = 2^2 + 2^1 + 2^0$ *så att* $14^7 = 14^4 \cdot 14^2 \cdot 14$ *och man får*

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

så att $\bmod(14^7, 55) = 9$.

Underskrifter och RSA-algoritmen

Antag att A vill skicka meddelandet a till B och övertyga B om att meddelandet verkligen kommer från A. De kan göra detta på följande sätt:

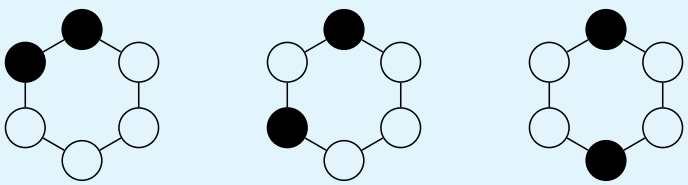
- *A räknar ut ett "sammandrag" $h(a)$ av a (ur vilket a inte kan bestämmas).*
- *A krypterar a med B:s publika nyckel (n_B, k_B) till $b = \mathrm{mod}\,(a^{k_B}, n_B)$.*
- *A krypterar $h(a)$ med sin egna privata nyckel (n_A, d_A) till $s = \mathrm{mod}\,(h(a)^{d_A}, n_A)$.*
- *A skickar b och s till B.*
- *B dekrypterar b med sin privata nyckel (n_B, d_B) till a.*
- *B räknar ut $h(a)$ och dekrypterar s med A:s publika nyckel (n_A, k_A) och om resultatet är samma som $h(a)$ så är det troligt att meddelandet a verkligen kom från A eftersom ingen annan borde kunna kryptera $h(a)$ med A:s privata nyckel (n_A, d_a).*

Det faktum att ett meddelande krypterat med (n_A, d_A) kan dekrypteras med (n_A, k_A) följer av att om $[d_A]_{m_A} = [k_A]_{m_A}^{-1}$ så är $[k_A]_{m_A} = [d_A]_{m_A}^{-1}$, dvs. de publika och privata nycklarna är utbytbara.

Ett färgningsproblem

Antag att man har 6 bollar. På hur många sätt kan man färga 2 bollar svart och resten vita?

- *Om bollarna är identiska finns det bara ett sätt, 2 blir svarta och 4 vita.*
- *Om bollarna är numrerade finns det $\binom{6}{2} = 15$ sätt att välja ut de som skall bli svarta och resten vita.*
- *Om bollarna ligger i hörnen på en reguljär 6-hörning och man kan vända och vrida på 6-hörningen finns det 3 alternativ som är:*



Hur skall man lösa mera komplicerade problem av den tredje typen? Observera också att "färgning" inte skall tas för bokstavligt: Bilderna ovan kan också tex. representera tre isomerer av xylen (C_8H_{10}) där två väteatomer i bensen bytts ut mot metylgrupper.

Grupper

En grupp är ett par $[G, \bullet]$ där G är en mängd och $\bullet$ en funktion $G \times G \to G$ så att

- *Slutenhet: $x \bullet y \in G$ ifall x och $y \in G$.* *(En följd av att $\bullet$ är en funktion $G \times G \to G$.)*
- *Associativitet: $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ ifall x, y och $z \in G$.*
- *Identitetselement: Det finns ett element $e \in G$* *(som visar sig vara entydigt)* *så att $e \bullet x = x \bullet e = x$ ifall $x \in G$.*
- *Inverst element: Om $x \in G$, så finns det ett element $x' \in G$ så att $x \bullet x' = x' \bullet x = e$.*

Obs!

- *Man säger ofta att "G är en grupp" om det är klart vad gruppoperationen är eller om det inte har så stor betydelse.*
- *Istället för att skriva $x \bullet y$ (eller ens $\bullet(x, y)$) kan man skriva xy och eftersom man kan visa att det inversa elementet är entydigt så skrivs det ofta som x^{-1}. Identitetselementet kan också skrivas som 1 eller I, beroende på sammanhanget.*

Kommutativa eller abelska grupper

Om $[G, \bullet]$ är en grupp så att $a \bullet b = b \bullet a$ för alla a och $b \in G$ så sägs gruppen vara **kommutativ** *eller* **abelsk**. *I detta fall använder man ofta $+$ som beteckning för gruppoperationen, 0 som identitetselement och $-a$ för inversen av a.*

Delgrupper

Antag att G (dvs. $[G, \bullet]$) är en grupp. En icke-tom delmängd H av G är en delgrupp av G om följande villkor gäller och då är H (egentligen $[H, \bullet]$) också en grupp:

- *Om x och $y \in H$ så gäller $x \bullet y \in H$.*
- *Om $x \in H$ så gäller $x^{-1} \in H$.*

Om H är ändlig så följer det senare villkoret av det första *eftersom $x^m \in H$ för alla $m \geq 1$ och eftersom $|H| < \infty$ så finns det ett tal $m > k \geq 1$ så att $x^m = x^k$ men då är $x^{m-k} = e$ och då är antingen $x = e$ om $m = k + 1$ eller så är $m > k + 1$ och då är $x^{-1} = x^{m+k-1} \in H$.*

Homomorfismer och isomorfismer

Antag att $[G_1, \bullet_1]$ *och* $[G_2, \bullet_2]$ *är två grupper och* ψ *är en funktion:* $G_1 \to G_2$.

- ψ *är en* **homomorfism** *ifall* $\psi(x \bullet_1 y) = \psi(x) \bullet_2 \psi(y)$ *för alla* x *och* $y \in G_1$.
- ψ *är en* **isomorfism** *ifall den är en homomorfism och en bijektion (och då är också* ψ^{-1} *en homomorfism).*

Det är inget speciellt med grupper här, det är frågan om att en homoformism "bevarar strukturen"!

Cykliska grupper

En grupp G *är cyklisk om det finns ett element* $x \in G$ *så att varje element i* G *är någon potens* x^j *av* x *där* $j \in \mathbb{Z}$. *I detta fall säger man att* G *genereras av* x *och man skriver* $G = \langle x \rangle$.
Om G *är en grupp och* $x \in G$ *så är gruppen* $\langle x \rangle = \{ x^j : j \in \mathbb{Z} \}$ *genererad av* x *en delgrupp av* G.
Eftersom alla cykliska grupper med m *element är isomorfa så betecknar man en sådan grupp med* C_m.

En grupps och ett elements ordning

Antag att G *är en grupp.*

- *Gruppen* G*:s ordning är antalet element* $|G|$ *i gruppen.*
- *Ett elements* $g \in G$ *ordning är* $\inf\{ j \geq 1 : g^j = e \}$ *och detta är ordningen av den cykliska gruppen genererad av* g.

Permutationer

En **permutation** *av en (ändlig) mängd* A *är en bijektion* $A \to A$.

