

SOUČASNÉ TRENDY TEORETICKÉ INFORMATIKY

26.–27. června 2015, Praha

Z. Dvořák (ed.)

Úvodní slovo

Konferenci Současné trendy teoretické informatiky pořádá Institut Teoretické Informatiky každé dva roky pravidelně již od roku 2003. Cíl a účel konference zůstává stejný: Rádi bychom vytvořili domácí fórum pro kvalitní výsledky českých a slovenských informatiků, které byly prezentovány na prestižních mezinárodních konferencích. Publikování na mezinárodních výběrových konferencích (např. APPROX, CAV, CCC, COCOON, CP, CONCUR, ESA, FOCS, GD, ICALP, ISAAC, LATIN, LICS, MFCS, RANDOM, SODA, STACS, STOC, SWAT nebo WADS), kde bývá troj- a vícenásobný počet zaslaných příspěvků vůči počtu přijatých příspěvků, měřítkem kvality a úspěšnosti vědecké práce.

Na konferenci STTI 2015 jsme pozvali ty mladé české a slovenské informatiky, kteří uspěli v této konkurenci v posledních letech 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 45 mladých českých a slovenských informatiků, z nichž 24 se konference zúčastní. Hlavní přednášku přednese Stanislav Živný, který aktuálně působí na University of Oxford ve Velké Británii. Velmi nás těší nebývale velký zájem o konferenci mezi českou a slovenskou odbornou veřejností, o kterém svědčí fakt, že na konferenci se zaregistrovala řada účastníků, kteří na ní nemají příspěvek.

Konference STTI 2015 se uskuteční ve dnech 26.–27. června 2015 v Praze v budově MFF UK na Malostranském náměstí. Konference je organizována Informatickým ústavem University Karlovy za podpory grantů CE-ITI¹, CORES (ERC CZ) a CMI (UNCE). Rád bych poděkoval paní Giorgadze, paní Milštainové a zvláště pak hlavnímu organizátorovi Zdeňku Dvořákovi za jejich pomoc při organizaci konference.

Jaroslav Nešetřil

¹Projekt P202/12/G061 Grantové agentury ČR.

Obsah

| | |
|---------------------------------------|---|
| Úvodní slovo | 1 |
| Obsah | 3 |
| Hlavní přednáška konference | 5 |
| Program konference | 7 |

Abstrakty příspěvků

| | |
|--|----|
| Stanislav Böhm: Verifikace programů využívajících MPI | 11 |
| Kateřina Böhmova: Rozvrhování intervalů | 12 |
| Jakub Bulín: Redukce problémů CSP na \mathbb{H} -barvení orientovaných grafů | 13 |
| Zdeněk Dvořák: Velké nezávislé množiny v rovinných grafech bez trojúhelníků | 14 |
| Vojtěch Forejt: Benevolentní syntéza kontrolerů pro pravděpodobnostní systémy | 15 |
| Peter Franěk: Robustní invarianty nelineárních soustav | 16 |
| Radoslav Fulek: Testovanie planarity stromov s tromi klastrami | 17 |
| Jakub Gajarský: Existenciální logika prvního řádu na číselně usporiadaných množinách omezené šířky | 18 |
| Robert Galian: Souostrovní řešitelnosti pro problém splnitelnosti omezení | 19 |
| Milan Hladík: Míra řešitelnosti a neřešitelnosti lineárních soustav | 21 |
| Jan Hladký: Pakování a krásné obarvování stromů pomocí Rödlova hryzání | 22 |
| Pavel Hubáček: Racionální argumenty | 23 |
| Martin Chmelík: Co je rozhodnutelné o paritních POMDP | 24 |
| Mikoláš Janota: O důkazové složitosti kvantifikovaných boolských formulí | 25 |
| Pavel Klavík: Algoritmické aspekty regulárních nakrytých grafů | 26 |
| Tereza Klímová: Dědičné vlastnosti permutací jsou silně testovatelné | 27 |
| Jan Křetínský: Od LTL k deterministickým automatům bez Safry | 28 |
| Tomáš Masopust: Od XML k separovatelnosti regulárních jazyků | 29 |
| Tomáš Petříček: Coeffects: Teorie kontextově závislých programovacích jazyků | 30 |

| | |
|---|----|
| Diana Piguet: Hypotéza Loeblova, Komlóse a Sósové | 31 |
| Ondřej Suchý: Řešení MULTIŘEZU rychleji než 2^n | 32 |
| Martin Tancer: Vnořitelnost do 3-sféry je rozhodnutelná | 33 |
| Lukáš Vokřínek: Úvod do výpočetní homotopické teorie | 34 |
| Lenka Zdeborová: Spektrální spása | 35 |

Hlavní přednáška konference

Optimální algoritmy pro vážené CSPčka

Stanislav Živný

University of Oxford

standa.zivny@cs.ox.ac.uk

V této přednášce se budeme zabývat diskrétním optimalizačním problémem které se dají formulovat jako tzv. vážená CSPčka. Konkrétně se budeme věnovat algoritmům a výpočetní složitosti pro optimální minimalizaci lokálně definovaných funkcí z konečné pevné množiny do množiny racionálních čísel rozšířených o nekonečno.

