$\Updownarrow$

$\exists y \in Y : x R y \;\&\; y (S \circ T) w$

$\Updownarrow$ def. složení $S \circ T$

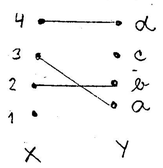
$\exists y \in Y, \exists z \in Z : x R y \;\&\; y S z \;\&\; z T w$

ZOBRAZENÍ

Zobrazení f z množiny X do množiny Y = **relace** $f \subset X \times Y$ taková, že $\forall x \in X \; \exists$ právě jedno $y \in Y$ tak, že $(x,y) \in f$

píšeme: $f(x) = y$

$f : X \mapsto Y$



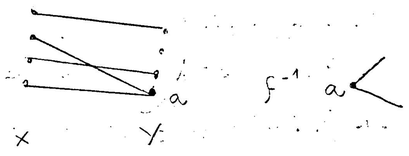
Zobrazení $f : X \to Y$ je **prosté**, pokud každé $y \in Y$ má **nejvýše jeden vzor**.

Zobrazení je **na**, pokud každé $y \in Y$ má **aspoň jeden vzor**.

" je **bijekce** (vzájemně jednoznačné zobrazení), pokud je **prosté a na**.

$f \rightsquigarrow f^{-1}$ (relace)

Je f^{-1} také zobrazení? Obecně ne

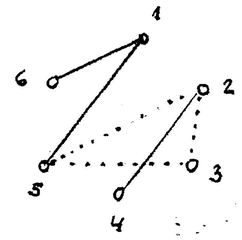


Tvrzení: Pro zobrazení f je relace f^{-1} zobrazení právě tehdy, když f je bijekce.

RELACE

Problém večírku

min 6 lidí; ex. trojice: — každé 2 osoby se znají
žádné 2 " se neznají



Binární

↓ **Relace** z množiny X do množiny Y =

= podmnožina kartézského součinu $X \times Y$

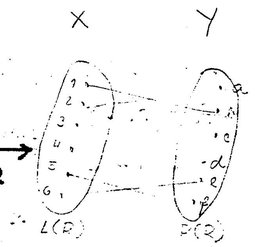
$R \subseteq X \times Y$

$\boxed{(x,y) \in R}$ $\quad x \in X, \; y \in Y$

$\Updownarrow$

" $x R y$ "

grafové znázornění R



(např. " $x < y$ " a ne $(x,y) \in <$)

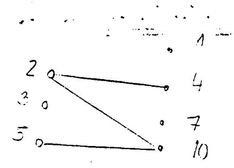
Když R je relace, tak **levý obor** relace R je $L(R) = \{ x \in X : \exists y \in Y : x R y \}$

pravý " " " $P(R) = \{ y \in Y : \exists x \in X : x R y \}$

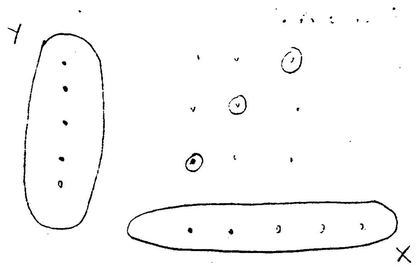
př. $X = \{2,3,5\}$ $\quad Y = \{1,4,7,10\}$

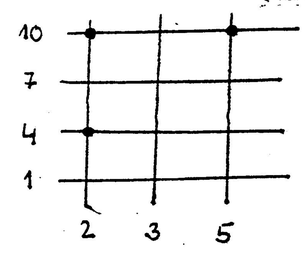
$R \subset X \times Y$

$R = \{ (2,4), (2,10), (5,10) \}$



shodě okolností platí: $x R y \iff x$ dělí y ... předpis relace (aspoň-a-ný)

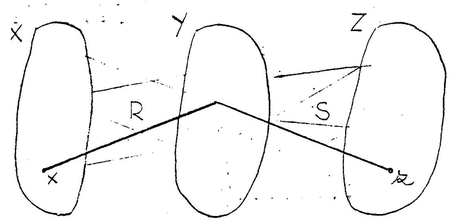




Relace $R, S \subset X \times Y$ ... R <u>implikuje</u> S, pokud $x R y \Rightarrow x S y \quad \forall x, y$

(jinými slovy: $R \subset S$)

$R \subset X \times Y$
$S \subset Y \times Z$



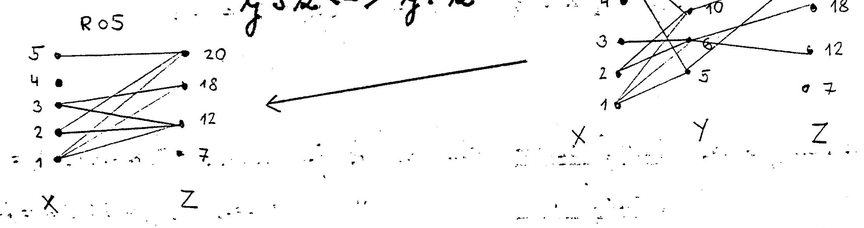
<u>Složení relací</u> R a S je relace <u>$R \circ S \subset X \times Z$</u>:

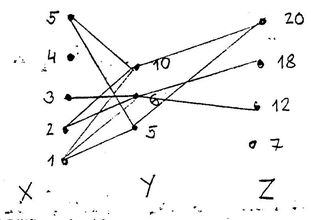
$x (R \circ S) z \iff \exists y \in Y : x R y \ \& \ y S z$

<u>př.</u> $X = \{1,2,3,4,5\}$ $Y = \{5,6,10\}$ $Z = \{7,12,18,20\}$

$R \subset X \times Y$
$S \subset Y \times Z$
} pomocí dělitelnosti

$x R y \iff x | y$
$y S z \iff y | z$





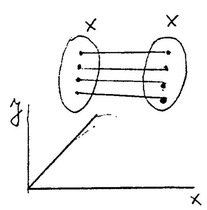
<u>Relace inverzní</u> k R ... $R^{-1} \subset Y \times X$

$R^{-1} = \{(y,x) : x R y\}$

$y R^{-1} x \iff x R y$

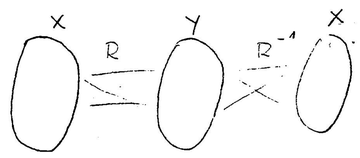
<u>Relace na množině X</u> ... = z X do X, $R \subset X \times X$

<u>Identická relace</u> na X $E_X = \{(x,x) : x \in X\}$



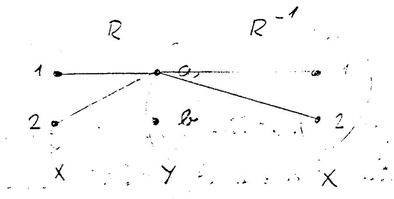
<u>př.</u>
- $R \subset X \times X$

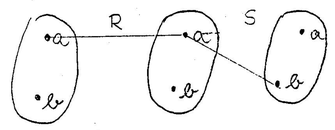
Jak vypadá $R \circ E_X$, $E_X \circ R$? ... stejně $R \circ R^{-1}$



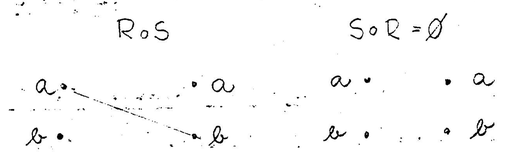
$R \circ R^{-1} = E_X$?

$R = \emptyset$ ↓ nedá se o tom nic říct





$R = \{(a,a)\}$
$S = \{(a,b)\}$



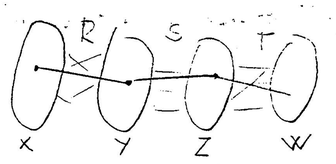
<u>Vlastnosti skládání relací</u>

$R, S \subset X \times X$

$R \circ S$ $S \circ R$ obě definovány

skládání relací není komutativní

asociativní operace $(R \circ S) \circ T$? $R \circ (S \circ T)$



<u>Věta</u> (asociativitě skládání relací)

$R \subset X \times Y$, $S \subset Y \times Z$, $T \subset Z \times W$, potom $R \circ (S \circ T) = (R \circ S) \circ T$

<u>Důkaz:</u>

Nechť $x \in X$, $w \in W$

Chceme: $(x,w) \in R \circ (S \circ T) \iff (x,w) \in (R \circ S) \circ T$

Máme x, w

... ex. cesta z X do W"

$*$ je <u>komutativní</u>, pokud $\forall x, y \in M: x * y = y * x$
" <u>asociativní</u>, " $\forall x, y, z \in M: (x * y) * z = x * (y * z)$

Prvek $n \in M$ je <u>neutrálním prvkem</u> (vzhledem k $*$) pokud:
$\forall x \in M: \quad x * n = x$
$n * x = x$

<u>Tvrzení</u>: Neutrální prvek je nejvýše jeden.
<u>Důkaz:</u> Ať jsou 2: n, n'
$n = n * n' = n'$

$M, *, n$ ... neutrální
<u>prvek inverzní</u> k $x \in M$ je y takové, že $x * y = n$
$y * x = n$

<u>Tvrzení</u>: Inverzní prvek k x je <u>nejvýše jeden</u>, je-li $*$ <u>asociativní</u>.

<u>Důkaz:</u>
Nechť y, y' jsou inverzní k x.
$(y * x) * y' = n * y' = y'$
$y * (x * y') = y * n = y$

$(M, *)$
GRUPA = množina M spolu s binární operací $*$ tak, že:
- $*$ je asociativní
- existuje neutrální prvek
- pro každé x ex. inverzní prvek
- je-li navíc $*$ komutativní → komutativní grupa (abelovská ")

<u>příklady grup:</u>
$(\mathbb{Z}, +)$
$(\mathbb{Q}, +)$
$(\mathbb{R}, +)$
$(\mathbb{Q} - \{0\}, \cdot)$
$(\mathbb{R} - \{0\}, \cdot)$
$(\mathbb{R}^{m \times m}, \cdot)$

grupy nejsou:
$(\mathbb{N}, +)$
$(\mathbb{Z}, \cdot)$
$(\mathbb{Q}, \cdot)$
$(\mathbb{R}^{m \times m}, \cdot)$
(relace na X, skládání)

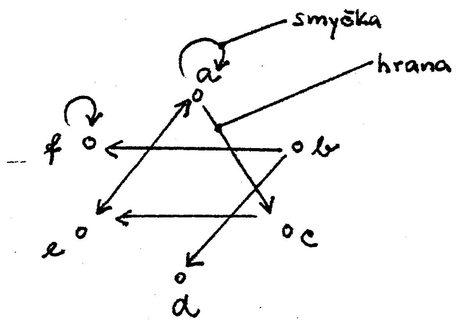
<u>Znázornění relací</u>

$R \subset X \times X$

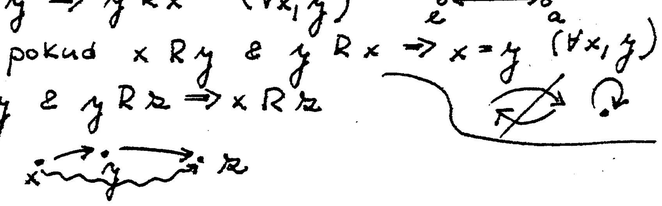
$X = \{a, b, c, d, e, f\}$
$R = \{(a,a), (f,f), (a,c), (a,e), (b,d), (b,f), (e,a), (c,e)\}$
maticové znázornění:

$M(R) =$

	a	b	c	d	e	f
a	1		1	0	1	
b				1	0	1
c					1	0
d						
e	1				0	
f						1



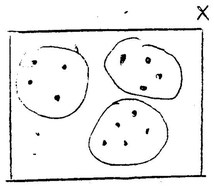
<u>R relace na množině X</u> je:
- <u>reflexní</u>, pokud $\forall x \in X: x R x$
- <u>symetrická</u>, " $x R y \Rightarrow y R x \quad (\forall x, y)$
- <u>slabě antisymetrická</u>, pokud $x R y$ a $y R x \Rightarrow x = y \quad (\forall x, y)$
- <u>tranzitivní</u>, pokud $x R y$ a $y R z \Rightarrow x R z$
$(\forall x, y, z)$



př.	množina	$x R y$, pokud ...	
	$\mathbb{R}$	$x \leq y$	reflexní, antisymetrická, tranzitivní
	$\mathbb{R}$	$x < y$	antisymetrická, tranzitivní
	obyvatelé ČR	„x je rodičem y"	antisymetrická
	rovina $\mathbb{R}^2$	vzdálenost x od y je ≤ 1	reflexní, symetrická
	přímky v $\mathbb{R}^2$	$x \parallel y$	reflexní, symetrická, tranzitivní
	prostor matic $\mathbb{R}^{3\times3}$	x je podobná y	reflexní, symetrická, tranzitivní
	$\mathbb{N}$	x dělí y	-"- , antisymetrická, -"-
	$\mathbb{Z} - \{0\}$	-"-	-"-

EKVIVALENCE

Definice
Relace R na množině X je **ekvivalence**, pokud je reflexivní, symetrická a tranzitivní
(refl. + sym. = **tolerance**)



Neuspořádaný soubor podmnožin $\{X_i\}_{i \in I}$ množiny X je rozkladem množiny X, pokud:
1) X_i jsou navzájem disjunktní a neprázdné
2) $\bigcup X_i = X$

Věta
Ekvivalence na X jednoznačně odpovídají rozkladům X.

Důkaz:
Mějme ekvivalenci $\sim$.
Pro $x \in X$ definujeme **třídu** prvku x jako $[x] = \{y \in X : x \sim y\}$

- Pro $x, y \in X$ jsou $[x], [y]$ buď **shodné** nebo **disjunktní**.

Důkaz:
Nechť $[x], [y]$ nejsou disjunktní
$z \in [x] \cap [y]$
$\hookrightarrow x \sim z$
$y \sim z$
chci: $[x] = [y]$
dokážeme $[x] \subseteq [y]$ a $[y] \subseteq [x]$
(důkaz)
uvažme libovolné $x' \in [x]$; chceme dokázat: $x' \in [y]$
víme: $x \sim x'$
$x' \sim x$ ... symetrie
$x \sim z$ ... víme
$x' \sim y$ ... tranzitivita
$y \sim x'$ ... symetrie
$x' \in [y]$
$\Rightarrow$ takže $[x] \subseteq [y]$ (podobně $[y] \subseteq [x]$)

Reflexivita $\sim \Rightarrow x \in [x]$ pro každé x
Vezmu soubor množin $X/\sim = \{[x] : x \in X\}$ ... to je **rozklad** mn. X
třídy = třídy ekvivalence $\sim$

Je-li dán rozklad $\{X_i\}_{i \in I}$ množiny X, definuji relaci R předpisem $x R y \Leftrightarrow$ leží v téže množině X_i

pozn. Nutno ověřit: ekvivalence $\to$ rozklad $\to$ ekvivalence
rozklad $\to$ ekvivalence $\to$ rozklad
} výsledkem je to, od čeho jsme vyšli

př. ekvivalence R, přímky v rovině $p R q$, pokud $p \parallel q$

př. matice $\mathbb{R}^{n \times n}$
$A \approx B$, pokud mají stejnou hodnost
$A \simeq B$, " jsou si podobné $B = P \cdot A \cdot P^{-1}$
víme: $A \simeq B \Rightarrow A \approx B$

- kolik je tříd ekvivalence $\approx$? ... konečně mnoho: $n+1$
" " " $\simeq$? ... nekonečně mnoho

matice cI pro různá $c \in \mathbb{R}$ si nejsou navzájem podobné
$P(cI) \cdot P^{-1} = cI$

GRUPY

př. grupy: vektorový prostor = množina vektorů

M množina
Zobrazení $* : M \times M \to M$ je (lineární) operace na M

"$\Leftarrow$" Nechť r, p jsou nesoudělné. Hledáme inverzní prvek k $[r]$.

$1 \cdot r, 2 \cdot r, \dots, p \cdot r$ ... p čísel

tvrdím: $i \cdot r \not\equiv j \cdot r$ pro každé $i \neq j$ $\quad 1 \leq i, j \leq p$

dejme tomu, že $i \cdot r \equiv j \cdot r$, potom $r(i-j)$ je násobkem p

p, r nesoudělné $\Rightarrow p \mid i-j$ (např. vidět z rozkladu na prvočísla)

ovšem $|i-j| \leq p-1 \Rightarrow i-j = 0$ ... spor $i \neq j$

$\Rightarrow$ v každé třídě bude právě jeden součin $i \cdot r$

$\Rightarrow$ ex. s tak, že $s \cdot r \in [1] \Rightarrow [s] \otimes [r] = [sr] = [1]$

tedy $[s]$ je inverzní k $[r]$

? Kdy je $\mathbb{Z}_p$ těleso?

Když p je prvočíslo $\Rightarrow$ nesoudělné s každým $r < p$, $r \neq 0$

" p není " $\Rightarrow p = a \cdot b \Rightarrow p$ je soudělné s a

$\Rightarrow [a]$ nema inverzní prvek

Důsledek: $(\mathbb{Z}_p, \oplus, \otimes)$ je těleso $\Leftrightarrow p$ je prvočíslo.

