

# **SOUČASNÉ TRENDY TEORETICKÉ INFORMATIKY**

30. června – 1.července 2017, Praha

Z. Dvořák, T. Klimošová (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, CRYPTO, ESA, EUROCRYPT, 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 2017 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 56 mladých českých a slovenských informatiků, z nichž 18 se konference zúčastní. Hlavní přednášku přednese prof. Peter Rossmanith z RWTH Aachen University v Německu.

Konference STTI 2017 se uskuteční ve dnech 30. června – 1. července 2017 v Praze v budově MFF UK na Malostranském náměstí. Konference je organizována Informatickým ústavem University Karlovy za podpory grantů CE-ITI<sup>1</sup> a CMI (UNCE). Rád bych také poděkoval paní Milštainové za její pomoc při organizaci konference.

Jaroslav Nešetřil

---

<sup>1</sup>Projekt P202/12/G061 Grantové agentury ČR.



## Obsah

Úvodní slovo . . . . .	1
Obsah . . . . .	3
Hlavní přednáška konference . . . . .	4
Program konference . . . . .	6

### Abstrakty příspěvků

Martin Böhm: Online rozvrhování se zárukou: algoritmy a strojové dolní odhady . . . . .	10
Kateřina Böhmová: Rozvrhování přesunů prostředků v čase aneb sdílení aut s volitelným místem návratu . . . . .	11
Josef Cibulka: Randomizované škrabání brambory . . . . .	12
Marek Eliáš: $(h, k)$ -server problém na stromoch obmedzenej hlĺbky . . . . .	13
Radoslav Fulek: Hanani-Tutte pre aproximácie zobrazení grafov . . . . .	14
Peter Fulla: Výpočtová zložitost surjektívnych booleovských VCSP . . . . .	15
Robert Galian: Strukturální Parametry pro Celočíselné Lineární Programování . . . . .	16
Peter Gaži: Ako bude vyzerat Bitcoin 2.0? . . . . .	18
Pavel Hubáček: Kryptografické předpoklady a bariéry algoritmické teorie her . . . . .	19
Mikoláš Janota: Od boolské kvantifikace směrem k teoriím . . . . .	20
Vojtěch Kaluža: Konstruktivní důkaz silné Hanani–Tuttovy věty na projek-tivní rovině . . . . .	21
Alexandr Kazda: Hranové CSP s delta-matroidovými podmínkami . . . . .	22
Marek Krčál: Malware classification of executable files by deep nets . . . . .	23
Jan Kynčl: Jak naporcovat diskretní kořeněné kuře . . . . .	24
Jakub Opršal: Robustní algoritmus s polynomiální ztrátou pro CSP s near-unanimity polymorfismem . . . . .	25
Pavel Paták: Skoro-vnořitelnost a související témata . . . . .	26
Zuzana Patáková: Barevná simplicialní hloubka . . . . .	27
Tomáš Valla: On the Tree Search Problem with Non-uniform Costs . . . . .	28
Pavel Veselý: Online rozvrhování paketů . . . . .	29

# Hlavní přednáška konference

## Algorithmic Meta-Theorems for Random Graphs

**Peter Rossmanith**

RWTH Aachen University  
rossmani@cs.rwth-aachen.de

New concepts of sparsity, in particular nowhere-dense graphs and graphs of bounded expansion, were successfully used to show that many problems can be solved efficiently on many graph classes, unifying many former results.

In this talk we will look at random graphs including Erdős–Rényi graphs and the preferential attachment model. It turns out that graphs in the Barabási–Albert model are some-where dense with high probability. Hence the usual meta-theorems cannot be applied directly. Nevertheless, all these models exhibit a structure that leads to efficient algorithms for many problems. Moreover they include random graph classes that look similar to many real-world networks.



