SOUČASNÉ TRENDY TEORETICKÉ INFORMATIKY

13.–14. května 2005, Praha

D. Kráľ (ed.)

Úvodní slovo

Tato konference navazuje na konferenci Současné trendy teoretické informatiky (STII2003), která se konala v květnu 2003 v Praze. Cíl a účel konference STTI2005, která se koná ve dnech 13.–14. května 2005 v Praze v budove MFF UK na Malostranském náměstí, zůstává stejný: Rádi bychom vytvořili domací fórum pro prezentaci kvalitních výsledků českých a slovenských informatiků. Jedním z měřítek kvality práce v soudobé teoretické informatice je publikování na mezinárodních výběrových konferencích (např. CAV, COCOON, CP, CONCUR, ESA, ETAPS, FOCS, GD, ICALP, IFIP TCS, ISAAC, LATIN, LICS, MFCS, SODA, STACS, STOC, SWAT, WADS). Na těchto konferencích je obvykle několikanásobně více přihlášených než přijatých příspěvků. Na konferenci STTI jsme pozvali ty mladé české a slovenské informatiky, kteří uspěli v této konkurenci a jejichž práce byly referovány na některé z těchto mezinárodních akcí. Uspořádáním této konference chceme dát možnost široké odborné veřejnosti seznámit se s výsledky, kterým se dostalo mezinárodního uznání. Doufáme, že konference splní svůj účel a povzbudí české informatiky v další práci.

Na konferenci bylo pozváno celkem 40 mladých českých a slovenských informatiků, z nichž 30 se konference zúčastní. Kromě nich, přednesou hlavní přednášky na konferenci Pavol Hell na téma barvení grafů a CSP a Petr Jančar na téma verifikace počítačových systémů.

Konference STTI je organizována a podporována Institutem teoretické informatiky (ITI) (projekt MŠMT 1M0021620808) ve spolupráci s Katedrou aplikované matematiky MFF UK. Programový výbor konference zahrnoval vedoucí jednotlivých týmů, které se podílí na projektu ITI. Rád bych poděkoval všem členům programového výboru za jejich práci a dále pak pí. Polišenské, J. Černému a D. Kráľovi za jejich pomoc při organizaci konference.

Jaroslav Nešetřil

Hlavní přednášky konference

Pavol Hell

Od farbenia grafov k problémom CSP

Petr Jančar

Verifikace počítačových systémů (teoretické aspekty)

Složení programového výboru konference

Prof. RNDr. Jan Kratochvíl, CSc. (MFF UK v Praze)

Doc. RNDr. Antonín Kučera, Ph.D. (FI MU v Brně)

Prof. RNDr. Jaroslav Nešetřil, DrSc. (MFF UK v Praze - předseda)

RNDr. Pavel Pudlák, DrSc. (MÚ AV ČR)

Prof. RNDr. Zdeněk Ryjáček, DrSc. (FAV ZČU v Plzni)

Doc. RNDr. Jiří Šíma, CSc. (ÚI AV ČR)

Obsah

Program konference

Pátek 13. května 2005

9:00 Petr Jančar: Verifikace počítačových systémů (teoretické aspekty)

9:50 přestávka

10:20 Tomáš Brázdil: Verifikace nekonečněstavových pravděpodobnostních systémů
10:45 Vojtěch Řehák: Rozšířené procesové přepisovací systémy: dosažitelnost a vyjadřovací síla
11:10 Zdeněk Sawa: Obtížnost testování ekvivalence konečně stavových systémů
11:35 Jiří Srba: Infinite-State Processes: Bisimulation Games and Hardness Results
12:00 Oldřich Stražovský: Rozhodnutelnost pravděpodobnostní bisimulace pro nekonečně-stavové pravděpodobnostní systémy

oběd

14:00 Jakub Černý: Nekřížící se hamiltonovské cesty v geometrických grafech
14:25 Jan Kynčl: Jak dlouhá může být alternující cesta spojující body na kružnici?
14:50 Martin Pergel: Problémy kolem polygon-circle grafů
15:15 Jan Štola: Geometrické reprezentace grafů
15:40 Ľubomír Török: Objemy trojrozmerných uložení grafov

16:05 přestávka

16:30 Roman Barták: Měkká řešení a neúplné prohledávací algoritmy
16:55 Petr Vilím: Jobshop a programování s omezujícími podmínkami
17:20 Janka Chlebíková: Je ťažké nájsť skoro minimálnu dominujúcu množinu v grafe?
17:45 Jan Kára: Složitost nalezení vyrovnaného uspořádání vrcholů grafu
18:10 Ondřej Pangrác: Algoritmus pro cyklickou souvislost kubických grafů

19:00 konferenční večeře

Sobota 14. května 2005

9:00 Pavol Hell: Od farbenia grafov k problémom CSP

9:50 přestávka

10:20 Jiří Fiala: Uspořádání grafů podle lokálně podmíněných homomorfismů
10:45 Miroslav Chlebík: O zložitosti kombinatorických problémov na množinách d-rozmerných intervalov
11:10 Martin Kochol: Obmedzenia na kontrapríklady pre hypotézu o 5-toku
11:35 Daniel Kráľ: Lokálně konzistentní CSP
12:00 Pavel Nejedlý: Grupové barvení a grupová vybíravost jsou Π_2^P-úplné

oběd

14:00 Zdeněk Dvořák: Tři optimální algoritmy pro koule tří barev
14:25 Michal Koucký: Obvody konstantní hloubky: hradla vs. hrany
14:50 Petr Hliněný: O matroidech v teoretické informatice
15:15 Tomáš Ebenlendr: Optimální a online rozvrhování na různých počítačích
15:40 Jan Vondrák: Stochastické pakovací problémy

16:05 přestávka

16:30 Dušan Guller: Binárna rezolúcia na reziduovaných zväzoch
16:55 Radek Pelánek: Ověřování modelů s využitím abstrakce
17:20 Tomáš Vojnar: Abstraktní regulární model checking
17:45 Petr Kolman: Porovnávání podobných řetězců: obtížnost a aproximace
18:10 Michal Kunc: O jednoduchých jazykových rovnicích

Abstrakty příspěvků

Měkká řešení a neúplné prohledávací algoritmy

Roman Barták[1]
MFF UK Praha, Malostranské náměstí 25, 118 00 Praha
E-mail: bartak@kti.mff.cuni.cz

Prohledávací algoritmy patří k populárním technikám řešení problémů v umělé inteligenci a konkrétně v její pod-oblasti zabývající se splňováním omezujících podmínek. Problém splňování omezujících podmínek (CSP – Constraint Satisfaction Problem) je dán konečnou množinou proměnných, kde každá proměnná má přiřazenu konečnou množinu hodnot, tzv. doménu, a konečnou množinou omezujících podmínek, tj. relací omezujících možné kombinace hodnot proměnných. Řešením CSP je potom přiřazení hodnot z příslušných domén všem proměnným tak, že jsou všechny omezující podmínky splněny.

V některých případech je obtížné nalézt úplné řešení CSP (CSP je obecně NP-úplný problém, barvení grafů je například jeho speciální instancí), případně takové řešení ani neexistuje (u tzv. příliš omezených problémů). Při řešení reálných problémů je ale zpravidla potřeba dodat řešení v (polynomiálně) omezeném čase a odpověď, že řešení neexistuje, také často není akceptovatelná (minimálně musí být doplněna odůvodněním). Pro tyto případy jsme navrhli definovat „měkké“ řešení CSP jako tzv. maximální konzistentní ohodnocení proměnných, tj. ohodnocení maximálního počtu proměnných takové, že jsou splněny alespoň podmínky mezi ohodnocenými proměnnými. Takové řešení existuje i pro příliš omezené problémy a v případě splnitelných problémů odpovídá původní definici řešení CSP. Výhodou nového přístupu je možnost vrátit „přibližné“ řešení i pro těžké problémy, kde by nalezení úplného řešení trvalo příliš mnoho času. Jinými slovy, řešící algoritmy mohou vrátit nejlepší nalezené měkké řešení (nejlepší = s největším počtem přiřazených proměnných) v daném (omezeném) čase a toto řešení prezentovat uživateli. Ten pak může na jeho základě upravit původní problém, například odstranit některé podmínky, které nejsou nutné, a opět se pokusit nalézt řešení modifikovaného problému (tzv. mixed-initiative problem solving).

Pro hledání maximálních konzistentních ohodnocení jsme navrhli úpravu neúplných algoritmů prohledávání do hloubky. Konkrétně se jednalo o algoritmy Depth-Bounded Backtrack Search (DBS), Credit Search (CS) a Iterative Broadening (IB). Tyto algoritmy používají různé limity na omezení po-

[1] Tato přednáška je založena na společné práci s Hanou Rudovou (FI MU).

