

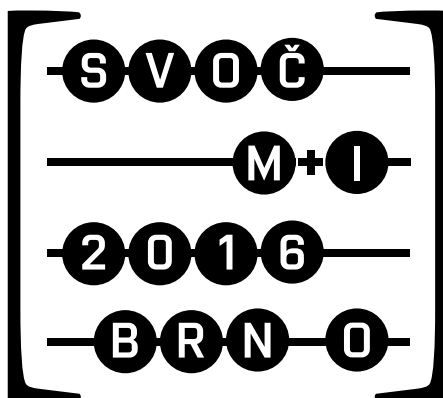
ČESKÁ MATEMATICKÁ SPOLEČNOST
SEKCE JEDNOTY ČESKÝCH MATEMATIKŮ A FYZIKŮ

SLOVENSKÁ MATEMATICKÁ SPOLOČNOSŤ
SEKCIA JEDNOTY SLOVENSKÝCH MATEMATIKOV A FYZIKOV

A

FAKULTA STROJNÍHO INŽENÝRSTVÍ
VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ

**SOUTĚŽ STUDENTŮ VYSOKÝCH ŠKOL
VE VĚDECKÉ ODBORNÉ ČINNOSTI
V MATEMATICE A INFORMATICE**



17. ročník soutěže SVOČ

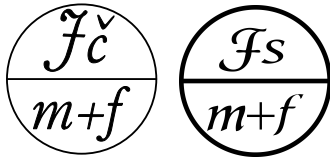
BRNO
25.–27. KVĚTNA 2016

SVOČ 2016

Soutěž studentů vysokých škol ve vědecké odborné činnosti
v matematice a informatice
Brno, 25.–27. května 2016

Vyhlašovatel

Česká matematická společnost, sekce Jednoty českých matematiků a fyziků
Slovenská matematická spoločnosť, sekcia Jednoty slovenských matematikov a fyzikov



Pořadatel

Fakulta strojního inženýrství Vysokého učení technického v Brně



Záštitu nad soutěží převzal

rektor VUT v Brně prof. RNDr. Ing. Petr Štěpánek, CSc.



Závěrečné kolo 17. ročníku soutěže SVOČ

vysázeno systémem L^AT_EX

Ústav matematiky, FSI VUT v Brně, 2016

Vážené kolegyně a kolegové, milí příznivci a vyznavači matematiky a informatiky.

Opravdu rád jsem převzal záštitu nad 17. ročníkem česko-slovenské soutěže o nejlepší studentskou vědeckou práci v oboru matematika a informatika. Musím konstatovat, že matematika je potřebná ve všech odvětvích lidské činnosti, není to jen řešení příkladů, je to systémové a logické myšlení, je to i přístup k životu a světu, je to – snad se na mne nikdo nebude zlobit – filozofie. Logická, zdůvodnitelná, dokazatelná, prostě se bez ní nikde neobejdeme.

S potěšením mohu konstatovat, že počet prací i počet zapojených fakult rok od roku mírně roste, nedochází však k devalvaci kvality prací. Nárůst počtu se projevuje jak v matematických, tak i v informatických sekcích. Myslím, že tento trend zejména v době, kdy se na vysokých školách technického a přírodovědného zaměření projevuje pokles zájemců o studium v souvislosti s demografickým vývojem i v souvislosti s tím, že přírodovědné vědní disciplíny jsou těžké a někdy bohužel nemají ani tu společenskou prestiž, která by jim právem náležela, je správný a podtrhuje i snahy nás všech o to, aby matematické, fyzické, chemii a dalším přírodovědným disciplínám byl jak na základních školách, tak i na školách středních poskytnut takový prostor, jaký jim po právu náleží.

Dovolte mi na závěr, abych poděkoval jak pořadatelům, tak i vyhlášovatelům soutěže, kterými jsou Česká matematická společnost Jednoty českých matematiků a fyziků a Slovenská matematická společnost Jednoty slovenských matematiků a fyziků za jejich úsilí o další propagaci matematiky.

V Brně dne 12. května 2016

*prof. RNDr. Ing. Petr Štěpánek, CSc.
rektor Vysokého učení technického v Brně*

Řídící výbor SVOČ

Prof. RNDr. Bohdan Maslowski, DrSc. (MFF UK Praha, předseda)

Prof. RNDr. Jan Franců, CSc. (FSI VUT Brno)

Prof. RNDr. Jan Kratochvíl, CSc. (MFF UK Praha)

Prof. RNDr. Karol Mikula, CSc. (SvF STU Bratislava)

RNDr. Martin Pergel, Ph.D. (MFF UK Praha)

Prof. RNDr. Luboš Píck, DSc. (MFF UK Praha)

Doc. RNDr. Tomáš Vinař, CSc. (FMFI UK Bratislava)

Místní organizační výbor

Prof. RNDr. Jan Franců, CSc.

Mgr. Jana Hoderová, Ph.D.

Doc. Mgr. Jaroslav Hrdina, Ph.D.

Doc. Ing. Luděk Nechvátal, Ph.D.

Mgr. Zdeněk Opluštil, Ph.D.

Sponzoři

HUMUSOFT, spol. s r.o. (www.humusoft.cz)

Red Hat Czech, s.r.o. (www.cz.redhat.com)

Vinařství Maděřič spol. s r.o. (www.vinarstvimaderic.cz)

Propozice 17. ročníku SVOČ

1. Vyhláшателеm soutěže SVOČ je Česká matematická společnost, sekce Jednoty českých matematiků a fyziků a Slovenská matematická spoločnosť, sekcia Jednoty slovenských matematikov a fyzikov.
2. Závěrečné kolo 17. ročníku soutěže se uskuteční ve dnech 25. – 27. května 2016 v Brně. Pořadatelem závěrečného kola je Fakulta strojního inženýrství Vysokého učení technického v Brně. Termín pro zúčastněné fakulty k přihlášení účastníků do závěrečného kola soutěže je 2. května 2016. Termín pro elektronické odevzdání prací studenty je 9. května 2016. Webová stránka soutěže je <http://jcmf.cz/svoc>.
3. Soutěž probíhá v následujících sekcích:
 - (M1) Matematická analýza – teorie funkcí a prostory funkcí;
 - (M2) Matematická analýza – teorie diferenciálních a integrálních rovnic;
 - (M3) Teorie pravděpodobnosti a matematická statistika;
 - (M4) Ekonometrie a finanční matematika;
 - (M5) Matematické struktury – algebra, topologie a geometrie;
 - (M6) Matematické struktury – teorie grafů a kombinatorika;
 - (M7) Aplikovaná matematika – numerická analýza;
 - (M8) Aplikovaná matematika – matematické modely dynamiky;
 - (I1) Teoretická informatika;
 - (I2) Umělá inteligence;
 - (I3) Počítačová grafika a počítačové vidění;
 - (I4) Aplikovaná informatika a softvérové inženýrství.
4. V případě, že v některé sekci bude přihlášeno méně než 6 prací, může řídicí výbor SVOČ rozhodnout o sloučení této sekce s příbuznou sekci, případně přerozdělit sekce jiným způsobem podle počtu a zaměření jednotlivých prací (obvykle v případě menšího počtu prací dochází ke sloučení sekcí s čísly $2n - 1$ a $2n$).
5. Studenti se do soutěže přihlašují prostřednictvím svých fakult. Každá fakulta může do každé sekce vyslat nejvýše 5 prací. Výběr prací mohou fakulty uskutečnit prostřednictvím fakultních soutěží SVOČ. Termíny a organizace fakultních soutěží nebo jiný způsob výběru prací je věcí jednotlivých fakult.
6. Řídicí výbor sestavuje zpravidla tříčlenné poroty jednotlivých sekcí. Člen poroty nesmí být vedoucím žádné práce soutěžící v dané sekci.

Přihlašování účastníků

7. Do závěrečného kola SVOČ studenty přihlašují fakulty vysokých škol působících v ČR nebo SR. Každá fakulta může do každé sekce přihlásit nejvýše 5 prací. Výběr prací mohou fakulty uskutečnit prostřednictvím fakultních kol soutěže nebo jiným vhodným způsobem podle uvážení fakulty.
8. Přihlášení studenti musí být v čase zaslání přihlášky studenty bakalářského, magisterského, inženýrského nebo jiného obdobného studia na dané fakultě. Přihlášení studenti v době zaslání přihlášky nesmí mít už ukončené magisterské, inženýrské nebo obdobné studium v oblastech zaměření soutěže.
9. Přihlášku, obsahující seznam prací, fakulta zasílá nejpozději do 2. května 2016 e-mailem na adresu svoc@jcmf.cz. Pro každou práci musí seznam obsahovat název práce, jména autorů a sekci, do které je práce přihlášena.

Odevzdávání prací

10. Elektronickou verzi práce každý účastník odevzdá nejpozději do 9. května 2016 prostřednictvím elektronického formuláře přístupného na webové stránce závěrečného kola soutěže. Prostřednictvím elektronického formuláře je potřebné odevzdat: abstrakt práce, text práce a naskenovaný posudek vedoucího práce nebo jiného vědecko-pedagogického pracovníka fakulty. Jeden vytištěný a pevně svázaný exemplář práce (například kroužkovou vazbou) s podepsaným originálem posudku práce účastník přiveze s sebou na soutěž a odevzdá při registraci.
11. Abstrakt, text práce a posudek musí být napsán v češtině, slovenštině nebo angličtině.
12. Abstrakt délky maximálně jedné strany A5 ve formátu PlainTeX obsahuje jen vlastní text (neobsahuje jména autorů, název práce, nebo školu/fakultu). Je v něm mimo jiného vymezený vlastní přínos autora, případně vztah k diplomové/bakalářské práci nebo k pracím podaným do SVOČ v předchozích letech, nebo jiných soutěží podobného charakteru.
13. Elektronický text práce se odevzdává ve formátu PDF se zabudovanými fonty. Na titulní straně soutěžní práce musí být uvedeno, že se jedná o práci pro soutěž SVOČ. Elektronická verze posudku se odevzdává ve formátu PDF se zabudovanými fonty nebo ve formátu JPEG. V posudku musí být kromě jiného přesně vymezen přínos autorů.
14. Další technické pokyny mohou být zveřejněny na webové stránce závěrečného kola soutěže.

Průběh soutěže

15. Soutěžní práce budou hodnoceny podle následujících kritérií:
 - vlastní výsledky a přínos práce,
 - celkové zpracování práce,
 - přednes referátu o práci během závěrečného kola a reakce na případné dotazy.
16. V rámci soutěžního dne každý účastník přednese referát o své soutěžní práci. Odborné poroty v jednotlivých sekcích vyhodnotí soutěžící práce podle následujících kritérií: vlastní výsledky a přínos práce, celkové zpracování práce, přednes referátu a reakce na případné dotazy. Nejlepší práce budou oceněné diplomy a finančními odměnami.
17. Soutěžícím a porotcům závěrečného kola SVOČ bude zajištěno bezplatné ubytování a stravování. Úhradu cestovného si účastníci zabezpečí sami.

Obsah

M1+M2: Matematická analýza – teorie funkcí a prostory funkcí + teorie diferenciálních a integrálních rovnic	10
M. Bathory, <i>Conjugate function</i>	11
E. Brabcová, <i>Počáteční a okrajové úlohy s hysterezní smyčkou</i>	11
E. Buriánková, <i>Optimal function spaces for one-dimensional operators</i>	11
V. Pravec, <i>On dynamics of triangular maps of the square with zero topological entropy</i>	12
V. Švígler, <i>On the Landesman–Lazer type of conditions for the elliptic BVP at resonance with measure data</i>	12
D. Uhrík, <i>Polospojité funkcie</i>	12
M. Výboštok, <i>Na intervale nekonečná ω-limitní množina s periodickým bodem implikuje podkovu: Priamy dôkaz</i>	13
M3+M4: Teorie pravděpodobnosti a matematická statistika + ekonomie a finanční matematika	14
K. Adamčíková, <i>Vzdialenostná korelácia</i>	15
J. Falath, <i>Sociálny, ekonomický a kultúrny status a jeho vplyv na pridanú hodnotu vo vzdelávaní</i>	15
R. Finger, <i>Asymptotické a robustní vlastnosti statistických odhadů a testů s minimální pseudovzdáleností</i>	16
T. Chlubnová, <i>Výběr modelu na základě penalizované věrohodnosti</i>	16
K. Koňasová, <i>Směrová K-funkce pro stacionární procesy</i>	16
D. Kuruczová, <i>Neparametrická analýza funkcionálních dat</i>	17
M. Malý, <i>Roystonove testy normality</i>	17
D. Novotná, <i>Konečné prostorové bodové procesy: analýza, simulace a asymptotika</i>	18
T. Rubín, <i>Stochastic evolution equations with singular fractional noise</i>	19
P. Šimon, <i>Topological support of solutions to stochastic differential equations</i>	19
J. Vacková, <i>Statistická rigidita systémů se socio-fyzikálními interakcemi</i>	19
V. Kubelka, <i>Markovovy procesy v analýze spolehlivosti složitých průmyslových systémů</i>	20
M. Outrata, M. Kouřilek, <i>On Cournot–Nash–Walras equilibria, social equilibria, their stability and computation</i>	21
M5: Matematické struktury – algebra, topologie a geometrie	22
P. Čoupek, <i>Tilting theory for quasi-coherent sheaves</i>	23
J. Krásenský, <i>Množiny generované číselnými soustavami v kvaternionech</i>	23
R. Půček, <i>Applications of invariant operators in real parabolic geometries</i>	23
J. Sedláková, <i>O Bäcklundově transformaci sinh-Gordonovy rovnice</i>	24
T. Svoboda, <i>Integrální formule pro topologické invarianty</i>	25
M. Tinková, <i>Poziční reprezentace čísel v kubických tělesech</i>	25
M. Vodička, <i>Rovnomerná vlastnosť stability pre duálne mriežky</i>	26
M6: Matematické struktury – teorie grafů a kombinatorika	27
M. Bezek, <i>Characterizing DAG-depth of directed graphs</i>	28
K. Čekanová, <i>Lahké hrany v rovinných grafoch s duálnou váhou aspoň 10</i>	28
P. Fratrič, <i>Circulant graphs of diameter 2 and sum-free sets</i>	29
M. Nedelová, <i>Archimedovské mapy na neorientovatelných plochách a operácie na hypermapách</i>	29

J. Sosnovec, <i>The Helly numbers of systems of sets with bounded algebraic and topological complexity</i>	29
T. Velká, <i>Generalized pseudopalindromic closures</i>	30
V. Veselý, <i>Binární projekce Arnouxových–Rauzyových slov</i>	30
M7: Aplikovaná matematika – numerická analýza	32
R. Blaschke, <i>Numerický výpočet funkcie času príchodu lesného požiaru v nehomogénnom prostredí</i>	33
L. Hrapková, <i>Registrácia mračien bodov z 3D skenerov</i>	33
J. Kružík, <i>Parallelizations of TFETI-1 coarse problem</i>	33
E. Straková, <i>Hľadanie koreňov komplexných funkcií</i>	34
M. Šimková, <i>Numerické metody pro hledání vlastních čísel</i>	34
M8: Aplikovaná matematika – matematické modely dynamiky	36
M. Dostalík, <i>Influence of material parameters on stability of thermal convection</i>	37
J. Klinkovský, <i>Numerické řešení dvoufázového nemísivého filtračního proudění s kapilaritou a jeho implementace na GPU</i>	37
P. Mihala, <i>Infiltrácia vody do nenasýteného porézneho valca v gravitačnom poli a pri centrifugácii</i>	38
J. Minarčík, <i>Applications of planar and space curve evolution</i>	38
M. Mrázek, <i>Modelování pohybu kapaliny v pohybující se nádrži</i>	39
T. Smejkal, <i>Testování fázové stability a výpočet rovnovážných stavů vícesložkových směsí</i>	39
M. Tóth, <i>Transport tepla a vody v pórovitom prostredí</i>	39
I1: Teoretická informatika	41
M. Ajdarów, <i>Minimality problems for promise versions of nite automata</i>	42
O. Suchý, T. Valla, <i>A simpler bit-parallel algorithm for swap matching</i>	42
M. Brzicová, <i>On-line multiplication and division in non-standard numeration systems</i>	42
A. Dresslerová, <i>$L(2, 1)$-farbenie kaktusov</i>	43
M. Gábriš, <i>State recovery of RC4 and Spritz revisited</i>	44
R. Korbaš, <i>Výpočty na konečných automatoch s pomocnou informáciou</i>	44
I. Krajňáková, <i>Štvorec na deterministických a alternujúcich automatoch</i>	44
K. Medková, <i>Synchronizační zpoždění DOL-systémů</i>	45
L. Pápay, <i>Evaluation of SAT-based preimage attack optimizations</i>	46
P. Zeman, <i>On H-topological intersection representations of graphs</i>	46
I2: Umělá inteligence	47
M. Filippi, <i>Genetické programování pro řízení hejna robotů</i>	48
M. Klučárová, <i>Použitie neurónových sietí pri spracovaní zvukového signálu</i>	48
K. Střelský, <i>Automatické generování realistického terénu pomocí technik strojového učení</i>	48
J. Šimek, <i>Skladanie DNA sekvencií pomocou paralelného modelu inšpirovaného imunitným systémom</i>	49
M. Šuppa, <i>Kaldi versus HTK: Evaluation of speech recognition frameworks on Alica dataset</i>	50

