SOUČASNÉ TRENDY TEORETICKÉ INFORMATIKY

10.-11. 2019, Praha

T. Klimošová (ed.)

Úvodní slovo

Konference *Současné trendy teoretické informatiky* se koná pravidelně každé dva roky 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, EUROCOMB, 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 2019 jsme pozvali 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.

Konference ze zúčastní 19 mladých českých a slovenských informatiků. Hlavní přednášku přednese Lenka Zdeborová z Institut de Physique Theorique, CEA Saclay ve Francii.

Konference STTI 2019 se uskuteční ve dnech 10.-11. června 2019 v Praze v budově MFF UK na Malostranském náměstí. Konference je organizována a podporována Katedrou aplikované matematiky a Informatickým ústavem University Karlovy a rovněž s podporou centra DIMATIA. Děkujeme také paní Milštainové za její pomoc při organizaci konference.

Jaroslav Nešetřil, Tereza Klimošová

Obsah

Hlavní přednáška konference

Statistical physics insight on computational hardness

Lenka Zdeborová
Institut de Physique Theorique, CEA Saclay
E-mail: lenka.zdeborova@gmail.com

What are the problems we can solve using a computer? is one of the very fundamental question in science. We will describe how do we use statistical physics to address this question. We will discuss what insights does physics bring to the field of algorithmic hardness and how is this insight used to develop better algorithms. We will describe examples of applications in artificial neural networks, and data clustering.

Program konference

Program STTI'19

pondělí 10. června

8:30 začátek registrace

9:00 Peter Gaži: *Proof-of-stake kryptomeny a rodina protokolov Ouroboros*

9:25 Kristina Hostáková: *Non-malleable kódy odolné vůči útočníkům s omezenou prostorovou složitostí*

9:50 Pavel Hubáček: *Implikace bezpečnosti Fiatovy-Shamirovy heuristiky pro hledání Nashova equilibria*

10:15 přestávka

10:35 Martin Koutecký: *Algoritmická teorie celočíselného programování*

11:00 Pavel Veselý: *Online rozvrhování paketů s termíny znovu a lépe*

11:25 Dušan Knop: *Férové alokace s velkým mnoostvím zdrojů*

11:50 Martin Böhm: *Online stíhání vnořených konvexních těles*

12:15 oběd

14:00 Lenka Zdeborová: *Statistical physics insight on computational hardness*

15:00 přestávka

15:30 Martin Doležal: *Strukturální uspořádání grafonů*

15:55 Matěj Konečný: *Ramseyova teorie: Na rozmezí kombinatoriky a teorie modelů*

16:20 Jakub Gajarský: *Interpretácie tried grafov s obmedzenou expanziou*

16:45 Tereza Klimošová: *Vnoření náhodného bipartitního grafu do náhodného biregulárního grafu*

19:00 večeře

úterý 11. června

9:00 Dominik Velan: *Asymptotická analýza doby terminace vector addition systémů se stavy*

9:25 Pavel Paták: *Shellovatelnost je NP-úplná*

9:50 Zuzana Patáková: *Průsečíkové struktury v rovině*

10:15 Martin Balko: *Téměř ekvidistantní množiny*

10:40 přestávka

11:10 Tomáš Peitl: *Učenie sa závislostí medzi premennými kvantifikovaných boolovských formúl*

11:35 Vojtěch Mrázek: *Přibližná ekvivalence aritmetických obvodů*

12:00 Jana Novotná: *Atomy grafů bez dvou zakázaných indukovaných podgrafů*

12:25 Tomáš Masařík: *Pakování čtvrtinových cyklů*

13:00 oběd

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

Abstrakty příspěvků

Téměř ekvidistantní množiny

Martin Balko
MFF, Univerzita Karlova
E-mail: balko@kam.mff.cuni.cz

Pro přirozené číslo d řekneme, že množina bodů P v $\mathbb{R}^d$ je téměř-ekvidistantní, pokud každá trojice bodů z P obsahuje dvojici bodů v jednotkové vzdálenosti. Jako $f(d)$ označíme maximální velikost téměř-ekvidistantní množiny bodů v $\mathbb{R}^d$. Je známo, že $f(2)7$ a $f(3) = 10$. Ukážeme nové odhady na $f(d)$ pro malé hodnoty d a odvodíme obecný horní odhad $f(d) \leq O(d^{3/2})$ a dolní odhad $f(d) \geq 2d + 4$.

Příspěvek obsahuje výsledky společné práce s Attilou Pórem, Manfredem Scheucherem, Konradem Swanepoelem, Pavlem Valtrem.