Nechť D , nazývaná doména, je libovolná konečná množina. Zdefinujeme $\overline{\mathbb{Q}} := \mathbb{Q} \cup \{\infty\}$. Nechť Γ je libovolná konečná množinu funkcí tvaru $f : D^{a(f)} \rightarrow \overline{\mathbb{Q}}$, kde $a(f)$ je arita (tj. počet argumentů) funkce f . V příspěvku se budeme zabývat výpočetní složitosti minimalizace funkcí tvaru $f(x_1, \dots, x_n) = \sum_{i=1}^q f_i(x_{i_1}, \dots, x_{i_{a(f_i)}})$, kde $f_i \in \Gamma$ a $x_{i_j} \in \{x_1, \dots, x_n\}$ pro všechna $1 \leq i \leq q$ a $1 \leq j \leq a(f_i)$.

Předneseme výsledky jež charakterizují kdy se dají použít základní relaxace lineárního programování a také rozšířené relaxace založené na Sherali-Adams metodách. Také předneseme důsledky těchto výsledků, které dávají klasifikace různých tříd problémů, a ukazují že různé relaxace jsou optimálními algoritmy, tedy, vyřeší vše co se dá.

Založeno na několika článcích publikovaných v ICALP'15, SICOMP'15, a JACM'15+.

Příspěvek obsahuje výsledky společné práce s J. Thapperem.

Program konference

Program STTI'15

pátek 26.6.

8:30 začátek registrace

9:00 Milan Hladík: *Míra řešitelnosti a neřešitelnosti lineárních soustav*

9:25 Lukáš Vokřínek: *Úvod do výpočetní homotopické teorie*

9:50 Peter Franěk: *Robustní invarianty nelineárních soustav*

10:15 přestávka

10:35 Jakub Gajarský: *Existenciální logika prvního rádu na číselně uspořádaných množinách omezené šířky*

11:00 Lenka Zdeborová: *Spektrální spása*

11:25 Robert Ganian: *Souostroví řešitelnosti pro problém splnitelnosti omezení*

11:50 Jakub Bulín: *Redukce problémů CSP na \mathbb{H} -barvení orientovaných grafů*

12:15 oběd

14:00 Stanislav Živný: *Optimální algoritmy pro vážené CSPčka*

14:50 Ondřej Suchý: *Řešení MULTIREZu rychleji než 2^n*

15:15 Zdeněk Dvořák: *Velké nezávislé množiny v rovinných grafech bez trojúhelníků*

15:40 přestávka

16:00 Stanislav Böhm: *Verifikace programů využívajících MPI*

16:25 Vojtěch Forejt: *Benevolentní syntéza kontrolerů pro pravděpodobnostní systémy*

- 16:50** Pavel Hubáček: *Racionální argumenty*
- 17:15** Martin Chmelík: *Co je rozhodnutelné o paritních POMDP*
- 17:40** Mikoláš Janota: *O důkazové složitosti kvantifikovaných boolských formulí*
- 18:05** Tomáš Petříček: *Coeffects: Teorie kontextově závislých programovacích jazyků*
- 19:30** večere

sobota 27.6.

- 9:00** Jan Křetínský: *Od LTL k deterministickým automatům bez Safry*
- 9:25** Tomáš Masopust: *Od XML k separovatelnosti regulárních jazyků*
- 9:50** Kateřina Böhmova: *Rozvrhování intervalů*
- 10:15** přestávka
- 10:35** Martin Tancer: *Vnořitelnost do 3-sféry je rozhodnutelná*
- 11:00** Diana Piguet: *Hypotéza Loeblova, Komlóse a Sósové*
- 11:25** Tereza Klimošová: *Dědičné vlastnosti permutací jsou silně testovatelné*
- 11:50** Jan Hladký: *Pakování a krásné obarvování stromů pomocí Rödlova hřezání*
- 12:15** oběd
- 13:30** Radoslav Fulek: *Testovanie planarity stromov s tromi klastrami*
- 13:55** Pavel Klavík: *Algoritmické aspekty regulárních nakrytých grafů*

Všechny přednášky se budou konat v posluchárně S5 v budově Matematicko-fyzikální fakulty UK na Malostranském náměstí.

Abstrakty příspěvků

Verifikace programů využívajících MPI

Stanislav Böhm

IT4Innovations Národní superpočítačové centrum, VŠB-TUO

E-mail: stanislav.bohm@vsb.cz

MPI (Message Passing Interface) je standard definující rozhraní pro komunikaci procesů v prostředí distribuované paměti, který je široce používán v oblasti superpočítačů. Přestože je toto rozhraní relativně jednoduché, vývoj aplikací nad MPI nemusí být triviální. MPI programy mohou velice snadno obsahovat špatně reprodukovatelné chyby. Nedeterministické chování aplikací je způsobeno jak paralelním výpočtem, tak také samotným MPI, které implementacím umožňuje v případě některých operací nedeterministické chování (z důvodu maximální efektivity na různém hardware). Pro podporu vývoje aplikací nad MPI existuje celá škála pokročilých nástrojů, většinou se však jedná o nástroje sledující aktuální běh programu. Nástroje poskytující pokrytí všech nedeterministických chování a tedy jistý druh formální verifikace nejsou příliš rozšířeny. Cílem prezentace je představit současný stav a problémy spojené s formální verifikací MPI programů a možnosti dalšího vývoje v této oblasti.

Rozvrhování intervalů

Kateřina Böhmova

ETH Zürich

E-mail: `katerina.boehmova@inf.ethz.ch`

Studujeme problém plánování a rozvrhování úloh na pracovní stroje. Je dáno n úloh a m strojů a každá úloha má na každém stroji přesně definovaný jeden souvislý interval (časový interval, který je třeba pro zpracování dané úlohy na daném stroji). Pro naplánování úlohy je nutné zvolit jeden z jejích intervalů, přičemž intervaly vybrané na stejném stroji se nesmí protínat. Cílem je naplánovat co nejvíce úloh.