čtu prozkoumávaných alternativ, čímž zkracují běhový čas oproti úplnému prohledávání do hloubky, na druhou stranu ale ztrácejí úplnost (negarantují nalezení řešení). DBS používá limit na hloubku prohledávání, do které zkouší alternativní větve. CS používá tzv. kredit, který rozděluje mezi alternativní větve a v případě vyčerpání kreditu volí pouze jednu z alternativních větví. IB prozkoumává v každém uzlu omezený počet alternativ. Při experimentech dosahoval IB nejlepších výsledků pokud jde o kvalitu nalezeného řešení, na rozdíl od DBS a CS má ale exponenciální časovou složitost. Pokusili jsme se proto navrhnout algoritmus používající podobný princip jako IB, tj. omezený počet přiřazení hodnot do proměnných, který by ale měl polynomiální časovou složitost. Nový algoritmus LAN (Limited Assignment Number) Search omezuje počet pokusů přiřadit proměnné nějakou hodnotu globálně, tj. v průběhu celého prohledávání, zatímco IB to dělá lokálně v každém uzlu prohledávání. Časová složitost LAN Search je pak O(b.n), kde b je příslušný limit a n je počet proměnných. V provedených experimentech s Random Placement Problem, který simuluje reálné rozvrhovací problémy, dosahoval LAN Search nejlepší kvality řešení (ve srovnání s CS, DBS a IB) při běhovém času lepším o několik řádů. Pro další dva experimentální problémy algoritmus sice nedosahoval nejlepší výsledky, oproti ostatním algoritmům byla ale zachována časová stabilita nalezení řešení.

Verifikace nekonečněstavových pravděpodobnostních systémů

Tomáš Brázdil[1]
FI MU Brno, Botanická 68a, 602 00 Brno
E-mail: xbrazdil@fi.muni.cz

Přednáška bude zaměřena na problematiku verifikace pravděpodobnostního rozšíření nekonečněstavových sekvenčních systémů, zejména pravděpodobnostních zásobníkových automatů. Jedním z nejúspěšnějších přístupů k verifikaci systémů je ověřování modelů (model checking). Tento přístup je založen na tom, že požadovaná vlastnost systému je vyjádřena pomocí formule temporální logiky a následně je ověřeno, zda systém tuto formuli splňuje.

Ověřování modelů bylo v minulosti zkoumáno v souvislosti s konečněstavovými pravděpodobnostními systémy a nekonečněstavovými nedeterministickými systémy. Teprve nedávno se začaly objevovat výsledky týkající se rozhodnutelnosti a složitosti ověřování modelů pro nekonečněstavové pravděpodobnostní systémy. V přednášce bude podán stručný přehled těchto výsledků společně s přehledem aktuálního stavu problematiky a otevřených problémů.

[1] Tato přednáška je založena na společné práci s Antonínem Kučerou a Oldřichem Stražovským.

Nekřížící se hamiltonovské cesty v geometrických grafech

Jakub Černý[1]
KAM MFF UK Praha, Malostranské náměstí 25, 118 00 Praha
E-mail: kuba@kam.mff.cuni.cz

Geometrický graf je graf nakreslený do roviny tak, že vrcholy jsou body v rovině a hrany jsou reprezentovány rovnými úsečkami. Nekřížící se hamiltonovská cesta v geometrickém grafu je hamiltonovská cesta neobsahující dvě protínající se hrany. Zabývali jsme se následující otázkou pocházející od Micha Perlese: Kolik nejvíc hran můžeme odebrat z úplného geometrického grafu, aby výsledný graf stále obsahoval nekřížící se hamiltonovskou cestu? Ukážeme, že můžeme odebratat aspoň $c_1\sqrt{n}$ hran. Pro některé třídy grafů ukážeme lepší výsledek. Pokud z geometrického grafu odebíráme úplný podgraf nebo párování nebo hvězdu, tak můžeme odebrat aspoň $c_2 n$ hran. Tento odhad je až na konstantu nejlepší možný, protože exitují grafy, které po odebrání $c_3 n$ hran neobsahují nekřížící se hamiltonovskou cestu.

[1] Tato přednáška je založena na společné práci s Zdeňkem Dvořákem, Vítem Jelínkem a Honzou Károu.

Tři optimální algoritmy pro koule tří barev

Zdeněk Dvořák[1]
ITI MFF UK Praha, Malostranské náměstí 25, 118 00 Praha
E-mail: rakdver@kam.mff.cuni.cz

Uvažujeme hru dvou hráčů, Alice a Boba. Alice si zvolí obarvení n koulí pomocí tří barev. Bob se snaží získat nějakou informaci o tomto obarvení, smí se však pouze ptát, zda dvě jím zvolené koule mají stejnou barvu. Alice mu na každou takovou otázku musí pravdivě odpovědet ano nebo ne, a Bob se chce zeptat na co nejméně otázek. Uvažujeme dva problémy: Problém Plurality, kdy se Bob snaží nalézt kouli s nejčastější barvou, a problém Rozdělení, kdy se Bob snaží rozdělit koule podle jejich barev. Ukážeme optimální deterministickou a pravděpodobnostní strategii pro problém Rozdělení, a asymptoticky optimální pravděpodobnostní strategii pro problém Plurality.

[1] Tato přednáška je založena na společné práci s Vítem Jelínkem, Danielem Kráľem, Honzou Kynčlem a Michalem Saksem.

Optimální a online rozvrhování na různých počítačích

Tomáš Ebenlendr[1]
MÚ AV ČR, Žitná 25, 115 67 Praha
E-mail: ebik@math.cas.cz

Studujeme problém rozvrhování s preempcemi na počítačích s různou rychlostí, nezávislou na zpracovávané úloze (related machines). Ukážeme semi-online algoritmus, který vytvoří optimální rozvrh pokud zná jeho makespan (délka rozvrhu) předem. Z něj pak standardním dvojnásobením odhadu optimálního makespanu dostáváme 4-kompetitivní deterministický a $e \approx 2.71$-kompetitivní pravděpodobnostní algoritmus. V offline prostředí máme možnost spočíst hodnotu optimálního makespanu v inicializační části algoritmu, pak je náš algoritmus stejně efektivní jako dřívější optimální algoritmy. Na rozdíl od nich je však samotný algoritmus i analýza správnosti výrazně jednodušší.

Také zmíníme výsledky naší analýzy hladového algoritmu v preemptivním prostředí. Dokázali jsme, že je $\Theta(\log m)$-kompetitivní. Jeho offline varianta (algoritmus LPT), je $2 - \frac{2}{m-1}$-kompetitivní.

Tento výsledek byl prezentován na konferenci STACS, viz: T. Ebenlendr and J. Sgall.: Optimal and online preemptive scheduling on uniformly related machines. In *Proc. 21st Symp. on Theoretical Aspects of Computer Science (STACS)*, volume 2996 of *Lecture Notes in Comput. Sci.*, pages 199–210. Springer, 2004.

[1] Tato přednáška je založena na společné práci s Jiřím Sgallem.

Uspořádání grafů podle lokálně podmíněných homomorfismů

Jiří Fiala[1]
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: fiala@kam.mff.cuni.cz

V přednášce se zaměřím na grafové homomorfismy s lokálními omezeními, t.j. takové homomorfismy jejichž zúžení se chovají buď bijektivně nebo injektivně popř. surjektivně na okolích každého vrcholu a jeho obrazu.

Lze ukázat, že existence takových homomorfismů vytváří částečné uspořádání na třídě konečných souvislých grafů. Tyto struktury dále přeneseme na matice popisující stupňové rozdělění grafu a dokážeme, že lze vhodným způsobem získat částečná uspořádání i na takovýchto maticích, a že tato uspořádání spolu úzce souvisí.

V závěru bych se rád zaměřil na otázky výpočetní složitosti porovnání dvou matic, resp. grafů v těchto uspořádáních a zmínil několik otevřených otázek.

[1] Tato přednáška je založena na společné práci s Danilem Paulusmou a Janem Arnem Tellem.

Binárna rezolúcia na reziduovaných zväzoch

Dušan Guller
KAI UK Bratislava, Mlynská dolina, 842 15 Bratislava
E-mail: guller@fmph.uniba.sk

Viachodnotové logiky a automatické dokazovanie hrajú dôležitú úlohu v reprezentácii znalostí a uvažovaní. Široko študovanými triedami sú signované (parakonzistentné, anotované) a fuzzy logiky. Pravdivostné hodnoty týchto logík tvoria rozličné zväzové štruktúry. V príspevku budeme diskutovať o úplnosti binárnej rezolučnej dokazovacej metóde nad gradovanými klauzulami.