I3: Počítačová grafika a počítačové vidění	51
P. Budzáková, <i>Lokálne príznaky vo farebných obrazoch</i>	52
R. Chovan, B. Pažický, P. Balajka, <i>Vyhľadávanie objektov pomocou deskriptora shape context</i>	52
O. Jariabka, M. Šuppa, <i>Generation of lecture notes as images from recorded whiteboard and blackboard based presentations</i>	52
V. Kačala, <i>Zrýchlenie výpočtu splajn povrchov</i>	53
P. Kunovský, <i>Snímanie HDR obrazu ustavanou kamerou v bežných mobilných zariadeniach</i>	53
T. Maták, <i>Rôzne formy OpenGL vizualizácie v prostredí Windows a Linux</i> .	53
J. Murín, <i>Prenos dát pomocou optického dátového toku</i>	54
J. J. Páleník, <i>Segmentácia exosómov</i>	54
M. Pecha, <i>Image segmentation techniques in the HPC environment and their applications</i>	55
A. Riečický, <i>Seamless texture space diffusion using skeleton texture mapping</i>	56
M. Tamajka, <i>Automatic brain segmentation method based on supervoxels</i> . .	56
I4: Aplikovaná informatika a softvérové inžénrství	57
L. Csóka, <i>Parallel genetic algorithm on model-based Gauss cluster analysis</i>	58
M. Dragúňová, <i>Considering human visual search abilities in eye tracking user studies</i>	58
T. Duda, <i>Detekce phishingových zpráv</i>	58
D. Formánek, <i>Detekce bezpečnostních chyb pomocí statické analýzy kódu</i> . .	59
J. Holas, <i>Efektívne vyhľadávanie vzorov v ETL súboroch</i>	60
M. Ilavský, <i>Testovacie údajové sady pre bezpečnostné technológie</i>	60
A. Kačengová, <i>Aplikácia stochastickej reaktívnej kinetiky na modelovanie rezistencie baktérií na antibiotiká</i>	60
J. Kotrady, <i>Problém faktorizácie v asymetrickej kryptografii alebo naozaj sa Ron mylil?</i>	61
M. Kováč, <i>Implementácia algoritmu násobenia matíc na GPGPU s optimalizáciou prenosu údajov</i>	62
M. Liskovec, <i>Beacon based localization refined by outputs from mobile sensors</i>	62
M. Sokolovský, <i>Hľadanie optimálnych ciest v rozvetvených štruktúrach</i> . . .	63
M. Súkeník, <i>ROS and filtering data from sensors</i>	63
Š. Šmihla, <i>The usage of Levenshtein distance in intrusion detection on web server</i>	63
M. Trník, <i>Mnohorozmerná analýza rozvrhovania vo vysokovýkonných počítačových systémoch</i>	64
Jmenný rejstřík	65

Sekce M1+M2

MATEMATICKÁ ANALÝZA

TEORIE FUNKCÍ A PROSTORY FUNKCÍ

TEORIE DIFERENCIÁLNÍCH A INTEGRÁLNÍCH ROVNIC

Porota

Vít Musil (MFF UK, Praha)
Martin Kolář (PřF MU, Brno)
Jozef Doboš (PF UPJŠ, Košice)

CONJUGATE FUNCTION

Michal Bathory

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: bathory1@seznam.cz

Using interpolation methods, new results on the boundedness of quasilinear joint-weak type operators on Lorentz–Karamata (LK) spaces are established. LK spaces generalize many function spaces introduced before in literature, for example, the generalized Lorentz–Zygmund spaces, the Zygmund spaces, the Lorentz spaces and, of course, the Lebesgue spaces. The focus is mainly on the limiting cases of interpolation, where the spaces involved are, in certain sense, very close to the endpoint spaces. The results contain both necessary and sufficient conditions for the boundedness of the given operator on LK spaces. The complete characterization of embeddings of LK spaces is also included and the optimality of achieved results is then discussed. Finally, we apply our results to the conjugate function operator.

POČÁTEČNÍ A OKRAJOVÉ ÚLOHY S HYSTEREZNÍ SMYČKOU

Eva Brabcová

Fakulta aplikovaných věd Západočeské univerzity v Plzni
e-mail: brabe@students.zcu.cz

Práce je zaměřena na počáteční a okrajové úlohy pro obyčejnou diferenciální rovnici s hysterezí a na studium vlastností jejich řešení. Nejprve je představen jev hystereze a několik matematických modelů systémů s hysterezí, poté zkoumáme vybrané počáteční a okrajové úlohy. V případě počátečních úloh se věnujeme především omezenosti řešení v závislosti na parametrech úlohy a u okrajových úloh množině hodnot parametrů, pro které mají úlohy netriviální řešení. Hlavní výsledky práce se týkají úloh se symetrickou a s nesymetrickou hysterezní smyčkou, u nichž zobecňujeme a rozšiřujeme teorii známou pro speciální případy. Součástí práce jsou rovněž numerické experimenty ze softwarů Matlab a Mathematica, které teoretickým výsledkům zcela odpovídají.

OPTIMAL FUNCTION SPACES
FOR ONE-DIMENSIONAL OPERATORS**Eva Buriánková**

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: eva.buriankova@seznam.cz

In this manuscript we study the action of one-dimensional operators on rearrangement-invariant Banach function spaces. Our principal goal is to characterize optimal target

and domain spaces corresponding to given spaces within the category of rearrangement-invariant Banach function spaces as well as making pointwise estimates of a nonincreasing rearrangement of a given operator applied on a given function. We apply these general results to establish an optimality relation between special rearrangement-invariant spaces under the Laplace transform.

ON DYNAMICS OF TRIANGULAR MAPS OF THE SQUARE WITH ZERO TOPOLOGICAL ENTROPY

Vojtěch Pravec

*Matematický ústav Slezské univerzity v Opavě
e-mail: voj.pravec@seznam.cz*

It is known that, for interval maps, zero topological entropy is equivalent to bounded topological sequence entropy as well as to the non-existence of Li-Yorke scrambled triples. In this Thesis we answer the question how the situation changes when instead of interval maps triangular maps of the unit square are concerned.

ON THE LANDESMAN–LAZER TYPE OF CONDITIONS FOR THE ELLIPTIC BVP AT RESONANCE WITH MEASURE DATA

Vladimír Švígler

*Fakulta aplikovaných věd Západočeské univerzity v Plzni
e-mail: svigler@students.zcu.cz*

This work concerns the solvability of the semi-linear elliptic partial differential equations with measure data in the very weak sense, i.e., the solution is an element of the space $L^1(\Omega)$. Particularly,

$$\begin{cases} -\Delta u - \lambda u = g(u) + \mu & \text{in } \Omega, \\ u = 0 & \text{on } \partial\Omega, \end{cases}$$

where Ω is bounded domain in \mathbb{R}^N with C^2 boundary $\partial\Omega$, g is a continuous function and μ is a bounded real Radon measure on Ω such that $|\mu|(\partial\Omega) = 0$. To the best of the author's knowledge, the original contributions to the topic are: the solvability of the problem with $\lambda = 0$ and $g = 0$ for the dimension $N = 2$, the Fredholm alternative for the Laplace's operator with homogeneous Dirichlet boundary conditions in the very weak sense and the solvability of the problem out of and at resonance. The latter is obtained through posing conditions of Landesman–Lazer type on the measure μ . This thesis contains selected results of the author's diploma thesis. Mentor suggested the topic, provided resources in the written and electronic form and consultations and also suggested the example of the application of the results in chemical reactions kinetics modelling.

POLOSPOJITÉ FUNKCIE

Dávid Uhrík

Prírodovedecká fakulta Univerzita Pavla Jozefa Šafárika v Košiciach
e-mail: david.uhrik@gmail.com

Polospojité funkcie zaviedol do matematiky René-Louis Baire vo svojej dizertačnej práci v roku 1899, študoval ich na reálnej osi a dokázal ich niektoré základné vlastnosti v tomto špeciálnom prípade. Odvtedy sa polospojité funkcie objavili v mnohých odvetviach matematickej analýzy či topológie, definované na ľubovoľných topologických priestoroch. Skúmanie ich vlastností trvá až dodnes a majú mnohé aplikácie v spomínaných oblastiach. Z dôvodu rozmanitosti disciplín, kde sa polospojité funkcie vyskytujú, sa táto práca snaží sprehľadniť doterajšie známe výsledky, upresniť ich na úroveň súčasnej matematiky, poprípade zovšeobecniť, keďže topologické priestory neboli ešte pri zrode polospojitých funkcií preskúmané ako dnes. Niektoré dôkazy známymi tvrdeniami sú v súčasnosti ťažko dostupné, v tom prípade sme dôkazy doplnili.

NA INTERVALE NEKONEČNÁ ω -LIMITNÁ MNOŽINA
S PERIODICKÝM BODOM IMPLIKUJE PODKOVU: PRIAMY DÔKAZ**Miroslav Výboštok**

Fakulta prírodných vied Univerzity Mateja Bela v Banskej Bystrici
e-mail: panmiroslav@yahoo.com

Nech $f : I \rightarrow I$ je spojité zobrazenie kompaktného reálneho intervalu I do seba. Ak má f nekonečnú ω -limitnú množinu obsahujúcu periodický bod, potom má f podkovu. V práci uvádzame nový, jednoduchý, priamy dôkaz tohto Šarkovského tvrdenia. Táto práca je súčasne aj zadaním bakalárskej práce autora.

Sekce M3+M4

TEORIE PRAVDĚPODOBNOSTI A MATEMATICKÁ STATISTIKA EKONOMETRIE A FINANČNÍ MATEMATIKA

Porota

Daniel Ševčovič (FMFI UK, Bratislava)
Zuzana Hübnerová (FSI VUT, Brno)
Dan Hlubinka (MFF UK, Praha)

VZDIALENOSTNÁ KORELÁCIA

Katarína Adamčíková*Prírodovedecká fakulta Univerzity Pavla Jozefa Šafárika v Košiciach*
e-mail: katarina.adamcikova.student@gmail.com

V tejto práci sa zaoberáme vzdialenostnou koreláciou. Ide o nový spôsob merania závislosti dvoch náhodných vektorov ľubovoľných rozmerov. Vzdialenostná korelácia má zaujímavú vlastnosť, ktorú všetky doterajšie miery závislosti postrádali. Je totiž rovná nule práve vtedy, keď sú náhodné veličiny nezávislé. V práci sú zhrnuté základné vlastnosti vzdialenostnej korelácie a výberovej vzdialenostnej korelácie. Táto práca zahŕňa aj aplikáciu výberovej vzdialenostnej korelácie pri testoch nezávislosti. V ďalšej časti sa venujeme výpočtu vzdialenostnej korelácie dvojrozmerného normálneho rozdelenia, dvojrozmerného gamma rozdelenia a dvojrozmerného symetrického Laplaceovho rozdelenia. V závere práce porovnávame Pearsonovu koreláciu so vzdialenostnou koreláciou pre rôzne vygenerované typy závislosti. Využívame k tomu vlastné naprogramované procedúry v štatistickom programe STATA.

SOCIÁLNY, EKONOMICKÝ A KULTÚRNY STATUS A JEHO VPLYV
NA PRIDANÚ HODNOTU VO VZDELÁVANÍ**Juraj Falath***Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave*
e-mail: juraj.falath@gmail.com

Lisabonská stratégia kladie na európske vzdelávacie systémy požiadavku produkcie uplatniteľných absolventov v prostredí najvyššej konkurencieschopnosti, dynamiky a súčasne zvyšujúcej sa sociálnej súdržnosti. V príspevku prinesieme metodológiu overovania pridanej hodnoty vo vzdelávaní (PHV) ako jedného z ukazovateľov efektívnosti školy. Pridaná hodnota vo vzdelávaní je nástroj na monitorovanie úrovne vedomostí a kompetencií žiakov využívanom priamo vo vyučovacom procese. V 26 stredných školách sme sledovali počas štyroch rokov 1229 tých istých žiakov a zozbierali pre každého žiaka údaje o výkonoch v celoplošných kognitívnych testovaniach, informácie o ich rodinnom pozadí a výsledky rôznych postojových dotazníkov. Prínosom našej práce je rozsiahle skúmanie a spracovanie faktora socioekonomického statusu (SES) ako novej kontextuálnej premennej vplyvajúcej na úspech žiaka. Použitím metód faktorovej analýzy a analýzy latentných tried spracúvame SES do premenných, ktoré na konci vkladáme do modelu pridanej hodnoty vo vzdelávaní. Naša práca ako prvá prináša metodológiu modelovania pridanej hodnoty vo vzdelávaní, ktorá zohľadňuje vplyv vonkajších kontextuálnych premenných. Prinášame množstvo nových prístupov, odporúčaní do budúcnosti a taktiež transparentne pomenúvame obmedzenia súčasného prístupu. Čiastočné výsledky boli už skôr prezentované na medzinárodnej konferencii Inclusive Growth and Employment in Europe v Bratislave, 3–4. novembra 2015 a práca bola zvolená na publikáciu v Ekonomickom časopise Slovenskej Akadémie Vied. Práca obdržala 1. miesto v súťaži o „Najlepšiu analytickú prácu študenta 2015“ na celoštátnej konferencii Slovenskej štatistickej a demografickej spoločnosti.

ASYMPTOTICKÉ A ROBUSTNÍ VLASTNOSTI STATISTICKÝCH ODHADŮ A TESTŮ S MINIMÁLNÍ PSEUDOVDÁLENOSTÍ

Richard Finger

*Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: richardfinger@gmail.com*

This paper studies robust hypothesis testing. Rényi pseudodistance is used to find robust minimum distance statistical estimators. Using these estimators a Wald-type statistic W_n is constructed and its asymptotic distribution is derived. Based on these results, robust hypothesis tests are constructed. Simulations of parametric tests of composite hypotheses for different families of distributions are carried out. The tests are used on real data examples. The performance of these tests based on a tuning parameter α is discussed.

VÝBĚR MODELU NA ZÁKLADĚ PENALIZOVANÉ VĚROHODNOSTI

Tereza Chlubnová

*Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: tclubnova@seznam.cz*

Často zmiňovaným tématem moderní statistiky je výběr proměnných a odhad regresních koeficientů v datech, kde počet proměnných výrazně převyšuje počet pozorování. V současnosti se na řešení tohoto problému používá penalizace maximální věrohodnosti pomocí vhodně zvolené funkce parametru. Dobrá penalizační funkce by měla ohodnotit přínos proměnné a případně zmenšit či vynulovat příslušný regresní koeficient. Pro svou schopnost vybrat vhodné regresory a zároveň odhadnout parametry v modelu jsou oblíbenými penalizační funkce SCAD a LASSO. Dosavadní pokusy o souhrn vlastností těchto dvou funkcí jsou nedostačující a často lehce zavádějící, jelikož prezentují pouze závěry z různých zdrojů bez jejich hlubšího prozkoumání, proto také některá tvrzení dezinterpretují. Navíc velké množství nově vznikající literatury tento úkol tvoří obtížným. Práce přináší přehled dosavadních výsledků v oblasti vlastností odhadů získaných metodou penalizovaných nejmenších čtverců pomocí LASSO a SCAD pro malý počet regresorů i pro mnohorozměrná data spolu s podrobnějším odvozením klíčových tvrzení. Jelikož míru penalizace a tedy i výběr správného modelu silně ovlivňuje ladící parametr, zaměříme se také na jeho volbu. Dokument je teoretickou částí aktuálně dokončované diplomové práce.

SMĚROVÁ K -FUNKCE PRO STACIONÁRNÍ PROCESY

Kateřina Koňasová

*Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: konasova.k@seznam.cz*

Hlavním tématem této práce je teorie stacionárních bodových procesů, s důrazem na směrovou variantu K -funkce pro bodové procesy v rovině. V první části vyložíme

základy teorie bodových procesů včetně klasické definice K -funkce a jejího neparametrického odhadu. Tato funkce představuje cenný nástroj pro posuzování regularity nebo naopak tendence k vytváření shluků u bodových procesů. Ve druhé části vyslovíme definici směrové K -funkce využívající kruhových výsečí. V této části také leží hlavní přínos práce spočívající v porovnání hodnot směrové K -funkce a jejího neparametrického odhadu pro anizotropní Thomasové procesy a ve využití směrové K -funkce při detekci dominantního směru pro shluková i regulární data. Práce obsahuje vhodně upravenou první a třetí kapitolu bakalářské práce autorky.

NEPARAMETRICKÁ ANALÝZA FUNKCIONÁLNÍCH DAT

Daniela Kuruczová

Přírodovědecká fakulta Masarykovy univerzity v Brně
e-mail: 369088@mail.muni.cz

Jadrové odhady pre reálne dáta patria medzi relatívne dobre preskúmané oblasti neparametrickej analýzy dát. V tejto práci sa venujeme zovšeobecneniu jadrových metód na nekonečne dimenzionálne (funkcionálne) priestory. To nám umožňuje rozšíriť možné vstupy do jadrových metód, napríklad o náhodné krivky. V rámci názornosti prechodu medzi reálnymi a funkcionálnymi dátami sa v práci zaoberáme len jadrovou regresiou. Sústreďme sa na odhad vyhladzovacieho parametra a to hneď štyrmi rôznymi metódami – krížové overovanie, metóda penalizačných funkcií, metóda k najbližších susedov a metóda Chagny-Roche. V praktickej časti tieto metódy porovnávame na simulovaných a reálnych dátach. Ukazuje sa, že na simulovaných dátach sa všetky metódy chovajú podobne, ale pre reálne dáta dostávame výrazne presnejšie odhady pomocou metód k najbližších susedov a Chagny-Roche. Výsledky práce hodlá autorka uplatniť ako svoju diplomovú prácu.