Online stíhání vnořených konvexních těles

Martin Böhm
Univerzita Brémy
E-mail: martin.boehm@uni-bremen.de

V problému Online stíhání konvexních těles je na vstupu zadán startovní bod v $\mathbb{R}^d$ a online posloupnost n konvexních těles $F_1, \ldots, F_n$. Jakmile přijde F_i, je naší povinnosti se do něj přesunout z předchozí pozice. Cílem je pak minimalizovat celkovou ušlou vzdálenost, jakmile vstup skončí.

Tento fundamentální online problém byl poprvé studován Friedmanem a Linialem (DCG 1993). Ti ukázali dolní odhad $\Omega(\sqrt{d})$ na kompetitivní poměr jakéhokoli online algoritmu, a vyřkli domněnku, že lze dosáhnout $f(d)$-kompetitivního algoritmu.

V tomto příspěvku se zaměřujeme na speciální případ tohoto problému, a to situaci, kdy následující tělesa jsou vnořená do předchozího, čili $F_1 \supset \ldots \supset F_n$. Tento případ se na první pohled nezdá fundamentálně jednodušším – ačkoli optimální trajektorie může být jen úsečka, algoritmus se musí přibližovat opatrně vůči všem možným optimálním řešením.

V tomto příspěvku předvedeme jednoduchý a pochopitelný $f(d)$-kompetitivní algoritmus pro stíháni vnořených konvexních těles v $\mathbb{R}^d$.

Na našem výsledku je jistě také důležité, že "prolomil ledy" na tomto 20 let starém problému. Na náš příspěvek na SODA 2018 odpověděly dva články:

1. Na SODA 2019 ukázali C. J. Argue, S. Bubeck, M. B. Cohen, A. Gupta a Y. T. Lee $O(d \log d)$-kompetitivní algoritmus pro náš vnořený problém;

2. Na STOC 2019 ukázali S. Bubeck, Y.T. Lee, Y. Li a M. Sellke první $f(d)$-kompetitivní algoritmus pro původní, nevnořený problém.

Příspěvek obsahuje výsledky společné práce s Nikhilem Bansalem, Markem Eliášem, Grigoriosem Koumoutsosem, S. Williamem Umboh.

Strukturální uspořádání grafonu

Martin Doležal
Matematický ústav AV ČR
E-mail: dolezal@math.cas.cz

Duležitými objekty pro studium hustých grafu jsou grafony, tj. symetrické měřitelné funkce $W\colon [0,1]^2 \to [0,1]$. Vzdálenost grafonu měříme pomocí tzv. cut-vzdálenosti, jejíž základní vlastností je kompaktnost: každá posloupnost grafonu (nebo grafu) má podposloupnost, která je konvergentní v cut-vzdálenosti. My jsme se věnovali zejména hledání souvislostí mezi cut-vzdáleností a o trošku lépe uchopitelnou slabou* konvergencí. Jako vedlejší produkt jsme obdrželi zcela nový dukaz kompaktnosti cut-vzdálenosti.

Naš přístup přirozeně vede k jistému uspořádání na grafonech, které se dá intuitivně interpretovat jako porovnávání strukturovanosti dvou grafonu. Pro každý grafon W je množina $\langle W\rangle$ všech grafonu, které jsou nejvýše stejně strukturované jako W, slabě* kompaktní. Navíc zobrazení $W \mapsto \langle W\rangle$ je vnořením prostoru grafonu s cut-vzdáleností do hyperprostoru všech slabě* kompaktních podmnožin množiny všech grafonu.

Motivováni těmito výsledky jsme dále zkoumali ruzné grafonové parametry, jejichž minimalizace (nebo maximalizace) nám dávají akumulační body v cut-vzdálenosti pro libovolnou posloupnost grafonu.

Příspěvek obsahuje výsledky společné práce s Janem Grebíkem, Janem Hladkým, Israelem Rochou, Václavem Rozhoněm.

Interpretácie tried grafov s obmedzenou expanziou

Jakub Gajarský
TU Berlin
E-mail: jakub.gajarsky@tu-berlin.de

Teória riedkych grafov zavedená Jaroslavom Nešetřilom a Patriceom Ossona de Mendezon sa ukázala veľmi užitočná z algoritmického hľadiska – parametrizované verzie mnohých NP-ťažkých algoritmických problémov je možné efektívne riešiť na veľmi všeobecných triedach (riedkych) grafov. V posledných rokoch sa ukázalo, že v niektorých prípadoch je možné rozšíriť tieto pozitívne algoritmické výsledky na husté grafy, ktoré je možné vytvoriť z riedkych grafov pomocou konštrukcie zvanej *interpretácia*. Základom týchto pozitívnych výsledkov "obrátenie" interpretácie, t.j. k zadanému hustému grafu H nájdenie riedkeho grafu G z ktorého je možné vytvoriť H pomocou interpretácie. Naším výsledom je charakterizácia tried grafov interpretovatelných v triedach grafov s obmedzenou expanziou. Táto charakterizácia je prvým krokom k nájdeniu algoritmu na obrátenie interpretácií na triedach grafov interpretovatelných v grafoch s obmedzenou expanziou.