Predpokladajme, že pravdivostné hodnoty tvoria reziduovaný zväz

$$\mathbb{L} = (L, \leq, \vee, \wedge, \star, {}^{-}, 0, 1)$$

$\mathbb{L}$-hodnotová logika bude obsahovať logické spojky $\neg$, negáciu a $\vee$, disjunkciu, interpretované pravdivostnými funkciami ${}^{-}$ a $\wedge$ na $\mathbb{L}$. Binárny $\mathbb{L}$-rezolučný systém pracuje nad gradovanými klauzulami, dvojicami

$$(l_1 \vee \cdots \vee l_n, c)$$

kde l_i sú literály a c je pravdivostný stupeň z $\mathbb{L}$. Gradované klauzuly môžu byť využívané ako reprezentačný prostriedok pre neúplné a neurčité znalosti, kde neúplnosť je vyjadrená disjunkciu a neurčitosť zase pravdivostným stupňom. Pre danú $\mathbb{L}$-interpretáciu $\mathcal{A}$, $(l_1 \vee \cdots \vee l_n, c)$ je pravdivé v $\mathcal{A}$, v symboloch $\mathcal{A} \models (l_1 \vee \cdots \vee l_n, c)$, ak $\|l_1 \vee \cdots \vee l_n\|^{\mathcal{A}} \geq c$. Propozičné binárne $\mathbb{L}$-rezolučné pravidlo nad gradovanými klauzulami je v tvare

$$\frac{(a \vee D_1, c_1), \quad (\neg a \vee D_2, c_2)}{(D_1 \vee D_2, c_1 \star c_2)} \qquad (c_1 \star c_2 \geq 0).$$

Vo všeobecnosti binárna rezolúcia nie je úplná na reziduovaných zväzoch. Stačí vziať Łukasiewiczovu logiku a nesplniteľnú teóriu $(a, \frac{1}{2})$, $(\neg a, \frac{1}{2})$, $(a \vee \neg a, 1)$; nemôžeme odvodiť $(\Box, c)$, $c > 0$, a tak ju zamietnuť. Avšak, úplnosť sa dá dosiahnuť v niektorých špecialnych prípadoch, ako sú boolovské a reziduované zväzy s ostrou negáciou, definovanou nasledovne:

$$\overline{a} = \begin{cases} 1, & a = 0, \\ 0, & \textit{inak.} \end{cases}$$

Druhý prípad implikuje úplnosť binárnej rezolúcie v Gödelovej a produktovej logike.

Od farbenia grafov k problémom CSP

Pavol Hell
SFU, University Drive 88, Burnaby, BC, Canada V5A 1S6
E-mail: pavol@cs.sfu.ca

Algoritmické úlohy o farbení grafov a ich rôzne zobecnenia (grafové homomorfizmy, problémy CSP), modelujú mnohé aplikované problémy a ich riešeniu sú venované celé knižky. Niektoré verzie sa riešia ľahko, polynomiálnymi algoritmami; iné verzie sú NP-úplné. Čo odlišuje ľahké problémy od ťažkých? V posledných rokoch sa ukázalo, že algebraické vlastnosti systémov majú pri tomto rozhodujúcu úlohu. Fokusom mojej prednášky bude takzvaná hypotéza dichotómie Federa a Vardiho a jej overenia v špeciálnych prípadoch. Okrem svojich výsledkov sa zmienim aj o prácach Jeavonsa, Bulatova, Krochina, Federa, Vardiho, Nešetřila, Kleinovej, Motwaniho, Kráľa, Sgalla a iných.

O matroidech v teoretické informatice

Petr Hliněný[1]
FEI VŠB-TU Ostrava, 17. listopadu 15, 708 33 Ostrava – Poruba
E-mail: petr.hlineny@vsb.cz

Matroidy jsou kombinatorické struktury, které široce zobecňují jak grafy, tak i třeba (konečné) geometrie. Pomineme-li algoritmy v kombinatorické optimalizaci [Edmonds a další], matroidy nejsou příliš rozšířeny v teoretické informatice. V naší přednášce bychom rádi ukázali přehled několika poměrně nových výsledků ukazujících užitečnost matroidů v informatice.

Centrálním pojmem naší prezentace je větvená a stromová šířka ve zobecnění na matroidy. (Pojem stromové šířky matroidu nám mimo jiné dává i zcela nový, „bezvrcholový“, pohled na klasickou stromovou šířku grafů.) V úzké návaznosti bychom shrnuli naše nedávné výsledky o rozhodnutelnosti MSO teorií na reprezentovatelných matroidech a nastínili možné směry budoucích zobecnění na abstraktní matroidy. Závěrem bychom využili příležitost ke krátké prezentaci nového online přístupu k našemu programu Macek pro strukturální výpočty s matroidy.

[1] Tato přednáška je založena na společné práci s D. Seesem a G. Whittlem.

O zložitosti kombinatorických problémov na množinách d-rozmerných intervalov

Miroslav Chlebík[1]
MPI Leipzig, Inselstrasse 22, 04103 Leipzig, SRN
E-mail: chlebik@mis.mpg.de

Viaceré kombinatorické optimalizačné problémy na grafoch sú, vzhľadom k početným aplikáciam, skúmané aj na rôznych špeciálnych podtriedach grafov; napríklad na priesečníkových grafoch istých geometrických objektov v $\mathbb{R}^d$. Medzi najviac skúmané patria problémy na priesečníkových grafoch množín (jednotkových) gúľ, alebo množín d-rozmerných intervalov.

Náš príspevok sa zaoberá viacerými kombinatorickými problémami na množinách d-rozmerných intervalov, t.j. s osami rovnobežne orientovaných d-rozmerných obdĺžnikov, pre fixované d. Ako prototyp spomedzi skúmaných problémov možno zmieniť problém maximálnej nezávislej množiny: pre danú množinu $\mathcal{R}$ pozostávajúcu z n d-rozmerných intervalov v $\mathbb{R}^d$ nájsť čo najväčšiu podmnožinu $\mathcal{R}^* \subseteq \mathcal{R}$ po dvoch disjunktných obdĺžnikov.

Aj v tomto geometrickom kontexte problém maximálnej nezávislej množiny je NP-ťažký pre každé fixované $d \geq 2$. Najlepšie známe polynomiálne aproximačné algoritmy nájdu približné riešenie, ktoré od optimálneho môže byť horšie o multiplikatívny aproximačný faktor $\lceil \log_2 n \rceil^{d-1}$. Existencia, resp. neexistencia polynomiálnej aproximačnej schémy bola donedávna otvoreným problémom. Tak ako na jednej strane špeciálna geometrická štruktúra inštancií problému pomáha vytvoriť lepšie aproximačné algoritmy než pre všeobecné grafy, táto dodatočná štruktúra na druhej strane spôsobuje, že dolné odhady a dôkazy aproximačnej zložitosti sú omnoho ťažšie a vyžadujú celkom nové prístupy.

V tomto príspevku popíšeme generickú metódu ako ukázať aproximačnú zložitosť (presnejšie, neexistenciu polynomiálnej aproximačnej schémy) pre celý rad kombinatorických optimalizačných problémov na množinách d-rozmerných obdĺžnikov, pre každé fixované $d \geq 3$.

[1] Tato přednáška je založena na společné práci s Jankou Chlebíkovou.

Je ťažké nájsť skoro minimálnu dominujúcu množinu v grafe?

Janka Chlebíková[1]
FMFI UK, Mlynská Dolina, 842 48 Bratislava
E-mail: chlebikova@fmph.uniba.sk

Problém nájsť dominujúcu množinu minimálnej veľkosti v grafe patrí medzi klasické grafové optimalizačné problémy. Skúmajú sa tiež varianty problému s dominujúcou množinou nezávislou, súvislou, alebo spĺňajúcou nejaké iné dodatočné vlastnosti. Takéto problémy vznikajú napríklad v distribuovaných sieťach, kde je treba nájsť najmenší počet centier v sieti tak, že každý vrchol je „blízko“ aspoň jedného centra.

V príspevku budú prezentované prehľadne výsledky týkajúce sa NP-ťažkosti polynomiálnej aproximácie pre varianty problémov dominujúcich množín v rôznych triedach grafov, napríklad v grafoch ohraničeného maximálneho stupňa alebo v orientovaných grafoch. Pre väčšinu problémov dominujúcich množín ukážeme, že dosiahnuť podstatne lepšiu aproximáciu, akú dosahujú známe algoritmy, je už NP-ťažké. Najväčšiu hodnotu takú, že dosiahnuť menší aproximačný faktor je už NP-tažké, voláme „kritický faktor“ pre problém.