ROYSTONOVE TESTY NORMALITY

Matej Malý

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: matejmaly8@gmail.com

Predmetom tejto práce je predstaviť testy mnohorozmernej normality vymyslené J. P. Roystonom na motívy Shapiro–Wilka. V prvej časti uvádzame konštrukciu testov a ich podrobné odvodenie. Pri programovaní týchto testov sme sa nevyhli sporným situáciám, kde si dva odlišné zdroje navzájom protirečili. Rozpory pokračovali aj pri porovnaní výsledkov našich simulácií pravdepodobnosti chyby prvého druhu s výsledkami z niektorých zdrojov. Stretli sme sa aj s hodnotami, ktoré boli výrazne odlišné od tých našich. Preto sme túto prácu venovali skúmaniu týchto nezrovnalostí a ich čo najpresnejšiemu objasneniu. Ako sa ukázalo, chyba sa vyskytla aj v jednom zo svetovo uznávaných štatistických časopisov, ktorý je indexovaný v prestížnej databáze Web of Science i Scopus. Táto práca predstavuje časť autorovej bakalárskej práce. Získané výsledky plánuje uverejniť v odbornom časopise.

KONEČNÉ PROSTOROVÉ BODOVÉ PROCESY:
ANALÝZA, SIMULACE A ASYMPTOTIKA

Daniela Novotná

*Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: dnlntv@gmail.com*

Práce se zabývá konečnými bodovými procesy s hustotou vzhledem k Poissonovu bodovému procesu. Příkladem této třídy procesů je proces faset, což je speciální případ bodového procesu v d -rozměrném eukleidovském prostoru, kde body jsou reprezentované kompaktními podmnožinami nadrovin s danou orientací, velikostí a tvarem. Dalším příkladem je hard-core proces, což je taktéž bodový proces v d -rozměrném eukleidovském prostoru s vlastností, že každé dva body procesu jsou od sebe vzdáleny alespoň o pevně zvolené $r > 0$. Práce poskytuje ucelené srovnání různých přístupů zkoumání charakteristik těchto dvou reprezentantů.

První přístup spočívá v analytických výpočtech charakteristik. Vlastním výsledkem je odvození tvaru normující konstanty v hustotě a funkce intenzity hard-core procesu na reálné přímce. V literatuře se píše, že analytický tvar těchto charakteristik, zejména u prostorových procesů, odvodit nelze. Na tomto příkladě autorka demonstruje obtížnost analytického přístupu. Najdeme zde ukázkou aplikace odvozených tvrzení spočívající v odhadu parametru hard-core procesu metodou maximální věrohodnosti.

Kontrastem k obtížnosti analytických výpočtů je přístup využívající simulačních technik. Metodou Markov chain Monte Carlo, tzv. Metropolis-Hastingsovým algoritmem je zde simulován speciální proces faset, u něž připustíme jen konečný počet orientací a definujeme pevný tvar. Jeho referenční Poissonův proces má míru intenzity závislou na parametru $a > 0$. Autorka zde využila výsledky simulací, které prováděla ve své bakalářské práci.

Zatímco simulační metody byly aplikovány na proces faset s pevně zvoleným parametrem a , poslední přístup spočívá ve zkoumání asymptotického chování rozdělení procesu faset pro $a \rightarrow \infty$. Ve své bakalářské práci autorka odvodila rozdělení počtů orientací pro pevné a procesu faset v rovině. Přínosem předložené práce je zobecnění výsledku na mnohorozměrné rozdělení v eukleidovském prostoru libovolné dimenze. V literatuře je řešena úloha asymptotického chování střední hodnoty míry všech k -dimenzionálních průsečíků obecného procesu faset v d -rozměrném eukleidovském prostoru. Jako důsledek tohoto výsledku je v práci SVOČ odvozeno asymptotické chování rozdělení pro speciální podmodel.

Výsledky této práce dosud nebyly prezentovány v rámci SVOČ ani v jakémkoliv podobné soutěži.

STOCHASTIC EVOLUTION EQUATIONS WITH
SINGULAR FRACTIONAL NOISE**Tomáš Rubín***Matematicko-fyzikální fakulta Univerzity Karlovy v Praze*
e-mail: tomas.rubin@gmail.com

In this paper, linear stochastic differential equations with additive noise in a Hilbert space driven by a cylindrical fractional Brownian motion with the Hurst parameter $H < 1/2$ are investigated. Under the assumptions on the diffusion coefficient, existence of the mild solution together with its measurability and continuity are proved. The analyticity of the semigroup is not assumed. The existence of a limiting distribution is shown for exponentially stable semigroups. The theory is illustrated on the Heath-Jarrow-Morton model and the stochastic wave equation.

The paper presents the author's original research. The main contribution is the extension of the theory to the case of non-analytic semigroups. The results of this paper are part of the author's Master thesis and have not yet been used in the SVOČ competition.

TOPOLOGICAL SUPPORT OF SOLUTIONS
TO STOCHASTIC DIFFERENTIAL EQUATIONS**Prokop Šimon***Matematicko-fyzikální fakulta Univerzity Karlovy v Praze*
e-mail: prokop.simon@gmail.com

Pro každou pravděpodobnostní míru můžeme definovat její nosič. Jedná se o nejmenší uzavřenou množinu, která má míru rovnou jedné. Tato práce pojednává o stochastických diferenciálních rovnicích a o nosiči jejich řešení. Protože řešením každé diferenciální rovnice je funkce, jedná se o nosič pravděpodobnostní míry na prostoru funkcí. Tato oblast byla poprvé zkoumána Stroockem a Varadhanem (1972). Z dalších významných výsledků jmenujme Gyöngy a Pröhle (1990), což je zároveň základní zdroj pro toto pojednání.

Přínos spočívá částečně v důkladné revizi článku Gyöngy a Pröhle a vyjasnění chybějících důkazů, hlavní je ovšem nový výsledek v podobě charakterizace nosiče řešení v Hölderovských funkcích (dokonce v průniku všech α -Hölderovských prostorů funkcí pro $\alpha \in (0, 1/2)$) za udržení nízkých předpokladů na koeficienty rovnice. Pro difuzi vyžadujeme spojitost druhých derivací a pro drift dokonce pouze lokální Lipschitzovskost a na rozdíl od podobných výsledků si vystačíme bez hladkosti koeficientů. Výsledky jsou ilustrovány možnými aplikacemi.

Práce je inspirována stejnojmennou prací diplomovou, informační obsah obou děl by měl být totožný, ačkoliv z důvodů omezeného rozsahu bylo nutné některé části zredukovat, ve druhé kapitole částečně i s důkazy. Veškerý vlastní přínos i s důkazy však zůstal v práci zachován. Jak tato práce, tak práce diplomová jsou psány v angličtině.

STATISTICKÁ RIGIDITA SYSTÉMŮ SE SOCIO-FYZIKÁLNÍMI INTERAKCEMI

Jana Vacková

*Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: vackoja4@jfifi.cvut.cz*

Nejprve matematicky korektně formalizujeme teorii statistické rigidity, definujeme základní pojmy, jakými jsou intervalové četnosti a unfoldované rozteče, a odvozujeme základní vztahy mezi nimi. Dále zavádíme také pojem shlukové funkce a analyzujeme odlišnost statistické rigidity od tzv. number variance (rozptylu počtu). Nově vybudovanou formalizaci statistické rigidity posléze používáme k odvození Laplaceova obrazu obecného vztahu pro statistickou rigiditu. V druhé části práce normalizujeme a škálovujeme hustotu pravděpodobnosti zobecněného inverzního Gaussova rozdělení (zn. GIG), zároveň přinášíme analytickou aproximaci škálovací konstanty, která zajišťuje její soulad s přesnou hodnotou i pro malé hodnoty parametru tohoto rozdělení. V závěrečné části práce pomocí vztahu pro Laplaceův obraz statistické rigidity predikujeme chování jejího lineárního chvostu v systému částic, jehož rozestupy se řídí právě GIG rozdělením. Nakonec se omezujeme na konkrétnější volbu GIG distribuce, pro níž provádíme vizualizaci a porovnání našich čistě analytických výpočtů s numerickými daty a s dosud používanými fenomenologicky korigovanými formullemi.

Formalizace statistické rigidity vznikla jako součást práce bakalářské (obhájena roku 2015), která byla taktéž prezentována jako soutěžní práce v Rektorysově soutěži v aplikované matematice (2015). Text o GIG distribuci je výňatkem z momentálně vznikajícího výzkumného úkolu (předpokládaná obhajoba roku 2016).

MARKOVOVY PROCESY V ANALÝZE SPOLEHLIVOSTI SLOŽITÝCH PRŮMYSLOVÝCH SYSTÉMŮ

Vít Kubelka

*Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: kubelkavit@gmail.com*

Tato práce se zabývá aplikací Markovových procesů v analýze spolehlivosti složitých průmyslových systémů. Je zde odvozen a podrobně popsán obecný algoritmus, jehož vstupem je strom poruch, ve speciálním tvaru, popisující spolehlivost složitého průmyslového systému, a jehož výstupem je Markovův proces, který popisuje vývoj provozuschopnosti daného systému v čase. Je zde použit předpoklad exponenciálního rozdělení doby do poruchy a doby opravy jednotlivých prvků. V práci je s využitím Markovových procesů popsáno řešení standardních úloh teorie spolehlivosti, které řeší i model využívající pouze stromy poruch. Výhodou je, že nový model analýzy spolehlivosti, který se opírá o Markovův proces popisující daný systém, umožňuje brát v úvahu dynamický vývoj systému a opravy jednotlivých prvků. Navíc oproti klasickému modelu spolehlivosti jsou v této práci s pomocí Markovových procesů řešeny úlohy jako například rozdělení stavů funkčnosti daného systému ve fázi ustáleného běhu či střední doba do selhání systému, které pomocí stromů poruch řešit nelze. Ke

spočítání střední doby do selhání systému je potřeba znát střední dobu do absorpce Markovových procesů se spojitým časem, což je složitá a málo známá úloha využívající hlubší teorie Markovových procesů a martingalů. Dále jsou v této práci odvozeny nestandardní ukazatele spolehlivosti, jako například odhad pravděpodobnosti selhání systému na dobu delší než h , $h > 0$, v průběhu delšího časového úseku t , $t > h$. Všechny výše zmíněné postupy jsou aplikovány na dva konkrétní podsystémy jaderné elektrárny Temelín a s jejich využitím je zde vyřešena důležitá úloha, která je klíčová při strategických rozhodnutích týkajících se řízení jaderné elektrárny Temelín a není možné ji efektivně řešit pouze pomocí stromů poruch. Jedná se o optimalizaci nastavení bezpečnostních předpisů v jaderné elektrárně Temelín tak, aby byla dodržena bezpečnost, ale nedocházelo ke zbytečným ztrátám zisku.

Jedná se o část autorovy diplomové práce.

ON COURNOT–NASH–WALRAS EQUILIBRIA, SOCIAL EQUILIBRIA, THEIR STABILITY AND COMPUTATION

Michal Outrata, Matěj Kouřilek

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: outrata.michal@gmail.com

This work focuses on the topic of so-called Cournot–Nash–Walras equilibrium (CNW) – a concept of equilibrium for hierarchical noncooperative games. In the first part, the aim is at further examination of CNW. We pick up the thread of the previous works referred in the paper and focus on relaxing the standing assumptions on the data of the problem while demanding the same results in both existence and stability.

Further on in the report, one finds a section devoted to a so called social equilibrium problem among the customers on one side and authority of the market on the other. Beside definition and description of the equilibrium, also the existential and numerical side of the problem is challenged and a few computed academical examples are presented.

Sekce M5

MATEMATICKÉ STRUKTURY ALGEBRA, TOPOLOGIE A GEOMETRIE

Porota

Miroslav Kureš (FSI VUT, Brno)
Jaroslav Guričan (FMFI UK, Bratislava)
Pavel Růžička (MFF UK Praha)

TILTING THEORY FOR QUASI-COHERENT SHEAVES

Pavel Čoupek*Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: coupek.p@seznam.cz*

We introduce definition of 1-cotilting object in a Grothendieck category and investigate its relation to the analogue of the standard definition of 1-cotilting module. The 1-cotilting quasi-coherent sheaves on a Noetherian scheme are studied in particular: using the classification of hereditary torsion pairs in the category of quasi-coherent sheaves on a Noetherian scheme X , to each hereditary torsion-free class F we assign a 1-cotilting quasi-coherent sheaf whose 1-cotilting class is F . This provides a family of pairwise non-equivalent 1-cotilting quasi-coherent sheaves which are parametrized by specialization closed subsets of X avoiding the set of associated points of a chosen generator of the category of quasi-coherent sheaves. In many cases (e.g. for separated schemes), this set of avoided points can be chosen as the set of associated points of the scheme. The presented work is a part of author's master thesis.

MNOŽINY GENEROVANÉ ČÍSELNÝMI SOUSTAVAMI
V KVATERNIONECH**Jakub Krásenský***Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: krasejak@fjfi.cvut.cz*

Poziční zápis komplexních čísel pomocí základu $-1 + i$ a cifer 0 a 1 byl zaveden Walterem F. Penneyem. Zobecnění Penneyho výsledků vedlo ke studiu tzv. kanonických numeračních systémů (CNS) na okruhu Gaussových celých čísel. Dnes jsou kanonické numerační systémy v komplexních číslech dobře prozkoumaným tématem.

Tato práce se zabývá pozičními číselnými soustavami a zvláště CNS v nekomutativním tělese kvaternionů. Po úvodu k pozičním soustavám a ke kvaternionům prozkoumáme základní kvaternionové okruhy, tedy Hurwitzova a Lipschitzova celá čísla, s nimiž budeme dále pracovat. Dále následují původní výsledky této práce. Zjistíme, jakou nejmenší abecedu může CNS mít. Ukážeme si, které z těchto minimálních abeced skutečně tvoří CNS se základem $-1 + i$, a posléze rozhodneme, která Hurwitzova celá čísla je možno použít jako základ nějakého CNS. Také prozkoumáme vlastnosti tzv. *kvazikomutujících* abeced, které se zdají být vhodnými pro praktické provádění násobení kvaternionů. V souvislosti s algoritmy pro provádění algebraických operací studujeme i základy teorie konečných automatů a odvozujeme, které operace se pomocí nich dají provést.

V neposlední řadě se práce zabývá i číselnými soustavami, které využívají rovněž záporných mocnin základu, a zkoumá vlastnosti různých množin, které se dají charakterizovat právě pomocí číselných rozvoju.

Poziční číselné soustavy v tělese kvaternionů dosud zkoumány nebyly. Tento text je rozšířenou a přepracovanou verzí bakalářské práce autora.

APPLICATIONS OF INVARIANT OPERATORS
IN REAL PARABOLIC GEOMETRIES**Roland Půček***Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: pucek.roland@gmail.com*

In Riemannian geometry, the fundamental fact is that there exists a unique torsion-free connection (called the Levi-Civita connection) compatible with the Riemannian metric g , i.e. having the property $\nabla g = 0$. In projective geometry, the class of covariant derivatives defining the geometry is fixed and all these covariant derivatives have the same class of (non-parametrized) geodesics. Old (and non-trivial) problem is to find whether these curves are geodesics of a (pseudo-)Riemannian metric. Such projective structures are called metrisable. Surprisingly enough, U. Dini and R. Liouville found in 19th century that the metrisability problem leads to a system of linear PDE's. In the last years, there were several papers dealing with these problems. The projective geometry is a representative example of the so called parabolic geometries (for full description, see the recent monograph by A. Cap and J. Slovák). It was realized recently that the corresponding linear metrisability operator is a special example of the so called first BGG operator. The flat model of projective geometry is the (real) projective space.

In this more general context, the metrisability problem for (pseudo-)Riemannian geometries is naturally generalized to the sub-Riemannian situation. In the recent preprint, D. Calderbank, J. Slovák and V. Souček are discussing the classification of (real) *irreducible* parabolic geometries for which the linearisation method can be applied. A part of the classification is the case of complex simple Lie algebras considered as real Lie algebras.

The aim of this paper is to formulate the linearization method in a full generality and to classify completely the cases of complex simple Lie algebras where the linearisation method is applicable. In Sect. 2, there is a summary of description of invariant differential operators on parabolic geometries and comments how to use it for real cases. A general discussion of the linearisation method is contained in Sect.3. The classification result for the case of complex simple Lie algebras is presented in Sect. 4. Some examples of explicit solutions are contained in Sect. 5. There are several Appendices summarizing results used in the paper.