Příspěvek obsahuje výsledky společné práce s Stephanom Kreutzerom, Jaroslavom Nešetřilom, Patriceom Ossona de Mendezon, Michalom Pilipzukom, Sebastianom Siebertzom a Szymonom Torunczykom.

Proof-of-stake kryptomeny a rodina protokolov Ouroboros

Peter Gaži
IOHK Research
E-mail: peter.gazi@iohk.io

Bitcoin a výrazná väčšina existujúcich kryptomien zakladá svoju bezpečnosť na takzvanom dôkaze vykonanej výpočtovej práce, teda "proof-of-work": účastník protokolu smie rozšíriť blockchain o ďalší blok (a získa odmenu) iba ak nájde riešenie inak zbytočného výpočtového problému, ktorý vyžaduje prehľadávanie hrubou silou. Tento princíp vedie k pretekom medzi jednotlivými účastníkmi o to, kto investuje viac výpočtového výkonu, a k znepokojivej spotrebe energie. Navyše, zjednodušene povedané, bezpečnosť celého systému je priamo úmerná takto vyplýtvanej energii, a prípadné masovejšie rozšírenie Bitcoinu by si vyžadovalo na zachovanie rovnakej bezpečnosti aj úmerný nárast spotrebovanej energie.

Možným východiskom z tejto neuspokojivej situácie je alternatívny prístup na dosiahnutie konsenzu v kontexte kryptomien, zvaný tiež "proof-of-stake". Pri tomto prístupe je právo rozširovať blockchain rozdeľované medzi účastníkov priamo úmerne ich vlastníckemu podielu na samotnej kryptomene, namiesto podielu na vynaloženej zbytočnej výpočtovej práci. Táto zdanlivo jednoduchá myšlienka je takmer taká stará ako Bitcoin samotný, ale jej dokázateľne bezpečná a efektívna realizácia sa ukázala byť netriviálna.

V tejto prednáške budem hovoriť o výhodách proof-of-stake prístupu k vytváraniu konsenzu v prostredí kryptomien, spomeniem existujúce návrhy riešení z prostredia akademickej komunity, a zameriam sa na rodinu proof-of-stake protokolov Ouroboros, na ktorej spolupracujem.

Reference

[1] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 357–388. Springer, Heidelberg, August 2017.

[2] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake

blockchain. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 66–98. Springer, Heidelberg, April / May 2018.

[3] Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 18*, pages 913–930. ACM Press, October 2018.

Non-malleable kódy odolné vůči útočníkům s omezenou prostorovou složitostí

Kristina Hostáková
TU Darmstadt
E-mail: kristina.hostakova@crisp-da.de

Dziembowski, Pietrzak a Wichs definovali non-malleable kódy v roce 2010 jako abstraktní nástroj na ochranu proti útokům na paměť kryptografických zařízení. Kódová schémata mají non-malleable vlastnost, pokud výsledkem manipulace s kódovým slovem c, odpovídající zprávě m, je kódové slovo c', které se dekóduje buď na původní zprávu m, nebo na zpravu m' zcela nesouvisející s m. Jinými slovy, porušení kódového slova informaci obsaženou v kódové slově buď vůbec nezmění, nebo ji zcela zničí. Není těžké dokázat, že žádné kódové schéma nemůže splňovat non-malleabilitu vůči třídě útoků, která obsahuje jak dekódovací, tak i kódovací algoritmus. Většina vědeckých prací v této oblasti se proto zaměřuje na navrhování non-malleable kódů pro různé třídy útoků, které neumožňují útočníkovi dekódovat kódové slovo. Tento předpoklad je však v mnoha situacích nerealistický.

V článku předneseném na CRYPTO 2017 zkoumáme se spoluautory Faustem, Mukherjee a Venturi jednu takovou situaci a uvažujeme třídu, která přirozeně zahrnuje dekódovací algoritmus (ale nikoli kódovací algoritmus). Naším cílem jsou non-malleable kódy odolné vůči útočníkům s omezenou prostorovou složitostí. Ukazuje se, že naše konstrukce, založená na kryptografickém primitivu zvaným Proof-of-Space, je odolná i vůči opakovaným útokům.