Pozn.

Ex. ovšem i tělesa neprvočíselné velikosti:

př. n-prvkové těleso $\{0,1,2,3\}, *, \circ$

$*$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\circ$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

$2 \circ (1 * 3) = 3$

$(2 \circ 1) * (2 \circ 3) = 3$ To není $\mathbb{Z}_4$!!!

těleso velikosti n existuje $\Leftrightarrow n$ je mocnina prvočísla

grupy:

(regulární matice $n \times n, \cdot$)

(permutace na X, skládání)

(spojité reálné f-ce, $+$)

$\mathbb{R}, +, \cdot$

$(\mathbb{R}, +)$ je komutativní grupa

$(\mathbb{R}, \cdot)$ ne, ale

$(\mathbb{R} - \{0\}, \cdot)$ je komutativní grupa

platí disjunktivní zákon: $x(y+z) = xy + xz$

Definice:

Nechť množina M spolu s operací $\oplus$ tvoří komutativní grupu s neutrálním prvkem 0 a nechť na množině $M - \{0\}$ je určena další operace $\otimes$.

Potom $(M, \oplus, \otimes)$ je těleso, jestliže $(M - \{0\}, \otimes)$ je také komutativní grupa a platí distributivita:

$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

př. $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ v obvyklým sčítáním, násobením

ARITMETIKA MODULU p

Nechť $p \geq 1$

Definujeme relaci na $\mathbb{Z}$:

$x \equiv y$, pokud p dělí $x - y$ (kongruence modulu p)

$x \equiv y \pmod p$

př. $2 \equiv 15 \pmod{13}$

$\equiv$ je ekvivalence na $\mathbb{Z}$

třídu prvku $x \in \mathbb{Z}$ značíme $[x]$ nebo $[x]_p$ (někdy: $\check{\alpha}_p(x)$)

zbytkové třídy mod p

$\mathbb{Z}/p$ ... množina všech zbytkových tříd (někdy: $\mathbb{Z}_p$)...

... p-prvková množina

př. $[2]_7 = \{\dots, -5, 2, 9, 16, \dots\}$
$[6]_7 = \{\dots, -1, 6, 13, 20, \dots\}$

Tvrzení:
Nechť $x \equiv x'$ a $y \equiv y'$. Potom $x+y \equiv x'+y'$, $xy \equiv x'y'$

Důkaz:
$x \equiv x' \rightarrow x - x' = p \cdot m$ $\quad m \dots$ celé
$y \equiv y' \rightarrow y - y' = p \cdot n$ $\quad n \dots$ celé
$(x+y)-(x'+y') = (x-x')+(y-y') = pm + pn$ ... dělitelné p
$(xy - x'y') = (x'+pm)(y'+pn) - x'y' = x' \cdot pn + y' \cdot pm + p^2 \cdot mn$

Definuji $\oplus$, $\otimes$ na $\mathbb{Z}/p$
$[x] \oplus [y] := [x+y]$
$[x] \otimes [y] := [x \cdot y]$ ... korektní definice (nezávisí na volbě reprezentantů)

? Co když $x' \in [x]$, $y \in [y']$, ale $[x'+y'] \neq [x+y]$
$x \equiv x'$, $y \equiv y'$ $\overset{Tv.}{\Rightarrow}$ $x'+y' \equiv x+y$

př. $[2]_7 \oplus [6]_7$ je definováno jako $[2+6] = [8] = \{\dots, -6, 1, 8, 15, \dots\}$

$[2]_7 \otimes [6]_7 = [12] = \{\dots, -9, -2, 5, 12, 19, 26, \dots\}$

př. $\mathbb{Z}/5$
můžeme pracovat s „úplnou soustavou zbytků modulu 5":
$3 \oplus 4 = 2$
$3 \otimes 4 = 2$

⊕	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

⊗	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Věta:
Pro libovolné $p \geq 1$:
1) $(\mathbb{Z}/p, \oplus)$ je komutativní grupa
2) $\otimes$ na $\mathbb{Z}/p - \{[0]\}$ je: komutativní
asociativní
má neutrální prvek
3) platí distributivita: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Důkaz:
např. v ① je $\oplus$ komutativní, protože $[x] \oplus [y] = [x+y] = [y+x] = [y] \oplus [x]$

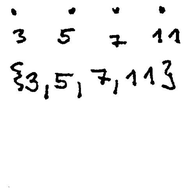
⋮

$[0]$ je neutrální ke sčítání
$[1]$ " " k násobení
$[-x]$ je inverzní k $[x]$ vzhledem k $\oplus$

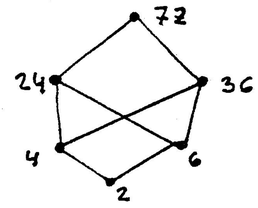
? Je $\mathbb{Z}/p$ tělesem ?
... ex. inverzní prvky při násobení?
$p=4$: inverzní prvek k $[2]$?
$[2] \otimes [1] = [2]$
$[2] \otimes [2] = [0]$
$[2] \otimes [3] = [2]$
$\Rightarrow$ $[2]$ nemá inverzní prvek

Tvrzení:
Ke třídě $[r] \in \mathbb{Z}_p$ existuje inverzní prvek vzhledem k $\otimes$
$\Longleftrightarrow$ r je nesoudělné s p.

Důkaz:
„$\Rightarrow$" nechť $[r]$ má inverzní prvek $[s]$ $\rightarrow$ $[r] \otimes [s] = [1]$
Sporem: předpokládejme, že r, p jsou soudělné, tj. ex. $d > 1$, které dělí r i p.
$[r] \otimes [s] = [1]$
$\quad \parallel$
$[rs] \Rightarrow rs - 1$ je dělitelné p, třeba $rs - 1 = p \cdot n$ $\quad n \dots$ celé
tedy $rs - pn = 1$ $\quad$ SPOR, protože d nemůže dělit 1



$\{3,5,7,11\}$



$\{2,4,6,24,36,72\}$

$a \in X$ je <u>největší</u> prvek množiny X, pokud $\forall x \in X : x \leq a$
<u>nejmenší</u> podobně

prvek $a \in X$ je <u>maximální</u>, pokud $\forall x \in X$ platí $x \not> a$ (kromě $x = a$)
(tj. pokud neexistuje $x \in X$ tak, že $a \leq a$ & $a \neq x$)
podobně <u>minimální</u>

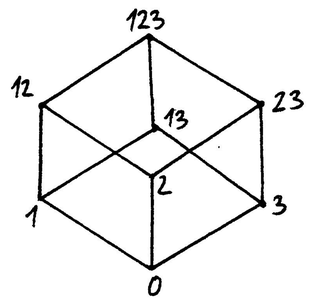
<u>Dm. cv.</u>
V uspořádané množině ex. nejmenší prvek $\Leftrightarrow$ ex. přesně jeden minimální

Prvek $z \in X$ je <u>horní závorou</u> dvojice x, y, pokud $x \leq z$
$y \leq z$

<u>Nejmenší horní závora</u> dvojice x, y (pokud existuje) = <u>supremum</u> prvků x, y

<u>Nejmenší dolní závora</u> dvojice x, y = <u>infimum</u> prvků x, y

<u>Svaz</u> = uspořádaná množina, ve které ex. supremum a infimum pro každou dvojici prvků.
značení: supremum $x \vee y$
infimum $x \wedge y$



svaz podmnožin množiny $\{1,2,3\}$

Vektorové prostory nad $\mathbb{Z}_p$ (p ... prvočíslo)

$(\mathbb{Z}_p)^m$ ... vektor. prostor nad $\mathbb{Z}_p$ dimenze m
$\mathbb{Z}_p^m = \{(a_1, \dots, a_m) : a_i \in \mathbb{Z}_p\}$
$(a_1, \dots, a_m) + (b_1, \dots, b_m) := (a_1 \oplus b_1, \dots, a_m \oplus b_m)$
$\alpha \in \mathbb{Z}_p \to \alpha(b_1, \dots, b_m) := (\alpha \otimes b_1, \dots, \alpha \otimes b_m)$

<u>př.</u> Řešte nad tělesem $\mathbb{Z}_5$: $x + 2y + 3z + 4t = 1$
$x + y + 2z = 0$

$$\left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 1 & 1 & 2 & 0 & 0 \end{array}\right] \sim \begin{array}{l}\text{přičtu} \\ \text{4-násobek} \\ \text{1. řádku} \\ \text{k 2. řádku} \\ 4+1=0\end{array} \left[\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 1 \\ 0 & 4 & 4 & 1 & 4 \end{array}\right]$$

$$\sim \left[\begin{array}{cccc|c} x & y & z & t & \\ 1 & 0 & 1 & 1 & 4 \\ 0 & 1 & 1 & 4 & 1 \end{array}\right]$$

Řešení: $\{(4+4z+4t, 1+4z+t, z, t) : z, t \in \mathbb{Z}_5\}$

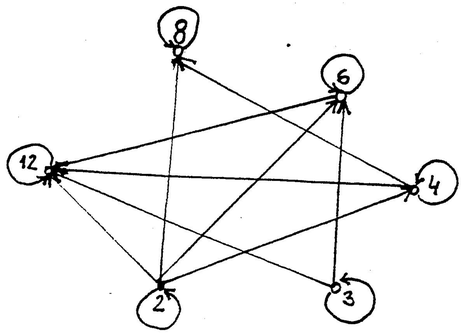
$x + z + t = 4$ $\qquad -1 \equiv 4$
$y + z + 4t = 1$ $\qquad -4 \equiv +1$
$x = 4 - z - t$
$y = 1 - z - 4t$
$x = 4 + 4z + 4t$
$y = 1 + 4z + t$

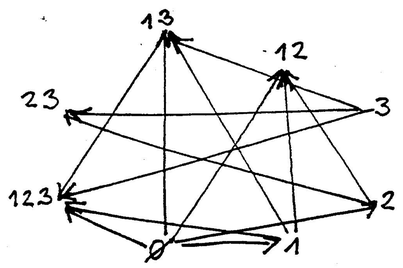
Relace R na X je <u>uspořádání</u> na X, pokud je
reflexivní
antisymetrická
tranzitivní

(<u>neostré</u> uspořádání, protože $x R x$)
(X, R) ... uspořádaná množina
Uspořádání se často značí $\leq, \trianglelefteq$
např. $x \leq y$ na $\mathbb{R}$ má vlastnosti uspořádání

<u>př.</u> uspořádání je i relace dělitelnosti na $\mathbb{N}$

Nechť $(x, \leq)$ je uspořádaná množina.
Prvky $x, y \in X$ jsou <u>porovnatelné</u>, pokud $x \leq y$ nebo $y \leq x$,
jinak jsou <u>neporovnatelné</u>





mn. A
$\mathcal{B}$ = soubor všech podmnožin množiny A

A
1 2 3

$\mathcal{B}$: $\varnothing$ $\{1\}, \{2\}, \{3\},$
$\{1,2\}, \{1,3\}, \{2,3\}$
$\{1,2,3\}$

$\mathcal{B}$ je přirozeně uspořádáno <u>inkluzí</u> ($B_1 \leq B_2$, pokud je $B_1 \subseteq B_2$)

$a \equiv b \Rightarrow [a] = [b]$
$1 \equiv 6 \pmod 5$

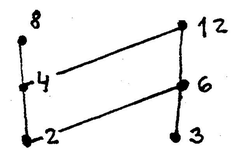
<u>Lineární (úplné)</u> uspořádání:
každé 2 prvky jsou porovnatelné

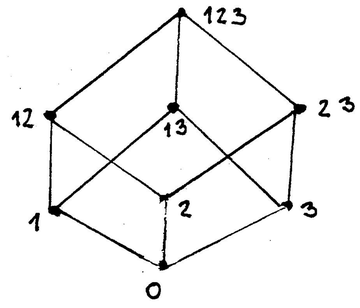
<u>Částečné</u> uspořádání = uspořádání
částečně uspořádaná množina → ČUM
→ poset

<u>Hasseův diagram</u>

$x, y \in X$ uspořádání $\leq$
x je <u>bezprostředním předchůdcem</u> y, pokud $x \leq y$ a
neexistuje z takové, že $x \leq z$ & $z \leq y$.
relace $\lhd$ na X (relace bezprostředního předcházení)

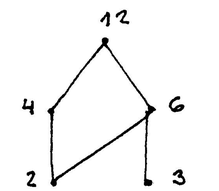
Hasseův diagram, usp. mn. $(x, \leq)$: prvky $x \rightsquigarrow$ body $x \lhd y$
$\Leftrightarrow$ x, y spojeny čárou, y je výš než x



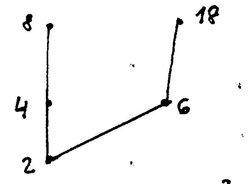


<u>Dm. cv.</u>
<u>Konečná</u> uspořádaná množina je jednoznačně určena svým Hasseův diagram

<u>př.</u> dělitelnost na



$\{2, 3, 4, 6, 12\}$

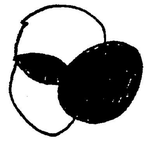


$\{2, 4, 6, 8, 18\}$

Věta (Duální distributivita)

V libovolném distributivním svazu $\forall x, y, z$:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$



Tvrzení

V konečném svazu ex. nejmenší a největší prvek.

Důkaz:

Hledáme největší:

očíslujeme prvky $(X, \leq)$ jako $a_1, \dots, a_n$.

Definujeme posloupnost prvků $s_1, \dots, s_n$

$s_1 := a_1$

$s_{i+1} := s_i \vee a_i$ pro $i = 1, \dots, n-1$

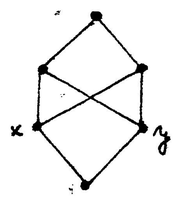
tvrdím: s_n je největší

plyne z ① $s_{i+1} \geq s_i$ (rostoucí posloupnost)

② $s_{i+1} \geq a_i$ (z def. s_{i+1})

Pozn. Obrácená implikace ne platí:

ex. totiž konečná uspořádaná množina s největším a nejmenším prvkem, která není svaz



$x \vee y$ neexistuje

⇓

není svaz.

značení: Největší prvek .... 1 } pokud existují

nejmenší " ... 0 }

Tvrzení

Ve svazu, kde existuje 0 a 1 platí $\forall x$:

$$0 \vee x = x$$
$$1 \wedge x = x$$

Význam:

0 je neutrální k $\vee$

1 " k $\wedge$

Tvrzení: Pro libovolné prvky a, b svazu $(X, \leq)$ platí:

$a \leq b$ právě když $a \vee b = b$

" $a \wedge b = a$

Důkaz:

I. Nechť $a \leq b$. Dokážeme, že $a \vee b = b$

1) b je horní závorou $\{a, b\}$? ANO

2) b je nejmenší horní závorou? ... pokud c je horní závora, potom $c \geq b$ (z definice horní závory)

...ANO

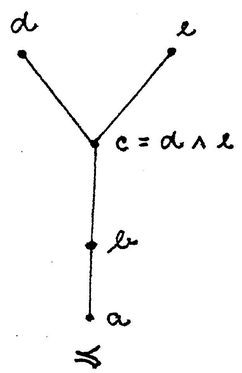
II. Nechť $a \vee b = b$.

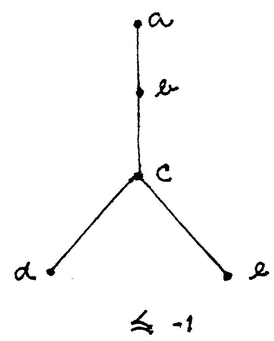
Potom b je nejmenší horní závora $\{a, b\} \Rightarrow$ speciálně $b \geq a$

... 2. pol. důkazu symetricky

Dm.cv. Dokažte, že inverzní relace $\leq^{-1}$ k uspořádání $\leq$ je zase uspořádání.

př.





$\leq^{-1}$

suprema $\leq$ $\Longleftrightarrow$ infima $\leq^{-1}$

infima $\leq$ suprema

Princip duality:
Pokud v tvrzení, které platí ve všech svazech, důsledně zaměníme symboly $\wedge$ a $\vee$ a otočíme směr nerovností, dostaneme opět tvrzení, platné ve všech svazech.

Věta (Vlastnosti suprema)
Pro operaci $\vee$ v libovolném svazu $(X, \leq)$ platí:
(i) je asociativní
(ii) je komutativní
(iii) $a \vee b = a$ pro $a \in X$
(iv) $a \vee (b \wedge a) = a$ pro $a, b \in X$

Důkaz
(ii) plyne přímo z definice suprema
(iii) z minulého Tvrzení: $a \leq a \Rightarrow a \vee a = a$
(iv) volme $b \wedge a \leq a$. Z minulého tvrzení $a \vee (b \wedge a) = a$

! (i) Mějme $a, b, c \in X$
Chceme $\underbrace{a \vee (b \vee c)}_{\ell} = (a \vee b) \vee c$

z definice $\ell \geq a$
$\ell \geq (b \vee c)$ $\Rightarrow a, b, c \leq \ell$
$\ell \geq b$
$\ell \geq c$

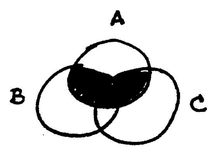
? Platí $\ell \geq a \vee b$?