Problém minimálnej dominujúcej množiny súvisí s problémom množinového pokrývania. Vzhľadom k tejto súvislosti, niektoré aproximačné algoritmy, či výsledky o NP-ťažkosti polynomiálnej aproximácie platiace pre množinové pokrývanie, môžu byť použité i pre niektoré problémy s dominujúcimi množinami. Toto bude ukázané na príklade všeobecných grafov a grafoch ohraničeného maximálneho stupňa. Ukážeme, že problém minimálnej nezávislej dominujúcej množiny je úplne odlišný v grafoch ohraničeného stupňa, podobne ako vo všeobecných grafoch.

Pre grafy malého stupňa určíme explicitné odhady kritického faktoru pre rôzne varianty problémov dominujúcich množín. V orientovaných grafoch s ohraničeným vnútorným alebo vonkajším stupňom dokážeme dolný odhad kritického faktoru, ktorý takmer dosahuje známy horný odhad approximačného faktoru. Dosiahnute výsledky budú aplikované na zlepšenie hodnoty kritického faktoru iných známych problémov, ako je problém maximálneho indukovaného párovania, alebo problém kostry s maximálnym počtom listov.

[1] Tato přednáška je založena na společné práci s Miroslavem Chlebíkem.

Verifikace počítačových systémů (teoretické aspekty)

Petr Jančar
Katedra informatiky FEI VŠB-TU, 17. listopadu 15, 708 33 Ostrava
E-mail: petr.jancar@vsb.cz

V přednášce plánuji načrtnout stručný přehled o historii a současných trendech v oblasti formální verifikace počítačových systémů.

Okruhy, kterých se dotkneme, zahrnují

- dokazování (matematických) vět (theorem proving)
- modální a temporální logiky, μ-calculus
- ověřování modelu (model checking)
- ověřování (behaviorálních) ekvivalencí, speciálně bisimulační ekvivalence
- analýza nekonečně stavových systémů
- systémy reálného času, pravděpodobnostní systémy

Přiblížíme rovněž několik idejí vybraných důkazů, včetně autorových výsledků z oblasti Petriho sítí.

Poznámka. K přednášce plánuji připravit prezentaci v elektronické formě. Příslušný pdf-soubor bude k dispozici na http://www.cs.vsb.cz/jancar.

Složitost nalezení vyrovnaného uspořádání vrcholů grafu

Jan Kára[1]
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: kara@kam.mff.cuni.cz

V přednášce se budeme zabývat problémem nalezení vyrovnaného uspořádání vrcholů grafu. Přesněji chceme minimalizovat součet přes všechny vrcholy v, z rozdílu mezi počtem levých a pravých sousedů v. Tento problém motivovaný kreslením grafů byl nedávno formulován T. Biedl a spoluautory. Ukážeme, že problém je NP-těžký pro rovinné grafy s maximálním stupněm čtyři, čímž zesílíme původní výsledek T. Biedl a dořešíme tím otázku složitosti problému pro grafy s omezenými stupni (pro grafy s maximálním stupněm tři existuje polynomiální algoritmus). Rovinnost grafů v důkazu NP-těžkosti navíc umožňuje aplikovat náš výsledek na pravoúhlé kreslení grafů. Dále ukážeme, že problém zůstane NP-těžký i pro 5-regulární grafy. Na druhou stranu uvedeme polynomiální algoritmus umožňující nalézt uspořádání vrcholů s nevyvážeností menší než pevně daný parametr a umožňující rozhodnout, zda má daný multigraf se sudými stupni „téměř vyvážené“ uspořádání.

[1] Tato přednáška je založena na společné práci s Honzou Kratochvílem a David R. Woodem.

Obmedzenia na kontrapríklady pre hypotézu o 5-toku

Martin Kochol
MÚ SAV, Štefánikova 49, 814 73 Bratislava 1
E-mail: kochol@savba.sk

Nech A označuje aditívnu abelovskú grupu. Hovoríme že daný graf má *nikde nulový A-tok*, ak jeho hranám možeme priradiť orientácie a nenulové hodnoty grupy A tak, že pre každý vrchol grafu je súčet hodnôt hrán do vrchola vchádzajúcich rovný súčtu hodnôt hrán z vrchola vychádzajúcich. *Hypotéza o* 5*-toku* od Tutta predpokladá, že každý graf bez mostov má nikde nulový $\mathbb{Z}_5$-tok. Nech $\overline{G}$ označuje kontrapríklad na túto hypotézu s najmenším počtom vrcholov. Je známe, že $\overline{G}$ je 3-regulárny graf.

Nech G je graf s jediným vrcholov v stupňa $n \geq 2$ a všetkými ostatnými vrcholami stupňa 3. Označme $C = \{e_1, \ldots, e_n\}$ množinu hrán incidentných s vrcholom v a zvoľme orientáciu grafu G takú, že všetky hrany z množiny C sú orientované smerom k v. Ak φ je nikde nulový $\mathbb{Z}_5$-tok v G, označme $\varphi(C) = (\varphi(e_1), \ldots, \varphi(e_n))$. Zrejme $\varphi(C) \in S_n = \{(s_1, \ldots, s_n);\ s_1, \ldots, s_n \in \mathbb{Z}_5 \setminus \{0\},\ s_1 + \cdots + s_n = 0\}$. Pre ľubovoľné $s \in S_n$ nech $F_{G,C}(s)$ označuje počet nikde nulových $\mathbb{Z}_5$-tokov φ v G takých že $\varphi(C) = s$.

Rozklad $P = \{Q_1, \ldots, Q_r\}$ množiny $\{1, \ldots, n\}$ nazývame *vlastným* ak $|Q_1|, \ldots, |Q_r| \geq 2$. Navyše hovoríme, že P a $s = (s_1, \ldots, s_n) \in S_n$ sú *kompatibilné*, ak $\sum_{i \in Q_j} s_i = 0$ pre $j = 1, \ldots, r$. Nech $P_{n,1}, \ldots, P_{n,p_n}$ sú všetky vlastné rozklady množiny $\{1, \ldots, n\}$. Pre ľubovoľné $s \in S_n$ označme $\chi_n(s)$ binárny vektor $(c_{s,1}, \ldots, c_{s,p_n})$ taký, že $c_{s,i} = 1$ ($c_{s,i} = 0$) ak $P_{n,i}$ je (nie je) kompatibilný s s $(i = 1, \ldots, p_n)$. Dokázali sme, že pre ľubovoľný graf G existuje vektor $x \in \mathbb{Z}^{p_n}$ taký, že pre každé $s \in S_n$ $F_{G,C}(s) = x \cdot \chi_n(s)$. Ako dôsledok tohoto tvrdenia vieme dokázať že $\overline{G}$ je cyklicky hranovo 6-súvislý.

Označme $H = G - v$, $S_H = \{s \in S_n; F_{G,C}(s) > 0\}$, a nech V_H je lineárny obal $\{\chi_n(s); s \in S_H\}$ v $\mathbb{R}^{p_n}$. Nech V_n je lineárny obal $\{\chi_n(s); s \in S_n\}$ v $\mathbb{R}^{p_n}$. Dokázali sme, že ak $V_H = V_n$, potom H nemôže byť podgrafom $\overline{G}$. Nech C_n označuje kružnicu dĺžky n. Za použitia počítačov sme doká zali že $V_{C_n} = V_n$ pre $n \leq 8$. Preto $\overline{G}$ má obvod aspoň 9.

Porovnávání podobných řetězců: obtížnost a aproximace

Petr Kolman[1]
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: kolman@kam.mff.cuni.cz

Porovnávání řetězců je jedním ze základních problémů informatiky, s aplikacemi v celé řadě rozmanitých oblastí jako jsou zpracování textů, komprese dat, ochrana počítačových sítí či výpočetní biologie. V této přednášce se budeme věnovat problému z poslední oblasti, problému nejmenšího společného dělení řetezců. Jednotlivá písmena zde reprezentují geny a problém porovnává podobnost dvou genových sekvencí. Problém úzce souvisí s tzv. tříděním pomocí překlápění.