# Program konference

## Program STTI'17

### pátek 30. června

**8:30** začátek registrace

**9:00** Jan Kynčl: *Jak naporcovat diskrétní kořeněné kuře*

**9:25** Pavel Paták: *Skoro-vnořitelnost a související témata*

**9:50** Pavel Veselý: *Online rozvrhování paketů*

**10:15** přestávka

**10:35** Zuzana Patáková: *Barevná simplicialní hloubka*

**11:00** Radoslav Fulek: *Hanani-Tutte pre aproximácie zobrazení grafů*

**11:25** Peter Gaži: *Ako bude vyzerat Bitcoin 2.0?*

**11:50** Robert Ganian: *Strukturální Parametry pro Celočíselné Lineární Programování*

**12:15** oběd

**14:00** Pavel Hubáček: *Kryptografické předpoklady a bariéry algoritmické teorie her*

**14:25** Vojtěch Kaluža: *Konstruktivní důkaz silné Hanani–Tuttovy věty na projektivní rovině*

**14:50** Alexandr Kazda: *Hranové CSP s delta-matroidovými podmínkami*

**15:15** Jakub Opršal: *Robustní algoritmus s polynomiální ztrátou pro CSP s near-unanimity polymorfismem*

**15:40** přestávka

**16:00** Mikoláš Janota: *Od boolské kvantifikace směrem k teoriím*



**16:25** Martin Böhm: *Online rozvrhování se zárukou: algoritmy a strojové dolní odhady*

**16:50** Peter Fulla: *Výpočtová složitost surjektivních booleovských VCSP*

**17:15** Marek Eliáš:  *$(h, k)$ -server problém na stromoch obmedzenej hlĺbky*

**17:40** Kateřina Böhmová: *Rozvrhování přesunů prostředků v čase aneb sdílení aut s volitelným místem návratu*

**19:30** večere

## **sobota 1. července**

**9:00** Peter Rossmanith: ***Algorithmic Meta-Theorems for Random Graphs***

**10:00** přestávka

**10:30** Josef Cibulka: *Randomizované škrabání brambory*

**11:00** Tomáš Valla: *On the Tree Search Problem with Non-uniform Costs*

**11:25** Marek Krčál: *Malware classification of executable files by deep nets*

**12:15** oběd

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

## Abstrakty příspěvků



## Online rozvrhování se zárukou: algoritmy a strojové dolní odhady

Martin Böhm

Univerzita Karlova

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

V problému online rozvrhování se zárukou se algoritmy snaží přiřazovat úkoly nějakému (například pevnému) počtu strojů bez znalosti budoucích úkolů, ale s jistou globální zárukou, kterou budoucí úkoly musí dodržet. Příkladem takovéto globální záruky může být například znalost celkového objemu práce nebo informace, že v optimálním rozvrhu by všechny úkoly šly rozdělit do předem známého maximálního zatížení. Druhý zmíněný případ se v literatuře také nazývá *roztahování košů* (bin stretching).

Cílem algoritmů může být například zajistit rozumný poměr maximálního zatížení (celkové délky úloh na jednom stroji) oproti zatížení optimálního rozvrhu, který lze navrhnout, pokud známe celou budoucnost.

Známa vlastnost všech online problémů je to, že je lze modelovat jako hry dvou hráčů. Většinu času se tato skutečnost objevuje pouze v názvosloví vědců při návrhu algoritmů: „kam algoritmus zahraje“, „co protivník pošle na vstup“ atd.

Online rozvrhování se zárukami je jedna z podoblastí online problémů, kde se uvažování na úrovni her využívá i hlouběji – algoritmy jsou často navrhovány tak, aby se snažily dostat co nejrychleji do „výherní pozice“. Na straně druhé se daří pomocí algoritmů na prohledávání stavového prostoru nacházet dolní odhady, které jsou silnější, než předchozí analyticky navržené odhady.

V přednášce představíme nedávné algoritmické výsledky v oblasti a pohovoříme o různých technikách strojového konstruování dolních odhadů na efektivitu online algoritmů.

Příspěvek obsahuje výsledky společné práce s Robem van Stee, Jiřím Sgallem a Pavlem Veselým.

# Rozvrhování přesunů prostředků v čase aneb sdílení aut s volitelným místem návratu

Kateřina Böhmová

ETH

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

Služby sdílení aut (car sharing) fungují tak, že podnik spravuje několik aut a ty svým zákazníkům nabízí na krátký časový úsek k půjčení. Každé vozidlo má vyhrazeno pevné parkovací místo a zákazník, který si přeje toto auto půjčit, jej musí navrátit na přesně stejné místo. Mnoho uživatelů by ocenilo, kdyby tato podmínka byla zjemněna, a je přirozenou otázkou hledat alternativy, které by zákazníkům ponechaly více flexibility ve volbě místa pro vrácení auta. V tomto příspěvku se proto zabýváme variantou, kdy si uživatelé volí místo návratu vozidla rozdílně od místa vypůjčení.

Konkrétně studujeme případ, kdy každý dopředu sdělí své požadavky cesty (v jakém místě a v kolik hodin si chce vůz vyzvednout a kdy a kde jej vrátí), a cílem je zjistit, kolik nejvíce požadavků může být splněno pomocí stávajících aut a parkovacích míst. Ukážeme, že tento problém se dá vyřešit v polynomiálním čase převodem na problém hledání maximálního toku minimální ceny v na míru postavené síti.

