MS-A0409 Grundkurs i diskret matematik
Exempel, del I

G. Gripenberg

Aalto-universitetet

17 oktober 2013

Euklides algoritm

Om vi vill räkna ut $\operatorname{sgd}(634, 36)$ *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 $\operatorname{sgd}(634, 36) = 2$.

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:*

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

Detta innebär att $(-32) \cdot 23 = 1 - 11 \cdot 67$ *så att* $(-32) \cdot 23 \equiv 1 \pmod{67}$
vilket är det samma som att $[23]_{67}^{-1} = [-32]_{67} = [-32 + 67]_{67} = [35]_{67}$.

Kontrollteckenet i finländska personnummer

Kontrollteckenet i finska personnummer räknas som resten vid division av det tal som de nio första siffrorna bildar med 31. *Kan kontrollteckenet 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*

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

För att kontrollteckenet 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 kontrollteckenet.*

RSA-algoritmen

Om man med RSA-algoritmen skall kryptera meddelandet 9 *och använda den publika nyckeln* $(55, 23)$ *så skall man räkna ut* $\mathrm{mod}\,(9^{23}, 55)$. *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*

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

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

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

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

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

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

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

så att $\mathrm{mod}\,(9^{23}, 55) = 14$.

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

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

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

Permutationer och cykelnotation

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

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

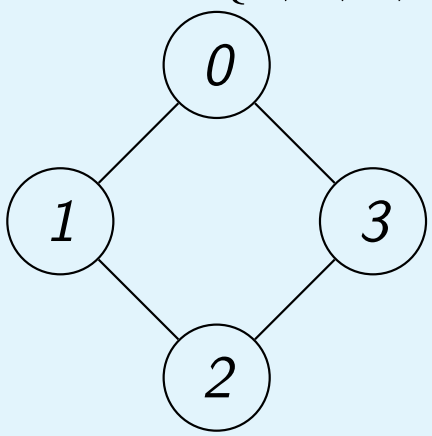
av A där alltså detta skrivsätt betyder att tex. $\alpha(1) = 2$ *och* $\alpha(4) = 3$. *Nu ser vi att* $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$ *(dvs.* $\alpha(1) = 2$, $\alpha(2) = 4$ *osv.) och detta ger cykeln* $\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ *som alltså är en permutation* β_1 *så att* $\beta_1(1) = 2$, $\beta_1(2) = 4$, $\beta_1(4) = 3$, $\beta_1(3) = 1$ *och* $\beta(x) = x$ *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.*

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

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

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 *banor som 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.*

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.*

Pólyas teorem och "tre-i-rad", forts.

Cykelindexet blir därför

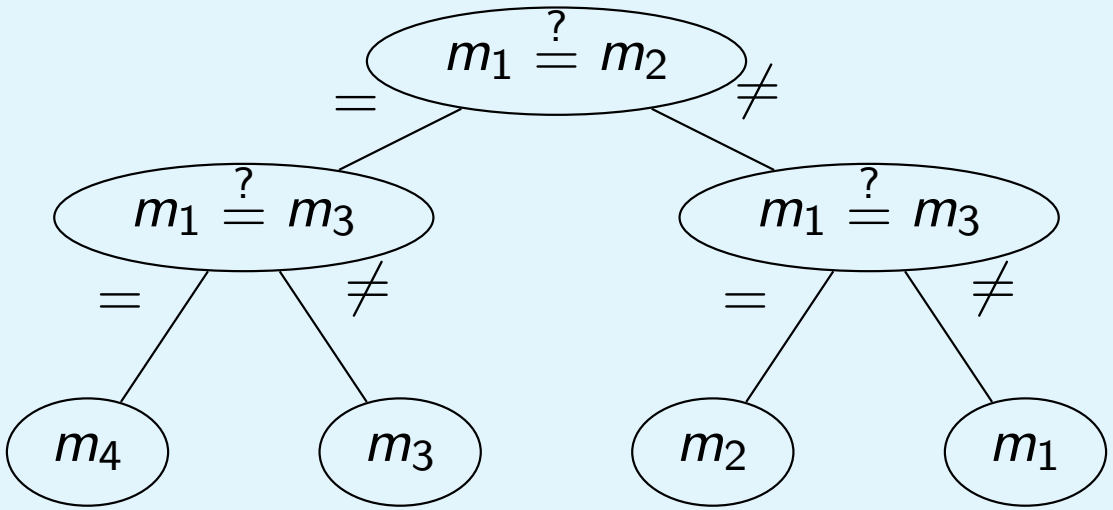
$$\zeta_{G,X}(t_1, t_2, \ldots, t_9) = \frac{1}{4}\left(t_1^9 + 2t_1 t_4^2 + t_1 t_2^4\right).$$

