DMA Přednáška – Speciální relace

Definice.
Nechť $\mathcal{R}$ je relace na nějaké množině A. Řekneme, že $\mathcal{R}$ je **částečné uspořádání**, jestliže je reflexivní, antisymetrická a tranzitivní.
V tom případě značíme relaci $\preceq$ a řekneme, že dvojice $(A, \preceq)$ je **částečně uspořádaná množina**.

Fakt.
Jestliže je $(A, \preceq)$ částečně uspořádaná množina, pak je i $(A, \preceq^{-1})$ částečně uspořádaná množina.

Definice.
Nechť $(A, \preceq)$ je částečné uspořádání. Definujeme relaci $\prec$ na A předpisem
$a \prec b$ právě tehdy, když $a \preceq b$ a $a \neq b$.

Algoritmus pro vytváření Hasseova diagramu částečného uspořádání $(A, \preceq)$ pro konečnou množinu A.
1. Najít prvky $a \in A$, které v ostrém srovnání nikdy nejsou napravo, tedy v pozici $x \prec a$ (nevedou do nich šipky). Dát do spodní řady. Odebrat tyto prvky z A, odebrat všechna srovnání s těmito body.
2. Ve zbylé množině hledat prvky, které v ostrém srovnání nikdy nejsou napravo (nevedou do nich šipky). Dát do druhé řady zdola, odebrat je z množiny prvků.
Spojit horní řadu s dolní tam, kde je relace, odebrat tyto dvojice ze seznamu srovnání.
3. Ve zbylé množině hledat prvky, které ve srovnání $\prec$ nikdy nejsou napravo (nevedou do nich šipky). Vytvořit z nich novou řadu nahoře, odebrat z množiny prvků.
Spojit horní řadu s nižšími tam, kde je relace, přičemž postupujeme shora dolů (nejprve spojujeme horní řadu s tou pod ní, pak horní s tou o jedno níže, atd. až po horní s dolní). Existující dvojice vyškrtáváme ze seznamu, ale do grafu je kreslíme jen tehdy, pokud ještě tuto cestu nelze absolvovat pomocí již nakreslených spojnit, a to vždy směrem zdola nahoru.
4. Opakovat krok 3., dokud jsou v množině body.

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina a $\prec$ odpovídající odvozená relace. Nechť M je neprázdná podmnožina A.
Řekneme, že prvek $m \in A$ je **nejmenší prvek** množiny M, jestliže $m \in M$ a pro všechna $x \in M$ platí $m \preceq x$.
Řekneme, že prvek $m \in A$ je **největší prvek** množiny M, jestliže $m \in M$ a pro všechna $x \in M$ platí $x \preceq m$.
Řekneme, že prvek $m \in A$ je **minimální prvek** množiny M, jestliže $m \in M$ a neexistuje $x \in M$: $x \prec m$.
Značíme to $m = \min(M)$.
Řekneme, že prvek $m \in A$ je **maximální prvek** množiny M, jestliže $m \in M$ a neexistuje $x \in M$: $m \prec x$.
Značíme to $m = \max(M)$.

Věta.
Nechť je $(A, \preceq)$ částečně uspořádaná množina, uvažujme neprázdnou podmnožinu $M \subseteq A$. Pak platí následující:
(i) Jestliže existuje nejmenší prvek M, pak je jediný.
Jestliže existuje největší prvek M, pak je jediný.
(ii) Jestliže je m nejmenší prvek M, pak $m = \min(M)$ a jiné minimum už není.
Jestliže je m největší prvek M, pak $m = \max(M)$ a jiné maximum už není.

Věta.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Jestliže je M konečná neprázdná podmnožina A, pak existuje $\min(M)$ a $\max(M)$.

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Řekneme, že $a, b \in A$ jsou **porovnatelné**, jestliže $a \preceq b$ nebo $b \preceq a$.

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Řekneme, že $\preceq$ je **lineární uspořádání**, jestliže jsou každé dva prvky z A porovnatelné.

Věta.
Nechť $(A, \preceq)$ je lineárně uspořádaná množina. Jestliže je M její neprázdná konečná podmnožina, pak má nejmenší a největší prvek.

Věta.
Nechť $(A, \preceq)$ je konečná částečně uspořádaná množina. Je to lineární uspořádání právě tehdy, jestliže lze prvky A napsat jako $A = \{a_1, \ldots, a_n\}$ tak, aby $a_1 \prec a_2 \prec \cdots \prec a_n$.

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Relace $\preceq_L$ na A se nazývá **lineární rozšíření** relace $\preceq$, jestliže je $(A, \preceq_L)$ lineárně uspořádaná množina a $\preceq \subseteq \preceq_L$, tedy pro všechna $a, b \in A$ splňující $a \preceq b$ platí i $a \preceq_L b$.