Dělení řetězce A je posloupnost řetězců $\mathcal{P} = (P_1, P_2, \ldots, P_m)$, zvaných *bloky*, jejichž spojení je rovno řětezci A. Je-li $\mathcal{P}$ dělení řetězce A a $\mathcal{Q}$ dělení řetězce B, řekneme, že dvojice $\langle \mathcal{P}, \mathcal{Q} \rangle$ je *společné dělení* A a B, jestliže $\mathcal{Q}$ je permutací $\mathcal{P}$. Problém *nejmenšího společného dělení řetězců* (MCSP) je najít společné dělení A a B s nejmenším počtem bloků. Omezenou verzi problému, ve které se každé písmeno vyskytuje v každém z řetězců nejvýšše k-krát, označujeme k-MCSP.

V přednášce se budeme věnovat obtížnosti problému a několika aproximačním algoritmům.

[1] Tato přednáška je založena na společné práci s Avrahamem Goldsteinem, Jie Zheng, Markem Chrobakem a Jiřím Sgallem.

Obvody konstantní hloubky: hradla vs. hrany

Michal Koucký[1]
MÚ AV ČR a CWI Amsterdam
E-mail: M.Koucky@cwi.nl

Booleovské obvody slouží jako obecný výpočetní model pro počítání Booleovských funkcí $f : \{0,1\}^n \to \{0,1\}$. Booleovské obvody sestávají z *hradel*, která počítají elementární Booleovské funkce jako AND, OR a MOD-q, a *hran*, které přenášejí výstupy z jedněch hradel na vstupy jiných hradel. (Obvod by měl být acyklický.) Mimo to obvod počítající funkci $f(x) : \{0,1\}^n \to \{0,1\}$ obsahuje n *vstupních hradel*, kterým je vždy na začátku výpočtu přiřazena hodnota vstupu x. Za výstup celého obvodu je považována hodnota jednoho vybraného hradla. Každý obvod tak počítá Booleovskou funkci hodnot svých vstupních hradel. Zároveň se dá snadno ukázat, že každá Booleovská funkce se dá počítat pomocí Booleovského obvodu. Fundamentální otázka výpočetní složitosti je, jak velké obvody jsou potřeba na počítání konkrétních Booleovských funkcí.

V případě obvodů, kde každé hradlo může mít neomezený počet vstupů, nastává otázka, zda za velikost obvodu považovat počet jeho hradel nebo počet jeho hran. Lze si představit situaci, že pro každou funkci $f : \{0,1\}^n \to \{0,1\}$, která se dá počítat obvodem s m hradly, kde $m \geq n$, lze nalézt obvod s m' hranami, kde $m' \leq cm$, pro nějakou univerzální konstantu c. Snadným početním argumentem se však dá ukázat, že tato situace nenastává. Tedy počet hradel a počet hran jsou různé míry. Nalézt však posloupnost konkrétních funkcí, pro které by byly tyto dvě míry alespoň n a lišily se více než konstanta-krát, byl dlouhodobě otevřený problém.

V této přednášce ukážeme takové funkce pro obvody konstantní hloubky (AC^0, $AC^0[q]$, ACC^0). K důkazu nám poslouží nová metoda analýzy komunikace v Booleovských obvodech. Tato metoda spolu s dalšími metodami nám pak též umožňuje podat přesnou (netriviální) charakterizaci regularních jazyků počítatelných obvody AC^0 a ACC^0 sestávajícími z lineárního počtu hran.

[1] Tato přednáška je založena na společné práci s P. Pudlákem a D. Thérienem.

Lokálně konzistentní CSP

Daniel Kráľ[1]
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: kral@kam.mff.cuni.cz

Instance Constraint Satisfaction Problem (CSP) je k-konzistentní, pokud každých k podmínek (constraints) lze naráz splnit. Pro jazyk Π, definujeme $\rho_k(\Pi)$ jako maximální frakci podmínek, které lze splnit v každé k-konzistentní instanci nad jazykem Π. Během přednášky se zaměříme lokálně konzistentní CSP s Booleaovskými jazyky Π a jazyky Π tvořenými jednou binární relací (nad libovolně velkou množinou).

Pokud je Π je Booleavský jazyk, lze limitu $\rho_\infty(\Pi) := \lim_{k\to\infty} \rho_k(\Pi)$ vyjádřit jako minimum jistého funkcionálu na konvexním obalu konečně mnoha polynomů odvozených od jazyka Π. Na základě těchto výsledků, navrhneme (pro pevný jazyk Π) robustní deterministický algoritmus, který v čase lineárním ve velikosti vstupu a $1/\varepsilon$ buď nalezne nekonzistentní množinu podmínek (velikosti omezené funkcí ε) nebo pravdivostní ohodnocení splňující frakci alespoň $\rho_\infty(\Pi) - \varepsilon$ všech podmínek.

Pro jazyky tvořené jednou binární relací, jsou problémy CSP ekvivalentní hledání homomorfismu ze vstupního orientovaného grafu G do pevného cílového orientovaného grafu H. Instance odpovídající grafu G je k-konzistentní, pokud každý podgraf grafu G s nejvýše k hranami je homomorfní H. V tomto případě určíme $\rho_k(H)$ pro všechny grafy H s alespoň jednou orientovanou kružnicí. Dále ukážeme, že $\lim_{k\to\infty} \rho_k(H) = 1$, pokud H má stromovou dualitu. V takovém případě též navrhneme lineární algoritmus, který pro zadaný graf G buď nalezne homomorfismus z téměř celého grafu G do H nebo identifikuje podgraf G omezené velikosti, který není homomorfní H.

[1] Tato přednáška je založena na společné práci s Manuelem Bodirskym, Zdeňkem Dvořákem a Ondrou Pangrácem.

O jednoduchých jazykových rovnicích

Michal Kunc
University of Turku, 20014 Turku, Finsko
E-mail: kunc@math.muni.cz

Díky tomu, že bezkontextové jazyky je možné s výhodou definovat jako složky nejmenších řešení systémů explicitních polynomiálních rovnic, tedy rovnic s operacemi sjednocení a zřetězení, existuje dnes již rozsáhlá teorie zabývající se vlastnostmi těchto systémů. Zcela jiná je však situace v případě implicitních jazykových rovnic, o jejichž vlastnostech nebylo donedávna známo téměř nic. Asi nejdiskutovanějším problémem týkajícím se implicitních rovnic je otázka regularity jejich maximálních řešení. Záměrem přednášky je prezentovat nejnovější výsledky výzkumu, jehož cílem je zjistit, které typy systémů jazykových rovnic a nerovnic mají všechna maximální řešení regulární, bez ohledu na to, jaké regulární konstanty obsahují.

Je známo několik zajímavých tříd systémů, jejichž maximální řešení jsou regulární, přestože tyto systémy obsahují i neregulární konstanty a jiné než regulární výrazy. Kromě pozitivních výsledků, které lze získat přímou konstrukcí konečných automatů rozpoznávajících řešení, předvedeme i výsledky využívající faktu, že regulární jazyky jsou právě jazyky nahoru uzavřené vzhledem k nějakému monotónnímu dobrému kvaziuspořádání volného monoidu.

Na druhou stranu uvedeme příklady velmi jednoduchých systémů rovnic nad regulárními jazyky, jejichž největší řešení mohou být značně komplikovaná, v některých případech dokonce nemusejí být rekurzívně vyčíslitelná. V posledních letech se pozornost soustředila především na rovnice tvaru $XL = LX$, přičemž otázka, zda největší jazyk komutující s daným regulárním nebo konečným jazykem je vždy regulární, formulovaná Conwayem v roce 1971, čekala na negativní zodpovězení více než 30 let.

Podrobnější přehled nejnovějších výsledků lze nalézt v článku: M. Kunc, Simple language equations, *Bulletin EATCS* **85**, 81–102, 2005, který je rovněž k dispozici na http://www.math.muni.cz/~kunc/math/math.html.

Jak dlouhá může být alternující cesta spojující body na kružnici?

Jan Kynčl[1]
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: kyncl@kam.mff.cuni.cz

Na kružnici je dáno n modrých a n červených bodů. Lomenou čáru p s vrcholy v daných bodech nazveme *alternující cestou*, pokud každé dva sousední vrcholy na p mají různou barvu a p sama sebe nikde neprotíná. Označme $l(n)$ maximální číslo takové, že v každé zadané konfiguraci existuje alternující cesta délky aspoň $l(n)$. Na přednášce naznačíme důkaz dolního odhadu $l(n) > n + c\sqrt{\frac{n}{\log n}}$ a konstrukci konfigurací, v nichž neexistuje alternující cesta delší než $\frac{4}{3}n + c'\sqrt{n}$.

[1] Tato přednáška je založena na společné práci s Jánosem Pachem a Gézou Tóthem.