O BÄCKLUNDOVĚ TRANSFORMACI SINH-GORDONOVY ROVNICE

Jana Sedláková*Matematický ústav Slezské univerzity v Opavě
e-mail: janule015@seznam.cz*

Zabýváme se sinh-Gordonovu rovnicí, popisující plochy kladné konstantní Gaussovy křivosti. Pro tyto plochy Bianchi odvodil Bäcklundovu transformaci a superpoziční princip. V předložené práci je prezentujeme ve tvaru, který je vhodnější pro konkrétní výpočty. Rovnice pro Bäcklundovu transformaci jsou v Riccatiho tvaru a superpoziční

princip je dán racionální funkcí. Ve třetí kapitole nacházíme výchozí řešení vhodné pro aplikaci Bäcklundovy transformace.

INTEGRÁLNÍ FORMULE PRO TOPOLOGICKÉ INVARIANTY

Tomáš Svoboda

Přírodovědecká fakulta Masarykovy univerzity v Brně
e-mail: potkolenky@seznam.cz

Tato práce má za cíl položit základy diferenciální topologie, přesněji, studujeme vektorové bandly a orientovatelnost, vložení do eukleidovských prostorů, transversalitu a obecnou polohu, stupeň hladkého zobrazení a další invarianty. Původním výsledkem je odvození integrálních formulí pro výpočet navíjecího a linkovacího čísla v obecné dimenzi a zobecnění tvrzení o linkovacím čísle z odborného článku. Práce je odevzdávána jako bakalářská.

POZIČNÍ REPREZENTACE ČÍSEL V KUBICKÝCH TĚLESECH

Magdaléna Tinková

Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: tinkomag@fjfi.cvut.cz

Práce je věnována pozičním číselným soustavám, tedy reprezentaci čísel ve tvaru $\sum_{k=1}^n a_k \beta^k$, kde β je báze a a_i jsou prvky konečné množiny cifer, zde nazývané abeceda. Zaměříme se především na takzvané hladové rozvoje čísel v bázi $\beta > 1$ tak, jak je zavedl v roce 1957 A. Rényi.

V soustavách s přirozenou bází má každé racionální číslo posléze periodický zápis. Algoritmy pro aritmetické operace ovšem pracují s čísly, jejichž zápis je konečný. Samozřejmě, a proto ani nezdůrazňovanou vlastností bází $\beta \in \mathbf{N}$ je fakt, že množina čísel s konečným zápisem tvoří okruh. Připustíme-li jako bázi i číslo $\beta \notin \mathbf{N}$, vzniká otázka, zda zmíněná důležitá vlastnost – v literatuře obvykle označovaná jako *Property (F)* – zůstane v platnosti. Jak ukázali Frougny a Solomyak, vlastnost *(F)* vynucuje, aby báze β byla algebraickým celým číslem, jehož sdružené kořeny jsou všechny v absolutní hodnotě menší než jedna. Takové číslo se nazývá Pisotovo. Tato podmínka však není postačující. Navíc se zatím zcela nepodařilo charakterizovat Pisotova čísla s vlastností *(F)*.

Pro Pisotova čísla stupně 2, tedy kvadratické iracionality, je tato otázka vyřešena. Pro Pisotova čísla stupně 3 studoval a vyřešil Akiyama zúženou otázku: které kubické Pisotovy jednotky mají vlastnost *(F)*. Pisotovy jednotky jsou Pisotova čísla, jejichž minimální celočíselný polynom má absolutní člen rovný 1 nebo -1 . Na rozdíl od Akiyamy, který upevnil Pisotovu jednotku a zkoumal, zda má vlastnost *(F)*, my zvolíme kubické reálné těleso K a zkoumáme, kdy v tomto tělese existuje $\gamma \in K$ tak, aby $\mathbf{Q}(\gamma) = \mathbf{K}$, číslo γ byla Pisotova jednotka a mělo vlastnost *(F)*.

Ukážeme, že všechna kubická tělesa $K \subset \mathbf{R}$, která nejsou totálně reálná, takovou Pisotovu jednotku obsahují. O její existenci v totálně reálných tělesech lze rozhodnout díky naší postačující podmínce. Předvedeme, že v případech, kdy není tato podmínka splněna, je vhodné přejít k bázi $-\beta$ a zkoumat analogickou vlastnost $(-F)$. Hlavním našim výsledkem je, že v každém reálném kubickém tělese existuje Pisotova jednotka s vlastností (F) nebo $(-F)$. Navíc, pokud se neomezíme na algebraické jednotky, dojdeme k závěru, že v každém reálném kubickém tělese existuje Pisotovo číslo s vlastností (F) .

ROVNOMERNÁ VLASTNOST STABILITY PRE DUÁLNE MRIEŽKY

Martin Vodička

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: mato.vodicka@gmail.com

V práci dokážeme istú rovnomernú vlastnosť stability pre duálne mriežky vektorových mriežok v \mathbb{R}^n . Intuitívne, ak sa nejaký vektor správa „takmer ako vektor z duálnej mriežky“ v tom zmysle, že dostatočne veľkú časť danej mriežky zobrazuje dostatočne blízko k celým číslam, tak tento vektor je už dostatočne blízko k nejakému vektoru duálnej mriežky. Dôkaz tohto tvrdenia je nekonštruktívny, keďže využíva konštrukciu ultraprojektu. Výsledok zovšeobecňuje analogické tvrdenie pre celočíselné mriežky z práce „M. Mačaj, P. Zlatoš – Approximate extension of partial ε -characters of Abelian groups with application to integral point lattices“. Dôkazom tohto zovšeobecného tvrdenia sa autor zaoberá aj v závere svojej bakalárskej práce.

Sekce M6

MATEMATICKÉ STRUKTURY TEORIE GRAFŮ A KOMBINATORIKA

Porota

Jaroslav Ivančo (PF UPJŠ, Košice)
Jaroslav Hrdina (FSI VUT, Brno)
Martin Pergel (MFF UK, Praha)

CHARACTERIZING DAG-DEPTH OF DIRECTED GRAPHS

Matůš Bezek*Fakulta informatiky Masarykovy Univerzity v Brně
e-mail: 422743@mail.muni.cz*

We study DAG-depth, a depth measure of directed graphs, which naturally extends the tree-depth of ordinary graphs. We define a DAG-depth decomposition as a strategy for the cop player in the lift-free version of the cops-and-robber game on directed graphs. The DAG-depth decomposition is defined from DAG-depth in a similar way as an elimination tree is defined from the tree-depth. We provide a definition of the mergeable and optimally mergeable vertices in order to make decomposition smaller and acceptable for the cop player as a strategy. We also define a closure, which finds the largest digraph for which the given decomposition represents a winning strategy for the cop player.

ĽAHKÉ HRANY V ROVINNÝCH GRAFOCH
S DUÁLNOU VÁHOU ASPOŇ 10**Katarína Čekanová***Prírodovedecká fakulta Univerzity Pavla Jozefa Šafárika v Košiciach
e-mail: k.cekanova@gmail.com*

Cieľom tejto práce bolo skúmať štrukturálne vlastnosti rovinných grafov s $\delta(G) \geq 2$, $\rho(G) \geq 3$, a vhodnými dodatočnými podmienkami. V roku 1955 Kotzig dokázal, že každý 3-súvislý rovinný graf obsahuje hranu, ktorej súčet stupňov koncových vrcholov je najviac 13. Borodin v roku 1989 rozšíril tento výsledok na normálne rovinné mapy (t.j. rovinné grafy s $\delta(G) \geq 3$ a $\rho(G) \geq 3$). Jendroľ dokázal existenciu hrany typu $(3, 10)$, $(4, 7)$, alebo $(5, 6)$ v takýchto grafoch.

Ak zmenšíme hodnotu $\delta(G)$ na 2, tak graf G nemusí nutne obsahovať ľahkú hranu, ale situácia sa podstatne zmení, ak do úvahy zoberieme obvod grafu. Cranston a West dokázali, že každý rovinný graf s $\delta(G) \geq 2$ a $g(G) \geq 7$ obsahuje 2-vrchol susedný s vrcholom stupňa najviac ak 3. Jendroľ a Maceková popísali štruktúru hrán v rovinných grafoch s $\delta(G) \geq 2$ a $g(G) \geq 5$.

V tejto práci ukážeme, že každý súvislý rovinný graf s $\delta(G) \geq 2$, $\rho(G) \geq 3$, a duálnou váhou $w^*(G) \geq 10$ obsahuje hranu typu $(2, 10)$ alebo $(3, 3)$. Navyše tieto hranice sú najlepšie možné.

CIRCULANT GRAPHS OF DIAMETER 2 AND SUM-FREE SETS

Peter Fratrič*Stavebná fakulta Slovenskej technickej univerzity v Bratislave*
e-mail: fratric.p@gmail.com

We study the relationship between sum-free sets and large circulant graphs of diameter 2 and given degree. Our investigation is supported by numerous computational experiments for both sum-free sets and generating sets of circulant graphs.

ARCHIMEDOVSKÉ MAPY NA NEORIENTOVATELNÝCH PLOCHÁCH
A OPERÁCIE NA HYPERMAPÁCH**Mária Nedelová***Fakulta prírodných vied Univerzity Mateja Bela v Banskej Bystrici*
e-mail: maria.nedelova@gmail.com

História skúmania mnohostenov siaha až k starovekým Grékom. Tých veľmi zaujímali symetrie, možno aj preto považovali Platónske telesá za symboly 4 základných živlov. Avšak ich kombinatorické zovšeobecnenia nie sú až také staré. V tejto práci nahliadneme do problematiky moderným jazykom. Preskúmame aj ďalšie plochy a primárne sa budeme venovať neorientovaným plochám. Zadefinujeme archimedovské mapy na neorientovateľných plochách, geometricky definujeme operácie na hypermapách, urobíme klasifikáciu archimedovských telies na sfére pomocou Riemann-Hurwitzovej vety a klasifikáciu archimedovských máp na projektívnej rovine. Súčasne uvedieme súhrn najdôležitejších pojmov a vzťahov v teórii máp. Táto práca sa bude venovať telesám ako aj hypermapám. Ďalej je v tejto práci spracovaná rozsiahla obrazová príloha archimedovských máp na sfére a projektívnej rovine. Práca priamo nadväzuje na moju bakalársku prácu s rovnakým názvom.

THE HELLY NUMBERS OF SYSTEMS OF SETS WITH BOUNDED
ALGEBRAIC AND TOPOLOGICAL COMPLEXITY**Jakub Sosnovec***Matematicko-fyzikální fakulta Univerzity Karlovy v Praze*
e-mail: j.sosnovec@email.cz

Maehara has shown that a family F of at least $d + 3$ spheres in \mathbb{R}^d has a nonempty intersection if every $d + 1$ spheres from F have a nonempty intersection. We extend this result in two directions.

On the one hand, we show an analogous theorem holds for families of pseudospheres, i.e., systems of sets such that the intersection of any subsystem is homeomorphic to a sphere of some dimension or is empty.

On the other hand, a sphere in \mathbb{R}^d can be expressed as a zero set of a real polynomial. For a set of polynomials P , the Helly number of the family of zero sets of

polynomials from P is bounded by the dimension of the vector space generated by P . For spheres, however, Maehara's result gives a stronger bound. We show some general sufficient assumptions that allow better bounds on the Helly number in this context.

GENERALIZED PSEUDOPALINDROMIC CLOSURES

Tereza Velká

*Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: velkater@jfifi.cvut.cz*

The work is devoted to a current topic of combinatorics on words – infinite binary words generated by a construction called generalized pseudopalindromic closure, known as generalized pseudostandard words. They were first introduced in 2006 and are a generalization of standard Sturmian words and pseudostandard words: instead of considering only one type of pseudopalindromic closure, an infinite sequence of involutory antimorphisms is considered. Binary generalized pseudostandard words were primarily studied in the paper of A. Blondin-Massé et al. in 2013. Based on their results, this work extends them and present several new results in the following directions:

- We recall their proposition about the normalized form of a directive bi-sequence of a binary generalized pseudostandard word and prove it in a different and simpler manner.
- We summarize their results concerning generalized pseudostandard words with complexity $2n$, also called Rote words. If we apply the operation S (addition of consecutive letters mod 2) on these words, we obtain standard Sturmian words, which are also a special class of generalized pseudostandard words. We ask and answer the question: Which generalized pseudostandard words remain generalized pseudostandard words after the application of the operation S ?
- We focused on the problem of finding which generalized pseudostandard words constructed with more antimorphisms are fixed points of morphisms. We found a new class of aperiodic binary words satisfying this condition and we conjecture that it is the only class having those properties.
- As an important part of this work, we implemented programs in order to work with generalized pseudostandard words. They are written in Python language and helped us to get and test our results. We present them in Appendices.

BINÁRNÍ PROJEKCE ARNOUXOVÝCH–RAUZYOVÝCH SLOV

Vojtěch Veselý

*Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: veselvo2@jfifi.cvut.cz*

V této práci se věnujeme binárním projekcím π , což jsou morfismy do dvoupísmenné abecedy, při kterých mají obrazy písmen délku 1. Aplikujeme je na k -ární Arnouxova–Rauzyova slova \mathbf{u} , která jsou zobecněním sturmovských slov na vícepísmenné abecedy.

Ukážeme, že od určitého N je ve slově $\pi(\mathbf{u})$ právě k levých speciálů, faktorová komplexita je tvaru $\mathcal{C}_{\pi(\mathbf{u})}(n) = (k-1)n + q$ pro nějaké $q \in \mathbb{Z}$, a popíšeme všechny bispeciály délky větší než N . Najdeme dolní mez pro počet návratových slov k dostatečně dlouhým faktorům slova $\pi(\mathbf{u})$ a nalezneme konstantu, která pro libovolnou délku omezí počet faktorů majících méně než k návratových slov.

Sekce M7

APLIKOVANÁ MATEMATIKA NUMERICKÁ ANALÝZA

Porota

Jiří Vala (FS VUT, Brno)
Angela Handlovičová (SvF STU, Bratislava)
Petr Nečesal (KMA ZČU, Plzeň)

NUMERICKÝ VÝPOČET FUNKCIE ČASU PRÍCHODU LESNÉHO POŽIARU V NEHOMOGENNOM PROSTREDÍ

Róbert Blaschke

Stavebná fakulta Slovenskej technickej univerzity v Bratislave
e-mail: robert.blaschke@gmail.com

Práca sa bude zaoberať numerickým riešením úlohy postupu hranice lesného požiaru, v ktorej sa pre každú priestorovú súradnicu výpočtovej oblasti bude určovať čas príchodu hranice požiaru. Hlavnou úlohou práce bude implementovať metódu pre prípad nerovnomernej rýchlosti šírenia sa požiaru zadanej pomocou lesníckej typologickej mapy.

REGISTRÁCIA MRAČIEN BODOV Z 3D SKENEROV

Lenka Hrapková

Stavebná fakulta Slovenskej technickej univerzity v Bratislave
e-mail: lenkahrapkova@gmail.com

Práca prezentuje proces registrácie 3D mračien bodov získaných pomocou skenerov a vytváranie virtuálnej podoby 3D objektov pomocou zarovnaných množín bodov. Objektom skúmania našej práce bola knižnica Point Cloud Library, predovšetkým jej funkcie zamerané na registráciu, hľadanie optimálnej transformácie, určovanie korešpondujúcich bodov a vizualizáciu. Cieľom práce bolo vysvetlenie jednotlivých krokov procesu registrácie, vytvorenie modelových situácií, návrh postupu hľadania optimálnej rotácie, translácie a porovnanie kvality registrácie, prípadne jej častí, zmenou parametrov vplývajúcich na proces zarovnania.

PARALLELIZATIONS OF TFETI-1 COARSE PROBLEM

Jakub Kružík

Fakulta elektrotechniky a informatiky
Vysoké školy báňské – Technické univerzity Ostrava
e-mail: jakub.kruzik@vsb.cz

The FETI based methods, used for the solution of elliptical partial differential equations, form a highly successful class of domain decomposition methods used for parallelization of well known finite element methods. In the FETI methods we partition the original problem into smaller problems defined on subdomains. Since the subdomains are non-overlapping we can naturally solve the smaller problems independently in parallel. We want to increase the number of subdomains so that the smaller problems are solved faster. This however leads to the increase in the size of the coarse problem. Moreover, for complex problems, the number of coarse problem solutions needed can be very high. Therefore, it is important to find the solution of the coarse problem

efficiently. This Bachelor's thesis deals with parallelization strategies of the TFETI-1 coarse problem. The contribution of this work lies in the evaluation of aforementioned strategies on large scale problems. These results are applicable for most of the FETI based methods. A thorough analysis of the strategies and their implementation into PERMON toolbox had been done before the numerical experiments.

HĚADANIE KOREŇOV KOMPLEXNÝCH FUNKCIÍ

Erika Straková

*Fakulta elektrotechniky a informatiky
Vysoké školy báňské – Technické univerzity Ostrava
e-mail: erika.strakova.st@vsb.cz*

Táto práca sa zaoberá hľadáním koreňov holomorfných funkcií vo vnútri istej Jordanovej krivky. V prvej časti práce sú pripomenuté niektoré pojmy z komplexnej analýzy, ktoré budú v práci často používané. Potom sa zameriame na známe vety z komplexnej analýzy, týkajúce sa koreňov holomorfných funkcií. Z týchto viet bude v druhej časti práce dôležitý dôsledok reziduovej vety. Prvá časť práce taktiež obsahuje niektoré dôkazy základnej vety algebry. Druhá časť práce popisuje metódy hľadania koreňov holomorfných funkcií. Prvou metódou je metóda Newtonových súm, ktorej cieľom je zostaviť polynóm s rovnakými koreňmi ako daná funkcia. Druhá metóda je založená na formálnych ortogonálnych polynómoch. Podstata tejto metódy spočíva vo vytvorení matic, ktorých vlastné čísla sú korene danej funkcie. Za prínos práce je možné považovať spracovanie a implementáciu oboch metód a taktiež porovnanie týchto metód na rôznych príkladoch. Práca je zároveň diplomovou prácou autorky a nikdy nebola podaná do súťaže SVOČ ani podobných súťaží.

