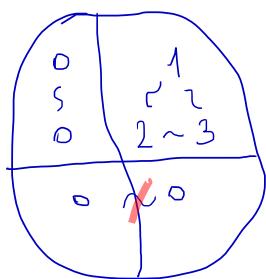


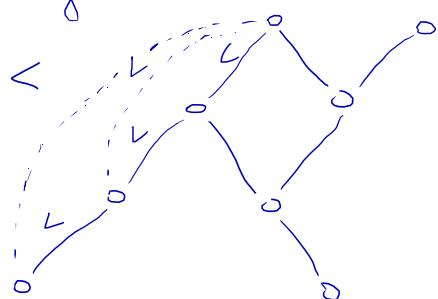
Equivalence

Rozklad množiny M / faktor množine podle ~
podle relace ~

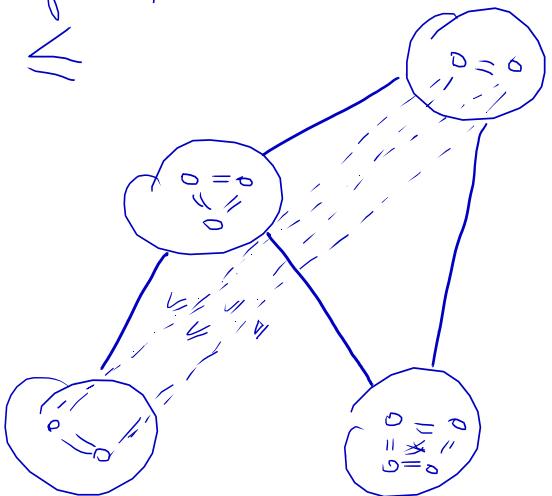
$$[1]_ \sim = \{1, 2, 3\}$$



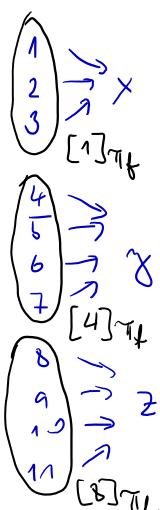
Částečné uspořádání (partial order poset)
Hasse diagram



Hasseův diagram (preorder)
reflex., transit.



jednu zobrazení $f : \sim_f$



$$f = g \circ \nu$$

$$\begin{matrix} 1 \\ 2 \\ 3 \end{matrix} \xrightarrow{\quad} [1]_ \sim_f \xrightarrow{g} X$$

$$\begin{matrix} 4 \\ 5 \\ 6 \\ 7 \end{matrix} \xrightarrow{\quad} [4]_ \sim_f \xrightarrow{g} Y$$

$$\begin{matrix} 8 \\ 9 \\ 10 \\ 11 \end{matrix} \xrightarrow{\quad} [8]_ \sim_f \xrightarrow{g} Z$$

Konické zobrazení

Homomorfismus \equiv , $A = (A, *)$

$$\forall a, b, a', b' \in A : a \equiv a' \wedge b \equiv b' \Rightarrow a * b \equiv a' * b'$$

homomorfismus $h : A \rightarrow B$, $B = (B, +)$

$$\forall a, b \in A \quad h(a * b) = h(a) + h(b)$$

$$(\mathbb{Z}, +, *) \quad n \in \mathbb{Z} \quad (\langle 0, n-1 \rangle, +_n, *_n)$$

Bijection / bijektiv
modulnem n

$$a +_n b = (a+b) \% n$$

$$a *_n b = (a * b) \% n$$

$$h: \mathbb{Z} \rightarrow \langle 0, n-1 \rangle$$

$$a \mapsto a \% n$$

Ist h homom.?

$$1) \quad h(a+b) \stackrel{?}{=} h(a) +_n h(b) \quad \checkmark$$

$$2) \quad h(a * b) \stackrel{?}{=} h(a) *_n h(b) \quad \checkmark$$

Wir zeigen, dass $\forall a, b$

$$\begin{aligned} a &= x_n + a \% n \\ b &= y_n + b \% n \end{aligned}$$

$$\left| \begin{aligned} h(a+b) &= (a+b) \% n = (x_n + a \% n + y_n + b \% n) \% n = \\ &= (a \% n + b \% n) \% n = h(a) +_n h(b) \\ h(a * b) &= (a * b) \% n = ((x_n + a \% n) * (y_n + b \% n)) \% n = \\ &= (x_n y_n + x_n (b \% n) + (a \% n) y_n + (a \% n)(b \% n)) \% n = \\ &= (a \% n * b \% n) \% n = h(a) *_n h(b) \end{aligned} \right.$$