Věta.
Pro každou konečnou částečně uspořádanou množinu $(A, \preceq)$ existuje lineární rozšíření $\preceq_L$ na A.

```
procedure topological sort((A, ⪯))
k := 0;
while A ≠ ∅ do
    k := k + 1
    a_k := min(A)
    A := A − {a_k};
output: (a_1 ≺_L a_2 ≺_L ··· ≺_L a_k);
```

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Řekneme, že $(A, \preceq)$ je **dobře uspořádaná množina**, jestliže každá neprázdná podmnožina množiny A má nejmenší prvek.

Fakt.
Každé dobré uspořádání je také lineární.

Axiom (princip dobrého uspořádání)
$(\mathbb{N}, \leq)$ je dobře uspořádaná množina.

Definice.
Uvažujme částečně uspořádané množiny $(A_1, \preceq_1), \dots, (A_n, \preceq_n)$. Definujeme **lexikografické uspořádání** na $A = A_1 \times \cdots \times A_n$ následovně: Pro $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in A$ platí $a \preceq_L b$ právě tehdy, jestliže $a_i = b_i$ pro všechna $i = 1, \dots, n$ (tedy $a = b$), nebo existuje index k takový, že $a_i = b_i$ pro všechna i splňující $1 \leq i < k$ a $a_k \prec_k b_k$.

Věta.
Uvažujme dobře uspořádané množiny $(A_1, \preceq_1), \dots, (A_n, \preceq_n)$. Pak je $A = A_1 \times \cdots \times A_n$ spolu s lexikografickým uspořádáním $\preceq_L$ dobře uspořádaná množina.

Definice.
Relace na množině se nazývá **ekvivalence**, jestliže je reflexivní, symetrická a tranzitivní.

Definice.
Nechť $\mathcal{R}$ je relace ekvivalence na nějaké množině A.
Pro $a \in A$ definujeme **třídu ekvivalence** prvku a vzhledem k $\mathcal{R}$ jako

$$[a]_{\mathcal{R}} = \{b \in A : a\mathcal{R}b\}.$$

Věta.
Nechť $\mathcal{R}$ je relace ekvivalence na nějaké množině A, nechť $a \in A$.
(i) Pro každé $b, c \in [a]_{\mathcal{R}}$ platí $b\mathcal{R}c$.
(ii) Pro každé $b \in [a]_{\mathcal{R}}$ a $c \in A$ platí, že jestliže $b\mathcal{R}c$, pak $c \in [a]_{\mathcal{R}}$.
(iii) Pro každé $b \in [a]_{\mathcal{R}}$: $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$.
(iv) Pro každé $a, b \in A$ platí: $a\mathcal{R}b$ právě tehdy, když $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$.
(v) Pro všechna $a, b \in A$ platí, že buď $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$, nebo $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$.

Definice.
Uvažujme množinu A. Jejím **rozkladem** rozumíme libovolný soubor $\{A_i\}_{i \in I}$ neprázdných podmnožin A takových, že $A = \bigcup\limits_{i \in I} A_i$ a pro všechna $i \neq j \in I$ jsou A_i, A_j disjunktní.

Věta.
Nechť A je množina.
(i) Jestliže je $\mathcal{R}$ ekvivalence na A, pak $\{[a]_{\mathcal{R}}\}_{a \in A}$ je rozklad množiny A.
(ii) Jestliže je $\{A_i\}_{i \in I}$ nějaký rozklad množiny A, pak existuje relace ekvivalence $\mathcal{R}$ na A taková, že $\{A_i\}_{i \in I}$ jsou přesně třídy ekvivalence $\mathcal{R}$.

Věta.
Pro každé $n \in \mathbb{N}$ je relace „být kongruentní modulo n“ ekvivalence na $\mathbb{Z}$.

Definice.
Prostor $\mathbb{Z}_n$ definujeme jako množinu všech tříd ekvivalence v $\mathbb{Z}$ vzhledem k relaci být kongruentní modulo n, tedy $\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\}$.
Pro $[a]_n, [b]_n \in \mathbb{Z}_n$ definujeme

$$[a]_n \oplus [b]_n = [a+b]_n,$$
$$[a]_n \odot [b]_n = [a \cdot b]_n.$$

Věta.
Nechť $n \in \mathbb{N}$, uvažujme $a, b, u, v \in \mathbb{Z}$ takové, že $[a]_n = [u]_n$ a $[b]_n = [v]_n$. Pak $[a+b]_n = [u+v]_n$ a $[a \cdot b]_n = [u \cdot v]_n$.

Věta.
Nechť $n \in \mathbb{N}$, uvažujme $[a]_n \in \mathbb{Z}_n$.
(i) Vždy existuje prvek opačný $-[a]_n = [n-a]_n$.
(ii) $[a]_n$ je invertibilní vůči $\odot$ právě tehdy, když jsou a a n nesoudělné.