NUMERICKÉ METODY PRO HLEDÁNÍ VLASTNÍCH ČÍSEL

Mária Šimková

*Přírodovědecká fakulta Masarykovy univerzity v Brně
e-mail: 379697@mail.muni.cz*

V tejto práci sa zaoberáme problémom vlastných čísel na konečne rozmernom priestore. Pričom dôraz hlavne kladieme na odvodenie konvergencie numerických metód za vhodných predpokladov prípadne odvodenie odhadu vzdialenosti medzi exaktnými a aproximativnými vlastnými hodnotami (vektormi) nejakého lineárneho operátora. Týmto spôsobom sa zaoberáme mocninovou metódou a metódou Rayleighovho podielu, pri ktorej konvergencia je odvodená na základe ideí o operátorovej funkcii. Ďalej sa venujeme projekčným metódam na Krylovove podpriestory, kde napríklad popisujeme Arnoldiho metódu za využitia Householderovej transformácie. V prípade niektorých projekčných metód diskutujeme vzťah medzi generátormi Krylovových podpriestorov a formálne ortogonálnymi polynómami. Tiež sa venujeme porovnaniu exaktných a aproximativných vlastných hodnôt (vektorov) určených Lanczosovým algoritmom

za využitia Čebyševových polynómov. Na záver porovnáme diskutované algoritmy na vhodných príkladoch. Táto práca je zároveň autorkinou diplomovou prácou.

Sekce M8

APLIKOVANÁ MATEMATIKA MATEMATICKÉ MODELY DYNAMIKY

Porota

Peter Frolkovič (SvF STU, Bratislava)
Richard Kollár (FMFI UK, Bratislava)
Zdeněk Pospíšil (PřF MU, Brno)

INFLUENCE OF MATERIAL PARAMETERS ON STABILITY
OF THERMAL CONVECTION

Mark Dostálík

*Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: mark.dostalik@gmail.com*

The thesis is focused on the investigation of Rayleigh-Bénard problem in an extended setting approximating the conditions in the Earth's mantle. The aim is to evaluate the influence of depth- and temperature- dependent material parameters, dissipation, adiabatic heating/cooling and heat sources on the qualitative characteristics of thermal convection. We identify the critical values of dimensionless parameters that determine the onset of convection and characterize the dominating convection patterns in marginally supercritical states. These issues are addressed by the application of linear stability analysis and weakly non-linear analysis. It has been found that the character of convection differ substantially from the standard case of Rayleigh-Bénard convection.

NUMERICKÉ ŘEŠENÍ DVOUFÁZOVÉHO NEMÍŠIVÉHO FILTRAČNÍHO
PROUDĚNÍ S KAPILARITOU A JEHO IMPLEMENTACE NA GPU

Jakub Klinkovský

*Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: klinkjak@fjfi.cvut.cz*

Tato soutěžní práce se zabývá numerickým řešením dvoufázového nemíšivého proudění v porézním prostředí a implementací masivně paralelního řešiče využívajícího moderní architektury GPU. Pro numerické řešení zformulované úlohy sestavíme semi-implicitní numerické schéma založené na hybridní metodě smíšených konečných prvků a metodě konečných objemů. Pro zlepšení numerických vlastností schématu je využita upwindová stabilizace a metoda mass-lumping. Schéma je implementováno pro paralelní architektury GPU s využitím platformy CUDA a knihovny TNL. Experimentální analýzou řádu konvergence pro testovací úlohy se známým semi-analytickým řešením ověříme správnost implementace a konvergenci numerického schématu. Chování různých modelů kapilarity a variant numerického schématu při řešení advekčně-difúzních úloh v heterogenním prostředí ověříme pomocí úlohy s referenčním řešením publikovaným v literatuře. Pro zvolenou testovací úlohu porovnáme efektivitu paralelního výpočtu na GPU a provedeme podrobnou analýzu efektivity paralelizovaného algoritmu.

INFILTRÁCIA VODY DO NENASÝTENÉHO PORÉZNEHO VALCA V GRAVITAČNOM POLI A PRI CENTRIFUGÁCII

Patrik Mihala

*Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislavě
e-mail: pmihala@gmail.com*

Táto práca sa zaoberá vypracovaním efektívnej numerickej metódy na riešenie matematického modelu infiltrácie vody v poréznom prostredí. Táto numerická metóda má slúžiť na riešenie inverzných úloh pri určovaní modelových dát vplyvu kapilárnych síl. Prúdenie v nenasýtenom poréznom prostredí je generované kapilárnymi silami a gravitačnou silou, prípadne silou centrifugácie. Vzorka porézneho materiálu je v tvare valca, ktorý je ponorený vo vode vo valci s väčším polomerom. Cez bočný plášť vzorky sa voda infiltruje vplyvom vnútorných kapilárnych síl a hydrostatického tlaku, prípadne tlaku z odstredivej sily centrifúgy. Je to originálny scenár pre určovanie hydrologických dát daného porézneho prostredia. Jediným požadovaným meraním je určovanie množstva vody, ktoré sa infiltrovalo do poréznej vzorky v skúmanom časovom intervale. Doteraz sa používali vzorky v tvare úzkeho valca, kde sa voda infiltrovala len hornou základňou valca a bočný plášť bol izolovaný. To viedlo na jednorozmernú úlohu pozdĺž osi valca. V praxi to spôsobovalo vážne technické problémy, kde bolo ťažko zabrániť prúdeniu medzi okrajom valca a izoláciou. Okrem toho vo valci vznikajú preferenčné cesty prúdenia a tak jednorozmerná aproximácia nie je dostatočne presná a ťažko realizovateľná. My skúmame vzorku ako trojrozmerný valec, kde infiltrácia prebieha po celej bočnej stene, čo významne redukuje predchádzajúce ťažkosti. Na druhej strane riešenie tohto problému je oveľa náročnejšie.

APPLICATIONS OF PLANAR AND SPACE CURVE EVOLUTION

Jiří Minářčík

*Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: minarji2@fjfi.cvut.cz*

In the presented work, we examine the theory of evolving curves and explore their use in commercial and academic applications. In the theoretical section of the text, both numerical and analytical aspects of the problem are investigated by three different approaches. Within the parametric approach, we derived a numerical algorithm for space curve evolution based on osculating circles. When coupled with the point redistribution process, this algorithm has been proven to satisfy the maximum principle in the context of the curve shortening flow. The work also contains a derivation of new mathematical framework for describing curves in space which is a combination of the parametric and implicit approach. The method has been developed to simulate the geodesic flow on both stationary and moving surfaces.

In the final chapter, we investigate four different applications of methods based on evolving curves. First three applications, namely image segmentation, noise reduction and shape matching, belong to the domain of image processing. Methods in all three listed categories have been implemented in C++ and tested on real data. In the last

application, we study a mathematical model for the river channel centreline migration caused by the meandering process. Several modifications to the model have been made and tested. The modified model is able to detect the creation of Oxbow lakes, it simulates the influence of local sinuosity to the streamwise bed slope and deals with heterogeneous river bed erodibility.

The content of this work will be included in my future bachelor thesis. The presented results have not yet been used in the SVOČ competition.

MODELOVÁNÍ POHYBU KAPALINY V POHYBUJÍCÍ SE NÁDRŽI

Michal Mrázek

Fakulta strojního inženýrství Vysokého učení technického v Brně
e-mail: y161568@stud.fme.vutbr.cz

Tato práce se zabývá matematickým modelem pohybu kapaliny v nádrži. Je zavedena základní Laplaceova rovnice a stanoveny okrajové podmínky pro obdélníkovou nádrž v klidu a pro nádrž podstupující horizontální oscilaci. Následně je odvozena rovnice pro vychýlení hladiny v oscilující nádrži a rovnice pro vlastní frekvence. Na základě těchto rovnic je navrženo opatření proti nadměrnému vychýlení hladiny v podobě příček. V závěru práce je porovnán analytický model s numerickým modelem jiného autora s uspokojivými výsledky. Práce se jen velmi málo liší od podoby autorovy bakalářské práce a nenavazuje na žádné dílo podané do SVOČ v předchozích letech.

TESTOVÁNÍ FÁZOVÉ STABILITY A VÝPOČET ROVNOVÁŽNÝCH STAVŮ VÍCESLOŽKOVÝCH SMĚSÍ

Tomáš Smejkal

Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: smejkaltomas@seznam.cz

V této práci odvodíme kritérium stability vícesložkové směsi při konstantní celkové vnitřní energii, objemu a látkovém množství. Zároveň představíme nový numerický algoritmus pro testování fázové stability, který bude založený na modifikované Newtonově metodě. Dále představujeme nový algoritmus pro výpočet fázové rovnováhy o p fázích při konstantní vnitřní energii, objemu a látkovém množství. Tento algoritmus je založen na přímé maximalizaci celkové entropie systému vzhledem k omezujícím podmínkám na vnitřní energii, objem a látková množství. Algoritmus využívá modifikovanou Newtonovu metodu a spolu s modifikovanou Choleského dekompozicí hessiánu generuje posloupnost stavů s rostoucí entropií. Vlastnosti algoritmů jsou ukázány na několika úlohách pro testování stability, případně pro hledání fázové rovnováhy vícesložkových směsí. Tato práce je první verzí výzkumného úkolu (ročníková práce studentů prvního ročníku magisterského studia na FJFI ČVUT v Praze).

TRANSPORT TEPLA A VODY V PÓROVITOM PROSTREDÍ

Michal Tóth

*Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: m.toth82@gmail.com*

V práci sa skúma transport vody a tepla v pórovitom prostredí. Tok vody je spôsobený kapilárnymi silami pórovitého prostredia a gravitačnou silou. Pri tomto transporte dochádza k výmene tepla medzi vodou a pórovitým prostredím. Okrem toho daný matematický model zahŕňa pôsobenie vonkajších teplotných a vlhkostných vplyvov.

Práca je zameraná na vytvorenie efektívnej numerickej metódy riešenia tejto zloženej úlohy. Matematický model systému vedie na riešenie troch silne viazaných parabolických konvekčno difúzných rovníc, z ktorých infiltrácia vody je popísaná silne nelineárnou a degenerovanou parabolickou rovnicou. Danú úlohu budeme aplikovať na skúmanie tepelno izolačných vlastností fasád, čo v kolmom reze vedie na 2D oblasť.

Táto problematika má využitie na skúmanie vplyvu vonkajších poveternostných podmienok na budovy a iných problémov v enviromentalistike, obzvlášť pri interpretácii, kde nahradíme teplo rozpustným kontaminantom, ktorý sa v pórovitom prostredí adsorbuje (v reverzibilnom móde).

Veľký dôraz sa kladie na presnosť a rýchlosť numerickej metódy, pretože výpočet priamej úlohy môže slúžiť pri riešení inverzných úloh (škálovanie daného modelu), kde je potrebné viacnásobne riešiť priamu úlohu s pozmenenými modelovými parametrami. Spomedzi viacerých numerickej metód sa ukázala ako najefektívnejšia metóda *operator-splitting*, ktorú sme použili.

Téma tejto práce je zároveň predmetom autorovej diplomovej práce odovzdávanej o rok. Autorovým prínosom je rozšírenie modelu na 2D, zahrnutie vedenia tepla a zavedenie parametrizácie iterácií, čím sa dospelo k značnému urýchleniu algoritmu.

Sekce I1

TEORETICKÁ INFORMATIKA

Porota

Tomáš Brázdil (FI MU, Brno)
Dana Pardubská (FMFI UK, Bratislava)
Martin Pilát (MFF UK, Praha)

MINIMALITY PROBLEMS FOR PROMISE VERSIONS
OF NITE AUTOMATA

Michal Ajdarów

Fakulta informatiky Masarykovy Univerzity v Brně
e-mail: 422654@mail.muni.cz

In this paper we explore some minimality problems concerning *promise version deterministic finite automata* (pvDFA) in recognizing and solving modes of acceptance. In particular we prove that the minimal pvDFA recognizing a promise problem is determined uniquely, and design a new algorithm for finding this pvDFA. We then describe an algorithm to decide whether a given pvDFA solves a given promise problem that is defined using pvDFA or deterministic push-down automata, and show that this problem is not always decidable for different promise problems. We show that the problem of finding a minimal pvDFA solving a given promise problem is not always solvable. We prove that it is not always decidable whether a given promise problem can be solved by a pvDFA. At the end we explore union, intersection and concatenation of promise problems.

A SIMPLER BIT-PARALLEL ALGORITHM FOR SWAP MATCHING

Václav Blažej, Ondřej Suchý, Tomáš Valla

Fakulta informačních technologií Českého vysokého učení technického v Praze
e-mail: blazeva1@fit.cvut.cz

The pattern matching problem with swaps is to find all occurrences of a pattern in a text while allowing the pattern to swap adjacent symbols. The goal is to design fast matching algorithm that takes advantage of the bit parallelism of bitwise machine instructions. We point out a fatal flaw in the algorithm proposed by Ahmed et al. [The swap matching problem revisited, Theor. Comp. Sci. 2014], which we describe in detail. Furthermore we devise a new swap pattern matching algorithm which is based on the same graph theoretical model as the algorithm by Ahmed et al. (thus still not based on FFT) and we prove its correctness. We also show that an approach using deterministic finite automata cannot achieve similarly efficient algorithms.

ON-LINE MULTIPLICATION AND DIVISION
IN NON-STANDARD NUMERATION SYSTEMS

Marta Brzicová

Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: m.brzicova@gmail.com

In 1977, Trivedi and Ercegovic invented algorithms for on-line multiplication and division in numeration systems with a positive integer base β and a symmetric integer set of digits $\mathcal{A} = \{-M, -M + 1, \dots, 0, 1, \dots, M\}$.

Generally, a numeration system is given by a base β , a real or complex number such that $|\beta| > 1$, and by a set of digits \mathcal{A} , a finite set of real or complex numbers (including 0). In the presented work, we first formulate a generalized version of the on-line algorithms for multiplication and division of Trivedi and Ercegovic for the cases that β is any real or complex number, and digits are real or complex.

We show that if (β, \mathcal{A}) satisfies the so-called (OL) Property, then on-line multiplication and division are feasible by our modification of the Trivedi–Ercegovic algorithms. For a real base β and a digit set \mathcal{A} of contiguous integers, we have a simple instrument for verifying the (OL) Property: the system (β, \mathcal{A}) has the (OL) Property if $\#\mathcal{A} > |\beta|$. For a given complex base β , our work provides a recipe for finding a symmetric alphabet \mathcal{A} of contiguous integers such that the system (β, \mathcal{A}) has the (OL) Property.

Provided that addition and subtraction are realizable in parallel in the system (β, \mathcal{A}) , our on-line algorithms for multiplication and division have linear time complexity – which means we receive the first n digits of the output with only (constant $\cdot n$) steps.

Four examples are presented in detail: base $\frac{3+\sqrt{5}}{2}$ with alphabet $\{-1, 0, 1\}$; base $2i$ with alphabet $\{-2, -1, 0, 1, 2\}$ (a redundant Knuth numeration system); base $-\frac{3}{2} + i\frac{\sqrt{3}}{2}$ with alphabet $\{0, \pm 1, \pm\omega, \pm\omega^2\}$ (a redundant Eisenstein numeration system); base $i - 1$ with alphabet $\{0, \pm 1, \pm i\}$ (a redundant Penney numeration system).

L(2, 1)-FARBENIE KAKTUSOV

Anna Dresslerová

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislavě
e-mail: anna.dresslerova@gmail.com

L(2, 1)-farbenie je vzdialenosťou podmienené farbenie, ktoré priradzuje vrcholom prirodzené čísla s nulou. Ak sú vrcholy u a v susedia, tak ich farby sa musia líšiť aspoň o dva a ak sú vo vzdialenosti dva, tak musia mať rôzne farby. Chceme vedieť, aké je najmenšie číslo k , že existuje *L(2, 1)*-farbenie grafu G , ktoré nepoužíva čísla väčšie ako k . Toto číslo potom označujeme $\lambda(G)$. Nájsť $\lambda(G)$ je vo všeobecnosti veľmi ťažké. Dokonca otestovať či $\lambda(G) \leq k$ je NP-úplný problém už pre sériovo-paralelné grafy. Existuje len málo tried grafov, kde je tento problém polynomiálne riešiteľný. Triedy, ktoré patria do tejto kategórie sú stromy a grafy s konštantným počtom cyklov. My sme tento poznatok rozšírili o triedu cyklových stromov (kaktusy s vrcholovo disjunktnými kružnicami). Ďalej sme určili tesné odhady $\lambda(G)$ vzhľadom na maximálny stupeň grafu. Dokázali sme, že pre kaktusy platí: $\Delta + 1 \leq \lambda(G) \leq \Delta + 3$. Ak navyše $\Delta \geq 5$, tak platí: $\Delta + 1 \leq \lambda(G) \leq \Delta + 2$.