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* $x^2 o^2 t^5$ *antalet icke-ekvivalenta färgningar med 2 stycken* x*, 2 stycken* o *och 5 stycken* t*. Denhär koefficienten blir*

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

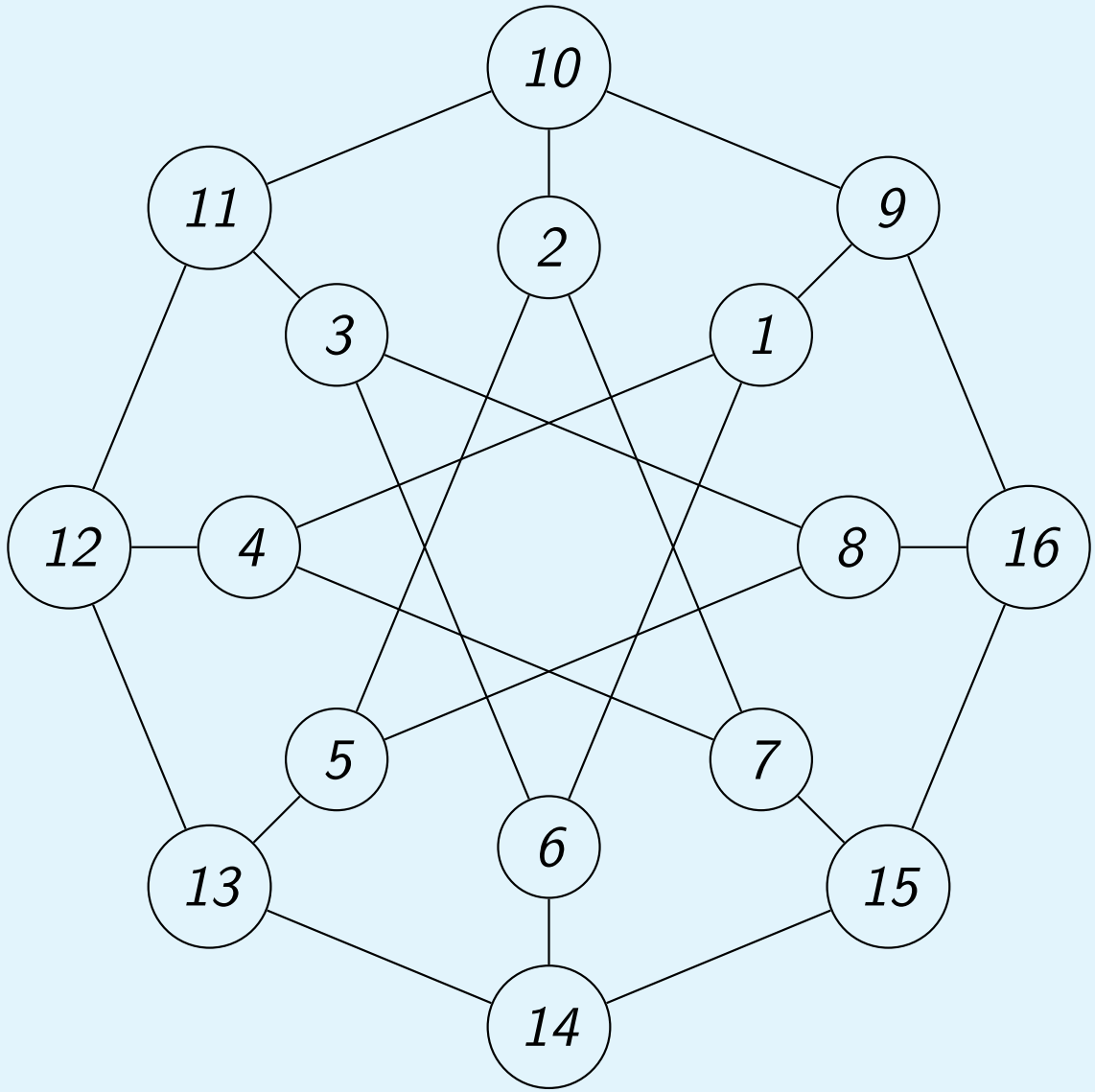
En graf som beskriver en beslutsprocess

Antag att man har fyra mynt och man vet att precis ett av dem är förfalskat så att dess vikt avviker från de äkta myntens (men man vet inte om det är lättare eller tyngre). Om man nu har en balansvåg med vilken man kan avgöra om två mynt (eller par av mynt, osv.) väger lika