Opakování

- výroková logika

x	y	$x \Rightarrow y$
0	0	1
0	1	1
1	0	$\boxed{0}$
1	1	1

$x \Rightarrow y \Leftrightarrow \neg x \vee y$

- predik. logika
  - univ. kvan. $\forall x . \varphi(x)$
  - ex. kvant. $\exists x . \varphi(x)$

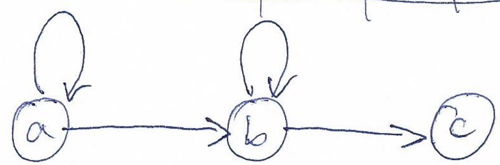
$\neg \forall x . \varphi(x) \equiv \exists x . \neg \varphi(x)$

- kartézský součin mn-n:
  - $A \times B = \{(x, y) \mid x \in A, y \in B\}$
  - $A_1 \times \dots \times A_n = \{(x_1, \dots, x_n) \mid x_1 \in A_1, \dots, x_n \in A_n\}$
- relace
  - binární relace na mn-ě: $\varrho \subseteq A \times A$
  - obecné $\varrho \subseteq A_1 \times \dots \times A_n$
  - tranzitivní uzávěr relace $\varrho \subseteq A \times A$ je relace $\varrho^+ \subseteq A \times A$ def. tak, že: $\forall a, b \in A: a \varrho^+ b \overset{def}{\Leftrightarrow} \exists c_1, \dots, c_n \in A: a = c_1 \wedge b = c_n \wedge \forall 1 \leq i \leq n-1: c_i \varrho c_{i+1}$

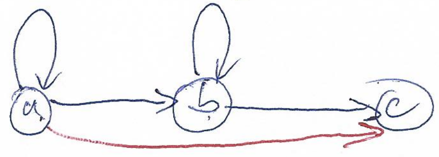
- reprezentace relací
  - množinově, např. $A = \{a, b, c\}$
    $\rho = \{(a,a), (a,b), (b,b), (b,c)\}$
  - maticí, např.

	a	b	c
a	1	1	0
b	0	1	1
c	0	0	0

  - grafem



- sestavte a grafem reprezentujte relaci ρ^+ pro ρ uvedené výše:



- vlastnosti relací na množině – předp., že ~~ale~~ relaci $R \subseteq A \times A$:
  - Řekneme, že R je relace souvislá, jestliže:
    $\forall x, y \in A : x \neq y \Rightarrow xRy \vee yRx$
  - R je reflexivní : $\forall x \in A : xRx$
  - R je ireflexivní : $\forall x \in A : x \not R x$
  - R je symetrická : $\forall x, y \in A : xRy \Rightarrow yRx$

- R je asymetrická: $\forall x,y \in A: xRy \Rightarrow y \not R x$
- R je antisymetrická: $\forall x,y \in A: xRy \wedge yRx \Rightarrow x = y$
- R je tranzitivní: $\forall x,y,z \in A: xRy \wedge yRz \Rightarrow xRz$

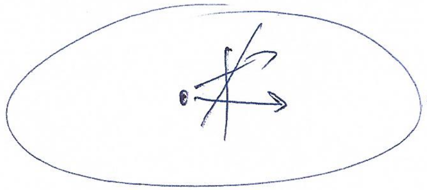
- Jaké vlastnosti mají výše uvedené relace ϱ a ϱ^+:

ϱ:
- není souvislá ($a \not\varrho c \wedge c \not\varrho a$)
- není reflex. ($c \not\varrho c$)
- není ireflex. ($a \varrho a$)
- není symetrická ($a \varrho b \wedge b \not\varrho a$)
- není asymetrická ($a \varrho a$)
- je antisymetrická
- není trans. ($a \varrho b$, $b \varrho c$, $a \not\varrho c$)

ϱ^+:
- je souvislá
- není reflex.
- není ireflex.
- není sym.
- není asym.
- je antisymetrická
- je tranzitivní.

- speciální typy relací:
  - ekvivalence: symetrická, reflex., tranzitivní.
  - ostré částečné uspořádání (např. $\subset$): ireflex., asymetrická, trans.
  - ne ——"—— ——"—— (např. $\subseteq$): reflex., antisym., trans.
  - ostré úplné uspořádání (např. $<$ na $\mathbb{Z}$): ireflex., asymetrická, trans., souv.
  - ne ——"—— ——"—— (např. $\leq$ na $\mathbb{Z}$): reflex., antisym., trans., souv.