V přednášce nejprve uvedu pojem non-malleable kódů a vysvětlím, jak lze taková kódová schémata využít v kryptografii. Poté představím kódové schéma z našeho článku a načrtnu hlavní ideu důkazu o jeho odolnosti vůči útočníkům s omezenou prostorovou složitostí.

Příspěvek obsahuje výsledky společné práce s Sebastianem Faustem, Pratyayem Mukharjeem, Danielem Venturim.

Implikace bezpečnosti Fiatovy-Shamirovy heuristiky pro hledání Nashova equilibria

Pavel Hubáček
Informatický ústav Univerzity Karlovy
E-mail: hubacek@iuuk.mff.cuni.cz

Fiatova-Shamirova heuristika transformuje interaktivní důkazové systémy s veřejnými náhodnými bity (public-coin) na neinteraktivní argumenty nahrazením ověřovatelových zpráv výstupem kryptografické hašovací funkce vyhodnocené na aktuálním transkriptu protokolu. Konstrukce hašovacích funkcí, pro které by byla tato transformace dokazatelně bezpečná je centrálním otevřeným problémem teoretické kryptografie.

V mé přednášce ukáži, že pokud je Fiatova-Shamirova heuristika bezpečná při použití na specifický standardní interaktivní protokol, pak libovolný výpočetně obtížný problém ve třídě #P indukuje distribuci výpočetně obtížných problémů ve třídě CLS; speciálně také pro problém nalezení Nashova equilibria.

Hlavní technickou částí našeho výsledku je inkrementálně ověřitelná procedura, která umožňuje nalézt počet splňujících ohodnocení pro SAT instance s n proměnnými. Naše procedura provádí exponenciální počet kroků, kde každý jednotlivý krok je efektivní (tj. běží v polynomiálním čase v n). Inkrementální ověřitelnost zaručuje, že každý jednotlivý krok obsahuje důkaz korektnosti výpočtu, jenž lze efektivně ověřit a také efektivně transformovat na důkaz pro následující krok výpočtu.

Příspěvek obsahuje výsledky společné práce s A. R. Choudhurim, C. Kamathem, K. Pietrzakem, A. Rosenem a G. N. Rothblumem.

Vnoření náhodného bipartitního grafu do náhodného biregulárního bipartitního grafu

Tereza Klimošová
Katedra aplikované matematiky MFF UK
E-mail: tereza@kam.mff.cuni.cz

Náhodný bipartitní graf $\mathbb{G}(n_1, n_2, m)$ je graf vybraný uniformně náhodně ze všech bipartitních grafů s partitami velikostí n_1 a n_2 a s m hranami. Náhodný biregulární bipartitní graf $\mathbb{R}(n_1, n_2, p)$ je graf uniformně náhodně vybraný ze všech bipartitních grafů s partitami velikostí n_1 a n_2, přičemž všechny vrcholy první partity mají stupeň pn_2 a všechny vrcholy druhé partity mají stupeň pn_1. Ukazujeme, že pro téměř každé $p \in (0, 1)$ existuje $\gamma = o(1)$ takové, že $\mathbb{G}(n_1, n_2, m)$ lze vnořit do $\mathbb{R}(n_1, n_2, p)$ pro $m = \lfloor (1 - \gamma) p n_1 n_2 \rfloor$.

Příspěvek obsahuje výsledky společné práce s Christianem Reiherem, Andrzejem Rucińskim a Matasem Šileikisem.

Férové alokace s velkým množstvím zdrojů

Dušan Knop
Algorithmics and Computational Complexity, Faculty IV, TU Berlin *and*
Department of Theoretical Computer Science, Faculty of Information Technology,Czech Technical University in Prague
E-mail: dusan.knop@tu-berlin.de

Zabýváme se studiem parametrizované složitosti problémů přidělování (alokace) nedělitelných zdrojů. Ukážeme parametrizovaný algoritmus pro širokou třídu problémů blízkých zavidění prostým alokacím (envy-free) při Pareto optimálitě. Tyto výsledky implikují existenci exaktního algoritmu pro tyto obecně výpočetně těžké problémy v případě, že jak počet agentů tak maximální ohodnocení zdroje (v absolutní hodnotě) jsou malé. Náš algoritmus dovoluje zadání velkých čísel, množství dostupných zdrojů je zadáno binárně kódovaným číslem na vstupu. V neposlední řadě naše řeší otevřený problém publikovaný v [Bliem et al., IJCAI 2016].