mycket eller inte så kan man med följande graf beskriva en procedur för att bestämma vilket av mynten m_j, $j = 1, 2, 3, 4$, som är förfalskat:



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*

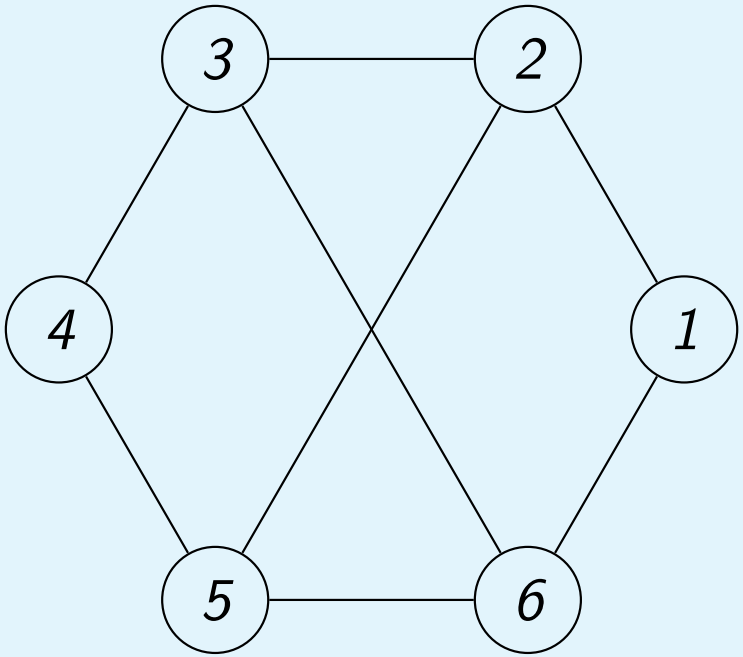
Om vi tar noderna i ordningen $9, 10, \ldots, 15, 16, 1, 2, 7, 8$ *så blir färgningen*

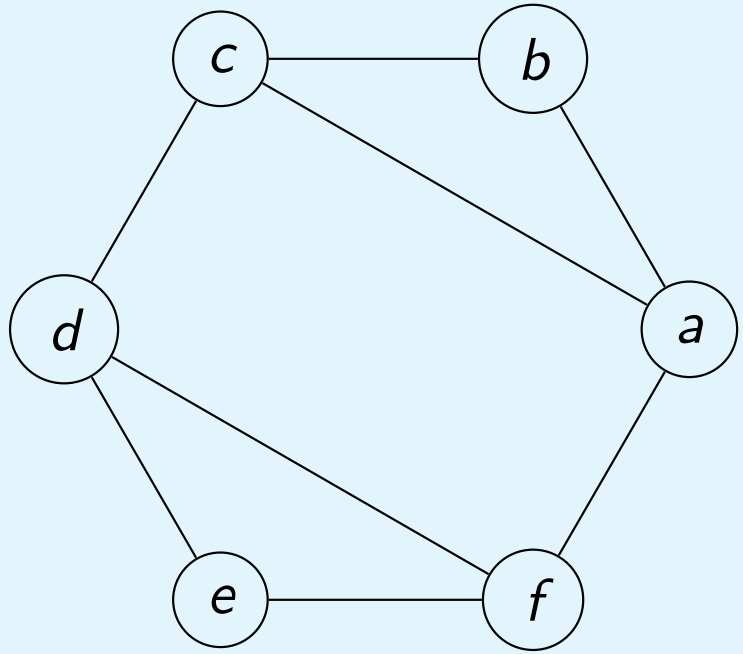
Nod	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
Färg	*a*	*b*	*a*	*b*	*a*	*b*	*a*	*b*	*b*	*a*	*b*	*a*	*b*	*a*	*b*	*a*

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.*

Isomorfa grafer

Är graferna nedan isomorfa?