STATE RECOVERY OF RC4 AND SPRITZ REVISITED

Martin Gábris

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislavě
e-mail: martin.gabris22@gmail.com

We provide an improved complexity analysis of backtracking-based state recovery attacks on RC4 and Spritz. Comparing new estimates with known results on Spritz, our analysis shows a significantly lower complexity estimate for simple state recovery attack as well as special state recovery attack. We validated the estimates by performing experiments for selected feasible parameters.

We also propose a prefix check optimization for simple state recovery attack on Spritz. We believe that the simple state recovery attack with this optimization and so-called “change order” optimization inspired by Knudsen et al. attack on RC4 constitutes currently the best state recovery attack on Spritz (when no special state is observed).

Results given in this work are included also in author’s master’s thesis.

VÝPOČTY NA KONEČNÝCH AUTOMATOCH
S POMOCNOU INFORMÁCIOU**Rafael Korbaš**

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: rafael.korbas@gmail.com

Konečné automaty s pomocnou informáciou sú podobné klasickým konečným automatom s tým, že okrem vstupu disponujú navyše ďalším reťazcom, tzv. pomocnou informáciou. V našej práci táto pomocná informácia bude závisieť iba od dĺžky vstupu, t.j. pre všetky vstupy rovnakej dĺžky bude pomocná informácia rovnaká. Budeme skúmať predovšetkým vplyv spôsobu dodania pomocnej informácie, jej dĺžky vzhľadom na dĺžku vstupu a napokon aj determinizmu, resp. nedeterminizmu na výpočtovú silu modelu. Naše výsledky sú zhrnuté v rovnomennej diplomovej práci.

ŠTVOREC NA DETERMINISTICKÝCH A ALTERNUJÚCICH
AUTOMATOCH**Ivana Krajňáková**

Prírodovedecká fakulta Univerzity Pavla Jozefa Šafárika v Košiciach
e-mail: ivana.krajnakova.vt@gmail.com

V práci študujeme operáciu štvorec na deterministických a alternujúcich konečnostavových automatoch. Najskôr ukážeme, že horný odhad $(n-k) \cdot 2^n + k \cdot 2^{n-1}$ pre zložitost štvorca jazyka reprezentovaného minimálnym deterministickým n stavovým automatom, v ktorom je k koncových stavov, je tesný na binárnej abecede ak $1 \leq k \leq n-2$.

Tento výsledek použijeme na definování takého binárního jazyka akceptovaného n stavovým alternujícím automatem, že každý alternující automat pro jeho štvorec má aspoň $n + 2^n + 1$ stavov. Zovšeobecněním tohto nášho výsledku dokazujeme tesnosť horného odhadu $n + 2^n + 1$ pre zložitosť zrežazenia jazykov reprezentovaných alternujúcimi automatmi. Týmto riešime otvorený problém, ktorý formulovali Fellah, Jürgensen, Yu [1990, Internat. J. Computer Math. 35, 117–132]. V druhej časti práce študujeme štvorec jazykov reprezentovaných deterministickými automatmi, v ktorých iba jeden stav je nekoncový. V tomto prípade dostávame tesnú hornú hranicu $(n + 3) \cdot 2^{n-2}$.

SYNCHRONIZAČNÍ ZPOŽDĚNÍ D0L-SYSTÉMŮ

Kateřina Medková

*Fakulta jaderná a fyzikálně inženýrská Českého vysokého učení technického v Praze
e-mail: katerinamedkova@gmail.com*

Práce se věnuje synchronizačnímu zpoždění, což je důležitá konstanta vztahující se k cirkularitě D0L-systémů. Zatímco o cirkularitě zadaného D0L-systému umíme snadno algoritmicky rozhodnout, na stanovení hodnoty synchronizačního zpoždění žádný efektivní algoritmus neexistuje. Nejsou známy ani žádné odhady jeho hodnoty. Proto se této konstantě věnujeme podrobněji. V úvodu zavádíme potřebné pojmy z kombinatoriky na slovech, definujeme D0L-systém a shrnujeme podstatné poznatky o některých vlastnostech D0L-systémů: věnujeme se zejména injektivitě, repetitivnosti, pushy vlastnosti a cirkularitě. Krátce představujeme dříve publikovanou metodu pro generování bispeciálních faktorů, která umožňuje popsat všechny bispeciální faktory v jazycích injektivních cirkulárních D0L-systémů, které nejsou pushy. Ukazujeme, že tuto metodu lze převést do algoritmické podoby, a vysvětlujeme, proč je pro takový algoritmus znalost synchronizačního zpoždění potřebná. Dále se zaměřujeme na stanovování odhadů hodnoty synchronizačního zpoždění. Předkládáme metodu pracující s tzv. přesahovými cihličkami a grafy přesahových cihliček a demonstrujeme její užitečnost u kódů a cirkulárních kódů. Dále se tuto metodu snažíme využít k určování přibližné hodnoty synchronizačního zpoždění cirkulárních D0L-systémů. Úspěšně ji aplikujeme v případě binárních uniformních cirkulárních D0L-systémů a získáváme tak horní odhad synchronizačního zpoždění pro takovéto systémy. Vysvětlujeme také problematičnost postupu v případě obecnějších typů D0L-systémů.

Významná část této práce je součástí bakalářské práce autorky na Fakultě jaderné a fyzikálně inženýrské, ČVUT v Praze. Výsledky této práce byly také publikovány v časopise Theoretical Computer Science.

EVALUATION OF SAT-BASED PREIMAGE ATTACK OPTIMIZATIONS

Ladislav Pápay

*Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislavě
e-mail: svk@lacop.net*

SAT solvers are a universal tool for finding solutions to boolean satisfiability problems. In the past they have been used for cryptographic problems, such as finding preimages for hash functions or obtaining the key for stream ciphers. However these solutions are not easily reusable or modifiable.

In our work we create a modeling library that allows simple creation of SAT instances. We specifically focus on various cryptographic problems, however the library is generic enough that it can be used for other purposes as well.

Using this library we create models for several cryptographic hash functions. Various SAT solvers, optimizations and heuristics are evaluated on these models to compare their performance. These include the use of the Espresso logic minimizer to reduce the instance size, forcing custom variable branching order with help of modified SAT solvers and others.

ON H -TOPOLOGICAL INTERSECTION REPRESENTATIONS
OF GRAPHS**Peter Zeman**

*Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: andrej.kupecky@gmail.com*

Biró et al. introduced in 1992 the concept of H -graphs, intersection graphs of connected subgraphs of a subdivision of H . They naturally generalize many important classes of graphs, e.g., interval graphs and circular-arc graphs. In this paper, we study the complexity of computational problems on H -graphs, i.e., the recognition problem and standard optimization problems such as minimum dominating set and maximum clique.

We partially answer the open question of Biró et al. which asks about the complexity of recognizing H -graphs. For a tree T , we give an XP-time algorithm for recognizing T -graphs. Further, we give an $O(n^4)$ time algorithm for recognizing star-graphs, which a generalization of the well-known split graphs. Moreover, for the minimum dominating set problem on H -graphs, we give an FPT algorithm when H is a star, and an XP algorithm for general H (both are parameterized by the size of H). For the maximum clique problem we give a polynomial time algorithm for Helly H -graphs and show that for some H , it is APX-hard on H -graphs.

Sekce I2

UMĚLÁ INTELIGENCE

Porota

Miloš Šeda (FSI VUT, Brno)
Martin Plátek (MFF UK, Praha)
Mária Lucká (FIIT STU, Bratislava)

GENETICKÉ PROGRAMOVÁNÍ PRO ŘÍZENÍ HEJNA ROBOTŮ

Michal Filippi*Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: michal.filippi@gmail.com*

Homogenní robotická hejna bývají zpravidla řízena programem, který je vytvořen ručně programátorem. Tato práce se zabývá alternativním přístupem, a to možností tvorby řídicích programů pomocí techniky inspirované biologickou evolucí, genetickým programováním. Za tímto účelem byl naprogramován jednoduchý simulátor 2D prostředí, ve kterém je možné vytvořené řídicí programy na homogenním hejnu virtuálních robotů testovat a pozorovat. Schopnost genetického programování vytvářet řídicí programy je zkoumána na třech různých scénách, ve kterých má robotické hejno za úkol plnit tři různé úkoly. Součástí práce je také porovnání genetického programování s technikou využívající neuronovou síť učenou evolučními strategiemi.

Jedná se o bakalářskou práci autora vedenou Mgr. Martinem Pilátem, Ph.D. odevzdanou v akademickém roce 2014/2015 na Matematicko-fyzikální fakultě Univerzity Karlovy.

POUŽITIE NEURÓNOVÝCH SIETÍ PRI SPRACOVANÍ
ZVUKOVÉHO SIGNÁLU**Miroslava Klučárová***Prírodovedecká fakulta Univerzity Pavla Jozefa Šafárika v Košiciach
e-mail: miroslava.klucarova@gmail.com*

V práci je navrhnutá a implementovaná aplikácia, ktorá spracováva zvukový signál do notového zápisu. Pre túto aplikáciu sme navrhli vhodný model klasifikujúcej neurónovej siete, ktorá klasifikuje signály do nôt. V aplikácii sme použili model ART2 neurónovej siete, ktorá úspešne určuje výšky tónov na flaute zahraných melódií a zapisuje ich do notovej osnovy. Aplikácia bola overená na viacerých jednoduchých hudobných skladbách. Dosiahnuté výsledky notového zápisu boli porovnané so skutočným notovým zápisom a úspešnosť je 90 až 98.8%.

AUTOMATICKÉ GENEROVÁNÍ REALISTICKÉHO TERÉNU
POMOCÍ TECHNIK STROJOVÉHO UČENÍ**Jakub Střelský***Matematicko-fyzikální fakulta Univerzity Karlovy v Praze
e-mail: jakub.strelsky@gmail.com*

Umělý terén je důležitou komponentou v oblastech jako jsou počítačové hry, simulace a filmy. Manuální tvorba umělého terénu může být náročný proces, který by v řadě aplikací bylo vhodné nahradit jeho automatickým generováním. V současné době se

dosahuje velkých pokroků při řešení generativních problémů pomocí umělých neuronových sítí, a tak se nabízí možnost prozkoumání jejich schopnosti automatického generování terénu. V této práci se budeme věnovat jedné z neúspěšnějších metod automatického generování obsahu – Generative Adversarial Networks a adaptujeme tuto metodu na problém generování terénu. Výsledný model je schopen generovat realisticky vypadající terén podle rastrového náčrtku zadaného uživatelem a umožňuje jeho interaktivní modelování. Jeho nevýhodou je potřeba velkého množství neoznačených trénovacích dat, avšak zemský povrch jich poskytuje více než dostatek, a tak by tento model mohl díky svým příznivým vlastnostem nalézt své uplatnění v odpovídajících aplikacích.

SKLADANIE DNA SEKVENCIÍ POMOCOU PARALELNÉHO MODELU INŠPIROVANÉHO IMUNITNÝM SYSTÉMOM

Juraj Šimek

*Fakulta informatiky a informačných technológií
Slovenskej technickej univerzity v Bratislave
e-mail: simekjuraj@gmail.com*

V tejto práci sa venujeme návrhu skladača DNA sekvencií, ktorý rieši problém skladania DNA sekvencií jeho pretypovaním na problém obchodného cestujúceho (skr. TSP). Pre potreby riešenia problému obchodného cestujúceho sme navrhli Paralelný imunitný algoritmus s pamäťou, klonovaním, výberom a distribuovanou operáciou zrenia protilátok (skr. PIMCSA-DMO) ako modifikáciu Paralelného imunitného algoritmu s pamäťou, klonovaním a výberom (skr. PIMCSA). Tento algoritmus, inšpirovaný imunitným systémom, používa na svoju činnosť Iterovanú Lin-Kernighanovu heuristiku a Vylepšený Inver-over operátor. Práve tieto dva algoritmy mu poskytujú značnú silu pri hľadaní ciest v TSP. Testovanie preukázalo, že PIMCSA-DMO je vhodný algoritmus pre riešenie veľkých inštancií TSP, ako z hľadiska kvality ciest (kde prekonáva mnohé iné algoritmy), tak aj z času potrebného pre hľadanie týchto ciest a preto je vhodný na aplikáciu v rámci riešenia problému skladania DNA sekvencií. Výsledkom našej práce je teda skladač DNA sekvencií, ktorý vďaka svojej architektúre a vďaka tomu, že implementuje množstvo operátorov pre riešenie TSP, možno použiť i ako framework pre skladanie DNA sekvencií prostredníctvom algoritmov určených na riešenie TSP.

Táto ŠVOČ vznikla ako výsledok riešenia diplomového projektu s názvom Skladanie DNA sekvencií na FIIT STU. Prezentované výsledky neboli doposiaľ použité v žiadnej súťaži, no pripravujeme ich publikáciu v medzinárodných výskumných časopisoch.

KALDI VERSUS HTK: EVALUATION OF SPEECH RECOGNITION FRAMEWORKS ON ALICA DATASET

Marek Šuppa

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: mareksuppa@gmail.com

Kaldi and HTK are both frameworks used for automated speech recognition and other related tasks. While the former is younger in age, it is currently considered to be the best in terms of accuracy on speech recognition tasks. The latter, however, is more established on the scene with high quality instructional material available.

As the name suggests, **HTK** (Hidden Markov Model Toolkit) is centered around Hidden Markov Models (HMMs) which were the central component of speech recognition systems for a long time. In the past decade, however, the speech recognition world has been “taken over” by Deep Learning methods. Given the difficult situation around copyright rights of HTK it was very difficult for it to adapt. HTK’s licensing issues were also part of the reason why the **Kaldi** framework came to be. Possibly thanks to its open license, it was the first of the two to include support for methods based on Deep Neural Networks (DNNs). Since then HTK managed to catch up and also has support for DNNs, but due to the size of its community, its implementation seems to be much less tested and also less robust.

In this work we present an evaluation of both of these frameworks on the Alica dataset. This dataset is comprised of number of recordings of numbers from zero to nine, spoken by 9 to 14 years old kids. The dataset contains 8663 training samples and 1907 testing samples. In the introductory paper of the Alica dataset the HTK framework was used and a HMM-GMM based model was trained using the training samples and tested using the testing samples. We managed to reproduce this experiment and the resulting testing and training accuracies of our model were comparable to the one described in the introductory paper. The same experiment was also reproduced in the Kaldi framework. Since it uses a different processing pipeline, the experiment was not exactly identical. However, without any specific parameter optimization we were able to obtain similar accuracies. The amount of time required to train and test these models on commodity hardware was in both cases significantly smaller than in the introductory paper.

We also trained a DNN-based model on the Alica dataset. The obtained results show an interesting insight into possible improvements of applications based on the Alica dataset.

Sekce I3

POČÍTAČOVÁ GRAFIKA A POČÍTAČOVÉ VIDĚNÍ

Porota

Miloslav Druckmüller (FSI VUT, Brno)
Mariana Remešíková (SvF STU, Bratislava)
Petr Matula (FI MU, Brno)

LOKÁLNE PRÍZNAKY VO FAREBNÝCH OBRAZOCH

Paula Budzáková*Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: budzana@gmail.com*

Aj keď je farba vnímaná ako nenahraditeľný prvok opisujúci svet okolo nás, techniky na extrakciu lokálnych príznakov sú najčastejšie založené na popise tvaru a úplne ignorujú farebnú informáciu. V práci navrhujeme metódu na extrakciu lokálnych príznakov z farebného obrazu. Ako základný model sme si vybrali prístup zameraný na ľudský vizuálny systém, s využitím chromatických oponentných kanálov a metódy SIFT. Ideou riešenia je zakomponovanie chromatických oponentných kanálov nahradením šedotónových informácií v metóde SIFT tak, že kľúčové body sú detegované na dvoch separovaných oponentných kanáloch. Pre nájdené zaujímavé body v oboch kanáloch sú vytvorené príznakové vektory, ktoré sú pre následné príznakové párovanie zrefazované.

VYHLADÁVANIE OBJEKTOV POMOCOU DESKRIPTORA
SHAPE CONTEXT**Roman Chovan**, Branislav Pažický, Pavol Balajka*Fakulta prírodných vied Univerzity Mateja Bela v Banskej Bystrici
e-mail: romco4@gmail.com*

Object detection based on shape context descriptor: The aim of the article is to introduce to a reader search objects based on shape context and their use. Firstly we talk about what shape context is. Secondly we talk about steps of shape context algorithm. Then we talk about Hungarian method. In the end we are presented the results achieved by our implementation.

GENERATION OF LECTURE NOTES AS IMAGES FROM RECORDED
WHITEBOARD AND BLACKBOARD BASED PRESENTATIONS**Ondrej Jariabka**, Marek Šuppa*Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: o.jariabka@gmail.com*

With raising amount of e-learning materials such as lecture videos or on-line video courses, we decided to develop an application, which can help students or content creators in their effort to prepare study materials. Main goal of our application is to create slides from given video, depicting a black or white board without any occluding objects such as lecturer standing in front of this board. Slides will contain valid information from key frames of the given lecture video. Based on the assumption, that the board is static in the video, this is done by extracting the board from video

frames, which is then segmented into equally sized rectangular cells. These cells are stored and the change of information inside them is tracked. Afterwards, the final image is created from saved cells when all cells are sufficiently stable.