Dále se zabýváme problémem, kdy každý uživatel má několik požadavků cesty a přitom bude spokojen jen pokud všechny jeho požadavky budou splněny (potřebuje dostat přidělené vozidlo na všechny své cesty a splnění jen části požadavků mu není k užitku). Ukážeme že splnit požadavky maximálního počtu uživatelů je APX-těžký problém již v případě, kdy jsou jen dvě parkovací lokace, každý uživatel má dva požadavky cesty, čas cesty je stejný pro všechny požadavky a k dispozici je jen jedno vozidlo. Je zajímavé, že tento problém je APX-těžký jen pokud je čas cesty nenulový, protože také ukážeme, že pokud by přesuny trvaly nulový čas, problém se stává řešitelným v polynomiálním čase.

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

# Randomizované škrabání brambory

Josef Cibulka

Univerzita Karlova

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

Uvažujeme algoritmický problém nalezení co největší konvexní množiny uvnitř zadaného jednoduchého mnohoúhelníka  $P$  s  $n$  vrcholy. Tento problém byl poprvé položen Goodmanem, který jej nazval *problémem škrabání brambory*.

Nejrychlejší známé řešení je od Changa a Yapa a běží v čase  $O(n^7)$ . Hall-Holt et al. našli konstantní aproximační algoritmus s časovou složitostí  $O(n \log n)$ .

Ukážeme randomizovaný  $(1 - \varepsilon)$ -aproximační algoritmus běžící v téměř lineárním čase. Přesněji, tento algoritmus v čase  $O(n(\log^2 n + (1/\varepsilon^3) \log n + 1/\varepsilon^4))$  nalezne konvexní mnohoúhelník obsažený v  $P$ , který má s pravděpodobností alespoň  $2/3$  plochu alespoň  $(1 - \varepsilon)$  krát plocha optimálního řešení. Podobný výsledek předvedeme i pro variantu, kdy hledáme konvexní mnohoúhelník obsažený v  $P$  s co největším obvodem.

Jednou z přísad důkazu je nový výsledek, který pro libovolný jednoduchý mnohoúhelník  $P$  ukazuje vztah mezi pravděpodobností  $Pr[ab \subset P]$ , že se navzájem vidí dva náhodné body z  $P$ , a plochou  $A^*(P)$  největší konvexní množiny obsažené v  $P$ . Konkrétně se jedná o horní odhad  $Pr[ab \subset P] \leq 12A^*(P) \cdot (1 + \log_2(1/A^*(P)))$ .

Příspěvek obsahuje výsledky společné práce s Sergiem Cabellem, Janem Kynčlem, Marií Saumellovou a Pavlem Valtrem.

## $(h, k)$ -server problém na stromoch obmedzenej hĺbky

Marek Eliáš

TU Eindhoven

E-mail: m.elias@tue.nl

$k$ -server problém je jedným z najznámejších a najviac študovaných problémov na poli Online algoritmov, kde vstup prichádza po častiach "online", a algoritmus musí urobiť nezvratiteľné rozhodnutia bez akejkoľvek informácie o budúcnosti. V štandardnom kontexte posudzujeme algoritmy pre  $k$ -server problém porovnaním riešenia vyprodukovaného algoritmom, s optimálnym riešením, ktoré je vypočítané offline (teda so znalosťou celého vstupu). Tento spôsob hodnotenia je vhodný na posúdenie "ceny informácie" v danom probléme, teda ako veľmi sa môžu zhoršiť naše riešenie, ak nepoznáme budúcnosť.

V tejto práci sa zaoberáme  $k$ -server problémom, avšak používame jemnejšie hodnotiace kritérium. Riešenie nájdené algoritmom s  $k$  servermi porovnáваме s offline optimálnym riešením s  $h$  servermi pre  $h \leq k$ . Môžeme o tom uvažovať tak, že pre pevné  $h$  zvyšujeme počet serverov algoritmu a sledujeme, ako sa vyvíja jeho kompetitívny pomer vzhľadom k offline optimu s  $h$  servermi. Tento model sa nazýva  $(h, k)$ -server problém, Weak adversaries model, alebo resource augmentation model. Jeho výhodou je, že dokáže porovnať, ako/či sa zlepšujú výsledky algoritmu s pridaním nových serverov, a tiež či veľkým množstvom serverov dokážeme kompenzovať nedostatok informácií o budúcnosti.

Aj keď tento prístup známy už niekoľko desaťročí, dostatočne preskúmaný je iba  $(h, k)$ -server problém na uniformných metrikách. Pre iné metriky sú známe iba čiastočné výsledky, mnohé z nich sú však nečakané a prekvapujúce. V tejto práci prinášame algoritmus, ktorý má konštantný kompetitívny pomer na stromoch obmedzenej hĺbky, a niekoľko menších negatívnych výsledkov, ktoré ukazujú, že štandardné algoritmy ako WFA a Double Coverage nedosahujú uspokojujúce výsledky.