- *Mängden av alla permutationer av en mängd* A *är en grupp då gruppoperationen är sammansättning av funktioner. Eftersom alla sådana grupper av permutationer av en mängd med* m *element är isomorfa så betecknar man en sådan grupp med* S_m.
- *Varje grupp* $[G, \bullet]$ *är isomorf med en delgrupp av gruppen av permutationer av en mängd, eftersom mängden kan tas som* G *och isomorfismen som* $\psi(a)(b) = a \bullet b$ *men detta betyder inte att det alltid är nyttigt eller nödvändigt att tänka på gruppen på dethär sättet.*

Permutationer, banor, cykelnotation

Antag att A är en ändlig (icke-tom) mängd.

- *Om α är en permutation av A så är α:s* **banor** *minsta möjliga delmängder $A_j \subset A$, $j = 1, 2, \ldots m$ så att $A_j \cap A_k = \emptyset$ då $j \neq k$, $\cup_{j=1}^{m} A_j = A$ och $\alpha(A_j) = \{\, \alpha(x) : x \in A_j \,\} = A_j$.*
- *En* **cykel** *är en permutation α så att $\alpha(x_j) = x_{j+1}$, $j = 1, 2, \ldots, k-1$ och $\alpha(x_k) = x_1$ där $x_1, x_2, \ldots, x_k \in A$ och $\alpha(x) = x$ för alla $x \in A \setminus \{x_1, \ldots, x_k\}$. Cykeln α skrivs med* **cykelnotation** *som $\alpha = \begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}$.* **Längden** *av en sådan cykel α är k och α sägs vara en k-cykel. Cykeln α:s banor är $\{x_1, x_2, \ldots, x_k\}$ och mängderna $\{x\}$ för alla $x \in A \setminus \{x_1, \ldots, x_k\}$.*

Obs!

Permutationen α:s banor kan också definieras som ekvivalensklasserna för en relation där $x \sim y$ ifall $\alpha^j(x) = y$ för något $j \in \mathbb{Z}$.

Permutationer och cykelnotation

Låt $A = \{1, 2, 3, 4, 5, 6, 7\}$ och antag att α är permutationen

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

av A där alltså detta skrivsätt betyder att tex. $\alpha(1) = 2$ och $\alpha(4) = 3$. Nu ser vi att $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$ (dvs. $\alpha(1) = 2$, $\alpha(2) = 4$ osv.) och detta ger cykeln $\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ som alltså är en permutation β_1 så att $\beta_1(1) = 2$, $\beta_1(2) = 4$, $\beta_1(4) = 3$, $\beta_1(3) = 1$ och $\beta_1(x) = x$ för alla $x \in \{5, 6, 7\}$. Eftersom $\alpha(5) = 5$ får vi cykeln $\beta_2 = (5)$ för vilken alltså $\beta_2(x) = x$ för alla $x \in A$. Slutligen ser vi att $6 \mapsto 7 \mapsto 6$ vilket ger cykeln $\begin{pmatrix} 6 & 7 \end{pmatrix}$. Med cykelnotation kan vi nu skriva α som

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

eftersom β_2 är identitetsfunktionen. Men det finns också många andra sätt att skriva α som en produkt av cykler, tex. $\alpha = \begin{pmatrix} 7 & 6 \end{pmatrix} \begin{pmatrix} 4 & 3 & 1 & 2 \end{pmatrix}$. Mängderna $A_1 = \{1, 2, 4, 3\}$, $A_2 = \{5\}$ och $A_3 = \{6, 7\}$ är permutationens banor eftersom $\cup_{j=1}^{3} A_j = A$, $A_j \cap A_k = \emptyset$ då $j \neq k$, $\alpha(A_j) = A_j$, $j = 1, 2, 3$ och det finns inga mindre mängder med dessa egenskaper.

Jämna och udda permutationer

- *Varje cykel med längden $k \geq 2$ kan skrivas som produkten av $k-1$ cykler med med längden 2 eftersom* $(x_1 \quad x_2 \quad \dots \quad x_k) = (x_1 \quad x_k)(x_1 \quad x_{k-1}) \dots (x_1 \quad x_3)(x_1 \quad x_2)$.
- *Varje permutation kan skrivas som en produkt av cykler med längden 2 (och 1).*
- *En permutation kan i allmänhet skrivas på flera sätt som en produkt av cykler med längden 2 men om permutationen α kan skrivas som en produkt av r, och som en produkt av r', cykler med längden 2 så är $(-1)^r = (-1)^{r'}$ och därför kan man definiera cykelns* **tecken** *med* $\operatorname{sign}(\alpha) = (-1)^r$.
- *Om α är en cykel med längden k så är* $\operatorname{sign}(\alpha) = (-1)^{k+1}$.
- *Om α är en permutation av en mängd med n element och α har m banor så är* $\operatorname{sign}(\alpha) = (-1)^{n-m}$.
- *En permutation α sägs vara* **jämn** *om* $\operatorname{sign}(\alpha) = 1$ *och* **udda** *annars.*
- *Om α och β är permutationer av samma mängd så är* $\operatorname{sign}(\alpha\beta) = \operatorname{sign}(\alpha)\operatorname{sign}(\beta)$.

Sidoklasser

Antag att G är en grupp, H är en delgrupp i G och $a \in G$.

- *Mängden $aH = \{ ax : x \in H \}$ är den* **vänstra sidoklassen** *av H som innehåller a.*
- *Mängden $Ha = \{ xa : x \in H \}$ är den* **högra sidoklassen** *av H som innehåller a.*

Sidoklasserna har följande egenskaper (som här endast formulerats för de vänstra sidoklasserna):

- $|aH| = |H|$ *för alla $a \in G$.*
- *Om a och $b \in G$ så är antingen $aH = bH$ eller $aH \cap bH = \emptyset$.*
- $\cup_{a \in G} aH = G$.
- *Om a och $b \in G$ och $aH = bH$ så gäller $b^{-1}a \in H$.*
- $|G| = |H| \cdot |\{ aH : a \in G \}|$ *och därför delar talet $|H|$ talet $|G|$.*

Homomorfismer, normala delgrupper och kvotgrupper

Antag att G är en grupp.

- *Om G' är en grupp med identitetselement e' och $\psi : G \to G'$ är en homomorfism så är $H = \{ x \in G : \psi(x) = e' \}$ (kärnan av ψ) en delgrupp i G.*
- *En delgrupp H i G har formen $\{ x \in G : \psi(x) = e' \}$ för någon homomorfism $G \to G'$ om och endast om $aH = Ha$ för alla $a \in G$ (eller ekvivalent, $axa^{-1} \in H$ för alla $a \in G$ och $x \in H$). I detta fall säger man att H är en* **normal** *delgrupp.*
- *Om H är en normal delgrupp i G så bildar sidoklasserna (med de vänstra och högra indentiska) en* **kvotgrupp**, *som betecknas med G/H, och som har gruppeoperationen operation $(aH)(bH) = (ab)H$, identitetselement H och invers $(aH)^{-1} = a^{-1}H$. Funktionen $\psi : G \to G/H$ definierad med $\psi(a) = aH$ är en homomorfism med kärna H.*

En rät linje som en sidoklass

$[\mathbb{R}^2, +]$ är en grupp med origo som identitetselement och inversen av $\mathbf{v}$ är $-\mathbf{v}$. Antag att $\mathbf{u} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}$. Då är $H = \{ t\mathbf{u} : t \in \mathbb{R} \}$ en delgrupp i $[\mathbb{R}^n, +]$ och sidoklassen $\mathbf{u} + H$ är mängden av alla (eller ortsvektorer till) punkter på linjen genom $\mathbf{u}$ med riktning $\mathbf{u}$.