ZRÝCHLENIE VÝPOČTU SPLAJN POVRCHOV

Viliam Kačala

Prírodovedecká fakulta Univerzity Pavla Jozefa Šafárika v Košiciach
e-mail: viliam.kacala.ml@gmail.com

Splajny sú dôležitá súčasť počítačovej grafiky. Jedná sa o matematický model krivky a plochy slúžiaci na čo najlepšie spojenie konečnej množiny bodov. Termín najlepšie spojenie v našom prípade znamená hladkú, matematicky ľahko vyjadriteľnú plochu s čo najmenším zakrivením. Využitie splajnov v grafike je veľmi široké od rôznych CAD aplikácií, v štatistike, alebo v analýze dát. Splajny existujú v mnohých formách, či už vo forme krivky v rovine, rôznych trojrozmerných telies, atď. Táto práca si dáva za cieľ navrhnúť, analyzovať a implementovať nový algoritmus pre bikubickú interpoláciu v trojrozmernom priestore.

SNÍMANIE HDR OBRAZU VSTAVANOU KAMEROU V BEŽNÝCH MOBILNÝCH ZARIADENIACH

Pavol Kunovský

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislavě
e-mail: palo.oneill@gmail.com

Cieľom práce je zachytiť a získať HDR obraz pomocou mobilného zariadenia. Presnejšie ide o rekonštrukciu sférickej panorámy “skydome” v HDR kvalite. Následne jej uloženie do použiteľného dátového formátu. Implementovať vhodný “tone-mapping” operátor umožňujúci uspokojivé zobrazenie HDR obrazu na displeji mobilného zariadenia. Neskôr sa tieto dáta dajú použiť na osvetľovanie objektov v 3D scéne.

RÔZNE FORMY OPENGL VIZUALIZÁCIE V PROSTREDÍ WINDOWS A LINUX

Timotej Maták

Stavebná fakulta Slovenskej technickej univerzity v Bratislave
e-mail: timotej.matak@gmail.com

V tejto práci sme sa zamerali na tvorbu multiplatformových vizualizačných aplikácií, slúžiacich na vizualizáciu dát ako na sfére a obdĺžnikovej mriežke, tak aj objemových dát. Vytvorené aplikácie využívajú na časť potrebných výpočtov grafickú kartu,

čím sa urýchľuje samotný proces vykresľovania používateľom zvolených dát. Oba programy sú napísané v jazyku C# pomocou vývojového prostredia Visual Studio 2013, pričom funkčnosť na rôznych platformách zabezpečuje knižnica OpenTK ktorá je voľne dostupným wrapperom pre OpenGL. Aplikácie umožňujú používateľovi zobrazenú scénu ľubovoľne rotovať, škálovať a posúvať, pričom pri objemových dátach, pri ktorých nie je možné dopredu určiť vyhovujúcu farebnú škálu, si túto môže používateľ sám vytvoriť a prípadne uložiť pre opätovné použitie.

PRENOS DÁT POMOCOU OPTICKÉHO DÁTOVÉHO TOKU

Ján Murín

Prírodovedecká fakulta Univerzity Pavla Jozefa Šafárika v Košiciach
e-mail: janmurin2@hotmail.com

Naša práca sa zaoberá analýzou princípov optického dátového prenosu pomocou dvojrozmerných QR kódov a metódami, ktoré tento proces realizujú. Ďalším cieľom je navrhnúť a implementovať nástroj pre prenos súborov, kde sme sa zamerali na prenos súborov medzi dvomi inteligentnými telefónmi. Odosielanie dát sa uskutočňuje ako animácia zakódovaných častí súboru v podobe QR kódov. Druhé zariadenie pomocou kamery kontinuálne sníma animované QR kódy a postupne ich dekoduje, čím dochádza k prenosu dát prostredníctvom jednosmerného optického kanála bez použitia rádiovkej technológie. Vzhľadom na dostatočnú výpočtovú kapacitu inteligentných zariadení a dostupnosť kamier v týchto zariadeniach s vysokým farebným rozlíšením sme navrhli farebný QR kód, ktorý umožňuje vyšší dátový tok. V závere práce porovnávame rýchlosť prenosu dát klasickým QR kódom a nami navrhnutým farebným QR kódom.

SEGMENTÁCIA EXOSÓMOV

Jakub Jozef Páleník

Fakulta informatiky Masarykovy univerzity v Brně
e-mail: 422453@mail.muni.cz

Táto práca sa venuje problému segmentácie exosómov z obrázkov vytvorených pomocou transmisnej elektrónovej mikroskopie. Vysvetľuje známe riešenia podobných problémov a diskutuje vhodnosť aplikácie týchto riešení na obrázky obsahujúce exosómy. Navrhne nový prístup k segmentácii, ktorý podrobne vysvetlí a porovná so známymi riešeniami. Všetky vysvetľované metódy vyhodnotí na sade obrázkov, ku ktorým sú k dispozícii potvrdené výsledky.

IMAGE SEGMENTATION TECHNIQUES IN THE HPC ENVIRONMENT
AND THEIR APPLICATIONS**Marek Pecha***Fakulta elektrotechniky a informatiky
Vysoké školy báňské – Technické Univerzity Ostrava
e-mail: marek.pecha@vsb.cz*

V posledních dvou dekadách se v komunitách, zabývajících se zpracováním obrazu, často skloňuje pojem segmentace obrazu, který je podle standardní definice chápán jako rozdělení obrazu na rozumné oblasti. Je prováděn rozsáhlý výzkum technik pro co nejlepší dosažení očekávaných výsledků, tj. dosažení takového rozdělení digitálního obrazu, aby výsledek vrácený řešičem co nejlépe korespondoval skontextem úlohy. A však podle standardní segmentační teorie dokážeme jenom částečně matematicky analyzovat používané algoritmy a odpovídající dosažené řešení. Navíc vsoučasné době neexistuje žádný obecně známý popis, co můžeme považovat za rozumnou segmentaci obrazu. Proto první část práce je zaměřena na vybudování teorie, která zohledňuje jednak teoretický popis dobře definovaného řešení, které je svázáno skontextem a podstatou segmentační úlohy, ale i reálné chování algoritmů. Tuto teorii jsme nazvali Extended Image Segmentation Theory, neboli Rozšířená teorie segmentace obrazu, a z praktických důvodů je vystavěna na teoriích míry, množin a teorii grafů. Z této teorie navíc vychází věta a její důkaz o topologii objektů na obrazové scéně.

V aplikační části práce jsme se zaměřili na analýzu dvou standardních přístupů tj. využití algoritmů Lloydova typu a metod spektrálního shlukování, a jejich modifikacemi pro běh na superpočítačových platformách a úpravou počátečních podmínek pro dosažení přesnějších výsledků. Rádi bychom vypíchlí, že jako modifikace algoritmů Lloydova typu, jsme navrhli dva algoritmy regular k -means+2 a start-fix k -means. Navíc se v práci povedlo matematicky ukázat typický tvar výsledných obrazových segmentů při použití metody spektrálního shlukování.

Pro řešení komplexnějších úloh z oblasti geomatematiky ve spolupráci s Ústavem Geoniky Akademie věd České republiky byly navrženy algoritmy Simple Method of Reference a Materials Method of Reference Materials, kterými nepřímo navazujeme na Steinhausovu práci z roku 1957. Tyto algoritmy využíváme pro detekci materiálů na CT scanech geokompozitů. Další spolupráci jsme pak navázali s Fakultní nemocnicí Ostrava. V závěru práce jsou představeny dosažené výsledky a je představen i naimplementovaný software, např. desktopová aplikace PermonGeodecomposer, postavená na technologii OpenCL, a masivně paralelní framework PermonGeoMeshCreator. Součástí práce je také publikovaný článek a dva články v přípravě. Průběžné výsledky byly prezentovány na konferencích HPCSE 2015, ICNAAM 2015 a SC 2015.

SEAMLESS TEXTURE SPACE DIFFUSION USING SKELETON TEXTURE MAPPING

Adam Riečický

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: a.riecicky@gmail.com

Our goal was to design and implement a procedure which uses skeleton texture mapping (STM) to improve results of texture-space diffusion algorithms. First step includes mesh and skeleton processing to extract vertex-node relations. Skeleton is afterwards divided into individual bones and assigned with parts of a mesh. Parametrizations for individual sub-meshes are then performed with bone placement taken into account. Result of this process are calculated texture coordinates for each vertex of the mesh. Original texture can be remapped into new STM coordinate texture. Such texture is be post-processed using our methods, and the result is used for texture-space diffusion. Using approach we propose should lead to diffused texture which does not include seam artifacts. The results presented for SVOČ 2016 were used in authors master's thesis. None of results were used in any other SVOČ or similar competitions.

AUTOMATIC BRAIN SEGMENTATION METHOD BASED ON SUPERVOXELS

Martin Tamajka

Fakulta informatiky a informačných technológií
Slovenskej technickej univerzity v Bratislave
e-mail: martin.tamajka@gmail.com

Medical image segmentation is an important part of medical practice. In this work we propose a fully automatic brain segmentation method based on oversegmentation and classification. We incorporate SLIC supervoxels to oversegment T1 MRI volumes into supervoxels, giving priority to intensity homogeneity before compactness. Generated supervoxels are described by novel features which are based on position of supervoxel centroid towards the brain centre. In addition to these features we describe supervoxels with their intensity histograms and intensity histograms based on their neighbours.

Supervoxels are classified by multilayer perceptron (MLP) with two hidden layers. In classification process we use priors based on intensity distributions of individual classes. In order to accelerate training process and increase segmentation success rate, we remove non-brain tissue in the preprocessing.

Thorough analysis forms a large part of this work. It supports choice of rather small, homogeneous supervoxels and values of parameters used in preprocessing for non-brain tissue removal.

In conclusion we compare our results with current state-of-the-art brain segmentation method using the same data and conclude that our results are clearly comparable.

The work consists of selected parts of author's Master's thesis. Two other papers based on this thesis were accepted to a research conference, too.

Sekce I4

APLIKOVANÁ INFORMATIKA A SOFTVÉROVÉ INŽENÝRSTVÍ

Porota

Radomil Matoušek (FSI VUT, Brno)
Michal Kompan (FIIT STU, Bratislava)
Róbert Špir (SvF STU, Bratislava)

PARALLEL GENETIC ALGORITHM ON MODEL-BASED
GAUSS CLUSTER ANALYSIS

Lukáš Csóka

*Fakulta informatiky a informačných technológií
Slovenskej technickej univerzity v Bratislave
e-mail: csoka.lukas@gmail.com*

This work deals with model-based Gaussian clustering and its parallelization possibilities. Model-based clustering can find clusters of elliptic shapes and smaller clusters embedded in larger ones. The paper presents several optimization criterions for model-based clustering, which are used as fitness functions in genetic algorithm. These optimization criterions are based on different properties of covariance matrices. The algorithms are parallelized using all cores of multi-core processors across multiple computers. It appears that the parallelization of genetic algorithm is very effective and scalable on many execution units. Our method is compared with the well-known method *K*-Means, that is solved by genetic algorithm and Particle Swarm Optimization, and we achieved better results. The analyzed data come from botany and astronomy. In my bachelor and diploma thesis I focus on improving data clustering and parallelization of this process.

CONSIDERING HUMAN VISUAL SEARCH ABILITIES
IN EYE TRACKING USER STUDIES

Mária Dragúňová

*Fakulta informatiky a informačných technológií
Slovenskej technickej univerzity v Bratislave
e-mail: majka.dragunova@gmail.com*

We present a method based on evaluation of participant's visual search ability through a calibration set containing visual search tasks, which should bring an improvement for the findability metrics. Our work is based on the natural diversity of human visual search abilities, which we evaluate not only by employing the standard visual search tasks, but also by our developed tasks, which contain icons from the web environment. This created evaluation of participant should be taken into consideration when analyzing measured metrics of a participant in a user study. Both of mentioned visual search tasks were parts of an eye tracking quantitative experiment, in which we collected usable data from 45 participants. We verify our proposal by computing correlation between our valuation of visual search abilities of participants and their measured values of findability metrics in search tasks on chosen websites.

This paper is written for SVOC competition. The work presented in the paper presents the author's bachelor thesis results. The work was presented at the Student Research Conference IIT.SRC 2016 organized by the Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava, where the best bachelor paper award for was conferred on the author.

DETEKCE PHISHINGOVÝCH ZPRÁV

Tomáš Duda

*Fakulta informačních technologií Českého vysokého učení technického v Praze
e-mail: dudatom2@fit.cvut.cz*

Bakalářská práce se zabývá detekcí phishingových zpráv v českém a anglickém jazyce. Popsány jsou různé formy phishingových útoků a charakteristické znaky phishingových zpráv. Práce popisuje různé přístupy, které se v současné době k potírání phishingu využívají a diskutuje jejich výhody a nevýhody.

Na základě zjištěných informací je navržen algoritmus detekce phishingových e-mailů, jenž je implementován v Javě. Uvedené řešení je založeno na abstrahování informací z příchozí zprávy do vektoru příznaků, pro který je následně metodami strojového učení rozhodnuto, zda reprezentuje phishingovou zprávu. Příznaky extrahované ze zpráv popisují klíčová slova a odkazy přítomné ve zprávách, shodu s charakteristickou strukturou phishingových zpráv a výstup existujících řešení pro detekci nevyžádané pošty. Testovány jsou různé podmnožiny příznaků a algoritmy pro tvorbu klasifikačního modelu. Podstatnou částí práce je modifikace těchto metod pro účely detekce česky psaných phishingových e-mailů.

Navržené řešení je testováno na korpusu složeném z reálných bezpečných i phishingových zpráv. Algoritmus dosahuje na anglicky psaných e-mailech přesnosti 99,0% a na česky psaných přesnosti 85,4%.

Hlavním přínosem práce je přenesení postupů pro detekci anglického phishingu na český phishing. Implementace řešení byla využita v rámci projektu pro odhalování nebezpečných e-mailů v síti CESNET. V soutěži SVOČ ani dalších podobných soutěžích dosud žádný z výsledků uplatněn nebyl.

DETEKCE BEZPEČNOSTNÍCH CHYB POMOCÍ
STATICKE ANALÝZY KÓDU**David Formánek**

*Fakulta informatiky Masarykovy univerzity v Brně
e-mail: 396518@mail.muni.cz*

Práce se zabývá automatickou statickou analýzou kódu a jejím využitím pro detekci třídy bezpečnostních zranitelností nazývaných jako injekce. Kromě nezbytné teorie je především popsána implementace mechanismu, který pomocí tzv. taint analýzy umožňuje tyto chyby detekovat v Java aplikacích. Tímto mechanismem bylo vybaveno rozšíření FindSecurityBugs pro volně dostupný nástroj FindBugs a vylepšení analýzy bylo ověřeno na testovací sadě Juliet. Jedná se o předběžnou verzi diplomové práce.

EFEKTÍVNE VYHLADÁVANIE VZOROV V ETL SÚBOROCH

Juraj Holas

Fakulta matematiky, fyziky a informatiky Univerzity Komenského v Bratislave
e-mail: holasjuraj@gmail.com

V tomto článku sa zameriavame na porovnávanie veľkého množstva špecifických zdrojových kódov za účelom ich následného zhlukovania. Naša práca zahŕňa dva hlavné aspekty; prvým je zefektívnenie výpočtu editačnej vzdialenosti dvojice súborov zavedením informovaného odhadu do Myersovho algoritmu. Druhým aspektom je zrýchlenie výpočtu vzdialenostnej matice, kde využitím metrických vlastností orezávame výpočty nepotrebných medzivýsledkov, čím sme ušetrili vyše 90% všetkých výpočtov. Implementáciou týchto zrýchlení sme vytvorili systém, ktorý dokáže vyhľadávať vzory aj v objemných ETL súboroch v priebehu niekoľkých sekúnd, nanajvýš minút.

Článok je zhrnutím mojej diplomovej práce a v apríli 2016 bol prezentovaný aj vo fakultnom kole Študentskej vedeckej konferencie na Fakulte matematiky, fyziky a informatiky Univerzity Komenského v Bratislave.

TESTOVACIE ÚDAJOVÉ SADY PRE BEZPEČNOSTNÉ TECHNOLOGIE

Martin Ilavský

Fakulta informatiky a informačných technológií
Slovenskej technickej univerzity v Bratislave
e-mail: ilavskymartinn@gmail.com

Informačná bezpečnosť je dôležitou súčasťou informačnej spoločnosti. Rokmi vývoja tejto oblasti vznikli viaceré princípy na detekciu a prevenciu kybernetických útokov. Jednou z možností ako sa pred týmito útokmi brániť, sú systémy detekcie prieniku, skrátene IDS. Účinnosť týchto systémov sa určuje podľa testovacích údajových sád, ktoré obsahujú rôzne simulované útoky. Existujúce údajové sady sú veľmi zastarané a preto sme sa rozhodli vytvoriť nové. V tejto práci sa venujeme možnosti vytvorenia takýchto sád pomocou voľne šíriteľných nástrojov na realizáciu útokov a analýze útokov obsiahnutých v týchto vygenerovaných sádach. Vytvorené sady sme otestovali na voľne šíriteľnom nástroji detekcie prieniku a porovnali sme ich s existujúcimi testovacími sadami.