ℓ je horní závorou pro $\{a \vee b; c\}$
$\ell \geq (a \vee b) \vee c$

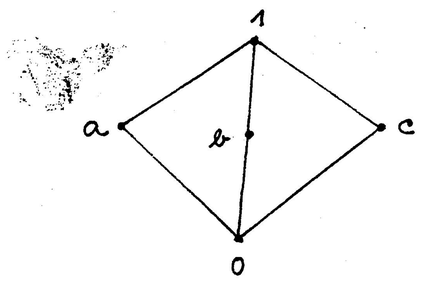
SYMETRICKY: $\ell \leq (a \vee b) \vee c$, z antisymetrie uspořádání: ROVNOST

v tělesech: $a(b+c) = ab + ac$

Otázka:
Platí ve svazech distributivita?
$a \wedge (b \wedge c) \stackrel{?}{=} (a \wedge b) \vee (a \wedge c)$
• např. ve svazech podmnožin ANO



• obecně NE

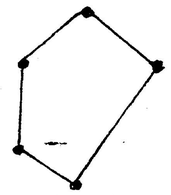


$a \wedge (b \vee c) = a$
$(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$

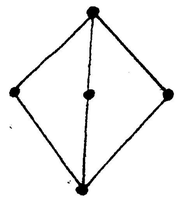
Definice:
Podsvazem svazu $(X, \leq)$ je libovolný svaz $(Y, \leq)$ takový, že:
(1) $Y \subseteq X$ a $\leq$ je zúžení $\leq$ na Y
$\forall x, y \in Y: x \leq y$ právě když $x \leq y$

! (2) suprema (infima) ve svazu $(Y, \leq)$ se shodují se supremy (infimy) v $(X, \leq)$

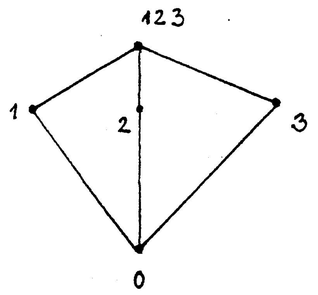
Věta
Svaz je distributivní, právě když neobsahuje jako podsvaz ani jeden ze svazů:



M_5



N_5



suprema se neshodují spirodními ... není podsvaz

6) $a+0=a$

7) $a\cdot 0=0$

8) $\bar{1}=0$

9) $a+\bar{a}=1$

10) $\bar{\bar{a}}=a$

11) $\overline{a+b}=\bar{a}\cdot\bar{b}$ (De Morganovy zákony)

a rovněž <u>duální tvary</u> těchto tvrzení vzniklé záměnou symbolů + a · a symbolů 0 a 1

<u>Důkaz:</u>

10) ... je-li $\bar{a}$ komplement prvku a, platí:

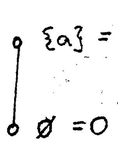
$a+\bar{a}=1 \quad a\cdot\bar{a}=0$

takže také a je komplement prvku $\bar{a}$.

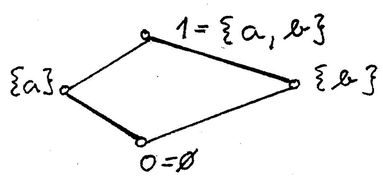
Tedy $a=\bar{\bar{a}}$

-př. Svaz podmnožin libovolné množiny je Bool. algebra

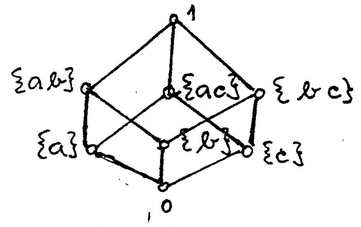
$A=\{a\}$



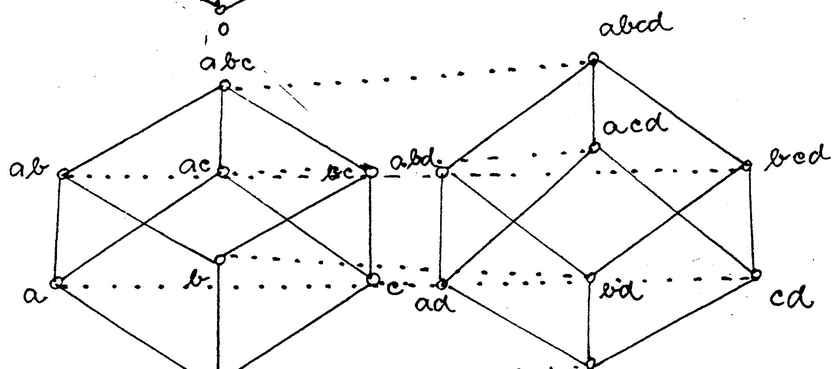
$A=\{a,b\}$



$A=\{a,b,c\}$

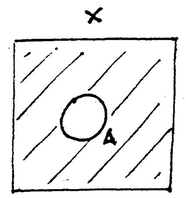


$A=\{a,b,c,d\}$



BOOLEOVY ALGEBRY

<u>Komplement (doplněk)</u>



podmnožiny množiny X → SVAZ

doplněk $\bar{A}$ množiny A:

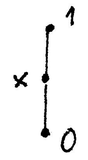
1) $A\cap\bar{A}=\emptyset$

2) $A\cup\bar{A}=X$

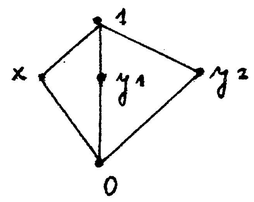
<u>Definice</u>

Nechť $(X,\leq)$ je svaz s 0 a 1. Komplement prvku $x\in X$ je prvek $y\in X$, pro který platí: $x\vee y=1$, $x\wedge y=0$

-př.



... x není komplement



... x má 2 komplementy

<u>Definice</u>

Svaz s 0 a 1, kde každý prvek má nějaký komplement, se nazývá <u>komplementární svaz</u>.

<u>Tvrzení</u>

Je-li $(X,\leq)$ distributivní svaz s 0 a 1, potom každý prvek má <u>nejvýše jeden komplement</u>

<u>Důkaz</u>

Nechť $x\in X$ má komplenty y a y'.

$p:=\underbrace{y\wedge(x\vee y')}_{y}=y$

Z distributivity:

$p = \underbrace{(y \wedge x)}_{0} \vee (y \wedge y') = y \wedge y'$

$\Rightarrow y = y \wedge y' \Rightarrow y \leq y'$

SYMETRICKÁ ÚVAHA $\Rightarrow y' \leq y \quad y = y'$

Pozn.

Ve svazech se používá i terminologie spojení (supremum)
průsek (infinum)

Definice

Booleova algebra je distributivní komplementární svaz s 0 a 1
(Booleův svaz)

Značení:

komplement prvku x .... $\bar{x}$
supremum prvků x, y .... $x+y$
infimum " .... $x \cdot y$

-př. Z definice komplementu je

$x + \bar{x} = 1$

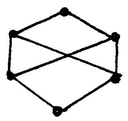
$x \cdot \bar{x} = 0$

-př. Zákony distributivity

$x(y+z) = xy + xz$

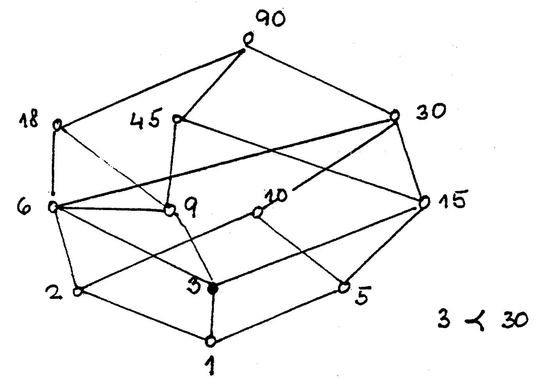
$x+(y \cdot z) = (x+y)(x+z)$

-př.



... není svaz → není Bool. alg.

-př. svaz dělitelů 90



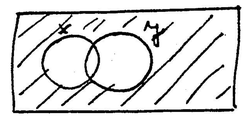
$3 \prec 30$

Věta (De Morganovy zákony)

V Booleově algebře A platí pro každé $x, y \in A$:

a) $\overline{x+y} = \bar{x} \cdot \bar{y}$

b) $\overline{x \cdot y} = \bar{x} + \bar{y}$



Důkaz (jen a), b) symetricky)

chci: $\bar{x} \cdot \bar{y}$ je komplementem prvku $x+y$

Nejprve: • $\underbrace{(x+y)}_{a} + \bar{x} + \underbrace{\bar{y}}_{b,c} \stackrel{?}{=} 1$

p

zákon distributivity:
$a+(b \cdot c) = (a+b)(a+c)$

$p = (\underbrace{x+y}_{a} + \underbrace{\bar{x}}_{b})(\underbrace{x+y}_{a} + \underbrace{\bar{y}}_{c}) = 1 \cdot 1 = 1$

• $\underbrace{(x+y)(\bar{x} \cdot \bar{y})}_{\text{distr.}} \stackrel{?}{=} 0$

$(x \cdot (\bar{x} \cdot \bar{y})) + (y(\bar{x} \cdot \bar{y}))$

$((x \cdot \bar{x}) \cdot \bar{y}) + ((y \cdot \bar{y}) \cdot \bar{x})$

$0 + 0 = 0$

Věta (Počítání v Booleových algebrách)

Pro libovolné prvky a, b, c Bool. alg. B platí:

1) $a + a = a$
2) $a + b = b + a$ (komutativita)
3) $a + (b+c) = (a+b)+c$ (asociativita)
4) $a + (ab) = a$
5) $a(b+c) = (ab) + (ac)$ (distributivita)

x_2	$x_2+x_2+x_2$
0	0
1	1

př. $x \oplus y$? b.p. ? (symetrická diference)

$x \oplus y = \bar{x}y + x\bar{y}$ ... b.p.

$x \oplus y = (x+y)(\bar{x}\bar{y})$ ... b.p.

$f(x,y)$	x	y	$\bar{x}$	$\bar{y}$	$x+y$	$\bar{x}+\bar{y}$
0	0	0	1	1	0	1
1	1	0	0	1	1	1
1	0	1	1	0	1	1
0	1	1	0	0	1	0

Součtový a součinový tvar

Definice

Literál v proměnných $x_1, \dots, x_m$ je libovolný b. polynom ve tvaru x_i nebo $\bar{x}_i$, kde $i = 1, \dots, m$

Bool. polynom p je v **součtovém tvaru**, je-li zapsán jako součet polynomů tak, že každý z nich je součinem literálů.

x_1, x_2, x_3 $\quad (x_1 \cdot \bar{x}_2 \cdot \bar{x}_3) + (\bar{x}_2 \cdot \bar{x}_3) + (\bar{x}_1 \cdot \bar{x}_3) + (x_1 \cdot x_2 \cdot x_3)$

$\qquad\qquad\quad p_1 \qquad\quad p_2 \qquad\quad p_3 \qquad\quad p_4$

• ... $\wedge$

+ ... $\vee$

Booleovský polynom p je v **součinovém tvaru**, je-li zapsán jako součin polynomů tak, že každý z nich je součtem literálů

$$(x_1+\bar{x}_2)(x_2+\bar{x}_3)(x_1+x_2+x_3)$$

Definice

Booleovský polynom v proměnných $x_1, \dots, x_m$ je **v úplném součtovém tvaru**, jestliže je v součtovém tvaru a každý ze sčítanců obsahuje pro každé i literál x_i nebo $\bar{x}_i$ (ne oba)

Booleovský polynom v proměnných $x_1, \dots, x_m$ je **v úplném součinovém tvaru**, jestliže je v součinovém tvaru a každý z činitelů obsahuje $\forall i$ literál x_i nebo $\bar{x}_i$ (ne oba)

př. x, y $\quad (\bar{x}+y)(x+y)$ → úplný součin. tvar (Ú. konj. forma)

$(x\,y)+(\bar{x}\,y)$ " součtový " (Ú disj. forma)

x, y, z $\quad (\bar{x}+\bar{y}+z)(x+y+z)$ ... úplný součin. tvar

$(\bar{x}+\bar{y}+z)$ .... součin

$(\bar{x})+(\bar{y})(z)$ .... součt. neúpl.

Věta

Každou nekonstantní b.f. m proměnných lze zapsat b.p. m proměnných v úpl. součtovém tvaru i v úpl. součinovém tvaru.

Důkaz:

lib. $a = (a_1, \dots, a_m) \in \mathcal{B}_2^m$

Nechť p_a je součin x_i přes všechna i taková, že $a_i = 1$ a všech $\bar{x}_i$ přes všechna i taková, že $a_i = 0$

$\rightarrow (1,0,0,1) = a \qquad p_a = (x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \cdot x_4)$

$\forall p_a$ je b. polynom v součin. tvaru

b. polynom v součt. tvaru

Mějme b. funkci f, kterou chceme reprezentovat b.p. v úplném součtovém tvaru.

$A \subset \mathcal{B}_2^m$ taková pro každé $z \in A \quad f(z) = 1$

$p_f = \sum_{z \in A} p_z$ $\qquad$ hodnota $p_f = 1$

úplný součin. tvar:

$\bar{f}$ $\quad p_{\bar{f}}$ v úplném součt. tvaru

$p_{\bar{f}}$ upravíme dle deMorganových zákonů

př.

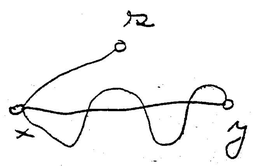
x	y	z	$f(x,y,z)$	$\bar{f}(x,y,z)$
0	0	0	0	1 ←
0	0	1	0	1 ←
0	1	1	1 ←	0
0	1	0	1 ←	0
1	0	0	0	1 ←
1	0	1	0	1 ←
1	1	1	1	0
1	1	0	0	1 ←

Souvislost

Definice

Graf G je souvislý, pokud pro každé 2 vrcholy x, y existuje cesta z x do y.
(jinak nesouvislý)

Definujeme na relaci $V(G)$: $x \sim y$ pokud ex. cesta z x do y
? Je to ekvivalence ?
reflexivní, symetrická ANO

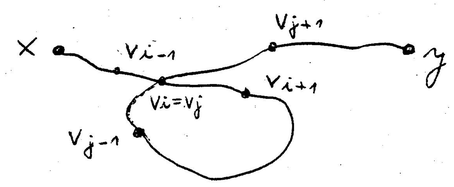


Tvrzení

Existuje-li v grafu G sled z x do y, potom $x \sim y$

Důkaz

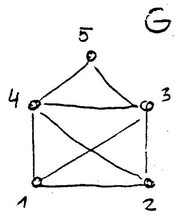
Nechť $(x = v_0, v_1, \dots, v_k = y)$ je sled z x do y, pro který k je nejmenší možné (označme jej S).
Tvrdím: S je cesta.
Dejme tomu, že není. Takže pro nějaké $i \neq j$ je $v_i = v_j$

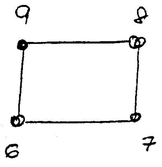


Vezmeme sled $(v_0, \dots, v_{i-1}, v_i, v_{j+1}, \dots, v_k)$
... sled z x do y, kratší než S ... spor

Důsledek:

$\sim$ je ekvivalence



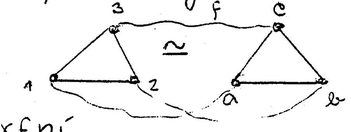


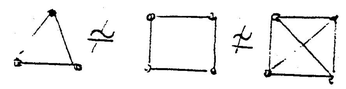
Třídy jsou $\{1,2,3,4,5\}$ a $\{6,7,8,9\}$

$f: V(G) \to V(H)$
$\{u, v\} \rightsquigarrow \{f(u), f(v)\}$

Definice

Izomorfismus grafů G a H je bijekce $f: V(G) \to V(H)$, pro kterou platí, že dvojice $\{x, y\} \in E(G)$ právě když $\{f(x), f(y)\} \in E(H)$.





př. G a H jsou izomorfní

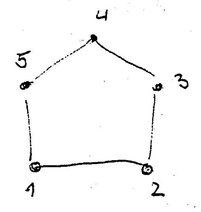
u	1	2	3	4	5
$f(u)$	a	d	e	c	b

$u \in V(\ )$
$f(u) \in V(H)$

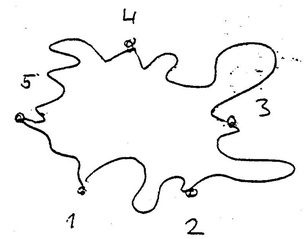
př. Dokažte, že konečné grafy s různým počtem vrcholů nemohou být izomorfní.
$G \simeq H$

Důkaz:

$f: V(G) \to V(H)$ je bijekce
v konečných množinách $V(G)$, $V(H)$ musí platit $|V(G)| = |V(H)|$ ↯



stejný graf

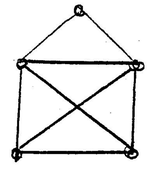


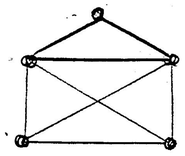
Definice

Graf H je podgrafem grafu G, pokud $V(H) \subset V(G)$ a $E(H) \subset E(G)$;
$H \subset G$ .... zápis

Definice

Graf H je indukovaným podgrafem grafu G, pokud $V(H) \subset V(G)$ a $E(H) \equiv \binom{V(H)}{2} \cap E(G)$





Definice

Stupeň vrcholu x v grafu G je počet hran, které obsahují vrchol x

značení: $d_G(x)$

Tvrzení

V grafu o n vrcholech je stupeň každého vrcholu nejvýše $n-1$

Věta

V každém grafu je počet vrcholů lichého stupně sudý.