Kongruensklasser som kvotgrupper

Antag att $n \geq 1$. Nu är $[\mathbb{Z}, +]$ en grupp och $n\mathbb{Z} = \{ n \cdot j : j \in \mathbb{Z} \}$ är en delgrupp i $[\mathbb{Z}, +]$ och eftersom addition är kommutativ $(a+b=b+a)$ så är den en normal delgrupp. Sidoklasserna till $n\mathbb{Z}$ är kongruensklasserna modulo n och de bildar kvotgruppen $\mathbb{Z}/n\mathbb{Z}$ med addition som operation.

Gruppverkan

Om G dvs. $[G, \bullet]$ är en grupp och X är en mängd så är **gruppverkan** *av G på mängden X en homomorfism från G till gruppen av permutationer: $X \to X$.*
Om man definerar sammansatta funktioner med $(f \circ g)(x) = f(g(x))$ så får man en **vänstergruppverkan** *och om man definierar den med $x.(f \circ g) = (x.f).g$ så får man en* **högergruppverkan** *. Istället för att skriva $\psi(a)(x)$ där ψ är homomorfismen, $a \in G$ och $x \in X$ skriver man ofta ax och säger att G **verkar** på X. För en vänstergruppverkan blir homomorfismegenskapen då $(ab)x = a(bx)$, $a, b \in G$, $x \in X$.*

Obs!

- *Om G är en grupp permutationer av X så är identititetsavbildningen homomorfismen och hela begreppet gruppverkan behövs inte.*
- *Om G är en grupp kan man definiera dess gruppverkan på sig själv tex. med $\psi(a)(x) = ax$ (en vänstergruppverkan), med $\psi(a)(x) = axa^{-1}$ (en vänstergruppverkan), med $\psi(a)(x) = xa$ (en högergruppverkan) eller med $\psi(a)(x) = a^{-1}xa$ (en högergruppverkan).*

Banor och stabilisatorer

Antag att G är en grupp som verkar på en mängd X (från vänster).

- *Om $x \in X$ så är dess* **bana** *under verkan av G mängden $Gx = \{ gx : g \in G \} \subset X$.*
- *Om $x \in X$ så är dess* **bana** *under verkan av ett element $g \in G$ mängden $\langle g \rangle x = \{ g^j x : j \in \mathbb{Z} \} \subset X$. ($\langle g \rangle$ är den cykliska gruppen genererad av g.)*
- *Om $x \in X$ så är dess* **stabilisator** *under verkan av G mängden $G_x = \{ g \in G : gx = x \}$ som är en delgrupp i G.*
- *För varje $x \in X$ gäller $|Gx| \cdot |G_x| = |G|$.*

Obs!

Om G verkar på X så kan man definiera en ekvivalensrelation $\sim$ i X med $x \sim y$ om och endast om $x = gy$ för något $g \in G$. Banorna är då ekvivalensklasserna och ofta kan det vara nyttigt att tänka på element i samma ekvivalensklass som om de vore desamma.

Cykelindex

- **Cykelindexet** *för en permutation g av X eller ett element g i en grupp som verkar på X är monomet*

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

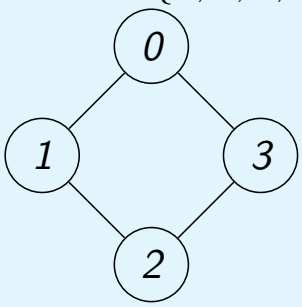
där j_k är antalet banor med längden k under verkan av g.

- **Cykelindexet** *för en grupp G av permutationer av X eller en grupp G som verkar på X är*

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

Symmetrier i en 4-hörning

Låt $X = \{0, 1, 2, 3\}$. Eftersom det finns 4 element i X så finns det $4! = 24$ permutationer av X. Men om elementen i X är noder i grafen till vänster och man kräver av en permutation α att om x och y är grannar, dvs. det finns en båge mellan c och y, så är också $\alpha(x)$ och $\alpha(y)$ grannar (dvs. man kräver att α är en graf-isomorfism) så blir situationen en annan. I en sådan permutation kan 0 avbildas på vilken som helst av noderna 0, 1, 2 eller 3. Men $\alpha(1)$ skall vara en granne till $\alpha(0)$ vilket betyder att $\alpha(1) = \mod(\alpha(0) + 1, 4)$ eller $\mod(\alpha(0) - 1, 4)$. Eftersom $\alpha(2)$ inte skall vara en granne till $\alpha(0)$ måste vi ha $\alpha(2) = \mod(\alpha(0) + 2, 4)$ och på samma sätt får vi att $\alpha(3) = \mod(\alpha(1) + 2, 4)$.



Vi får alltså följande permutationer skrivna med cykelnotation:
(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) *och* (0 3)(1 2) *av vilka 4 är rotationer och 4 reflektioner.*
Gruppen som dessa permutationer är en sk. dihedral grupp och betecknas med D_4.

Symmetrier i en 4-hörning, forts.

Om man nu vill använda Pólyas teorem för att räkna ut på hur många sätt man kan färga noderna i grafen så att man har en svart, en vit och två röda noder och om man säger att två färgningar är olika om man inte får den ena av andra genom att tillämpa en permutation i D_4 på grafen så skall man först räkna ut cykelindexet som i detta fall blir

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

Antalet icke-ekvivalenta färgningar en svart, en vit och två röda noder blir nu koefficienten för svr^2 i polynomet
$\zeta_{D_4,X}(s+v+r,s^2+v^2+r^2,s^3+v^3+t^3,s^4+v^4+r^4)$.
Eftersom svr^2 bara kan förekomma i termerna som motsvarar $\frac{1}{8}t_1^4$ och $\frac{1}{8}2t_1^2t_2$ så skall vi bestämma koefficienten för svr^2 i polynomet

$$\frac{1}{8}(s+v+r)^4+\frac{1}{4}(s+v+r)^2(s^2+v^2+r^2),$$

och den blir

$$\frac{1}{8}\cdot\frac{4!}{1!\cdot1!\cdot2!}+\frac{1}{4}\cdot2=2.$$

Antalet banor under verkan av en grupp (Burnsides lemma)

Antag att (den ändliga) gruppen G verkar på mängden X. Definiera för varje $g\in G$ mängden X_g av **fixpunkter** *till g med*

$$X_g=\{\,x\in X:gx=x\,\}.$$

(Denhär mängden betecknas ibland också med X^g eller $F(g)$.) Då är antalet banor i X under verkan av G

$$\frac{1}{|G|}\sum_{g\in G}|X_g|.$$

Gruppverkan och "färgningar"

Antag att gruppen G verkar på en mängd X.