Príspevek obsahuje výsledky spoločnej práce s Nikhilem Bansalem, Lukaszem Jeżem a Grigoriosem Koumoutsosom.

## Hanani-Tutte pre aproximácie zobrazení grafov

**Radoslav Fulek**

IST Austria

E-mail: rfulek@ist.ac.at

Hanani-Tutte veta hovorí, že graf je planárny, ak sa dá kresliť v rovine tak, že každé dve nesusedné hrany sa pretínajú párne veľakrát. Potvrdíme hypotézy A. Skopenkova a Repovša (1998), a M. Skopenkova (2003), ktoré zobecňujú Hanani-Tutte vetu v kontexte aproximácií spojitých zobrazení grafov v rovine vnoreniami ľubovoľne blízko daným zobrazeniam. Zaujímave zobrazenia z tohto pohľadu sú tie, ktoré zodpovedajú nakresleniam grafov v rovine bez transversálnych priesečníkov, v ktorom sa ale hrany prekrývajú. Náš dôkaz tohto výsledku je konštruktívny a vedie k polynomiálnemu algoritmu na testovanie toho, či sa dá dané zobrazenie grafu v rovine aproximovať vnorením, ktoré je ľubovoľne blízko danému zobrazeniu. Výsledok taktiež rozšírime pre spojitú zobrazenia grafu do ľubovoľnej uzavretej dvojrozmernej plochy. Náš výsledok má zaujímavé dôsledky pre problém "c-planarity" a tiež generalizuje nedávne výsledky pre testovanie "weakly simple polygons".

Príspevek obsahuje výsledky spoločnej práce s Janem Kynčlem.



# Výpočtová zložitosť surjektívnych booleovských VCSP

**Peter Fulla**

Oxford

E-mail: `peter.fulla@cs.ox.ac.uk`

Booleovské vážené problémy splniteľnosti zadaných podmienok (VCSP, valued constraint satisfaction problems) sú diskkrétne optimačné problémy, v ktorých môžu premenné nadobúdať hodnoty 0 alebo 1. Inštancia problému zadáva súbor podmienok, z ktorých každá sa vzťahuje len na podmnožinu premenných ohraničenej veľkosti. Podmienky spolu určujú váhu riešenia v závislosti od hodnôt premenných. Cieľom je nájsť riešenie s minimálnou váhou. V surjektívnom variante sa navyše vyžaduje, aby boli obe hodnoty 0 a 1 priradené aspoň jednej premennej. Klasický príklad problému tohto typu je minimálny rez grafu. V tejto práci skúmame výpočtovú zložitosť surjektívnych booleovských VCSP a klasifikujeme problémy podľa množiny podmienok, ktoré sú k dispozícii.

# Strukturální Parametry pro Celočíselné Lineární Programování

Robert Ganian

TU Wien

E-mail: rganian@ac.tuwien.ac.at

Celočíselné lineární programování (ILP) je archetypickým představitelem NP-úplného optimalizačního problému a má nespočet aplikací v mnoha rozličných oblastech informatiky, jako například plánování, rozvrhování, balení a trasování vozidel. Ale i přes rozsah aplikací tohoto problému doposud víme jenom velmi málo ohledně toho, které fragmenty ILP lze vyřešit efektivně; nejznámějším příkladem je klasický výsledek, že ILP lze vyřešit v polynomiálním čase na totálně unimodulárních maticích.

V tomto souhrnném příspěvku se zaměříme na zcela odlišný přístup k analýze a identifikaci strukturálních parametrů, které vedou k efektivnímu vyřešení ILP instancí; konkrétně se zaměříme na strukturální parametry založené na přirozených grafových reprezentacích ILP. Tento přístup již v minulosti slavil úspěchy v jiných, podobně prominentních oblastech, jako jsou například SAT a CSP, ale v aréně ILP nebyl až donedávna použit. Příspěvek předvede řadu nových výsledků získaných na základě tohoto přístupu; některé se již objevily na prestižních konferencích [1, 2], zatímco jiné jsou zcela nové [3].

První skupina výsledků se zaměří na takzvané primální grafy ILP instancí. Zde ukážeme, že stromová šířka (*treewidth*) není vhodná k řešení ILP instancí ani ve velmi omezených případech, ale stromová hloubka (*tree-depth*) umožňuje návrh FPT algoritmů pro ILP za předpokladu takovýchto dalších (nutných) omezení. Druhá skupina výsledků se týká jiné přirozené grafové reprezentace ILP instancí, tzv. incidence grafů: předvedeme kompletní analýzu složitosti ILP v souvislosti s parametrizací stromové šířky incidence grafů. Dále zavedeme nový strukturální parametr zvaný *torso-width*, který jako první svého druhu umožňuje řešení nejen ILP ale i tzv. MILP instancí. Nakonec se zmíníme o možnostech řešení ILP instancí s malým počtem globálních proměnných nebo globálních podmínek.