\equiv_n -jedro homom. h (ist also steigende Bijection modulnem n)

$x \mapsto [x]_{\equiv_n}$... prius. homomorphismus

$\{[0]_{\equiv_n}, [1]_{\equiv_n}, \dots, [n-1]_{\equiv_n}\}$ aufgebaut \mathbb{Z} podle \equiv_n

$$\begin{array}{ccc} \equiv_n \text{ je Kongruenz} & a \stackrel{\equiv_n}{=} a' & \Rightarrow \begin{array}{l} a + b \stackrel{\equiv_n}{=} a' + b' \\ a * b \stackrel{\equiv_n}{=} a' * b' \end{array} \end{array}$$

faktor algebra podle \equiv_n

$$[a]_{\equiv_n} + [b]_{\equiv_n} = [a+b]_{\equiv_n}$$

$$[a]_{\equiv_n} * [b]_{\equiv_n} = [a * b]_{\equiv_n}$$

(je einde' priels ne libovolnych reprezentantech b'ud)

Co znamená 'round', vize níže deskující míst?

$$\text{round}(a+b) \stackrel{?}{=} \text{round}(a) + \text{round}(b)$$

0,4

0,4

0,4

1

+

0

0

round

nem' homom.

podobně

$$\text{round}(1,4 * 1,4) \neq \text{round}(1,4) * \text{round}(1,4)$$

$$\text{floor}(1,5 * 1,5) = \text{floor}(1,5) * \text{floor}(1,5)$$

2,25

1

1

floor

nem' homom

} důsledek:

Chybou se akumuluje

Lecht

$(R, \cdot, +, *)$ je algebraická struktura

$(A, \cdot_A, +_A, *_A)$ algebraická struktura s aritmetickými operacemi implementovanými $\cdot, +, *$ (viz. Operační TIN)

$(L, \cdot_L, +_L, *_L)$ algebraická struktura s jazykovými operacemi

Necht $h: R \rightarrow A$ je pravodležná homomorfizma aritmetiky.

h je homomorfismus

$$h(r \cdot r') = h(r) \cdot_A h(r')$$

$$h(r+r') = h(r) +_A h(r')$$

$$h(r^*) = h(r)^*_A$$

Relace $\equiv \subseteq R \times R \rightarrow A$.

$r \equiv r' \Leftrightarrow L(r) = L(r')$ je kongruence: $L(\cdot)$ je jazyk reprezentace r

$$r \equiv r' \wedge s \equiv s' \Rightarrow L(r \cdot s) = L(r' \cdot s') \Rightarrow r \cdot s \equiv r' \cdot s'$$

a podobně pro $+ \wedge ^*$

Je \equiv jazykem h ? T.j. platí, že reg. n. jsou převedeny na stejný aritmetické provedení reprezentující stejný jazyk?

1) Necht $h(t) = h(t')$. Potom platí $L(t) = L(t')$, t.j. $t \equiv t'$. ✓

2) Necht $t \equiv t'$. Platí, že $h(t) = h(t')$? x

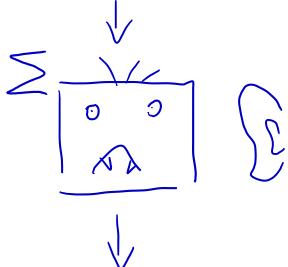
Ne! Protipříklad: $t = e + a \cdot a^*, t' = a^*$. Tj. $t \equiv t'$ jazykem h .

Homomorphic encryption

Chci počítat, ale nechci, aby procesor mal možnost data, nárobení v matice

Chci Π data

encapsulation $\downarrow h$
 $h(\text{data})$



$\Sigma(h(\text{data}))$

decapsulation $\downarrow h^{-1}$
 $h^{-1}(\Sigma(h(\text{data}))) = \Pi \text{ data}$

$$h(a) = \log_P(a), h^{-1}(a) = P^a$$

kde P je reálnou

h je homomorfické do $(\mathbb{R}, +)$:

$$h(a+b) = \log_P(a+b) = \log_P(a) + \log_P(b) = h(a) + h(b) \quad \checkmark$$

$$h^{-1}(h(a) + h(b)) = P^{\log_P(a) + \log_P(b)} = a+b, \text{ t.j., funguje do}$$