Dosažené výsledky implikují existenci tzv. metavěty pro mnoho v současné literatuře studovaných alokačních problémů pro aditivní uživatelské preference (tj. celkový užitek je suma užitků jednotlivých přidělených zdrojů). Tohoto dosáhneme kombinací dvou známých technik pro řešení celočíselných lineárních programů (ILP) – Lenstrova algoritmu a tzv. N-složených celočíselných programů. Spojením těchto dvou velmi studovaných technik je jedním z hlavních výsledků, jehož další využití, jak doufáme, v budoucnu přesáhne svět alokací.

Příspěvek obsahuje výsledky společné práce s Robertem Bredereckem, Andrzejem Kaczmarczykem a Rolfem Niedermeierem.

Ramseyova teorie: Na rozmezí kombinatoriky a teorie modelů

Matěj Konečný
KAM MFF UK
E-mail: matej@kam.mff.cuni.cz

Strukturální Ramseyova teorie je oblast na rozmezí kombinatoriky, teorie modelů a topologické dynamiky, která souvisí také s dalšími disciplínami (např. teorie CSP, teorie kategorií či logika). V této přednášce vysvětlím, co jsou homogenní struktury, představím některé kombinatorické problémy, které se jich týkají, a popíšu několik vlastních výsledků, především framework pologrupových metrických prostorů a zesílení Herwig–Lascarovy věty.

Příspěvek obsahuje výsledky společné práce s J. Hubičkou & J. Nešetřilem.

Algoritmická teorie celočíselného programování

Martin Koutecký
Informatický ústav Karlovy Univerzity
E-mail: koutecky@iuuk.mff.cuni.cz

Teorie celočíselného programování v omezené dimenzi se rozvíjí již od 80. let 20. století na základě technik a idejí z teorie čísel. Pomocí zcela jiných technik a idejí rozvineme teorii celočíselného programování v proměnné dimenzi, která zobecňuje a sjednocuje téměř dvě dekády předchozích výsledků. Naše hlavní věta říká, že celočíselné programy se separovatelně konvexní účelovou funkcí lze vyřešit v čase $g(a,d)\text{poly}(n)$ pro vyčíslitelnou funkci g, kde n je dimenze programu, a je největší absolutní hodnota koeficientu matice omezujících podmínek, a d je minimum mezi primární a duální stromovou hloubkou matice A. Stromová hloubka je zásadní pojem z teorie řídkých grafů a zachycuje jistou kombinatorickou složitost matice A. Naše výsledky jsou v jistém smyslu "těsné": nelze je zobecnit na jiné účelové funkce, nelze odstranit závislost na koeficientech matice, a stromová hloubka nelze nahradit obecnější stromovou šířkou.

Klíčový pojem naší teorie je Graverova báze, která představuje množinu "elementárních" zlepšujících kroků. Dalšími ingrediencemi jsou horní odhady na normy prvků Graverovy báze, dynamické programy pro výpočet prvků Graverovy báze, nové věty o blízkosti řešení zlomkové relaxace k celočíselným optimům, či silnější odhady na ekvivalentní účelové funkce. Tyto nástroje nám též umožňují zkonstruovat téměř lineární a silně polynomiální algoritmy.

Příspěvek obsahuje výsledky společné práce s Friedrichem Eisenbrandem, Christophem Hunkenschröderem, Kim-Manuelem Kleinem, Asafem Levinem a Shmuelem Onnem.

Pakování čtvrtinových cyklů

Tomáš Masařík
Charles University
E-mail: masarik@kam.mff.cuni.cz

Slavná Erdős-Pósova věta říká, že každý neorientovaný graf, který neosahuje k vrcholově disjunktních cyklů obsahuje množinu feedback vrcholů (množina vrcholů grafu, která protne každý cyklus) velikosti $O(k \log k)$. Obdobné tvrzení pro orientované grafy bylo dokázáno Reedem, Robertsonem, Seymourem a Thomasem v roce 1996 poté, co by bylo po mnoho let známé jako Youngerova doměnka. Nicméně v jejich důkaze je neelementární závislost mezi feedback množinou vrcholů a vrcholově disjunktními cykly.

Ukážeme, že pokud porovnáme závislost mezi minimální feedback množinou vrcholů v orientovaném grafu a čtvrtinovým pakováním cyklů, tak dostaneme polynomiální závislost. Přesněji dostaneme, že pokud v orientovaném grafu G není žádná množina k cyklů taková, že Každý vrchol G je v nejvíce 4 cyklech, potom existuje exisuje v grafu feedback množina vrcholů velikosti nejvýše $O(k^4)$. Navíc dokážeme daleko obecnější tvrzení o čtvrtinovém pakováním podgrafů velké orientované stromové šířky: Pro každá přirozená čísla a a b platí, že pokud orientovaný graf G má orientovanou stromovou šířku alespoň $\Omega(a^6b^8log_2(ab))$ potom nalezneme v G množinu a podgrafů každý orientované stromové šířky alespoň b takových, že každý vrchol G je v nejvýše čtyřech podgrafech.