APLIKÁCIA STOCHASTICKEJ REAKTÍVNEJ KINETIKY NA
MODELOVANIE REZISTENCIE BAKTÉRIÍ NA ANTIBIOTIKÁ**Alica Kačengová**

Prírodovedecká fakulta Univerzity Pavla Jozefa Šafárika v Košiciach
e-mail: alica.kacengova@gmail.com

Práca, ktorá vznikla v rámci prípravy bakalárskej práce, sa zaoberá modelovaním populačnej dynamiky bakteriálnych populácií v prostredí nemocničného ekosystému

ako Markovovského procesu, pričom na tieto predpovede využíva postupy stochastickej reaktívnej kinetiky. Vzniknutý model má za cieľ preskúmať okolnosti empiricky doloženého faktu obnovenia citlivosti baktérií na antibiotiká, ktoré boli vysadené z používania. Popisuje viacero možných scenárov na úrovni nemocnice a pacientov, pričom vychádza z experimentálne získaných dát zo stredne veľkej slovenskej nemocnice. Na vyladenie modelu sú použité techniky genetických algoritmov. Výsledkom práce je model popisujúci dynamiku vývoja rezistencie u baktérie *Staphylococcus aureus*.

PROBLÉM FAKTORIZÁCIE V ASYMETRICKEJ KRYPTOGRAFII ALEBO NAOZAJ SA RON MÝLIL?

Ján Kotrady

Prírodovedecká fakulta Univerzita Pavla Jozefa Šafárika v Košiciach
e-mail: kotrady.johnny@gmail.com

Faktorizovanie verejného modulu kryptografického systému RSA sa pred niekoľkými rokmi ukazovalo ako neriešiteľný problém, avšak v roku 2012 Lenstra a kol. poukázali na určité možnosti faktorizácie verejných modulov algoritmom najväčšieho spoločného deliteľa, spôsobené chybou v generátoroch náhodných čísel. Aj niekoľko rokov po objavení tohto problému je možnosť faktorizácie verejných modulov algoritmom najväčšieho spoločného deliteľa stále aktuálna a problém ako taký nie je v širšom zmysle stále vyriešený. Z pomerne malej množiny verejných modulov, ide o približne 1,2 milióna, sme boli schopní faktorizovať 65 verejných modulov o dĺžke minimálne 1024 bitov, čo predstavuje stále reálne riziko bezpečnosti informačných systémoch. Podarilo sa nám pritom faktorizovať niekoľko verejných modulov z protokolu SSH, dokonca aj z protokolu SSL a ukazuje sa, že PGP servery obsahujú pomerne vysoké množstvo chybné generovaných modulov z hľadiska dĺžky prvočísel. V práci sa venujeme spôsobu získavania dát, efektívnemu algoritmu výpočtu najväčšieho spoločného deliteľa, ale hlavne výsledkom výskumu faktorizácie, ktorý bol realizovaný na vzorke približne 1,2 milióna verejných modulusov. Ďalej sme skúmali vzťahy medzi jednotlivými faktorizovanými verejnými modulmi a pritom sme poukázali na vzťah medzi faktorizovanými verejnými modulmi a zariadeniami, ktoré tento chybný modul obsahujú, ako aj na ich spoločné vlastnosti a špecifikácie. Zisťovali sme taktiež aj vzťah medzi vlastníctvom zariadení, respektíve vlastníctvom IP adries týchto zariadení, ktoré boli faktorizované a faktorizovanými verejnými modulmi, pričom sme dospeli k záveru, ktorý nám len potvrdzuje doterajšie dohady ohľadne problému faktorizácie algoritmom najväčšieho spoločného deliteľa. Zároveň sme sa snažili zodpovedať na otázku, či sa naozaj Ron Riverst so svojím kryptografickým systémom RSA mýlil. Naším výskumom sme poukázali na fakt, že problém faktorizácie algoritmom najväčšieho spoločného deliteľa v kryptografickom systéme RSA je stále veľkým bezpečnostným rizikom informačných systémov.

IMPLEMENTÁCIA ALGORITMU NÁSOBENIA MATÍC NA GPGPU S OPTIMALIZÁCIOU PRENOSU ÚDAJOV

Miroslav Kováč

Fakulta prírodných vied Univerzity Mateja Bela v Banskej Bystrici
e-mail: 1991kovac.miroslav@gmail.com

In this paper we present a thorough experience on tuning double-precision matrix-matrix multiplication (DGEMM) on the Kepler GPU architecture. In early beginning of using matrix-matrix multiplications on GPU, we found that data transfer is taking a considerable amount of time. Reducing this time would significantly help to get results of multiplication. In this paper we focus on the problem of reducing time spent in copying data. We present an optimal algorithm with data transfer optimization. Our optimization strategy is further guided by a performance modeling based on benchmarks. We constructed a functional method that can be used in any CUDA program. Our optimization includes using asynchronous methods on every mathematic operations and Strassen algorithm for operations on divided matrices. Transferring data while making some other operations is the key part of speeding up the performance. The best CUDA algorithm that we created outperforms algorithm from the CUBLAS library. We received 26% increase in speed performance in average.

BEACON BASED LOCALIZATION REFINED BY OUTPUTS FROM MOBILE SENSORS

Matej Liskovec

Fakulta informatiky a informačných technológií
Slovenskej technickej univerzity v Bratislave
e-mail: matej.liskovec@gmail.com

In internal navigation with an emphasis on accuracy has become a highly desirable today. Since GPS does not work inside buildings. Therefore, researchers are looking for alternative approaches. On the other hand, mobile devices have become high-performance devices with sensors that allow mobile devices to integrate important functionality. The paper deals with Bluetooth technology, discusses Beacon transmitters as an appropriate means for the needs of indoor navigation. The paper also presents method applicable for the purposes of internal navigation using a combination of Beacon transmitters and mobile sensors. Method has two main parts. The first part deals with calculating the user's localization in the building using trilateration, respectively multilateration. The second part of the method serves to validate the first part. This part using mobile sensors for evaluating. At work, we experimented with different input parameters to achieve higher accuracy.

HĽADANIE OPTIMÁLNYCH CIEST V ROZVETVENÝCH ŠTRUKTÚRACH

Martin Sokolovský

Stavebná fakulta Slovenskej technickej univerzity v Bratislave
e-mail: soky314@gmail.com

Práca sa zoberá automatickým vyhľadávaním ciest v rozvetvených štruktúrach, ktoré sú hladké, idú stredom oblasti a sú asymptoticky rovnomerne rozdelené. V práci bola využitá predovšetkým literatúra týkajúca sa hľadania najkratších ciest, výpočtu vzdialenostných funkcií a pohybu kriviek. Medzi naštudovanou literatúrou bola práca venujúca sa hľadaniu ideálnej cesty pre kameru virtuálnej kolonoskopie, prezentovaná okrem iného aj na ČS SVOČ v roku 2010. Tieto myšlienky boli použité a rozšírené pre algoritmus na automatické hľadanie ciest v rozvetvených štruktúrach s jednoduchou topológiou. Navrhnutý algoritmus bol následne implementovaný v jazyku C++ pre 2D prípady. Nakoľko sa uvažovalo o využití algoritmu v reálnych aplikáciách bol algoritmus definovaný všeobecne. Vstupom programu sú dáta s vysegmentovanými štruktúrami, v ktorých sa má hľadať cesta. Výstupom navrhnutého algoritmu sú rozvetvené cesty, reprezentované diskretnými bodmi. Cesty získané ako výstup algoritmu by v 3D prípadoch mohli byť použité pre virtuálnu bronchoskopiu, angioskopiu, ale i kolonoskopiu. Taktiež sú využiteľné aj v iných oblastiach, napríklad v robotike.

ROS AND FILTERING DATA FROM SENSORS

Marek Súkeník

Fakulta prírodných vied Univerzity Mateja Bela v Banskej Bystrici
e-mail: m45sukenik@gmail.com

The aim of this article is to introduce to a reader system ROS (Robotics operating system) and its use. Firstly, we are going to talk about what ROS is and how it was created. Secondly, we are going to talk about the structure of this system and basic principles of its application. Then, we are going to talk about Kalman's filter algorithm. In the end, we will combine our knowledge with an arduino microcontroller and with sensors and we will filter the data we get from sensors.

THE USAGE OF LEVENSHTAIN DISTANCE IN INTRUSION DETECTION ON WEB SERVER

Štefan Šmihla

Fakulta informatiky a informačných technológií
Slovenskej technickej univerzity v Bratislave
e-mail: morzeux@gmail.com

In current time, when web servers are on the rise, there is a growing attraction for potential attackers. As a number of attacks and other unwanted activities are on

a rise, the problem of web security has become a very important research topic. This work focus on how to improve existing web application firewalls and intrusion detection systems by adding an additional security layer. We propose unique anomaly and misuse detection method based on a Levenshtein distance algorithm, which we would like to use to determine if HTTP request to the server has malicious intend.

MNOHOROZMERNÁ ANALÝZA ROZVRHOVANIA
VO VYSOKOVÝKONNÝCH POČÍTAČOVÝCH SYSTÉMOCH

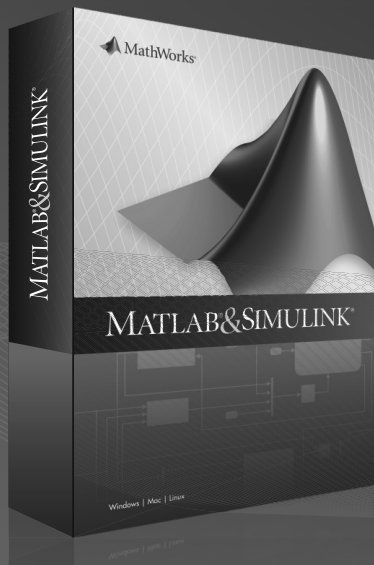
Martin Trník

Fakulta prírodných vied Univerzity Mateja Bela v Banskej Bystrici
e-mail: trnik.martin@gmail.com

The paper deals with analysis of scheduling in Clusters for High Performance Computing (HPC). Clusters for HPC are very important parts of scientific workplaces. They offer powerful computing power and capacious storages. In the article, we are analysing one of these systems. We focus on finding the best schedule for this system in view of the lowest power consumption of the system. Power consumption data are based on measurement from system Zabbix. We also have data about executed jobs from TORQUE logs. Hadoop system and MapReduce framework are used for analysing the data. We make analysis of this job, we design a solution and, finally, we create three Java MapReduce programs in which we parse the input data and find the best distribution of jobs on nodes of the cluster in view of the lowest power consumption. For visualization of the result of analysis we use Tableau.

Jmenný rejstřík

- Adamčíková Katarína, 15
Ajdarow Michal, 42
Balajka Pavol, 52
Bathory Michal, 11
Bezek Matúš, 28
Blaschke Róbert, 33
Blažej Václav, 42
Brabcová Eva, 11
Brzicová Marta, 42
Budzáková Paula, 52
Buriánková Eva, 11
Csóka Lukáš, 58
Čekanová Katarína, 28
Čoupek Pavel, 23
Dostalík Mark, 37
Dragúňová Mária, 58
Dresslerová Anna, 43
Duda Tomáš, 58
Falath Juraj, 15
Filippi Michal, 48
Finger Richard, 16
Formánek David, 59
Fratrich Peter, 29
Gábriš Martin, 44
Holas Juraj, 60
Hrapková Lenka, 33
Chlubnová Tereza, 16
Chovan Roman, 52
Ilavský Martin, 60
Jariabka Ondrej, 52
Kačala Viliam, 53
Kačengová Alica, 60
Klinkovský Jakub, 37
Klučárová Miroslava, 48
Korbaš Rafael, 44
Kotrady Ján, 61
Kouřilek Matěj, 21
Kováč Miroslav, 62
Koňasová Kateřina, 16
Krajňáková Ivana, 44
Kružík Jakub, 33
Krásenský Jakub, 23
Kubelka Vít, 20
Kunovský Pavol, 53
Kuruczová Daniela, 17
Liskovec Matej, 62
Malý Matej, 17
Maták Timotej, 53
Medková Kateřina, 45
Mihala Patrik, 38
Minarčík Jiří, 38
Mrázek Michal, 39
Murín Ján, 54
Nedelová Mária, 29
Novotná Daniela, 18
Oustrata Michal, 21
Pažický Branislav, 52
Pecha Marek, 55
Pravec Vojtěch, 12
Páleník Jakub Jozef, 54
Pápay Ladislav, 46
Púček Roland, 23
Riečický Adam, 56
Rubín Tomáš, 19
Sedláková Jana, 24
Smejkal Tomáš, 39
Sokolovský Martin, 63
Sosnovec Jakub, 29
Straková Erika, 34
Střelský Jakub, 48
Suchý Ondřej, 42
Svoboda Tomáš, 25
Súkeník Marek, 63
Šimek Juraj, 49
Šimková Mária, 34
Šimon Prokop, 19
Šmihla Štefan, 63
Šuppa Marek, 50, 52
Švígler Vladimír, 12
Tamajka Martin, 56
Tinková Magdaléna, 25
Trník Martin, 64
Tóth Michal, 39
Uhrík Dávid, 12
Vacková Jana, 19
Valla Tomáš, 42
Velká Tereza, 30
Veselý Vojtěch, 30
Vodička Martin, 26
Výboštok Miroslav, 13
Zeman Peter, 46



MATLAB[®] & SIMULINK[®]

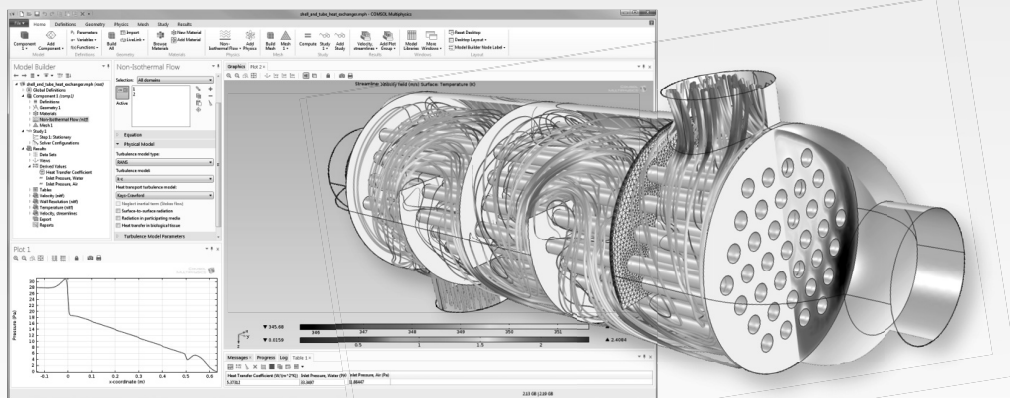
Jak Vám může pomoci?

Mnohem více než očekáváte.

Integrované prostředí pro vědeckotechnické výpočty, modelování, návrhy algoritmů, simulace, analýzu a prezentaci dat, paralelní výpočty, měření a zpracování signálů, návrhy řídicích a komunikačních systémů.

TEPELNÝ VÝMĚNÍK slouží k ochlazení či ohřevu tekutin v ropných rafineriích. Obrázek ukazuje výpočet rozložení teploty a tlaku uvnitř výměníku a určení koeficientu přestupu tepla.

COMSOL
MULTIPHYSICS[®]



COMSOL Multiphysics je inženýrský nástroj určený k modelování a simulaci fyzikálních dějů. Program pomáhá snáze pochopit a rychle analyzovat jevy reálného světa, dokáže proniknout do podstaty navrhovaných výrobků či procesů a tím nejen zkracuje vývojový cyklus prototypů, ale i výrazně šetří náklady.

Měřicí karty

I/O zařízení pro Thunderbolt, PCIe, PCI

Systemy dSPACE

simulace v reálném čase

Výukové modely

pro výuku teorie řízení

zjistěte více na www.humusoft.cz



Humusoft s.r.o.
Pobřežní 20, Praha 8

E-mail: info@humusoft.cz
Tel: +420 284 011 730



LEARN WITH RED HAT

on campus or at work

**RED HAT GIVES YOU THE FREEDOM TO EXPRESS YOUR OPINIONS
AND THE CHANCE TO MAKE AN IMPACT.**





Red Hat is the world's leading provider of open source enterprise IT software, offering solutions for cloud, virtualization, storage, Linux®, and middleware. But we're more than a software company. We are the bridge between the communities that create open source software and the enterprise customers who use it. We make rapidly innovating open source software consumable for mission-critical, enterprise environments.

RED HAT OFFERS STUDENTS:

- > free technical guidance and topics for diploma and bachelors' theses: diplomky.redhat.com
- > local university courses led by Red Hatters
- > Red Hat labs, where you can work on open source projects: research.redhat.com
- > internships, part-time, and full-time jobs in our Brno office

> Find a job or internship: redhat.com/jobs

WE ARE
RED HAT
ON CAMPUS

follow Life at Red Hat    

Maderic



Vína, která nenajdete u hlavní
cesty, neb pro to dobré se
vyplatí vydat se dál.

www.vinarstvimaderic.cz