$$g(a) = P^a, g^{-1}(a) = \log_P(a)$$

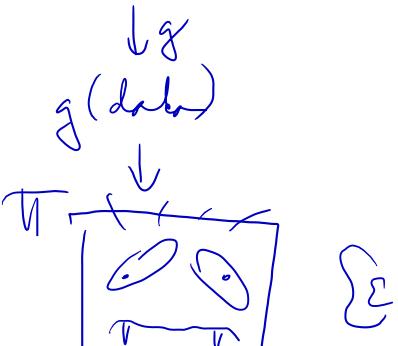
g je homomorfické do $(\mathbb{R}, *)$:

$$g(a+b) = P^{(a+b)} = P^a * P^b = g(a) * g(b) \quad \checkmark$$

$$g^{-1}(g(a) * g(b)) = \log_P(P^{a+b}) = a+b \dots$$

funguje do

Chci Σ data



$\Sigma(g(\text{data}))$

$\downarrow \bar{g}$

$\bar{g}^{-1}(\Sigma(g(\text{data}))) = \Pi \text{ data}$

Chci Π data

$\downarrow f$
 \vdots



podobně

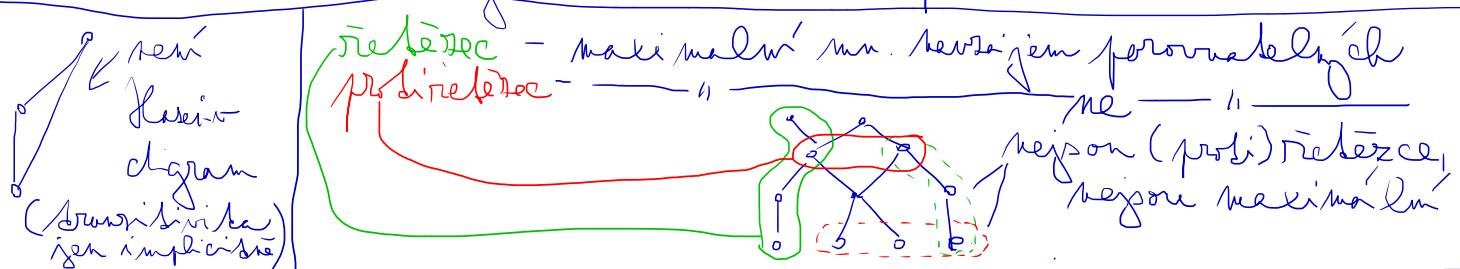
lze zjistit, že násobení
permutovalo

decr. je
násoben jeji
inverzí

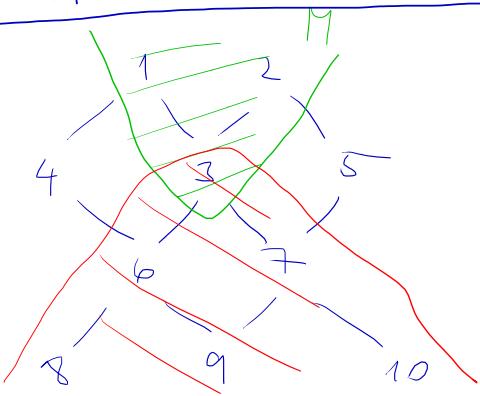
Gloss

foming

číslové uspořadávání, minum, maximum,
největší/největší prvek, dolní/borní hranice, supremum, infimum,
Hasseho diagram, svař, řetězec, prostředník



$$\begin{aligned} 3 \wedge 5 &= 7 \\ 6 \vee 5 &= 2 \\ 6 \wedge 5 &= 9 \end{aligned}$$



Není svaz prvek ve všechny
prvek / lze všechny podmínky
nej. sup. a inf.,
např. $8 \wedge 9$ neexistuje