Příspěvek obsahuje výsledky společné práce s Stephan Kreutzer, Paweł Rzążewski, Irene Muzi, Marcin Pilipczuk, Manuel Sorge.

Přibližná ekvivalence aritmetických obvodů

Vojtěch Mrázek
Fakulta informačních technologií, Vysoké učení technické v Brně, ČR
Institute of Computer Engineering, Vienna University of Technology, AT
E-mail: mrazek@fit.vutbr.cz

Rozšiřování moderních vestavěných a mobilních systémů napájených bateriemi zvyšuje požadavky na návrh těchto systémů s ohledem na příkon. Přestože moderní návrhové techniky příkon optimalizují, elektrická spotřeba těchto obvodů stále roste díky jejich složitosti. Nicméně existuje celá řada aplikací, kde nepotřebujeme získat úplně přesný výstup. Díky tomu se objevuje technika zvaná aproximativní (přibližné) počítání, která umožňuje za cenu zanesení malé chyby do výpočtu významně redukovat příkon obvodů.

Ukázalo se, že takové obvody je vhodné konstruovat za použití evolučních algoritmů (kartézského genetického programování - CGP), které mohou vytvářet obvody s dobrým poměrem mezi chybou a příkonem. Navržený algoritmus je řízen tzv. fitness funkcí, která je určena jednak velikostí (spotřebou) obvodu a také tím, jaká je aritmetická chyba kandidátního řešení oproti přesnému obvodu. Vzhledem k tomu, že rychlost výpočtu fitness funkce je klíčová pro kvalitní návrh, musíme se zaměřit zejména na efektivní vyhodnocení podobnosti obvodů (přibližné ekvivalence). V příspěvku budou představeny techniky založené na formální verifikaci, které nám buď přesně určí chybu obvodů, nebo zaručí, že chyba je menší než stanovený limit. Pro garanci maximální chyby jsme zvolili vyhodnocování s použitím SAT-solveru. Díky dodatečnému zavedení časového omezení verifikace do fitness funkce se podařilo snížit časovou náročnost evaluace. To přispělo k nalezení velmi kvalitních obvodů s garantovanou chybou (až 32-bit násobiček). Druhá technika využívá reprezentaci obvodů založenou na binárních rozhodovacích diagramech (BDD). Analýza BDD umožňuje vypočítat jak průměrnou a maximální aritmetickou chybu, tak i přepínací aktivitu hradel, která byla následně použita pro odhad spotřeby obvodu.

Příspěvek obsahuje výsledky společné práce s Lukášem Sekaninou, Zdeňkem Vašíčkem, Jiřím Matyášem, Milanem Češkou a Tomášem Vojnarem.

Atomy grafů bez dvou zakázaných indukovaných podgrafů

Jana Novotná
KAM MFF UK
E-mail: janca@kam.mff.cuni.cz

Graf je H-free, pokud neobsahuje graf H jako svůj indukovaný podgraf. Nedávno byla publikovaná zevrubná studie o tom, které třídy (H_1, H_2)-free grafů mají omezenou klikovou šířku. Pro grafy omezené klikové šířky přitom existuje efektivní algoritmus na řešení řady grafových problémů. Některé problémy kombinatorické optimalizace se však dají efektivně vyřešit i na větší třídě grafů. Michaël Rao 2007 ukazuje obdobný algoritmus pro grafy, které lze složit z atomů malé klikové šířky pomocí klikových řezů, přičemž atom je indukovaný podgraf, ve kterém neexistuje klikový řez. Přes tyto klikové řezy je poté možné složit řešení z jednotlivých částí a tak získat efektivní algorimy například na barvení, či nezávislou množinu.

Pro grafy bez jednoho indukovaného grafu přechod k atomům však nijak nepomůže. Zatímco pro dva zakázané podgrafy ukázal první použití Serge Gaspers, Shenwei Huang, Daniël Paulusma pro (C_4, P_6)-free grafy. Ty mají neomezenou klikovou šířku, ale omezenou klikovou šířku atomů. My rozšiřujeme studii klikové šířky a pro většinu grafů neomezené klikové šířky se dvěma indukovanými podgrafy ukazujeme, že i jejich atomy mají neomezenou klikovou šířku. Na druhou stranu ukazujeme, že tato metoda lze využít pro (Triplet, $2P_2$)-free grafy (triplet je C_4 s jedním dalším vrcholem sousedícím se třemi vrcholy C_4), pro které dokážeme omezenost atomů.