Pokud $m = 1$, tedy máme-li jen jeden stroj, jedná se o klasický problém ekvivalentní problému barvení intervalového grafu. Tento problém lze optimálně vyřešit jednoduchým hladovým algoritmem v čase $O(n \log n)$.

Naproti tomu jsme ukázali, že pokud je strojů více, problém rozhodnout, zda je možné naplánovat všechny úlohy, je NP-úplný již v různých jednoduchých případech. Konkrétně jsme ukázali NP-úplnost problému již v případech kdy všechny intervaly končí ve stejném okamžiku (také známé jako Just-in-time plánování) a tím jsme vyřešili otevřený problém (Sung a Vlach, J. Sched., 2005). Dále jsme ukázali NP-úplnost pro variantu, ve které jsou všechny intervaly stejné délky a intervaly příslušící jedné úloze mají společný průsečík, a pak pro variantu s intervaly stejné délky a pouhými třemi stroji.

Ukázali jsme, že problém maximalizovat počet naplánovaných úloh je NP-těžký již pro případ se dvěma stroji a intervaly shodné délky. Pro problém se dvěma stroji (a intervaly libovolné délky) jsme navrhli deterministický $2/3$ -aproximační algoritmus.

Příspěvek obsahuje výsledky společné práce s Yannem Disserem, Matúšem Mihalákem a Peterem Widmayerem.

Redukce problémů CSP na \mathbb{H} -barvení orientovaných grafů

Jakub Bulín

Jagiellonian University in Kraków

E-mail: jakub.bulin@gmail.com

Mnoho rozhodovacích problémů z různých oblastí informatiky (teorie databází, umělá inteligence, rozvrhování, teorie grafů aj.) lze přirozeně vyjádřit v jazyce Problému splňování omezení (CSP): cílem je přiřadit proměnným hodnoty z předem dané konečné domény, za přítomnosti omezení (constraints) na možná ohodnocení k -tic proměnných (constraint scopes). Tento problém je NP-úplný, pozornost je proto soustředěna na hledání podproblémů o menší složitosti.

Přirozenou restrikcí jsou CSP s pevnou šablonou, kde fixujeme doménu a konečně mnoho relací, které mohou vystupovat v omezeních. Známa dichotomická hypotéza Feder a Vardiho říká, že třída problémů CSP s pevnou šablonou neobsahuje NP-intermediární problémy. Velký pokrok v této oblasti přinesl tzv. algebraický přístup k CSP: složitost a další vlastnosti CSP závisí na tzv. polymorfismech šablony, a dokonce jen na rovnicové teorii univerzální algebry z nich sestavené.

Feder a Vardi mimo jiné ukázali, že každé CSP s pevnou šablonou je polynomiálně ekvivalentní problému \mathbb{H} -barvení pro nějaký orientovaný graf \mathbb{H} . Představíme jednoduchou variantu takové konstrukce, která dává redukci v logspace a zachovává většinu relevantních rovnicových vlastností polymorfismů. Jedním z důsledků je, že hypotézy charakterizující CSP problémy řešitelné v L, NL a P stačí dokázat pro \mathbb{H} -barvení orientovaných grafů.

Velké nezávislé množiny v rovinných grafech bez trojúhelníků

Zdeněk Dvořák

Matematicko-fyzikální fakulta UK v Praze

E-mail: rakdver@iuuk.mff.cuni.cz

Každý rovinný graf na n vrcholech, který neobsahuje trojúhelníky, má nezávislou množinu velikosti alespoň $(n + 1)/3$ a tento dolní odhad je těsný. Popíšeme algoritmus, který pro zadaný rovinný graf G na n vrcholech bez trojúhelníků a pro zadané celé číslo $k \geq 0$ rozhodne, zda G má nezávislou množinu velikosti alespoň $(n + k)/3$ v čase $2^{O(\sqrt{k})}n$. Tento problém je tedy efektivně řešitelný, je-li parametrizován hodnotou k . Jako důsledek tvrzení používaného v důkazu správnosti tohoto algoritmu také ukážeme, že pro nějaké $\varepsilon > 0$ má každý rovinný graf obvodu 5 na n vrcholech nezávislou množinu velikosti alespoň $n/(3 - \varepsilon)$.

Příspěvek obsahuje výsledky společné práce s Matthiasem Mníchem.

Benevolentní syntéza kontrolerů pro pravděpodobnostní systémy

Vojtěch Forejt

University of Oxford

E-mail: vojfor@cs.ox.ac.uk

Tento článek navrhuje nové algoritmy pro syntézu kontrolerů v pravděpodobnostních systémech popsanych jako hry dvou hráčů. Naším cílem je navrhnout robustní kontroler, tak aby nepředepisoval pro každý stav konkrétní akci, kterou hráč může použít, ale místo toho dával na výběr co největší množinu akcí tak, že jakýkoli výběr akcí z množiny zajistí splnění cíle. Tento přístup může najít uplatnění například v měnicích se prostředích ve kterých se nějaké akce mohou stát nedostupnými.

Nejdříve formalizujeme pojem benevolence tak, že každé akci je přiřazena číselná hodnota (penále), kterou kontroler zaplatí za zakázání akce. Podle způsobu, jakým se následně ceny zakázaných akcí interpretují, definujeme buď „statické penále“ nebo „dynamické penále“. Cílem kontroleru je potom zajistit splnění cíle při minimalizaci statického/dynamického penále.