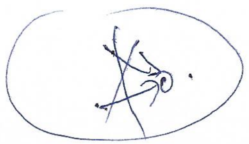
- funkce z množiny A do B:
  ($f: A \to B$) je relace $f \subseteq A \times B$
  taková, že: 1. $\forall x \in A \ \exists y \in B: (x,y) \in f$
  nebolí $f(x) = y$



  2. $\forall x \in A \ \forall y_1, y_2 \in B: f(x) = y_1 \wedge f(x) = y_2 \Rightarrow y_1 = y_2$

částečné f-ce – nutno zmínit explicitně: $f: A \longrightarrow B$

- jednoznačná f-ce (injekce) je f-ce $f: A \to B$ taková, že
  $\forall x_1, x_2 \in A \ \forall y \in B: f(x_1) = y \wedge f(x_2) = y \Rightarrow x_1 = x_2$



- zobrazení na množinu (surjekce) je f-ce $f: A \to B$ taková, že $\forall y \in B \ \exists x \in A: f(x) = y$
- jedno-jednoznačná f-ce (bijekce): injekce i surjekce zároveň
- řekneme, že A je spočetná množina, jestliže existuje bijekce $f: A \leftrightarrow N$
- řekneme, že ekvivalence $\equiv \subseteq A \times A$ je kongruence vůči f-ci $f: A \to A$, jestliže $\forall x, y \in A: x \equiv y \Rightarrow f(x) \equiv f(y)$

např. $\equiv_3$ (ekvivalence zbytku při dělení 3) a funkce +5.

konečné. nesmí-li $1 \equiv_3 4$, pak $\underbrace{1+5}_{6} \equiv_3 \underbrace{4+5}_{9}$

Formální jazyky

- abeceda Σ
- jazyk $L \subseteq \Sigma^*$
- konkatenace "·": – pro řetězce $x = a_1 \dots a_n$, $y = b_1 \dots b_m$:
  $x \cdot y = a_1 \dots a_n b_1 \dots b_m$
  – pro jazyky $L_1 \cdot L_2 = \{ x \cdot y \mid x \in L_1, y \in L_2 \}$
- iterace: $L^* = \bigcup_{n \geq 0} L^n$, kde $L^0 = \{\varepsilon\}$, $L^{n+1} = L \cdot L^n$

  poz. iterace $L^+ = \bigcup_{n > 0} L^n$

- Určete $L_1 \cup L_2$, $L_1 \cap L_2$, $L_1 \setminus L_2$, L_1^*, L_1^+, $L_1 \cdot L_2$ pro jazyky $L_1 = \{a, b\}$ a $L_2 = \{a, \varepsilon\}$ nad $\Sigma = \{a, b\}$.

- $L_1 \cup L_2 = \{a, b, \varepsilon\}$
- $L_1 \cap L_2 = \{a\}$
- $L_1 \setminus L_2 = \{b\}$
- $L_1 \cdot L_2 = \{aa, a, ba, b\}$

- $L_1^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, \dots\}$
- $L_1^+ = \{a, b, aa, ab, ba, bb, \dots\}$

- Určete, zda platí následující tvrzení:

$$\forall \Sigma \, \forall L_1, L_2 \subseteq \Sigma^* : L_1 \subseteq L_1 \cdot L_2$$

Neplatí: např. $L_1 = \{a\}$ $L_2 = \{b\}$

$L_1 = \{a\} \not\subseteq L_1 \cdot L_2 = \{a\}\{b\} = \{ab\}$

- Dokažte, že platí $\forall \Sigma \, \forall L_1, L_2 \subseteq \Sigma^* : L_1 \subseteq L_1 \cdot L_2 \Leftrightarrow L_1 = \emptyset \vee \varepsilon \in L_2$.

Důkaz:

1. Ukážeme „$\Leftarrow$":
   a) Předpokládejme, že $L_1 = \emptyset$.
      Pak nutně platí $L_1 \subseteq L_1 \cdot L_2$, protože L_1 je nejmenší mn-a vůči $\subseteq$.
   b) Předpokládejme, že $\varepsilon \in L_2$. Ukážeme, že $L_1 \subseteq L_1 \cdot L_2$ tak, že ukážeme platnost $\forall w \in L_1 . \; w \in L_1 \cdot L_2$.
      i) Pokud $L_1 = \emptyset$, tvrzení platí triviálně

$\varphi_1 \Leftrightarrow \varphi_2$

1) najdeme $\psi_1, \psi_2, \dots \psi_n$:
$\psi_1 = \varphi_1$, $\psi_n = \varphi_2$
$\psi_1 \Leftrightarrow \psi_2$,
$\psi_2 \Leftrightarrow \psi_3$
⋮

ii) Pokud $L_1 \neq \emptyset$, uvažme libovolné $w \in L_1$.
Víme, že $\varepsilon \in L_2$. Z def. "$\cdot$" víme, že $w \cdot \varepsilon \in L_1 \cdot L_2$.
Z def. "$\cdot$", $w \cdot \varepsilon = w$ a tedy $w \in L_1 \cdot L_2$.