## Reference

- [1] Robert Galian and Sebastian Ordyniak. The complexity landscape of decompositional parameters for ILP. In *Proc. AAAI*, pages 710–716, 2016.
- [2] Robert Galian, Sebastian Ordyniak, and M. S. Ramanujan. Going beyond primal treewidth for (m)ilp. In *to appear in Proc. AAAI*, 2017.
- [3] Pavel Dvořák, Eduard Eiben, Robert Galian, Dušan Knop, and Sebastian Ordyniak. Solving integer linear programs with a small number of global variables and constraints. In *Submitted*.

Příspěvek obsahuje výsledky společné práce s Pavlem Dvořákem, Eduardem Eibenem, Dušanem Knopem, Sebastianem Ordyniakem a M. S. Ramanujanem.

## Ako bude vyzerat' Bitcoin 2.0?

**Peter Gaži**

IOHK Research

E-mail: [peter.gazi@iohk.io](mailto:peter.gazi@iohk.io)

Bitcoin je najznámejším reprezentantom fenoménu elektronických peňazí založených na kryptografii – kryptomien. Funguje od roku 2009 a za ten čas sa vyvinul z okrajovej zaujímavosti pre technologických nadšencov až do podoby verejne obchodovanej komodity a platobnej metódy, ktorá sa bežne objavuje v médiách a začína byť známa aj medzi širokou verejnosťou.

Aj keď je Bitcoin technicky prevratným riešením problému, ktorým sa kryptológovia zaoberali desaťročia, má aj mnoho nedostatkov. Snaha zlepšiť pôvodný protokol viedla k vzniku niekoľkých stoviek alternatívnych kryptomien – altcoinov.

Oblasť kryptomien je vzrušujúcim mladým odvetvím na pomedzí kryptológie, návrhu protokolov, distribuovaných systémov, ekonómie a teórie hier. V mojej prednáške sa pokúsím publikum presvedčiť, že k tejto téme rozhodne má čo povedať aj teoretická informatika. Pozrieme sa na niekoľko otázok, ktoré sú motivované praktickými potrebami tohto odvetvia, ale vedú k zaujímavým teoretickým problémom.

# Kryptografické předpoklady a bariéry algoritmické teorie her

**Pavel Hubáček**

IDC Herzliya

E-mail: [pavel.hubacek@weizmann.ac.il](mailto:pavel.hubacek@weizmann.ac.il)

Jedním z hlavních výsledků teorie her je Nashova věta, která zaručuje, že každá konečná hra má alespoň jedno rovnovážné řešení. Všechny důkazy této věty jsou však existenciální a žádný efektivní algoritmus pro nalezení takového řešení není momentálně znám. Vysvětlením tohoto stavu by bylo například vyloučení existence efektivních algoritmů pro řešení konečných her. Bitansky, Paneth a Rosen (FOCS'15) ukázali, že moderní kryptografické metody jako secure program obfuscation lze použít ke konstrukcím her, pro které dokazatelně nelze nalézt Nashovo rovnovážné řešení v polynomiálním čase. Tyto prvotní výsledky nabízejí přirozenou otázku, zda je možné dokázat obdobné výsledky za použití základních kryptografických předpokladů, jakým je například existence jednosměrných funkcí.

Ve své přednášce představím naše výsledky, které ilustrují souvislosti mezi výpočetní třídou TFNP (problémů, pro které řešení vždy existuje) a hierarchií kryptografických předpokladů od jednosměrných funkcí až po secure program obfuscation. Jako hlavní tvrzení ukáži, že existence náročných TFNP problémů vyplývá z existence distribucí NP problémů, které nelze řešit v polynomiálním čase.

Příspěvek obsahuje výsledky společné práce s Moni Naorem a Eylonem Yogevem.

## Od boolské kvantifikace směrem k teoriím

**Mikoláš Janota**

Microsoft Research, Cambridge

E-mail: `mikolas.janota@gmail.com`

Kvantifikované boolské formula (QBF) jakožto přirozené rozšíření problému splnitelnosti (SAT) jsou populárním cílem výzkumu v oblasti automatického dokazování. V této přednášce se podíváme na některé řešení pro QBF a jak se tyto dají přenést do kontextu jiných teorií.

## Konstruktivní důkaz silné Hanani–Tuttovy věty na projektivní rovině

Vojtěch Kaluža

Univerzita Karlova

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

Důkaz silné Hanani–Tuttovy věty na projektivní rovině podali Pelsmajer, Schaefer a Stasi v roce 2009. Jejich důkaz však používá charakterizaci grafů vnořitelných do projektivní roviny pomocí zakázaných minorů, a je tedy nekonstruktivní.