Důkaz:

Nechť $S = \sum_{v \in V(G)} d_G(v)$

každá dvojice (v, e), kde e je hrana vycházející z vrcholu v, přispěje k S jedničkou.

S dostanu také jako součet přes všechny hrany $\sum_{e \in E(G)} 2 = 2m$ (počet hran grafu G)

Tedy: součet stupňů je sudý.

$\Rightarrow$ počet lichých stupňů je sudý

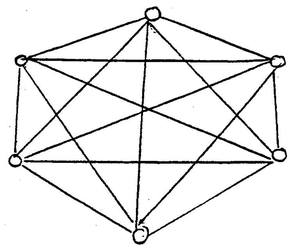
Základní grafy

Nechť $[n] = \{1, 2, \dots, n\}$

K_n **Úplný graf** na n vrcholech

$V(K_n) = [n]$

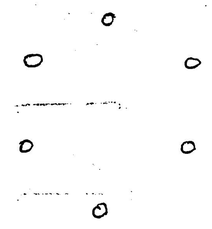
$E(K_n) = \binom{[n]}{2}$



D_n **Diskrétní graf** na n vrcholech

$V(D_n) = [n]$

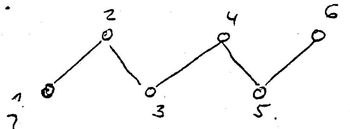
$E(D_n) = \emptyset$



P_n **Cesta** na n vrcholech

$V(P_n) = [n]$

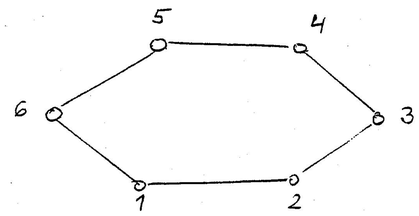
$E(P_n) = \{\{i, i+1\} : 1 \le i \le n-1\}$



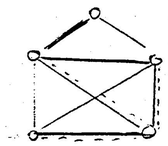
C_n **Kružnice** na n vrcholech

$V(C_n) = [n]$

$E(C_n) = E(P_n) \cup \{\{1, n\}\}$



Sled a cesta



Definice

Sled (z vrcholu u do vrcholu v) v grafu G je posloupnost vrcholů $(u = v_0, v_1, v_2, \dots, v_k = v)$ taková, že pro $i = 1, \dots, k$ $v_{i-1} v_i \in E(G)$

k ... **délka** sledu

Definice

Cesta (z u do v) v grafu G je sled z u do v, který prochází každým vrcholem nejvýše jednou.

Cvičení:

Je-li $(v_0, \dots, v_k)$ cesta v grafu G, definujeme $V' = \{v_0, \dots, v_k\}$

$E' = \{v_i v_{i+1} : i = 0, \dots, k-1\}$

Dokažte, že podgraf (V', E') grafu G je izomorfní s P_{k+1} (cesta na $k+1$ vrcholech).

Důkaz:

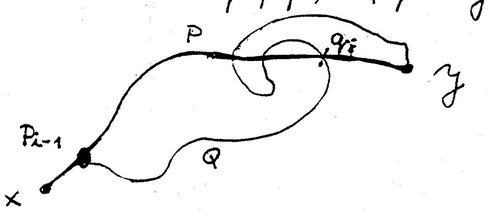
„⇒" Nechť G je strom, x, y dva vrcholy.

víme: G je souvislý ⇒ ex. aspoň 1 cesta z x do y

dejme tomu, že ex. 2 cesty P, Q z x do y

$P = (x = p_0, p_1, \dots, p_k = y)$

$Q = (x = q_0, q_1, \dots, q_k = y)$



$p_0 = q_0 = x$

Nechť i je nejmenší takové, že $p_i \neq q_i$

$1 \leq i \leq k, \ell$

Zvolme j nejmenší takové, že $j > i$ a q_j leží na cestě P

Takové j nutně existuje, protože $y = q_\ell$ leží na P

Definuji sled S: —

vyjdeme z $p_i = q_i$, po cestě Q dorazíme do q_j a

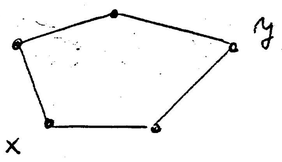
po cestě P zpátky do p_i

toje kružnice ..... SPOR s předpokladem, že G je strom

„⇐" dokazujeme, že G je souvislý a neobsahuje kružnice

. víme, že ex. právě 1 cesta mezi x, y $\forall x, y$

Kdyby G obsahoval kružnici, pak libovolné 2 vrcholy na ní jsou spojeny aspoň 2 cestami



Pozn:

Víme, že souvislý graf na n vrcholech má $\geq n-1$ hran.

Věta

Graf G je stom ⇔ je souvislý a má $n-1$ hran.

Definice

Komponenta grafu G je indukovaný podgraf na libovolné třídě ekvivalence $\sim$.

Pozorování:

G je souvislý ⇔ má jedinou komponentu

Definice

Nechť v je vrchol grafu G. Graf $G - v$ vzniklý odstraněním vrcholu v je definován jako indukovaný podgraf grafu G na množině $V(G) \setminus \{v\}$.

(„odstraním v a hrany, které z něj vychází")

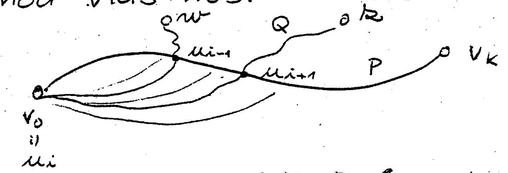
Věta

Každý souvislý graf obsahuje vrchol v takový, že $G - v$ je zase souvislý.

Důkaz:

Nechť $P = (v_0, \dots, v_k)$ je cesta maximální možné délky v grafu G.

Tvrdím: v_0 má požadovanou vlastnost



Všichni sousedi vrcholu v_0 leží na cestě P (jinak by šla prodloužit)

Předpokládejme, že $G - v_0$ není souvislý, konkrétně mezi w a z nejvede cesta

G souvislý je ⇒ obsahuje cestu Q z w do z.

$Q = (w = u_0, u_1, \dots, u_\ell = z)$

Q musí procházet vrcholem v_0 .... nechť třeba $v_0 = u_i$.

Sousedi u_{i-1}, u_{i+1} vrcholu u_i musí ležet na P.

Lze definovat sled:

z w po cestě Q do u_{i-1}, potom po cestě P do u_{i+1}, dále po Q do z

} sled z w do z ⇒ ex. cesta z w do z v grafu $G - v_0$ SPOR

Úmluva:
Počet vrcholů budeme označovat n,
" hran " m
(bude-li graf jasný z kontextu)

Věta
V souvislém grafu je $m \geq n-1$.
Důkaz: indukcí přes n
1) $n=1$ .... OK
2) předpokládejme, že platí pro grafy s méně než n vrcholy
Nechť G má n vrcholů.
Předchozí věta $\Rightarrow \exists v: G-v$ je souvislý
Ať $G-v$ má n' vrcholů a m' hran.
Podle ind. předpokladu je $m' \geq n'-1$ ①
Víme, že $n' = n-1$ ②
$m' \leq m-1$ ③ (vyhodil jsem aspoň jednu hranu)
$m \overset{③}{\geq} m'+1 \overset{①}{\geq} (n'-1)+1 \overset{②}{=} n-1$
Tedy $m \geq n-1$.

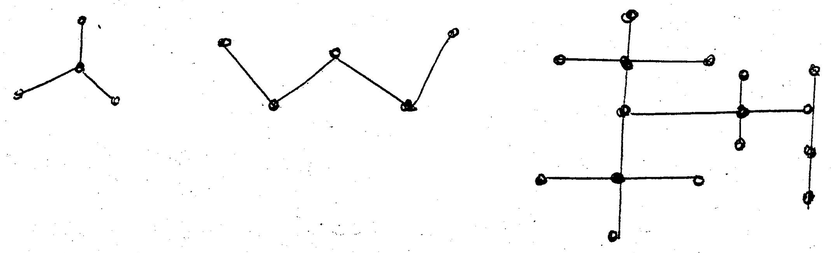
Věta
Jsou-li stupně všech vrcholů v grafu G aspoň $n/2$, pak G je souvislý.
Důkaz
Dejme tomu, že G je nesouvislý. Má tedy aspoň 2 komponenty A, B. Buď A nebo B obsahuje nejvýše $n/2$ vrcholů.
(dohromady je n vrcholů)
Dejme tomu, že A obsahuje $\leq n/2$ vrcholů. Z každého vrcholu komponenty A vedou hrany pouze do jiných vrcholů v A.
Vrcholů v A je $\leq n/2$.
$\Rightarrow$ Stupně vrcholů v A jsou $\leq n/2 - 1$
SPOR s předpokladem, že všechny stupně jsou $\geq n/2$

Stromy

Definice
Kružnice v grafu G je sled $(v_0, \dots, v_k)$, kde $v_k = v_0$, $k \geq 3$, v_0 se vyskytuje právě dvakrát, ostatní vrcholy nejvýše jednou.

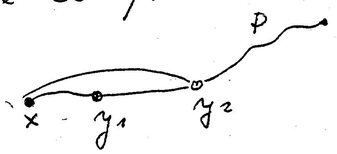
Pozn.
Kružnice v grafu lze ztotožnit s podgrafy izomorfními s C_k

Definice
Strom je souvislý graf, který neobsahuje žádnou kružnici.



List stromu G je každý vrchol stupně 1.

Tvrzení:
Každý strom má aspoň 2 listy.
Důkaz:
Vezmeme cestu P maximální možné délky.
Nechť x je její koncový vrchol.
Všichni sousedi vrcholu x leží na P.



Pokud x není list, má aspoň 2 sousedy y_1, y_2
Definuji sled: z x do y_1 dále po P do y_2 a zpět do x.
To je kružnice v $G \Rightarrow$ SPOR s tím, že G je strom.
Druhý list: druhý konec P

Věta
Graf G je strom, právě když pro každé 2 vrcholy x, y existuje právě jedna cesta z x do y

Důsledek:
Počet prvků konečné B. algebry $\mathcal{A}$ je mocnina čísla 2.
Konkrétně $At(\mathcal{A}) = m$, počet prvků B. alg. je 2^m.

👁 $g: Y \to Z$ je bijekce mezi konečnými množinami Y a Z.
$2^g : 2^Y \to 2^Z \qquad 2^g(A) = \{ g(a); a \in A \}$

Důsledek:
2 konečné B. algebry se stejným počtem prvků jsou izomorfní.

Důkaz: $\mathcal{A}, \mathcal{B}$ $\quad$ $\mathcal{A}, \mathcal{B}$ jsou stejně velká
$\mathcal{A} \cong 2^{(At(\mathcal{A}))}$ $\quad$ $g: \mathcal{A} \rightsquigarrow \mathcal{B}$
$\mathcal{B} \cong 2^{(At(\mathcal{B}))}$ $\quad$ $2^g : 2^{At(A)} \rightsquigarrow B^{At(B)}$ izomorfismus

Definice
Direktní součin B. algeber $(A_1; \leq_1)$ a $(A_2; \leq_2)$ je kartézský součin $A_1 \times A_2$ s uspořádáním def. po složkách:
$(a_1, b_1) \leqq (a_2, b_2) : a_1 \leq_1 a_2, \wedge\ b_1 \leq_2 b_2$

$\mathcal{B}_2 = \{0,1\}$ $\quad$ $\mathcal{B}_1 \times \mathcal{B}_2 = \{(0,0),(0,1),(1,0),(1,1)\} = \mathcal{B}_2^2$
$\mathcal{B}_2^2 \times \mathcal{B}_2 = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),\dots\} = \mathcal{B}_2^3$

Tvrzení
Je-li X n-prvková, potom $2^X \cong \mathcal{B}_2^n$

Důkaz:
$X = \{1,2,3,\dots,n\}$
$\forall i \in X \dots\ w_1 = (0,0,\dots 0,1,0\dots 0)$ (↑ i-té místo)

$f: 2^X \rightsquigarrow \mathcal{B}_2^n$
$f(Y) = \sum_{i \in Y} w_i$

$\{1\} \subseteq \{1,2\}$ $\quad$ $f(\{1\}) \leq f(\{1,2\})$ (1,0,…,0 ≤ 1,1,0…0)

Důsledek:
každá konečná B. algebra je izomorfní s B. algebrou $\mathcal{B}_2^n$ pro nějaké n

+	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

·	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

$\bar{0} = 1,\ \bar{1} = 0,\ \bar{a} = b,\ \bar{b} = a$

Stoneova věta reprezentaci konečných Booleových algeber

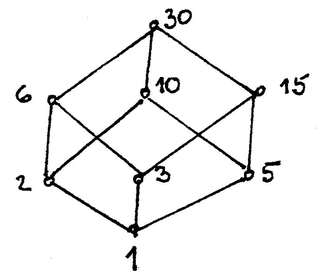
Pozn. Bool. algebra všech podmnožin množiny A se značí 2^A

Pozn. ve svazu je definováno $x \vee y$
A je svaz, $B = \{b_1, \dots, b_m\} \subseteq A$
lze definovat $\sup B = ((b_1 \vee b_2) \vee b_3) \vee \dots \vee b_k$
sup B je tím jednoznačně určeno díky asociativitě a komutativitě
(samozřejmě definujeme $\sup\{a\} = a$) (nezáleží na pořadí b_i)
$\sup \emptyset = 0$, pokud svaz má prvek 0

Ekvivalentně lze sup B definovat jako nejmenší horní závoru množiny B

Definice
Prvek x Bool. algebry B je atom, pokud neexistuje prvek $y \in B \setminus \{0, x\}$ tak, že $0 \lneq y \lneq x$

př. Svaz dělitelů 30



atomy = prvočísla

Definice

Booleovy algebry $\mathcal{A}, \mathcal{B}$ jsou <u>izomorfní</u>, pokud ex. $f: \mathcal{A} \to \mathcal{B}$ tak, že 1) f je bijekce

2) pro každé $x, y \in \mathcal{A}$:

$x \leq y \iff f(x) \leq f(y)$

$(v\ \mathcal{A})$ $\qquad$ $(v\ \mathcal{B})$

(definici lze vlastne vztáhnout na libovolné uspoř. množiny)

Zobrazení f ... izomorfismus mezi $\mathcal{A}$ a $\mathcal{B}$

Věta

<u>Konečná</u> Booleova algebra $\mathcal{B}$ je izomorfní s Bool. alg. 2^A, kde A je množina všech atomů Bool. algebry $\mathcal{B}$

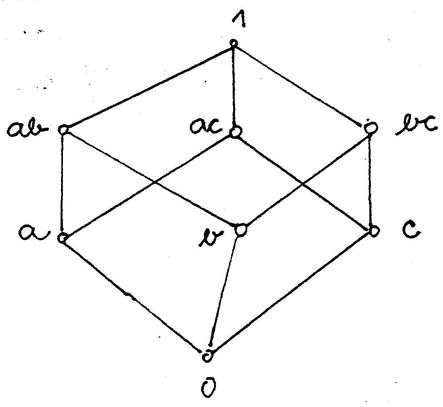
<u>Důkaz:</u>

Sestrojíme izomorfismus $f: \mathcal{B} \to 2^A$

Pro $x \in \mathcal{B}$ položím $x^* = \{a \in A : a \leq x\}$

Tedy $x^* \subset A$, takže $x^* \in 2^A$

př. $2^{\{a,b,c\}}$



Definuji f vztahem: $f(x) = x^*$ pro $x \in \mathcal{B}$

Je f izomorfismus mezi $\mathcal{B}$ a 2^A?

1) je prosté?
2) je na?
3) $x \leq y \implies x^* \subseteq y^*$?
4) $x^* \subseteq y^* \implies x \leq y$?

a...atom

3) Nechť $x \leq y$. Potom $a \leq x \underset{\text{tranz.}}{\implies} a \leq y$

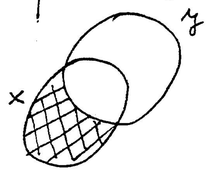
Tedy $x^* \subseteq y^*$

4) ukážeme $x \not\leq y \implies x^* \not\subseteq y^*$

pozorování: Pro každý nenulový prvek $x \in \mathcal{B}$ ex. atom $a \leq x$.