Příspěvek obsahuje výsledky společné práce s Konrad Dabrowsky, Tomáš Masařík, Daniël Paulusma, Paweł Rzążewski.

Shellovatelnost je NP-úplná

Pavel Paták
Univerzita Karlova
E-mail: patak@kam.mff.cuni.cz

Prezentujeme řešení několik desetiletí otevřeného problému a ukážeme, že shellovatelnost je NP-úplná.

Shellovatelnost je velice důležitá vlastnost, která lze formulovat např. takto: *Lze daný model (simpliciální komplex) K sestavený z trojúhelníků vybudovat tak, že každý další trojúhelník lepíme k předchozím pouze za hrany?* Definice shellovatelnosti pro ostatní dimenze je analogická.

Tato vlastnost nachází uplatnění v mnoha matematických disciplínách (teorie konvexních mnohostěnů, teorie uspořádání, komutativní algebra, teorie grup) a vedla k důkazu několika fundamentálních vět. Zmiňme například Schläfliho zobecnění Eulerovy formule do vyšších dimenzí (1852), Dehn-Sommervillovy relace (1927), či McMullenův důkaz Upper Bound Theoremu (1970).

S rozvojem teorie složitosti se lidé začali ptát, jak složité je rozhodnout, zda daný komplex je či není shellovatelný. „Je tento problém NP-úplný?“ zeptali se v roce 1978 Danaraj a Klee.

V rámci přednášky zmíníme i další souvislosti a otázky.

Příspěvek obsahuje výsledky společné práce s Xavierem Goaocem, Zuzanou Patákovou, Martinem Tancerem a Uli Wagnerem.

Průsečíkové struktury v rovině

Zuzana Patáková
Univerzita Karlova
E-mail: zuzka@iuuk.mff.cuni.cz

Mnoho geometrických algoritmů využívá pouze informace, které zadané i-tice množin, $i = 1, 2, \ldots$, mají neprázdný průnik. Říkáme, že pracují s *nervem* onoho systému. Určení složitosti nervu tudíž patří ke stěžejním otázkám výpočetní geometrie i topologie. V praxi se používá několik parametrů, které tuto složitost popisují: Hellyho číslo a jeho zlomková verze, VC-dimenze, perzistentní homologie, apod. Určení těchto parametrů pro zadaný množinový systém nebývá zpravidla jednoduché. Poměrně snadno lze oproti tomu určit topologické parametry daných množin, jakými jsou například počet komponent souvislosti, počet jednodimenzionálních děr, či obecněji homologie/homotopie zadaných množin a jejich průniků.

Mnoho důležitých matematických vět pak ukazuje, jak odvodit vlastnosti nervu z topologických předpokladů. Např. Hellyho věta říká, že pokud jsou všechny neprázdné průniky daných množin kontraktibilní (např. konvexní) a leží v $\mathbb{R}^d$, pak Hellyho i zlomkové Hellyho číslo je nejvýše $d + 1$. Snadným důsledkem je, že k popisu nervu stačí spodních $d + 1$ vrstev! VC-dimenze oproti tomu může být neomezená.

Může malá změna topologických předpokladů zapříčinit velkou změnu vlastností nervu? Toť hlavní otázka této přednášky.

Soustředíme se na systémy množin v rovině. Ukážeme, že pro otevřené množiny, které mají, stejně jako jejich libovolné průniky, omezený počet komponent souvislosti, prázdná čtvrtá vrstva nervu implikuje, že velikost třetí vrstvy je nejvýše konstantní násobek velikosti vrstvy druhé. To je výrazné zlepšení proti obecnému případu. Uvedený výsledek platí obecněji pro k-tou vrstvu.

Příspěvek obsahuje výsledky společné práce s Gilem Kalaiem.

Učenie sa závislostí medzi premennými kvantifikovaných boolovských formúl

Tomáš Peitl
TU Wien
E-mail: peitl@ac.tuwien.ac.at

Kvantifikované boolovské formule (QBF), ako napríklad

$$\forall x \exists y (x \vee \neg y) \wedge (\neg x \vee y),$$

predstavujú rozšírenie výrokovej logiky o kvantifikátory, vďaka ktorým sa do QBF dajú zakódovať mnohé prakticky užitočné problémy, napríklad formálna verifikácia, plánovanie či syntéza programov, ktoré spadajú mimo triedy **NP**. Jedna z hlavných paradigiem pre riešenie QBF je QCDCL (quantified conflict-driven clause learning). Aby bol výsledok korektný, QCDCL musí skúšať ohodnotenia premenných v poradí danom kvantifikátormi, čiže tak, aby boli zachované závislosti medzi premennými. Použitím *schém závislosti* (dependency schemes) sa dá toto pevné poradie uvoľniť, cenou za to je však zmena dôkazového systému, ktorý QCDCL používa, a s tým súvisiaca strata niektorých žiadúcich vlastností.