Grupové barvení a grupová vybíravost jsou Π_2^P-úplné

Pavel Nejedlý[1]
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: bim@kam.mff.cuni.cz

Grupové barvení (group coloring) je duální koncept ke grupové souvislosti (group connectivity), která je zobecněním nikde nenulových toků (nowhere-zero flows): máme-li Abelovskou grupu A a graf G, řekneme, že G je A-obarvitelný právě tehdy když pro každou orientaci jeho hran a každé označení hran grafu prvky grupy $\varphi : E(G) \to A$ existuje označení (obarvení) vrcholů grafu prvky grupy $c : V(G) \to A$ tak, že pro každou orientovanou hranu uv platí, že $c(v) - c(u) \neq \varphi(uv)$. Nejmenší k takové, že daný graf G je A-obarvitelný pro libovolnou Abelovskou grupu A řádu alespoň k, se nazývá grupová barevnost grafu G (group chromatic number). Spojením grupové barevnosti a vybíravosti grafů dostáváme grupovou vybíravost grafů: máme-li graf G, Abelovskou grupu A a zobrazení $L : V(G) \to \mathcal{P}(A)$, které každému vrcholu G přiřazuje množinu povolených barev, řekneme, že graf G je A-obarvitelný ze seznamů L právě tehdy když pro každou orientaci jeho hran a každé označení hran grafu prvky grupy $\varphi : E(G) \to A$ existuje obarvení vrcholů grafu prvky grupy $c : V(G) \to A$ tak, že pro každou orientovanou hranu uv platí, že $c(v) - c(u) \neq \varphi(uv)$, a zároveň platí, že barva vrcholu v je v seznamu $L(v)$. Graf je A-ℓ-vybíravý (A-ℓ-choosable), pokud je A-obarvitelný z libovolných seznamů L takových, že seznam přiřazený každému vrcholu má alespoň ℓ prvků.

V práci se zabýváme výpočetní složitostí určení grupové barevnosti a grupové vybíravosti grafů. Dokazujeme, že rozhodnutí, zda daný graf je A-ℓ-vybíravý, je řešitelné v polynomiálním čase pro $\ell = 1, 2$ a Π_2^P-úplné pro $\ell \geq 3$. Dále ukazujeme, že složitost určení, zda grupová barevnost daného grafu je nejvýše k, je obdobná: problém je řešitelný v polynomiálním čase pro $k = 1, 2$ a Π_2^P-úplný pro $k \geq 3$.

[1] Tato přednáška je založena na společné práci s Danielem Kráľem.

Algoritmus pro cyklickou souvislost kubických grafů

Ondřej Pangrác[1]
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: pangrac@kam.mff.cuni.cz

Cyklická (hranová) souvislost byla jako grafový paramentr poprvé zmíněna P. G. Taitem v roce 1880. Cyklický hranový řez je takový hranový řez, který od sebe odděluje dvě kružnice. Pokud graf není souvislý a alespoň dvě jeho komponenty obsahují kružnici, potom je cyklickým řezem prázdná množina hran. Cyklická souvislost grafu je definována jako velikost nejmenšího cyklického řezu. Poznamenejme, že některé grafy nemají žádný cyklický řez, například stromy (nemají žádnou kružnici) nebo grafy K_4, K_5, $K_{3,3}$ a W_n (nemají disjukní kružnice).

Podobně jako obvyklá vrcholová a hranová souvislost, snaží se i cyklická souvislost postihnout určitým způsobem míru souvislosti grafu. Pro grafy s omezenými stupni a speciálně pro grafy kubické je obvyklá souvislost omezená a není tedy v některých aplikacích tím správným popisem souvislosti grafu. V takovém případě může být cyklická souvislost vhodnou náhradou pojmu souvislosti.

V příspěvku představíme dva algoritmy pro určení cyklické souvislosti kubických grafů, první běžící v čase $O(n^3 \log n)$ a druhý v čase $O(n^2 \log^2 n)$. Oba algoritmy není obtížné implementovat a jejich návrh neobsahuje žádné „skryté velké konstanty“ a jsou tedy vhodné pro praktické použití.

[1] Tato přednáška je založena na společné práci s Z. Dvořákem, J. Károu a D. Kráľem.

Ověřování modelů s využitím abstrakce

Radek Pelánek[1]
FI MU Brno, Botanická 68a, 602 00 Brno
E-mail: xpelanek@fi.muni.cz

Ověřování modelů (model checking) je úspěšná metoda formální verifikace, která se již používá i v průmyslu. Tato metoda je založena na procházení celého stavového prostoru daného modelu a je tedy použitelná pouze pro modely s konečně mnoha stavy. Abychom mohli použít tuto metodu i pro nekonečně-stavové systémy, je potřeba použít abstrakce. Pomocí abstrakce získáme konečně stavový model, který pak můžeme ověřovat standartním způsobem. Hlavní otázky, které potřebujeme řešit jsou:

- Jak volit abstrakci, aby abstrahovaný systém měl stejné vlastnosti jako původní systém?
- Lze abstrakce hledat mechanicky?

Přednáška poskytne stručný úvod do využití abstrakcí při metodě ověřování modelů, přičemž se zaměříme zejména na abstrakce vhodné pro ověřování softwaru (abstrakce založené na predikátech) a pro ověřování systémů s reálným časem (abstrakce založené na zónách).

[1] Tato přednáška je založena na společné práci s Gerdem Behrmannem, Patricií Bouyer, Kimem G. Larsenem, Corinou Pasarean, Willem Visserem.

Problémy kolem polygon-circle grafů

Martin Pergel[1]
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: perm@kam.mff.cuni.cz

Průnikové grafy se často používají k popisu geometrických konstelací, především v rovině. Pro množinový systém S definujeme průnikový graf G tak, že každé množině přiřadíme vrchol grafu a dva vrcholy jsou spojeny hranou, právě když odpovídající množiny mají neprázdný průnik. Význam průnikových grafů je dán kupříkladu tím, že na některých třídách grafů jsou v polynomiálním čase řešitelné různé problémy obecně NP-těžké. Navíc (opět prakticky motivován kupříkladu návrhem destiček plošných spojů) vyvstává problém, zda zadaný graf má určitou geometrickou reprezentaci. To vede na problém rozpoznání určité třídy průnikových grafů.

Předmětem této přednášky budou zejména grafy reprezentovatelné polygony vepsanými do kružnice známé jako Polygon-circle či Spider-grafy, krátce PC-grafy a různé podtřídy. Zejména nás budou zajímat třídy grafů majících PC-reprezentaci pomocí k-úhelníků, kde k je pevně zadané číslo (případně závisí na n). Položíme si otázku, kolikaúhelníky potřebujeme k reprezentaci PC-grafu s n vrcholy. Formálně definujeme $\mathrm{cmp}(n)$=min k, že každý PC-graf s n vrcholy je průnikový graf k-úhelníků. Ukážeme, že $\mathrm{cmp}(n) = n - \log n + o(\log n)$. Dále ukážeme, že je NP-těžké rozhodnout, zda lze zadaný PC-graf reprezentovat pomocí k-úhelníků pro pevné $k \geq 3$ a dokonce i pro $k = cn$, kde $0 < c < 1$ je konstanta.

O třídě PC-grafů je známo, že je skoro-perfektní, problém maximální kliky a nezávislé množiny je polynomiálně řešitelný (i pro vážené případy) a mnoho dalších věcí. Řada algoritmů se ale opírá o určitou (zadanou) PC-reprezentaci, jejíž nalezení (poté co již 15 let nebyl publikován slíbený algoritmus dokazující polynomialitu) je znovu považováno za otevřený problém. NP-úplnost nalezení PC-reprezentace pomocí k-úhelníků vrhá na PC-grafy nové světlo a ukazuje, že ač třída PC-grafů může být polynomiálně rozpoznatelná, minimálně ukrývá nekonečně mnoho tříd, jejichž rozpoznání je NP-úplné. V každém případě je NP-úplné najít optimální reprezentaci PC-grafu.

[1] Tato přednáška je založena na společné práci s Honzou Kratochvílem.

Rozšířené procesové přepisovací systémy: dosažitelnost a vyjadřovací síla

Vojtěch Řehák[1]
FI MU Brno, Botanická 68a, 602 00 Brno
E-mail: rehak@fi.muni.cz

Procesové přepisovací systémy (Process Rewrite Systems – PRS) jsou formalismem pro modelování nekonečně stavových systémů. Termy PRS odpovídají stavům systému, jednotlivé přepisovací kroky korespondují výpočetním či komunikačním akcím modelovaného systému. PRS lze rozšířit o konečně stavovou jednotku umožňující řídit přepisování, avšak toto tzv. 'stavové' rozšíření PRS má u řady relevantních tříd plnou Turingovskou sílu, a tedy z hlediska automatizované verifikace není adekvátní.

