Inovace předmětu Složitost

(FRVŠ 166/2013/G1)

Řešitel: Ondřej Lengál

Spoluřešitelé: Mgr. Adam Rogalewicz, Ph.D.
Ing. Lukáš Charvát

Fakulta informačních technologií
Vysoké učení technické v Brně

25. února 2014

http://www.fit.vutbr.cz/~ilengal/grants.php?id=640

Motivace

Výuka teorie výpočetní složitosti:

- snaha o pochopení
  - inherentní složitosti problémů
    - např. řazení prvků na základě porovnání nelze provést rychleji než v $\mathcal{O}(n \cdot \log n)$,
  - a jejich vzájemné souvislosti
    - např. problém testování splnitelnosti formule výrokové logiky je *stejně obtížný* jako problém testování 3-obarvitelnosti grafu,
- chytré algoritmy a řešení problémů
  - např. důkazy Immerman-Szelepcsényiho věty nebo Cookovy věty,
- přesah do jiných oblastí:
  - kryptografie,
  - fyzika (kvantová složitost),
  - ...

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle

1. Rozšíření látky vyučované v předmětu Složitost na FIT VUT:
   a) souvislost teorie složitosti a kryptografie,
   b) čítací třídy (counting classes),
2. aktualizace 5 stávajících prezentací:
   a) Úvod to teorie výpočetní složitosti,
   b) RAM a RASP stroje,
   c) Vztahy mezi složitostními třídami,
   d) **NP**-úplné problémy,
   e) Paralelní výpočty.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle a jejich řešení

Průběh řešení:

1. nákup a studium literatury,
2. cesta řešitele na konference ETAPS'13 (březen 2013, Řím, Itálie),
3. příprava prezentací.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle a jejich řešení (1/7)

Dílčí cíl:

1. Rozšíření látky vyučované v předmětu Složitost na FIT VUT:
   a) souvislost teorie složitosti a kryptografie

Výstupy:

- Vytvořena prezentace v systému LaTeX (17 slajdů)
  - úvod do kryptografie z pohledu teorie výpočetní složitosti, popis kryptografie s veřejným klíčem, kryptografického systému RSA, třídy **UP** a některých protokolů založených na kryptografii.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle a jejich řešení (2/7)

Dílčí cíl:

1. Rozšíření látky vyučované v předmětu Složitost na FIT VUT:
   b) čítací třídy (counting classes)

Výstupy:

- Vytvořena prezentace v systému LaTeX (20 slajdů)
  - definice čítacích problémů, příklady čítacích problémů počtu perfektních párování v bipartitním grafu a spolehlivosti grafu, zavedení složitostní třídy #**P** a pojmu redukce pro čítací složitostní třídy, důkazy #**P**-úplnosti problémů #SAT a PERMANENT, zavedení třídy $\oplus$**P** a důkaz její uzavřenosti vzhledem k doplňku,
  - prezentováno v LS 2013.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle a jejich řešení (3/7)

Dílčí cíle:

2. Aktualizace 5 stávajících prezentací:
   a) Úvod do teorie výpočetní složitosti

Výstupy:

- Vytvořena prezentace v systému LaTeX (21 slajdů)
  - oproti původní prezentaci přidány příklady a rozepsány typy problémů, přidána zmínka o Kolmogorově složitosti, některé výpočetní modely, Cobhamova teze a přesnější definice konstruovatelných funkcí.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle a jejich řešení (4/7)

Dílčí cíle:

2. Aktualizace 5 stávajících prezentací:
   b) RAM a RASP stroje

Výstupy:

- Vytvořena prezentace v systému LaTeX (22 slajdů)
  - oproti původní prezentaci přidány přesnější definice RAM a RASP strojů, logaritmické časové složitosti a důkaz ekvivalence RAM strojů a Turingových strojů.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle a jejich řešení (5/7)

Dílčí cíle:

2. Aktualizace 5 stávajících prezentací:
   c) Vztahy mezi složitostními třídami

Výstupy:

- Vytvořena prezentace v systému LaTeX (27 slajdů)
  - oproti původní prezentaci přidány důkazy platnosti inkluzí mezi některými třídami a podány důkazy Savitchovy věty a Immerman-Szelepcsényiho věty.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle a jejich řešení (6/7)

Dílčí cíle:

2. Aktualizace 5 stávajících prezentací:
   d) **NP**-úplné problémy

Výstupy:

- Vytvořena prezentace v systému LaTeX (19 slajdů)
  - oproti původní prezentaci přidány důkazy **NP**-úplnosti problémů CNF, *k*-CNF, CLIQUE, INDEPENDENT SET, VERTEX COVER, GRAPH COLOURING, SUBSET SUM, PARTITION, KNAPSACK.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Cíle a jejich řešení (7/7)

Dílčí cíle:

2. Aktualizace 5 stávajících prezentací:
   e) Paralelní výpočty

Výstupy:

- Vytvořena prezentace v systému LaTeX (28 slajdů)
  - oproti původní prezentaci přidány popisy složitosti Booleovských obvodů včetně důkazu simulace mezi Booleovskými modely a paralelními RAM stroji, přidán důkaz **P**-úplnosti problému CVP a důkaz **P**-úplnosti problému MAXFLOW pomocí redukce z problému MCVP2.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Čerpání finančních prostředků

- Běžné náklady

Položka	Částka [Kč]
Stipendia	40.000,00
L. Charvát, O. Lengál	
Cestovné zahraniční	24.000,00
cesta O. Lengála na konference ETAPS'13	
Ostatní náklady	11.000,00
nákup 7 knih	
Celkem	75.000,00

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

Výsledky a výstupy

- Hlavní výstupy—7 prezentací
  - úvod to teorie výpočetní složitosti,
  - RAM a RASP stroje,
  - vztahy mezi složitostními třídami,
  - **NP**-úplné problémy,
  - paralelní výpočty,
  - kryptografie z pohledu výpočetní složitosti,
  - čítací třídy.
- Vedlejší výstupy:
  - pořízení 7 knih k tématu teorie výpočetní složitosti.

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`

ETAPS'13

- A. Bouajjani, E. Derevenetc, R. Meyer. *Checking Robustness against TSO*. ESOP'13.
  - Trace robustness under TSO is **PSPACE**-complete.
- A. Bohy, V. Bruyère, E. Filiot, J.-F. Raskin. *Synthesis from LTL Specifications with Mean-Payoff Objectives*. TACAS'13.
  - LTL_{MP} realizability is **2EXPTIME**-complete.
- P. Godefroid, M. Yannakakis. *Analysis of Boolean Programs*. TACAS'13.
  - Complexity results about Boolean programs.
- ...

`http://www.fit.vutbr.cz/~ilengal/grants.php?id=640`