Oproti tomu my předkládáme konstruktivní důkaz, který popisuje, jak dané nakreslení grafu splňující předpoklady silné Hanani–Tuttovy věty na projektivní rovině převést na vnoření. To dává naději, že bude možné tento postup rozšířit na další plochy.

Příspěvek obsahuje výsledky společné práce s Éricem Colinem de Verdière, Pavlem Patákem, Zuzanou Patákovou a Martinem Tancerem.

## Hranové CSP s delta-matroidovými podmínkami

Alexandr Kazda

Univerzita Karlova

E-mail: alex.kazda@gmail.com

Problém splnitelnosti omezujících podmínek (Constraint Satisfaction Problem – CSP) spočívá v tom, rozhodnout, zda existuje přiřazení hodnot proměnným, které splňuje daný seznam podmínek.

V tomto příspěvku se budeme zabírat případem *hranového CSP*, kde se každá proměnná vyskytuje právě ve dvou podmínkách. Příkladem je hledání perfektního párování v grafech: Proměnné jsou hrany grafu, podmínky jsou vrcholy grafu, povolené hodnoty proměnných jsou 0 a 1 a vrchol stupně  $k$  si na hranách  $e_1, \dots, e_k$  s ním incidentních vynucuje podmínku „právě jedna z hodnot  $e_1, \dots, e_k$  je 1, ostatní jsou 0.“

Už od 60. let je známo, jak perfektní párování efektivně hledat pomocí Edmondsova algoritmu. Ukážeme si jak tento algoritmus zobecnit a řešit v polynomiálním čase hranové CSP jehož podmínky mají tvar tzv. sudých  $\Delta$ -matroidů (to je případ i perfektních párování).

Tento výsledek vznikl ve spolupráci s Vladimírem Kolmogorovem a Michalem Rolínkem na Institute of Science and Technology Austria. Algoritmus pro sudé  $\Delta$ -matroidy je první krok naší (doposud neukončené) snahy klasifikovat varianty hranového CSP s hodnotami proměnných 0 a 1.

Příspěvek obsahuje výsledky společné práce s Vladimírem Kolmogorovem a Michalem Rolínkem.



## Malware classification of executable files by deep nets

**Marek Krčál**

Akademie věd ČR/AVAST

E-mail: [marek.krcal@avast.com](mailto:marek.krcal@avast.com)

I give a concise overview of deep neural nets including some of their successful applications. Then I present preliminary results on how well can be deep nets trained in malware detection when supplied by Windows executable files without any domain-specific preprocessing or feature engineering.

## Jak naporcovat diskrétní kořeněné kuře

Jan Kynčl

Univerzita Karlova

E-mail: kync1@kam.mff.cuni.cz

Mějme  $nk$  červených nebo modrých bodů v rovině v obecné poloze, od každé barvy aspoň  $n$  bodů. Ukážeme, že pak jdou tyto body rozdělit do  $n$  disjunktních konvexních množin tak, že každá obsahuje přesně  $k$  bodů, aspoň jeden červený a aspoň jeden modrý. Dokonce počty červených bodů v různých množinách rozkladu se budou lišit maximálně o 1.

Dále ukážeme, že pokud  $P$  je množina  $n(d+1)$  bodů v obecné poloze v  $\mathbb{R}^d$  obarvená  $d$  barvami tak, že od každé barvy máme aspoň  $n$  bodů, pak existuje  $n$  disjunktních  $d$ -rozměrných simplexů s vrcholy v  $P$  takových, že každý obsahuje aspoň jeden bod od každé barvy.

Tyto výsledky se dají považovat za speciální případy diskrétní verze věty o kořeněném kuřeti. Zformulujeme hypotézu, která zobecňuje tuto diskrétní větu a dalších několik dřívějších výsledků týkajících se konvexních rozkladů barevných množin bodů.

Příspěvek obsahuje výsledky společné práce s Andreas F. Holmsenem a Claudiu Valculescu.

# Robustní algoritmus s polynomiální ztrátou pro CSP s near-unanimity polymorfismem

Jakub Opršal

TU Dresden

E-mail: jakub.oprsal@tu-dresden.de

Je-li dána relační struktura  $\Gamma$ , problém splnitelnosti omezení (CSP) s pevnou doménou  $\Gamma$  je problém, který na vstupu dostane systém omezení, které jsou dané jednou z relací struktury  $\Gamma$ , nad překrývajícími se množinami proměnných; cílem je pak přiřadit proměnným hodnoty z domény  $\Gamma$  tak, aby všechna omezení byla splněna. V optimalizační verzi je úkolem najít přiřazení, při kterém je splněno co nejvíce omezení. Approximační algoritmus pro CSP se nazývá robustní, pokud na vstupech, které jsou z  $(1 - \epsilon)$ -části splnitelné, vrátí přiřazení splňující alespoň  $(1 - g(\epsilon))$ -část podmínek, kde  $g$  je funkce splňující  $g(\epsilon) \rightarrow 0$  jak  $\epsilon \rightarrow 0$ .