V této prezentaci se zaměřujeme na procesové přepisovací systémy rozšířené o konečně stavovou jednotku, jejíž přechodová funkce podléhá restrikcím inspirovaným teorií slabých (weak) konečných automatů.

Klasifikujeme PRS třídy podle jejich vyjadřovací síly vzhledem k silné bisimulaci a dokazujeme jejich vzájemné vztahy, a to vzhledem k dříve definovaným rozšířením i k třídám (nerozšířených) procesových přepisovacích systémů. Konkrétně v této prezentaci zmíníme i výsledek ukazující, že třída Petriho sítí je vzhledem k silné bisimulaci vlastní podtřídou třídy stavově rozšířených PA procesových algeber.

Stěžejní část tvoří prezentace rozhodnutelnosti problému dosažitelnosti pro procesové přepisovací systémy rozšířené o slabou konečně stavovou jednotku, doplněná o důsledky a aplikace tohoto výsledku.

[1] Tato přednáška je založena na společné práci s Mojmírem Křetínským a Janem Strejčkem.

Obtížnost testování ekvivalence konečně stavových systémů

Zdeněk Sawa
FEI VŠB-TU Ostrava, 17. listopadu 15, 708 33 Ostrava
E-mail: Zdenek.Sawa@vsb.cz

Jedním z důležitých typů problémů týkajících se verifikace systémů je testování ekvivalence systémů (equivalence checking). Pro účely verifikace jsou systémy modelovány jako tzv. přechodové systémy, což jsou v podstatě orientované grafy, jejichž vrcholy tvoří všechny možné stavy daného systému (přičemž množina těchto stavů může být i nekonečná), a jejichž hrany představují možné přechody mezi těmito stavy. Instancí problému testování ekvivalence je dvojice přechodových systémů (resp. popisy těchto systémů) a otázka je, zda jsou tyto dva systémy ekvivalentní vzhledem k nějakému určitému typu ekvivalence. V literatuře byla navržena celá řada různých ekvivalencí. Van Glabbeek uspořádal tyto ekvivalence do hierarchie nazývané linear time/branching time spectrum. Nejjemnější ekvivalencí v tomto spektru je bisimulační ekvivalence a nejhrubší trace ekvivalence.

V příspěvku budou prezentovány dva výsledky týkající se výpočetní složitosti testování ekvivalence v případě konečně stavových systémů. Oba tyto výsledky ukazují obtížnost problému testování ekvivalence, a oba platí pro celou třídu problémů zahrnující všechny ekvivalence ve van Glabbeekově spektru, protože oba ve skutečnosti platí pro libovolnou relaci, která leží mezi bisimulační ekvivalencí a trace preorder.

Prvním výsledkem je důkaz PTIME-obtížnosti testování libovolné relace ležící mezi bisimulační ekvivalencí a trace preorder v případě konečně stavových systémů, jež jsou dány explicitně (tj. jako seznam explicitně vyjmenovaných stavů a přechodů). Tento důkaz je společnou prací s Petrem Jančarem a byl publikován na konferenci Sofsem'02.

Technika požitá ve výše zmíněném důkazu PTIME-obtížnosti byla poté v modifikované podobě použita v důkazu EXPTIME-obtížnosti testování ekvivalence v případě, že systémy jsou dány jako paralelní kompozice konečně stavových systémů, které komunikují pomocí sdílených akcí, a kde některé akce mohou být „skryty". Tento výsledek opět platí pro libovolnou relaci mezi bisimulační ekvivalencí a trace preorder, a dokazuje, že platí domněnka, kterou vyslovil A. Rabinovich (1997). Pro zjednodušení důkazu byl zaveden nový model nazvaný reaktivní lineárně omezený automat, který umožňuje snadno

odvodit EXPTIME-obtížnost i pro jiné podobné typy systémů, jako například pro 1-bezpečné Petriho sítě. Důkaz EXPTIME-obtížnosti byl publikován na konferenci Concur'03.

Infinite-State Processes: Bisimulation Games and Hardness Results

Jiří Srba
BRICS, Aalborg University, Fr. Bajersvej 7B, 9220 Aalborg, Dánsko
E-mail: srba@brics.dk

Porovnávání nekonečně stavových systému vzhledem k sémantickým ekvivalencím je aktivní výzkumná oblast, která během posledních deseti let přinesla řadu originálních technik a výsledků uplatnitelných i v jiných oborech informatiky. V této přednášce se podíváme na hierarchii nekonečně stavových procesů definovaných pomocí tzv. systémů na přepisování termů, elegantního formalismu pro jednotný popis systémů se sekvenční a paralelní kompozici. Tato hierarchie obsahuje například zásobníkové automaty a Petriho sítě. My budeme porovnávat procesy nadefinované ve vybraných formalismech vzhledem k silné a slabé bisimulační ekvivalenci. Zvláště se zaměříme na charakterizaci těchto ekvivalenci pomoci bisimulačních her mezi útočníkem a obráncem, které umožňují jednoduché a intuitivní pochopení i značně složitých konstrukcí. Představíme si rovněž novou techniku nazvanou „obráncova volba“ a ukážeme si její využití při dokazování dolních složitostních odhadů a nerozhodnutelnosti bisimulačních problemů pro vybrané třídy z hierarchie systémů na přepisování termů.

Geometrické reprezentace grafů

Jan Štola
KAM MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: Jan.Stola@mff.cuni.cz

Budu se zabývat otázkou, které grafy mají geometrickou reprezentaci daného typu. Zaměřím se na viditelnostní a ortogonální reprezentace a na třídu úplých grafů a grafů omezené barevnosti. Mimo jiné ukáži vylepšení horního a dolního odhadu maximální velikosti úplného grafu s viditelnostní reprezentací pomocí pravidelných n-úhelníků a odhadu maximální barevnosti takové, že všechny grafy nejvýše této barevnosti mají trojrozměrnou ortogonální reprezentaci s hranami bez ohybu.

Rozhodnutelnost pravděpodobnostní bisimulace pro nekonečně-stavové pravděpodobnostní systémy

Oldřich Stražovský[1]
FI MU Brno, Botanická 68a, 602 00 Brno
E-mail: strazovsky@fi.muni.cz

Na přednášce bude dokázáno, že pravděpodobnostní bisimulace je rozhodnutelná pro pravděpodobnostní rozšíření BPA a BPP procesů. Pro normované podtřídy pravděpodobnostních BPA a BPP procesů budou prezentovány algoritmy, jejichž časová složitost je polynomiální. Dále bude dokázáno, že pravděpodobnostní bisimulace mezi pravděpodobnostními zásobníkovými automaty a konečně-stavovými pravděpodobnostními systémy je rozhodnutelná v exponenciálním čase. Pokud je počet kontrolních stavů zásobníkového automatu omezen fixní konstantou, pak je tato časová složitost polynomiální.

[1] Tato přednáška je založena na společné práci s Tomášem Brázdilem a Antonínem Kučerou.

Objemy trojrozmerných uložení grafov

Ľubomír Török[1]
MÚ SAV, Severná 5, 974 01 Banská Bystrica
E-mail: torok@savbb.sk

V prezentovanej práci sa zaoberáme štúdiom trojrozmerných uložení hyperkocky v dvoch zaužívaných modeloch: v modeli s jednou aktívnou vrstvou a všeobecnom modeli. Tento problém je možné chápať ako kreslenie grafu v trojrozmernom priestore a bol uvedený na konferencii Graph Drawing 2003. V modeli s jednou aktívnou vrstvou je vrchol stupňa d reprezentovaný štvorcom o strane d. Je uložený v spodnej vrstve trojrozmernej mriežky. Vo všeobecnom modeli je vrchol stupňa d reprezentovaný kockou o strane d a na jeho pozíciu v mriežke nie sú kladené žiadne obmedzenia. Pre obidva modely ukážeme všeobecné dolné hranice, ktoré dávajú do súvisu objem uloženia s parametrom cutwidth. Potom ukážeme konštrukcie horných hraníc, ktoré sú v oboch prípadoch presné na prvorádový člen. Konkrétne máme $VOL_{1-AL}(Q_{\log N}) = \frac{2}{3}N^{\frac{3}{2}} \log N + O(N^{\frac{3}{2}})$, pre párny $\log N$ a $VOL(Q_{\log N}) = 0.54N^{\frac{3}{2}} + O(N^{\frac{4}{3}} \log N)$, pre $\log N$ delitelný tromi. Model s jednou aktívnou vrstvou môže byť jednoducho rozšírený na model s dvomi aktívnymi vrstvami, ktorým vylepšujeme výsledky prezentované na Graph Drawing 2003. Zovšeobecnením tohto postupu získavame koncepciu pre konštrukciu optimálnych objemov uložení homogénnych produktov grafov. Ako výsledok dostávame asymptoticky optimálne objemy uložení produktov, kde faktor grafy tvoria niektoré známe siete, ako napríklad Cube connected cycles, Butterfly, star graph, De Bruijn a iné. Toto zovšeobecnenie je analógia podobnej práce pre dvojrozmerné uloženia grafov, s použitím odlišnej techniky a bolo prezentované na konferencii SOFSEM 2005.