Naše výsledky zahrnují složitostní klasifikaci problémů a implementaci, která za pomoci lineárního programování umožňuje vypočítat, zda pro danou instanci problému existuje benevolentní kontroler.

Robustní invarianty nelineárních soustav

Peter Franěk

Ústav informatiky Akademie věd ČR

E-mail: franek@cs.cas.cz

Uvažujme soustavu rovnic $f(x) = 0$ kde $f : X \rightarrow \mathbf{R}^n$ je spojitá funkce na nějakém topologickém prostoru X . Pro studium robustních vlastností řešení definujme pro každé $r > 0$ množinu

$$Z_r(f) = \{g^{-1}(0) : \|g - f\|_\infty \leq r, g \text{ spojité}\}.$$

Tuto množinu a vlastnosti společné všem jejím prvkům (invarianty) chceme studovat pomocí spočitatelných vlastností funkce f . Příkladem takového invariantu je neprázdnost každé množiny v $Z_r(f)$. Pro f po částech lineární je $\emptyset \in Z_r(f)$ algoritmicky rozhodnutelné za podmínky $\dim X < 2n - 2$. Je však přirozené hledat další invarianty řešení a jejich robustnost.

V literatuře byl diskutován koncept tzv. well grup: jde o grupu homologických tříd které mají všechny množiny v $Z_r(f)$ v určitém smyslu společné. Výpočet well grup byl znám pouze v případech $\dim X = n$ nebo $n = 1$ (skalární funkce). V nedávné práci jsme vylepšili status well grup a ukázali jsme, jak spočítat její význačnou podgrupu, která v řadě případů splývá s celou well grupou. Na druhé straně jsme ukázali, že well grupy netvoří úplnou sadu invariantů řešení rovnic. Lze je nahradit posloupností určitých kohomotopických grup, které lze vizualizovat metodami perzistentní homologie a které jsou vizualizovat metodami perzistentní homologie a které jsou teoreticky úplnější a mají lepší výpočetní status. Konkrétně, tyto grupy lze spočítat přesně pokud $\dim X < 2n - 2$ a aproximovat v ostatních případech.

Testovanie planarity stromov s tromi klastrami

Radoslav Fulek

IST Austria

E-mail: radoslav.fulek@gmail.com

Planárny graf $G = (V, E)$ s vrcholmi rozdelenými do k navzájom disjunktných množín $V_1 \uplus \dots \uplus V_k = V$ je c-planárny (c-planar), ak existuje planárny graf $G' = (V, E')$ taký, že $E \subseteq E'$ a indukovaný podgraf $G'[V_i]$ je súvislý pre každé $i = 1, \dots, k$.

Dokážeme, že testovanie c-planárnosti je riešiteľné v polynomiálnom čase pre stromy s vrcholmi rozdelenými do troch skupín. Analogický výsledok bol dopsiaľ dosiahutý pre cykly.

Existenciálna logika prvého rádu na čiastočne usporiadaných množinách obmedzenej šírky

Jakub Gajarský

Fakulta informatiky Masarikovy university

E-mail: xgajar@fi.muni.cz

V prednáške sa budeme venovať problému overovania platnosti formulí logiky prvého rádu na čiastočne usporiadaných množinách. Tento problém začali skúmať Bova, Ganian a Szeider, ktorí ukázali jeho efektívnu riešiteľnosť vzhľadom k rôznym parametrom (LICS 2014). Jedným z ich hlavných výsledkov je algoritmus, ktorý rieši problém overovania platnosti existenciálnych prvorádových formulí v čase $f(|\phi|).n^{g(w)}$, kde n je veľkosť čiastočne usporiadanej množiny a w jej šírka (šírka čiastočne usporiadanej množiny je veľkosť jej najväčšej podmnožiny takej, že všetky jej prvky sú vzájomne neporovnateľné).

Prednáška bude zameraná na dvojaké vylepšenie tohto výsledku: (1) Náš algoritmus beží v čase $f(|\phi|, w).n^2$ a (2) naše dôkazy sú priamočiarejšie a jednoduchšie oproti vyššie spomenutému výsledku. Prezentované boli publikované na konferencii ISAAC 2014.

Souostroví řešitelnosti pro problém splnitelnosti omezení

Robert Ganian

Vienna University of Technology

E-mail: rganian@gmail.com

Problém splnitelnosti omezení (CSP) je centrálním problémem v informatice, jenž zobecňuje velkou řadu problémů v teorii i v praktických aplikacích. Jedna z hlavních výzkumných linií se zabývá identifikací tříd vstupů, kde lze CSP vyřešit v polynomiálním čase; těmto třídám se často říká „ostrovy řešitelnosti“. Jedním z hlavních způsobů jak definovat ostrovy řešitelnosti pro CSP je omezení relací, které se v omezeních vyskytují, na fixní množinu; těmto množinám říkáme *jazyk omezení*. Schaeferův proslulý teorém (STOC 1978) identifikuje všechny ostrovy řešitelnosti ve vztahu k řešitelným jazykům omezení pro booleovské hodnoty proměnných. V nedávné době se objevily plné charakterizace všech ostrovů řešitelnosti pro CSP a jeho počítačací verzi #CSP v rámci tzv. konzervativních jazyků omezení, tedy jazyků obsahujících všechny unární relace (Bulatov – TOCL 2011, JACM 2013).