(jinými slovy $x^* \neq \emptyset$)

(důkaz: předposlední prvek na cestě z x do 0 v Hasseově diagramu je atom)



Nechť $z = x \cdot \bar{y}$. Jistě $z \neq 0$.

Víme: $x \not\leq y \implies x \cdot y \neq x$

nicméně: $x = x(y + \bar{y}) = xy + x\bar{y}$ (1, x, z musí být nenulový)

Podle pozorování ex. atom $a \leq z$

Tvrdím: $a \leq x$, ale $a \not\leq y$

$a \leq x$ jasné z toho, že $a \leq x\bar{y}$

podobně platí $a \leq \bar{y}$

Kdyby $a \leq y$, pak by a bylo dolní závorou $y, \bar{y}$, a tedy $a \leq y \cdot \bar{y} = 0$ ... SPOR

Našli jsme $a \in x^*$, přičemž $a \notin y^*$, takže $x^* \not\subseteq y^*$

1) je f prosté?

$x \neq y \overset{?}{\implies} x^* \neq y^*$?

Ovšem pokud $x \neq y$, tak buď $x \not\leq y$ nebo $y \not\leq x$ (z antisymetrie)

dejme tomu, že $x \not\leq y$, pak z části 4) plyne $x^* \not\subseteq y^*$ speciálně $x^* \neq y^*$

Stoneova věta

Konečná booleovská algebra je izomorfní s algebrou $2^{(At(A))}$.

<u>Důkaz:</u> na $\mathcal{B}^* \in 2^{(At(A))}$ $\exists\ \mathcal{B}(A)$

$B = \{a_1, a_2, \dots, a_r\}$ $\quad \forall a_i \in \mathcal{B}^*\ a_i \leq \mathcal{B}$

$\nexists\ c \in B \quad c \leq \mathcal{B}$

$\sup(a_1, \dots, a_r) = \mathcal{B}$ $\quad$ X $c \cdot \mathcal{B} \overset{?}{=} c$

$c \cdot \mathcal{B} = c(a_1 + a_2 + \dots + a_r) =$

$= c \cdot a_1 + c \cdot a_2 + \dots c \cdot a_r = 0 + \dots 0$

$\implies c = 0$, ale 0 není atom

$\implies$ obrazem $\mathcal{B}$ je B

$p_f = (\bar{x}\cdot y\cdot \bar{z}) + (\bar{x}\cdot y\cdot z) + (x\cdot y\cdot \bar{z}) = 0+0+0 = 0$

$x=0,\ y=1,\ z=0$; $x=0,\ y=1,\ z=1$; $x=1,\ y=1,\ z=0$

$x=0,\ y=0,\ z=0$

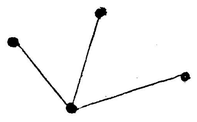
$p_{\bar{f}} = (\bar{x}\cdot\bar{y}\cdot\bar{z}) + (\bar{x}\cdot\bar{y}\cdot z) + (x\cdot\bar{y}\cdot\bar{z}) + (x\cdot\bar{y}\cdot z) + (x\cdot y\cdot z)$

$\overline{p_{\bar{f}}} = (x+y+z)(x+y+\bar{z})(\bar{x}+y+z)(\bar{x}+y+\bar{z})(\bar{x}+\bar{y}+\bar{z}) = 1$

$x=1,\ y=1,\ z=0$; $x=1,\ y=1,\ z=1$; ... $=0$

- $f(x,y) = ((\overline{\bar{x}y})\cdot\bar{x}) + y = ((x+\bar{y})\cdot\bar{x}) + y =$
  $= \underbrace{x\cdot\bar{x}}_{0} + \bar{y}\bar{x} + y = \bar{y}\bar{x} + y\cdot\underbrace{1}_{x+\bar{x}=1} = \bar{y}\bar{x} + y(x+\bar{x}) =$
  $= \bar{y}\bar{x} + yx + y\bar{x}$ ... úplný součt. tvar

GRAFY



vrcholy (uzly) hrany

$V(G)$... množina vrcholů
$E(G)$... " hran ($H(G)$)

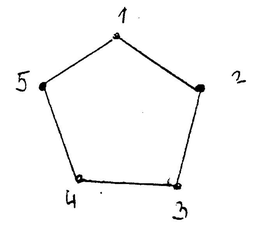
Definice
Grafem nazveme uspoř. dvojici $G = (V(G), E(G))$

$e \in E(G) = \{x,y\}$ $x,y \in V(G)$

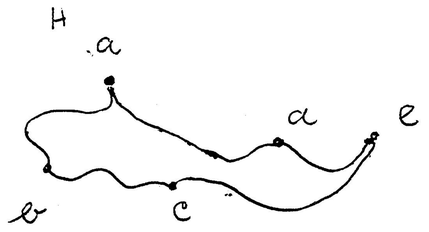
$E(G) \subseteq \binom{V}{2} = \{\{x,y\};\ x,y \in V;\ x \neq y\}$

Izomorfismus a podgrafy

G



H



BOOLEOVSKÉ FUNKCE

Definice
Booleovská f-ce n proměnných je libovolná f-ce $f: \mathcal{B}_2^n \rightsquigarrow \mathcal{B}_2$

$\mathcal{B}_2^2$	"+"	+	·	$\mathcal{B}_2'$
		$00 \rightsquigarrow 0$	$00 \rightsquigarrow 0$	$0 \rightsquigarrow 1$
		$01 \rightsquigarrow 1$	$01 \rightsquigarrow 0$	$x=0 \rightsquigarrow \bar{x}=1$
		$10 \rightsquigarrow 1$	$10 \rightsquigarrow 0$	$x=1 \rightsquigarrow \bar{x}=0$
		$11 \rightsquigarrow 1$	$11 \rightsquigarrow 1$	

př.
$x \oplus y = \bar{x}y + x\bar{y} = f(x,y)$

x	y	$\bar{x}$	$\bar{y}$	$\bar{x}\cdot y$	$x\cdot\bar{y}$	$f(x,y)$
0	0	1	1	0	0	0
0	1	1	0	1	0	1
1	0	0	1	0	1	1
1	1	0	0	0	0	0

př. $x \to y = \bar{x} + y$

	x	y	$\bar{x}$	$\bar{x}+y$
	0	0	1	1
→	0	1	1	1
→	1	0	0	0
	1	1	0	1

(z pravdy neplyne nepravda)

Definice (Booleovské polynomy)
1) Výrazy $0, 1, x_i$ (libovolné $i = 1,\dots,n$) jsou b. polynomy
2) f, g 2 b. polynomy v proměnných $x_1,\dots,x_n$
$(f+g)$ $(f\cdot g)$ a $\bar{f}$ jsou rovněž b. polynomy
+ ... spojení
· ... průsek
$\rightsquigarrow$ 2 b. polynomy si jsou rovny, pokud určují stejnou b. funkci.

př. $x_2 + x_2 + x_2$ je to b.p. $x_2 + x_2 + x_2 = x_2$

$x_2 + x_2$
$\{x_2 + x_2\} + x_2$

Silná souvislost

Definice

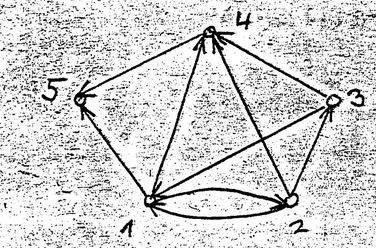
Orientovaný sled z x do y v orient. grafu G je posloupnost $(x = v_0, v_1, \dots, v_k = y)$, ve které je pro každé $i = 1, \dots, k$ dvojice $v_{i-1}\, v_i$ hranou G.

Orient. cesta z x do y v G je orient. sled z x do y, ve kterém se žádný vrchol neopakuje

Cyklus je orient. sled z x do x, ve kterém se x vyskytuje jen dvakrát a ostatní body nejvýše jednou

Definice

Orient. graf G je silně souvislý, pokud $\forall x, y \in V(G)$ existují orientované cesty z x do y i z y do x



př.:
(3,1,2,4,4) je sled v G
(4,3,2,1) není sled
G není souvislý
(4,4) je cyklus v G (délky 1)

Cvičení:
Dokažte, že v orient. grafu ex. orient. sled z x do y, právě když existuje orient. cesta z x do y.

Věta

Slabě souvislý orient. graf je silně souvislý, právě když každá hrana je obsažena v nějakém cyklu.

Důkaz

„⇒" Nechť G je silně souvislý. ... je v cyklu?

Důkaz:

„⇒" Strom je souvislý. Má $n-1$ hran?

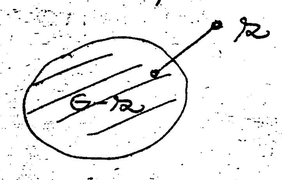
Indukce přes n:

1) $n=1$ .... nutně $m = 0 = n-1$ ... ok

2) indukční krok: předpokládejme platnost dokazovaného tvrzení pro všechny stromy s $n' < n$ vrcholy, dokažme pro strom G na n vrcholech:
Víme, že G má list ℓ. Odstraníme list ℓ .... $G-\ell$ je pořád strom.
Z indukčního předpokladu plyne, že $G-\ell$ má $(n-1)-1 = \underline{n-2}$ hran
Tím pádem G má $n-1$ hran ($n-2$ hran v $G-\ell$ plus 1 hrana vycházející z ℓ) a má n vrcholů
⇒ tvrzení platí

„⇐" Nechť G je souvislý a $m = n-1$.
tvrdím: G obsahuje vrchol stupně 1. (pokud $n > 1$)
⊛ dejme tomu, že ne.
ze souvislosti plyne, že neex. vrchol stupně 0, tedy všechny stupně jsou ≥ 2.
víme: $m = \frac{1}{2}\left(\sum_{x \in V} d_G(x)\right) \geq \frac{1}{2} \cdot 2n = n$ ← stupeň x
SPOR s předpokladem $m = n-1$

Dokazujeme indukcí, že G je strom;
stačí dokázat, že G neobsahuje kružnici:
1) $n=1$ .... graf s jediným vrcholem je jistě strom → platí
2) indukční krok: nechť G má n vrcholů
podle pomocného tvrzení ⊛ G obsahuje vrchol x stupně 1.



$G-x$ má
- $n-1$ vrcholů
- $n-1$ hran
- $= n-2$
- je souvislý

} ⇒

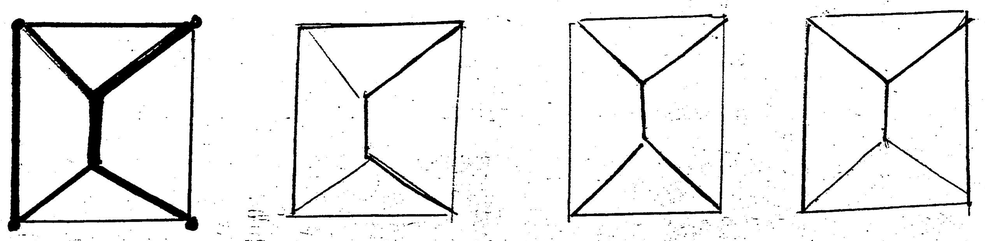
⇒ lze použít indukční předpoklad na $G-x$ ⇒ $G-x$ je strom
tedy i G je strom (díky tomu, že vrchol x je stupně ?)

Kostry

Definice

Kostra grafu G je libovolný podgraf $H \subset G$, který je stom a $V(H) = V(G)$.

Pozorování:
kostra může mít jen souvislý graf.

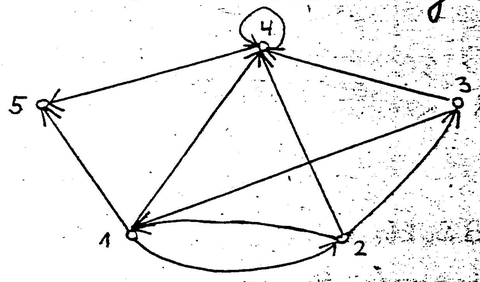


Věta

Každý souvislý graf má aspoň jednu kostru

Důkaz:
Nechť $G = (V, E)$. Uvažme množinu hran $M \subset E$ s vlastností:
(A) graf (V, M) neobsahuje kružnice, která je maximální taková vzhledem k inkluzi.
tvrdím, že graf (V, M) je souvislý (tím pádem to bude kostra grafu G.
Dejme tomu, že je nesouvislý a má komponenty A, B.
Ale G je souvislý $\Rightarrow$ nějaká hrana e vede mezi A, B.
Přidáním hrany e k množině M nemůže vzniknout kružnice
$\rightarrow$ SPOR s maximalitou množiny M
Tedy podgraf (V, M) je souvislý a je tudíž kostrou grafu G.

Orientované grafy



Definice

Orientovaný graf je dvojice (V, E), kde V je množina vrcholů a $E \subset V \times V$ je množina hran.
Dvojici $(x, y) \in E$ budeme psát xy a reprezentovat jako hranu vycházející z x a končící v y

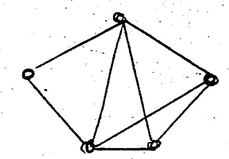
Definice

Symetrizací orientovaného grafu G je neorientovaný graf, získaný „zapomenutím" šipek, odstraněním případných smyček a nahrazením násobných hran jednoduchými.

Definice

Orientovaný graf G je orientací grafu H, pokud H je symetrizací grafu G.
(pozn. H má obecně mnoho orientací)

symetrizace.



Definice

Orientovaný graf G je slabě souvislý, pokud jeho symetrizace je souvislá.

Definice $d^+_G(v)$

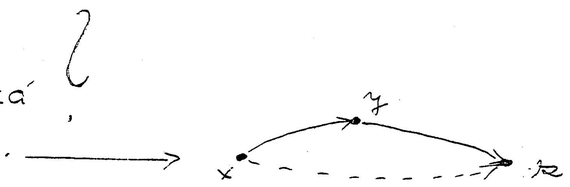
Vstupní stupeň vrcholu v orient. grafu G je počet hran, které končí ve vrcholu v, tj. počet dvojic x, y (kde $x \in V(G)$) v množině $E(G)$.
Výstupní stupeň je podobně počet hran, které z v vycházejí; značení: $d^-_G(v)$

Cvičení:
V orient. grafu G s m hranami je $\sum_{v \in V(G)} d^+_G(v) = \sum_{v \in V(G)} d^-_G(v) = m$

Cvičení:

Jak poznáme z grafa $G(R)$, zda relace R je:

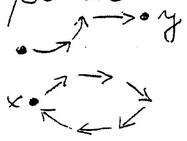
- reflexivní
- symetrická
- antisymetrická
- tranzitivní ...



obecněji: pokud v $G(R)$ ex. orient. sled z x do y, pak musí být $xy \in E(G(R))$

Definice

Tranzitivní uzávěr orient. grafu G je orient graf G^+ takový, že $V(G^+) = V(G)$ a platí $xy \in E(G^+)$, pokud
- $x \neq y$ a v G ex. orient. cesta z x do y
- $x = y$ a vrchol x leží na nějakém cyklu



Pozorování

a) $G \subset G^+$

b) G je acyklický $\Leftrightarrow$ G^+ neobsahuje žádnou smyčku

Věta

Orientovaný graf G bez smyček je acyklický $\Leftrightarrow$ graf G^*, vzniklý z G^+ přidáním všech smyček, je grafem uspořádání na $V(G)$ (jinými slovy relace $E(G^*)$ je uspořádání)

Důkaz

„$\Rightarrow$" Nechť G je acyklický.

1) je $E(G^*)$ reflexivní? ANO (přidané smyčky)

2) je $E(G^*)$ tranzitivní? ANO (z definice tranzitivního uzávěru)

3) je $E(G^*)$ antisymetrická?

kdyby $xy \in E(G^*)$ a $yx \in E(G^*)$, pak v G ex. orient. cesta z x do y i cesta z y do x; potom v G najdeme cyklus

vezmeme orient. cestu P z y do x.
P spolu s hranou xy tvoří cyklus obsahující xy

„$\Leftarrow$" Nechť G je slabě souvislý, každá hrana v cyklu

? je G silně souvislý ?

Mějme vrcholy x, y

Ex. orient. cesta z x do y ?