$a < b \Leftrightarrow$ cesta z a nahoru do b
např. $10 < 1$

$$M = \{1, 2, 3\}$$

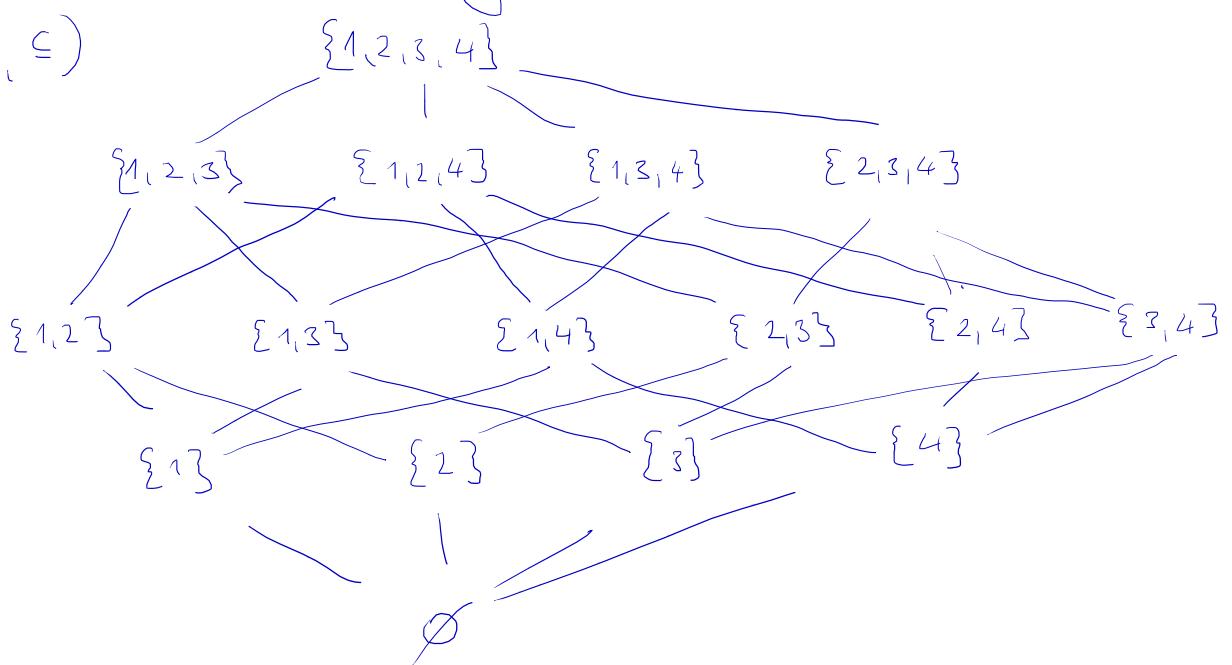
- nemá největší prvek
- maxima jsou 1 a 2
- nejmenší prvek = jediné minimum = 3
- dolní hranice M je $\{3, 6, 7, 8, 9, 10\}$
- infimum je 3
- $\{1, 2\}$ má největší dolní hranice
a infimum 3

Uplný svaz: všechny podmínky (i nekonečné)
mají sup. a inf.

- konečný svaz je vždy uplný
- (\mathbb{N}, \leq) je svaz, nemá vždy prvek \mathbb{N} nemá sup.
- $(\mathbb{N} \cup \{\infty\}, \leq)$ je uplný svaz, sup $(\mathbb{N}) = \infty$
- (\mathbb{R}, \leq) svaz, ne vždy (nemá sup (\mathbb{R})),
- $(\mathbb{R} \cup \{-\infty, \infty\}, \leq)$ uplný svaz
- $(\mathbb{Q} \cup \{-\infty, \infty\}, \leq)$ nemá uplný svaz, např. $(-\infty, \sqrt{2})$ nemá supremum, protože $\sqrt{2} \notin \mathbb{Q}$.

Graf podmnožin částečného pořadí

$(2^{\{1,2,3,4\}}, \subseteq)$



$$\sup(\{\{1\}, \{2\}\}) = \{1\} \cup \{2\} = \{1, 2\}$$

$$\inf(\{\emptyset\}) = \emptyset$$

$$\inf(\emptyset) = \{1, 2, 3, 4\} \quad | \quad \sup(\emptyset) = \emptyset$$

Násoby je možno nahradit částečnou řízenou:

$$\begin{array}{c} \text{násy. množiny} \\ \times \\ (2^{\{1,2,3,4\}}, \subseteq) \end{array} \quad \times \quad \begin{array}{c} \text{algebra} \\ \times \\ (2^{\{1,2,3,4\}}, \cap, \cup) \end{array}$$

$$\sup(\{a, b\}) = a \cup b$$

$$\inf(\{a, b\}) = a \cap b$$

Definice 1 Svaz (V, \leq) je úplný pokud pro každou $U \subseteq V$, $\inf(U) \in V$ a $\sup(U) \in V$.

Definice 2 Mějme dva svazy (V, \leq) a (V', \leq') a funkci $f : V \rightarrow V'$.

1. f je monotónní pokud $\forall u, v \in V : u \leq v \implies f(u) \leq' f(v)$.