Tento příspěvek se zabývá obecným nedostatkem všech výše zmíněných pozitivních výsledků pro CSP a #CSP: lze je aplikovat pouze, pokud všechna omezení patří do jediného řešitelného jazyka (obecně platí, že sjednocení dvou řešitelných jazyků omezení není řešitelné). Ukážeme, že tento nedostatek lze překonat, pokud máme určitou formu kontroly nad tím, jak mezi sebou omezení z různých řešitelných jazyků interagují. K tomuto účelu využíváme tzv. *silných backdoorů* (Williams et al. IJCAI 2003), což je množina proměnných, kde po jakékoli instanciaci těchto proměnných padne vstup do ostrova řešitelnosti. Konkrétně nás zajímají silné backdoory do tzv. roztroušených tříd vstupů, tedy takových, které sestávají ze vstupů, jejichž souvislá část patří do alespoň jednoho ostrova řešitelnosti; takovéto roztroušené třídy si lze představit jako „souostroví řešitelnosti“. Hlavní překážkou tohoto přístupu je nalezení silného backdooru do takto definovaného souostroví o velikosti k ; jakmile je nalezen, je možné zkusit všechny instanciaci proměnných v (malém) backdooru a poté aplikovat příslušné polynomiální algoritmy pro jednotlivé ostrovy řešitelnosti. Náš hlavní výsledek je algoritmus, který v CSP nebo #CSP instanci s n proměnnými najde silný backdoor do roztroušené třídy (charakterizované seznamem konečných konzervativních jazyků omezení) v čase $f(k)n^{O(1)}$, nebo pozná, že takový backdoor v dané instanci neexistuje.

Příspěvek obsahuje výsledky společné práce s M.S. Ramanujanem a Stefanem Szeiderem.

Míra řešitelnosti a neřešitelnosti lineárních soustav

Milan Hladík

Matematicko-fyzikální fakulta UK v Praze

E-mail: `hladik@kam.mff.cuni.cz`

Metoda totálních nejmenších čtverců spočívá v nalezení nejmenší perturbace matice dané soustavy lineárních rovnic tak, aby soustava byla řešitelná. V principu můžeme uvažovat minimum v jakékoli maticové normě. My se zaměříme na hledání minima v Čebyševově normě. Ukážeme, že problém je nejenom NP-těžký, ale dokonce i neaproximovatelný. Na druhou stranu, při pevném počtu regresorů se stává polynomiálním.

Výše zmíněný problém dále zobecníme na obecné soustavy rovnic a nerovnic, a kromě míry řešitelnosti budeme uvažovat i míru neřešitelnosti. Pro všechny tyto případy ukážeme explicitní formulaci problému jako optimalizační úlohy a klasifikujeme v rámci P/NP hierarchie. Zmíníme vztahy mezi různými měrami a jednoduché horní odhady. Na závěr ponecháme zobecnění na neuniformní perturbace.

Pakování a krásné obarvování stromů pomocí Rödlova hryzání

Jan Hladký

Matematický ústav Akademie věd ČR

E-mail: honzahladky@gmail.com

Domněnky Gyarfáse (1976) a Ringela (1963) říkají, že úplný graf se dá perfektně napakovat v podstatě libovolným souborem stromů. Pakováním tady rozumíme rozmístění, ve kterém se stromy nepřekrývají na hranách. Samozřejmě, nutná podmínka je, že celkový počet hran není větší než počet hran v daném úplném grafu (a domněnky se liší v další specifikaci). Ve společné práci s Böttcherovou, Piguetovou, a Tarazem jsme dokázali asymptotickou verzi zobecnění obou těchto domněnek pro stromy s omezeným stupněm.

Ve společné práci s Adamaszkovou, Adameszkem, Allenem a Grosu jsem dokázali asymptotickou verzi tzv. Graceful Tree conjecture publikované Rosou v roce 1967. Otázka v této domněnce je, zda-li existuje speciální - „krásné“ - obarvení vrcholů daného stromu.

Důkazy obou tvrzení jsou alespoň na základní úrovni podobné. Analyzujeme randomizovaný algoritmus, který daný úkol (pakování nebo barvení) zpracovává v dávkách; tomuto přístupu se říká Rödl nibble.

Racionální argumenty

Pavel Hubáček

Weizmann Institute of Science

E-mail: `pavel.hubacek@weizmann.ac.il`

Racionální důkazy, nedávno představené Azarem a Micalim (STOC 2012), jsou variantou interaktivních důkazových systémů mezi dokazujícím (prover) a ověřujícím (verifier), v nichž dokazující není ani čestný (honest) ani zlomyslný (malicious), ale chová se racionálně. Výhodou racionálních důkazových systémů oproti jejich klasickým verzím je extrémně nízká komunikační složitost, a také minimální výpočetní složitost pro ověřující stranu. Azar a Micali prokázali potenciál racionálních důkazů na příkladě protokolu pro #SAT s lineární časovou složitostí pro ověřující stranu.

V mé přednášce uvedu model racionálních důkazových systémů a poté představím racionální argumenty, nový koncept, jenž kromě předpokladu racionality také omezuje výpočetní sílu dokazujícího. Guo, Hubáček, Rosen a Vald (ITCS 2014) ukázali, že pro třídu NC1 (jazyků rozeznatelných logspace-uniformními obvody logaritmické hloubky) existují racionální argumenty, jež vyžadují pouze minimální interakci mezi dokazujícím a ověřujícím a současně umožňují ověřujícímu pracovat v sublineárním (polylogaritmickém) čase. Racionální argumenty se tak nabízejí jako alternativa pro ověřitelné delegování výpočtů (zejména v kontextu cloud computing). Přestože poskytují slabší záruku (jež však může být dostačující v praktických situacích) než klasické důkazové systémy, dosahují mnohé v porovnání s předešlými protokoly pro ověřitelné delegování výpočtů; jsou jednoduché, staví na klasických předpokladech výpočetní složitosti, poskytují záruku pro všechny instance a nevyžadují preprocessing.