Ze slabé souvislosti: cesta Q z x do y v symetrizaci grafu G

Některé hrany cesty Q .... „dobře" orientované (ve směru od x k y), jiné: „špatně" (od y k x)

Pro každou špatně orientovanou hranu $e = uv$ cesty Q vezmu cyklus obsahující e
ten určuje cesta Q_e z V do U
V cestě Q nahradím každou špatně orientovanou hranu příslušnou cestou Q_e.
Výsledkem je orientovaný sled z x do y.
Existuje tedy i orient. cesta z x do y.
V opačném směru - podobně.
Závěr: G je silně souvislý

Definujeme relaci $\sim$ na $V(G)$ (relace oboustranné dosažitelnosti): $x \sim y \Leftrightarrow$ v G ex. orient. cesta z x do y i naopak

Pozorování: $\sim$ je ekvivalence

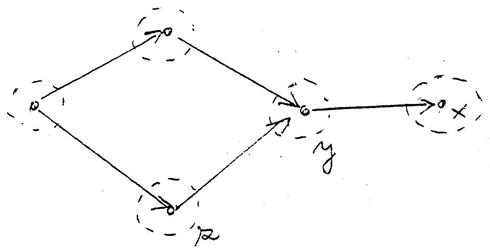
Definice

Kvazi Komponentu orient. grafu G je indukovaný podgraf grafu G na libovolné třídě ekvivalence $\sim$.

třídy ekvivalence $\sim$	
$\{1,2,3\}$....	
$\{4\}$	•
	•

Cvičení:
Dokažte, že kvazikomponenty grafu G jsou právě maximální silně souvislé podgrafy, tj. právě silně souvislé podgrafy H s vlastností, že je-li H vlastním podgrafem jiného $k \subset G$, potom k není silně souvislý

Acyklické orientované grafy



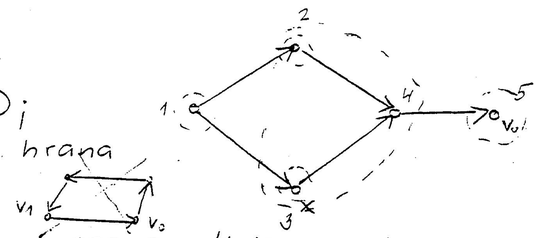
kvazikomponenta grafu G
indukovaný podgraf na libovolné třídě ekvivalence oboustranné dosažitelnosti

Definice
Orientovaný graf G je acyklický, pokud neobsahuje jako podgraf žádný orientovaný cyklus.

Definice
Vstupní vrchol orient. grafu G je vrchol, do kterého nevchází žádná hrana ($d_G^+(v)=0$)
Výstupní vrchol .... $d_G^-(v)=0$

Věta
konečný orientovaný graf G je acyklický $\Leftrightarrow$ každý neprázdný podgraf $H \subset G$ obsahuje vstupní vrchol

Důkaz:
„$\Rightarrow$" Nechť G je acyklický.
Zvolme vrchol $v_0 \in V(H)$;
pokud není vstupní, ex. hrana $v_1 v_0 \in E(H)$
pokud v_1 není vstupní, proces opakujeme



G acyklický => nevrátíme se do navštíveného vrcholu
G konečný => po konečném počtu kroků najdeme vstup. vrchol

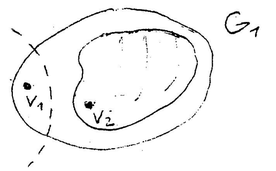
„$\Leftarrow$" Nechť G obsahuje cyklus C.
C musí obsahovat vstupní vrchol. SPOR

Důsledek:
G je acyklický $\Leftrightarrow$ každý neprázdný $H \subset G$ obsahuje výstupní vrchol

Důkaz:
Otočení hran zachová acykličnost a vstupní vrcholy se změní za výstupní.

Věta
Orient. graf G je acyklický, právě když jeho vrcholy lze seřadit do posloupnosti $v_1, \dots, v_n$ tak, že $v_i v_j \in E(G) \Rightarrow i < j$

Důkaz:
„$\Rightarrow$" Položme $G_1 = G$
Podle minulé věty ex. vstupní vrchol v_1 grafu G_1
Nechť $G_2 = G_1 - v_1$ (odstraníme v_1 a všechny hrany, které ho obsahují)
V_2 := vstupní vrchol grafu G_2
(ex., protože $G_2 \subset G$)



$G_3 = G_2 - v_2$ ... opakujeme n-krát => dostaneme posl. $v_1, \dots, v_n$, kde v_i je vstup. vrchol grafu G_i
• Dejme tomu, že $v_i v_j \in E(G)$ a potom $i > j$. Potom $v_i \in V(G_j)$ a tedy $v_i v_j$ je hranou $E(G_j)$, => v_j nemůže být vstupní v G_j .... SPOR

Tranzitivní uzávěr

orient. graf G na V $\rightsquigarrow$ binární relace na V

příslušná relace je právě množina hran E(G)

Je-li R relace, budeme značit její orient. graf jako G(R).

Důkaz

$\Leftarrow$" triviální ... vím, že $\sum_{r_i \in J} r_i = \mathcal{O}$ a to je lineární závislost na množině J (je totiž $\sum_{r_i \in J} \alpha_i r_i = \mathcal{O}$ pro $\alpha_i = \begin{cases} -1 & r_i \in J \\ 0 & \text{jinak} \end{cases}$)

↑ řádky matice

$\Rightarrow$"

$M(G)$

	0
v_i	+1
	0
	-1
	0

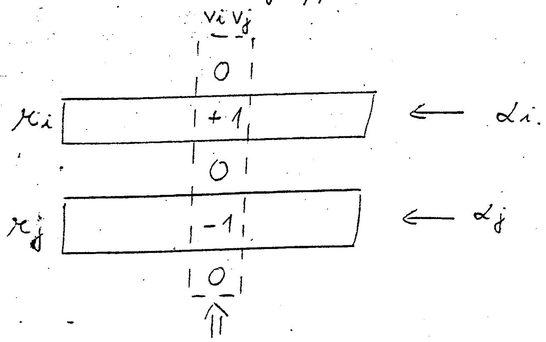
V každém sloupci $M(G)$:
- jedna +1
- jedna -1
- jinak samé 0

i-tý řádek $M(G)$ označíme r_i (odpovídá vrcholu v_i)

Předpokládáme: množina řádků J je lin. závislá:

$$\sum_{r_i \in J} \alpha_i r_i = \mathcal{O} \dots \text{kde ne, všechny } \alpha_i = 0$$

Pozorování: pokud J obsahuje řádky r_i, r_j a v G ex. hrana $v_i v_j$, potom musí platit $\alpha_i = \alpha_j$



Pozorování č. 2: Pokud $r_i \in J$ a $\alpha_i \neq 0$, potom pro každého souseda v_j vrcholu v_i musí platit $r_j \in J$ a $\alpha_j = \alpha_i$

- Hledám $J' \subset J$ s nulovým součtem.

Zvolím $v_{i_0} \in J$, pro který je $\alpha_{i_0} \neq 0$.

Nechť C je komponenta slabé souvislosti obsahující v_{i_0}.

Z pozorování č. 2 plyne: řádky odpovídající vrcholům C jsou všechny v J, pro každý z nich je $\alpha_j = \alpha_{i_0}$

Tvrdím, že $\sum_{v_i \in V(C)} r_i = \mathcal{O}$. Určitě je $\sum_{v_i \in V(C)} \alpha_i \cdot r_i = \mathcal{O}$ (omezil jsem původní lin. kombinaci na $V(C)$, vrcholy $v_k \notin V(C)$ totiž nemohou tuto lin. komb. ovlivnit)

Nechť P_1 je cesta z x do y
P_2 " y do x

Vyjdeme z x po P_1 až k 1. průsečíku s P_2. Pak jdeme po P_2 zpět do x;
cyklus $\Rightarrow$ spor s acykličností

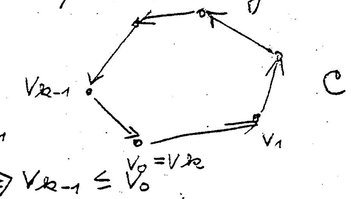
$\Leftarrow$" Nechť $E \in E(G^*)$ je uspořádání.

Sporem: nechť G obsahuje cyklus $C = (v_0, v_1, \dots, v_{k-1}, v_k = v_0)$

Místo „$(x,y) \in E(G^*)$" budeme psát „$x \leq y$"

Pro cyklus C vidíme:

$v_0 \leq v_1 \leq v_2 \leq \dots \leq v_{k-1}$



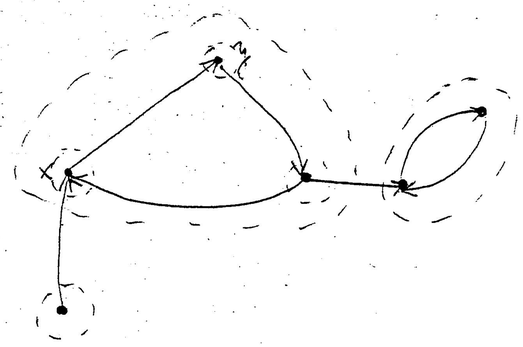
a z tranzitivity: $v_0 \leq v_{k-1}$

ale $v_{k-1} v_0$ je hrana $G \Rightarrow v_{k-1} \leq v_0$

antisymetrie: $\Rightarrow v_0 = v_{k-1} \Rightarrow k = 1$ a cyklus C je smyčka

SPOR s předpokladem, že G je bez smyčky

Kondenzace



Definice

Kondenzace orient. grafu G je orientovaný graf G_c, jehož vrcholy jsou kvazikomponenty grafu G a platí, že kvazikomponenty $Q_1 \neq Q_2$ jsou spojeny hranou $Q_1 Q_2$, pokud ex. $v_1 \in V(Q_1)$, $v_2 \in V(Q_2)$ tak, že $v_1 v_2 \in E(G)$.

Věta o kondenzaci:

Pro ~~acyklický~~ orient. graf G platí:

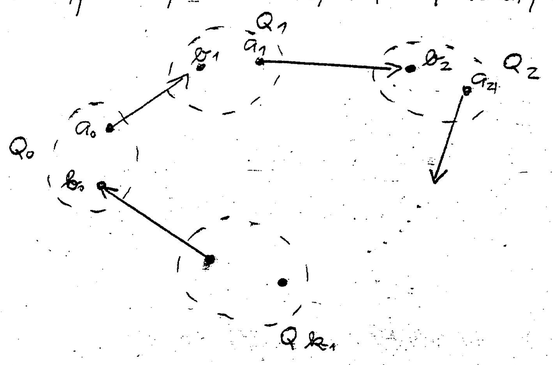
1) G_c je acyklický
2) G je silně souvislý $\Leftrightarrow$ G_c má jediný vrchol
3) G je acyklický $\Leftrightarrow$ $G = G_c$

Důkaz

1) SPOREM

Nechť G_c obsahuje cyklus $(Q_0, Q_1, \dots, Q_{k-1}, Q_k = Q_0)$

v grafu G



2 definice kondenzace ex. $a_i, b_i \in V(Q_i)$ pro $i = 0, \dots, k-1$ s vlastností, že $a_i b_{i+1} \in E(G)$ (přičemž $b_k = b_0$)

Tvrdím: ex. orient. cesta z b_1 do a_0: z b_1 jistě najdu cestu P_1 do a_1 (protože Q_1 je kvazikomponent), přejdu po hraně $a_1 b_2$, totéž pro další Q_i, skončím v a_0

Tedy a_0, b_1 jsou v relaci oboustranné dosažitelnosti... SPOR

2) „G je silně souvislý $\Leftrightarrow$ G_c má jen 1 vrchol"
G je silně " $\Leftrightarrow$ má jedinou kvazikomponentu.
$\Leftrightarrow$ G_c má jediný vrchol

3) „G je acyklický $\Leftrightarrow$ $G = G_c$"
„$\Rightarrow$" G acyklický. Tvrdím: $\forall x, y$ buď neex. cesta z x do y do x

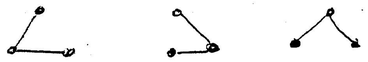
tím pádem žádné 2 vrcholy nejsou v relaci oboustran. dosaž. $\Rightarrow$ kvazikomp. jsou jednobodové
$\Rightarrow G_c = G$

„$\Leftarrow$" Kdyby G obsahoval cyklus C, potom všechny $v \in V(C)$ musí být spolu v kvazikomponentě, takže $G = G_c$

Grafy a matice

Motivace: Kolik existuje různých stromů na pevné n-bodové množině?

$n = 2$

$n = 3$ 

$n = 4$

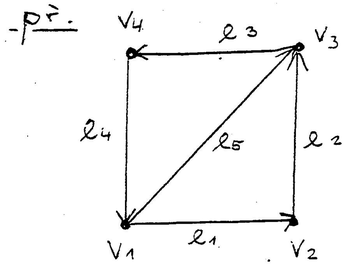
Definice

Nechť G je orient. graf s očíslovanými vrcholy: $V = \{v_1, \dots v_m\}$ a hranami $E = \{e_1, \dots, e_n\}$.

Potom incidenční matice $M(G)$ grafu G je reálná matice o rozměrech $n \times m$. (řádky odpovídají vrcholům, sloupce hranám) taková, že $M(G) = (m_{ij})_{\substack{i=1\dots n \\ j=1\dots m}}$ a platí

$m_{ij} = \begin{cases} 0 & \text{když } v_i \notin e_j \\ +1 & " \quad e_j \text{ vychází z } v_i \\ -1 & \quad e_j \text{ vchází do } v_i \end{cases}$

př.



$$M(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & -1 & 1 & 0 \end{pmatrix} \end{array}$$

Tvrzení:

Množina J řádků matice $M(G)$ je lineárně závislá, právě když existuje $J' \subset J$ s nulovým součtem

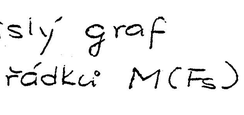
„⇐" když F_S je kostra $\Rightarrow$ (je to) slabě souvislý graf
$\Rightarrow$ prvních $n-1$ řádků $M(F_S)$ je nezávislých
$\Rightarrow h(\underbrace{M_R(F_S)}_{A_S}) = n-1$

Počítání koster

Věta (Cauhy-Binetova)
Nechť B je matice o rozměrech $r \times .$, kde $r \leq$.
Potom platí, že $\det(B \cdot B^T) = \sum_S (\det A_S)^2$, kde S probíhá r-prvkové množiny sloupců a A_S je příslušná podmatice.

Věta
Je-li $M(G)$ incidenční matice orient. grafu G, a je-li C její čtvercová podmatice řádu r ($1 \leq r \leq n$), potom $\det C$ je 0 nebo ± 1.

Důkaz: indukcí přes r



$r=1$ .... jasné
indukční krok: 3 případy:
1) C obsahuje nulový sloupec $\Rightarrow \det = 0$
2) C " sloupec s jedinou hodnotou $\neq 0$;
rozvoj $\det C$ přes ten sloupec
$\det C = \pm \det C'$
podle ind. předp. platí: $\det C = 0, 1, -1$
3) všechny sloupce obsahují 1 i -1
$\Rightarrow$ řádky jsou závislé
$\Rightarrow \det C = 0$

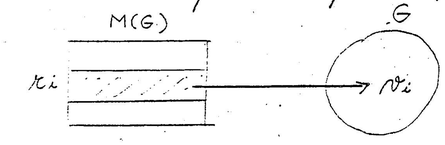
Věta
Nechť G je slabě souvislý orient. graf bez smyček $A = M_R(G)$.
Potom počet koster G je roven $\det(A \cdot A^T)$.

Důkaz:
Podle C.-B. věty je $\det(A \cdot A^T) = \sum_S (\det A_S)^2$
víme, že A_S je regulární $\Leftrightarrow$ F_S je kostra a potom je $\det A_S = \pm 1$
a tedy $\det^2 = +1$

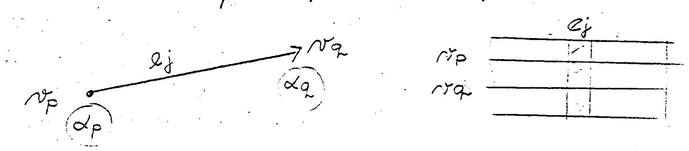
Řádky $M(G)$ ... vektory v $\mathbb{R}^m$
Množina vektorů $w_1, \ldots, w_k$ z vektorového prostoru W je lineárně závislá, pokud ex. lin. kombinace $\sum_{i=1}^{k} \alpha_i w_i = 0$, kde ne všechny α_i jsou 0. (α_i ... prvky tělesa)

Tvrzení:
Nechť K je komponenta slabé souvislosti orient. grafu G, a nechť $\sum \alpha_i r_i = 0$ je lin. kombinace řádků $M(G)$.

Potom pro všechny vrcholy v_i z komponenty K jsou koeficienty α_i shodné.



Důkaz
Pokud na K nejsou všechny koeficienty shodné, potom (ze slabé souvislosti) existuje hrana $e_j \in E(K)$ taková, že její koncové vrcholy v_p, v_q mají různé koeficienty $\alpha_p \neq \alpha_q$.



ve sloupci hrany e_j jsou nenulové položky jen v p-tém a q-tém řádku;
tedy na j-tém místě v lin. kombinaci $\sum \alpha_i v_i = 0$ bude $\alpha_p - \alpha_q \neq 0$, což je SPOR

hodnost matice = max. velikost lineárně nezávislé množiny řádků
Může být $h(M(G)) = m$?
NE: Součet všech řádků je 0 ($= 1 + (-1) +$ samé nuly)

Věta
Pro slabě souvislý orient. graf je $h(M(G)) = m-1$.
Platí dokonce, že každých $m-1$ řádků $M(G)$ je lin. nezávislých

Důkaz: (2. polovina věty)

Nechť G je slabě souvislý a S je množina $n-1$ řádků.

