NTIN090 — Základy složitosti a vyčíslitelnosti

Zkouškové otázky, školní rok 2022/23

Petr Kučera

U zkoušky jsou zadávány dvě otázky, jednu ze skupiny A a jednu ze skupiny B.

K tvrzením, jež jsme dokazovali na přednášce, bude požadován důkaz (ačkoli není nutné umět přesně ty důkazy, které jsme si ukazovali na přednášce a je možné použít alternativní důkazy).

A

(A1) Definice m-převoditelnosti a m-úplnosti. Riceova věta.

(A2) Savičova věta.

(A3) Deterministická prostorová hierarchie.

(A4) Deterministická časová hierarchie.

(A5) Cookova-Levinova věta (NP-úplnost SAT)

B

(B1) Univerzální Turingův stroj a nerozhodnutelnost jazyka univerzálního Turingova stroje.

(B2) RAM a ekvivalence s Turingovým strojem.

(B3) Vlastnosti (turingovsky) rozhodnutelných a částečně rozhodnutelných jazyků (uzávěrové vlastnosti, Postova věta, enumerátory).

(B4) Definice základních tříd složitosti a důkaz $\mathrm{NTIME}(f(n)) \subseteq \mathrm{SPACE}(f(n))$.

(B5) Definice základních tříd složitosti a důkaz věty o vztahu prostoru a času $((\forall L \in \mathrm{NSPACE}(f(n)))(\exists c_L)[L \in \mathrm{TIME}(2^{c_L f(n)})])$.

(B6) Dvě definice třídy NP a jejich ekvivalence.

(B7) Polynomiální převod SAT na 3-SAT.

(B8) Polynomiální převod 3-SAT na Vrcholové pokrytí.

(B9) Definice třídy FPT a kernelu a jejich souvislost. Kernelizace Vrcholového pokrytí

(B10) Definice třídy FPT a parametrizovaný algoritmus pro Vrcholové pokrytí založený na prohledávání s omezenou hloubkou (se složitostí menší než $O^*(2^k)$).

(B11) Třída #P a #P-úplnost.

(B12) Třída co-NP a co-NP-úplnost.

(B13) Pseudonáhodné generátory, jednosměrné funkce a jejich souvislost s kryptografií (symetrické šifrování, bit-commitment).

(B14) Příklad zjemnělé redukce (redukce SETH na OV nebo OV na hledání regulárního výrazu v textu).