2. Ukážeme, že "$\Rightarrow$"
- Provedeme důkaz sporem.
- Předpokládejme, že $\neg \overbrace{(\forall \Sigma\ \forall L_1, L_2 \subseteq \Sigma^* : L_1 \subseteq L_1 \cdot L_2 \Rightarrow L_1 = \emptyset \vee \varepsilon \in L_2.)}^{\varphi}$
- Provedeme několik ekv. úprav.

$$\varphi \Leftrightarrow \exists \Sigma\ \exists L_1, L_2 \subseteq \Sigma^* : \neg(L_1 \subseteq L_1 \cdot L_2 \Rightarrow L_1 = \emptyset \vee \varepsilon \in L_2)$$
$$\Leftrightarrow \text{—"—} : \neg(\neg L_1 \subseteq L_1 \cdot L_2 \vee (L_1 = \emptyset \vee \varepsilon \in L_2))$$
$$\Leftrightarrow \text{—"—} : \neg\neg(L_1 \subseteq L_1 \cdot L_2) \wedge \neg(L_1 = \emptyset \vee \varepsilon \in L_2)$$
$$\Leftrightarrow \text{—"—} : L_1 \subseteq L_1 \cdot L_2 \wedge L_1 \neq \emptyset \wedge \varepsilon \notin L_2.$$

- Uvažme libovolné Σ, L_1, L_2 takové, že
  $L_1 \subseteq L_1 \cdot L_2 \wedge L_1 \neq \emptyset \wedge \varepsilon \notin L_2$.
- Víme, že $L_1 \neq \emptyset$ a jsou v něm tedy nějaké řetězce. Vybereme si libovolný řetězec $w \in L_1$, který patří mezi nejkratší řetězce v L_1.
- Z toho, že $L_1 \subseteq L_1 \cdot L_2$, víme, že $w \in L_1 \cdot L_2$
- Pak ale z def. "$\cdot$": $w = w_1 \cdot w_2$, kde $w_1 \in L_1 \wedge w_2 \in L_2$.

$L_1 \neq \emptyset$

$L_1 \subseteq L_1 \cdot L_2$

$\emptyset \subset L_1 \cdot L_2$
$\Rightarrow L_2 \neq \emptyset$

- Ovšem $\varepsilon \notin L_2$ a tedy $|w_2| > 0$.
- Tedy $|w_1| = |w| - |w_2| < |w|$. Neboli $w_1 \in L_1$ je kratší než nejkratší řetězec v L_1, což je spor. $\square$

- Vypočtěte:
  - $\emptyset^* = \{\varepsilon\}$
  - $\emptyset^+ = \emptyset$
  - $\emptyset \cup \{\varepsilon\} = \{\varepsilon\}$
  - $\emptyset \cap \{\varepsilon\} = \emptyset$
  - $\emptyset \cdot \{\varepsilon\} = \emptyset$
  - $\emptyset \cdot L = \emptyset$
  - $\{\varepsilon\}^* = \{\varepsilon\}$
  - $\{\varepsilon\}^+ = \{\varepsilon\}$
  - $\emptyset \cap L = \emptyset$
  - $\{\varepsilon\} \cap L = \begin{cases} \emptyset & \text{jestliže } \varepsilon \notin L \\ \{\varepsilon\} & \text{jestliže } \varepsilon \in L \end{cases}$
  - $\{\varepsilon\} \cdot \{\varepsilon\} = \{\varepsilon\}$
  - $\{\varepsilon\} \cdot L = L$

$\{ \ldots \}$ – množiny
$(, \ldots ,)$ – n-tice
$[\quad]$ – ekv. třídy

NEPLÉST!!!

$x \in \{ \dots \}$ ~~$x \in (\dots)$~~

$\{ \dots \} \times \{ \dots \}$ ~~$(\dots) \times (\dots)$~~

- Dokažte mat. indukcí, že pro každou konečnou množinu A platí $|2^A| = 2^{|A|}$.

mn-a všech podmnožin mn-y A.

<u>důkaz indukcí dle $|A| = n \geq 0$.</u>

1. bázový případ: $|A| = 0$
   - z $|A| = 0$ plyne, že $A = \emptyset$
   - $2^\emptyset = \{\emptyset\}$
   - $|2^\emptyset| = |\{\emptyset\}| = 1 = 2^0 = 2^{|A|}$,

     tedy $|2^\emptyset| = 2^{|\emptyset|}$.

2. Indukční krok: Předpokládejme, že tvrzení platí pro mn-y A takové, že $|A| = n$ pro $n \geq 0$. Ukažme, že pak tvrzení platí i pro množiny velikosti $|A| = n+1$.

- Uvažme mn-u A takovou, že $|A| = n+1$ pro $n \geq 0$.
- V A tedy existuje prvek $a \in A$, zvolme libovolný takový prvek a a uvažme $A' = A \setminus \{a\}$
- $|A'| = n+1-1 = n$.
- Pro A' tedy platí ind. předpoklad a tedy

  $|2^{A'}| = 2^{|A'|}$.

- $2^A = \{B, B \cup \{a\} \mid B \in 2^{A'}\}$ přičemž je

  zřejmé, že $B \neq B \cup \{a\}$, protože $a \notin A'$
- $|2^A| = 2 \cdot |2^{A'}| = 2 \cdot 2^{|A'|} = 2^{|A'|+1} = 2^{n+1} = 2^{|A|}$.

  Neboli $|2^A| = 2^{|A|}$. $\square$