Na závěr ukáži, že práci Guo et al. lze rozšířit pro všechny formální jazyky rozhodnutelné v polynomiálním čase. Naše nová konstrukce využívá racionální protokoly jako efektivní stavební blok v rámci klasických interaktivních důkazů. Naším hlavním příspěvkem je konstrukce racionálního protokolu pro kontrolní součet (sumcheck protocol), jenž nahrazuje klasický protokol pro kontrolní součet používaný v mnoha interaktivních důkazových systémech a umožňuje nám obejít kritický bod z hlediska časové složitosti v stávajících protokolech pro ověřitelné delegování výpočtů.

Příspěvek obsahuje výsledky společné práce s Siyao Guo, Alonem Rosenem a Margaritou Vald..

Co je rozhodnutelné o paritních POMDP

Martin Chmelík

IST Austria

E-mail: martin.chmelik@ist.ac.at

V naší práci se zajímáme o částečně pozorovatelné Markovské rozhodovací procesy (POMDP) s omega-regulárními cíli. Třída omega-regulárních jazyků rozšiřuje regulární jazyky nad konečnými slovy na jazyky nad nekonečnými slovy a je robustním specifikačním jazykem vystihujícím všechny vlastnosti, které se běžně používají při verifikaci. Paritní cíle jsou kanonickou reprezentací omega-regulárních jazyků. Kvalitativní analýza se pro dané POMDP a paritní cíl zajímá o strategii, která by zajistila splnění cíle s pravděpodobností 1 (nebo s pravděpodobností větší než 0). Zatímco kvalitativní analýza je nerozhodnutelná již pro velmi speciální případy paritních cílů, v naší práci ukazujeme rozhodnutelnost (s optimální časovou složitostí) problému kvalitativní analýzy pro POMDP se všemi paritními cíli pro konečně-stavové strategie. Dále ukazujeme optimální (exponenciální) paměťovou náročnost a ukazujeme, že problém kvalitativní analýzy s konečně stavovými strategiemi v POMDP s paritními cíli je úplný ve třídě EXPTIME. Na základě našich teoretických algoritmů také prezentujeme praktickou aplikaci našich výsledků. S pomocí nových heuristik ukazujeme, že námi prezentovaný algoritmus syntetizuje strategie pro množství dobře známých příkladů POMDP z robotiky.

O důkazové složitosti kvantifikovaných boolských formulí

Mikoláš Janota

INESC-ID

E-mail: mikolas.janota@gmail.com

Kvantifikované boolské formule (QBF) obohacují problém splnitelnosti (SAT) o kvantifikátory \exists a \forall které lze interpretovat jako zkratky pro disjunkce a konjunkci. Tímto se dostáváme z P-úplnosti do PSPACE-úplnosti. Úspěch SAT řešičů v posledním desetiletí motivuje výzkum řešičů pro QBF. Současně je nutné budovat teoreticky základ, který by nám umožnil tyto řešiče charakterizovat a porovnávat. *Teorie důkazů* se tady nabízí jako přirozený nástroj.

V současné době existuje několik různých řešičů pro QBF. Tyto řešiče lze dělit na *prohledávací* a *expanzní*. V tomto duchu můžeme zadefinovat různé důkazové kalkuly. Prohledávacím řešičům odpovídá systém *Q-rezoluce* a pro expanzní řešiče byl nedávno zaveden kalkulus $\forall\text{Exp}+\text{Res}$ (spolu s několika rozšířeními). Nabízí se otázka, který z těchto kalkulů je silnější. Ukážeme, že jsou neporovnatelné (navzájem separované), t.j. že existuje třída formulí kde jeden kalkulus vede k exponenciálně delším důkazům než druhý. Tento výsledek ukazuje na fundamentální rozdíl mezi prohledávacími a expanzními řešiči. Pro důkaz separace použijeme známé výsledky z teorie složitosti obvodů.

Algoritmické aspekty regulárních nakrytých grafů

Pavel Klavík

Matematicko-fyzikální fakulta UK v Praze

E-mail: klavik@kam.mff.cuni.cz

Velký graf G nakryvá malý graf H , pokud existuje lokálně bijektivní homomorfismus z G do H , tedy G je lokálně stejný jako H . Zabýváme se regulárním nakrytím, ve kterém je homomorfismus popsán strukturou některých symetrií grafu G . Konkrétně semiregulární podgrupou Γ grupy $\text{Aut}(G)$ takovou, že kvocient G/Γ je izomorfní H .

Zabýváme se složitostním problémem rozhodnout pro dva grafy G a H na vstupu, jestli G regulárně nakryvá H . Tento problém zobecňuje grafový izomorfismus (když velikost G a H je stejná) a testování Cayleyho grafu (pokud H je jednovrcholový graf se smyčkami a půlhranami). Naším hlavním výsledkem je existence netriviálního FPT algoritmu ve velikosti H pro případ, kdy G je rovinný. Výsledek je založen na pochopení chování regulárního nakrytí vůči 1-řezům a 2-řezům.