- *En "färgning" av X är en funktion $\omega : X \to K$ där K är en mängd "färger". Gruppen G verkar på mängden K^X av alla färgningar med $(g\omega)(x) = \omega(g^{-1}x)$. Om $\Omega \subset K^X$ är en delmängd av mängden färgningar av X så verkar G på Ω förutsatt att $G\Omega = \Omega$.*
- *Dethär är en vänstergruppverkan eftersom*

$$(g(h\omega))(x) = (h\omega)(g^{-1}x) = \omega(h^{-1}g^{-1}x) = \omega((gh)^{-1}x) = ((gh)\omega)(x).$$

- *Gruppverkan av G på en mängd färgningar bestämmer en ekvivalensrelation så att färgningar som hör till samma bana i G:s verkan på Ω är ekvivalenta, dvs. $\omega \sim \eta$ om och endast om $\omega = g\eta$ för något $g \in G$ och då kan man anse att dessa färgningar är desamma.*
- *Antalet färgningar i Ω som inte är ekvivalenta under verkan av G är*

$$\frac{1}{|G|}\sum_{g\in G}|\Omega_g|$$

där $\Omega_g = \{\, \omega \in \Omega : g\omega = \omega \,\}$ är mängden av fixpunkter till g.

Vilka färgningar är invarianta under verkan av ett gruppelelement g?

Antag att gruppen G verkar på mängden X. Antag att $g \in G$ och att $B_{g,1}, B_{g,2}, \ldots B_{g,m_g}$ är banorna i X under verkan av g, dvs. banorna i gruppverkan av den cykliska gruppen $\{\, g^j : j \in \mathbb{Z} \,\}$ på X.
Om ω är en färgning av X (dvs. en funktion: $X \to K$ där K är en mängd färger) då är $g\omega = \omega$ om och endast om ω är konstant på varje bana $B_{g,j}$, $j = 1, \ldots, m_g$.

Varför?

Eftersom $g\omega = \omega$ så gäller $g^j\omega = \omega$ för alla $j \in \mathbb{Z}$. Om nu x och y hör till samma bana under verkan av g så finns det ett tal j så att $g^j x = y$ eller $g^{-j}y = x$. Enligt definitionen av gruppverkan på färgningar $((g\omega)(x) = \omega(g^{-1}x))$ och det faktum att $g^j\omega = \omega$ så får vi

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

Om igen ω är konstant på alla banor så är $\omega(x) = \omega(g^{-1}x)$ för alla $x \in X$. Detta betyder att $\omega(x) = (g\omega)(x)$ för alla x, dvs. $\omega = g\omega$.

Pólyas teorem om antalet "färgningar"

Antag att gruppen G verkar på mängden X och låt K^X vara mängden av färgningar av X med "färgerna" $K = \{f_1, f_2, \ldots, f_r\}$. Då är koefficienten av monomet

$$f_1^{i_1} \cdot f_2^{i_2} \cdot \ldots \cdot f_r^{i_r}$$

i polynomet

$$\zeta_{G,X}(f_1^1 + \ldots + f_r^1, f_1^2 + \ldots + f_r^2, \ldots, f_1^n + \ldots + f_r^n)$$

antalet färgningar av X som använder färgen f_j exakt i_j gånger (dvs. $|\{ x : \omega(x) = f_j \}| = i_j$) och som inte är ekvivalenta under verkan av G.

Om man använder r färger men inte har andra begränsingar så är $\zeta_{G,X}(r, r, \ldots, r)$ antalet färgningar av X som inte är ekvivalenta under verkan av G.

Pólyas teorem och "tre-i-rad"

Antag att man på ett papper ritat 3×3 och i 2 rutor skrivit ett x:s, i 2 rutor ett o och 5 rutor är ännu tomma. Det finns $\binom{9}{2,2,5} = 756$ olika sätt att göra detta om man håller pappret fixerat. Men om vi kan vrida pappret med vinkeln 0, $\frac{\pi}{2}$, π eller $\frac{3\pi}{2}$ runt mittpunkten så minskar antalet alternativ och för att bestämma detta antal på ett systematiskt sätt skall vi undersöka hur gruppen som genereras av en rotation med vinkeln $\frac{\pi}{2}$ verkar på rutorna och i synnerhet bestämma dess cykelindex, dvs. bestämma banornas längder. Resultaten är följande:
Identiteten (vridning med vinkeln 0) har 9 banorsom alla innehåller 1 element.
En vridning med vinkeln $\frac{\pi}{2}$ har 2 banor som båda innehåller 4 element (den ena består av hörnen och den andra de yttre rutorna mellan hörnen) och 1 bana som innehåller 1 element (rutan i mitten). Samma gäller om man vrider med vinkeln $\frac{3\pi}{2}$ vilket är detsamma som att vrida vinkeln $\frac{\pi}{2}$ i negativ riktning.

Pólyas teorem och "tre-i-rad", forts.

Om vi vrider pappret med vinkeln π får vi 4 banor som innehåller 2 rutor (motsatta hörn och motsatta ytterrutor mellan hörnen) och 1 bana som består av 1 ruta.
Cykelindexet blir därför

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

För att bestämma antalet icke-ekvivalenta färgningar så ersätter vi t_j med $x^j + o^j + t^j$ i detta uttryck och då är koefficienten för termen $x^2o^2t^5$ antalet icke-ekvivalenta färgningar med 2 stycken x, 2 stycken o och 5 stycken t. Denhär koefficienten blir

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

Normala delgrupper och kvotgrupper

Antag att G är en grupp och att H är en delgrupp av G.

- *$aH = Ha$ för alla $a \in G$ om och endast om $axa^{-1} \in H$ för alla $a \in G$ och $x \in H$.*
  Varför? Antag att $a \in G$ och $x \in H$. Nu gäller $ax \in aH$ så att om $aH = Ha$ så finns det ett $y \in H$ så att $ax = ya$. Men då är $axa^{-1} = y \in H$. Ifall, å andra sidan, $axa^{-1} = y \in H$ så då är $ax = ya$ så att $aH \subset Ha$. Men om vi tar a^{-1} istället för a så får vi $a^{-1}H \subset Ha^{-1}$ från vilket det följer att $Ha = aa^{-1}Ha \subset aHa^{-1}a = aH$ också gäller.
- *Om $aH = Ha$ för alla $a \in G$ så följer det att om $a_1H = a_2H$ och $b_1H = b_2H$ så gäller $a_1b_1H = a_2b_2H$ vilket betyder att man definiera produkten av sidoklasserna aH och bH med $(aH)(bH) = abH$.*
  Varför? Genom att använda antagandet $aH = Ha$ flera gånger får vi

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

Varför är $|Gx| \cdot |G_x| = |G|$?

