

Úvod do teoretické informatiky

Zdeněk Sawa

Katedra informatiky, FEI,
Vysoká škola báňská – Technická universita Ostrava
17. listopadu 15, Ostrava-Poruba 708 33
Česká republika

13. února 2013

Jméno: Ing. Zdeněk Sawa, Ph.D.

E-mail: zdenek.sawa@vsb.cz

Místnost: A1024

Web: <http://www.cs.vsb.cz/sawa/uti>

Na těchto stránkách najdete:

- Informace o předmětu
- Učební texty
- Slidy z přednášek
- Zadání příkladů na cvičení
- Aktuální informace
- Odkaz na stránku s animacemi

- **Zápočet** (22 bodů):

- Zápočtová písemka (22 bodů) — bude se psát na cvičení

Minimum pro získání zápočtu je 7 bodů.

Možnost opravy za 14 bodů.

- **Zkouška** (78 bodů)

- Písemná zkouška skládající se ze tří částí po 26 bodech, přičemž z každé části je nutné získat nejméně 10 bodů.

Různé oblasti teoretické informatiky:

- algoritmy
- výpočetní složitost
- výpočetní modely
- teorie automatů
- formální jazyky
- syntaxe a sémantika programovacích jazyků
- teorie typů
- paralelní a distribuované systémy
- ...

Překrývá se s mnoha dalšími oblastmi matematiky a informatiky:

- logika
- teorie grafů
- teorie čísel
- kryptografie
- výpočetní geometrie
- teorie her
- numerická matematika
- ...

Některé důležité charakteristiky teoretické informatiky:

- formální matematický přístup k problémům
- používání matematických definic a důkazů
- rigorózní matematické důkazy

Pojem důkazu, axiomatický přístup.

Logika — obor zkoumající vyplývání, důkazy, formalismy

Konjunkce: $A \wedge B$

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

Poznámka: označuje se též $\&$ nebo **and**

$$\wedge i: \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

$$\wedge e_1: \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$$

$$\wedge e_2: \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\text{Assm: } \frac{}{\Gamma, A, \Delta \vdash A}$$

$$A \wedge B, C \wedge D \vdash B \wedge C$$

1. $A \wedge B, C \wedge D \vdash A \wedge B$ (Assm)
2. $A \wedge B, C \wedge D \vdash B$ ($\wedge e_2$ 1)
3. $A \wedge B, C \wedge D \vdash C \wedge D$ (Assm)
4. $A \wedge B, C \wedge D \vdash C$ ($\wedge e_1$ 3)
5. $A \wedge B, C \wedge D \vdash B \wedge C$ ($\wedge i$ 2,4)

$$A \wedge B, C \wedge D \vdash B \wedge C$$

1. $\Gamma \vdash A \wedge B$ (Assm)
2. $\Gamma \vdash C \wedge D$ (Assm)
3. $\Gamma \vdash C$ ($\wedge e_1$ 2)
4. $\Gamma \vdash B$ ($\wedge e_2$ 1)
5. $\Gamma \vdash B \wedge C$ ($\wedge i$ 4,3)

Poznámka: $\Gamma := A \wedge B, C \wedge D$

Důkaz znázorněný jako strom

$$A \wedge B, C \wedge D \vdash B \wedge C$$

$$\frac{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \quad \frac{\Gamma \vdash C \wedge D}{\Gamma \vdash C}}{\Gamma \vdash B \wedge C}$$

Poznámka: $\Gamma := A \wedge B, C \wedge D$

$$\frac{\Gamma \vdash (A \wedge B) \wedge C}{\Gamma \vdash A \wedge (B \wedge C)}$$

1. $\Gamma \vdash (A \wedge B) \wedge C$ (premise)
2. $\Gamma \vdash A \wedge B$ ($\wedge e_1$ 1)
3. $\Gamma \vdash A$ ($\wedge e_1$ 2)
4. $\Gamma \vdash B$ ($\wedge e_2$ 2)
5. $\Gamma \vdash C$ ($\wedge e_2$ 1)
6. $\Gamma \vdash B \wedge C$ ($\wedge i$ 4,5)
7. $\Gamma \vdash A \wedge (B \wedge C)$ ($\wedge i$ 3,6)

permutace:

$$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, B, A, \Delta \vdash C}$$

zeslabení:

$$\frac{\Gamma, \Delta \vdash B}{\Gamma, A, \Delta \vdash B}$$

kontrakce:

$$\frac{\Gamma, A, A, \Delta \vdash B}{\Gamma, A, \Delta \vdash B}$$

$$\text{Ant: } \frac{\Gamma \vdash A}{\Gamma' \vdash A} (\Gamma \subseteq \Gamma')$$

$$\text{Ch: } \frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}$$

Disjunkce: $A \vee B$

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Poznámka: označuje se též **or**

XOR

xor (exclusive or): $A \oplus B$

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Pravidla pro disjunkci

$$\vee_{i_1}: \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$$

$$\vee_{i_2}: \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

$$\vee_e: \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$(A \vee B) \vee C \vdash A \vee (B \vee C)$$

1. $\varphi \vdash (A \vee B) \vee C$ (Assm)
2. $\varphi, A \vee B \vdash A \vee B$ (Assm)
3. $\varphi, A \vee B, A \vdash A$ (Assm)
4. $\varphi, A \vee B, A \vdash A \vee (B \vee C)$ ($\vee i_1$ 3)
5. $\varphi, A \vee B, B \vdash B$ (Assm)
6. $\varphi, A \vee B, B \vdash B \vee C$ ($\vee i_1$ 5)
7. $\varphi, A \vee B, B \vdash A \vee (B \vee C)$ ($\vee i_2$ 6)
8. $\varphi, A \vee B \vdash A \vee (B \vee C)$ ($\vee e$ 2,4,7)
9. $\varphi, C \vdash C$ (Assm)
10. $\varphi, C \vdash B \vee C$ ($\vee i_2$ 9)
11. $\varphi, C \vdash A \vee (B \vee C)$ ($\vee i_2$ 10)
12. $\varphi \vdash A \vee (B \vee C)$ ($\vee e$ 1,8,11)

Poznámka: $\varphi := (A \vee B) \vee C$