Budeme se zabývat tím, jak robustní aproximovatelnost závisí na dané struktuře  $\Gamma$ . Struktury, pro které existuje polynomiální robustní algoritmus (s nějakou ztrátovou funkcí  $g$ ) byly posány Bartem a Kozikem. Nicméně obecný odhad na ztrátu funkce  $g$  je dvojitě exponenciální. Přirozenou otázkou je, kdy můžeme dosáhnout menší ztráty, speciálně polynomiální ztráty,  $g(\epsilon) \in O(\epsilon^{1/k})$  pro nějakou konstantu  $k$ . V přednášce se zaměříme na struktury s tzv. near-unanimity polymorfismem a popíšeme algoritmus, který v polynomiálním čase robustně řeší příslušné CSP s polynomiální ztrátou.

Příspěvek obsahuje výsledky společné práce s V. Dalmau, M. Kozikem, A. Krohkinem, K. Makarychevem a Y. Makarychevem.

## Skoro-vnořitelnost a související témata

**Pavel Paták**

Hebrew University of Jerusalem

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

Simpliciální komplexy slouží k modelování celé škály objektů. Jednou z fundamentálních otázek je, zda lze daný komplex vnořit do cílového prostoru. Ukázalo se však, že tato otázka je algoritmicky nerozhodnutelná.

My se proto zaměříme na zobecnění pojmu vnoření – takzvaná nezávisle sudá zobrazení (neboli také  $\mathbb{Z}_2$ -skoro vnoření), kdy pouze požadujeme, aby obrazy disjunktních stěn měly sudý počet “křížení”. Nespornou výhodou nezávisle sudých zobrazení je, že jejich existenci lze rozhodnout algoritmicky.

Ukážeme, že neexistence nezávisle sudého zobrazení některých komplexů do cílového prostoru má četné algoritmické důsledky, jež neplynou z pouhé neexistence vnoření.

Zmíníme i související témata:

1. Silnou Hanani-Tuttovu domněnku pro povrchy, tedy otázku, zda pro grafy a plochy pojmy vnoření a nezávisle sudého zobrazení splývají,
2. Van Kampen-Floresovu větu popisující komplexy s minimálním počtem vrcholů, které nejdou nezávisle sudě zobrazit do  $\mathbb{R}^{2k}$ ,
3. Heawoodovu nerovnost a Ringel-Youngsovou větu charakterizující, jaké úplné grafy lze vnořit na danou plochu. Lze Heawoodova nerovnost rozšířit na nezávisle sudá zobrazení?
4. Kühnelovu domněnku o nevnořitelnosti do variet, společné zobecnění van Kampen-Floresovy věty a Heawoodovy nerovnosti.

# Barevná simplicialní hloubka

Zuzana Patáková

IST Austria

E-mail: zuzana.patakova@ist.ac.at

Jednou z možných vícedimenzionálních analogií mediánu je bod s největší simplicialní hloubkou. Pokud se navíc některé body řídí podle jiných rozdělení, mluvíme o tzv. barevné simplicialní hloubce. Tato veličina se studuje ve statistice a datové analýze, ale zabývá se jí i diskrétní a výpočetní geometrie.

Formální definice zní takto: Pokud  $S_1, \dots, S_{d+1}$  jsou množiny bodů v  $\mathbb{R}^d$  (zvané barevné třídy),  $d$ -dimenzionální simplex je *barevný*, pokud jeho vrcholy leží v různých barevných třídách. *Barevnou simplicialní hloubkou bodu*  $p$  pak rozumíme počet barevných simplexů, které bod  $p \in \mathbb{R}^d$  obsahují. Ve větší obecnosti máme  $(d+1)$  pravděpodobnostních měr  $\mu_1, \dots, \mu_{d+1}$  a studujeme pravděpodobnost, že daný bod  $p \in \mathbb{R}^d$  leží v náhodném simplexu jehož  $i$ -tý vrchol vybíráme dle  $\mu_i$ .