V tejto prednáške predstavíme *učenie sa závislostí* (dependency learning)—techniku, ktorá umožňuje QCDCL naučiť sa všetky potrebné závislosti za behu. QCDCL s učením sa závislostí má väčšiu voľnosť pri skúmaní priestoru ohodnotení, vylepšenú propagáciu „vynútených ťahov“ a zároveň si ponecháva *long-distance Q-resolution* ako svoj dôkazový systém, rovnako ako obyčajný QCDCL. Naviac dokážeme, že QCDCL s učením sa závislostí v niektorých prípadoch získava exponenciálnu výhodu oproti obyčajnému QCDCL.

Příspěvek obsahuje výsledky společné práce s Friedrichom Slivovskym a Stefanom Szeiderom.

Asymptotická analýza doby terminace vector addition systémů se stavy

Dominik Velan
Masarykova Univerzita, Fakulta Informatiky
E-mail: xvelan1@fi.muni.cz

Vector addition systémy se stavy (VASS) se využívají jako fundamentální model pro analýzu souběžných procesů, parametrizovaných systémů a také jako abstraktní model programů pro získání odhadů potřebných zdrojů. V naší práci studujeme problém asymptotické doby terminace pro daný VASS. Zejména se soustředíme na problém zajímavý z praktického hlediska, a to na získání polynomiálních odhadů doby terminace.

Prvním výsledkem je přesná charakterizace lineárních VASSů. Dále ukazujeme, že pokud VASS nemá lineární časovou složitost, pak je tato složitost alespoň kvadratická.

Dalším výsledkem je klasifikace VASSů podle kvantitativních vlastností jejich cyklů. Ukazujeme, že jisté singularity v těchto vlastnostech jsou klíčovým důvodem pro nepolynomiální asymptotickou složitost. Pokud VASS tyto singularity neobsahuje, je doba terminace vždy polynomiální, a to tvaru $\Theta(n^k)$, pro $k \leq d$, kde d je dimenze VASSu. V tomto případě předkládáme polynomiální algoritmus, který spočítá příslušné k. Dosažené výsledky jsou založeny na geometrickém popisu chování VASSu. Získaný vhled do geometrie VASSů má potenciál pro další použitelnost při jejich analýze.

Příspěvek obsahuje výsledky společné práce s Tomášem Brázdilem, Krishnendu Chatterjeem, Antonínem Kučerou, Petrem Novotným a Florianem Zulegerem.

Online rozvrhování paketů s termíny znovu a lépe

Pavel Veselý
University of Warwick
E-mail: Pavel.Vesely@warwick.ac.uk

V problému rozvrhování paketů s termíny přicházejí do síťového přepínače pakety, které mají být odeslány kanálem dál. Každý paket je charakterizován termínem a váhou, reprezentující prioritu paketu. Čas je rozdělen na kroky a pouze jeden paket může být odeslán v jednom kroku. Pokud je tedy přepínač přetížený, některým paketům vyprší termín a musí být zahozeny. Proto chceme navrhnout algoritmus odesílání paketů, který preferuje pakety vyšší priority, konkrétně maximalizuje celkovou váhu odeslaných paketů. Problém je přirozeně online a algoritmus se musí rozhodovat bez znalosti paketů, jež přijdou v budoucnosti.

K porovnávání algoritmů použijeme standardní kompetitivní poměr, který udává, kolikrát může být celková váha paketů odeslaných optimálním offline algoritmem větší než váha paketů odeslaných online algoritmem v nejhorším případě. Pro problém je dlouho znám dolní odhad na kompetitivní poměr deterministických algoritmů rovný zlatému řezu $\phi \approx 1.618$.

Na konferenci STTI'17 jsme ukázali ϕ-kompetitivní algoritmus pro 4-omezené instance, v nichž je rozdíl mezi příchodem a termínem paketu maximálně 4 sloty, čili životnost paketu může být pouze krátká. V této přednášce představíme ϕ-kompetitivní algoritmus pro obecné instance, v nichž pakety mohou mít libovolně dlouhou životnost.

Příspěvek obsahuje výsledky společné práce s Markem Chrobakem, Łukaszem Ježem a Jiřím Sgallem.