Antag att G är en ändlig grupp. Om H är en delgrupp av G så är $|H| \cdot m = |G|$ där m är antalet (tex. vänstra) sidoklasser av H. Eftersom G_x är en delgrupp av G så räcker det att konstruera en bijektion ψ från mängden av vänstra sidoklasser av G_x till banan Gx.
Definiera $\psi(gG_x) = gx$. Om $g_1G_x = g_2G_x$ så gäller $g_2^{-1}g_1 \in G_x$ så att $g_2^{-1}g_1x = x$ och därför gäller $g_1x = g_2x$ så att ψ är väl definierad.
Om $g_1x = g_2x$ så gäller $g_2^{-1}g_1x = x$ så att $g_2^{-1}g_1 \in G_x$ och därför $g_1G_x = g_2G_x$ vilket betyder att ψ är en injektion. Om $y \in Gx$ så finns det ett $g \in G$ så att $y = gx$ och därför gäller $y = \psi(gG_x)$ vilket betyder att ψ är en surjektion.

Varför är antalet banor i gruppverkan på en mängd $\frac{1}{|G|}\sum_{g\in G}|X_g|$?

Låt $F = \{\,[g,x] \in G \times X : gx = x\,\}$. Genom att byta summeringsordning får vi

$$|F| = \sum_{g\in G}|\{\,x \in X : gx = x\,\}| = \sum_{x\in X}|\{\,g \in G : gx = x\,\}|,$$

så att $\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x|$.
Mängden banor betecknar vi med X/G och de är ekvivalensklasser när ekvivalensrelationen $\sim$ definieras med $x \sim y$ om och endast om $x = gy$ för något $g \in G$. Olika banor har inga gemensamma element och deras union är X. Eftersom $|G_x| = \frac{|G|}{|Gx|}$ och Gx är banan som innehåller x så får vi påståendet med följande räkning:

$$\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x| = \sum_{A\in X/G}\sum_{x\in A}\frac{|G|}{|Gx|} = |G|\sum_{A\in X/G}\sum_{x\in A}\frac{1}{|A|}$$
$$= |G|\sum_{A\in X/G}\frac{1}{|A|}\sum_{x\in A}1 = |G|\sum_{A\in X/G}1 = |G||X/G|.$$

Rotationers cykelindex

Permutationen $p = (0\ 1\ 2\ \ldots\ n-1)$ *av mängden* $X = \{0, 1, 2, \ldots, n-1\}$ *genererar den cykliska gruppen (kallad* C_n*) med element* $e, p, p^2, \ldots, p^{n-1}$ *där* e *är identitetselementet. Denna permutation* p *motsvarar rotation med vinkeln* $\frac{2\pi}{n}$ *av en reguljär* n*-hörning.*
Låt $k \in \{0, 1, 2 \ldots, n-1\}$*. För varje* $j \in \mathbb{Z}$ *och* $x \in X$ *är*

$$(p^k)^j(x) = p^{k \cdot j}(x) = \operatorname{mod}(x + k \cdot j, n) = \operatorname{mod}(x + \operatorname{mod}(k \cdot j, n), n).$$

Nu väljer vi d *som minsta möjliga positiva heltal så att* $\operatorname{mod}(k \cdot d, n) = 0$*. Detta innebär att för varje* $x \in X$ *gäller* $(p^k)^j(x) \neq x$ *då* $1 \leq j < d$ *men* $(p^k)^d(x) = x$*. Detta innebär att varje bana för permutationen har längden* d *och eftersom unionen av banorna är* X *så delar* d *talet* n *och* p^k *har* $\frac{n}{d}$*. Nästa steg är att bestämma för hur många värden på* k *längden av banorna är* d *för varje* d *som delar* n*. Eftersom* $\operatorname{mod}(k \cdot d, n) = 0$ *så är* $k \cdot d = j \cdot n$ *och* $\operatorname{sgd}(j, d) = 1$ *eftersom vi annars kunde dividera bort en gemensamma delaren och få ett mindre tal* d*. Eftersom* $k < n$ *måste vi ha* $j < d$ *så att* $k = j \cdot \frac{n}{d}$ *där* $0 \leq j < d$ *och* $\operatorname{sgd}(j, d) = 1$*. Men om vi väljer* j

Rotationers cykelindex, forts.

på detta sätt får vi ett tal k *mellan* 0 *och* $n-1$ *vilket betyder att antalet element* p^k *som är sådana att banornas längd är* d *är antalet element i mängden* $\{\, j : 0 \leq j - 1,\ \operatorname{sgd}(j, d) = 1 \,\}$ *och detta antal är den sk. Eulers funktion* $\varphi(d)$*.*
Cykelindexet blir därför

$$\zeta_{C_n, \mathbb{N}_n}(t_1, t_2, \ldots, t_n) = \frac{1}{n} \sum_{d \mid n} \varphi(d) t_d^{\frac{n}{d}}.$$

Bevis för Pólyas teorem om antalet färgningar

Vi antar att Ω är en mängd färgningar av X och att $G\Omega \subset \Omega$ där G är en grupp som verkar på X och därför också på färgningarna i Ω. Då är antalet banor i G:s gruppverkan på Ω (dvs. icke-ekvivalenta färgningar, dvs. antalet ekvivalensklasser)

$$\frac{1}{|G|}\sum_{g\in G}|\Omega_g|$$

där $\Omega_g = \{\,\omega \in \Omega : g\omega = \omega\,\}$ är mängden av färgningar som förblir oförändrade under verkan av g och dehär är i sin tur de färgningar som är konstanta på varje bana då g verkar på X.
Om nu Ω är mängden av färgningar i vilka vi använder färgen f_j exakt i_j gånger så skall vi visa att

$$|\Omega_g| = \text{koefficient}\Big(\zeta_{g,X}(f_1+\ldots+f_r,\ldots,f_1^n+\ldots+f_r^n), f_1^{i_1}\cdot\ldots\cdot f_r^{i_r}\Big).$$

Bevis för Póyas teorem om antalet färgningar, forts.