Za první výsledek týkající se barevné simplicialní hloubky v diskrétní geometrii lze považovat barevnou verzi Carathéodoryho věty, kterou dokázal Imre Bárány v roce 1982: „Každý bod  $p \in \mathbb{R}^d$  obsažený v konvexním obalu všech barevných tříd má nenulovou barevnou simplicialní hloubku, pokud má každá barevná třída aspoň  $d+1$  bodů.“

V roce 2006 se Deza a spol. ptali na minimální a maximální hodnotu barevné simplicialní hloubky bodu  $p$  v barevné verzi Carathéodoryho věty. S využitím metod z algebraické topologie dokážeme těsný horní odhad  $1 + \prod_{i=1}^{d+1} (|S_i| - 1)$ .

Příspěvek obsahuje výsledky společné práce s Karimem Adiprasitem, Philipem Brinkmannem, Arnau Padrolem, Pavlem Patákem a Ramanem Sanyalem.

# On the Tree Search Problem with Non-uniform Costs

Tomáš Valla

ČVUT

E-mail: valla@ucw.cz

Searching in partially ordered structures has been considered in the context of information retrieval and efficient tree-like indices, as well as in hierarchy based knowledge representation. In this paper we focus on tree-like partial orders and consider the problem of identifying an initially unknown vertex in a tree by asking edge queries: an edge query  $e$  returns the component of  $T - e$  containing the vertex sought for, while incurring some known cost  $c(e)$ . The Tree Search Problem with Non-Uniform Cost is the following: given a tree  $T$  on  $n$  vertices, each edge having an associated cost, construct a strategy that minimizes the total cost of the identification in the worst case.

Finding the strategy guaranteeing the minimum possible cost is an NP-complete problem already for input trees of degree 3 or diameter 6. The best known approximation guarantee was an  $O(\log n / \log \log \log n)$ -approximation algorithm of [Cicalese et al. TCS 2012].

We improve upon the above results both from the algorithmic and the computational complexity point of view: We provide a novel algorithm that provides an  $O(\frac{\log n}{\log \log n})$ -approximation of the cost of the optimal strategy. In addition, we show that finding an optimal strategy is NP-hard even when the input tree is a spider of diameter 6, i.e., at most one vertex has degree larger than 2.

## Online rozvrhování paketů

Pavel Veselý

Univerzita Karlova

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

Pakety jednotkové délky přicházejí do routeru v průběhu času a mají být odeslány přes síť. Čas si můžeme představit jako diskrétní, rozdělený na sloty, přičemž v každém slotu lze odeslat jen jeden paket. Abychom modelovali priority, každý paket má dva atributy: nezápornou váhu a termín na odeslání. Cílem je maximalizovat celkovou váhu paketů odeslaných před jejich termínem. Jedná se tedy o variantu online rozvrhování na jednom stroji s jednotkovými délkami úloh a s cílem maximalizovat celkovou váhu rozvrhnutých úloh.

K porovnávání algoritmů použijeme standardní kompetitivní poměr, který udává, kolikrát je celková váha optimálního rozvrhu větší než celková váha rozvrhu algoritmu v nejhorším případě. Pro problém je dlouho znám dolní odhad na kompetitivní poměr deterministických algoritmů rovný zlatému řezu  $\phi \approx 1.618$ . Zatímco nejlepší známý algoritmus je 1.828-kompetitivní, obecně se věří, že existuje  $\phi$ -kompetitivní algoritmus.

V přednášce se zaměříme na  $k$ -omezené instance, v nichž je rozdíl mezi termínem a příchodem paketu nejvýše  $k$ , tedy každý paket lze odeslat v jednom z maximálně  $k$  slotů. Dolní odhad  $\phi$  platí už pro 2-omezené instance a  $\phi$ -kompetitivní algoritmus je znám pro 3-omezené instance. V přednášce tento výsledek zlepšíme a ukážeme  $\phi$ -kompetitivní algoritmus pro 4-omezené instance.

Budeme se též zabývat algoritmy s tzv.  $\ell$ -lookaheadem, jež umožňuje algoritmu vidět trochu do budoucnosti, tedy pro nějaké  $\ell \geq 0$  spatřit v čase  $t$  všechny pakety, které přijdou do času  $t + \ell$ . To odpovídá situaci, kdy je router schopen sledovat pakety přicházející do bufferu, ještě než je možné je zpracovat. Ukážeme 1.303-kompetitivní algoritmus s 1-lookaheadem pro 2-omezené instance a dolní odhad pro algoritmy s  $\ell$ -lookaheadem, který je roven  $\frac{1}{2(\ell+1)}(1 + \sqrt{5 + 8\ell + 4\ell^2})$  a platí už pro 2-omezené instance. Pro 1-lookahead tak získáme dolní odhad 1.281.

Příspěvek obsahuje výsledky společné práce s Martinem Böhmem, Markem Chrobakem, Łukaszem Jeżem, Fei Li a Jiřím Sgallem publikované na konferenci ISAAC 2016.