2. f je spojitá pokud je monotónní a pro každý (i nekonečný) řetěz C platí

$$f(\sup(C)) = \sup\{f(c) \mid c \in C\} .$$

Věta 1 (Knaster-Tarski) Mějme úplný svaz (V, \leq) a monotónní funkci $f : V \rightarrow V$. Potom množina pevných bodů f je také úplným svazem.

Zejména existuje nejmenší pevný bod μf a největší pevný bod νf .

Věta 2 (Kleene) Nechť je (V, \leq) úplný svaz a $f : V \rightarrow V$ spojitá funkce. Potom

$$\mu f = \sup\{f^i(\perp) \mid i \leq 0\} .$$

μf může být vypočítán jako supremum neklesajícího řetězce

$$\perp \leq f(\perp) \leq f(f(\perp)) \leq f^3(\perp) \leq \dots$$

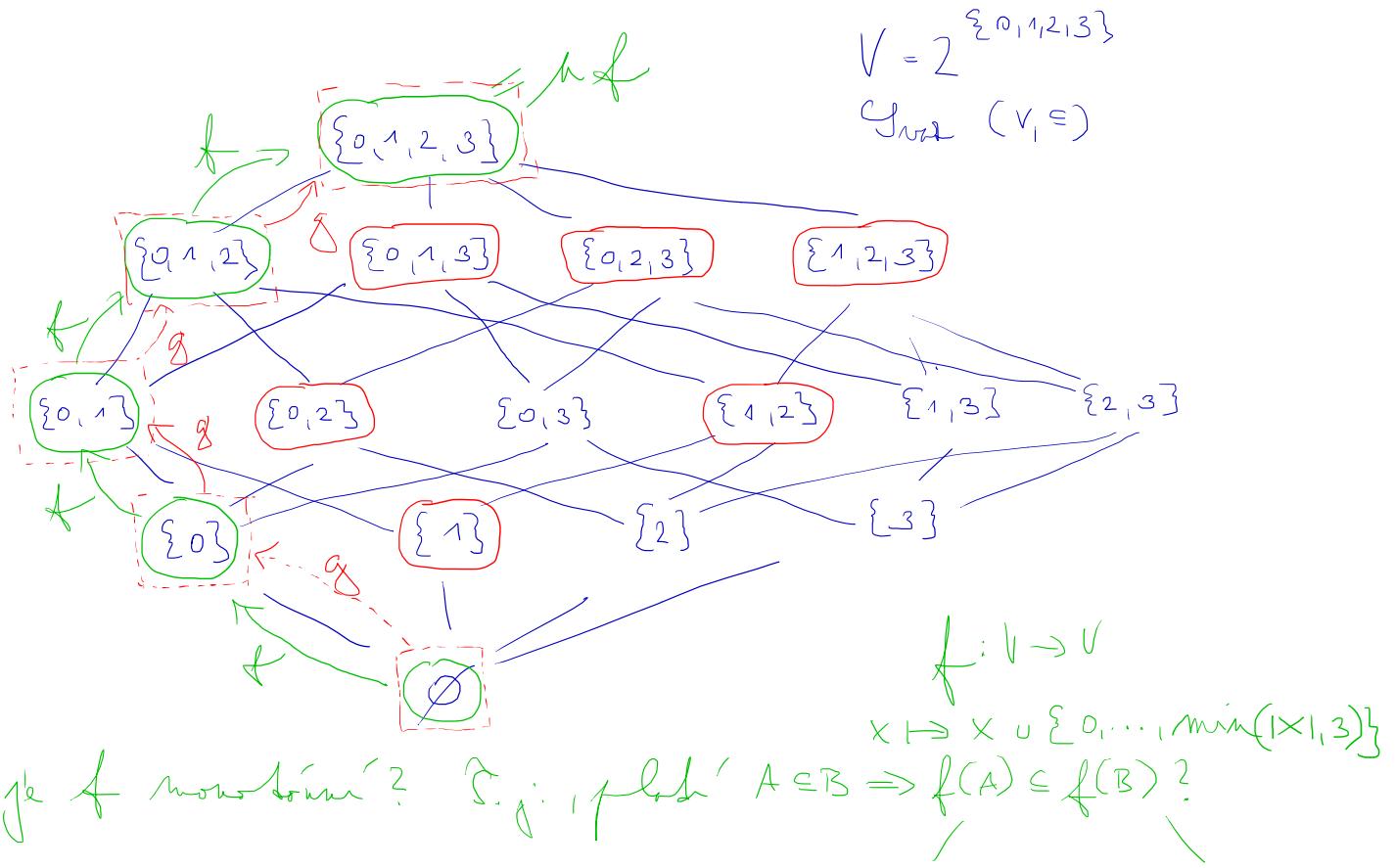
Podobně nejmenší fixpoint větší než nějaký prvek x může být vypočítán jako supremum řetězce

$$x \leq f(x) \leq f(f(x)) \leq f^3(x) \leq \dots$$

Duálně pro νf .