Vi antar att $B_{g,1}, B_{g,2}, \ldots B_{g,m_g}$ är banorng i a:s verkan på X och vi skriver $s_j = |B_{g,j}|$. Nu finns det förstås exakt ett sätt att använda färgen f_j exakt s_1 gånger då vi färgar elementen i mängden $B_{g,1}$ med färgen f_j. Vi kan uttrycka dethär påståendet med (den sk. genererande) funktionen $f_1^{s_1}+\ldots+f_r^{s_1}$ där koefficienten för termen $f_j^{s_1}$ antalet alternativ(som här alltså är 1).
I nästa steg antar vi att $p_k(f_1,\ldots,f_r) = \prod_{j=1}^k (f_1^{s_j}+\ldots+f_r^{s_j})$ är en (genererande) funktion så att koefficineten för termen $f_1^{i_1}\cdot f_2^{i_2}\cdot\ldots\cdot f_r^{i_r}$ är antalet alternativ då vi fårgar banorna $B_{g,1},\ldots B_{g,k}$ så att vi använder färgen f_j exakt i_j gånger. Elementen på banan $B_{g,k+1}$ kan vi färga så att vi använder en viss färg s_{k+1} och olika val leder till olika färgningar.
Om vi färgar banan $B_{g,k+1}$ med färgen f_q och vill använda färgen f_p exakt i_p gånger för att färga banorna $B_{g,1},\ldots B_{g,k}, B_{g,k+1}$ så skall vi för att färga banorna $B_{g,1},\ldots B_{g,k}$ använda färgen f_p exakt i_p gånger då $p \neq q$ och färgen f_q exakt $i_q - s_{k+1}$ gånger.

Bevis för Póyas teorem om antalet färgningar, forts.

Då vi färgar banan $B_{g,k+1}$ så är de enda alternativen valet av färgen f_q och då blir enligt induktionsantagandet antalet färgningasalternativ

$$\sum_{q=1}^{r} \text{koefficient}(p(f_1,\ldots,f_r), f_1^{j_1}\cdot\ldots\cdot f_{q-1}^{j_{q-1}}\cdot f_q^{j_q-s_{k+1}}\cdot f_{q+1}^{j_{q+1}}\cdot\ldots\cdot f_r^{j_r}).$$

Men detta är samma tal som

$$\text{koefficient}(p(f_1,\ldots,f_r)\cdot(f_1^{s_{k+1}}+\ldots+f_r^{s_{k+1}}), f_1^{j_1}\cdot\ldots\cdot f_r^{j_r}),$$

så vi ser att induktionssteget fungerar och vi har bevisat den första delen av teoremet.
Om vi använder r färger, så att det alltså inte finns andra begränsningar så skall vi räkna ut summan av koefficienterna för alla termer av typen $f_1^{j_1}\ldots f_r^{j_r}$ i $\zeta_{G,X}(f_1+\ldots+f_r,\ldots,f_1^n+\ldots+f_r^n)$ där $j_1+j_2+\ldots j_r=n=|X|$ och denna summa får vi om vi väljer $f_1=f_2=\ldots f_r=1$ och då skall vi räkna ut $\zeta_{G,X}(r,r,\ldots,r)$.

Grafer

- *En riktad graf $G=[V,E]$ består av en mängd V vars element är noder (eller hörn) och en mängd E av bågar (eller kanter) som (i det riktade fallet) är en delmängd av $V\times V$ (dvs. en relation i V).*
- *En (icke-riktad) graf $G=[V,E]$ består av en mängd V vars element är noder (eller hörn) och en mängd E av bågar (eller kanter) vars element är delmängder av V med 1 eller 2 element.*
- *En enkel graf $G=[V,E]$ är en icke-riktad graf i vilken bågarna i E är delmängder av V med exakt två element.*

Antalet element i V antas vanligen vara positivt men ändligt.

Obs!

Om $V=\{v_1,v_2,\ldots v_m\}$ och $[V,E]$ är en enkel graf så kan mängden $\{v_j,v_j\}=\{v_j\}$ inte höra till E eftersom den innehåller bara ett element och detta innebär att i en enkel graf finns det ingen båge mellan en nod och den själv, en sk. ögla eller loop. I alla graferna som här behandlas kan det finns högst en båge mellan två noder.

Definitioner

Antag att $G = [V, E]$ är en graf.

- *En* **väg** *i G är en följd $[v_0, v_1, \ldots, v_n]$ där v_j, $j = 0, 1, \ldots, n$ är noder i G (dvs. $v_j \in V$) och för varje $j = 1, \ldots, n$ finns det en båge i G mellan v_{j-1} och v_j, (dvs. $\{v_{j-1}, v_j\} \in E$ eller $[v_{j-1}, v_j] \in E$).*
- **Längden** *av vägen $[v_0, v_1, \ldots, v_n]$ i G är n.*
- *En* **cykel** *(eller krets) i G är en väg $[v_0, v_1, \ldots, v_n]$ i G så att $v_n = v_0$.*
- *En väg $[v_0, v_1, \ldots, v_n]$ i G är* **enkel** *om ingen nod i vägen upprepas (dvs. $v_j \neq v_k$ då $0 \leq j < k \leq n$).*
- *En cykel $[v_0, v_1, \ldots, v_0]$ i G är* **enkel** *om vägen $[v_0, v_1, \ldots, v_{n-1}]$ är enkel.*
- *En* **Euler**-*väg (eller -cykel) i G är en väg (eller cykel) i G så att vägen eller cykeln går genom varje båge precis en gång (dvs. $\cup_{j=1}^{n}\{\{v_{j-1}, v_j\}\} = E$ och $\{v_{j-1}, v_j\} \neq \{v_{k-1}, v_k\}$ då $1 \leq j < k \leq n$ ($\cup_{j=1}^{n}\{[v_{j-1}, v_j]\} = E$ ja $[v_{j-1}, v_j] \neq [v_{k-1}, v_k]$ då $1 \leq j < k \leq n$)).*

Definitioner, forts.

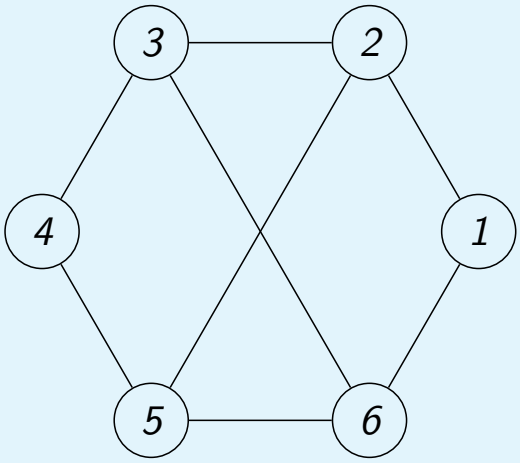
- *En* **Hamilton**-*väg (eller -cykel) i G är en enkel väg (eller cykel) i G så att vägen eller cykeln går genom varje nod, frånsett startnoden i cykelfallet, precis en gång (dvs. $\{v_0, \ldots, v_n\} = V$).*
- *En graf är* **sammanhängande** *om det finns en väg från varje nod till varje annan nod.*
- *En graf är ett* **träd** *om det finns exakt en enkel väg från varje nod till varje annan nod.*
- *En graf är en* **skog** *om det finns högst en enkel väg från varje nod till varje annan nod.*
- *En graf är* **bipartit** *med delarna X och Y om $V = X \cup Y$, $X \cap Y = \emptyset$ och $E \subset \{\{x, y\} : x \in X, y \in Y\}$ (eller $E \subset X \times Y$).*
- *En* **matchning** *i en graf är en mängd bågar $M \subset E$ så att två olika bågar i M inte har någon gemensam ändnod, dvs. om $e_1 = \{v_1, v_1'\}$ och $e_2 = \{v_2, v_2'\}$ och $e_1 \neq e_2$ så är $e_1 \cap e_2 = \emptyset$ (ifall $[v_1, v_1'] \in M$ och $[v_2, v_2'] \in M$ så gäller $\{v_1, v_1'\} \cap \{v_2, v_2'\} \neq \emptyset \leftrightarrow [v_1, v_1'] = [v_2, v_2']$).*