Dejme tomu, že $\sum_{r_i \in S} \alpha_i r_i = 0$.

Rozšířím na všechny řádky, dodefinuji $\alpha_k = 0$ pro (jediný) řádek $r_k \notin S$. Dostanu $\boxed{\sum_{i=1}^{n} \alpha_i r_i = 0}$ *

Podle minulého tvrzení jsou všechny α_i v * SHODNÉ (slabá souvislost). Protože $\alpha_k = 0$, jsou všechny $\alpha_i = 0$.

Věta

Graf G má přesně k komponent slabé souvislosti, právě když $h(M(G)) = n-k$.

Důkaz:

„⇒" komponenty $C_1, \dots, C_k$

1) hodnost $\leq n-k$?

S ... množina $n-k+1$ řádků

tvrdím: S musí obsahovat všechny „vrcholy" některé komponenty C_p

Sečteme všechny řádky r_i pro $v_i \in V(C_p)$. Dostanu 0, protože pro $e \in E(C_p)$ sčítám $+1+(-1)+$ samé nuly (e má oba konce v C_p) a pro $e \notin E(C_p)$ sčítám samé nuly (ani jeden konec v C_p)

⇒ Našel jsem lin. závislost.

2) Najdeme lin. nezávislou množina S o velikosti $n-k$.

z každé komponenty vynecháme právě 1 (vybraný) vrchol.

Kdyby S byla závislá, pak $\sum_{r_i \in S} \alpha_i r_i = 0$.

Pro zbývající řádky dodefinuji $\alpha_k = 0$ a použiji tvrzení, že koeficienty jsou na každé komponentě shodné → všechny nulové.

„⇐" Nechť $h(M(G)) = n-k$. Podle dokázané implikace „⇒" nemůže být komponent jiný počet než k, protože by hodnost vyšla jinak.

víme: poslední řádek $M(G)$ lze spočítat z předchozích

Definice

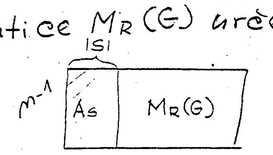
Redukovaná matice incidence $M_R(G) = M(G)$ bez posledního řádku.

Definice

Faktor grafu G je podgraf $H \subset G$, pro který je $V(H) = V(G)$.

Faktory F_S ⟷ množiny hran ⟷ množiny sloupců S matice $M_R(G)$

Faktor určený množinou sloupců S označím F_S, podmatici matice $M_R(G)$ určenou množinou sloupců S označím A_S



Věta

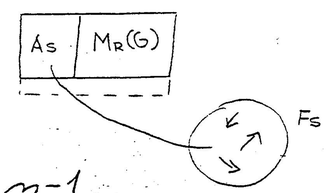
Nechť G je slabě souvislý orient. graf. (bez smyček) Potom čtvercová podmatice A_S řádu $n-1$ matice $M_R(G)$ je **regulární** ⟺ odpovídající faktor F_S je **kostrou** grafu G

Definice

Podgraf H orient. grafu G je jeho kostrou, pokud symetrizace grafu H je kostrou symetrizace grafu G a navíc H neobsahuje smyčky ani protichůdné hrany.

Důkaz věty:

„⇒" Nechť A_S je regulární.



Přímo z definice: $A_S = M_R(F_S)$

z předpokladu: $h(A_S) = n-1$,

proto také $M(F_S)$ má hodnost $n-1$,

takže F_S je souvislý (jistě neobsahuje protichůdné hrany)

Ale souvislý graf s $n-1$ hranami je STROM.

Faktor, který je stromem, musí být kostrou G

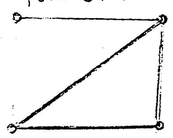
Vektory a faktory

→ podgraf $H \subset G$ tak, že $V(H) = V(G)$

vektor z $\mathbb{Z}_2^m$ ⟷ množina hran grafu G

$E = \{e_1, \dots, e_m\}$ ↕ faktor grafu G

faktor F



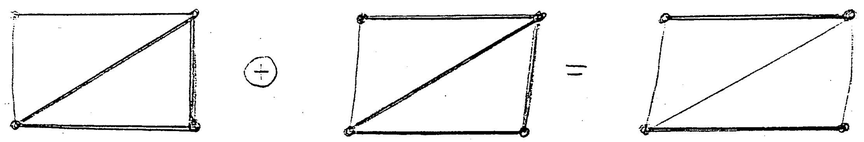
↕ $(11001) \in \mathbb{Z}_2^5$

↕ $\{e_1, e_2, e_5\} \subset E(G)$

Sčítání vektorů v $\mathbb{Z}_2^m$ – co znamená v řeči faktorů?

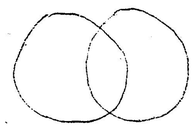
↳ po složkách modulo 2

$(11001) \oplus (01101) = (10100)$



Symetrický rozdíl množin A, B

$A \oplus B = A \cup B \setminus (A \cap B)$



Sudé faktory

Definice

Faktor F grafu G je sudý faktor, pokud každý vrchol má v F sudý stupeň

Kolik má graf G sudých faktorů?

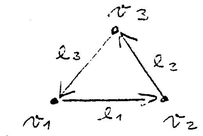
jeden existuje vždy: faktor bez hran

pokud G je strom, pak už další neexistují

Věta

Sudé faktory grafu G tvoří podprostor vektor. prostoru $\mathbb{Z}_2^m$

-př.



G = ... 3 kostry

$\underbrace{M_R(G)}_{A} = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix} \begin{matrix} v_1 \\ v_2 \end{matrix}$

$e_1 \quad e_2 \quad e_3$

$\det(A \cdot A^T) = \det \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} = 3$

Kostry neorientovaného grafu

Věta

Nechť G je neorient. graf s vrcholy $V = \{v_1, \dots, v_n\}$ a $\vec{G}$ je jeho libovolná orientace bez smyček a násobných hran.

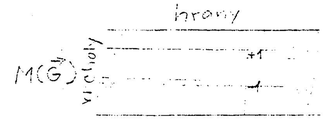
Dále položme $L = M(\vec{G}) \cdot (M(\vec{G}))^T$ ... Laplaceova matice grafu G

Potom pro položky (ℓ_{ij}) matice L platí:

$$\ell_{ij} = \begin{cases} \deg(v_i) & \text{pokud } i = j \\ -1 & \text{pokud } v_i v_j \in E(G) \\ 0 & \text{jinak} \end{cases}$$

Navíc: matici $L' = M_R(\vec{G}) \cdot M_R(\vec{G})^T$ dostanu vypuštěním posledního řádku a sloupce z L

Důkaz



ℓ_{ij} = skalární součin i-tého řádku s j-tým

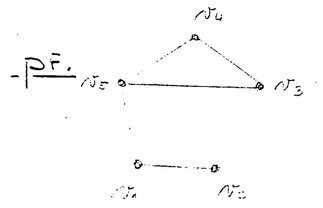
$i = j$ ... stupeň

$i \neq j$ .... 0 pokud mezi v_i a v_j nevede hrana

-1 " " " vede "

„Navíc" je triviální důsledek definice násobení

-př.



$$L = \left(\begin{array}{ccccc} 2 & -1 & 0 & 0 & -1 \\ -1 & 3 & -1 & 0 & 0 \\ 0 & -1 & 3 & -1 & -1 \\ 0 & 0 & -1 & 2 & -1 \\ \hline -1 & 0 & -1 & -1 & 3 \end{array}\right)$$

počet koster $= \det \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 3 & -1 & 0 \\ 0 & -1 & 3 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix} = 11$

-př. Stromy na n vrcholech
počet = počet koster K_n
Laplaceova matice grafu K_n: $L = \begin{pmatrix} n-1 & -1 & \dots \\ -1 & n-1 & \ddots \\ \vdots & \ddots & -1 \\ -1 & & n-1 \end{pmatrix}$ $n \times n$

$L' = \begin{pmatrix} n-1 & -1 & -1 & \dots & -1 \\ -1 & n-1 & & & \\ & & \ddots & & \\ \vdots & & & \ddots & \\ -1 & & & & n-1 \end{pmatrix}$

přičtu k 1. řádku všechny ostatní: $\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ -1 & n-1 & & & \\ & & \text{stejné} & & \end{pmatrix}$

dále 1. řádek přičtu k ostatním:

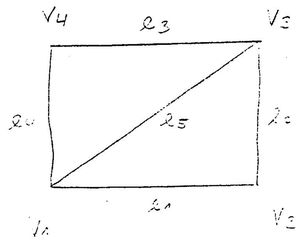
$\left(\begin{array}{c|ccc} 1 & 1 & 1 & \dots & 1 \\ \hline 0 & n & 0 & \dots & 0 \\ & & n & & \\ & & & \ddots & \\ & & & & n \end{array}\right)$ rozvoj podle 1. sloupce

$n-1 > n-1$ $\Rightarrow \det = n^{n-2}$

Matice incidence neorientovaného grafu

Definice
Matice incidence $M(G)$ neorient. grafu G je matice (m_{ij}) o rozměrech $n \times m$, kde $m_{ij} = \begin{cases} 1 & \text{pokud } v_i \in e_j \\ 0 & \text{jinak} \end{cases}$

-př.



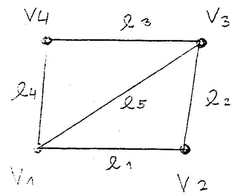
$M(G) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$

všechny řádky jsou lin. závislé! Proč?
S maticí $M(G)$ budeme vždy počítat nad $\mathbb{Z}_2$.
To ovlivňuje i lin. nezávislost (součet řádků matice $M(G)$ je tak 0)

- hodnůst matice M nad $\mathbb{Z}_2$ $h_2(M)$ = max. velikost množiny řádků, která je LN nad $\mathbb{Z}_2$

Neorientované grafy a matice (Lineární prostory grafu)

Incidenční matice neorientovaného grafu



$M(G) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$

řádky $M(G)$... m-tice 0, 1
→ vektory z $\mathbb{Z}_2^m$ — vektor. prostor dimenze m nad tělesem $\mathbb{Z}_2$

$h_2(M(G)) = 3$, přestože $h(M(G)) = 4$

Připomenutí
Množina vektorů $\{w_1, \dots, w_k\} \subset \mathbb{Z}_2^m$ je lin. závislá nad $\mathbb{Z}_2$, pokud existuje lin. kombinace $\sum_{i=1}^{k} \alpha_i w_i = 0$ (ne všechny $\alpha_i = 0$), $\alpha_i \in \mathbb{Z}_2$

Pozorování
Množina je LZ nad $\mathbb{Z}_2$ právě tehdy, když nějaká neprázdná podmnožina má nulový součet.

Hodnost matice M nad $\mathbb{Z}_2$
$h_2(M)$ = neex. velikost lin. nezávislé (nad $\mathbb{Z}_2$) množiny řádků

Věta
Pro neorient. graf G platí:
(i.) Hodnost $h_2(M(G)) = n - k$, kde k je počet komponent
(ii.) Je-li G souvislý, pak dokonce každých $n-1$ řádků $M(G)$ je lin nezávislých nad $\mathbb{Z}_2$.
Nadále předpokládáme, že graf G je souvislý.

Skalár. součin je zobrazení $V \times V \to T$

1) $u \cdot u = 0 \iff u = 0$
2) symetrické $(u \cdot v = v \cdot u)$
3) bilineární $u(v+w) = uv + uw$

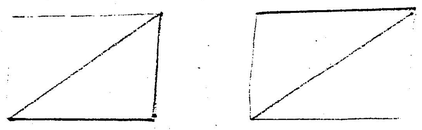
obecně $(\alpha u + \beta v)w = \alpha(uw) + \beta(vw)$

v našem případě může být $u \cdot u = 0$ i když $u \neq 0$

$(1111)(1111) = 0$

Symetrie i bilinearita platí

Skalární součin: co znamená n faktorů G?



$(1100) \cdot (0011) =$

Platí: $u \cdot v = 0 \iff$ příslušné faktory G se shodují v sudém počtu hran

Definice

Je-li W podprostor prostoru Z_2^m, pak jeho ortogonální doplněk $W^\perp$ je tvořen vektory kolmými na každý $w \in W$.

Věta

je-li W podprostor Z_2^m, potom $\dim W - \dim W^\perp = m$.

Důkaz:

označím $\dim W = k$

M := matice $k \times m$

řádky = prvky nějaké báze W

Pozorování

Vektor z je kolmý na každý $w \in W \iff$ je kolmý na každý prvek báze.

Důvod: $z(w_1 + w_2) = zw_1 + zw_2$

Závěr:

$z \in W^\perp \iff M \cdot z = 0$

Důkaz:

1) 0 je sudý faktor, protože všechny stupně = 0
2) součet 2 sudých faktorů je sudý faktor

F_1, F_2 ... sudé faktory

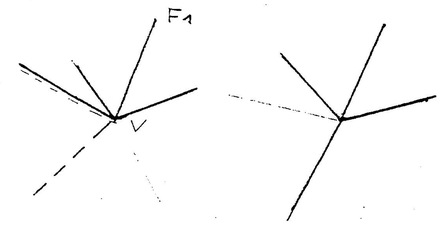
? $F_1 \oplus F_2$?

Nechť $v \in V(G)$ je libovolný

Jaký je stupeň v ve faktoru $F_1 \oplus F_2$?

A_1 := množina hran F_1 obsahující v

A_2 := " F_2 "



Hrany obsahující v ve $F_1 \oplus F_2$ jsou právě $A_1 \oplus A_2$

tvrdím: $|A_1|, |A_2|$ sudé $\Rightarrow |A_1 \oplus A_2|$ sudé

Proč?

$A_1 \oplus A_2 = (A_1 \cup A_2) \setminus (A_1 \cap A_2)$

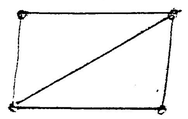
$|A_1 \oplus A_2| = |A_1 \cup A_2| - |A_1 \cap A_2| = |A_1| + |A_2| - 2|A_1 \cap A_2| =$

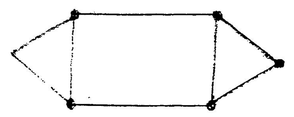
($|A_1|$, $|A_2|$ sudé)

$\Rightarrow |A_1 \oplus A_2|$ ... sudé

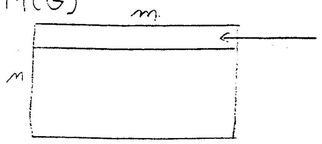
Definice

Podprostor z minulé věty = prostor kružnic grafu G, $C(G)$



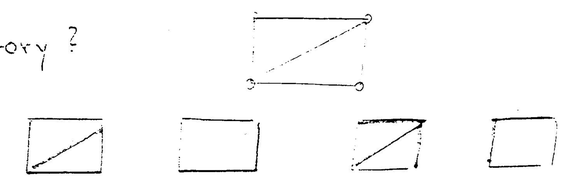


M(G)



řádky M(G) = vektory z Z_2^m

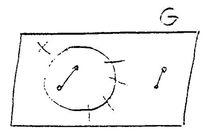
faktory?



Definice

Hvězda vrcholu $v_i \in V(G)$ je faktor složený ze všech hran, obsahujících v_i. Značí se H_i.

Pojem hvězda lze zobecnit → separace
Pro $X \subset V(G)$ definujeme $\partial X \subset E(G)$ jako množina všech hran, které mají v X právě 1 koncový vrchol



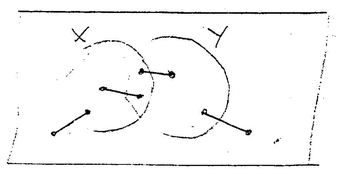
Každý faktor tohoto tvaru označíme separace.

Pozorování:
Separace jsou: - všechny hvězdy ... $H_i = \partial\{v_i\}$
- faktor bez hran ... $\partial\emptyset$

Pozorování:
∂X sestává z hran, které vedou mezi X a $V(G)\setminus X$.

Věta
Množina všech separací je podprostorem $\mathbb{Z}_2^m$.

Důkaz:
1) faktor bez hran je separace ... OK
2) součet ?
chceme dokázat: pro libovolné $X, Y \subset V(G)$ je $\partial X \oplus \partial Y$ opět separací



hrana e patří do $\partial X \oplus \partial Y$ • právě když $e \in \partial X$ a $e \notin \partial Y$ nebo naopak
• a právě když e má v jedné z množin X, Y jeden konec a v druhé 0 nebo oba
• právě když $e \in \partial(X \oplus Y)$

Závěr:
$\partial(X) \oplus \partial(Y) = \partial(X \oplus Y)$, takže $\partial(X) \oplus \partial(Y)$ je separace

Definice
Podprostor tvořený všemi separacemi se nazývá prostor řezů grafu G ... $\mathcal{R}(G)$
všimněme si: S... separace
$\Rightarrow G - S$ (odstraním $S \subset G$) - je nesouvislý.

Definice
Řez v grafu G je množina hran $A \subset E(G)$ s vlastností, že $G-A$ je nesouvislý, ale $\forall A' \subsetneq A : G-A'$ je souvislý.