Věta 3 (slabší Knaster-Tarski) Nechť (V, \leq) je částečně uspořádaná množina s nejmenším prvkem \perp , kde každý nekonečný řetěz má supremum, a nechť je $f : V \rightarrow V$ spojitá funkce. Pak $\mu f = \sup^{i \geq 0} f^i(\perp)$ je nejmenším pevným bodem f .

Perne' body, monotón funkce



je f monotoní? T. j., plášť $A \subseteq B \Rightarrow f(A) \subseteq f(B)$?

Ano

$$A \cup \{0, \dots, \min(|A|, 3)\} \subseteq B \cup \{0, \dots, \min(|B|, 3)\}$$

Sedly podle Kuratowski, plášť

perne' body je kovarijný mas,

a podle Kleene můžeme počítat nejmenší perne' body pro f jako supremum $\varnothing, f(\varnothing), f^2(\varnothing), \dots$

Tyto jsou $f = \{0, 1, 2, 3\}$, což je opravdu nejm. pern. b.

Nechť $g: V \rightarrow V$, $x \mapsto x \cup \{\min(1|x|, 3)\}$

g nemá monotóní: nechť $A = \varnothing$, $B = \{1\}$

Máme $A \subseteq B$, ale $g(A) \neq g(B)$.

$$\begin{array}{c} \{0\} \\ \{1\} \end{array}$$

Udělejme si tenco do $\{1, 2, 3, 4\}$, takže g je ale $\{1\}$.

Tripointy kovarijný mas: $\{0, 2\} \cap \{1, 2\}$ nemá fixní

Jde o číslo k počtu nájídech na vlastní hodnoty

formulace algoritmu:

* Oprek TIN podle 4.2.1 nájdech dvojí hodnota

$$f(M) = \{S\} \cup \{X \mid A \rightarrow X \in P \wedge A \in M\}$$

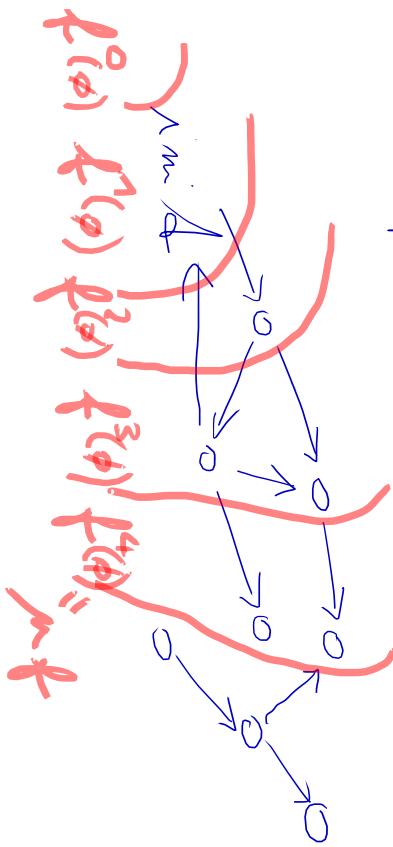
dvojí hodnota $V = f^{\circ n} f$

Poklíněk řeší fiktivně nájdech nájdech podle 4.1, 4.4., 10. a mnoho dalších.

* Jde o kódovanou číslice na grafu a mítla nájdech?

$$f(X) = \left\{ \min_{i=1}^n \sum_{j=1}^m f_{ij} x_{ij} \mid X \in \{0,1\}^{(m,n)} \right\}$$

$f^{\circ n} f$



$$\begin{aligned} f^0(\phi) &= \phi \\ f^1(\phi) &= S \\ f^2(\phi) &= f(\{S\}) = \text{symbol na první straně} \\ f^3(\phi) &= \dots \\ f^5(\phi) &= \dots \end{aligned}$$

$f^2(\phi) = \text{symbol na druhé straně}$
S pravidlem