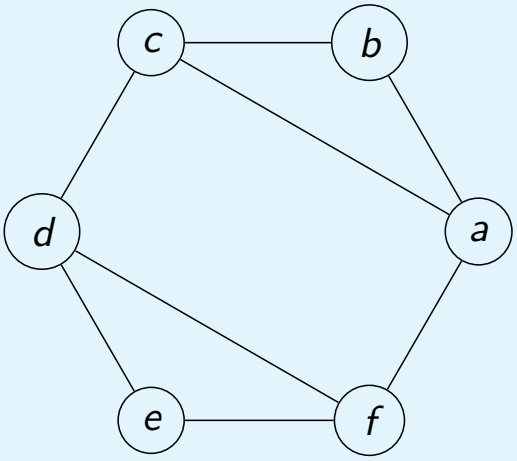
Definitioner, forts.

- *Graferna* $[V, E]$ *och* $[V', E']$ *är isomorfa om det finns en bijektion* $\psi : V \to V'$ *så att* $\{\psi(a), \psi(b)\} \in E' \leftrightarrow \{a, b\} \in E$ *(och i en riktad graf* $[\psi(a), \psi(b)] \in E' \leftrightarrow [a, b] \in E$*) dvs. "grannar avbildas på grannar".*
- *I en* **nodfärgning** *av en graf får noder som är grannar olika färg, dvs. färgningen är en funktion* $\omega : V \to K$ *så att* $\omega(v_j) \neq \omega(v_k)$ *om* $\{v_j, v_k\} \in E$ *eller* $[v_{j-1}, v_j] \in E$*. Det* **kromatiska** *talet för en graf är minimiantalet färger som behövs för en nodfärgning.*

Isomorfa grafer

Är graferna nedan isomorfa?

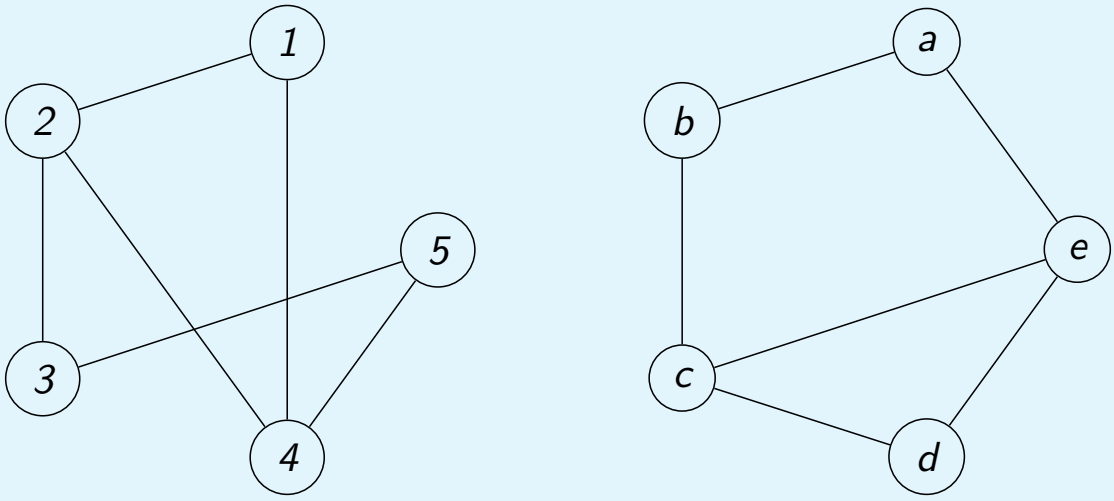




I båda graferna finns 4 *noder med gradtalet* 3*, dvs. som har* 3 *grannar och* 2 *med gradtalet* 2*, så av detta kan man inte dra slutsatsen att de graferna inte skulle vara isomorfa. Däremot finns det ingen cykel i grafen till vänster med längden* 3 *men det finns det däremot i grafen till höger. Detta innebär att graferna inte kan vara isomorfa.*

Isomorfa grafer

Är graferna nedan isomorfa?



I detta fall är graferna isomorfa eftersom funktionen som definieras med $f(1) = d$, $f(2) = c$, $f(3) = b$, $f(4) = e$, *och* $f(5) = a$ *har de önskade egenskaperna.*

Grannmatris

Om $G = [V, E]$ *är en graf med* m *noder* $V = \{v_1, \ldots v_m\}$ *så är dess grannmatris den* $m \times m$*-matris för vilken gäller*

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

Om $n \geq 1$ *och* $B = A^n$ *så är* $B(j,k)$ *antalet vägar från nod* v_j *till nod* v_k *med längden* n.

Bipartita grafer och matchningar

Om $G = [X \cup Y, E]$ *är en bipartit graf (med delarna* X *och* Y*) så finns det en matchning* M *i* G *så att varje* $x \in X$ *är ändnod för någon båge i* M*, dvs. en sk. fullständig matchning*
om och endast om det är sant att
för varje $A \subset X$ *är antalet noder i* A *mindre eller lika med antalet noder i* Y *som är granne med någon nod i* A.