Tvrzení:
Hvězdy generují celý prostor $\mathcal{R}(G)$
Důkaz:
Nechť ∂X je separace.
Jak vyjádřit ∂X jako součet hvězd?
tvrdím: $\partial X = \sum_{v \in X} H_i$
(hrany, které mají v X 0 nebo 2 konce, nejsou ve výsledku zahrnuty, hrany, které tam mají 1 konec tvoří právě ∂X _)

Víme: $h_2(M(G)) = n-1$
hvězdy = řádky $M(G)$
takže:

Věta
$\dim \mathcal{R}(G) = n-1$
Důkaz:
Hvězdy generují $\mathcal{R}(G)$, vyberu z nich bázi a ta musí mít $n-1$ prvků

Definice
Pro vektory $u = (u_1, \dots, u_m)$
$v = (v_1, \dots, v_m) \in \mathbb{Z}_2^m$ je skalární součin
$u \cdot v$ definován jako $u \cdot v = \sum_{i=1}^{m} u_i \cdot v_i$
(sčítání nad $\mathbb{Z}_2$)
Vektory u, v jsou ortogonální (kolmé) pokud $u \cdot v = 0$ $u \perp v$
Pro $U, V \subset \mathbb{Z}_2^m$ je $U \perp V$ (U ortog. V), pokud $\forall u \in U, \forall v \in V : u \perp v$
Podobně $u \perp V$ (u ... vektor, V ... množina)

Pozn.
Obecná definice skalárního součinu ve vektor. prostorech (prostor V nad T).

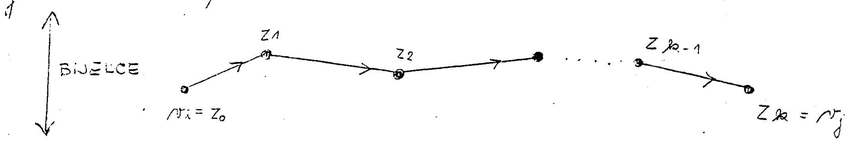
Důkaz: (indukcí přes k)

1) $k=0$ ... $(S(G))^0 = E_m$, takže $\sigma_{ij}^{(0)} = \begin{cases} 1 & \text{pokud } i=j \\ 0 & \text{" } i \neq j \end{cases}$

to je přesně počet sledů délky 0 z v_i do v_j

2) Nechť je dokázáno pro všechna $k' < k$

$v_i v_j$ - sled délky k:



$v_i x$ - sled délky $k-1$, kde $x v_j \in E(G)$

počet $v_i v_j$ - sledů délky k =

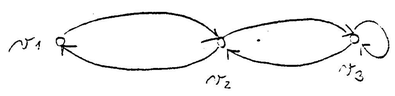
$$= \sum_{\substack{x \in V(G) \\ x v_j \in E(G)}} (\text{počet } v_i x\text{- sledů délky } k-1) =$$

$$\overset{\text{IND.}}{=} \sum_{\substack{v_x \in V(G) \\ v_2 v_j \in E(G)}} \sigma_i^{(k-1)} = \sum_{l=1}^{m} \sigma_{il}^{(k-1)} \cdot \sigma_{lj}$$

$\sigma_{il}^{(k-1)}$: položka matice $(S(G))^{k-1}$; σ_{lj}: položka matice $S(G)$

$$\overset{\text{DEF. NÁSOBENÍ}}{=} \sigma_{ij}^{(k)}$$

př.

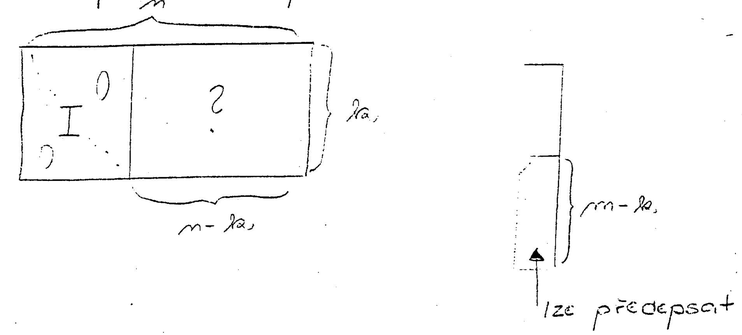


sled délky 3

$$S(G) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad (S(G))^3 = \begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 3 \end{pmatrix}$$

- jeden sled z v_3 do v_1 délky 3 : $(v_3\ v_3\ v_2\ v_1)$
- 3 sledy z v_2 do v_3 " : $(v_2\ v_1\ v_2\ v_3)$
  $(v_2\ v_3\ v_2\ v_3)$
  $(v_2\ v_3\ v_3\ v_3)$

Standartními úpravami upravím M na tvar



Všimnu si:

pro libovolně zvolené $x_{k+1}, \dots, x_m$ lze doplnit na vektor $x = (x_1, \dots, x_m)$ jednoznačně tak, že $M^T x = 0$

$\Rightarrow$ dim prostoru řešení je $m-k$

$\Rightarrow \dim W + \dim W^\perp = m$

Víme:

F_1, F_2 jsou faktory

$F_1 \perp F_2 \iff |F_1 \cap F_2|$ je sudý

F je sudý faktor $\iff$ je kolmý na každou hvězdu.

Hvězdy generují prostor $\mathcal{R}(G)$. Proto F je sudý faktor $\iff$ je kolmý na každý prvek $\mathcal{R}(G)$.

Věta

$$\mathcal{C}(G) = (\mathcal{R}(G))^\perp$$

Věta

$\dim \mathcal{C}(G) = m - n + 1$

Důkaz

$\dim \mathcal{C}(G) = m - \dim \mathcal{R}(G) = m - n + 1$

Důsledek:

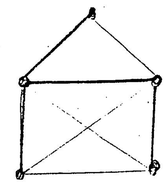
Graf G má: 2^{m-n+1} sudých faktorů

Jak najít nějakou bázi $\mathcal{C}(G)$?

Zvolme kostru grafu G

Fundamentální soustava kružnic

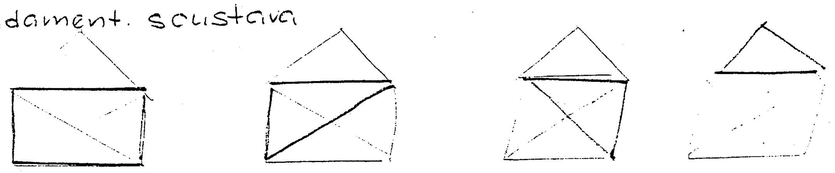
vzhledem ke kostře T



T je strom na m-vrcholech $\Rightarrow n-1$ hran

Hrany mimo T ... tětivy kostry T ... $m-n+1$

pro tětivu e_j graf $T+e_j$ obsahuje právě jednu kružnici C_j
Pokud e_j probíhá $m-n+1$ tětiv, dostaneme $m-n+1$ kružnic C_j
... fundament. soustava



Tvrzení:

Fund. soustava kružnic vzhledem k T je lin. nezávislé množina.

Důkaz

Tětiva e_j je obsažena jen v jedné kružnici soustavy, totiž C_j
$\Rightarrow$ žádné C_j nemůže být součtem ostatních prvků.

Důsledek

Fund. soustava kružnic je báze $\mathcal{C}(G)$

Obdobně: Fundament. soustava řezů
báze prostoru $\mathcal{R}(G)$

Kostra T má $n-1$ hran
Pro každou hranu $e_j \in E(T)$ je $T-e_j$ má 2 komponenty.
Definuji faktor R_j složený ze všech hran G
$\longrightarrow$ $n-1$ různých faktorů R_j
jsou to řezy, jsou LN $\Rightarrow$ tvoří bázi $\mathcal{R}(G)$

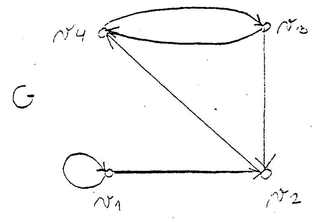
Pozn.

G je nesouvislý, k komponent
$\dim \mathcal{C}(G) = m-n+k$
$\dim \mathcal{R}(G) = n-k$

Cesty v grafu

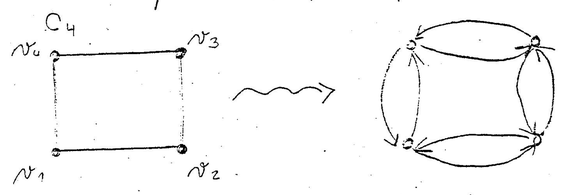
Definice

Nechť G je orientovaný graf na vrcholech $v_1, \dots, v_n$.
Matice sousednosti grafu G je reálná $n \times n$ matice definovaná
$S(G) = (G_{ij})$, kde $G_{ij} = \begin{cases} 1 & \text{pokud } v_i v_j \in E(G) \\ 0 & \text{jinak} \end{cases}$



$$S(G) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

G neorientovaný ... vezmu symetrickou orientaci

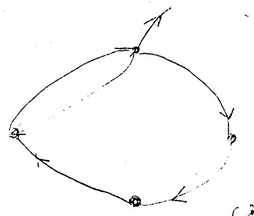


$$S(G_4) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Cvičení

Nechť $L(G)$ je Laplaceova matice neorientovaného grafu G.
Určete součet $L(G)+S(G)$.

Sled:

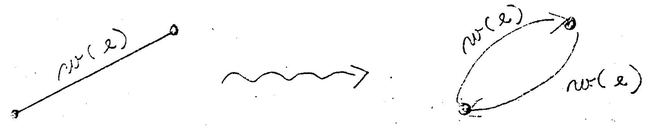


x-y sled = sled z x do y $(x, y \in V(G))$
Úmluva: $(S(G))^0 = E_n$ ... identická matice

označení: $G_{ij}^{(k)}$ - prvek na pozici (i,j) v matici $(S(G))^k$

Věta

Nechť G je orientovaný graf a $k \geq 0$. Prvek $G_{ij}^{(k)}$ je roven počtu sledů z v_i do v_j o délce přesně k



Definice

Vážené matice sousednosti ohodnoceného orient. grafu (G, w) je matice $W(G) = (w_{ij})$, kde $w_{ij} = \begin{cases} w(v_i v_j) & \text{pokud } v_i v_j \in E(G) \\ 0 & \text{jinak} \end{cases}$

pro $i, j = 1, \dots, n$

Pozn.

Nezáporné čtvercové matice jednoznačně odpovídají ohodnoceným orient. grafům

Definice

Váha $w(P)$ cesty P v ohodnoceném grafu G je součet vah jejích hran.
Pro $u, v \in V(G)$ minimální cesta z u do v je cesta nejmenší možné váhy.
Vážená vzdálenost $d^w(u, v)$ vrcholů u, v je váha minimální cesty z u do v (případně ∞)

Pozn.

Minimální cesta nemusí být nejkratší!

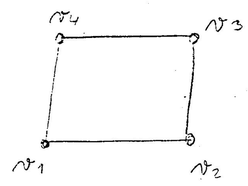
Dijkstrův algoritmus

na hledání minimální cesty

vstup: ohodnocený orient. graf (G, w) vrchol $v \in V(G)$
výstup: pro každý vrchol $x \in V(G)$
1) vážená vzdálenost $d^w(v, x)$
2) minimální cesta P_x z v do x

-př. C_4 ... neorient. kružnice délky 4

$$(S(C_4))^4 = \begin{pmatrix} 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 4 \\ 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 4 \end{pmatrix}$$



mezi sousedními vrcholy:
neex. žádný sled délky 4
jinak ex. právě 4 sledy z v_1 do v_2:
$v_1 v_2 v_1 v_2 v_1$
$v_1 v_4 v_1 v_1 v_1$
$v_1 v_2 v_3 v_4 v_1$
$v_1 v_4 v_3 v_2 v_1$

Vzdálenost

Definice

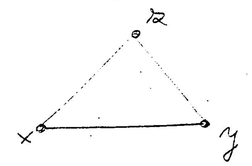
Vzdálenost $d(x, y)$ vrcholů x, y orient. grafu G je délka nejkratší cesty z x do y. Pokud taková cesta neexistuje, položíme $d(x, y) = \infty$.

Pozn.

Pro neorient. grafy: přes symetrickou orientaci.

Cvičení

Vzdálenost v grafu splňuje axiomy metriky: Ověřte!
Metrika na množině X je funkce $d: X^2 \to X$ taková, že:
(1) $d(x, y) \geq 0$, přičemž $d(x, y) = 0 \iff x = y$
(2) $d(x, y) = d(y, x)$
(3) $d(x, y) + d(y, z) \geq d(x, z)$ ... trojúhelníková nerovnost

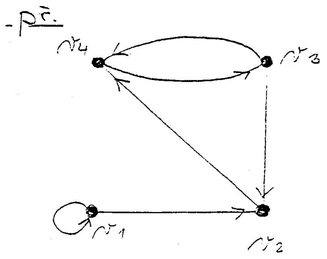


Definice

Distanční matice orient. grafu G s vrcholy $[v_1, \dots, v_n]$ je matice

$$D(G) = (d(v_i, v_j))_{i,j=1}$$

př.



$$D(G) = \begin{pmatrix} 0 & 1 & 3 & 2 \\ \infty & 0 & 2 & 1 \\ \infty & 1 & 0 & 1 \\ \infty & 2 & 1 & 0 \end{pmatrix}$$

Tvrzení:
Prvek $d(v_i, v_j)$ distanční matice $D(G)$ je roven nejmenšímu k, pro které $G_{ij}^{(k)} \neq 0$
(pokud takové k existuje, pak $d(v_i, v_j) = \infty$)

Důkaz:
Nechť M je množina všech k, pro které $G_{ij}^{(k)} \neq 0$.
Víme: Ex. cesta z v_i do v_j $\Leftrightarrow$ ex. sled z v_i do v_j
Obráceně: $d(v_i, v_j) = \infty \Leftrightarrow M = \emptyset$.
To dokazuje druhou polovinu věty.

Nechť nejkratší sled z v_i do v_j má délku k_0.
Potom 1) $k_0 = \min M$
2) ten sled je cestou (kdyby)

$$D(G) = \begin{pmatrix} 0 & 1 & 3 & 2 \\ \infty & 0 & 2 & 1 \\ \infty & 1 & 0 & 1 \\ \infty & 2 & 1 & 0 \end{pmatrix}$$

Proč stačí mocniny $S(G)$ jenom do $n-1$?
Pokud neexistuje sled délky $\leq n-1$ z x do y, pak neexistuje žádný.

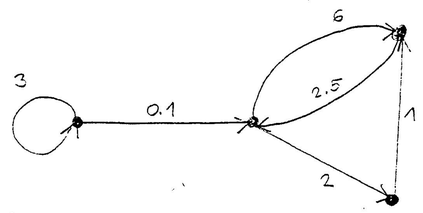
Cvičení:
Jak se z $D(G)$ pozná, zda je G silně souvislý?

Tvrzení:
Orient. graf G je acyklický právě když nějaká mocnina $S(G)$ je nulová

Důkaz:
$\Rightarrow$" G je acyklický $\Rightarrow$ každý sled v G je cestou.
víme: délka každé cesty je $\leq n-1$
tedy: v G neex. sled délky n, takže $(S(G))^n = 0$

$\Leftarrow$" Nechť $(S(G))^{k_2} = 0$. Tj. neex. sled délky k_2.
Kdyby G obsahoval cyklus C, pak by obsahoval sled každé délky (stačí obcházet C kolem dokola) $\Rightarrow G$ je acyklický

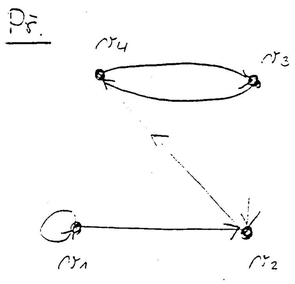
Ohodnocené grafy



Definice
Ohodnocený orient. graf (G, w) je orient. graf G spolu s funkcí $w: E(G) \to (0, \infty)$
$e \in E(G)$.... $w(e)$ je ohodnocení nebo váha hrany e

Pozn.
Neorient. graf: „stejná" definice. Při přechodu k sym. orientaci:

př.



$$(S(G))^0 = \begin{pmatrix} \underline{1} & 0 & 0 & 0 \\ 0 & \underline{1} & 0 & 0 \\ 0 & 0 & \underline{1} & 0 \\ 0 & 0 & 0 & \underline{1} \end{pmatrix} \quad (S(G))^2 = \begin{pmatrix} 1 & 1 & 0 & \underline{1} \\ 0 & 0 & \underline{1} & 0 \\ 0 & 0 & 1 & 1 \\ 0 & \underline{1} & 0 & 1 \end{pmatrix}$$

$$(S(G))^1 = \begin{pmatrix} 1 & \underline{1} & 0 & 0 \\ 0 & 0 & 0 & \underline{1} \\ 0 & \underline{1} & 0 & \underline{1} \\ 0 & 0 & \underline{1} & 0 \end{pmatrix} \quad (S(G))^3 = \begin{pmatrix} 1 & 1 & \underline{1} & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$