Dědičné vlastnosti permutací jsou silně testovatelné

Tereza Klimošová

University of Warwick

E-mail: T.Klimosova@warwick.ac.uk

Oblast *testování vlastností* (property testing) se zabývá studiem rychlých pravděpodobnostních algoritmů pro rozhodování, jestli má velký vstupní objekt testovanou vlastnost, nebo je od testované vlastnosti daleko. Takový algoritmus se nazývá *tester*. Požadujeme, aby jeho časová složitost byla konstantní vzhledem k velikosti vstupu, proto musí algoritmus pracovat pouze se znalostí malé části vstupu. Je tudíž nutné počítat s chybou, závisující na robustnosti testované vlastnosti.

Vlastnost je testovatelná, pokud pro každé $\varepsilon > 0$ existuje tester, který přečte pouze část vstupu jejíž velikost je omezena funkcí ε a nezávisí na velikosti vstupu, a s pravděpodobností alespoň $1 - \varepsilon$ správně rozhodne, že vstup má testovanou vlastnost, nebo že je ε daleko od testované vlastnosti.

Nejlépe prostudované je testování vlastností grafů. Nejvýznamnějším v této oblasti je výsledek Alona a Shapiry, kteří dokázali, že každá dědičná vlastnost grafů, t.j. vlastnost, kterou zachovávají indukované podgrafy, je testovatelná v editační vzdálenosti.

Hoppen, Kohayakawa, Moreira, Sampaio dokázali podobný výsledek pro permutace. Ukázali, že každá dědičná vlastnost permutací je slabě testovatelná, t.j., je testovatelná v obdélníkové vzdálenosti a vyslovili domněnku, že je testovatelná i v Kendallově tau vzdálenosti, která je jemnější než obdélníková vzdálenost a je považována za ekvivalent editační vzdálenosti.

Tuto domněnku jsme potvrdili. Narozdíl od algoritmu Hoppena a spol., který je založen na regulárních rozkladech permutací, je náš algoritmus založen na přímých kombinatorických argumentech a dává lepší závislost na parametrech problému.

Příspěvek obsahuje výsledky společné práce s Danem Král'em.

Od LTL k deterministickým automatům bez Safry

Jan Křetínský

afiliace

E-mail: jan.kretinsky@gmail.com

Při analýze vlastností lineárního času (LTL) u pravděpodobnostních systémů a her je často nezbytné přeložit tyto vlastnosti na deterministické automaty nad nekonečnými slovy. Tradiční přístup toho dociluje tak, že se nejprve vlastnost přeloží na nedeterministický Büchiho automat, který je následně determinizován, například Safrovou konstrukcí. V dřívější práci jsme ukázali, že některé fragmenty LTL lze přeložit na deterministické automaty přímo. Nyní pomocí odlišné konstrukce ukazujeme, jak rozšířit tento výsledek na celou LTL. Protože tento přístup je šitý na míru LTL, výsledné automaty jsou často řádově menší a tím i řádově zrychlují některé aplikace, např. ověřování pravděpodobnostních modelů.

Od XML k separovatelnosti regulárních jazyků

Tomáš Masopust

TU Dresden a Matematický ústav AV ČR

E-mail: masopust@math.cas.cz

XML Schema je jazyk pro popis XML dokumentů, který je navržen pro snadné zpracování počítačem na úkor srozumitelnosti pro člověka. To přirozeně vede ke snaze vytvořit user-friendly náhradu či rozhraní. Jednou z takových snah je i BonXai. Jde o kombinaci jednoduchosti DTD s expresivitou XML Schema, jejíž cílem je zjednodušit návrh a analýzu XML Schema Definitions (XSDs). BonXai je sada pravidel tvaru $L_i \rightarrow R_i$, kde L_i a R_i jsou regulární výrazy. XML dokument (chápán jako strom) patří do jazyka schematu, pokud pro každý uzel stromu platí, že slovo definované jeho přímými potomky patří do jazyka R_k a slovo tvořené jeho předchůdci patří do jazyka L_k . Jelikož regulární výrazy L_i jsou konstruovány z automatu vnořeného v XSD a stávající techniky transformace konečných automatů na regulární výrazy zatím negenerují výrazy srozumitelné pro člověka, omezíme se pouze na jednoduché třídy regulárních výrazů. Praktické a teoretické studie naznačují, že regulární výrazy tvaru $\Sigma^* a_1 \Sigma^* \cdots \Sigma^* a_n$, $a_i \in \Sigma$, a jejich varianty jsou vhodné a dostatečné. Nicméně, regulární výrazy takového tvaru popisující jazyky L_i jsou pouze jejich aproximace a je třeba zajistit, aby tyto aproximace byly disjunktní, což vede na problém separovatelnosti: Nechtě K a L jsou jazyky a \mathcal{F} je třída jazyků. Existuje jazyk S v \mathcal{F} takový, že S obsahuje K a je disjunktní s L ? Czerwiński et al. (2013) a Place et al. (2013) nezávisle ukázali, že problém separovatelnosti pro regulární jazyky reprezentované nedeterministickými konečnými automaty a třídu po částech testovatelných (piecewise testable) jazyků je rozhodnutelný v polynomiálním čase vzhledem k velikosti automatu. Jednoduchá metoda konstrukce po částech testovatelného separátoru a její složitost je studována v Holub et al. (2014). V přednášce budou shrnuty dosažené výsledky a související problémy.