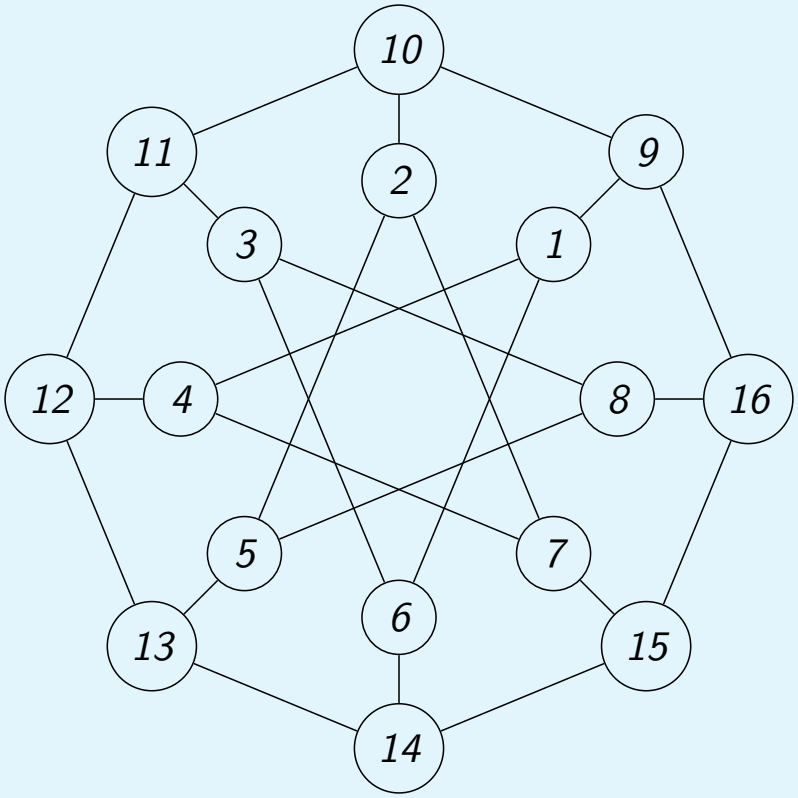
Girig nodfärgning

Ett enkelt men inte nödvändigtvis optimalt sätt att bestämma en nodfärgning är följande giriga algoritm:

- *Sätt noderna i någon ordning:* $[v_1, v_2, \ldots, v_n]$.
- *Sätt färgerna i någon ordning:* $[a_1, a_2, \ldots, a_r]$.
- *Färga den första noden med den första färgen, dvs.* $\omega(v_1) = a_1$.
- *Om noderna* $v_1, \ldots, v_k$ *är färgade så färga* v_{k+1} *med den första färg som kan användas så att villkoret att grannar inte får samma färg uppfylls, dvs.* $\omega(v_{k+1}) = a_j$ *där*
  $j = \min\{\, i \geq 1 : \{v_p, v_{k+1}\} \in E \text{ AND } p \leq k \rightarrow \omega(v_p) \neq a_i \,\}$.

Girig nodfärgning

Vi skall bestämma nodfärgningar för grafen



Girig nodfärgning, forts.

och använder den sk. giriga algoritmen: Sätt färgerna i någon ordning och gå genom alla noderna (i ordning) och ge varje nod den första färgen i färgordningen som den kan få med beaktande av de färger man redan gett till noder och villkoret att två noder inte kan ha samma färg om det finns en båge mellan dem.
Om vi använder färgerna a, b, c, ... och tar första noderna först i ordningen $1, 2, 3, 4 \ldots, 16$ *så blir färgningen följande:*

Nod	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Färg	*a*	*a*	*a*	*b*	*b*	*b*	*c*	*c*	*b*	*c*	*b*	*a*	*c*	*a*	*b*	*a*

Om vi tar noderna i ordningen $9, 10, \ldots, 15, 16, 1, 2, 7, 8$ *så blir färgningen*

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

Av detta ser vi att det minsta möjliga antalet färger är 2 *eftersom det inte kan vara* 1 *om det finns minst en båge i grafen.*

Minimalt uppspännande träd, girig algoritm I (Prim)

Om $G = [V, E]$ *är en sammanhängande graf så att varje båge* $\{v_j, v_k\}$ *har getts en vikt* $w(\{v_j, v_k\})$ *(och* $w(\{v_j, v_k\}) = \infty$ *ifall* $\{v_j, v_k\} \notin E$*) så är det minimalt uppsännande trädet en delgraf* $T = (V, E_T)$ *(dvs.* $E_T \subset E$*) som är ett träd och sådan att* $\sum_{\{v_j, v_k\} \in E_T} w(v_j, v_k)$ *är så litet som möjligt. Ett sätt att konstruera ett minimalt uppspännande träd är att använda följande giriga algoritm (Prims algoritm):*

- *Låt* $T_1 = [\{v_1\}, \emptyset]$ *där* v_1 *är en godtyckligt vald nod (dvs.* T_1 *är en graf som bara innehåller en nod och ingen båge).*
- *Om man redan bestämt* $T_m = [V_m, E_m]$ *så väljer man* $v_j \in V_m$ *och* $v_k \in V \setminus V_m$ *så att* $w(\{v_j, v_k\})$ *är så litet som möjligt och sedan* $T_{m+1} = [V_m \cup \{v_k\}, E_m \cup \{\{v_j, v_k\}\}]$*, dvs. man lägger till noden* v_k *och bågen mellan* v_j *och* v_k *till* T_m *för att få* T_{m+1}*.*

Minimalt uppspännande träd, girig algoritm I (Kruskal)

Om $[V, E]$ är en sammanhängande (icke-riktad) graf verkko så att varje båge $\{v_j, v_k\}$ har getts en vikt $w(\{v_j, v_k\})$ (och $w(\{v_j, v_k\}) = \infty$ ifall $\{v_j, v_k\} \notin E$) så kan man konstruera ett minimalt uppspännande träd med följande giriga algoritm (Kruskals algoritm):

- *Välj $E_0 = \emptyset$.*
- *Så länge som $[V, E_m]$ inte är ett träd så blir $E_{m+1} = E_m \cup \{e\}$ där $e \in E \setminus E_m$ väljs så att $w(e)$ är så liten som möjligt och grafen $[V, E_m \cup \{e\}]$ är en skog (dvs. den innehåller inga cykler med längd minst 3).*

Dynamisk optimering och grafer

Antag att $G = [V, E]$ är en enkel sammanhängande graf så att varje båge $e \in E$ har getts en vikt $w(e) \geq 0$ (och $w(\{v_j, v_k\}) = \infty$ ifall $\{v_j, v_k\} \notin E$). En fråga som ofta dyker upp hur man kan bestämma en väg $[v_0, v_1, \ldots, v_n]$ från en given nod v_0 till en annan given nod v_n så att $\sum_{j=1}^{n} w(\{v_{j-1}, v_j\})$ är så liten som möjligt.

- *Definiera $s(v) = \min\{\sum_{j=1}^{k} w(\{v_{j-1}, v_j\} : [v_0, v_1, \ldots, v_k]$ är en väg från v_0 till $v_k = v\}$.*
- *Observera att för funktionen s gäller principen för* **dynamisk optimering**:

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

- *Bestäm de optimala värdena $s(v)$ på följande sätt:*
  - *Låt $V_0 = \{v_0\}$ och $s(v_0) = 0$.*
  - *Om de optimala värden $s(v)$ är bestämda för $v \in V_j$ så beräknas testvärden för grannarna till V_j i $V \setminus V_j$ med $t(v) = \min_{v' \in V_j}(s(v') + w(\{v', v\})$.*
  - *Välj $V_{j+1} = V_j \cup \{v\}$ och $s(v) = t(v)$ där $t(v) = \min_{v' \in V \setminus V_j} t(v')$.*