[1] Tato přednáška je založena na společné práci s Imrichom Vrťom.

Jobshop a programování s omezujícími podmínkami

Petr Vilím
KTIML MFF UK, Malostranské náměstí 25, 118 00 Praha
E-mail: vilim@kti.mff.cuni.cz

Rozvrhovací úlohy patří mezi poměrně staré problémy informatiky, přesto však pro mnoho z nich dodnes neznáme efektivní algoritmy. Důvodem je většinou NP-úplnost těchto úloh. Ukázkovým příkladem takového problému je tzv. *jobshop*.

Úkolem je v co nejkratším čase vyrobit n výrobků. Výroba jednoho výrobku se však skládá z m kroků, každý krok vyžaduje jiný stroj. Pořadí kroků a jejich doba jsou předem dány, liší se však podle výrobku. Stroj nelze použít pro více než jeden výrobek současně, zpracování jednoho výrobního kroku nelze přerušovat.

Programování s omezujícími podmínkami je jeden z nejúspěšnějších postupů používaných při řešení podobných problémů. Pro uživatele jde o poměrně jednoduchý postup, protože problém popíše pouze jako seznam vlastností, které musí řešení mít (tzv. *omezující podmínky*). Systém pak pomocí metody zvané *propagace podmínek* omezuje prostor řešení. Pokud není řešení nalezeno ihned, nastupuje backtracking či další metody prohledávání prostoru řešení, přičemž propagace podmínek dále slouží jako prostředek ořezávání prohledávacího stromu.

Jádrem systému jsou tedy propagační algoritmy, které jsou šité na míru jednotlivým podmínkám. V případě jobshopu se jedná zejména o *unary resource* podmínku, která zaručuje, že daný stroj bude použit přesně podle zadání. Propagační algoritmy musí být dostatečně chytré, aby byly schopny omezit prohledávací prostor. Musí však být také velmi rychlé, protože budou během prohledávání prostoru řešení mnohokrát opakovány.

V příspěvku budou naznačeny některé propagační algoritmy, které můžeme použít pro rozvrhovací problémy.

Abstraktní regulární model checking

Tomáš Vojnar[1]
FIT VUT v Brně, Božetěchova 2, 612 66 Brno
E-mail: vojnar@fit.vutbr.cz

Model checking (MC) je v současné době obvykle přijímán jako moderní a mocná technika pro formální verifikaci požadovaných vlastností konečně stavových systémů. V praxi se ovšem setkáváme s celou řadou systémů, jejichž různé rysy vyžadují práci s nekonečnými stavovými prostory. Příčinou může být např. práce s neomezenými datovými strukturami (jako jsou zásobníky, fronty, čítače apod.) nebo parametrizace zkoumaných systémů. Jednou z technik, které byly relativně nedávno navrženy jako zobecnění MC pro práci s takovými systémy, je tzv. *regulární model checking* (RMC).

Při použití RMC jsou konfigurace zkoumaných systémů reprezentovány jako slova nad vhodnou abecedou, případně nekonečné množiny konfigurací jsou reprezentovány konečnými automaty a přechody mezi konfiguracemi jsou reprezentovány jako konečné převodníky. *Množina dosažitelných stavů* je pak konstruována pomocí opakované aplikace převodníků na doposud známou množinu dosažitelných stavů. Alternativně je rovněž možno zkonstruovat *relaci dosažitelnosti* zkoumaného systému, a to opakovaným skládáním převodníků reprezentujících jeden krok systému. Ovšem vzhledem k tomu, že řešený problém není obecně rozhodnutelný, popsaný výpočet nemusí skončit. Aby byla zajištěna konečnost výpočtu v co největším počtu praktických případů, byla navržena řada technik *akcelerujících* popsaný výpočet – např. techniky založené na tzv. rozšiřování (widening), na slučování některých stavů automatů s ohledem na historii jejich vzniku apod. Většina z těchto technik se ovšem snaží o výpočet přesné množiny dosažitelných stavů, případně přesné relace dosažitelnosti.

Snaha o výpočet přesné množiny dosažitelných stavů, resp. relace dosažitelnosti, však vede na stavovou explozi v podobě práce s extrémně velkými automaty. Znalost přesné množiny dosažitelných stavů, resp. přesné relace dosažitelnosti, nemusí být přitom nutná k ověření požadovaných vlastností zkoumaného systému. Právě této skutečnosti využívá *abstraktní regulární model checking* (ARMC), který kombinuje RMC s technikou abstrahuj-ověř-zjemni (abstract-check-refine). Cílem je akcelerovat výpočet pomocí abstrakce nad

[1] Tato přednáška je založena na společné práci s Ahmedem Bouajjanim a Peterem Habermehlem.

automaty (resp. převodníky), která k danému automatu vrací automat, jenž reprezentuje nadmnožinu jazyka původního automatu. Abstrakční funkce je přitom konstruována automaticky postupným zjemňováním na základě vylučování falešných protipříkladů k dokazovaným vlastnostem, jež plynou pouze z aplikace příliš hrubé abstrakce.

V původním návrhu ARMC byly navrženy dva základní mechanismy abstrakce automatů založené na slučování některých jejich stavů. Stavy byly slučovány na základě porovnání jejich jazyků s tzv. *predikátovými jazyky* nebo na základě porovnání jejich *jazyků vět až do určité omezené délky*. V poslední době pak byl tento koncept rozšířen o tzv. *lokální abstrakci*, založenou na zkoumání a zobecňování struktury jednotlivých slov přítomných v jazyce abstrahovaných automatů.

ARMC byl v prototypové implementaci úspěšně aplikován na reprezentanty celé řady různých typů systémů (parametrické sítě procesů, systémy se zásobníkem, s frontou, čítači apod.). V poslední době pak byl navržen obecný způsob reprezentace *programů s dynamickými datovými strukturami s jedním ukazatelem na následníka* (seznamy, kruhové seznamy apod.) pomocí konečných automatů a převodníků a ARMC byl úspěšně aplikován při verifikaci různých procedur pracujících s takovými strukturami.

V současné době je připravována řádná implementace ARMC. Dále probíhá výzkum možností aplikace ARMC nad systémy s nelineární strukturou stavů (např. stromy), se stavy reprezentovanými nekonečnými slovy a také výzkum možností zobecnění ARMC na práci s neregulárními množinami stavů.

Stochastické pakovací problémy

Jan Vondrák[1]
MIT, Cambridge, MA, USA
E-mail: vondrak@math.mit.edu

„Pakovací problémy“ zahrnují širokou třídu optimalizačních úloh, kde je cílem nalézt řešení maximalizující zisk a přitom splňující jisté „pakovací podmínky“. Tyto problémy lze formulovat pomocí celočíselného programování, kde všechny nerovnosti jsou typu $\sum a_{ij}x_j \leq b_i$ nebo $x_j \geq 0$. (Třída PIP: Packing Integer Programs.) Příkladem je problém batohu, maximální klika, maximální párování v grafech a hypergrafech, a další.

V této přednášce se zaměřím na přibližná řešení těchto úloh a především na vliv náhodnosti na vstupu na možnost efektivní aproximace. Popíšu „stochastické pakovací problémy“ a dva základní přístupy k jejich řešení: „adaptivní“ a „neadaptivní“. Ukazuje se, ze existuje zajímavá (ne zcela pochopená) souvislost mezi aproximovatelností adaptivních řešení pomocí neadapativních, a mezi aproximovatelností odpovídajících deterministických úloh v polynomiálním čase. Vysvětlím naše výsledky a hypotézy o adaptivitě a aproximovatelnosti. Pokud zbyde čas, zmíním se také o souvislosti mezi stochastickými pakovacími problémy a třídou PSPACE.

[1] Tato přednáška je založena na společné práci s Brianem Deanem a Michelem Goemansem.