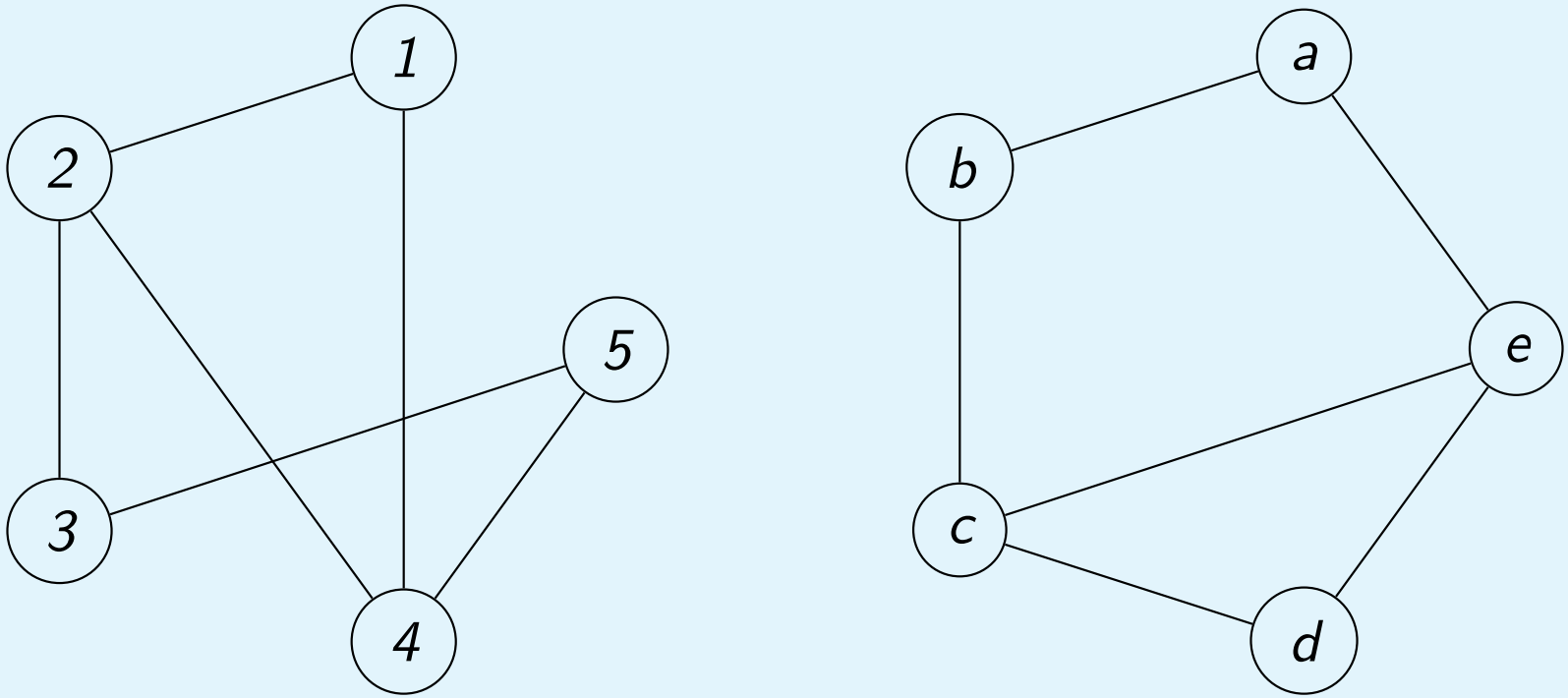




I båda graferna finns 4 *noder med gradtalet* 3, *dvs. som har* 3 *grannar och* 2 *med gradtalet* 2, *så av detta kan man inte dra slutsatsen att de graferna inte skulle vara isomorfa. Däremot finns det ingen cykel i grafen till vänster med längden* 3 *men det finns det däremot i grafen till höger. Detta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