Coeffects: Teorie kontextově závislých programovacích jazyků

Tomáš Petříček

University of Cambridge

E-mail: `tomas.petricek@cl.cam.ac.uk`

Rozvoj programovacích jazyků je často inspirován změnami v tom jakým způsobem jsou programy spouštěny. Důležitou aktuální změnou je narůstající význam *prostředí* neboli *kontextu* ve kterém programy běží, nebo ke kterému mohou přistupovat. Cílem práce na tzv. *coeffects* je navrhnout jednotné abstrakce pro programování s kontextem a verifikaci toho, jak programy ke kontextu přistupují.

V této přednášce demonstruji jak představená teorie unifikuje několik vlastností programů, které bylo dříve nutné posuzovat samostatně. Mezi tyto vlastnosti patří kontrola požadované verze platformy (např. Android) při více-platformním vývoji, kontrola přístupu ke zdrojům poskytovaným prostředím (např. GPS senzor nebo osobní data v sociálních sítích), ale také klasické problémy z teorie programovacích jazyků („liveness“ analýza proměnných nebo vlastnosti z lineární logiky a „data-flow“ programování).

V přednášce představíme hlavní výsledky prezentované ve dvou člácích (ICALP 2013 a ICFP 2014), tedy dvě varianty typovaného lambda kalkulu, které zachycují kontextuální vlastnosti programovacích jazyků. Zaměříme se zejména na syntaktické vlastnosti daných systémů, ale zmíníme i jejich teoretický model, který používá strukturu *comonad* z teorie kategorií (duální strukturu k více známým monádám).

Hypotéza Loeblo, Komlóse a Sósové

Diana Piguet

Ústav informatiky Akademie věd ČR

E-mail: piguet@cs.cas.cz

Hypotéza Loeblo, Komlóse a Sósové dává do souvislosti medián stupňů vrcholů v grafu s přítomností podstromů dané velikosti. S použitím Szemerédiho regularity lemma byla tato hypotéza dokázána pro husté grafy, ale tuto metodu nelze použít pro řídké grafy. Pomocí nově vyvinutých technik dokážeme přibližnou verzi této hypotézy pro řídké grafy.

Řešení MULTIŘEZU rychleji než 2^n

Ondřej Suchý

Fakulta informačních technologií ČVUT

E-mail: ondrej.suchy@fit.cvut.cz

MULTIŘEZ je problém, kde je zadán neorientovaný graf $G = (V, E)$ a systém párů vrcholů $\mathcal{T} = \{(s_i, t_i) \mid s_i, t_i \in V\}$, představující požadavky, a úkolem je najít množinu minimální velikosti $S \subseteq V$ tak, aby každá komponenta souvislosti grafu $G \setminus S$ obsahovala nejvýše jeden z s_i a t_i pro každý pár $(s_i, t_i) \in \mathcal{T}$. V této přednášce představíme první netriviální algoritmu pro MULTIŘEZ pracující v čase $O(1.987^n)$.

Příspěvek obsahuje výsledky společné práce s Danielem Lokshtanovem a Saketem Saurabhem.

Vnořitelnost do 3-sféry je rozhodnutelná

Martin Tancer

Matematicko-fyzikální fakulta UK v Praze

E-mail: `tancer@kam.mff.cuni.cz`

Během přednášky nastíníme důkaz, že je algoritmicky rozhodnutelné, zda lze daný 2-rozměrný simplicialní komplex (topologicky) vnořitelný do \mathbf{R}^3 . Pomocí známé redukce stačí rozhodnout vnořitelnost dané triangulované 3-variety X do trojrozměrné sféry S^3 . Hlavní krok, který umožňuje zjednodušit X a pokračovat rekurzivě, je důkaz následujícího tvrzení: Pokud je X vnořitelné do S^3 , potom také má vnoření, ve kterém má X krátký meridián, tj., esenciální křivku na hranici X , která ohraničuje disk v $S^3 \setminus X$ a jejíž délka je omezená vyčíslitelnou funkcí v počtu čtyřstěnů triangulace X .

Příspěvek obsahuje výsledky společné práce s Jiřím Matouškem, Ericem Sedgwickem a Ulim Wagnerem.

Úvod do výpočetní homotopické teorie

Lukáš Vokřínek

Masarykova univerzita v Brně

E-mail: koren@math.muni.cz

Cílem bude vysvětlit, čím se zabývá výpočetní homotopická teorie, a na vybraných výsledcích přiblížit metody, které jsme v nedávných článcích použili k řešení těchto problémů. Tyto problémy jsou specifické tím, že jsou obecně nerozhodnutelné, řešení proto existuje pouze ve „stabilních“ případech, mým druhým cílem bude tento fenomén vysvětlit.

Spektrální spása

Lenka Zdeborová

CEA/SACLAY

E-mail: lenka.zdeborova@gmail.com

Spektrální algoritmy se široce používají v oblasti analýzy dat, příkladem je například algoritmus Pagerank, který stál u zrodu vyhledávače Google, nebo metoda analýzy hlavních komponent. Tyto algoritmy jsou založené na výpočtu největších vlastních hodnot a příslušných vlastních vektorů pro matice odvozené z příslušných dat. Elementy těchto matic typicky reprezentují relace mezi různými prvky studovaného systému. V případě, že jsou tyto matice velmi řídké, t.j. počet nenulových elementů je srovnatelný s rozměrem matice, standartní spektrální metody nejsou optimální ve smyslu, že vyžadují značně více informace či méně šumu než je nezbytně nutné. Na příkladu hledání komunit v řídkých grafech odvodíme spektrální metodu, založenou na tzv. matici bez vracení, která optimality dosahuje. Zmíníme fascinující spektrální vlastnosti této matice a příklady problémů, pro které je užitečná.